ARGENT ENCYCLOPEDIA

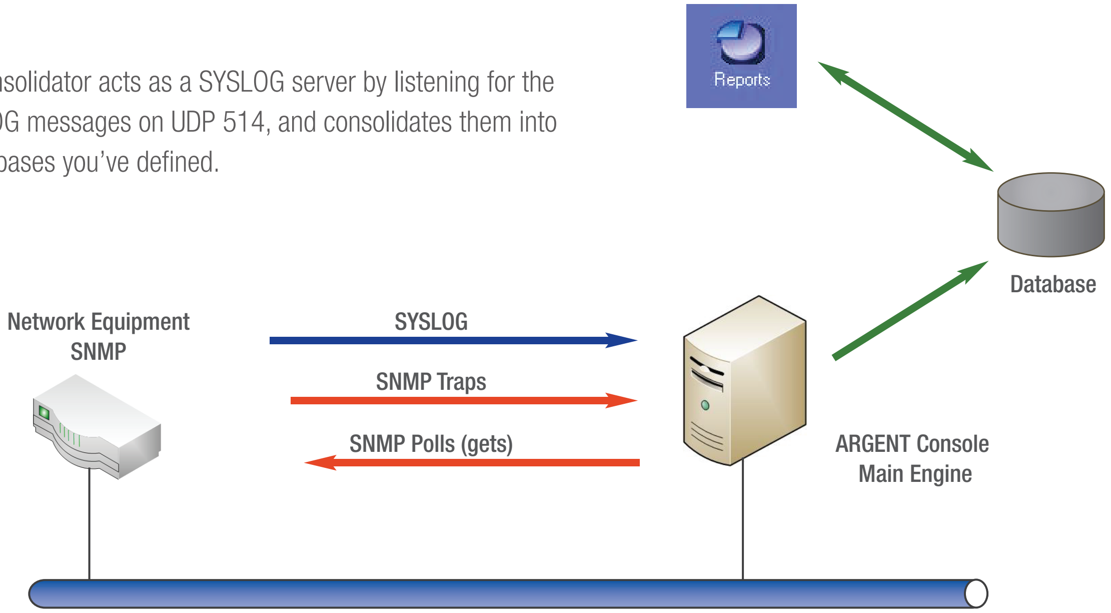
Argent Extended Technology
SNMP Overview

Contents

Network Device Monitoring Using Argent Extended Technology

The Argent SNMP Monitor is a comprehensive SNMP monitoring and alerting solution that periodically checks SNMP statistics and listens for SNMP traps.

Argent Data Consolidator acts as a SYSLOG server by listening for the incoming SYSLOG messages on UDP 514, and consolidates them into the central databases you've defined.



Argent SNMP Monitor

Connectivity Rules

These Rules check whether an application is running and accessible over the network and can also be used to provide SLA reporting for Downtime vs. Uptime.

The Rules provide the following options for checking connectivity:

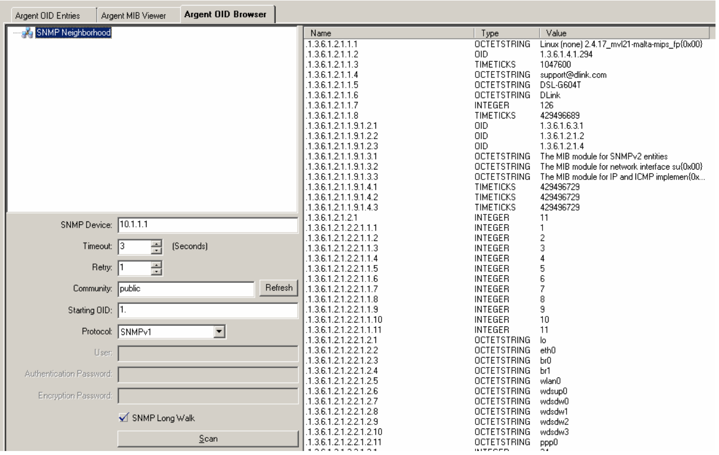
- Ping
- TCP/IP port scan (Port 23 for example)
- Contact Installed Remote SNMP Service On Device

The Contact Installed Remote SNMP Service On Device option verifies the device is online, and also verifies the SNMP community string is accurate.

NOTE: An SNMP community string is a text string that acts much like a password. It is used to authenticate messages sent between the management station (the SNMP manager -- Argent SNMP Monitor, in this case) and the device (the SNMP agent). The community string is included in every packet between Argent and the device.

SNMP Rules

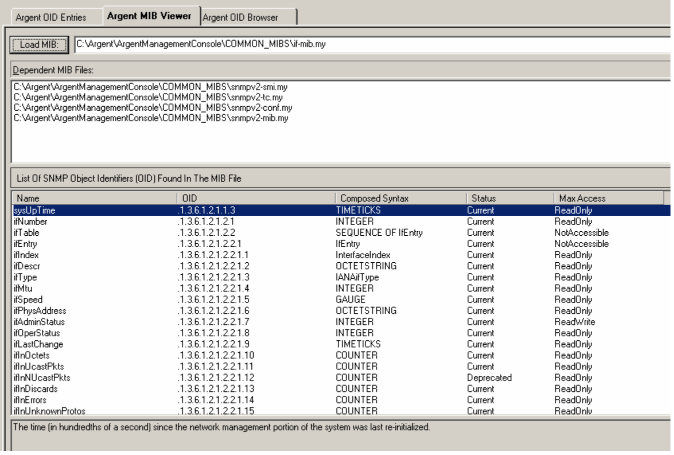
These allow the polling of OID's by either manually specifying the value or using the Argent OID Browser.



