CICM Performance Management

This document provides the performance management strategy and procedures for Centrex IP Client Manager (CICM) nodes (gateways) and their element managers (CICM-EMs). This document is part of the CICM customer documentation suite. The complete list of documents in the suite is identified in *CICM Basics*, NN0044-111.

Performance management includes these topics:

- What's new for performance management
- Performance management overview
- What's new for performance management
- Operational Measurements
- Performance management procedures
- IEMS with CICM and CICM-EM nodes
- Performance metrics

What's new for performance management

For SN08, the changes to this document include the following:

- changed the value of provisionable lines for SAM16 in the table CICM capacity attributes
- changed the threshold of the BHHCA critical alarm
- changed all occurrences of Windows NT to Windows XP, especially in Software resilience
- added SAM16 information throughout the document
- deleted the Microsoft procedure "Use MS Performance Monitoring" (Perfmon), which is no longer supported

Performance management overview

Operational Measurements (OMs) define measurement criteria. Office Parameters set OMs collections and reporting criteria.

Office parameters are initially set by Nortel to meet design criteria and switch configuration. Service providers can provision performance management on the Centrex IP Client Manager (CICM) by configuring Office Parameters for OMs on all element managers (EMs).

Capacity and performance limitations

CICM 8.0 supports up to 8 pairs of CPN5385 CPU cards per SAM21 shelf and one pair of CPV5370 CPU cards per SAM16 shelf. Each pair's capacity limits are identified in the table CICM capacity attributes.

Table 1 CICM capacity attributes

Capacity attribute (maximum)	SAM16 platform (CPV5370)	SAM21 platform (CPN5385)
Provisionable lines	1,023	3,069
Simultaneous Terminal Sessions	2,500	4,096
Historical Terminal Entries	10,000	10,000
Simultaneous Active Half-Calls	512	3,069
BHHCA	7,200	21,600
RUDP Messages/Sec	500	500
H.248 Messages/Sec	100	250

The definitions of these attributes are as follows.

- **Provisionable Lines**
  The maximum number of lines (a CICM line corresponds to a LEN on the CS2000). This represents the number of users that a CICM node can accommodate.

- **Simultaneous Terminal Sessions**
  The maximum number of terminals that can be connected and presented with a login prompt by the CICM node at any given time. A user that logs into a joint session uses 2 session resources on the

CICM node. Therefore, on a CPN5385-based CICM, the value 4,096 could be interpreted as allowing all provisioned users (lines) to connect at least one terminal, but allowing 1,000 of these users to login as a joint session. However, the system does not enforce this, so it is possible that 1,000 + n (number of users) could have 2 of their terminals connected to the CICM node, thus preventing N users connection to a terminal.

- **Historical Terminal Entries**
  As a new terminal connects to the CICM node, information about the terminal is automatically added to the CICM MIB (that is, firmware load, etc). As each terminal identifies itself uniquely to the CICM node, it is possible to ensure that the same entry is re-used when this terminal connects again.

  Each new terminal that has never connected to a CICM node generates a new entry in the MIB. However, since this configuration data uses memory resources, there is a limit to the amount of historical information that is saved on the CICM node. When this maximum is reached, additional new connections are denied access until other entries are cleared manually using the CICM-EM. When this maximum is reached, an alarm is raised.

  This limit also represents the maximum number of terminals that can be serviced by a single enterprise profile.

  It is recommended to remove the historical terminal entry for terminals that are removed from the network to conserve memory resources.

- **Simultaneous Active Half-Calls**
  The CICM node knows only about half-calls. Even if the second half of a call is also hosted by the same CICM node, the CICM has no knowledge of this and treats them as independent call halves.

  The number of simultaneous half-calls represents the maximum number of half-calls that can be established at any one time by the CICM node. Once the maximum is reached, new call attempts (incoming or outgoing) are denied.

  Any single terminals can support up to eight simultaneous active call halves, using various features such as multiple DNs, call hold, etc.

- **BHHCA**
  Busy Hour Half Call Attempts (BHHCA) represents the maximum rate at which half call attempts can be made per hour. Once the BHHCA reaches 80% of the set value, a minor alarm is raised. At 100%, a major alarm is raised, and at 150% a critical alarm is raised and no additional calls are permitted. The critical alarm clears automatically once the BHHCA drops to below 100% for more than

5 minutes. The major alarm is cleared once the BHHCA drops to below 80% for 5 minutes. The minor alarm clears once BHHCA drops below 80% for 15 minutes.

