

Building Scalable Syslog Management Solutions

White Paper

Last Updated: April, 2011



Clayton Dukes

Network Management Consulting Engineer

Advanced Services - Central Engineering

cdukes@cisco.com

7025-10 Kitt Creek Road RTP, NC 27709-4987

Contents

Benefits of Syslog management	4
Introduction to Syslog Management	5
Syslog Basics.....	6
The Syslog Message Format and Contents	6
Priority.....	7
Facility	7
Severity	8
Header	8
Timestamp	8
Hostname or IP address of the device	9
MSG.....	9
Cisco IOS Commands	9
Configuration Command Detail	10
Time	10
Logging	10
Network Time Protocol	11
Recommendations:	12
Syslog vs. SNMP	13
Management Techniques.....	13
Actionable vs. Non-actionable Syslogs	14
Determining Actionable Syslogs	14
Syslog Architecture	15
Event Analysis	16
Event Reporting	17
Event Remediation.....	18
Event Viewer	19
Event Logging Architecture	20
syslog-ng Basics	20
syslog-ng Server Design Considerations	22
Single-Server Deployment	22
Multi-Server Deployment.....	23
Logging Architecture Guidelines	23
Collection Stations	24
Syslog Event Manager.....	24
Log Rotation and Retention	24
Server Sizing	24
Database Types	25
MyISAM	25
ARCHIVE	25
Syslog Applications.....	26
Open Source and Commercial Syslog Products	26
Open Source.....	26
LogZilla (Formerly Php-syslog-ng)	26
Commercial.....	28
CiscoWorks LMS.....	28
loglogic	29
Splunk	30
Appendix	31
ITIL V3 Event Management	31
Cisco Embedded Syslog Manager.....	32

Actionable Syslogs.....	32
Cisco IOS Syslogs	32
Switch Syslogs (CAT-OS).....	34
Storage Syslogs (MDS 9000).....	38
Other Syslogs	39
Review History	39
References	40

Executive Summary

This document defines the design and methodology for a scalable Syslog solution. It provides leading practices for deploying a robust and scalable set of tools and applications to support effective collection, storage, and analysis of Syslog messages. Collecting and storing Syslog messages helps to provide reporting capabilities for identifying trends and failures, as well as data mining capabilities that focus on problem and incident management tasks.

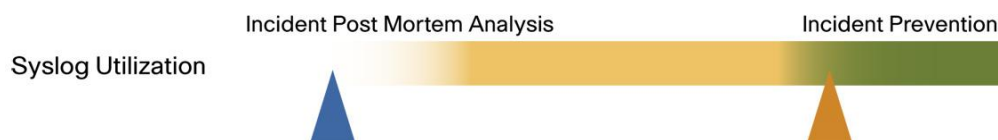
This paper primarily focuses on Cisco IOS Software implementations, but is applicable to other Syslog message types and general event management. It is meant to help get you started on the road to managing Syslog messages in your environment.

The document will address six main topics:

1. Introduction to Syslog management
2. Methodology
3. Architectures
4. Server sizing
5. Database types
6. Tools

The objective is to lay the foundation so that the organization's capability moves from a reactive state (utilizing Syslog messages after the fact) to a more proactive state by providing predictive analysis on systems. In Figure 1, the blue pointer indicates where most companies tend to reside (reactive); the orange pointer indicates where they should be (proactive).

Figure 1. Syslog Utilization



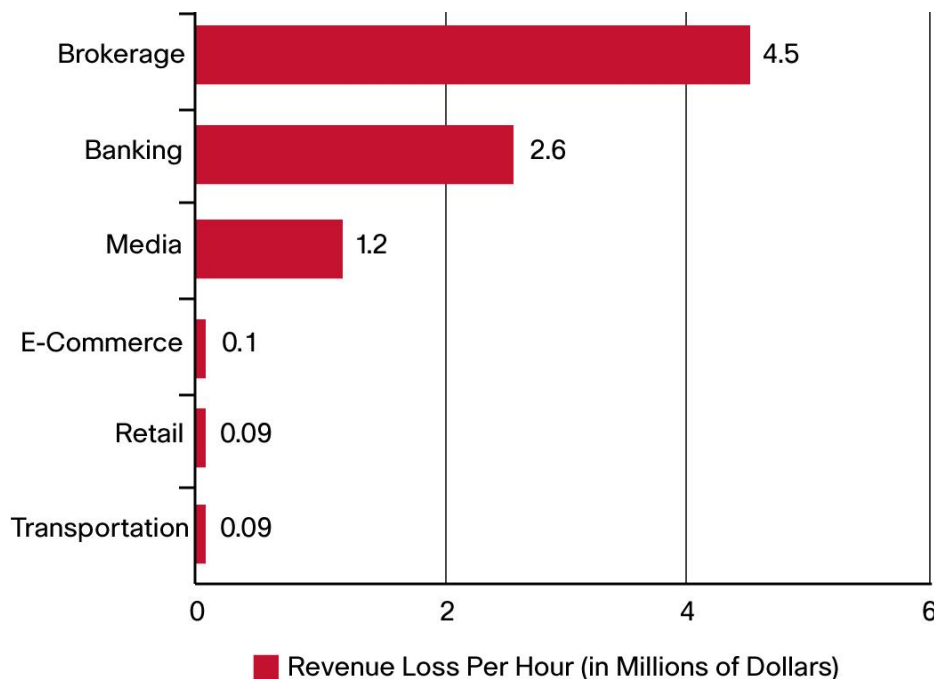
Benefits of Syslog management

Proactive Syslog management benefits both operations personnel and the company as a whole from a cost savings perspective. Successful event management architectures can:

- Reduce downtime, which reduces operational costs
- Improve incident management through real-time detection and self-remediation
- Reduce the volume of trouble tickets
- Reduce the severity of business interruptions
- Help operations staff avoid “fire fighting” mode (reactive troubleshooting)

The following table provides an industry average cost of downtime according to a Yankee Group (<http://www.yankeegroup.com>) report published in 2004:

Figure 2. Industry Cost of Downtime



The Yankee Group report made apparent the benefits of proactive problem management. This paper explores how organizations can use Syslog to provide effective event management.

Introduction to Syslog Management

The purpose of this section is to familiarize you with Syslog and describe the types of management techniques that are available.

Syslog is a valuable monitoring mechanism that proactively captures chronic issues affecting a network. It can identify many more exceptions and network degradation warnings than other forms of monitoring metrics, such as SNMP traps.

There have been several instances where Syslog messages have identified a critical network issue for which there existed no SNMP traps. In one case, an organization was able to identify a critical issue with its switch fabric module by the recording of the %SYS-3-FAB_SYNCERR Syslog message. (This message indicates that a fabric channel error has been detected.) This helped the customer avoid any service downtime since they were able to rectify the problem before their end customers started feeling the symptoms. Without such instrumentation, the only way the organization would have known about the problem would have been when users began complaining.

Because of its verbose nature, Syslog must be implemented precisely. Adequate thresholds and filters must be defined to generate actionable alerts based on the Syslog messages. The problem management team must be able to identify critical Syslog messages easily, and, with equal ease, create incident or problem tickets in their internal ticketing system (Remedy, Peregrine, etc.). The Syslog messages must also be prioritized according to the nature and function of the site that is generating them; for example, messages from critical core sites that contain one or more devices must take precedence over those in noncritical deployments.

These requirements will be very customer-specific, due to the uniqueness of each organization's network deployment.

This section will cover:

- Syslog Basics
- The Syslog Message Format
- Relevant Cisco IOS commands
- Syslog vs. SNMP
- Management Techniques/Methodologies
- Syslog Analysis
- Syslog Architectures
- Analysis Tools

Note: If you are an advanced user or are already familiar with these topics, this section may be skipped.

Syslog Basics

Syslog is a client/server protocol. Originally developed in the 1980s by Eric Allman as part of the Sendmail project, Syslog is defined within the Syslog working group of the IETF (RFC 3164) and is supported by a wide variety of devices and receivers across multiple platforms. Although there are exceptions, Syslog can be used to integrate log data from many disparate systems into a central repository for real-time and historical analysis.

The Syslog sender sends a small (less than 1KB) text message to the Syslog receiver. The Syslog receiver is commonly called “syslogd,” “Syslog daemon,” or “Syslog server.” Syslog messages can be sent via UDP (port 514) and/or TCP (typically, port 5000). While there are some exceptions, such as SSL wrappers, this data is typically sent in clear text over the network.

Being a connectionless protocol, UDP does not provide acknowledgments to the sender or receiver. Additionally, at the application layer, Syslog servers do not send acknowledgments back to the sender for receipt of Syslog messages. Consequently, the sending device generates Syslog messages without knowing whether the Syslog server has received the messages. In fact, the sending devices send messages even if the Syslog server does not exist; these messages get “lost” in the network.

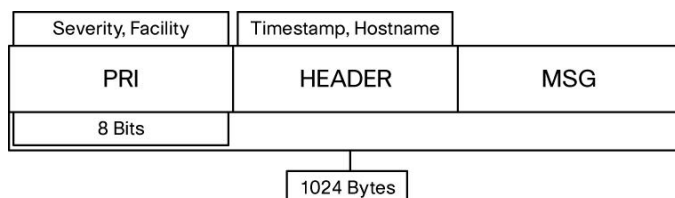
The Syslog Message Format and Contents

The full format of a Syslog message seen on the wire has three distinct parts, as shown in Figure 3.

- PRI (priority)
- HEADER
- MSG (message text)

The total length of the packet cannot exceed 1024 bytes. There is no minimum length.

Figure 3. Syslog Packet



Priority

The Priority is an 8-bit number that is enclosed in angle brackets. This represents both the Facility and Severity of the message. The three least significant bits represent the Severity of the message (with three bits you can represent eight different Severities), and the other five bits represent the Facility of the message.

You can use the Facility and Severity values to apply certain filters on the events in the Syslog Daemon.

Note: Syslog Daemons (running on the Syslog server) do not generate these Priority and Facility values. The values are created by the Syslog clients (applications or hardware) on which the event is generated.

The Priority value is calculated by first multiplying the Facility number by 8 and then adding the numerical value of the Severity. For example, a kernel message (Facility=0) with a Severity of Emergency (Severity=0) would have a Priority value of 0. Also, a “local use 4” message (Facility=20) with a Severity of Notice (Severity=5) would have a Priority value of 165. In the PRI part of a Syslog message, these values would be placed between the angle brackets as <0> and <165>, respectively.

Facility

Syslog messages are broadly categorized on the basis of the sources that generate them. These sources can be the operating system, the process, or an application.

These categories, called Facilities, are represented by integers, as shown in Table 1. The local use facilities are not reserved; the processes and applications that do not have pre-assigned Facility values can choose any of the eight local use facilities. As such, Cisco devices use one of the local use facilities for sending Syslog messages.

By default, Cisco IOS® Software-based devices, Cisco Catalyst® switches, and Cisco VPN 3000 Concentrators use Facility **local7** while Cisco PIX® firewalls use **local4** to send Syslog messages. Most Cisco devices provide options to change the facility level from their default value. Table 1 lists all Facility values.

Table 1. Facility Values

Integer	Facility
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons
4	Security/authorization messages
5	Messages generated internally by Syslogd
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon
10	Security/authorization messages
11	FTP daemon
12	NTP subsystem
13	Log audit
14	Log alert
15	Clock daemon
16	Local use 0 (local0)

Integer	Facility
17	Local use 1 (local1)
18	Local use 2 (local2)
19	Local use 3 (local3)
20	Local use 4 (local4)
21	Local use 5 (local5)
22	Local use 6 (local6)
23	Local use 7 (local7)

Severity

The log source or facility (a router or mail server, for example) that generates the Syslog message also specifies the severity of the message using single-digit integers 0-7 (shown in Table 2).

Note: Network devices should log levels 0-6 under normal operation. Level 7 should be used for console troubleshooting only.

Table 2. Severity Values

Integer	Facility
0	Emergency: System is unusable
1	Alert: Action must be taken immediately
2	Critical: Critical conditions
3	Error: Error conditions
4	Warning: Warning conditions
5	Notice: Normal but significant condition
6	Informational: Informational messages
7	Debug: Debug-level messages

Header

The header contains the following:

Timestamp

The timestamp field is used to indicate the local time, in MMM DD HH:MM:SS format, of the sending device when the message is generated.

The * (asterisk) and. (period) characters preceding a syslog message are indicators of a problem with NTP.

* Means that time is not authoritative: the software clock is not in sync or has never been set.

Means that time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers

For the timestamp information to be accurate, it is good administrative practice to configure all the devices to use the Network Time Protocol (NTP). In recent years, however, the timestamp and hostname in the header field have become less relevant in the Syslog packet itself as the Syslog server will stamp each received message with the server timestamp of when the message is received and the IP address (or hostname) of the sender, as taken from the source IP address of the packet.

Hostname or IP address of the device

The hostname field consists of the host name (as configured on the host itself) or the IP address. In devices such as routers or firewalls, which have multiple interfaces, Syslog uses the IP address of the interface from which the message is transmitted (unless otherwise configured using the “logging source” IOS command, such as **logging source-interface loopback0**).

Many people can get confused by “host name” and “hostname.” The latter is typically associated with a DNS lookup. If the device contains its “host name” in the actual message, it may be (and often is) different than the actual DNS hostname of the device. A properly configured DNS system should include reverse lookups in order to help facilitate proper sourcing for incoming messages.