SNMP Device: 10.1.1.1
Timeout: 3 (Seconds)
Retry: 1
Community: public
Starting OID: 1.
Protocol: SNMPv1
User:
Authentication Password:
Encryption Password:
☑ SNMP Long Walk

Name	Type	Value
.1.3.6.1.2.1.1.1	OCTETSTRING	Linux (none) 2.4.17_mvl21-malta-mips_fp{0x00}
.1.3.6.1.2.1.1.2	OID	1.3.6.1.4.1.294
.1.3.6.1.2.1.1.3	TIMETICKS	1047600
.1.3.6.1.2.1.1.4	OCTETSTRING	support@dlink.com
.1.3.6.1.2.1.1.5	OCTETSTRING	DSL-G604T
.1.3.6.1.2.1.1.6	OCTETSTRING	DLink
.1.3.6.1.2.1.1.7	INTEGER	126
.1.3.6.1.2.1.1.8	TIMETICKS	429496689
.1.3.6.1.2.1.1.9.1.2.1	OID	1.3.6.1.6.3.1
.1.3.6.1.2.1.1.9.1.2.2	OID	1.3.6.1.2.1.2
.1.3.6.1.2.1.1.9.1.2.3	OID	1.3.6.1.2.1.4
.1.3.6.1.2.1.1.9.1.3.1	OCTETSTRING	The MIB module for SNMPv2 entities
.1.3.6.1.2.1.1.9.1.3.2	OCTETSTRING	The MIB module for network interface su{0x00}
.1.3.6.1.2.1.1.9.1.3.3	OCTETSTRING	The MIB module for IP and ICMP implemen{0x...
.1.3.6.1.2.1.1.9.1.4.1	TIMETICKS	429496729
.1.3.6.1.2.1.1.9.1.4.2	TIMETICKS	429496729
.1.3.6.1.2.1.1.9.1.4.3	TIMETICKS	429496729
.1.3.6.1.2.1.2.1	INTEGER	11
.1.3.6.1.2.1.2.2.1.1.1	INTEGER	1
.1.3.6.1.2.1.2.2.1.1.2	INTEGER	2
.1.3.6.1.2.1.2.2.1.1.3	INTEGER	3
.1.3.6.1.2.1.2.2.1.1.4	INTEGER	4
.1.3.6.1.2.1.2.2.1.1.5	INTEGER	5
.1.3.6.1.2.1.2.2.1.1.6	INTEGER	6
.1.3.6.1.2.1.2.2.1.1.7	INTEGER	7
.1.3.6.1.2.1.2.2.1.1.8	INTEGER	8
.1.3.6.1.2.1.2.2.1.1.9	INTEGER	9
.1.3.6.1.2.1.2.2.1.1.10	INTEGER	10
.1.3.6.1.2.1.2.2.1.1.11	INTEGER	11
.1.3.6.1.2.1.2.2.1.2.1	OCTETSTRING	lo
.1.3.6.1.2.1.2.2.1.2.2	OCTETSTRING	eth0
.1.3.6.1.2.1.2.2.1.2.3	OCTETSTRING	br0
.1.3.6.1.2.1.2.2.1.2.4	OCTETSTRING	br1
.1.3.6.1.2.1.2.2.1.2.5	OCTETSTRING	wlan0
.1.3.6.1.2.1.2.2.1.2.6	OCTETSTRING	wdsup0
.1.3.6.1.2.1.2.2.1.2.7	OCTETSTRING	wdsdw0
.1.3.6.1.2.1.2.2.1.2.8	OCTETSTRING	wdsdw1
.1.3.6.1.2.1.2.2.1.2.9	OCTETSTRING	wdsdw2
.1.3.6.1.2.1.2.2.1.2.10	OCTETSTRING	wdsdw3
.1.3.6.1.2.1.2.2.1.2.11	OCTETSTRING	ppp0

OID values can also be added by using the device specific MIB file - The Argent MIB Viewer allows you to create SNMP Rules from any manufacturer's MIB files. Argent can create these Rules for you as well - The MIB files govern what's possible to do or see via SNMP for a particular device.



