Network Monitoring and Logging Software

by Sophia

WHAT'S COVERED

In this lesson, you will learn about software tools for network monitoring and logging.

Specifically, this lesson will cover the following:

1. Network Monitoring

There are many ways to find out what's really going on within your network. Most administrators opt to directly keep tabs on network performance by looking at important factors like data rates and available bandwidth, using the many tools on the market designed to help with that.

When you hear people refer to things like load testing, connectivity testing, and throughput testing, they're talking about **network monitoring**. You'll also hear network monitors referred to as **protocol analyzers**.

Several third-party companies specialize in producing network monitors. One example is Fluke Networks, which makes some cool tools like the OptiView Network Analyzer. Microsoft had a graphical utility called

Network Monitor that could be used to capture network traffic. It is now retired, but you can still download it here.

TERMS TO KNOW

Network Monitoring

Observing the activity on a network in order to prevent or solve problems or optimize performance.

Protocol Analyzers

A tool that analyzes protocols to help solve problems, detect malware, and gather network utilization metrics.

1a. Packet Sniffing Revisited

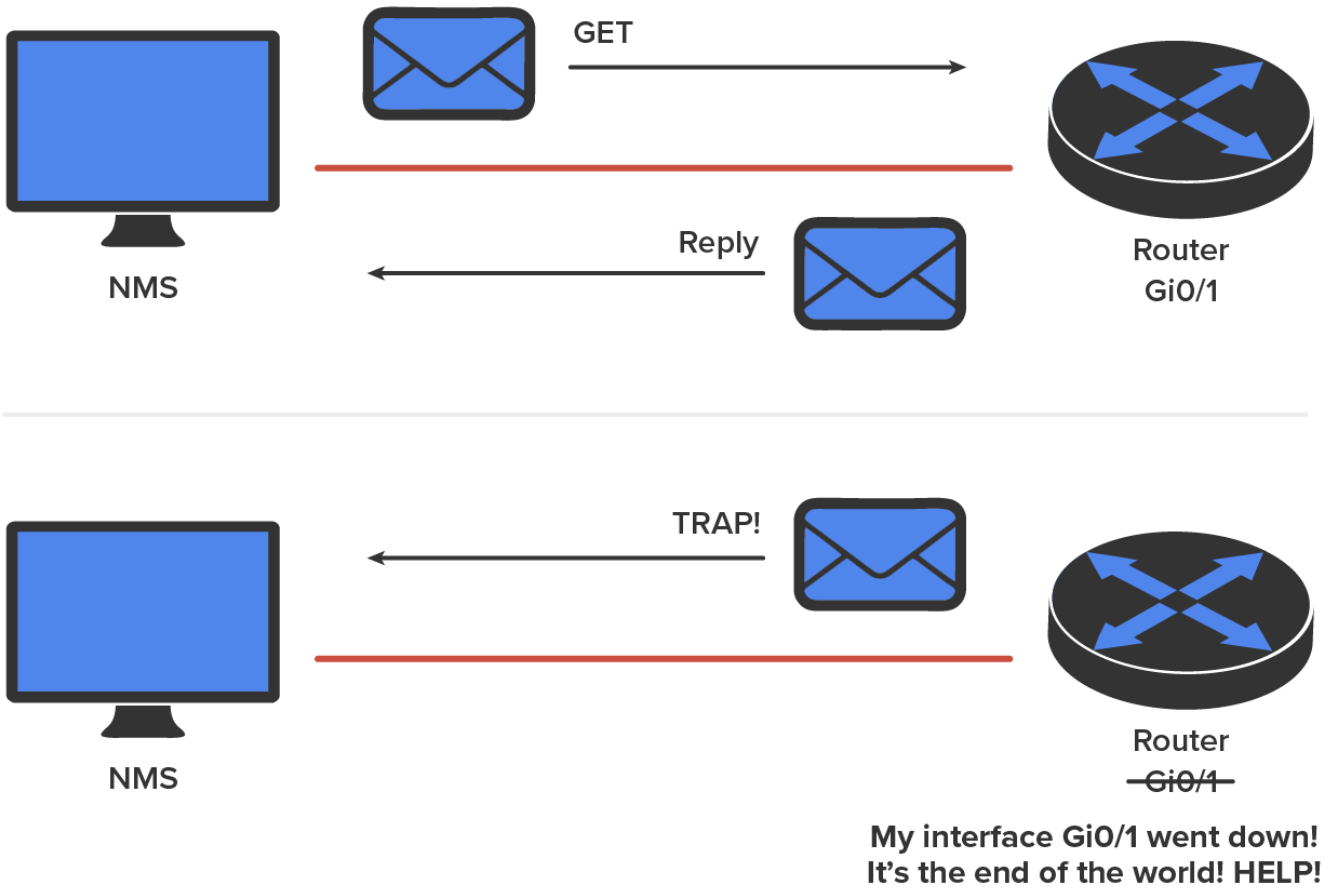
Some key network-monitoring tools and diagnostic utilities are software additions that run on an existing server operating system like Windows Server or Unix. Others are stand-alone hardware devices that you plug into your network. Both are versions of the packet sniffers we talked about in the previous tutorial.

