DISCOVERING DEVICES
using HP Web Jetadmin

CONTENTS

OVERVIEW

Device discovery enables HP Web Jetadmin to find both network-connected and PC-connected printers, scanners, and multifunction products (MFPs) and add them to the HP Web Jetadmin **All Devices** list. In many cases, the administrator may have information about the network that can improve discovery. However, some discovery features enable the administrator to search for devices without the benefit of networking details.

The powerful discovery engine in HP Web Jetadmin can locate most devices on both small and large networks. HP Web Jetadmin also includes a new discovery for printing devices located in Microsoft® Active Directory. Scheduling and discovery templates allow administrators to tailor HP Web Jetadmin to any topology or geographically deployed device fleet.

New in HP Web Jetadmin discovery

- Improved workflow for discovery using credentials
- Specified IP discovery groups
- Specified IP discovery files

PART 1—HOW DISCOVERY WORKS

Discovery is a two-part process. HP Web Jetadmin discovery always begins by scanning the network to find active nodes. Active nodes are any networked device that responds to the discovery method used by HP Web Jetadmin. Once this is complete, HP Web Jetadmin begins a resolution process to qualify whether devices are PC-connected or network-connected. Here is a look at what HP Web Jetadmin does during a typical discovery sequence:

Figure 1—Node discovery and Node resolve

- **Node discovery**
  - Scans using the first method according to discovery settings
  - Scans using the second method according to discovery settings
  - Continues to scan, using each method selected in discovery settings
- **Node resolve**
  - Queries all discovered nodes to find either PC-connected or network-connected devices
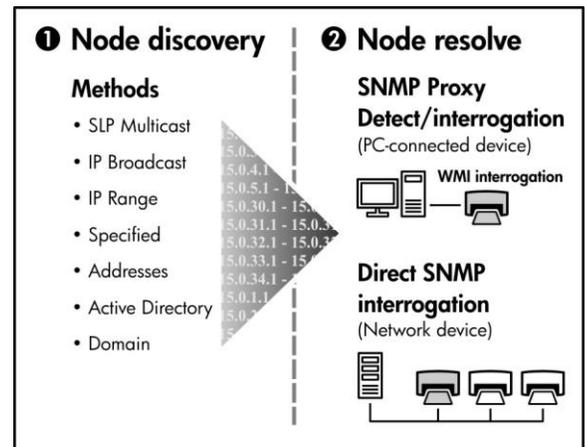 - Adds resolved nodes to **All Devices**

Discovery settings

The **Device Discovery** wizard's **Specify discovery options** pane is used to initialize discovery settings (Figure 2). Launch the **Device Discovery** wizard by right-clicking the **Discovery** node in the HP Web Jetadmin navigation tree. **Use template**, **Specify settings,** and **Schedule discovery** are the discovery options covered in this document. To begin a new discovery, select **Specify settings** and choose either **Network connected devices** or **PC connected devices**. Then choose one or more of the various methods of discovery (the options in the next few screens will vary depending on the methods selected). It is not possible to run both PC-connected and network device discovery at the same time, but it is possible to schedule them to run consecutively. Click **Next** to go on to the rest of the settings needed to complete the discovery setup.
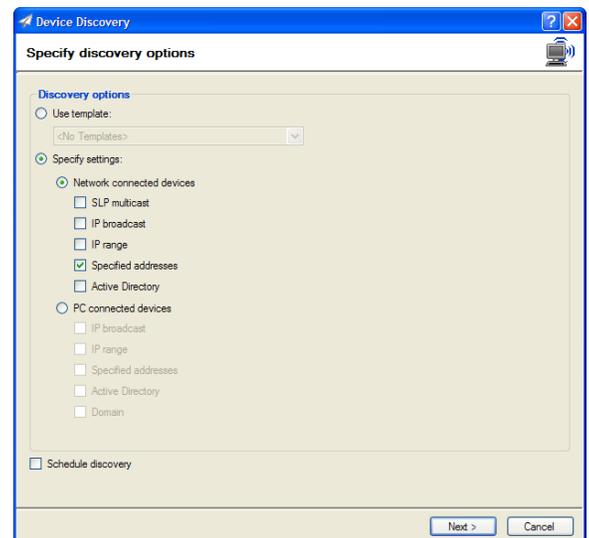

Figure 2—Device Discovery > Specify discovery options

Network device discovery vs. PC-connected discovery

Both PC-connected and network-connected device discoveries result in devices added to the **All Devices** list. Network devices, when discovered, are manageable from within HP Web Jetadmin. Administrators can remotely change device settings, get troubleshooting details, collect device specifics, and create device reports. PC-connected devices are less manageable due to the restrictive nature of the connection.

Network discovery specifics

SNMP is used as the primary communication method for discovering and qualifying network-connected devices before they are added to the **All Devices** list. HP Web Jetadmin uses a combination of standard and proprietary management information base (MIB) objects to both discover and manage network devices. In fact, HP Web Jetadmin is capable of discovering non-HP devices through the standard MIB (manageability varies depending on the manufacturer and model).

PC discovery specifics

HP Web Jetadmin finds PC-connected devices by first discovering the Microsoft® Windows® host and then querying it to find devices connected to the LPT or USB port. Once HP Web Jetadmin has finished the first (node detection) portion of the discovery, it uses either SNMP or Windows Management Instrumentation (WMI) to discover devices. To use SNMP, the HP SNMP Proxy Agent must be deployed onto the Windows hosts (see "Appendix D" on page 20 for more information). To use WMI, HP Web Jetadmin requires Windows credentials for local administrator access to the Windows host.

If a PC-connected device has been discovered with the HP SNMP Proxy Agent, HP Web Jetadmin collects a limited set of details from the device and supports a few management features such as **Status**, **Troubleshooting**, and **Reporting**. When the PC-connected device has been discovered via WMI, only limited device model information will appear in the **All Devices** list.

It is important to note how HP Web Jetadmin performs the second portion (node resolution) in PC-connected discovery. Each Windows host discovered is first queried using SNMP—if a response is encountered, special printer queries are used to discover a device on the LPT or USB port. If the HP SNMP Proxy Agent and other requirements are met, a device connected to that host is discovered.

For more information about SNMP Proxy Agent, see the *Discovering PC-connected Devices in HP Web Jetadmin* white paper. This white paper is available from the HP Web Jetadmin support page (in English). If the SNMP discovery is not successful and if the user added Windows credentials to the discovery settings, HP Web Jetadmin performs a WMI query to determine whether a plug-and-play device is installed on any system ports. If a Windows plug-and-play device is installed and active on the host, the device is discovered and added to the HP Web Jetadmin **All Devices** list.