C:\Argent\ArgentManagementConsole\COMMON_MIBS\if-mib.my

Dependent MIB Files:

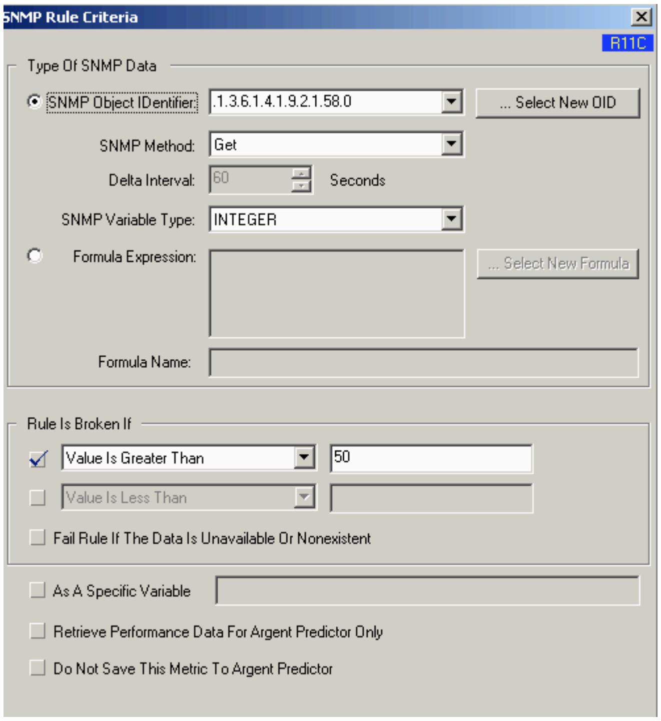
C:\Argent\ArgentManagementConsole\COMMON_MIBS\snmpv2-smi.my
C:\Argent\ArgentManagementConsole\COMMON_MIBS\snmpv2-tc.my
C:\Argent\ArgentManagementConsole\COMMON_MIBS\snmpv2-conf.my
C:\Argent\ArgentManagementConsole\COMMON_MIBS\snmpv2-mib.my

List Of SNMP Object Identifiers (OID) Found In The MIB File

Name	OID	Composed Syntax	Status	Max Access
sysUpTime	.1.3.6.1.2.1.1.3	TIMETICKS	Current	ReadOnly
ifNumber	.1.3.6.1.2.1.2.1	INTEGER	Current	ReadOnly
ifTable	.1.3.6.1.2.1.2.2	SEQUENCE OF IfEntry	Current	NotAccessible
ifEntry	.1.3.6.1.2.1.2.2.1	IfEntry	Current	NotAccessible
ifIndex	.1.3.6.1.2.1.2.2.1.1	InterfaceIndex	Current	ReadOnly
ifDescr	.1.3.6.1.2.1.2.2.1.2	OCTETSTRING	Current	ReadOnly
ifType	.1.3.6.1.2.1.2.2.1.3	IANAifType	Current	ReadOnly
ifMtu	.1.3.6.1.2.1.2.2.1.4	INTEGER	Current	ReadOnly
ifSpeed	.1.3.6.1.2.1.2.2.1.5	GAUGE	Current	ReadOnly
ifPhysAddress	.1.3.6.1.2.1.2.2.1.6	OCTETSTRING	Current	ReadOnly
ifAdminStatus	.1.3.6.1.2.1.2.2.1.7	INTEGER	Current	ReadWrite
ifOperStatus	.1.3.6.1.2.1.2.2.1.8	INTEGER	Current	ReadOnly
ifLastChange	.1.3.6.1.2.1.2.2.1.9	TIMETICKS	Current	ReadOnly
ifInOctets	.1.3.6.1.2.1.2.2.1.10	COUNTER	Current	ReadOnly
ifInUcastPkts	.1.3.6.1.2.1.2.2.1.11	COUNTER	Current	ReadOnly
ifInNUcastPkts	.1.3.6.1.2.1.2.2.1.12	COUNTER	Deprecated	ReadOnly
ifInDiscards	.1.3.6.1.2.1.2.2.1.13	COUNTER	Current	ReadOnly
ifInErrors	.1.3.6.1.2.1.2.2.1.14	COUNTER	Current	ReadOnly
ifInUnknownProtos	.1.3.6.1.2.1.2.2.1.15	COUNTER	Current	ReadOnly

The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

Different SNMP Methods are available such as (Get, Get Next, Walk within Branch, Long Walk, Delta and Delta since last Poll).



Type Of SNMP Data

● SNMP Object IDentifier: .1.3.6.1.4.1.9.2.1.58.0
SNMP Method: Get
Delta Interval: 60 Seconds
SNMP Variable Type: INTEGER
○ Formula Expression:
Formula Name:

Rule Is Broken If

☑ Value Is Greater Than 50
□ Value Is Less Than
□ Fail Rule If The Data Is Unavailable Or Nonexistent

□ As A Specific Variable
□ Retrieve Performance Data For Argent Predictor Only
□ Do Not Save This Metric To Argent Predictor

Once all appropriate OID information has been populated the Rule Is Broken If criteria can be constructed. As shown above a Rule Is Broken If threshold can be set.

Formula Expressions offer added flexibility in monitoring SNMP Metrics. For example, if your environmental monitor returns the temperature of the server room in Celsius, you can convert this metric to Fahrenheit. Or you could measure the uptime of a server or device by converting TIMETICKS to hours. (TIMETICKS are hundredths of a second.) Or you could add together several SNMP metrics to get a total traffic figure.

