solarwinds

NETWORK TROUBLESHOOTING AND PROBLEM IDENTIFICATION

By: Brad Hale

SOLARWINDS
WHITEPAPER

TABLE OF CONTENTS

NETWORK TROUBLESHOOTING AND PROBLEM IDENTIFICATION

INTRODUCTION

The only things in life that are certain are death, taxes, and network issues. Okay, I added the last one, but we all know that no matter how carefully planned your network design is, how much redundancy you have built in, or how much you proactively monitor your network, you are bound to have a problem at some point. And when that problem occurs, you need to know the steps and tools to troubleshoot the problem so you can minimize the impact on end-users.

This paper will look at five common network issues and provide some basic troubleshooting and problem identification tips and tools. If you are not familiar with basic network fundamentals and protocols, please see SolarWinds® Network Monitoring for Dummies.

TROUBLESHOOTING NETWORK PERFORMANCE ISSUES

"The network is slow today," is, without a doubt, one of the most disliked phrases heard by network administrators. The network has become a dumping ground for problems that originate as often as not from servers and applications as from the network. Thus, one of the biggest jobs of the network administrator is to defend their network from being accused of being the cause of today's problem. Because slow performance is often first—and often incorrectly— attributed to the network, rapid identification and problem isolation is critical to the administrator's workload.

Baseline Network Performance

Hopefully you have performed a baseline of your network performance so you know the normal working conditions of your network infrastructure. This baseline can then be used for comparison to catch changes that could indicate a problem, provide early indicators that application and network demands are pushing near the available capacity, and align network performance baselines with Service Level Agreements (SLAs).

If you haven't established a baseline, you will need to rely on your equipment vendors and their recommended or best practice thresholds. You can also use various network equipment or monitoring forums to see what other IT professionals are doing.

Collect Network Device Performance Metrics

Network device performance metrics provide information about the system resources on each individual device. These metrics are critical in ascertaining whether a resource overuse problem is a central cause of a reduction in performance. Collecting and reporting on network devices helps the troubleshooting administrator quickly identify whether the device is a source of the problem or the problem lies within the network traffic or application communication itself.

Device monitoring using Simple Network Management Protocol (SNMP) provides a very device-centric view of network conditions. Using SNMP, counters on a device such as a router, switch, or firewall can be measured and forwarded to a network management system for review. This data is useful for understanding performance conditions that are specific to that device. Performance statistics such as CPU utilization, interface/bandwidth utilization, and memory utilization represent the majority of performance issues encountered in the day-to-day operation of network devices. You can monitor these device statistics using one of many commercially available network monitoring software products.

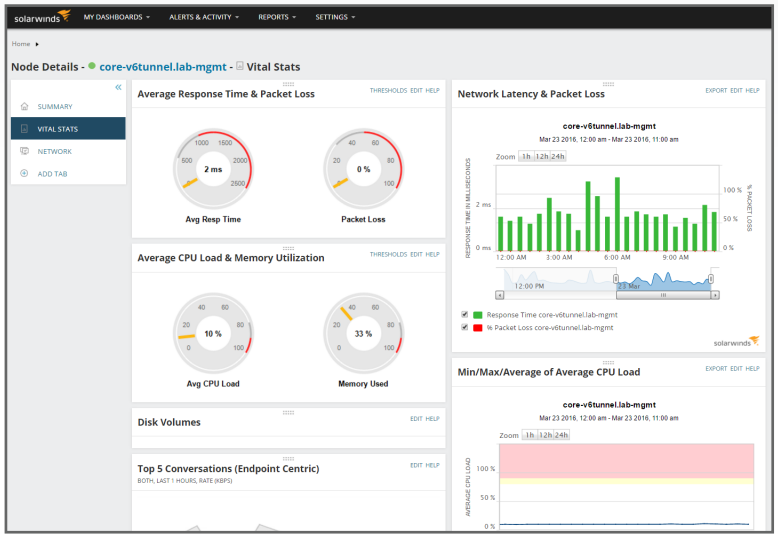


Figure 1: CPU load and memory utilization from SolarWinds Network Performance Monitor

Switch/Router CPU Utilization

Common symptoms of high CPU utilization within your switch or router include:

- High percentages in the show process cpu command output
- Input queue drops
- Slow performance
- Services such as Telnet, console response, ping response, or updates fail
- High buffer failures

If you are able to connect to the router, then you can use the show process cpu (for Ciscorouters) command to check if CPU utilization is high due to interrupts or processes.

```
router#show processes
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID  Q  Ty         PC   Runtime(uS)    Invoked   uSecs      Stacks  TTY  Process
   1  C  sp   602F3AF0             0       1627       0   2600/3000    0  Load Meter
   2  L  we   60C5BE00             4        136      29   5572/6000    0  CEF Scanner
   3  L  st   602D90F8          1676        837    2002   5740/6000    0  Check heaps
   4  C  we   602D08F8             0          1       0   5568/6000    0  Chunk Manager
   5  C  we   602DF0E8             0          1       0   5592/6000    0  Pool Manager
   6  M  st   60251E38             0          2       0   5560/6000    0  Timers
   7  M  we   600D4940             0          2       0   5568/6000    0  Serial Backgroun
   8  M  we   6034B718             0          1       0   2584/3000    0  OIR Handler
   9  M  we   603FA3C8             0          1       0   5612/6000    0  IPC Zone Manager
  10  M  we   603FA1A0             0       8124       0   5488/6000    0  IPC Periodic Tim
  11  M  we   603FA220             0          9       0   4884/6000    0  IPC Seat Manager
  12  L  we   60406818           124       2003      61   5300/6000    0  ARP Input
  13  M  we   60581638             0          1       0   5760/6000    0  HC Counter Timer
  14  M  we   605E3D00             0          2       0   5564/6000    0  DDR Timers
  15  M  we   605FC6B8             0          2       0 11568/12000    0  Dialer event
```

Cisco provides two great documents on Troubleshooting High CPU Utilization and Troubleshooting High CPU Utilization Caused by Interrupts.

