



What is Cisco IOS NetFlow?

Cisco NetFlow technology is software contained within Cisco IOS on routers and switches that provides important information about traffic on the wide area network (WAN). Using Cisco NetFlow, IT staff can determine the applications consuming bandwidth, who is using them, and when.

With Cisco NetFlow, the approach to data collection is simplified: a NetFlow-enabled router or switch collects network data – a less costly alternative to data collection by probes, which require deployment by network staff to gain visibility of traffic on the WAN. As its name suggests, Cisco NetFlow technology tracks the flow of IP packets as they enter the router through an interface. Each flow is unique and is identified by seven criteria (Source IP address, Destination IP address, Source Port number (TCP/UDP), Destination Port number (TCP/UDP), Layer 3 Protocol Type (IP/ICMP), Type of Service (ToS), and Input logical interface); any variation in these criteria distinguishes one flow from another.

Cisco NetFlow can collect information on a very granular basis, and this data can be analyzed to report such information as:

- IP applications (for every interface or group of interfaces)
- IP hosts (for each application)
- IP conversations (for each application)
- IP Type of Service Markings (commonly used for applying Quality of Service to applications such as VoIP and Video)
- Data volumes, rates, and utilization for all of the above

How can network staff benefit from Cisco NetFlow Monitoring?

Cisco NetFlow technology provides the data necessary to effectively analyze, trend, and baseline application data as it passes through the network. It can then be exported to a reporting package and can provide the information necessary to manage critical business applications. The types of information Cisco NetFlow monitoring can provide include:

Network Traffic Analysis/Capacity Planning – Cisco NetFlow data reveals when traffic has exceeded a defined threshold (utilization, rate, or volume) on a network link. Using Cisco NetFlow monitoring data, an engineer can determine if increasing capacity will solve a problem on a link, or if there are links that can be downgraded to save money.

Network/Server/Application Monitoring & Troubleshooting – Cisco NetFlow monitoring enables extensive, real-time network monitoring to help provide problem detection, efficient troubleshooting, and rapid problem resolution.

Anomaly Detection – Cisco NetFlow measures traffic on routers and switches and includes details about the source, destination, and service ports of packets. This information can be used to identify anomalous network traffic patterns and port-scanning activity – common indications of worms.

Cisco NetFlow Technology vs. RMON2 Data

Prior to the widespread use of NetFlow monitoring data, information about network performance was primarily gathered with the assistance of RMON2 probes. These dedicated instruments monitor data packets crossing the network at certain critical points, such as near WAN or LAN interfaces on a router. While there are benefits to RMON2 network monitoring, the expense associated with establishing and maintaining such probes over a large-scale enterprise network is formidable – both in terms of capital expense and the personnel required to manage them. Cisco NetFlow technology is available on nearly all Cisco routers and switches and the financial and personnel investments necessary to benefit from Cisco NetFlow monitoring are substantially lower than an RMON2 solution. The chart below outlines the benefits and considerations of each monitoring technology.

Benefits

Cisco NetFlow Technology

- Low Capital Investment – The majority of networks are already instrumented with Cisco routers.
- Simple Configuration – configuring NetFlow involves a few global commands and an interface command for each interface running NetFlow.
- Dynamic Application Detection – NetFlow measures and reports automatically on all IP application traffic (most probe solutions require that each probe be configured to look for each traffic type).
- Real-time Traffic Analysis

RMON2

- Information on non-IP protocols such as IPX, AppleTalk, and DECnet
- Packet capture capability
- No additional router load
- Sub-minute traffic analysis

Considerations

Cisco NetFlow Technology

- Support for IP traffic only
- Increase in CPU utilization on configured routers (The amount of increase on router CPU utilization varies by router platform and the number of flows traversing the router. Typically the increase is less than 5 percent.)
- Increase in network traffic along path between configured routers and NetFlow collectors (Typically the increase is less than 1 percent of the capacity of the circuit.)

RMON2

- High capital investment (e.g., how many probes will be needed to cover all or part of the network, and how much will that level of coverage cost?)
- Resource intensive (to perform configuration, planning, and deployment of probes)
- Medium to high lifecycle maintenance (licensing, software upgrades, probe interface upgrades, and network bandwidth increases)