VIGITRON

SNMP Vs SYSLOG

MONITORING
THE HEALTH OF YOUR NETWORK

DESIGN

INSTALL

VERIFY

Backgound

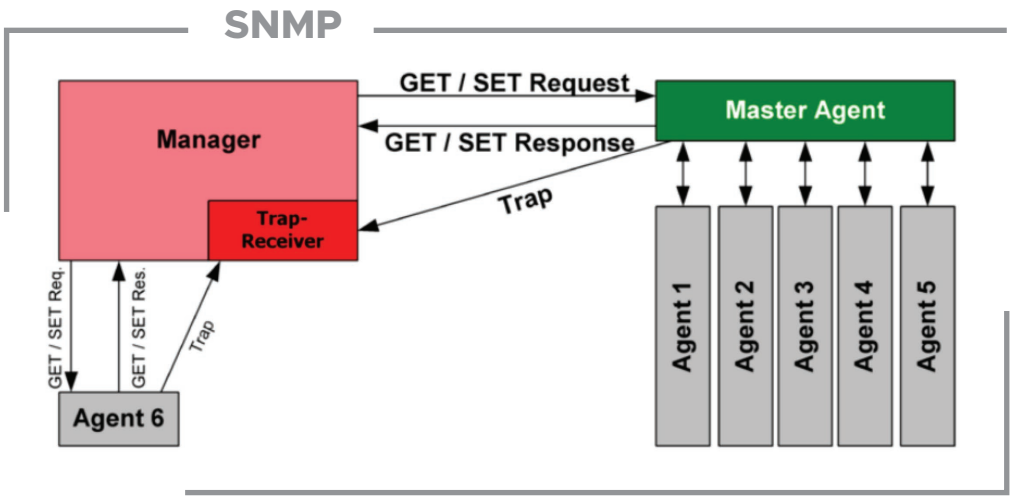
As security networks evolve and become more complex, there is an increasing demand for higher bandwidth, larger packet sizes, and Power over Ethernet (PoE) capabilities. These demands can put a significant strain on the network equipment, which may lead to equipment failures. The nature of these failures can be variable and depend on the performance requirements placed on the equipment during normal operation. Packet size and bandwidth requirements change with activity within a camera's viewing image. PoE increases as accessory functions such as Day/Night, Back Focus, LED turn on and PTZs are used. This changes result in network connected devices operate normally when in a "resting" stage but not when these other operating conditions are active.

Often, this results in mistaking blame for the failure on the connected device and sending it in for service, only for it to be returned labeled as "No problem found." As a result, there is prolonged system downtime, increased service costs, and no issue is resolved.

To avoid this, network monitoring is becoming increasingly more important in helping network managers and determine the nature of these problems.

How to monitor Network Status.

There are two methods for network devices to communicate their status. They are SNMP (Simple Network Management Protocol) and Syslog (System Logging Protocol). While both are considered standards, they operate very differently in their communication and complexity.



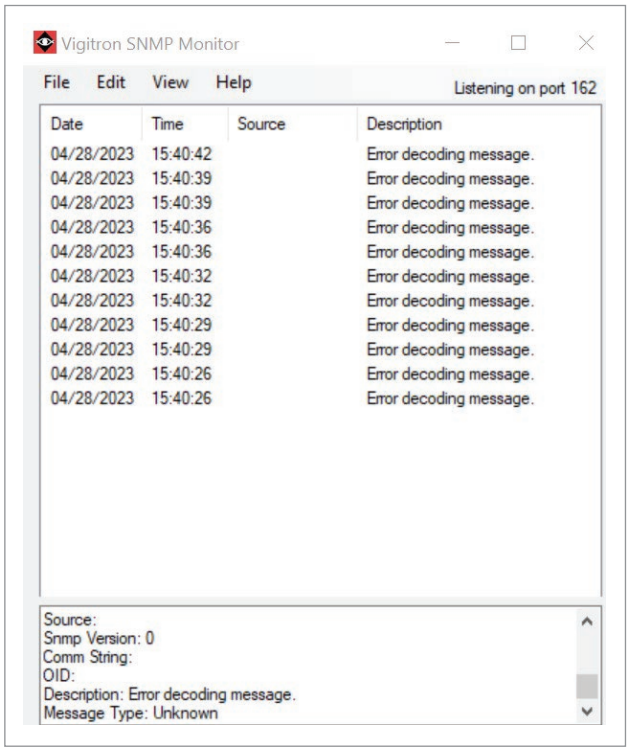
The internal standard protocol for SNMP contained in most managed network products can be anyone of three different versions; SNMPv1, SNMPv2, SNMPv3. Each defines the progression as SNMP developed. It is important the method of transmission must match the method of reception.

