

## Comparison between Auto-IP and DHCP Option 82

As the Industrial market searches for a method to simplify the addition and replacement of Ethernet devices there currently exist two potential Solutions. The following information compares these two different approaches and how they are currently addressing the problem of simple IP addressing.

This document is intended to highlight the differences between each approach and the impact that this may have on current and future Industrial Ethernet installations. Below is a chart that highlights the differences and that are covered in the following text.



	IntraVUE w/Auto- IP	DHCP Option 82
Can work with all existing networking equipment (switches)	Yes	No
Can support both BootP and DHCP enabled end devices	Yes	No
Can detect and alarm if cables are inadvertently reversed on a switch	Yes	No
Can support redundancy of the IP address server	Yes	Not easily
Can support Devices connected to a Hub	Yes	No
Requires programming or configuration at each switch	No	Yes
Can be developed standalone and then coexist with other IP-address servers	Yes	No
Able to handle any switch replacement in addition to end devices	Yes	No

### Detail Comparison

The origin of DHCP Option 82 is from Cable TV and DSL Internet Service Providers which have made use of a DHCP option originally intended to allow end user devices to classify themselves to the DHCP server, and thus allow the DHCP server to allocate them different settings because of their particular needs.

The trick is performed by having the managed switch intercept an incoming request, and note which port the request came from. The DHCP request is then regenerated as a 'DHCP forwarding request' and at the same time an 'Option 82 record' is added which identifies which switch and which port received the query. The DHCP request is forwarded to the 'real' DHCP server elsewhere on the network, where IP address allocations have been previously associated with the 'Option 82' data.

#### Auto-IP Configuration

All managed switches support Simple Network Management Protocol (SNMP), and specifically the 'Bridge MIB' defined in RFC1493. They can therefore be asked by a central management station to report which port a particular MAC was found on.

The Auto-IP technique involves a modified BOOTP server which is capable of issuing SNMP queries to switches to identify the switch and port number. The server uses this information, along with knowledge of whether a station is currently up or down, to determine whether a newly-seen MAC represents a new device or a replacement for an existing one.

## 1. Device configuration needs for Auto-IP versus Option 82

The Option 82 technique requires that two pieces of data be maintained about a target. The DHCP database must include an entry designating the IP and associating it with the Option 82 tag, and the switch must be configured to add the Option 82 tag to all incoming DHCP requests before forwarding them.

Typically, this requires that all switches have unique configurations, and this in turn requires maintenance of a hierarchy of configuration files by IP address. Once installed all these new switches, you must now configure each of them to 'arm' the DHCP relay capability, designating which ports of which switch are to be intercepted by the DHCP relay and associated with a location tag. Note that this configuration has to affect each individual switch, since the arrangement of ports supporting option 82 is likely to be unique to each location in the plant. Now you need to configure entries in my central DHCP database for each automation device to be added, associating the location tags with the IP address. Having to maintain information in distributed equipment is costly and cumbersome.

DHCP Option 82 must use a DHCP server. This in practice makes it almost impossible to separate address management of the industrial devices from that of the laptops and office computers which may coexist on the network. The DHCP server must be a very modern one, since Option 82 has not been supported for more than a couple of years.

Now you must deploy switches which support Option 82. Since Option 82 is defined by a relatively new Internet standard (RFC 3046 – January 2001) and, the description of its intent was very specific to Internet Service Provider use, most vendors of managed switches have up to now ignored the requirement. You will not see RFC3046 listed in the datasheets of many existing managed switches.

Conversely, Auto-IP does not require any special configuration of the switches, and both model and manufacturer of switch can typically be substituted without any reconfiguration. The complete details about the configuration and the addressing mechanism is located at just one location.

