Appplication Monitoring Using NetFlow

Technology Design Guide

December 2013

CISCO VALIDATED DESIGN

Table of Contents

Preface

Cisco Validated Designs (CVDs) provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- Technology design guides provide deployment details, information about validated products and software, and best practices for specific types of technology.
- Solution design guides integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd/wan

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- Visibility into Application Performance—Organizations want visibility into the network in order to enable resource alignment, ensuring that corporate assets are used appropriately in support of their goals.

For more information, see the “Use Cases” section in this guide.

Scope

This guide covers the following areas of technology and products:

- Wide area networking
- Routers
- Application optimization
- Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
- Quality of service
- NetFlow and external collectors
- Network Based Application Recognition (NBAR)

For more information, see the “Design Overview” section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- CCNA Routing and Switching—1 to 3 years installing, configuring, and maintaining routed and switched networks

Related CVD Guides

MPLS WAN Technology Design Guide

Layer 2 WAN Technology Design Guide

VPN WAN Technology Design Guide

To view the related CVD guides,
click the titles or visit the following site:
http://www.cisco.com/go/cvd/wan

Introduction

There are several trends in the enterprise today driving requirements to build application awareness within the network. The network is the critical infrastructure that enables and supports business processes throughout all the functions of an organization.

For the staff responsible for planning, operation, and maintenance of the network and network services, it is indispensable to have visibility into the current health of the network from end-to-end.

It is also essential to gather short and long-term information in order to fully understand how the network is performing and what applications are active on the network. NetFlow data from a network is equivalent to the call detail records available from voice and video call control systems.

Capacity planning is one of the most important issues faced by organizations in managing their networks. More of an art than a science until recently, network capacity planning is all about balancing the need to meet user performance expectations against the realities of capital budgeting.

Cisco Application Visibility and Control (AVC) combine several key technologies such as NetFlow and Network Based Application Recognition (NBAR) in order to gain deeper insight into application and user traffic flows on the network. Greater visibility helps to quickly isolate and troubleshoot application performance and security related issues.

Technology Use Cases

WAN bandwidth is expensive. Many organizations attempt to control costs by acquiring the minimum bandwidth necessary to handle traffic on a circuit. This strategy can lead to congestion and degraded application performance.

Use Case: Visibility into Application Traffic Flows

Organizations want visibility into the network in order to enable resource alignment, ensuring that corporate assets are used appropriately in support of their goals.

Organizations need a way to help IT staff verify that quality of service (QoS) is implemented properly, so that latency-sensitive traffic, such as voice or video, receives priority. They also want continuous security monitoring to detect denial-of-service (DoS) attacks, network-propagated worms, and other undesirable network events.

This design guide enables the following capabilities:

- Deploy flexible NetFlow (FNF) with NBAR2 to identify application traffic and impacts on the network.
- Reduce peak WAN traffic by using NetFlow statistics to measure WAN traffic changes associated with different application policies, and understand who is utilizing the network and who the network's top talkers are.
- Diagnose slow network performance, bandwidth hogs, and bandwidth utilization in real-time with command-line interface (CLI) or reporting tools.
- Detect and identify unauthorized WAN traffic and avoid costly upgrades by identifying the applications that are causing congestion.
- Detect and monitor security anomalies and other network disruptions and their associated sources.

- Export FNF with NBAR data to Cisco Prime Infrastructure and other third-party collectors by using NetFlow v9 and IP Flow Information Export (IPFIX).
- Validate proper QoS implementation and confirm that appropriate bandwidth has been allocated to each class of service (CoS).

Design Overview

NetFlow is an embedded capability within Cisco IOS Software on routers and switches as well as Cisco Wireless Controllers and Cisco WAAS appliances. It is one of the key component technologies of Cisco Application Visibility and Control (AVC). Together with Network Based Application Recognition (NBAR), Cisco NetFlow allows an organization to gather traffic-flow information and enable application visibility in the network. This integrated approach greatly simplifies network operations, and reduces total cost of ownership.

Information collected by network devices is done by using Flexible NetFlow, which can collect application information provided by NBAR2, traffic flow information, and application statistics such as byte and packet count.

All of this information is aggregated and then exported through open export formats such as NetFlow version 9 and IPFIX to Cisco and third-party network management applications.

Use with network management tools such as Cisco Prime Infrastructure, Cisco AVC provides an integrated solution for discovering and controlling applications within the network. Empowered with these tools, network administrators gain greater visibility into the applications running in their networks, while applying policies to improve security, performance, and gain control of network resource utilization.

Traditional NetFlow

Cisco IOS NetFlow allows network devices that are forwarding traffic to collect data on individual traffic flows. Traditional NetFlow (TNF) refers to the original implementation of NetFlow, which specifically identified a flow as the unique combination of the following seven key fields:

- IPv4 source IP address
- IPv4 destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type-of-service (ToS) byte
- Input logical interface

These key fields define a unique flow. If a flow has one different field than another flow, then it is considered a new flow.

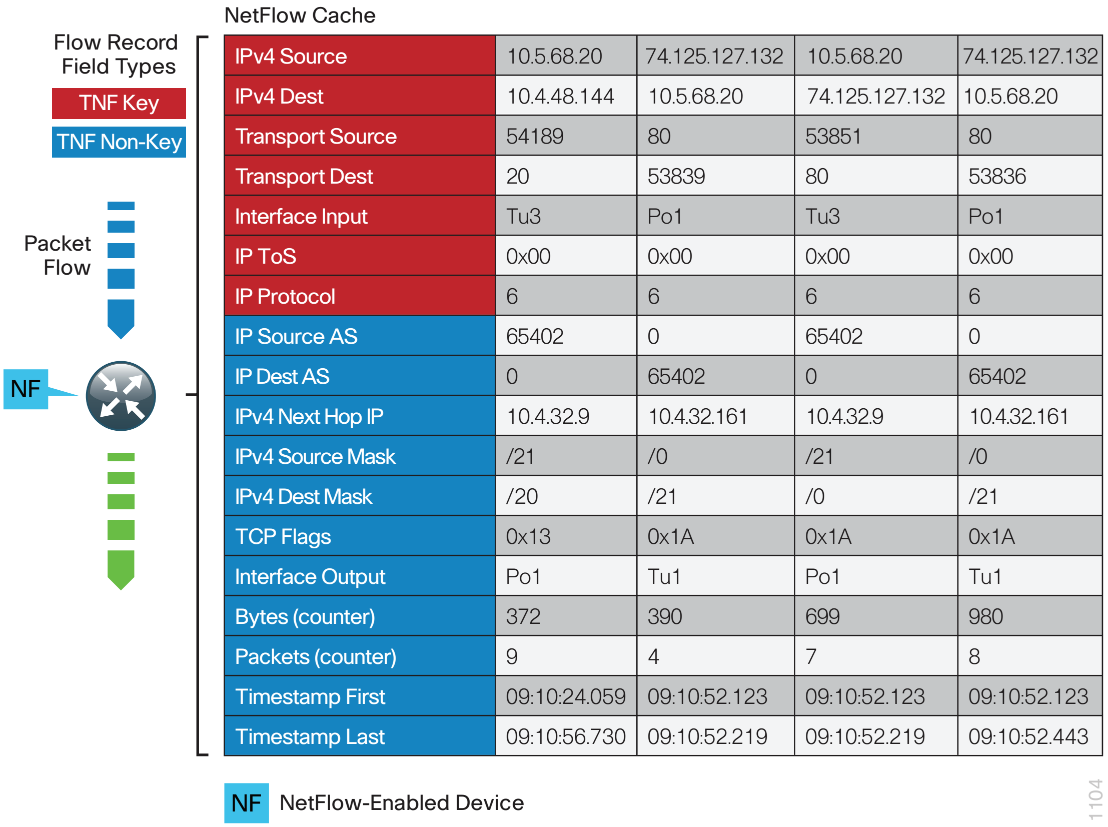
NetFlow operates by creating a NetFlow cache entry that contains the information for all active flows on a NetFlow-enabled device. NetFlow builds its cache by processing the first packet of a flow through the standard switching path. It maintains a flow record within the NetFlow cache for all active flows. Each flow record in the NetFlow cache contains key fields, as well as additional non-key fields, that can be used later for exporting data to a collection device. Each flow record is created by identifying packets with similar flow characteristics and counting or tracking the packets and bytes per flow.

Tech Tip

NetFlow key fields uniquely determine a flow.

NetFlow non-key fields contain additional information for each flow and are stored along with key-field information.

Figure 1 - TNF cache



NetFlow Cache

IPv4 Source	10.5.68.20	74.125.127.132	10.5.68.20	74.125.127.132
IPv4 Dest	10.4.48.144	10.5.68.20	74.125.127.132	10.5.68.20
Transport Source	54189	80	53851	80
Transport Dest	20	53839	80	53836
Interface Input	Tu3	Po1	Tu3	Po1
IP ToS	0x00	0x00	0x00	0x00
IP Protocol	6	6	6	6
IP Source AS	65402	0	65402	0
IP Dest AS	0	65402	0	65402
IPv4 Next Hop IP	10.4.32.9	10.4.32.161	10.4.32.9	10.4.32.161
IPv4 Source Mask	/21	/0	/21	/0
IPv4 Dest Mask	/20	/21	/0	/21
TCP Flags	0x13	0x1A	0x1A	0x1A
Interface Output	Po1	Tu1	Po1	Tu1
Bytes (counter)	372	390	699	980
Packets (counter)	9	4	7	8
Timestamp First	09:10:24.059	09:10:52.123	09:10:52.123	09:10:52.123
Timestamp Last	09:10:56.730	09:10:52.219	09:10:52.219	09:10:52.443

Originally, TNF used ingress and egress NetFlow accounting features, which are now considered legacy. NetFlow-enabled devices continue to provide backward compatibility with these accounting features implemented within a new configuration framework. These are detailed in the following sections.

Tech Tip

Traditional NetFlow (also called Classic NetFlow) and NetFlow version 5 are not suitable for AVC solutions because they can report only L3 and L4 information. When possible, it's highly recommended to migrate to Flexible NetFlow with NBAR as outlined in this guide.

Flexible NetFlow

Flexible NetFlow (FNF), unlike TNF, allows you to customize and focus on specific network information. You can use a subset or superset of the traditional seven key fields to define a flow. FNF also has multiple additional fields (both key and non-key). This permits an organization to target more specific information so that the total amount of information and the number of flows being exported is reduced, allowing enhanced scalability and aggregation.

The available key fields are listed in the following table. The key fields can also be used as non-key fields if desired.

Table 1 - All FNF key fields

Key field type	Key field value
application	name
datalink	dot1q vlan input dot1q vlan output dot1q mac destination address input dot1q mac destination address output dot1q mac source address input dot1q mac source address output
flow	direction sampler
interface	input output
IPv4	destination address destination mask destination prefix dscp fragmentationflags fragmentation offset header-length id length header length payload length total option map precedence protocol section header size [value] section payload size [value] source address source mask source prefix tos total-length ttl version
routing	destination as destination traffic-index forwarding-status is-multicast multicast replication-factor next-hop address source as source traffic-index vrf input

transport	destination-port icmp code icmp type igmp type source-port tcp acknowledgement-number tcp destination-port tcp flags tcp header-length tcp sequence-number tcp source-port tcp urgent-pointer tcp window-size udp destination-port udp message-length udp source-port

The non-key fields that can be collected for each unique flow are shown in the following table.

Table 2 - Additional non-key fields

Non-key field type	Non-key field value
counter	bytes packets
timestamp	sys-uptime first sys-uptime last
IPv4	total-length maximum total-length minimum ttl maximum ttl minimum

Migration from TNF to FNF

The introduction of FNF support on network devices requires a new method of configuration for the additional capabilities. You can also use this new configuration CLI to configure legacy TNF, making the original configuration CLI (now referred to as classic CLI) unnecessary.

FNF includes several predefined records that you can use to start monitoring traffic in your network. The predefined records ensure backward compatibility with NetFlow collector configurations that may not include FNF support. They have a unique combination of key and non-key fields that are backward compatible with legacy TNF configurations.

The predefined record **netflow ipv4 original input** used in our deployment is functionally equivalent to the original TNF ingress and egress NetFlow accounting features that predate the usage of flow records. A comparison between the classic and new configuration methods follows.

Traditional NetFlow—Classic CLI

```
interface GigabitEthernet0/0
 ip flow [ingress|egress]
!
ip flow-export destination 10.4.48.171 2055
ip flow-export source Loopback0
ip flow-export version 9
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
```

The new configuration CLI example uses the predefined **record netflow ipv4 original-input**, which includes the TNF key and non-key fields listed in Figure 1.

This example should be used to migrate legacy-TNF deployments to the new CLI without changing device behavior.

Tech Tip

The predefined flow record is supported only on Cisco ASR 1000 Series Aggregation Services Routers (ASR 1000) and Cisco Integrated Services Routers Generation 2 (ISR-G2).

Traditional NetFlow—New Configuration CLI

```
interface GigabitEthernet0/0
 ip flow monitor Monitor-NF [input|output]
!
flow exporter Export-NF-1
 destination 10.4.48.171
 source Loopback0
 transport udp 2055
 export-protocol netflow-v9
 !
flow monitor Monitor-NF
 record netflow ipv4 original-input
 exporter Export-NF-1
 cache timeout active 1
 cache timeout inactive 15
```

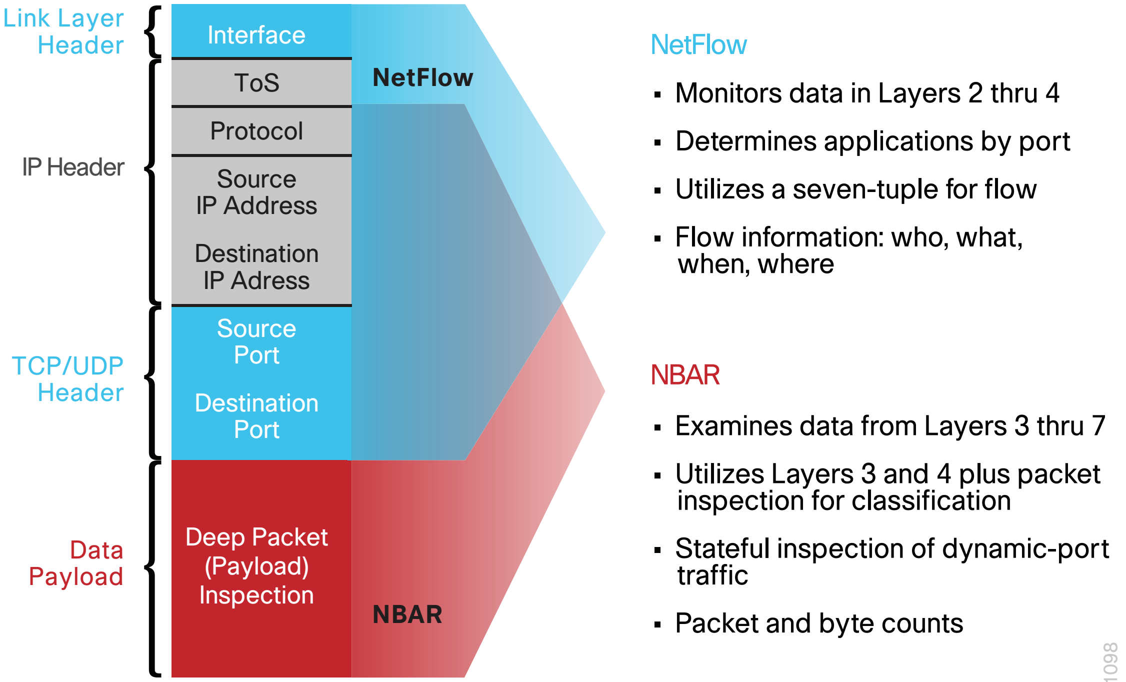
Network-Based Application Recognition (NBAR)

In the past, typical network traffic could easily be identified using well known port numbers. Today, many applications are carried on the network as HTTP and HTTPS, so identifying applications by their well-known port number is no longer sufficient.

