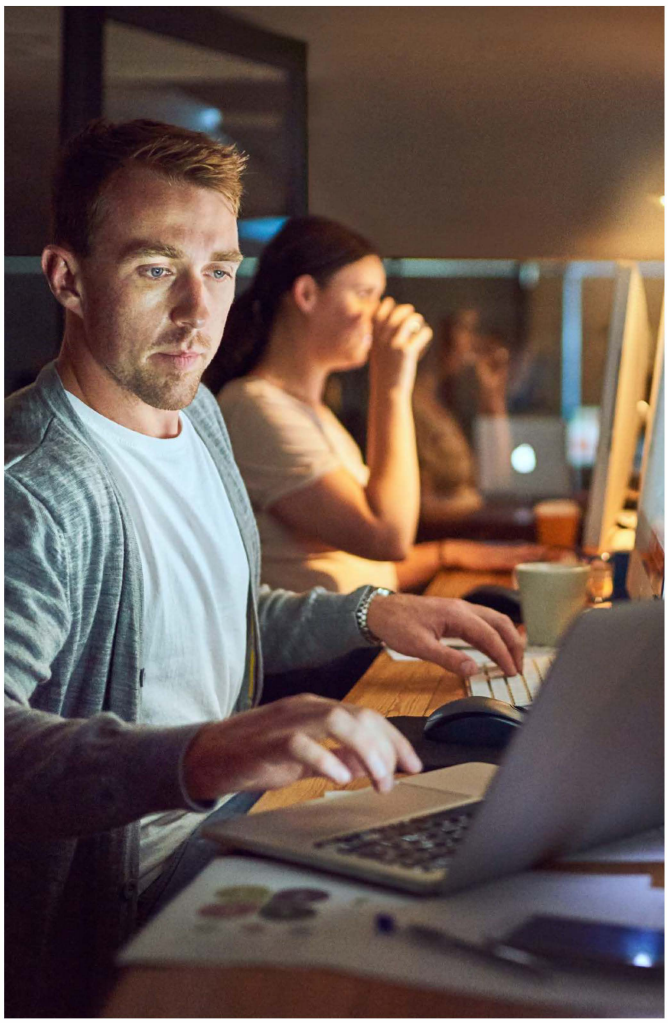
Network Monitoring with Opsview

Bring more of your IT estate under Opsview's single pane of glass

Automatically discover and visualize the topology of your network - improving knowledge, reducing misconfiguration and reducing security risks. Monitor your network devices for health, availability, and throughput with out-of-the-box SNMP capabilities. Gain insight into which applications and users are using your bandwidth, with Netflow, sFlow and jFlow support. Back up your current configuration and identify changes in your environment with NetAudit.

Monitor software-defined networks with a comprehensive Opspack for Cisco ACI (Application Centric Infrastructure).



Manage more of your IT estate with SNMP Monitoring

SNMP (Simple Network Management Protocol) is a communication protocol that lets you monitor managed network devices including Routers, Switches, Servers, Printers and other devices that are IP-enabled, all through a single management system/software.

With Opsview Monitor and Opsview Cloud, you can receive SNMP traps from any device, translate the traps using SNMP MIBs (Management Information Bases), apply rules using a 'rules engine' to determine whether to raise an alert and what the alert message should be.

SNMP polling is provided through quick-to-create checks which poll a single OID (Object Identifier) given either the OID as a number, or the name based on a MIB. This includes 'SNMPwalk' functionality where Opsview scans the device and returns the SNMP data for the user to select which OID they want to poll as part of the check.

This allows users to add their own SNMP monitoring of simple devices such as temperature sensors, fan speeds, and so on, without the need to write any code or use the command line.

Add the Network Analyzer to your monitoring capabilities

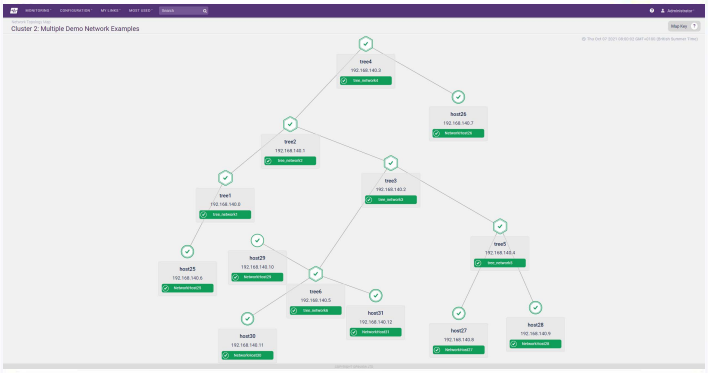
The Network Analyzer automates the discovery and visualization of your network topology, and provides insight into the protocol usage on a network, data transfers that are saturating the network, the end nodes that are transmitting and receiving data, and more. Network Analyzer consists of three modules: Network Topology, Flow Collector and Net Audit.

