whitepaper

How to Locate and Quarantine Unidentified Systems on Your Network

solarwinds

whitepaper

How to Locate and Quarantine Unidentified Systems on Your Network

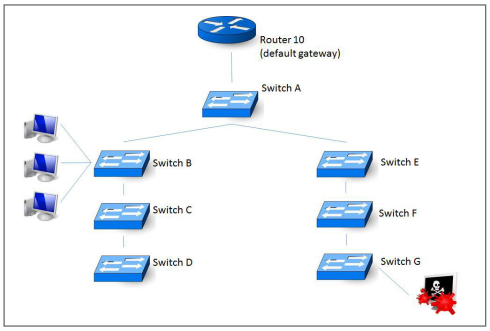
Classics are great when talking about cars and rock-n-roll. But when it comes to network administration, doing things "old school" can cost you. Sure, you can use open source tools and basic CLI commands to get the job done, but during an incident it's speed that counts and during those times, metaphorically speaking, a Bugatti Veyron is simply better than a '67 Mustang.

Many network admins have faced, at one time or another, the pressure of having to quickly locate a device that resides somewhere on their network and when a network consists of tens or hundreds of routers and switches, many don't know where to start or how to perform the task – especially in a mixed vendor environment. This may explain why you see Internet discussion boards filled with pleas for help. But a crisis is not the time to be learning how to perform a network trace back. When you have a rogue DHCP server or a DoS attack originating within the network, it's all about finding the offending system fast and terminating network access. It's all about speed.

The Long and Winding Road

The challenge of finding rogue devices is complicated by two factors. The first is network complexity and the second is the persistence of forensic data.

In the old days, networks were fairly flat. However, today network topologies are much more hierarchical and complex. Each node gets its own virtual network segment. Network segments are logically grouped and concentrated into peripheral switches. Peripheral switches are organized hierarchically under core switches. Core switches are connected via routers. The many combinations and possibilities are almost endless. This leads us to the central problem: In order to locate a device, you need to identify the switch that the device is connected to. Let's see how this is done.



Finding a rogue device on a large, complex network can be difficult, because it can be located behind one or many routers and switches on your network.

Assume it's 8:30 a.m. and the finance department is getting ready to run quarter-end reports. Suddenly your network management system begins to throw alerts about a crippling problem (like high bandwidth usage or captures SNMP details from a node that does not belong on your network) and identifies an offending IP address. Time to mobilize. So you ask "what system owns that address and where is it located?"

If you're lucky, you might get a quick hit by using the Microsoft® Windows® getmac command. From a Windows system, type getmac –s xxx.xxx.xxx.xxx. If the target system also happens to be a Windows system, then the utility will return the Windows domain and User Name assigned. However, as helpful as this might be, you still have to locate the switch port the system is connected to so you can remove the system from the network.
Another relatively easy (but not foolproof) way to get the MAC address of an IP address within the same network or subnet is to ping the IP address and then immediately inspect the local ARP table. To do this, follow these steps (assuming it's from a Windows PC):

- Click Window Start and in the search programs and files, type CMD and then Enter. This should open a "DOS window"

- At the command prompt, type ping xxx.xxx.xxx.xxx, where xxx.xxx.xxx.xxx is the offending IP address. For example, ping 192.168.10.1. If the ping is successful, you should see a reply from the remote device. However, if the ping request could not find the host then you will not be able to proceed with the next step.

- Immediately again at the command prompt type arp –a. This command will return a table listing all of the IP addresses your PC knows how to contact. Examine this table for the offending IP and immediately to the right you should see its corresponding "physical address". This is the MAC address you are looking for. Write this down. It will be a six-part hexadecimal number. For example: 20.1F.AF.FF.00.16.

As an aside, now that you have an MAC address, it's sometimes helpful to know what kind of hardware you're looking for. There are several websites, like www.MACVendorLookup.com, that can do a lookup on the MAC address and tell you what vendor assigned that address. For example, you may learn your offending MAC address was assigned by Dell®. This suggests you're looking for a "Wintel" system.

