



Network Management – Back to the Basics

Brad Hale

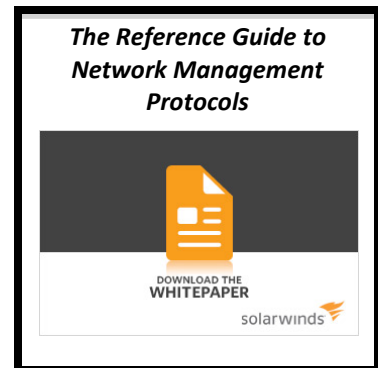
Table of Contents

The Fundamental Protocols of Network Management	3
Simple Network Management Protocol (SNMP)	4
Management Information Base (MIB)	6
Telnet	6
SSH	7
Syslog	7
Windows Management Protocols	8
Remote Desktop Protocol (RDP)	8
Windows Management Instrumentation (WMI)	9
WS-Management	9
Flow Based Protocols.....	9
NetFlow, J-Flow, sFLOW, IPFIX, and NetStream	10
Cisco IP Service Level Agreements	12
FCAPS	12
ITIL (Information Technology Infrastructure Library)	12
Selecting a Network Management System	13
Simple Interface	13
Multi-Vendor Capability	13
Real-time Agentless Monitoring.....	13
Intelligent Alerting	14
Reporting.....	14
Extensibility & Scalability.....	14
SolarWinds Network Performance Monitor (NPM)	14

Addressing IT infrastructure and related issues is easier if we understand networking basics and keep them in mind while choosing the best means for addressing issues. Network engineers, system admins, IT managers, and all IT infrastructure management professionals can treat this as a refresher on the topic. Let's start with some of the fundamentals and concepts of network management.

The Fundamental Protocols of Network Management

Starting with the basics are the two fundamental protocols of network management, Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP). Having been in service for nearly as long as the earliest networks, these two protocols remain useful as core tools for troubleshooting and managing your network. Most commonly known through its "ping" command, ICMP creates a low-level request and response that ensures core connectivity between two network endpoints. SNMP goes a step further. It elevates that level of gathered data by enabling devices to share their basic configuration and onboard metrics.



Internet Control Message Protocol (ICMP)

One of the core Internet protocols in network management and administration, ICMP is used to send error messages. ICMP is a control protocol, meaning that it does not carry application data, but rather information about the status of the network itself. There are many commonly used network utilities based on ICMP messages that will help detect errors in the underlying communications of network applications; availability (up/down status) of remote hosts; network congestion; and latency.

One of the common ICMP utilities, **Ping** sends ICMP echo request packets and tests the reachability or availability of a device or host on a network. Ping also measures the round-trip time for messages sent between the originating host and the destination. Ping is lightweight (small packets = fast results), low level (Typically handled by the NIC), very flexible, and has a near zero impact on the network.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\geek>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128
Reply from 192.168.1.200: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\geek>
```

Figure 1: Ping Test Result

Although the result from a ping command provides information about a network route’s latency, this information is exceptionally coarse in its granularity. Latency as defined by a ping response represents little more than the amount of time that occurred between sending the ping request and receiving its reply. As such, its response illuminates little about the actual route taken and behaviors seen through its journey from source to target.

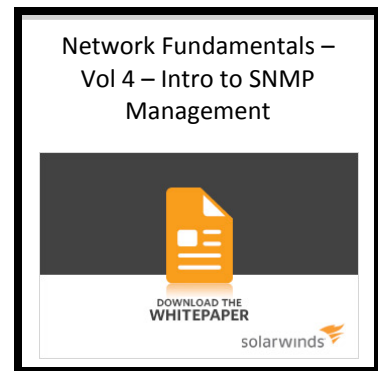
A ping response will also report on the number of hops required to complete the travel from source to destination as well as information about the connection’s packet loss.

Although the specifics of a problem are left to other more granular protocols, this simple command provides a very easy way to gauge a connection’s health at the highest level.

Simple Network Management Protocol (SNMP)

SNMP goes beyond ICMP’s very simple and highly-structured information to enable the gathering of virtually any kind of data from a network device. Due to SNMP’s long history and widespread use, virtually every network device—and even many servers and applications—have been made SNMP-aware. “Awareness” in this context means that the device is configured to receive and respond to SNMP requests from a central Network Management Solution (NMS).

SNMP works by polling the MIB (Management Information Base) of an SNMP enabled device to obtain information stored on the target device.



No.	Time	Source	Destination	Protocol	Info
167	6.231911	10.110.66.124	10.110.66.69	SNMP	get-request SNMPv2-MIB::sysuptime.0
168	6.232183	10.110.66.69	10.110.66.124	SNMP	get-response SNMPv2-MIB::sysuptime.0

