SOLARWINDS WHITEPAPER

Managing the BYOD Chaos

Follow SolarWinds:

solarwinds

Table of Contents

Managing the BYOD Chaos

Enterprise computing, as we know it, is facing a dimensional shift with the widespread diffusion of the BYOD (Bring Your Own Device) phenomenon. BYOD is the latest trend where employees bring their personally-owned mobile devices, smartphones and tablets to their place of work, and use these devices to access files, e-mail, and many other network applications. While this may be a real boon to the employees due to the convenience of using their own personal devices, it can be a real problem for IT departments, who will face challenges in terms of:

- protecting secure data
- beefing up IT infrastructure security
- regulating the usage of an increase of IP-enabled devices
- monitoring Wi-Fi access points and user logon
- keeping a check on the bandwidth consumption
- strengthening Wi-Fi connectivity and security
- revamping enterprise IT policy to make provisions for BYOD and mobile device proliferation

The good news is that this can be a win-win situation for both the company and the employees if the situation is properly managed. While employees can consolidate hardware, have improved connectivity, and work with more user-friendly personal devices to access network resources, enterprises can benefit from potentially lower hardware and support costs, as well as improved employee productivity.

And, BYOD is here to stay. The following statistics are obtained from a BYOD study by Gartner Inc.

- By 2015, as a response to widespread mobile device adoption, enterprises will have to deliver 300% more wireless access points to provide future Internet performance that is similar to the performance in the pre-BYOD era
- Enterprises are aware of only 80% of devices accessing their networks. The remaining 20%, being unsecured (and possibly jail-broken) mobile devices, threaten to introduce malware to network resources

The statistics illustrate the fact that the BYOD explosion is in the offing, and managing the Wi-Fi-enabled devices while leveraging their benefits is going to be an enterprise challenge. One can deduce from this that as the number of non-enterprise devices on the network increases, so too will the number of switches, ports and Wi-Fi access points you need to monitor. Additionally, there exists the potential for chaos with IP address provisioning and management, and an increase in the number of users and devices that need to be identified and tracked on the network. What is now required is an affordable, easy-to-use solution that will effectively address these challenges and establish the necessary security, IT management, control, and policy compliance.

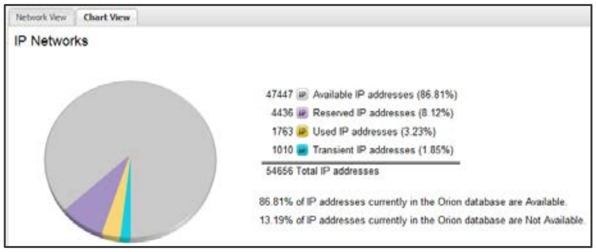
This paper will focus on two particular areas for managing potential BYOD chaos: IP infrastructure management, and user device tracking & switch port monitoring.

IP Infrastructure Management

With numerous BYOD devices on the network, and given the dynamic allocation of IP addresses, IT professionals need the ability to simplify management of their IP infrastructure. This includes **IP address management** and **DHCP/DNS management & monitoring**. Without real-time monitoring and centralized management capabilities, it becomes increasingly difficult to maintain your IP infrastructure.

IP Address Management includes IP address planning, space allocation, alerting, address conflict resolution, address tracking and event recording, and reporting of the IP address space in a network. As networks become larger and increasingly complex and with the looming transition to IPv6, the need for IPAM tools becomes increasingly important.

- **IP Address Planning** – Allocating, recycling, and documenting IP addresses and subnets in a network can get confusing very quickly if you have not laid out an IP addressing plan. A sound plan will help you prepare the network to support the increased demand for IP addresses as a result of BYOD through the avoidance of overlapping or duplicate subnets, duplicate IP address device assignments, and wasted IP address space. There are a number of free and commercially available products in the market that will help you plan your IP address space accordingly.
- **IP Space Allocation** – It is critical to know exactly how your IP space is being used. Addresses will typically fall into one of four categories: Available, Reserved, Used, or Transient. Again, without some kind of regular monitoring, it will always be difficult to see how your IP addresses are allocated. Only when this information is readily available, can you justify allocating newer IP addresses, or reallocating the available ones, and identify non-responsive IP addresses to optimize IP allocations.



