Unified Communications and Contact Center Remote Management Service: Cisco Management Application Platform Reporting Guide

With its universal reporting structure, the Cisco® Management Application Platform (Cisco MAP) offers comprehensive access to reports and log files that can be used to provide a graphical analysis and history of areas ranging from case statistics to network performance. Such access provides a view into your IT operational health, service level management, and network and system activities providing for improvement in overall IT service levels and operational efficiency while cost-effectively meeting compliance and operational integrity needs.

In addition to built-in Cisco MAP graphs, the Cisco Management Application Platform provides the ability to export incident and network data so you can store and analyze this information in other applications.

Scheduling and On-Demand Reporting

Cisco MAP offers users the ability to schedule commonly reviewed reports on a regular basis based on their defined criteria.

Table of Contents

Overview

The primary reporting features covered in this reporting guide include:

- Authentication Reporting
- Incident Management Reporting
- Infrastructure Management Reporting
- Configuration Manager Application and Reporting
- IP Telephony Management Reports
- Contact Center Reporting
- Event Log Viewer
- IP SLA Manager

Cisco Unified Communications and Contact Center (UC/UCC) Standard Reports

Authentication Reporting

Cisco MAP Authentication Reporting provides organizations with a better understanding into when employees logged in to the Cisco Management Application Platform to provide audit capabilities. This is especially critical as organizations continue to implement stronger levels of access security to meet regulatory compliance demands and to better secure their valuable information assets.

Cisco MAP Authentication Reports are based upon Authentication Logs within the Cisco Management Application Platform and are available in Adobe® Portable Document Format (PDF) file format. After entering in the report criteria and setting confines such as the range of time desired and the user to query on, a report can be generated and delivered via email to a designated address or saved in a directory on your local hard drive or other available network drive.

Authentication Failures

The Authentication Failures Report presents a list of failed authentication events for a selected Cisco MAP user, or users, during a selected time period. The report results include the date and time of the failed event, and the IP address of the associated device attempting to authenticate to Cisco MAP.

Table 1. Example of the Cisco MAP Authentication Failures Report

Description: List of Failed Authentication Events		Time Period: Prior Half		Run By: Rob Halford
Run Date: 2010-02-24 14:53:41		Time Zone: EST		
Date/Time	**Username**	**Real Name**	**IP Address**	**Event**
2009-09-18 08:26:12	User	User	10.15.161.146	Incorrect Password
2009-09-18 08:26:12	User	User	10.15.161.146	Incorrect Password
2009-09-18 08:26:12	User	User	10.15.161.146	Incorrect Password

Last Login

The Last Login presents a list of users by their Cisco MAP username and full name (first name, last name) along with the corresponding date and time of their last login along with the number of days since their last login.

Table 2. Example of the Cisco MAP Last Login Report

Description: Last Time A User Logged In	Time Period: 2009-12-11 00:00:00 to 2010-02-24 00:00:00	Run By: Rob Halford
Run Date: 2010-02-24 14:58:21	Time Zone: EST	

Username	Real Name	Date of Last Login	Days Since Last Login
User	User	2010-02-24	0
User	User	2010-02-24	0
User	User	2010-02-05	19
User	User	2010-02-28	30
User	User	2009-12-11	75

Last Password Change

The Last Password Change Report displays the date that a selected user, or users, last changed their Cisco MAP password and the number of days since their last password change.

Table 3. Example of the Cisco MAP Last Password Change Report

Description: Last Time A User Change Passwords	Time Period: 2009-09-18 00:00:00 to 2010-02-24 00:00:00	Run By: Rob Halford
Run Date: 2010-02-24 15:01:14	Time Zone: EST	

Username	Real Name	Date of Last Change	Days Since Last Change
User	User	2009-09-18	159
User	User	2010-02-24	0

Simultaneous Logins

The Simultaneous Logins Report displays the primary and secondary IP addresses of the device with concurrent Cisco MAP logins. The date and time of the event are logged as well as the Cisco MAP username.

Table 4. Example of the Cisco MAP Simultaneous Logins Report

Description: List of Multiple Login Events	Time Period: Prior Year	Run By Rob Halford
Run Date: 2010-02-24 15:04:54	Time Zone: EST	

Date/Time	Username	Real Name	Primary Login IP Address	Secondary Login IP Address
2009-12-15 12:15:54	User	User	XX.XX.XX.XXX	XX.XX.XX.XXX
2009-12-11 11:48:26			XX.XX.XX.XXX	XX.XX.XX.XXX
2009-12-11 11:28:05	User	User	XX.XX.XX.XXX	XX.XX.XX.XXX
2009-11-11 14:01:40	User	User	XX.XX.XX.XXX	XX.XX.XX.XXX

Time Logged In By Day

The Time Logged In By Day Report displays the number of hours logged in each day for a selected Cisco MAP user, or users, during a defined time period.

Table 5. Example of the Cisco MAP Time Logged In By Day Report

Description: Total Login Time By Day	Time Period: Last 30 Days		Run By: Rob Halford
Run Date: 20120-02-24 15:07:30	Time Zone: EST		
Username	**Real Name**	**Date**	**Total Time (HH:MM)**
User	User	2010-01-25	01:22
User	User	2010-01-25	00:34
User	User	2010-01-28	01:39

Time Logged In By User

The Time Logged In By User Report displays the total login time for a selected Cisco MAP user, or users, during a defined time period.

Table 6. Example of the Cisco MAP Time Logged In By User Report

Description: Total Login Time by User	Time Period: Current Year	Run By: Rob Halford
Run Date: 2010-02-24 15:10:41	Time Zone: EST	
Username	**Real Name**	**Total Time (HH:MM)**
User	User	31:56
User	User	13:47
User	User	00:34
User	User	00:00

Incident Management Reporting

The Cisco Management Application Platform’s Incident Management Reporting allows you to ensure infrastructure availability and raise service levels while reducing costs. Such reports create an audit trail that can be used for future analysis to make better decisions about the man hours needed to properly maintain the network, systems, and applications.

Several Cisco MAP Incident Management reports are available in Comma Separated Value (CSV) file format or Adobe Portable Document Format (PDF). After entering in the report criteria and setting confines such as the range of time desired, a user can generate the report and either have it emailed to a designated address or save it in a directory on their hard drive or other network drive they have access to.

The CSV file can then be opened in Microsoft® Excel or other comparable spreadsheet or database program, from which data can be graphically displayed and/or custom reports generated.

Case Activity Report

The Case Activity Report provides the daily total number of updates to active cases in Cisco MAP for a defined time period. Active cases are those cases having a case status of anything other than “Closed.” Since the Case Activity Report tallies the number of system-wide case updates per day, a single case may be responsible for many updates in the daily count. Examples of case updates include adding text to the case history, changing the status of a case, or re-assigning the case to a different person. The report results are displayed in CSV file format.

Table 7. Example of the Cisco Case Activity Report

Case Activity Report Data Export	
Created by Management Application Platform 20091027113141	
Case Activity for the Date Range: 2009-01-01 to 2009-09-30	
Date	**Active Case Updates**
9/1/2009	0
9/2/2009	4666
9/3/2009	2399
9/4/2009	1912
9/5/2009	1025
9/6/2009	960
9/7/2009	1129
9/8/2009	1744
9/9/2009	1668
9/10/2009	1666
9/11/2009	2369
9/12/2009	1110
9/13/2009	754
9/14/2009	1688
9/15/2009	2971
9/16/2009	1815

Case Detail By User

The Case Detail By User Report provides Cisco MAP administrators with valuable information about the cases touched by any one of their Cisco MAP users. The report can contain any or all of the following information regarding cases for a particular Cisco Management Application Platform user:

- User Currently Assigned to Case
- Last Update Date
- Last Updated By
- Text of Last Update
- Closed Cases

Table 8. Example of the Cisco MAP Case Details By User Report

Case Detail By User Report Data Export							
Created by Management Application Platform on Tues							
27 Oct 2009 11:57:34-0400							
Site	**Case Created By**	**Case Number**	**Case Name**	**Case Description**	**Current Status**	**Current Priority**	**Create Date**
Superior Healthcare System	User	718	MRH2-3745-1A11:THRESH:mem	AutoCase: Threshold Violation	Closed	3-Medium	10/1/2009 10:31
B-Cast	Cisco_ROS	427	Paging Notification	Self Test	Closed	3-Medium	10/1/2009 14:02

Table 8 Cont'd. Example of the Cisco MAP Case Details By User Report

Case Category	Currently Assigned To	Date of Last Update	Last Updated By	Text of Last Update
AutoCase, Cisco_ROS	ROS-Support	10/2/2009 16:35		Case assigned to: Cisco_ROS, Support Status changed to: Closed Notification for User change to: on Remote Case#: 182 Remote Site: Sybase Case assigned to: Cisco_ROS, Support Status changed to: Closed Notification for User changed to: on Closing cases. Carly Jones
Cisco_ROS, Individualized	Cisco_ROS	10/1/2009 15:11	ROS-Support	Status changed to: Closed Notification for User changed to: on Remote Case#: 24B Remote Site: Bundercast-EAST Status changed to: Closed Notification for User changed to: on

Case Suppression Report

The Case Suppression Report shows cases that have/had suppressions on them and the details of the suppression, including the case number, the case name, and both the start and end dates of the suppression. The report results are displayed in PDF file format.

Table 9. Example of the Cisco MAP Case Suppression Report

CASE SUPPRESSION REPORT

Start Time: 2010-02-01 00:00:00
End Time: 2010-02-24 00:00:00
Generated by rhalford on 2010-02-24 03:32:14 PM
Matching data for active suppressions for your time frame.
Historical Data:

Case Number	Name	Start Date	End Date	By
161	Upgrade IOS® version	2009-09-11 16:30:00	2009-09-11 17:30:00	Scheduled
169	IOS® Update	2009-09-14 17:00:00	2009-09-14 19:00:00	Scheduled
162	syr-vmx1:ICMP:	2009-09-14 17:00:03	2009-09-14 19:00:00	Scheduled
171	BS-3221 Test	2009-09-15 09:30:00	2009-09-15 10:30:00	Scheduled
192	StandardServiceRequest_190	2009-09-25 11:55:07	2009-09-26 11:55:10	Scheduled
123	NY-35-3745-1:IF:Fa0/1	2009-12-11 11:33:00	2009-12-11 12:33:00	User

Cases Created By

The Cases Created By Report provides Cisco MAP administrators with valuable information about the various ways a case can be created in the Cisco MAP application. The report can contain any or all of the following information regarding case creation:

- Original Requested By Date
- Impacted Call Centers
- Brief Description of Work Change
- User Currently Assigned to Case
- Last Update Date
- Last Updated By
- Text of Last Update
- Closed Cases

The report results are displayed in CSV file format.

Table 10. Example of the Cisco MAP Cases Created By Report

Cases Created By Report Data Export

Created by Management Application Platform on Wed

24 Feb 2010 15:51:46-0500

Case Created By	Case Number	Case Name	Case Description	Brief Description of Work Change	Current Status	Current Priority	Create Date
User	1992	twtelecom-syr:ICMP:	AutoCase		Closed	4-Low	11/12/2009 10:05
User	1993	twtelecom-syr:ICMP:	AutoCase		Closed	3-Medium	11/12/2009 10:06
User	1994	twtelecom-syr:ICMP:	AutoCase		Closed	3-Medium	11/12/2009 10:06
User	1995	twtelecom-syr:ICMP:	AutoCase		Closed	3-Medium	11/12/2009 10:14
User	1996	twtelecom-syr:ICMP:	AutoCase		Closed	3-Medium	11/12/2009 10:22
User	1997	twtelecom-syr:ICMP:	AutoCase		Closed	4-Low	11/12/2009 10:29

Table 10 Cont'd. Example of the Cisco MAP Cases Created By Report

Case Category	Currently Assigned To	Original Request Date	Impacted Call Centers	Date of Last Update	Last Updated By	Text of Last Update
				2010—0-2-04:1:0:	SG-Support	Priority changed to: 4 -Low Status changed to: Closed Notification for User changed to: on Closing stale case. –Kelly
				2010—0-2-04:1:0:	SG-Support	Status changed to: Closed Notification for User changed to: on Closing stale case. –Kelly
				2010—0-2-04:1:0:	SG-Support	Status changed to: Closed Notification for User changed to: on Closing stale case. –Kelly
AutoCase,Infrastructure	User			2010—0-2-04:1:0:	SG-Support	Status changed to: Closed Notification for User changed to: on Closing stale case. –Kelly
AutoCase,Infrastructure	User			2010—0-2-04:1:0:	SG-Support	Status changed to: Closed Notification for User changed to: on Closing stale case. –Kelly
	User			2010—0-2-04:1:0:	SG-Support	Priority changed to: 4-Low Status changed to: Closed Notification for User changed to: on Closing stale case. –Kelly

Cases Opened or Closed

The Cases Opened Or Closed Report provides Cisco MAP administrators with information on the case number of open and/or closed cases and who the current assignee of the case is. The report results are displayed in CSV file format.

Table 11. Example of the Cisco MAP Opened or Closed Report

<table>
<tr><td colspan="4">Cases Opened or Closed Report Data Export</td></tr>
<tr><td colspan="4">Created by Management Application Platform on Wed 24 Feb 2010 16:03:33-0500</td></tr>
<tr><td colspan="4">Cases Opened or Closed for the Date Range: Jan 25 2009 – Feb 24 2010</td></tr>
<tr><th>Case Number</th><th>Create Date</th><th>Closed Date</th><th>Assigned</th></tr>
<tr><td><b>1</b></td><td>8/24/2009 14:23</td><td>9/15/2009 16:22</td><td>User</td></tr>
<tr><td><b>2</b></td><td>2/24/2009 14:25</td><td>10/19/2009 11:53</td><td>User</td></tr>
<tr><td><b>3</b></td><td>5/24/2009 14:25</td><td>6/8/2009 11:36</td><td>User</td></tr>
<tr><td><b>4</b></td><td>1/11/2010 13:33</td><td>1/11/2010 13:33</td><td>User</td></tr>
<tr><td><b>5</b></td><td>1/11/2010 23:33</td><td>1/13/2010 9:17</td><td>User</td></tr>
<tr><td><b>6</b></td><td>1/14/2010 13:13</td><td>9/11/2009 16:23</td><td>User</td></tr>
<tr><td><b>7</b></td><td>1/19/2010 23:33</td><td>9/11/2009 16:23</td><td>User</td></tr>
<tr><td><b>8</b></td><td>2/1//2010 20:03</td><td>9/11/2009 16:23</td><td>User</td></tr>
<tr><td><b>9</b></td><td>1/14/2010 23:33</td><td>9/11/2009 16:23</td><td>User</td></tr>
</table>

Notification Detail By User

The Notification Detail By User Report lists the details on all case notifications generated by Cisco MAP for a selected user, or users, during a defined time period and information on cases where notifications have been sent. Administrators gain insight into:

- Date/time case notification was sent
- Username receiving the notification
- Case number
- Type of notification sent (e.g., email)
- Notification address
- Subject of the notification

The report results are displayed in PDF file format.

Table 12. Example of the Cisco MAP Notification Detail By User Report

<table>
<tr><td colspan="3">Description: List of All Notifications</td><td colspan="2">Time Period: To Date</td><td>Run By: User</td></tr>
<tr><td colspan="3">Run Date: 2010-02-24 16:14:11</td><td colspan="2">Time Zone: EST</td><td></td></tr>
<tr><th>Date/Time</th><th>Username</th><th>Case Number</th><th>Type</th><th>Notification Address</th><th>Notification Subject</th></tr>
<tr><td>**2009-01-07 18:16:02**</td><td>User</td><td>878</td><td>Email-text</td><td>user@cisco.com</td><td>Case 878 for test created by User</td></tr>
<tr><td>**2009-01-08 03:41:04**</td><td>User</td><td>461</td><td>Email-</td><td>user@cisco.com</td><td>Case 461 for syr-com6-pub:GRP:NODE updated by Cisco_Appliance</td></tr>
<tr><td>**2009-01-09 03:41:04**</td><td>User</td><td>461</td><td>Email-</td><td>user@cisco.com</td><td>Case 461 for syr-com6-pub:GRP:NODE updated by Cisco_Appliance</td></tr>
<tr><td>**2009-01-10 03:41:04**</td><td>User</td><td>461</td><td>Email-</td><td>user@cisco.com</td><td>Case 461 for syr-com6-pub:GRP:NODE updated by Cisco_Appliance</td></tr>
<tr><td>**2009-01-11 03:41:04**</td><td>User</td><td>461</td><td>Email-</td><td>user@cisco.com</td><td>Case 461 for syr-com6-pub:GRP:NODE updated by Cisco_Appliance</td></tr>
<tr><td>**2009-01-12 03:41:04**</td><td>User</td><td>461</td><td>Email-</td><td>user@cisco.com</td><td>Case 461 for syr-com6-pub:GRP:NODE updated by Cisco_Appliance</td></tr>
<tr><td>**2009-01-13 03:41:04**</td><td>User</td><td>461</td><td>Email-</td><td>user@cisco.com</td><td>Case 461 for syr-com6-pub:GRP:NODE updated by Cisco_Appliance</td></tr>
</table>

Notify By Assignee

The Notify By Assignee Report provides data on the number and method of notifications sent to an assignee over time. This report provides a mechanism to manage and have better visibility on the extent of notifications being generated to network personnel. The report results are displayed in CSV file format.

Table 13. Example of the Cisco MAP Notify By Assignee Report

<table>
<tr><td colspan="2">Notify By Assignee Report Data Export</td></tr>
<tr><td colspan="2">Created by Management Application Platform on Wed 24 Feb 2010 16:31:15-0500</td></tr>
<tr><td colspan="2">Notifications By Assignee for the Date Range 2009-01-25 to 2010-02-24</td></tr>
<tr><th>Login</th><th>Number of Notifications</th></tr>
<tr><td>User</td><td>1</td></tr>
<tr><td>User</td><td>1</td></tr>
<tr><td>User</td><td>706</td></tr>
<tr><td>User</td><td>5</td></tr>
<tr><td>User</td><td>33</td></tr>
<tr><td>User</td><td>21</td></tr>
<tr><td>User</td><td>590</td></tr>
</table>

Performance By Assignee

The Performance By Assignee Report provides Cisco MAP administrators with data on case handling history. This allows monitoring of such things as how cases are being distributed, case handling performance by type and assignee, and case load being assumed by each staff member. The report results are displayed in CSV file format.

Table 14. Example of the Cisco MAP Performance By Assignee Report

<table>
<tr><td colspan="5">Performance By Assignee Report Data Export</td></tr>
<tr><td colspan="5">Created by Management Application Platform on Wed 24 Feb 2010 16:41:50-0500</td></tr>
<tr><td colspan="5">Performance By Assignee for the Date Range 2009-02-01 to 2010-01-31</td></tr>
<tr><th>Login</th><th>Case Priority</th><th>Number of Cases</th><th>Total Duration in Hours</th><th>Average Duration in Hours</th></tr>
<tr><td>User</td><td>3-Medium</td><td>1</td><td>1.11</td><td>1.11</td></tr>
<tr><td>User</td><td>1-Critical</td><td>1</td><td>25.08</td><td>25.08</td></tr>
<tr><td>User</td><td>3-Medium</td><td>2</td><td>25.82</td><td>12.91</td></tr>
<tr><td>User</td><td>1-Critical</td><td>155</td><td>236.92</td><td>1.98</td></tr>
<tr><td>User</td><td>2-High</td><td>178</td><td>62.56</td><td>0.35</td></tr>
<tr><td>User</td><td>3-Medium</td><td>114</td><td>587.49</td><td>2.84</td></tr>
</table>

Time To Closure

The Time To Closure Report provides Cisco MAP administrators with data on the length of time for case completion by priority. These time attributes provide insight into how long it is taking network management personnel to resolve and close cases of different priorities. In support of service management initiatives, this data can be used to compile and report on average times and trends for responding to and completing cases of various priorities. The report results are displayed in CSV file format.

Table 15. Example of the Cisco MAP Time To Closure Report

<table>
<tr><td colspan="7">Time To Closure Report Data Export</td></tr>
<tr><td colspan="7">Created by Management Application Platform 201002241165042</td></tr>
<tr><td colspan="7">Time To Closure Data for the Date Range 2010-01-25 to 2010-02-24</td></tr>
<tr><th>Case Number</th><th>Assigned To</th><th>Closed By</th><th>Autoclose</th><th>Opened</th><th>Closed</th><th>Opened in Hours</th></tr>
<tr><td><b>19783</b></td><td>User</td><td>User</td><td>N</td><td>2/12/2010</td><td>2/12/2010</td><td>0.9</td></tr>
<tr><td><b>18189</b></td><td>User</td><td>User</td><td>N</td><td>1/26/2010</td><td>1/26/2010</td><td>7.8</td></tr>
<tr><td><b>19455</b></td><td>Cisco_ROS</td><td>User</td><td>N</td><td>2/9/2010</td><td>2/9/2010</td><td>6.8</td></tr>
<tr><td><b>18192</b></td><td>User</td><td>User</td><td>N</td><td>1/26/2010</td><td>1/26/2010</td><td>7.8</td></tr>
<tr><td><b>19736</b></td><td>User</td><td>User</td><td>N</td><td>2/11/2010</td><td>2/12/2010</td><td>20.3</td></tr>
<tr><td><b>19067</b></td><td>User</td><td>Cisco-MAP</td><td>N</td><td>2/6/2010</td><td>2/11/2010</td><td>115.8</td></tr>
<tr><td><b>18512</b></td><td>User</td><td>User</td><td>N</td><td>1/30/2010</td><td>2/3/2010</td><td>99.7</td></tr>
<tr><td><b>18581</b></td><td>User</td><td></td><td>N</td><td>1/30/2010</td><td>2/2/2010</td><td>59.7</td></tr>
<tr><td><b>19844</b></td><td>User</td><td>Cisco-MAP</td><td>N</td><td>2/13/2010</td><td>2/18/2010</td><td>124.3</td></tr>
<tr><td><b>18832</b></td><td>User</td><td>User</td><td>N</td><td>2/4/2010</td><td>2/5/2010</td><td>30.7</td></tr>
<tr><td><b>18540</b></td><td>Unassigned</td><td>Cisco-MAP</td><td>N</td><td>1/30/2010</td><td>2/1/2010</td><td>48.1</td></tr>
</table>

Total Notifications By User

The Notifications Detail By User Report displays the total number of notifications for a selected Cisco MAP user, or users, generated during a defined time period. The report results are displayed in PDF file format.

Case Summary Graphs

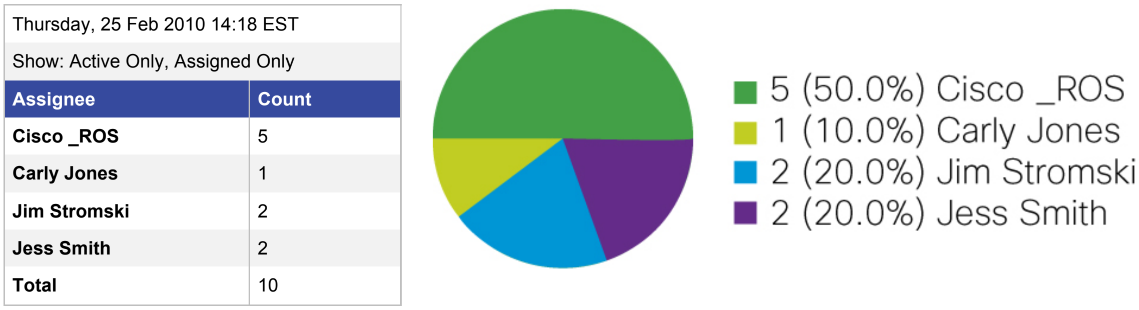
Cisco MAP Incident Management reports are also provided in an online graphical dashboard. The summary reports are available by:

- Assignee
- Priority
- Status

Case Summary Graphs: Cases By Assignee

The Cases By Assignee graph shows the percentage of cases grouped by assignee. Assignees are established based on the list of user accounts. Accounts in this list are included in the report for statistical analysis. Note that cases not having a person assigned to them do not appear on the report.

Table 16. Cases By Assignee



Thursday, 25 Feb 2010 14:18 EST

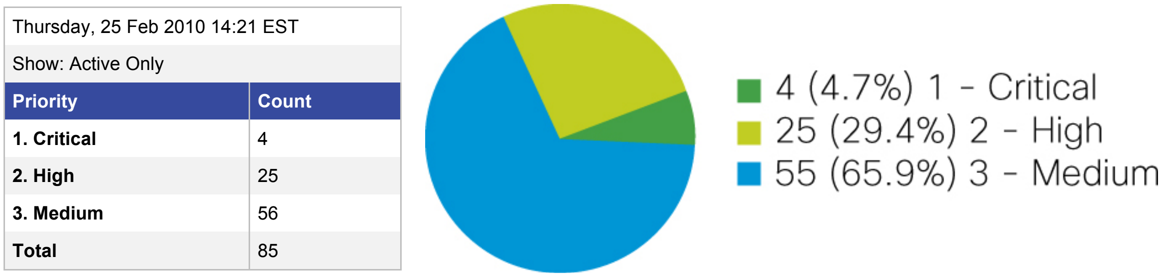
Show: Active Only, Assigned Only

Assignee	Count
Cisco _ROS	5
Carly Jones	1
Jim Stromski	2
Jess Smith	2
Total	10

Case Summary Graphs: Cases By Priority

The Cases By Priority graph shows the percentage of cases grouped by priority.

