

Ethernet based Software Tools allow Control Technicians better visibility

As Ethernet becomes a common carrier of not only business information but also a core element in Foundation Fieldbus HSE, EtherNet/IP, ModbusTCP and PROFINet there will be an explosion of devices with TCP/IP addresses. Software to assist the non-IT professional's support of these devices will be very important to ensure availability and peak performance. The ease at which one can deploy devices using Ethernet may also create issues as to the current status and structure on an existing network. The ability to select not only industrial grade equipment but also commercial and even consumer class equipment may also create challenges for real time networks. The following article will discuss three common issues facing the controls department as Ethernet deployment continues.

- Identifying what is currently on the network.
- Identifying situations in which bandwidth is consumed.
- Identifying hard or intermittent failures and providing quick recovery

Device Discovery, Mapping & Documentation

A major issue with resolving network problems, whether Fieldbus or Ethernet, is to get an accurate understanding of everything that is connected to the network. The ease of connecting devices to Ethernet makes the job of accurately knowing what and where all of the devices that are connected difficult. Software is now available that not only auto-discovers the devices but can auto-map the interconnection details that typically take hours to verify and document.

The following picture shows a newly discovered network with all IP addressable devices and their interconnections. Many software solutions claim to auto-discover devices but only place the devices in a table. The ability to auto-map is important for applications that have more distributed devices that may be placed into a number of separated electrical enclosures. Since many applications may also contain hubs or unmanaged switches the software adds these devices automatically. Sensing that more than one device is connected to a managed switch the software adds the device (auto inserted node). Color-coding allows for details such as proper communications, warning and alarm conditions. The overview makes it easy to oversee the entire network on a single screen.

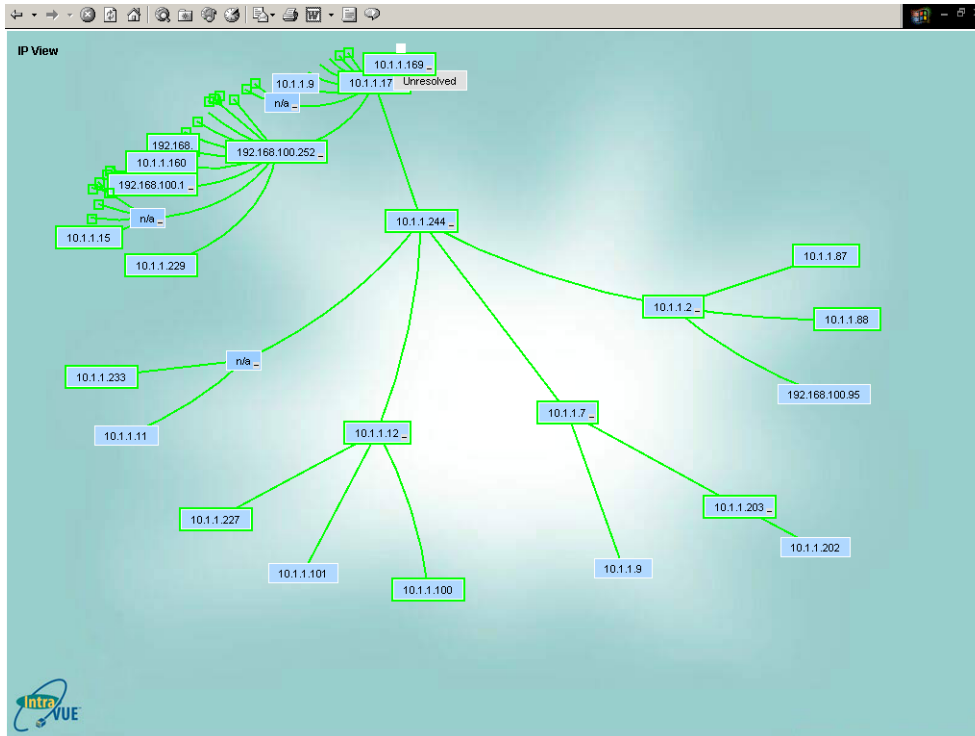


Figure 1. The auto-discovery and auto-mapping of an Ethernet Network

Individuals that have used the Auto-discovery and Auto-mapping function as a tool on their laptop have indicated that they will not go to a new site for troubleshooting without it. The Auto-discovery and mapping techniques have also allowed the software to quickly identify duplicate addresses (IP or MAC) that are on the network. Since most addressing is fixed the occurrence of an accidentally duplicated address is a too frequent problem that can takes hours or days to resolve.