Although it is true that hackers can and do use sniffers to capture network traffic and gather data for an attack, system administrators make good use of them too. And strange but true, being a bit of a hacker yourself can make you a much better system admin. Knowing your enemies and their methods can help you find the same holes they would use for evil, and you can use that knowledge to plug security holes and even optimize your network's performance.

1b. SNMP

Simple Network Management Protocol (SNMP) is an Application Layer Protocol that provides a message format for agents on a variety of devices to communicate with network management stations (NMSs), for example, Cisco Prime or HP Openview. These agents send messages to the NMS station. The NMS station then reads or writes information in the database. The information is then stored on the **management information base (MIB)**.

The NMS periodically queries or polls the SNMP agent on a device to gather and analyze statistics via GET messages. These messages can be sent to a console or alert you via email or SMS. The command `snmpwalk` uses the SNMP GET NEXT request to query a network for a tree of information. End devices running SNMP agents would send an SNMP trap to the NMS if a problem occurs. This is demonstrated in the figure below.



Admins can also use SNMP to provide some configurations to agents as well. These configurations are called SET messages. In addition to polling to obtain statistics, SNMP can be used for analyzing information and compiling the results in a report or even a graph. Thresholds can be used to trigger a notification process when exceeded. Graphing tools are used to monitor the CPU statistics of devices like a core router. The CPU should be monitored continuously, and the NMS can graph the statistics. Notification will be sent when any threshold you've set has been exceeded.

SNMP has three versions, with version 1 being rarely, if ever, implemented today. The table below shows a summary of these three versions.

SNMPv1	It supports plaintext authentication with community strings and uses only UDP.
SNMPv2c	It supports plaintext authentication with MD5 or SHA with no encryption but provides GET BULK, which is a way to gather many types of information at once and minimize the number of GET requests. It offers a more detailed error message reporting method, but it is not more secure than v1. It uses UDP even though it can be configured to use TCP.
SNMPv3	It supports strong authentication with MD5 or SHA, providing confidentiality (encryption) and data integrity of messages via DES or DES-256 encryption between agents and managers. GET BULK is a supported feature of SNMPv3, and this version also uses TCP.

TERMS TO KNOW

Simple Network Management Protocol (SNMP)