MSG

The Message is the text of the Syslog message, along with some additional information about the process that generated the message. The Syslog messages generated by Cisco IOS devices begin with a percent sign (%) and use the following format:

%FACILITY-SEVERITY-MNEMONIC: Message-text

The mnemonic is a device-specific code that uniquely identifies the message such as “up,” “down,” “changed,” “config,” etc. For example:

```
*Sep 16 08:50:47.359 EDT: %SYS-5-CONFIG_I: Configured from console by vty0
10.18.86.123
```

Note: The “Facility” in Cisco Mnemonics are not the same as the RFC definition of “facility” (such as local7). Cisco Facilities are a free-form method of identifying the source message type such as SYS, IP, LDP, L2, MEM, FILESYS, DOT11, LINEPROTO, etc. (the list is very large)

Cisco IOS Commands

Configuring a Cisco IOS device for Syslog involves more than just defining the actual Syslog destination receiver. Each device must be configured to include the proper timestamp information, time zone, a logging source, the console buffer size, the logging level, and NTP (Table 3).

Table 3. Sample IOS Configuration

```
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
clock timezone GMT 0
!
logging source-interface loopback0
logging buffered 65536
logging host <ip address 1>
logging host <ip address 2>
logging host <ip address 3>
logging trap informational
!
ntp server <ip address 4>
ntp server <ip address 5>
ntp peer <ip address 6>
ntp peer <ip address 7>
ntp update-calendar
```

Configuration Command Detail

Time

```
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
clock timezone GMT 0
```

Time stamps can be added to either debugging or logging messages independently. The uptime form of the command adds time stamps in the format HHHH:MM:SS, indicating the time since the system was rebooted. The datetime form of the command adds time stamps in the format MMM DD HH:MM:SS, indicating the date and time according to the system clock.

Adding a timestamp to messages allows you to tell what time the message was generated instead of getting a message indicating how long the device has been powered up.

Note: Correlating log files of devices may be difficult if the time stamps on the log messages have to be adjusted for the summer time clock settings. Therefore, consideration should be given to using the "clock summer-time" option.

Logging

The examples below are for IOS:

```
logging source-interface loopback0
logging buffered 65536
logging host <ip address 1>
logging host <ip address 2>
logging host <ip address 3>
logging trap informational
```

The “logging source” command instructs the system to generate logging to the remote system from this source interface. This ensures that all messages appear to come from the same IP across reboots and makes it easier to track in the destination syslog receiver. This also allows you to create a DNS entry for that source interface. If the source command is not used and the system reloads, the first IP that comes up will be used.

The “logging buffered” command is used to reserve a memory buffer for logging to the console of the device. Since today’s devices have plenty of memory, feel free to set this number higher than the old 16k buffer, but be aware that there is a point of diminishing returns. The typical recommendation is to have 256K buffers on core devices and 64K elsewhere.

Note: Console refers to the output of the screen when attached to the device either by serial or via telnet/ssh using the “Terminal Monitor” command.

The “logging host” command sets the remote syslog daemon to send messages to.

Note: As a best practice, network devices should be configured with a maximum of four Syslog servers. The Syslog server can then be configured to forward or “fork” messages to other network management systems if more than four IP addresses are required. This reduces the changes needed on network devices.

One technique is to deploy a tool like syslog-ng, an open source implementation of the Syslog protocol for UNIX (Solaris) and UNIX-like systems (Linux). It extends the original syslog daemon model with content-based filtering, rich filtering capabilities, and flexible configuration options, and adds important features to Syslog, like using TCP for its transport protocol between syslog-ng servers. (Many hardware vendors do not support TCP transport at this time.¹)

Syslog-ng is used to secure communication between syslog-ng servers. It is also capable of forwarding or “forking” messages to a database server. While not officially endorsed by Cisco, it is used by many of our customers and has become a standard in Syslog message reception, filtering, and forwarding.

The “logging trap informational” command tells the device to log all messages of severity 0-6 to the remote syslog daemon. The “trap” portion of this command should not be confused with SNMP traps - it is simply the command used to indicate which Syslog logging level to send.

Devices should be set to log all messages 0-6 for normal operation and possibly 0-7 for debugging (although, if you are debugging, you’re probably doing so on the console of the device and should not need to send level 7 to the collectors).

Network Time Protocol

```
ntp server <ip address 4>
ntp server <ip address 5>
ntp peer <ip address 6>
ntp peer <ip address 7>
ntp update-calendar
```

It is recommended that you enable NTP throughout the network and system architecture to ensure proper timestamps are reported. This ensures that all incoming Syslog messages are synchronized so that you can effectively determine the correct time and correlation of incoming events.

¹ TCP Support is available with some syslog daemons, such as syslog-ng as well as Cisco IOS Software Releases after 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and Cisco IOS XE Release 2.1 12.2(33)SX1.

One issue that the management platform must address is the differences in the manner in which timestamps are attached to messages by different network elements. The management system will need to recognize which method the elements are using and adjust appropriately. To alleviate some of the timing issues, NTP (RFC 1305) should be used in the network.

Note: The timestamp and hostname in the header field are becoming increasingly less relevant in the syslog packet itself as the syslog server should be capable of stamping each received message with the server's timestamp of when the message is received and the IP address (or hostname) of the sender, as taken from the source IP address of the packet.

The "ntp update-calendar" command is used to synchronize the time of the internal clock with the clock of the NTP reference server.

Recommendations:

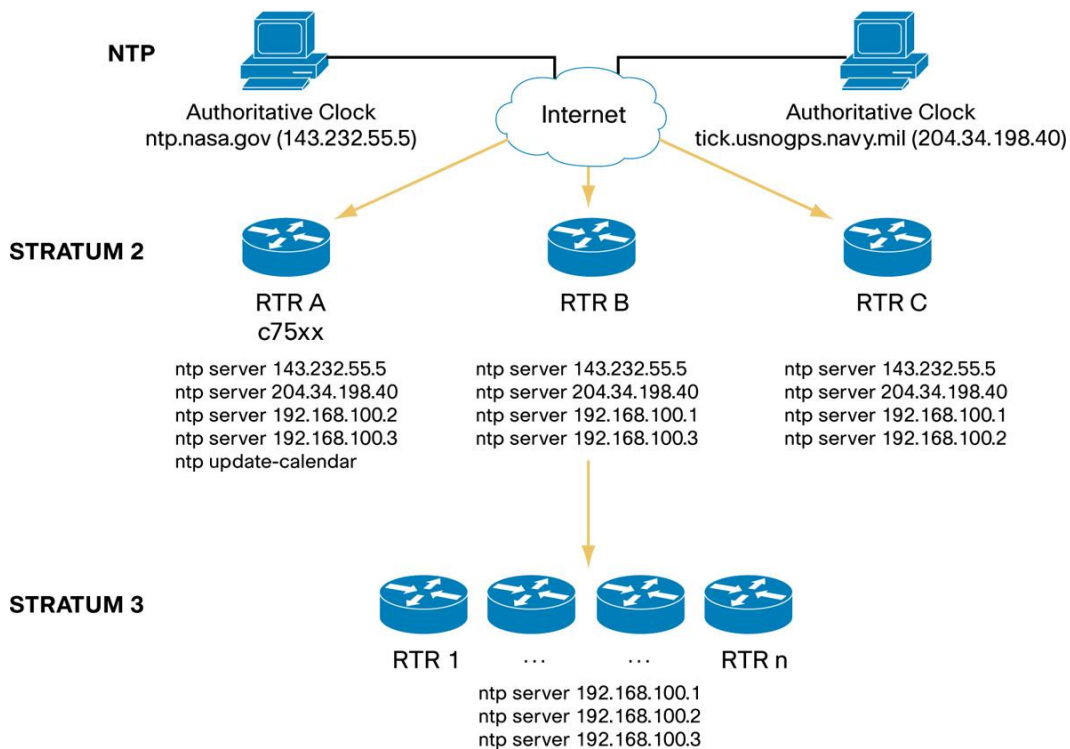
Use a minimum of two reference clocks (GPS and Internet-derived are popular) - three references are recommended.

"Peer" time between the reference clocks.

Subnets of multiple NMSs and/or routers and switches may consider using NTP in multicast mode.

Figure 4 shows a hierarchical NTP model.

Figure 4. NTP Hierarchical Model



Syslog vs. SNMP

One of the most common questions about Syslog is: “Can’t I just turn on SNMP traps and forget about Syslog?”

The simple answer is: no. In general, there are significantly more Syslog messages available within IOS as compared to SNMP Trap messages. For example, a Cisco Catalyst 6500 switch running Cisco IOS Software Release 12.2(18)SXF contains about 90 SNMP trap notification messages, but has more than **6000** Syslog event messages.

If there is a choice to be made between using SNMP traps or Syslog, the logical answer is Syslog. However, it’s also important to recognize that messaging support varies by hardware platform, technology, and specific software release; consequently, a truly robust and full-featured event management solution would take advantage of all event indicators. Where there are redundancies between SNMP traps and Syslog messages, de-duplication to eliminate excessive notices is necessarily part of the Syslog analysis process. Additionally, you may opt to send Syslog messages in a trap to your SNMP manager by using the **“snmp-server enable traps syslog”** command.

Management Techniques

Traditionally, Syslog daemons stored all incoming messages to one or more files that were later parsed. This led to a very reactive use of Syslog for “after-the-fact” troubleshooting or forensic analysis after an event is resolved (such as during root cause analysis), which did not scale beyond a handful of devices.

Traditional Syslog management consisted of file-based storage mechanisms and utilities such as “tail” or “grep” to parse through the information stored in the files. While it’s still useful to keep such logs for later forensics, this type of logging does not allow for more robust reporting.

Since it is impossible to scan through streaming log data when the input rate exceeds that which humans are capable of effectively reading, new mechanisms have been developed to enhance the way problem analysis is performed on the large amount of log data, such as database storage and reporting.

Today’s relational database storage mechanisms are designed to handle very large amounts of data. This allows operators to perform metric (statistical) analysis on the data and generate reports, and provides a much faster response time for querying the database about individual devices or events.

With Syslog data being stored in a database, we can define metrics and design reporting tools to gather and report on the collected data as well as integrate with other network management systems. Examples of these include:

- Collecting metrics to show fault indicators and performance degradation such as fan failures, redundant power supply failures, or duplex mismatch (Figure 5).

Figure 5. Sample Performance Metric Indicator

```
1. %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on [chars] ([chars]), with [chars] [chars] ([chars]).
```

CDP has discovered a mismatch of duplex configuration.

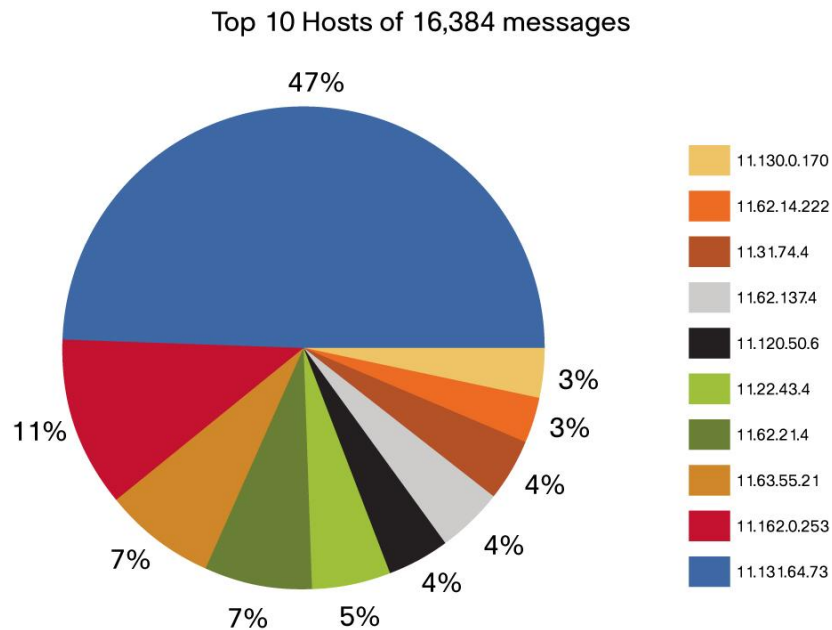
Recommended Action: Configure the interfaces so they are both running at the same duplex (full- or half-duplex).

Related documents-

- [Spanning Tree Protocol Problems and Related Design Considerations](#)
- [Troubleshooting Switch Port and Interface Problems](#)
- [Understanding the Ethernet LAN/WAN Interface Card Network Modules](#)

- Graphing Top-N and Bottom-N talkers (most and least frequently recurring events) daily (Figure 6).

Figure 6. Sample Top 10



- Integrating Syslog data with performance management systems; for example, collecting the number of average messages per second that a single device generates, and alerting on variations outside the derived baseline.
- Integrating with inventory systems. If a device is talking to you, there's a good chance it exists on your network. New devices being added to the network will have to wait until the next polling cycle by discovery systems, but if syslog is turned on in that system, your syslog manager will pick it up almost immediately. Additionally, some applications, such as CiscoWorks LMS, allow for frequent reports on unknown Syslog devices.