```

Frame 167 (83 bytes on wire (83 bytes captured) on interface 0)
  Ethernet II, Src: Vmware_3e:6f:d0 (00:0c:29:3e:6f:d0), Dst: Dell_12:4c:65 (00:1a:a0:12:4c:65)
  Internet Protocol, Src: 10.110.66.124 (10.110.66.124), Dst: 10.110.66.69 (10.110.66.69)
  User Datagram Protocol, Src Port: mdap-port (3235), Dst Port: snmp (161)
  Simple Network Management Protocol
    version: v2c (1)
    community: public
    data: get-request (0)
      get-request (0)
        request-id: 9395
        error-status: noError (0)
        error-index: 0
        variable-bindings: 1 item
          SNMPv2-MIB::sysuptime.0 (1.3.6.1.2.1.1.3.0): unspecified
            Object Name: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysuptime.0)
            Scalar Instance Index: 0
  
```

Figure 2: SNMP Request Sent

No.	Time	Source	Destination	Protocol	Info
167	6.231911	10.110.66.124	10.110.66.69	SNMP	get-request SNMPv2-MIB::sysUpTime.0
168	6.232163	10.110.66.69	10.110.66.124	SNMP	get-response SNMPv2-MIB::sysUpTime.0

```

Frame 168 (87 bytes on wire, 87 bytes captured)
  Ethernet II, Src: Dell_12:4c:65 (00:1a:a0:12:4c:65), Dst: vmware_3e:6f:d0 (00:0c:29:3e:6f:d0)
  Internet Protocol, Src: 10.110.66.69 (10.110.66.69), Dst: 10.110.66.124 (10.110.66.124)
  User Datagram Protocol, Src Port: snmp (161), Dst Port: mdap-port (3235)
  Simple Network Management Protocol
    version: v2c (1)
    community: public
    data: get-response (2)
      get-response
        request-id: 9395
        error-status: noError (0)
        error-index: 0
        variable-bindings: 1 item
          SNMPv2-MIB::sysUpTime.0 (1.3.6.1.2.1.1.3.0): 12037748
            object Name: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
              Scalar Instance Index: 0
              SNMPv2-MIB::sysUpTime: 12037748
  
```

Figure 3: SNMP Reply Obtained

An **SNMP trap** allows a network device to notify a network management system (NMS) of an event through an SNMP message. SNMP traps differ from SNMP queries in that the device initiates the trap while the query is initiated by the NMS.

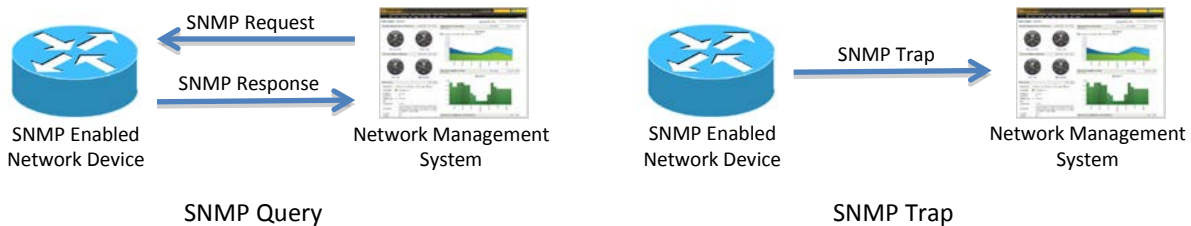


Figure 4: SNMP Query vs. SNMP Trap

Comparing both SNMP and ICMP comes down to addressing the requirement on the type of information that is to be polled. If it's only availability or status information, then ICMP ping can be effective. If more

specific device performance data is required for monitoring, then only SNMP can be used to query the device to get what's needed.

ICMP	SNMP
<ul style="list-style-type: none"> Device availability obtained by ping from the source/server across the network 	<ul style="list-style-type: none"> Obtains data from the network device directly by querying the device on its performance and retrieving results

Management Information Base (MIB)

A MIB is the collection of management information available on a network device and contains Object Identifiers (OIDs). Each OID identifies a variable that can be read or set via SNMP. A MIB is a kind of a virtual database that can be queried using SNMP to retrieve device information, and the OID is the location of the specific data.

