

# Device Profiling

## Managing BYO Device Programs

### Introduction

Extending the traditional enterprise data network to support a growing number of real time services and mobile devices provides economic, operational and productivity benefits. Providing connectivity for all of these devices on a single network reduces capital equipment costs by eliminating redundant networks. Operational costs are reduced by having a single group manage the converged network and productivity is increased by eliminating the barriers between the enterprise network and mobile devices and users. This new converged network also provides a unique set of challenges for network managers.

### Converged Networks

Converged networks combine real-time services such as video and voice over IP with traditional data services. Convergence can also mean using the enterprise network to provide connectivity for an ever growing list of time-sensitive data services, including retail point of sale terminals, physical access control systems (card readers, Biometrics readers, etc.), medical devices such as patient heart monitors, building environmental controls (HVAC), virtual desktop infrastructure (VDI) and, of course, smartphones and tablets. Converged networks can also combine the wired and wireless networks into one seamless environment.



Figure 1: Converged Network

Real time services each have their own set of network requirements for access, bandwidth, latency and jitter. In order to provision them correctly the network must be able to correctly identify them. It must be able to differentiate an IP phone from a card reader or a video camera from a medical device. For users it must know the difference between a user logging in from their office and that same user accessing the network from an iPad or Android device.

### Benefits

#### Automation

- Automatic network provisioning for end stations improves the performance of time sensitive services

#### Visibility and Control

- Operating system profiling increases security by automatically applying correct access policy to mobile devices

#### Reduced costs

- Automatic detection and profiling of end stations reduces management overhead by providing an accurate inventory of devices and their locations

# Determining Device OS

Enterasys [Network Management Suite](#) (NMS) uses multiple techniques to automatically determine the operating systems running on the end system, including:

- Agent-based scans
- Network-based scans
- DHCP fingerprinting
- OS detection using captive portal

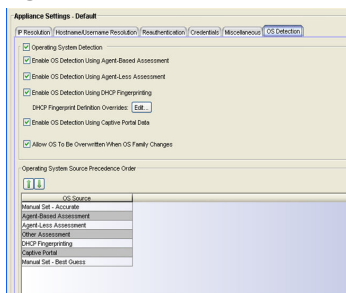


Figure 2: OS Detection

## Agent-Based Scanning

Two types of agents are available:

- Dissolvable Agent – a temporary agent (can be loaded and unloaded on the end system using various vendor-specific techniques)
- Persistent Agent – a persistent suite of assessment software established on the end system

Agent-based scanning provides the most detailed information about the end system's operating system, but it is also the most intrusive. In some environments, such as medical devices that have to be certified and locked down, adding any software, including an agent, would not be permitted.

## Network-Based Scanning

Network-based scanning relies on the fact that different operating systems respond differently to network-based probes. Scanners like NMAP use fingerprint databases that list how each operating system responds to a range of probes and then matches the unknown end system's fingerprint to that database. Network-based scanning is not as reliable as agent-based scans but it is less intrusive. The problem with network-based scans is that end system firewalls will reduce their reliability and security systems including IDS/IPS, SIEM and antivirus software might report the scans as attacks on the end system.



## DHCP Fingerprinting

Unlike the active probing done by network-based scanning, DHCP fingerprinting is a passive technique. Different operating systems use different default values for DHCP message option fields and have different protocol message exchange timing. By snooping the DHCP message exchange a fingerprint of the end system can be developed. This fingerprint consists of the timing of the messages and the values of various DHCP message option fields. The fingerprint is compared to a database of known operating system fingerprints to identify the end system's operating system. DHCP vendor attributes can be used to identify the type of device being connected to the network.

## OS Detection using Captive Portal

If the user is redirected to the Enterasys NMS NAC captive portal for remediation, the user agent string from the HTTP message header can be examined to determine the OS of the requesting end system.

## Determining End System Type

The explosive growth of devices being connected to the network raises a new set of problems for network administrators. Many of these devices are embedded or single purpose devices such as IP phones, video cameras, medical devices and physical access control systems. These devices are generally single purpose standalone devices. Since many of these devices use common off-the-shelf operating systems and network stacks we need a different way of categorizing them to ensure they are correctly identified and given the appropriate network access and provisioning.

### MAC OUI

A MAC address consists of two parts: an OUI (Organizationally Unique Identifier) and a serial number. The OUI can be used to identify some IP Phones by matching it to the OUIs used by different phone vendors.

### Use Cases

Adding the operating system type to the end system rules adds an additional level of granularity to networks access and provisioning policies.

- Many enterprises and educational institutions are faced with a growing number of user owned mobile devices. They want to allow students and employees to use their mobile devices to access the network but they need to place bandwidth and access limits on them. This growing trend is called Bring Your Own Device (BYOD). Since the operating systems associated with mobile devices like iPhones, iPads and Androids can be detected they can be given restricted priorities and access levels.

