Performance management

Performance management overview

Service providers can provision performance management on the Centrex IP Client Manager by configuring Office Parameters for Operational Measurements (OMs) on all element managers. Office Parameters set OMs collections & reporting criteria.

Office parameters are initially set by Nortel Networks to meet design criteria and switch configuration.

Traffic loading

Series 7.0 supports one or more pairs of CPN5385 CPU cards or 5370 cards per shelf.

Series 7.0 CICM has the following capacity limits:

- Per CICM resource card pair:
  - 3,069 subscriber line provisioning capacity for the 5385 platfor, and 1023 for the 5370 [platform
  - 21,600 BHHCA for the 5385 platform, and 7,200 for the 5370 platform
  - 3,069 active calls
- Scalable solution by adding more CICM resource cards
- One pair of CICM-EM cards is needed for CS 2000
  - Able to support up to 100 CICM resource card pairs
- Per GWC resource card pair:
  - 8,200 subscriber line provisioning capacity
  - 38,000 BHHCA

For more capacity information refer to:
http://livelink-ott.ca.nortel.com/livelink/livelink.exe?func=ll&objId=8715441&objAction=browse&sort=name

Any single terminal can support up to eight simultaneous active call halves, using functionality such as multiple DNs and call hold. Acting as a slave processor to the core and GWC in the CS2k network, the CICM performance cannot accurately be measured in BHCA. The CICM only has knowledge about half calls, the other half of the call, even if it is hosted from the same CICM, is made anonymous by the CS2k and GWC.

Architectural resilience

The CICM node is partitioned into two identical independent physical nodes: Node A and Node B. The CICM uses a SAM 16 hardware platform with dual cPCI backplane.

The two CICM nodes 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 warm-standby slave). The terminals are configured with the address of both CPUs. The terminal will failover between them when a failure occurs.

The resulting flexibility allows the CICM to react promptly by adjusting itself to operation in failure conditions, thus ensuring the overall impact on the service provided is kept to a minimum.

Software resilience

The CICM uses Microsoft Windows NT Embedded Server Version 4.0 as its operating system. This is a highly specialized version of Windows NT which is suitable for high availability applications.

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.

There are three types of OMs: 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 CS2000 documentation *CS2000 Operational Measurements Reference Manual*.

Performance management procedures

This section provides procedures for viewing performance measurements.

View OMs (OMSHOW)

The OMSHOW command causes the system to display or print a report for the OM group specified.

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.

Procedure 1 View CICM OMs

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.

View CICM node status and statistics

Use this procedure to view the following CICM status and statistics for each node:

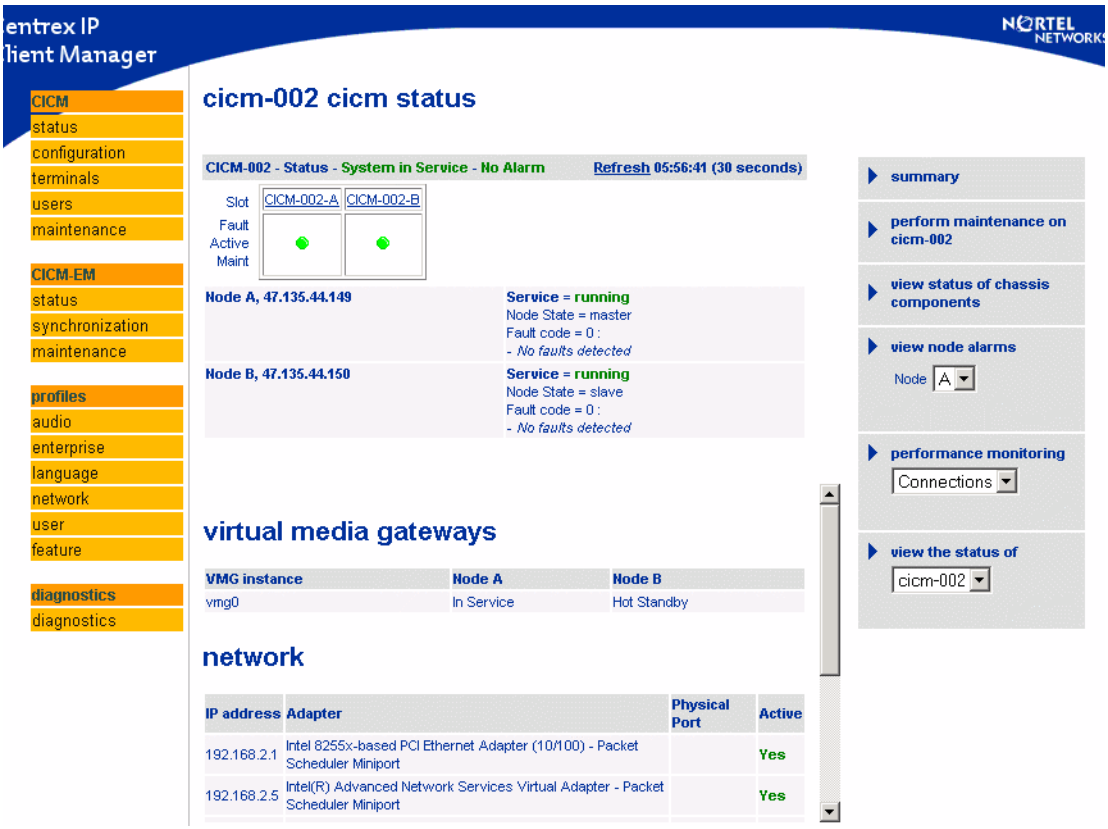
- Node status (dual node: master or slave)
- Service status (running or idle)
- Node maintenance status
  - current reboot count
- Version (of the software running on the node)
- Terminal service status (**started**, **stopped**, or **shutting down**)
- Number of logged in users (total login count)
- Number of active terminals
  - Details of terminal login statistics show the type of terminals
- Number of active calls (total call count)