The ability of the software to save the information in a file which can be restored at a later date allows individuals who make frequent service calls to know exactly what has changed on the network since the last time they were there. Networks that are stored can also be brought up and analysis done back in the office. This capture of the actual network allows for greater planning and design of future expansions. The software can also generate reports and spreadsheets indicating the device information coupled with connection information. The event logs can also be put into a report with the ability to not only identify which device is misbehaving but the frequency of the events as well.

Bandwidth and Intermittent problems

The ability to use an Ethernet for a number of different applications makes it the ideal infrastructure network. Since most devices are now being supplied with Ethernet ports the ability to use the connection for interfacing to HMI/SCADA, Programming or Configuration, and Peer-to-Peer communications is becoming commonplace. The

increased usage by a variety of applications coupled with the use of multicast data will put different loads on the network at different times. This coupled with environmental factors such as heat, humidity, vibration, and noise can create unexplainable issues that may appear and disappear.

In the following example a service technician had connected his programming panel to an open port on a switch and downloads the program to the PLC. Without being aware of the data path the connection will take, they assume that as long as the program is loading everything is fine. However the communications disrupts streaming data from another device in another application. Timeouts and sluggish responses to an operator station are a result and by the time someone starts to investigate the program load is completed and communication is back to normal. This may happen as more devices are connected this will be a growing problem.

IntraVUE software, which has been designed to resolve these problems, can also be integrated into most operator stations. Residing in an application such as Active-X the operator can get an alarm and push a button to bring details of the actual network. As seen in the following diagrams IntraVUE can be integrated into most of the popular HMI and SCADA packages.

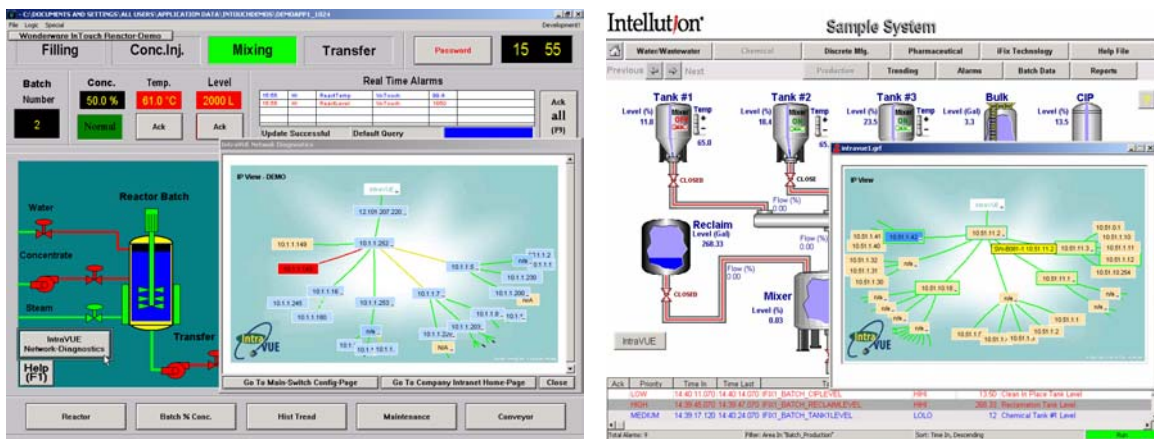


Figure 2. IntraVUE embedded in iFix and InTouch software

In figure 3 you can see that a newly added device (tan box 10.1.1.227) has been added to a network and communication between the device and a PLC (10.1.1.9) have exceeded the preset limits (indicated by yellow lines) of the network. The excessive communication has caused intermittent communications at a device (10.1.1.8), which will show a red and then green line indicating intermittent communications problems. An event log will also monitor the entire event sequence including the new device added with time and name and port connected to. The bandwidth alarms and intermittent communications of the device will also be logged. The ability to provide a graphical view to allow a quick observation and easy identification coupled with a event log to review

the sequence at a later date is important to solving many of these difficult to find problems.