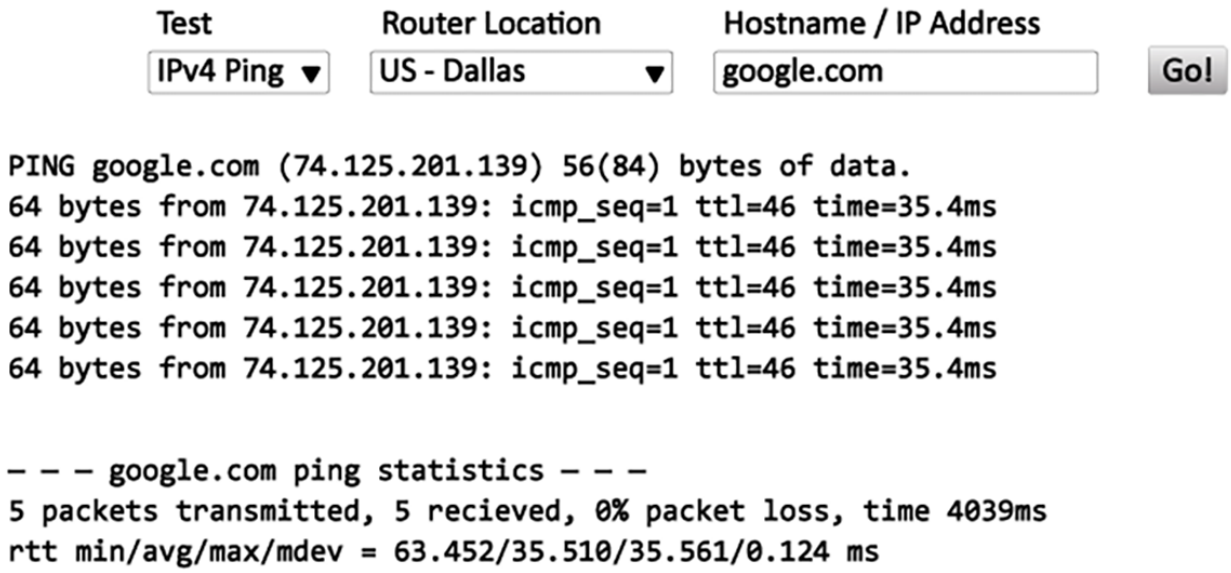
An Application Layer Protocol that provides a message format for agents on a variety of devices to communicate with network management stations (NMSs).

Management Information Base (MIB)

A database that stores information collected during network monitoring.

1c. Looking Glass Sites

You can access a **Looking Glass (LG) server** remotely to view routing information. These are servers on the internet that run Looking Glass software that is available to the public. The servers are essentially read-only portals to the routers belonging to the organizations running them. They provide a ping or traceroute from a remote location for you. The following figure shows output from a Looking Glass server.