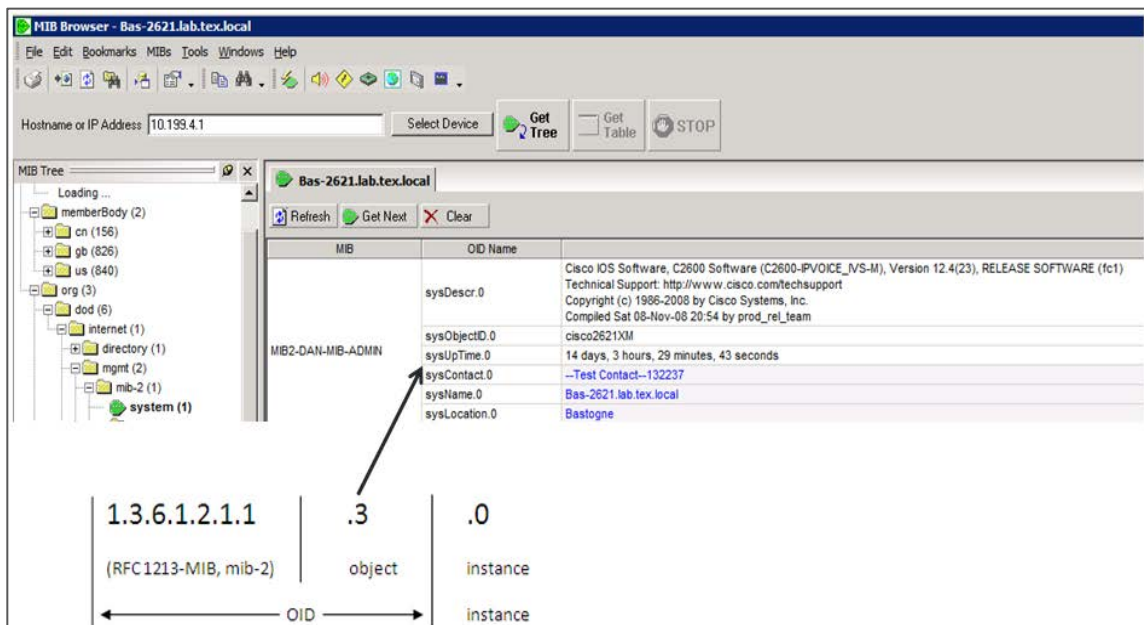


Figure 5: MIB Structure

Telnet

Telnet is considered one of the oldest protocols still in common use today. Today's use of the telnet command is primarily as a mechanism for accessing a UNIX or Linux system's command-line interface. In networking domains, telnet is also commonly used for connecting to a network device's command-line management interface. Telnet functionally operates as both a management protocol and a data transfer protocol.

Today's use of telnet has fallen out of common practice for many business networks due to its inherent incapability to authenticate target servers. Telnet also lacks key encryption capabilities that ensure its data is secure in transit. The combination of these limitations means that telnet and "telnetting" to a server or device is no longer a security best practice. Replacing the telnet command is the ssh command, discussed in the next section, which includes the necessary capabilities for connection security.

SSH

The ssh or "secure shell" command has in most environments superseded telnet as the best practice for connecting to remote servers and desktops. From the perspective of the user, ssh's most basic functionality performs essentially the same function as telnet—it opens a connection to the command-line interface on an identified remote server. Where ssh differs is in how it secures that connection from end to end.

The actual use of ssh differs from telnet in that ssh can be a platform upon which additional functionality can be hosted. In addition to creating a secure connection to a command-line interface, the ssh protocol can be leveraged for many uses:

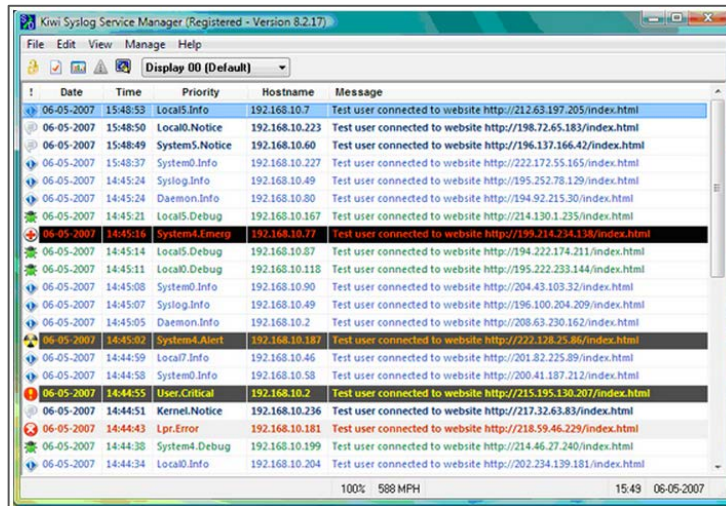
- Single-line command execution
- File transfer, manifested as SCP, SFTP, or rsync
- Port forwarding or tunneling
- Creation of VPN connections, enabled through the OpenSSH distribution
- Web browsing via the SOCKS protocol
- Remote directory mounting, manifested as SSHFS

In short, although most network devices retain the capability to use telnet for remote management, it is considered the industry best practice to use ssh. Although ssh is not natively available in the Microsoft Windows OS in any edition, clients for ssh are available as installed applications to accomplish necessary management.

Syslog

Syslog is a logging standard for error messages, warning messages, and/or other system messages that are sent to the NMS from network devices such as switches, routers and firewalls. Some benefits of syslog include: they are event-driven; they offer automated analysis of events from disparate sources; they can be used for incident response; they are useful for compliance verification.





Date	Time	Priority	Hostname	Message
06-05-2007	15:48:53	Local5.Info	192.168.10.7	Test user connected to website http://212.63.197.205/index.html
06-05-2007	15:48:50	Local0.Notice	192.168.10.223	Test user connected to website http://198.72.65.183/index.html
06-05-2007	15:48:49	System5.Notice	192.168.10.60	Test user connected to website http://196.137.166.42/index.html
