



WHAT IS NETFLOW?

Originally developed by Darren Kerr and Barry Bruins in 1996 as part of the Cisco IOS, NetFlow™ was first used as a packet switching path selector designed to make the forwarding process within the router more efficient. Only later was NetFlow’s true value as a network accounting technology fully realized, providing numerous benefits not available with other network or security technologies:

- network application and user monitoring
- accounting and billing
- network analysis and planning
- traffic engineering
- security analysis
- NetFlow data warehousing and data mining

Using NetFlow correctly is the single most important step remaining for enterprises to secure their networks.

- Richard Stiennon

Network Traffic “Telemetry”

The aerospace telemetry analogy best illustrates how NetFlow operates. Aerospace telemetry is a highly automated communications process by which measurements are made at remote or inaccessible points and transmitted to receiving equipment for monitoring and post processing. As an example, aerospace telemetry started in the 1930s with the radiosonde, a device that automatically measured temperature, barometric pressure and humidity from a balloon high in space, and transmitted data to Earth using a radio signal. Terrestrial equipment would then process and scrutinize the incoming radio waves to determine the conditions surrounding the weather balloon.

Similarly, NetFlow-enabled routers and switches capture measurements of the network traffic at points in the network and transmit this captured data in the form of User Datagram Protocol (UDP) datagrams or Stream Control Transmission Protocol (SCTP) packets to a NetFlow collector for further processing, analysis and archiving.

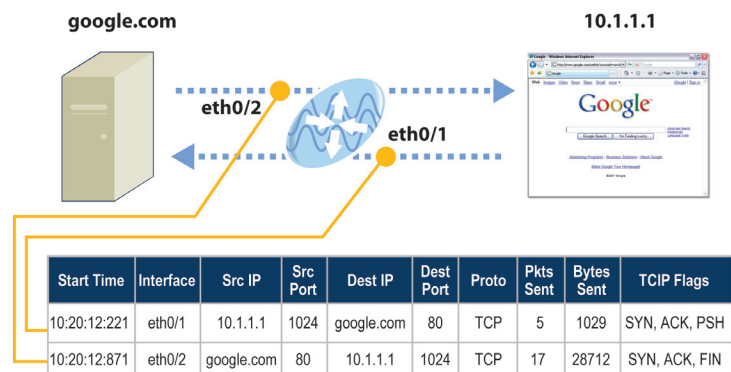
Enabling NetFlow

Enabling NetFlow and directing it to a NetFlow collector can be easily accomplished using the following commands. Administrators should note that because NetFlow capture and export are performed independently on each device, not every router needs to be NetFlow-enabled.

```
ip flow ingress
ip route-cache flow
ip flow-export destination <collector ip address> <collector port>
```

How NetFlow Collection Works

NetFlow-enabled Cisco routers generate NetFlow records, export them to a collector once the flow has finished and then purge the data from their in memory NetFlow cache. These NetFlow records are exported in UDP or SCTP packets in one of five formats (NetFlow v1, 5, 7, 8, 9). Routers and switches supporting NetFlow include Cisco 800, 1700, 2600, 3600, 3700, 4500/4700, AS5300/5800, 7200/7300/7400/7500, 4500, Catalyst 6500/7600, 10000, 12000 and CSR-1.



NetFlow Impact On Router Performance

Paying no attention to packet payloads greatly reduces the processing overhead and makes NetFlow an extraordinarily good fit for busy, high-speed network environments. In addition, this characteristic makes NetFlow very useful in zero-day or "mutant attack" detection in cases where signature-based intrusion detection systems would fail.¹

CPU utilization varies from one platform to the next. A router by router performance comparison is too extensive to include here. For example, Cisco's performance analysis indicates the NetFlow impact for the 2600 router utilizes 16% CPU for between 10,000 and 45,000 flows stored in the cache. Comparatively, the 7600 series of routers utilizes 2% CPU for 10,000 flows and 3% for 45,000 flows. Regarding impact to the network itself, NetFlow typically consumes less than 1% of total bandwidth. For more information on the impact of enabling NetFlow on Cisco routers and switches, see http://www.cisco.com/en/US/tech/tk812/technologies_

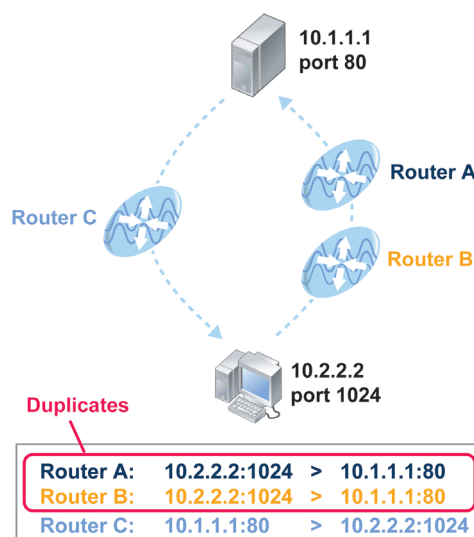
A few years back, NetFlow from Cisco Systems was correctly accused of being a performance hog and too cumbersome to deploy. Fortunately, these issues have been addressed and now the technology is fast becoming a networking must within the enterprise.²

white_paper0900aec802a0eb9.shtml

In rare cases, maintaining NetFlow data in the cache can exceed a router's capacity. To avoid this, Cisco provides *Sampled NetFlow*, which looks at every nth packet rather than every packet to maintain NetFlow records. This then allows the administrator to tune the NetFlow collection to meet any network speed.

NetFlow De-duplication

One of the primary challenges with processing NetFlow includes *duplicate flow records* from routers along the same data path. Security-focused analysis of NetFlow fails when collectors receive multiple reports for single flows. Therefore, it is critical to "de-duplicate" flow records in order to capture accurate, unique host-to-host conversations.



Examples of NetFlow-based technologies

There are three types of NetFlow technologies:

- Low cost "classic" NetFlow solutions offer traditional network traffic analysis functionality, such as top talkers, traffic trending, ASN Reporting, interface utilization and QoS reporting.
- Enterprise "classic" NetFlow solutions offer the same features listed above along with more advanced reporting, application performance monitoring, scalability, and appliance-based models for easier deployment and maintenance.
- Enterprise NetFlow-based Network Behavior Analysis (NBA) solutions, such as StealthWatch® by Lancope®, provide these same enterprise features and deliver a wide-breadth of network security functionality for the enterprise.

About Lancope, Inc.

Lancope®, Inc. is the leader in NetFlow Analysis and the provider of the StealthWatch® for flow-based anomaly detection and network performance monitoring. Delivering unified visibility across physical and virtual networks, StealthWatch eliminates network blind spots and reduces total network and security management costs.

Lancope Headquarters

3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022

+1.770.225.6500 (US)
888.419.1462 (Toll Free)
+1.770.698.8827 (International)

Website: www.lancope.com
E-mail: sales@lancope.com

©2009 Lancope, Inc. All rights reserved. Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. All other trademarks are properties of their respective owners. StealthWatch is covered by U.S. Patent Nos. 7,290,283; 7,185,368; 7,475,426; 7,512,980 and other U.S. and foreign patents pending.

MB11042009

¹ Yiming Gong, "Detecting Worms and Abnormal Activities with NetFlow, Part 1"

² Michael Patterson, "Networking Becoming an Enterprise Must for the Enterprise", Enterprise Networks and Servers