TERM TO KNOW

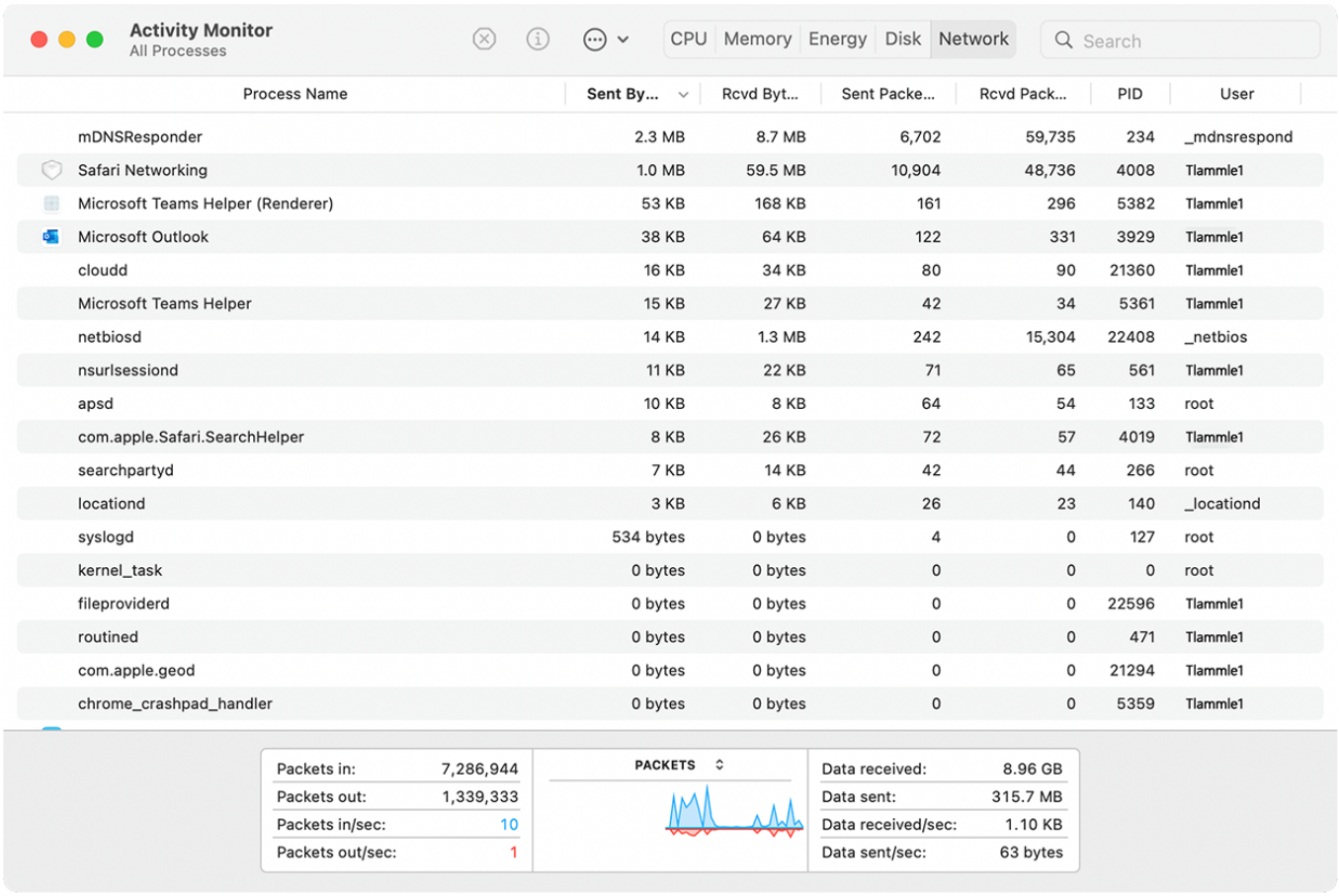
Looking Glass (LG) Server

A server on the internet that offers read-only portals to network infrastructure routers, providing ping or traceroute information.