06-05-2007	15:48:37	System0.Info	192.168.10.227	Test user connected to website http://222.172.55.165/index.html
06-05-2007	14:45:24	Syslog.Info	192.168.10.49	Test user connected to website http://195.252.78.129/index.html
06-05-2007	14:45:24	Daemon.Info	192.168.10.80	Test user connected to website http://194.92.215.30/index.html
06-05-2007	14:45:21	Local5.Debug	192.168.10.167	Test user connected to website http://214.130.1.235/index.html
06-05-2007	14:45:18	System4.Emerg	192.168.10.77	Test user connected to website http://199.214.234.138/index.html
06-05-2007	14:45:14	Local5.Debug	192.168.10.87	Test user connected to website http://194.222.174.211/index.html
06-05-2007	14:45:11	Local0.Debug	192.168.10.118	Test user connected to website http://195.222.233.144/index.html
06-05-2007	14:45:08	System0.Info	192.168.10.90	Test user connected to website http://204.43.103.32/index.html
06-05-2007	14:45:07	Syslog.Info	192.168.10.49	Test user connected to website http://196.100.204.209/index.html
06-05-2007	14:45:05	Daemon.Info	192.168.10.2	Test user connected to website http://208.63.230.162/index.html
06-05-2007	14:45:02	System4.Alert	192.168.10.187	Test user connected to website http://222.128.25.86/index.html
06-05-2007	14:44:59	Local7.Info	192.168.10.46	Test user connected to website http://201.82.225.89/index.html
06-05-2007	14:44:58	System0.Info	192.168.10.58	Test user connected to website http://200.41.187.212/index.html
06-05-2007	14:44:55	User.Critical	192.168.10.2	Test user connected to website http://215.195.130.207/index.html
06-05-2007	14:44:51	Kernel.Notice	192.168.10.236	Test user connected to website http://217.32.63.83/index.html
06-05-2007	14:44:43	Lpr.Error	192.168.10.181	Test user connected to website http://218.59.46.229/index.html
06-05-2007	14:44:38	System4.Debug	192.168.10.199	Test user connected to website http://214.46.27.240/index.html
06-05-2007	14:44:34	Local0.Info	192.168.10.204	Test user connected to website http://202.234.139.181/index.html

Figure 6: Syslog Message Format

Windows Management Protocols

The successful monitoring and management of Windows-based systems requires more than standards-based protocols such as Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP). Also needed are Windows-specific protocols. These protocols exist high in the IP stack’s Application layer and by design rely on others below them for routing and switching support. These added protocols are used for applications such as DNS, the Web, FTP, and mail transfer among many others.

The Microsoft Windows Operating System (OS) leverages its own suite of protocols for communications between Windows servers and workstations. These protocols layer atop core TCP and UDP to enable server and service communication across an IP network. Two examples of these high-level protocols are the Remote Procedure Call (RPC) protocol used for Windows inter-process communications, and the Remote Desktop Protocol (RDP), which is used for transferring display and control information between a server and client.