IP Networks

47447	Available IP addresses (86.81%)
4436	Reserved IP addresses (8.12%)
1763	Used IP addresses (3.23%)
1010	Transient IP addresses (1.85%)
54656	Total IP addresses

86.81% of IP addresses currently in the Orion database are Available.

13.19% of IP addresses currently in the Orion database are Not Available.

Figure 1 - Chart View of IP Space Allocation Shown in SolarWinds IP Address Manager

- **Preventative Alerting** – It is also crucial to recognize and correct issues before your users experience fault or performance problems, which is why a powerful alert engine is such a vital piece of any IPAM solution.
- **IP Address Tracking and Event Recording** –The ability to track addresses and see how certain properties have changed over time, as well as record who made what changes and when has become increasingly important, not only for forensic analysis for problem resolution, but for auditing purposes to prove compliance.
- **Resolving IP Conflicts** – Too many IP addresses dynamically being assigned can sometimes lead to IP address conflicts, which result in downtime and lost productivity. By performing regular IP address scans, you can ensure that your IP address space is always updated with the IP address and MAC address assignment data.
- **IP Address Reporting** – Intelligent built-in reporting and the ability to easily create and share customized IP reports, is especially useful in enterprise networks with a multi-person IT team.

DHCP/DNS Management and Monitoring – Your DHCP and DNS servers are at the core of your IP infrastructure. The DHCP server provides a centralized database of IP addresses that are dynamically assigned to devices connected to the network. This eliminates the error-prone and laborious task of manually assigning IP addresses to each device, thereby avoiding duplicate resource assignments and IP conflict. Your DNS server works in conjunction with your DHCP server to translate human-readable domain names and hostnames into the corresponding numeric IP address.

By tightly integrating IP address management with DHCP/DNS management and monitoring, you get better manageability of your IP infrastructure through a unified global view. This will result in improved network security, increased efficiency by eliminating duplicate efforts in IP administration, decreased network downtime due to IP address conflicts, and improved regulatory compliance through historical tracking and event recording of all IP related activities.

User Device Tracking & Switch Port Monitoring

BYOD clearly increases the number of devices and users connecting to your network, resulting in both increased security risks and additional capacity burden on switch ports and wireless access points. This, in turn, increases the need for an effective method to track those users and devices and manage switch port capacity. For the purpose of this paper, we will refer to this as User Device Tracking and Switch Port Monitoring. Proper user device tracking and switch port monitoring can provide a wealth of information.

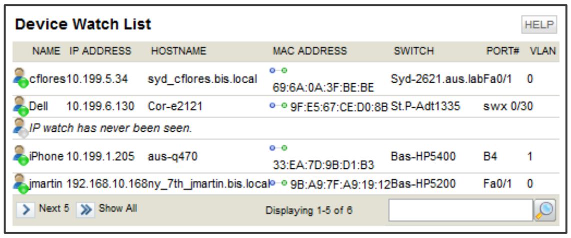
- Where (which switch port) a user is connected to the network
- Where a device is currently or was previously connected to the network by just knowing its IP or MAC address
- Which user connected the device on the network
- Historical data on when and where the device was connected, and who used it
- Switch capacity
- Information on individual ports per switch

Tracking Down Rogue or Suspicious BYOD Devices

There are a couple of methods for tracking down rogue or suspicious devices on your network.

First, you can do a quick search for a device by user name, MAC address, IP address or Hostname. Once the device has been located on the network, you can determine the switch, port, and VLAN the device is connected to in order to get the location. Once this information is obtained, you can isolate or shut down the port that the suspected device is on. As the number of devices on your network increases, you can see how this could get to be a very time consuming and tedious manual process. This leads us to the second method.

Create a device watch list to keep an eye out for specific devices and receive an alert when they connect to the network. With an automated tool for user tracking, you can automatically scan your network for the suspicious devices and receive an alert when they are located. Once they are located, you will, again, be able to determine the switch, port, or VLAN and take appropriate action.



