The ABCs of Diagnostics

Managed switches provide many features. Some of these features can be used to help monitor the state of the network and can help diagnose problems when they occur. These features include SNMP, Port Monitoring and Port Mirroring.

SNMP Protocol

SNMP (Simple Network Management Protocol) can be used to monitor the network communication statistics. For example, SNMP can be used to display the link status of each port of the switch, the number of messages received/transmitted by each port, the number of errors received by each port, and much more.

For more information about SNMP see **http://www.ccontrols.com/pdf/abc11.pdf**.

Network Management Station (NMS) applications can be used to display the SNMP information captured on each managed switch and other SNMP supported devices. Applications such as iSNMP™ can be used to make this information available to OPC-compliant HMI applications such as Wonderware's Intouch, Rockwell's RSView, etc. By using this software, the network status can be displayed along with the entire system status on one HMI screen.

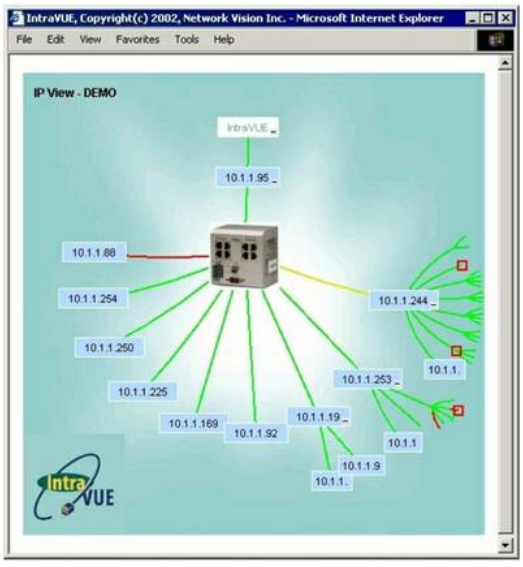

Figure 1

Another application, IntraVUE™, uses SNMP information to automatically create an active, graphical, network map (see Figure 1). This map is automatically updated when devices go offline or online. IntraVUE also logs problems with network devices.

Some of the diagnostic information provided via SNMP can also be provided directly from the managed switch. This can viewed from console screens (see Figures 2 & 3) or via a web browser (see Figure 4).

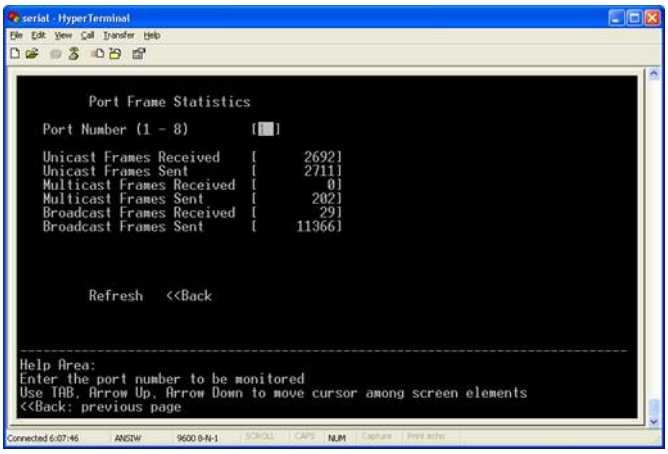

Figure 2

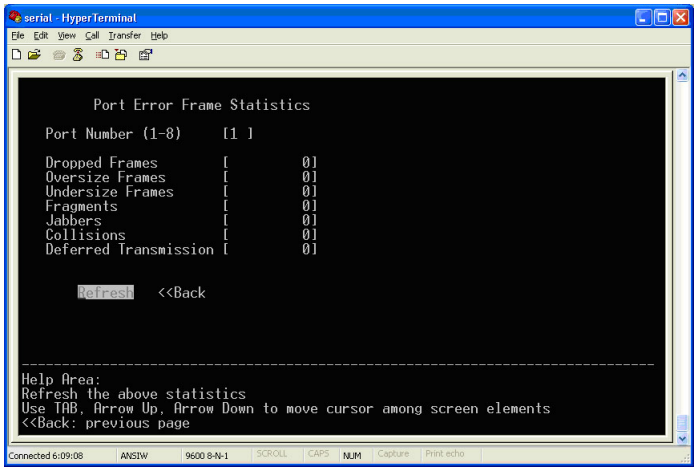

Figure 3

Port Packet Statistics	
Unicast Packets Received	8449
Unicast Packets Sent	7785
Multicast Packets Received	0
Multicast Packets Sent	246
Broadcast Packets Received	58
Broadcast Packets Sent	12870
Dropped Packets	0
Oversize Packets	0
Undersize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Deferred Transmissions	0

Figure 4

Port Monitoring

Port Monitoring allows the managed switch to monitor selected ports for proper link status. If a monitored port loses link, a fault relay is engaged. An SNMP trap is also sent to the network SNMP trap receiver. NMS applications such as iSNMP can receive these traps. Any port which should not have a link can also cause the fault relay to be engaged if a link becomes present. This can be used to monitor for improper connections being made to a switch. The contacts of the fault relay can be directly connected to the control system as a standard contact closure input. The control system can then make appropriate decisions based on the link status of specific ports. For example, the control system may need to enter a safe state if a device which connects to the switch loses its network connection.

Port Mirroring

Port Mirroring allows a protocol analyzer or “sniffer” to receive all traffic from a selected group of ports. Switched networks provide efficient use of bandwidth by only passing messages to those parties in the conversation, however, one side effect of this is that protocol analyzers cannot receive all messages sent through the switch. For example, if a file is being passed between ports 1 & 2 of a switch, the rest of the ports will not see this traffic. If someone needs to capture this traffic for diagnostic purposes they will only be able to so by the use of port mirroring.

Port mirroring allows the switch to “copy” traffic sent/received on selected ports to one “mirror” port. The protocol analyzer is then connected to the mirror port so that it can receive all of the traffic sent/received between selected ports. On some switches all traffic from all ports can be copied to the mirror port — provided this traffic does not exceed the available bandwidth of the mirror port.

There are many Ethernet protocol analyzers available. One popular analyzer is Ethereal (**www.ethereal.com**). One reason for its popularity is that it is an open source application which is freely available from ethereal.com. For more information about Ethereal see **http://www.ccontrols.com/pdf/abc8.pdf**.

Protocol Analyzers are useful tools when diagnosing network problems. Even if you are not an expert in networking you can still understand some network problems when using protocol analyzers. Also you can send the information captured by your protocol analyzer to your equipment supplier so they can better understand your problem. We have authored a document which can help you understand the information that Ethereal provides even if you are not a networking expert **(http://www.ccontrols.com/pdf/abc5.pdf)**.