- **RUDP Messages/Sec**
  Reliable User Datagram Protocol (RUDP) is the transport mechanism for the UNIStim protocol. UNIStim is the protocol used for all messaging between the CICM node and its terminals. The incoming message rate is throttled to prevent the CICM node from becoming overloaded.

- **H.248 Messages/Sec**
  H.248 is the messaging protocol used between the CICM node and the GWC. Similarly the incoming message rate (from the GWC) is throttled to prevent the CICM node becoming overloaded.

Traffic loading

Release SN08 supports the following capacities for either the SAM16 (CPV5370) or the SAM21 (CPN5385) platforms:

- per CICM node resource card pair:

  — subscriber line provisioning capacity for SAM21 is 3,069 and SAM16 is 1,023

  — BHHCA is 21,600 for SAM21 and 7,200 for SAM16

  — active calls is 3,069 for SAM21 and 512 for SAM16

- scalable solution by adding more CICM node resource cards

- one pair of CICM-EM cards is needed for CS2000

  — able to support up to 100 CICM resource card (node) pairs

- per gateway controller (GWC) resource card pair:

  — subscriber line provisioning capacity is 8,200

  — BHHCA is 38,000

Architectural resilience

Each CICM node pair is partitioned into two identical independent physical nodes: Node A and Node B, one card per node. The CICM node uses a SAM21 hardware platform with dual cPCI backplane.

The two CICM nodes for a SAM16 hardware platform are contained in two half shelves. There is one pair of CPV5370 CPU cards per shelf. Each CICM node, or half shelf, having one CPU card and a hot swap controller card.

Towards the GWC, the two cards present themselves as a single network entity (one CPU is the master, the other is a hot-standby slave).

The terminals are configured with one IP address which fails over to the other node when a failure or maintenance occurs.

The redundancy of node pairs allows the CICM or CICM-EM to react promptly to a node failure by switching all terminals to the remaining active node with minimal service loss. With CPN5385 CPU cards, redundancy for the CICM and CICM-EM node pairs can be increased by installing them onto different SAM21 shelves.

With CPV5370 CPU cards, redundancy for the CICM and CICM-EM node pairs is achieved by installing them onto the same SAM16 shelf.

Software resilience

The CICM nodes use Microsoft Windows XP as their operating system, while the CICM-EM uses Microsoft Windows 2000.

Operational Measurements

Operational Measurements (OMs) provide information on the performance of the components of the network. Periodic scans of network components and activities result in the collection, storage and transmission of data. Operating company personnel set the office parameters that define the way OMs are collected, stored, transmitted and reported.

The types of OMs are: Event OMs, Usage OMs, and High Watermark OMs.

- **Event OMs** are incremented each time a predetermined event occurs. These events are predefined in the software.

- **Usage OMs** are incremented at preset intervals if the appropriate device is in use. These registers are pre-defined in the software.

- **High Watermark OMs** measure the highest level of usage within a set time interval.

The OMs, and especially the High Watermark OMs, can be used as a benchmark of the levels of traffic-dependent activity on the switch during the current interval.

For additional OM information and the reasons for incrementing each register, refer to the document *CS2000 Operational Measurements Reference Manual*.

Performance management procedures

This section provides these procedures for viewing performance measurements:

- Viewing CICM OMs
- Viewing CICM node status and statistics
- Viewing connections, terminals, and packets performance statistics
- Viewing chassis components status

Viewing CICM OMs

View CICM operational measurements (OMs) using the command OMSHOW which displays or prints a report for the specified OM group.

The Active class of OMs contains the OM groups that are current for the software load. The Holding class of OMs contains the OM groups for the previous measurement cycle.

At the LMM Interface

1 To view the current 15 minute operational measurements for the peripheral modules, type:

OMSHOW LMD ACTIVE

then press Enter.

Where

    LMD

        is the OM group that provides traffic information for the peripheral modules (PM).

Response: Display of all remote units on the CS2K, each with an index number before its name.

    Note: To show the OMs for a specific remote unit, add the index number after the entry.

        Example
        OMSHOW LMD ACTIVE 2

2 To view the previous 15 minute measurements, type:

OMSHOW LMD HOLDING

then press **Enter**.

3 This procedure is complete.

Viewing CICM node status and statistics

View the following CICM node status and statistics for each node:

- Node status (master or slave)

- Service status (running or idle)

- Node maintenance status

  — current reboot count

- Version (of the software running on the node)

- Terminal service status (**started**, **stopped**, or **shutting down**)

- Number of logged in users (total login count)

- Number of active terminals

  — Details of terminal login statistics show the type of terminals

- Number of active calls (total call count)

At the CICM-EM home page

1   On the **CICM home** page, select the CICM node to view from the drop-down menu in the right navigation menu, then click on the **view the status of the following CICM** text.