Cloud applications and services such as WebEx, SalesForce.com, and Microsoft Office 365 are delivered over HTTP and HTTPS using the same ports as other web-based traffic such as Netflix, Hulu, Pandora, and iTunes. In addition, many applications such as voice, video, and Microsoft Exchange use dynamic ports and therefore are not uniquely identifiable by their port numbers alone. Network administrators need enhanced visibility into different types of traffic that use well-known and dynamic port numbers.

Network Based Application Recognition (NBAR) is an intelligent classification engine in Cisco IOS Software that can recognize a wide variety of applications, including web-based and client/server applications. NBAR uses deep packet inspection to look within the transport layer payload in order to determine the associated application, as shown in the following figure.

Figure 2 - NetFlow and NBAR integration



NetFlow

- Monitors data in Layers 2 thru 4
- Determines applications by port
- Utilizes a seven-tuple for flow
- Flow information: who, what, when, where

NBAR

- Examines data from Layers 3 thru 7
- Utilizes Layers 3 and 4 plus packet inspection for classification
- Stateful inspection of dynamic-port traffic
- Packet and byte counts

NBAR can classify applications that use:

- Statically assigned Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port numbers.
- Non-UDP and non-TCP IP protocols.
- Dynamically assigned TCP and UDP port numbers negotiated during connection establishment; stateful inspection is required for classification of applications and protocols. This is the ability to discover data connections that will be classified, by passing the control connections over the data connection port where assignments are made.

- Sub-port classification; classification of HTTP (URLs, mime or host names) and Citrix applications Independent Computing Architecture (ICA) traffic, based on published application name.
- Classification based on deep packet inspection and multiple application-specific attributes. Real-Time Transport Protocol (RTP) payload classification is based on this algorithm, in which the packet is classified as RTP, based on multiple attributes in the RTP header.

Next Generation NBAR (NBAR2)

NBAR2 is the next-generation architectural evolution of NBAR. NBAR2 or Next Generation NBAR is part of the Cisco AVC solution, which enables greater classification and visibility of network traffic flows. NBAR2 is a stateful, deep packet inspection technology based on the Cisco Service Control Engine (SCE) with advanced classification techniques, greater accuracy, and many more application signatures supporting over 1000 applications and sub-classifications.

- NBAR2 includes Cisco's cross platform deep packet inspection (DPI) and field extraction technology and is currently supported on Cisco ASR 1000 and ISR G2 platforms.
- The heuristic analysis engine allows NBAR2 to identify applications regardless of their ports and can identify applications such as Skype, Youtube, and BitTorrent.
- Support for NBAR2 protocol packs (PP) provides the ability to update and add application signatures while the routers are service independent of full Cisco IOS Software updates. New protocol packs with new application signatures are typically released every month.
- Application categorization uses NBAR2 attributes to group similar applications in order to simplify application management for both classification and reporting.

NBAR2 Application Attributes

NBAR2 provides six pre-defined attributes for every application in order to group applications of similar types. This simplifies the classification rules and reporting by matching applications using attributes in class-map, or reporting based on attributes.

Table 3 - NBAR2 attributes

NBAR2 attributes	Attribute definition
Category	First level grouping of applications with similar functionalities (Example: browsing, business-and-productivity-tools, email, file-sharing, gaming, net-admin, location-based-services, layer3-overip, etc.)
Sub-category	Second level grouping of applications with similar functionalities (Example: client-server, voice-video-chat-collaboration, storage, backup-systems, rich-media-http-content, authentication services, etc.)
Application-group	Grouping of applications based on brand or application suite (Example: flash-group, corba-group, wap-group, network-management, epayment, etc.)
P2P-technology	Indicates if the application is peer-to-peer (yes or no)
Encrypted	Indicates if the application is encrypted (yes or no)
Tunneled	Indicates if the application uses a tunneling technique (yes or no)

Tech Tip

The following network conditions affect the ability for NBAR to properly classify network traffic

Asymmetric flows—If both directions of a flow do not pass through the same device, stateful classification will fail.

IP fragmentation—Classification is attempted on only the first fragment before reassembly. If visibility into the full original packet is required, then classification will fail.

Out-of-order packets—Traffic may not be classified properly.

Flexible Netflow (FNF) integration with NBAR

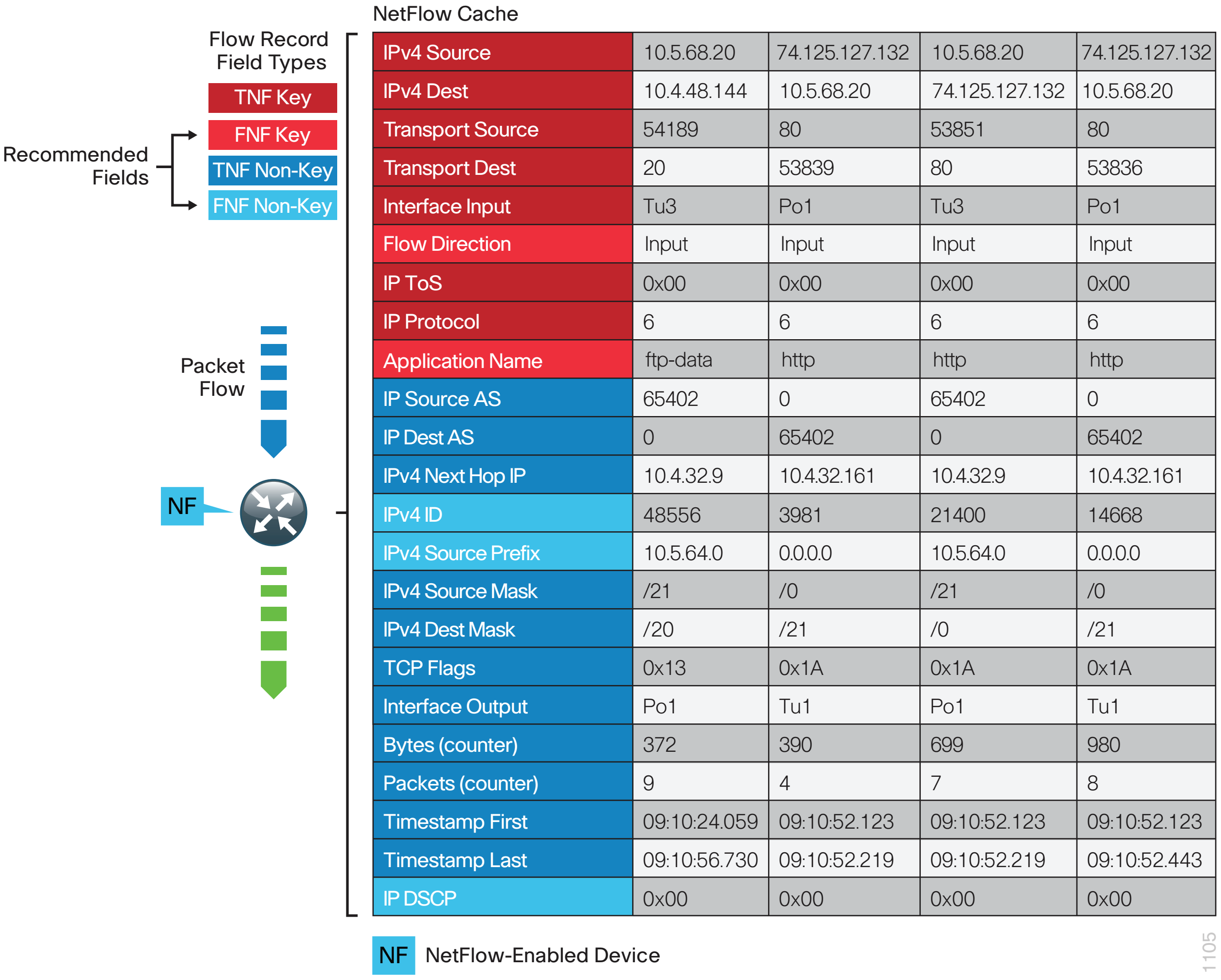
FNF integrates seamlessly with NBAR and is enabled to gather data by using "**application name**" as a key field within a FNF flow record. The application identification provided by NBAR is more effective than using the TCP/UDP well-known-port mapping.

Tech Tip

Application identification with NBAR is one of the key reasons to make the migration from TNF to FNF.

This implementation of FNF selects additional fields that provide improved application visibility within the deployed architecture. These additional fields are listed in the following figure.

Figure 3 - FNF cache



IPv4 Source	10.5.68.20	74.125.127.132	10.5.68.20	74.125.127.132
IPv4 Dest	10.4.48.144	10.5.68.20	74.125.127.132	10.5.68.20
Transport Source	54189	80	53851	80
Transport Dest	20	53839	80	53836
Interface Input	Tu3	Po1	Tu3	Po1
Flow Direction	Input	Input	Input	Input
IP ToS	0x00	0x00	0x00	0x00
IP Protocol	6	6	6	6
Application Name	ftp-data	http	http	http
IP Source AS	65402	0	65402	0
IP Dest AS	0	65402	0	65402
IPv4 Next Hop IP	10.4.32.9	10.4.32.161	10.4.32.9	10.4.32.161
IPv4 ID	48556	3981	21400	14668
IPv4 Source Prefix	10.5.64.0	0.0.0.0	10.5.64.0	0.0.0.0
IPv4 Source Mask	/21	/0	/21	/0
IPv4 Dest Mask	/20	/21	/0	/21
TCP Flags	0x13	0x1A	0x1A	0x1A
Interface Output	Po1	Tu1	Po1	Tu1
Bytes (counter)	372	390	699	980
Packets (counter)	9	4	7	8
Timestamp First	09:10:24.059	09:10:52.123	09:10:52.123	09:10:52.123
Timestamp Last	09:10:56.730	09:10:52.219	09:10:52.219	09:10:52.443
IP DSCP	0x00	0x00	0x00	0x00

NetFlow Interaction with Encryption

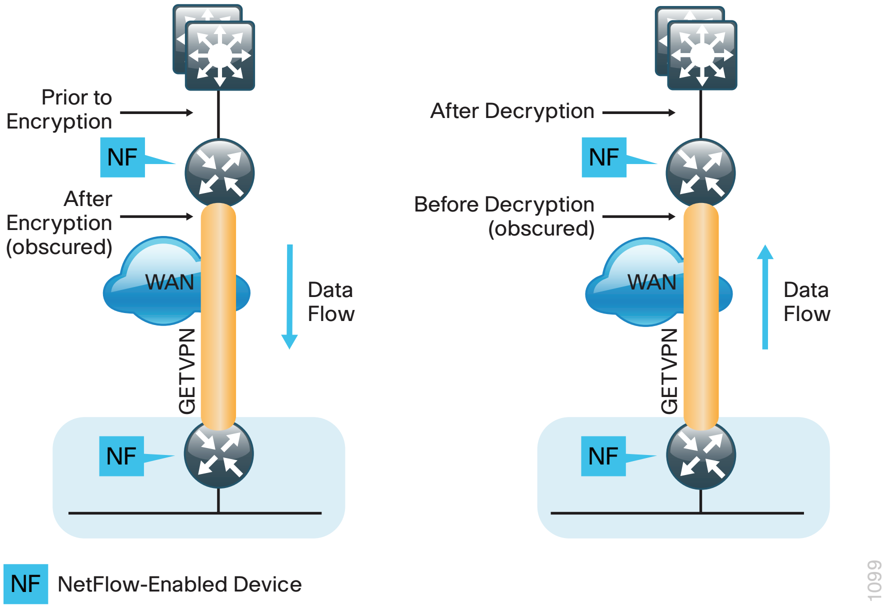
When configuring NetFlow, it is useful to understand how Cisco IOS Software processes traffic when transmitting and receiving network traffic on an interface. This is best shown as an ordered list, as illustrated in the following figure.

Table 4 - Cisco IOS order of operations

Order	Ingress features	Egress features
1	Virtual Reassembly	Output IOS IPS Inspection
2	IP Traffic Export	Output WCCP Redirect
3	QoS Policy Propagation through BGP (QPPB)	NIM-CIDS
4	**Ingress Flexible NetFlow (FNF)**	NAT Inside-to-Outside or NAT Enable
5	Network Based Application Recognition (NBAR)	Network Based Application Recognition (NBAR)
6	Input QoS Classification	BGP Policy Accounting
7	**Ingress NetFlow (TNF)**	Lawful Intercept
8	Lawful Intercept	Check crypto map ACL and mark for encryption
9	IOS IPS Inspection (Inbound)	Output QoS Classification
10	Input Stateful Packet Inspection (IOS FW)	Output ACL check (if not marked for encryption)
11	Check reverse crypto map ACL	Crypto output ACL check (if marked for encryption)
12	Input ACL (unless existing NetFlow record was found)	Output Flexible Packet Matching (FPM)
13	Input Flexible Packet Matching (FPM)	Denial of Service (DoS) Tracker
14	**IPsec Decryption (if encrypted)**	Output Stateful Packet Inspection (IOS FW)
15	Crypto to inbound ACL check (if packet had been encrypted)	TCP Intercept
16	Unicast RPF check	Output QoS Marking
17	Input QoS Marking	Output Policing (CAR)
18	Input Policing (CAR)	Output MAC/Precedence Accounting
19	Input MAC/Precedence Accounting	**IPsec Encryption**
20	NAT Outside-to-Inside	Output ACL check (if encrypted)
21	Policy Routing	**Egress NetFlow (TNF)**
22	Input WCCP Redirect	**Egress Flexible NetFlow (FNF)**
23	–	Egress RITE
24	–	Output Queuing (CBWGQ, LLQ, WRED)

Based on the order of operations, to classify traffic properly, NetFlow must monitor prior-to-encryption when transmitting and after-decryption when receiving. Otherwise, the actual protocols in use remain obscured, and all traffic appears as IP Security (IPSec) with no other details available. Encrypted traffic from the WAN is properly classified by NetFlow with an outbound monitor on a corresponding LAN interface. Similarly, traffic bound for the WAN is properly classified by NetFlow with an inbound monitor on a corresponding LAN interface. This is illustrated in in the following figure.