SNMP Data can be saved to the database for future reporting and trending using the Argent Predictor.

Typical SNMP Polling Metrics

Device Availability (Ping or SNMP Port Check)
Device CPU
Device Memory Pool
Critical Interface State (Up / Down)
Critical Interface Errors

Cisco publishes the MIB for managing various network devices. The Cisco MIB files are located on the Cisco.com website, and include the following information.

- MIB files published in SNMPv1 format
- MIB files published in SNMPv2 format
- Supported SNMP traps on Cisco devices
- OIDs for Cisco current SNMP MIB objects

SNMP Trap Monitor

SNMP Traps are unsolicited SNMP information packets sent from any SNMP-compliant device to an SNMP manager such as Argent. Traps can be sent for many reasons, such as hard drive failures, cooling fans that aren't spinning at the right speed (or not spinning at all), network interfaces suddenly dropping, or even for simple informational reasons like the SNMP service starting.

SNMP Rules are run in Relators at scheduled intervals, so something like a fan problem that comes and goes quickly might not be noticed. On the other hand, if the device sends an SNMP Trap that the fan isn't running right, Argent can notify you immediately.

The Argent's SNMP Trap Monitor definitions are like Relators.
Argent may be configured to listen for specific traps, even for specific information within a trap, and which alerts to fire if that trap arrives. If a trap that arrives matches an SNMP Trap Monitor definition that's in Production Mode, the selected alerts are fired.

The Argent SNMP Monitor comes equipped with a large number of pre-defined SNMP Trap Monitor definitions for a wide variety of devices.

This following lists some SNMP trap types - These traps are generic and available to all network devices.

Authentication Failure - An authenticationFailure(4) trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated. While implementations of the SNMP must be capable of generating this trap, they must also be capable of suppressing the emission of such traps via an implementation-specific mechanism.

Cold Start - A coldStart(0) trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.

Link Down - A linkDown(2) trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.

The Trap-PDU of type linkDown contains as the first element of its variable-bindings, the name and value of the ifIndex instance for the affected interface.

Link Up - A linkUp(3) trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.

The Trap-PDU of type linkUp contains as the first element of its variable-bindings, the name and value of the ifIndex instance for the affected interface.

Some configuration on network devices is required to enable the correct type of SNMP Traps to be sent.

Typical SNMP Traps

Power Supply Failure

Fan Failure

Temperature Warnings

Voltage Warnings

Link Up

Link Down

Authentication

The following shows the Cisco Application Specific Trap enable commands available.

`atm`	`Enable SNMP atm traps`
`bgp`	`Enable BGP state change traps`
`config`	`Enable SNMP config traps`
`dial`	`Enable SNMP dial control traps`
`dlsw`	`Enable SNMP dlsw traps`
`dsp`	`Enable SNMP dsp traps`
`entity`	`Enable SNMP entity traps`
`envmon`	`Enable SNMP environmental monitor traps`
`frame-relay`	`Enable SNMP frame-relay traps`
`hsrp`	`Enable SNMP HSRP traps`
`ipmulticast`	`Enable SNMP ipmulticast traps`
`isdn`	`Enable SNMP isdn traps`
`msdp`	`Enable SNMP MSDP traps`
`rsvp`	`Enable RSVP flow change traps`
`rtr`	`Enable SNMP Response Time Reporter traps`
`snmp`	`Enable SNMP traps`
`syslog`	`Enable SNMP syslog traps`
`tty`	`Enable TCP connection traps`
`voice`	`Enable SNMP voice traps`
`xgcp`	`Enable XGCP protocol traps`

The following table lists the CISCO-STACK-MIB traps that are supported by, and can be used to monitor fault conditions on, Cisco Catalyst local area network (LAN) switches.

moduleUp - The agent entity has detected that the **moduleStatus** object in this MIB has transitioned to the **ok(2)** state for one of its modules.

moduleDown - The agent entity has detected that the *moduleStatus* object in this MIB has transitioned out of the **ok(2)** state for one of its modules.

chassisAlarmOn - The agent entity has detected that the *chassisTempAlarm*, *chassisMinorAlarm*, or *chassisMajorAlarm* object in this MIB has transitioned to the **on(2)** state.

A *chassisMajorAlarm* indicates that one of the following conditions exists:

- Any voltage failure Simultaneous temperature and fan failure
- One hundred percent power supply failure (two out of two, or one out of one)
- Electrically erasable programmable read-only memory (EEPROM) failure
- Nonvolatile RAM (NVRAM) failure
- MCP communication failure
- NMP status unknown

A *chassisMinorAlarm* indicates that one of the following conditions exists:

- Temperature alarm
- Fan failure
- Two power supplies of incompatible type
- Partial power supply failure (one out of two)

chassisAlarmOff - The agent entity has detected that the *chassisTempAlarm*, *chassisMinorAlarm*, or *chassisMajorAlarm* object in this MIB has transitioned to the **off(1)** state.