Actionable vs. Non-actionable Syslogs

Syslog messages should be clear and actionable for NOC and staff notification. Many NOC managers try to limit the amount of Syslogs because they can be non-actionable or because they don't have staff to effectively deal with all of them. End-user ports coming up or down are examples of non-actionable events.

Determining Actionable Syslogs

To support proactive network management and problem management, after any kind of major incident, Syslogs should be reviewed and analyzed for the devices involved to determine if there was a specific Syslog or a pattern of Syslogs that could be monitored for in the future. This way, when this issue next occurs, it will be proactively detected and impact will be minimized.

A partial list of "actionable" system messages is included in the appendix section of this document.

Syslog Architecture

Harnessing the full potential of Syslog requires a streamlined process and an underlying tool structure that provides for the collection, analysis, and “call to action” on all received Syslog messages from the network. Many of the recommendations in this event management architecture can be applied to general event management, not just Syslogs.

In June 2007, ITIL V3 was introduced, adding a new “event management” process that conforms to the architecture for Syslog messages defined in this document.

ITIL V3 describes an event as “any detectable or discernible occurrence that has significance for the management of the IT infrastructure or the delivery of IT service, and evaluation of the impact that a deviation might cause to the services²”.

This can be summarized as:

- Real-time monitoring of the infrastructure, listening for things that are “bad”.
- Event correlation to filter, de-duplicate, and combine individual events to detect more serious issues.

Cisco recommends implementing a Syslog architecture that addresses the following five key elements:

- Event analysis
- Event reporting
- Event remediation
- Event viewer
- Event logging architecture

The following sections provide an overview of each of these elements.

The solution itself is best defined within the **Event Analysis** section, which outlines the steps necessary to ensure review and classification of messages.

The **Event Reporting** section suggests approaches to managing the initial large volume of messages that will require classification. Once completed, the ongoing maintenance becomes very manageable.

The **Event Remediation** section will address the response to critical messages.

The **Event Viewer** section outlines the tool structure necessary to collect, store, and classify incoming messages. There are tools readily available today that can be customized to your environment and augmented to provide ticket generation.

Finally, the **Event Logging Architecture** addresses how to deploy Syslog in small, medium-sized, and large deployment scenarios.

Cisco believes this architectural approach will provide organizations with a platform that effectively categorizes Syslog messages, establishes the baseline for normal operation, and ensures that messages of consequence are recognized and acted upon. Once in place, this system will properly organize messages and ensure those of importance are given the attention required.

² IT Service Management Based on ITIL V3 – A Pocket Guide.

Event Analysis

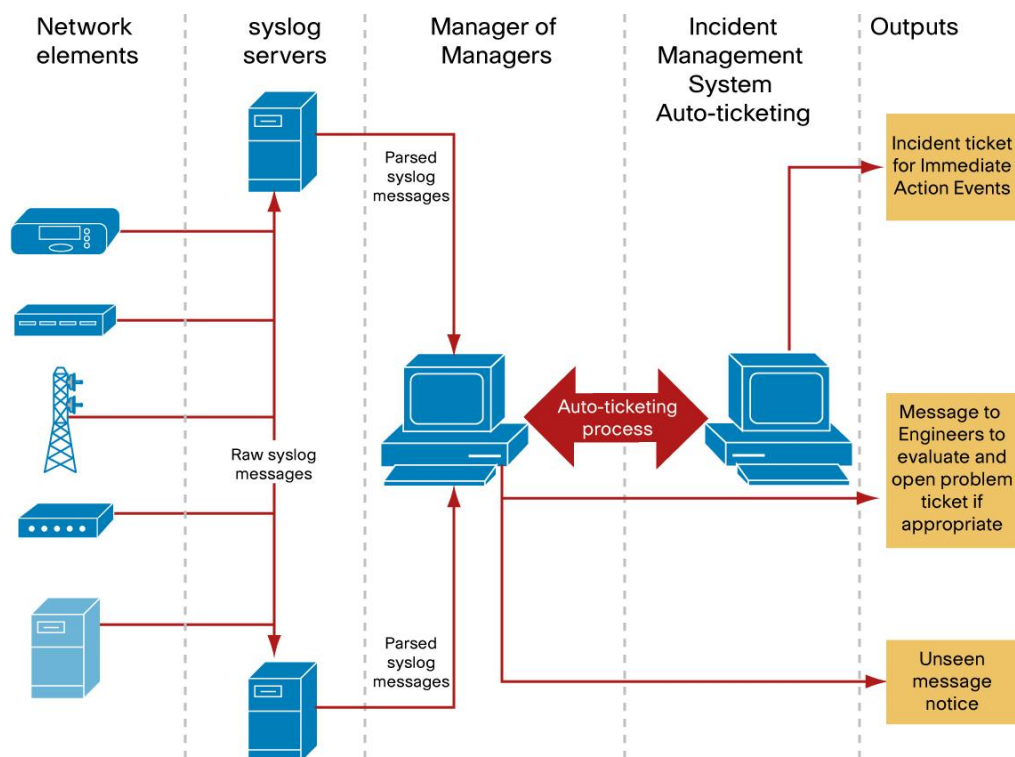
There are approximately 35,000 possible Syslog messages supported by various versions of Cisco IOS Software. Naturally, it is imperative that only the critical, relevant messages are identified to make any analysis coherent.

When an incoming event is received, two immediate questions need to be asked:

- Have we seen the event before?
- Is this a non-actionable event?

A database should be set up to store all incoming events along with a field indicating whether or not this is a non-actionable event. If the event has been seen before and it is marked as non-actionable, then no further action needs to be taken. If the event has **never** been seen before, it needs to be forwarded to operations for further review and, at that time, either acted upon or marked in the database as non-actionable. Likewise, if the event is an actionable event, an automated process needs to be executed to open a trouble/incident ticket for it. Figure 7 gives an overview of Syslog Event Analysis

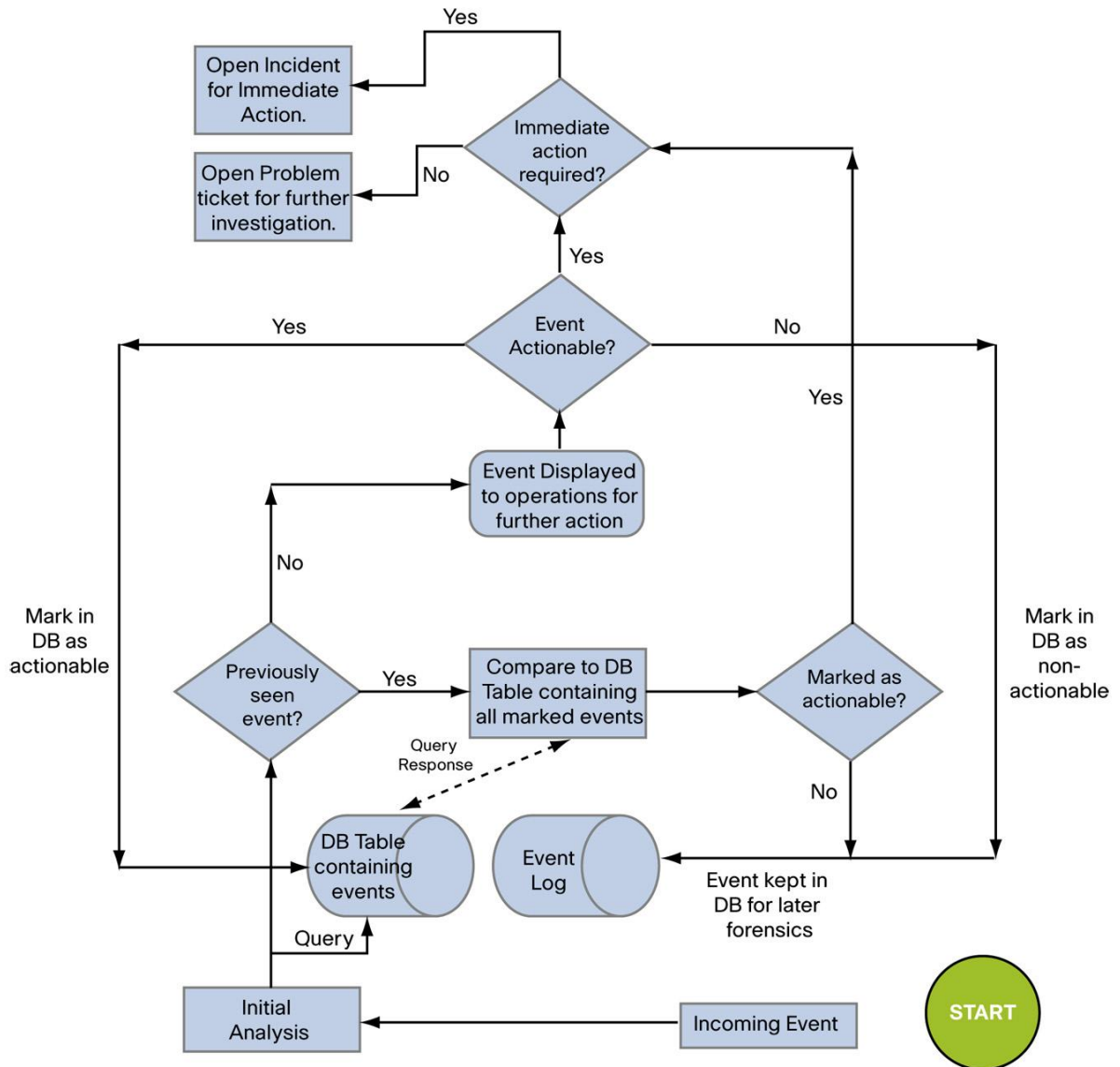
Figure 7. Syslog Event Analysis



Consideration can also be given to prioritizing incoming events based on the sending source. A “metric” field can easily be inserted into the database to indicate that this host/device has a higher priority than another host/device of the same type but in a different location (e.g., a trading floor device versus a device of the same type in a back room).

An outline of this proposed process is provided in the flowchart in Figure 8. The process follows a simple workflow that enables the organization to begin filtering event logs as they enter the architecture. As the implementation matures, fewer non-critical events will be seen by the operations personnel, thus surfacing only the necessary events that need attention.

Figure 8. Logic Flow for Syslog Analysis



This process provides the opportunity for forensic analysis to support problem management for security-related and non-security-related issues. When further investigation is required, the messages around the time of the incident (several hours before and after) can be queried.

An analysis of these messages should show some symptomatic causes of the problem. These symptomatic messages can then be added to the list of known Syslogs and relevant actions can be defined for future proactive identification of this problem.

Event Reporting

Due to the size of today's network environments, it is nearly impossible to view every event coming into your management systems; this is especially true during the initial deployment phase of the event analysis, since all incoming events will be displayed by default until they are marked as non-critical events.

One of the simplest methods used to understand the nature of event logs is to produce daily Syslog reports that can immediately be used by the problem management team to eliminate potential problems in the network.

This can include a mix of standard reports such as:

- Number of Syslog occurrences broken down by severity
- Top-N Syslog messages in the network by severity
- Top-N devices generating Syslogs by severity

Note: With regards to long-term stability of the network, simply following up on the results of these two reports (opening incident/problem tickets and repairing the reported problems) will likely yield more dividends than any other action you can take.

As a complement to these reports, several other reports that look for trends and problem events can be generated. These trends or events can be identified via intelligent analysis methods using event correlation, device health metric systems, and baseline management techniques.

Based on this analysis, engineers can collaborate by creating a set of dynamic Syslog rules that are then applied to all Syslog messages generated in the network. This process combination provides a more insightful view of network health and network optimization opportunities from a broad base of network expert knowledge. These custom reports include, but are not limited to:

- Number of Syslog occurrences broken down by “problem” messages
- Detailed reports on each of the top 20 unhealthy devices (including problem description and recommended actions)

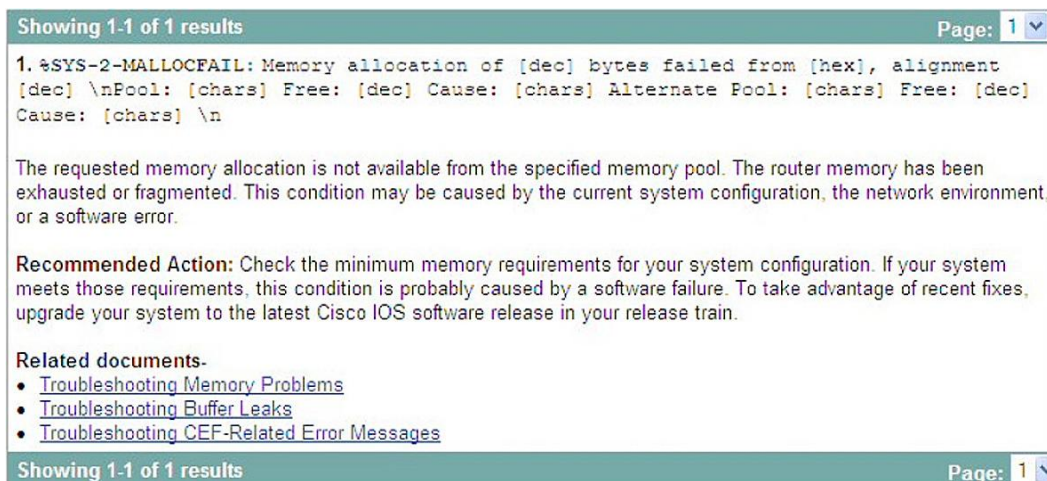
Event Remediation

It is recommended that problem tickets be opened against all critical and actionable messages. The problem management team would be responsible for these tickets.