Figure 4 - Encryption and NetFlow



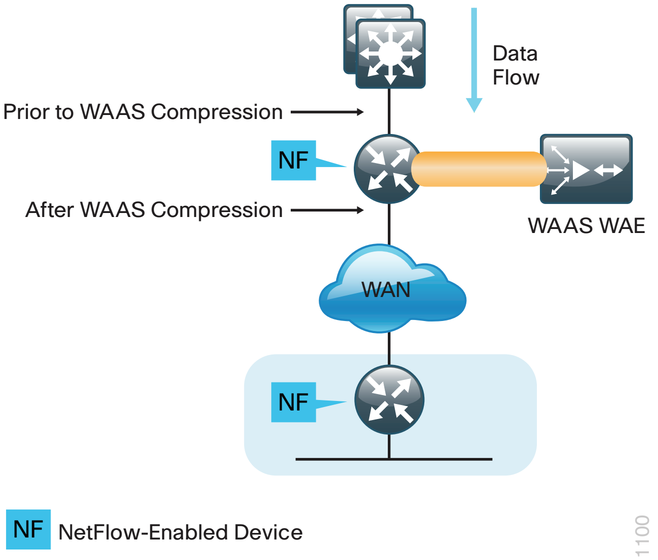
NetFlow Interaction with Application Optimization

The design includes application optimization using Cisco Wide Area Application Services (WAAS) to accelerate and optimize data over a WAN network. Full deployment details are available in the Application Optimization Using Cisco WAAS Technology Design Guide.

You can configure NetFlow so that information can be gathered at multiple points along the path between a source and destination. When you use application optimization, the interface you select to monitor and the direction being monitored affect the data cached by the network device. The topology in Figure 5 illustrates the potential complexity.

You can monitor traffic bound for a remote site across the WAN in two places. The flows cached inbound on the LAN-facing interface reflect uncompressed data before being optimized by Cisco WAAS. The same flows when cached outbound on the WAN-facing interface reflect compressed data that has been optimized by Cisco WAAS.

Figure 5 - Application optimization and NetFlow



The recommendation for NetFlow with application optimization is to configure inbound and outbound flow monitoring on both the LAN-facing and WAN-facing interfaces. This ensures that all of the flow information is captured. The flow data that is collected on the LAN-facing interfaces provides an accurate view of the applications in use and their true network usage. The flow data that is collected on the WAN-facing interfaces accurately reflects the amount of network traffic that is transmitted and received to and from the WAN.

Tech Tip

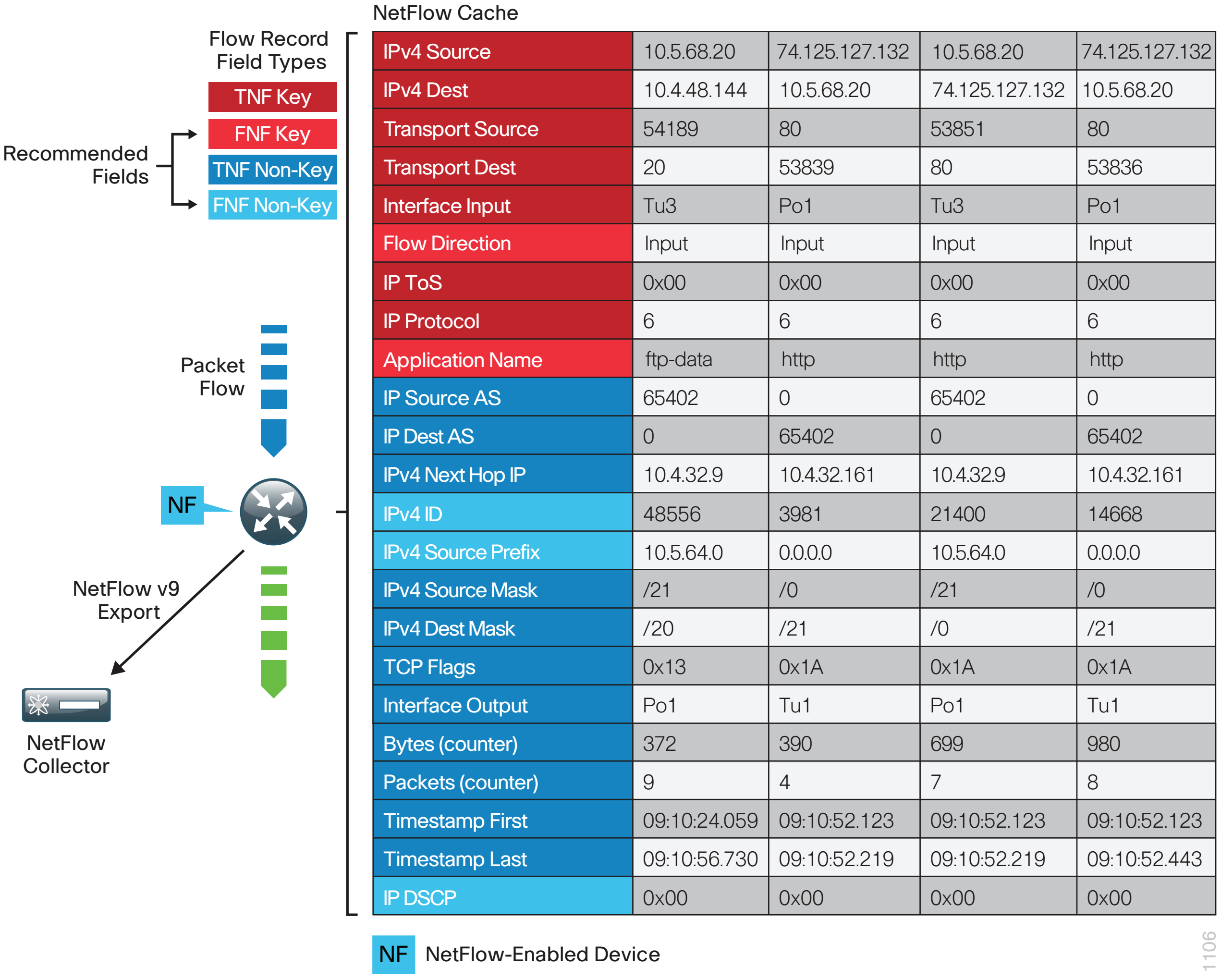
It is necessary to filter data during analysis depending on whether a LAN-facing or WAN-facing analysis is required.

Monitoring

The NetFlow data can be viewed directly from the NetFlow-enabled device through the use of CLI show commands, but this method is somewhat cumbersome, and it is difficult to correlate the data across multiple devices.

The flow details are exported to an external device running a flow collector service, as shown in Figure 6. The cached flow data is sent periodically, based upon configurable timers. The collector is capable of storing an extensive history of flow information that was switched within the NetFlow device. NetFlow is very efficient; the amount of export data is only a small percentage of the actual traffic in the router or switch. NetFlow accounts for every packet (when in non-sampled mode) and provides a highly condensed and detailed view of all network traffic that entered the router or switch. The NetFlow collector should be located in the server room or data center.

Figure 6 - NetFlow export to collector



IPv4 Source	10.5.68.20	74.125.127.132	10.5.68.20	74.125.127.132
IPv4 Dest	10.4.48.144	10.5.68.20	74.125.127.132	10.5.68.20
Transport Source	54189	80	53851	80
Transport Dest	20	53839	80	53836
Interface Input	Tu3	Po1	Tu3	Po1
Flow Direction	Input	Input	Input	Input
IP ToS	0x00	0x00	0x00	0x00
IP Protocol	6	6	6	6
Application Name	ftp-data	http	http	http
IP Source AS	65402	0	65402	0
IP Dest AS	0	65402	0	65402
IPv4 Next Hop IP	10.4.32.9	10.4.32.161	10.4.32.9	10.4.32.161
IPv4 ID	48556	3981	21400	14668
IPv4 Source Prefix	10.5.64.0	0.0.0.0	10.5.64.0	0.0.0.0
IPv4 Source Mask	/21	/0	/21	/0
IPv4 Dest Mask	/20	/21	/0	/21
TCP Flags	0x13	0x1A	0x1A	0x1A
Interface Output	Po1	Tu1	Po1	Tu1
Bytes (counter)	372	390	699	980
Packets (counter)	9	4	7	8
Timestamp First	09:10:24.059	09:10:52.123	09:10:52.123	09:10:52.123
Timestamp Last	09:10:56.730	09:10:52.219	09:10:52.219	09:10:52.443
IP DSCP	0x00	0x00	0x00	0x00

The most effective to way to view NetFlow data is through a dedicated analysis application, which is typically paired with the flow-collector service. The various applications are typically focused on traffic analysis, security (anomaly detection and denial of service), or billing. TNF-monitoring applications expect a standard set of fields to be exported. Each specific FNF-monitoring application will likely have a custom set of NetFlow attributes and a particular export format that must be configured on the NetFlow-enabled device before data can be sent to the collector.

The requirements for implementing FNF are highly dependent on which collector/analysis application you are using. In the Deployment Details section of this guide, example deployment guidance is provided for both TNF and FNF for the following applications.

Traditional NetFlow only:

- SolarWinds Orion NetFlow Traffic Analyzer (NTA)

Flexible NetFlow:

- ActionPacked! LiveAction
- Lancope StealthWatch
- Plixer Scrutinizer
- SevOne Network Management System (NMS)

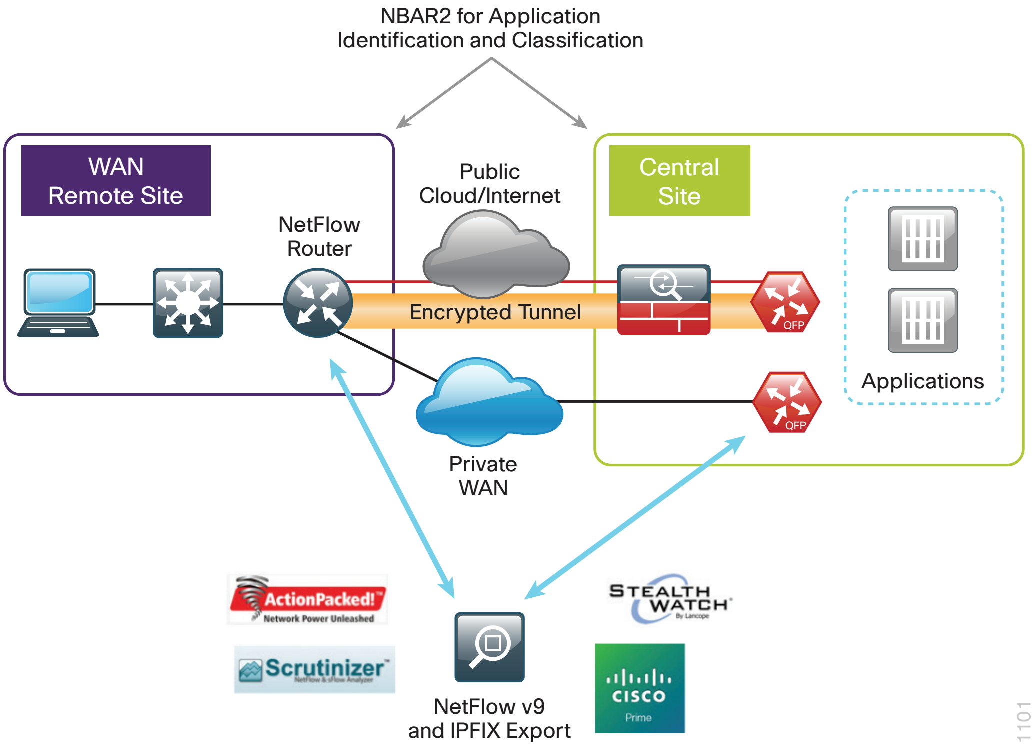
This guide uses these applications for the following reasons:

- Significant usage within a typical organization
- Dedicated focus on NetFlow analysis
- Ease of use
- Industry leadership with FNF support

This guide focuses on configuring TNF and FNF within a network topology and enables NetFlow on all devices that support FNF and NBAR with the tested hardware and software combinations. This includes the headquarters' WAN router and the remote-site routers.

Internet Protocol Flexible Export (IPFIX)

Internet Protocol Flow Information Export (IPFIX) is an IETF–defined, standards-based protocol for exporting IP flow information based on Cisco Netflow v9 and is sometimes referred to as Netflow v10.



The IPFIX export format enables several new capabilities that are not supported with NetFlow v9IPFIX, such as the ability to put multiple messages into a single datagram, allow vendor unique elements, and allow variable length strings.

Support for variable length fields becomes important when you need to export NBAR2 extracted fields. NBAR2's field extraction capability, such as HTTP URL, SIP domain, and Mail server, allows you to extract information for classification or exporting. When you need to export this type of information, you are required to use IPFIX.

Tech Tip

IPFIX is defined in RFC 5101/5102/5103 and is based on Cisco Netflow version 9 (RFC3954). IPFIX is supported for Cisco ISRG2 routers beginning with 15.2(4)M) M and for Cisco ASR1000 routers beginning with Cisco IOS XE Release 3.7S.

Cisco routers support two NetFlow configuration methods: a newer method, which is required for FNF deployments, and an older method, which is limited to TNF deployments only. This guide focuses on the newer method, which you can use to support both FNF and TNF deployment.

The WAN aggregation routers should monitor both the LAN-facing and WAN-facing interfaces, with the exception of port-channel interfaces on the Cisco ASR1000 Series, as shown in Figure 7. Remote-site routers should monitor WAN-facing interfaces and either access-layer or distribution-layer-facing interfaces, as shown in Figure 8. The specific data fields collected and the appropriate timer values used on the NetFlow-enabled devices are documented in the following procedures.

Figure 7 - Where to monitor NetFlow–WAN aggregation

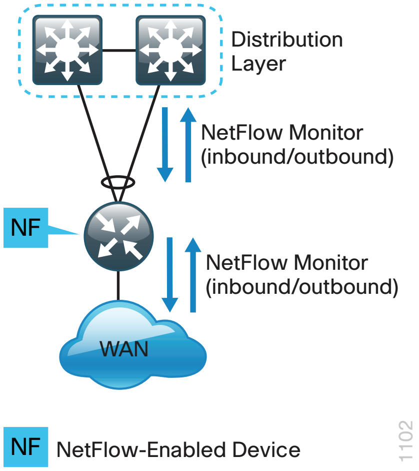
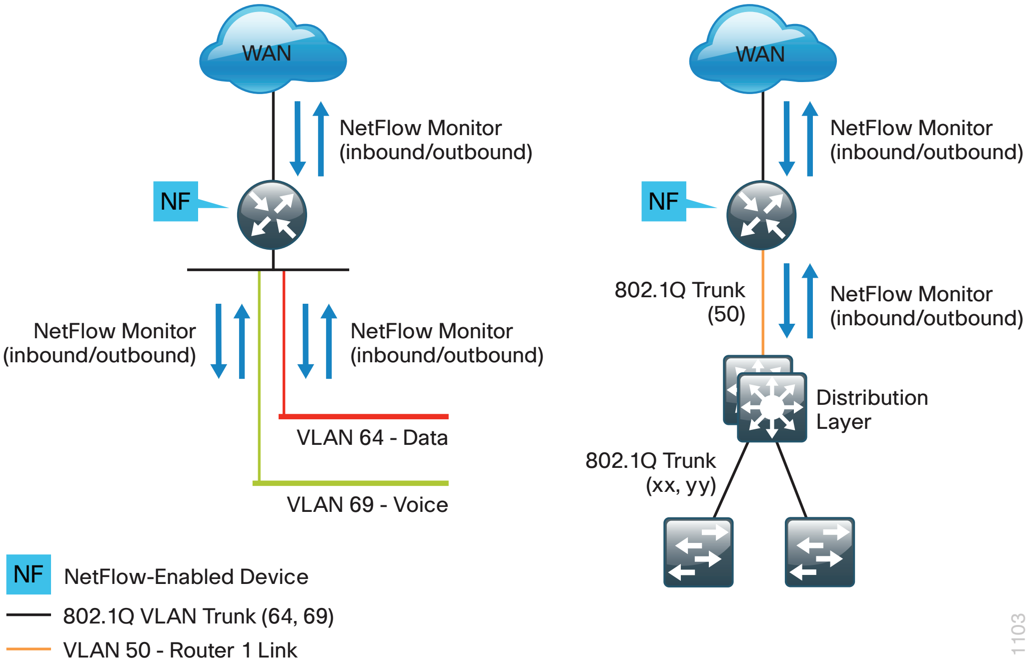

Distribution Layer
NetFlow Monitor (inbound/outbound)
NF
NetFlow Monitor (inbound/outbound)
WAN
NF NetFlow-Enabled Device
1102

Figure 8 - Where to monitor NetFlow–WAN remote sites


WAN
NetFlow Monitor (inbound/outbound)
NF
NetFlow Monitor (inbound/outbound)
NetFlow Monitor (inbound/outbound)
VLAN 64 - Data
VLAN 69 - Voice
NF NetFlow-Enabled Device
802.1Q VLAN Trunk (64, 69)
VLAN 50 - Router 1 Link
WAN
NetFlow Monitor (inbound/outbound)
NF
802.1Q Trunk (50)
NetFlow Monitor (inbound/outbound)
Distribution Layer
802.1Q Trunk (xx, yy)
1103

The following process must be completed to enable NetFlow data collection and optional data export:.