Device Watch List

NAME	IP ADDRESS	HOSTNAME	MAC ADDRESS	SWITCH	PORT#	VLAN
cflores	10.199.5.34	syd_cflores.bis.local	69:6A:0A:3F:BE:BE	Syd-2621.aus.lab	Fa0/1	0
Dell	10.199.6.130	Cor-e2121	9F:E5:67:CE:D0:8B	St.P-Adt1335	swx 0/30	
IP watch has never been seen.						
iPhone	10.199.1.205	aus-q470	33:EA:7D:9B:D1:B3	Bas-HP5400	B4	1
jmartin	192.168.10.168	ny_7th_jmartin.bis.local	9B:A9:7F:A9:19:12	Bas-HP5200	Fa0/1	0

Displaying 1-5 of 6

Figure 2 - Device Watch List as Shown in SolarWinds User Device Tracker

Switch Port Monitoring

With the increasing number of devices on your network, you place additional burden on your switches and wireless access points. As a result, you need to understand the status, performance and capacity of your switches and their ports.

The first step in proactively monitoring your switch ports is to map your current switches. By mapping your switches, you can see exactly which ports are in use on any given switch.

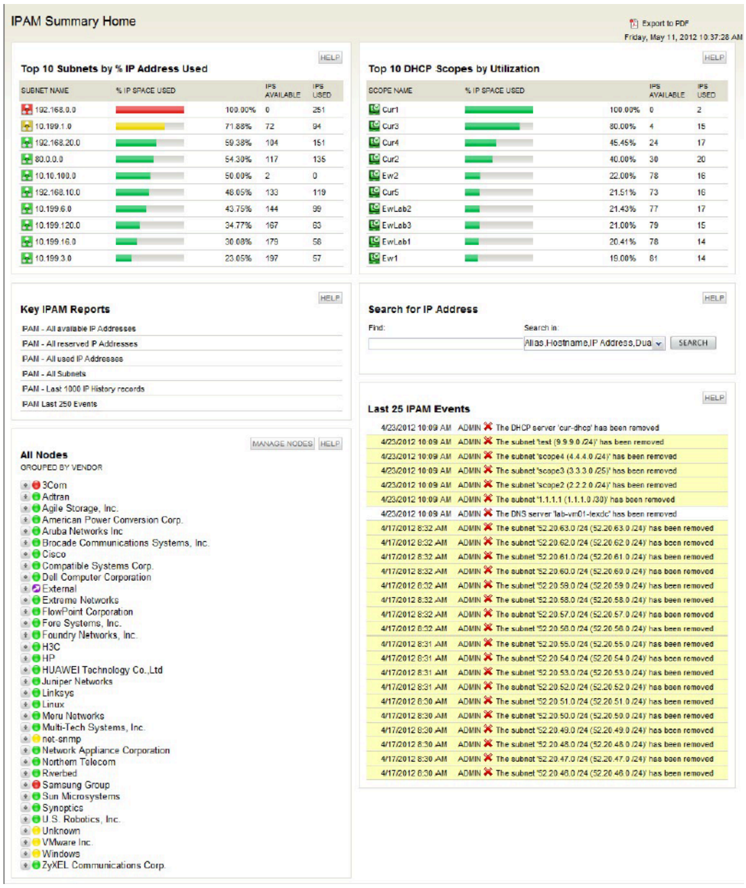
Once the ports are mapped, you will want to begin monitoring them, preferably in real-time. Monitoring your switches and ports will allow you to see key performance indicators such as ports used, CPU load, memory used and more so you can identify potential problems before they arise.

And lastly, you will want the ability to historically track configuration details and historical data pertaining to the port. Details that you will want to track include port name, port number, and VLAN, along with a complete history of devices that have been attached to the port.

Automated Tools

By now you should be able to see that the use of automated tools to perform these tasks becomes more beneficial as the number of devices on your network increases. SolarWinds provides two such tools to help you manage the BYOD chaos: SolarWinds IP Address Manager and SolarWinds User Device Tracker.

SolarWinds IP Address Manager is an easy-to-use software solution that provides role-based IP Address management, DHCP Management and Monitoring, and DNS Monitoring. With the SolarWinds IPAM solution, you can manage your entire IP infrastructure from an intuitive, centralized web console.