Complexity results from the data management contained within SNMP. This organization is contained within its Management Information Base (MIB). Communication is also bi-directional being transmitted on Port 161 and received on Port 162.

This results in the need to set up SNMP using several functions:

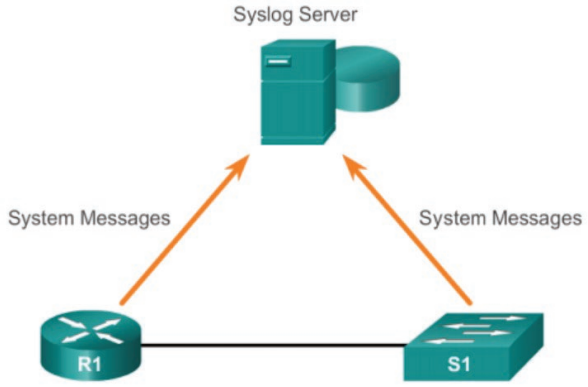
- SNMP
  - System
  - Trap
  - Communities
  - Users
  - Groups
  - Views
  - Access

The need of a specific MIB and its various formats means the receiver, usually in the form of SNMP Traps will not always be able to read the messages sent. The MIB must match between the transmitter and receiver. The result is an acknowledgement that a message was sent but a not the ability to read that message. This is known as a decoding error.



Syslog is Simpler

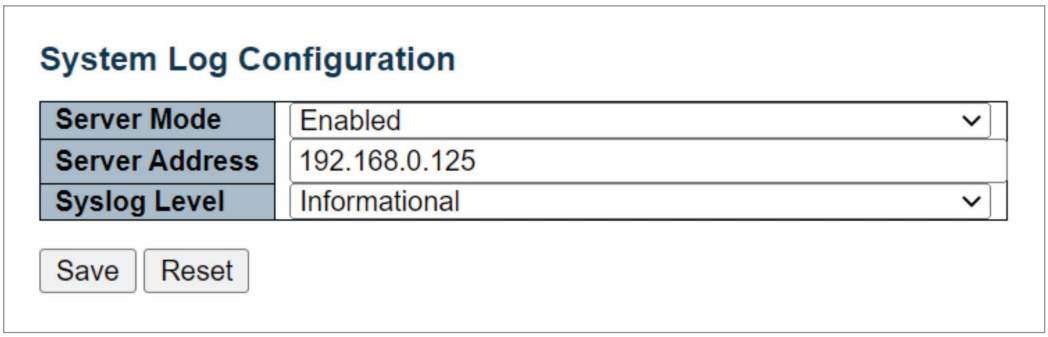
Syslog stands for System Logging Protocol and is a standard protocol used to send system log or event messages to a specific server, called a syslog server. It is primarily used to collect various device logs from several different machines in a central location for monitoring and review.



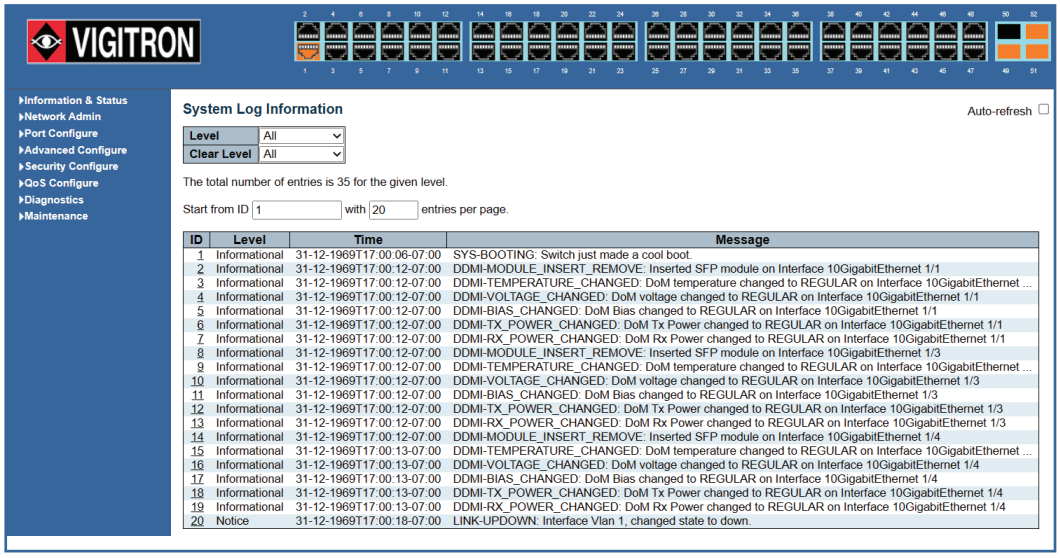
Syslog message routing is simpler than SNMP resulting in simpler set up and operation.