Environmental monitor (envmon) traps are defined in CISCO-ENVMON-MIB. The envmon trap sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. When envmon is used, a specific environmental trap type can be enabled, or all trap types from the environmental monitor system can be accepted. If no option is specified, all environmental types are enabled.

It can be one or more of the following values:

Voltage: A ciscoEnvMonVoltageNotification is sent if the voltage measured at a given test point is outside the normal range for the test point (such as is at the warning, critical, or shutdown stage).

Shutdown: A ciscoEnvMonShutdownNotification is sent if the environmental monitor detects that a test point is reaching a critical state and is about to initiate a shutdown.

Supply: A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where extant) fails.

Fan: A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where extant) fails.

Temperature: A ciscoEnvMonTemperatureNotification is sent if the temperature measured at a given test point is outside the normal range for the test point (such as is at the warning, critical, or shutdown stage).

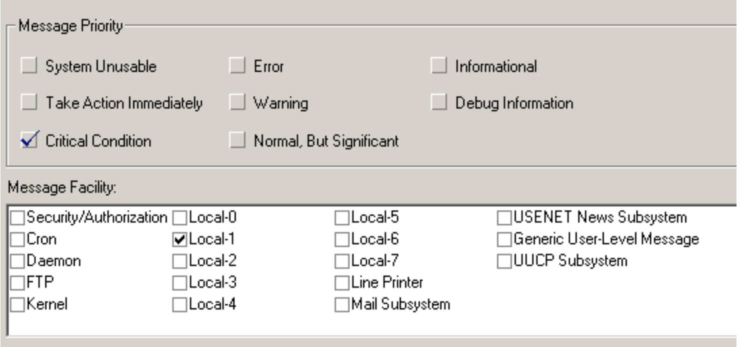
The CSAA/RTR Service Assurance Agent (SAA)/Response Time Reporter (RTR) feature in Cisco IOS can be utilized for measuring the response time between IP devices. A source router configured with CSAA configured is capable of measuring the response time to a destination IP device that can be a router or an IP device. The response time can be measured between the source and the destination or for each hop along the path. SNMP traps can be configured to alert management consoles if the response time exceeds the predefined thresholds.

Argent Data Consolidator

SYSLOG Message rules are used to consolidate SYSLOG events. SYSLOG is an event logging protocol (IETF standard http://www.ietf.org/html.charters/syslog-charter.html) running over the network.

Argent acts as a SYSLOG server by listening for the incoming SYSLOG messages on UDP 514, and consolidates them into the central databases you've defined.

The SYSLOG rule below will consolidate all events according to the selections in the Message Priority section and the Message Facility section.



Message Priority

☐ System Unusable
☐ Take Action Immediately
☑ Critical Condition
☐ Error
☐ Warning
☐ Normal, But Significant
☐ Informational
☐ Debug Information

Message Facility:

☐ Security/Authorization
☐ Cron
☐ Daemon
☐ FTP
☐ Kernel
☐ Local-0
☑ Local-1
☐ Local-2
☐ Local-3
☐ Local-4
☐ Local-5
☐ Local-6
☐ Local-7
☐ Line Printer
☐ Mail Subsystem
☐ USENET News Subsystem
☐ Generic User-Level Message
☐ UUCP Subsystem

Filtering SYSLOG Messages - By default, all records are consolidated into the central ODBC database. Data consolidated and stored in the database may be refined. This can be achieved by using a simple text comparison (Contains or Does NOT Contain match).

Alerting on SYSLOG Messages - Rule Alerts are the main way you are alerted when anomalies are detected based on simple text comparisons.

Any captured SYSLOG files can be reported against.

NOTE

Cisco devices use:

The warning through emergency level displays error messages about software or hardware malfunctions.

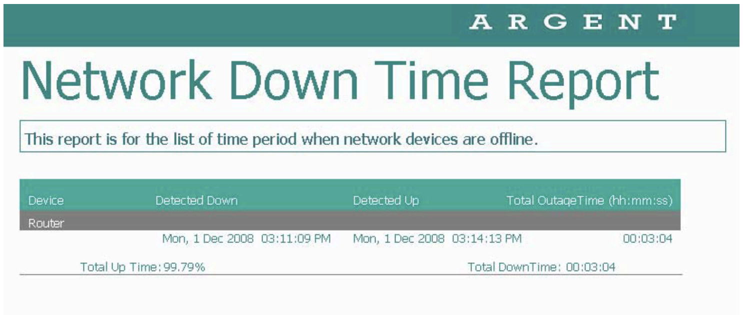
The debugging level displays the output of debug commands.

The notice level displays interface up or down transitions and system restart messages.

The informational level displays reload requests and low-process stack

Reports

The following are examples of types of network reports available.