Table 17. Cases By Priority



Thursday, 25 Feb 2010 14:21 EST

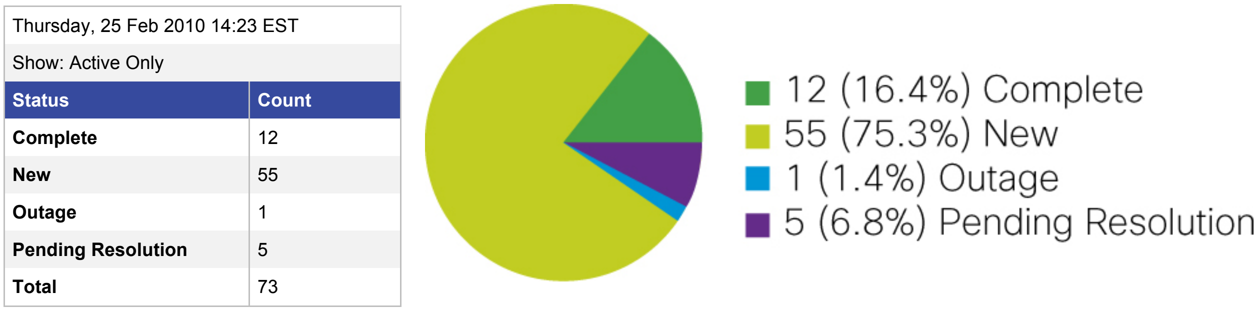
Show: Active Only

Priority	Count
1. Critical	4
2. High	25
3. Medium	56
Total	85

Case Summary Graphs: Cases By Status

The Cases By Status graph shows the percentage of cases grouped by status.

Table 18. Cases By Status



Thursday, 25 Feb 2010 14:23 EST

Show: Active Only

Status	Count
Complete	12
New	55
Outage	1
Pending Resolution	5
Total	73

Entity Activity

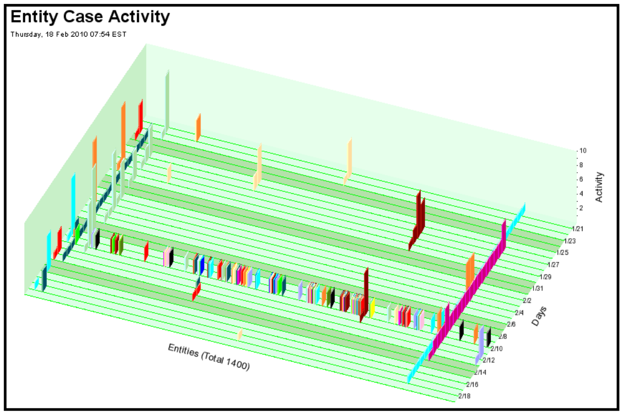
Trends can provide important feedback on the health of your systems and network. The Cisco MAP Entity Case Activity Graph illustrates the case activity for all managed entities over the prior thirty-day (30) period. The Entity Case Activity Graph is measuring the number of individual case entries that pertain to entities in the network. This provides a better gauge of the actual activity level than simply counting the number of cases opened for a given object.

Using the metrics as presented in the current Entity Case Activity Graph, this online graphical report will list all objects according to their case update activity sorted from largest activity to smallest activity over a thirty-day (30) period. Generally, objects with the greatest number of case updates are the most trouble prone monitored objects, and/or those that are consuming the largest amount of workgroup time.

The Entity Activity graph is interpreted as follows:

- The long axis along the front of the three dimensional array represents individual polled entities.
    - Each managed entity is represented by a row of colored bars in the graph.
    - Entities appear only if there has been corresponding case activity over the thirty-day (30) period.
    - An entity is represented with the same color for each day in which there is reportable activity.
- The second axis, running from front to back, represents the days included in the graph. Weekdays are a lighter shade of the color green while weekends are a slightly darker shade of the color green.
- The third axis, running from bottom to top, represents the magnitude of case activity. The magnitude indicates at-a-glance what objects are seeing the largest amount of case activity. The frequency of the entity appearing on the graph and duration of each appearance indicate those entities that are the most problematic.
    - By clicking on one of the entity bars, a search is performed to identify the entity and list those cases pertaining to that entity at that point in time.

Figure 1. Entity Case Activity



Infrastructure Management Reporting

The Cisco Management Application Platform's Infrastructure Management Reporting allows you to build and operate your organization's entire IT infrastructure more efficiently – you can improve the quality and reliability of your IT operations across various locations. You'll gain insights into the status of your network, servers, and systems and will be provided with real-time alerts and performance reports.

Cisco MAP Infrastructure Management reports are available in Comma Separated Value (CSV) file format. After entering in the report criteria and setting confines such as the range of time desired, a user can generate the report and either have it emailed to a designated address or save it in a directory on their hard drive or other network drives they have access to.

The CSV file can then be opened in Microsoft Excel or other comparable spreadsheet or database program, from which data can be graphically displayed and/or customer reports generated.

Bandwidth Utilization

The Bandwidth Utilization Report provides data on the amount of peak input and output bandwidth and average input and output bandwidth utilized over time. Devices configured for bandwidth graphing will display for selection within the report. This report is useful in comparing actual bandwidth utilized versus bandwidth provisioned at different points in the network. This can identify areas where additional bandwidth is needed to increase service levels, or where bandwidth can be reduced resulting in cost savings.

Table 19. Example of the Cisco MAP Bandwidth Utilization Report

Raw Bandwidth Data Export					
Created by Cisco MAP on Fri 23 Oct 2009 11:14:21-0400					
Device	**Date**	**Max In**	**Max Out**	**Average In**	**Average Out**
SYR-CCM-6	Bw_eth0	1301.934159	1221.241289	936.9897738	917.6439829
SYR-CCM-6	Bw_eth0	1102.563414	1038.0378	890.1672333	865.4199222
SYR-CCM-7	Bw_eth0	1433.891714	1014.851181	1164.694113	841.3391892
SYR-CCM-7	Bw_eth0	2083.647647	9820.156193	858.6405299	638.2129195

Hardware Inventory Report

The Hardware Inventory Report assists administrators in tracking which devices are being backed up. This report will list the device name, IP address, type, model, serial number, and the last successful backup. The Hardware Inventory Report is automatically generated by Cisco MAP on the first of every month for the previous month’s data. The report results are displayed in Microsoft Excel file format.

Table 20. Example of the Cisco MAP Hardware Inventory Report

Description: Identify Hardware Components Under Management				Customer/Site Name: Local				
Run Date: 2010-02-08				Run By: System				
Time Zone: EST								
Site Name	**Site Location**	**Device Name**	**Device IP Address**	**Device Type**	**Device Model**	**Device Serial Number**	**Contract Expiration Date**	**Date of Last Successful Backup**
Eric Wilcox	Syracuse, NY	Home-871-ewilcox	10.18.255.33	Router				
New Windsor Office	New Windsor, NY	Nw-st-2801-eg1	10.4.255.1	Router	Cisco 2801	FTX1031Y1GW		2010-02-08 09:53:32
New Windsor Office	New Windsor, NY	Nw-st-ap1231-1	10.4.1.160	Switch	Cisco 1231	FTX1135R0SC		2010-02-08 09:53:30
New Windsor Office	New Windsor, NY	Nw-st-c3524xl-1	10.4.1.100	Switch	Cisco 3500XL	FAB0603Q1G7		2010-02-08 09:53:30
New York City Office	New York, NY	Nyc-35-ap1231-1fl	10.5.1.160	Switch				2010-02-08 09:53:30
New York City Office	New York, NY	Nyc-35-ap1231-2fl	10.5.1.161	Switch				2010-02-08 09:53:29
New York City Office	New York, NY	Nyc-apcsu2200	10.5.1.22	Other	SmartUPS 2200			
New York City Office	New York, NY	Nyc-c3524-1	10.5.1.10	Switch				
New York City Office	New York, NY	Nyc-c3524-2	10.5.1.11	Switch				
New York City Office	New York, NY	Nyc-c3524-3	10.5.1.12	Switch				
New York City Office	New York, NY	Nyc-c3524-4	10.5.1.13	Switch				
New York City Office	New York, NY	Nyc-c3524xl-100	10.5.1.100	Switch				
New York City Office	New York, NY	Nyc3550-12g-1	10.5.2.1	Router				

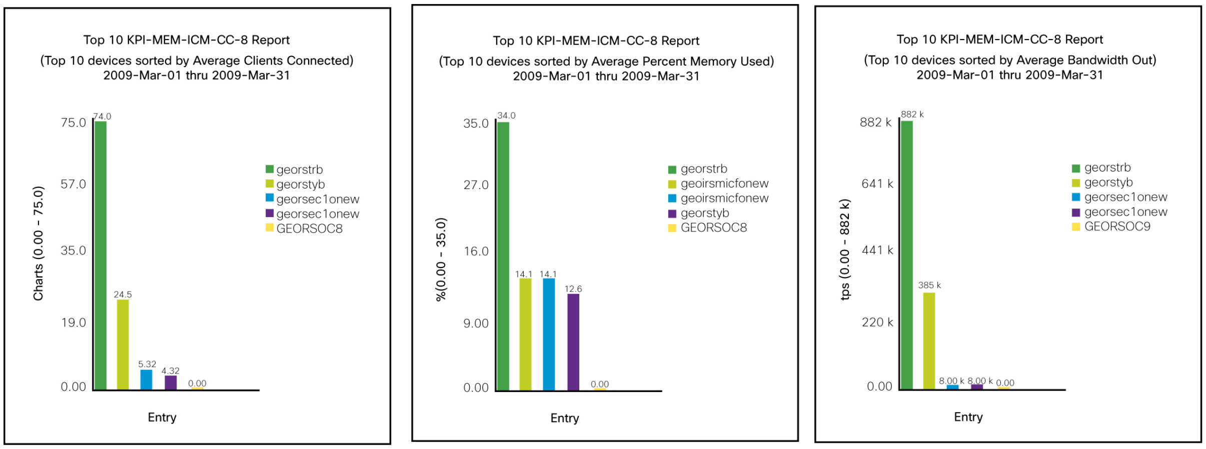
Site Name	Site Location	Device Name	Device IP Address	Device Type	Device Model	Device Serial Number	Contract Expiration Date	Date of Last Successful Backup
New York City Office	New York, NY	Nyc-hplj2200dn-1	10.5.2.15	Other	LaserJet 2200DN			
New York City Office	New York, NY	Nyc-hplj4050-1	10.5.2.14	Other				
New York City Office	New York, NY	Nyc-hplj4250-1	10.5.2.62	Other	LaserJet 2200DN			

Key Performance Indicators (KPI) Report

Key Performance Indicator (KPI) Reports enable a support organization to define desired performance levels for managed systems and application attributes, and measure progress toward their established goals. Establishing and managing to clear performance targets on a granular basis creates a process for continual operational improvement within the IT environment. Applications and systems falling below established benchmarks can be the focus for proactive replacement, upgrade or reconfiguration efforts to maximize availability and performance on an ongoing basis. Key Performance Indicator Reports are displayed in a PDF file format.

At the core of this report is the Cisco Management Application Platform's Performance Management application. Through extensive and continual performance monitoring of systems and applications across your network, the comprehensive database of performance metrics forms a vast knowledge-base from which KPI analysis is performed and results quantified. As longer-term views are frequently required to support effective KPI management, Cisco MAP archives and makes available up to one-year of performance data. Utilizing the Cisco Management Application Platform's Report Server, performance data may be provided for two years or more.

Figure 2. Example of the Cisco MAP Key Performance Graph of IPT Servers



Monthly Device Availability

The Monthly Device Availability Report displays percentage uptime and downtime for the previous two months. The report runs on a scheduled basis on the first of each month and will pull data for the previous two months. For example, a report run on July 1st will pull data for May and June. The report columns ‘This Period Avg Down Time %’ and ‘This Period Avg Uptime %’ would represent data for the month of June while columns ‘Last Period Avg Down Time %’ and ‘Last Period Avg Uptime %’ would represent data for the month of May. The up/downtime percentage is calculated by Cisco MAP from SNMP system uptime information obtained through polling each device. The report results are displayed in Microsoft Excel file format.

Note: Cisco MAP configuration is required before the Monthly Device Availability Report can be generated. Contact your Cisco MAP Customer Service Manager for additional information on configuring the Monthly Device Availability Report.

Table 21. Example of the Cisco MAP Device Availability Report

Description: Exception Report/Device Unavailability – All Devices Sorted By Availability (Lowest To Highest)						
Run Date: 2010-02-01			Customer/Site Name: Local			
Time Zone: EST			Overall Device Availability %: 100.00			
Site Name	**Device Description**	**This Period Avg Down Time %**	**Last Period Avg Down Time %**	**This Period Avg Uptime %**	**Last Period Avg Uptime %**	**SLA Target %**
New Windsor Office	Nw-st-2801-eg1	0.00	0.00	100.00	100.00	99.99
New Windsor Office	Nw-st-ap123-1	0.00	0.00	100.00	100.00	99.99
New Windsor Office	Nw-stc3524xl-1	0.00	0.00	100.00	100.00	99.99
New York City Office	Nyc-35-ap1231-1fl	0.00	0.00	100.00	100.00	99.99
New York City Office	Nyc-35-ap1231-2fl	0.00	0.00	100.00	100.00	99.99
New York City Office	Nyc-apcsu2200	0.00	0.00	100.00	100.00	99.99
New York City Office	Nyc-c3524-1	0.00	0.00	100.00	100.00	99.99
New York City Office	Nyc-c3524-1	0.00	0.00	100.00	100.00	99.99
New York City Office	Nyc-c3524-2	0.00	0.00	100.00	100.00	99.99
New York City Office	Nyc-c3524-3	0.00	0.00	100.00	100.00	99.99
New York City Office	Nyc-c3524-4	0.00	0.00	100.00	100.00	99.99
New York City Office	Nyc-c3524xl-100	0.00	0.00	100.00	100.00	99.99
New York City Office	Nyc3550-12g-1	0.00	0.00	100.00	100.00	99.99
New York City Office	Nyc-hplj4050-1	0.00	0.00	100.00	100.00	99.99
Boston	C2821-VXML-GW1	0.00	0.00	100.00	100.00	99.99

Site Name	Device Description	This Period Avg Down Time %	Last Period Avg Down Time %	This Period Avg Uptime %	Last Period Avg Uptime %	SLA Target %
Boston	C2851-CVP-GK2	0.00	0.00	100.00	100.00	99.99
Boston	Hplj4050	0.00	0.00	100.00	100.00	99.99
Boston	Bos-1pp-2811-g1	0.00	0.00	100.00	100.00	99.99

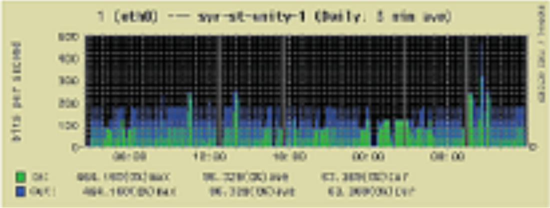
Performance Reports

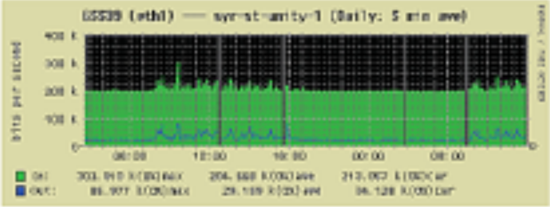
Performance Reports graphically display key network and server statistics in PDF file format. The statistics displayed are based on the same data gathering and processing methodology as used for KPI Reports.

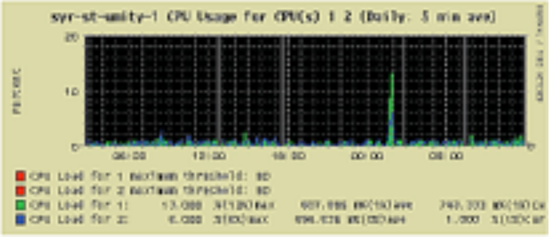
Note: Cisco MAP configuration is required before the Performance Reports can be generated. Contact your Cisco MAP Customer Service Manager for additional information on configuring the Performance Reports.

Table 22. Example of the Cisco MAP Performance Reports

Description: Performance Report For Components Under Management	Customer/Site Name: Local
Run Date: 2009-12-18 at 11:55:43	Run By: User
Time Zone: EST	
Charts For syr-st-unity1 – bw-eth0 : syr-st-unity – bweth1 – cpu2 : syr-st-unity-1 – cpu4	







Raw Bandwidth Report

The Raw Bandwidth Report provides the non-aggregated (raw) data for capacity planning and long-term reporting. The report results are displayed in CSV file format.

Table 23. Example of the Cisco MAP Raw Bandwidth Report

Raw Bandwidth Data Export

Created by Management Application Platform on Thu 25 Feb 2010 11:41:58-0500

Device	Date	Max In	Max Out	Average In	Average Out
Nyc-c3524xl-100	2/12/2010	8736.76	7901.25	2378.12	1987.34
Nyc-c3524xl-101	2/12/2010	6713.67	6783.78	4798.54	2365.81
Nyc-c3524xl-102	2/12/2010	7569.09	5132.89	3167.89	1578.61
Nyc-c3524xl-103	2/12/2010	5132.89	8736.76	4256.04	1827.48
Nyc-c3524xl-104	2/12/2010	6783.78	7569.09	2178.19	2002.79
Nyc-c3524xl-105	2/12/2010	7901.25	7569.09	3894.12	1631.45

Scheduled Outages

The Scheduled Outages Report lists outages by date, outage duration, and the devices affected by the outage for a defined time period. The report results are displayed in PDF file format.

Table 24. Example of the Cisco MAP Scheduled Outages Report

SCHEDULED OUTAGES REPORT

Group By Outage, Display Name
Start Time: 2012-08-19 23:59
End Time: 2012-09-18 23:59
Generated by Cisco ROS

Outage	Description	Start Date	End Date	Duration	Created By	Name
Replication issues between Logger and HDS see case 848.	Replication issues between Logger and HDS see case 848.	2009-09-06 20:00	2009-09-06 21:14	0d 1h 13m	User	C1760-1-Testlab

System Infrastructure Report

The System Infrastructure Report will provide detail on Cisco-specific hardware. This report will list IOS® devices, IOS® version, flash size, RAM size and modules installed for devices managed by Cisco MAP. Only devices that respond to SNMP queries will appear in the report. The report is automatically generated by Cisco MAP on the first of every month for the previous month’s data. The report results are displayed in Microsoft Excel file format.

Table 25. Example of the Cisco MAP System Infrastructure Report

Description: Identifies IOS® Image and Flash/RAM Per Managed Device					Customer/Site Name: iBank				
Run Date: 2010-05-14					Run By: System				
Time Zone: EDT									
Site Name	**Site Location**	**Device Name**	**Device IP Address**	**Device Model**	**Module Count**	**IOS® Version**	**IOS® Image Name**	**Flash (Bytes)**	**System RAM (Bytes)**
Corporate	NYC	Nyc-Telco1	XX.XX.XX.XX	CiscoAs5350XM	11	12	C5350-IS-M	128176128	1011858528
Corporate	NYC	Nyc-Telco2	XX.XX.XX.XX	CiscoAs5350XM	11	12	C5350-IS-M	128176128	1011858528
Corporate	NYC	Nyc-ipccpvt56	XX.XX.XX.XX	Cisco3845	11	12	C3845-IPVOICEK9-M	512065536	983655468
Corporate	NYC	Nyc-CCAP_2811	XX.XX.XX.XX	Cisco2811	3	12	C2800NM-ADVIPSERVICES	64225280	175099008
Corporate	NYC	Nyc-CCAP_2611	XX.XX.XX.XX	Cisco2611	0	12	C2600-I-M	8388608	17201508
Corporate	BOS	Bos-Telco2	XX.XX.XX.XX	Cisco3845	8	12	C3845-IPVOICEK9-M	64012288	178342208
Corporate	BOS	Bos-CCAP-2611	XX.XX.XX.XX	CiscoAs5350XM	3	12	C5350-IS-M	130273280	476815112
Corporate	BOS	Bos-Telco1	XX.XX.XX.XX	Cisco3845	7	12	C3845-IPVOICEK9-M	64012288	178353888
Corporate	BOS	Bos-ism-private-2811	XX.XX.XX.XX	Cisco3845	7	12	C3845-IPVOICEK9-M	64012288	178313360
Corporate	BOS	Bos-CCAP_2811	XX.XX.XX.XX	Cisco3845	7	12	C3845-IPVOICEK9-M	64012288	178347552
Corporate	BOS	Bos-CCAP-2611	XX.XX.XX.XX	Cisco3845	8	12	C3845-IPVOICEK9-M	64012288	178324624
Corporate	BOS	Bos-Telco3	XX.XX.XX.XX	Cisco3845	8	12	C3845-IPVOICEK9-M	64012288	178303552

Table 26. Example of the Cisco MAP System Infrastructure Report Displaying Modules Installed Per Managed Device

Description: Modules Installed Per Managed Device				Customer/Site Name: Local			
Run Date: 2009-12-01				Run By: System			
Time Zone: EST							
Device Name	**Device IP**	**CISCO3845-MB**	**WS-SVC-CMM**	**WS-SVC-CMM-24FXS**	**WS-SVC-CMM-6T1**	**WS-SVC-CMM-ACT**	**Counts**
NYBOMNCMM	10 xxx.xxx.xxx		1	2	1	1	5
NYBOMNCMM2	10 xxx.xxx.xxx		1	2	1	1	5
paovpkcmm	10 xxx.x.xx		1	1	1	1	4
nywamcmm	10 xxx.xxx.xx		1	2	1	1	5
cohnvacccmm	10 xxx.xx.xxx		1	2	1	1	5
cadblndcgtkpr	10 xx.xxx.xxx	1					1
nwlclncmm	10 xx.xx.xx		1	1	1	1	4
		1	6	10	6	6	

Top Active Devices

The Top Active Devices Report displays the devices and associated case numbers that have caused the most incidents during a given time period. The report results are displayed in CSV file format.

Table 27. Example of the Cisco MAP Top Active Devices Report

Active Devices Report Data Export	
Created by Management Application Platform 20100225132939	
Top Active Devices for the Date Range 2010-01-26 00:00:00 to 2010-02-24 23:59:59	
Device Name	**Number of Cases**
Syr-st-pgrb	19
Syr-pl-ivr-a	4
Syr-ccm7-pub	3
Syr-pl-pgra	3
Syr-st-bes-1	2
Device Name	**Case List**
Syr-st-pgrb	2323,2324,2343,2344,2346,2347,2348,2349,2350,2351,2352,2353,2354 2355,2356,2357,2358,2359
Syr-pl-ivr-a	2309,2310,2311,2312
Syr-ccm7-pub	2316,2320,2340
Syr-pl-pgra	2321,2322,2341
Syr-st-bes-1	2308,2336

Cisco Version Report

The Cisco Version Report gathers Cisco IOS®/CatOS version information by polling the devices listed in the Cisco Management Application Platform via SNMP. Although Cisco MAP can poll all monitored devices, the report is formatted and tailored around Cisco release conventions.

Note: The Cisco Version Report is generated for environments with Cisco IOS®/CatOS and Foundation devices.

Table 28. The Cisco Version Report Displays Hostname, IP Address, SNMP String and Version Information

Tools	Name	IP	SNMP_RO	Type	Version (OS)	Version (Revision)	Version (Release)
⚒	Nw-st-2801-eg1	10.4.255.1	Hav2guess	Cisco	IOS® 2800 Software (C2800NM-ADVENTERPRISEk9-M)	Version 12.4(15)T6	RELEASE SOFTWARE (fc2)
⚒	Nw-st-ap1231-1	10.4.1.160	Hav2guess	Cisco	IOS® C1200 Software (C1200-K9W&-M)	Version 12.3(8)JEB	RELEASE SOFTWARE (fc2)
⚒	Nw-st-c3524xl-1	10.4.1.100	Hav2guess	Cisco	IOS® C3500XL Software (C3500CL-C3H2S-M)	Version 12.0(5)WC17	RELEASE SOFTWARE (fc1) Copyright © 1986-2007 by Cisco Systems, Inc.
⚒	Ny-1pp-2811-g1	10.20.255.1	Hav2guess	Cisco	IOS® 2800 Software (C2800NM-ADVENTERPRISEK9-M)	Version 12.4(15)T5	RELEASE SOFTWARE (fc4)
⚒	Ny-35-3745-1	10.5.255.10	Hav2guess	Cisco	IOS® 3700 Software (C3745-ADVENTERPRISEK9-M)	Version 12.4(17)	RELEASE SOFTWARE (fc1)
⚒	Nyc-35-ap1231-1fl	110.5.1.160	Hav2guess	Cisco	IOS® C1200 Software(C1200-K9W7-M)	Version 12.3(7)JA	RELEASE SOFTWARE (fc1)

Table 28 Cont'd: The Cisco Version Report Displays Hostname, IP Address, SNMP String and Version Information

Tools	Name	IP	SNMP_RO	Type	Version (OS)	Version (Revision)	Version (Release)
⚒	Nyc-35-ap1231-2fl	10.5.1.161	Hav2guess	Cisco	IOS® C1200 Software(C1200-K9W7-M)	Version 12.3(7)JA	RELEASE SOFTWARE (fc1)
⚒	Nyc-c3524-1	10.5.1.10	Hav2guess	Cisco	IOS® C3500XL Software (C3500XL-C3H2S-M)	Version 12.0(5)WC17	RELEASE SOFTWARE (fc1) Copyright © 1986-2007 by cisco Systems,Inc.
⚒	Nyc-c3524-2	10.5.1.11	Hav2guess	Cisco	IOS® C3500XL Software (C3500XL-C3H2S-M)	Version 12.0(5)WC17	RELEASE SOFTWARE (fc1) Copyright © 1986-2007 by cisco Systems,Inc.
⚒	Nyc-c3524-3	10.5.1.12	Hav2guess	Cisco	IOS® C3500XL Software (C3500XL-C3H2S-M)	Version 12.0(5)WC17	RELEASE SOFTWARE (fc1) Copyright © 1986-2007 by cisco Systems,Inc.
⚒	Nyc-c3524-4	10.5.1.13	Hav2guess	Cisco	IOS® C3500XL Software (C3500XL-C3H2S-M)	Version 12.0(5)WC17	RELEASE SOFTWARE (fc1) Copyright © 1986-2007 by cisco Systems,Inc.

