Infoblox
CONTROL YOUR NETWORK

Infoblox DHCP Fingerprinting
Enabling Endpoint Discovery and Control

SOLUTION NOTE

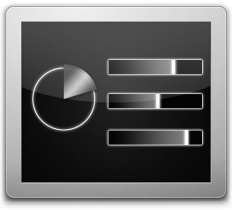
Benefits

- Discover, organize, group and control unknown devices on network automatically
- Flexibly enforce corporate policy
- More effective network planning; plan for growth, and application trends
- Enhanced device supportability and security

Mobile Device Explosion and the Challenges of BYOD

In 2012 for the first time, globally there were more tablets and smartphones sold than personal computers. From a business point of view, there are both pros and cons to this shift. Organizations that embrace the BYOD movement, share costs with the user, improve worker satisfaction, and benefit from the latest features and capabilities. But as these personal devices find their way into the work place, IT is being challenged with dynamic network device detection and control. How do you gain visibility, enforce policy, report on and secure this environment when the devices are unknown? There may also be issues of compliance, information security and ownership when it comes to data. Rules must still be followed even if the data is on a device owned by an employee. Bottom line – you need to discover the devices so you can manage them on your network.

Visibility and Control Comes at a Premium



Mobile Device Management (MDM) software secures, monitors, and manages mobile devices. It is a common way of optimizing the functionality and security of a mobile communications network, but comes at a price and does not work in all BYOD scenarios, like games. And some people won't allow you to put an agent on their phone. With or without MDM, network administrators are missing critical data about these personal devices, printers, IP phones – what they are, extent of use and if they should be allowed on the network at all. And MDM is intrusive. So if you are supporting and managing BYOD policy you need automatic enforcement that is less invasive. Effective management will also require tracking changes in usage over time so trending and reporting are essential.

DHCP Fingerprinting – Non-invasive Visibility and Control with Your Existing Infrastructure

DHCP Fingerprinting is an easy way to gain this information and control. With the introduction of Infoblox NIOS 6.7 and DHCP Fingerprinting the device type is determined during the DHCP process automatically without additional overhead like other network discovery options. When making a DHCP discover request, most operating systems' DHCP clients will ask for DHCP options in a specific sequence. This makes DHCP Fingerprinting possible – identifying a device or operating system requesting an IP address based on the requested DHCP options. And this does not slow down or change the DHCP process. It simply maps the IP address to the MAC address and operating system as part of that DHCP process. As part of your device usage enforcement policy, if a device requesting the IP address is not allowed, it will just not receive an address.

The advantage of this is the ability to identify the device and/or operating system without a

Infoblox DHCP Fingerprinting
Enabling Endpoint Discovery and Control

SOLUTION NOTE

separate discovery mechanism, dynamically and in real-time without requiring additional infrastructure, processes or network activity. Not only will Infoblox DDI detect and populate the IPAM datastore, it will enable you to flexibly enforce corporate policy – enabling smartphones and laptops, while blocking games, routers and other prohibited devices. This can be set per range providing policy enforcement flexibility.