The sequence is as follows:

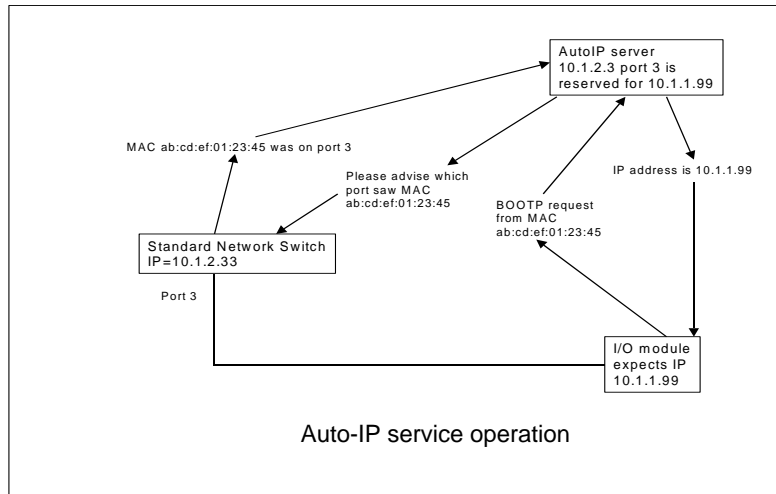
An I/O device issues a BOOTP request (which naturally includes its MAC address)

The Auto-IP server sees the request, and checks its database for a MAC match. If the MAC is already known, the IP address is returned just like in a conventional BOOTP service.

If the MAC address does not match, Auto-IP sends out SNMP queries to the switch(es) to determine which port of which switch sent the request.

If the switch address and port number matches one for which automatic assignment is configured, it is considered a 'potential replacement'.

If there is one and only one Auto-IP configured device at that switch and port position which is currently 'down', the replacement is authorized. The IP address for the 'down' device is transferred to the new MAC and thus recorded in the database, and the correct BOOTP response is sent.



## 2. Devices on the wrong port

With Auto-IP, if the cable locations of two I/O devices connected to a switch are inadvertently swapped while the target devices are live, typically the devices will not notice, and communication will continue as normal. When the devices next reset, they will send out their BOOTP/DHCP requests, the MAC addresses will be recognized, and the correct IP addresses will continue to be assigned. The IntraVUE software can be set to graphically displays and alarms if any selected connection has been moved. The possibility of connections being removed and replaced in the wrong port is more common than one would think. The replacement of a switch and all of its connections is another source for such an occurrence.

With DHCP Option 82, or any other technique involving hard tagging of the port numbers, the situation would be much more serious and confusing. When the cables were swapped, all would continue OK. But at the next reset, the devices would both be issued the wrong IP addresses. Catastrophic!

Regardless of the technique used, it is important to use a tool such as IntraVUE to monitor for inadvertent wiring changes.

## 4. Redundancy

Auto-IP encourages a simple redundancy technique. A primary Auto-IP server is the one configured by a user. Secondary (satellite) IP servers are set up closer to the plant, and slaved to the primary so that the database is copied at regular intervals. When a BOOTP (or DHCP) request is received, all operable servers will answer, but the answers will naturally be the same. Similarly, all servers will update their MAC in their records if a replacement is seen.

With DHCP it is very cumbersome to set up more than one server, and almost impossible to agree to devolve responsibility for different pools of addresses to different sets of servers. So IP address management must always remain a responsibility of the traditional IT department.

## 5. Devices connected to a Hub or unmanaged switch

With Option 82 you MUST have only a single device on each port of a managed switch, since it has no mechanism to resolve ambiguity. The linking is on to one as the transmission to the address server is specific to port number and not the individual device MAC address.

Auto-IP allows unmanaged switches or hubs to be used in most cases. The ability to know additional information such as only one device is currently down is very important, because what it allows is for multiple Auto-IP – configured devices to be assigned to the same port of a managed switch. So long as all of the devices are normally operable (as would be the case in an industrial I/O situation), a single device which has failed can be replaced automatically. (This method has been implemented successfully on several fieldbuses also requiring that all devices other than the one being replaced be operable.)

So it is no longer necessary to insist that all devices requiring IP assignment be directly connected to a managed switch. This can be a significant help in environments where an unmanaged switch or hub is more appropriate for embedding in equipment.

Determining whether a device is up or down is performed by a continuous 'ping scan' which attempts to communicate with each device under Auto-IP control every 30 seconds or so. Failure to respond to more than one such ping in sequence is considered failure. So devices can be replaced and complete the Auto-IP assignment process within 60 seconds, which is faster than most technicians can replace a device!

## **Comparison**

At first sight, it would appear that the two techniques give similar benefits. But a look below the surface exposes some issues.