Cisco.com and various other sources contain details for each of the Syslog messages identified, including Cisco recommended actions. These can be used as a starting point for troubleshooting an issue and identifying the root cause.

The Cisco Error Message Decoder is located at <http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>.

Figure 9. Example of a Critical Syslog Message and Recommended Action



Event Viewer

Developing or enhancing an existing Syslog management tool is a pivotal activity that contributes to the success of an effective Syslog management solution. The Event Viewer serves as a “one-stop shop” for the problem management team to have a correlated event list, sorted by both site and Syslog criticality.

The high-level requirements for this tool are outlined in this section; however, software-level requirements are outside the scope of this document. Some general guidelines are provided to maximize the tool’s scalability and robustness.

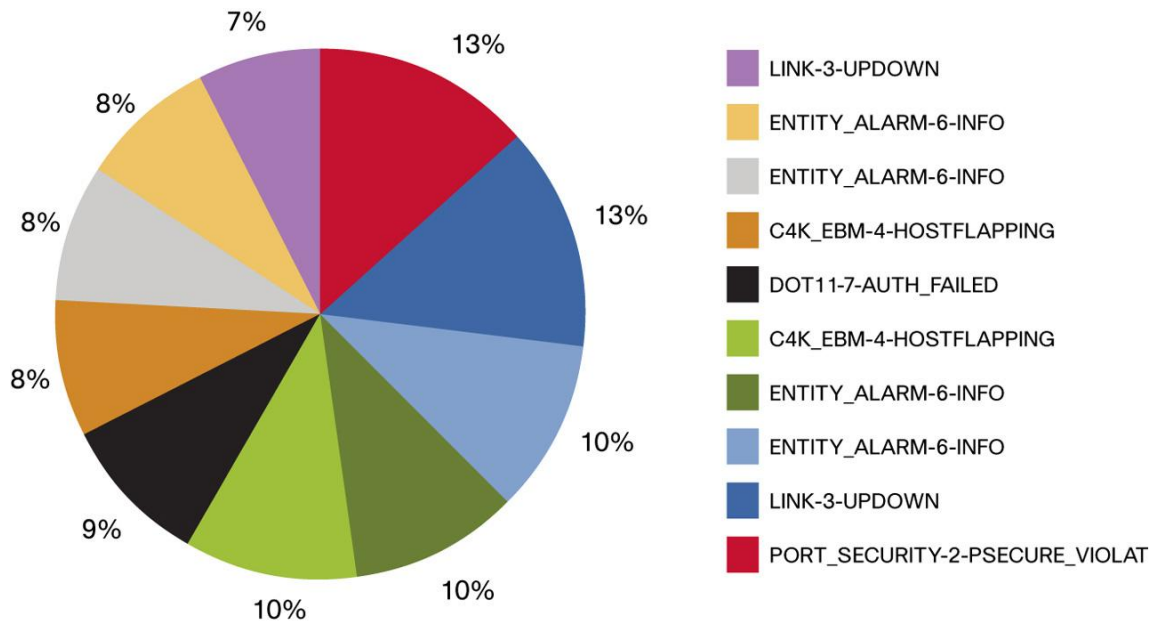
- The tool should use a web front end, which should allow easy access to all support groups within the organization.
- The tool should incorporate a standard user authentication system, which can then be used in incident/problem ticket generation.
- The tool should be able to de-duplicate incoming Syslog messages. For example, a device running low on memory with accounting turned on can send the following message very frequently:

%AAAA-3-DROPACCTLOWMEM: Accounting record dropped due to low memory

The tool should show this message only **once** and display the “received count” in another column, along with a timestamp of the first and last time the message was seen. This helps to make the GUI more usable. Syslog storage, de-duplication, and correlation information associated with the messages require a back-end relational database.

- The tool should incorporate a Top-N Syslog severity report. The report is very useful in highlighting “chatty” devices and directly helps the review activity detailed below. Charts can enhance such a report and provides a better visual breakdown of the messages.

Figure 10. Sample Pie Chart Display of Syslog Event Breakdown



- The tool should be able to differentiate between messages received from critical sites and non-critical sites. This distinction will assist the problem management team in event prioritization, so that they handle the high-impact messages first. This can be provided as another sortable column in the database table that marks the message with a weighted metric number based on the sending device.

The tools development team needs to collaborate cross-functionally with the inventory/asset management team that typically stores all the inventory data, including information on which sites and devices are critical as deemed by the organization.

A small sample of tools available is listed in section 6: Applications.

Event Logging Architecture

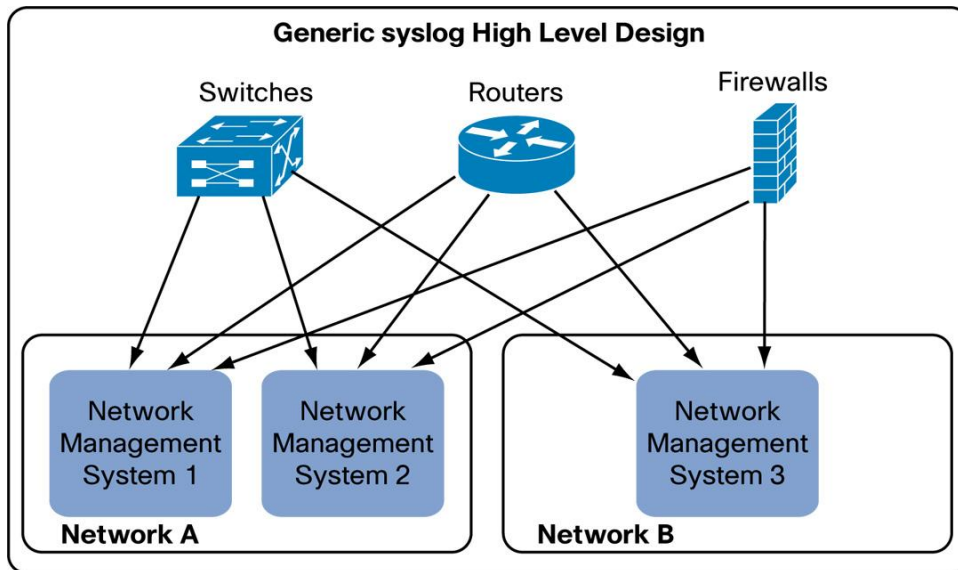
This section discusses two architectures for Syslog management system deployment. Each model has specific scalability limits that can be used to determine which is best suited for your environment. Keep in mind that as we go up in size, we increase the level of complexity for the deployment. This design is based on the use of syslog-ng as previously mentioned in this document.

syslog-ng Basics

As previously mentioned, syslog-ng allows for collection and “forking” of Syslog messages to many hosts. This allows log data to be collected and distributed in a much more robust fashion.

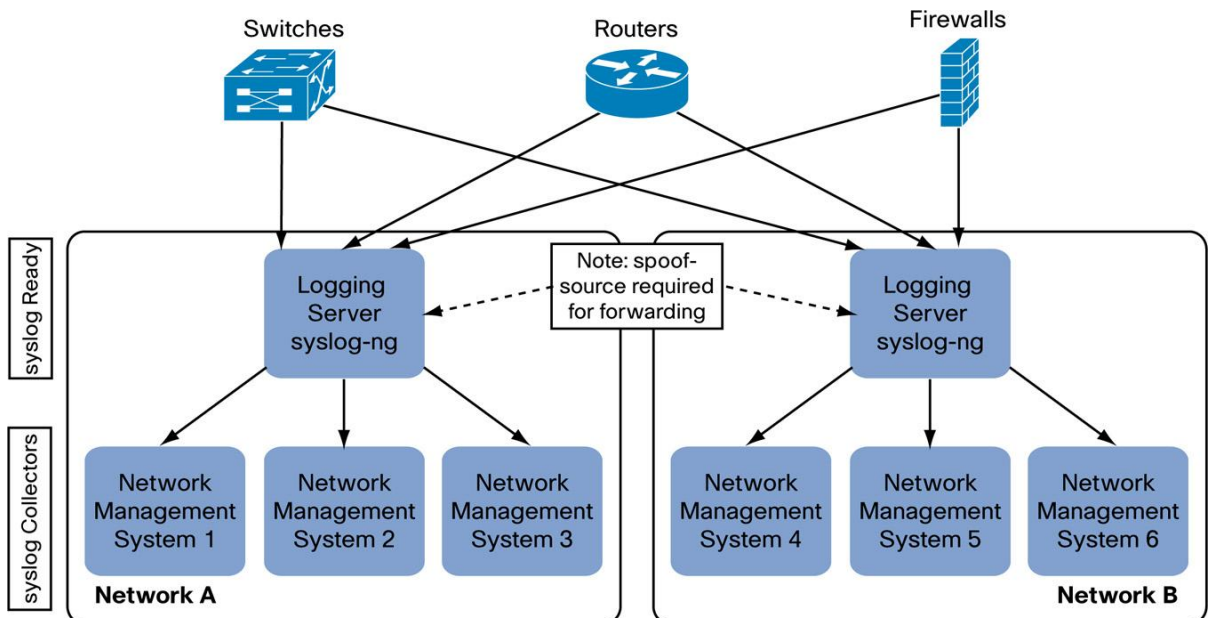
Traditional logging collection requires that many logging destinations be stored in each device:

Figure 11. Traditional logging reception



The implementation of syslog-ng collectors allows for only a few logging hosts to be configured in your devices, but then replicates these messages to end hosts such as network managers, analysis and reporting systems, etc.

Figure 12. Sample syslog-ng Architecture



syslog-ng Server Design Considerations

As you begin to consider design scenarios, several factors will affect which one you may actually need to deploy. Performance will vary greatly based on the following:

1. OS architecture - 64-bit vs. 32-bit (64-bit is a must!)
2. CPU
3. Memory
4. Disk speed - For example: deploying a server with a single SATA disk versus four SAS 15K RPM disks in a RAID 10 configuration.

The objective is to minimize the complexity of this architecture. For instance, a single-server deployment might become possible by simply upgrading the server to handle more demand (e.g., 4-8 CPUs, 16-32 GB RAM, SAS disks, etc.).

However, for larger organizations, it would probably be more suitable to place collectors closer to their networks and filter/forward messages to a master collector as noted in the multi-server scenario.

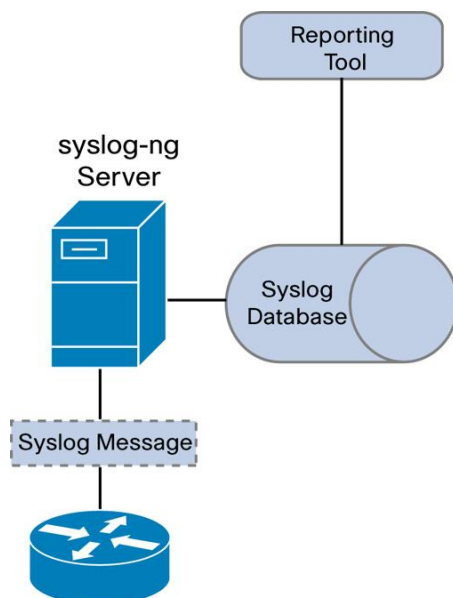
Finally, it's worth noting that the bottlenecks in the amount of messages these architectures can handle are predicated on the speed of the database, not the syslog-ng application. When logging to files, syslog-ng itself can process more than 70,000 messages per second.

Single-Server Deployment

This deployment consists of a single server containing the Syslog receiver, the SQL database for storing messages, and a reporting tool. These types of implementations are, by far, the easiest to set up and manage but may be limited in their ability to handle very large volumes of data.

This configuration should be able to handle anywhere from twenty to fifty million messages per day on a midrange server (quad-core, multi-processor, 32-64 GB RAM).