IPAM Summary Home

Export to PDF

Friday, May 11, 2012 10:37:28 AM

Top 10 Subnets by % IP Address Used

SUBNET NAME	% IP SPACE USED		IPS AVAILABLE	IPS USED
192.168.0.0	🟥	100.00%	0	251
10.199.1.0	🟨	71.88%	72	94
192.168.20.0	🟩	59.38%	104	151
80.0.0.0	🟩	54.30%	117	135
10.10.100.0	🟩	50.00%	2	0
192.168.10.0	🟩	48.05%	133	119
10.199.6.0	🟩	43.75%	144	99
10.199.120.0	🟩	34.77%	167	63
10.199.16.0	🟩	30.08%	179	58
10.199.3.0	🟩	23.05%	197	57

Top 10 DHCP Scopes by Utilization

SCOPE NAME	% IP SPACE USED		IPS AVAILABLE	IPS USED
Cur1	🟩	100.00%	0	2
Cur3	🟩	80.00%	4	15
Cur4	🟩	45.45%	24	17
Cur2	🟩	40.00%	30	20
Ew2	🟩	22.00%	78	16
Cur5	🟩	21.51%	73	16
EwLab2	🟩	21.43%	77	17
EwLab3	🟩	21.00%	79	15
EwLab1	🟩	20.41%	78	14
Ew1	🟩	19.00%	81	14

Key IPAM Reports

- PAM - All available IP Addresses
- PAM - All reserved P Addresses
- PAM - All used IP Addresses
- PAM - All Subnets
- PAM - Last 1000 IP History records
- PAM Last 250 Events

Search for IP Address

Find:

Search in: Alias,Hostname,IP Address,Dua

All Nodes

GROUPED BY VENDOR

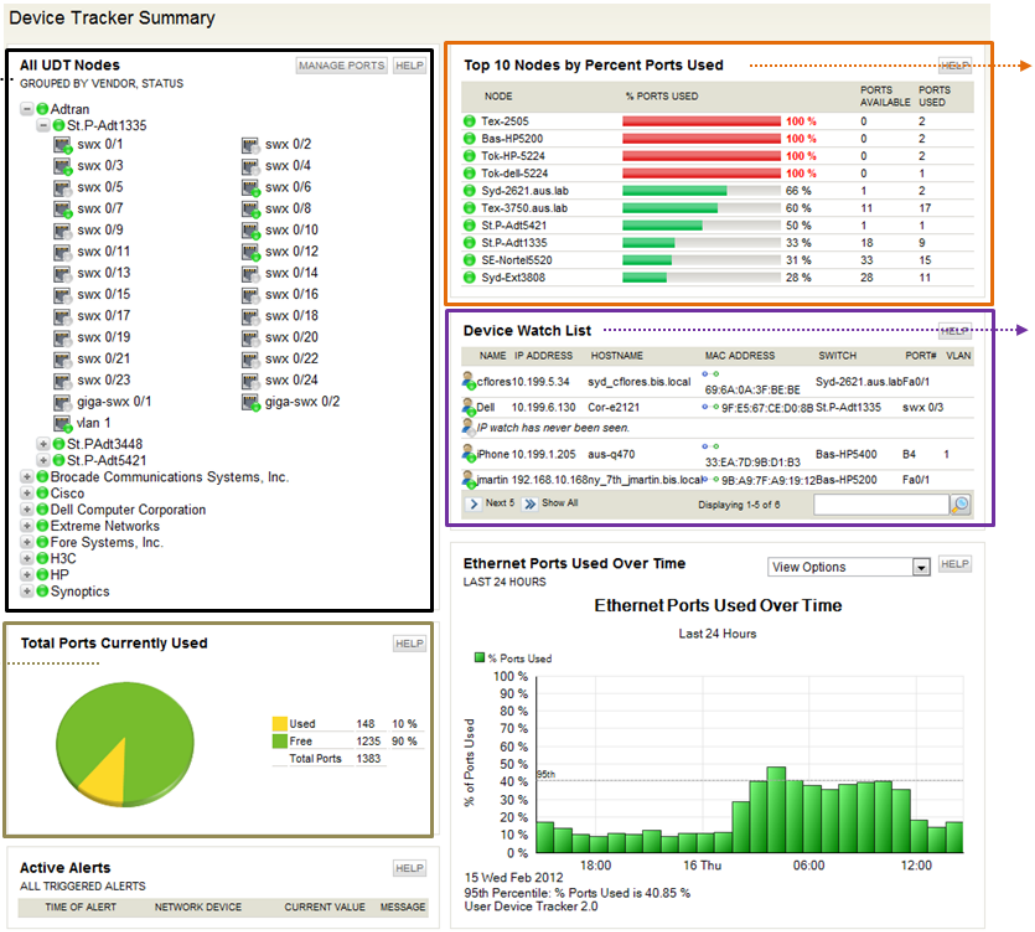
- ● 3Com
- ● Adtran
- ● Agile Storage, Inc.
- ● American Power Conversion Corp.
- ● Aruba Networks Inc
- ● Brocade Communications Systems, Inc.
- ● Cisco
- ● Compatible Systems Corp.
- ● Dell Computer Corporation
- ● External
- ● Extreme Networks
- ● FlowPoint Corporation
- ● Fore Systems, Inc.
- ● Foundry Networks, Inc.
- ● H3C
- ● HP
- ● HUAWEI Technology Co.,Ltd
- ● Juniper Networks
- ● Linksys
- ● Linux
- ● Meru Networks
- ● Multi-Tech Systems, Inc.
- ● net-snmp
- ● Network Appliance Corporation
- ● Northern Telecom
- ● Riverbed
- ● Samsung Group
- ● Sun Microsystems
- ● Synoptics
- ● U.S. Robotics, Inc.
- ● Unknown
- ● VMware Inc.
- ● Windows
- ● ZyXEL Communications Corp.