### **1. Complexity of installation**

All of the above operations will require use of skilled network technicians.

### **2. Need to upgrade all end devices**

The other major problem is that almost all installed devices today, the controllers, robots, I/O modules, sensors, actuators, do not support DHCP configuration. But probably 90% of them do support BOOTP as an option, since it was in widespread use when Industrial Ethernet was first used.

So special maintenance procedures will continue to be required until all Ethernet-capable devices already in stock have been made obsolete.

As use of Ethernet has increased in the industrial space, particularly for connection of simple sensors and I/O devices to PLC's and SCADA systems, customers are having to rethink device addressing techniques.

All devices on a TCP/IP communication network require assignment of an IP address before they can communicate with any other station.

These IP addresses must be assigned carefully, since a misconfigured IP address can cause significant disruption on a functioning network, particularly in cases where a new device is assigned an address already in use somewhere else on the network. Industrial networks have the characteristic that they are expected to be continuously available, but individual devices have finite failure rates and the number of devices requiring replacement during the operating life of the network will be large. The failure rate for an individual class of device may be sufficiently low that maintenance and restart procedures may be unfamiliar to the repair technician at time of replacement.

Any delay researching the correct replacement and restart procedures, or required coordination between maintenance technician and network services professional, will lead to increased 'Mean Time To Repair' (MTTR) and thus loss of production. The replacement operations being considered must include not only the sensors and actuators themselves, but also major infrastructure components such as network switches and PLC's.

It must also be usable in environments where there is no direct communication from a central location to all devices on the industrial networks, such as where a vendor includes a private Ethernet network as part of a machine, only accessible through dedicated interface on the tool control computer or PLC.

## **DHCP Option 82 Relay**

Instead of maintaining a rigid database a DHCP server instead keeps a 'pool' of addresses, each of which may be 'leased' or 'free' at any time. When a DHCP server receives a request for an address, it checks the table to see if an address is already allocated for that device, and returns it if so. If not, but there are free addresses in the 'pool', a 'lease' is created from one of the 'free' addresses, and this is allocated.

This method is very convenient for devices such as laptop computers which only run 'client' software such as web browsers, and do not care which IP address they actually are allocated so long as it works.

However this dynamic assignment method is not useful for most PLC and I/O devices, or network switches and web servers, which require to be allocated a well-defined IP address. Most PLC's expect to transmit configuration changes and similar directly to an IP address, and must know in advance what IP addresses to use for each target.

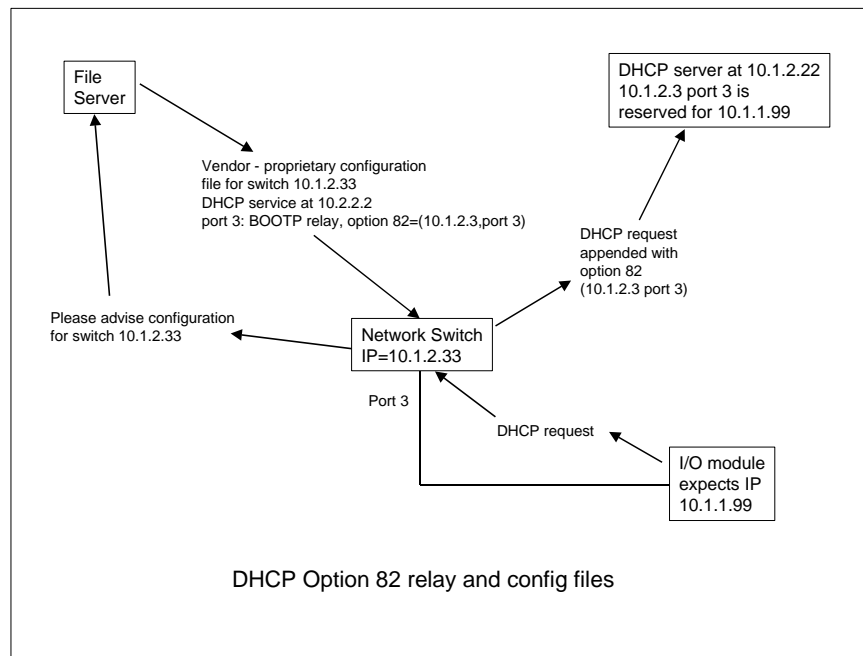
Some infrastructure vendors, in particular Cisco and Hirschmann, have proposed adoption of this technique for industrial IP address assignment.

