



Discovering Devices in HP Web Jetadmin

This technical brief examines the different techniques for discovering devices in HP Web Jetadmin 6.5 in order to configure or manage those devices.

What Is Discovery?

Devices such as networked printers must be discovered in HP Web Jetadmin before they can be configured or managed. Discovery is the process of searching the network for devices, storing them in a cache, and displaying the results in a list.

The main benefit of automatic discovery is that devices are

dynamically added to a cache and maintained. Having to manually enter or populate a cache would be inefficient and burdensome.

HP Web Jetadmin provides several techniques for performing a discovery on a network. Each technique has advantages and disadvantages that will be discussed further in this paper.

When Does Discovery Occur?

After initial installation of HP Web Jetadmin and launching it for the very first time, the administrator will be prompted to perform a discovery. If the administrator declines to perform a discovery at this time, a discovery can

be initiated at any later time by performing the following steps (see Figure 1):

1. Under the *Choose* menu, select *Preferences*.
2. Under the *Select* menu, choose *Discovery*.
3. Select *Properties*.
4. Enable any desired discovery techniques.
5. Select *Start* next to *Start Background Discovery*.

A discovery can also be performed from the main screen of all devices by selecting the *Start Discovery* button.. Furthermore, a discovery can be scheduled to occur at regular intervals by selecting the *Schedule* tab.

The *Quick Device Find* box, located in the upper right hand portion of the screen, can also be used to perform a discovery, only for a single device rather than multiple devices. Any of the following criteria can be entered to find the device:

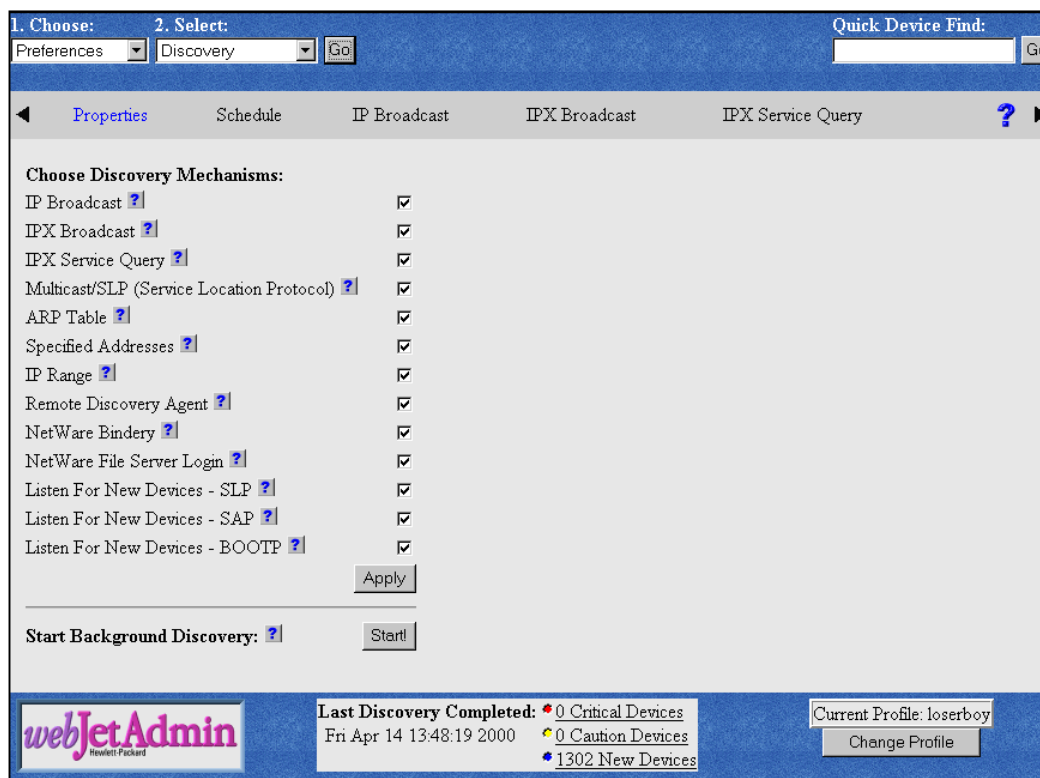


Figure 1

- IP address
- IP host name
- Hardware address
- IPX address
(network number: MAC address)

For a *Quick Device Find*, HP Web Jetadmin will first search for the device in the cache of previously discovered devices. If the device is found, HP Web Jetadmin will display the *Status* page of the device. If the device is not found in the cache, HP Web Jetadmin will add the device to the cache, and will then perform a discovery on the network for the device. If the device still cannot be found on the network, it remains in the cache for future searches.

How Do I Know When a Network Discovery Is Occurring?

HP Web Jetadmin will display the current status of a discovery at the bottom center of the screen. It will either display that a discovery is in progress, or it will display the time when a discovery was last completed.

Last Discovery Completed: ● 0 Critical Devices Fri Apr 14 13:48:19 2000 ● 0 Caution Devices ◆ 1350 New Devices

Discovery Mechanisms

Initiated and scheduled discoveries will use all selected or enabled discovery methods from the *Choose Discovery Mechanisms* screen (see Figure 1).

These discovery mechanisms will use one of two general tactics to discover devices on the network:

- Send a query (broadcast or directed) to the device and listen for responses.
- Monitor the network for signals sent out by devices to indicate their presence on the network.

It is difficult to make discovery usage recommendations since every environment is different. However,

here are some guidelines to follow when deciding which discovery techniques to use:

1. All discovery techniques will issue SNMP packets (broadcast or directed UDP port 161) in some manner. If this type of packet is filtered at the routers, IP discovery accuracy will suffer on remote subnets unless RDA is being used..
2. Use the discovery scheduler feature to perform discoveries during time intervals that will not conflict with peak network traffic hours.
3. Broadcast discovery techniques, such as *IP Broadcast* and *IPX Broadcast*, will initially send a very minimal number of packets. However, spikes can occur in network traffic when all devices respond simultaneously.
4. *IP Range* will send SNMP packets to every IP address specified in the range(s), regardless of the type of device, and whether or not the IP address is in use. Use caution when choosing ranges.
5. *Specified Addresses* is a more static type of discovery method, meaning it finds devices of which administrators are already aware. Other discovery techniques are more dynamic in nature, meaning they will help in discovering devices of which administrators are unaware.
6. Activating *Listen for New Devices* will minimize the number of full scale discoveries that need to occur in order to maintain an accurate list of devices. This technique can take an accurate list of devices and maintain its accuracy by just adding new devices as they appear on the network.
7. For devices that are enabled for IPX/SPX only (such as in a Novell NetWare environment), the

following discovery techniques should suffice in finding these devices:

- *IPX Broadcast*
- *IPX Service Query*
- *Specified Addresses*
- *NetWare Bindery*

Of these techniques, only *NetWare Bindery* requires that SAPs be enabled on the device. However, *IPX Service Query* will increase in accuracy if SAPs are enabled on the devices and SAPs are not filtered at the routers.