Last 25 IPAM Events

```
4/23/2012 10:09 AM   ADMIN ✗ The DHCP server 'cur-dhcp' has been removed
4/23/2012 10:09 AM   ADMIN ✗ The subnet 'test (9.9.9.0 /24)' has been removed
4/23/2012 10:09 AM   ADMIN ✗ The subnet 'scope4 (4.4.4.0 /24)' has been removed
4/23/2012 10:09 AM   ADMIN ✗ The subnet 'scope3 (3.3.3.0 /25)' has been removed
4/23/2012 10:09 AM   ADMIN ✗ The subnet 'scope2 (2.2.2.0 /24)' has been removed
4/23/2012 10:09 AM   ADMIN ✗ The subnet '1.1.1.1 (1.1.1.0 /30)' has been removed
4/23/2012 10:09 AM   ADMIN ✗ The DNS server 'lab-vm01-lexdc' has been removed
4/17/2012 8:32 AM    ADMIN ✗ The subnet '52.20.63.0 /24 (52.20.63.0 /24)' has been removed
4/17/2012 8:32 AM    ADMIN ✗ The subnet '52.20.62.0 /24 (52.20.62.0 /24)' has been removed
4/17/2012 8:32 AM    ADMIN ✗ The subnet '52.20.61.0 /24 (52.20.61.0 /24)' has been removed
4/17/2012 8:32 AM    ADMIN ✗ The subnet '52.20.60.0 /24 (52.20.60.0 /24)' has been removed
4/17/2012 8:32 AM    ADMIN ✗ The subnet '52.20.59.0 /24 (52.20.59.0 /24)' has been removed
4/17/2012 8:32 AM    ADMIN ✗ The subnet '52.20.58.0 /24 (52.20.58.0 /24)' has been removed
4/17/2012 8:32 AM    ADMIN ✗ The subnet '52.20.57.0 /24 (52.20.57.0 /24)' has been removed
4/17/2012 8:32 AM    ADMIN ✗ The subnet '52.20.56.0 /24 (52.20.56.0 /24)' has been removed
4/17/2012 8:31 AM    ADMIN ✗ The subnet '52.20.55.0 /24 (52.20.55.0 /24)' has been removed
4/17/2012 8:31 AM    ADMIN ✗ The subnet '52.20.54.0 /24 (52.20.54.0 /24)' has been removed
4/17/2012 8:31 AM    ADMIN ✗ The subnet '52.20.53.0 /24 (52.20.53.0 /24)' has been removed
4/17/2012 8:31 AM    ADMIN ✗ The subnet '52.20.52.0 /24 (52.20.52.0 /24)' has been removed
4/17/2012 8:30 AM    ADMIN ✗ The subnet '52.20.51.0 /24 (52.20.51.0 /24)' has been removed
4/17/2012 8:30 AM    ADMIN ✗ The subnet '52.20.50.0 /24 (52.20.50.0 /24)' has been removed
4/17/2012 8:30 AM    ADMIN ✗ The subnet '52.20.49.0 /24 (52.20.49.0 /24)' has been removed
4/17/2012 8:30 AM    ADMIN ✗ The subnet '52.20.48.0 /24 (52.20.48.0 /24)' has been removed
4/17/2012 8:30 AM    ADMIN ✗ The subnet '52.20.47.0 /24 (52.20.47.0 /24)' has been removed
4/17/2012 8:30 AM    ADMIN ✗ The subnet '52.20.46.0 /24 (52.20.46.0 /24)' has been removed
```