Procedure 2 View CICM gateway statistics

At the CICM EM home page

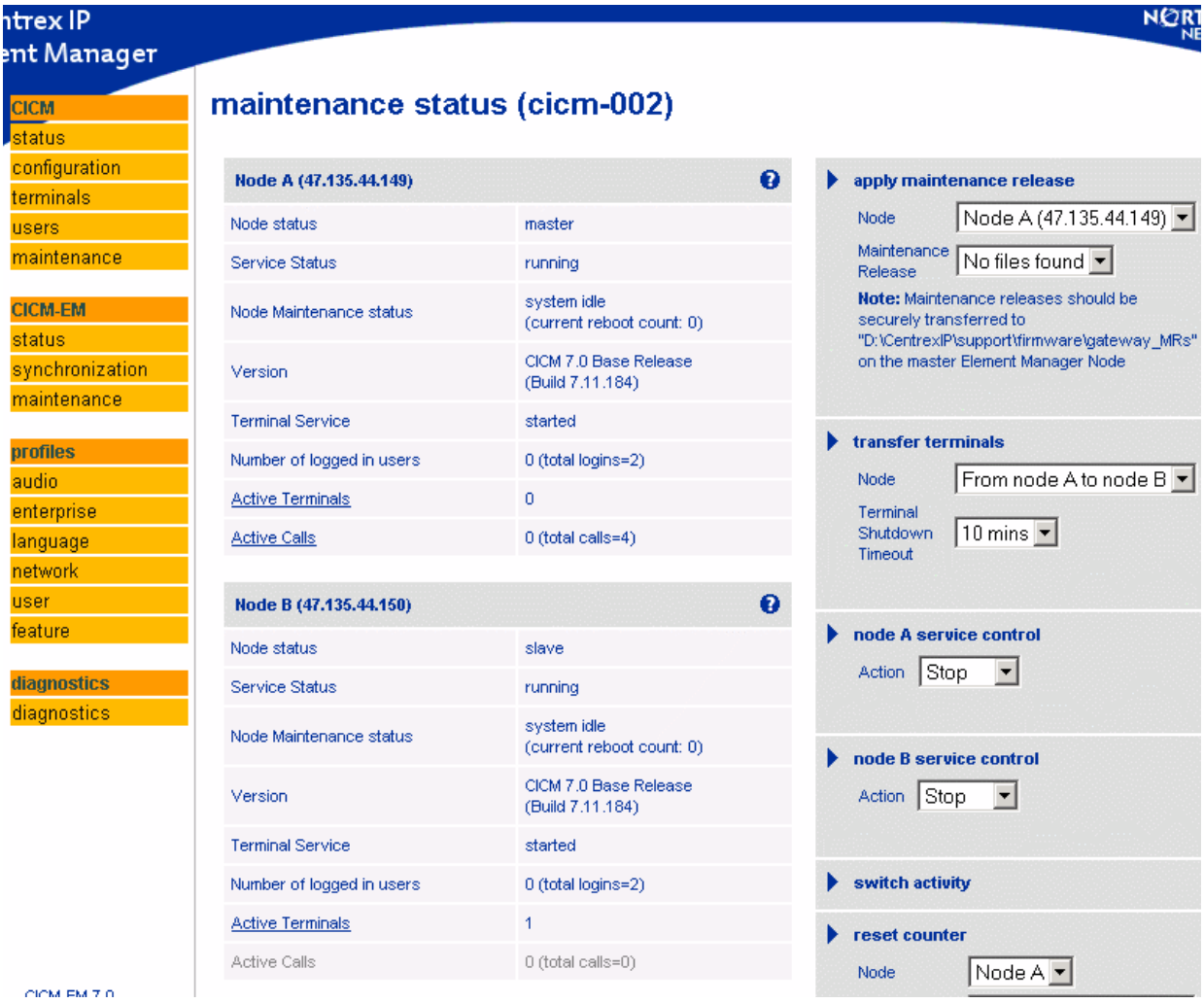
1 On the **CICM home** page, select the CICM to view from the drop-down menu in the right navigation menu, then click on the **view the status of the following CICM** text.

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



2 Select the **perform maintenance on <cicm_name>** option from 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** option 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.