1. Create an FNF flow record or select a built-in flow record to use with TNF.
2. Create a flow exporter for each external NetFlow collector.
3. Create a flow monitor and associate it with either a custom or built-in flow record. You must also assign one or more flow exporters if you want the data to be analyzed on an external collector.
4. Assign the flow monitor to interfaces on the network device.

PROCESS

Installing NBAR2 Protocol Packs

1. Verify Cisco AVC licensing is active
2. Verify current NBAR information
3. Install or update the NBAR2 protocol pack

In order to ensure the most recent application definitions are available, you need to update the NBAR2 protocol packs. This process helped you to verify the proper Cisco IOS Software and Cisco AVC licensing is installed and explains how to check the status of the active NBAR protocol pack.

The NBAR2 protocol pack is available for download on the Cisco website in the same location as the Cisco IOS Software for the routers. NBAR2 protocol packs are created for every supported Cisco IOS and IOS XE release and they are dependent on the IOS/IOS XE release version. Once the new protocol pack and the proper Cisco AVC licensing are installed, all of the updated NBAR2 application definitions are available for use.

Procedure 1 Verify Cisco AVC licensing is active

Step 1: Verify the licensing is installed for Cisco AVC features. In this example, there is an active temporary license for “data9” features on the Cisco ISRG2 router.

```
RS240-3945#Show license

Index 4 Feature: datak9
Period left: 8 weeks 3 days
Period Used: 16 minutes 23 seconds
License Type: EvalRightToUse
License State: Active, In Use
License Count: Non-Counted
License Priority: Low
```

Tech Tip

If you do not have the proper licenses installed, you will receive errors when installing the protocol pack. NBAR2 requires the Cisco AVC feature license to load an NBAR2 Advanced protocol pack.

```
% NBAR Error: Advanced Protocol Pack cannot be loaded on top of
Standard Protocol Pack
```

Procedure 2 Verify current NBAR information

Verify the version and status of NBAR on the router before you update the NBAR2 protocol pack. This will determine the active protocol pack running on the router.

Step 1: Verify the current *active* NBAR protocol pack. The output shows “Standard Protocol Pack” without a protocol pack file name listed. This means the router is currently running an NBAR1 standard protocol pack that is integrated with the base Cisco IOS image.

```
RS240-3945#show ip nbar protocol-pack active

ACTIVE protocol pack:
Name:                            Standard Protocol Pack
Version:                         1.0
Publisher:                       Cisco Systems Inc.
```

If there is an NBAR2 protocol pack installed, you will see “Advanced Protocol Pack” and the filename and location of the protocol pack image that is installed and active:

```
ACTIVE protocol pack:
Name:        Advanced Protocol Pack
Version:     5.1
Publisher:   Cisco Systems Inc.
File:        flash0:/pp-adv-isrg2-152-4.M1-13-5.1.0.pack
```

Step 2: Verify the version of the NBAR software.

```
RS240-3945#sh ip nbar version | include software
NBAR software version:  13
```

Tech Tip

The NBAR software version represents the version of the Cisco IOS deep packet inspection engine used for NBAR2 to classify traffic. This is also referred to as the NBAR classification engine. This version is specific to the router platform and IOS image.

For verification purposes, the file name can be matched against the Cisco IOS version and the NBAR classification engine version.

In this NBAR protocol pack file name **pp-adv-isrg2-152-4.M1-13-5.1.0.pack**, the elements are broken down as follows:

pp—protocol pack

adv—advanced protocol pack

isrg2-152-4.M1—the Cisco ISRG2 platform and minimum version Cisco IOS 15.2(4)M1

13—the NBAR software or classification engine version

5.1.0—the protocol pack version for this base Cisco IOS train

It is recommended that you use the protocol pack that is a match for the classification engine and use the latest protocol pack for the Cisco IOS image.

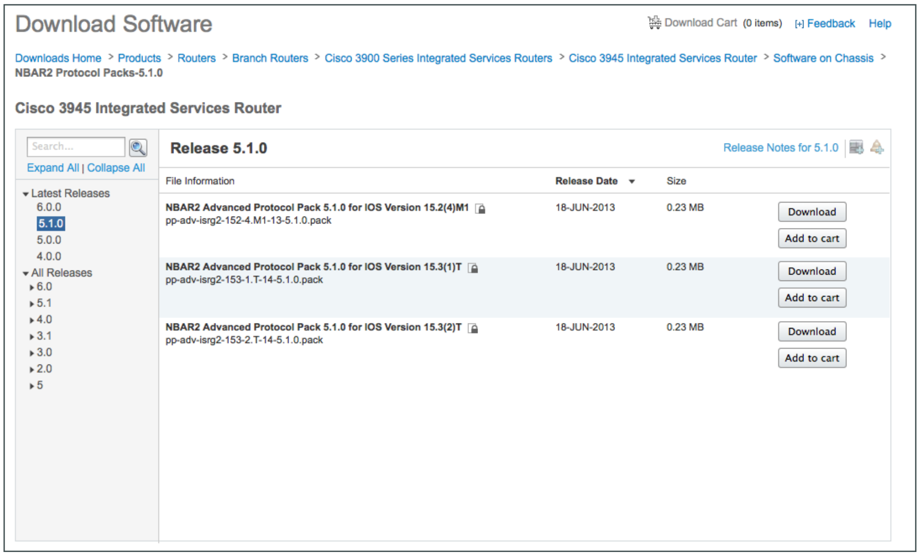
Procedure 3 Install or update the NBAR2 protocol pack

The following steps show an example for downloading and installing the NBAR2 protocol pack on a Cisco 3945 ISRG2 router. Download a protocol specific to the router platform you are using.

Step 1: In a browser, access http://www.cisco.com/, log in using your Cisco.com account name, and then navigate to **Support > All Downloads**.

Step 2: From the Download Home section, navigate to **Routers > Branch Routers Cisco 3900 series Integrated Services Routers > Cisco 3945 Integrated Services Router > Software on Chassis**, and then, under **Select a Software Type**, click **NBAR2 Protocol Packs**.

Step 3: Select the latest version for the Cisco IOS Software, and then click **Download** and copy this file to the router flash memory.



Download Software

Downloads Home > Products > Routers > Branch Routers > Cisco 3900 Series Integrated Services Routers > Cisco 3945 Integrated Services Router > Software on Chassis > NBAR2 Protocol Packs-5.1.0

Cisco 3945 Integrated Services Router

Release 5.1.0

File Information	Release Date	Size
NBAR2 Advanced Protocol Pack 5.1.0 for IOS Version 15.2(4)M1 pp-adv-isrg2-152-4.M1-13-5.1.0.pack	18-JUN-2013	0.23 MB
NBAR2 Advanced Protocol Pack 5.1.0 for IOS Version 15.3(1)T pp-adv-isrg2-153-1.T-14-5.1.0.pack	18-JUN-2013	0.23 MB
NBAR2 Advanced Protocol Pack 5.1.0 for IOS Version 15.3(2)T pp-adv-isrg2-153-2.T-14-5.1.0.pack	18-JUN-2013	0.23 MB

Step 4: From configuration mode, install the new protocol pack.

```
RS240-3945(config)# ip nbar protocol-pack flash0:/pp-adv-isrg2-152-4.
M1-13-5.1.0.pack
```

Tech Tip

During the protocol pack installation, protocol pack data forwarding will continue, but traffic is classified as unknown (ID:0) until the new protocol pack becomes active.

Loading times will differ depending on the platform. The router CLI will pause during the installation process after you press enter in order to install the protocol pack image.

On the Cisco ISRG2, it will take about 3 minutes to install the protocol pack.

On the Cisco ASR1K, it will take about 15-30 seconds to load the protocol pack.

If an incompatible protocol pack is accidentally installed on a router, it will be rejected. The router will display an error message saying the protocol pack is incompatible with underlying Cisco IOS NBAR software version. The previous protocol pack will remain active on device.

Step 5: Verify the new protocol pack is active.

```
RS240-3945#show ip nbar protocol-pack active

ACTIVE protocol pack:
Name:         Advanced Protocol Pack
Version:      5.1
Publisher:    Cisco Systems Inc.
File:         flash0:/pp-adv-isrg2-152-4.M1-13-5.1.0.pack
```

Tech Tip

If needed you can revert back to the default NBAR protocol pack installed with the Cisco IOS version running on the router by using the IOS command:

```
ip nbar default protocol-pack
```

PROCESS

Configuring Flexible NetFlow with NBAR2

1. Create flexible NetFlow flow record
2. Create flow exporter
3. Create a flow monitor
4. Apply flow monitor to WAN and LAN

These procedures include best practice recommendations for which key fields and non-key fields need to be collected in order to allow for effective application monitoring on your network. There are two sets of examples included. These examples illustrate how to integrate with NetFlow collectors that support only TNF, as well as NetFlow collectors that support FNF with integrated NBAR2.

Procedure 1 Create flexible NetFlow flow record

Flexible NetFlow (FNF) requires the explicit configuration of a flow record that consists of both key fields and non-key fields. This procedure provides guidance on how to configure a user-defined flow record that includes all of the TNF fields (key and non-key) as well as additional FNF fields (key and non-key). The resulting flow record includes the full subset of TNF fields used in classic NetFlow deployments.

Step 1: Specify key fields. This determines unique flow. Be sure to include a separate match statement for each key field.

Tech Tip

It is recommended that you use the TNF key fields, listed in Table 5, and the additional FNF key fields, listed in Table 6.

```
flow record [record name]
 description [record description]
 match [key field type] [key field value]
```

Table 5 - Recommended TNF key fields (TNF and FNF)

Key field type	Key field value
ipv4	tos protocol source address destination address
transport	source port destination port
interface	input
flow	sampler

Table 6 - Recommended additional FNF key fields (FNF only)

Key field type	Key field value	Comments
flow	direction	Allows for ingress/egress flow collection on same interface
application	name	Enables collection of NBAR information for each flow

Tech Tip

Adding the command **match application name** specifically enables NBAR integration for this flow record.

Step 2: Specify non-key fields to be collected for each unique flow. Be sure to include a separate collect statement for each non-key field.

Flexible NetFlow allows for the use of additional user specified non-key fields. It is recommended that you use the additional TNF non-key fields listed in Table 7, and the additional FNF non-key fields listed in Table 8.

```
flow record [record name]
 collect [non-key field type] [non-key field value]
```

Table 7 - Recommended TNF non-key fields (TNF and FNF)

Non-key field type	Non-key field value
routing	source as destination as next-hop address ipv4
ipv4	source mask destination mask
transport	tcp flags
Interface	output
counter	bytes packets
timestamp	sys-uptime first sys-uptime last

Table 8 - Recommended additional FNF non-key fields (FNF only)

Non-key field type	Key field value	Comments
ipv4	dscp id source prefix source mask	Additional IPv4 information for each flow

Example

```
flow record Record-FNF
 description Flexible NetFlow with NBAR Flow Record
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 match flow direction
 match application name
 collect routing source as
 collect routing destination as
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source prefix
 collect ipv4 source mask
 collect ipv4 destination mask
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
```

Procedure 2 Create flow exporter

The NetFlow data that is stored in the cache of the network device can be more effectively analyzed when exported to an external collector.

Creating a flow exporter is only required when exporting data to an external collector. This procedure may be skipped if data is analyzed only on the network device.

Reader Tip

Most external collectors use Simple Network Management Protocol (SNMP) to retrieve the interface table from the network device. Ensure that you have completed the relevant SNMP procedures for your platform.

WAN router procedures are listed in the MPLS WAN Technology Design Guide, Layer 2 WAN Technology Design Guide, or VPN WAN Technology Design Guide.

Different NetFlow collector applications support different export version formats (v5, v9 IPFIX) and expect to receive the exported data on a particular UDP or TCP port (ports 2055, 9991, 9995, 9996 are popular). The NetFlow RFC 3954 does not specify a specific port for collectors to receive Netflow data. In this deployment, the collector applications used for testing use the parameters designated in the following table.

Table 9 - Tested NetFlow collector parameters

Vendor	Application	Version	Export capability	Netflow destination port
ActionPacked	LiveAction	3.0	Flexible NetFlow v9	UDP 2055
Cisco	Prime Infrastructure	2.0	Flexible NetFlow v9, IPFIX	UDP 9991
Plixer	Scrutinizer	11.0.1.28644	Flexible NetFlow v9, IPFIX	UDP 2055
SevOne	Network Performance Management	5.2.3	Flexible NetFlow v9, IPFIX	UDP 9996
SolarWinds	Orion NetFlow Traffic Analyzer	3.11.0	Traditional NetFlow v9	UDP 2055
Lancope	StealthWatch	6.3.3	Flexible NetFlow v9, IPFIX	UDP 2055

Option 1: Configure Netflow v9 flow exporter

Step 1: Configure a basic flow exporter by using Netflow v9.

```
flow exporter [exporter name]
 description [exporter description]
 destination [NetFlow collector IP address]
 source Loopback0
 transport [UDP or TCP] [port number]
 export-protocol netflow
```

Option 2: Configure IPFIX flow exporter

IPFIX is the standards-based alternative method to export flows to an external collector. In some cases, IPFIX export is required when you need to export NBAR2 extracted fields such as URL or hostname. IPFIX as defined in RFC 5101 specifies that the collection process should be listening on port UDP 4739.

Tech Tip

Because not all collector application use UDP port 4739 as specified in the RFC, you must verify the correct port prior to the configuration of your NetFlow device.

If exporting flow data to Cisco Prime using IPFIX, use UDP port 9991 as with Netflow version 9.

