



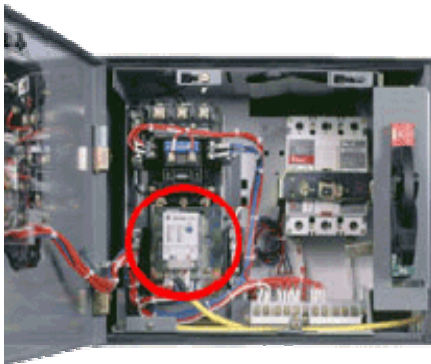
## *IntraValue*

### The *Financial* benefit of IntraVUE

In today's economic environment it is important to ensure that any purchase provides a financial return, no matter how technically attractive it may seem. Gone are the days of acquiring the latest and greatest only to discover that the costs cannot produce a justified return on investment. This can be especially true regarding software where, not only the initial purchase price, but also the added resource cost to deploy, can be much higher than the achieved financial savings.

As Ethernet networks bridge the front office with the factory floor, it promises to reduce the complexities and improve responsiveness by interfacing directly to production equipment, creating a common network infrastructure that transcends the office onto the plant floor. Adapting Commercial and Enterprise software systems to the factory floor has been one of the most difficult areas. Trying to leverage and/or utilize the current network support software developed for enterprise computing and server applications may not, however, be the answer, as these packages may cost more in deployment than targeted software geared toward plant technicians. The following highlights the cost savings of IntraVUE, a package specifically targeted at supporting plant floor equipment Ethernet TCP/IP connections.

The plant floor is a much different environment with a great deal of focus on the end devices (PLCs, robots, power management, and drives). As Ethernet moves to replace proprietary communications on the plant floor, it is a costly mistake to assume that network support software used in the enterprise computing area can be used as a cost effective solution for the plant floor devices. There are several reasons for this, such as:



A majority of problems on the plant floor will be associated with connection or connected device failures. Some studies indicate that close to 80% of plant floor problems are device or connection related. The harsh environment with vibration, heat, humidity, dirt and electrical noise degrading the life of components is a major cause of these early failures. Industrial equipment with Ethernet connections are unfamiliar to IT and network specialists. Some of this equipment is connected to high voltage and may be running production equipment.

Figure.1 Motor Control center with an Ethernet connection



The time to respond to a problem if the individual is not resident on the plant floor will mean additional down time. Response time even for simple problems may result in an additional delay of one or two hours. The main cause being that the Ethernet devices are not located in an easily accessible area or centrally located in an IT closet, but rather distributed in electrical enclosures on the plant floor. During this time, the process or machinery may also be down awaiting resolution or replacement.

It will also be important to use the appropriate resource to address basic networking or device connection problems. This will reduce the need to tie up valuable IT / Networking specialists on these local device or connection problems. The plant floor personnel, if given the proper tools, can be an extremely cost effective resource.

IntraVUE automatically discovers, displays and documents the TCP/IP devices of the network. The key emphasis of IntraVUE is support of the large variety of IP addressable devices with a very easy to use tool. A tool that can be configured to not only easily highlight the device, provide all the necessary information to support or replace the device, but actually automate a secure system for the actual device replacement.

Analyses of costs show that there are three basic stages in the deployment of a network solution.

***Initial design and installation***

***Routine maintenance and documentation***

***Device failure identification and recovery***

The following areas will be covered and details of the savings of each are outlined in the material below. The figures are developed from information retrieved from several active applications. It is used to provide a baseline for cost savings pointing out the intended "Value Proposition" of IntraVUE.



## Initial design and installation

### Network discovery, layout and design

Since Ethernet network infrastructure may already be installed, IntraVUE can be deployed initially to connect to the existing network to discover and map the current “AS-IS” state, providing not only a list of devices but their actual connection layout. The ability of this automatic layer-2 mapping is very unique even for IT software packages. Drawing the point to point connections on a single display and using hyperbolic display techniques also simplifies navigation and viewing of the actual connections of hundreds of devices.

The IntraVUE map can be used in an off-line mode allowing this information to be taken back to the office for planning. The back-up of the network capture can be sent to other individuals (OEMs or System Integrators) for their review. Details including current network traffic are captured and viewable in this off-line mode. The ability to manually add devices can allow the user to configure new components and connection information on to an existing network layout. This method allows all involved to see the requested additions and changes as they may appear once connected.

Cost associated with performing a network layout and connection drawing vary but on average will cost \$30 per connection. A 100-device network (10 computer workstations, 15 switches, 10 hubs, 2 routers, 63 IP addressable devices) with two connections per device will cost \$6000. The ability to use the network capture as a layout tool is an additional \$800 package not including the cost to add your configuration to the drawing package. This cost is greater than the cost of an IntraVUE package and many people have justified the package on this feature alone.

### Documenting acceptance test

Many systems are staged in a separate location and then, after an acceptance test proves the system’s ability to meet the functional requirements, are shipped to the final location. The process of reinstalling the system at the final location requires reconnecting the equipment. Time is spent ensuring that the final system is configured exactly as tested. The ease of Ethernet connectivity allows individuals to connect different ports. These errors may cause performance issues (moving a connection from a full-duplex to half-duplex) or service problems later when the wiring documentation does not line up with the connected equipment. These issues are subtle but can cause confusion and hours of additional delays when a problem arises.



IntraVUE can capture the system as accepted and stored. In this way, System Integrators or OEMs can archive every system built and shipped. These backups can then be used at the final location to indicate if every connection is accurate as well as any new device that may have been added to the system. IntraVUE will graphically display all devices that have been moved with an indicator of the original location as well as the new location. This is done in minutes, allowing the process of system checkout to be greatly simplified. The costs of the checkout vary by application. In applications in which the distances between devices are great, many have calculated that these costs are much greater than purchasing IntraVUE for this specific application.