View connections, terminals, and packets performance statistics

Use this procedure to view the performance statistics on each node:

Procedure 3 View connections, terminals, and packets statistics

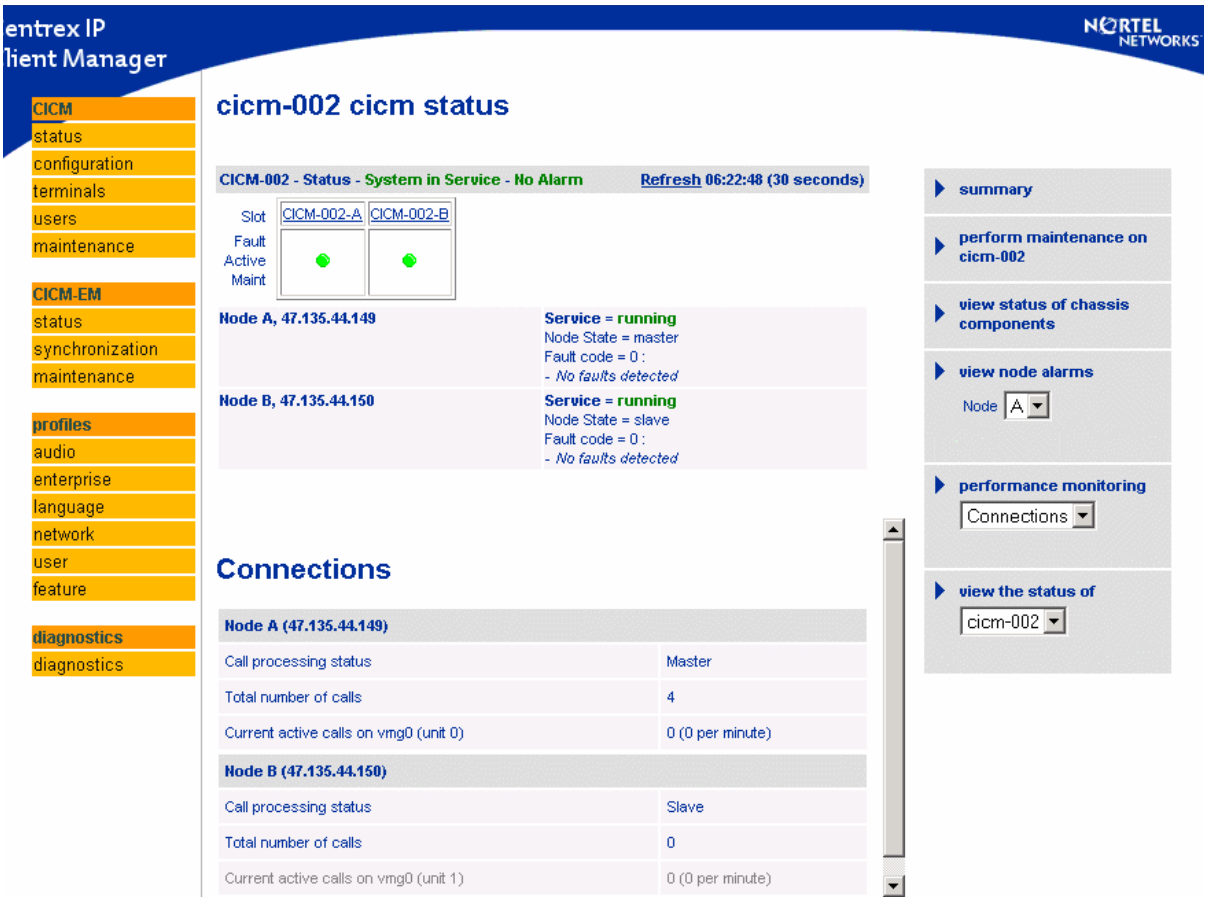
At the CICM EM web pages

1 On 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.*

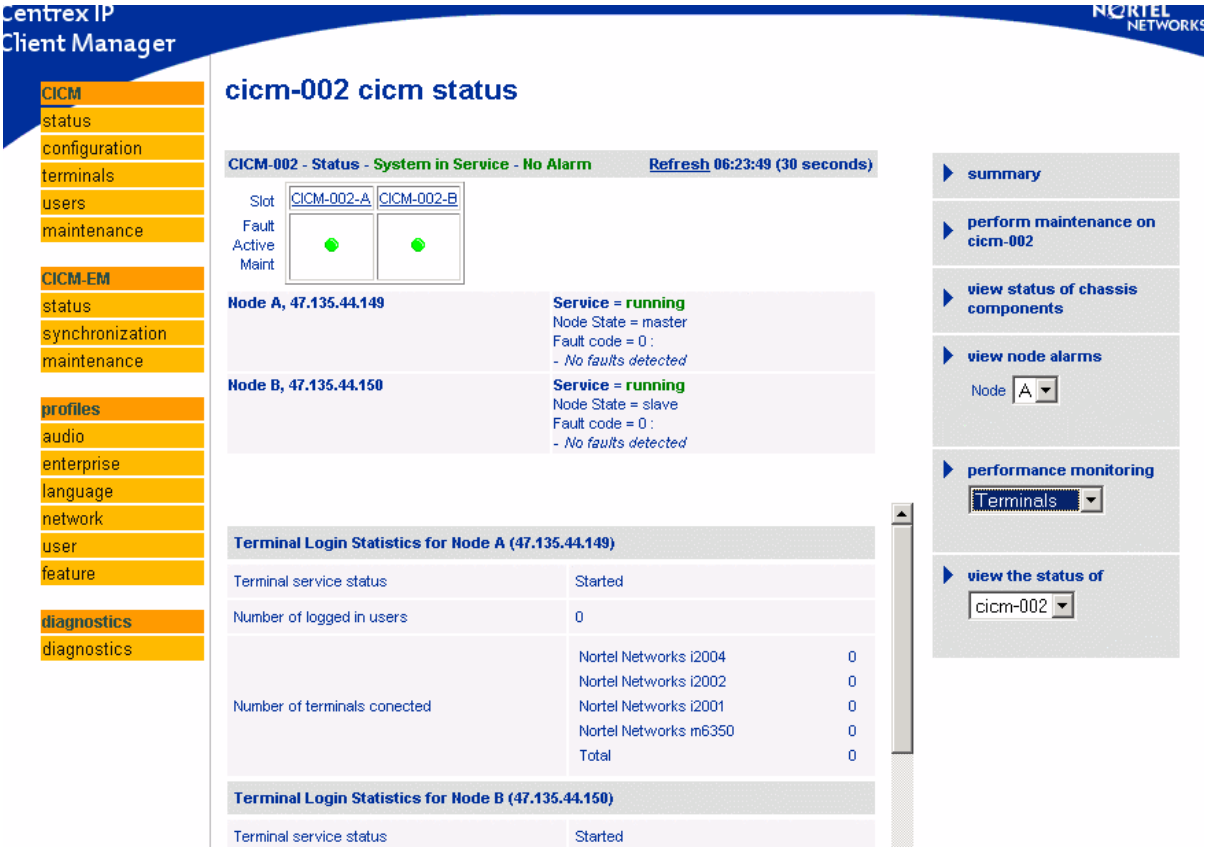
2 To view the connections statistics, in the **performance monitoring** menu