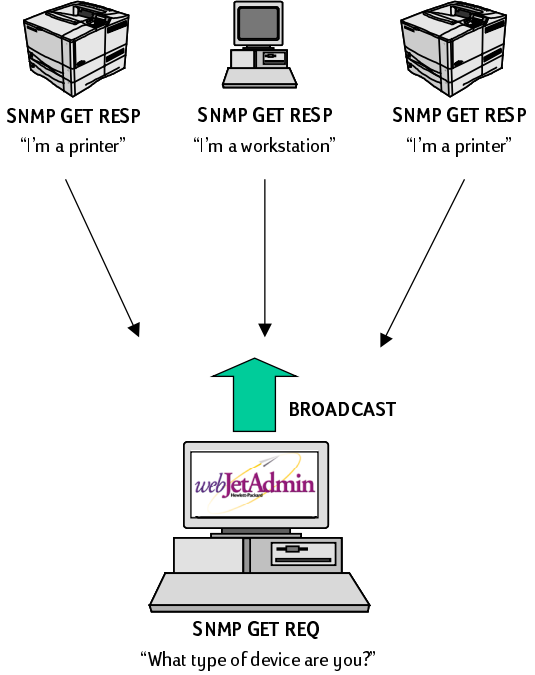
8. The *Remote Discovery Agent* technique will decrease the SNMP traffic that occurs over routers during discovery. It uses TCP, not SNMP, to communicate between the Web Jetadmin server and the RDA client. SNMP packets are issued on the remote subnet only by the RDA client machine.

The following pages will examine each discovery mechanism in more detail.

IP Broadcast

How Does It Work?

HP Web Jetadmin sends an SNMP GET REQ broadcast packet over TCP/IP to any subnets that contain devices listed under the *Specified Broadcast Address* drop-down list. All SNMP compliant, TCP/IP capable devices will respond to this broadcast packet. HP Web Jetadmin will send additional directed SNMP GET REQ packets to responding devices that it supports (i.e. printers, scanners, etc.) to gather more specific information about each device.

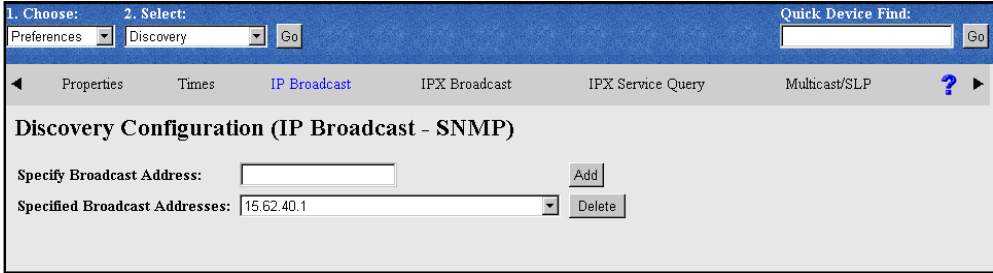


Advantages

- Very fast. All devices respond immediately to a single broadcast packet per subnet. However, total discovery time will be directly related to the number of subnets queried.
- Can discover devices on remote subnets if configured to send to remote broadcast addresses.
- Sends minimal packets on the network initially to get devices to respond.

Disadvantages

- Spike in network traffic as responses come in.
- Collisions and buffer overflows on large subnets can greatly affect accuracy.
- No guaranteed delivery of requests or responses.
- Remote discovery not possible if broadcast traffic is filtered at routers.
- Unconfigured IP devices on remote subnets will not be discovered.

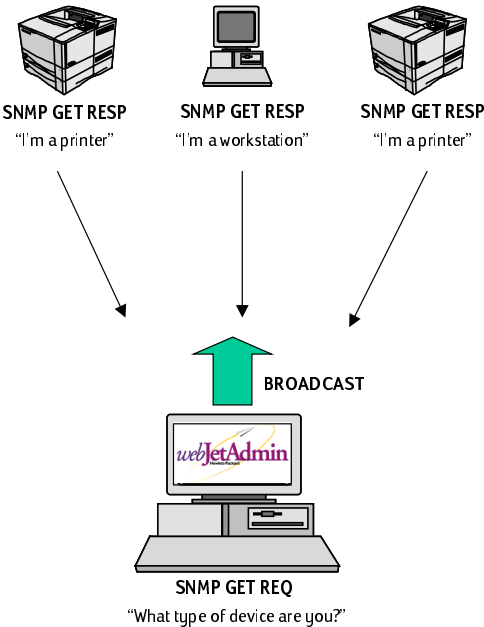


IPX Broadcast

How Does It Work?

HP Web Jetadmin sends an SNMP GET REQ broadcast packet over IPX to all network numbers selected. All SNMP compliant, IPX/SPX capable devices will respond to this broadcast packet. HP Web Jetadmin will send additional directed SNMP GET REQ packets to responding devices that it supports (i.e. printers, scanners, etc.) to gather more specific information about each device.

HP Web Jetadmin will attempt to discover all network numbers on the network and display those in a pull-down list. Administrators can choose to have a broadcast packet sent to all discovered network numbers or to individual network numbers.

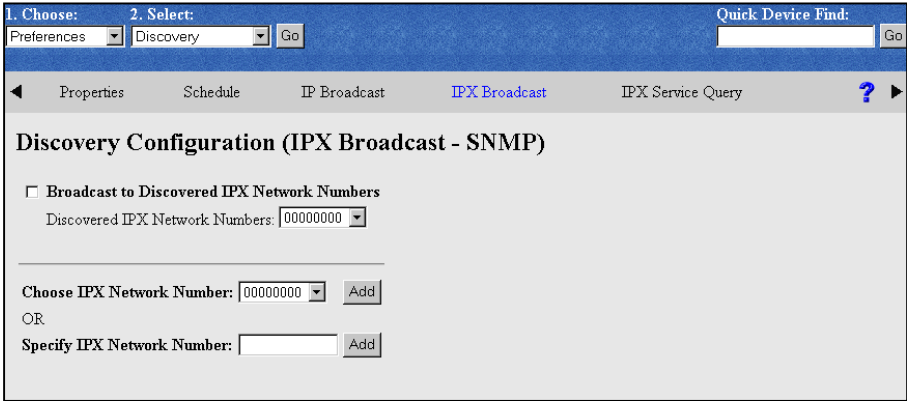


Advantages

- Very fast. All devices respond immediately to a single broadcast packet per subnet. However, total discovery time will be directly related to the number of network segments queried.
- Can discover devices on remote segments if configured to send to remote broadcast addresses.
- Sends minimal packets on the network initially to get devices to respond.
- SAPs can be disabled on devices and will not affect accuracy.