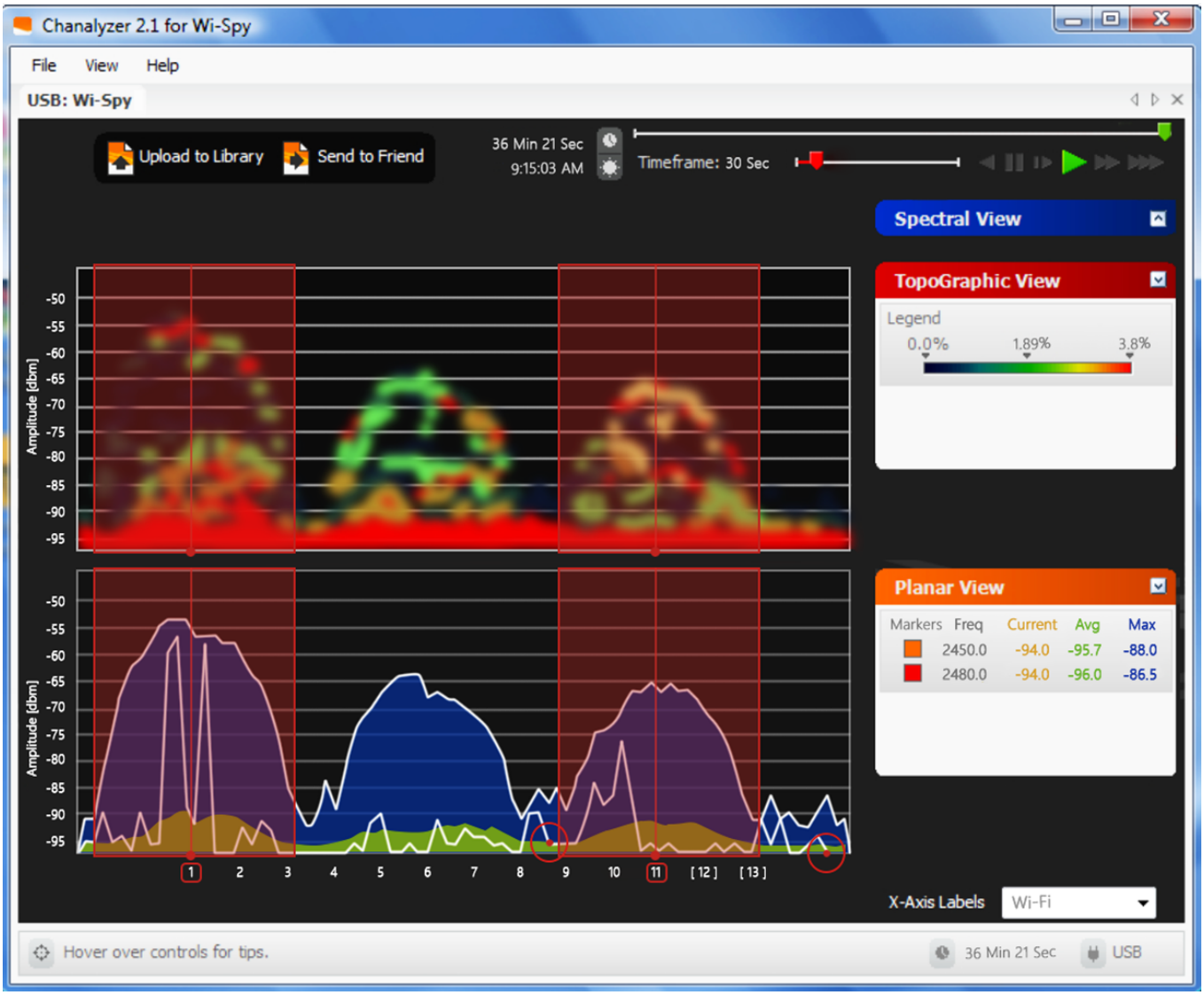
1d. Utilization Analyzers

Wired and wireless analyzers can show you the bandwidth used on your network segments or wireless area. There are tools to help you find the stats on storage, network device CPU, and device memory for your servers and hosts.

For example, if you have a Mac, you can use the built-in activity monitor, which provides the CPU usage, memory statistics, energy used by the applications, disk usage, and network bytes sent and received, as shown in the screenshot below.



In addition to utilization information for your hosts, servers, networks, and so on, you need information about the wireless channel utilization on your network. To get this information, you can use a wireless analyzer. The wireless analyzer in the following screenshot shows channel utilization information. Notice that three channels—1, 6, and 11—are in use.



1e. Protocol Analyzers

A protocol analyzer is often confused with a packet sniffer because some products really are both. Remember, a packet sniffer looks at all traffic on a network segment. On the other hand, a **protocol analyzer** (surprise!) analyzes protocols. These tools come in both software and hardware versions, but compared to the products discussed earlier, a network protocol analyzer is likely to give you more information and help than a sniffer will. This is because a bona fide protocol analyzer can actually help you troubleshoot problems, whereas most sniffers just provide information for you to have a ball deciphering.

A network protocol analyzer can perform the following functions:

- Troubleshoot hard-to-solve problems
- Detect and identify malicious software (malware)
- Gather information such as baseline traffic patterns and network-utilization metrics
- Identify unused protocols so that you can remove them from the network
- Provide a traffic generator for penetration testing
- Possibly even work with an Intrusion Detection System (IDS)

And the last function, and perhaps most important one for you, is that they can really help you learn about networking in general. This means if you just want to find out why a network device is functioning in a certain way, you can use a protocol analyzer to sniff (there's that word again) the traffic and expose the data and protocols that pass along the wire.

DID YOU KNOW

You'll find a whole bunch of network analyzers you can use for free at the following location: www.snapfiles.com/freeware/network/fwpacketsniffer.html. The terms "sniffer" and "analyzer" are used to define the same products found at this link. For example, both Microsoft's Network Monitor (NetMon) and Wireshark are called sniffers and analyzers, and they both are—at least to some degree.