Switch/Router Memory Utilization

Memory is a limited resource on all network devices and must be controlled and monitored to help ensure that utilization is kept in check. A memory allocation failure means either the network device has used all available memory, or the memory has fragmented such that the device cannot find a usable available block.

For Cisco routers, the symptoms of memory allocation failure include, but are not limited to:

- The console or log message: "%SYS-2-MALLOCFAIL: Memory allocation of 1028 bytes failed from 0x6015EC84, Pool Processor, alignment 0"
- Refused Telnet sessions
- The show processor memory command is displayed no matter what command you type on a console
- No output from some show commands
- "Low on memory" messages
- The console message "Unable to create EXEC - no memory or too many processes"
- Router hanging, no console response

Possible causes of memory failure include:

- In Processor Memory ("Pool Processor" on all platforms)
  - Memory Size Does not Support the Cisco IOS Software Image
  - Memory Leak Bug
  - Large Quantity of Memory Used for Normal or Abnormal Processes
  - Memory Fragmentation Problem or Bug
  - Memory Allocation Failure at Process = <interrupt level>
- In Packet Memory
  - Not Enough Shared Memory for the Interfaces
  - Buffer Leak Bug
  - Router Running Low on Fast Memory

Interface/Bandwidth Utilization

Before you start digging into the gory details of your router interfaces, it is best to simply monitor the overall bandwidth utilization to determine if you even have a problem. Numerous open source or free tools from network management suppliers exist in the market that greatly simplify the process of gathering bandwidth utilization data and presenting it in an easy-to-consume graphical format. SolarWinds free Real-Time Bandwidth Analyzer is an example of a commercially developed free tool that displays network device interface utilization.

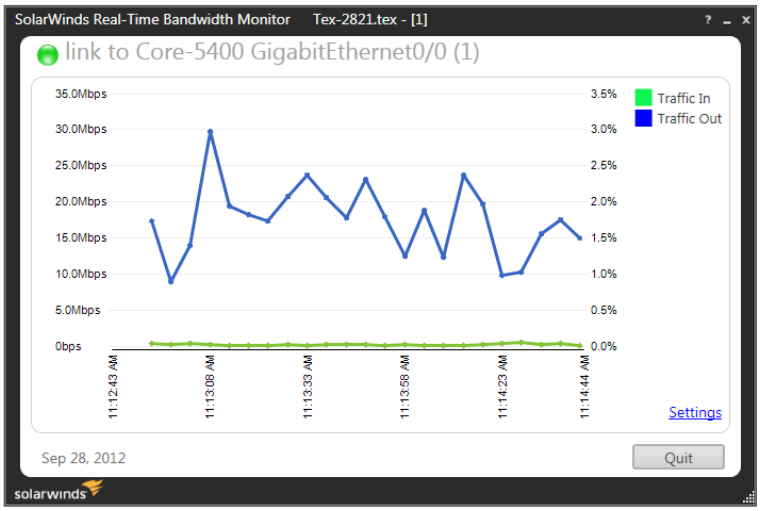


Figure 2: Interface utilization using SolarWinds free Real-Time Bandwidth Monitor

If you determine that you have a problem, you will want to get detailed information about the interface on your router. On Cisco routers, you can view the information about a particular interface using the **show interface** command:

```
Router# show interfaces

Ethernet 0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
  Internet address is 131.108.28.8, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters 0:00:00
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 2000 bits/sec, 4 packets/sec
     1127576 packets input, 447251251 bytes, 0 no buffer
     Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5332142 packets output, 496316039 bytes, 0 underruns
     0 output errors, 432 collisions, 0 interface resets, 0 restarts
```

TROUBLESHOOTING BANDWIDTH AND TRAFFIC

Bandwidth monitoring and traffic analysis are two key activities for every business environment. Performing each correctly assists the network administrator with identifying bottlenecks. It helps

the admin identify the network needs and uses of servers and their hosted applications, as well as how the network needs of one IT service impacts another. It also delivers hard data that objectively verifies the ability of the network to meet stated SLAs.

The two most common ways in which network traffic can be monitored and measured for performance are through packet and flow analysis. Traditional packet-based monitoring tools enable you to peer into individual packets to determine their contents, the transactions between systems, and the details of communications being passed along that network. Flow analysis provides insight into the flow of traffic within the network, specifically the who and what of traffic consumption.