Other protocols that are used by the Microsoft Windows OS include the Windows Management Instrumentation (WMI) protocol as well as the more-recent implementation of WS-Management. WS-Management is manifested within the Microsoft Windows OS through its Windows Remote Management v1.1 and v2.0 implementations.

Remote Desktop Protocol (RDP)

Originally designed for specialized use in connecting remote users to applications on a centralized set of servers, use of RDP has grown to include administrative connections to server desktops. Unlike the more transaction-based protocols seen in SNMP, WMI, and others, RDP can be considered more like a “streaming” protocol, although this description is not completely accurate.

RDP's stream-driven nature enables it to pass updates across very low-bandwidth connections. Thus, high-use connections can remain in the data center, with only the resulting presentation data being submitted to the user. For certain applications, this is a boon to remote support. However, this same interactivity makes the protocol highly latency-insensitive. As a result, monitoring needs for RDP tend towards aggregate statistics over and above specific session details.

Windows Management Instrumentation (WMI)

RPC traffic in and of itself provides only a high-level representation of the overall communication flow. In its Windows OS, Microsoft has developed the WMI protocol as a proprietary alternative to SNMP. WMI operates much like SNMP in that WMI can be used for gathering metrics data and updating certain configurations. However, WMI is much different than SNMP in that WMI's reach is limited to the Windows OS and installed applications.

WS-Management

Microsoft adopted the industry-standard WS-Management framework in Windows Server 2008. Microsoft's implementation of WS-Management is represented with its Windows Remote Management (WinRM) service. This industry specification is based on DMTF open standards and Internet standards for Web Services. It leverages the firewall-friendly Simple Object Access Protocol (SOAP) for its exchange of information, extending the monitoring reach of WMI to many new areas.

As a Web Services implementation rather than relying on RPC, WS-Management (and thus WinRM) can much more easily pass WMI data over firewalled networks. It is important to recognize that Microsoft's implementation of WS-Management layers atop the traditional WMI/DCOM stack, enabling exposure to the stack through the structured Web Service. When enabled (as it is not enabled by default), this architecture retains the former WMI/DCOM compatibility with traditional WMI scripts and application infrastructures while adding the ability for SOAP-aware clients to interact with the server via a Web-friendly transport.

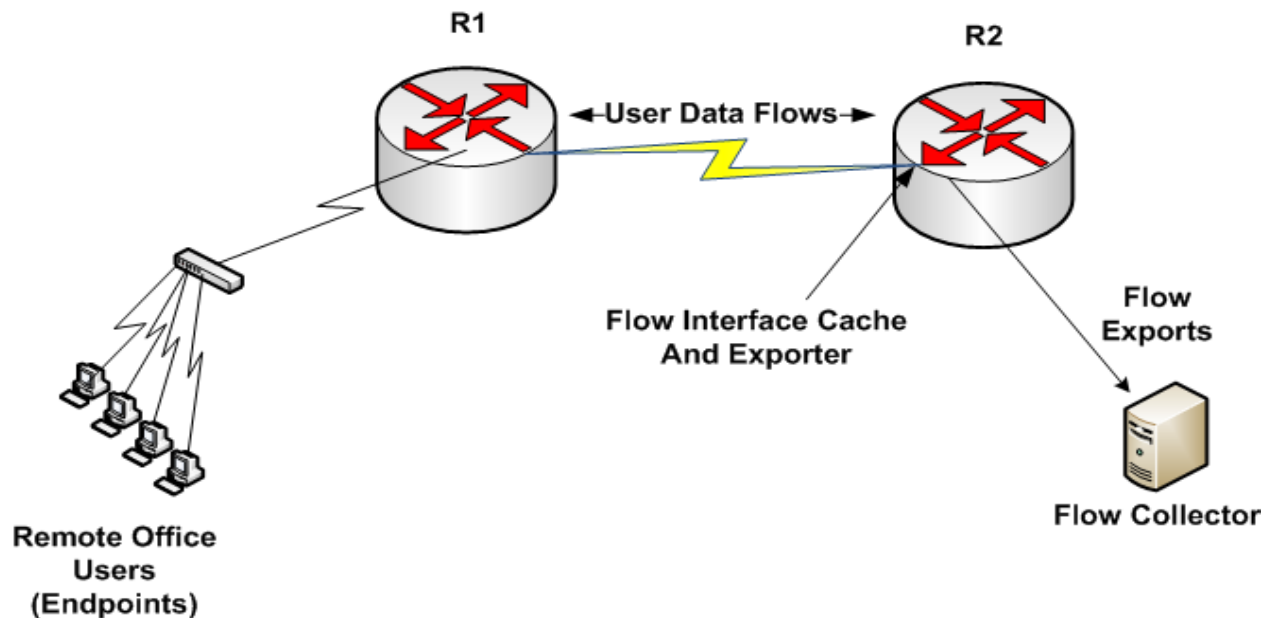
What this means to the average IT organization is that traditionally unmanageable systems—such as those in DMZs or on Extranets—can now be managed through WS- Management-enabled NMSs. In effect, the same types of information that can be gathered through WMI-based solutions can be now obtained in these systems that aren't on the LAN.

Flow Based Protocols