Cisco Content Services Switch (CSS) Report

The Content Services Switch (CSS) Report is a report for use by customers who have a Content Services Switch (CSS) as part of their Cisco Customer Voice Portal (CVP) solution. The report can be configured to display the services running on your Cisco CVP gateway devices. The report displays a summary of the monitored devices.

Note: The Cisco Content Services Switch (CSS) Report is configured for customers having a Cisco Content Services Switch in their Customer Voice Portal (CVP) environments.

Table 29. Example of the Cisco MAP CSS Dashboard Detail Report Displaying "All Services Group"

Services Summary						
Service Group	**CVP Related**	**Total Services**	**Alive**	**Down**	**Dying**	**Suspended**
ASR	Yes	2	0	2	0	0
APPSERVERS	Yes	1	1	0	0	0
MEDIA	Yes	1	1	0	0	0
TTS	No	1	0	1	0	0
VXML	Yes	1	0	1	0	0

Table 29 Cont'd: Example of the Cisco MAP CSS Dashboard Detail Report Displaying "All Services Group"

ASR

Service Name	State
ASR	Down
RICK	Down

APPSERVERS

Service Name	State
CVP3.1	Alive

MEDIA

Service Name	State
MEDIA	Alive

TTS

Service Name	State
TTS	Down

VXML

Service Name	State
VXML	Down

Content Services Switch (CSS) Dashboard

The Content Services Switch Detail Dashboard View displays the real time status of services on monitored Cisco Content Services Switch (CSS) devices. The dashboard view displays the Content Services Switch Summary

Report, a consolidated view of all Content Services Switches being monitored by Cisco MAP. The Content Services Switch Summary displays connection and rejection counts for managed Content Services Switches for

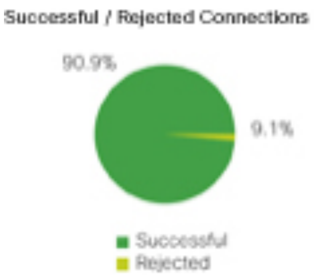
the previous 24 hours and a pie chart indicating the overall connection success rate. A separate area of the Content Services Switch Summary displays a list of all monitored CSS hosts and their associated status.

Table 30. Content Services Switch Server Summary Window

Wednesday, 16 Jun 2010 14:56:40 EDT

Content Services Switch Statistics (Last 24 Hours)

Statistic	Value
Total CSS Devices Polled	2
Total Connections	3786
Error Rejects	327
Overload Rejects	11
Total Rejects	6



Current Content Services Switch Statistics

Host Name	IP	Last Polled	Inst. CPU	Free Memory	Status	Current Connections
CSS11500	xx.xx.xx.xx.	2010-06-16 11:30:27	7%	127.2 MB	●	0
CSS11501	xx.xx.xx.xx.	2010-06-16 11:30:27	6%	127.2 MB	●	0

Clicking on a link found under the **Hostname** column of the **Content Services Switch Summary** window will display the **Content Services Switch Detail View**. The **Content Services Switch Detail View** consists of several subsections that offer an in-depth view of the CSS operational state. The information displayed provides a detailed view of a single CSS device and assists in quickly narrowing down the source and cause of an alarm.

Table 31. Content Services Switch Detail View Window

DEVICE INFORMATION		
Hostname: CSS11503-CSS1	**Product Name: CSS11501 N0**	**Serial Number:JMX12325043**
IP: XX.XX.XX.XX	**SW Version: 07.50.1.03**	**Base Mac Address: 00-22-55-d^-21-5c**

Slot #	Module Name	Status	Total Mem	Free Mem	CPU Load
1	CSS501-SCM-INT	Primary	256MB	127MB	4%

DOS ATTACK SUMMARY		
Last Clearing Of Stats Counter: 09/21/2009 14:45:46		
Attack Type	Count	Max Per Sec.
SYN	**67**	**12**
LAND	0	0
Illegal Src	0	0
Illegal Dest	0	0
Smurf	0	0
Total Attacks: 67		

CONTENT RULES

Content Name	Owner	Virtual IP: Port	Type	URL	Balance	Status	Total Conn.	Overload Reject	Total Reject	Last Cleared
VXML	SG	xx.xx.xx.xx: 7000	HTTP		Round Robin	Suspended	364728	0	327	09/21/2009 14:45:25
ASR	SG	xx.xx.xx.xx: 554	HTTP	/*	Round Robin	Active	8543	0	0	09/21/2009 14:45:25
TTS	SG	xx.xx.xx.xx: 554	HTTP		Round Robin	Active	6393	0	0	09/21/2009 14:45:25
MEDIA **- Media1** **- Media2**	SG	xx.xx.xx.xx: 80	HTTP		Round Robin	Active	9788620	93	0	09/21/2009 14:45:25

SERVICES

Service Name	Owner: Content	IP	Status	State Trans.	Load	Current Conn.	Total Conn.	Max Conn.	Last Cleared
VXML	SG: VXML	xx.xx.xx.xx	Down	8	255	0	364728	65543	09/21/2009 14:45:48
ASR	SG: ASR	xx.xx.xx.xx	Alive	0	9	22	8543	65543	09/21/2009 14:45:48
TTS	SG: TTS	xx.xx.xx.xx	Alive	0	9	15	6393	65543	09/21/2009 14:45:48
Media1	SG: MEDIA	xx.xx.xx.xx	Alive	0	69	87	4796239	65543	09/21/2009 14:45:48
Media2	SG: MEDIA	xx.xx.xx.xx	Dying	1	86	121	4992381	65543	09/21/2009 14:45:48

SOURCE GROUPS	
Last Clearing Stats Counter: 9/21/2009 14:45:46	
Group Names	Virtual IP
APPSERVERS	xx.xx.xx.xx
APPSERVERS	xx.xx.xx.xx
MEDIASERVERS **- Media1** **- Media2**	xx.xx.xx.xx

The subsections of the **Content Services Switch Detail View** provide the following information:

- **Device Information** – The **Device Information** section lists basic CSS information such as hostname, IP address, product name, software version, serial number and MAC address. It also lists modules installed in the chassis alone with simple memory and CPU load.
- **DOS Attack Summary** – The CSS is the gateway to application services and is likely to receive large numbers of connections from clients. In a Customer Voice Portal (CVP) configuration, this is further complicated as clients are VXML gateways making large numbers of concurrent connections from a single client. This type of connection "flooding" by a single device can sometimes be interpreted as a Denial of Service (DOS) attack, causing the CSS to reject connections. Therefore, it is important to monitor the DOS counters to determine if the rejections are due to DOS protection. This section provides a breakdown of the attack types and the rate of attacks. If an attack is observed, further analysis is necessary to determine the source of the connections/attacks.
- **Content Rules** – This section lists all rules configured on the CSS. Each rule displayed expands to show the associated service. The services will display a simple Red, Yellow, Green icon to indicate the status of the service. Content Rule detail information displayed includes the content rule owner, virtual IP and port of the rule, traffic type, URL pattern, balance method, and rule status. Total connections, overload rejects counts, and total reject counts per content rule are also displayed.
- **Services** – The Services section contains a list of services available to the CSS and the operational state of the service. Each service entry includes service name, associated owner/content rule, IP of the service, status, state transition count, and service load. Counters for current, maximum, and total connections are also displayed.
- **Source Groups** – Source Groups are used to return traffic with the virtual IP address as the source IP address. Used in conjunction with Content Rules, Source Groups allow the client/session to communicate with the same destination and return source IP address. As Source Groups are added to the CSS, each IP address will allow additional connection ports, necessary in large, high volume deployments. Source Groups provide validation of proper configuration when compared to the associated Content Rule.

Note: The CSS Dashboard View is only available to customers having a Cisco Content Services Switch in their networked environment.

Note: Cisco MAP configuration is required before the CSS Dashboard View can be generated. Contact your Cisco MAP Customer Service Manager for additional information on configuring the Content Services Switch (CSS) Dashboard.

Switch Port Information Report

The Switch Port Information Report provides network port level information across all switches.

Table 32. Example of the Cisco MAP Switch Port Information Report

SEARCH: Entity to Search: All

Status: Access Ports Only

Tools	Switch Name	Switch IP Address	Switch MAC Address	Switch Port	Disco very	VLAN	Device Port	Device MAC Address	Device IP Address	Tools	Application Platform Name	DNS Name
🔨	Nw-st-ap1231-1	10.4.1.160	00:07:0e:5b:6f:af	Fa0	cdp		Fa0/2	00:08:a3:2d:eb:42	10.4.1.100	🔨	Nw-st-c3524xl-1:ICMP:	
🔨	Nw-st-c3524xl-1	10.4.1.100	00:08:a3:2d:eb:52	Fa0/18	cdp		Po1	00:18:19:25:2a:f6	10.4.10.107			
🔨	Nw-st-c3524xl-1	10.4.1.100	00:08:a3:2d:eb:47	Fa0/7	Bridge	2		00:c0:b7:a3:01:e3	10.4.2.5			
🔨	Nw-st-c3524xl-1	10.4.1.100	00:08:a3:2d:eb:4d	Fa0/13	cdp		Po1	00:18:18:d7:59:37	10.4.10.121			
🔨	Nw-st-c3524xl-1	10.4.1.100	00:08:a3:2d:eb:58	Fa0/24	cdp		Po1	00:18:19:0e:2f:87	10.4.10.103			
🔨	Nw-st-c3524xl-1	10.4.1.100	00:08:a3:2d:eb:51	Fa0/17	cdp		Po1	00:18:19:16:71:a6	10.4.10.120			

System Uptime

The System Uptime Report enables the export of availability data that Cisco MAP has obtained through SNMP Get requests on monitored network objects. This report can be used to help identify problem areas on the network.

Table 33. Example of the Cisco MAP System Uptime Report

System Uptime Report Data Export

Created by Management Application Platform 20100225151449

System Name	IP Address	Up Time
Ny-1pp-2811-g1	10.20.255.1	22w4d17h25m84s
Nyc-pl-2811-wan2	10.15.255.11	1y9w4d17h13m41s
Nyc-pl-ccm6-sub	10.15.10.242	2w0d12h57m18s
Nyc-pl-ivr-a	10.15.10.234	2w1d13h40m17s
Nyc-st-2811-wan1	10.16.255.10	1y15w2d13h11m56s
Nyc-st-3745-vpn1	10.16.2.250	1y15w2d12h38m29s
Nyc-st-bfs-1	10.16.2.110	1w0d11h9m54s
Nyc-st-c3560-core1	10.16.255.252	1y15w2d13h21m13s
Nyc-st-c3560-core2	10.16.255.253	1y15w2d14h19m12s
Nyc-st-ccm6-sub	10.16.10.242	2w0d13h2m43s
Nyc-st-dc-1	10.16.2.100	9w0d23h37m2s
Nyc-st-dmxl-1	10.16.80.120	1y7w6d4h25m2s
Nyc-st-dmxl-2	10.16.80.121	1y7w6d4h20m52s
Nyc-st-intersvr-1	10.16.80.100	1y15w2d9h13m44s
Nyc-st-ipivr-b	10.16.10.234	2w1d13h31m25s
Nyc-st-mpx1-rtmp	10.16.100.140	No SNMP Response

System Name	IP Address	Up Time
Nyc-st-mpx1-voip	10.16.100.135	17w5d16h12m55s
Nyc-st-tmis-1	10.16.80.125	11h12m5s
Nyc-st-unity-1	10.16.10.220	7w2d15h58m38s
Nyc-st-unity-2	10.16.10.221	16w4d18h55m59s

Configuration Manager Application and Reporting

System administrators face a variety of challenges managing the configuration of devices that they administer – events such as an admin changing a device configuration without informing the team or not having a rollback plan in place to restore back to a functioning point in case configuration errors are made. The Cisco MAP Configuration Manager application is designed to address the need for system and network administrators to effectively manage system configurations.

Configuration Manager has been designed to meet the configuration file retrieval, change alert, and disaster recovery needs of system administrators. At its core, the Cisco MAP Configuration Manager creates and maintains a repository of device configuration files. Configuration Manager can gather configuration files for Cisco IOS® devices.

With Cisco MAP Configuration Manager, an administrator will be able to:

- Have on-demand access to currently loaded configuration files from an easy-to-use GUI.
- Store the device configuration for backup and rollback and would be able to track the changes made and the user involved in making the changes.
- Conduct scheduled device configuration retrieval. Available scheduling options include Daily, Weekly, or Monthly.
- Receive notifications via email or pager if a device configuration has changed.
- Have access to all the previous versions of the device configurations, and can track device configuration changes over time.

Enabling Device for Configuration Manager

The Configuration Manager Application and Reporting feature requires configuration settings to be enabled for devices within Cisco MAP. Please contact your Cisco MAP Customer Service Manager to discuss the devices you want to enable configuration management on.

At least one (1) device must be configured to use Configuration Manager for Configuration Manager Reports to be enabled.

Switch Port Information Report provides network port level information across all switches.

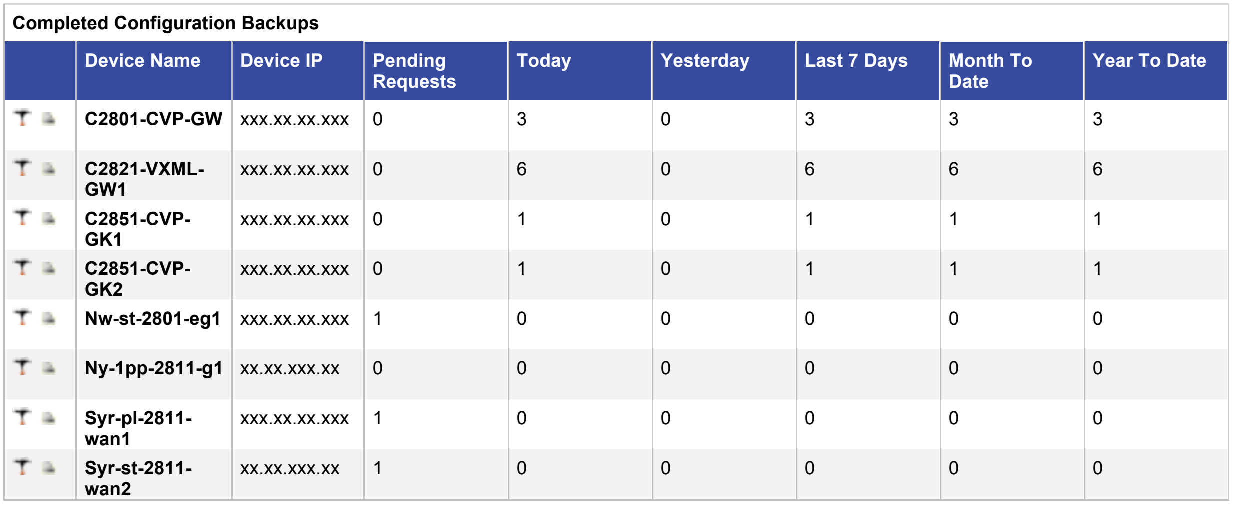
Note: The Configuration Manager Application and Reporting feature is configured for environments with Cisco IOS®/CatOS and Foundation devices.

Configuration Manager Reporting

The Configuration Manager Device Activity Summary page opens in a new browser window.

1. The Completed Downloads tab on the Configuration Manager – Device Activity Summary page provides:
   - A link to Entity Manager via the Tools icon.
   - The ability to download a history log for each device listed.
   - The device name.
   - The device IP address (clicking on the device IP address will redirect the user to the Device Configuration Management page for that particular device).
   - The Completed Configuration Backups section of the page provides information on the number of backups completed Today, Yesterday, Last 7 Days, Month to Date, and Year to Date.

Table 34. Completed Downloads Tab



Completed Configuration Backups

	Device Name	Device IP	Pending Requests	Today	Yesterday	Last 7 Days	Month To Date	Year To Date
	C2801-CVP-GW	xxx.xx.xx.xxx	0	3	0	3	3	3
	C2821-VXML-GW1	xxx.xx.xx.xxx	0	6	0	6	6	6
	C2851-CVP-GK1	xxx.xx.xx.xxx	0	1	0	1	1	1
	C2851-CVP-GK2	xxx.xx.xx.xxx	0	1	0	1	1	1
	Nw-st-2801-eg1	xxx.xx.xx.xxx	1	0	0	0	0	0
	Ny-1pp-2811-g1	xx.xx.xxx.xx	0	0	0	0	0	0
	Syr-pl-2811-wan1	xxx.xx.xx.xxx	1	0	0	0	0	0
	Syr-st-2811-wan2	xx.xx.xxx.xx	1	0	0	0	0	0

2. The Detected Changes/Commits tab on the Configuration Manager – Device Activity Summary window provides:
   - A link to Entity Manager via the Tools icon.
   - The ability to download a history log for each device listed.
   - The device name.
   - The device IP address (clicking on the device IP address will direct the user to the Device Configuration Management window for that particular device).
   - The Detected Configuration Changes/Commits section of the window provides information on the number of detected configuration changes and commits for Today, Yesterday, Last 7 Days, Month to Date, and Year to Date.

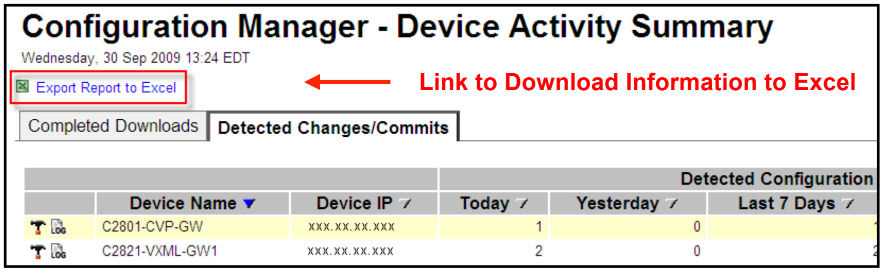
Table 35. Detected Changes/Commits Tab

Detected Configuration Changes / Commits

	Device Name	Device IP	Today	Yesterday	Last 7 Days	Month To Date	Year To Date
	C2801-CVP-GW	xxx.xx.xx.xxx	1	0	1	1	1
	C2821-VXML-GW1	xxx.xx.xx.xxx	2	0	2	2	2
	C2851-CVP-GK1	xxx.xx.xx.xxx	1	0	1	1	1
	C2851-CVP-GK2	xxx.xx.xx.xxx	1	0	1	1	1
	Nw-st-2801-eg1	xxx.xx.xx.xxx	0	0	0	0	0
	Ny-1pp-2811-g1	xx.xx.xxx.xx	0	0	0	0	0
	Syr-pl-2811-wan1	xxx.xx.xx.xxx	0	0	0	0	0
	Syr-st-2811-wan2	xx.xx.xxx.xx	0	0	0	0	0

3. You can also download Configuration Manager reports to Microsoft Excel by clicking on the Export Report to Excel link.

Figure 3. Export Reports To Excel Link



Configuration Manager - Device Activity Summary

Wednesday, 30 Sep 2009 13:24 EDT

Export Report to Excel

Link to Download Information to Excel

Completed Downloads | Detected Changes/Commits

			Detected Configuration		
	Device Name	Device IP	Today	Yesterday	Last 7 Days
	C2801-CVP-GW	xxx.xx.xx.xxx	1	0	1
	C2821-VXML-GW1	xxx.xx.xx.xxx	2	0	2

IP Technology Management Reports

The Cisco Management Application Platform’s IP Telephony Management Reporting provides insight into understanding how your IP Telephony system is being used and the service levels it is delivering. Having a firm grasp on knowing whether or not you’re achieving agreed upon service levels and understanding how to properly plan for meeting future capacity requirements has always been a problem for network, telecom, and operations managers. Visibility into utilization and performance trends are needed to identify inefficient use of existing infrastructure, understand the impact on the business as well as to effectively plan for the future.

The Cisco Management Application Platform’s IP Telephony Management Reports will help you to realize and monitor capacity requirements in your current IP Telephony deployment as well as planning for tomorrow. You’ll be able to proactively demonstrate how your IP Telephony services are performing against KPIs and/or SLAs, and identify and troubleshoot problem trends in your IP Telephony environment

Active Phone Report

The Active Phone Report lists all phones that have placed a call (was active) in the previous month. Depending on customer needs, the report will query for all extensions or just unique extensions to build the content of the report.

Cisco MAP checks Cisco Unified Communications Manager (CallManager) records every 4 hours to see if a phone has been recently used. If any one of the polls during the month finds that a phone had recently made a call, it is determined to be an Active (in use) phone and an entry is made into a system table. At the beginning of each month, the system table is read and a listing of the details for each phone is determined to be in either an 'Active' or 'Unknown' state for the previous month, and saves the resultant file as a Microsoft Excel workbook. This workbook consists of two worksheets:

- The **Active Phone Report** worksheet displays the Site Name, Site Location, CallManager (CM) Hostname, CallManager (CM) IP Address, Device Type, Device IP, Device MAC Address/Registration ID, Device Description, and the date and time Last Registered for each phone.

Table 36. Example of the Cisco MAP Active Phone Report

Description: Identifies Active Phones At The Time That The Report Is Generated								
Run Date: 2012-09-10								
Time Zone: MST								
Run By: System								
Site Name	**Site Location**	**CM Hostname**	**CM IP Address**	**Device Type**	**Device IP**	**Device MAC Address / Registration ID**	**Device Description**	**Last Registered**
Syracuse, NY	Syracuse, NY	Syr-pl-sub-1	xxx.xx.xxx.xx	Subscriber	xxx.xx.xxx.xx	SEP003094C340CC	Username	2012-08-01 00:07:08
Syracuse, NY	Syracuse, NY	Syr-pl-sub-1	xxx.xx.xxx.xx	Subscriber	xxx.xx.xxx.xx	SEP00170E6DC999	Username	2012-08-01 00:07:08
Syracuse, NY	Syracuse, NY	Syr-pl-sub-1	xxx.xx.xxx.xx	Subscriber	xxx.xx.xxx.xx	SEP003094C443F2	Username	2012-08-01 00:07:08
Syracuse, NY	Syracuse, NY	Syr-pl-sub-1	xxx.xx.xxx.xx	Subscriber	xxx.xx.xxx.xx	SEP003094C347E7	Username	2012-08-01 00:07:08
Syracuse, NY	Syracuse, NY	Syr-pl-sub-1	xxx.xx.xxx.xx	Subscriber	xxx.xx.xxx.xx	SEP0018B93BACA5	Username	2012-08-01 00:07:08
Syracuse, NY	Syracuse, NY	Syr-pl-sub-1	xxx.xx.xxx.xx	Subscriber	xxx.xx.xxx.xx	SEP003094C44602	Username	2012-08-01 00:07:08
Syracuse, NY	Syracuse, NY	Syr-pl-sub-1	xxx.xx.xxx.xx	Subscriber	xxx.xx.xxx.xx	SEP000E84C05E4E	Username	2012-08-01 00:07:08
Syracuse, NY	Syracuse, NY	Syr-pl-sub-1	xxx.xx.xxx.xx	Subscriber	xxx.xx.xxx.xx	SEP003094C3410A	Username	2012-08-01 00:07:08

- The second worksheet, **Active Phone Summary**, displays a month-to-month total number of active phones.

Table 37. The Active Phone Summary Tab

Description: Identifies Active Phones At The Time That The Report Is Generated		
Run Date: 2012-08-20	Customer / Site Name: syrsmvm-tst14	
Time Zone: EDT	Run By: System	
Month	**Active Phones (Max)**	**Active Phones (Peak)**
10-2009	313	
11-2009	325	
12-2009	341	
01-2010	493	
02-2010	322	
03-2010	792	
04-2010	43100	
05-2010	43510	
06-2010	43938	0
07-2010	44432	0

Note: The Active Phone Report is configured for customers with a Cisco CM/Unity environment.

CallManager License Count Report

License management administrators need accurate licensing information for Cisco Unified Communications Manager applications and the number of devices to compare it with the number of license units that have been purchased. Having up-to-date licensing information helps in the management of Cisco Unified Communications Manager and enforces the licenses for Cisco Unified Communications Manager applications and the number of devices. This provides the ability to plan for additional capacity before reaching a critical state as well as aiding in troubleshooting customer related issues.