option on the right menu bar, select **Connections** from the drop-down menu, then click on the **performance monitoring** text.

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



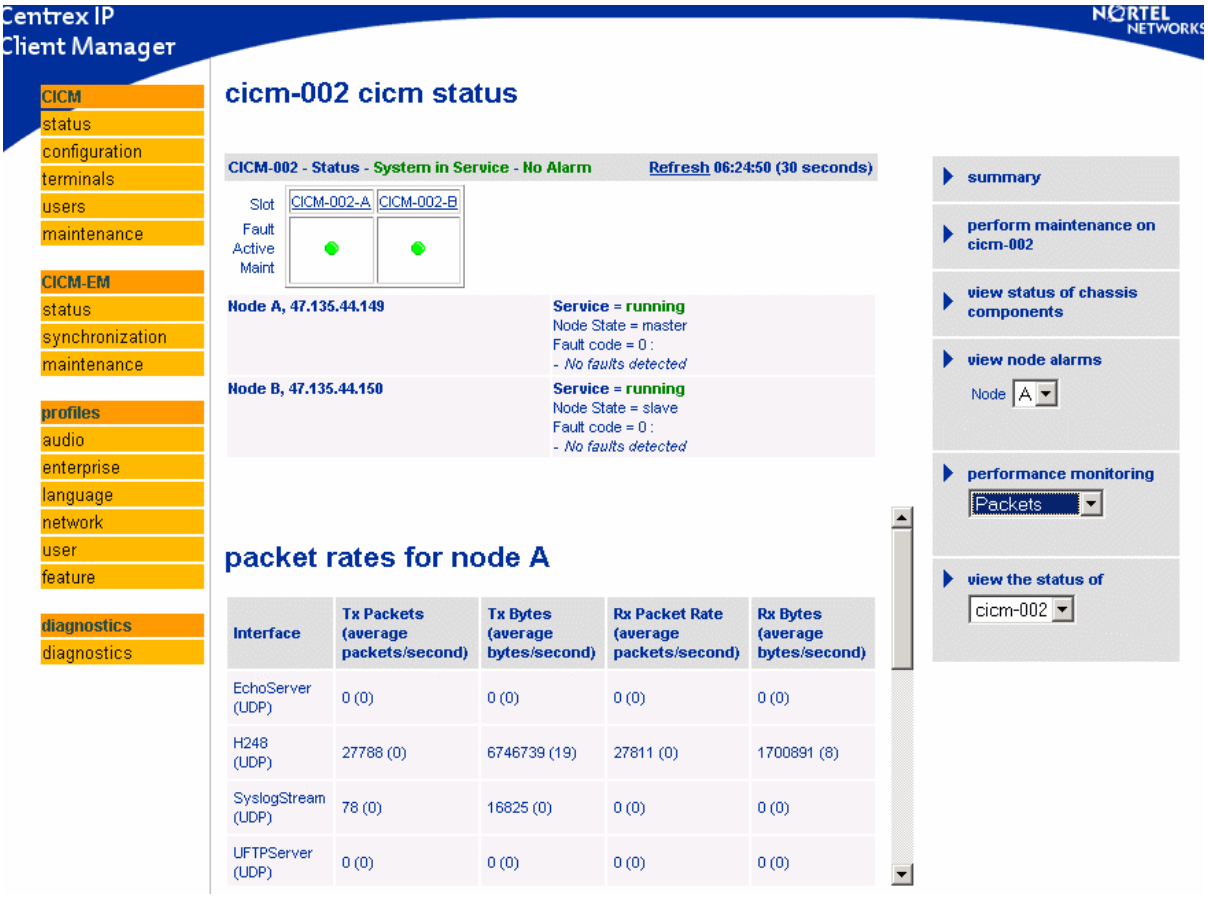
3 To view the terminals statistics, in the **performance monitoring** menu option on the right menu bar, select **Terminals** from the drop-down menu, then click on the **performance monitoring** text.