To start with Syslog messaging is transmitted over a single Port, that being Port 514 over a secure port 6514. Second, unlike SNMP most network managed devices record Syslog activity directly on the device itself.

Setting up is a matter of programming in the transmitting device and receiving computer/server.



It can even be simpler and in many cases when managed devices with Syslog capability record messaging directly on the device itself then, Viewing messages is simply a matter of accessing the devices' Graphical User Interface (GUI).



While there are no standards for the actual messages, many managed devices follow messaging format similar to the following:

Levels of Syslog

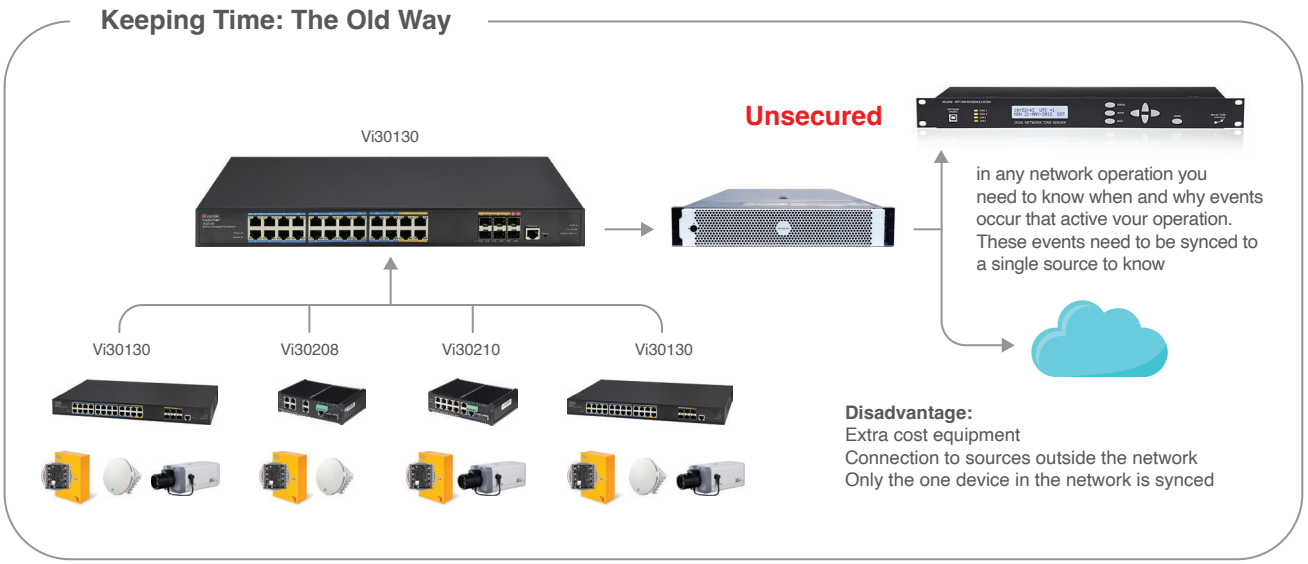
1. Emergency: system is unusable
2. Alert: action must be taken immediately
3. Critical: critical conditions
4. Error: error conditions
5. Warning: warning conditions
6. Notice: normal but significant condition
7. Informational: informational messages
8. Debug: debug-level messages

This means you can program Syslog messaging to only transmit a specific type of message helping to reduce the amount of message traffic.

The actual message contents transmitted by the connected device is also not standard. What is sensed, transmitted and the actual messaging itself is a matter of the firmware as determined by the device developer and is contained within the firmware.