Figure 3 - SolarWinds IP Address Manager Summary Page

SolarWinds User Device Tracker allows you to track and locate users and devices by username, IP address, Hostname, or MAC address. In addition, with SolarWinds UDT you can map and monitor all of the switches and ports on your network from a single, centralized view.



Device Tracker Summary

All UDT Nodes MANAGE PORTS HELP
GROUPED BY VENDOR, STATUS

- Adtran
  - St.P-Adt1335
    - swx 0/1
    - swx 0/2
    - swx 0/3
    - swx 0/4
    - swx 0/5
    - swx 0/6
    - swx 0/7
    - swx 0/8
    - swx 0/9
    - swx 0/10
    - swx 0/11
    - swx 0/12
    - swx 0/13
    - swx 0/14
    - swx 0/15
    - swx 0/16
    - swx 0/17
    - swx 0/18
    - swx 0/19
    - swx 0/20
    - swx 0/21
    - swx 0/22
    - swx 0/23
    - swx 0/24
    - giga-swx 0/1
    - giga-swx 0/2
    - vlan 1
  - St.PAdt3448
  - St.P-Adt5421
- Brocade Communications Systems, Inc.
- Cisco
- Dell Computer Corporation
- Extreme Networks
- Fore Systems, Inc.
- H3C
- HP
- Synoptics

Switch Monitoring dashboard with drill-down facility to discover and monitor port status

Top 10 Nodes by Percent Ports Used HELP

NODE	% PORTS USED	PORTS AVAILABLE	PORTS USED
Tex-2505	100 %	0	2
Bas-HP5200	100 %	0	2
Tok-HP-5224	100 %	0	2
Tok-dell-5224	100 %	0	1
Syd-2621.aus.lab	66 %	1	2
Tex-3750.aus.lab	60 %	11	17
St.P-Adt5421	50 %	1	1
St.P-Adt1335	33 %	18	9
SE-Nortel5520	31 %	33	15
Syd-Ext3808	28 %	28	11

Shows the Top 10 Nodes by Percent Utilization of Ports in a simple ready reckoner dashboard

Device Watch List HELP

NAME	IP ADDRESS	HOSTNAME	MAC ADDRESS	SWITCH	PORT#	VLAN
cflores	10.199.5.34	syd_cflores.bis.local	69:6A:0A:3F:BE:BE	Syd-2621.aus.lab	Fa0/1	
Dell	10.199.6.130	Cor-e2121	9F:E5:67:CE:D0:8B	St.P-Adt1335	swx 0/3	
IP watch has never been seen.						
iPhone	10.199.1.205	aus-q470	33:EA:7D:9B:D1:B3	Bas-HP5400	B4	1
jmartin	192.168.10.168	ny_7th_jmartin.bis.local	9B:A9:7F:A9:19:12	Bas-HP5200	Fa0/1	

Next 5 Show All Displaying 1-5 of 6

Add a device with MAC address, IP address or hostname and keep alerted about the device connections and users