This method can be made to work, but requires special configuration at the switches. It is (at minimum) necessary for the switches to determine which of their ports support Option 82 forwarding, and which should leave the DHCP requests alone. Also the address of the DHCP server to which the requests must be forwarded must be known. And the DHCP server must be a very modern one which understands Option 82 (ruling out the standard DHCP server on Windows 2000 for example)

In the event of replacement of a switch, all this information must be recreated. The methods by which switch vendors achieve this are usually to require maintenance at some central location of a file server containing images of the configuration files for each switch, and the switches are configured to query the server at restart to obtain their configuration.

To make provision for an additional I/O device on a network, it is now necessary to update two files – the central DHCP database, and the configuration file for the switch whose port will be attached

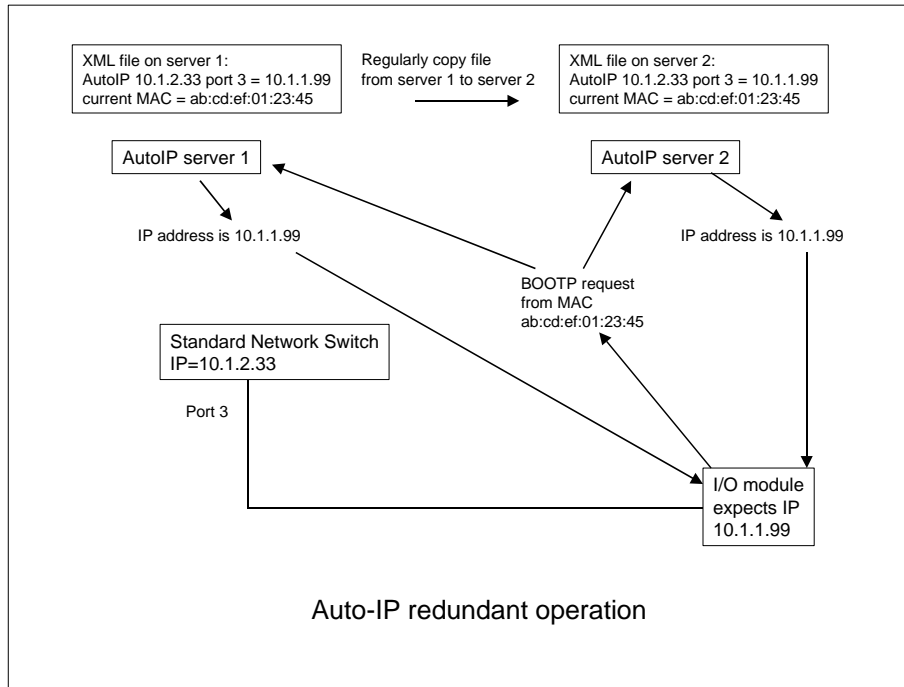
And of course, the end user must use switches and DHCP server software which support this use of Option 82 relay. Since the specification is very new, only the newest models of switch from each of the vendors is likely to support the facility, and that can imply costly infrastructure upgrades. And because of limited choice of vendor and model, the issues of vendor lock-in are significant.



## 6. Network Vision Auto-IP assignment

This technique combines the best features of variants 4 and 5, and significantly reduces the administrative burden while avoiding vendor lock-in by supporting almost all existing managed switches.

Since Auto-IP requires only that the replaced devices support BOOTP, and that managed switches support RFC1493, it can be easily retrofitted to almost all existing Ethernet – based control networks.



## Auto-IP implementation

The Auto-IP product takes the form of a software package running on a Windows 2000 or XP computer, and which uses a web browser as its user interface for configuration and monitoring.

The Auto-IP service generates a very low 'load' in terms of memory and CPU usage, and almost always can coexist with a SCADA system or similar on the same computer.