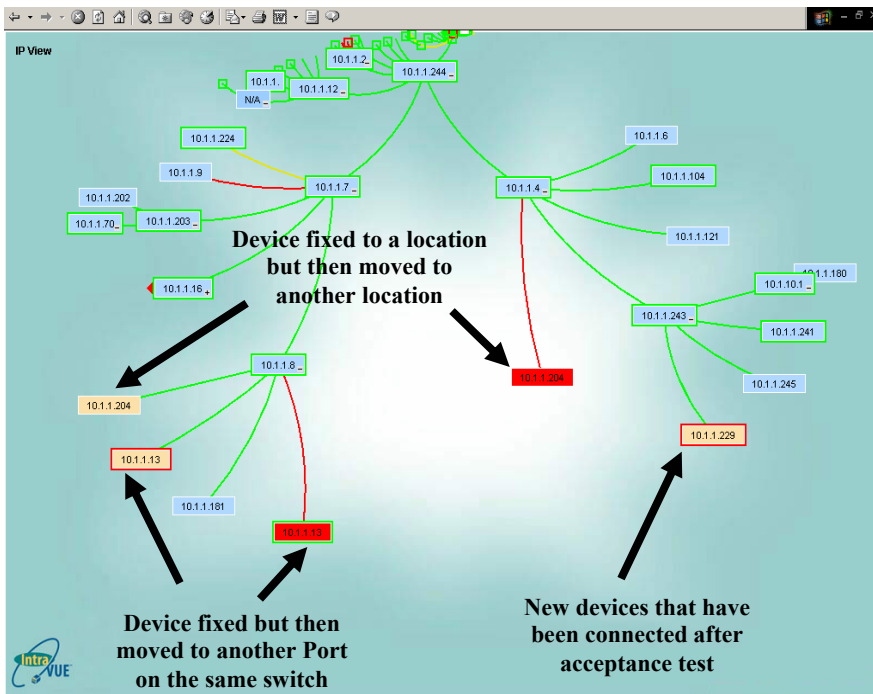


Figure 2. IntraVUE highlighting changes between acceptance test and installation

New devices that have been added to the network are also the cause of problems that can be initially blamed on the original system installed. Having the ability to highlight newly connected devices can quickly separate issues. The typical issues created by newly installed devices can be as simple as creating additional traffic and affecting currently operating equipment.



The ability to use IntraVUE as a verification tool will save many hours as well as providing assurance that the system initially accepted is connected accurately. System validation, which is done in the field or on the manufacturing floor, is very expensive and can cause unnecessary delays in the start-up.

Even if all the connections are properly made to the right location, there are other issues that can arise during the installation of equipment. In a recent project at a manufacturer, IntraVUE had uncovered many grounding and connector problems that were causing devices to have intermittent communication failures in a matter of minutes. Before IntraVUE was installed they had spent weeks with network sniffers without much success. IntraVUE provides a system that is continually polling devices to check their connection status. This system-wide approach provides an overview of all devices and can allow someone to drill down to the potentially affected devices. Many tools are point tools and require individuals to know exactly where to start looking and sometimes require the individual to be at that connection. In systems with large geographic areas this creates greater difficulties.

No	IP Address	Date	Description	Type
1979	10.1.1.101	01/19/2004 13:54:26	Device 10.1.1.101 reconnected with new mac addr 00 00 54 10 35 05 (no name)	Conn
1976	10.1.1.101	01/19/2004 13:44:47	Device 10.1.1.101 disconnected (00 30 DE 00 15 1A, no name)	Conn
1974	10.1.1.101	01/19/2004 13:44:19	Device 10.1.1.101 reconnected (00 30 DE 00 15 1A, no name)	Conn
1972	10.1.1.101	01/19/2004 13:44:04	Device 10.1.1.101 disconnected (00 30 DE 00 15 1A, no name)	Conn
1968	10.1.1.101	01/19/2004 13:42:55	Device 10.1.1.101 reconnected (00 30 DE 00 15 1A, no name)	Conn
1967	10.1.1.101	01/19/2004 13:42:51	Device 10.1.1.101 disconnected (00 30 DE 00 15 1A, no name)	Conn
1964	10.1.1.101	01/19/2004 13:42:03	Device 10.1.1.101 reconnected (00 30 DE 00 15 1A, no name)	Conn
1961	10.1.1.101	01/19/2004 13:41:58	Device 10.1.1.101 disconnected (00 30 DE 00 15 1A, no name)	Conn
1959	10.1.1.101	01/19/2004 13:40:42	Device 10.1.1.101 reconnected (00 30 DE 00 15 1A, no name)	Conn

Figure 3 Event logs clearly identify devices that are having problems

### Quickly finding Duplicate Device addresses

Installing new equipment to an existing network has created additional issues in which IntraVUE has proven its value. The use of fixed IP addressing in closed networks (private networks) in which common address ranges can be used is a standard practice. One of the major features of IntraVUE is its ability to help identify when either duplicate IP or MAC addresses have been used on a network. These are difficult and time-consuming problems that create performance problems at the least and safety problems in the most serious of cases. Since devices use IP or MAC addresses to indicate who they are, if another device sends information and is interpreted wrongly, the data from the device may mislead the systems they are feeding data to.



By continually monitoring the addresses and locations of devices, IntraVUE has the ability to find these problems appearing as devices changing or alternating addresses. The time required to find affected devices can be days and may only appear randomly. Cost of identifying these problems can be in the thousands of dollars not to mention the cost if the data affects the process or machinery.

If we consider that 5% of the connected devices may have connection problems, then a 120-node system will have 6 bad connections. A time per connection that covers the identification of the appropriate connection and confirmation that communication is active after changes are made is about 4 hours based on the distribution of devices. For a 128-node network this can mean about 24 hours of effort. IntraVUE's visualization will reduce this searching to 15 minutes per connection, cutting 90% of this activity. The dynamic real-time display will keep everyone updated to the actual changes taking place and indicate immediately that communication is occurring. IntraVUE is found to be optimal for a distributed network topology with an emphasis on both switches and edge IP addressable devices.