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



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

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



5 This procedure is complete.

View chassis components status

Use this procedure to view the chassis components status for a CICM.

Procedure 4 View chassis components status

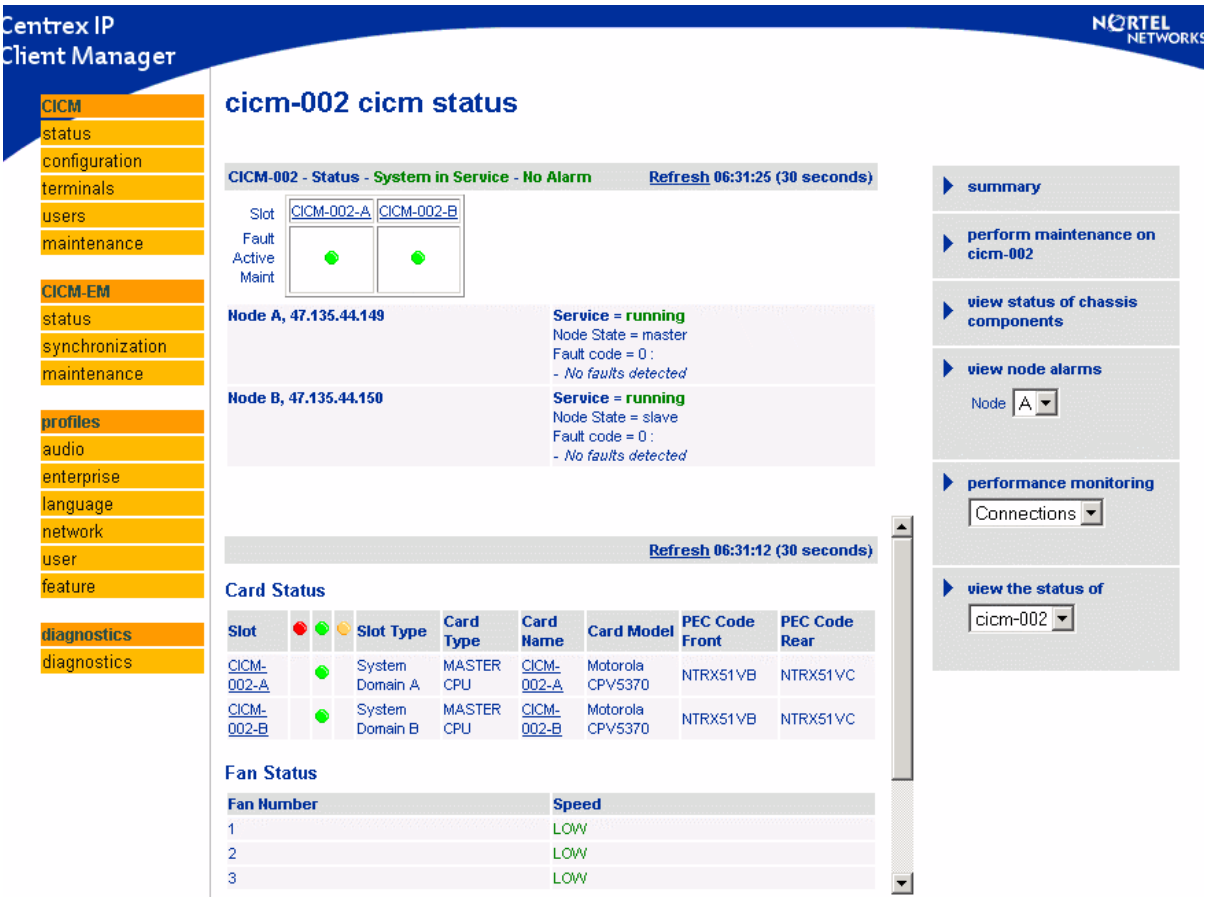
At the CICM Home page

1 In the **view the status of the following cicm** menu option on the right, select the CICM to view from the drop-down menu.