PC-connected discovery uses SNMP as the primary protocol, and WMI as the secondary protocol, for each of the following discovery methods:

- IP Broadcast
- IP Range
- Specified Addresses
- Active Directory
- Domain

NOTE   The HP SNMP Proxy Agent is required as a deployed service on remote Windows hosts. When using WMI, local administrator credentials are required.

Using credentials with discovery

During discovery setup, users have the option of entering credentials via the **Specify credentials** interface (Figure 3). This interface shows different options depending on whether PC discovery, network discovery, and SNMPv3 settings are enabled. Credentials are needed when:

- Performing PC-connected device discovery using WMI
- Performing network device discovery on devices with **SNMPv1 Get Community Name**
- Performing network connected device discovery on SNMPv3 devices

All of these conditions are outlined below.

NOTE   In the Device Discovery wizard, the **Specify credentials** interface follows the **Specify discovery settings** pane (covered in more detail in "Part 2—Discovery methods" on page 9).

Figure 3—Device Discovery > Specify credentials

PC-connected device discovery using WMI

PC-connected device discovery via WMI takes place only when an SNMP proxy agent cannot be found on the Windows host and when the user supplies Windows credentials as part of the discovery process. These credentials should allow local administrator access to the PC hosts. To enable WMI discovery, check **WMI Credentials** and add your **User name**, **Password**, and **Domain** in the **Specify credentials** pane.

Network device discovery using SNMPv1 Get Community Name

If SNMP Get community names other than the default "public" are used, HP Web Jetadmin must have awareness of the Get community name value. Devices with a Get community name other than "public" do not respond and therefore are not discovered.

Figure 3 shows two options for providing HP Web Jetadmin with Get community names. Under **SNMPv1 Get Community Name**, check the box and add the appropriate string in the field provided. Global credentials can also be used to designate SNMP Get community names. Check **Use global**

5

credentials and add the appropriate value(s) into **Tools** > **Options** > **Application Management** > **Credentials** > **SNMPv1 Get Community Name** (Figure 4).

Network device discovery on SNMPv3 devices

SNMPv3 devices can be discovered by HP Web Jetadmin when SNMPv3 discovery is enabled and HP Web Jetadmin contains valid SNMPv3 credentials. Once HP Web Jetadmin has discovered these devices, the SNMPv3 credentials are placed into the **Credential Store**. Initial discovery of these devices can be completed by following these steps:

Figure 4—Global Credentials > SNMPv1 Get Community Name

1. Navigate to **Tools** > **Options** > **Device Management** > **Discovery** > **General**. Enable **Discover SNMPv3 Devices**, and then click **OK**.

2. Navigate to **Tools** > **Options** > **Application Management** > **Credentials** > **SNMPv3 Credentials**. Add the appropriate credentials, and then click **OK**.

With these items complete, HP Web Jetadmin will detect and discover SNMPv3 devices.

Device Discovery Progress pane

The **Progress** pane in the **Device Discovery** wizard (Figure 5) displays the status of both the node and node-resolve portions of a discovery. This can make it easy to determine which stage has begun and which is currently running. The **Nodes found** counter shows the number of devices found using all discovery methods. After the first stage of discovery is complete, **Nodes resolved** and **Devices found** indicate device resolution. A counter showing devices new to this discovery is also included. The active discovery can be stopped at any time with the **Stop** button or sent into background tasks with the **Hide** button. Any user can see whether a discovery is currently running by navigating to the task module under **Devices** > **Active Tasks** (found under **Overview** in the navigation tree). The **Progress** pane shown here can be launched by clicking **View** from within this task module.

Figure 5—Device Discovery > Progress

Discovery in Progress

Any time a user invokes a discovery when a discovery is already running in the background, a dialogue box appears that allows the user to **View current discovery**, **Queue a discovery**, or **Schedule a discovery** (Figure 6). Any user logged into HP Web Jetadmin has the ability to invoke any of these controls.
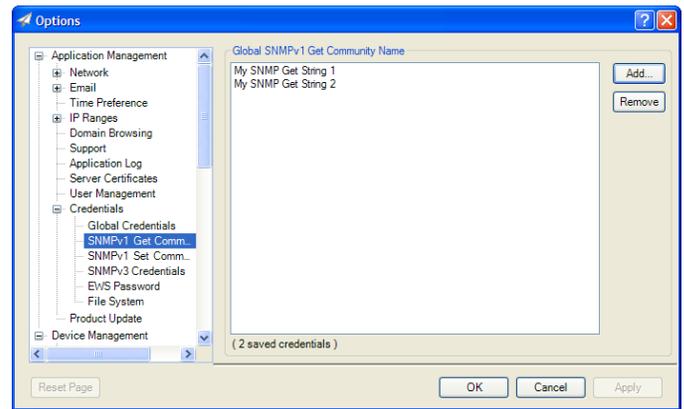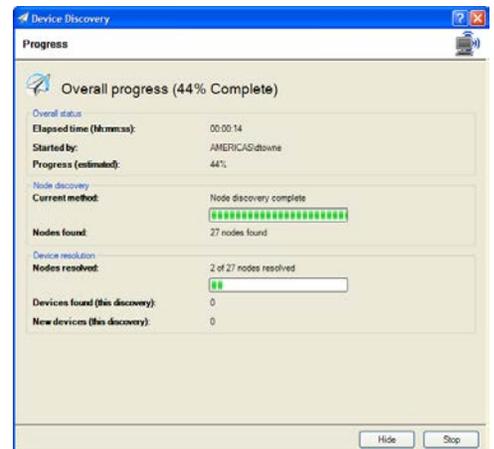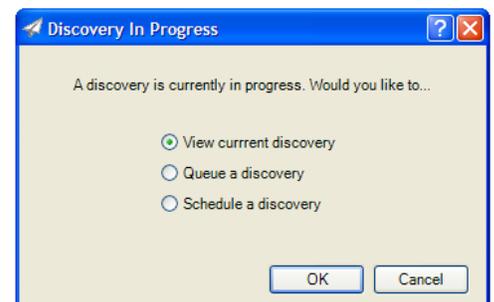