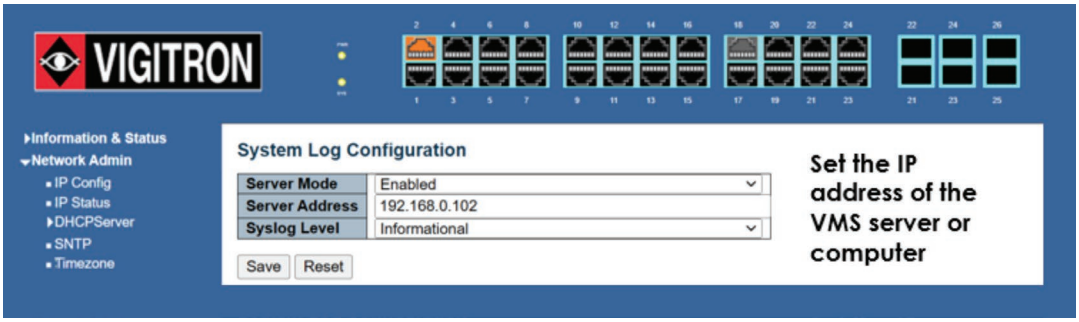
Other Syslog Considerations:

When something occurs can be as important as what has occurred. The problem is maintaining a system time and date reference. One method involves using NTP (Network Time Protocol). The problem is this requires synchronizing your system (main network switch) to either an internal NTP server or and external source over the internet. The former requires extra expenses in the form of purchasing an NTP server. The latter requires an external internet connection which raises security concerns.

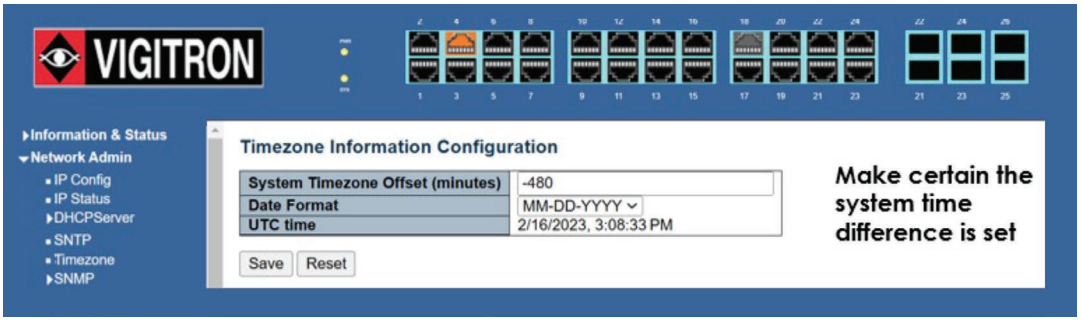


The Vigitron Solution:

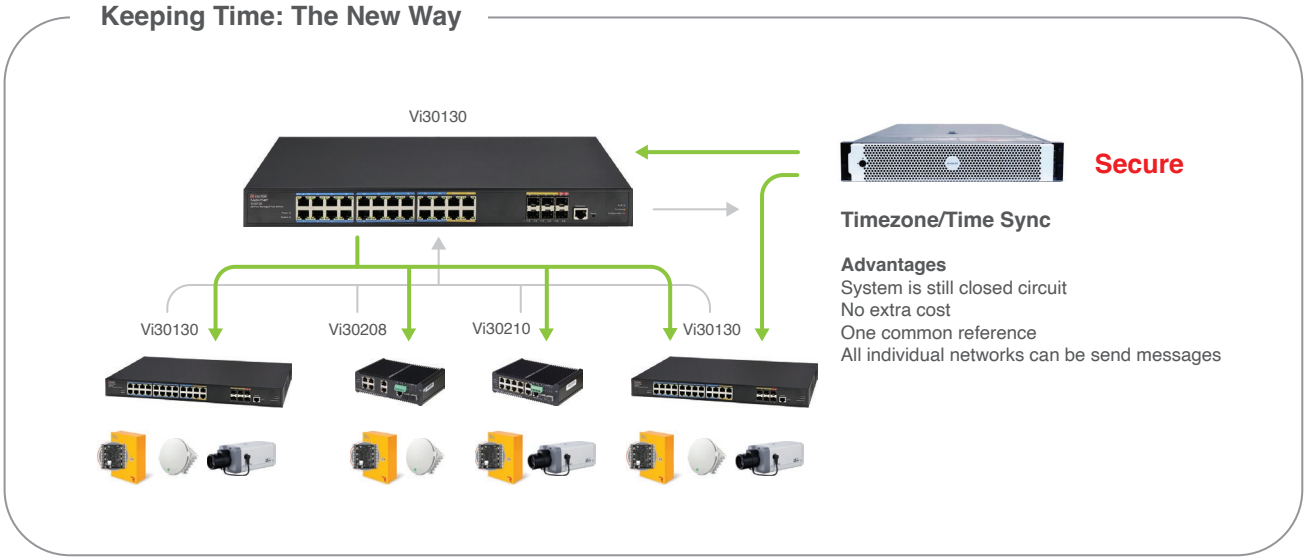
Vigitron's Enterprise level network switches all have Syslog programing features and are able to define the messaging level. Their GUI provides the ability to view the recorded messages both in total and as detailed individual messages.