A network flow is a data entity that contains information related to the sequence of packet flows on an IP network. This is chiefly implemented in traffic and bandwidth monitoring solutions allowing network administrators to get a more granular picture of what's consuming their bandwidth and where the traffic is flowing.

Flow technologies can reveal key data such as who and what are consuming network traffic, where the traffic is coming from, and when traffic is being consumed. This can help in keeping a check on the network usage, implementation of network and IT security policies, and trending and QoS purposes.

Most major IT infrastructure vendors support the generation of network flows. Some widely-used flow technologies are Cisco NetFlow, Juniper J-Flow, IPFIX, sFlow, and Huawei NetStream.



NetFlow, J-Flow, sFLOW, IPFIX, and NetStream

Industry vernacular uses the term “NetFlow” generically, but the NetFlow protocol is actually a development of Cisco Systems. As such, any Cisco-based devices will use the NetFlow implementation of flow-based analysis. Four versions of Cisco’s NetFlow protocol remain in use today, with two rarely seen in today’s business networks:

- **NetFlow Version 5** — Originally developed by Cisco Systems but currently in use by other vendors
- **NetFlow Version 7** — Rarely seen today; specific to Cisco Catalyst switches
- **NetFlow Version 8** — Also rarely seen today, as it has been superseded by version 9; version 8 introduced aggregation technology
- **NetFlow Version 9** — Most common version in deployment today; includes mainstream availability of earlier-introduced aggregation features while introducing flexible NetFlow concepts

Although Cisco Systems is credited with developing the first implementation, other vendors have developed their own variants of the architecture for use within their hardware. These alternative implementations enable a similar set of operational functionality but with each supporting their own unique feature set. Three major examples include:

- **J-Flow** — Developed by Juniper Networks for use in their hardware; effectively the same as Cisco NetFlow Version 5
- **sFlow** — A standards-based implementation (RFC 3176) whose development is shared by HP, Extreme, Foundry, Juniper, and Nortel, sFlow is unique in that its measurements are based on a statistical sampling of flow data, which has the effect of reducing the total amount of data that is required to be sampled to achieve a statistically similar result
- **IPFIX** — Commonly considered the next version of NetFlow, or NetFlow Version 10, IPFIX is based on Cisco NetFlow Version 9; among other capabilities, IPFIX offers template-based exporting of data
- **NetStream** – Developed by Huawei for use in their hardware

As with the Simple Network Management Protocol (SNMP), the necessary code and processing to enable and use flow-based protocols is already included with virtually all network hardware available today. Thus, existing hardware components need only have NetFlow configured and enabled to begin enjoying its analysis capabilities.

For a Cisco IOS router, the configuration steps might resemble the following example: `router#enable`