Figure 6—Discovery In Progress

Discovery History

Discovery History (Figure 7) can be opened by selecting its node from the navigation tree beneath **Discovery**. This tool makes it easy to analyze discovery methods and effectiveness. By expanding a specific discovery, you can see each discovery by date, the user who launched it, the time it took to complete, and the number of devices found. Users can compare methods within one discovery session by looking at the **New Devices** metric. Session to session comparisons can be made by using the **New Devices Found** metric. See HP Web Jetadmin Help for complete definitions and descriptions.
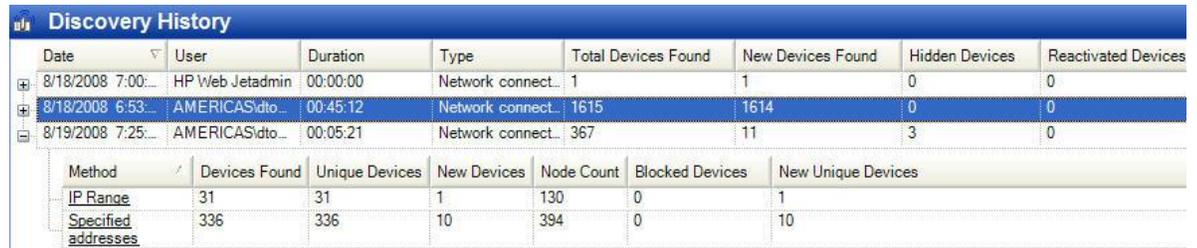
Date	User	Duration	Type	Total Devices Found	New Devices Found	Hidden Devices	Reactivated Devices
⊞ 8/18/2008 7:00:...	HP Web Jetadmin	00:00:00	Network connect...	1	1	0	0
⊞ 8/18/2008 6:53:...	AMERICAS\dto...	00:45:12	Network connect...	1615	1614	0	0
⊟ 8/19/2008 7:25:...	AMERICAS\dto...	00:05:21	Network connect...	367	11	3	0

Method	Devices Found	Unique Devices	New Devices	Node Count	Blocked Devices	New Unique Devices
IP Range	31	31	1	130	0	1
Specified addresses	336	336	10	394	0	10

Figure 7—Discovery History

Scheduling discovery

The **Device Discovery** wizard has a flexible scheduler with a wide variety of options (Figure 8). Unique device discovery schedules can be created that allow scanning different parts of the network on different days, times, and recurrence levels. For example, PC-connected discoveries can be scheduled during the day, when most users are logged onto the network—while network-connected discoveries can run later in the evening. Use the **Allow start time to occur between the specified hours of** option to prevent discoveries from running outside appropriate timeframes. This is especially helpful on systems where many scheduled tasks have been configured. Existing discovery schedules can be viewed and edited by using one of two task modules: launch **Scheduled Tasks** from the **Application Management** > **Overview** workspace or **Discovery** > **Scheduled Discoveries**.
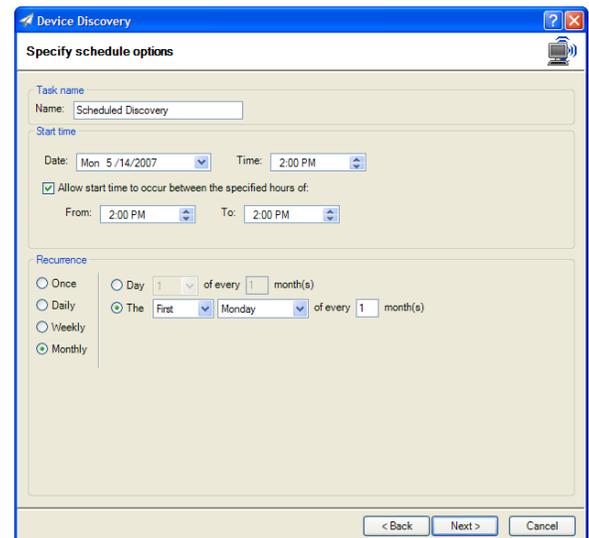
Figure 8—Device Discovery > Specify schedule options pane

Discovery templates

Discovery templates are like other templates in HP Web Jetadmin; they store pre-defined settings that can be retrieved at a later time. Both PC-connected and network device discovery settings can be stored in many uniquely named templates. Once a discovery template has been created, it can be launched or scheduled for launch through the **Device Discovery** wizard with the **Use template** option. **Create**, **Edit**, **Remove**, **Launch**, and **View** features are all available through **Device Management** > **Discovery** > **Templates**.

Last Communication and Last Discovered columns

Two columns in HP Web Jetadmin allow the administrator to track the date and time of both the last discovery date and the last application-to-device communication (Figure 9). These columns are useful for troubleshooting to determine whether a device exists on the network, has communication issues, and more. These also allow the administrator to determine when device data in HP Web Jetadmin was last updated.

Figure 9—Last Communication and Last Discovered

Quick Monitor

HP Web Jetadmin allows discovery of a specific device to monitor its status from anywhere in the client application. The **Quick Monitor** task module (Figure 10) can be enabled from the **Task Module** docking area or from within the **Discovery** > **Overview** workspace. Enter the device's IP address in **Device** and click **Go**, or drag a device from any device list into the **Quick Monitor** task module.
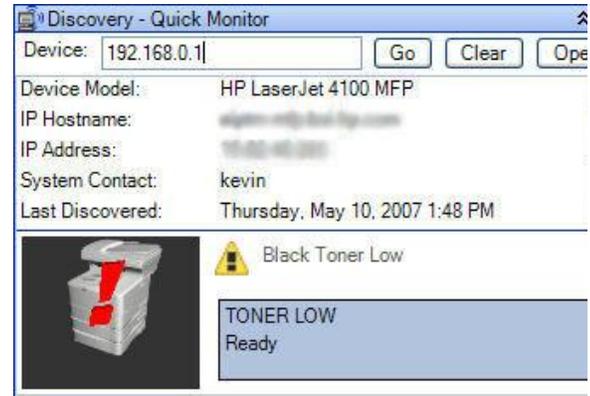

Figure 10—Device Quick Monitor task module

NOTE   Task modules are elements that can be activated from within most of the top level summary workspaces and from within the **Task Module** docking area. Task modules supply the user with instant information and can offer actions or controls relevant to the specific feature.

Device blocking

A list exists in **Tools** > **Options** > **Device Management** > **Device Lists** > **Blocked Devices** that keeps HP Web Jetadmin from discovering a device. Sometimes, administrators may desire that a device not appear in **Discoveries**. This list can be manually edited or devices can be added by using right-click from the **All Devices** list. The **Delete and Block** option places the device into the blocked devices list where it will stay until manually removed.

Device uniqueness

Each time HP Web Jetadmin performs a discovery and finds a qualified device, it checks certain device *uniqueness* attributes. It does this to both test the device's unique identity (for devices that have already been registered at a specific IP address and have had uniqueness attributes stored) and to register and store new uniqueness details. Uniqueness attributes include device serial number, device model number, and device model name. Devices that do not support serial number objects are registered as non-unique. It is important to understand that changing device identities can only be detected by HP Web Jetadmin during a full discovery (not through **Quick Device Discovery**.) Devices stored with unique identities enable a number of HP Web Jetadmin features, such as reporting, because Web Jetadmin is able to distinguish devices from one other.