The packet-based approach is a lot like attempting to determine the cause of a traffic jam by peeking into each individual vehicle. Knowing what people and cargo are travelling within each vehicle may be helpful in answering some questions, but it's not likely to illuminate the cause of the system-wide slowdown. Flow analysis, on the other hand, allows us to step back to see conditions in the system as a whole. To help you understand the differences in perspective here, let's take a look at common ways to measure traffic on a network:

- **Protocol analyzers** - Protocol analyzers take a look at network conditions from the perspective of the packet. These tools analyze conversations between devices on the network from the location where the analyzer is measuring. This information gives the network administrator an extremely detailed view of individual transactions between two devices and the specific data being transferred between them.
- **Hardware probes and distributed analyzers** - Hardware probes and distributed analyzers are an early attempt to overcome the limitations of an individual protocol analyzer. These tools can be positioned across the network to gather information. They go far in providing the whole-system perspective that is so difficult to obtain via the previous two perspectives.
- **Traffic flow analyzers** - These tools overcome the administration headaches of hardware probes and distributed analyzers by leveraging the data flow capture capabilities of the network device itself. Traffic flow analyzers receive flow data directly from monitored devices and analyze that data to gain the high-level perspective needed to troubleshoot incidents across the network.

Troubleshooting Paths Outside Your Network

In today's modern networks, more and more of your applications and services are SaaS-based and reside in the cloud or in a hybrid network environment, which makes it difficult to monitor once it leaves your network. Traditional diagnostic tools, such as traceroute, are severely limited in their ability to provide useful information outside your network. Advanced tools in the market such as SolarWinds Network Performance Monitor's NetPath™ deliver critical path hop-by-hop analysis, in on-premises, cloud, and hybrid networks.

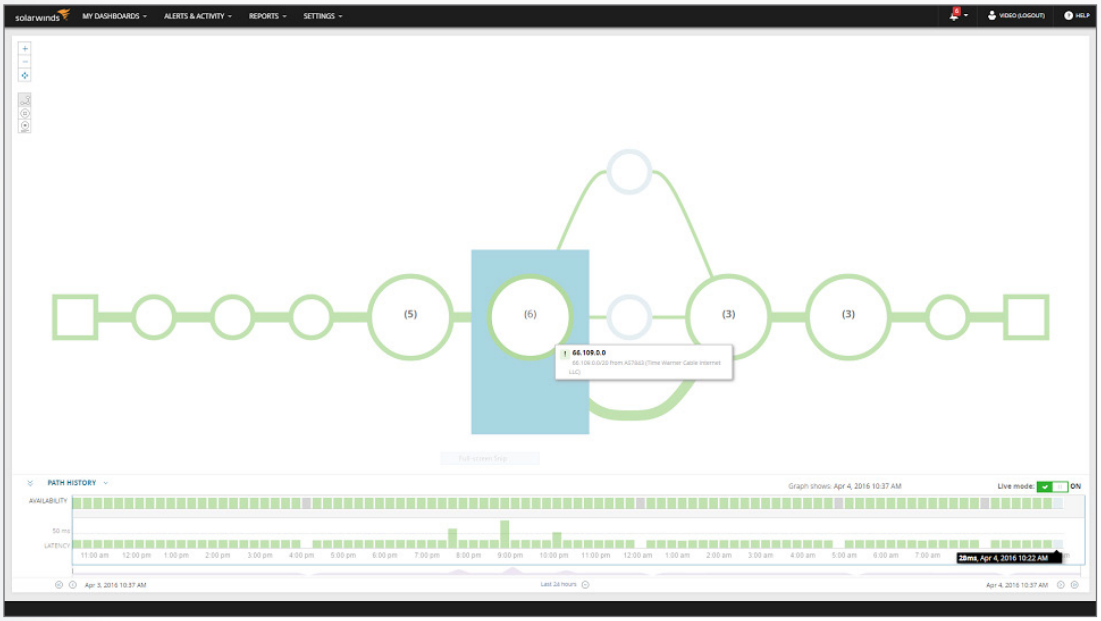


Figure 3: SolarWinds NetPath™ critical path hop-by-hop analysis

NetFlow

NetFlow is a network traffic monitor protocol developed by Cisco Systems for collecting IP traffic information. While the term NetFlow has become a de facto industry standard, many other manufacturers support alternative flow technologies, including Juniper® J-Flow®, HP® 3Com, Dell®, NETGEAR®, sFlow®, Huawei, Netstream®, and more.

Routers and switches that support NetFlow collect IP traffic statistics on all interfaces where NetFlow is enabled. Later, they export those statistics as NetFlow records, toward at least one NetFlow collector, typically a server that does the actual traffic analysis. The NetFlow collector then processes the data to perform the traffic analysis and presentation in a user-friendly format. NetFlow collectors can take the form of hardware-based collectors or probes, or software-based collectors. SolarWinds NetFlow Traffic Analyzer (NTA) is an example of a software-based NetFlow collector that collects traffic data, correlates it into a useable format, and then presents it to the user in a web-based interface.

Monitoring and analyzing NetFlow will help obtain valuable information about network users and applications, peak usage times, and traffic routing. In contrast with traditional SNMP-dependent systems, NetFlow-based traffic monitoring has the ability to characterize traffic from applications and users, understand the traffic patterns, provide a holistic view into bandwidth utilization and WAN traffic, support CBQoS validation and performance monitoring, be used for network traffic forensics, and aid in compliance reporting.