Disadvantages

- Spike in network traffic as responses come in.
- Collisions and buffer overflows on large subnets can greatly affect accuracy.
- No guaranteed delivery of requests or responses.
- Remote discovery not possible if broadcast traffic is filtered at routers.



IPX Service Query

How Does It Work?

HP Web Jetadmin sends a General Service Query (GSQ) broadcast packet on the local network asking devices of a type that HP Web Jetadmin supports (0x030C) to respond. Routers should also be able to respond with information about remote devices as long as SAPs are enabled on the devices and are not being filtered at the routers.

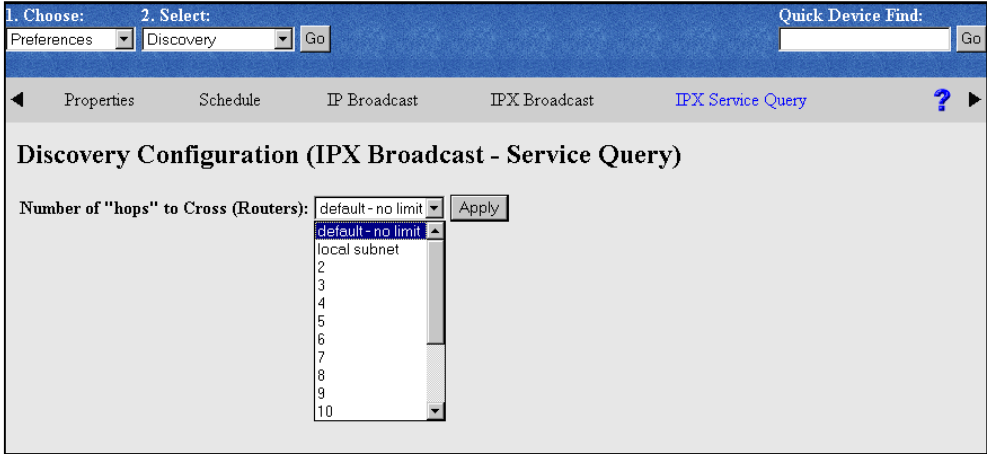
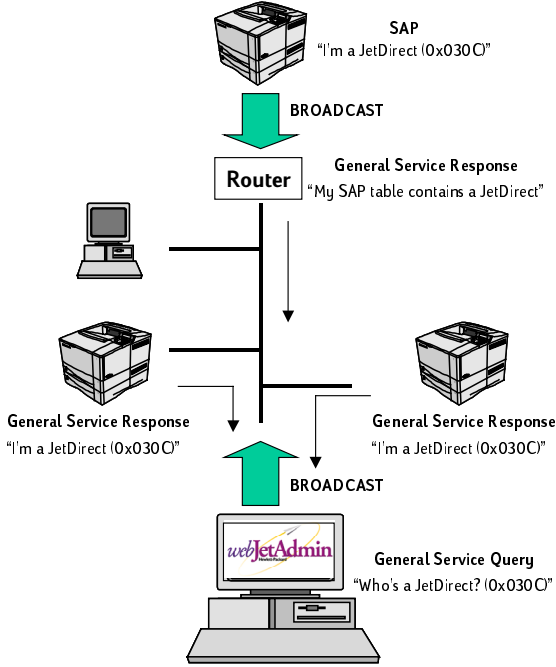
The number of hops can be configured to filter out devices that are beyond the number of hops entered.

Advantages

- Low network traffic. Only supported devices respond. Sends minimal packets on network.
- Fast discovery time.
- Accuracy is very good on local network, even if SAPs are disabled.
- Accuracy is very good on remote networks if SAPs are enabled on devices and not filtered at routers. Local network devices can have SAPs disabled.

Disadvantages

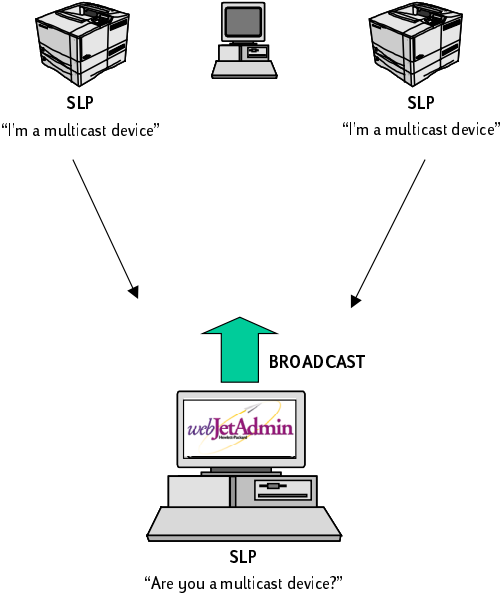
- Remote devices with SAPs disabled will not be discovered.
- If SAPs are filtered at routers, remote devices will not be discovered.



Multicast/SLP (Service Location Protocol)

How Does It Work?

HP Web Jetadmin sends out a single request over an HP-specific multicast address. Only HP multicast-capable devices respond to this request (currently x.06.00 firmware and greater). HP Web Jetadmin then listens for responses from these devices, and sends SNMP requests to gather more information. The multicast can be limited to the local subnet, or configured to cross up to 15 routers for discovery on remote subnets.

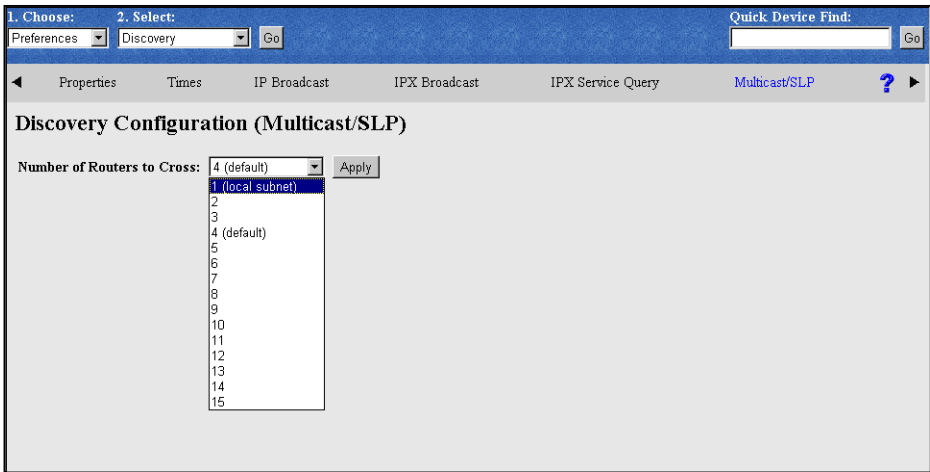


Advantages

- Minimal network traffic. Since multicast only looks for specific devices, it does not generate very much network traffic.
- Can discover remote devices.