Response: The ***<cicm_name> cicm status*** *page opens.*

2   Click on **perform maintenance on <cicm_name>** on the right menu.

*Response: The **maintenance status <cicm_name>** page opens.*

3   Scroll down the **maintenance status <cicm_name>** page to view the status and statistics for each node.

4   To reset the **Current Reboot Count**, the **Total Login Count** or **Total Call Count**:
In the **reset counter** on the right menu bar:

    a   select the node,

  b then select the counter from the drop-down menu

  c then click on the **reset counter** text

Response: The selected counters will reset.

> ***Note:*** The **Line Login Count** and **Total Call Count** statistics are automatically reset when the node reboots.

5   This procedure is complete.

Viewing connections, terminals, and packets performance statistics

View the performance statistics on each CICM node.

At the CICM-EM web pages

1 At the **CICM home** page, select the CICM to view from the drop-down menu in the right navigation menu, then click on the **view the status of the following CICM** text.

*Response: The **<cicm_name> cicm status** page opens.*

2 To view the connections statistics, under **performance monitoring** on the right menu, select **Connections** from the drop-down menu, then click on **performance monitoring**.

*Response: The **Connections** section opens in the **<cicm_name> cicm status** page.*

3 To view the terminals statistics, under **performance monitoring** on the right menu, select **Terminals** from the drop-down menu, then click on **performance monitoring**.

*Response: The **Terminal login statistics** section opens in the **<cicm_name> cicm status** page.*

4 To view the packets statistics, under **performance monitoring** on the right menu, select **Packets** from the drop-down menu, then click on **performance monitoring**.

*Response: The **Packet rates statistics** section opens in the **<cicm_name> cicm status** page.*

5 This procedure is complete.

Viewing chassis components status

View the chassis components status for a CICM node.

At the CICM Home page

1   From the drop-down menu of **view the status of the following cicm**, select the CICM node to view.

*Response: The **<cicm_name> cicm status** page opens.*

2   Click on **view status of chassis components** on the right menu.

*Response: The **<CICM_name> cicm status** page updates to display the chassis components details.*

3   Scroll down the **chassis components for <cicm_name>** section of the **<cicm_name> cicm status** page to view the card and fan status and CPU temperature.

4   This procedure is complete.

IEMS with CICM and CICM-EM nodes

The Integrated Element Manager System (IEMS) is an interface in the Carrier Voice over IP (VoIP) network which gives access to the alarms and logs for a network element. The IEMS is accessed using a GIU, and it also interacts with the CICM-EM GUI.

The CICM-EM integrates with the IEMS. The CICM alarms, logs, and performance metrics are formatted to be compatible with IEMS.

Both the CICM and the CICM-EM nodes can raise alarms and faults to the IEMS. The CICM-EM raise alarms associated with the EM Platform (for example, memory shortage), and communicate with the CICM nodes that it manages, but does not have knowledge of the alarms and faults generated by the CICM nodes. Each CICM node sends alarms as SNMP traps directly to the IEMS such that the CICM-EM is unaware of the alarms.

The figure CICM fault architecture provides an overview of the CICM fault architecture.

Figure 1 CICM fault architecture
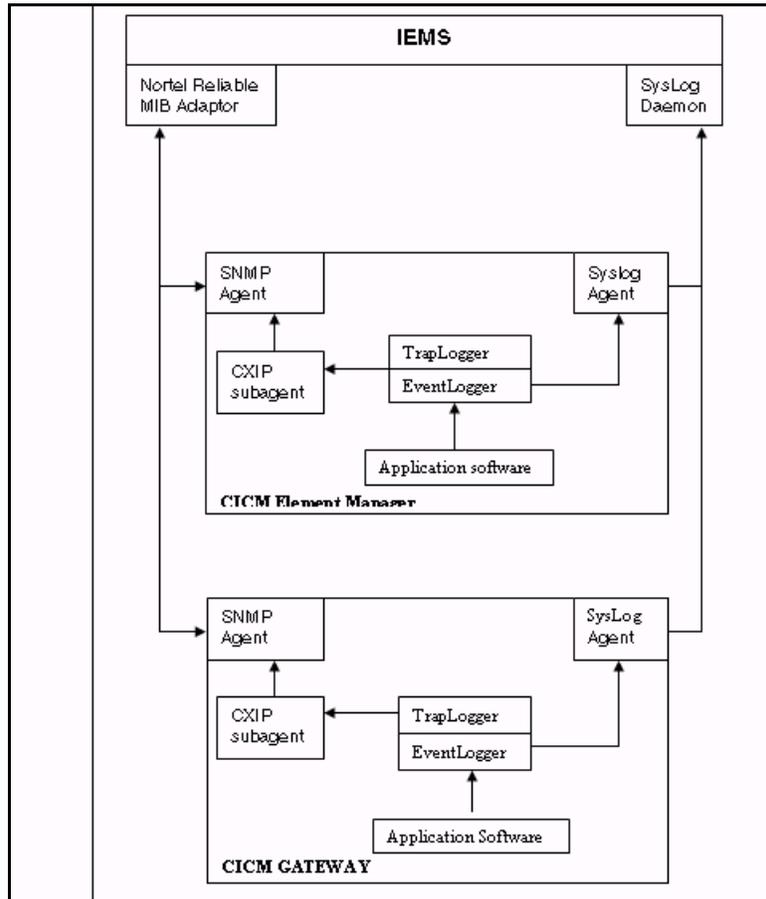
The figure CICM performance architecture shows the elements of the CICM Performance architecture.