Configuring NetFlow on a Cisco router is a very straightforward and easy process. You can use a free tool, such as SolarWinds NetFlow Configurator, or you can manually configure using the following steps:

STEP	COMMAND	PURPOSE
1	*Router> enable*	Enters privileged EXEC mode Enter your password if prompte
2	*Router# configure terminal*	Enters global configuration mode
3	*Router(config)# ip flow-export Version 9*	Enables v9 data export for the main cache
4	*Router(config)# ip flow-export templates refresh-rate 15*	(Optional) Specifies the refresh rate in number of export packets. packets is an integer from 1 to 600. The default is 20 packets.
5	*Router(config)# ip flow-export template timeout-rate 90*	(Optional) Specifies the timeout rate in minutes. minutes is an integer from 1 to 3600. The default is 30 minutes
6	*Router(config)# ip flow-export template options export-stats*	Specifies the options template export statistics, including how many export packets have been sent and how many flows have been exported.
7	*Router(config)# ip flow-export template options refresh-rate 25*	(Optional) Specifies the refresh rate in number of export packets. packets is an integer from 1 to 600. The default is 20 packets.
8	*Router(config)# ip flow-export template options timeout-rate 120*	(Optional) Specifies the timeout rate in minutes. minutes is an integer from 1 to 3600. The default is 30 minutes.
	Router(config)# end	Ends the configuration session and returns to privileged EXEC mode

To display the statistics from the NetFlow data export, including statistics for the main cache and all other enabled caches, use the ***show ip flow export*** command in user EXEC or privileged EXEC mode. The following is sample output from the ***show ip flow export*** command:

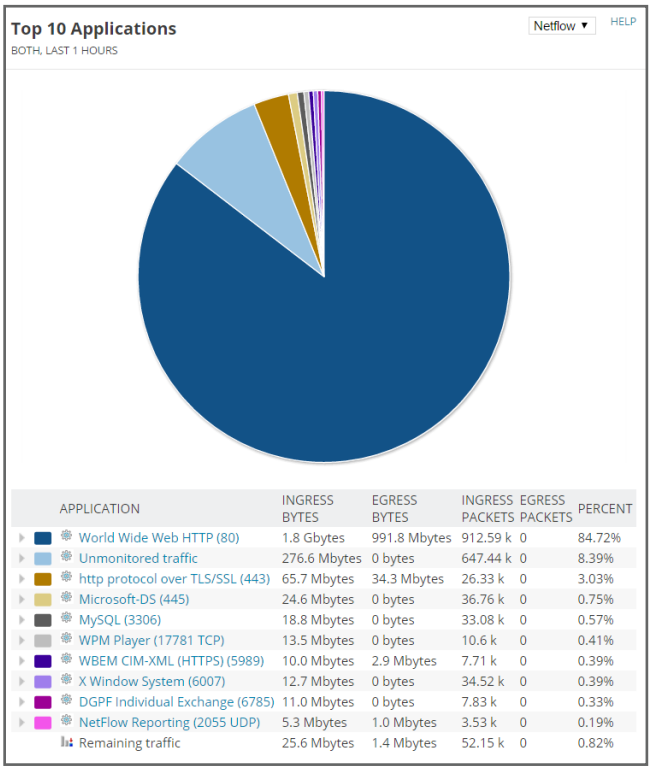
```
Router# show ip flow export

Flow export is enabled
Exporting flows to 10.42.42.1 (9991) 10.0.101.254 (9991)
   Exporting using source IP address 10.0.101.203
   Version 5 flow records
Export Stats for 10.42.42.1 (9991)
           3 flows exported in 3 udp datagrams
           0 flows failed due to lack of export packet
           3 export packets were sent up to process level
           0 export packets were dropped due to no fib
           0 export packets were dropped due to adjacency issues
           0 export packets were dropped enqueuing for the RP
           0 export packets were dropped due to IPC rate limiting
Export Stats for 10.0.101.254 (9991)
           7 flows exported in 7 udp datagrams
           0 flows failed due to lack of export packet
           6 export packets were sent up to process level
           0 export packets were dropped due to no fib
           0 export packets were dropped due to adjacency issues
           0 export packets were dropped enqueuing for the RP
           0 export packets were dropped due to IPC rate limiting
```

There are a number of commercially available flow analysis and bandwidth monitor products that greatly simplify the process of enabling NetFlow and displaying the raw numbers into easy-to-interpret charts and tables.

Let's take a look at three particular use cases for using flow analysis for troubleshooting bandwidth and traffic.

Applications

When an application on the network begins consuming more than its fair share of network bandwidth, its use will impact the capacity available for other network services. The problem with identifying these incidents using other types of network tools is that reporting problems tends to draw focus to the network service being impacted. For example, when the problem occurs, the network administrator is usually alerted to the fact that Application B "is slow today." The job is then theirs to determine why the service is slow and what is impacting performance. Using effective flow analysis tools, the administrator can easily view the traffic and usage patterns across the entire network to identify that Application A is actually the culprit. Conversely, using tools with a closer perspective may incorrectly focus the administrator's troubleshooting on Application B, while ignoring the impact of Application A.



APPLICATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
World Wide Web HTTP (80)	1.8 Gbytes	991.8 Mbytes	912.59 k	0	84.72%
Unmonitored traffic	276.6 Mbytes	0 bytes	647.44 k	0	8.39%
http protocol over TLS/SSL (443)	65.7 Mbytes	34.3 Mbytes	26.33 k	0	3.03%
Microsoft-DS (445)	24.6 Mbytes	0 bytes	36.76 k	0	0.75%
MySQL (3306)	18.8 Mbytes	0 bytes	33.08 k	0	0.57%
WPM Player (17781 TCP)	13.5 Mbytes	0 bytes	10.6 k	0	0.41%
WBEM CIM-XML (HTTPS) (5989)	10.0 Mbytes	2.9 Mbytes	7.71 k	0	0.39%
X Window System (6007)	12.7 Mbytes	0 bytes	34.52 k	0	0.39%
DGPF Individual Exchange (6785)	11.0 Mbytes	0 bytes	7.83 k	0	0.33%
NetFlow Reporting (2055 UDP)	5.3 Mbytes	1.0 Mbytes	3.53 k	0	0.19%
Remaining traffic	25.6 Mbytes	1.4 Mbytes	52.15 k	0	0.82%

