

## Discover and report network assets and computers that do not have BigFix Agents

### The Challenge

---

The BigFix Enterprise Suite (BES) provides a scalable, flexible, agent-based platform and automation-assisted solutions that enable enterprises to use the distributed power of all their computers to manage their security and configuration, no matter where they are or how they connect to the enterprise network.

In order to be managed by BES, there must be an agent on the device. This highlights two challenges:

- How can BES help find **unmanaged computers** that are on the network, but do not have the BigFix Agent installed and that are not in Active Directory or any known location?

Unmanaged computer can be anything from employee or contractor computers brought in from outside the network, to old forgotten servers, to computers that were installed but never properly inventoried. These computers must to be tracked, patched, and secured just as any other asset in the network. In fact, these computers are sometimes the most vulnerable because they are often neglected and if they are infected, they are difficult to locate.

- How can BES help identify **network assets** that cannot have a BES Agent installed?

Network assets such as routers, switches, printers, or any other network device are important to identify so that these devices can be tracked and maintained. In addition, any rogue or unauthorized devices must be identified and dealt with appropriately.

### The Solution

---

To discover network devices and unmanaged computers, BES offers the ability to designate “**Scan Points**” that scan network segments and send the scan results to the central BES Database. Using a scanning solution built on NMAP technology, information is discovered about network devices and unmanaged computers including IP address, OS, MAC address, DNS name, and other attributes.

BES Asset Discovery uses the existing distributed architecture of BES to provide the following benefits:

- **Enterprise Wide Unmanaged Computer Visibility** – Scan Points can be designated on virtually any computer on the network on which a BigFix Agent is installed. This allows scans to be performed in data centers, corporate headquarters, and remote offices. In addition, Scan Points can easily be placed inside previously “unscannable” areas such as DMZs or offices protected by a firewall, yielding all the benefits of a scanner without having to relax security by opening inbound scanning ports.
- **Fast “in Parallel” Scans** – Multiple subnets can be scanned concurrently. Scans run very fast (in just a few minutes), because scanning is performed locally in the subnet rather than scanning over slow WAN links.
- **Minimal WAN Usage** – By scanning locally on the fast LAN rather than across the WAN, precious, limited bandwidth is conserved. When the scans are complete, the reports are compressed and sent to the central BES database for viewing.
- **Timely Asset Discovery Information** – Scans with BES Asset Discovery have little network impact and can be run very frequently. Instead of scanning the whole network from one location once a month (as is common with alternate approaches), scans can be performed multiple times each day. This provides timely, updated, enterprise-wide unmanaged computer discovery.