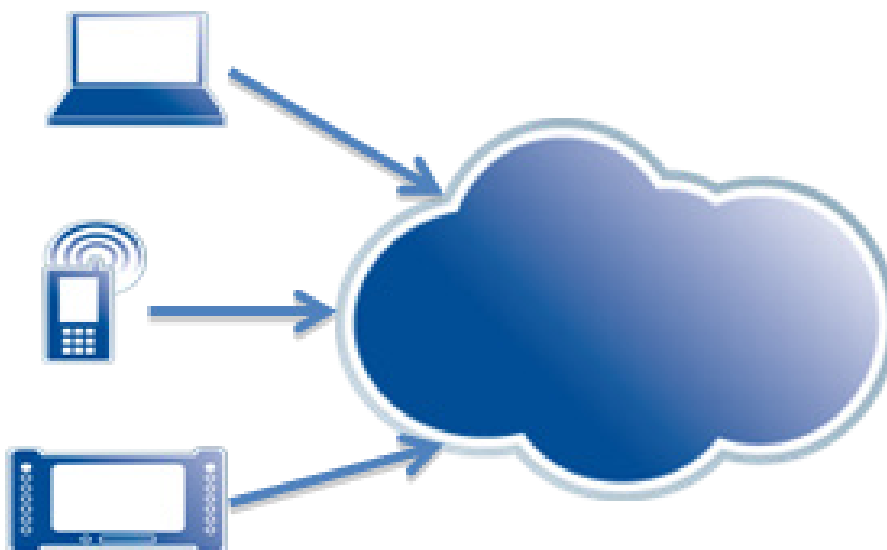


Figure 3: BYO Devices in Today's Enterprise

- In some enterprises all of the corporate approved systems use the same operating system. In this case if a user authenticates from a system running a different operating system they might be given limited or no access to networked resources.
- Enterprises need to restrict access when users connect to the network with valid credentials but are connecting from potentially unsecure devices such as smartphones, iPads and Android-based tablets.

## Enterasys Device Profiling Solution

Enterasys NMS automatically detects new devices and profiles them to determine the type of device that's connecting to the network. Device type can be an Operating System Family, Operating System or Hardware Type – for example, Windows, Windows 7, Debian 3.0, HP Printer, iPhone, iPad etc.

MAC Address	Mobile Device Type	Operating System	Owner
90-21-55-D3-91-2E	HTC EVO	Android	Chris
00-23-76-CD-3C-DB	HTC Hero	Android	Mike
40-FC-89-A5-2D-41	Droid Pro	Android	Tanya
3C-8B-FE-37-3C-6E	Samsung Galaxy Tablet	Android	IT
5C-DA-D4-05-50-7C	Samsung SCH-I500	Android	Joel
BC-47-60-8A-10-FD	Samsung Intercept	Android	Andre
DC-2B-61-AE-B4-A4	iPhone	iPhone	Jamie
F4-0B-93-F7-3B-C0	Blackberry Bolt 9700	Blackberry	Tanya
00-25-AE-91-E9-25	Zune HD	Windows CE	Riley

Figure 4: End Systems Detected by Enterasys NAC

Normally the operating system running on the end system should not change, so if the operating system associated with an end system's MAC address changes it could indicate a MAC Spoofing attack. Enterasys NMS will detect the change and generate a warning.

### Captive Portal

Enterasys NMS provides a captive portal that allows authenticated users to register their own devices on the network. For example, a university student could use the portal to register an Xbox game system.

## Specialized Device Profiling Services

To further assist enterprises in supporting a variety of devices, customized NMS functionality will be available through Enterasys professional services engagements, including:

- Behavior based identification
- Discovery
- Inventory Mode
- Provisioning Mode

### Behavior Based Identification

Since most enterprise devices are single purpose it's possible to identify them based on their network behavior. The two primary methods of identification include:

- Examine message content: Using custom signatures Enterasys [IPS](#) can categorize the end station by device type / function.
- Analyze message flows: The Enterasys [SIEM](#) can analyze data flows from end stations and categorize them by device type / function.

After the end station is categorized it is updated in the NMS end system table and the correct network access and provisioning can be applied.

---

## Discovery

During the discovery phase end stations are discovered and they are categorized by NMS by device type / function. New devices will be presented to the administrator categorized by MAC address, IP address, location and type / function.

The administrator will have the option to confirm the categorization or assign the device to a different type / function. For example, a newly installed video camera would be displayed as an entry showing the MAC address, IP address and Location, and the type field would be set to "video camera". If the information is correct the administrator could confirm the information and it would be added to the end system table. After confirming the information the administrator can apply the access and provisioning policies for this type of device.



## Inventory Mode

In inventory mode end stations are identified and categorized but network access and provisioning policies are not applied, so all devices will receive the default access and provisioning policies. This mode can be used to create an inventory showing the MAC address, IP address, device type and location of devices connected to the network. This is particularly useful for devices that are frequently moved from one location to another. For example, an administrator could sort the end system table to show all of the medical devices connected in a single room or the table could be sorted to show the location of all of the heart monitors connected to the network.

## Provisioning Mode

In this mode the correct access control, bandwidth and priority policies are applied to the network access port based on the type / function of device connected to it. For example, the port associated with a newly discovered IP Phone would be provisioned with a policy that:

- Permits access to the appropriate VoIP resources and protocols
- Assigns the appropriate bandwidth
- Applies the correct prioritization to the VoIP traffic

Correctly configuring the access port is critical since the resources, protocols, applications, bandwidth and prioritization for an IP Phone would be very different from those assigned to a card reader or video camera. In provisioning mode, NMS can automatically provision the access ports or it can be set up to require manual confirmation before applying the controls.

---

## Conclusion

The explosive growth of networks is the result of converging more services, such as voice, video and physical controls, onto the data network and adding a host of real-time single purpose devices to the network. Network managers need the visibility tools to automatically detect, locate, and classify these devices as they are attached to the network. To ensure that these devices receive the network resources they require, network managers also need tools that will automatically apply the correct access control, resource allocation, bandwidth and prioritization to the network. Enterasys professional services can customize the NMS solution to provide customers with the device profiling required for effective management of all of the devices connected to today's converged networks.

## Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at [enterasys.com](http://enterasys.com)



© 2011 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