Figure 4: SolarWinds NetFlow Traffic Analyzer Top 10 Applications Resource

Protocols

A second and similar issue occurs when a specific protocol overconsumes network resources. Streaming protocols are an excellent example of this type of constant and predictable network flow. When users on a network make use of streaming applications, their consumption typically occurs at a constant level over an extended period of time. Different than transaction-based protocols, streaming protocols have the tendency to saturate available network resources due to the additive effect of multiple streams. One user making use of one stream may not be likely to cause a network problem, but 50 or 100 users employing an equal number of streams quickly begins saturating the network. Unlike packet-based tools that analyze individual pieces as they go by, flow analysis tools enable the identification of the source, destination, and protocol of streams across the network. The end result is the ability to craft effective network policies that enable streaming protocols where necessary, while preventing those that negatively impact the functionality of the network.

Top Talkers

A final area for which flow analysis tools are particularly well suited is identifying top talkers. The Top Talkers feature of NetFlow can be useful for analyzing and troubleshooting network traffic in any one of the following ways: Security by viewing a list of the top talkers to see if traffic patterns are consistent with Denial of Service (DoS) attacks; load-balancing through the identification of the most heavily used parts of your network, and general traffic study and planning for your network.

TROUBLESHOOTING CONFIGURATION ISSUES

One of the first questions network administrators should ask themselves when troubleshooting is, "Did something on my network change?" More than 80% of network issues are the result of device configuration errors, many of which were unplanned, unauthorized, or not fully tested prior to deployment.

Hopefully you have been keeping an archive of your device configurations so you can compare the current version to the previously archived versions. If you haven't been, then you need to start immediately.

For a Cisco router, the ***archive config*** command allows you to save your IOS configuration in the configuration archive using a standard location and filename prefix that is automatically appended with an incremental version number as each consecutive file is saved.

```
Router# configure terminal
Router(config)# archive
Router(config-archive)# path disk0:myconfig
```

You save the current running configuration in the configuration archive as follows:

```
Router# archive config
```

The **show archive** command displays information on the files saved in the configuration archive as shown in the following sample output:

```
Router# show archive

There are currently 1 archive configurations saved.
The next archive file will be named disk0:myconfig-2
 Archive #  Name
   0
   1       disk0:myconfig-1 <- Most Recent
   2
```

Assuming that you have a config archive, you can perform a line-by-line comparison of any two configuration files and generate a list of the differences between them using the ***show archive config differences*** command.

```
show archive config differences[filename1(path)[filename2(path)][ignorecase]]
```

The output will display the results of the diff operation performed on the configuration files. A plus symbol (+) indicates that the configuration line exists in filename2(path), but not in filename1(path, while a minus symbol (-) indicates that the configuration line exists in filename1(path). but not in filename2(path). An exclamation point (!) with descriptive comments is used to identify order-sensitive configuration lines whose location is different in filename1(path) than in filename2(path).

```
+ip subnet-zero
+ip name-server 10.4.4.4
+voice dnis-map 1
 +dnis 111
interface Ethernet1/0
 +no ip address
 +shutdown
+ip default-gateway 10.5.5.5
+ip classless
+access-list 110 deny ip any host 10.1.1.1
+access-list 110 deny ip any host 10.1.1.2
+access-list 110 deny ip any host 10.1.1.3
+snmp-server community private RW
-no ip subnet-zero
interface Ethernet1/0
 -ip address 10.7.7.7 255.0.0.0
-no ip classless
-snmp-server community public RO
```

Instead of relying on a cumbersome and hard-to- decipher CLI troubleshooting process, the network administrator may want to consider one of the many commercially available network change and configuration management tools that will automate and simplify the process of managing device configurations.

Once you determine that a config has changed, you can replace the current running config with any saved config file using the **configure replace** command. This functionality can be used to revert to a previous configuration state, effectively rolling back any configuration changes that were made since the previous configuration state was saved.

```
Router# configure replace disk0:myconfig

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y

Total number of passes: 1

Rollback Done
```

Figure 6: SolarWinds Network Configuration Manager Compare Configs

TROUBLESHOOTING IP ADDRESS CONFLICTS

IP address conflicts occur when two devices on a network are assigned the same IP address resulting in one or both being disabled and losing connectivity until the conflict is resolved. IP address conflicts are almost always the result of configuration errors, including assignment of the same static IP address by a network administrator, assignment of a static IP address within the DHCP range (dynamic range) resulting in the same address being automatically assigned by the local DHCP server, an error in the DHCP server, or a system coming back online after an extended period in stand-by or hibernate mode with an IP address that has been re-assigned and is in use on the network.

Here are a number of steps that you can take to troubleshoot this pesky problem.

Step 1 – Look For Overlapping IP Address Ranges on Your DHCP Server

If you are using multiple DHCP servers, you will first want to verify that no two servers have overlapping IP address ranges. This can be as simple as comparing the IP address ranges and looking for overlaps when the servers are using dynamic or automatic allocation of IP addresses. If they are using static allocation, then you will need to review each hard-coded IP address assignment.