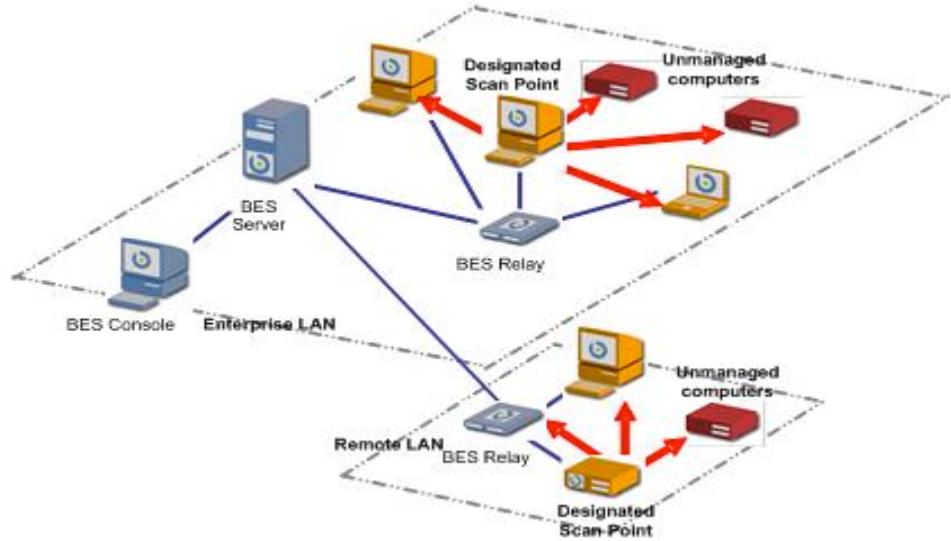
## How it Works

Alternative approaches for asset discovery scan over slow WAN links, consume excessive bandwidth, and take hours or even days to scan an entire enterprise network. The BES Asset Discovery solution leverages the existing BES infrastructure to scan each subnets from a computer within the same subnet. These scans can occur in parallel so that the scans are performed in designated network segments using little to no WAN bandwidth.

## Designate Scan Points and Periodically Run Scans of the Local Networks

Using the BES Asset Discovery Fixlet site, BES Console users can designate “**Scan Points**” anywhere in the network and then schedule scans of the local network.

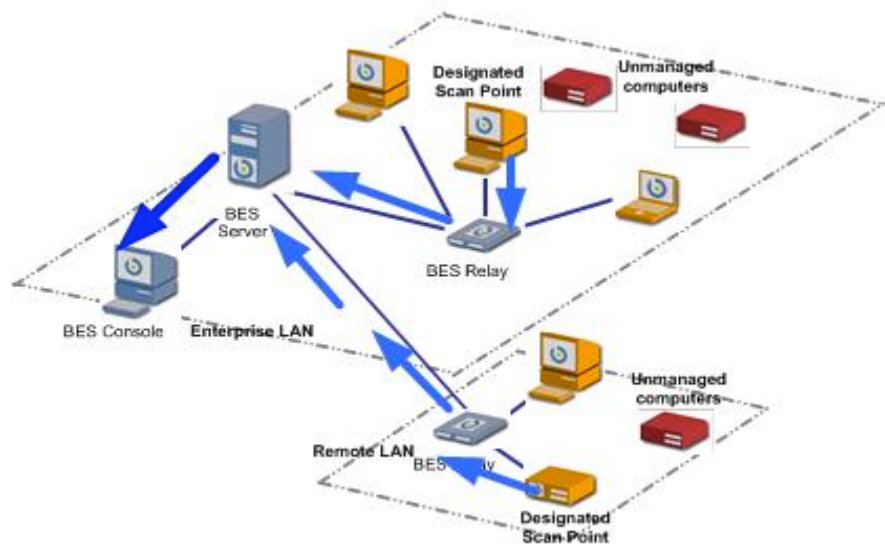
Leveraging the BES Relay hierarchy within an enterprise, scans are conducted on the local LAN segments, eliminating the need to scan over slow WAN links.



## Scan Results are Automatically Sent to the BES Database

Scan results from the Scan Points are automatically compressed and sent to the main BES Server (through the BES Relays), and aggregated within the BES Database.

BES Console users can then view the automatically updated information. The user can view the data, create reports, and export the information for further analyses.



## View Unmanaged and Managed Assets in the BES Console

The screenshot shows the BigFix Enterprise Console interface. The top window displays a table of unmanaged assets with columns for Asset ID, Source Name, Running Client, MAC Address, Creation Time, IP Address, OS, and Device Type. The bottom window shows a detailed view for 'Unmanaged Asset 246', including identifying properties like Hostname (bowser), IP Address (192.168.100.58), and MAC Address (00:0D:56:9B:CE:B4), as well as open ports (tcp 22 ssh, tcp 23 telnet, tcp 80 http, tcp 235, udp 52311, udp 61616).