**Savings in installation assistance** 21.6hrs x \$120/hr\* start up costs = \$2592

\*Typical installations require two individuals for troubleshooting wiring.



## Routine maintenance and documentation

The majority of problems experienced on a running network are caused by simple connection problems created by vibration or individuals working on other equipment near the Ethernet device. Another common problem is the intermittent communication failures caused by degrading devices. Such problems appear as a slowdown of the network only to ultimately fail completely, typically at the worst possible time. IntraVUE runs continuously 24 x 7 and identifies immediately when a device fails to communicate or starts to randomly fail. These failures may start out infrequently, only to accelerate with age and quality of equipment. We frequently hear

“my network is fine” only to have IntraVUE scan the network and uncover several devices having intermittent communication problems. These will lead into larger problems as more devices are added and communication traffic increases. The ease of use of IntraVUE, with access from any computer with a browser, will provide a simple color-coded troubleshooting overview that can pinpoint problems.

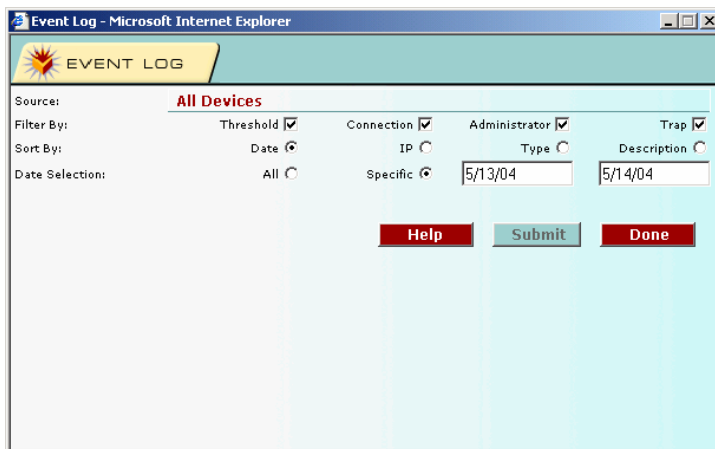
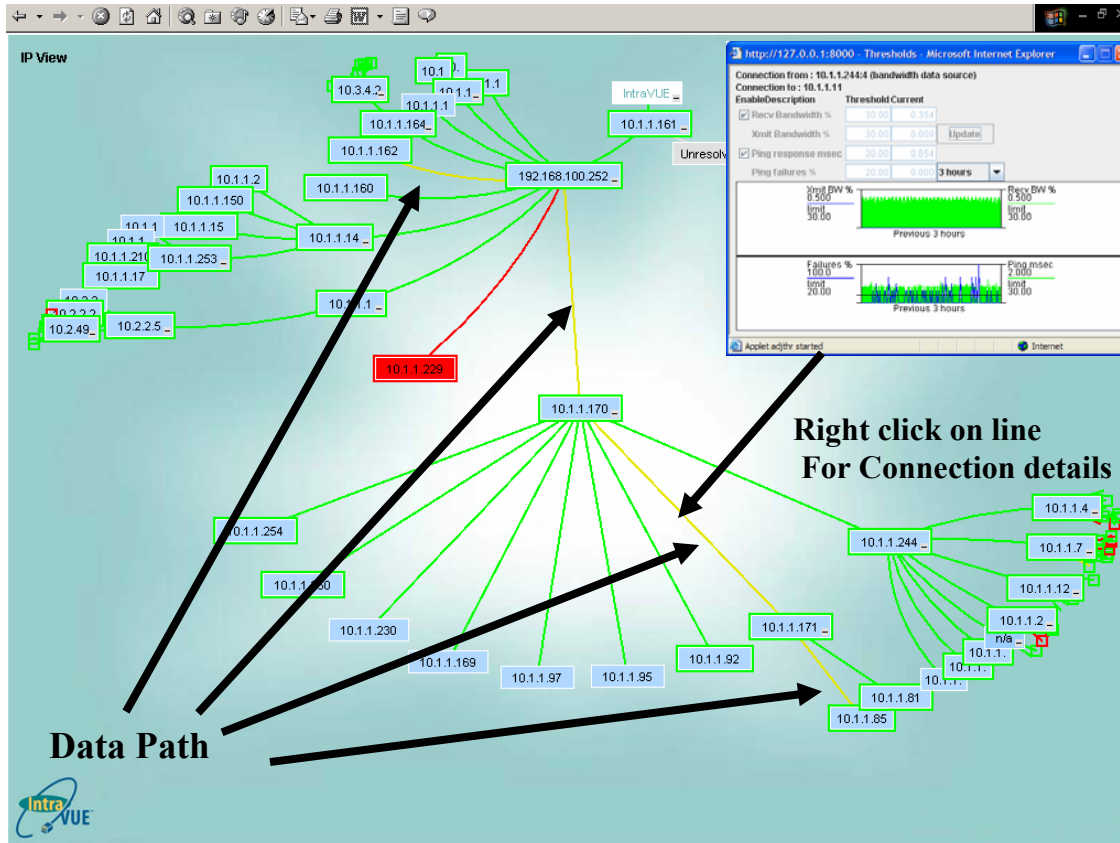


Figure 4 Event Log can be sorted or filtered to find specific problems

Searching for IP addresses or a specific vendor’s MAC address to locate a specific product is also very time consuming activities. Finding vendor’s equipment that may be embedded in the equipment is another feature that IntraVUE can perform to save hours of tedious work. The Search function provides individuals the ability to search easily to locate equipment on the network.