The user interface allows an administrator to designate an Auto-IP device by assigning the following data

- IP address
- Netmask and Gateway
- Switch address
- Port number of switch
- SNMP 'community' (password) of switch

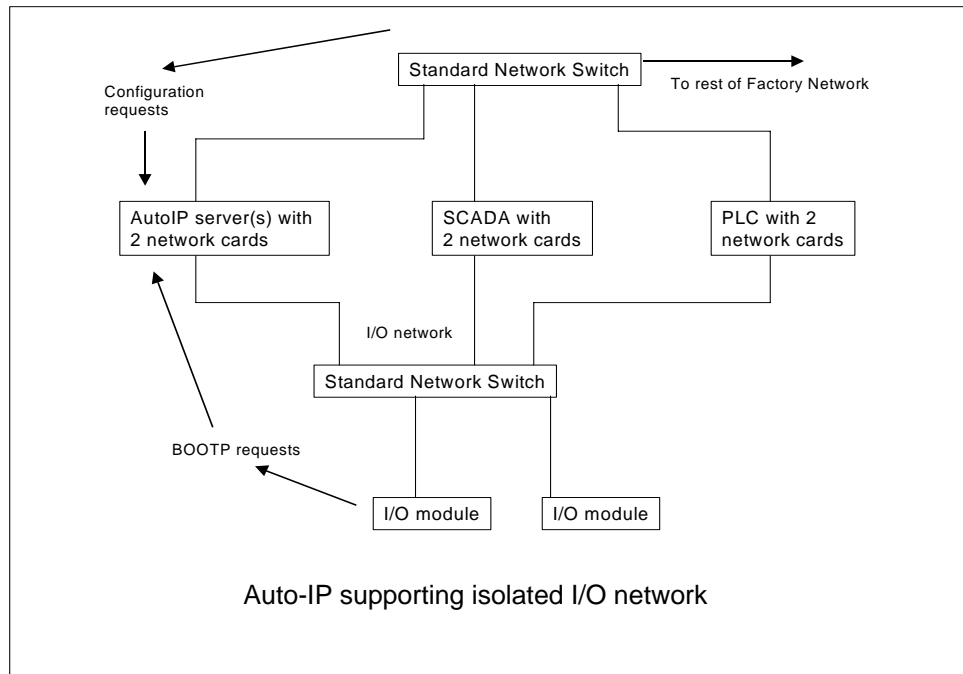
The data is entered and displayed in a 'spreadsheet – like' format which takes advantage of the likely similarity of settings for all devices on the same network.

There is also a facility allowing automatic data entry using Network Vision's graphical 'Intravue' package, where the administrator can simply designate an existing station for Auto-IP assignment by clicking on the node and setting a checkbox in its properties. This again minimizes the possibility of misconfiguration.

There is absolutely no problem in arranging redundancy on the IP assignment mechanism. Because the software uses BOOTP and not DHCP, there is no concept of a 'pool' of addresses whose leases must be coordinated. So long as multiple Auto-IP servers are operating from the same database, they will issue the same IP address data to any client requesting it. It is often wise to arrange at least two servers to cover the same plant area, one being close to the targets, and one being close to the 'center'. That way, if there is any sort of network disturbance during the time that BOOTP service is required (such as one of the switches going through a reset), there will be less delay at the target.

Auto-IP uses simple text files structured in XML format as its database, and normal file mirroring techniques can be used to ensure that all servers responsible for a given plant area remain synchronized.

### ***Use on isolated I/O networks***



In many cases, customers deliberately separate the Ethernet networks used for I/O from those used for general-purpose supervision. This may be for security reasons, or simply to allow an OEM to pre-configure and test a tool before delivery, and not have to alter any IP addresses or similar on installation.

These arrangements can be a challenge for server-based schemes such as Option 82 or distributed DHCP, where it is important to be able to access central servers containing configuration data for the switches or the targets.

In the case of Auto-IP, the simplest solution is to arrange for the Auto-IP workstation to have twin Ethernet interfaces, so that it can 'see' the I/O and enterprise network concurrently. Auto-IP will communicate correctly with the switches and targets on the I/O network, and still be able to service web requests and file mirroring on the main network. And users requiring redundancy can arrange two such computers if necessary.

For details, contact [info@intravue.net](mailto:info@intravue.net)  
or visit our website, [www.auto-ip.com](http://www.auto-ip.com)

IntraVUE™ is a product of Network Vision, Inc.  
Newburyport, MA, USA 1.978.499.7800

Copyright 2004, Network Vision, Inc.