Step 2 – Look for Duplicate Static IP Addresses

Look for devices on the network segment that have been statically configured with the duplicate IP address. Once found, you can either reconfigure the device to use DHCP or you can configure the DHCP server to stop assigning the duplicated IP address.

Step 3 – Find the Conflicting MAC Addresses

If steps 1 and 2 do not produce results, you will need to find the MAC addresses of the conflicting devices. Since the MAC address is unique for each device on the network, you can look for devices that contain the same IP address but with different MAC addresses. You can use the Address Resolution Protocol (ARP) to establish a correspondence between the IP address and the MAC address. Start at your core router and use the ***show ip arp*** command:

```
Router# show ip arp

Protocol  Address          Age(min)  Hardware Addr   Type   Interface
Internet  172.16.233.229        -   0000.0c59.f892  ARPA   Ethernet0/0
Internet  172.16.233.218        -   0000.0c07.ac00  ARPA   Ethernet0/0
Internet  172.16.233.19         -   0000.0c63.1300  ARPA   Ethernet0/0
Internet  172.16.233.309        -   0000.0c36.6965  ARPA   Ethernet0/0
Internet  172.16.168.11         -   0000.0c63.1300  ARPA   Ethernet0/0
Internet  172.16.168.254        9   0000.0c36.6965  ARPA   Ethernet0/0
```

If you were to see two IP addresses with differing hardware addresses, you have located your problem devices.

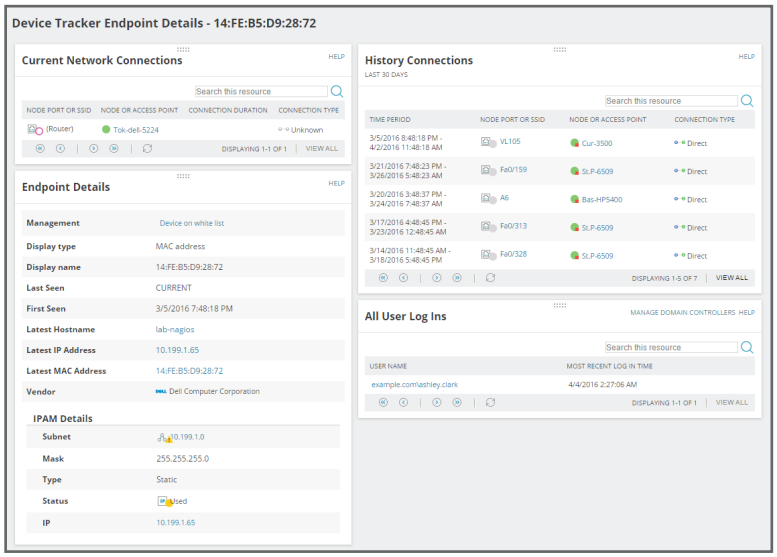
Step 4 - Trace the Location of the Device

Perhaps you want to know the physical location of at least the switch port that the offending devices are connected to. One way is to go to the switch and use the ***show mac-address table*** command. This will show you the MAC address for each port.

```
switch# show mac-address-table
          Mac Address Table
 -------------------------------------------

 Vlan    Mac Address       Type        Ports
 ----    -----------       --------    -----
    1    0007.e9e2.2d7d    DYNAMIC     Fa0/5
    1    0009.0f30.07e9    DYNAMIC     Fa0/48
    1    0009.5bbc.af04    DYNAMIC     Fa0/28
    1    00e0.bb2c.30d1    DYNAMIC     Gi0/1
    1    00e0.bb2c.3e5f    DYNAMIC     Gi0/1
 Total Mac Addresses for this criterion: 5

 Switch#
```

Unfortunately, you need to run this command from each switch and, if the network is down, you will have to go to the console of each switch. This can be very tedious and time-consuming, not to mention logistically challenging in the case of geographically distributed networks.

Another alternative is to use commercially available switch port management tools that will automatically trace the location of a device on a network. SolarWinds User Device Tracker is a device tracking and switch port management tool that quickly locates a device on the network by searching on the IP address, host name, or MAC address.



DOWNLOAD FREE TRIAL

Preventing Conflicts in the Future

Once you have identified and corrected IP address conflicts, here are some tips to prevent future conflicts:

- Use DHCP to reduce the chances of manually assigning duplicate addresses.
- Set your DHCP server to detect IP address conflicts.
- Modify the DHCP lease duration to something less than the default lease time of eight days.
- Use multiple DHCP servers, each having its own specific scope.
- Reserve IP addresses instead of assigning static IP addresses.
- Use automated DHCP, DNS, and IP address management and monitoring tools.

Even by following these tips, there still remains the possibility that IP conflicts will occur. I would encourage you to evaluate a commercially available IP address management product that allows you to centrally manage, monitor, alert, and report on your IP infrastructure. By proactively managing and monitoring your IP address space, you can significantly reduce the chances of IP address conflicts.

NETWORK TROUBLESHOOTING STEPS

There are literally hundreds of network troubleshooting flow charts available on the internet today. That's great, but even with flow charts, successful troubleshooting relies on logic, methodology, and following these basic steps:

1. Identify and document the symptoms.
2. Identify the scope (geographic, demographic, or chronologic) of the problem.
3. Determine if anything has changed on the network. Has there been a hardware or software change?
4. Determine the most probable cause of the problem. (No, it's not always the end-user.)
5. Implement a solution.
6. Test the solution.
7. Document the solution.

And while not specifically called out in these steps, it is important to remember to pay attention to the obvious and don't discount the simple questions. To put it bluntly, don't forget to check the cables.