## Identifying Bandwidth problems

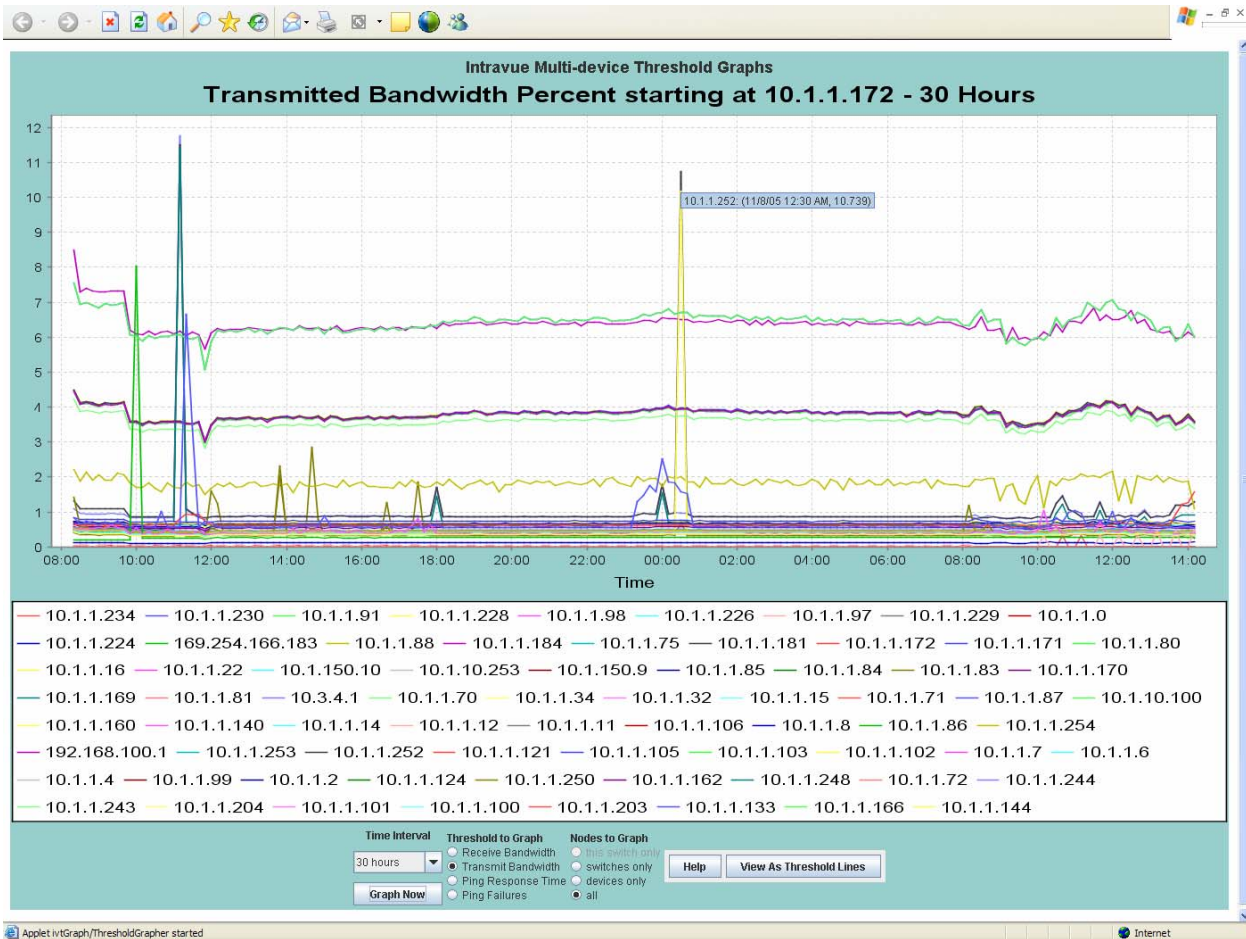
IntraVUE will monitor the traffic between all connections. In the figure below, a computer is downloading a large program from another computer that was located several switches away. This again is a frequent occurrence that disrupts traffic in unpredictable ways. The use of multicast messages that allow subscribers at remote locations to access streaming data can also cause these problems. As video surveillance and automation systems make use of multicast messaging, the need to visualize traffic and bandwidth problems down at a LAN level will be very important. IntraVUE provides a clear overview that can quickly identify when this problem occurs.



**Figure 5 IntraVUE overview colors indicating Bandwidth problem created as device 10.1.1.85 communicates with 10.1.1.162 and exceeds bandwidth limits**

Right clicking on the line will bring up the Threshold box and provide details on the problem. Here, one can see that the Bandwidth had been exceeded causing the line to go into yellow alarm level. The event log also captures the time that the event happened. Traffic problems are random and may last only a short time. IntraVUE can quickly and easily display these problems allowing for better understanding and planned resolution. IntraVUE can also send an alarm message to another software package, email or text message on these occurrences.

A new multiple device trending feature allows the selection of all devices, whether switches or end devices, to all be graphed on a single time-based chart. The ability to filter by area or type of device allows quick identification of the specific device from hundreds that may be installed on the network. As seen in the Figure below, the transmitted traffic of all devices can be displayed on a single screen.



The transmitted bandwidth used by 72 devices over the last 30 hours is displayed in a method that clearly identifies the devices generating periodic spikes in traffic.

As multicast traffic and broadcast storms become more common, the ability to quickly identify the source of the problem will reduce support and potential downtime. The ability to show relationships between devices offers the ability to drill down to a specific area or device having difficulty.



## Network Security

The ability to immediately identify newly added devices on a network, and then generates an alarm, provides added security and can eliminate potential problems of unauthorized attachments to the network. IntraVUE can notify immediately if a new device is connected to the network. The software identifies all the necessary information such as where the device was connected, how long it was on the network, and provides specific information such as IP address used, MAC address, and even computer name (if it was a computer/laptop). Since many manufacturing networks are isolated, the ability to capture the data in an event log as well as indicate the device is very important.