17

Figure 2 CICM performance architecture
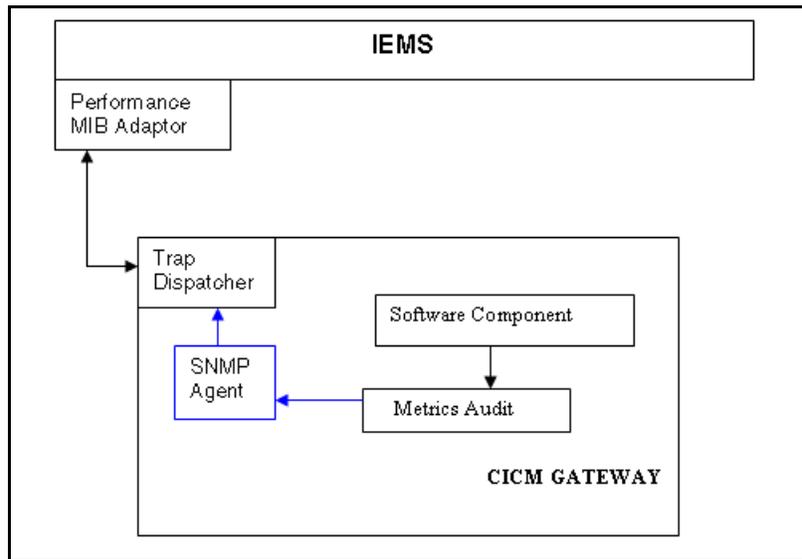
Alarms

All alarms are sent to the IEMS as an SNMP trap, and as a log to SYSlog. Each trap sent from the CICM incorporates the following information:

- Sequence number
- Severity indicator
- Component ID
- Category of alarm
    — communications
    — quality of service
    — processing error
    — equipment
    — environment
- Notification ID
- Description
- Time stamp
- Probable cause
- Specific problem
- Correlation ID list

The alarm severity is classification is shown in the figure Alarm severity.

Figure 3 Alarm severity

	Critical	Major	Minor	Warning
Service Affecting	Yes	Yes	No (or few affected)	No
Action required	Yes	Yes	Yes	No
Recommended Timeliness of Action	Immediately – drop everything	Rapidly – in next work shift	Soon – could be delayed until next day	Later – investigate if reoccurance
Target Reporting time	Within 2 Sec	Within 30 Sec	Within 2 Min	Within 5 Min

Fields which are valid for alarm raises are:

* nortelNMIcurrentTxNotificationSequenceNum
* nortelNMIalarmComponentId
* nortelNMIalarmCategory
* nortelNMIalarmNotificationID
* nortelNMIalarmDescription
* nortelNMIalarmTimeStamp
* nortelNMIalarmProbableCause
* nortelNMIalarmSpecificProblem
* nortelNMIalarmCorrelationIdList
* nortelNMIalarmNeVendorSpecificInfo
* nortelNMIalarmTechnologySpecificInfo

Fields which are valid for alarm clears are:

* nortelNMIcurrentTxNotificationSequenceNum
* nortelNMIalarmComponentId
* nortelNMIalarmDescription
* nortelNMIalarmTimeStamp
* nortelNMIalarmCorrelationIdList

Component IDs

The CICM is divided into the following objects for reporting alarms:

* the CICM Element Manager (CICM-EM)
* a CICM node
* the platform which the CICM-EM and the CICM nodes use

These objects contain sub-objects which, appended together with the alarm type, form the Component ID (as shown in the figure Component IDs).