Step 1: Configure basic flow exporter parameters specifying IPFIX as the export protocol using UDP port 4739 for transport.

```
flow exporter [exporter name]
 description [exporter description]
 destination [NetFlow collector IP address]
 source Loopback0
 transport UDP 4739
 export-protocol ipfix
```

Step 2: For FNF records, export the interface table for FNF. The **option interface-table** command enables the periodic sending of an options table. This provides interface names via NetFlow export.

```
flow exporter [exporter name]
 option interface-table
```

Step 3: If you are using an NBAR flow record, export the NBAR application table. The **option application-table** command enables the periodic sending of an options table that allows the collector to map the NBAR application IDs provided in the flow records to application names.

```
flow exporter [exporter name]
 option application-table
```

Step 4: If you are using an NBAR flow record, export the NBAR application attributes. The **option application-attributes** command causes the periodic sending of NBAR application attributes to the collector.

```
flow exporter [exporter name]
 option application-attributes
```

Step 5: If you are using the Cisco ISR-G2 series routers, enable **output-features**. Otherwise, NetFlow traffic that originates from a WAN remote-site router will not be encrypted or tagged using QoS.

```
flow exporter [exporter name]
 output-features
```

Example: FNF with Plixer

```
flow exporter Export-FNF-Plixer
 description FNF v9
 destination 10.4.48.171
 source Loopback0
 output-features    ! this command is not required on IOS-XE routers
 transport udp 2055
 export-protocol netflow-v9
 option interface-table
 option application-table
```

Example: TNF with SolarWinds

```
flow exporter Export-TNF-Solarwinds
 description TNF v9
 destination 10.4.48.173
 output-features    ! this command is not required on IOS-XE routers
 source Loopback0
 transport udp 2055
 export-protocol netflow-v9
```

Step 6: Verify Netflow Exporter configuration.

```
RS240-3945#sh flow exporter Export-FNF-Plixer

Flow Exporter Export-FNF-Plixer:
  Description:              IPFIX-NBAR2
  Export protocol:          IPFIX (Version 10)
  Transport Configuration:
    Destination IP address: 10.4.48.171
    Source IP address:      10.255.251.240
    Source Interface:       Loopback0
    Transport Protocol:     UDP
    Destination Port:       4739
    Source Port:            55474
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
  Options Configuration:
    interface-table (timeout 600 seconds)
    application-table (timeout 600 seconds)
    application-attributes (timeout 600 seconds)
```

Step 7: If you need to view the exporter options “application-table” information that is available for export, you can show a list of all of the available application IDs and names for reference.

```
RS240-3945#show flow exporter option application table

Engine: prot (IANA_L3_STANDARD, ID: 1)

appID  Name                         Description
-----  ----                         -----------
1:8    egp                          Exterior Gateway Protocol
1:47   gre                          General Routing Encapsulation
1:1    icmp                         Internet Control Message Protocol
1:88   eigrp                        Enhanced Interior Gateway Routing Protocol
1:4    ipinip                       IP in IP
1:89   ospf                         Open Shortest Path First
1:46   rsvp                         Resource Reservation Protocol
1:0    hopopt                       DEPRECATED, traffic will not match
1:3    ggp                          Gateway-to-Gateway
```

Procedure 3 Create a flow monitor

The network device must be configured to monitor the flows through the device on a per-interface basis. The flow monitor must include a flow record and optionally one or more flow exporters if data is to be collected and analyzed. After the flow monitor is created, it is applied to device interfaces. The flow monitor stores flow information in a cache, and the timer values for this cache are modified within the flow monitor configuration. It is recommended that you set the timeout active timer to 60 seconds, which exports flow data on existing long-lived flows.

Step 1: Create the flow monitor, and then set the cache timers.

```
flow monitor [monitor name]
 description [monitor description]
 cache timeout active 60
```

Step 2: Associate the flow record to the flow monitor. You can use either a custom or a built-in flow record.

```
flow monitor [monitor name]
 record [record name]
```

Step 3: If you are using an external NetFlow collector, associate the exporters to the flow monitor. If you are using multiple exporters, add additional lines.

```
flow monitor [monitor name]
 exporter [exporter name]
```

Example: FNF with Plixer

```
flow monitor Monitor-FNF
 description FNF/NBAR Application Traffic Analysis
 record Record-FNF
 exporter Export-FNF-Plixer
 cache timeout active 60
```

Example: TNF using a predefined record with SolarWinds

Tech Tip

netflow ipv4 original-input is a predefined built-in record that emulates the classic CLI for TNF.

```
flow monitor Monitor-TNF
 description TNF Traffic Analysis
 record netflow ipv4 original-input
 exporter Export-TNF-Solarwinds
 cache timeout active 60
```

Step 4: Verify Flow monitor configuration.

```
RS240-3945#sh flow monitor

Flow Monitor Monitor-FNF:
  Description:       FNF/NBAR Application Traffic Analysis
  Flow Record:       Record-FNF
  Flow Exporter:     Export-FNF-Lancope
                     Export-FNF-Prime20
                     Export-FNF-Plixer
                     Export-FNF-Action-Packed
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 376856 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    60 secs
    Update Timeout:    1800 secs

Flow Monitor Monitor-TNF:
  Description:       TNF Traffic Analysis
  Flow Record:       netflow ipv4 original-input
  Flow Exporter:     Export-TNF-Solarwinds
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 344088 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    60 secs
    Update Timeout:    1800 secs
```

Procedure 4 Apply flow monitor to WAN and LAN

A best practice for NetFlow is to monitor all inbound and outbound traffic to the network device. This method covers all traffic regardless of encryption or application optimization.

Tech Tip

Be sure to apply the flow monitor to all device interfaces, including port-channel, tunnel, and sub-interfaces.

Step 1: Apply the flow monitor to the device interface.

```
interface [name]
 ip flow monitor [monitor name] input
 ip flow monitor [monitor name] output
```

Example: FNF

```
interface GigabitEthernet0/0
 description MPLS WAN Uplink
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-FNF output
interface GigabitEthernet0/2.64
 description Wired Data
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-FNF output
```

Example: TNF

```
interface GigabitEthernet0/0
 description MPLS WAN Uplink
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-TNF output
interface GigabitEthernet0/2.64
 description Wired Data
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-TNF output
```

Step 2: Verify the proper interfaces are configured for Netflow monitoring.

```
RS240-3945#sh flow interface

Interface GigabitEthernet0/0
  FNF:  monitor:          Monitor-FNF
        direction:        Input
        traffic(ip):      on
  FNF:  monitor:          Monitor-FNF
        direction:        Output
        traffic(ip):      on
```

```
Interface GigabitEthernet0/1
  FNF:  monitor:          Monitor-FNF
        direction:        Input
        traffic(ip):      on
  FNF:  monitor:          Monitor-FNF
        direction:        Output
        traffic(ip):      on
```

PROCESS

Monitoring IOS NetFlow Data

1. View raw flow data unfiltered
2. Filter and view flow data

The data stored in the cache of the network device can be viewed in a number of different ways to address common-use cases. These methods are covered briefly to provide examples of how to access the flow data.

Procedure 1 View raw flow data unfiltered

The simplest method to view the NetFlow cache is via the following command, which provides a summary of the cache status followed by a series of individual cache entries.

Step 1: Display the NetFlow cache.

```
show flow monitor [monitor name] cache
```

Example

```
Router#show flow monitor Monitor-FNF cache
  Cache type:                                Normal
  Cache size:                                 4096
  Current entries:                              55
  High Watermark:                             4096
  Flows added:                             2188410
  Flows aged:                              2188355
    - Active timeout      (    60 secs)     153722
    - Inactive timeout    (    15 secs)    1984047
    - Event aged                                 0
    - Watermark aged                         37846
    - Emergency aged                         12740
IPV4 SOURCE ADDRESS:       10.11.4.10
IPV4 DESTINATION ADDRESS:  172.16.50.80
TRNS SOURCE PORT:          52790
TRNS DESTINATION PORT:     80
INTERFACE INPUT:           Po1.64
FLOW DIRECTION:            Input
IP TOS:                    0x00
IP PROTOCOL:                6
APPLICATION NAME:           nbar http
ipv4 next hop address:      192.168.6.134
ipv4 id:                    355
ipv4 source prefix:         10.11.4.0
ipv4 source mask:           /24
ipv4 destination mask:      /0
tcp flags:                  0x18
interface output:           Gi0/0
counter bytes:              2834
counter packets:            38
timestamp first:            14:30:03.102
timestamp last:             14:30:03.734
ip dscp:                    0x00
```

Procedure 2 Filter and view flow data

(Optional)

If you know specific fields, such as the source or destination IP address or the TCP or UDP port number, then you can search the cache for exact matches or use regular expressions for broader match criteria.

Step 1: Display the filtered NetFlow cache.

```
show flow monitor [monitor name] cache filter [filter parameters]
```

Table 10 - NetFlow cache filter parameters

Field type	Available parameters
application	name **[value]**
counter	bytes **[value]** flows **[value]** packets **[value]**
flow	direction input direction output
interface	input **[interface type][number]** output **[interface type][number]**
IPv4	destination address **[value]** destination mask **[value]** dscp **[value]** id **[value]** protocol **[value]** source address **[value]** source mask **[value]** tos **[value]**
routing	next-hop address ipv4 **[value]**
timestamp	sys-uptime first **[value]** sys-uptime last **[value]**
transport	destination-port **[value]** source-port **[value]** tcp flags **[value]**

Example

The following Cisco ISR IOS command shows how to verify that RTP streams have the proper QoS differentiated-services code point (DSCP) settings.

Tech Tip

Interactive video is configured to use DSCP cs4 and af41.

cs4 = 0x20
af41 = 0x22

```
Router#show flow monitor Monitor-FNF cache filter application name regexp rtp
      IPV4 SOURCE ADDRESS:        10.11.4.40
      IPV4 DESTINATION ADDRESS:   10.10.48.27
      TRNS SOURCE PORT:           2454
      TRNS DESTINATION PORT:      51124
      INTERFACE INPUT:            Gi0/0
      FLOW DIRECTION:             Input
      IP TOS:                     0x88
      IP PROTOCOL:                17
      APPLICATION NAME:           nbar rtp
      ipv4 next hop address:      10.10.32.1
      ipv4 id:                    0
```

```
ipv4 source prefix:        10.11.0.0
ipv4 source mask:          /16
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Po32
counter bytes:             875384
counter packets:           2391
timestamp first:           15:32:52.027
timestamp last:            15:33:39.827
ip dscp:                   0x22
```

Step 2: Sort and format flow data.

The same fields that are available for searching the NetFlow cache are also available as simple sort fields. You can select any parameter from Table 11 and sort from either highest to lowest or lowest to highest. Additionally, you can format the command output in multiple ways, as listed in Table 12, with the table output being most suitable for determining top traffic sources or destinations.

```
show flow monitor [monitor name] cache sort [filter parameters]
```

Table 11 - NetFlow cache sort parameters

Field type	**Available parameters**
application	Name
counter	bytes flows packets
flow	direction input direction output
highest (default)	–
interface	input **[interface type][number]** output **[interface type][number]**
IPv4	destination address **[value]** destination mask **[value]** dscp **[value]** id **[value]** protocol **[value]** source address **[value]** source mask **[value]** tos **[value]**
lowest	–
routing	next-hop address ipv4 **[value]**
timestamp	sys-uptime first **[value]** sys-uptime last **[value]**
transport	destination-port **[value]** source-port **[value]** tcp flags **[value]**

Table 12 - NetFlow cache output formats

Format type	Available parameters
csv	Suitable for cut/paste export
record (default)	Best for viewing individual cache entries
table	Suitable for on-screen display (requires 316 character width)

Example

The following command shows how to view the cache sorted by **counter bytes** and formatted as a table for on-screen viewing.

```
Router#show flow monitor Monitor-FNF cache sort counter bytes format table
```

The following example shows partial output from the **show flow monitor** command. For an example of the full output, go to http://cvddocs.com/fw/130-a-13.

```
Router#show flow monitor Monitor-FNF cache sort counter bytes format table
Processed 57 flows
Aggregated to 57 flows
Showing the top 20 flows

IPV4 SRC ADDR    IPV4 DST ADDR    TRNS SRC PORT  TRNS DST PORT...
===============  ===============  =============  =============...
10.10.48.27      10.11.4.40               51128           2456...
10.11.4.40       10.10.48.27               2456          51128...
10.10.48.27      10.11.4.40               51124           2454...
10.11.4.40       10.10.48.27               2454          51124...
10.11.4.40       10.10.48.27               2457          51129...
.                .                            .              .
.                .                            .              .
.                .                            .              .
```

PROCESS

Viewing Netflow Collector Data

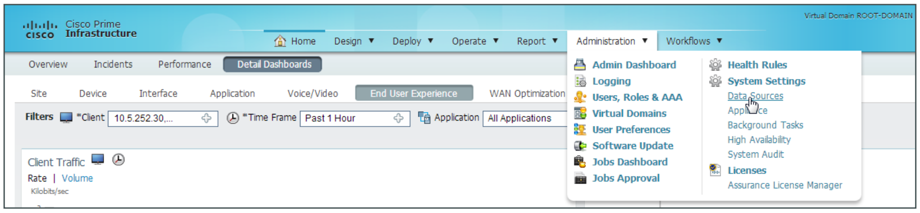
1. Use Cisco Prime for IOS Netflow Reporting
2. Review reports from third party NetFlow collectors

Netflow data can be exported to one or multiple collectors for detailed traffic analysis and reporting.

Procedure 1 Use Cisco Prime for IOS Netflow Reporting

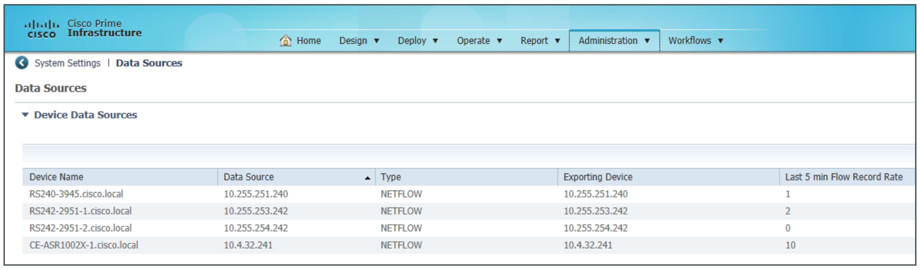
This procedure assumes NetFlow configuration on the router has been completed and NetFlow data is being exported to Cisco prime.

Step 1: In the Cisco Prime interface, go to **Administration>System Settings>Data Sources** and ensure the data source is shown for the Cisco IOS devices sending flow data.



Filters *Client 10.5.252.30,... *Time Frame Past 1 Hour Application All Applications

Step 2: Verify that the Device Name is shown in the list as an Exporting device, and then, in the **Last 5 Min Flow Record Rate** column, verify that data is being collected. A value of zero indicates that no NetFlow data is being received by Cisco Prime.