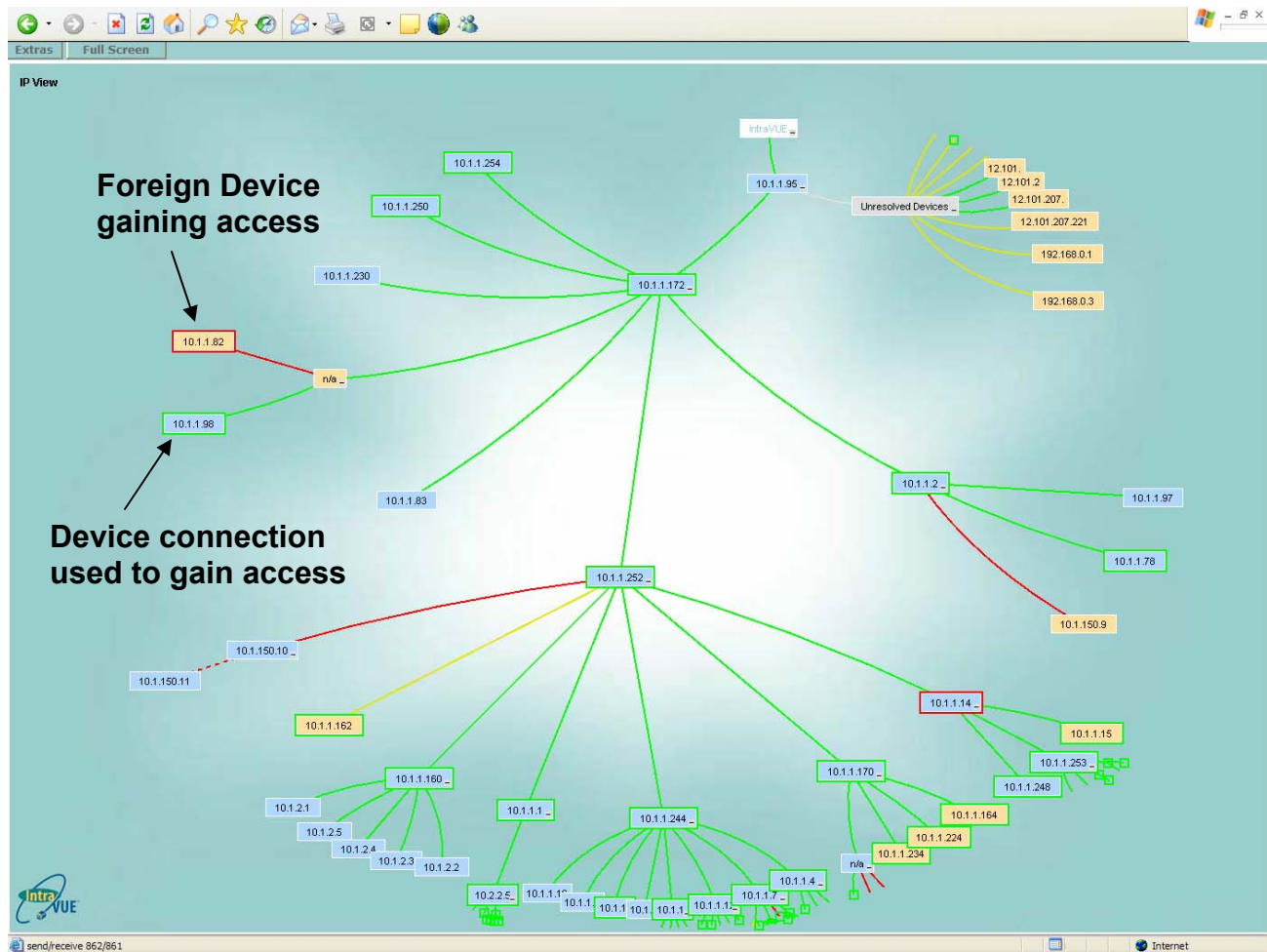


Figure 6. Unauthorized device (10.1.1.82) connected to the network by using the connection of device (10.1.1.98) and then it was disconnected and the cable replaced back to the original connection.



Information on the event can be sent to other HMI or SCADA stations or it can be emailed and/or text messaged via a pager. The ease at which you can connect to Ethernet can be one of its biggest detriments. The use of IntraVUE with its continuous monitoring capability allows you to be sure that you are knowledgeable of all devices gaining access.

A typical 100+ node system may experience a problem or two a week, especially if additions/connections are frequent, or as the network ages. The use of lower cost switches has also created unpredictable performance problems on factory floor networks that become heavily used. As network loads are increased (due to automation vendors using multicast traffic in their applications) some switches cannot support the loads or bottlenecks will cause unwanted collisions on the uplink ports.

Having a real-time interconnection display will provide a valuable view as to where devices should be connected for optimal performance and elimination of bottlenecks. Viewing the actual connection, rather than connecting to the nearest available port, will provide a better-constructed network architecture. IntraVUE will be a place that most will view to decide the best location to add a device. It will also provide an overview to determine if additional switches are required

The average time to bring in a network specialist and run the necessary test, if there is a problem, can be up to three hours. If the system is experiencing an intermittent problem, then this resolution may be significantly longer, as it may not be exhibiting the symptoms at the time the specialist arrives, perhaps 6 hours to several days. A wire swapped to another port on the switch that is not configured in the same manner may also take 3 hours even after a problem is identified. Newly added devices are depicted as Tan boxes identifying the time and location they were placed on the network.

These basic problems are identified immediately and opening an IntraVUE screen will highlight the problem in minutes. The event log, which is continually running, will pick up intermittent communication failures. This provides the plant floor personnel with the information to quickly solve these simple, but common problems. New devices added to the network are easily identified.