BIG IDEA

When using any of the tools discussed in this tutorial, especially the network testing tools, collecting and comparing metrics over time is a valuable exercise. Once a baseline has been established for these metrics, you can determine when an issue has gotten better or worse over time. It also allows you to determine if measures you have taken to improve a scenario have worked. One of the key metrics for which a baseline should be established is network error rate. Since network errors typically lead to retransmissions, they typically result in reduced throughput, because each retransmission represents a lost opportunity to use that time slot to send new data.

2. Network Logging

Another good strategy for assessing a network's health and well-being is via the more indirect route of monitoring the logs that your server operating systems keep. A **log** is a written record of activity. These can help you spot problems on your physical network as well as services or applications that aren't running properly and could eventually bring the network or its resources down and make your users really unhappy.

TERM TO KNOW

Log

A written record of activity.

2a. Syslog

Reading system messages from a switch's or router's internal buffer is a popular and efficient method of seeing what's going on with your network at a particular time. But it's even more useful to log messages to a **syslog server**, which stores messages from you and can even time-stamp and sequence them for you. The following figure depicts a syslog server and client in action.

Syslog enables you to display, sort, and even search messages, all of which makes it a really great troubleshooting tool. The search feature is especially powerful because you can use keywords and even severity levels. Plus, the server can email admins based on the severity level of the message.

Network devices can be configured to generate a syslog message and forward it to various destinations. The following four examples are popular ways to gather messages from Cisco devices:

- Logging buffer (on by default)
- Console line (on by default)
- Terminal lines (using the terminal monitor command)
- Syslog server

All system messages and debug output generated by the IOS go out only the console port by default and are also logged in buffers in RAM. And routers aren't exactly shy about sending messages! To send messages to the virtual teletype (VTY) lines, use the terminal monitor command.
So, by default, we'd see something like this on our console line:

```
*Oct 21 17:33:50.565:%LINK-5-CHANGED:Interface FastEthernet0/0,
changed state to administratively down
*Oct 21 17:33:51.565:%LINEPROTO-5-UPDOWN:Line protocol on
Interface FastEthernet0/0, changed state to down
```

And the router would send a general version of the message to the syslog server that would be formatted something like this:

```
Seq no:timestamp: %facility-severity-MNEMONIC:description
```

The system message format can be broken down as shown in the table below.

`seq no`	Logs messages with a sequence number; As this does not get logged by default, you will have to configure it to get this output
`Timestamp`	Logs messages with date and time of the message or event
`Facility`	Logs the facility to which the message refers
`Severity`	Logs a single-digit code from 0 to 7 that indicates the severity of the message
`MNEMONIC`	Logs a text string that uniquely describes the message
`Description`	Logs a text string containing detailed information about the event being reported

The severity levels, from the most severe level to the least severe, are explained in the following table. “Informational” is the default and will result in all messages being sent to the buffers and console. If you are studying for your CompTIA Network+ exam, you need to memorize this table.

Severity Level	Severity	Explanation
Emergency	Severity 0	System unusable
Alert	Severity 1	Immediate action needed
Critical	Severity 2	Critical condition
Error	Severity 3	Error condition
Warning	Severity 4	Warning condition
Notification	Severity 5	Normal but significant condition
Information	Severity 6	Normal information message
Debugging	Severity 7	Debugging message

Understand that only emergency-level messages will be displayed if you’ve configured severity level 0. But if, for example, you opt for level 4 instead, level 0 through 4 will be displayed, giving you emergency, alert, critical, error, and warning messages too. Level 7 is the highest level security option and displays everything, but be warned that going with it could have a serious impact on the performance of your device. So always use debugging commands carefully with an eye on the messages you really need to meet your specific business requirements!

TERM TO KNOW

Syslog Server

A server that stores log information and can time-stamp and sequence messages.

2b. SIEM

Security information and event management (SIEM) is a category of software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications.

DID YOU KNOW

You can get this as a software solution or a hardware appliance, and some businesses sell managed services using SIEM. Any one of these solutions provides log security data and can generate reports for compliance purposes.