Disadvantages

- Only HP devices will be discovered.
- HP Jetdirect device must support multicast (x.06.xx or greater firmware)



ARP Table

How Does It Work?

HP Web Jetadmin first looks at the ARP table maintained on the machine running HP Web Jetadmin, and sends SNMP requests to each entry to gather information. HP Web Jetadmin then searches the ARP tables of those machines/devices, and so on, until no more devices can be discovered.

ARP tables are maintained on all IP capable machines or devices. An ARP table is responsible for supplying a corresponding MAC address to each IP address that was recently accessed from that machine or device. An IP address must be resolved to a MAC address before communication can occur to that IP address.

Administrators can specify how much of the network to search by selecting one of the following:

- Local subnet only
- Local subnet and one hop (router) away
- Entire network (unrestricted)

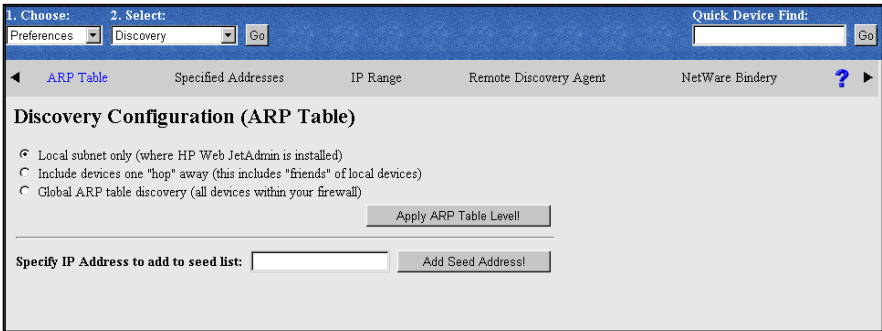
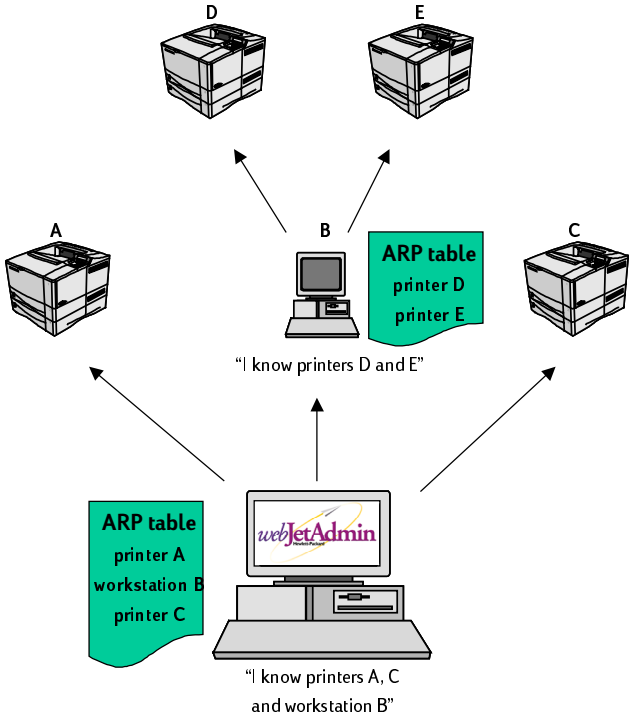
This discovery level setting determines how extensive the discovery will be, as well as how long it will take.

Advantages

- Avoids the use of broadcast traffic.
- Relatively thorough, if IP printing is prevalent such as HP Jetdirect Port, HP Standard Port, or LPR Port.

Disadvantages

- Can be time consuming if many hops are configured.
- Not very powerful if IP printing is not prevalent, such as in a strict Novell printing environment.



Specified Addresses

How Does It Work?

HP Web Jetadmin searches for devices defined in a hosts file (*hosts.txt*). The hosts file can contain any combination of IP addresses, IP host names, IPX addresses, or hardware addresses. This technique discovers devices by sending directed SNMP GET REQ packets to each device defined in the hosts file.

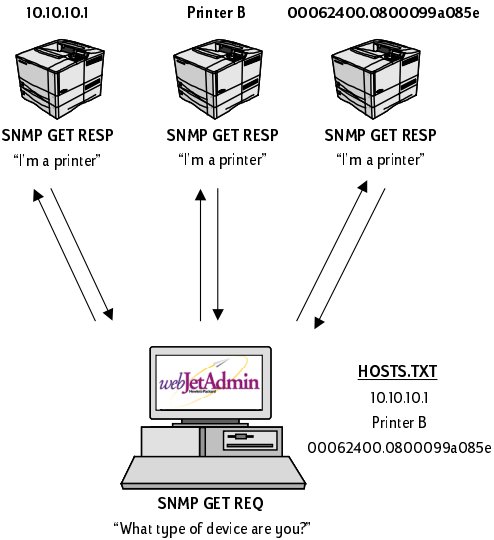
An existing hosts file can be uploaded by browsing for it under *Upload or Append a Host File*. Entries can be added to the hosts file either manually through an editor or under the *Add a Device to Host File* box. If HP JetAdmin was used prior, and a JETSET.ini file was being used for discovery, that file can be imported into HP Web JetAdmin to be used for the *Specified Addresses* technique under *Import a Jetadmin JETSET.ini File*.

Each line in the hosts.txt file represents one device. Comments can be added by preceding the line with a # symbol. The size of this hosts file has no limit.

The hosts.txt file MUST reside under the following subdirectory:

```
<drive>:\Program Files\HP Web Jetadmin\doc
```

HP Web Jetadmin will only search for a file named *hosts.txt* to use for this discovery mechanism. Therefore, the *hosts.txt* file cannot be renamed.

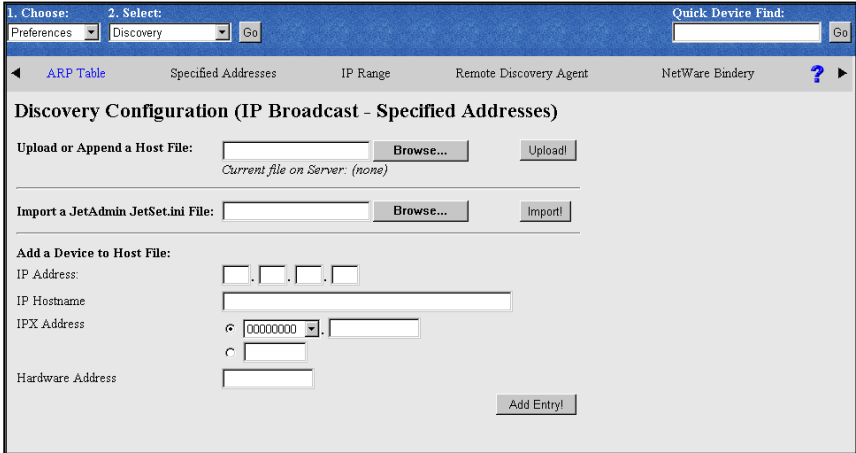


Advantages

- Generates very little network traffic.
- Exceptionally accurate for local and remote subnets or networks, as long as the devices listed in the file actually exist on the network.