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

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

Use MS Performance Monitoring

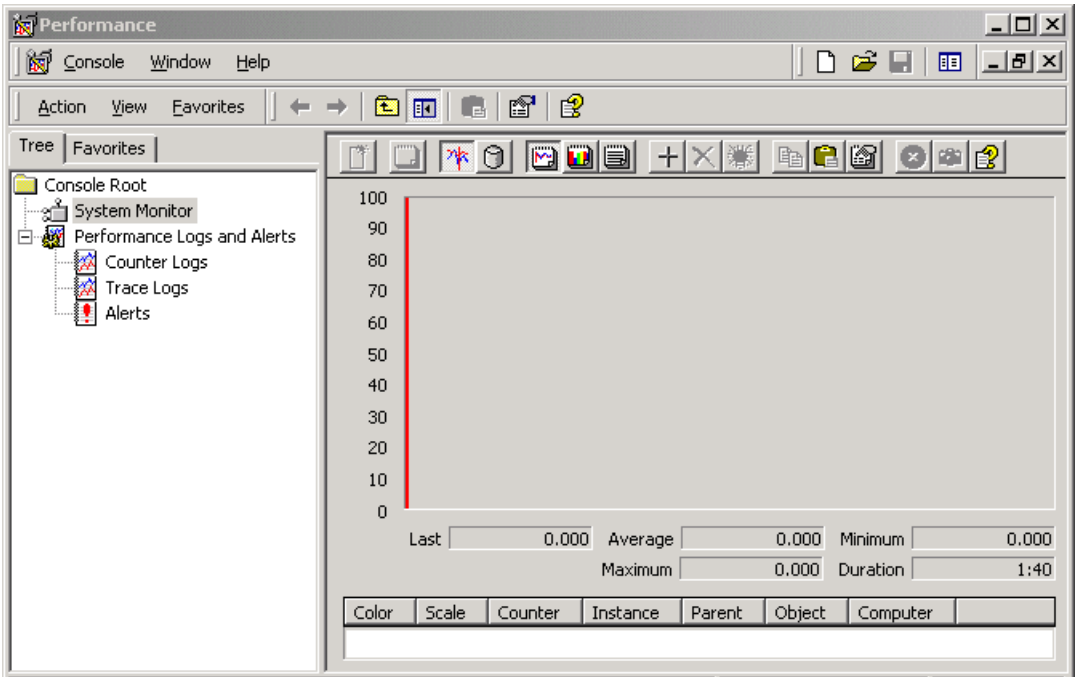
This section describes how to use the Microsoft Performance Monitoring tool (Perfmon).

Procedure 5 Use MS Performance Monitoring

At the MS2000 desktop of the CICM EM

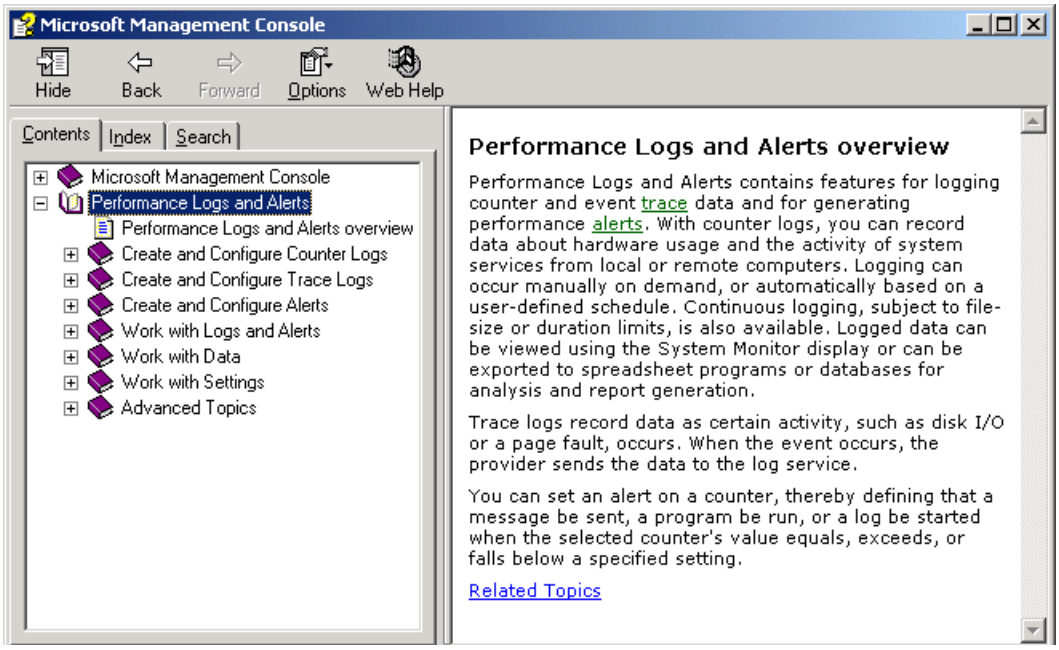
1 From the **Start** menu of the desktop,
select **Programs**,
then select **Administrative Tools**,
then select **Performance**

*Response: the **Performance** window opens.*



2 For additional help and procedures for the Performance Management tool:
From the **Action** menu,
select **Help**,
then enter **Performance** in the index search.