This method of finding the MAC address using PC utilities ping and arp will often work. However, if it does not, then it will require a lot more effort to locate the offending MAC address. Plan B will be to visit each router and issue this command (assuming Cisco® IOS): sharp. Issuing this command will show all IP addresses and their corresponding MAC addresses known to the router. However, your chances of finding what you are looking for on the first attempt are slim. Therefore, you will need to repeat this process on all routers until you find the offending IP and MAC address.

If you are successful in locating the MAC address then congratulations! Now you are ready to find the switch and switch port that the device is connected to. We must do this in order to physically disconnect the offending device from the network. And to state what might not be obvious, in an emergency, it is often faster to locate the connecting switch and switch port than actually try and physically locate the PC. This is why your priority should be to find the switch and port.

So now that you have a MAC address you can begin your search for the switch and port by doing the following:

- For each switch in your network, issue the following switch command "show mac-address-table" (NOTE: this example assumes a Cisco IOS or compatible switch). The switch will return a table showing what MAC addresses are associated with each active switch port. Review this table for the MAC address in question.

    - If you find it, then you now know the device is connected to this switch and you can now disconnect the offending device from the network.

    - If you do not find the MAC address in this table, then move to the next connected switch and repeat the process.

When taken together, these procedures can help you locate a device on your network. However, it should apparent that there are painful limitations to this approach. First, as you can see this process is very time consuming and requires not only technical expertise but also privileged login access to your network routers and switches. Second, sometimes it would be very helpful to know who owns the system we are trying to locate. Unfortunately, there may not be utilities that can uniformly query and return this user information.

Earlier we also said there were two factors that complicated our efforts to locate devices. The first was network complexity (requiring us to query a number of routers and switches). The second is the persistence of forensic data. Our discovery technique relies heavily on inspecting cached network operations data (ARP caches). However, from time to time this cached data is cleared. Once cleared, it is impossible to determine where the system resides until the system becomes active again. Clearly this is a problem for mobile or intermittent rouge systems and may make it impossible to perform an analysis days after an incident has occurred.

Take It Easy

As we said at the beginning, during a crisis you want something like a user device tracker that locates distressed systems fast and drop-dead easy – like being able to search for a device like using Google to search for sushi. Typing in an IP address or MAC address would certainly be faster and much easier than reviewing Port/MAC address tables from tens or even hundreds of switches! PLUS having the added bonus of seeing what user (or users) had an offending IP address over time AND as a double bonus being able to create alerts and whitelists to automatically track and isolate offending systems.

SolarWinds User Device Tracker is like that fast and elegant Bugatti that you have always dreamed of driving. It delivers automated user and device tracking along with port tracker and powerful switch port management capabilities so you can stay in control of who and what are connecting to your network. Quickly find a computer or user, as well as track down lost or rogue devices with a simple search on a user name, IP address, Hostname, or MAC address. And, if the user or device is no longer connected, historical data will show its last known location. You can even perform whitelisting or create a watch list, and be alerted immediately when a specific user or device connects. Plus, SolarWinds User Device Tracker lets you take immediate action to shut down a port and mitigate a threat or alleviate a network performance issue. Best of all, you can do it all from an easy-to-use, point-and-click Web interface!

Fortunately the choice is not limited between loving the classics and working smart. Why not have it all? Classic cars, rock-n-roll and SolarWinds User Device Tracker. Life is good. Download your FREE fully functional 30-day trial today!

About User Device Tracker (UDT)

SolarWinds User Device Tracker (UDT) delivers automated user and device tracking along with powerful switch port management capabilities so you can stay in control of who and what are connecting to your network. Quickly find a computer or user, as well as track down lost or rogue devices with a simple search on a user name, IP address, Hostname, or MAC address. And, if the user or device is no longer connected, historical data will show its last known location. You can even perform whitelisting or create a watch list, and be alerted immediately when a specific user or device connects. Plus, SolarWinds User Device Tracker lets you take immediate action to shut down a port and mitigate a threat or alleviate a network performance issue. Best of all, you can do it all from an easy-to-use, point-and-click Web interface!

LEARN MORE » DOWNLOAD FREE TRIAL

whitepaper