PART 2—DISCOVERY METHODS

Now that we have looked at discovery features and workflows, we can return to the issue of individual methods of discovery. The variety of methods available provides the flexibility to tailor discoveries for specific environments. Some administrators need to find all devices in an enterprise and may find that **IP range** discovery, when correctly configured, results in successful and efficient device discoveries. Other administrators may only need to discover local devices. These administrators might find that **IP broadcast** in combination with **SLP multicast** work best. In all cases, HP Web Jetadmin discoveries require SNMP communication between the devices and the application. Most modern networks allow this protocol, which makes HP Web Jetadmin a robust platform for performing device discoveries.

Quick Device Discovery

Quick Device Discovery is comparable to **Quick Device Find** in earlier versions of HP Web Jetadmin (Figure 11). Characteristics of **Quick Device Discovery** include:

- Discovers only one device at a time based on user-supplied IP hostnames or IP address

- Does not discover PC-connected devices

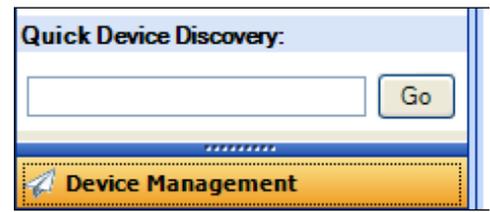- Is not launched from the **Device Discovery** wizard

Figure 11—Quick Device Discovery

This feature is always visible in the **Device Management** view just beneath the navigation tree. Simply enter either an IP hostname or IP address string and click **Go**. **Quick Device Discovery** only acts on address information. The feature searches device addresses in the HP Web Jetadmin database before performing a network query. If a device is found at the address provided, it is added to the **All Devices** list. This feature is different from **Search** and **Advanced Search** (found in the device list toolbar) which parse all or selected strings within device lists.

SLP (Service Location Protocol) multicast discovery

SLP multicast discovery requires minimal settings to launch and multicasts a query onto the network to find a specific device type. Characteristics of an **SLP multicast** discovery are:

- Only HP Jetdirect-connected devices are discovered

- Multicast packets are sent to the HP Jetdirect specific multicast address: 224.0.1.60

- Packets contain a router hop-counter (IP time-to-live attribute) that is configurable from within HP Web Jetadmin (default 4 hops)

- Packets expire when the router hop-counter reaches zero

- Fast discovery mechanism

- Low impact on network traffic

The **SLP multicast** discovery was implemented in early HP Web Jetadmin releases and is effective in finding HP Jetdirect devices on both local and remote subnets. It has a small footprint on the network.

IP broadcast discovery

IP broadcast discovery enables administrators to find devices when IP broadcast addresses are known. Characteristics of **IP broadcast** discoveries are:

- Works on both PC-connected and network devices

- Sends SNMP queries over one or more IP broadcasts

- Devices that reply are placed into the **Nodes found** group and await node resolution

- Fast and thorough, especially on a local segment
- Most modern networks block broadcast traffic
- PC discovery settings are the same as network discovery settings
- May not find PC-connected devices without the HP SNMP Proxy Agent

IP broadcast discoveries send SNMP query packets in the form of IP broadcasts, to one or more IP network(s). One network-specific broadcast address exists for each IP subnet on an IP intranet. In addition, a broadcast containing only "1" in all its digits can be used on any IP network (HP Web Jetadmin uses this as the default IP broadcast address). IP subnets are determined by the IP network number and the IP subnet mask.
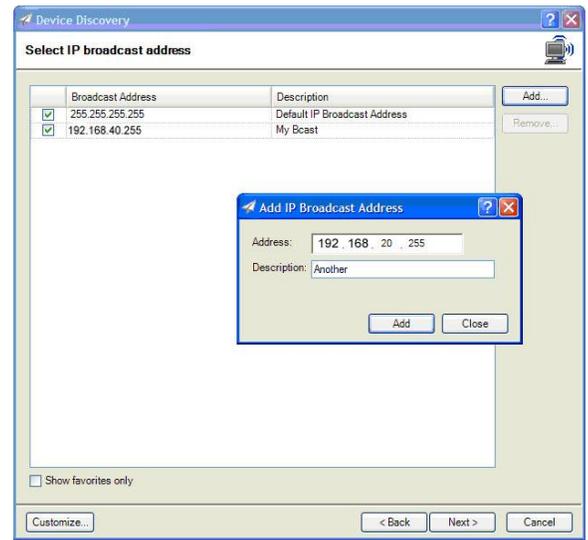

Figure 12—Select IP broadcast address pane

Administrators can calculate and enter any variety of **IP broadcast** addresses into the **Select IP broadcast address** pane in the **Device Discovery** wizard (Figure 12). IP range calculators, available for free on the web, are a great way to determine **IP broadcast** addresses. Broadcasting is typically blocked by routers due to traffic spike concerns.

IP range discovery

IP range discovery is the most powerful way to discover all or nearly all devices in an enterprise. The **Select IP ranges** interface is used to add, remove, or edit IP range data (Figure 13). IP ranges can also be imported from or exported to flat text files. The **Calculate range** feature adds IP ranges based on the client host, server host, or known IP address information. Large subnet protection is engaged by default which keeps the application from spanning too many addresses, unless absolutely necessary. Characteristics of **IP range** discoveries are:

- Discovers both PC-connected and network devices
- IP ranges are simply two addresses that represent range begin and end points
- Multiple ranges can be specified
- Users can manually edit or import ranges from a file
- Descriptive tags help to identify ranges
- Application sends one query to each address represented by the range
- HP Web Jetadmin pings the device ranges in bursts, which limits the network footprint
- **Calculator** feature adds IP ranges based on:
  - Local client host
  - HP Web Jetadmin server host
  - Device
- Can be very slow if not configured properly
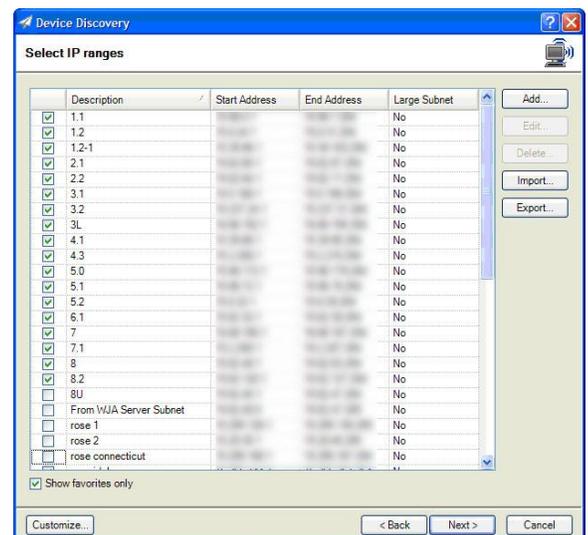- Can draw security attention

Figure 13—Select IP ranges pane

Importing ranges from a file

Many IP ranges can be imported via text files. In many cases, administrators work with hundreds and even thousands of IP ranges and have to manage the data in another form, such as a spreadsheet. In these cases, a very simple file format can be used as the link between the administrator's preferred application and HP Web Jetadmin **IP range** discovery. Here is a look at the file format used in importing (and exporting) IP range data:

> 15.121.10.2-15.121.17.254=My Range
>
> 15.255.14.1-15.255.21.254=Your Range
>
> 15.121.10.2-15.121.17.254=Our Range
>
> 15.255.12.1-15.255.19.254=Their Range

- One range per line
- Begin and end addresses separated by a hyphen
- Optional text description separated from the range data by an equal sign

This text file and the **IP range** discovery feature have no known size limit. For more details on using the **IP range** discovery feature, see "Appendix C" on page 18.