Figure 13. Single-Server Deployment



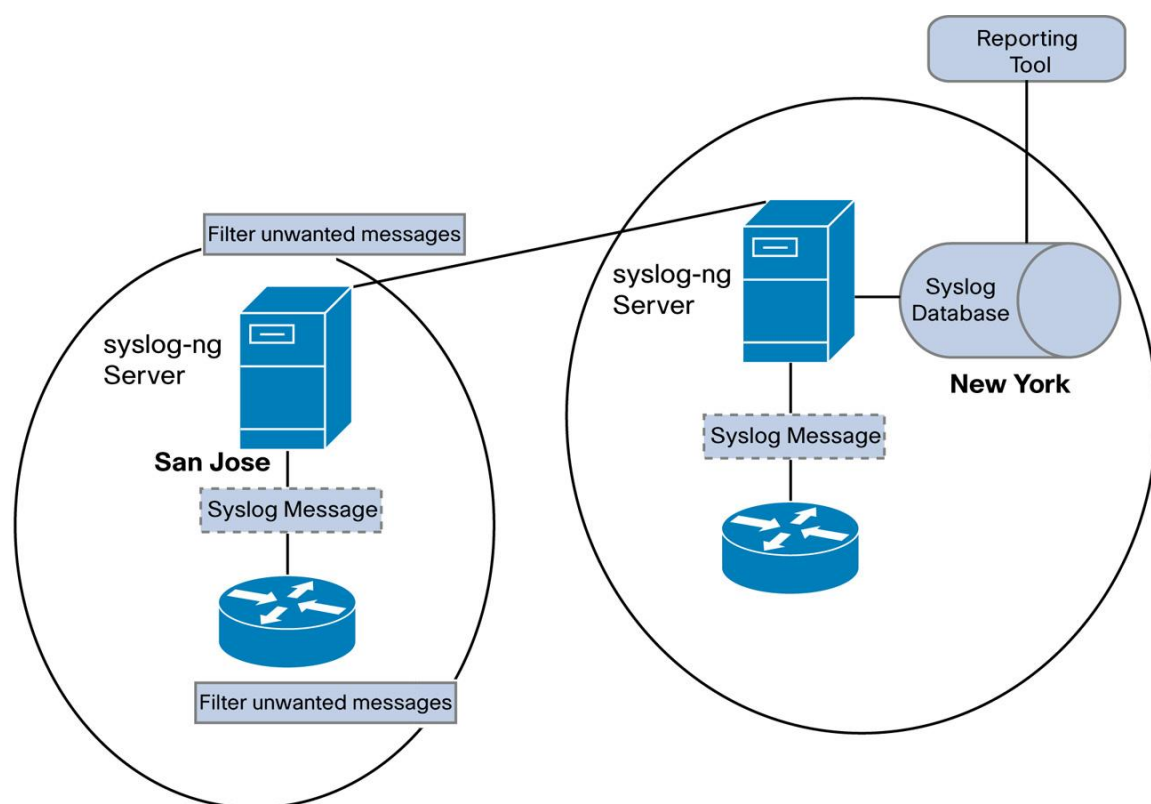
Multi-Server Deployment

This type of deployment involves placement of Syslog “collectors” at multiple geographic locations and is used to filter out unwanted messages before sending them over the wide area network to a Syslog receiver. These collectors can be very simple, workstation-class systems that are running a Linux OS and the Syslog collector itself, which listens for a Syslog message and forwards post-filtered messages to a receiver on the other end.

Alternatively, you may opt to use Cisco’s Embedded Syslog Manager (ESM) to filter and categorize any Syslog traffic prior to leaving the devices. The advantage of using ESM is that you won’t have to deploy collectors everywhere. This method is preferred among many customers in order to avoid placing additional hardware at the network edges for collection. More information on ESM is included in the Appendix section of this document, or available at http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_esm.html.

At this level, you could expect the architecture to handle millions of messages per day, depending on server specifications.

Figure 14. Multi-Server Deployment



Logging Architecture Guidelines

Following is a list of leading practices for large-scale Syslog management that Cisco believes can be beneficial. Like many leading practices, these are not meant to be adopted blindly, but rather evaluated on how each one may or may not fit into your environment.

Collection Stations

- Design your Syslog architecture in a distributed, hierarchical fashion.
- Place Syslog collectors as close to their networks as possible (e.g., assuming a hub-and-spoke architecture, the collectors would lie at the spokes and forward to the hub).
- Conduct some filtering at the collection level to filter out unnecessary log data.
- Configure the collectors forward all filtered messages to a centralized server/database for further processing and filtering.
- Store all log data in a database such as MySQL rather than into flat text files.

Syslog Event Manager

- Deploy an automated tool to establish a baseline of your logs.
- Assign people (or groups) to monitor daily Top X errors and remediate common problems.

Log Rotation and Retention

- Establish a log retention and rotation policy.
- Archive old log data to disk. The number of days, weeks, or months to store “live” log data depends on both company policy and server capability. A typical starting point for larger environments is to keep “live” data (online, searchable) for 1 week and then offline the data (either to an ARCHIVE type of SQL table, or to disk in case it is needed later).
- If your company adheres to Payment Card Industry (PCI) regulations, you must retain offline logs for a period of one year.
- Include logs and log archives in the standard backup process.

Server Sizing

The following tables are provided to help you decide which of these deployment scenarios is right for your organization. Please be aware that this is only a **rough** estimation. These calculations are based on data collected from Cisco’s internal IT management, and are meant merely as a starting frame of reference; many factors in your environment could greatly increase or decrease these numbers.

The calculations for each field are:

1. Approximate Messages Per Week = Device Count * multiplier (Table 5)
2. Approximate Messages Per Day = Msgs Per Week/7
3. Approximate Messages Per Minute = Msgs Per Day/1440
4. Approximate Messages Per Second = Msgs Per Min/60
5. Approximate storage capacity (in MB) needed per day = Msgs Per Day/1024/4

Table 4. Syslog Server Sizing Estimate

Device Type	Device Count	Average Msgs/Week	Per Day	Per Min	Per Second	DB Size (MB)
ACLs	100.00	471,500.00	67,357.14	46.78	0.78	16.44
Aironet Access Point	100.00	7,500.00	1,071.43	0.74	0.01	0.26
LAN Switch	100.00	27,900.00	3,985.71	2.77	0.05	0.97
PIX Security Appliance	100.00	53,381,800.00	7,625,971.43	5,295.81	88.26	1,861.81
Router	100.00	323,800.00	46,257.14	32.12	0.54	11.29
VPN	100.00	181,800.00	25,971.43	18.04	0.30	6.34

Table 5. Device Multipliers

Device Type	Multiplier
ACLs	4715
Aironet Access Point	75
LAN Switch	279
PIX Security Appliance	533818
Router	3238
VPN	1818

Database Types

There are many databases available in today's environments, but for the sake of simplicity and "openness," the database of choice for this design is MySQL. This section provides a reference for the types of database engines used in this architecture.

The following list assumes at least a basic knowledge of MySQL and its various engine types.

MyISAM

MyISAM (Indexed Sequential Access Method) is MySQL's extended ISAM format and default database engine. MyISAM uses a table-locking mechanism to optimize multiple simultaneous reads and writes. Table locking and non-clustered indexes vastly increase the speed of writing at the cost of forcing reads to wait. Since the logging architecture will do much more writing than reading, this is optimal. MySQL's table locking vs. row locking mechanism is what really sets MyISAM apart from almost all other databases, including Oracle, MSSQL, and PostgreSQL. The trade-off is that you need to run the OPTIMIZE TABLE command from time to time to recover space wasted by the update algorithms (which can easily be done during a nightly log rotation routine). MyISAM also has a few useful extensions such as the MyISAMChk utility to repair database files and the MyISAMPack utility for recovering wasted space.

MyISAM, with its emphasis on speedy read/write operations, is probably the major reason MySQL is so popular for web development. While the vast majority of the data operations you'll be carrying out are write operations, we'll also need to be able to read and display our data for the fastest possible reporting on large systems.

ARCHIVE

ARCHIVE tables are used to store large amounts of data without indexes in a very small footprint (decreased disk space). This is particularly useful when using log rotation methods such as the one used in this design. As tables are rotated, an ARCHIVE engine type is created to allow for historical searching and post-mortem troubleshooting as well as compliance standards such as SOX, HIPAA, and PCI.

Syslog Applications

The tools and applications listed below (in no specific order) provide collection and analysis of Syslog event streams. While each one may have its own set of advantages and disadvantages, it's ultimately up to your organization to decide which fits best in your environment. Please note that this is not an exhaustive list, but merely an example of some of the available tools to help get you pointed in the right direction.

Open Source and Commercial Syslog Products

There are advantages and disadvantages to each of these implementations. Many customers will opt for an open source solution in order to cut back on cost, but keep in mind that this also invites more administrative overhead.

Open Source

Many open source tools may require knowledge of one or more of the following technologies and products:

- Perl
- MySQL
- PHP
- Unix/Linux
- syslog-ng
- Apache Web Server
- SSL

LogZilla (Formerly Php-syslog-ng)

LogZilla (<http://www.logzilla.pro/>) is a scalable, multi-vendor, enterprise class syslog event viewer for centralized network event and problem management. LogZilla features real-time alerting, intelligent event deduplication, extensive search and reporting capabilities and also includes a built-in capability to track Cisco Mnemonics.

Figure 15. LogZilla Main Interface

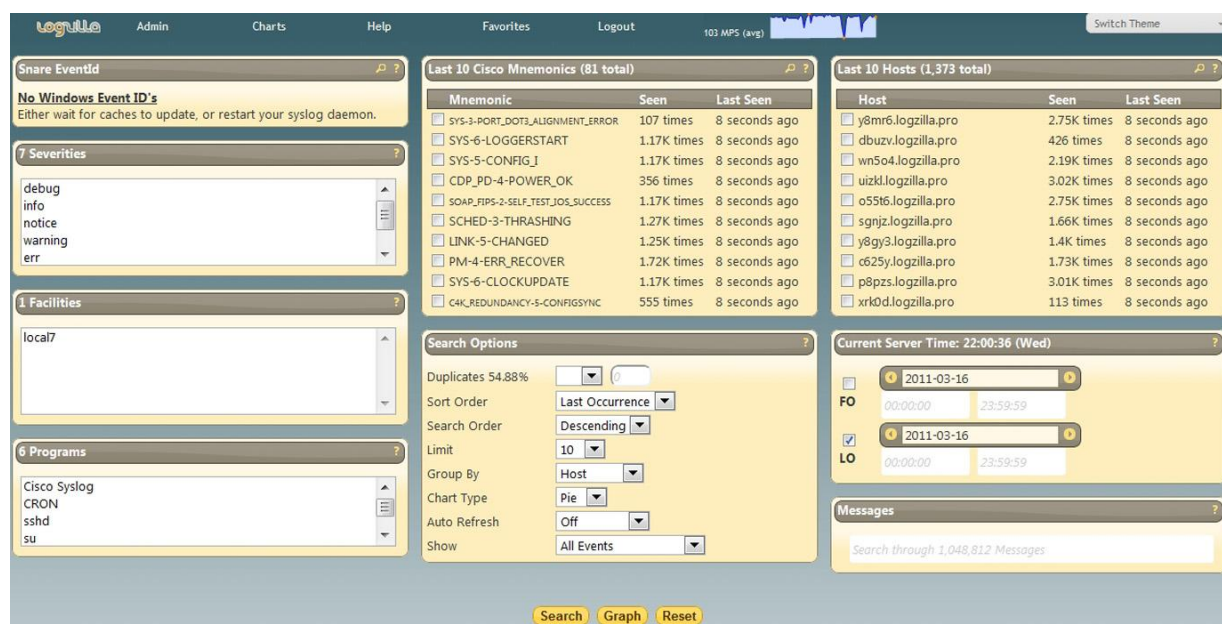
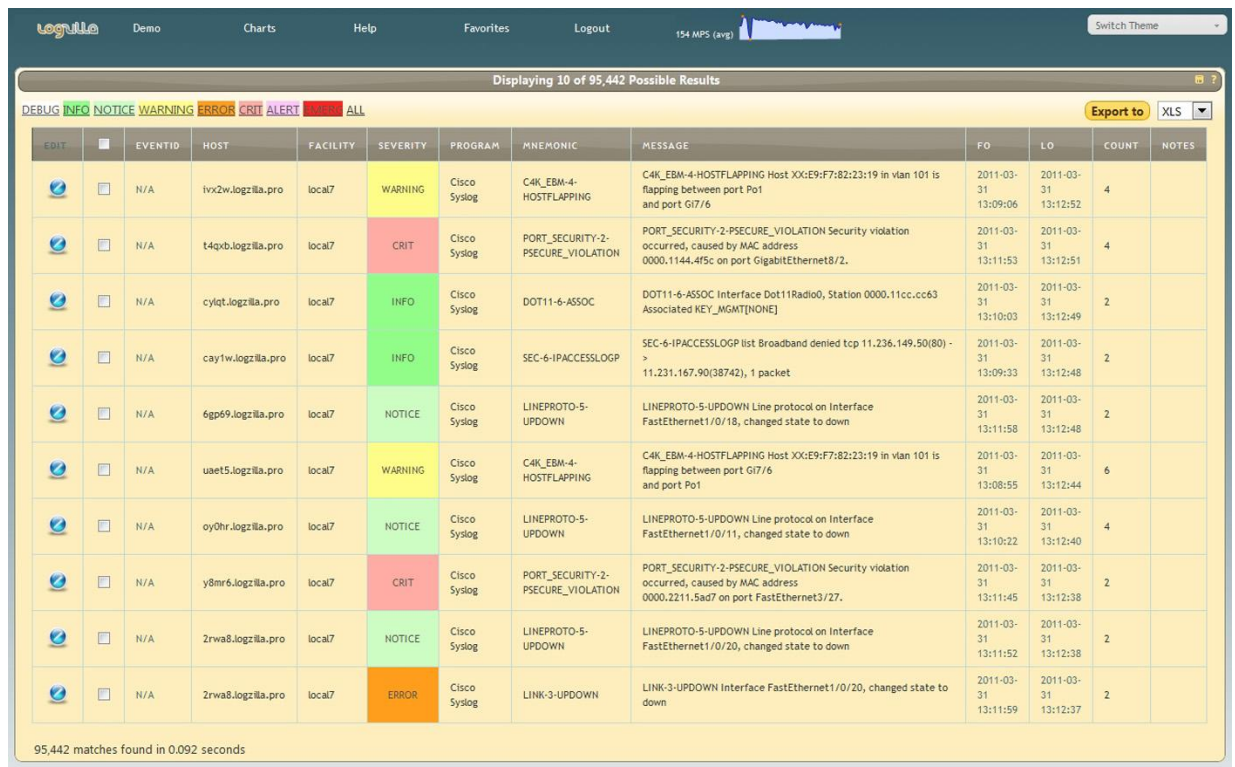