ARGENT

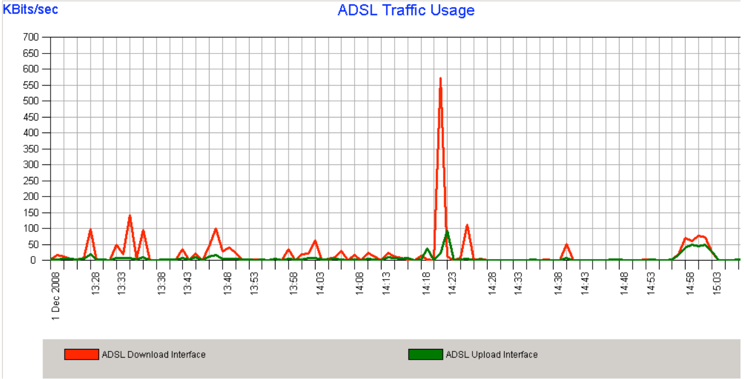
Network Down Time Report

This report is for the list of time period when network devices are offline.

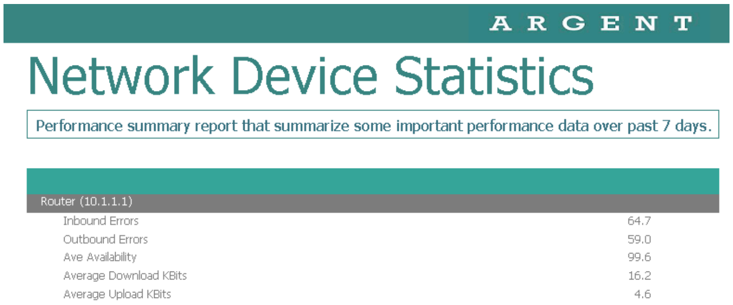
Device	Detected Down	Detected Up	Total OutageTime (hh:mm:ss)
Router			
	Mon, 1 Dec 2008 03:11:09 PM	Mon, 1 Dec 2008 03:14:13 PM	00:03:04

Total Up Time: 99.79% Total DownTime: 00:03:04

The following relies on tracking the delta for Inbound and Outbound Octets on a single interface.



The following report provides a summary of the last 7 day critical metrics



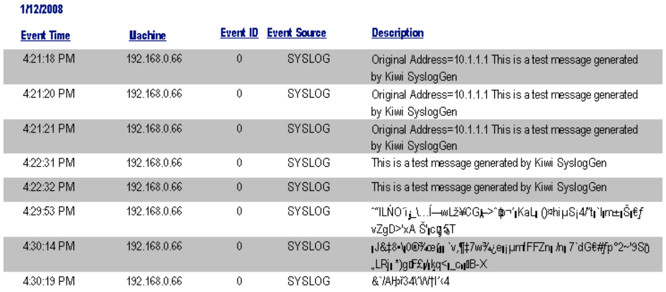
ARGENT

Network Device Statistics

Performance summary report that summarize some important performance data over past 7 days.

Router (10.1.1.1)	
Inbound Errors	64.7
Outbound Errors	59.0
Ave Availability	99.6
Average Download KBits	16.2
Average Upload KBits	4.6

Simple Report showing SYSLOG entries for the last 1 Hour



1/12/2008

Event Time	Machine	Event ID	Event Source	Description
4:21:18 PM	192.168.0.66	0	SYSLOG	Original Address=10.1.1.1 This is a test message generated by Kiwi SyslogGen
4:21:20 PM	192.168.0.66	0	SYSLOG	Original Address=10.1.1.1 This is a test message generated by Kiwi SyslogGen
4:21:21 PM	192.168.0.66	0	SYSLOG	Original Address=10.1.1.1 This is a test message generated by Kiwi SyslogGen
4:22:31 PM	192.168.0.66	0	SYSLOG	This is a test message generated by Kiwi SyslogGen
4:22:32 PM	192.168.0.66	0	SYSLOG	This is a test message generated by Kiwi SyslogGen
4:29:53 PM	192.168.0.66	0	SYSLOG	˜˝ILŃO´i¡_\...Í—wLž¥CG¡–>ˆþ¬'¡KaL¡ ()¤hi µS¡4/'t¡`l¡m±¡Š¡€ƒ vZgD>'xA Š'¡cq¶T
4:30:14 PM	192.168.0.66	0	SYSLOG	¡J&‡8•\0®%œ{¡ `v,¶‡7w¾¿e¡¡µmfFFZn¡ /n¡ 7`dG€#fp°2~'9S0 „LRj¡ *)gfF£¡¡kq<¡_c¡¡0B-X
4:30:19 PM	192.168.0.66	0	SYSLOG	&`/AHþï34\'W†I'‹4

An Overview Of The Cisco Use Of SYSLOG

Configuring Cisco Devices To Use A Syslog Server

Most Cisco devices use the syslog protocol to manage system logs and alerts. But unlike their PC and server counterparts, Cisco devices lack large internal storage space for storing these logs. To overcome this limitation, Cisco devices offer the following two options:

- **Internal buffer** - The device's operating system allocates a small part of memory buffers to log the most recent messages. The buffer size is limited to few kilobytes. This option is enabled by default. However, when the device reboots, these syslog messages are lost.
- **Syslog** - Use a UNIX-style SYSLOG protocol to send messages to an external device for storing. The storage size does not depend on the router's resources and is limited only by the available disk space on the external syslog server. This option is not enabled by default.