**Savings** 6 incidents per month @ 4hrs per incident = 24 hrs per month

24 hrs per month x \$60 per hr = \$1440 per month

Return on Investment is less than 6 months for solving just run time problems.



## Device failure identification and recovery

Not everything can run forever. When a device fails or locks-up it will stop communicating. IntraVUE will not only notify you of a failure but provide a framework in which all the necessary information about the device is present.

### Creating a complete support tool

The main focus of IntraVUE is to support the large number and variety of IP addressable devices located in remote enclosures that may run for years before experiencing a problem. When the problem occurs, it may take hours to locate the proper documentation. The use of IntraVUE as a framework leveraging hypertext links provides the simplest method to organize and retrieve information. Pictures of the enclosure can be added to easily identify the device in question. Using open technologies means that any device can use this technique.

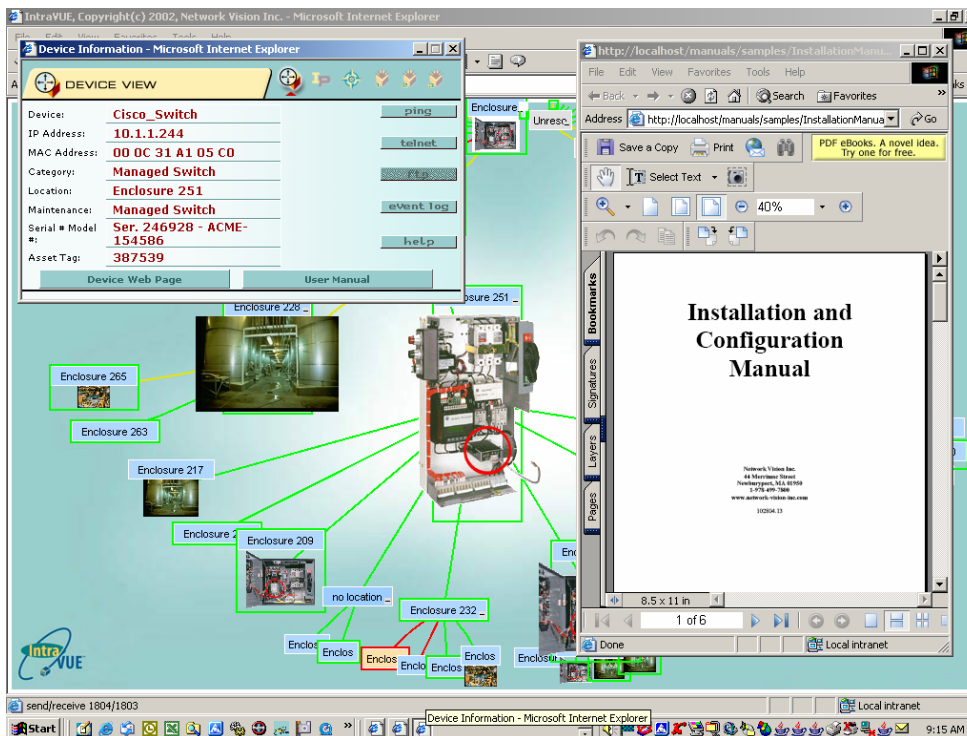


Figure 6. IntraVUE with Thumbnails and links opened to identify all that is required for support.



## Additions and changes to the system

The addition of devices to the factory will continue as equipment is introduced or older equipment is replaced with newer versions that communicate over Ethernet. The ability to view the actual network, as a connection diagram, will provide the proper information required to properly place new equipment. In addition to viewing, it will be important to inventory all equipment periodically.

Documenting an inventory of all the IP addressable devices and their interconnections can take days. One account spent a full week to fully document all the IP devices and connection details in their facility. IntraVUE, with its export feature, can provide all the details in a matter of minutes. The manual process of checking and documenting is time consuming and may open up the opportunity for errors. Lack of current documentation may mean hours of downtime and the potential for larger issues created by devices given the wrong address.

