Cisco IOS Flexible NetFlow

Last updated: December 2008

Q. What is Flexible NetFlow?

A. Cisco is now innovating flow technology to a new level beyond what has been traditionally available. *Cisco IOS Flexible NetFlow* is Cisco's next-generation *flow* technology. Flexible NetFlow provides enhanced optimization of the network infrastructure, reduces costs, and improves capacity planning and security detection beyond other flow based technologies available today.

Q. What are the key advantages of Flexible NetFlow above traditional NetFlow?

A.

- Flexibility, scalability, aggregation of flow data beyond today's NetFlow.
- The ability to monitor a wider range of IP packet information from layer 2 to 7
- Enhanced network anomaly and security detection
- User configurable flow information to perform customized traffic identification and the ability to focus and monitor specific network behavior
- Convergence of multiple accounting technologies into one accounting mechanism

Q. How will your network benefit from Flexible NetFlow?

A. Flexible NetFlow provides information about how the network is being utilized. It will let you understand who, what, when, where, and how network traffic is flowing.

Including:

- Application and network usage
- Network productivity and utilization of network resources
- The impact of changes to the network
- Network anomaly and security vulnerabilities
- Long term compliance, business process and audit trail

Q. What are the primary uses of Flexible NetFlow?

A. Applications for NetFlow data are constantly being invented but the key usages include:

- Real-time Network monitoring
- Application and user Profiling
- Network planning and capacity planning
- Security incident detection and classification
- Accounting and billing
- Network data warehousing, forensics and data mining
- Troubleshooting

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Q. Can Flexible NetFlow track different applications simultaneously?

A. Yes, NetFlow applications such as security monitoring, traffic analysis and billing can be tracked separately and the information customized per application. Flexible NetFlow has the capability to create multiple flow caches or information databases to track NetFlow information. Traditionally NetFlow has a single cache and all applications use the same cache information. In Flexible NetFlow the user can collect specific security information in one flow cache and traffic analysis in another. Each cache will have the specific and customized information required for the application. For example multicast and security information can be tracked separately and the results sent to two different NetFlow reporting systems.

Q. How does Flexible NetFlow provide greater scalability and customization?

A. Flexible NetFlow allows the user to select what is monitored and this allows efficient tracking of information. In today's NetFlow typically seven IP packet fields are tracked to create NetFlow information. The fields used to create the flow information are not configurable. In Flexible NetFlow the user configures what to track and the result is fewer flows produced increasing scalability of hardware and software resources. For example IPv4 header information, BGP information, and multicast or IPv6 data can all be configured and tracked in Flexible NetFlow

Q. How does Flexible NetFlow enhance security monitoring?

A. NetFlow typically tracks IP information such as IP addresses, ports, protocols, TCP Flags and most security systems look for anomalies or changes in network behavior to detect security incidents. Flexible NetFlow allows the user to track a wide range of IP information including all the fields in the IPv4 header or IPv6 header, a variety of individual TCP flags and it can also export sections of a packet. The information being tracked may be a key field (used to create a flow) or non-key field (collected with the flow). The user has the ability to use one NetFlow cache to detect security vulnerability (anomaly detection) and then create a second cache to focus or zoom in on the particular problem.

Q. How does Flexible NetFlow enhance troubleshooting?

A. Flexible NetFlow allows the user to create multiple caches and because of this it is possible to inspect specific information. For example, if the user determines a problem related to a specific server using normal traffic analysis (i.e. high byte count) then a secondary cache can be created with an input filter showing only traffic to the destination. This allows the user to focus and track specifically what is happening to the server. If one user is utilizing most of the bandwidth or a rogue server is consuming bandwidth, this will clearly visible in the secondary cache. The ability to continue normal traffic analysis and also view data in greater details is a key advantage of Flexible NetFlow.

Q. What is a Flexible NetFlow key field?

A. Each packet that is forwarded within a router or switch is examined for a set of IP packet attributes. These attributes are the IP packet identity or *key fields* for the flow and determine if the packet information is unique or similar to other packets. Traditionally, an IP Flow is based on a set of seven IP packet attributes. This set of key fields is tracked and if the set of values for these fields are unique a new flow record is created in the NetFlow cache. For example, all packets with the same source/destination IP address, source/destination ports, protocol, interface and class of service are grouped into a flow and then packets and bytes tallied. In Flexible NetFlow key fields are configurable allowing detailed traffic analysis.

Q. What is a Flexible NetFlow Flow Monitor?

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

A. A flow monitor is essentially a NetFlow cache. The *Flow Monitor* has two major components the *Flow Record* and the *Flow Exporter*. The flow monitor can track both ingress and egress information. The flow record contains what information being tracked by NetFlow (i.e. IP address, ports, protocol…). The Flow exporter describes the NetFlow export. Flow monitors may be used to track IPv4 traffic, IPv6 traffic, multicast or unicast, MPLS, bridged traffic. Multiple Flow monitors can be created and attached to a specific physical or logical interface. Flow monitors can also include packet sampling information if sampling is required.

Q. What is a Flexible NetFlow Flow Record?

A. The flow record defines what information NetFlow will track. The flow record may be user defined or a pre-defined scheme available in IOS. The flow record is defined as a set of key and non-key fields. Typical NetFlow key fields are IP addresses and ports and if the set of key fields are unique a new flow is created. The non-key field information is collected and attached to the flow. Typical non-key fields include timestamps, packet and byte counters and TCP flag information. Essentially the flow record tells NetFlow what information to obtain from the packets being forwarded.