Automate topology discovery, reduce security risks, fix broken configurations

It's surprising how many system administrators use Visio, or even their office whiteboard to draw a picture of their network topology. Less surprising is the fact that these diagrams are rarely up-to-date, and not truly showing all of the hosts in the network, their interconnections and their importance.

The network topology discovery and visualization feature will walk the neighborhood tables of SNMP-enabled devices, using LLDP or CDP, to capture and draw a dynamically-scaling picture of your network. Discover un-connected hosts, uncover unexpected hosts, and recover device misconfigurations.

What's more, you can run a discovery walk at any time - and you can automate this to run regularly, ensuring that your knowledge of the network topology is very much up-to-date. This enhances your corporate memory, automates a manual and error-prone process, and increases the security of sensitive information. No more diagrams on open-office whiteboards, or shared by email. The visualisations are fully-dynamic, automatically scaling for 10s, 100s or 1000s of devices.



Once you've discovered and visualized your network topology - and fixed any issues that you might have found - Opsview monitoring will automatically overlay device up/down/unknown status for each host - in real-time.

Flow Collector Module

Opsview's Flow Collector Module enables the collection and analysis of flow-enabled network devices, such as NetFlow from Cisco routers, sFlow from HP Switches and more.The main benefit of flow protocols such as NetFlow and sFlow is that they allow you to look 'inside' the connection to see not only that the 'link is 95% utilized', but to understand why, i.e., is a user downloading large files continuously, is a router misconfigured, etc. In turn, this will allow you to quickly pinpoint offending applications and take steps to mitigate any issues, perhaps by increasing bandwidth, re-routing traffic or optimizing configuration.

Net Audit Module

Opsview's Net Audit Module allows you to easily backup (using RANCID) any network configurations, providing visibility via one of your dynamic dashboards, and alerting you of any changes that might have been made. For example, with more remote working and more home working, you may have had to make numerous configuration changes to your network. If you do not have a backup of that configuration, it is going to take a very long time to recreate.
Using a networking auditing tool, this risk can be removed, allowing network administrators peace of mind and a view not just into the performance of the router or switch, but also a view into the actual configuration itself.

The combined power of Network Analyzer

Use Network Topology, Flow Collector and NetAudit in combination to support uses cases including:

- Identifying hosts missed during import to then be monitored by NetFlow and NetAudit
- Understanding areas of interest, digging into the connection information, identifying when breaking changes were made
- Fixing network mis-configurations before something breaks

Software-defined networking defined

"Software-defined" refers to any technology that involves both software and the virtualization of some physical computing, storage or networking/ communications device. Software-defined represents a new class of products where the software is the focus and is used to provide the solution rather than the hardware. For example, in years past, data center growth was often a hardware path and software was used to support the function. However, traditional networks can't keep up and meet current networking requirements such as:

- Dynamic scalability
- Central control and management
- On the fly changes or experiments
- Less error-prone manual configurations on each networking node
- Handling of network traffic (which has massively increased due to the boom of mobile data)
- Server virtualization traffic in data centers

Monitoring Cisco ACI

Cisco's Application Centric Infrastructure (ACI) is a Software-Defined Networking (SDN) solution for data centers.

Cisco ACI allows application requirements to define the network. The Application Policy Infrastructure Controller (APIC) manages the scalable ACI multi-tenant fabric. The APIC provides a unified point of automation and management, policy programming, application deployment, and health monitoring for the fabric.

The Cisco ACI Opspack allows you to comprehensively monitor: ACI Pods, ACI APIC Nodes, ACI Tenants, ACI Fabric, ACI Custom Monitoring of a specific attribute from the Cisco ACI Object store, ACI APIC Clusters, ACI Endpoint Groups, ACI Bridge Domains, ACI Application Profilers, ACI Spine Nodes, and ACI Leaf Nodes.

FIND OUT MORE

Email: sales@opsview.com

USA: +1 866 662 4160 **EMEA:** +44 1183 242 100