Disadvantages

- Can be time consuming if a large number of devices are entered into the hosts.txt file.
- Can be labor intensive to create the hosts.txt file.



IP Range

How Does It Work?

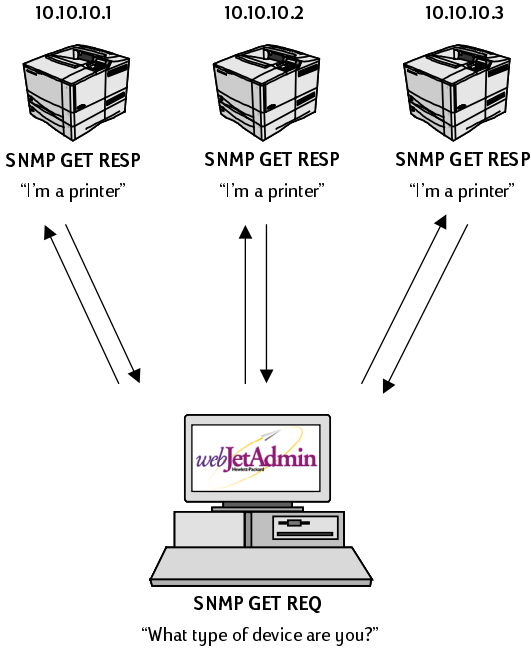
HP Web Jetadmin will send "bursts" of directed SNMP GET REQ packets to each IP address or range of IP addresses entered, regardless of whether the IP address is a printer or exists at all.

In order to locate each device, the operating system will generate ARP packets for each device to resolve the IP address of the device to a MAC address. The ARP packets will be followed by SNMP GET REQ packets to each IP address to gather information about the device.

To specify a range of devices to be discovered, enter the starting IP address of the range in the *Start Search from* box, and the ending IP address of the range in the *End Search on* box, and select *Apply* under *Add a Range of IP Addresses to Discover*.

To automatically enter the current subnet where HP Web Jetadmin is running, select *Add Current Subnet* under *Determine Current Subnet and IP Range*.

To delete a range of devices from being discovered, select the range from the drop-down list under *Current IP Ranges* and select *Delete Range*.

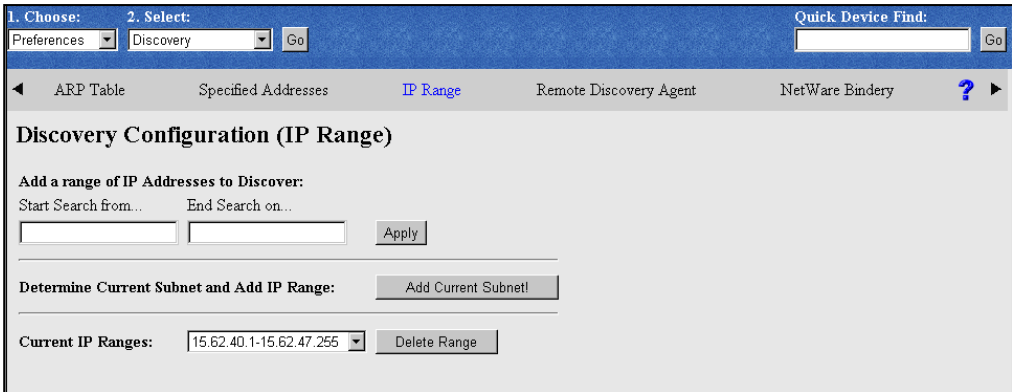


Advantages

- Very accurate for the range(s) selected,
- Can discover devices on remote subnets.

Disadvantages

- Can be very slow since it queries each and every IP address in the range(s) entered, no matter what type of device (workstation, printer, etc.) is in that range.



Remote Discovery Agent

How Does It Work?

HP Web Jetadmin allows an administrator to select a machine (NT, 2000, UNIX, Linux) on a remote subnet that will act as a discovery proxy. *Remote Discovery Agent* (RDA) is a piece of software that HP Web Jetadmin pushes to a machine on a remote subnet to perform a discovery of devices on that subnet. This software runs as a service (NT/2000) or daemon process (Unix/Linux) on the remote machine, performing a discovery using any available HP Web Jetadmin discovery mechanism(s). Once completed, the RDA agent will report its discovered information back to the machine running HP Web Jetadmin through TCP packets.

The primary purpose of *Remote Discovery Agent* is to discover unconfigured IP devices on a remote subnet. However, this technique is also useful if SNMP traffic is being filtered at the routers. While RDA will issue SNMP packets on the subnet where it is running, it will use only TCP packets to communicate back and forth with the Web Jetadmin machine. This means no SNMP traffic across the router. If SNMP or directed UDP port 161 packets are being filtered at routers, this discovery method is still a viable option

A machine running the RDA service can be instructed to perform any of the available discovery options that HP Web Jetadmin offers. It can also schedule exactly when discoveries will be performed.

The machine pushing the RDA service must have appropriate rights (administrator/root) on the remote machine to launch a service.

A Microsoft NT/2000 machine can push the RDA service to another Microsoft NT/2000 machine without adding any additional plug-in software to the HP Web Jetadmin machine. However, for a Microsoft NT/2000 machine to