Figure 4 Component IDs

Object	Sub Object	Component Id
CICM element manager	Node (CICM)	CICMEM<NN>;CICMEM.NODE.<cicmID+node>
	General	CICMEM<NN>;CICMEM.GENERAL.<cicmID+node>
CICM node	User	CICM<NN>;CICM.USER.<user id>.<event>
	Terminal	CICM<NN>;CICM.TERMINAL.<Terminal id>.<event>
	Endpoints	CICM<NN>;CICM.EP.<Endpoint Number>.<event>
	Network Transport	CICM<NN>;CICM.NET.<event>
	VMG	CICM<NN>;CICM.VMG.<VMG id>.<event>
	General	CICM<NN>;CICM.GENERAL.<event>
CICM platform	User	CICM[EM]<NN>;CICMP.USER.<event>
	Console	CICM[EM]<NN>;CICMP.CON.<event>
	Network connections	CICM[EM]<NN>;CICMP.NET.<event>
	Mate node	CICM[EM]<NN>;CICMP.MATE.<event>
	Chassis	CICM[EM]<NN>;CICMP.CHAS.<event>
	Cards	CICM[EM]<NN>;CICMP.CARD.<card number>.<event>
	Logs	CICM[EM]<NN>;CICMP.LOGS.<event>
	Software Component	CICM[EM]<NN>;CICMP.SW.COMP<component number>
	Configuration database	CICM[EM]<NN>;CICMP.CONF.<event>

Logs

Both the CICM nodes and the CICM-EM are responsible for sending their logs to the IEMS. Logs are not exchanged between the CICM and CICM-EM.

Logs are sent to the IEMS using CUSTLOG or security log formats through a syslog agent. Three log streams are used to send logs to up to three different syslog daemons (that is, IEMS). This is a change from previous CICM releases, where all logs were stored on the CICM. In (I)SN08, logs are still stored on the CICM, but the CICM also sends logs to CUSTLOG, Audit Log, and Security Log streams.

Note: Each log is formatted specifically for each of the three streams.

The CICM uses the syslog protocol to send logs to the IEMS. The CICM and CICM-EM both act as log senders. They are only able to send syslog messages; they are not able to receive or relay syslog messages. UDP port 514 (the syslog port) is used to send the syslog messages to the IEMS. The log packet must be no greater than 1024 bytes.

Custlog

The CICM logs the following events using the custlog format, and output the logs to the custlog stream.

- Service affecting state changes

- Specific customer/blm requested events

- Data corruptions/data mismatches

- Shutdown and restart of processes

Security logs

Security Logs are generated from the CICM nodes as follows:

- upon successful/unsuccessful login from an IP Phone or m6350 Softclient

- logout from an IP Phone or m6350

Security Logs are generated from a CICM-EM as follows:

- upon launching CICM-EM from IEMS

The CICM logs the following events using the security log format and output the logs to the security log stream.

- Unsuccessful terminal logins

- Successful terminal logins

Audit logs

Audit logs are generated from the CICM on executing flow-through commands at OSSGATE (for example, ado, deo, etc).

The audit logs are in the same format as the security logs. The following actions are logged to the audit stream:

- All configuration changes made by the CICM-EM administrator. (for example, adding CICM nodes)

- All mtc actions performed by the device (for example, restarts)

Debug logs

Debug logs are used by Nortel support personnel only; not the service provider. Debug logs are not changed in (I)SN08, but they can now be viewed using the CICM-EM web page interface. Debug logs are not sent through syslog to the IEMS.

Performance metrics

Performance metrics are generated by both the CICM nodes and the CICM-EMs. They are passed northbound into the IEMS, where they are

available for display and are aggregated with other IEMS southbound feeds into a single OSS feed.

The CICM node and CICM-EM gather the following metrics:

- Percentage Memory usage
- Percentage Disk C Usage
- Percentage Disk D Usage
- Number of Active Users
- Number of Active connections
- Percentage CPU Usage
- Number of Busy hour call attempts
- Number of logged in users
- Number of failed call attempts
- Messaging throughput

Each of these metrics is collected, averaged over a specified time interval, and stored in the MIB. Measurements relating to call traffic are taken every 5 minutes. Other measurements are collected and averaged over either 15 or 30 minute intervals. This 15 or 30 minute period is configurable.

The metrics are transferred in the standard Carrier Voice over IP (VoIP) performance MIB. Each metric contains:

- the instance of the object (for example, SAM21 x blade y)
- the property of the object being reported (for example, processor occupancy)
- the type of the property (for example, gauge)
- the value (for example, 22%)