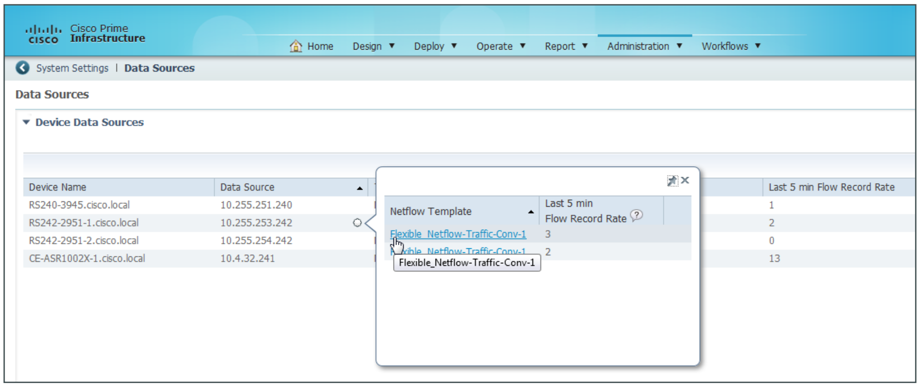
Data Sources

Device Data Sources

Device Name	Data Source	Type	Exporting Device	Last 5 min Flow Record Rate
RS240-3945.cisco.local	10.255.251.240	NETFLOW	10.255.251.240	1
RS242-2951-1.cisco.local	10.255.253.242	NETFLOW	10.255.253.242	2
RS242-2951-2.cisco.local	10.255.254.242	NETFLOW	10.255.254.242	0
CE-ASR1002X-1.cisco.local	10.4.32.241	NETFLOW	10.4.32.241	10

Next, verify and view RAW Netflow Data for a unique data source.

Step 3: Place the cursor over the **Data Source** IP address and right-click the bubble that appears in that column. This identifies the NetFlow conversation associated with this device.



Data Sources

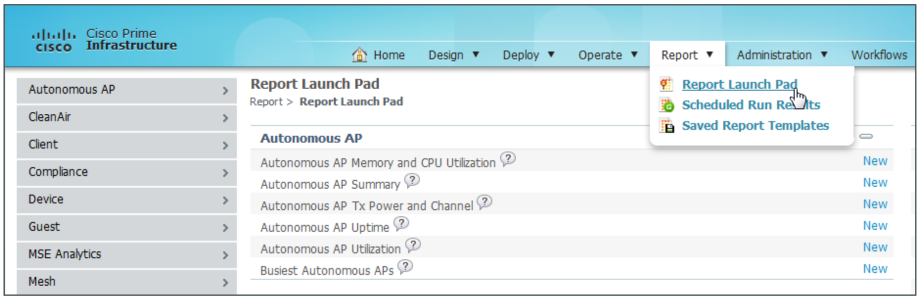
Device Data Sources

Device Name	Data Source	Last 5 min Flow Record Rate
RS240-3945.cisco.local	10.255.251.240	1
RS242-2951-1.cisco.local	10.255.253.242	2
RS242-2951-2.cisco.local	10.255.254.242	0
CE-ASR1002X-1.cisco.local	10.4.32.241	13

Netflow Template	Last 5 min Flow Record Rate
Flexible_Netflow-Traffic-Conv-1	3
...xible_Netflow-Traffic-Conv-1	2

Flexible_Netflow-Traffic-Conv-1

Step 4: Go to **Reports > Report Launch Pad**.



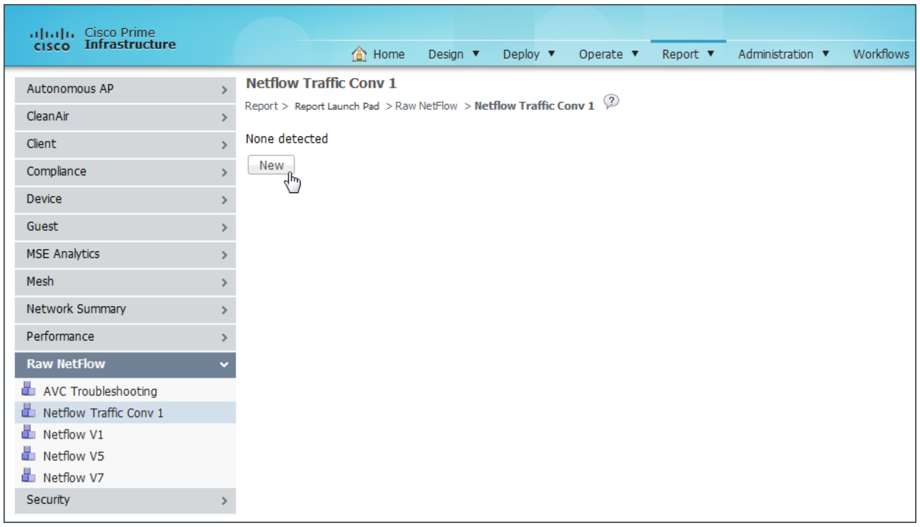
Report Launch Pad

Report > Report Launch Pad

Autonomous AP

Autonomous AP Memory and CPU Utilization	New
Autonomous AP Summary	New
Autonomous AP Tx Power and Channel	New
Autonomous AP Uptime	New
Autonomous AP Utilization	New
Busiest Autonomous APs	New

Step 5: On the left side of the page, click **Raw NetFlow**, highlight the conversation identified in the previous step, and then click **New**.

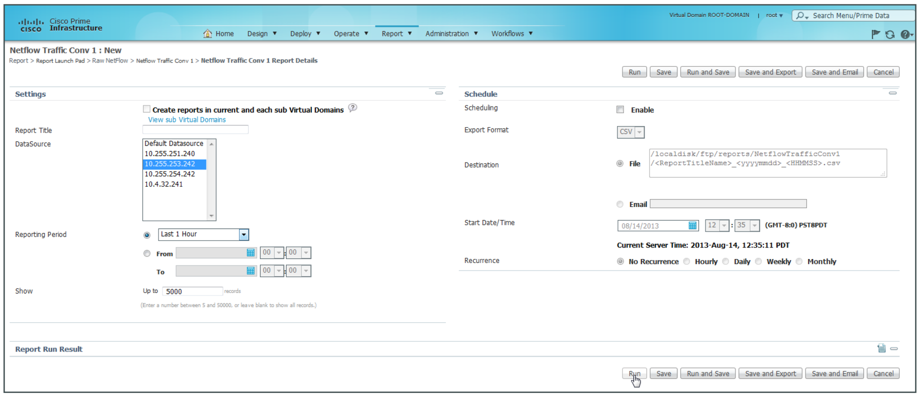


Netflow Traffic Conv 1

Report > Report Launch Pad > Raw NetFlow > Netflow Traffic Conv 1

None detected

Step 6: Select the **Data Source** and **Reporting Period**, and then click **Run** to generate the raw NetFlow report for this device.



Netflow Traffic Conv 1 : New

Report > Report Launch Pad > Raw NetFlow > Netflow Traffic Conv 1 > Netflow Traffic Conv 1 Report Details

Settings

□ Create reports in current and each sub Virtual Domains

View sub Virtual Domains

Report Title

DataSource: Default Datasource / 10.255.251.240 / **10.255.253.242** / 10.255.254.242 / 10.4.32.241

Reporting Period: ● Last 1 Hour
○ From 00 : 00
To 00 : 00

Show: Up to 5000 records

(Enter a number between 5 and 50000, or leave blank to show all records.)

Schedule

Scheduling: □ Enable

Export Format: CSV

Destination: ● File /localdisk/ftp/reports/NetflowTrafficConv1/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.csv

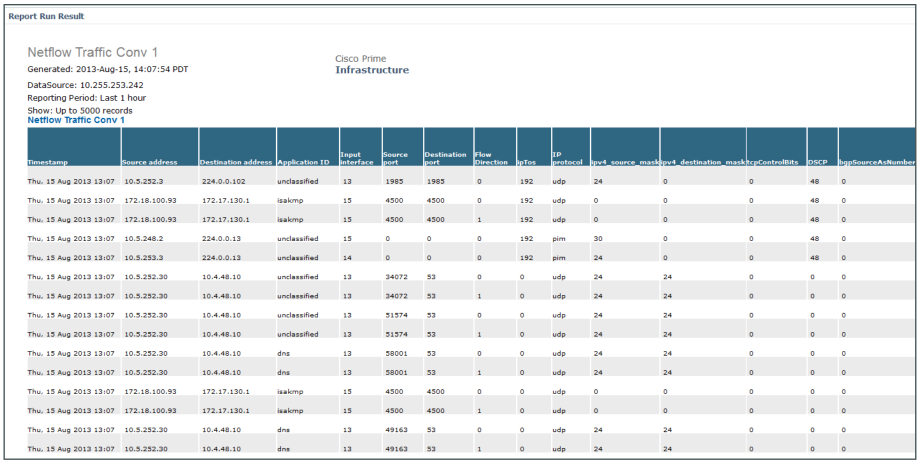
○ Email

Start Date/Time: 08/14/2013 12 : 35 (GMT-8:0) PST8PDT

Current Server Time: 2013-Aug-14, 12:35:11 PDT

Recurrence: ● No Recurrence ○ Hourly ○ Daily ○ Weekly ○ Monthly

Report Run Result



Report Run Result

Netflow Traffic Conv 1

Generated: 2013-Aug-15, 14:07:54 PDT

DataSource: 10.255.253.242

Reporting Period: Last 1 hour

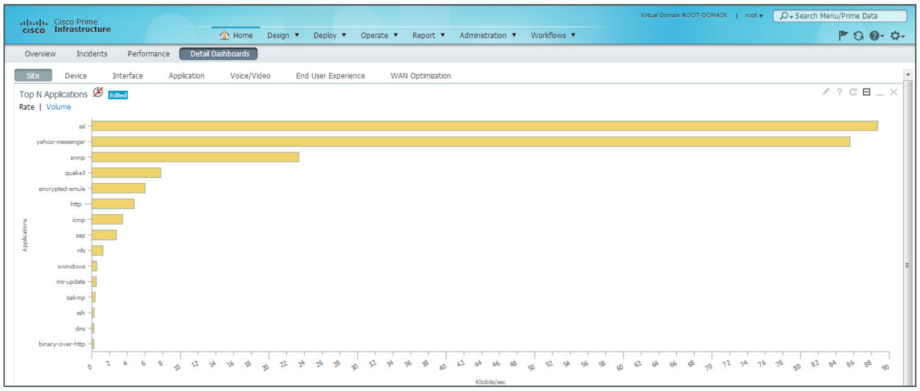
Show: Up to 5000 records

Cisco Prime Infrastructure

Netflow Traffic Conv 1

Timestamp	Source address	Destination address	Application ID	Input interface	Source port	Destination port	Flow Direction	ipTos	IP protocol	ipv4_source_mask	ipv4_destination_mask	tcpControlBits	DSCP	bgpSourceAsNumber
Thu, 15 Aug 2013 13:07	10.5.252.3	224.0.0.102	unclassified	13	1985	1985	0	192	udp	24	0	0	48	0
Thu, 15 Aug 2013 13:07	172.18.100.93	172.17.130.1	isakmp	15	4500	4500	0	192	udp	0	0	0	48	0
Thu, 15 Aug 2013 13:07	172.18.100.93	172.17.130.1	isakmp	15	4500	4500	1	192	udp	0	0	0	48	0
Thu, 15 Aug 2013 13:07	10.5.248.2	224.0.0.13	unclassified	15	0	0	0	192	pim	30	0	0	48	0
Thu, 15 Aug 2013 13:07	10.5.253.3	224.0.0.13	unclassified	14	0	0	0	192	pim	24	0	0	48	0
Thu, 15 Aug 2013 13:07	10.5.252.30	10.4.48.10	unclassified	13	34072	53	0	0	udp	24	24	0	0	0
Thu, 15 Aug 2013 13:07	10.5.252.30	10.4.48.10	unclassified	13	34072	53	1	0	udp	24	24	0	0	0
Thu, 15 Aug 2013 13:07	10.5.252.30	10.4.48.10	unclassified	13	51574	53	0	0	udp	24	24	0	0	0
Thu, 15 Aug 2013 13:07	10.5.252.30	10.4.48.10	unclassified	13	51574	53	1	0	udp	24	24	0	0	0
Thu, 15 Aug 2013 13:07	10.5.252.30	10.4.48.10	dns	13	58001	53	0	0	udp	24	24	0	0	0
Thu, 15 Aug 2013 13:07	10.5.252.30	10.4.48.10	dns	13	58001	53	1	0	udp	24	24	0	0	0
Thu, 15 Aug 2013 13:07	172.18.100.93	172.17.130.1	isakmp	15	4500	4500	0	0	udp	0	0	0	0	0
Thu, 15 Aug 2013 13:07	172.18.100.93	172.17.130.1	isakmp	15	4500	4500	1	0	udp	0	0	0	0	0
Thu, 15 Aug 2013 13:07	10.5.252.30	10.4.48.10	dns	13	49163	53	0	0	udp	24	24	0	0	0
Thu, 15 Aug 2013 13:07	10.5.252.30	10.4.48.10	dns	13	49163	53	1	0	udp	24	24	0	0	0

Step 7: On Cisco Prime, go to **Home > Detail Dashboards > Site** and look at the **Top N Applications**. The list of applications identified is displayed.

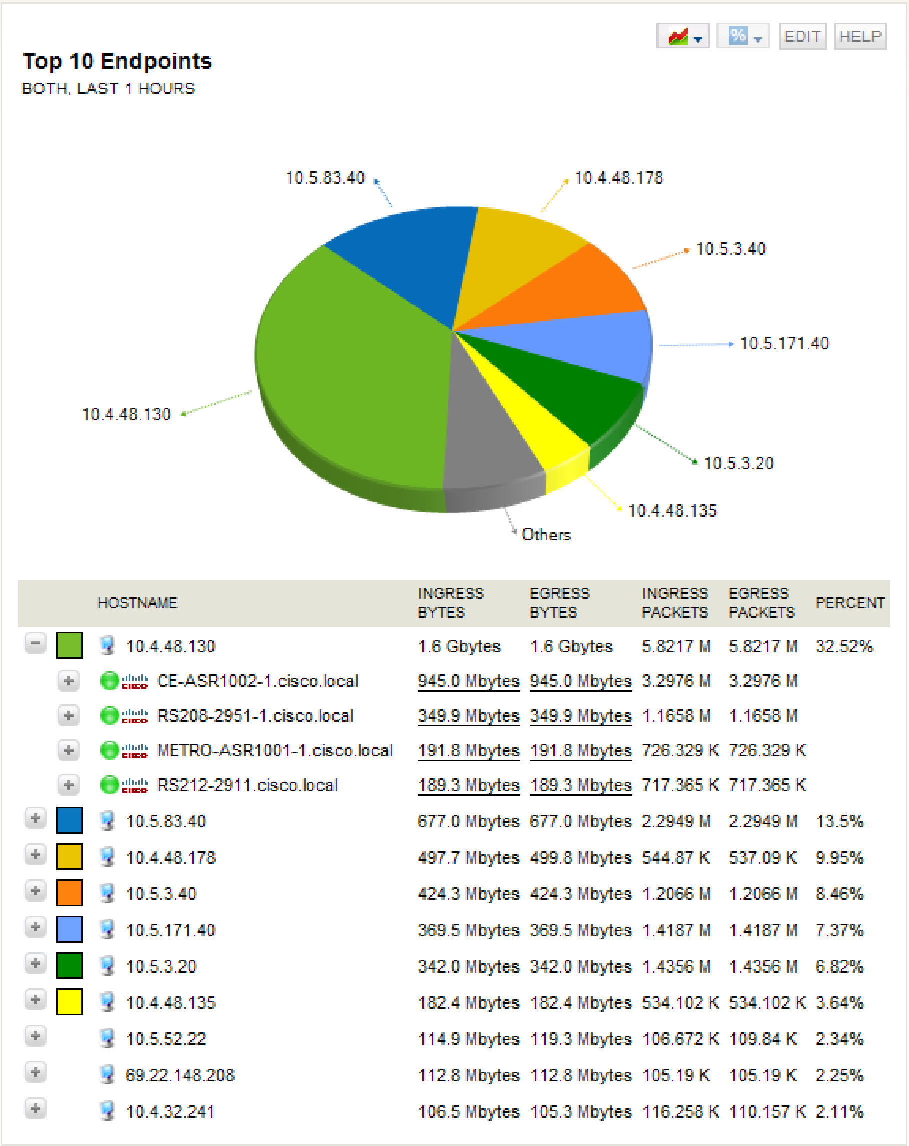


Procedure 2 Review reports from third party NetFlow collectors

This procedure highlights the types of reports that are available from Plixer Scrutinizer and SolarWinds Orion NTA.