Figure 16. LogZilla Search

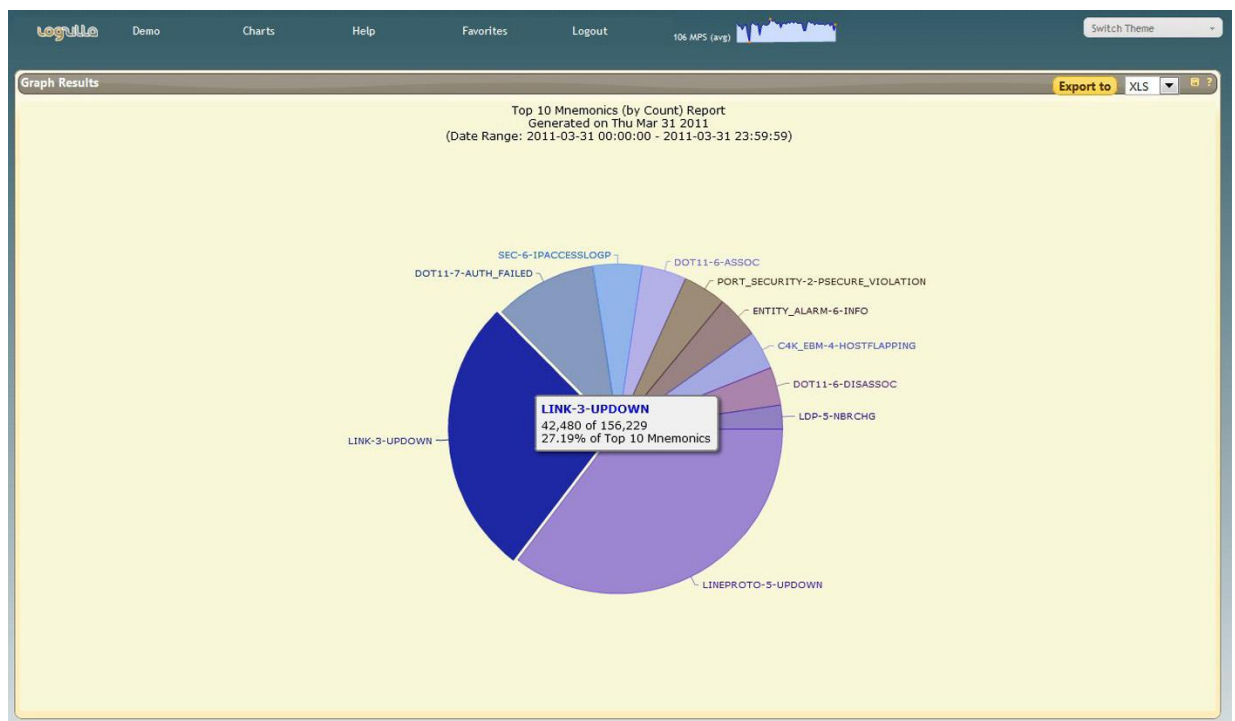


The screenshot shows the LogZilla search results interface. At the top, there's a navigation bar with 'LogZilla', 'Demo', 'Charts', 'Help', 'Favorites', 'Logout', and a status bar showing '154 MPS (avg)'. Below this, a header indicates 'Displaying 10 of 95,442 Possible Results'. A filter bar shows tabs for 'DEBUG', 'INFO', 'NOTICE', 'WARNING', 'ERROR', 'CRIT', 'ALERT', 'EMERG', and 'ALL'. An 'Export to' button is set to 'XLS'. The main table has columns: EDIT, EVENTID, HOST, FACILITY, SEVERITY, PROGRAM, MNEMONIC, MESSAGE, FO, LO, COUNT, and NOTES. The table lists 10 log entries with various severity levels (WARNING, CRIT, INFO, NOTICE, ERROR) and mnemonics like C4K_EBM-4-HOSTFLAPPING, PORT_SECURITY-2-PSECURE_VIOLATION, and LINK-3-UPDOWN. At the bottom, it states '95,442 matches found in 0.092 seconds'.

EDIT	EVENTID	HOST	FACILITY	SEVERITY	PROGRAM	MNEMONIC	MESSAGE	FO	LO	COUNT	NOTES
	N/A	lvx2w.logzilla.pro	local7	WARNING	Cisco Syslog	C4K_EBM-4-HOSTFLAPPING	C4K_EBM-4-HOSTFLAPPING Host X0:E9:F7:82:23:19 in vlan 101 is flapping between port Po1 and port Gi7/6	2011-03-31 13:09:06	2011-03-31 13:12:52	4	
	N/A	t4qxb.logzilla.pro	local7	CRIT	Cisco Syslog	PORT_SECURITY-2-PSECURE_VIOLATION	PORT_SECURITY-2-PSECURE_VIOLATION Security violation occurred, caused by MAC address 0000.1144.4f5c on port GigabitEthernet8/2.	2011-03-31 13:11:53	2011-03-31 13:12:51	4	
	N/A	cyqqt.logzilla.pro	local7	INFO	Cisco Syslog	DOT11-6-ASSOC	DOT11-6-ASSOC Interface Dot11Radio0, Station 0000.11cc.cc63 Associated KEY_MGMT[NONE]	2011-03-31 13:10:03	2011-03-31 13:12:49	2	
	N/A	cay1w.logzilla.pro	local7	INFO	Cisco Syslog	SEC-6-IPACCESSLOGP	SEC-6-IPACCESSLOGP list Broadband denied tcp 11.236.149.50(80) -> 11.231.167.90(38742), 1 packet	2011-03-31 13:09:33	2011-03-31 13:12:48	2	
	N/A	6gp69.logzilla.pro	local7	NOTICE	Cisco Syslog	LINEPROTO-5-UPDOWN	LINEPROTO-5-UPDOWN Line protocol on Interface FastEthernet1/0/18, changed state to down	2011-03-31 13:11:58	2011-03-31 13:12:48	2	
	N/A	uuet5.logzilla.pro	local7	WARNING	Cisco Syslog	C4K_EBM-4-HOSTFLAPPING	C4K_EBM-4-HOSTFLAPPING Host X0:E9:F7:82:23:19 in vlan 101 is flapping between port Gi7/6 and port Po1	2011-03-31 13:08:55	2011-03-31 13:12:44	6	
	N/A	oy0hr.logzilla.pro	local7	NOTICE	Cisco Syslog	LINEPROTO-5-UPDOWN	LINEPROTO-5-UPDOWN Line protocol on Interface FastEthernet1/0/11, changed state to down	2011-03-31 13:10:22	2011-03-31 13:12:40	4	
	N/A	y8mr6.logzilla.pro	local7	CRIT	Cisco Syslog	PORT_SECURITY-2-PSECURE_VIOLATION	PORT_SECURITY-2-PSECURE_VIOLATION Security violation occurred, caused by MAC address 0000.2211.5ad7 on port FastEthernet3/27.	2011-03-31 13:11:45	2011-03-31 13:12:38	2	
	N/A	2rwa8.logzilla.pro	local7	NOTICE	Cisco Syslog	LINEPROTO-5-UPDOWN	LINEPROTO-5-UPDOWN Line protocol on Interface FastEthernet1/0/20, changed state to down	2011-03-31 13:11:52	2011-03-31 13:12:38	2	
	N/A	2rwa8.logzilla.pro	local7	ERROR	Cisco Syslog	LINK-3-UPDOWN	LINK-3-UPDOWN Interface FastEthernet1/0/20, changed state to down	2011-03-31 13:11:59	2011-03-31 13:12:37	2	

95,442 matches found in 0.092 seconds

Figure 17. LogZilla Chart



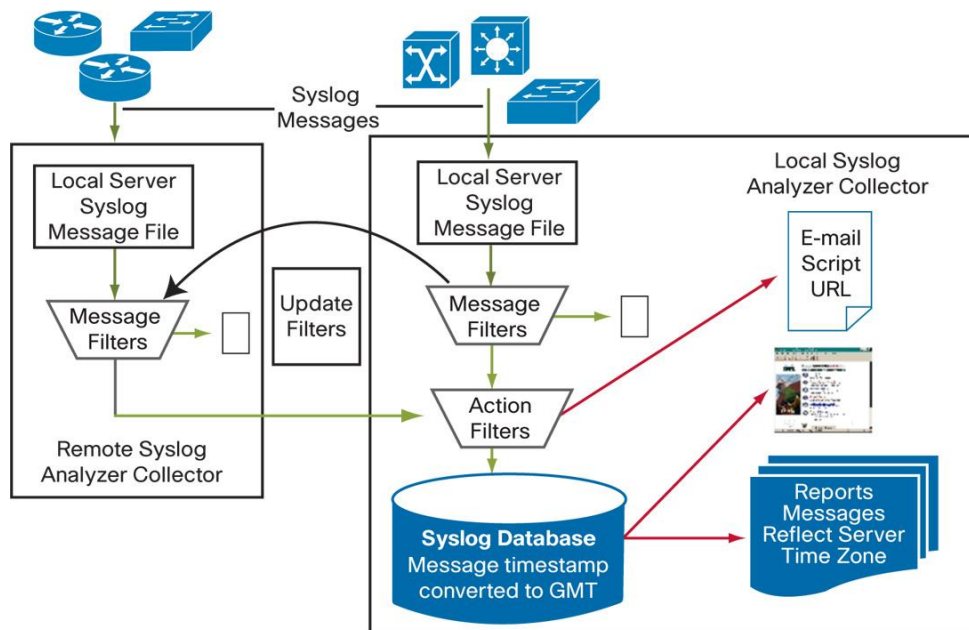
Commercial

Commercial tools provide you with turnkey solutions without having to hire employees that can develop or maintain the technologies that drive them. The disadvantage of commercial tools is, of course, the cost involved of purchasing and maintaining the product.

CiscoWorks LMS

CiscoWorks LAN Management Solution (LMS) (<http://www.cisco.com/go/lms>) is a suite of powerful management tools that simplify the configuration, administration, monitoring, and troubleshooting of Cisco networks. The Resource Manager Essentials (RME) component of the LMS suite offers a syslog management and reporting tool for site implementations of 5000 or less end devices (Figure 19).

Figure 18. CiscoWorks Syslog Processing

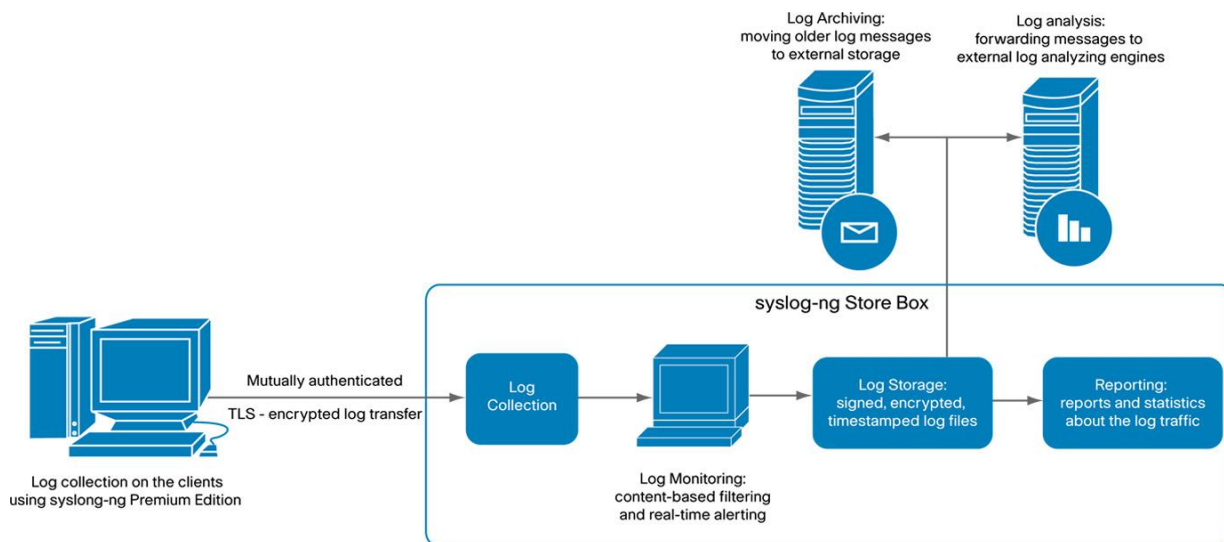


Note: Some message filters are enabled by default in CiscoWorks, including: Link Up/Down, ASA, DEBUG, and IOS Firewall Audit Trail messages. Large amounts of messages may lock up a server, so plan wisely!

syslog-ng Store Box (SSB)

SSB (<http://www.balabit.com/network-security/syslog-ng/log-server-appliance/>) offers a simple, reliable, and convenient way of collecting log messages centrally. It is essentially a high-capacity log server with high-availability support. Being able to collect logs from several different platforms makes it easy to integrate into any environment.