TOOLS FOR NETWORK TROUBLESHOOTING

As we have shown, there are hundreds of open source, free, or commercially licensed products available to monitor and troubleshoot network performance, traffic, bandwidth, configurations, and IP infrastructure. Below are some guidelines on picking the right tool for your needs.

- Multiple vendor device support – It would be very difficult in this day and age to find a network that consists of equipment from a single vendor. While all vendors provide some type of tool or utility that will manage and monitor their own equipment, it is critical that you look for a tool that allows you to monitor all of your different vendors in a single pane of glass.
- Support for multiple standard protocols, including SNMP, ICMP, and syslog for network management; RDP, WMI, and WS for Windows® management; and NetFlow, J-Flow, sFlow, IPFIX, and NetStream for flow-based traffic monitoring.
- Real-time and historical analysis capabilities. Although most problems in network administration directly relate to how the network operates right now, the only effective way to ascertain today's behaviors is to view them in comparison with yesterday's or last week's.
- Visualizations accessible from anywhere. As a network administrator, you're not always sitting in your office. Problems and issues tend to pop up all across the network, some of which require on-site support. In these cases, having visualizations that can be accessed from anywhere, for example, using a standard web browser, gives you the ability to take your toolset to wherever the problem exists.
- Drill-down support. With drill-down support, it is possible to quickly move from the highest-level view down into specific problems as needed. Drill-down support reduces on-screen clutter, enabling a single-glimpse and high-level view during periods of nominal activity.

- Affordability. Any toolset used in troubleshooting and resolving issues must cost less than the amount of benefit it provides. Expensive solutions take longer to pay for themselves and may be more difficult to obtain in a time of shrinking IT budgets. Finding the tool that meets your needs at an acceptable cost is important to gaining the biggest return on your investment.

HOW SOLARWINDS CAN HELP

SolarWinds' award-winning network management software makes it easy to discover and map network devices, monitor network performance, analyze network traffic, manage and back up network configurations, track IP addresses, find rogue devices, and much more.

SolarWinds Network Performance Monitor

SolarWinds Network Performance Monitor (NPM) makes it easy to quickly detect, diagnose, and resolve performance issues. It delivers real-time views and dashboards that enable you to visually track network performance at a glance. Plus, using dynamic network topology maps and automated network discovery, you can deploy and keep up with your evolving network.

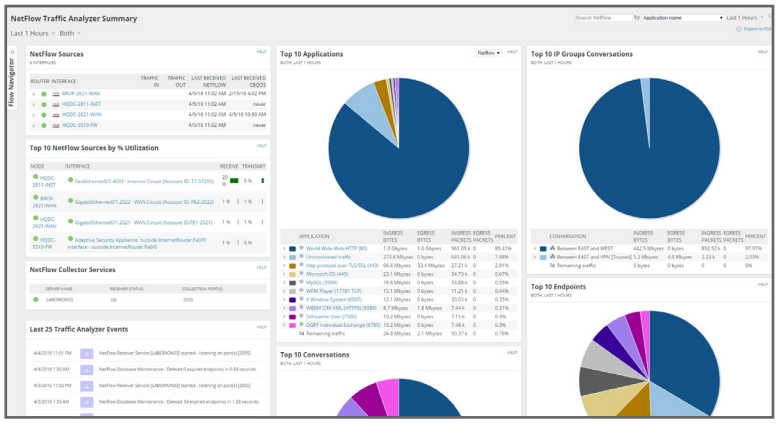
- Simplifies detection, diagnosis, and resolution of network issues, before outages occur
- Provides critical path hop-by-hop analysis for on-premises, cloud, and hybrid networks, apps, and services
- Tracks response time, availability, and uptime of routers, switches, and other SNMP-enabled devices
- Shows performance statistics in real-time via dynamic, drillable network maps
- Includes out-of-the-box dashboards, alerts, reports, and expert guidance on what to monitor and how
- Automatically discovers SNMP-enabled network devices and typically deploys in less than an hour

DOWNLOAD FREE TRIAL

SolarWinds NetFlow Traffic Analyzer

SolarWinds NetFlow Traffic Analyzer (NTA) enables you to capture data from continuous streams of network traffic and convert those raw numbers into easy-to-interpret charts and tables that quantify exactly how the corporate network is being used, by whom, and for what purpose.

- Monitors network bandwidth and traffic patterns down to the interface level
- Identifies which users, applications, and protocols are consuming the most bandwidth
- Highlights the IP addresses of top talkers
- Analyzes Cisco NetFlow, Juniper J-Flow, IPFIX, sFlow, and NetStream.



DOWNLOAD FREE TRIAL

SolarWinds Network Configuration Manager

SolarWinds Network Configuration Manager (NCM) keeps you ahead of network issues with immediate visibility into the cause and effect relationship between configuration errors and network performance. Plus, you can rest easy and save time with features, such as nightly config backups, bulk config changes, user tracking, and inventory and compliance reporting.