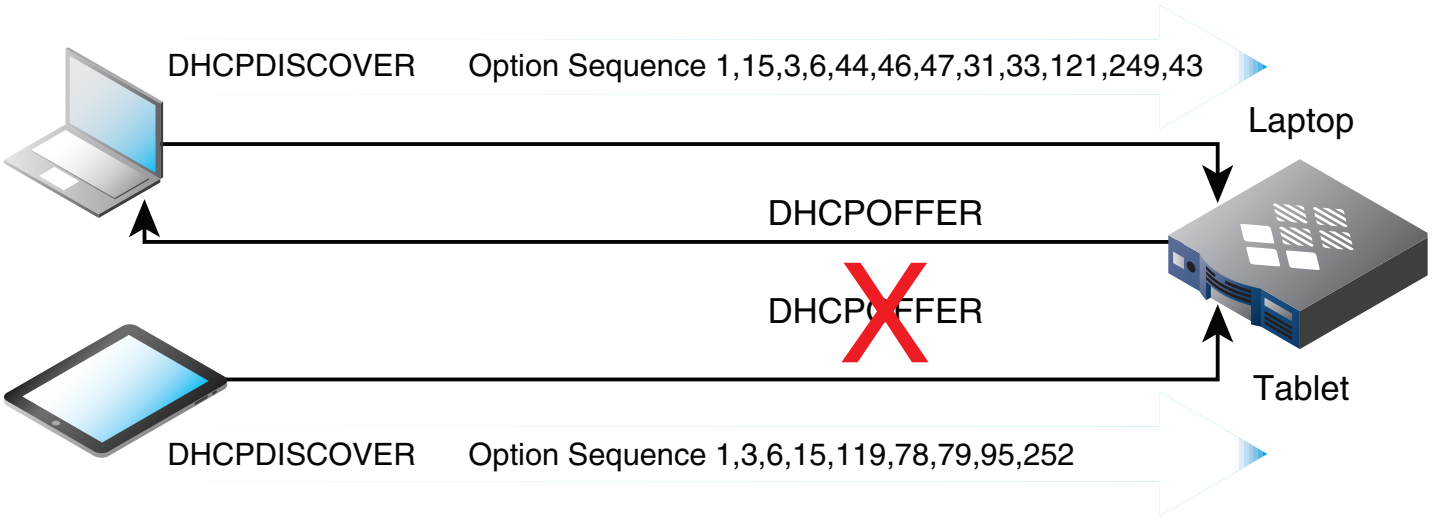
Integrating with Your Infrastructure

The value of DHCP Fingerprinting is fully realized when implemented as part of Infoblox's robust DNS, DNSSEC, DHCP and IPAM solution. When run on the Infoblox Grid with Infoblox purpose-built appliances that share a common, real-time distributed database, it guarantees that all appliances in the Grid have timely and accurate data, enabling you to deliver state-of-the-art network services. Infoblox fully integrated DDI solution ensures dynamic applications, such as wireless networking, VoIP and BYOD operate properly. Real-time reporting leverages the Infoblox platform of DNS, DHCP, IPAM and DHCP Fingerprinting to provide current and historical network reporting, trending and tracking. This helps detect security issues proactively and you do a better job capacity planning. Some devices will increase in use, others will decrease. This is useful for network planning, application trends, BYOD policy and more.

DHCP Fingerprinting provides all new capabilities to materially improve network visibility, control and security. All without the need of any agents, or MDM software.

- Provides visibility to BYOD device types on your network
- Enables you to set network connectivity policies based on device type and enforce them
- Protects you against potential BYOD security risks

DHCP Fingerprinting – How IT Works



A DHCP discover request asks for DHCP options in a specific sequence. This makes DHCP Fingerprinting possible – identifying a device or OS requesting an IP address based on the requested DHCP options.

Infoblox
CONTROL YOUR NETWORK

Infoblox DHCP Fingerprinting
Enabling End-Point Discovery and Control

SOLUTION NOTE

Attributes

- Automatically detects DHCP clients including BYOD operating systems during the DHCPDISCOVER process enabling visibility into what devices are on your network. It is un-intrusive and without the overhead of additional network discovery within the DHCP Range so you know where the devices are.
- Manage DHCP leases by corporate asset or BYOD device
  - Enhanced DHCP lease, DHCP lease history, global filters and default smart folders helps build a profile of how those devices are being used, and where in the network
- Enforces corporate device use policy by blocking selected OS's from obtaining an IP address enabling device access control
  - NIOS DHCPv4 filter options have been extended to include fingerprints
- Enhances network planning by automatically providing new device OS focused reports (via reporting appliance) and enhancing existing DHCP lease reports
- Auto organize and group devices in smart folders
- Reporting additions
  - DHCP lease history: modified existing report to add DHCP fingerprint
  - DHCP top lease clients
  - DHCP top device OS by network – for each network shows number of device operating systems
  - DHCP device operating system trend – new report showing leases by device type over time

About Infoblox

Infoblox delivers critical network services that protect Domain Name System (DNS) infrastructure, automate cloud deployments, and increase the reliability of enterprise and service provider networks around the world. As the industry leader in DNS, DHCP, and IP address management, the category known as DDI, Infoblox (www.infoblox.com) reduces the risk and complexity of networking.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com