The acronyms SEM, SIM, and SIEM are often used interchangeably, but there are minor differences. SEM is typically used to describe the management that deals with real-time monitoring and correlation of events, notifications, and console views. SIM is used to describe long-term storage, analysis, and reporting of log data. And recently the term vSIEM (voice security information and event management) was introduced to cover voice data visibility.

SIEM can collect useful data about the following items:

- Data aggregation
- Correlation
- Alerting
- Dashboards
- Compliance
- Retention
- Forensic analysis

SIEM systems not only assess the aggregated logs in real time, they also generate alerts or notifications when an issue is discovered. This allows for continuous monitoring of the environment in a way not possible with other log centralization approaches such as syslog.

TERM TO KNOW

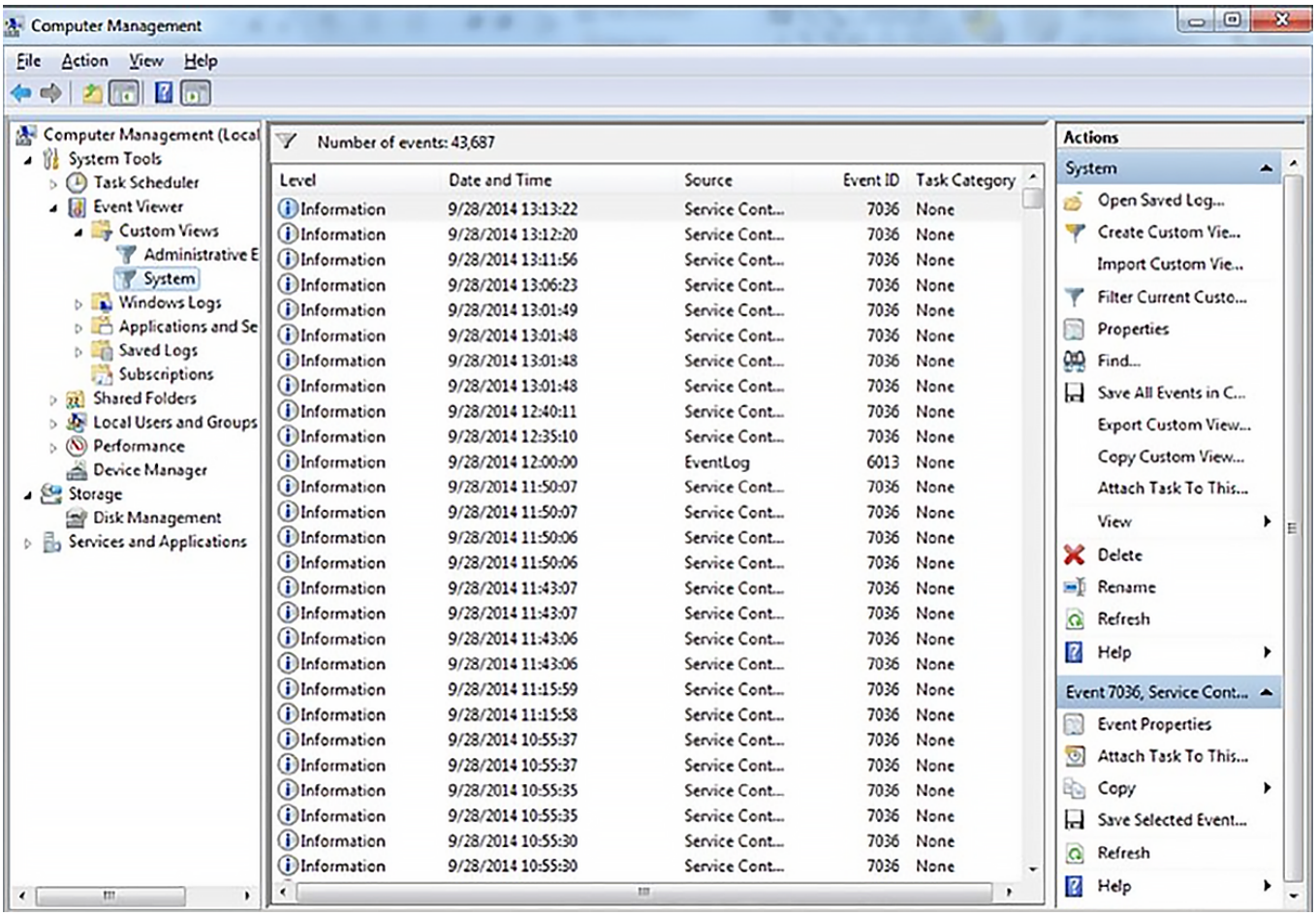
Security Information and Event Management (SIEM)