For customers having a Unified Communications environment with a Cisco Unified Communications Manager (CUCM) as an element of their environment, a new CUCM (CallManager) License Count Report and license usage alerting feature is available with the installation of this patch file. This enhancement enables Cisco MAP to gather phone and node license usage data from CallManagers, defined as entities within Cisco MAP, on a daily basis, storing such information in the Cisco MAP database for historical reporting and alerting functions.

CallManager license reporting and license threshold alerting are related but separate functions; a customer with the appropriate environment may elect to utilize only one of the features or both of the features.

If configured, the **CallManager License Count Report**, by default, will generate a weekly report in Microsoft Excel file format and will open with the **Maximum Levels** tab displayed. The report will provide a 30-day history, from the date it is generated, of CallManager license usage in both summary and daily detail views.

Table 38. Example of the Maximum Levels Tab In Association With The CallManager Cluster Defined To Cisco MAP

Description: Shows CallManager License Unit Maximum Levels For Report Period, and Historical Maximum Levels									
Time Period: 2011-08-07 through 2011-09-16								Time Zone: EST	
Run Date: 2011-09-16								Run By: System	
				Historical Max Levels *				**Historical Max Levels ***	
CallManager Publisher	**CallManager IP**	**Max Phone Units Authorized – Report Period**	**Max Phone Units Used – Report Period**	**Max Phone Units Used - Historical**	**Date of Phone Units Used Max Level - Historical**	**Max Node Units Authorized – Report Period**	**Max Node Units Used – Report Period**	**Max Node Units Used - Historical**	**Date of Node Units Used Max Level - Historical**
zSys-ccm7-pub	xx.xx.xx.xx	2000	318	318	13-Aug-11	8	4	4	17-Aug-11
zSys-ccm6-pub	xx.xx.xx.xx	2000	371	371	14-Jul-11	8	4	4	14-Aug-11
	Totals:	**4000**	**689**	**689**		**16**	**8**	**8**	
* Reflects maximum level reached since data collection began.									
NOTE: “Maximum” for use in this report defined as the highest count reached.									
NOTE: Number of phone license units may be different from number of phone sets, as different phones require different numbers of license units. Please see your Cisco CallManager documentation for more information.									

The **Maximum Levels** tab provides information on the following:

- The name and IP address of each CallManager Publisher in a CallManager cluster defined to Cisco MAP.
- The maximum number of phones authorized for use with each cluster and the number actually used during the reporting period.
- Historical information regarding the maximum number of phones used and the date that the maximum level was reached.

Note: The date that the maximum level of phones used was reached can fall outside of the reporting period for the report.

- A node license is required for each server in a CallManager cluster.
- The **Maximum Levels** tab will also show the maximum node units authorized as well as the maximum node units used during the reporting period.
- Historical information regarding the maximum number of node units used and the date that the maximum number of node units was reached.

Note: The date that the maximum number of node units was reached can fall outside of the reporting period for the report.

The **Daily Detail** tabs provide information on the following:

- The name of each CallManager Publisher in a CallManager cluster defined to Cisco MAP and its IP address.
- The number of phone units authorized for use with each cluster and the number actually used during the reporting period.
- The percentage of phone units used and remaining during the reporting period.
- The number of node units authorized as well as node units used by each cluster for each day during the reporting period.
- The percentage of node units used and node units remaining by each cluster for each day during the reporting period.

Table 39. Example Of The Daily Detail Tap In Association With The CallManager License Count Report

Description: Shows CallManager License Units Available and In Use									
Time Period: 2011-08-17									Time Zone: EDT
Run Date: 2011-09-16									Run By: System
CallManager Publisher	**CallManager IP**	**Phone Units Authorized**	**Phone Units Used**	**Percent Phone Units Used**	**Phone Units Remaining**	**Node Units Authorized**	**Node Units Used**	**Percent Node Units Used**	**Node Units Remaining**
zSys-ccm7-pub	xx.xx.xx.xx	2000	318	16.00%	1682	8	4	50.00%	4
zSys-ccm6-pub	xx.xx.xx.xx	2000	371	18.50%	1629	8	4	50.00%	4
	Totals:	**4000**	**689**			**16**	**8**		**8**
NOTE: Number of phone license units may be different from number of phone sets, as different phones require different numbers of license units. Please see your Cisco CallManager documentation for more information.									

Note: A phone license and a phone type do not necessarily have a 1-to-1 correspondence. For example, each phone type requires a fixed number of licenses and this number is called a phone license unit. For example, Cisco 7920 phones require four (4) license units and Cisco 7970 phones require five (5) license units.

Note: A node license is required for each server in a CallManager cluster.

CallManager License Count Usage Threshold Alerting

When CallManager license count alerting is enabled, threshold values (and how often an alert will be generated if a threshold is exceeded) can be configured for the phone and/or node licenses associated with each CallManager defined in Cisco MAP. If the phone or node license threshold value is exceeded, a Cisco MAP AutoCase will be opened. License count alerts can be configured to generate on a daily, weekly or monthly basis and can be defined to open at a Priority 2 (P2), Priority 3 (P3), or Priority 4 (P4) level; license count threshold alerts are not opened at a Priority 1 (P1) case.

For Cisco MAP customers, CallManager license threshold AutoCases can be configured to open at a priority that best fits the customer environment. Cisco Remote Management Services (RMS) customers will be alerted to CallManager license threshold violations by Cisco RMS staff.

H323 Voice Gateway Traffic Report

The H323 Voice Gateway Traffic Report provides utilization data particular to the H.323 protocol standard for multimedia communications over IP networks, including audio, video, and data conferencing. The H323 Voice Gateway Traffic Report will be of particular interest to Cisco MAP customers having an IP Telephony (IPT) environment with Cisco Voice Gateways. The report results are displayed in Microsoft Excel file format.

The H323 Voice Gateway Traffic Report Microsoft Excel workbook consists of two parts: a monthly Summary worksheet and Daily Detail worksheets displaying hourly detail for each day of the month. The Summary worksheet, which displays upon opening the report, provides running daily totals for each registered voice gateway for the current month. The Daily worksheets detail hourly totals for each registered voice gateway for the previous day(s) of the current month. The H323 Gateway Traffic Report is automatically generated by Cisco MAP on the first of every month for the previous month's data.

Table 40. Example of the H323 Voice Gateway Traffic Report Summary Worksheet

Description: Provides Max DS0s In Use and Busy Seconds Per Gateway. See Daily Tabs For Hourly Statistics										
Run Date: 2010-01-04										
Time Zone: EST										
Run By: System										
Voice Gateway Name	**DS0s Available**	**Total Calls**	**Seconds In**	**Seconds Out**	**Total Seconds**	**Busy Hour**	**Erlangs**	**Max DS0s In Use**	**% DS0s In Use**	**Seconds Busy**
De-newark-telco2	184	86,913	5,812,483	22,441,416	28,253,899	Mon 28 Dec 2009 1-2PM	76	106	57.6%	0
De-newcastle-telco1	184	259,815	98,272,359	0	98,272,359	Mon 28 Dec 2009 12-1PM	130	138	75.0%	0
De-newcastle-telco2	184	254,005	73,074,788	6,658,597	79,733,385	Mon 28 Dec 2009 12-1PM	110	128	69.6%	0

Table 43 Cont'd. Example of the H323 Voice Gateway Traffic Report Summary Worksheet

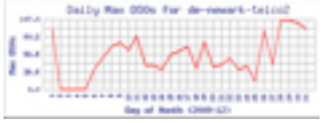
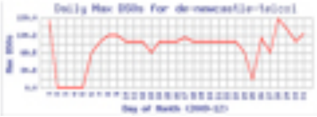
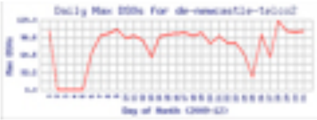
MAX DS0s Daily Trend




Table 41. Example of the H323 Voice Gateway Traffic Report Daily Detail Worksheet

Description: Provides Hourly Call Counts, Erlangs and Busy Seconds Per Gateway

Run Date: 2010-01-04

Time Zone: EST

Run By: System

Hour	Voice Gateway Name	DS0s Available	Calls In	Calls Out	Total Calls	Seconds In	Seconds Out	Total Seconds	Erlangs	Max DS0s In Use	% DS0s In Use	Seconds Busy
Tuesday 1 December 2009 12AM-AM	Bos-CiscoCCM-telco1	184	6	0	6	1.963	0	1,963	1	2	1.1%	0
Tuesday 1 December 2009 12AM-AM	Bos-CiscoCCM-telco2	184	0	38	38	0	9,915	9,915	3	7	3.8%	0
Tuesday 1 December 2009 12AM-AM	Bos-CiscoCCM-telco1	184	59	0	59	9,831	0	9.831	3	7	3.8%	0
Tuesday 1 December 2009 12AM-AM	Bos-CiscoCCM-telco2	184	156	4	160	48,741	130	48,871	14	23	12.5%	0
Tuesday 1 December 2009 12AM-AM	Bos-CiscoCCM-telco3	184	3	0	3	2,010	0	2,010	1	2	1.1%	0
Tuesday 1 December 2009 12AM-AM	Bos-CiscoCCM-telco4	161	0	33	33	0	14,243	14,243	4	6	3.7%	0
Tuesday 1 December 2009 12AM-AM	Bos-CiscoCCM-telco5	161	0	2	2	0	295	295	0	2	1.2%	0
Tuesday 1 December 2009 12AM-AM	LA-CiscoCCM-telco1	138	0	0	0	0	0	0	0	0	0.0%	0
Tuesday 1 December 2009 12AM-AM	LA-CiscoCCM-telco2	46	0	0	0	0	0	0	0	0	0.0%	0

Hour	Voice Gateway Name	DS0s Available	Calls In	Calls Out	Total Calls	Seconds In	Seconds Out	Total Seconds	Erlangs	Max DS0s In Use	% DS0s In Use	Seconds Busy
Tuesday 1 December 2009 12AM-AM	Atl-CorpHQ-telco1	184	11	0	11	2,913	0	2,913	1	3	1.6%	0
Tuesday 1 December 2009 12AM-AM	Atl-CorpHQ-telco2	184	43	0	43	11,061	0	11,061	3	10	5.4%	0

Note: The H323 Gateway Traffic Report is configured for Cisco CallManager/Unity and Customer Voice Portal (CVP) environments.

Media Gateway Control Protocol (MGCP) Traffic Report

The MGCP Traffic Report derives utilization data from Cisco CDR records that is particular to the MGCP standard used to control Voice over IP (VoIP) calls by external call-control devices such as media gateway controllers (MGCs) or call agents (CAs). The MGCP Traffic Report Microsoft Excel workbook consists of two parts: a Monthly Summary worksheet and Daily Detail worksheets displaying hourly detail for each day of the month.

Table 42. Example Of The MGCP Traffic Report Summary Worksheet

Description: Provides Monthly Total Call Counts, and Busy Hour Erlangs, Max Ports In Use and Busy Seconds Per MGCP Gateway. See Daily Tabs For Hourly Statistics.

Run Date: 2010-02-24

Time Zone: EST

Run By: System

CCM Cluster	MGCP Gateway	Ports Availa-ble	Calls Orig	Calls Recv	Total Calls	Seconds Orig	Seconds Recv	Total Seconds	Busy Hour	Erlan-gs	Max Ports In Use	% Ports In Use	Seconds Busy
NPPUB	Alb_2821.iBank.com	27	3,915	2,749	6,664	553,845	782,666	1,336,511	Tues 1 Dec 2009	4	10	37.0%	0
NPPUB	Buf_2821.iBank.com	27	4,052	3,601	7,653	635,400	1,001,381	1,636,781	Fri 4 Dec 2009	6	11	40.7%	0
NPPUB	Chi_2821.iBank.com	27	4,979	4,974	9,953	804,979	1,213,027	2,018,006	Wed 9 Dec 2009	9	13	48.1%	0
NPPUB	Li_3825.iBank.com	27	7,644	7,012	14,656	1,308,008	1,529,168	2,837,176	Thur 10 Dec 2009	9	14	51.9%	0

Table 45 Cont'd. Example Of The MGCP Traffic Report Summary Worksheet

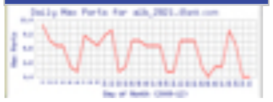
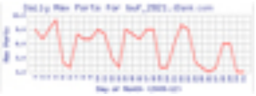
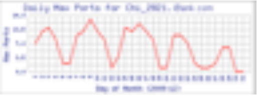
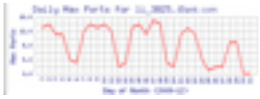
MAX Ports Daily Trend





Table 43. Example Of The MGCP Traffic Report Daily Detail Worksheet

Description: Provides Hourly Call Counts, Erlangs and Busy Seconds Per MGCP Gateway

Run Date: 2010-02-24

Time Zone: EST

Run By: System

Hour	CCM Cluster	MGCP Gateway	Ports Availa-ble	Calls Orig	Calls Rec	Total Calls	Seconds Orig	Seconds Rec	Total Seconds	Erla-ngs	Max Ports In Use	% Ports In Use	Seconds Busy
Sat 5 Dec 2009 1-2PM	iBPUB	MAN_2821.iBank.com	27	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 1-2PM	iBPUB	Nyc_3845.iBank.com	99	9	18	27	251	2,058	2,309	1	2	2.0%	0
Sat 5 Dec 2009 1-2PM	iBPUB	PRS_3825.iBank.com	34	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 1-2PM	iBPUB	Roc_3825.iBank.com	123	12	3	15	1,972	60	2,032	1	3	2.4%	0
Sat 5 Dec 2009 1-2PM	iBPUB	Sf_3845.iBank.com	76	44	0	44	274	0	274	0	1	1.3%	0
Sat 5 Dec 2009 1-2PM	iBPUB	Sha_2821.iBank.com	32	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 1-2PM	iBPUB	Ska_2821.iBank.com	1	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 1-2PM	iBPUB	Sv_2821.iBank.com	27	1	0	1	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 1-2PM	iBPUB	VGC1647668d95xx	60	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 1-2PM	iBPUB	Wpb_2821.iBank.com	27	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 2-3PM	iBPUB	Alb_2821.iBank.com	27	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 2-3PM	iBPUB	Buf_2821.iBank.com	27	4	2	6	1,432	323	1,755	0	2	7.4%	0
Sat 5 Dec 2009 2-3PM	iBPUB	Chi_2821.iBank.com	27	0	0	0	0	-	0	0	0	0.0%	0
Sat 5 Dec 2009 2-3PM	iBPUB	Li_3825.iBank.com	27	1	2	3	280	79	359	0	1	3.7%	0

Hour	CCM Cluster	MGCP Gateway	Ports Available	Calls Orig	Calls Rec	Total Calls	Seconds Orig	Seconds Rec	Total Seconds	Erlangs	Max Ports In Use	% Ports In Use	Seconds Busy
Sat 5 Dec 2009 2-3PM	iBPUB	MAN_2821.iBank.com	27	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 2-3PM	iBPUB	Nyc_3845.iBank.com	99	3	3	6	356	1,039	1,395	0	2	2.0%	0
Sat 5 Dec 2009 2-3PM	iBPUB	PRS_3825.iBank.com	34	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 2-3PM	iBPUB	Roc_3825.iBank.com	123	21	3	24	2,023	144	2,167	1	3	2.4%	0
Sat 5 Dec 2009 2-3PM	iBPUB	Sf_3845.iBank.com	76	1	2	3	156	13	169	0	1	1.3%	0
Sat 5 Dec 2009 2-3PM	iBPUB	Sha_2821.iBank.com	32	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 2-3PM	iBPUB	Ska_2821.iBank.com	1	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 2-3PM	iBPUB	Sv_2821.iBank.com	27	2	0	2	33	0	33	0	1	3.7%	0
Sat 5 Dec 2009 2-3PM	iBPUB	VGC1647668d95xx	60	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 2-3PM	iBPUB	Wpb_2821.iBank.com	27	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 3-4PM	iBPUB	Alb_2821.iBank.com	27	1	1	2	90	90	180	0	2	7.4%	0
Sat 5 Dec 2009 3-4PM	iBPUB	Buf_2821.iBank.com	27	2	0	2	286	0	286	0	1	3.7%	0
Sat 5 Dec 2009 3-4PM	iBPUB	Chi_2821.iBank.com	27	2	0	2	105	0	105	0	1	3.7%	0
Sat 5 Dec 2009 3-4PM	iBPUB	Li_3825.iBank.com	27	3	1	4	210	112	322	0	2	7.4%	0
Sat 5 Dec 2009 3-4PM	iBPUB	MAN_2821.iBank.com	27	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 3-4PM	iBPUB	Nyc_3845.iBank.com	99	3	3	6	330	134	464	0	2	2.0%	0
Sat 5 Dec 2009 3-4PM	iBPUB	PRS_3825.iBank.com	34	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 3-4PM	iBPUB	Roc_3825.iBank.com	123	11	4	15	2,096	199	2,295	1	2	1.6%	0
Sat 5 Dec 2009 3-4PM	iBPUB	Sf_3845.iBank.com	76	0	2	2	0	233	233	0	1	1.3%	0
Sat 5 Dec 2009 3-4PM	iBPUB	Sha_2821.iBank.com	32	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 3-4PM	iBPUB	Ska_2821.iBank.com	1	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 3-4PM	iBPUB	Sv_2821.iBank.com	27	0	0	0	0	0	0	0	0	0.0%	0
Sat 5 Dec 2009 3-4PM	iBPUB	VGC1647668d95xx	60	0	0	0	0	0	0	0	0	0.0%	0

Note: The MGCP Traffic Report is configured for customers with a Cisco CallManager/Unity environment.

System Applications Versions Report

The System Applications Versions Reports displays OS type, OS version, IPT application version, and Windows Hotfixes for monitored IPT servers. Only devices that respond to SNMP queries will appear in the report. The System Applications Versions Report is automatically generated by Cisco MAP on the first of every month for the previous month's data. The report results are displayed in Microsoft Excel file format.

Table 44. Sample Cisco IPT Server Versions Report for Servers Located In The Northwestern Part Of The United States

Description: IPT Applications & Windows Hotfix Summary

Run Date: 2009-09-29

Time Zone: EDT

Run By: System

Region	Site Name	Site Location	Device Name	Device IP	Device Model	Device Manufacturer	Application/ Function	Application Version	OS Type	OS
Northwest	NW_Elgin	Portland, OR	Orgvmoh01	xx.xxx.xxx.xx	ProLiant DL380 G5	Cisco	Subscriber	6.1.2.1002	UCOS	UCOS 3.0.0.0
Northwest	MW_Elgin	Portland, OR	Orgvpub01	xx.xxx.xxx.xx	ProLiant DL380 G5	Cisco	Publisher	6.1.2.1002-1	UCOS	UCOS 3.0.0.0
Northwest	MW_Elgin	Portland, OR	Orgvsub01	xx.xxx.xxx.xx	ProLiant DL380 G5	Cisco	Subscriber	6.1.2.1002-1	UCOS	UCOS 3.0.0.0
Northwest	ID_Call_Managers	Boise, ID	Idvp01mch	xx.xxx.x.xx	ProLiant DL380 G4	Cisco	Subscriber		Windows	Windows 2000
Northwest	ID_Call_Managers	Boise, ID	Idvp01pub1	xx.xxx.x.xx	ProLiant DL380 G4	Cisco	Publisher	4.1(3)sr6	Windows	Windows 2000
Northwest	ID_Call_Managers	Boise, ID	Idvp01sub1	xx.xxx.x.xx	ProLiant DL380 G4	Cisco	Subscriber	4.1(3)sr6	Windows	Windows 2000
Northwest	WA_Call_Managers	Vancouver, Washington	Wa01moh1	xx.xxx.x.xx	ProLiant DL380 G4	Cisco	Subscriber	4.1(3)sr6	Windows	Windows 2000
Northwest	WA_Call_Managers	Vancouver, Washington	Wa01pub1	xx.xxx.x.xx	ProLiant DL380 G4	Cisco	Publisher	4.1(3)sr6	Windows	Windows 2000
Northwest	WA_Call_Managers	Vancouver, Washington	Wa01moh1	xx.xxx.x.xx	ProLiant DL380 G4	Cisco	Subscriber	4.1(3)sr6	Windows	Windows 2000

Table 45. Example Of The Windows Installed Hotfix Matrix Report

Description: Windows Installed Hotfix Summary

Run Date: 2009-09-29

Time Zone: EDT

Run By: System

Note: Click on a column header or an X mark to jump to the MS knowledgebase article for the hotlis.

Device Name	Device IP	KB324446	KB820361	KB822720	KB823818	KB829246	KB831576	KB831577	KB831877
Nydub01vpub01	xx.xxx.xxx.xx	x	x	x	x	x	x	x	x
Nydub01vsub01	xx.xxx.xxx.xx	x	x	x	x	x	x	x	x
Northeast01pub1	xx.xxx.x.xx	x	x	x	x	x	x	x	x
Northeast01sub1	xx.xxx.x.xx	x	x	x	x	x	x	x	x
Northeast01moh1	xx.xxx.x.xx	x	x	x	x	x	x	x	x
		5	**5**	**5**	**5**	**5**	**5**	**5**	**5**

Note: The System Applications Version Report is configured for customers with a Cisco CallManager/Unity environment.

UCCE Trunk Availability Report

The UCCE (Unified Contact Center Enterprise) Trunk Availability Report displays utilization data by Cisco CallManager trunk group in a UCCE environment. The UCCE Trunk Availability Report workbook consists of two parts: a Monthly Summary worksheet and Daily Detail worksheets displaying hourly detail for each day of the month (both worksheets are displayed in Microsoft Excel file format).

Table 46. Example of the UCCE Trunk Availability Report Summary Worksheet

Description: Provides Monthly Total Call Counts, and Busy Hour Erlangs, Busy Seconds and Availability Per Trunk Group. See Daily Tabs For Hourly Statistics.										
Run Date: 2009-03-17										
Time Zone: EDT										
Run By: System										
Trunk Group Name	**Trunk Available**	**Calls Out**	**Total Calls**	**Seconds In**	**Seconds Out**	**Total Seconds**	**Busy Hour**	**Erlangs**	**Seconds Busy**	**Percent Avail**
IPIVR_PIM_2.IPIVR_TGO	10	1,161	1,161	0	15,057	15,057	Wed 25 Feb 2009 12 – 1 AM	0	0	99.99%
	Totals =	**1,161**	**1,161**	**0**	**15,057**	**15,057**				

Erlangs Daily Trend

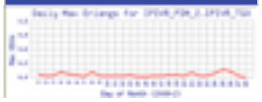


Table 47. Example Of The UCCE Trunk Availability Report Daily Detail Worksheet

Description: Provides Hourly Call Counts, Erlangs, Busy Seconds, and Available Per Trunk Group										
Run Date: 2009-03-17										
Time Zone: EDT										
Run By: System										
Hour	**Trunk Group Name**	**Trunks Avail**	**Calls In**	**Calls Out**	**Total Calls**	**Seconds In**	**Seconds Out**	**Total Seconds**	**Erla-ngs**	**Seconds Busy**	**Percent Avail**
Mon 9 Feb 2009 12 -1 AM	PIVR_PM_2 IRVR_TG0	10	0	0	0	0	0	0	0	0	100.00%
Mon 9 Feb 2009 1-2AM	PIVR_PM_2 IRVR_TG0	10	0	0	0	0	0	0	0	0	100.00%
Mon 9 Feb 2009 2-3AM	PIVR_PM_2 IRVR_TG0	10	0	0	0	0	0	0	0	0	100.00%
Mon 9 Feb 2009 3-4AM	PIVR_PM_2 IRVR_TG0	10	0	0	0	0	0	0	0	0	100.00%
Mon 9 Feb 2009 4-5AM	PIVR_PM_2 IRVR_TG0	10	0	0	0	0	0	0	0	0	100.00%
Mon 9 Feb 2009 5-6AM	PIVR_PM_2 IRVR_TG0	10	0	0	0	0	0	0	0	0	100.00%
Mon 9 Feb 2009 6-7AM	PIVR_PM_2 IRVR_TG0	10	0	0	0	0	0	0	0	0	100.00%

Hour	Trunk Group Name	Trunks Avail	Calls In	Calls Out	Total Calls	Seconds In	Seconds Out	Total Seconds	Erla-ngs	Seconds Busy	Percent Avail
Mon 9 Feb 2009 7-8AM	PIVR_PM_2 IRVR_TG0	10	0	1	1	0	4	4	0	0	100.00%
Mon 9 Feb 2009 8-9AM	PIVR_PM_2 IRVR_TG0	10	0	2	2	0	22	22	0	0	100.00%
Mon 9 Feb 2009 9 -10AM	PIVR_PM_2 IRVR_TG0	10	0	6	6	0	23	23	0	0	100.00%
Mon 9 Feb 2009 10-11AM	PIVR_PM_2 IRVR_TG0	10	0	4	4	0	71	71	0	0	100.00%
Mon 9 Feb 2009 11AM-12PM	PIVR_PM_2 IRVR_TG0	10	0	2	2	0	27	27	0	0	100.00%
Mon 9 Feb 2009 12-1PM	PIVR_PM_2 IRVR_TG0	10	0	3	3	0	52	52	0	0	100.00%
Mon 9 Feb 2009 1-2PM	PIVR_PM_2 IRVR_TG0	10	0	3	3	0	27	27	0	0	100.00%
Mon 9 Feb 2009 2-3PM	PIVR_PM_2 IRVR_TG0	10	0	2	2	0	30	30	0	0	100.00%
Mon 9 Feb 2009 3-4PM	PIVR_PM_2 IRVR_TG0	10	0	3	3	0	13	13	0	0	100.00%
Mon 9 Feb 2009 4-5PM	PIVR_PM_2 IRVR_TG0	10	0	4	4	0	38	38	0	0	100.00%
Mon 9 Feb 2009 5-6PM	PIVR_PM_2 IRVR_TG0	10	0	0	0	0	0	0	0	0	100.00%
Mon 9 Feb 2009 6-7PM	PIVR_PM_2 IRVR_TG0	10	0	1	1	0	4	4	0	0	100.00%
Mon 9 Feb 2009 7-8PM	PIVR_PM_2 IRVR_TG0	10	0	1	1	0	3	3	0	0	100.00%
Mon 9 Feb 2009 8-9PM	PIVR_PM_2 IRVR_TG0	10	0	1	1	0	1	1	0	0	100.00%
Mon 9 Feb 2009 9-10PM	PIVR_PM_2 IRVR_TG0	10	0	2	2	0	39	39	0	0	100.00%
Mon 9 Feb 2009 10-11PM	PIVR_PM_2 IRVR_TG0	10	0	0	0	0	0	0	0	0	100.00%
Mon 9 Feb 2009 11PM-12AM	PIVR_PM_2 IRVR_TG0	10	0	0	0	0	0	0	0	0	100.00%
		Totals	**0**	**35**	**35**	**0**	**354**	**354**			

Note: The UCCE Trunk Availability Report is configured for Cisco Intelligent Contact Manager (ICM) or Unified Contact Center Enterprise environments.