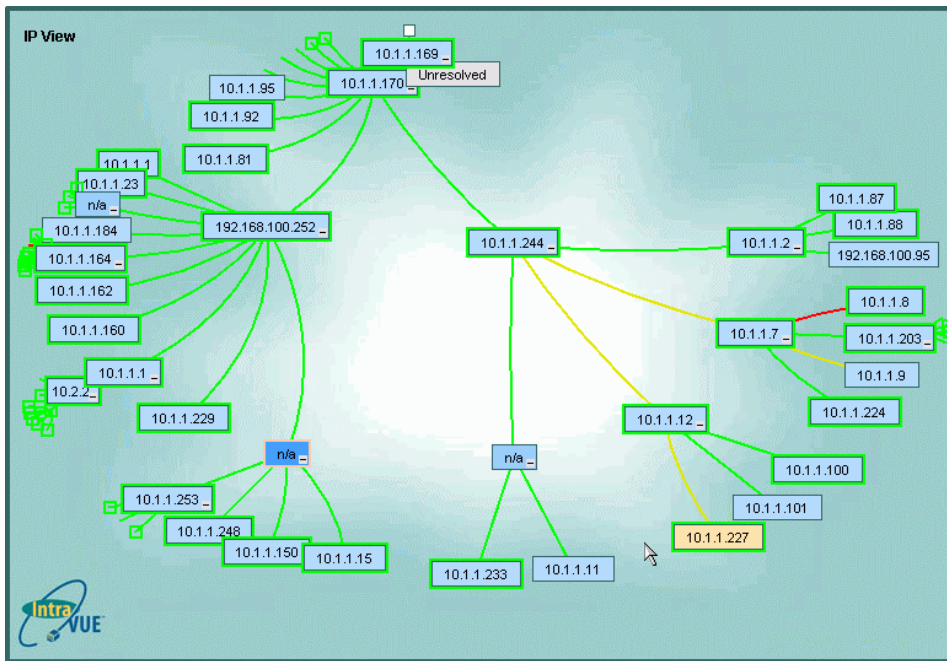


Figure 3. Overview provides a clear picture of cause and effect on the network.

Intermittent problems can also be caused by connection or device problems. These problems that do not provide a hard failure and loss of communication are also difficult to track down. In many networks they are happening without the user even being aware that they are occurring. Have you ever experience the network appearing to slow down at times? The robustness of Ethernet and the retry mechanism are covering for and preventing message loss but eventually if the losses become great there will be losses of data or significant time-outs.

Quick device recovery

The ability to quickly and accurately replace a failed device is an other important consideration. This is complicated in the industrial space as many devices are required to have fixed addresses. Since several systems are accessing data from them it is important that the address remain fixed. Your computer acting mostly as a client and not providing continuous data to another system can be given an address from a pool of addresses. This is known as DHCP (Dynamic Host Configuration Protocol) and is commonly used in most offices. This automatic address management system would cause major problems with fixed IP devices. To set a fixed IP address on need to connect a serial cable or a

point-to-point Ethernet connection using a Boot-P server. Both cases require manual intervention and present the possibility of an error in addressing.

Software now called Auto-IP from Network Vision essentially acts as a DHCP server with all of the ease of use but specifically targeting fixed IP devices. The software monitors the section of the network it is configured for. There can be redundant systems monitoring the same network for added security. If a device fails the technician is only required to obtain the replacement unit and then first plug in the network cable and then power up the unit. The device will send out a request for an address and the Auto-IP software will detect the request and identify the location at which the request is coming from. It can be set to also ensure that the vendor ID is also a match and with the correct information and if the original device has not been moved will respond with the address of the failed unit. After receiving the address the software can also initiate a configuration file transfer and configure the unit to the settings of the previous unit. The ability to automate the process will greatly improve the security and reduce address errors.

Conclusion

Automation Software targeted at Ethernet devices and support of the various applications and services is now available for non-IT people. The ease of use and integration into other applications will provide controls people the necessary tools to provide level one support of the large number of devices being deployed in the plant. From process applications, Power Management, Water Treatment, Pipeline and Tank Farm the use of Ethernet is gaining unique support from software such as Network Vision's IntraVUE.

For more information contact Network Vision at 978 499-7800 or info@intravue.net
Visit www.intravue.net