In addition to programming the Syslog Level, messages can be directed to individual server address.



Unique to Vigitron's Enterprise level switches, is a Timezone setting feature. This references the time/date setting to the network's central computer. This is usually in the form of its computer or VMS server. The server address is the same as where Syslog messages are directed to. This system has several major advantages:

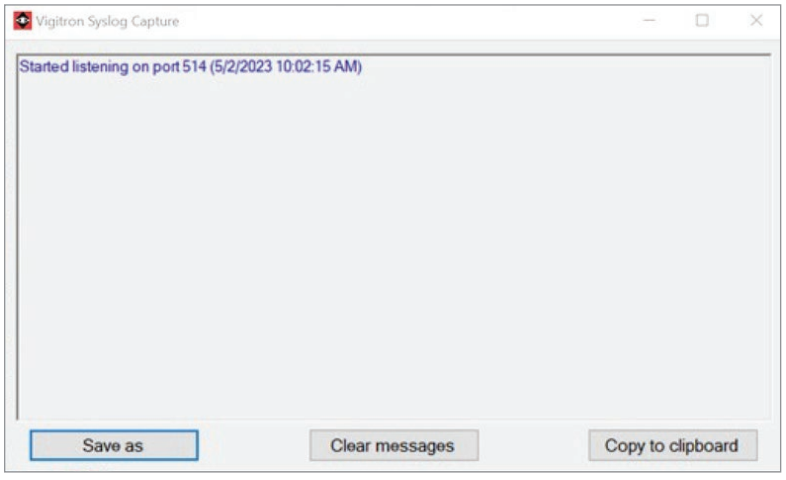


1. Security within the system is maintained as the time/date reference is completely contain within the system with no external reference is required.
2. No extra cost is required.
3. Each connected device within the system with TimeZone capacity can be individually time/date synced to the same source.
4. Vigitron programming also provides naming conventions to both the individual device and in some cases the individual port connection.
5. The result is an easy to identify messaging containing location, time/date and event information.

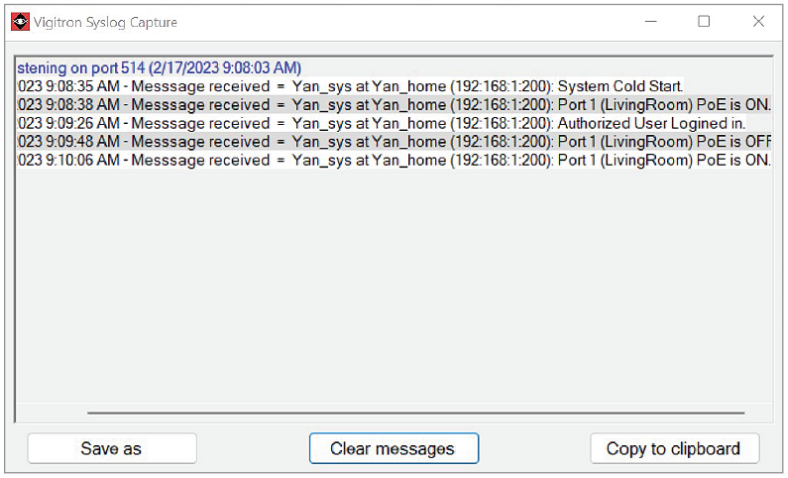
Maintaining the log:

The ability of a connected device to display and retain the number of messages is dependent upon its memory. At some point there are limitations and usually the system will replace the oldest messages with newest.

Another method to maintain and even print out a syslog can be achieved by using Vigitron's SysCap™ program. When installed and active the program will link to port 514 and be ready to receive messages from the connected device.



Received messages can be "Saved" or copied to a computer's Clipboard:



Received messages can be “Saved” or copied to a computer’s Clipboard:

Download SysCap™ →

SysCap™ is part of Vigitron’s software suit which includes NetObserver™ for monitoring up to 240,000 IP address and NeTester™ for evaluating and troubleshooting.

Vigitron offers free and without obligation network design services providing the most reliable and cost-effective network solution for your specific requirement. Our Design Center is staffed by experienced design engineers who can work with your staff as required. To request design services, email us at support@vigitron.com or visit our website www.vigitron.com.

Vigitron’s Design Center →

VIGITRON

Headquarters

7810 Trade Street, Suite 100,
San Diego, CA 92121
United States

Phone: 858 484 5209
Email: info@vigitron.com
www.**vigitron**.com