- Enables bulk configuration, community string, ACL, and MAC address changes
- Automates network configuration backups and compliance reporting
- Detects and reports on configuration policy violations and delivers real-time alerts
- Protects against unauthorized, unscheduled, or erroneous config changes
- Automatically discovers SNMP-enabled network devices and typically deploys in less than an hour

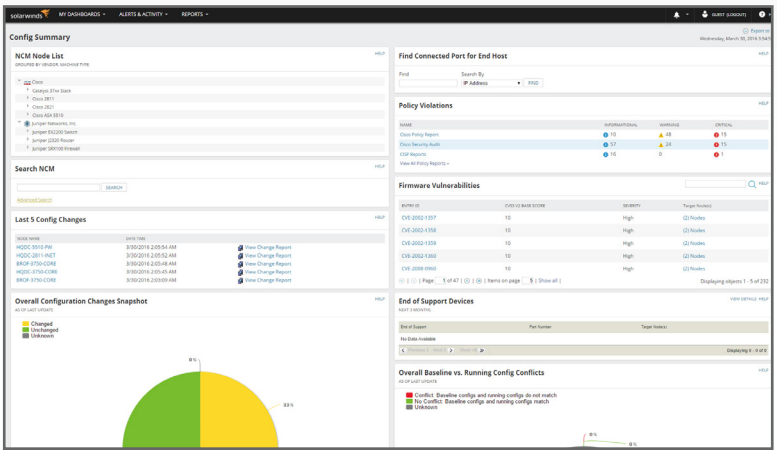


Figure 9: SolarWinds Network Configuration Manager Summary Page

DOWNLOAD FREE TRIAL

SolarWinds IP Address Manager

SolarWinds IP Address Manager (IPAM) enables you and your team to ditch your spreadsheets for an easy-to-use, centralized IP address monitoring and management solution. Now it's easier than ever to manage Microsoft® DHCP services, monitor Microsoft DNS and Cisco DHCP servers, and manage your IP address space, all from an intuitive, centralized web console.

- Centrally manage, alert, and report on your IP address space
- Manage and monitor Microsoft DHCP/DNS services, and monitor Cisco DHCP servers
- Deliver role-based access and control from an intuitive web-based interface
- Alert notifications help prevent your subnets and DHCP scopes from filling up
- Automatically discovers used and unused addresses, and typically deploys in less than an hour

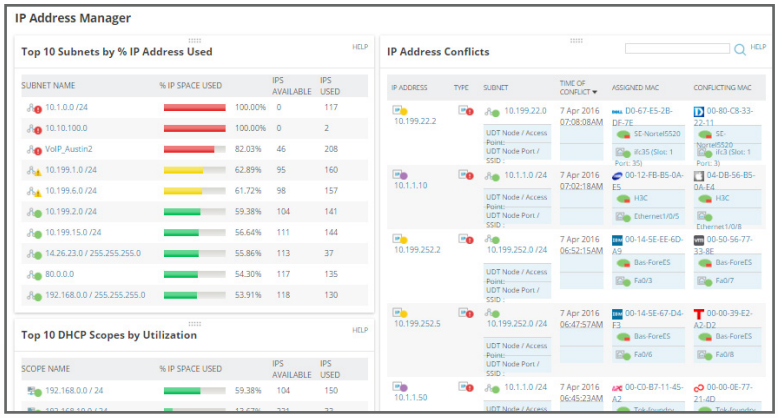


Figure 10: SolarWinds IP Address Manager Summary Page

DOWNLOAD FREE TRIAL

SolarWinds User Device Tracker

SolarWinds User Device Tracker enables you to quickly find devices on your network, create device watch lists, map switch ports, and track switch capacity.

» Track user and device locations by MAC address, IP address, or host name

» Map and monitor switches by ports used, CPU load, memory used, and more

» Receive immediate alerts when a specified device connects to the network

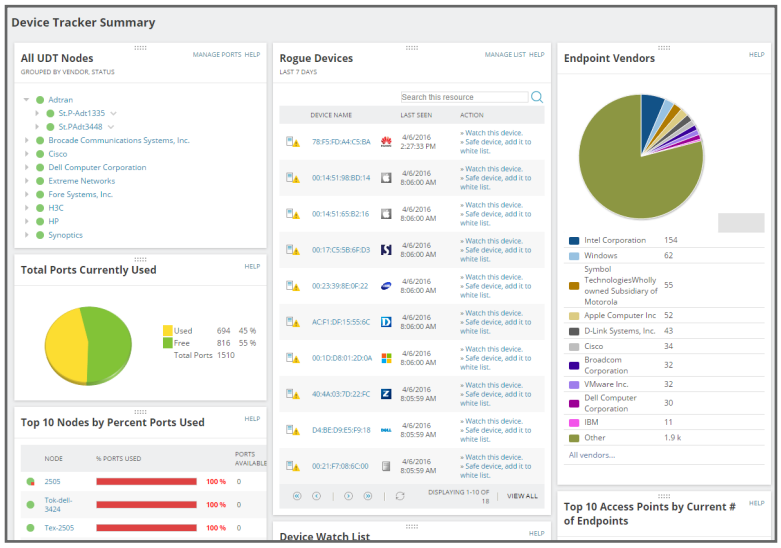


Figure 11: SolarWinds User Device Tracker Summary Page

DOWNLOAD FREE TRIAL

ABOUT SOLARWINDS

SolarWinds provides powerful and affordable IT management software to customers worldwide from Fortune 500® enterprises to small businesses, government agencies and educational institutions. We are committed to focusing exclusively on IT Pros, and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or user sits, SolarWinds delivers products that are easy to find, buy, use, maintain, and scale while providing the power to address all key areas of the infrastructure from on premises to the Cloud. Our solutions are rooted in our deep connection to our user base, which interacts in our THWACK® online community to solve problems, share technology and best practices, and participate in our product development process. Learn more today at http://www.solarwinds.com/.