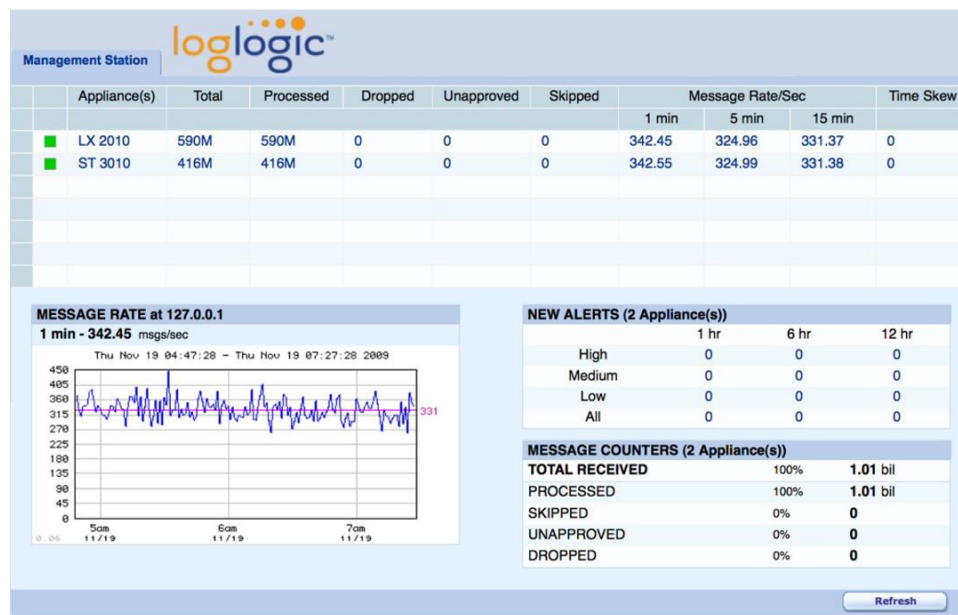
Figure 19. syslog-ng Store Box



loglogic

loglogic (<http://www.loglogic.com>) offers a highly scalable Syslog solution based on turnkey hardware (Figure 21).

Figure 20. LogLogic



Splunk

Splunk (<http://www.splunk.com>) offers both a free and commercial version of its tool. The free version is limited to 500 MB of log storage per day and, therefore, is only useful in smaller networks. The software allows you search and analyze all of your IT infrastructure data from a single location in real time (Figure 22).

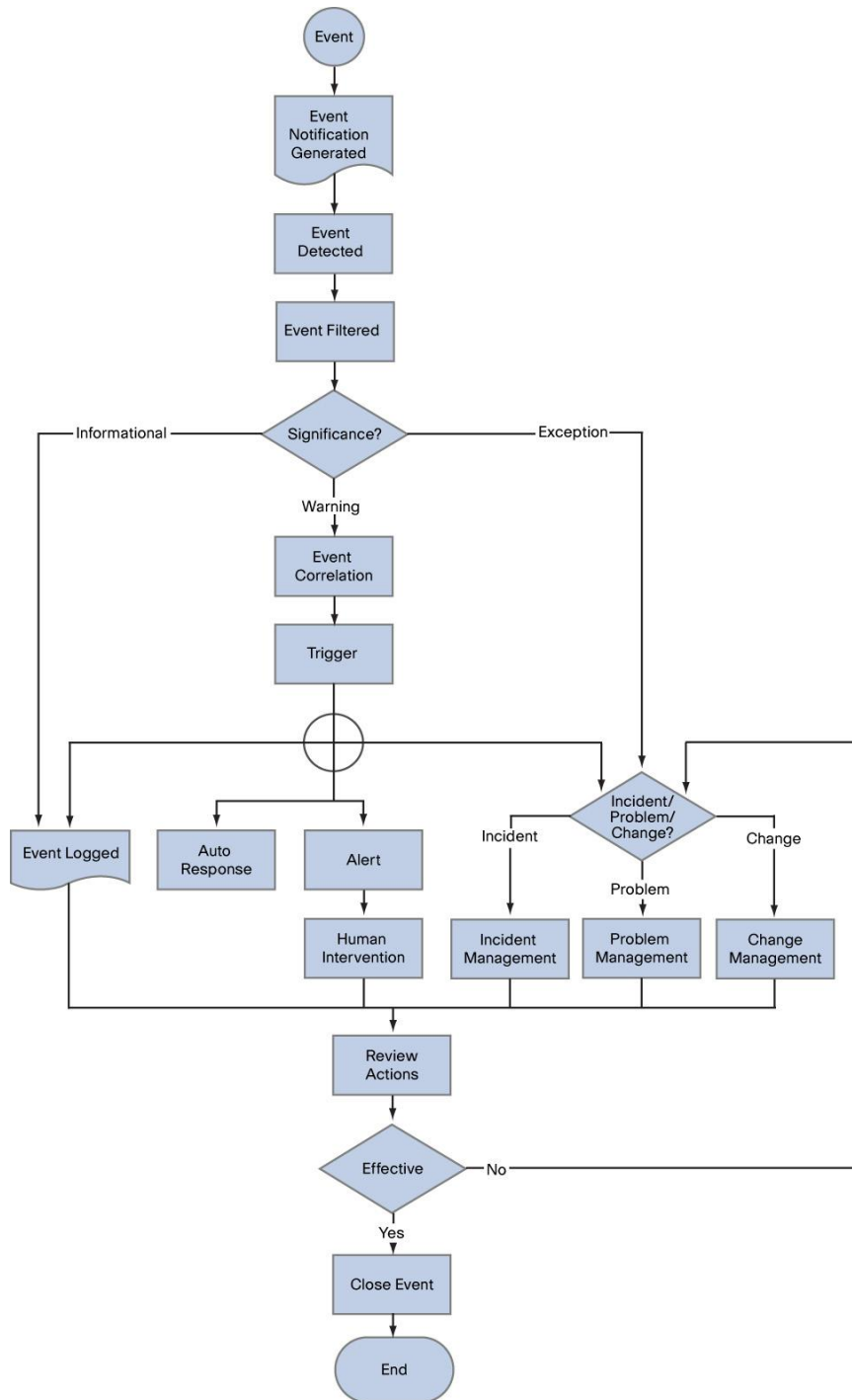
Figure 21. Splunk Web Interface



Appendix

ITIL V3 Event Management

Figure 22. ITIL V3 Event Management



Source: IT Service Management Based on ITIL V3 - A Pocket Guide

Cisco Embedded Syslog Manager

The Embedded Syslog Manager (ESM) is a feature integrated in Cisco IOS Software that allows complete control over system message logging at the source. ESM provides a programmatic interface to allow you to write custom filters that meet your specific needs in dealing with system logging. Benefits of this feature include:

- Customization - Fully customizable processing of system logging messages, with support for multiple, interfacing syslog collectors.
- Severity escalation for key messages - The ability to configure your own severity levels for syslog messages instead of using the system-defined severity levels.
- Specific message targeting - The ability to route specific messages or message types, based on type of facility or type of severity, to different syslog collectors.
- SMTP-base email alerts - Capability for notifications using TCP to external servers, such as TCP-based syslog collectors or Simple Mail Transfer Protocol (SMTP) servers.
- Message limiting - The ability to limit and manage Syslog "message storms" by correlating device-level events.

The ESM is not a replacement for the current UDP-based syslog mechanism; instead, it is an optional subsystem that can operate in parallel with the current system logging process. For example, you can continue to have the original syslog message stream collected by server A, while the filtered, correlated, or otherwise customized ESM logging stream is sent to server B. All of the current targets for syslog messages (console, monitor, buffer, and syslog host list) can be configured to receive either the original syslog stream or the ESM stream. The ESM stream can be further divided into user-defined streams and routed to collectors accordingly.

Additional information on Cisco's ESM feature is located at

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_esm.html

Actionable Syslogs

The following is a sample list of Syslogs that may be found in an environment. **This is by no means a comprehensive list. Syslog reporting should be carried out on all message and device types, level 0-6,** to look for other interesting messages pertaining to your network.

To get more details about the messages, refer to the Cisco Error Message Decoder tool at

<http://www.cisco.com/cgi-bin/Support/Errordecoder/home.pl>.

Each syslog includes one or more samples of events that you would expect to see. Not all of these would be seen in a given network, so an investigation should be done to determine if they are happening,

Many of the tools listed in the Applications section of this document can be used to monitor for these events and send or take another action.

Cisco IOS Syslogs

%SYS-3-CPUHOG

This problem can be caused by many conditions such as traffic, system load, hardware, operational configuration, a configuration change, initialization of many interfaces, a high momentary error rate, or a sustained abnormal condition.

```
May 9 03:34:57 ROUTER.foo.com 23772: May 9 03:34:53.911: %SYS-3-CPUHOG: Task ran  
for 18428 msec (22/9), process = IP SNMP, PC = 32976EC.
```


%LINEPROTO-5-UPDOWN

This message is best monitored from more critical devices only; this will be seen many times a day from access switches.

```
Jun 19 10:25:32 ROUTER.foo.com 77: Jun 19 10:25:31.093: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Serial4/0, changed state to up
Jun 19 10:26:02 ROUTER.foo.com 78: Jun 19 10:26:01.093: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Serial4/0, changed state to down
```

%OSPF-5-ADJCHG

This message describes the change and the reason for it. This message appears only if the log-adjacency-changes command is configured for the Open Shortest Path First (OSPF) process.

```
Apr 12 19:18:47 ROUTER.foo.com 12313: Apr 12 19:18:46.536: %OSPF-5-ADJCHG: Process
100, Nbr 1.2.3.4 on Serial2/1.2 from FULL to DOWN, Neighbor Down: Interface down or
detached
Apr 12 19:20:35 ROUTER.foo.com 12316: Apr 12 19:20:34.387: %OSPF-5-ADJCHG: Process
100, Nbr 1.2.3.4 on Serial2/1.2 from LOADING to FULL, Loading Done
```

%BGP-5-ADJCHANGE

This message appears only if the bgp log-neighbor-changes command is configured for the Border Gateway Protocol (BGP) autonomous system.

```
Apr 5 00:25:39 router.foo.com 2116715: Apr 5 00:25:38.849: %BGP-5-ADJCHANGE:
neighbor 202.43.137.17 Down Peer closed the session
Apr 5 00:26:08 ROUTER.foo.com 27: *Mar 1 10:01:19: %BGP-5-ADJCHANGE: neighbor
1.2.3.4 Up
Apr 25 12:30:07 ROUTER.foo.com 1001: Apr 25 12:30:06.936: %BGP-5-ADJCHANGE:
neighbor 1.2.3.4 Down BGP Notification sent
Apr 20 20:03:38 router.foo.com 997: Apr 20 20:03:37.468: %BGP-5-ADJCHANGE: neighbor
1.2.3.4 Up
```

%DUAL-5-NBRCHANGE

This message appears only if the eigrp log-neighbor-changes command is configured for the Enhanced Interior Gateway Routing Protocol (EIGRP) autonomous system.

```
Sep 7 07:45:25 router.foo.com 477: Sep 7 22:44:32.086: %DUAL-5-NBRCHANGE: IP-EIGRP
109: Neighbor 10.1.1.1 (ATM3/0.1) is down: holding time expired
Sep 11 10:18:48 router.foo.com 345: Sep 12 01:17:57.293: %DUAL-5-NBRCHANGE: IP-
EIGRP 109: Neighbor 10.1.1.1 (GigabitEthernet1/2) is down: peer restarted
Sep 13 10:46:08 router.foo.com 523809: Sep 13 18:45:18.100: %DUAL-5-NBRCHANGE: IP-
EIGRP 109: Neighbor 10.1.1.1 (GigabitEthernet1/2) is down: interface down
Sep 13 10:48:43 router.foo.com 523847: Sep 13 18:47:52.950: %DUAL-5-NBRCHANGE: IP-
EIGRP 109: Neighbor 10.1.1.1 (GigabitEthernet1/2) is up: new adjacency
```

%STANDBY-6-STATECHANGE

Events generated when Hot Standby Router Protocol (HSRP) changes state.

```
May 1 18:11:52 ROUTER.foo.com 181: 000172: May 1 18:11:51.540: %STANDBY-6-STATECHANGE: Vlan42 Group 42 state Standby -> Active
May 1 18:11:52 ROUTER.foo.com 836: 000827: May 1 18:11:51.543: %STANDBY-6-STATECHANGE: Vlan42 Group 42 state Active -> Speak
May 1 18:13:43 ROUTER.foo.com 838: 000829: May 1 18:13:42.879: %STANDBY-6-STATECHANGE: Vlan42 Group 42 state Standby -> Active
May 1 18:13:43 ROUTER.foo.com 182: 000173: May 1 18:13:42.880: %STANDBY-6-STATECHANGE: Vlan42 Group 42 state Active -> Speak
```

%FTSP-2-INTERNAL_ERROR

This message indicates that an internal software error has occurred. If the error message occurs, copy the message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

```
Feb 24 14:45:32 ROUTER.foo.com 1100142: 1100138: Feb 24 13:45:31.439: %FTSP-2-INTERNAL_ERROR: Internal software error. ftps_csm_conn: NULL hwidb
```

Switch Syslogs (CAT-OS)

While these are “switch” Syslogs, most of these are, in fact, Catalyst OS Syslog messages. However, some can come from Catalyst IOS.