Response: A Performance Logs and Alerts overview is displayed, and additional logs and alert procedures are available.



3 This procedure is complete.

Monitor the CPU load on CICM nodes

Use this procedure to monitor the CPU load on CICM nodes.

Procedure 6 Monitor the CPU load on CICM nodes

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure in the *CICM Security and Administration* document.

At the DOS command prompt

2 Type

net use \\<remote_IP_address> /user:<admin_name> <admin_password>
Or
net use \\<node_name> /user:<admin_name> <admin_password>

then press **Enter**.

Example
net use \\47.165.169.95 /user:admin1 admin1password

3 Verify that you receive the following response:

```
The command completed successfully.
```

4 Start the Performance Monitoring tool:
From the MS desktop, select:

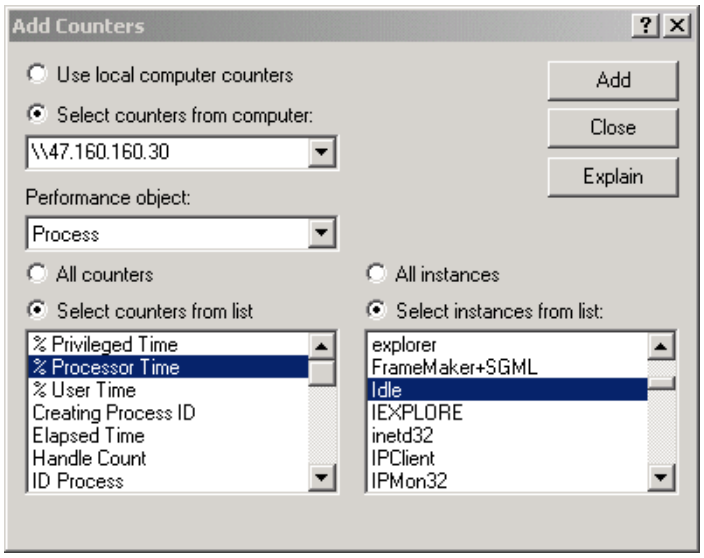
Start > Programs > Administrative Tools > Performance

Response: the Performance window opens.

5 From the Performance window's left menu tree panel, select **System Monitor**.

6 Right-click the mouse in the Performance window's right panel (graph area),
then select **Add Counters.**

*Response: the **Add Counters** window opens.*



7 In the **Add Counters** window:

a Change the **Select counters from computer** field to:

node_IP_address
or
node_name

b In the **Performance object** field, select **Process** from the drop-down menu.

c In the **Select counters from list** field, select **% Processor Time**.

d In the **Select instances from list** field, select **Idle**

Response: The idle % time for the chosen node is displayed.

8 Repeat this procedure for the mate node or other CICM nodes to be monitored.

9 This procedure is complete.

Feature: Enhanced FCAPS Interfaces and Integration into IEMS

CICM 7.0 provides enhanced interfaces for provisioning, fault reporting, performance measurements, and security. It provides capabilities to pass on fault and alarms to the overlaying OSS systems of the service provider.

Feature: Fault and Performance management

This section summarizes the Fault and Performance management changes for (I)SN07. It includes the changes for the alarms, logs, and performance features for the (I)SN07 release.

Note: These changes affect the Succession version of the CICM product only. The TDM version does not support these changes.

IEMS

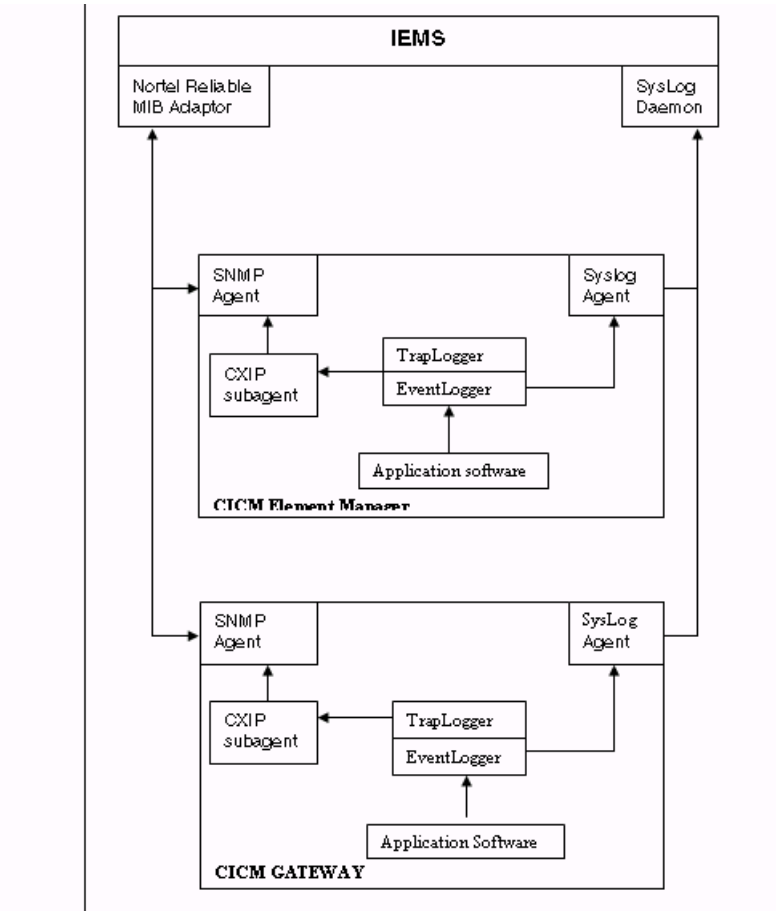
A new interface has been introduced to the Succession network that will manage the output used by external OSS to monitor the network element and detect alarm conditions. This new interface is the Integrated Element Manager System (IEMS). The IEMS is accessed using a GIU, which will give access to the alarms and logs for a network element. This will also interact with the EM GUI.