IntraVUE's graphic representation of the actual network saves 8 to 16 hours in maintaining an up-to-date drawing through connection verification and documentation for a typical 128-node network. This includes IP address, MAC Address, the Switch port, and Port to Port wiring between switches.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	10.1.1.250	1.00.01.02.06.31.10	239	172.10.1.1172	17	0	INTERNAL SERVER								
18	10.1.1.2	1.00.03.03.09.13.07	71	172.10.1.1172	19	0	EtherWan 100BC								
19	10.1.1.97	1.00.01.00.04.A8.F6	123	71.10.1.1.2	2	0	WINDK-PRO-TEST								
20	10.1.1.100.9	1.00.01.00.03.D9	460	71.10.1.1.2	5	0	CDM-RND-02-IP								
21	10.1.1.78	1.00.09.70.5F.90	451	71.10.1.1.2	6	0	MARK								
22	10.1.252	1.00.0A.F4.0A.D9.80	243	172.10.1.1.172	21	1	cisco2950switch								
23	10.1.1.1	1.00.10.70.01.CF.EE	9	243.10.1.252	2	0	Router								
24	10.2.2.5	1.00.00.03.0E.3F.3E	152	9.10.1.1.1	0	1	Hirschmann RS2								
25	10.2.2.250	1.00.40.80.22.57.49	196	152.10.2.2.5	2	0	Dig 232 to IP								
26	10.2.2.254	1.00.0F.64.0E.10.27	219	152.10.2.2.5	3	0	no name								
27	10.2.48.10	1.00.0A.0C.01.01.05	251	152.10.2.2.5	7	5	RuggedCOM-10 #1								
28	na		360	251.10.2.48.10	1	0	Hub								
29	10.2.10.2	1.00.00.A3.31.04.B7	93	243.10.2.10.2	0	0	ETS_3150B7								
30	NA		467	93.10.2.10.2	0	0	Servo Motor								
31	NA		489	93.10.2.10.2	0	0	Servo Motor								
32	NA		474	93.10.2.10.2	0	0	Servo Motor								
33	10.2.2.7	1.00.20.4A.91.C8.01	154	360.na	0	0									
34	10.2.2.40	1.00.40.80.02.80.03	160	251.10.2.48.10	2	0	Dig 1 IARP								
35	10.2.2.251	1.00.20.87.00.18.9A	200	251.10.2.48.10	3	0	EtherPAD								
36	10.2.2.249	1.00.20.4A.21.17.96	186	251.10.2.48.10	4	0									
37	10.2.2.252	1.00.20.87.00.18.9E	210	251.10.2.48.10	6	0	EtherPAD								
38	10.1.150.10	1.00.0E.38.04.02.00	103	243.10.1.252	4	0	Main Building Access point								
39	10.1.150.11	0.00.0E.38.04.02.40	313	303.10.1.150.10	0	0	Building 3 Wireless bridge								
40	10.1.1.14	1.00.0A.0C.01.01.84	89	243.10.1.252	6	4	RuggedCom Switch #2								
41	10.1.1.15	1.00.07.7C.0A.02.12	91	89.10.1.1.4	1	0	On-Time								
42	10.1.253	1.00.00.06.2A.A9.BB	245	89.10.1.1.4	2	5	Siemens OSM TP62								
43	10.1.1.32	1.00.00.06.94.7C.B6	95	243.10.1.253	1	0	Switch SIEMENS Scalance X-200								
44	10.1.1.210	1.00.C0.30.0B.9C	206	95.10.1.1.32	0	0	CS-V 100BT 1.0								
45	10.1.1.253	1.00.00.06.94.BC.ED	301	243.10.1.253	2	1	Siemens Test Switch								
46	10.1.1.34	1.00.A0.45.00.A1.9F	97	301.10.1.1.253	11	1	FL SWITCH MM HS								
47	10.1.10.100	1.00.01.95.00.0E.40	253	301.10.1.253	15	0	no name								
48	10.1.1.195	1.00.00.54.10.00.80	144	243.10.1.253	4	0	Camera 21								
49	10.1.1.184	1.00.0E.CF.20.05.AA	176	243.10.1.253	6	0	Camera 21								
50	10.1.1.248	1.00.20.4A.81.06.CC	235	89.10.1.1.4	5	0									
51	10.1.1.162	1.00.E9.6B.8B.A9	482	243.10.1.252	7	0	adeflinux								
52	10.1.1.160	1.00.50.54.01.01.80	156	243.10.1.252	9	0	oldlinux								
53	10.1.2.2	1.5A.FF.FF.01.02.02	336	156.10.1.1.160	0	0	Laptop								
54	10.1.2.3	1.5A.FF.FF.01.02.03	338	156.10.1.1.160	0	0	no name								
55	10.1.2.4	1.5A.FF.FF.01.02.04	340	156.10.1.1.160	0	0	Laptop								
56	10.1.2.5	1.5A.FF.FF.01.02.05	342	156.10.1.1.160	0	0	Laptop								
57	10.1.2.1	1.5A.FF.FF.01.02.01	377	156.10.1.1.160	0	0	no name								
58	10.1.1.170	1.00.00.4E.37.36.8C	168	243.10.1.252	11	12	Konex Switch								
59	na		442	168.10.1.170	2	0	MicoSwitch								
60	10.1.1.80	0.00.08.74.03.23.7A	491	442.na	0	0	MC4006								
61	10.1.1.86	0.00.0F.74.03.2E.2E	440	442.na	0	0	ACC0501								
62	10.1.2.22	1.00.00.C9.90.26.0B	483	442.na	0	0	DEM-70542NF0328								
63	10.1.2.34	1.00.C0.30.00.BF.3A	229	168.10.1.1.170	4	0	CS-V MNR 4.0								
64	10.1.2.24	1.00.90.A3.10.8F.04	214	168.10.1.1.170	5	0	EPS_100F04								

Exporting data from the device or events is as easy as select and click

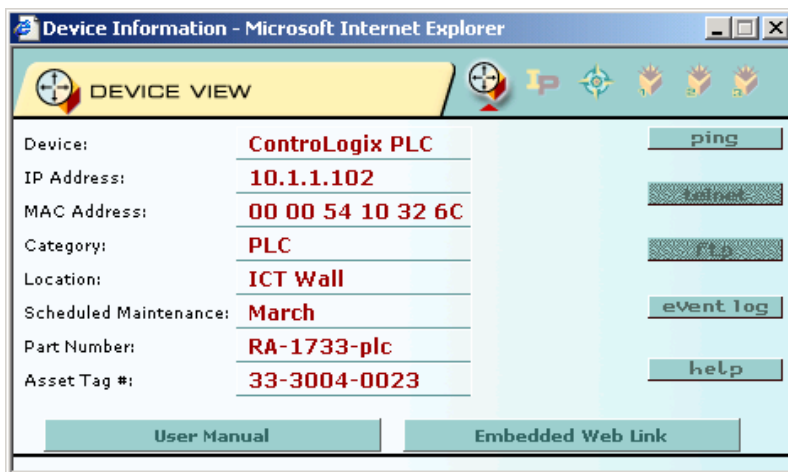
16 Hours average x \$50 per hour = \$800 per system update.

Searching for problems like duplicate IP addressing and location of devices are standard features of IntraVUE, a problem that is common when fixed IP addresses are used.