TIP

Setting the devices with accurate time is helpful for syslog event correlation. It may be desirable to configure all network devices to use NTP such that system clock on all network devices are correct and synchronized. To enable syslog functionality in a Cisco device you must configure the built-in syslog client in the devices.

Configuring Cisco Routers To Use Syslog

To configure a Cisco IOS-based router for sending syslog messages to an external syslog server, follow the steps using privileged EXEC mode.

Step	Command	Purpose
1	Router# **configure terminal**	Enters global configuration mode.
2	Router(config)# **service timestamps** type **datetime** [msec] [localtime] [show-timezone]	Instructs the system to timestamp syslog messages; the options for the type keyword are debug and log.
3	Router(config)#**logging** host	Specifies the syslog server by IP address or host name; you can specify multiple servers.
4	Router(config)# **logging trap** level	Specifies the kind of messages, by severity level, to be sent to the syslog server. The default is informational and lower. The possible values for level are as follows: Emergency: 0 Alert: 1 Critical: 2 Error: 3 Warning: 4 Notice: 5 Informational: 6 Debug: 7 Use the debug level with caution, because it can generate a large amount of syslog traffic in a busy network.
5	Router(config)# **logging facility** facility-type	Specifies the facility level used by the syslog messages; the default is local7. Possible values are local0, local1, local2, local3, local4, local5, local6, and local7.
6	Router(config)# **End**	Returns to privileged EXEC mode.
7	Router# **show logging**	Displays logging configuration.

Note

When a level is specified in the **logging trap** level command, the router is configured to send messages with lower severity levels as well. For example, the **logging trap** warning command configures the router to send all messages with the severity warning, error, critical, and emergency. Similarly, **the logging trap** *debug* command causes the router to send all messages to the syslog server. Exercise caution while enabling the debug level. Because the debug process is assigned a high CPU priority, using it in a busy network can cause the router to crash.

Example shows how to configure a Cisco router to send syslog messages at facility local3. Also, the router will only send messages with a severity of warning or higher. The syslog server is on a machine with an IP address of 192.168.0.30.

Example - Router Configuration for Syslog

```
Router-Dallas#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router-Dallas(config)#logging 192.168.0.30
Router-Dallas(config)#service timestamps debug datetime localtime show-timezone msec
Router-Dallas(config)#service timestamps log datetime localtime show-timezone msec
Router-Dallas(config)#logging facility local3
Router-Dallas(config)#logging trap warning
Router-Dallas(config)#end
Router-Dallas#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
        Console logging: level debugging, 79 messages logged
        Monitor logging: level debugging, 0 messages logged
        Buffer logging: disabled
        Trap logging: level warnings, 80 message lines logged
                Logging to 192.168.0.30, 57 message lines logged
```

Configuring a Cisco Switch for Syslog

To configure a Cisco CatOS-based switch for sending syslog messages to an external syslog server, use the privileged EXEC mode commands shown.

Configuring a Cisco Switch for Syslog

Step	Command	Purpose
1	Switch>(enable) **set logging time-stamp {enable I disable}**	Configures the system to timestamp messages.
2	Switch>(enable) **set logging server** ip-address	Specifies the IP address of the syslog server; a maximum of three servers can be specified.
3	Switch>(enable) **set logging server severity** server_severity_level	Limits messages that are logged to the syslog servers by severity level.
4	Switch>(enable) **set logging server facility** server_facility_parameter	Specifies the facility level that would be used in the message. The default is local7. Apart from the standard facility names, Cisco Catalyst switches use facility names that are specific to the switch. The following facility levels generate syslog messages with fixed severity levels: **5**: System, Dynamic-Trunking-Protocol, Port- Aggregation Protocol, Management, Multilayer Switching **4**: CDP, UDLD **2**: Other facilities
5	Switch>(enable) **set logging server enable**	Enables the switch to send syslog messages to the syslog servers.
6	Switch>(enable) **Show logging**	Displays the logging configuration.

Example shows how to configure a CatOS-based switch to send syslog messages at facility local4. Also, the switch will only send messages with a severity of warning or higher. The syslog server is on a machine with an IP address of 192.168.0.30.

Example - CatOS-Based Switch Configuration for Syslog

```
Console> (enable) set logging timestamp enable
System logging messages timestamp will be enabled.
Console> (enable) set logging server 192.168.0.30
192.168.0.30 added to System logging server table.
Console> (enable) set logging server facility local4
System logging server facility set to <local4>
Console> (enable) set logging server severity 4
System logging server severity set to <4>
Console> (enable) set logging server enable
System logging messages will be sent to the configured syslog servers.
Console> (enable) show logging
Logging buffered size: 500
timestamp option: enabled
Logging history size: 1
Logging console: enabled
Logging server: enabled
{192.168.0.30}
server facility: LOCAL4
server severity: warnings(4
Current Logging Session: enabled
```