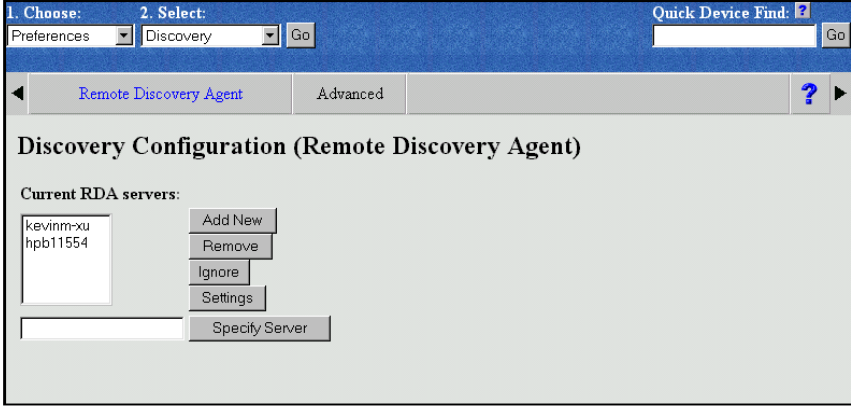
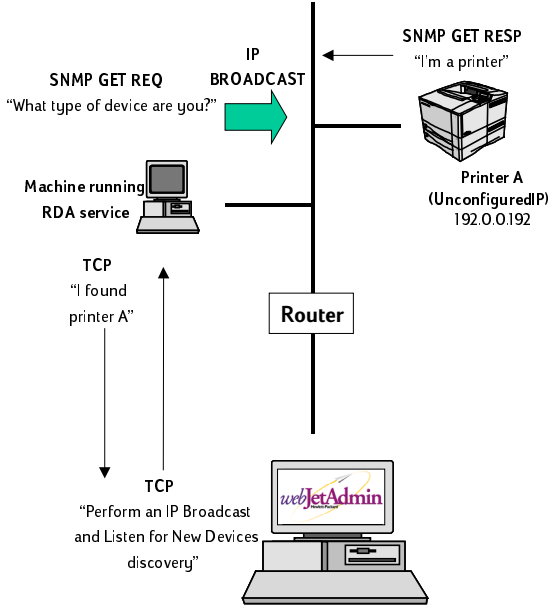
push the RDA service to a Linux machine, an additional plug-in must be obtained from the HP web site. Also, a Linux machine can push the RDA service to another Linux machine, but not to a Microsoft NT/2000 machine.

Advantages

- Can discover IP devices on remote subnets.
- Reduces SNMP traffic across routers. Communication between Web JetAdmin and RDA agent uses TCP packets. SNMP or directed UDP port 161 packets can be filtered at routers without affecting accuracy.

Disadvantages

- May take time to select machines to act as proxy agents for all remote subnets.



NetWare Bindery Scan

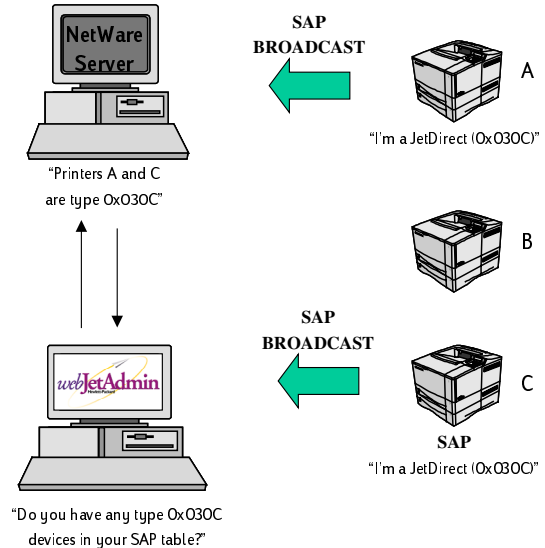
How Does It Work?

HP Web Jetadmin scans the binderies, or SAP tables, of all selected Novell NetWare file servers for HP JetDirect devices (type 0x030C). This technique relies upon HP Jetdirect devices to send SAP packets to advertise their existence. NetWare file servers populate their SAP tables with information contained within these packets. HP Web Jetadmin will parse these tables to find HP Jetdirect devices.

HP Web Jetadmin will send additional SNMP queries to the devices that it finds to gather more detailed information about each device.

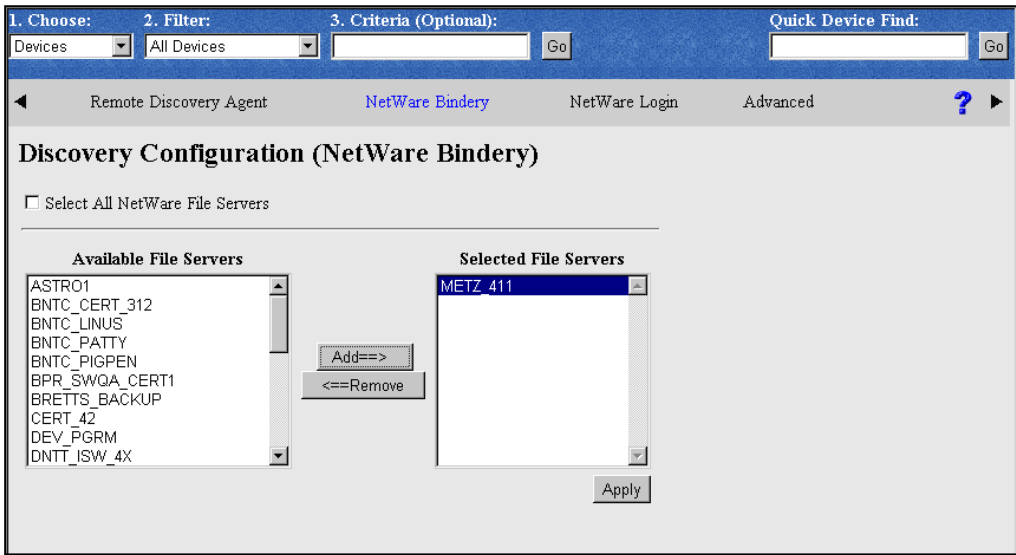
Advantages

- Allows the ability to select any or all NetWare file servers in which to parse for HP Jetdirect devices. This can be beneficial if SAPs are filtered at routers, in which case individual NetWare file servers may have different devices populating their SAP tables.
- Accuracy is very good if SAPs are not disabled.
- SAPs can be disabled at routers since all servers can be chosen from which to perform the bindery scan.



Disadvantages

- Disabling SAPs on the Jetdirect devices will affect accuracy.
- Discovery time can be long (especially over WANs)
- Network traffic can be high if binderies are being scanned on multiple servers



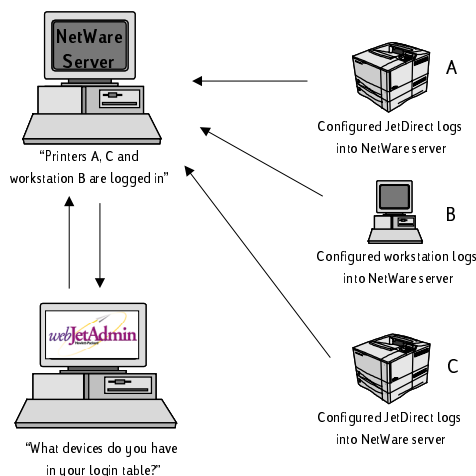
NetWare Login Scan

How Does It Work?

Configured HP Jetdirect devices log into a Novell NetWare server (take up a license) if configured for Queue Server Mode.

HP Web Jetadmin scans the connection table (login list) on each NetWare server it is logged into, generates a list of HP Jetdirect devices connected, and searches for them.

The NetWare server reply will include all HP Jetdirect devices logged in as well as all users logged in from various workstations.