```
Password:*****
router#configure terminal
router-1234(config)#interface FastEthernet 0/1
router-1234(config-if)#ip route-cache flow
router-1234(config-if)#exit
router-1234(config)#ip flow-export destination 192.168.1.100 9996
router-1234(config)#ip flow-export source FastEthernet 0/1
router-1234(config)#ip flow-export version 5
router-1234(config)#ip flow-cache timeout active 1
router-1234(config)#ip flow-cache timeout inactive 15
router-1234(config)#snmp-server ifindex persist
router-1234(config)#
router#write
```

These steps enable the export of flow information on the interface FastEthernet 0/1 to be directed to the server at 192.168.1.100 over port 9996. This configuration must be enabled for each of the interfaces on which flow information should be exported.

Obviously, configuring NetFlow information across the network devices and interfaces in your environment only accomplishes one-half of the setup. The level of information being gathered by a NetFlow-enabled interface is large and requires additional calculation by a server at the target endpoint if its data is to be useful to an administrator. Thus, the job of that server is in calculating the data, measuring it against other inbound flow information, and creating visualizations that display actionable information.

Cisco IP Service Level Agreements

IP SLA is a Cisco proprietary technology that is built into all Cisco network devices. IP SLA leverages the code built into Cisco IOS of network devices and allows you to measure transport metrics from one Cisco device to another, or even to other types of IP devices. This gives you the ability to measure performance from many different points in your network at the same time giving you a perspective from the standpoint of the device on the network performance. This can be really useful in a network that connects multiple geographies and needs to be monitored from one central location.

Network Management Framework

Network management is a very complex topic that would require multiple white papers to discuss in depth. With that caveat, however, there are two fundamental frameworks that exist that can be used as basic guidelines: FCAPS and ITIL.

FCAPS

The International Standards Organization (ISO) has defined a network management model and framework referred to as FCAPS (fault, configuration, accounting, performance, security).

- Fault Management – monitoring and management of faults that occur in a network
- Configuration Management – management of network device configurations and changes
- Accounting Management – billing management
- Performance Management – monitoring and management of the efficiency or utilization of the network
- Security Management – controlling access to the network and network devices

ITIL (Information Technology Infrastructure Library)

ITIL was designed to align itself with current IT organizational structures and expand upon the FCAPS model by providing a better framework to deliver high-quality, consistent application delivery over a network infrastructure. These practices include a framework for application, service, and security management.

- Service Support – ensure that applications are available to end users
- Service Delivery – how well the applications are being delivered to end users

- Security Management – ensure that unauthorized or unintended access of sensitive applications data is not obtained
- Infrastructure Management – change and configuration management
- Application Management – ensure that applications are enabled to provide service and delivery to end users
- Software Asset Management – software configuration management and accounting

Selecting a Network Management System

Network management systems range from free, open-source tools, to complex and pricey applications. Balancing the trade-offs between price, features, and user preference can be very challenging. Here are some key considerations that should help you create a short list of tools for evaluation.

Simple Interface