Total Ports Currently Used HELP

Used	148	10 %
Free	1235	90 %
Total Ports	1383	

Shows the Port Utilization Pie Chart

Active Alerts HELP
ALL TRIGGERED ALERTS

TIME OF ALERT	NETWORK DEVICE	CURRENT VALUE	MESSAGE

Ethernet Ports Used Over Time View Options HELP
LAST 24 HOURS

95th Percentile: % Ports Used is 40.85 %
User Device Tracker 2.0

Figure 4 - SolarWinds User Device Tracker Summary Page

Enterprise Mobile Device Security – Best Practices

Access and Usage

It is important for organizations to understand how employee-owned devices are being used in the corporate network. There is the likelihood that bandwidth consumption will increase if the BYOD devices are used for unofficial purposes, such as streaming videos, music, and other personal use. But, blocking all access to these devices is not the answer since utilization of personal devices can actually lead to increased work productivity. A better approach would be for network admins to focus on enabling safe access. This calls for robust IT security user privileges in terms of bandwidth consumption and user logon. The risk is constantly growing with new devices being added to the network. It is left to the IT department to fasten a harness to ensure security and control resource utilization.

Creating and Enforcing Security Policies

Security policies chart the guidelines and set out restrictions that govern the functionality and usage of employee-owned devices within the corporate network. These policies should be tailored to include employees' specific devices, roles, and locations. Access rights and user privileges for accessing secure data, servers, and databases must also be regulated based on employees' devices and their roles. It's also imperative for employees to understand the security aspects and the risks, threats and vulnerabilities faced with BYOD. Employees must be educated on how the extra precautions that should be taken when using personal devices within the corporate network, how to safeguard credentials, and how these devices can become a gateway to launch malicious attacks on the organization's secure data and IT assets.

Implementing Intelligent and Advanced Security Equipment

It should be noted that BYOD is being allowed by enterprises not just to keep the work environment employee-friendly, but also to get better productivity. So, in addition to implementing effective IP address management and user device tracking tools, organizations should evaluate the ROI in advanced security equipment and appliances. Within affordable limits, and in the objective of meeting higher productivity, companies can upgrade their perimeter security devices, including IDS/IPS, firewalls, and VPNs to further secure their network from the onslaught of personal devices.

Summary

At the end of the day, BYOD is definitely a boon towards mobilizing the enterprise and gaining higher employee productivity, but this is a bet that needs to be well thought out before implementation. With the right tools and policies to keep it under control, BYOD can substantially benefit businesses and employees alike in developing a more conducive and productive work environment. So, rather than fearing BYOD, fighting against it, or just plain ignoring it, IT departments should embrace its benefits and address it head on with effective, easy-to-use solutions from SolarWinds.

Download SolarWinds IP Address Manager and User Device Tracker now and get a handle on BYOD today.

About SolarWinds IP Address Manager

SolarWinds IP Address Manager (IPAM) provides detailed visibility into IP address space usage; making it easy to minimize conflicts and ensure your network is always humming. Now you can manage, alert and report on your IP address space, manage and monitor Microsoft® DHCP and DNS services, and monitor Cisco® DHCP servers; all from a centralized Web console.

IPAM Highlights:

- Centrally manage, monitor, alert, & report on entire IP infrastructure
- Maintain Microsoft DHCP/DNS & Cisco DHCP services from a single web interface
- Optimize IP space utilization & avoid IP conflicts via automatic scans & preventative alerts
- Deliver role-based access control along with detailed event recording & activity logs
- Gain critical insight into IP address space through real-time views & historical tracking
- Generate powerful IP address reports using customizable out-of-the-box templates

About SolarWinds User Device Tracker

SolarWinds User Device Tracker (UDT) delivers the device-tracking capabilities of an expensive switch port-tracking appliance at a price point that even your CFO will love. Why buy an expensive appliance when you can use SolarWinds User Device Tracker to quickly find devices, create a device watch list, and even track switch capacity.

UDT Highlights:

- Quickly finds a computer & retrieves the user name, switch name, port, port description, VLAN, & more
- Enables searching on IP address, user name, Hostname, or MAC address to trace the location of a device
- Tracks last known location of a device & delivers an alert when a device connects to the network
- Shows available network ports & discovers switches operating near full capacity

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide - from Fortune 500 enterprises to small businesses. The company works to put its users first and remove the obstacles that have become “status quo” in traditional enterprise software. SolarWinds products are downloadable, easy to use and maintain, and provide the power, scale, and flexibility needed to address users’ management priorities. SolarWinds’ online user community, http://thwack.com, is a gathering-place where tens of thousands of IT pros solve problems, share technology, and participate in product development for all of the company’s products. Learn more today at http://solarwinds.com.