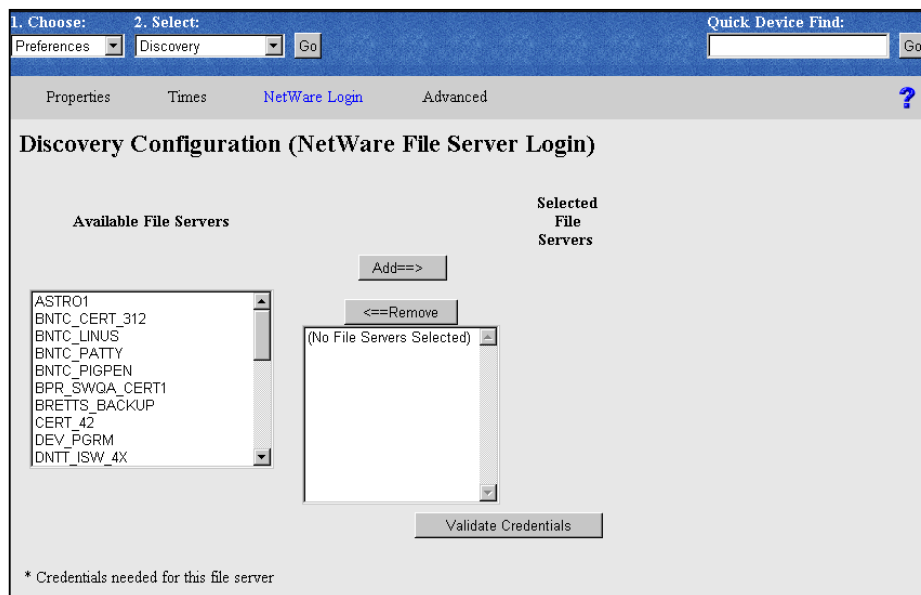


Advantages

- Very low network traffic.
- Very fast discovery.
- Very accurate for servers logged into.
- HP Jetdirect devices with SAPs disabled will be discovered.

Disadvantages

- Cannot find unconfigured IPX devices.
- Cannot find devices configured for Remote Printer Mode.



Listen for New Devices

How Does It Work?

Listen for New Devices is a passive form of discovery that continually monitors the network for new print devices. Specifically, it listens for the following signals sent from devices:

- Service Advertising Protocol (SAP) packets
- BOOTP requests
- DHCP requests
- Service Location Protocol (SLP) packets

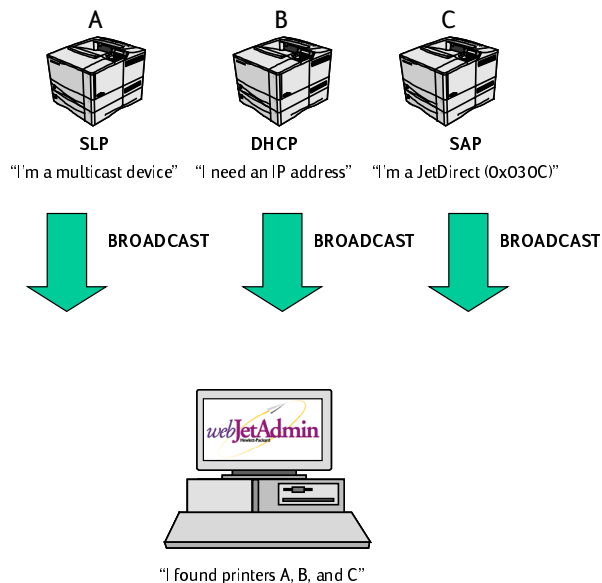
When HP Web Jetadmin detects one of these signals, it collects additional information by sending SNMP request packets, and adds the device to the list of discovered devices.

Advantages

- Keeps new devices added to the list of discovered devices as they are powered up.
- It is the least intrusive form of discovery since it takes advantage of normally occurring network traffic.

Disadvantages

- The results are not as reliable as other methods. It can find most unconfigured devices if they are powered on while HP Web JetAdmin is running. However, it cannot find devices that have been configured for static IP addresses or have SAPs disabled.



BOOTP Server

How Does It Work?

HP Web Jetadmin includes a BOOTP server service to aid in discovering unconfigured IP devices on remote subnets. As long as BOOTP packets are not being filtered at routers, HP Web JetAdmin can provide basic IP parameters to unconfigured devices on remote subnets in order to discover them. By entering the MAC address of the device into HP Web Jetadmin, the following IP parameters can be configured on the device:

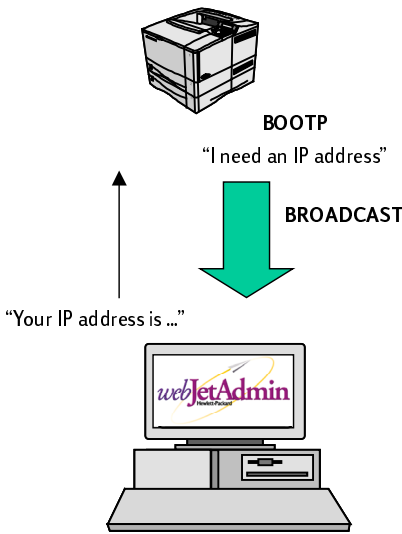
- IP address
- Subnet mask
- Default gateway
- IP hostname

Advantages

- Allows for Web Jetadmin to discover unconfigured IP devices on remote subnets.
- Can configure remote unconfigured IP devices as long as BOOTP packets are not being filtered at routers.
- Can set the IP hostname on a device.
- Can replace an existing BOOTP server.

Disadvantages

- No TFTP parameters can be configured. Thus, this service may not be a true replacement for an existing BOOTP server that has TFTP parameters.
- If routers are filtering BOOTP packets, configuration can only occur for devices on same subnet.



1. Choose: Preferences		2. Select: Discovery		Go		Quick Device Find: <input type="text"/>		Go	
Remote Discovery Agent		NetWare Bindery		NetWare Login		BOOTP		Advanced ?	
BOOTP Server Configuration									
Add device to bootp table:									
MAC Address:	<input type="text"/>	(e.g. "0060b042a569")							
IP Hostname:	<input type="text"/>	(e.g. "myhost.domain.com")							
IP Address:	<input type="text"/>	(e.g. "192.168.1.4")							
Subnet Mask:	<input type="text"/>	(e.g. "255.255.255.0")							
Gateway Address:	<input type="text"/>	(e.g. "192.168.1.1")							
<input type="button" value="Add Entry!"/>									

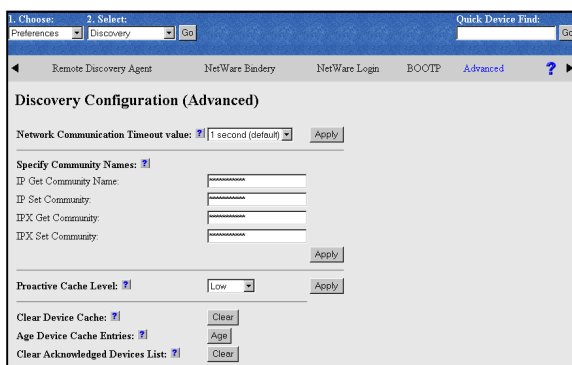
Advanced Discovery Settings

HP Web Jetadmin contains advanced discovery settings to allow for customization of network parameters that can improve discovery accuracy, minimize the amount of time taken to perform discovery, and control network traffic.