The CICM must integrate with the IEMS. The CICM alarms, logs and performance metrics have all been formatted to be compatible with IEMS.

Both the CICM and the CICM-EM can raise alarms and faults to the IEMS. The EM will raise alarms associated with the EM Platform (e.g. memory shortage), and communication with the CICMs that it manages, but will not have knowledge of the alarms and faults generated by the CICM. The CICM sends alarms as SNMP traps directly to the IEMS.

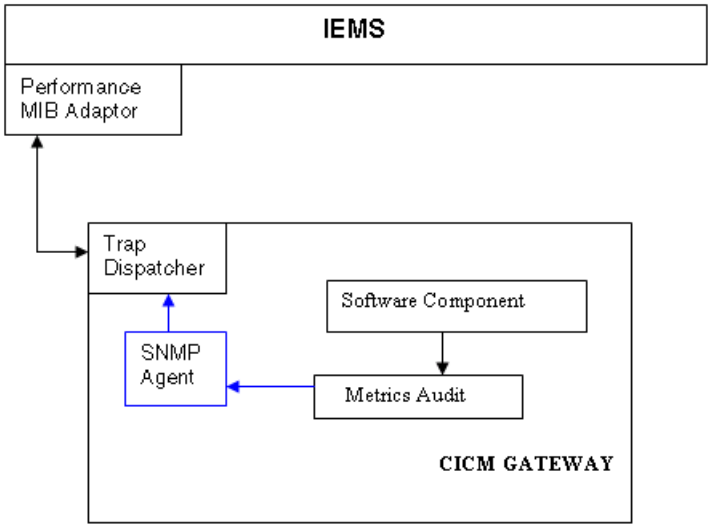
The following Figure 5 provides an overview of the CICM fault architecture.

Figure 1 CICM Fault Architecture



The following Figure 6 illustrates the CICM Performance architecture.

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 gateway 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 provided in the following table.

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 3 objects for the purpose of reporting alarms:

- The CICM Element Manager
- A CICM node
- The platform which the EM and the CICM use.

These objects contain sub-objects which, appended together with the alarm type, form the Component ID. Component IDs are defined in Figure 8.

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 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 via a syslog agent. Three log streams are used to send logs to up to three different syslog daemons (i.e. IEMS). This is a change from previous CICM releases, where all logs were stored on the CICM. In (I)SN07, 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 will use 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 will log 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 gateway as follows:

- upon successful/unsuccessful login from an etherset (Nortel Networks IP Phone 200x) or m6350 Softclient
- logout from an etherset (IP Phone 200x) or m6350

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

- upon launching CICM-EM from IEMS

The CICM will log 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 Gateway on executing flow-through commands at OSSGATE (e.g. ado, deo, etc.).

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

- All configuration changes made by the CICM-EM administrator. (e.g. adding CICM nodes)
- All mtc actions performed by the device (e.g. restarts)

Debug logs

Debug logs are used by Nortel Networks support personnel only; not the service provider. Debug logs are not changed in (I)SN07, but they can now be viewed using the EM Web page interface. Debug logs will not be sent via syslog to the IEMS.

Performance

The new interface introduced to the Succession network that manages the output used by external OSS' to monitor CICM network elements is

the IEMS. Performance metrics have been re-formatted in (I)SN07 to be compatible with IEMS.

The following performance metrics are supported in CICM 7.0:

- Percentage Memory Usage
- Number of Active Connections
- Percentage CPU Usage
- Number of logs
- Number of Active Sessions
- Number of Busy Hour Call Attempts
- Transmitted Bytes/Sec
- Received Bytes/Sec
- Number of Logged in Users

The metrics will be stored in the performance MIB and will be collected at intervals by the IEMS.

Performance metrics

Performance metrics are generated by both the CICM and the CICM-EM. 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 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 Succession performance MIB. Each metric contains the following information:

- The instance of the object (e.g. SAM21 x blade y)
- The property of the object being reported (e.g. processor occupancy)
- The type of the property (e.g. gauge)
- The value (e.g. 22%)