Specified address discovery

Specified address discovery sends a query to each address listed in its discovery settings. Characteristics of **Specified address** discovery are:

- Finds both PC-connected and network devices
- Based on user-supplied addresses
- IP address and hostnames are valid address forms
- Works quickly and only queries specified addresses
- Only effective to the extent that the specified addresses are accurate
- Addresses can be imported from a text file

This discovery is powerful when device addresses are known. It does require some maintenance when addresses change or devices are added to or removed from the fleet. Device address types include IPv4 addresses, network resolvable IP Hostnames, and network resolvable fully qualified domain names (FQDNs).

An address base can also be imported from or exported to a text file for use in other applications or editors. Here is an example of a specified address file using the various types of address forms:

> 15.5.2.1
>
> 15.5.62.4
>
> 15.5.8.3
>
> 15.5.8.7
>
> BP065
>
> BP076.yourco.com

Figure 14 shows the **Select addresses** interface for **Specified address** discovery. Address groups can be created, allowing the administrator to manage
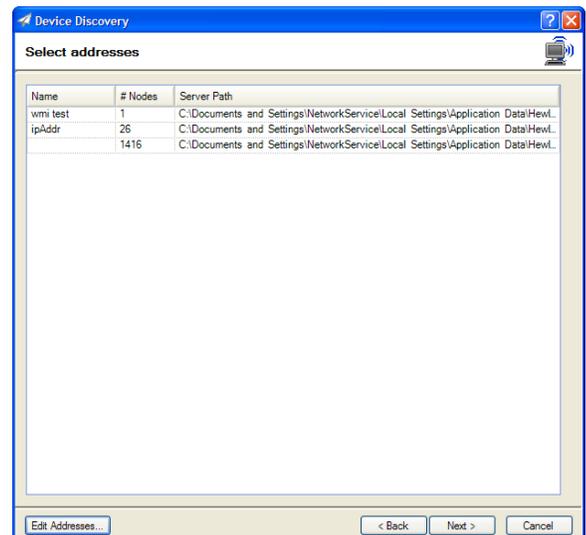

Figure 14—Specified address settings

11

blocks of IP addresses in named groups. In addition, the named IP address groups can be found in an HP Web Jetadmin server file once they have been created. The contents of this file can be manipulated on the fly to support discovery automation.

The path of these files is:

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin \WjaService\config\FileStore\Discovery\Specified

Active Directory discovery

HP Web Jetadmin provides a new discovery feature that queries Active Directory using an Active Directory starting point such as domain, Organizational Unit (OU), or other Active Directory containers. Characteristics of an **Active Directory** discovery are:

- Finds both PC-connected and network devices
- Requires a directory search start point (multiples possible)
- Searches within a specified container or includes all sub-containers
- Allows filtering based on Active Directory queue attributes: Location and Description
- Populates Active Directory device attributes viewable in HP Web Jetadmin filters and columns

Figure 15 shows the **Specify Active Directory options** pane within the **Device Discovery** wizard. To enable **Active Directory** discovery, administrators specify a starting point such as:

LDAP://YourOrg.com/OU=US,OU=Printers…

Administrators can also choose to perform recursive queries, such that any sub-units below the specified path are searched. If the **Current level** option is selected, HP Web Jetadmin searches the immediate child objects of the base object, excluding the base object. The **All levels** option searches the whole subtree, including the base object and all child objects. The administrator can also perform discovery on multiple Active Directory locations. And, the discovery can also be filtered on both location and description strings if these are published to the Active Directory.
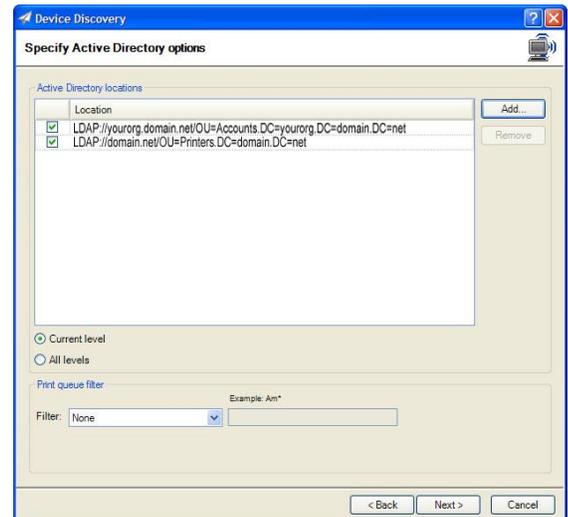
Figure 15—Specify Active Directory options pane

Active Directory and network device discovery

The **Active Directory** discovery method scans the directory for shared Windows printers when it is used to find network connected devices. From the printer shares, the discovery is able to extract IP address information from the printer port name. The following IP address string formats are supported in discovering devices with this method:

- ip_<ip-addr> (case insensitive)
- mt:<ip-addr> (case insensitive)
- ***ip_<ip-addr> (case insensitive, "***" can be anything not containing "ip_")
- <ip-addr>:*** (case insensitive, colon after the IP address)
- <ip-addr> *** (case insensitive, space after the IP address)
- <ip-addr>-*** (case insensitive, dash after the IP address)
- <ip-addr>_*** (case insensitive, underscore after the IP address)

When the port name contains a valid IP address in any one of these formats, a node discovery is completed. If the port name does not match one of these seven formats or if the IP address is not valid, the network device may not be discovered. Later, in the node resolve portion of discovery, these IP addresses are checked for valid devices which are added to the HP Web Jetadmin **All Devices** list.

Active Directory and PC-connected device discovery

The **Active Directory** discovery method for PC-connected devices simply scans the directory for supported Windows hosts. When a qualified Windows host is found, its address detail is added to the **Nodes found** group. Later, these nodes are queried to determine whether the HP SNMP Proxy Agent is deployed on them or, if Windows credentials are supplied, the discovery attempts to find a qualified device via a WMI query. Valid devices, if found, are placed in the HP Web Jetadmin **All Devices** list.