%MODULE-4-MOD_WARNING

Module reported a warning in the runtime diagnostic because of a failure in some of the ports.

```
Oct 7 11:52:28 SWITCH.foo.com : 2006 Oct 07 12:52:28 AUEDST: %MODULE-4-MOD_WARNING: Module 1 reported warnings on ports 1/15-1/15 (0x0) due to FC Port not receiving R_RDY in device 3 (device error 0x18)
Oct 9 22:38:05 SWITCH.foo.com : 2006 Oct 09 23:38:05 AUEDST: %MODULE-4-MOD_WARNING: Module 2 reported warnings on ports 2/15-2/15 (0x0) due to FC Port not receiving R_RDY in device 3 (device error 0x18)
```

%PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN

This is a PortChannel interface and all its members are operationally down.

```
Oct 14 18:37:08 SWITCH.foo.com : 2006 Oct 14 19:37:08 AUEDST: %PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: %$VSAN 3%$ Interface port-channel 4 is down (No operational members)
```

%PORT_CHANNEL-5-FOP_CHANGED

The first operational port in a port-channel is changed.

```
Oct 14 20:53:28 SWITCH.foo.com : 2006 Oct 14 21:53:28 AUEDST: %PORT_CHANNEL-5-FOP_CHANGED: port-channel 4: first operational port changed from fc2/2 to fc1/2
Oct 14 18:56:49 SWITCH.foo.com : 2006 Oct 14 18:56:49 AUEDST: %PORT_CHANNEL-5-FOP_CHANGED: port-channel 4: first operational port changed from none to fc2/13
```

%SYS-2-PS_FAIL

This message indicates that the power supply failed. [dec] is the power supply number.

```
Apr 6 12:41:35 SWITCH.foo.com 2005 Apr 06 12:41:35 AEST +10:00 %SYS-2-PS_FAIL:
Power supply 2 failed
```

%SYS-2-PS_OK

This message indicates the power supply has been turned on or has returned to a proper state. [dec] is the power supply number.

```
Mar 26 17:33:57 SWITCH.foo.com 2005 Mar 26 16:33:55 AEST +10:00 %SYS-2-PS_OK:Power
supply 2 okay
```

%SYS-2-FAN_FAIL

This message indicates that the chassis fan failed.

```
Jun 13 08:27:48 SWITCH.foo.com 2006 Jun 13 07:42:51 AEST +10:00 %SYS-2-FAN_FAIL:Fan
failed
```

%SYS-2-FAN_OK

This message indicates that the chassis fan tray was plugged back in or returned to a proper state.

```
Jun 13 08:27:48 SWITCH.foo.com 2006 Jun 13 07:42:51 AEST +10:00 %SYS-2-FAN_OK:Fan
okay
```

%SYS-2-PS_NFANFAIL

This message indicates that the power supply and power supply fan failed. [dec] is the power supply number.

```
Mar 15 13:23:09 SWITCH.foo.com 2005 Mar 15 12:23:11 AEST +10:00 %SYS-2-
PS_NFANFAIL:Power supply 2 and power supply fan failed
```

%SYS-0-SYS_LCPERR0

This message indicates an error in the port ASIC. The first [dec] is the module number. The second [dec] is the ASIC port number.

```
Mar 22 01:29:49 SWITCH.foo.com 2006 Mar 22 00:29:48 AEST +10:00 %SYS-0-
SYS_LCPERR0:Module 6: Linecard received system exception: Module needs
troubleshooting or TAC assistance
```

%C6KPWR-SP-4-DISABLED

The module in the indicated slot was powered off for the reason stated in the error message.

```
Apr 6 15:19:20 SWITCH.foo.com 39748: Apr 6 15:19:18.499: %C6KPWR-SP-4-DISABLED:
power to module in slot 3 set off (Reset)
```

%SYS-4-SYS_LCPERR4 and %SYS-3-SYS_LCPERR3

This is a debugging message for Cisco development purposes. [dec] is the module number, and [hex] is debugging information. If the error is limited to a single module, replace the module. If the error occurs several times, contact your technical support representative.

```
Oct 4 00:07:46 SWITCH.foo.com 2005 Oct 04 00:07:45 AEST +10:00 %SYS-4-SYS_LCPERR4:
Module [dec]: RChip Port#[dec] Boc Header Crc Error
```

%SYS-1-MOD_MINORFAIL

This message indicates that a module failed the self-test. [dec] is the module number.

```
Apr 30 16:00:36 SWITCH1.foo.com 2005 Apr 30 16:00:35 AEST +10:00 %SYS-1-
MOD_MINORFAIL:Minor problem in module 1
```

%SYS-3-MOD_FAIL

This message indicates that module [dec] failed to come online; [dec] is the module number.

```
Apr 6 19:11:10 SWITCH.foo.com 2005 Apr 06 19:11:10 AEST +10:00 %SYS-3-
MOD_FAIL:Module 1 failed to come online
```

%SYS-3-MOD_PWRFAIL

This message indicates that a module did not power up. [dec] is the number of the module that did not power up.

```
Aug 22 12:19:17 SWITCH.foo.com 2006 Aug 22 12:19:17 AEST +10:00 %SYS-3-
MOD_PWRFAIL:Module 1 failed to power up
Aug 22 12:39:37 SWITCH.foo.com 2006 Aug 22 12:39:37 AEST +10:00 %SYS-3-
MOD_PWRFAIL:Module 1 failed to power up
```

%SYS-5-MOD_RESET

This message indicates that the module was reset from a specified requestor. [dec] is the module number, and [chars] could be a console number if the request is from a console session or an IP address if the request is from a Telnet session or SNMP.

```
Feb 21 16:00:40 SWITCH.foo.com 2005 Feb 21 15:00:40 AEST +10:00 %SYS-5-
MOD_RESET:Module 6 reset from Software
```

%SYS-5-MOD_REMOVE

This message indicates that a module was removed. [dec] is the module number.

```
Apr 30 15:36:32 SWITCH.foo.com 2005 Apr 30 15:36:32 AEST +10:00 %SYS-5-
MOD_REMOVE:Module 1 has been removed
```

%SYS-5-MOD_INSERT

This message indicates that a module was inserted. [dec] is the module number.

```
Apr 30 15:57:42 SWITCH.foo.com 2005 Apr 30 15:57:42 AEST +10:00 %SYS-5-
MOD_INSERT:Module 1 has been inserted
```

%SYS-5-MOD_OK

This message indicates that the module passed the diagnostic self-test and is online. [dec] is the module number

```
Apr 30 15:36:17 SWITCH.foo.com 2005 Apr 30 15:36:17 AEST +10:00 %SYS-5-  
MOD_OK:Module 12 is online  
Mar 20 20:13:18 SWITCH.foo.com 2005 Mar 20 19:13:17 AEST +10:00 %SYS-5-  
MOD_OK:Module 1 (WS-X6K-SUP2-2GE,SAL130DDDDD) is online
```

%SYS-2-MALLOCFAIL

The requested memory allocation is not available from the specified memory pool. The device memory has been exhausted or fragmented. This condition may be caused by the current system configuration, the network environment, or a software error.

```
Sep 25 18:06:58 ROUTER.foo.com 3144: Sep 25 18:06:56.263: %SYS-2-MALLOCFAIL: Memory  
allocation of 27 bytes failed from 0x3560638, alignment 0
```

%RTD-1-ADDR_FLAP

Normally, MAC addresses are learned once on a port. Occasionally, when a switched network reconfigures, due to either manual or STP reconfiguration, addresses learned on one port are relearned on a different port. However, if there is a port anywhere in the switched domain that is looped back to itself, addresses will jump back and forth between the real port and the port that is in the path to the looped back port. In this message, [chars] is the interface, and [dec] is the number of addresses being learned.

```
Apr 26 13:21:31 SWITCH.foo.com 44: Apr 26 13:21:30.054: %RTD-1-ADDR_FLAP:  
FastEthernet0/9 relearning 5 addrs per min
```

%RTD-1-LINK_FLAP

This message means that an excessive number of link down-up events have been noticed on this interface: [chars] is the interface, and [dec] is the number of times the link goes up and down. This might be the result of reconfiguring the port, or it might indicate a faulty device at the other end of the connection.

```
Dec 19 19:25:28 SWITCH.foo.com 147: Dec 19 18:25:27.601: %RTD-1-LINK_FLAP:  
FastEthernet0/1 link down/up 5 times per min
```

%PORT_SECURITY-2-PSECURE_VIOLATION

This message means that an unauthorized device attempted to connect on a secure port. MAC [enet] is the MAC address of the unauthorized device, and port [chars] is the secure port.

```
Nov 28 17:00:19 SWITCH.foo.com 1175: *Jul 7 15:00:46.608: %PORT_SECURITY-2-  
PSECURE_VIOLATION: Security violation occurred, caused by MAC address  
1234.38c8.6637 on port FastEthernet0/24.
```

%SECURITY-1-PORTSHUTDOWN

This message indicates that a port has been shut down due to an insecure host sourcing a packet into that port. [dec]/[dec] is the module number/port number of the port that has shut down, and [chars] can be either a security violation or no space in the forwarding engine lookup table.

```
Nov 28 22:02:05 SWITCH.foo.com 2005 Nov 28 21:02:04 AEST +10:00 %SECURITY-1-PORTSHUTDOWN:Port 4/11 shutdown due to security violation 00-14-22-c0-c9-52
Dec 18 00:29:02 SWITCH.foo.com 2005 Dec 17 23:29:02 AEST +10:00 %SECURITY-1-PORTSHUTDOWN:Port 2/21 shutdown due to security violation.
```

Storage Syslogs (MDS 9000)

These are some interesting SAN-OS Syslog messages.

%MODULE-4-MOD_WARNING

Module reported a warning in the runtime diagnostic because of a failure in some of the ports.

```
Oct 7 11:52:28 SWITCH.foo.com : 2006 Oct 07 12:52:28 AUEDST: %MODULE-4-MOD_WARNING:
Module 1 reported warnings on ports 1/15-1/15 (0x0) due to FC Port not receiving
R_RDY in device 3 (device error 0x18)
Oct 9 22:38:05 SWITCH.foo.com : 2006 Oct 09 23:38:05 AUEDST: %MODULE-4-MOD_WARNING:
Module 2 reported warnings on ports 2/15-2/15 (0x0) due to FC Port not receiving
R_RDY in device 3 (device error 0x18).
```

%PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN

This is a PortChannel interface and all its members are operationally down.

```
Oct 14 18:37:08 SWITCH.foo.com : 2006 Oct 14 19:37:08 AUEDST: %PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: %$VSAN 3%$ Interface port-channel 4 is down (No operational members.
```

%PORT_CHANNEL-5-FOP_CHANGED

The first operational port in a port channel is changed.

```
Oct 14 20:53:28 SWITCH.foo.com : 2006 Oct 14 21:53:28 AUEDST: %PORT_CHANNEL-5-FOP_CHANGED: port-channel 4: first operational port changed from fc2/2 to fc1/2
Oct 14 18:56:49 SWITCH.foo.com : 2006 Oct 14 18:56:49 AUEDST: %PORT_CHANNEL-5-FOP_CHANGED: port-channel 4: first operational port changed from none to fc2/13.
```

Other Syslogs

The following list contains other Syslogs that may be deemed actionable in your network.

```
PLATFORM_ENVMON_2_ENV_POWER_FAILURE
PLATFORM-ENVMON-2-POWERSUPPLY_NONOP
C4K_IOSMODPORTMAN-4-INLINEPOWERSUPPLYBAD
C4K_IOSMODPORTMAN-4-POWERSUPPLYFANBAD
C4K_IOSMODPORTMAN-4-POWERSUPPLYBAD
PS-3-MULTFAIL
RPS-3-MULTFAIL
CI-3-PSFAIL
CI-3-PWRA_FAIL
SYS-2-PS_INSUFFICIENT
SYS-2-PS_NFANFAIL
SYS-2-PS_FAIL
PLATFORM_ENVMON_2_ENV_POWER_FAULT
PLATFORM_ENVMON_2_POWERSUPPLY_VOLTAGE
PLATFORM_ENVMON_2_POWERSUPPLY_CURRENT.
```

Review History

Table 6. Review History

Reviewer's Name	Version No.	Date
Bryan Hawkins	2	2009-01-31
Rizwan Mushtaq	3	2009-02-09
Paul Guarneri	8	2009-03-02
Rob Pavone	8	2009-03-05
Lew Colgan	9	2009-03-11
Ralf Wolter	9	2009-03-16
Ka Wai Ng	9	2009-03-18
Keith Sinclair	10	2009-03-31
Keith Sinclair	11	2009-04-16
Robert Fekete	13	2009-06-09
Matt Lewis	15	2009-07-03
Martin Holste	16	2009-07-12
Anton Chuvakin	17	2009-08-04

References

An Overview of the Syslog Protocol

<http://www.ciscopress.com/articles/article.asp?p=426638>

RFC 3164 - The BSD Syslog Protocol

<http://tools.ietf.org/html/draft-ietf-syslog-syslog-04>

Enterprise-Class Syslog Management

http://nms.gdd.net/index.php/Enterprise_Class_Syslog_Management

LogZilla E-Learning Videos

<http://www.logzilla.pro>

Cisco Debug Command Reference

http://www.cisco.com/en/US/docs/ios/11_0/debug/command/reference/dintro.html

Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3

http://www.cisco.com/en/US/docs/ios/12_3/configfun/command/reference/fun_r.html

Reliable Delivery and Filtering for Syslog

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_reliable_del_filter.html

Cisco Guide to Harden Cisco IOS Devices

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#logbest



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA

C11-557812-01 04/11