Asset ID	Source Name	Running Client	MAC Address	Creation Time	IP Address	OS	Device Type
240	NMAP	no	00:03:8A:2D:47:72	2/10/2005 1:18:55 PM	192.168.100.140	Sun Solaris 8	general purpose
241	NMAP	no	00:06:A4:11:9F:CC	2/10/2005 1:18:55 PM	192.168.100.29	<not reported>	<not reported>
242	NMAP	no	00:08:74:30:E1:02	2/10/2005 1:18:55 PM	192.168.100.57	<not reported>	<not reported>
243	NMAP	no	00:0C:29:28:87:40	2/10/2005 1:18:55 PM	192.168.100.254	OpenBSD/OpenBSD 3.3	general purpose
244	NMAP	no	02:00:07:208:8D:9C	2/10/2005 1:18:55 PM	192.168.100.2	Intel embedded	switch
245	NMAP	no	08:00:20:85:ED:4B	2/10/2005 1:18:55 PM	192.168.100.242	Sun Solaris 2.X or Sun Sol...	general purpose
246	NMAP	no	00:0D:56:9B:CE:B4	2/10/2005 1:18:55 PM	192.168.100.58	<not reported>	<not reported>
247	NMAP	no	00:03:03:80:CE:63	2/10/2005 1:18:55 PM	192.168.100.1	Cisco IOS 12.X	router
248	NMAP	no	00:08:AA:11:92:04	2/10/2005 1:18:55 PM	192.168.100.108	<not reported>	<not reported>
249	NMAP	no	00:04:95:80:9B:88	2/10/2005 1:18:55 PM	192.168.100.178	<not reported>	<not reported>
250	NMAP	no	00:11:11:CB:5B:84	2/10/2005 1:18:55 PM	192.168.100.125	<not reported>	<not reported>
251	NMAP	no	00:30:8E:2F:5A:10	2/10/2005 1:18:55 PM	192.168.100.24	HP embedded	printer
252	NMAP	no	00:06:5B:75:49:41	2/10/2005 1:18:55 PM	192.168.100.45	<not reported>	<not reported>
253	NMAP	no	00:06:5B:75:87:F9	2/10/2005 1:18:55 PM	192.168.100.13	<not reported>	<not reported>
254	NMAP	no	00:90:27:87:86:71	2/10/2005 1:18:55 PM	192.168.100.124	Linux Linux 2.4.X or Linu...	general purpose
255	NMAP	no	00:11:44:5C:7E:68	2/10/2005 1:18:55 PM	192.168.100.30	<not reported>	<not reported>

The information about discovered assets is available in the BES Console.

- MAC Address
- Network IP Address
- Network Subnet
- Operating System
- Time scanned
- Hostname
- Device type (printer, switch, etc.)
- And more...

## Support for Other Asset Discovery Sources

Other scanning technologies in addition to NMAP can be used to perform the scan in the BES Asset Discovery solution. The open BES Asset & Vulnerability Discovery API enables the BES platform to integrate with existing scanning technology to provide a central view of managed and unmanaged assets. Talk to a sales engineer for more information about integrating other scanning solutions into BES.

## About BigFix, Inc.

BigFix enterprise security configuration management solutions help large organizations maintain the security, health, and performance of their systems. The foundation for all BigFix solutions is a scalable, secure, agent-based platform, the BigFix Enterprise Suite, which gives IT departments complete visibility into every computer running on a corporate network, and the automation-assisted control to rapidly identify, assess and remediate vulnerabilities and configuration issues. BigFix provides solutions for endpoint security, patch management, vulnerability remediation, and configuration management. BigFix technology has received awards and recognition from numerous organizations and was recently named "Best New Security Solution for 2004" by *SC Magazine*, and is a finalist for the *Software & Information Industry Association's* Codie awards in both "Best Systems Management Solution" and "Best Security Product" categories for 2005.



**BigFix, Inc.**  
 6121 Hollis Street  
 Emeryville, California 94608  
 [t] 510 652-6700  
 [f] 510 652-6742  
 [e] info@bigfix.com

**Sales**  
 [t] 510 652-6700 x116  
 [f] 510 652-6742  
 [e] sales@bigfix.com

© 2005 BigFix® and the BigFix logo are registered trademarks of BigFix Inc. All other trademarks are the property of their respective owners. DS 1007

More information about NMAP is available at <http://www.insecure.org/nmap/index.html>.