Domain discovery

- For PC-connected discovery only
- Uses Active Directory or non-Active Directory domain as a starting point
- Finds and uses Windows hosts to discover local printers
- Multiple domains can be specified

The **Domain** discovery method uses the Active Directory or Windows domain as a starting point to search for supported Windows hosts. All supported Windows hosts are placed into the **Nodes found** group and queried for the HP SNMP Proxy Agent. If the HP SNMP Proxy Agent is not found on the host and if the user supplied Windows credentials, a WMI query is attempted. All discovered devices are placed into the **All Devices** list.

Using the Customize feature

The **Customize** button is found in most of the settings panes for each discovery method and is used to control a list of personalized favorites (Figure 16). All users have the ability to select favorites from a global set of discovery settings, such as IP ranges, and then choose to display their favorites using the **Show favorites only** checkbox. This keeps them from having to see all discovery settings.
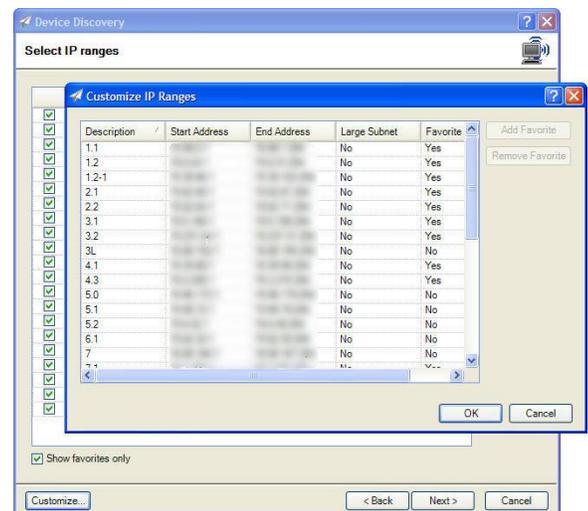
Figure 16—Customize IP Ranges

DISCOVER AND SYNCHRONIZE OTHER HP WEB JETADMIN SERVERS

To discover other installations of HP Web Jetadmin, go to **Application Management** > **Web Jetadmin Installations**. Here, HP Web Jetadmin instances are listed with features for discovery, viewing, removing, and even launching the remote instance. Discovery via a variety of methods allows finding instances on both local and remote subnets. Here are a few characteristics of HP Web Jetadmin installation discovery:

- HP Web Jetadmin can discover other instances of HP Web Jetadmin
- Discovery is possible to versions as early as 6.5.xxxx
- Three discovery features for finding other HP Web Jetadmin installations include **WS Discovery**, **IP broadcast**, and **IP range**

- **IP range** and **IP broadcast** discoveries share stored settings data with other discovery features
- HP Web Jetadmin applications are discovered via an "always-on" Universal Datagram Protocol (UDP) port 8000 listener
- HP Web Jetadmin instances can be launched directly from the discovery listing
- The list can be modified by performing other discoveries or by manually removing instances

Once found, HP Web Jetadmin installations are visible in the **Web Jetadmin Installations** workspace with a discovery progress display (Figure 17).

These installations are also viewable from the feature found in **Tools** > **Data Synchronization** from the HP Web Jetadmin menu bar (Figure 18). This feature can be used to run a **Quick Device Discovery** for individual HP Web Jetadmin installations and to invoke or schedule data synchronization.

Figure 17—Web Jetadmin Installations pane

Figure 18—Data Synchronization

The **Synchronize** feature activates a one-way data transfer from the discovered HP Web Jetadmin installation to the HP Web Jetadmin installation launching the feature. Many different data elements can be enabled as part of the data transfer. **Serial number**, **Port**, **Model number**, **Last discovered**, **Last communication**, **HP Jetdirect model**, **IP hostname**, **IP address**, and **Discovery date and time** always transfer. This transfer is a one-time event that can be rescheduled.
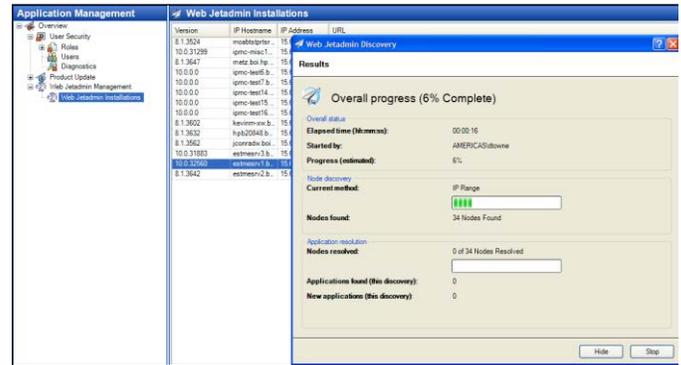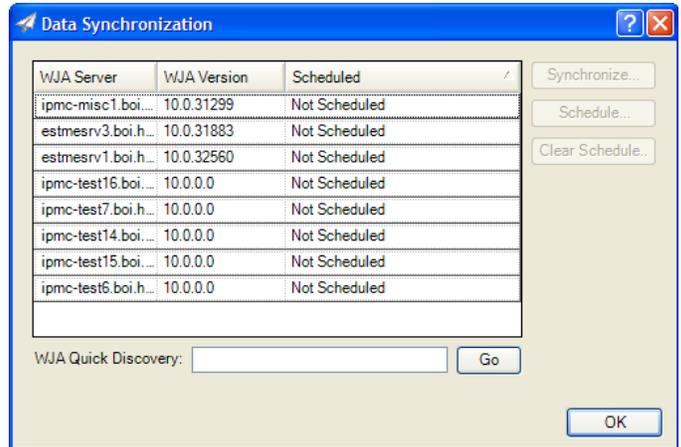
APPENDIX A—TROUBLESHOOTING DISCOVERY

Discovery troubleshooting can seem a daunting task. Most of the time, troubleshooting network-connected devices can be broken down into one question: is SNMP communication possible? Here are some helpful tips for these possible scenarios:

"Quick Device Discovery finds one device at a time, but I can't find a lot of devices with other discovery settings."

- The IP ranges may be too large, causing discovery to run too long and never search the part of the network where devices exist. Try using a small range where devices are known to exist.
- IP broadcasts may be blocked. Try using another method such as **IP range** or **Specified addresses**.
- SLP traffic may be blocked. Try using another method such as **IP range** or **Specified addresses**.
- Check the local firewall, which may be blocking traffic on incoming or outgoing ports.

"I can't find the device through Quick Device Discovery, nor through any other means in HP Web Jetadmin. HP Embedded Web Server (EWS) works, telnet works, ping works."

- The device's SNMP stack may be disabled. Open the device's HP EWS interface, select **Network,** and look at the SNMP settings. The **Disable SNMPv1/v2** option will keep HP Web Jetadmin from discovering the device.
- The device may have had the "public" Get community name disabled. Learn the community name for that device and use HP Web Jetadmin global credentials to configure well-known community names.