One key advantage of using an external collector is the ability to aggregate the information collected across multiple network devices. A good collector provides the ability to view data collected from a particular device and interface, as well as correlate data collected across multiple devices and interfaces across the network.

Figure 9 - SolarWinds Orion NTA endpoint summary



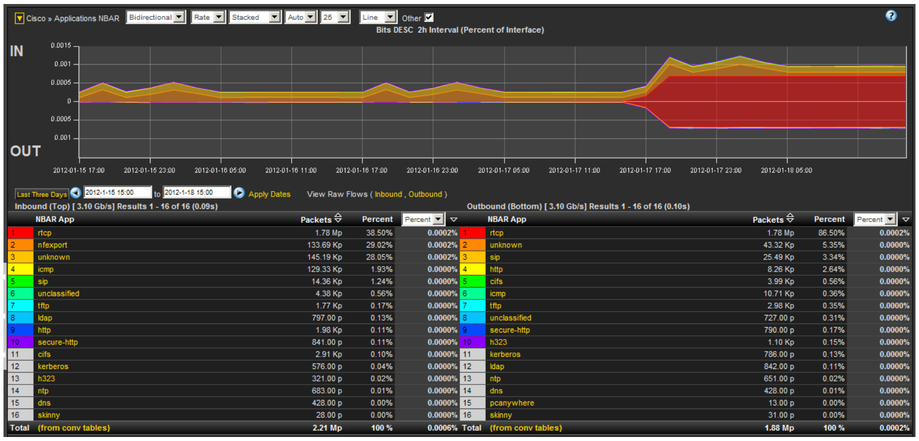
Top 10 Endpoints

BOTH, LAST 1 HOURS

		HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
−	🟩	10.4.48.130	1.6 Gbytes	1.6 Gbytes	5.8217 M	5.8217 M	32.52%
+		CE-ASR1002-1.cisco.local	945.0 Mbytes	945.0 Mbytes	3.2976 M	3.2976 M	
+		RS208-2951-1.cisco.local	349.9 Mbytes	349.9 Mbytes	1.1658 M	1.1658 M	
+		METRO-ASR1001-1.cisco.local	191.8 Mbytes	191.8 Mbytes	726.329 K	726.329 K	
+		RS212-2911.cisco.local	189.3 Mbytes	189.3 Mbytes	717.365 K	717.365 K	
+	🟦	10.5.83.40	677.0 Mbytes	677.0 Mbytes	2.2949 M	2.2949 M	13.5%
+	🟨	10.4.48.178	497.7 Mbytes	499.8 Mbytes	544.87 K	537.09 K	9.95%
+	🟧	10.5.3.40	424.3 Mbytes	424.3 Mbytes	1.2066 M	1.2066 M	8.46%
+	🟦	10.5.171.40	369.5 Mbytes	369.5 Mbytes	1.4187 M	1.4187 M	7.37%
+	🟩	10.5.3.20	342.0 Mbytes	342.0 Mbytes	1.4356 M	1.4356 M	6.82%
+	🟨	10.4.48.135	182.4 Mbytes	182.4 Mbytes	534.102 K	534.102 K	3.64%
+		10.5.52.22	114.9 Mbytes	119.3 Mbytes	106.672 K	109.84 K	2.34%
+		69.22.148.208	112.8 Mbytes	112.8 Mbytes	105.19 K	105.19 K	2.25%
+		10.4.32.241	106.5 Mbytes	105.3 Mbytes	116.258 K	110.157 K	2.11%

The NetFlow data, cached locally on the network device, is relatively short lived and is typically aged-out by new flows within minutes. An external collector is essential to maintain a long-term view of the traffic patterns on a network. The applications in use are most accurately determined by using FNF and NBAR.

Figure 10 - Plixer Scrutinizer–applications NBAR report (72-hour timespan)



2012-1-15 15:00 to 2012-1-18 15:00

Inbound (Top) [3.10 Gb/s] Results 1 - 16 of 16 (0.09s)

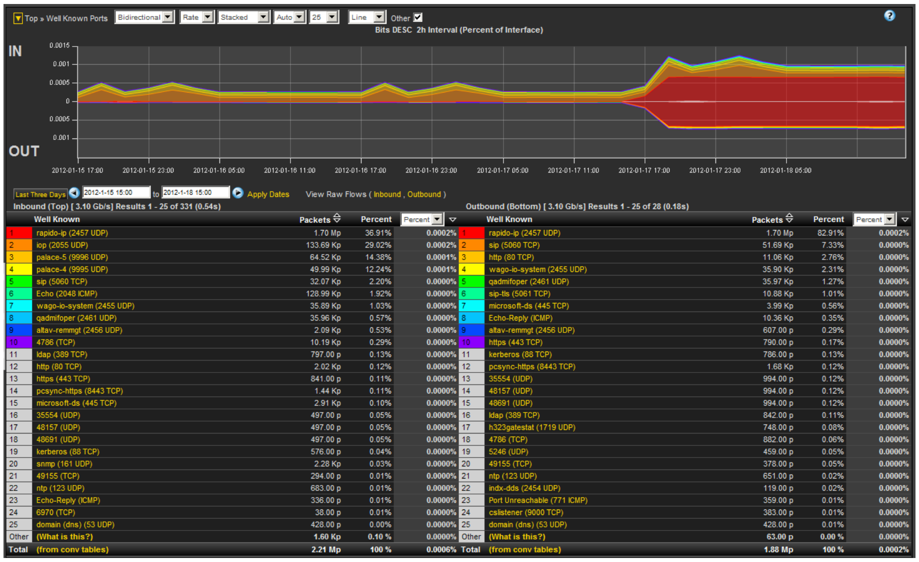
	NBAR App	Packets	Percent	Percent
1	rtcp	1.78 Mp	38.50%	0.0002%
2	nfexport	133.69 Kp	29.02%	0.0002%
3	unknown	145.19 Kp	28.05%	0.0002%
4	icmp	129.33 Kp	1.93%	0.0000%
5	sip	14.36 Kp	1.24%	0.0000%
6	unclassified	4.38 Kp	0.56%	0.0000%
7	tftp	1.77 Kp	0.17%	0.0000%
8	ldap	797.00 p	0.13%	0.0000%
9	http	1.98 Kp	0.11%	0.0000%
10	secure-http	841.00 p	0.11%	0.0000%
11	cifs	2.91 Kp	0.10%	0.0000%
12	kerberos	576.00 p	0.04%	0.0000%
13	h323	321.00 p	0.02%	0.0000%
14	ntp	683.00 p	0.01%	0.0000%
15	dns	428.00 p	0.00%	0.0000%
16	skinny	28.00 p	0.00%	0.0000%
Total	(from conv tables)	2.21 Mp	100 %	0.0006%

Outbound (Bottom) [3.10 Gb/s] Results 1 - 16 of 16 (0.10s)

	NBAR App	Packets	Percent	Percent
1	rtcp	1.78 Mp	86.50%	0.0002%
2	unknown	43.32 Kp	5.35%	0.0000%
3	sip	25.49 Kp	3.34%	0.0000%
4	http	8.26 Kp	2.64%	0.0000%
5	cifs	3.99 Kp	0.56%	0.0000%
6	icmp	10.71 Kp	0.36%	0.0000%
7	tftp	2.98 Kp	0.35%	0.0000%
8	unclassified	727.00 p	0.31%	0.0000%
9	secure-http	790.00 p	0.17%	0.0000%
10	h323	1.10 Kp	0.15%	0.0000%
11	kerberos	786.00 p	0.13%	0.0000%
12	ldap	842.00 p	0.11%	0.0000%
13	ntp	651.00 p	0.02%	0.0000%
14	dns	428.00 p	0.01%	0.0000%
15	pcanywhere	13.00 p	0.00%	0.0000%
16	skinny	31.00 p	0.00%	0.0000%
Total	(from conv tables)	1.88 Mp	100 %	0.0002%

To fully illustrate the value of NBAR to identify applications requires a comparison, because TNF can only identify applications through the use of either TCP or UDP well-known port (WKP). Since Plixer supports FNF and NBAR, as well as TNF, you can generate the same report by using WKP.

Figure 11 - Plixer Scrutinizer WKP report (72-hour timespan)



2012-1-15 15:00 to 2012-1-18 15:00

Inbound (Top) [3.10 Gb/s] Results 1 - 25 of 331 (0.54s)

	Well Known	Packets	Percent	Percent
1	rapido-ip (2457 UDP)	1.70 Mp	36.91%	0.0002%
2	iop (2055 UDP)	133.69 Kp	29.02%	0.0002%
3	palace-5 (9996 UDP)	64.52 Kp	14.38%	0.0001%
4	palace-4 (9995 UDP)	49.99 Kp	12.24%	0.0001%
5	sip (5060 TCP)	32.07 Kp	2.20%	0.0000%
6	Echo (2048 ICMP)	128.99 Kp	1.92%	0.0000%
7	wago-io-system (2455 UDP)	35.89 Kp	1.03%	0.0000%
8	qadmifoper (2461 UDP)	35.96 Kp	0.57%	0.0000%
9	altav-remmgt (2456 UDP)	2.09 Kp	0.53%	0.0000%
10	4786 (TCP)	10.19 Kp	0.29%	0.0000%
11	ldap (389 TCP)	797.00 p	0.13%	0.0000%
12	http (80 TCP)	2.02 Kp	0.12%	0.0000%
13	https (443 TCP)	841.00 p	0.11%	0.0000%
14	pcsync-https (8443 TCP)	1.44 Kp	0.11%	0.0000%
15	microsoft-ds (445 TCP)	2.91 Kp	0.10%	0.0000%
16	35554 (UDP)	497.00 p	0.05%	0.0000%
17	48157 (UDP)	497.00 p	0.05%	0.0000%
18	48691 (UDP)	497.00 p	0.05%	0.0000%
19	kerberos (88 TCP)	576.00 p	0.04%	0.0000%
20	snmp (161 UDP)	2.28 Kp	0.03%	0.0000%
21	49155 (TCP)	294.00 p	0.01%	0.0000%
22	ntp (123 UDP)	683.00 p	0.01%	0.0000%
23	Echo-Reply (ICMP)	336.00 p	0.01%	0.0000%
24	6970 (TCP)	38.00 p	0.01%	0.0000%
25	domain (dns) (53 UDP)	428.00 p	0.00%	0.0000%
Other	(What is this?)	1.60 Kp	0.10 %	0.0000%
Total	(from conv tables)	2.21 Mp	100 %	0.0006%

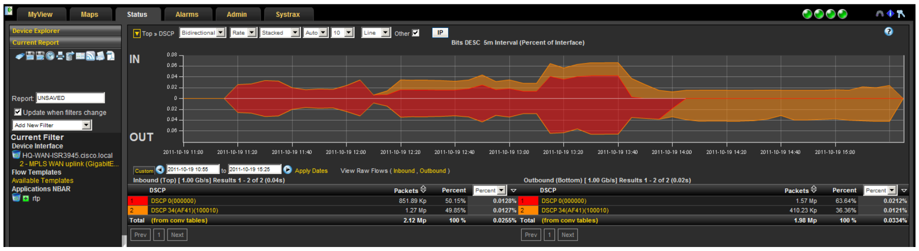
Outbound (Bottom) [3.10 Gb/s] Results 1 - 25 of 28 (0.18s)

	Well Known	Packets	Percent	Percent
1	rapido-ip (2457 UDP)	1.70 Mp	82.91%	0.0002%
2	sip (5060 TCP)	51.69 Kp	7.33%	0.0000%
3	http (80 TCP)	11.06 Kp	2.76%	0.0000%
4	wago-io-system (2455 UDP)	35.90 Kp	2.31%	0.0000%
5	qadmifoper (2461 UDP)	35.97 Kp	1.27%	0.0000%
6	sip-tls (5061 TCP)	10.88 Kp	1.01%	0.0000%
7	microsoft-ds (445 TCP)	3.99 Kp	0.56%	0.0000%
8	Echo-Reply (ICMP)	10.36 Kp	0.35%	0.0000%
9	altav-remmgt (2456 UDP)	607.00 p	0.29%	0.0000%
10	https (443 TCP)	790.00 p	0.17%	0.0000%
11	kerberos (88 TCP)	786.00 p	0.13%	0.0000%
12	pcsync-https (8443 TCP)	1.68 Kp	0.12%	0.0000%
13	35554 (UDP)	994.00 p	0.12%	0.0000%
14	48157 (UDP)	994.00 p	0.12%	0.0000%
15	48691 (UDP)	994.00 p	0.12%	0.0000%
16	ldap (389 TCP)	842.00 p	0.11%	0.0000%
17	h323gatestat (1719 UDP)	748.00 p	0.08%	0.0000%
18	4786 (TCP)	882.00 p	0.06%	0.0000%
19	5246 (UDP)	459.00 p	0.05%	0.0000%
20	49155 (TCP)	378.00 p	0.05%	0.0000%
21	ntp (123 UDP)	651.00 p	0.02%	0.0000%
22	indx-dds (2454 UDP)	119.00 p	0.02%	0.0000%
23	Port Unreachable (771 ICMP)	359.00 p	0.01%	0.0000%
24	cslistener (9000 TCP)	383.00 p	0.01%	0.0000%
25	domain (dns) (53 UDP)	428.00 p	0.01%	0.0000%
Other	(What is this?)	63.00 p	0.00 %	0.0000%
Total	(from conv tables)	1.88 Mp	100 %	0.0002%

The primary difference is that, today, many applications, including video conferencing, tend to use a broad range of TCP or UDP ports that are dynamically chosen within a large, known range. Various WKPs may fall within these ranges, and without additional application awareness provided by NBAR, the NetFlow collectors identify the applications incorrectly.

NetFlow is well-suited for identifying, isolating, and correcting network problems, especially configuration problems that might manifest across multiple devices, such as a misconfigured QoS policy. You can generate a report that filters down to an individual conversation between two endpoints that should be tagged bi-directionally with a specific DSCP value, such as an RTP video stream. If any intermediate devices along the path between the endpoints do not consistently show the data to be properly tagged, then there is likely to be a misconfigured device.