Voice Mail Traffic Reporting

The VMail Traffic Report is based on Cisco CDR/CMR records generated in a Cisco Unity Enterprise environment and provides voice mail usage details such as call totals, time busy, and the percentage of ports available. The Voice Mail Traffic Report workbook consists of two parts: a Monthly Summary worksheet and Daily Detail worksheets displaying hourly detail for each day of the month (both worksheets are displayed in Microsoft Excel file format).

Table 48. Example Of The Voice Mail Traffic Report Summary Worksheet

Description: Provides Monthly Totals In Use and Busy Seconds Per CCM-Cluster/VMail-Server Pair. See Daily Tabs For Hourly Statistics.												
Run Date: 2010-04-08												
Time Zone: EDT												
Run By: System												
CCM Cluster	**VMail Server**	**Calls Recv**	**Total Calls**	**Seconds Orig**	**Seconds Recv**	**Seconds Orig**	**Total Seconds**	**Busy Hour**	**Erlangs**	**Max Ports In Use**	**% Ports In Use**	**Seconds Busy**
NPPUB	FIRM24 B4-VI	7.521	7,644	422	6,664	380,460	380,882	Wed 17 Feb 2010 3-4PM	1	4	40.0%	0
Syr-st-cmpub-1	Syr-st-u1-VI	0	0	0	7,653	0	0	NA	0	0	0.0%	0
Syr-st-cmpub-1	Syr-st-u2-VI	0	0	0	9,953	0	0	NA	0	0	0.0%	0
	Totals =	**7,521**	**7,644**	**422**	14,656	**380,460**						

Table 51 Cont'd. Example Of The Voice Mail Traffic Report Summary Worksheet

MAX Ports Daily Trend

Table 49. Example Of The Voice Mail Traffic Report Daily Detail Worksheet

Description: Provides Hourly Call Counts, Erlangs and Busy Seconds Per CCM-Cluster/VMail-Server Pair

Run Date: 2010-04-08

Time Zone: EDT

Run By: System

Hour	CCM Cluster	Vmail Server	Ports Available	Calls Orig	Calls Recv	Total Calls	Seconds Orig	Seconds Recv	Total Seconds	Erlangs	Max Ports In Use	% Ports In Use	Seconds Busy
Tues 2 Mar 2010 8-9AM	NPPUB	FIRM24B4-VI	10	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 8-9AM	Syr-stcmpub-1	Syr-st-u1-VI	16	8	16	24	0	2,217	2,217	1	2	12.5%	0
Tues 2 Mar 2010 8-9AM	Syr-stcmpub-1	Syr-st-u2-VI	16	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 9-10AM	NPPUB	FIRM24B4-VI	10	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 9-10AM	Syr-stcmpub-1	Syr-st-u1-VI	16	11	27	38	1	2,633	2,634	1	3	18.8%	0
Tues 2 Mar 2010 9-10AM	Syr-stcmpub-1	Syr-st-u2-VI	16	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 10-11AM	NPPUB	FIRM24B4-VI	10	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 10-11AM	Syr-stcmpub-1	Syr-st-u1-VI	16	18	40	58	3	2,290	2,293	1	4	25.0%	0
Tues 2 Mar 2010 10-11AM	Syr-stcmpub-1	Syr-st-u2-VI	16	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 11AM-12PM	NPPUB	FIRM24B4-VI	10	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 11AM-12PM	Syr-stcmpub-1	Syr-st-u1-VI	16	5	17	22	0	1,189	1,189	0	2	12.5%	0
Tues 2 Mar 2010 11AM-12PM	Syr-stcmpub-1	Syr-st-u2-VI	16	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 12-1PM	NPPUB	FIRM24B4-VI	10	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 12-1PM	Syr-stcmpub-1	Syr-st-u1-VI	16	16	33	49	0	2,273	2,273	1	3	18.8%	0
Tues 2 Mar 2010 12-1PM	Syr-stcmpub-1	Syr-st-u2-VI	16	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 1-2PM	NPPUB	FIRM24B4-VI	10	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 1-2PM	Syr-stcmpub-1	Syr-st-u1-VI	16	26	33	59	2	1,784	1,786	1	4	25.0%	0
Tues 2 Mar 2010 1-2PM	Syr-stcmpub-1	Syr-st-u2-VI	16	0	0	0	0	0	0	0	0	0.0%	0

Hour	CCM Cluster	Vmail Server	Ports Available	Calls Orig	Calls Recv	Total Calls	Seconds Orig	Seconds Recv	Total Seconds	Erlangs	Max Ports In Use	% Ports In Use	Seconds Busy
Tues 2 Mar 2010 2-3PM	NPPUB	FIRM24B4-VI	10	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 2-3PM	Syr-stcmpub-1	Syr-st-u1-VI	16	21	40	61	1	1,688	1,689	0	3	18.8%	0
Tues 2 Mar 2010 2-3PM	Syr-stcmpub-1	Syr-st-u2-VI	16	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 3-4PM	NPPUB	FIRM24B4-VI	10	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 3-4PM	Syr-stcmpub-1	Syr-st-u1-VI	16	6	15	21	0	1,314	1,314	0	3	18.8%	0
Tues 2 Mar 2010 3-4PM	Syr-stcmpub-1	Syr-st-u2-VI	16	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 4-5PM	NPPUB	FIRM24B4-VI	10	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 4-5PM	Syr-stcmpub-1	Syr-st-u1-VI	16	15	24	39	0	2,097	2,097	1	3	18.8%	0
Tues 2 Mar 2010 4-5PM	Syr-stcmpub-1	Syr-st-u2-VI	16	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 5-6PM	NPPUB	FIRM24B4-VI	10	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 5-6PM	Syr-stcmpub-1	Syr-st-u1-VI	16	7	15	22	0	415	415	0	3	18.8%	0
Tues 2 Mar 2010 5-6PM	Syr-stcmpub-1	Syr-st-u2-VI	16	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 6-7PM	NPPUB	FIRM24B4-VI	10	0	0	0	0	0	0	0	0	0.0%	0
Tues 2 Mar 2010 6-7PM	Syr-stcmpub-1	Syr-st-u1-VI	16	3	5	8	0	92	92	0	1	6.3%	0
Tues 2 Mar 2010 6-7PM	Syr-stcmpub-1	Syr-st-u2-VI	16	0	0	0	0	0	0	0	0	0.0%	0

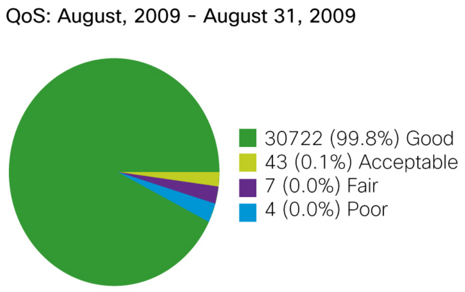
Note: The Voice Mail Traffic Report is configured for customers with a Cisco CallManager/Unity environment.

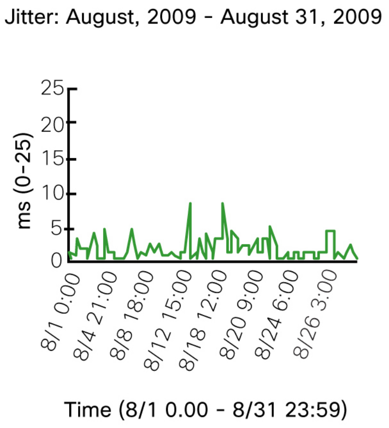
Voice Service Level Reporting

Voice Service Level (VSL) reporting is based on Cisco CallManager CDR/CMR records and the analysis that Cisco MAP conducts on the records to derive such factors as voice quality. Voice Service Level reporting will provide historical data on call information such as quality of service, jitter, packet loss percentage, and latency. The report results are displayed in PDF file format.

Table 50. Example Of Voice Service Level Report Results

	Lost Packets (%)		Jitter (ms)		Latency (ms)	
QoS Rating	**From**	**To**	**From**	**To**	**From**	**To**
Good	0.00	15.00	0.00	20.00	0.00	25.00
Acceptable	15.01	30.00	21.00	149.00	26.00	100.00
Fair	30.01	45.00	150.00	199.00	101.00	200.00
Poor	45.01	Infinity	200.00	Infinity	201.00	Infinity





Note: The Voice Service Levels Reporting application is available to customers having the Cisco MAP IP Telephony Advanced Management application.

CVP CallServer Monitoring

The **CVP CallServer** Summary dashboard displays in a new browser window. The CVP CallServer Summary lists CVP CallServer devices, CVP statistics such as the number of active calls, active SIP legs, active H323 legs, active VRU legs, and port license usage information.

Clicking the Show Detailed Statistics link will open the **CallServer Statistics Detail** window for the selected device. The **CallServer Statistics Detail** window displays in-depth information on the protocols and services available on the device.

The following are displayed in the **CVP CallServer Summary** dashboard view:

- CVP CallServer Hostname
- Active SIP Call Legs
- Active VRU Call Legs
- Port Licenses Available
- Actions
- Active Calls
- Active H.323 Call Legs
- Port Licenses in Use
- Last Polled At

Table 51. CVP CallServer Summary Window

CVP CallServer Hostname	Active Calls	Active SIP Call Legs	Active H.323 Call Legs	Active VRU Call Legs	Port Licenses in Use	Port Licenses Available	Last Polled At	Actions
SYRCVPCS04	76	0	17	76	76	924	2009-10-29 10:55:03	Show Detailed Statistics
SYRCVPCS05	83	0	32	83	83	917	2009-10-29 10:55:03	Show Detailed Statistics
SYRCVPCS06	69	0	19	69	69	931	2009-10-29 10:55:03	Show Detailed Statistics
SYRCVPCS07	57	0	14	57	57	943	2009-10-29 10:35:03	Show Detailed Statistics
SYRCVPCS08	62	0	21	61	62	938	2009-10-29 10:35:03	Show Detailed Statistics
SYRCVPCS09	79	0	25	79	79	921	2009-10-29 10:35:03	Show Detailed Statistics
SYRCVPCS10	53	0	18	53	53	947	2009-10-29 10:35:03	Show Detailed Statistics
SYRCVPCS11	56	0	17	55	56	944	2009-10-29 10:35:03	Show Detailed Statistics
SYRCVPCS12	61	0	19	59	61	939	2009-10-29 10:35:03	Show Detailed Statistics
SYRCVPCS13	50	0	15	50	50	950	2009-10-29 10:35:03	Show Detailed Statistics

Clicking on the Show Detailed Statistics link for a managed device in the Summary window will display detailed service statistics for that device. You can use the (➕) and (➖) icons to expand or contract the display of a service's statistics.

Table 52. Detail Statistics For CVP CallServer

ICM STATISTICS					
Realtime		**Interval**		**Aggregate**	
Service Status	In Service	Start Time	2009-04-27 09:29:37	Start Time	2009-02-11 05:29:37
Active Calls	0	Duration Elapsed	7m 38s	Duration Elapsed	75d 3h 7m 38s
Active SIP Call Legs	0	Interval Duration	30 m	Total Calls	156
Active H323 Call Legs	0	New Calls	0	Total SIP Call Legs	0
Active VRU Call Legs	0	SIP Call Legs	0	Total H323 Call Legs	156
		H323 Call Legs	0	Total VRU Call Legs	155
		VRU Call Legs	0		
H323 STATISTICS (Service was Disabled at Last Poll)					
SIP STATISTICS (Service was Disabled at Last Poll)					
IVR STATISTICS					
Realtime		**Interval**		**Aggregate**	
Service Status	In Service	Start Time	2009-04-27 09:29:37	Start Time	2009-02-11 05:29:37
Active Calls	0	Duration Elapsed	7m 38s	Duration Elapsed	75d 3h 7m 38s
Active HTTP Requests	4	Interval Duration	30 min	Total New Calls	156
		Peak Active Calls	0	Peak Active Calls	1
		New Calls	0	Total HTTP Requests	416,989
		Calls Finished	0	Peak Active HTTP Requests	5
		Avg. Call Latency	0 ms		
		Max Call Latency	0 ms		
		Min Call Latency	0 ms		

Realtime		Interval		Aggregate	
		Total HTTP Requests	59		
		Avg. HTTP Requests / Sec	0		
		Peak Active HTTP Requests / Sec	0		

VXML STATISTICS (Service was Disabled at Last Poll)

INFRASTRUCTURE STATISTICS

Licensing

Realtime		Interval		Aggregate	
Port Licenses Avail	1,000	Start Time	2009-04-27 09:29:37	Start Time	2009-02-11 05:29:37
Current Port Licenses in Use	0	Duration Elapsed	7m 38s	Duration Elapsed	75d 3h 7m 38s
Current Port Licenses State	Safe	Interval Duration	30 min	Total New Port License Requests	156
		Total New Port License Requests	0	Avg. License Requests/Min	0
		Avg. License Requests/Min	0	Peak Port License Used	1
		Max Port Licenses Used	0	Total Denied Port License Requests	0

Threadpool Realtime	
Idle Threads	300
Running Threads	0
Core Threads	300
Max Threads	300
Peak Threads Used	300

JVM Realtime	
Peak Memory Usage	94,748,216 bytes
Current Memory Usage	72,657,800 bytes
Total Memory	1,056,484,288 bytes
Available Memory	992,826,488 bytes
Threads In Use	373
Peak Threads In Use	373
Uptime	72d 4h 44m 55s

Table 53. Example Of The Cisco MAP CVP CallServer Statistics Detail Report

ICM STATISTICS					
Realtime		**Interval**		**Aggregate**	
Service Status	In Service	Start Time	2009-04-27 09:29:37	Start Time	2009-02-11 05:29:37
Active Calls	0	Duration Elapsed	7m 38s	Duration Elapsed	75d 3h 7m 38s
Active SIP Call Legs	0	Interval Duration	30 m	Total Calls	156
Active H323 Call Legs	0	New Calls	0	Total SIP Call Legs	0
Active VRU Call Legs	0	SIP Call Legs	0	Total H323 Call Legs	156
		H323 Call Legs	0	Total VRU Call Legs	155
		VRU Call Legs	0		
H323 STATISTICS (Service was Disabled at Last Poll)					
SIP STATISTICS (Service was Disabled at Last Poll)					
IVR STATISTICS					
Realtime		**Interval**		**Aggregate**	
Service Status	In Service	Start Time	2009-04-27 09:29:37	Start Time	2009-02-11 05:29:37
Active Calls	0	Duration Elapsed	7m 38s	Duration Elapsed	75d 3h 7m 38s
Active HTTP Requests	4	Interval Duration	30 min	Total New Calls	156
		Peak Active Calls	0	Peak Active Calls	1
		New Calls	0	Total HTTP Requests	416,989
		Calls Finished	0	Peak Active HTTP Requests	5
		Avg. Call Latency	0 ms		
		Max Call Latency	0 ms		
		Min Call Latency	0 ms		
		Peak Active HTTP Requests	4		
		Total HTTP Requests	59		
		Avg. HTTP Requests / Sec	0		
		Peak Active HTTP Requests / Sec	0		
VXML STATISTICS (Service was Disabled at Last Poll)					
INFRASTRUCTURE STATISTICS					
Licensing					
Realtime		**Interval**		**Aggregate**	
Port Licenses Available	1,000	Start Time	2009-04-27 09:29:37	Start Time	2009-02-11 05:29:37
Current Port Licenses in Use	0	Duration Elapsed	7m 38s	Duration Elapsed	75d 3h 7m 38s
Current Port Licenses State	Safe	Interval Duration	30 min	Total New Port License Requests	156
		Total New Port License Requests	0	Avg. License Requests/Min	0
		Avg. License Requests/Min	0	Peak Port License Used	1
		Max Port Licenses Used	0	Total Denied Port License Requests	0

Threadpool Realtime	
Idle Threads	300
Running Threads	0
Core Threads	300
Max Threads	300
Peak Threads Used	300
JVM Realtime	
Peak Memory Usage	94,748,216 bytes
Current Memory Usage	72,657,800 bytes
Total Memory	1,056,484,288 bytes
Available Memory	992,826,488 bytes
Threads In Use	373
Peak Threads In Use	373
Uptime	72d 4h 44m 55s

Note: The CVP CallServer Summary is configured for Cisco Customer Voice Portal (CVP) environments.

DS1 Interface Monitoring

The DS1 Interface Statistics report displays a near real time dashboard of interface operational status, error counts, synchronization status, and statistics collected from the DS1 (T1) interface(s) in the networked environment. The dashboard displays both historical and real time DS1 statistics in text and graphs. Clicking on a link located in the **Device** column from the **DS1 Statistics – Enterprise View** window displays detailed real time DS1 interface information. A link is provided to the device's Entity Manager, allowing the user to bring focus to the device when troubleshooting. Additionally, customers can elect to have AutoCases opened if error count thresholds are found to have been exceeding during Cisco MAP's interface polling activities.

Table 54. DS1 Statistics – Enterprise View Dashboard

Overview / Summary									
Time Period	**Total Devices Polled**	**Total Devices Without DS1 Errors**	**Total Devices With DS1 Errors**	**Total DS1 Interfaces Found**	**Total DS1 Interfaces Administratively Up**	**Total DS1 Interfaces Administratively Down**	**Total DS1 Interfaces Operationally Up**	**Total DS1 Interfaces Operationally Down**	**Total DS1 Interfaces With Errors**
Current	3	1	2	9	8	1	4	5	5
Last 24 Hours	3	1	2	9	8	1	4	5	5

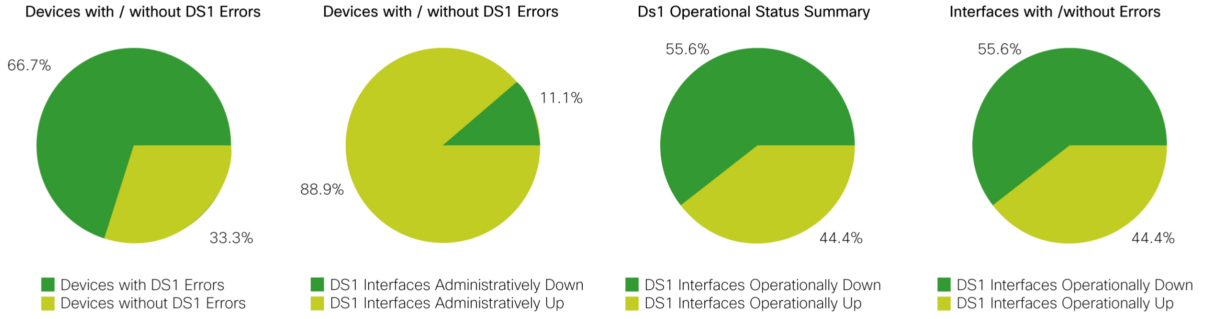


Table 54 Cont'd: DS1 Statistics – Enterprise View Dashboard

Current Interface Errors																
Tool	**Device**	**Interface (Index)**	**Alias/ Desc.**	**LCV**	**PCV**	**CSS**	**SEFS**	**LES**	**DM**	**ES**	**BES**	**SES**	**UAS**	**Elapsed Sec.**	**% Error Sec.**	**Last Poll**
🔨	Syr-pl-2811-wan2 (10.15.255.11)	T1 0/0/0 (7)		0	0	0	0	0	0	0	0	0	522	521	100%	2010-04-16 08:15:10
🔨	Syr-pl-2811-wan2 (10.15.255.11)	T1 0/0/1 (8)		0	0	0	0	0	0	0	0	0	521	521	100%	2010-04-16 08:15:10
🔨	Syr-st-2811-wan2 (10.16.255.11)	T1 0/0/1 (6)		0	0	0	0	0	0	0	0	0	502	502	100%	2010-04-16 08:15:10
🔨	Syr-st-2811-wan2 (10.16.255.11)	T1 0/0/0 (5)		0	0	0	0	0	0	0	0	0	502	502	100%	2010-04-16 08:15:10
🔨	Syr-st-2811-wan2 (10.16.255.11)	T1 0/1/0 (7)		0	0	42	0	0	0	42	0	0	0	494	8.502 %	2010-04-16 08:15:10

Table 55. DS1 Interface Error History – Last 10 Days Window

Current Interface Errors													
Tool	**Device**	**Interface (Index)**	**Alias/ Desc.**	**2010-04-16**	**2010-04-15**	**2010-04-14**	**2010-04-13**	**2010-04-12**	**2010-04-11**	**2010-04-10**	**2010-04-09**	**2010-04-08**	**2010-04-07**
📊 🔨	Syr-pl-2811-wan1 (10.15.254.23)	T1 0/0/0 (9)		0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)
📊 🔨	Syr-pl-2811-wan1 (10.15.254.23)	T1 0/0/1 (10)		0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)
📊 🔨	Syr-pl-2811-wan2 (10.15.255.11)	T1 0/0/0 (7)		86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)
📊 🔨	Syr-pl-2811-wan2 (10.15.255.11)	T1 0/0/1 (8)		86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)
📊 🔨	Syr-pl-2811-wan2 (10.15.255.11)	T1 0/2/0 (6)	Test description	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)	0 (0.000%)
📊 🔨	Syr-st-2811-wan2 (10.16.255.11)	T1 0/0/0 (5)		86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)
📊 🔨	Syr-st-2811-wan2 (10.16.255.11)	T1 0/0/1 (8)		86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)	86400 (100.000 %)
📊 🔨	Syr-st-2811-wan2 (10.16.255.11)	T1 0/1/0 (7)		7250 (8.391%)	7250 (8.391%)	7250 (8.391%)	7250 (8.391%)	7250 (8.391%)	7250 (8.391%)	7250 (8.391%)	7250 (8.391%)	7250 (8.391%)	7250 (8.391%)

Figure 4. DS1 Percent Time In Error Graph (10 Day History)

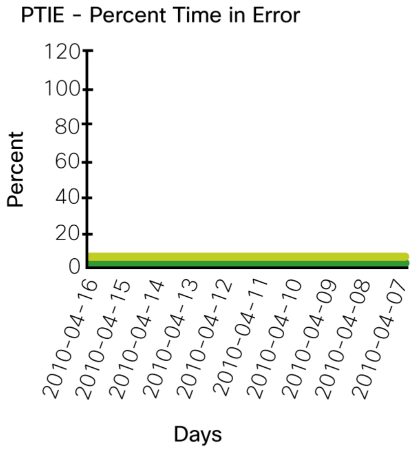


Table 56. DS1 Statistics – Enterprise View Dashboard – Detailed Statistics

T1 Controller Status			
Device	**Interface (Index)**	**Attributes**	**Last Poll**
Syr-st2611-wan2 (10.16.255.11)	T1 0/0/0 (5)	Admin Status: up (1) Operational Status: down(2) Line Status: dsx1XmtFarEndLOF(4), dsx1LossOFFrame(32), dsx1LossOfSignal(64) If Alias: Framing: dsx1ESF(2) Line Code: dsx1B8ZS(2) Clock Type: localTiming(2)	2010-04-16 08:20:08
	T1 0/0/1 (6)	Admin Status: up (1) Operational Status: down(2) Line Status: dsx1XmtFarEndLOF(4), dsx1LossOFFrame(32), dsx1LossOfSignal(64) If Alias: Framing: dsx1ESF(2) Line Code: dsx1B8ZS(2) Clock Type: localTiming(2)	2010-04-16 08:20:08
	T1 0/1/0 (7)	Admin Status: up (1) Operational Status: up(1) Line Status: dsx1NoAlarm(1) If Alias: Framing: dsx1ESF(2) Line Code: dsx1B8ZS(2) Clock Type: loopTiming(1)	2010-04-16 08:20:08
DSX-1 Line Status			
Please select a filter: [Current View] 24 Hour View			