"HP Web Jetadmin can only discover devices on the local network. Any devices on remote networks cannot be discovered."

- Routers may be blocking SNMP queries. Work with network administration teams to resolve this issue.

"I've tried everything and cannot discover the device with HP Web Jetadmin."

- Check the **Blocked Devices** list under **Tools** > **Options** > **Device Management Discovery**. If the device address exists in this list, HP Web Jetadmin will never find it.

"PC-connected device discovery does not find devices."

- Make sure the HP SNMP Proxy Agent is installed on the remote hosts and that port 161 is not being blocked by a firewall. Make sure the WMI service is started on the remote hosts and that local administrative credentials are being used in discovery settings. This discovery is best planned in coordination with workstation and server administrative teams.

"HP FutureSmart devices do not display correct features."

- Beginning in Web Jetadmin 10.3 SR4, Universal Plug-ins (UPI) are used to define which features are displayed for recent FutureSmart devices. For UPI device resolution during discovery, Web Jetadmin performs Web Service discovery for Enterprise devices to determine if the device is and enterprise device and supports Web Service communication. Based on those responses, Web Jetadmin selects the HP Enterprise UPI to manage the device using the Web Service protocol. If the WS* discovery option under EWS is disabled for the device, it will fail the UPI resolution and will fall on the SNMP generic plug-in instead of UPI. Generic support will only display a fraction of the features that should be displayed for a FutureSmart device. In order to ensure FutureSmart devices are supported correctly, make sure the WS* discovery option under EWS is enabled for the device

NPI11A045 / 16.185.14.6

| Information | General | Copy/Print | Scan/Digital Send | Fax | Troubleshooting | Security | HP Web Services | Networking |

Configuration
TCP/IP Settings
Network Settings
Other Settings
AirPrint
Select Language
Security
Settings
Authorization
Mgmt. Protocols
802.1X Authentication
IPsec/Firewall

Other Settings

| Misc. Settings | LPD Queues | Support Info | Refresh Rate |

Enabled Features

- ☑ SLP Config
- ☑ 9100 Printing
- ☑ LPD Printing
- ☑ Telnet Config
- ☑ LLMNR
- ☑ Enable WINS Port
- ☑ Bonjour
- ☑ AirPrint
- ☑ IPP Printing
- ☑ HP Jetdirect XML Services
- ☑ Certificate Mgmt Service
- ☑ WINS Registration
- ☑ Multicast IPv4
- ☑ FTP Printing
- ☑ IPPS Printing
- ☑ WS-Discovery
- ☑ Verify Certificate for IPP/IPPS Pull Printing
- ☑ TFTP Configuration File
- ☑ Web Services Print

"IP Range discovery is not finding devices it should."

- IP Range discovery pings nodes to make sure they active before attempting the SNMP interrogation to potentially save on unnecessary network traffic. Pings may be blocked at the routers or firewalls, or the pings may be slow to respond. The length of time Web Jetadmin waits for ping responses can be edited through ha configuration file as well the number of pings Web Jetadmin will send per device. To control these parameters, edit the following file:

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config\DiscoveryMethodIpRange.config.xml

-or-

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config\DiscoveryMethodIpRange.config.xml

```
<ipmc:configuration
xmlns:ipmc="www.hp.com/schemas/imaging/ipmc/config/2004/02/24">
    <property name="DefaultSnmpGetCommunityName">

<type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
</type>
        <value>public</value>
    </property>
    <property name="PingTimeout">

<type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
</type>
        <value>1000</value>
    </property>
    <property name="PingRetryCount">

<type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
</type>
        <value>1</value>
    </property>
</ipmc:configuration>
```

APPENDIX B—DISCOVERY TRAFFIC

For your reference, a sampling of network traffic generated by discoveries follows below.

NOTE   Values are traffic-generated for each device discovered. All discovery settings are at default values. The SNMP query/response sequence varies depending on the device used in the sample.

NOTE   Testing was performed on an HP internal network and may not reflect results observed on other networks.

SLP multicast—Network device

- SLP multicast response = 2 packets, 768 bytes over 24.5 Sec
- SNMP follow-up query/response = 6 packets, 1.9 Kbytes over 60 mSec

IP broadcast—Network device

- Each IP broadcast address = 3 SNMP packets, 255 bytes over 7 Sec
- IP broadcast response = 3 SNMP packets, 468 bytes over 7 Sec
- SNMP follow-up query/response = 34 packets, 5.4 Kbytes over 109 mSec

IP range—Network device

- ICMP echo request send and receive = 2 packets, 148 bytes over 70 ms
- SNMP follow-up query/response from printer = 28 packets, 3.6 Kbytes over 2.6 Sec

Specified address—Network device

- SNMP query/response from printer = 38 packets, 6.1 Kbytes over 1.1 Sec

Active Directory—Network device

- SNMP follow-up query/response from printer = 34 packets, 4.2 Kbytes over 5 Sec

IP broadcast—PC-connected device

- SNMP query/response from printer = 23 packets, 3.6 Kbytes over 27.5 Sec

APPENDIX C—SETTING REALISTIC IP RANGES

IP range discovery can perform to expectations when the range data has been correctly developed. It is very easy to configure ranges that are larger than needed, causing the discovery to take a long time and sometimes yield few devices. For example, a class A range could easily be developed for the HP intranet but would take weeks to complete. The class A range that represents HP's intranet is:

15.0.0.1 – 15.255.255.254

which represents over 16 million address combinations. On most large networks, the majority of these addresses won't answer the HP Web Jetadmin query and will cause timeouts to occur, leading to very long discovery times.

Setting ranges based on subnets or contiguous subnets

In reality, most networks are divided into subnets. Subnets can be used to describe a network IP addressing scheme and generally reflect the actual portions of the network being used. These subnets, when put together into one list, represent an IP map. This type of a map can be obtained from an IT or network infrastructure team. HP strongly recommends that you discuss plans for implementing HP Web Jetadmin discoveries with these teams.

A subnet within a large network can be described with a network number and a subnet mask. A typical combination might look like this:

Network number example: 15.5.188.0

Subnet mask example: 255.255.252.0

This is one subnet with an IP range of 15.5.188.1 through 15.5.191.254 and up to 1,022 possible addresses. It may take HP Web Jetadmin only about 10 minutes to discover devices—depending on the network, the number of devices, and the host running HP Web Jetadmin.

NOTE   IP address calculators are an easy way to analyze IP networks. Many free versions of IP calculators exist and can be obtained on the web.