Q. What is a NetFlow version 9 export format?

A. NetFlow exports information to reporting servers in various formats including NetFlow version 5 and version 9. NetFlow version 5 is used with traditional NetFlow and is a fixed export format with a limited set of information being exported. NetFlow version 9 is a flexible and extensible NetFlow format used by Flexible NetFlow. NetFlow version 9 includes a template to describe what is being exported and the export dat The template is periodically sent to the NetFlow collector telling it what data to expect from the router or switch. The data is then sent for the reporting system to analyze. NetFlow version 9 is extensible and flexible and therefore any data available in the device can theoretically be sent in NetFlow version 9 format. Flexible NetFlow allows the user to configure and customize what information is exported using NetFlow version 9. NetFlow version 9 is the basis for the IETF standard IPFIX associated with the IP Flow and Information working group in IETF.

Q. What is a Flexible NetFlow Flow Exporter?

A. The flow exporter describes information about the NetFlow export that is sent to the reporting server or NetFlow collector. The NetFlow exporter includes the destination address of the reporting server, the type of transport (i.e. UDP or SCTP), and the export format (ie: version 9, version 5 or IPFix). There can be multiple exporters per flow monitor (up to 8).

Q. Is the Flexible NetFlow Exporter QoS aware ?

A. Flexible NetFlow allows to set a DSCP value to export packets: this DSCP value is configurable on a per Exporter basis. Starting with Cisco IOS Software Release 12.4(20)T, The export stream will be prioritized/queued locally with other traffic based on its class of service or DSCP value: this requires the output-features command to be configured in the exporter definition.

Q. Does Flexible NetFlow support NetFlow v5 export format ?

A. Flexible NetFlow is able to export Flow records using NetFlow v5 Format starting with Cisco IOS Software Release 12.4(22)T. NetFlow v5 export format should be used in conjunction of predefined flow record. The main benefits of this feature is to allow customers to migrate from Traditional NetFlow to Flexible NetFlow without impacting existing NetFlow Collectors.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Q. What is an example of Flexible NetFlow configuration with a pre-defined flow record?

A. This example will configure traditional NetFlow export using the new Flexible NetFlow CLI. The user will create the Flow Monitor and attaches the Flow Record and Flow Exporter to the Flow Monitor. In this example the flow exporter is named *export-to-server* and the destination address of the server is 172.16.1.1. The flow monitor is named *my-flow-monitor* and contains the pre-defined flow record *netflow-original*. The flow monitor is the attached to the interface to track input (ingress) traffic.

```
flow exporter export-to-server
 destination 172.16.1.1

flow monitor my-flow-monitor
 record netflow-original
 exporter export-to-server

interface Ethernet 1/0
 ip flow monitor my-flow-monitor input
```

Q. What is a simple example of Flexible NetFlow configuration with a user flow record?

A. This example will configure a user defined flow record using the new Flexible NetFlow CLI. A user defined flow record can match a specific field in a packet. The *match* statement indicates the field is a key field (see question: what is a key field above). The *collect* keyword is used to identify non-key field or information added to the flow and exported with the flow. In this example the flow exporter is named *export-to-server* and the destination address of the server is 172.16.1.1. The flow monitor is named *app-traffic-analysis* and the user is tracking TCP applications packet and byte count from specific IP source address to a destination. The flow monitor is the attached to the interface to track input (ingress) traffic.

```
flow record app-traffic-analysis
 description This flow record tracks TCP application usage
 match transport tcp destination-port
 match transport tcp source-port
 match ipv4 destination address
 match ipv4 source address
 collect counter bytes
 collect counter packets

flow exporter export-to-server
 destination 172.16.1.1

flow monitor my-flow-monitor
 record app-traffic-analysis
 exporter export-to-server
```

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
interface Ethernet 1/0
 ip flow monitor my-flow-monitor input
```

Q. What types of Flexible NetFlow caches are available?

A. There are three types of flow caches that can be used in Flexible NetFlow:

- Normal cache
- Permanent caches
- Immediate cache

In traditional NetFlow the only cache that is available is what we call the normal cache in Flexible NetFlow. The normal cache uses flow timers to expire and export flows to a NetFlow collector. As flows are created and terminated in the NetFlow cache timers track when to push the flows in the flow cache to the NetFlow collector. Additionally in Flexible NetFlow two other cache types are now available the permanent cache and immediate cache. The permanent cache is very different from a normal cache and will be useful for accounting or security monitoring. The permanent cache will be a fixed size chosen by the user. After the permanent cache is full all new flows will be dropped but all flows in the cache will be continuously updated over time (i.e similar to interface counters). The immediate export cache will be very effective for security monitoring or when the user wants each packet to effectively create a new flow. The immediate cache can be used with packet section export.

Q. How is Flexible NetFlow a superset of other accounting technologies?

A. Flexible NetFlow can monitor ingress and egress traffic and will track information from layer 2 though 7 in the IP packet. For example, Flexible NetFlow can track BGP policy accounting traffic index and marry the traditional packet and byte counts with flow information including AS, subnet and other key fields.

For more information on NetFlow go to: http://www.cisco.com/go/fnf

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Printed in USA

c67-513100-00 12/08

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.