Tools	Device	Interface (Index)	LCV	PCV	CSS	SEFS	LES	DM	ES	BES	SES	UAS	Elapsed
	Syr-st-2811-wan2 (10.16.255.11)	T1 0/0/0 (5)	0	0	0	0	0	0	0	0	0	802	802 sec
		T1 0/0/1 (6)	0	0	0	0	0	0	0	0	0	802	802 sec
		T1 0/1/0 (7)	0	0	68	0	0	0	68	0	0	0	794 sec

Legend		
LCV – Line Code Violation	SEFS = Severely Errored Framing Seconds	ES = Errored Seconds
PCV = Path Code Violation	LES = Line Errored Seconds	BES = Bursty Errored Seconds
CSS = Controlled Slip Seconds	DM = Degraded Minutes	SES = Severely Errored Seconds
	Percent time in error greater than 1%	UAS = Unavailable Seconds

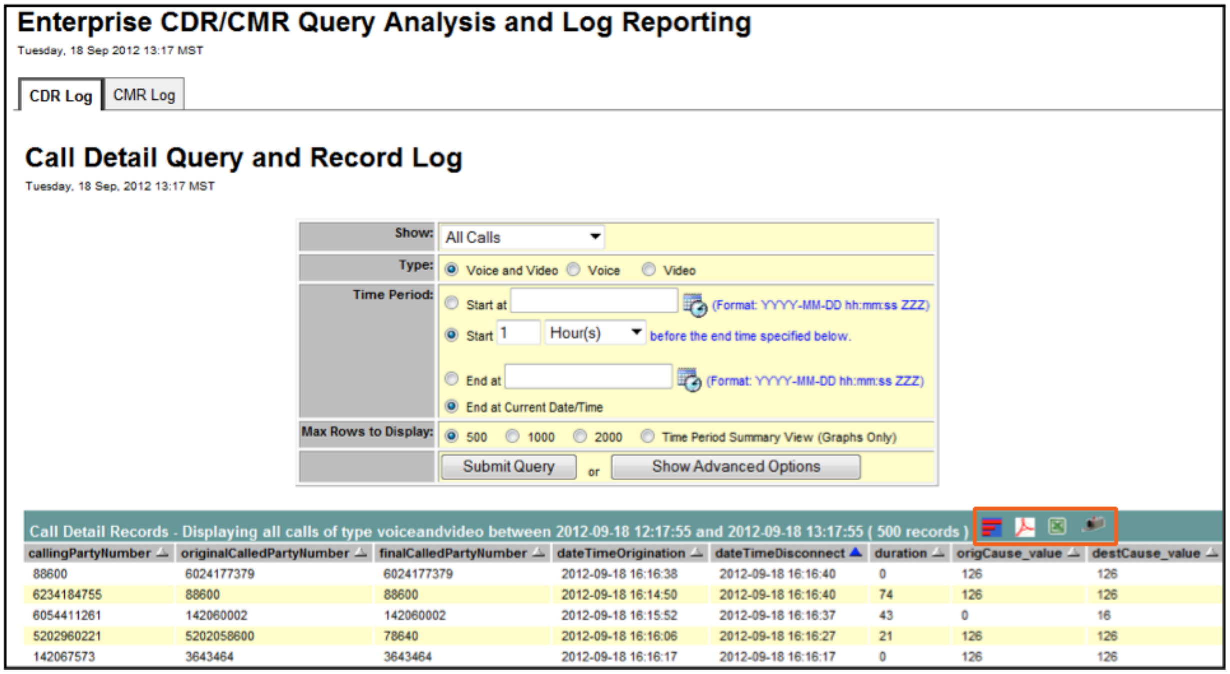
Note: The **DS1 Interface Statistics** dashboard is available for networked environments having DS-1 (T1) links as part of the environment. Contact your Network Administrator or Cisco MAP Customer Service Manager for assistance in determining if your environment meets the prerequisites required for the **DS1 Interface Statistics** dashboard.

Note: Configuration of the Cisco MAP appliance is required for the proper functioning of the **DS1 Interface Statistics** dashboard. Contact your Cisco MAP Customer Service Manager for more information.

Enterprise CDR/CMR Query Analysis and Log Reporting

The CDR/CMR Analysis application allows users to search all of the Call Detail Records (CDR) and Call Management Records (CMR) to search for problem calls, trends for reporting or retrieving call summary details for management/Human Resource reports. Users can search by date/time period, individual extensions, devices, clusters, partitions and service quality. All results can be modified to show pertinent fields and report results can be summarized and/or exported to Microsoft Excel or Adobe PDF file formats.

Figure 5. Enterprise CDR/CMR Query Analysis and Log Reporting Default Reporting Window



Enterprise CDR/CMR Query Analysis and Log Reporting

Tuesday, 18 Sep 2012 13:17 MST

Call Detail Query and Record Log

Tuesday, 18 Sep, 2012 13:17 MST

Show: All Calls

Type: ● Voice and Video ○ Voice ○ Video

Time Period:
○ Start at ____ (Format: YYYY-MM-DD hh:mm:ss ZZZ)
● Start 1 Hour(s) before the end time specified below.
○ End at ____ (Format: YYYY-MM-DD hh:mm:ss ZZZ)
● End at Current Date/Time

Max Rows to Display: ● 500 ○ 1000 ○ 2000 ○ Time Period Summary View (Graphs Only)

Call Detail Records - Displaying all calls of type voiceandvideo between 2012-09-18 12:17:55 and 2012-09-18 13:17:55 (500 records)

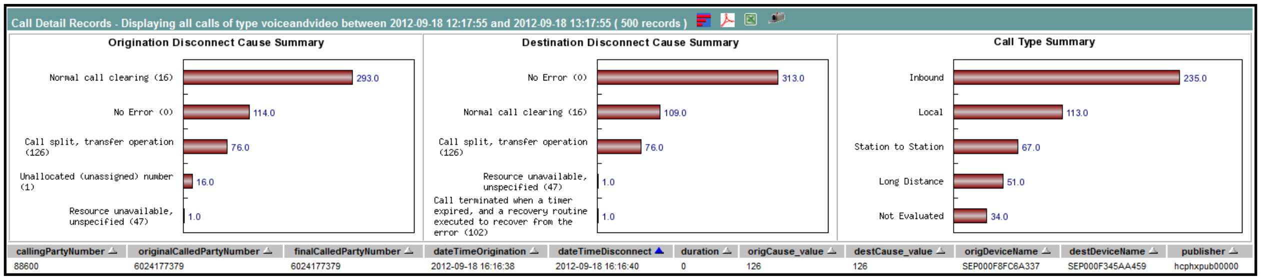
callingPartyNumber	originalCalledPartyNumber	finalCalledPartyNumber	dateTimeOrigination	dateTimeDisconnect	duration	origCause_value	destCause_value
88600	6024177379	6024177379	2012-09-18 16:16:38	2012-09-18 16:16:40	0	126	126
6234184755	88600	88600	2012-09-18 16:14:50	2012-09-18 16:16:40	74	126	126
6054411261	142060002	142060002	2012-09-18 16:15:52	2012-09-18 16:16:37	43	0	16
5202960221	5202058600	78640	2012-09-18 16:16:06	2012-09-18 16:16:27	21	126	126
142067573	3643464	3643464	2012-09-18 16:16:17	2012-09-18 16:16:17	0	126	126

The figure above represents the default window for the CDR/CMR Analysis application. By default, the last 500 calls for the previous hour will show. Users can change the standard options such as the start and end date/time, the max records to display, and file format options for exporting.

On the header bar below the query form are the following icons representing links that offer CDR information in different formats:

- The **Toggle Graph Panel** icon will toggle on/off graphical representations covering the Origination Disconnect Cause Summary, the Destination Disconnect Cause Summary, and Call Type Summary.
- Clicking the **Adobe Acrobat** icon will download only the graphical information into a PDF file format.
- Clicking the **Microsoft Excel** icon will download only the tabular data into a Microsoft Excel file format.
- – The **Mailbox** icon will allow a user to select individuals they wish to email the results of the query to. Both the graphs (PDF) and tabular data (XLS) will be sent to the selected individuals.

Figure 6. Toggle Graph Panel Icon Has Been Toggled "On" To Display Three Unique Bar Graphs



Call Detail Records - Displaying all calls of type voiceandvideo between 2012-09-18 12:17:55 and 2012-09-18 13:17:55 (500 records)

Origination Disconnect Cause Summary
Normal call clearing (16)
293.0
No Error (0)
114.0
Call split, transfer operation (126)
76.0
Unallocated (unassigned) number (1)
16.0
Resource unavailable, unspecified (47)
1.0
Destination Disconnect Cause Summary
No Error (0)
313.0
Normal call clearing (16)
109.0
Call split, transfer operation (126)
76.0
Resource unavailable, unspecified (47)
1.0
Call terminated when a timer expired, and a recovery routine executed to recover from the error (102)
1.0
Call Type Summary
Inbound
235.0
Local
113.0
Station to Station
67.0
Long Distance
51.0
Not Evaluated
34.0

callingPartyNumber	originalCalledPartyNumber	finalCalledPartyNumber	dateTimeOrigination	dateTimeDisconnect	duration	origCause_value	destCause_value	origDeviceName	destDeviceName	publisher
88600	6024177379	6024177379	2012-09-18 16:16:38	2012-09-18 16:16:40	0	126	126	SEP000F8FC6A337	SEP000F345AA459	hcphxpub00000

Within the **Call Detail Query and Record Log** window of the **CDR Log** tab, users can drill down into a particular call by clicking on one of the alternately shaded lines in the lower portion of the window. The **Call Detail Record Table View** window will open, which will show Call Detail Records (CDR) from all legs of the call as well as any Call Management Records (CMR) associated in addition to all of the detailed information.

Table 57. Example Of The Call Detail Record Table View Window

CALL DETAIL RECORD SUMMARY						
Record	**Start Time**	**Connect Time**	**Disconnect Time**	**Duration**	**Calling Party**	**Called Party**
1.	2012-09-19 08:27:07	2012-09-19 08:27:08	2012-09-19 08:29:03	115s	7069376464	8206100
2.	2012-09-19 08:29:03	2012-09-19 08:29:03	2012-09-19 08:29:04	1s	8206100	B00703206008
3.	2012-09-19 08:29:03	2012-09-19 08:29:03	2012-09-19 08:29:04	1s	9990112484477469	B00703206008
4.	2012-09-19 08:27:07	2012-09-19 08:29:03	2012-09-19 08:29:04	1s	7069376464	B00703206008

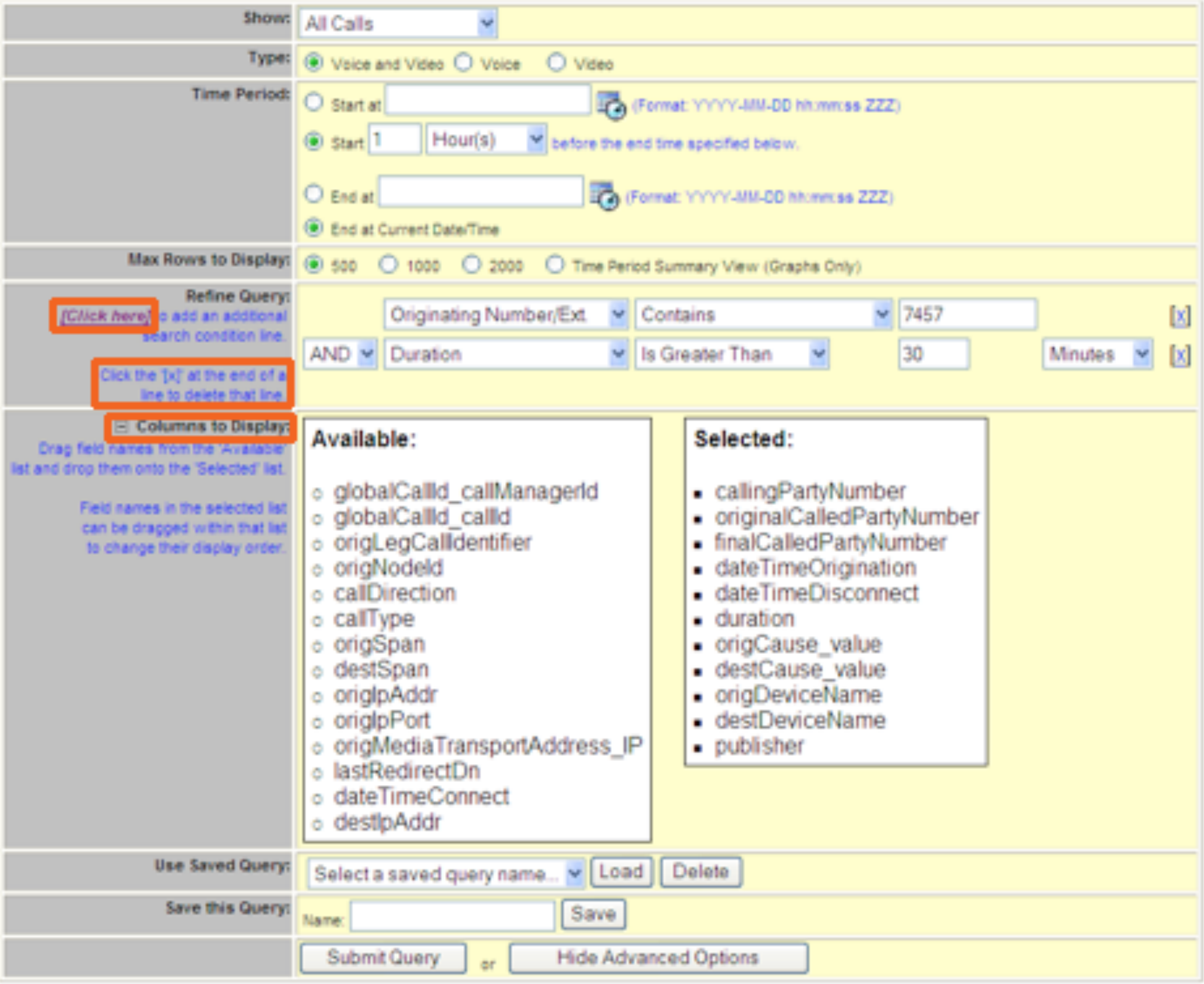
CALL MANAGEMENT RECORD SUMMARY					
Record	**Start Time**	**Connect Time**	**Disconnect Time**	**Directory Number**	**Mean Opion Score**
1.	2012-09-19 08:28:59	2012-09-19 08:27:08		8206100	Good
2.	2012-09-19 08:29:04	2012-09-19 08:29:03		8206100	Good

CALL DETAIL RECORD -1							
	Origination	**Connect**	**Disconnect**	**Duration**		**Origin**	**Destination**
DateTime	2012-09-19 08:27:07	2012-09-19 08:27:08	2012-09-19 08:29:03	115s	**DeviceName**	NewSP-STR-Trunk	SEP00270DBF7183
		Called Party			**IPAddress**	xx.xx.xx.xx	
	Calling Party	**Original**	**Final**	**Last Redirect**	**MediaTransportAddress_IP (Port)**	xx.xx.xx.xx 18648	xx.xx.xx.xx 17688
Party Number	7069376464	8206100	8206100	8206100	**Ipv4v6Addr**		
Participation		ICM-PT	ICM-PT	ICM-PT	**Span**	122843173	0
OutpulsedParty Number					**Cause_location**	0	0
UnicodeLogin UserID					**TerminationCause (Value)**	Call split, transfer operation (393216)	Call split, transfer operation (393216)
ProtocolCall Ref					**CallTerminationOnBehalfOf (Value)**	Conference (4)	Conference (4)
ProtocolID					**ConversationID**		0
RedirectReason (Value)		Unknown (0)		Unknown (0)	**LegIdentifier**	122843173	122843174
RedirectOnBehalfOf (Value)		Unknown (0)		Unknown (0)	**PrecedenceLevel (Value)**	Routine (4)	Routine (4)
RoutingReason					**DTMFMethod**		
CallManager Name (!D)	7 (7)				**NodeID**	7	7
GlobalCallID	5971466				**MediaCap_Bandwidth**		
ClusterID	StandAloneCluster				**MediaCap_PayloadCapability**	G729AnnexB	G729AnnexB
CallType					**MediaCap_mMxFramesPerPacket**	20	20
Comment					**RAVPAudioStat**		
JoinOnBehalfOf (Value)	Unknown (0)				Not a video call.		
CallSecured Status							
AuthCode Description							
Authorization CodeValue							

By clicking on the **Show Advanced Options** button on the Enterprise CDR/CMR Query Analysis and Log Reporting query form, users can refine the default search into something very specific. By clicking the Click Here link found within the **Refine Query** field, users can build their own query. Users can search by such items as extension, duration, device, publisher and cause code. To add more search terms, continue to click on the Click Here link. To remove a search term, click on the “X” link. You can also choose the fields to display in your output. Click on the Show/Hide icon (⊞) in the **Columns to Display** field of the query form to display the **Available** and **Selected** swap boxes. The fields shown in the **Selected** swap box are the field that will be shown in query output. You can select or deselect items to be displayed in the query output by clicking the name and dragging and dropping it into either the **Available** or **Selected** area of the query form. You can also move items up or down to put them in a select order as they will be seen in the query output. Click the **Submit Query** button to execute the query and display the CDR records meeting the specified search criteria. Prior to clicking the **Submit Query** button, if the constructed query will be used frequently, the user has the option to save the query parameters for future use. In the **Save this Query** field, enter a name for the query and click the **Save** button.

- To use a saved query in the future, use the drop down menu in the **Use Saved Query** field, select the name of the query by clicking on it, click the **Load** button and then the **Submit Query** button.
- To delete the saved query, use the drop down menu in the **Use Saved Query** field, select the name of the query by clicking on it, and click the **Delete** button.

Figure 7. Advance Search Options Showing An Example Of Criteria Entered In The Refine Query Field As Well As The Available/Selected Swap Boxes Associated With Expanded Columns To Display Field



Show: All Calls

Type: ● Voice and Video ○ Voice ○ Video

Time Period:
○ Start at (Format: YYYY-MM-DD hh:mm:ss ZZZ)
● Start 1 Hour(s) before the end time specified below.
○ End at (Format: YYYY-MM-DD hh:mm:ss ZZZ)
● End at Current Date/Time

Max Rows to Display: ● 500 ○ 1000 ○ 2000 ○ Time Period Summary View (Graphs Only)

Refine Query:
[Click here] to add an additional search condition line.
Click the '[x]' at the end of a line to delete that line.

	Originating Number/Ext.	Contains	7457		[x]
AND	Duration	Is Greater Than	30	Minutes	[x]

⊟ Columns to Display:
Drag field names from the 'Available' list and drop them onto the 'Selected' list.
Field names in the selected list can be dragged within that list to change their display order.

Available:

- globalCallId_callManagerId
- globalCallId_callId
- origLegCallIdentifier
- origNodeId
- callDirection
- callType
- origSpan
- destSpan
- origIpAddr
- origIpPort
- origMediaTransportAddress_IP
- lastRedirectDn
- dateTimeConnect
- destIpAddr

Selected:

- callingPartyNumber
- originalCalledPartyNumber
- finalCalledPartyNumber
- dateTimeOrigination
- dateTimeDisconnect
- duration
- origCause_value
- destCause_value
- origDeviceName
- destDeviceName
- publisher

Use Saved Query: Select a saved query name... Load Delete

Save this Query: Name: Save

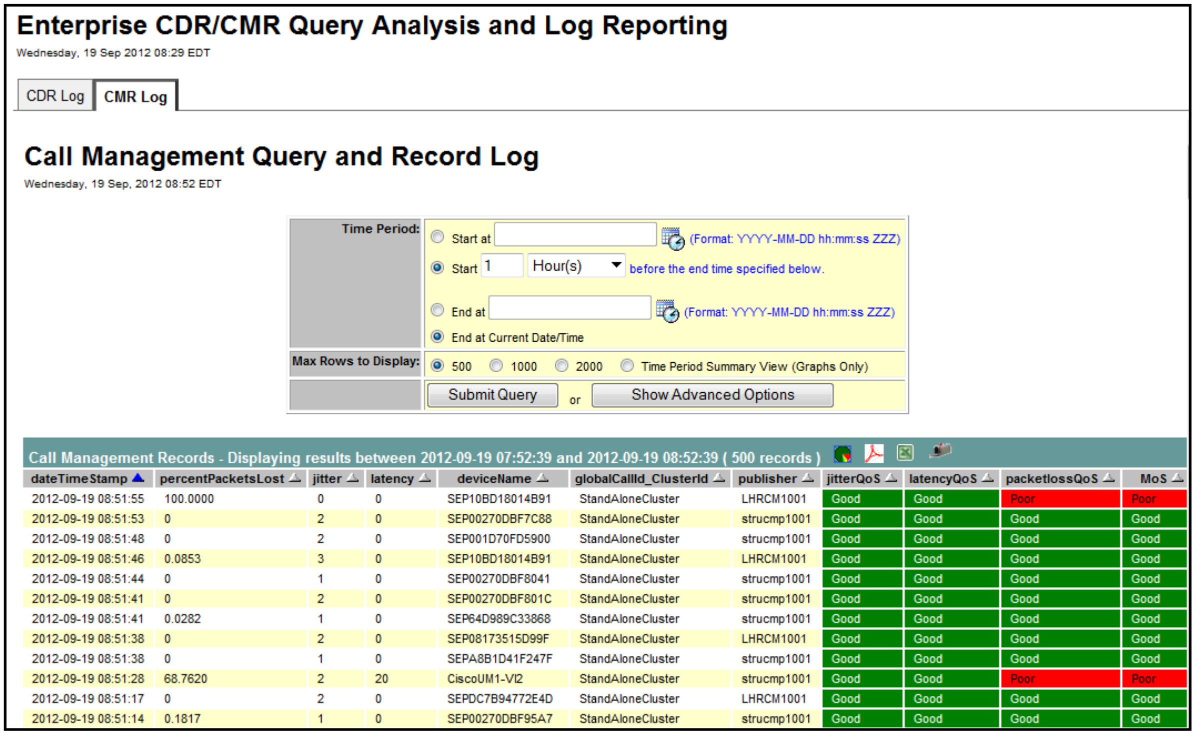
Submit Query or Hide Advanced Options

Note: The Enterprise CDR/CMR Query Analysis and Log Reporting application is configured for customers with Enterprise Cisco IP Telephony applications.

Call Management Record (CMR) Analysis

The **CMR** Log tab works similar to the **CDR Log** tab. The **Call Management Query and Record Log** is accessed by clicking on the **CMR Log** tab within the **Call Detail Query and Record Log** window.

Figure 8. Default View Of The CMR Log Tab



Enterprise CDR/CMR Query Analysis and Log Reporting

Wednesday, 19 Sep 2012 08:29 EDT

Call Management Query and Record Log

Wednesday, 19 Sep, 2012 08:52 EDT

Time Period:	○ Start at (Format: YYYY-MM-DD hh:mm:ss ZZZ) ● Start 1 Hour(s) before the end time specified below. ○ End at (Format: YYYY-MM-DD hh:mm:ss ZZZ) ● End at Current Date/Time
Max Rows to Display:	● 500 ○ 1000 ○ 2000 ○ Time Period Summary View (Graphs Only)
	Submit Query or Show Advanced Options

Call Management Records - Displaying results between 2012-09-19 07:52:39 and 2012-09-19 08:52:39 (500 records)

dateTimeStamp	percentPacketsLost	jitter	latency	deviceName	globalCallId_ClusterId	publisher	jitterQoS	latencyQoS	packetlossQoS	MoS
2012-09-19 08:51:55	100.0000	0	0	SEP10BD18014B91	StandAloneCluster	LHRCM1001	Good	Good	Poor	Poor
2012-09-19 08:51:53	0	2	0	SEP00270DBF7C88	StandAloneCluster	strucmp1001	Good	Good	Good	Good
2012-09-19 08:51:48	0	2	0	SEP001D70FD5900	StandAloneCluster	strucmp1001	Good	Good	Good	Good
2012-09-19 08:51:46	0.0853	3	0	SEP10BD18014B91	StandAloneCluster	LHRCM1001	Good	Good	Good	Good
2012-09-19 08:51:44	0	1	0	SEP00270DBF8041	StandAloneCluster	strucmp1001	Good	Good	Good	Good
2012-09-19 08:51:41	0	2	0	SEP00270DBF801C	StandAloneCluster	strucmp1001	Good	Good	Good	Good
2012-09-19 08:51:41	0.0282	1	0	SEP64D989C33868	StandAloneCluster	strucmp1001	Good	Good	Good	Good
2012-09-19 08:51:38	0	2	0	SEP08173515D99F	StandAloneCluster	LHRCM1001	Good	Good	Good	Good
2012-09-19 08:51:38	0	1	0	SEPA8B1D41F247F	StandAloneCluster	strucmp1001	Good	Good	Good	Good
2012-09-19 08:51:28	68.7620	2	20	CiscoUM1-VI2	StandAloneCluster	strucmp1001	Good	Good	Poor	Poor
2012-09-19 08:51:17	0	2	0	SEPDC7B94772E4D	StandAloneCluster	LHRCM1001	Good	Good	Good	Good
2012-09-19 08:51:14	0.1817	1	0	SEP00270DBF95A7	StandAloneCluster	strucmp1001	Good	Good	Good	Good

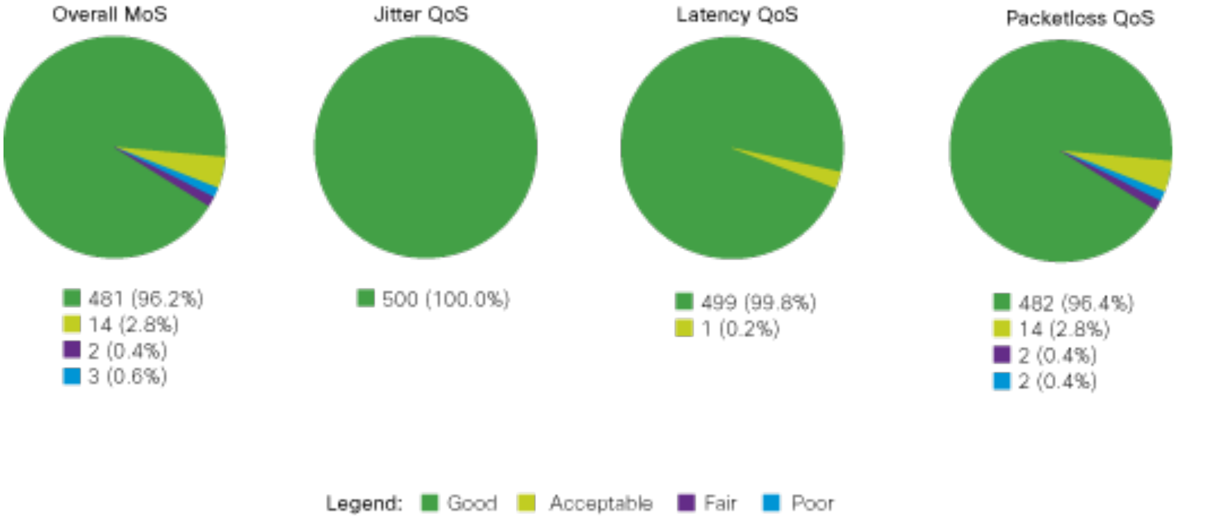
The figure above represents the default view for the **CMR Log** tab. The last 500 calls for the previous hour will show. Users can change the standard options such as the start and end date/time, the max records to display, and file format options for exporting.