Software that provides real-time analysis of security alerts generated by network hardware and applications.

2c. Server Logs

Windows Server 2016 (and most other Windows operating systems) comes with a tool called **Event Viewer** which provides several logs containing vital information about events happening on your computer. Other server operating systems have similar logs, and many connectivity devices like routers and switches also have graphical logs that gather statistics on what's happening to them. These logs can go by various names, like history logs, general logs, or server logs .

The following screenshot shows an Event Viewer system log display from a Windows Server 2003 machine.



On Windows servers, a minimum of three separate logs hold different types of information. They are described in the table below.

Application	Contains events triggered by applications or programs determined by their programmers Example applications: LiveUpdate, the Microsoft Office suite, and SQL and Exchange servers
Security	Contains security events like valid or invalid logon attempts and potential security problems
System	Contains events generated by Windows system components, including drivers and services that started or failed to start

BIG IDEA

The basic “Big Three” can give us lots of juicy information about who’s logging on, who’s accessing the computer, and which services are running properly (or not). If you want to find out whether your Dynamic Host Configuration Protocol (DHCP) server started up its DHCP service properly, just check out its system log. Because the computer depicted above is configured as a domain controller, its Event Viewer serves up three more logs: Directory Service, DNS Server, and File Replication Service, for a total of six.

Windows 2000 Server and Windows Server 2003 came with System Monitor—another graphical tool used to create network baselines, provide performance logs, and identify bottlenecks. Windows Server 2008 R2 offered an optional monitoring and optimization tool called System Center Operations Manager 2010.

TERMS TO KNOW

Event Viewer
A Windows application that provides single-pane access to several different logs containing vital information about events happening on a computer.

Application
Contains events triggered by applications or programs determined by their programmers. Example applications include LiveUpdate, the Microsoft Office suite, and SQL and Exchange servers.

Security
Contains security events like valid or invalid logon attempts and potential security problems.

System
Contains events generated by Windows system components, including drivers and services that started or failed to start.

SUMMARY

In this lesson, you learned about software tools for **network monitoring** and logging. Network monitoring tools covered included **packet sniffing**, **SNMP**, **Looking Glass sites**, **utilization analyzers**, and **protocol analyzers**. **Networking logging** tools covered included **Syslog**, **SIEM**, and **server logs**.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)

TERMS TO KNOW

Application
Contains events triggered by applications or programs determined by their programmers. Example applications include LiveUpdate, the Microsoft Office suite, and SQL and Exchange servers.

Event Viewer
A Windows application that provides single-pane access to several different logs containing vital information about events happening on a computer.

Log
A written record of activity.

Looking Glass (LG) Server
A server on the internet that offers read-only portals to network infrastructure routers, providing ping or traceroute information.

Management Information Base (MIB)

A database that stores information collected during network monitoring.

Network Monitoring

Observing the activity on a network in order to prevent or solve problems or optimize performance.

Protocol Analyzers

A tool that analyzes protocols to help solve problems, detect malware, and gather network utilization metrics.

Security

Contains security events like valid or invalid logon attempts and potential security problems.

Security Information and Event Management (SIEM)

Software that provides real-time analysis of security alerts generated by network hardware and applications.

Simple Network Management Protocol (SNMP)

An Application Layer Protocol that provides a message format for agents on a variety of devices to communicate with network management stations (NMSs).

Syslog Server

A server that stores log information and can time-stamp and sequence messages.

System

Contains events generated by Windows system components, including drivers and services that started or failed to start.