Whether you like to see your network data presented in a graphical or tabular format, everything you need to see should be easy to get to, should be customizable, and should be accessible by your entire team based on their access and roles. Look for a system with a web-based interface that provides out-of-the-box charts and graphs that can be customized and includes role-based access control.

Network Discovery

When you first install a network management system (NMS), you will need the ability to both discover all the devices on your network and map those devices and their connections. At a minimum, you will want to be able to map at layer 3, ideally you will want to map layer 2 and layer 3 so you can associate a MAC address with a specific switch port. In addition to discovering devices at the initial installation, you want the ability to automatically discover new devices as they are added to your network.

Multi-Vendor Capability

In today's network environment, it is virtually impossible to find a network that does not include devices from multiple vendors. While all device manufacturers offer some kind of utility or package that supports their devices, more often than not they do not support devices from other manufacturers. Make sure your NMS can support devices from multiple manufacturers.

Real-time Agentless Monitoring

You'll want the ability to continually collect and monitor data in real-time to pinpoint network issues and take proactive measures to prevent network outages. Systems that use standard network protocols such as SNMP, ICMP, and WMI typically do not require the installation of agents on your network devices or servers.

Intelligent Alerting

Network alerts are a checkbox for any modern NMS. Intelligent alerting goes one step beyond by including device dependencies, correlated events, sustained conditions, and multiple condition checks so you only get alerted for critical issues.

Reporting

Do you have a need to generate and distribute performance reports throughout your team or to management? Look for a system that provides customizable out-of-the-box reports that can be automated.

Extensibility & Scalability

It is likely that your NMS will be the foundation of your overall IT management system. As such, you should look for a modular system that can be extended across your infrastructure and include elements such as network traffic, network configuration, systems and applications, virtualization, and storage to name a few.

No doubt your infrastructure will also grow over time, therefore, you need to ensure that the system you choose can easily scale.

SolarWinds Network Performance Monitor (NPM)

[SolarWinds Network Performance Monitor \(NPM\)](#) makes it easy to quickly detect, diagnose, and resolve performance issues and 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, & resolution of network issues – before outages occur
- Tracks response time, availability, & uptime of routers, switches, & other SNMP-enabled devices
- Shows performance statistics in real time via dynamic, drillable network maps
- Includes out-of-the-box dashboards, alerts, reports, & expert guidance on what to monitor & how
- Automatically discovers SNMP-enabled network devices & typically deploys in less than an hour

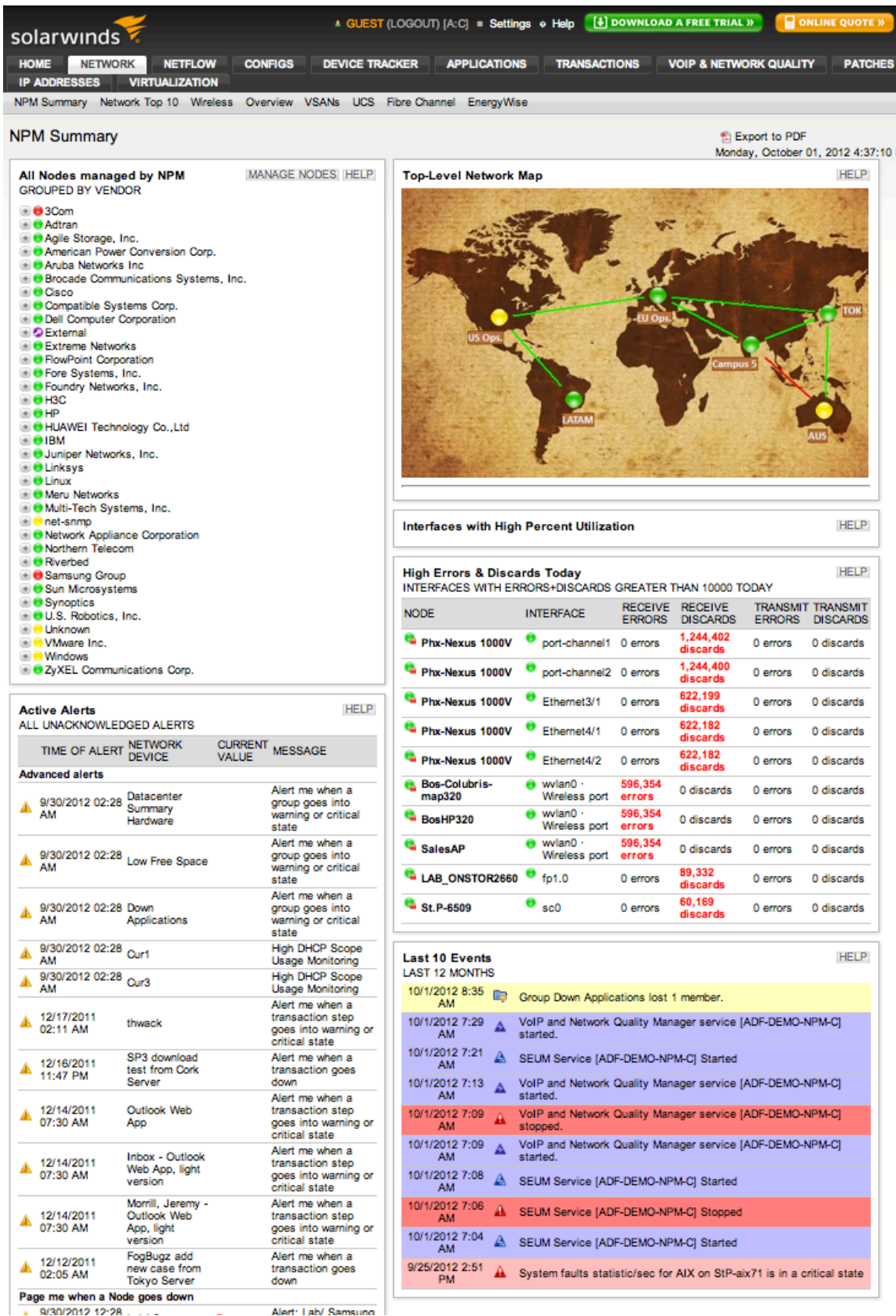


Figure 7: Network Performance Monitor's Summary Page

Additionally, NPM is the foundation of SolarWinds Network, Systems, and Applications management portfolio, and provides comprehensive IT management in a single pane of glass when integrated with the following SolarWinds products:

- [SolarWinds Network Configuration Manager](#) – Network change and configuration management
- [SolarWinds NetFlow Traffic Analyzer](#) – Network traffic and bandwidth management
- [SolarWinds Server & Application Monitor](#) – Server, application, and OS monitoring
- [SolarWinds IP Address Manager](#) – IP infrastructure management
- [SolarWinds VoIP & Network Quality Manager](#) – VoIP & WAN monitoring and troubleshooting
- [SolarWinds User Device Tracker](#) – Switch port monitoring and mapping
- [SolarWinds Virtualization Manager](#) – VMWare performance monitoring and capacity planning
- [SolarWinds Synthetic End User Monitor](#) – Web applications monitoring

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>.