On the header bar below the query form are the following icons representing links that offer CMR information in different formats:

- The **Toggle Graph Panel** icon will toggle on/off graphical representations of the call quality characteristics of Overall MoS, Jitter QoS, Latency QoS, and Packetloss QoS.
- Clicking the **Adobe Acrobat** icon will download only the graphical information into a PDF file format.
- Clicking the **Microsoft Excel** icon will download only the tabular data into a Microsoft Excel file format.
- The **Mailbox** icon will allow a user to select individuals they wish to email the results of the query to. Both the graphs (PDF) and tabular data (Excel) will be sent to the selected individuals.

By clicking on the **Toggle Graph Panel** icon, users can see summary graphs displaying metrics for Overall MoS, Jitter QoS, Latency QoS, and Packetloss QoS for the selected time period.

Figure 9. Toggle Graph Panel Icon Has Been Toggle “On” To Display Four Unique Pie Graphs – Overall, MoS Jitter QoS, Latency, and Packetloss Qos



Date Time Stamp	Percent Packets Lost	Jitter	Latency	Device Name	GlobalCall Id_Cluster ID	Publisher	JitterQoS	Letncy QoS	PacketlossQoS	MoS
2012-09-19 08:51:55	100.0000	0	0	SEP10BD18014B91	Stand Alone Cluster	LHRCM1001	Good	Good	Poor	Poor
2012-09-19 08:51:53	0	2	0	SEP00270DBF7C88	Stand Alone Cluster	Strucmp1001	Good	Good	Good	Good
2012-09-19 08:51:48	0	2	0	SEP001D70FD5900	Stand Alone Cluster	Strucmp1001	Good	Good	Good	Good
2012-09-19 08:51:46	0.0853	3	0	SEP10BD18014B91	Stand Alone Cluster	LHRCM1001	Good	Good	Good	Good
2012-09-19 08:51:44	0	1	0	SEP00270DBF8041	Stand Alone Cluster	Strucmp1001	Good	Good	Good	Good
2012-09-19 08:51:41	0	2	0	SEP00270DBF801C	Stand Alone Cluster	Strucmp1001	Good	Good	Good	Good

Within the Call Management Query and Record Log window of the CMR Log tab, users can drill down into a particular call by clicking on one of the alternately shaded lines in the lower portion of the window. The Call Detail Record Table View window will open, which will show Call Detail Records (CDR) from all legs of the call as well as any Call Management Records (CMR) associated in addition to all of the detailed information.

Table 58. Example Of A Detailed Call Management Record

CALL DETAIL RECORD SUMMARY						
Record	**Start Time**	**Connect Time**	**Disconnect Time**	**Duration**	**Calling Party**	**Called Party**
1.	2012-09-19 08:47:10	2012-09-19 08:47:16	2012-09-19 08:51:48	272s	918040255000	8204175

CALL MANAGEMENT RECORD SUMMARY			
Record	**Disconnect Time**	**Directory Number**	**Mean Opion Score**
1.	2012-09-19 08:51:48	8204175	Good

CALL DETAIL RECORD -1							
	Origination	**Connect**	**Disconnect**	**Duration**		**Origin**	**Destination**
DateTime	2012-09-19 08:47:10	2012-09-19 08:47:16	2012-09-19 08:51:48	272s	**DeviceName**	NewSP-STR-Trunk	SEP001D70FD5900
		Called Party			**IPAddr**	10.62.22.57	10.210.115.178
	Calling Party	**Original**	**Final**	**Last Redirect**	**MediaTransportAddress_IP (Port)**	10.12.190.13 (17052)	10.210.115.178 (18136)
Party Number	918040255000	8204175	8204175	8204175	**Ipv4v6Addr**		
Participation		ICM-PT	ICM-PT	ICM-PT	**Span**	122843700	0
OutpulsedParty Number					**Cause_Location**	0	0
UnicodeLogin UserID					**TerminationCause (Value)**	No Error (0)	Normal Call Clearing (16)
ProtocolCall Ref					**CallTerminationOnBehalfOf (Value)**	Unknown (0)	Device (12)
ProtocolID					**ConversationID**		0
RedirectReason (Value)		Unknown (0)		Unknown (0)	**Legidentifier**	122843700	122843701
RedirectOnBehalfOf (Value)		Unknown (0)		Unknown (0)	**PrecedenceLevel (Value)**	Routine (4)	Routine (4)
RoutingReason					**DTMFMethod**		
CallManager Name (!D)	7 (7)				**NodeID**	7	8
GlobalCallID	5971466				**MediaCap_Bandwidth**		
ClusterID	StandAloneCluster				**MediaCap_PayloadCapability**	G711u-law 64k	G711u-law 64k
CallType					**MediaCap_MaxFramesPerPacket**	20	20
Comment					**RAVPAudioStat**		
JoinOnBehalfOf (Value)	Unknown (0)				Not a video call.		
CallSecured Status							
AuthCode Description							
Authorization CodeValue							

Just like the **CDR Log** tab, the **CMR Log** tab query form also supports the **Show Advanced Options** button for users to refine the default search into something very specific. By clicking the Click Here link found within the **Refine Query** field, users can build their own query. Users can search by such items as extension, duration, device, publisher and cause code. To add more search terms, continue to click on the Click Here link. To remove a search term, click on the “X” link. You can also choose the fields to display in your output. Click on the Show/Hide icon (**+**) in the **Columns to Display** field of the query form to display the **Available** and **Selected** swap boxes. The fields shown in the **Selected** swap box are the field that will be shown in query output. You can select or deselect items to be displayed in the query output by clicking the name and dragging and dropping it into either the **Available** or **Selected** area of the query form. You can also move items up or down to put them in a select order as they will be seen in the query output. Click the **Submit Query** button to execute the query and display the CDR records meeting the specified search criteria. Prior to clicking the **Submit Query** button, if the constructed query will be used frequently, the user has the option to save the query parameters for future use. In the **Save this Query** field, enter a name for the query and click the **Save** button.

- To use a saved query in the future, use the drop down menu in the **Use Saved Query** field, select the name of the query by clicking on it, click the **Load** button and then the **Submit Query** button.
- To delete the saved query, use the drop down menu in the **Use Saved Query** field, select the name of the query by clicking on it, and click the **Delete** button.

Note: The Enterprise CDR/CMR Query Analysis and Log Reporting application is configured for customers with Enterprise Cisco IP Telephony applications.

Gatekeeper Statistics

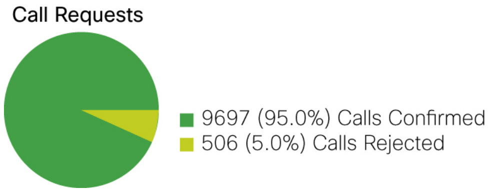
The CVP Gatekeeper report provides a near-real time dashboard of the gatekeeper zone call requests, calls confirmed, calls rejected, disengaged calls, concurrent calls, total bandwidth (if configured on the Cisco equipment), allocated bandwidth, and registered endpoints. The data updates either every minute or every five minutes depending on site traffic.

You will need to work with the Cisco Remote Management Services Service Desk or your designated Cisco MAP Engineer to ensure all elements required to generate the report are properly configured.

Table 59. Example Of The Cisco MAP Current Gatekeeper Statistics Report

Current Enterprise Gatekeeper Statistics

Statistic	Value
Gatekeepers Polled	6
Total Zones Polled	6
Zones Up	6
Concurrent Calls	6,279



Call Requests

Current Enterprise Gatekeeper Metrics

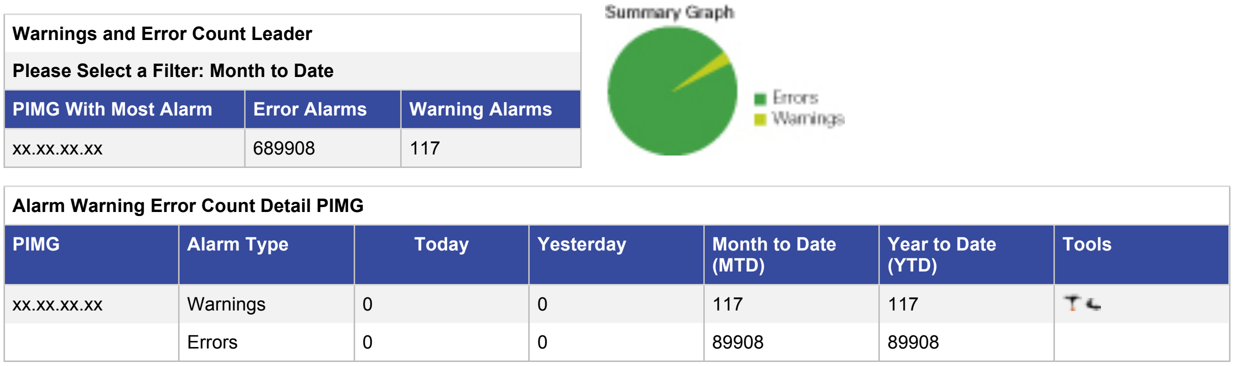
Zone	Gatekeeper	Requests	Confirmed	Rejected	Disengaged	Concurrent Calls	TotalBandwidth	AllocBandwidth	Endpoints	Last Poll	Duration
Gk_dcc	(123.213.113.131)	0	0	0	0	0	0.00 bps	0.00 bps	0	2009-10-29 11:00:03	301 s
Gk_dcc	(123.213.113.133)	5125	4855	257	4554	3116	0.00 bps	399 Mbps	49	2009-10-29 11:00:03	301 s
Gk_mcc	(123.213.113.134)	5070	4831	239	4548	3163	0.00 bps	405 Mbps	49	2009-10-29 11:00:03	301 s

Zone	Gatekeeper	Requests	Confirmed	Rejected	Disengaged	Concurrent Calls	TotalBandwidth	AllocBandwidth	Endpoints	Last Poll	Duration
Gk_mcc	(123.213.113.135)	0	0	0	0	0	0.00 bps	0.00 bps	0	2009-10-29 11:00:03	301 s
Gk_tcc	(123.213.113.139)	0	0	0	0	0	0.00 bps	0.00 bps	0	2009-10-29 11:00:04	302 s
Gk_tcc	(123.213.113.137)	0	0	0	0	0	0.00 bps	0.00 bps	49	2009-10-29 11:00:04	302 s

PIMG Alarm Statistics

The **PIMG Alarm Stats** dashboard view displays real time information for alarms generated by Cisco Unity PBX IP Media Gateway (PIMG) devices. The summary dashboard displays monitored devices and their warning and error counts, numerically and graphically, during a selected time period. Clicking on the IP address of a PIMG will display the Alarm Detail view for the device, which displays the date and time, alarm level, alarm code (in decimal and hex) and an alarm description for each alarm generated by the device.

Table 60. PIMG Alarm Stats Summary Dashboard View



Warnings and Error Count Leader

Please Select a Filter: Month to Date

PIMG With Most Alarm	Error Alarms	Warning Alarms
xx.xx.xx.xx	689908	117

Alarm Warning Error Count Detail PIMG

PIMG	Alarm Type	Today	Yesterday	Month to Date (MTD)	Year to Date (YTD)	Tools
xx.xx.xx.xx	Warnings	0	0	117	117	
	Errors	0	0	89908	89908	

From the PIMG Alarm Statistics summary view, you have the options of:

- Selecting the time period to view. Selecting a new time period will update the error and warning counts for the displayed devices.
- Clicking on the IP address of a PIMG to open the PIMG Alarm Details window for the device, which displays detailed warning and error information for the device.

Table 61. PIMG Alarm Details Window

Alarm History

Alarm Datetime	Alarm Level	Alarm Code (Decimal)	Alarm Cod3 (Hex)	Alarm Description
2010-02-14 04:40:01	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:39:56	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:39:50	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:39:44	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:39:39	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:39:33	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:39:27	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:39:22	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:39:17	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:39:12	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:39:07	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:39:01	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:38:56	Error	258	0x0102	SIP Resources Unavailable
2010-02-14 04:38:50	Error	258	0x0102	SIP Resources Unavailable

Note: The PIMG Alarm Stats dashboard is configured for customers with Cisco CallManager/Unity environments having a Cisco Unity PBX IP Media Gateway (PIMG) device as an element.

PIMG Call Statistics

The **PIMG Call Stats** dashboard view displays near real time information for call serviced by Cisco Unity PBX IP Media Gateway (PIMG) devices. The summary dashboard displays monitored devices and their switched and VoIP call counts, numerically and graphically, during a selected time period. Clicking on the name of a PIMG will display the Call Detail view for the device, which displays inbound and outbound call information for each call serviced by the device.

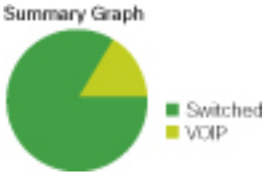
Table 62. PIMG Call Statistics Summary Dashboard View

Call Leader

Please Select a Filter: Year to Date

PIMG With Most Call Activity	Switch Network	VOIP Network
Nyc05-pimg01	728	165

Summary Graph



Call Summary by PIMG

PIMG	Alarm Type	Today	Yesterday	Month to Date (MTD)	Year to Date (YTD)	Tools
Nyc05-pimg01	Switch Network	0	0	0	728	⚒ ↩
	VoIP Network	0	0	0	165	

From the PIMG Call Statistics summary view, you have the options of:

- Selecting the time period to view. Selecting a new time period will update the call counts for the displayed devices.
- Clicking on the IP address of a PIMG to open the PIMG Call Record Details window for the device, which displays detailed inbound and outbound call information for the device.

Table 63. PIMG Call Request Record Details Window

Show: Switched &YoP Calls

Call History

Syslog Record Time	Call Record Num	Call Direction	Call Start Time	Call End Time	Inbound Info	Outbound Info	
2010-12-28 11:33:46	151481	From TDM Network	2921:26:002	2921:27:004	[7:1 8154051.->->, [Rsn=FwdAll]]	[8154051.->,,xx.xx.xx.xx ,->, [Rsn=Direct]]	
2010-12-28 11:33:05	151479	From TDM Network	2921:25:059	2921:26:020	[5:1 8155236,->,->8153442, [Rsn=FwdAll]]	[8155236,->,, xx.xx.xx.xx:,->8153442, [Rsn=FwdAll]]	TDM: Normal
2010-12-28 11:32:58	151478	From TDM Network	2921:25:057	2921:26:016	[4:! 9735719091,, TEXAS ->'->,->8152207, [Rsn=Busy]]	[9735719091, TEXAS->'->,,xx.xx.xx.xx ,->8152207 , [Rsn=Busy]]	TDM: Normal
2010-12-28 11:32:54	151474	From TDM Network	2921:25:049	2921:26:008	[1:1 6464451151, SUNGARD,->,->8157068, [Rsn=NoAns]]	[6464451151, SUNGARD,->,, xx.xx.xx.xx,->8157068, [Rsn=NoAns]]	TDM: Normal
2010-12-28 11:32:42	151476	From VoIP Network	2921:25:052	2921:25:054	[,,10.59.212.77 xx.xx.xx.xx'->8152207 xx.xx.xx.xx. ,8152207@xx.xx.xx.xx.'Msg Set]]		
2010-12-28 11:31:51	151472	From TDM Network	2921:25:055	2921:25:012	[7:1 8563040857, SUNGARD, ->,IN->,->8155616, [Rsn=NoAns]]	[8563040857,,SUNGARD,OHN->,,xx.xx.xx.xx,->8155616, [Rsn=NoAns]]	TDM: Normal
2010-12-28 11:31:05	151473	From VoIP Network	2921:25:022	2921:24:024	[,,10.59.212.77 xx.xx.xx.xx'->8152207 xx.xx.xx.xx. ,8152207@xx.xx.xx.xx.'Msg Set]]	[8:1,->8158210, [MsgSet]]	TDM: Normal
2010-12-28 11:29:57	151468	From TDM Network	2921:25:035	2921:23:016	[3:1 5158683809,SUNGARD,->,x->,->8155241, [Rsn=FwdAll]]	[5158653809,,SUNGARD,EX->,,xx.xx.xx.xx:,->8155241, [Rsn=FwdAll]]	TDM: Normal
2010-12-28 11:29:49	151467	From TDM Network	2921:25:032	2921:23:008	[2:1 2144685000, TEXAS->,->815532, [Rsn=NoAns]]	[8155532,->,, xx.xx.xx.xx_->8155532, [Rsn=Busy]]	TDM: Normal
2010-12-28 11:29:45	151471	From TDM Network	2921:25:042	2921:22:057	[6:1 8151161,->,->8152734, [Rsn=NoAns]]	[8151161,->, xx.xx.xx.xx ,->8152734 , [Rsn=NoAns]]	TDM: Normal
2010-12-28 11:29:35	151469	From TDM Network	2921:25:039	2921:22:048	[4:1 9084033014, NEW JERSEY ->,->8152162, [Rsn=NoAns]]	[9084033014, NEW JERSEY ->,, xx.xx.xx.xx ,->8152162, [Rsn=NoAns]]	TDM: Normal

Note: The PIMG Call Stats dashboard is configured for customers with Cisco CallManager/Unity environments having a Cisco Unity PBX IP Media Gateway (PIMG) device as an element.

Contact Center Reporting

The System Activity Report is designed to provide a report on the daily traffic of Peripheral Gateways (PGs) and the Peripheral Interface Managers (PIMs) associated with them. The System Activity Report utilizes data stored on a customer's Historical Data Server (HDS) for the Cisco ICM environment, which logs data from the ICM logger for historical purposes.

The System Activity Report details the daily network traffic for a selected Peripheral Gateway(s) (PGs) or Peripheral Interface Manager(s) (PIMs) for a selected date.

The System Activity Report displays the hourly and running total of CVP, ICM, Dialer, WIM, and EIM calls handled by the Peripheral Gateway(s) or Peripheral Interface Manager(s) during the reporting period. The results are displayed in a new browser window with the option to download the report in either CSV or PDF file format.

Table 64. System Activity Report

Description: Report On Daily Traffic Of Peripheral Gateways (Pgs) and The Peripheral Interface Managers (PIMs) Associated With Them
Run Date: 2010-Jun-30 13:56:41
Time Zone: EDT Time Period: 2010-06-30
Run By: mchambers

Active Calls					
PG	**CVP**	**ICM**	**Dialer**	**WIM**	**EIM**
SG_UCCE_PG01	0	0			

		CVP Calls		**ICM Calls**		**Dialer Calls**		**WIM Calls**		**EIM Calls**	
PG	**Date & Time Slice**	**Total By Hour**	**Running Total**	**Total By Hour**	**Running Total**	**Total By Hour**	**Running Total**	**Total By Hour**	**Running Total**	**Total By Hour**	**Running Total**
SG_UCCE_PG01	2010-Jun-30 00:00	0	0	0	0						
SG_UCCE_PG01	2010-Jun-30 01:00	2	2	2	2						
SG_UCCE_PG01	2010-Jun-30 02:00	1	3	1	3						
SG_UCCE_PG01	2010-Jun-30 03:00	6	9	6	9						
SG_UCCE_PG01	2010-Jun-30 04:00	2	11	2	11						
SG_UCCE_PG01	2010-Jun-30 05:00	3	14	3	14						
SG_UCCE_PG01	2010-Jun-30 06:00	1	15	1	15						
SG_UCCE_PG01	2010-Jun-30 07:00	2	17	2	17						
SG_UCCE_PG01	2010-Jun-30 08:00	10	27	10	27						
SG_UCCE_PG01	2010-Jun-30 09:00	5	32	5	32						
SG_UCCE_PG01	2010-Jun-30 10:00	8	40	8	40						
SG_UCCE_PG01	2010-Jun-30 11:00	4	44	4	44						
SG_UCCE_PG01	2010-Jun-30 12:00	3	47	3	47						
SG_UCCE_PG01	2010-Jun-30 13:00	11	58	11	58						

Note: The System Activity Report is configured for customers with a Cisco Intelligent Contact Manager (ICM) or Unified Contact Center Enterprise environment.

Note: Please be aware that before the System Activity Report can be run, Cisco MAP must be configured with access information for the Customer's Historical Database Server (HDS). Customers can contact their Cisco MAP Customer Service Manager to discuss the back-end configuration required to run this report.

- **Host** – IP or Resolvable hostname for the HDS, including Port Number for access (default: 1433)
- **Username** – Login to the system with privileges to access the database
- **Password** – Password for login
- **Database** – Database with applicable PG and PIM data

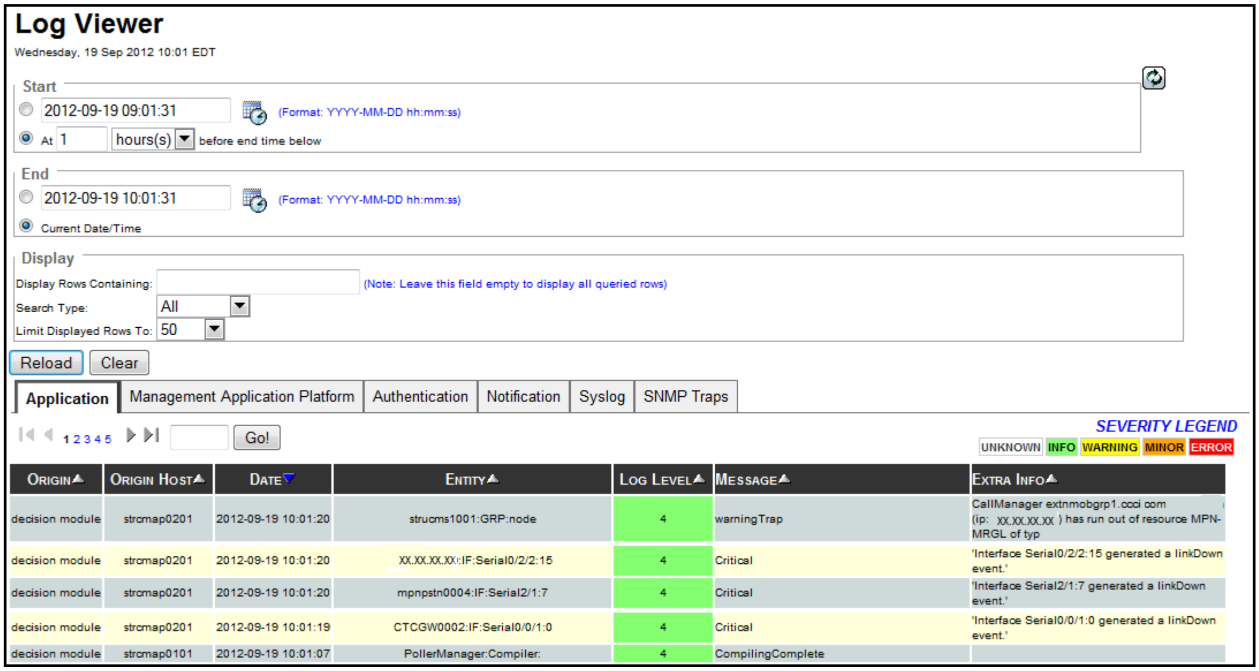
Event Log Viewer

Cisco MAP provides a central repository for event logging. Use Cisco MAP to collect and analyze your event logs from a central location in real time. Cisco MAP's Event Log Viewer allows administrators to manage event logs from one central location as well as correlate different events over multiple machines or multiple days. Cisco MAP administrators will be able to audit and report on all event log information from one place.