**Failed device recovery** is a requirement addressed uniquely by the Auto-IP feature of IntraVUE. IntraVUE will highlight the failed unit and can even send an email upon failure. The responsible person can just click on the properties of the highlighted device to get all the necessary details including part number and asset tag for verification. The ability of IntraVUE to have up to 12 web Links associated to every device provides the ability to have, at a mouse click away, all the necessary documentation required to service or replace the device. This key maintenance feature can point to asset management packages available from the Automation supplier, OEM, or Corporate system.

The structuring of information to bring in other packages that may already be in use will also simplify the learning process and reduce cost. Rather than having someone remember what IP address to assign a web server in a PLC or Switch, one merely pushes the button marked Web Link.



**IntraVUE can store device specific information and links to user manuals for easy servicing and or device replacement.**

Once the replacement unit is retrieved, the technician replaces the unit by first connecting the communication cable and then powering the unit up. Auto-IP will sense a request from the device on startup looking for an address (BootP). Auto-IP will identify the location of where the request is coming from and search its database for the appropriate fixed IP address. This simplifies the replacement and provides additional security with respect to wrong addresses being added to the network.



Cannot find server - Microsoft Internet Explorer

Address: http://127.0.0.1:9090/

Auto	IP Address	Switch Port	MAC	V.MAC	Status	NetMask	Gateway	Community	DNS	Boot File
<input checked="" type="checkbox"/>	10.1.1.252	10.1.1.172.21	00:0a:14:0a:09:90	<input checked="" type="checkbox"/>	failed	255.255.0.0	10.1.1.230	public		
<input checked="" type="checkbox"/>	10.1.1.223	10.1.1.172.22	00:00:00:00:00:00	<input type="checkbox"/>	failed	255.255.0.0	10.1.1.230	public		
<input checked="" type="checkbox"/>	10.1.1.224	10.1.1.172.23	00:00:00:00:00:00	<input type="checkbox"/>	failed	255.255.0.0	10.1.1.230	public		
<input checked="" type="checkbox"/>	10.1.1.133	10.1.1.7.2	00:07:5f:01:93:21	<input checked="" type="checkbox"/>	failed	255.255.0.0	10.1.1.230	public		
<input checked="" type="checkbox"/>	10.1.1.100	10.1.1.12.3	00:a0:45:00:33:1b	<input checked="" type="checkbox"/>	failed	255.255.0.0	10.1.1.1	public		
<input checked="" type="checkbox"/>	10.1.1.108	10.1.1.12.7	00:a0:45:00:33:1b	<input checked="" type="checkbox"/>	failed	255.255.0.0	10.1.1.1	public		
<input checked="" type="checkbox"/>	10.1.1.109	10.1.1.12.9	00:00:00:00:00:00	<input checked="" type="checkbox"/>	failed	255.255.0.0	10.1.1.1	public		
<input checked="" type="checkbox"/>	10.1.1.110	10.1.1.12.10	00:00:00:00:00:00	<input checked="" type="checkbox"/>	failed	255.255.0.0	10.1.1.1	public		
<input checked="" type="checkbox"/>	10.1.1.230	10.1.1.172.23	00:50:fc:b3:b2:ce	<input checked="" type="checkbox"/>	failed	255.255.0.0	10.1.1.230	public		

Copyright (c) 2004 Network Vision Inc.  
All rights reserved.  
Version V1.3.22.10/31/05 (licence level: 8.0)

Auto Bootp     Lock to Vendor MAC

IP Address:

Switch : Port:

MAC Address:

NetMask:

Gateway:

Community:

DNS Server:

Boot File:

**Auto-IP** provides an automated method to assign IP addresses to ports on a switch for new device additions or automatic assignment of fixed IP addresses to replacement devices.



IntraVUE also frees up the IT staff to remain focused on higher-level problems, which require their skill and advanced software tools. Allowing the plant floor to address the common issues they experience provides several benefits, such as:

- \* Quicker response time and reduced equipment downtime. We have not added the cost of lost production in this calculation.
- \* Better working relationship between your Controls and IT departments, a sore spot for many companies.
- \* A balanced and appropriate use of your employees

Total Yearly Cost savings. (128 device network)

Initial Mapping of Network .....	\$6,800.
Quarterly update of system map or Verification of Acceptance Test.....	\$6,000.
Quarterly maintenance savings .....	\$4,320.
Fault recovery (one incident per quarter).....	\$1,200.
Total yearly Savings .....	\$ 52,880.



**Ethernet is rapidly expanding on the plant floor however:**

- You may think that you do not have enough devices to justify the purchase of IntraVUE. IntraVUE, however, is scaleable and can start with a package of 16 nodes for less than \$1000. As you grow, the package can be easily upgraded.
- You may feel that the IT group will be responsible for the network. However, who is responsible for the control equipment connected to the network? IntraVUE has been designed for support of the devices with the ability to picture the activities of the network. It is a great common tool that both departments can use providing value for a number of activities.
- You may feel that there is nothing wrong with the network; it is running with no problems. The question is, can you be sure that systems are not having intermittent problems and you just do not know it? Have you ever felt that the network slowed down for a while or a device was having problems getting the data? Like when a spark plug starts to misfire, the vehicle still runs, but gas mileage starts to decrease. The check engine light similar to IntraVUE can keep your performance optimal and save you money in the long run.
- You may feel that network software is just too complex for you, or your people. IntraVUE is the most intuitive and easy to use package on the market. We provide a money back guarantee – if, after 30 days, you do not feel the package can be used by your operators, technicians, or maintenance personnel, you can return it for a full refund.

Network Vision has developed this package to address a growing need for anyone that will be responsible for supporting IP addressable devices on an Ethernet network. The Auto-discovery and display technologies are state of the art. We have strategically priced the package to provide a return on investment in less than 6 months. Many have had IntraVUE pay for itself in the first month. It is fully complementary to all IP devices and is even being used in applications outside of the plant floor. It is better to have it running before a communication problem causes your company to experience downtime or apply significant amounts of resources searching for problems easily identified by IntraVUE.