An example of IP range planning

A hypothetical network has 20 subnets. All of these subnets use the same subnet mask of 255.255.255.0. Here are the network numbers that represent 20 subnets:

15.0.1.0, 15.0.2.0, 15.0.3.0, 15.0.4.0, 15.0.5.0, 15.0.30.0, 15.0.31.0, 15.0.32.0, 15.0.33.0, 15.0.34.0, 15.0.35.0, 15.0.36.0, 15.0.37.0, 15.0.38.0, 15.0.39.0, 15.0.55.0, 15.0.64.0, 15.0.65.0, 15.0.66.0, 15.0.67.0., 15.0.68.0, 15.0.69.0, 15.0.70.0, 15.0.71.0, 15.0.72.0, 15.0.73.0, 15.0.74.0

From this information, we can formulate the following IP address ranges and import them into HP Web Jetadmin:

15.0.1.1 - 15.0.1.254	15.0.1.1 - 15.0.1.254
15.0.2.1 - 15.0.2.254	15.0.2.1 - 15.0.2.254
15.0.3.1 - 15.0.3.254	15.0.3.1 - 15.0.3.254
15.0.4.1 - 15.0.4.254	15.0.4.1 - 15.0.4.254
15.0.5.1 - 15.0.5.254	15.0.5.1 - 15.0.5.254
15.0.30.1 - 15.0.30.254	15.0.30.1 - 15.0.30.254
15.0.31.1 - 15.0.31.254	15.0.31.1 - 15.0.31.254
15.0.32.1 - 15.0.32.254	15.0.32.1 - 15.0.32.254
15.0.33.1 - 15.0.33.254	15.0.33.1 - 15.0.33.254
15.0.34.1 - 15.0.34.254	15.0.34.1 - 15.0.34.254
15.0.35.1 - 15.0.35.254	15.0.35.1 - 15.0.35.254
15.0.36.1 - 15.0.36.254	15.0.36.1 - 15.0.36.254
15.0.37.1 - 15.0.37.254	

We can take the formulation one step further and simplify things. Some of our IP ranges are contiguous and in order, making it easy to combine them. The final result looks like this:

15.0.1.1 - 15.0.5.254

15.0.30.1 - 15.0.39.254

15.0.55.1 - 15.0.55.254

15.0.64.1 - 15.0. 74.254

We have reduced the number of IP ranges to four. We can convert this to a form that is easily imported into HP Web Jetadmin via a text file and also reflects descriptions:

15.0.1.1-15.0.5.254 = subnet range for western region

15.0.30.1-15.0.39.254 = subnet range for central region

15.0.55.1-15.0.55.254 = subnet range for branch office

15.0.64.1-15.0. 74.254 = subnet range for eastern region

Of course, leaving the 20 ranges as separate items would also work. Consolidating ranges makes dealing with large quantities of data simpler, but may not help when descriptions are needed for the purpose of cataloging ranges.

IP range files—Import and export features

IP range data can be developed in other applications and imported as text files. HP Web Jetadmin can also export IP range data to text files. This makes it easier to deal with large numbers of IP ranges, manipulate complex data and archive data for use in multiple instances. Let's break down the file format for IP range import/export:

- Characteristics of IP range files:
  - One range per line.
  - Each IP address is separated by a hyphen (-).
  - Comment or description strings can be appended to the IP range by using an equal sign (=).
- Example of one IP range with a comment (where xxx represents an octet in the IP address):
  xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx=descriptive text string

APPENDIX D—MAINTAINING ACCURATE ADDRESS INFORMATION

HP Web Jetadmin can adjust IP addresses stored for each device. In many cases, IP addresses on devices remain static and changes within the HP Web Jetadmin **All Devices** list aren't needed. In a few cases, device addresses may change due to device moves or when device addresses are assigned with DHCP. In these cases, HP Web Jetadmin should be able to cope with the changes and quickly change its internal record of a device's IP address.

HP Web Jetadmin automatically changes a device's IP address anytime it detects a change in that address. For instance, a device might have been configured with the IP address 15.62.40.203 yesterday but today it has the IP address 15.62.42.198. HP Web Jetadmin only recognizes changes when some communication has taken place with the new device address. **IP range** discoveries may be performed from time to time if IP addresses are prone to changing.

APPENDIX E—GLOBAL DISCOVERY SETTINGS

Discovery settings

The discovery settings in **Tools** > **Options** > **Device Management** > **Discovery** generally affect discovery behavior and performance. These are typically set by administrators.

Type of setting	Detail	Explanation
General	SLP listen:	Select this option to use passive discovery on port 427 for SLP signals propagated at HP Jetdirect power-on. The default for this field is Off or unselected.
	Listen for new devices	Checkbox enables the passive discovery mechanism that listens on port 427 for SLP signals propagated at HP Jetdirect power-on. Default is "off" (unchecked).
	Discover SNMPv3	Select this option to enable SNMPv3 credential entry fields in HP Web Jetadmin discovery settings. When these credentials are added for discovery settings or global credentials, HP Web Jetadmin attempts SNMPv3 queries on devices. The default for this field is Off or unselected. NOTE SNMPv3 discoveries can be slow if not properly set. These should be targeted only at parts of the network that are known to have SNMPv3-enabled devices. Also, SNMPv3 devices require that SNMPv3 credentials are entered.
	WS-Discovery listen:	Select this option to use passive discovery on port 3702 for WS-Discovery signals propagated at HP Jetdirect power-on. The default for this field is Off or unselected.
Blocked Devices		The **Blocked Devices** list contains device addresses for which device discoveries are blocked. Devices are populated into this list in one of two ways. First, the device can be deleted from the **All Device** list with the **Delete and Block** option which adds the device to the **Blocked Devices** list. Second, devices can be added to (or removed from) the list in **Tools** > **Options** > **Devices Lists** > **Blocked Devices**. The device's presence in the **Blocked Devices** list prevents HP Web Jetadmin from discovering it. Adding a device to the list through the **Tools** > **Options** > **Device Lists** > **Blocked Devices** interface does not cause it to be removed from the **All Devices** list.

Other related network settings

The menu under **Tools** > **Options** > **Application Management** > **Network** contains most of the other settings that affect discovery.

Setting	Explanation	Default
SNMPv1 Timeout	Value sets the number of milliseconds HP Web Jetadmin waits for a reply from a network query SNMPv1.	400
SNMPv3 Timeout	Value sets the number of milliseconds HP Web Jetadmin waits for a reply from a network query SNMPv3.	500

Setting	Explanation	Default
SNMP Retries	Value sets the number of retry queries HP Web Jetadmin executes when no response is detected.	4
Enable DNS Lookups	Forces HP Web Jetadmin to query name services for each device discovered. This setting is sometimes disabled in environments where DNS responses are slow or are not functioning.	Enabled
IP Ranges	Global store for IP range settings used by network device discovery, PC-connected device discovery and HP Web Jetadmin application discovery.	None or blank
Credentials	In some cases, credentials like SNMP Get community names or SNMPv3 are used. Use the **Credentials** interface to set well-known device credentials. These are tried during discovery when devices don't respond to queries that use default credentials.	None or blank