From the Cisco MAP Log Viewer window, the user can view up-to-the-minute log files of various Cisco MAP modules and processes and other systems. Entries in the Log Viewer are color coded by severity.

The upper portion of the Log Viewer window constitutes a search feature and is present when any of the Log Viewer tabs is selected. The search feature allows the user to focus the log viewer on specific messages or traps.

Figure 10. Cisco MAP Log Viewer Window



Log Viewer

Wednesday, 19 Sep 2012 10:01 EDT

Start

○ 2012-09-19 09:01:31 (Format: YYYY-MM-DD hh:mm:ss)

● At 1 hours(s) before end time below

End

○ 2012-09-19 10:01:31 (Format: YYYY-MM-DD hh:mm:ss)

● Current Date/Time

Display

Display Rows Containing: (Note: Leave this field empty to display all queried rows)

Search Type: All

Limit Displayed Rows To: 50

Origin	Origin Host	Date	Entity	Log Level	Message	Extra Info
decision module	strcmap0201	2012-09-19 10:01:20	strucms1001:GRP:node	4	warningTrap	CallManager extnmobgrp1.ccci com (ip: XX.XX.XX.XX) has run out of resource MPN-MRGL of typ
decision module	strcmap0201	2012-09-19 10:01:20	XX.XX.XX.XX:IF:Serial0/2/2:15	4	Critical	'Interface Serial0/2/2:15 generated a linkDown event.'
decision module	strcmap0201	2012-09-19 10:01:20	mpnpstn0004:IF:Serial2/1:7	4	Critical	'Interface Serial2/1:7 generated a linkDown event.'
decision module	strcmap0201	2012-09-19 10:01:19	CTCGW0002:IF:Serial0/0/1:0	4	Critical	'Interface Serial0/0/1:0 generated a linkDown event.'
decision module	strcmap0101	2012-09-19 10:01:07	PollerManager:Compiler:	4	CompilingComplete	

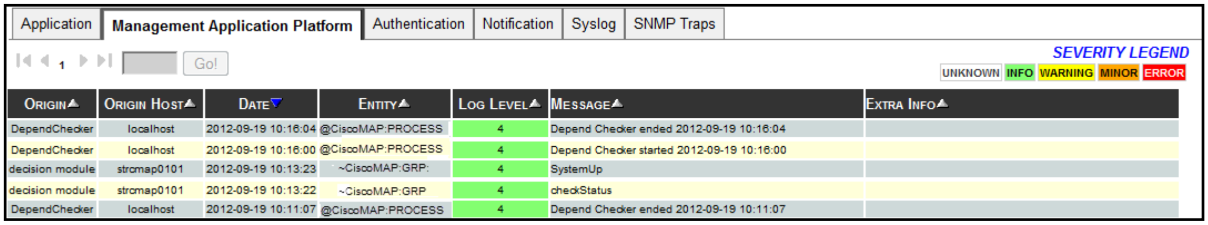
There are six tabs available in the Log Viewer window:

- Application
  - **Origin** – The creation technique that generated the message
  - **Date/Time** – The entry time of the message
  - **Entity** – The service, process, or device
  - **Log Level** – The priority of the message
  - **Message** – The description of fault discovered
- Management Application Platform

  The Management Application Platform tab displays the log file entries for various Cisco MAP running processes including the SnapshotStatus Poller and the DependChecker. The information displayed in the Cisco MAP tab of the Log Viewer window is:

  - **Origin** – The creation technique that generated the message
  - **Date/Time** – The entry time of the message
  - **Entity** – The service, process, or device
  - **Log Level** – The priority of the message
  - **Message** – The description of fault discovered

Figure 11. Log Viewer: Management Application Platform Tab



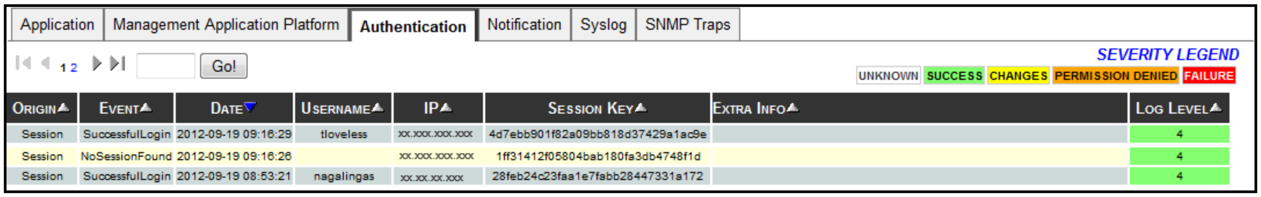
ORIGIN	ORIGIN HOST	DATE	ENTITY	LOG LEVEL	MESSAGE	EXTRA INFO
DependChecker	localhost	2012-09-19 10:16:04	@CiscoMAP:PROCESS	4	Depend Checker ended 2012-09-19 10:16:04	
DependChecker	localhost	2012-09-19 10:16:00	@CiscoMAP:PROCESS	4	Depend Checker started 2012-09-19 10:16:00	
decision module	strcmap0101	2012-09-19 10:13:23	~CiscoMAP:GRP:	4	SystemUp	
decision module	strcmap0101	2012-09-19 10:13:22	~CiscoMAP:GRP	4	checkStatus	
DependChecker	localhost	2012-09-19 10:11:07	@CiscoMAP:PROCESS	4	Depend Checker ended 2012-09-19 10:11:07	

- Authentication

  The Authentication tab displays user login, logout, and session information. The information displayed in the Authentication tab of the Log Viewer window is:

  - **Origin** – The creation technique that generated the message
  - **Event** – The authentication event type
  - **Date** – The entry time of the message
  - **Username** – The username associated with the authentication event
  - **IP** – The originating IP address of the authentication event
  - **Message** – The description of fault discovered
  - **Log Level** – The priority of the message

Figure 12. Log Viewer Authentication Tab



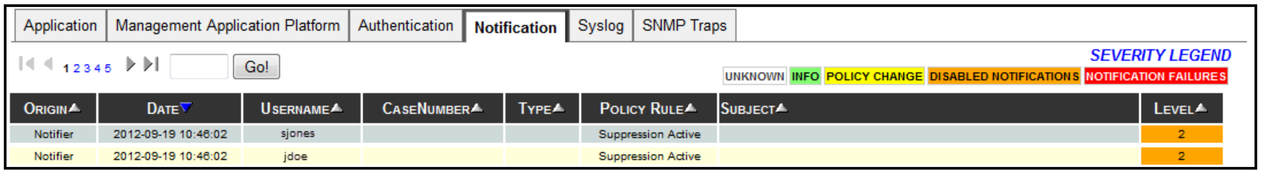
Origin	Event	Date	Username	IP	Session Key	Extra Info	Log Level
Session	SuccessfulLogin	2012-09-19 09:16:29	tloveless	xx.xxx.xxx.xxx	4d7ebb901f82a09bb818d37429a1ac9e		4
Session	NoSessionFound	2012-09-19 09:16:26		xx.xxx.xxx.xxx	1ff31412f05804bab180fa3db4748f1d		4
Session	SuccessfulLogin	2012-09-19 08:53:21	nagalingas	xx.xx.xx.xxx	28feb24c23faa1e7fabb28447331a172		4

- Notification

  The Notification tab displays log file entries for all notifications generated within Log Level (the priority of the message). The information displayed in the Notification tab of the Log Viewer window is:

  - **Origin** – The creation technique that generated the message
  - **Date** – The entry time of the message
  - **Username** – The username associated with the authentication report
  - **Case Number** – The Cisco MAP case number associated with the logged notification
  - **Type** – The type of notification report
  - **Policy Rule** – Notes the policy rule that generated the notification
  - **Level** – The priority of the message

Figure 13. Log Viewer: Notification Tab



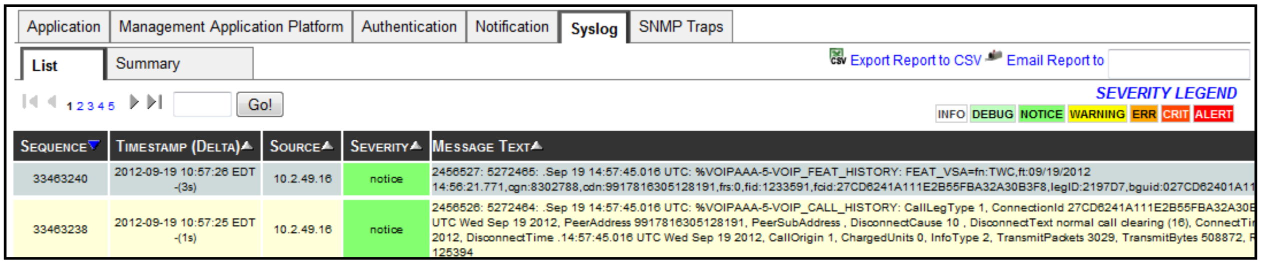
Origin	Date	Username	CaseNumber	Type	Policy Rule	Subject	Level
Notifier	2012-09-19 10:46:02	sjones			Suppression Active		2
Notifier	2012-09-19 10:46:02	jdoe			Suppression Active		2

- Syslog

  The Syslog tab displays syslog messages generated by devices configured to send syslog messages to Cisco MAP. The entries appear with the following details:

  - **Sequence** – The sequence number of the trap
  - **Timestamp (Delta)** – The time that the syslog message was generated
  - **Source** – The IP address of the device generating the message
  - **Severity** – The severity of the generated message (e.g., info, error, etc.)
  - **Message Text** – The text of the generated message

Figure 14. Log Viewer: Syslog Tab



Sequence	Timestamp (Delta)	Source	Severity	Message Text
33463240	2012-09-19 10:57:26 EDT -(3s)	10.2.49.16	notice	2456527: 5272465: .Sep 19 14:57:45.016 UTC: %VOIPAAA-5-VOIP_FEAT_HISTORY: FEAT_VSA=fn:TWC,ft:09/19/2012 14:56:21.771,cgn:8302788,cdn:9917816305128191,frs:0,fid:1233591,fcid:27CD6241A111E2B55FBA32A30B3F8,legID:2197D7,bguid:027CD62401A11
33463238	2012-09-19 10:57:25 EDT -(1s)	10.2.49.16	notice	2456526: 5272464: .Sep 19 14:57:45.016 UTC: %VOIPAAA-5-VOIP_CALL_HISTORY: CallLegType 1, ConnectionId 27CD6241A111E2B55FBA32A30E UTC Wed Sep 19 2012, PeerAddress 9917816305128191, PeerSubAddress , DisconnectCause 10 , DisconnectText normal call clearing (16), ConnectTi 2012, DisconnectTime .14:57:45.016 UTC Wed Sep 19 2012, CallOrigin 1, ChargedUnits 0, InfoType 2, TransmitPackets 3029, TransmitBytes 508872, F 125394

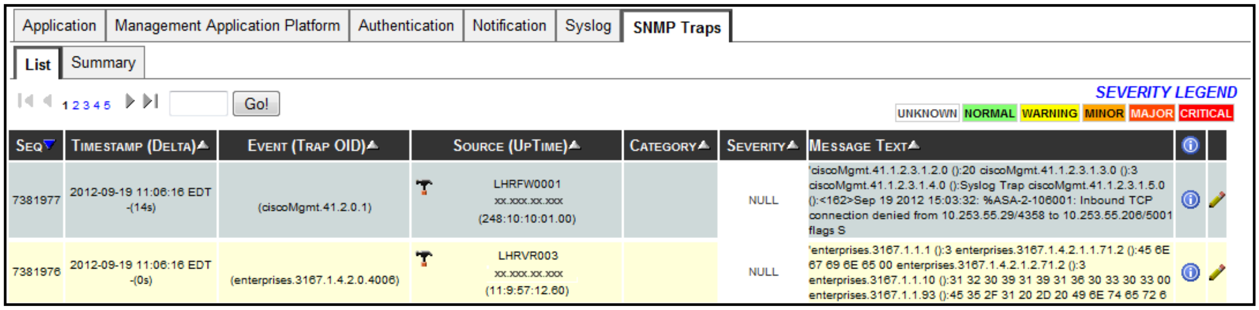
- SNMP Traps

  The SNMP Traps tab displays the SNMP Trap messages received from the monitored network devices and used by Cisco MAP for identification and validation of system fault conditions. This information is useful in evaluating the precise steps that were involved in the identification and validation of a system fault. Clicking on the SNMP Traps tab will open a List and Summary tab to open.

  The information displayed in the **List** tab is:

  - **Seq** – The sequence number of the trap
  - **Timestamp (Delta)** – The time that the trap message was generated
  - **Event (Trap IOD)** – The event causing the trap message to be generated
  - **Source (Uptime)** – The source name, IP address, and device uptime of the device generating the trap message
  - **Category** – The category defined for the trap message
  - **Severity** – Severity level of the trap message
  - **Message Text** – The text of the trap message

Figure 15. Log Viewer: SNMP Traps > List Subview Tab

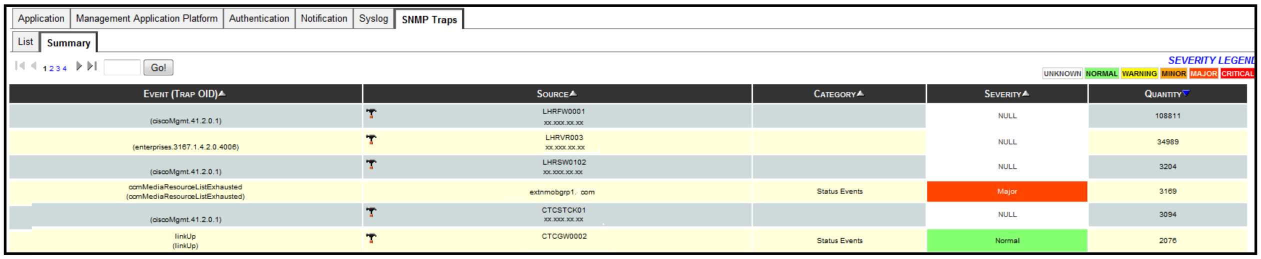


Seq	Timestamp (Delta)	Event (Trap OID)	Source (UpTime)	Category	Severity	Message Text		
7381977	2012-09-19 11:06:16 EDT -(14s)	(ciscoMgmt.41.2.0.1)	LHRFW0001 xx.xxx.xx.xxx (248:10:10:01.00)		NULL	'ciscoMgmt.41.1.2.3.1.2.0 ():20 ciscoMgmt.41.1.2.3.1.3.0 ():3 ciscoMgmt.41.1.2.3.1.4.0 ():Syslog Trap ciscoMgmt.41.1.2.3.1.5.0 ():<162>Sep 19 2012 15:03:32: %ASA-2-106001: Inbound TCP connection denied from 10.253.55.29/4358 to 10.253.55.206/5001 flags S	ⓘ	✎
7381976	2012-09-19 11:06:16 EDT -(0s)	(enterprises.3167.1.4.2.0.4006)	LHRVR003 xx.xxx.xx.xxx (11:9:57:12.60)		NULL	'enterprises.3167.1.1.1 ():3 enterprises.3167.1.4.2.1.1.71.2 ():45 6E 67 69 6E 65 00 enterprises.3167.1.4.2.1.2.71.2 ():3 enterprises.3167.1.1.10 ():31 32 30 39 31 39 31 36 30 33 30 33 00 enterprises.3167.1.1.93 ():45 35 2F 31 20 2D 20 49 6E 74 65 72 6	ⓘ	✎

The information displayed in the **Summary** tab is:

- **Event (Trap IOD)** – The event causing the trap message to be generated
- **Source** – The source name, IP address, and device uptime of the device generating the trap message
- **Category** – The category defined for the trap message
- **Severity** – Severity level of the trap message
- **Quantity** – The total number of trap messages generated by an Event type

Figure 16. Log Viewer: SNMP Traps > Summary Subview Tab



Event (Trap OID)	Source	Category	Severity	Quantity
(ciscoMgmt.41.2.0.1)	LHRFW0001 xx.xxx.xx.xx		NULL	108811
(enterprises.3167.1.4.2.0.4006)	LHRVR003 xx.xxx.xx.xx		NULL	34989
(ciscoMgmt.41.2.0.1)	LHRSW0102 xx.xxx.xx.xx		NULL	3204
cmMediaResourceListExhausted (cmMediaResourceListExhausted)	extnmobgrp1. com	Status Events	Major	3169
(ciscoMgmt.41.2.0.1)	CTCSTCK01 xx.xxx.xx.xx		NULL	3094
linkUp (linkUp)	CTCGW0002	Status Events	Normal	2076

IP SLA Manager

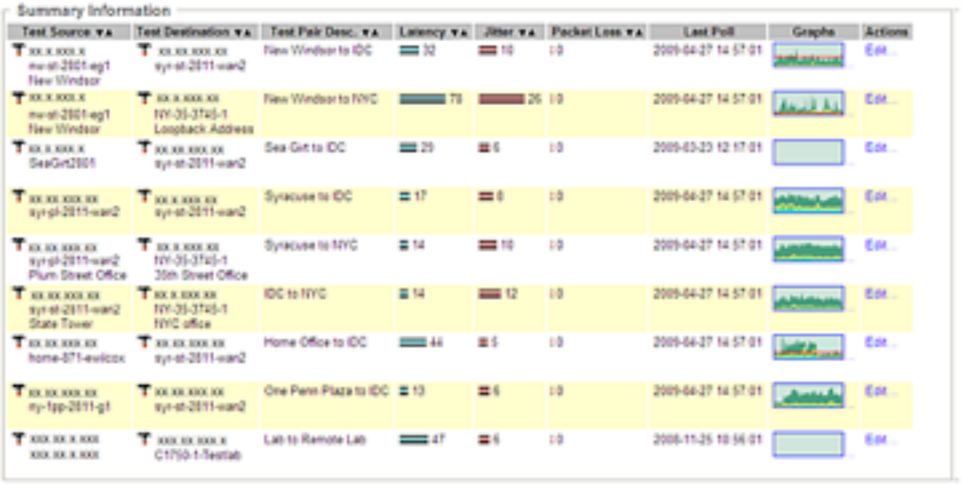
Network services are changing dramatically with the addition of voice, video, and other mission-critical delay-and-performance-sensitive applications. As usage and reliance on these IP-based applications continues to grow, so has the user and business expectation that they are not only highly available services, but that they also offer quality levels of service necessary to increase productivity, lower operational costs, reduce the frequency of outages, and increase the success of collaboration.

Service levels are crucial because they affect the performance of IP services and business-critical applications. SLAs between service providers and customers, or between corporate Enterprise IT departments and end-users, are intended to provide service guarantees and validate network performance on an ongoing basis. SLAs should be simple to understand and should improve Mean Time to Repair (MTTR).

When there is no network performance visibility, there is a higher chance of network downtime and greater potential for decreased network reliability. If network administrators and support personnel can measure how well the network is performing for each service, they can use that information to improve network performance, network operations, and user satisfaction. Effectively measuring and monitoring IP services in real-time contributes to increased availability, effective troubleshooting, and faster deployment of network applications in order to further business or organizational goals.

Manually implementing IP SLA commands can be time consuming; however, Cisco engineers do the work so you don’t have to – they will work with you to ensure IP SLA on Cisco routers and switches is enabled and they will configure the operational details associated with each source and destination pair. The performance information will be presented in an easy-to-read dashboard. The intuitive dashboard interface allows you to easily monitor common IP SLA operations, including latency, jitter, packet loss, and DNS resolution. The Cisco Management Application Platform’s IP SLA will allow you to track trends, create threshold alerts, and monitor the performance between devices anywhere on the network.

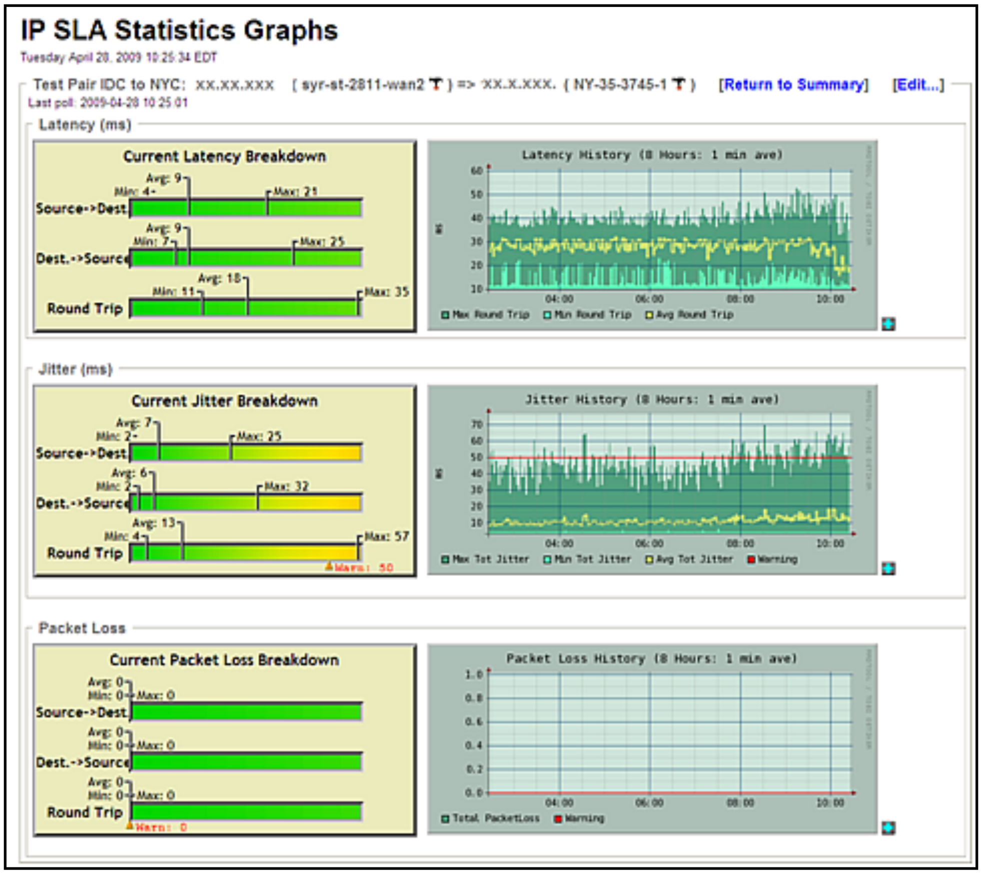
Figure 17. IP SLA Summary Dashboard Showing The Test Sourse And Destination, Description, Latency, Jiter, And Packet Loss Statistics For Each Source/Destination Pair



Summary Information

Test Source ▼▲	Test Destination ▼▲	Test Pair Desc. ▼▲	Latency ▼▲	Jitter ▼▲	Packet Loss ▼▲	Last Poll	Graphs	Actions
xx.x.xxx.x nw-st-2801-eg1 New Windsor	xx.xx.xxx.xx syr-st-2811-wan2	New Windsor to IDC	32	10	0	2009-04-27 14:57:01		Edit...
xx.x.xxx.x nw-st-2801-eg1 New Windsor	xx.x.xxx.xx NY-35-3745-1 Loopback Address	New Windsor to NYC	78	26	0	2009-04-27 14:57:01		Edit...
xx.x.xxx.x SeaGirt2801	xx.xx.xxx.xx syr-st-2811-wan2	Sea Girt to IDC	25	6	0	2009-03-23 12:17:01		Edit...
xx.xx.xxx.xx syr-pl-2811-wan2	xx.x.xxx.xx syr-st-2811-wan2	Syracuse to IDC	17	6	0	2009-04-27 14:57:01		Edit...
xx.xx.xxx.xx syr-pl-2811-wan2 Plum Street Office	xx.x.xxx.xx NY-35-3745-1 35th Street Office	Syracuse to NYC	14	10	0	2009-04-27 14:57:01		Edit...
xx.xx.xxx.xx syr-st-2811-wan2 State Tower	xx.x.xxx.xx NY-35-3745-1 NYC office	IDC to NYC	14	12	0	2009-04-27 14:57:01		Edit...
xx.xx.xxx.xx home-871-ewilcox	xx.xx.xxx.xx syr-st-2811-wan2	Home Office to IDC	44	5	0	2009-04-27 14:57:01		Edit...
xx.xx.xxx.xx ny-1pp-2811-g1	xx.xx.xxx.xx syr-st-2811-wan2	One Penn Plaza to IDC	13	6	0	2009-04-27 14:57:01		Edit...
xxx.xx.x.xxx xxx.xx.x.xxx	xxx.xx.xxx.x C1700-1-Testlab	Lab to Remote Lab	47	6	0	2008-11-25 10:56:01		Edit...

Figure 18. Additional Sampling of IP SLA Graphs When Drilling Down Into A Test Pair



IP SLA Statistics Graphs

Tuesday April 28, 2009 10:25:34 EDT

Test Pair IDC to NYC: xx.xx.xxx (syr-st-2811-wan2) => xx.x.xxx. (NY-35-3745-1) [Return to Summary] [Edit...]

Last poll: 2009-04-28 10:25:01

Please note that charges may be incurred for configuration time depending on the scope of work required. In addition, larger enterprise customers may require an additional appliance(s) depending on the number of routers.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 10/12