For example, if HP Web Jetadmin is performing a discovery on a network where response times are slow, such as a large WAN or through dialup networking, then the accuracy of the discovery may suffer due to slow response times.

The following areas of HP Web Jetadmin contain configuration options that can improve the accuracy of information obtained for devices, decrease discovery times, and minimize network traffic:

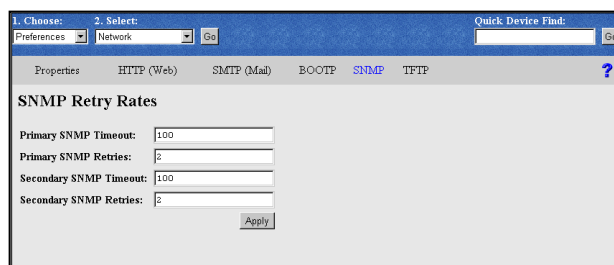
Preferences, Discovery, Advanced



- *Network Communication Timeout* controls the amount of time HP Web Jetadmin will wait for responses to directed SNMP packets during a discovery. Default is *1 second*. This parameter may need to be increased for large WANs or dialup networking if responses are suspected to be taking longer than one second. Also, if there is doubt concerning the accuracy of discovery, increasing this parameter may help.
- *Proactive Cache Level* controls the accuracy of the information stored in the database of devices. *Low* means that device information stored in the database will be queried more often. While this increases network traffic, it provides better accuracy of device information stored in the database. *High* means that information stored in the database will not be queried as often. While this decreases network traffic, the possibility exists that information stored in the database for some devices may be old or incorrect information.

- *Age Device Cache Entries* marks all of the information stored in cache about each device as old information. When HP Web Jetadmin needs to display any of this cached information, it will query the device for new information in case the cached information is no longer correct. This parameter should be enabled if discoveries are not performed very often, and it is believed that information stored in the cache for each device may not be accurate.

Preferences, Network, SNMP

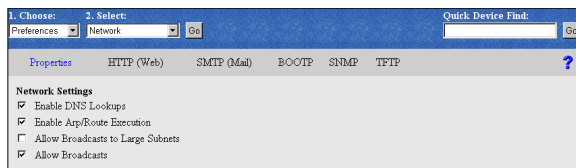


- *SNMP Retry Rates*

Primary and Secondary SNMP Timeout configures the amount of time HP Web Jetadmin will wait for a response to a directed query to a device while populating the cache with information. Default for *Primary* is *100 ms (1/10 s)*. If the *Primary* inquiries receive no responses, the *Secondary* inquiries will be attempted, in which the default timeout will be increased to *1000 ms (1 s)*. If it is suspected that some devices are not displaying all capabilities or functionality, increase this parameter.

Primary and Secondary SNMP Retries configures the number of times HP Web JetAdmin will send the same query to a device if it doesn't receive a response in the allotted amount of time while populating the cache with information about the device. If the *Primary* inquiries receive no responses, the *Secondary* inquiries will be attempted. The default number of attempts for both *Primary* and *Secondary* is *2* attempts. Increasing this parameter can increase network traffic because additional inquiries will be sent. These values can be increased if collisions are suspected as a reason for responses not being received to inquiries.

Preferences, Network, Properties



- *Enable DNS Lookups* will force HP Web Jetadmin to attempt to locate the hostnames for devices through a WINS/DNS server when displaying the list of devices. This parameter can cause drastic increases in the length of discovery time if the WINS/DNS servers are not responding or are configured incorrectly.
- *Enable ARP/Route Execution* allows HP Web Jetadmin to perform ARP table lookups. This parameter must be enabled to perform an ARP discovery.
- *Allow Broadcast to Large Subnets* allows HP Web Jetadmin to send broadcast packets to class B or larger subnets (255.255.0.0). Enabling this parameter can cause a substantial increase in network traffic during broadcast discoveries since class B subnets are comprised of 65K+ devices.
- *Allow Broadcasts* allows HP Web Jetadmin to send broadcast packets during discovery. If this box is unchecked, HP Web Jetadmin will not perform any discovery techniques that involve broadcast packets, even if they are enabled.

Additional Broadcast Parameters

A file titled *HPENUM.INI* contains additional parameters not found in the HP Web Jetadmin user interface that can affect discovery techniques that issue broadcast packets. The file can be found under the following subdirectory:

<drive>\Program Files\HP Web JetAdmin

A category titled *[settings]* contains the following parameters that can affect broadcast discovery behavior:

BroadcastRepeatCount=3 - configures the number of broadcast packets sent to each network segment for discovery techniques that utilize a broadcast. Default value is 3. Increasing this parameter can improve accuracy for broadcast discovery techniques since it can potentially discover devices that were lost due to collisions in a prior broadcast. However, increasing this parameter will substantially increase network traffic during broadcast discoveries. An algorithm is performed so that

unnecessary broadcasts will not occur. For example, if the first broadcast returns zero entries, a second and third broadcast will not be attempted. Also, if the first and second broadcast results are identical, a third broadcast will not be attempted.

NumBroadcasts=1 - Configures the number of different types of IP broadcast packets that will be sent to each subnet for discovery techniques that utilize an IP broadcast. Default value is 1. Increasing this parameter can improve discovery accuracy because different types of IP broadcast packets may discover different devices. This value is multiplied by the value set for *BroadcastRepeatCount*. For example, if this value is set to 2, and *BroadcastRepeatCount* is set to 3, a total of 6 IP broadcast packets will be sent during discovery.

BroadcastBufSize=640000 - configures the memory size that is allotted for all broadcast responses to broadcast inquiries sent by HP Web Jetadmin. For large subnets or segments, if it is suspected that the number of responses is exceeding this amount of memory, increase the value appropriately.

Conclusion

Devices such as networked printers must be discovered before they can be configured or managed. Desirable factors for discovery include speed, accuracy, and simplicity. HP Web Jetadmin provides a multitude of search and discovery mechanisms to fulfill these desirable discovery factors. Also, many configuration options are available to minimize discovery traffic, increase discovery accuracy, and speed up discovery times greatly.