Facility	Default Severity	Current Session Severity
cdp	3	4
drip	2	4
dtp	5	4
dvlan	2	4
earl	2	4
fddi	2	4
filesys	2	4
gvrp	2	4
ip	2	4
kernel	2	4
mgmt	5	4
mls	5	4
pagp	5	4
protfilt	2	4
pruning	2	4
radius	2	4
security	2	4
snmp	2	4
spantree	2	4
sys	5	4
tac	2	4
tcp	2	4
telnet	2	4
tftp	2	4
udld	4	4
vmps	2	4
vtp	2	4

There are eight different levels of logging:

0(emergencies)

1(alerts)

2(critical)

3(errors)

4(warnings)

5(notifications)

6(information)

7(debugging)

Configuring a Cisco PIX Firewall for Syslog

Proactive monitoring of firewall logs is an integral part of an admin's duties. The firewall syslogs are useful for forensics, network troubleshooting, security evaluation, worm and virus attack mitigation, etc. The configuration steps for enabling syslog messaging on a PIX are conceptually similar to those for IOS- or CatOS-based devices. To configure a Cisco PIX Firewall with PIX OS 4.4 and above, perform the steps shown in privileged EXEC mode.

PIX Configuration for Syslog

Step	Command	Purpose
1	Pixfirewall# config terminal	Enters global configuration mode.
2	Pixfirewall(config)# **logging timestamp**	Specifies that each syslog message should have a timestamp value.
3	Pixfirewall(config)#**logging host** *[interface connected to syslog server] ip_address [protocol / port]*	Specifies a syslog server that is to receive the messages sent from the Cisco PIX Firewall. You can use multiple **logging host** commands to specify additional servers that would all receive the syslog messages. The protocol is UDP or TCP. However, a server can only be specified to receive either UDP or TCP, not both. A Cisco PIX Firewall only sends TCP syslog messages to the Cisco PIX Firewall syslog server.
4	Pixfirewall(config)#**logging facility** *facility*	Specifies the syslog facility number. Instead of specifying the name, the PIX uses a 2-digit number, as follows: local0 - **16** local1 - **17** local2 - **18** local3 - **19** local4 - **20** local5 - **21** local6 - **22** local7 - **23** The default is **20.**

Step	Command	Purpose
5	pixfirewall(config)**#logging trap** *level*	Specifies the syslog message level as a number or string. The level that you specify means that you want that level and those values less than that level. For example, if level is 3, syslog displays **0**, **1**, **2,** and **3** messages. Possible number and string level values are as follows: **0**: Emergency; System-unusable messages **1**: Alert; Take immediate action 2: Critical; critical condition **3**: Error; error message **4**: Warning; warning message **5**: Notice; normal but significant condition **6**: Informational: information message **7**: Debug; debug messages and log FTP commands and WWW URLs
6	pixfirewall(config)#**logging on**	Starts sending syslog messages to all output locations.
7	pixfirewall(config)#**no logging message** *<message id>*	Specifies a message to be suppressed.
8	pixfirewall(config)#**exit**	Exits global configuration mode.

Example shows how to configure Cisco PIX Firewall to send syslog messages at facility local5 and severity debug and below to the syslog server. The Netadmin does not want the PIX to log message 111005. The syslog server has an IP address of 192.168.0.30.

Configuring a Cisco PIX Firewall for Syslog

```
Firewall-Dallas#
Firewall-Dallas# config terminal
Firewall-Dallas(config)# loggin time
Firewall-Dallas(config)# logging host 192.168.0.30
Firewall-Dallas(config)# logging facility 21
Firewall-Dallas(config)# logging trap 7
Firewall-Dallas(config)# logging on
Firewall-Dallas(config)# no logging message 111005
rewall-Dallas(config)# exit
Firewall-Dallas# show logging
Syslog logging: enabled
    Facility: 21
    Timestamp logging: enabled
    Standby logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level debugging, 6 messages logged
        Logging to inside 192.168.0.30
    History logging: disabled
    Device ID: disabled
```

If the PIX stop's because of a disk-full condition, you must first free some disk space. Then disable syslog messaging on the PIX by using the **no logging host** *host* command, followed by re-enabling syslog messaging using the **logging host** *host* command.

Caution

The change in facility level for a particular message in the previous example is for illustration purposes only. Changing the facility level from its default value is an advanced admin function and is strongly discouraged.

A Cisco PIX Firewall facing the Internet is subjected to a large amount of unsolicited traffic in the form of ping scans, port scans, and probes. This can cause the log file to become large within days. It will be filled with data, making it difficult to search for useful information. You should fine-tune your firewall to suppress certain common messages using the no logging message message-id-number command. Additionally, use the IOS firewall features on the edge router to filter unwanted traffic before it hits the Cisco PIX Firewall.

Note: ArgSoft Intellectual Property Holdings Limited has created this White Paper for informational purposes only. ArgSoft Intellectual Property Holdings Limited makes no warranties, express or implied, in this document. The information contained in this document is subject to change without notice. ArgSoft Intellectual Property Holdings Limited shall not be liable for any technical or editorial errors, or omissions contained in this document, nor for incidental, indirect or consequential damages resulting from the furnishing, performance, or use of the material contained in this document, or the document itself. All views expressed are opinions of ArgSoft Intellectual Property Holdings Limited. All trademarks are the property of their respective owners.