Figure 12 - Plixer Scrutinizer DSCP report (before and after resolving QoS trust boundary)



Report: UNSAVED

☑ Update when filters change

Add New Filter

Current Filter
Device Interface
HQ-WAN-ISR3945.cisco.local
2 - MPLS WAN uplink (GigabitE...
Flow Templates
Available Templates
Applications NBAR
rtp

Top » DSCP | Bidirectional | Rate | Stacked | Auto | 10 | Line | Other ☑

Bits DESC 5m Interval (Percent of Interface)

2011-10-19 10:55 to 2011-10-19 15:25

View Raw Flows (Inbound , Outbound)

Inbound (Top) [1.00 Gb/s] Results 1 - 2 of 2 (0.04s)

	DSCP	Packets	Percent	Percent
1	DSCP 0(000000)	851.89 Kp	50.15%	0.0128%
2	DSCP 34(AF41)(100010)	1.27 Mp	49.85%	0.0127%
Total	(from conv tables)	2.12 Mp	100 %	0.0255%

Outbound (Bottom) [1.00 Gb/s] Results 1 - 2 of 2 (0.02s)

	DSCP	Packets	Percent	Percent
1	DSCP 0(000000)	1.57 Mp	63.64%	0.0212%
2	DSCP 34(AF41)(100010)	410.23 Kp	36.36%	0.0121%
Total	(from conv tables)	1.98 Mp	100 %	0.0334%

The report shown in Figure 12 was generated by selecting a DSCP report for a headquarters' WAN router and filtered to show only RTP traffic. The report shows RTP incorrectly tagged with DSCP 0.

This issue was resolved by checking the QoS trust boundaries between LAN switches that connected the router to the video endpoints. After finding and correcting the problem, the report was regenerated to verify that the configuration change worked properly. The report now shows that RTP is properly tagged as AF41 (DSCP 34).

Appendix A: Product List

WAN Aggregation

Functional Area	Product Description	Part Numbers	Software
WAN-aggregation Router	Aggregation Services 1002X Router	ASR1002X-5G-VPNK9	IOS-XE 15.3(3)S Advanced Enterprise license
	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	
WAN-aggregation Router	Cisco 3945 Security Bundle w/SEC license PAK	CISCO3945-SEC/K9	15.2(4)M4 securityk9 license datak9 license
	Cisco 3925 Security Bundle w/SEC license PAK	CISCO3925-SEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco ISR 4451 w/ 4GE,3NIM,2SM,8G FLASH, 4G DRAM, IP Base, SEC, AX license with: DATA, AVC, ISR-WAAS with 2500 connection RTU	ISR4451-X-AX/K9	IOS-XE 15.3(3)S securityk9 license appxk9 license
	Cisco ISR 3945 w/ SPE150, 3GE, 4EHWIC, 4DSP, 4SM, 256MBCF, 1GBDRAM, IP Base, SEC, AX licenses with DATA, AVC, and WAAS/vWAAS with 2500 connection RTU	C3945-AX/K9	15.2(4)M4 securityk9 license datak9 license
	Cisco ISR 3925 w/ SPE100 (3GE, 4EHWIC, 4DSP, 2SM, 256MBCF, 1GBDRAM, IP Base, SEC, AXlicenses with DATA, AVC, WAAS/vWAAS with 2500 connection RTU	C3925-AX/K9	
	Cisco ISR 2951 w/ 3 GE, 4 EHWIC, 3 DSP, 2 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with DATA, AVC, and WAAS/vWAAS with 1300 connection RTU	C2951-AX/K9	
	Cisco ISR 2921 w/ 3 GE, 4 EHWIC, 3 DSP, 1 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with DATA, AVC, and WAAS/vWAAS with 1300 connection RTU	C2921-AX/K9	
	Cisco ISR 2911 w/ 3 GE,4 EHWIC, 2 DSP, 1 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with DATA, AVC and WAAS/vWAAS with 1300 connection RTU	C2911-AX/K9	
	Cisco ISR 1941 Router w/ 2 GE, 2 EHWIC slots, 256MB CF, 2.5GB DRAM, IP Base, DATA, SEC, AX license with AVC and WAAS-Express	C1941-AX/K9	
Fixed WAN Remote-site Router	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.2(4)M4 securityk9 license datak9 license

Appendix B: NetFlow-Enabled Device Configuration

NetFlow-Enabled Cisco ASR 1000 Series Router

TNF and FNF are both enabled in these router configurations.

WAN-Aggregation—MPLS CE Router

```
version 15.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no platform punt-keepalive disable-kernel-core
!
hostname CE-ASR1002X-1
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
ip nbar protocol-pack flash:/pp-adv-asr1k-153-2.S-15-5.1.0.pack
```

```
!
flow record Record-FNF
 description Flexible NetFlow with NBAR2 Flow Record
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 match flow direction
 match application name
 collect routing source as
 collect routing destination as
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source prefix
 collect ipv4 source mask
 collect ipv4 destination mask
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
flow exporter Export-FNF-Plixer
 description FNF-NBAR2 with IPFIX export
 destination 10.4.48.171
 source Loopback0
 transport udp 4739
 export-protocol ipfix
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-FNF-Prime20
 description FNF-NBAR2
 destination 10.4.48.35
 source Loopback0
 transport udp 9991
 option interface-table
 option application-table
 option application-attributes
```

```
!
!
flow exporter Export-FNF-LiveAction
 description FNF-NBAR2
 destination 10.4.48.178
 source Loopback0
 transport udp 2055
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-FNF-SevOne
 description FNF-NBAR2
 destination 10.4.48.172
 source Loopback0
 transport udp 9996
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-FNF-Lancope
 description FNF-NBAR2
 destination 10.4.48.174
 source Loopback0
 transport udp 2055
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-TNF-Solarwinds
 description TNF v9
 destination 10.4.48.173
 source Loopback0
 transport udp 2055
!
!
flow monitor Monitor-FNF
 description FNF Traffic Analysis
 exporter Export-FNF-Plixer
 exporter Export-FNF-Prime20
 exporter Export-FNF-LiveAction
 exporter Export-FNF-Lancope
 exporter Export-FNF-SevOne
 cache timeout active 60
 cache entries 200000
 record Record-FNF
!
!
flow monitor Monitor-TNF
 description TNF Traffic Analysis
 exporter Export-TNF-Solarwinds
 cache timeout active 60
 cache entries 200000
 record netflow ipv4 original-input
!
!
ip domain name cisco.local
ip multicast-routing distributed
!
ip wccp source-interface Loopback0
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAE password 7 141443180F0B7B7977
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAE password 7 104D580A061843595F
!
multilink bundle-name authenticated
!
!
username admin password 7 0205554808095E731F
!
redundancy
 mode none
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
 match dscp af21
class-map match-any BGP-ROUTING
 match protocol bgp
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4  af41
class-map match-any CRITICAL-DATA
 match dscp cs3  af31
class-map match-any VOICE
 match dscp ef
class-map match-any SCAVENGER
 match dscp cs1  af11
class-map match-any NETWORK-CRITICAL
 match dscp cs2  cs6
!
policy-map MARK-BGP
```

```
 class BGP-ROUTING
  set dscp cs6
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
   service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0/3
 class class-default
  shape average 300000000
   service-policy WAN
!
!
interface Loopback0
 ip address 10.4.32.241 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel1
 ip address 10.4.32.2 255.255.255.252
 ip wccp 61 redirect in
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-TNF output
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-FNF output
 ip pim sparse-mode
 no negotiation auto
 !
interface GigabitEthernet0/0/0
 description WAN-D3750X Gig1/0/1
 no ip address
 negotiation auto
 cdp enable
 channel-group 1 mode active
```

```
!
interface GigabitEthernet0/0/1
 description WAN-D3750X Gig2/0/1
 no ip address
 negotiation auto
 channel-group 1 mode active
!
interface GigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/3
 description MPLS PE router
 bandwidth 300000
 ip address 192.168.3.1 255.255.255.252
 ip wccp 62 redirect in
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF output
 ip flow monitor Monitor-TNF output
 negotiation auto
 !
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
!
router eigrp 100
 distribute-list route-map BLOCK-TAGGED-ROUTES in
 default-metric 300000 100 255 1 1500
 network 10.4.0.0 0.1.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface Port-channel1
 eigrp router-id 10.4.32.241
!
router bgp 65511
 bgp router-id 10.4.32.241
 bgp log-neighbor-changes
 network 0.0.0.0
 network 192.168.3.0 mask 255.255.255.252
 redistribute eigrp 100
 neighbor 10.4.32.242 remote-as 65511
 neighbor 10.4.32.242 update-source Loopback0
 neighbor 10.4.32.242 next-hop-self
 neighbor 192.168.3.2 remote-as 65401
!
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip pim autorp listener
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
!
ip access-list standard WAE
 permit 10.4.32.162
 permit 10.4.32.161
!
ip access-list extended WAAS-REDIRECT-LIST
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq tacacs any
 deny   tcp any any eq tacacs
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any
!
ip sla responder
logging 10.4.48.35
access-list 55 permit 10.4.48.0 0.0.0.255
!
route-map BLOCK-TAGGED-ROUTES deny 10
 match tag 65401 65402 65512
!
route-map BLOCK-TAGGED-ROUTES permit 20
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server trap-source Loopback0
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 01200307490E12242455
!
```

```
!
control-plane
!
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
!
end
```

NetFlow-Enabled ISR-G2 Series Routers

TNF and FNF are both enabled in these router configurations.

Remote-Site with Access Layer (RS201)

```
version 15.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS201-2945
!
!
enable secret 5 $1$Rmfp$Btut/0xCUYDOmlruhEsPt1
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authentication login MODULE none
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
```

```
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
!
ip nbar protocol-pack flash0:/pp-adv-isrg2-152-4.M1-13-5.1.0.pack
!
!
flow record Record-FNF
 description Flexible NetFlow with NBAR Flow Record
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 match flow direction
 match application name
 collect routing source as
 collect routing destination as
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source prefix
 collect ipv4 source mask
 collect ipv4 destination mask
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
flow exporter Export-TNF-Solarwinds
 description TNF v9
 destination 10.4.48.173
 source Loopback0
 output-features
 transport udp 2055
!
```

```
!
flow exporter Export-FNF-Plixer
 description IPFIX-NBAR2
 destination 10.4.48.171
 source Loopback0
 output-features
 transport udp 4739
 export-protocol ipfix
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-FNF-Prime20
 description FNF-NBAR2
 destination 10.4.48.35
 source Loopback0
 output-features
 transport udp 9991
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-FNF-LiveAction
 description FNF-NBAR2
 destination 10.4.48.178
 source Loopback0
 output-features
 transport udp 2055
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-FNF-SevOne
 description FNF-NBAR2
 destination 10.4.48.172
 source Loopback0
 output-features
 transport udp 9996
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-FNF-Lancope
```

```
 description FNF-NBAR2
 destination 10.4.48.174
 source Loopback0
 output-features
 transport udp 2055
 option interface-table
 option application-table
option application-attributes
!
!
flow monitor Monitor-TNF
 description TNF Traffic Analysis
 record netflow ipv4 original-input
 exporter Export-TNF-Solarwinds
 cache timeout active 60
!
!
flow monitor Monitor-FNF
 description FNF Traffic Analysis
 record Record-FNF
 exporter Export-FNF-SevOne
 exporter Export-FNF-Lancope
 exporter Export-FNF-LiveAction
 exporter Export-FNF-Prime20
 exporter Export-FNF-Plixer
 cache timeout active 60
!
ip source-route
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
ip cef
!
ip vrf INET-PUBLIC1
 rd 65512:1
!
ip multicast-routing
!
!
ip domain name cisco.local
ip name-server 10.4.48.10
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAE password 7 110A4816141D5A5E57
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAE password 7 130646010803557878
!
multilink bundle-name authenticated
!
!
!
```

```
!
voice-card 0
!
!
!
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1347A1TN
license boot module c2900 technology-package datak9
hw-module sm 1
!
!
!
username admin password 7 04585A150C2E1D1C5A
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
 match  dscp af21
class-map match-any BGP-ROUTING
 match protocol bgp
class-map match-any INTERACTIVE-VIDEO
 match  dscp cs4  af41
class-map match-any CRITICAL-DATA
 match  dscp cs3  af31
class-map match-any VOICE
 match  dscp ef
class-map match-any SCAVENGER
 match  dscp cs1  af11
class-map match-any NETWORK-CRITICAL
 match  dscp cs2  cs6
 match access-group name ISAKMP
!
!
policy-map MARK-BGP
 class BGP-ROUTING
  set dscp cs6
policy-map WAN
 class VOICE
```

```
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
  service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/1
 class class-default
  shape average 10000000
  service-policy WAN
policy-map WAN-INTERFACE-G0/0
 class class-default
  shape average 10000000
  service-policy WAN
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
!
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
   keyring DMVPN-KEYRING1
   match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
```

```
!
!
!
interface Loopback0
 ip address 10.255.251.201 255.255.255.255
 ip pim sparse-mode
!
interface Tunnel10
 bandwidth 10000
 ip address 10.4.34.201 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip wccp 62 redirect in
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF output
 ip flow monitor Monitor-FNF output
 ip nhrp authentication cisco123
 ip nhrp map multicast 172.16.130.1
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
 ip summary-address eigrp 200 10.5.40.0 255.255.248.0
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC1
 tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Port-channel1
 description EtherChannel link to RS201-A2960S
 no ip address
 hold-queue 150 in
!
interface Port-channel1.64
 description Wired Data
 encapsulation dot1Q 64
 ip address 10.5.44.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip wccp 61 redirect in
 ip pim sparse-mode
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF output
 ip flow monitor Monitor-FNF output
!
interface Port-channel1.65
 description Wireless Data
 encapsulation dot1Q 65
 ip address 10.5.42.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip wccp 61 redirect in
 ip pim sparse-mode
!
interface Port-channel1.69
 description Wired Voice
 encapsulation dot1Q 69
 ip address 10.5.45.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF output
 ip flow monitor Monitor-FNF output
!
interface Port-channel1.70
 description Wireless Voice
 encapsulation dot1Q 70
 ip address 10.5.43.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 bandwidth 10000
 ip address 192.168.3.21 255.255.255.252
 ip wccp 62 redirect in
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF output
 ip flow monitor Monitor-FNF output
 duplex auto
 speed auto
 no cdp enable
 service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
 bandwidth 10000
 ip vrf forwarding INET-PUBLIC1
 ip address dhcp
 ip access-group ACL-INET-PUBLIC in
 duplex auto
 speed auto
 no cdp enable
 service-policy output WAN-INTERFACE-G0/1
!
interface GigabitEthernet0/2
 description RS201-A2960S Gig1/0/24
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface GigabitEthernet0/0/0
 description RS201-A2960S Gig2/0/24
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface SM1/0
 ip address 192.0.2.2 255.255.255.252
 service-module external ip address 10.5.44.8 255.255.255.0
 !Application: Restarted at Wed Jun  6 21:07:33 2012
 service-module ip default-gateway 10.5.44.1
!
interface SM1/1
 description Internal switch interface connected to Service Module
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
!
!
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.255.251.201
 eigrp stub connected summary
!
router bgp 65511
 bgp router-id 10.255.251.201
 bgp log-neighbor-changes
 network 10.5.44.0 mask 255.255.255.0
 network 10.5.45.0 mask 255.255.255.0
 network 10.255.251.201 mask 255.255.255.255
 network 192.168.3.20 mask 255.255.255.252
 aggregate-address 10.5.40.0 255.255.248.0 summary-only
 neighbor 192.168.3.22 remote-as 65401
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list standard WAE
 permit 10.5.44.8
!
ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
ip access-list extended WAAS-REDIRECT-LIST
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq tacacs any
 deny   tcp any any eq tacacs
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any
!
ip sla responder
logging 10.4.48.35
access-list 55 permit 10.4.48.0 0.0.0.255
access-list 67 permit 192.0.2.2
!
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 0538030C33495A221C1C
!
!
control-plane
!
!
mgcp profile default
!
!
gatekeeper
 shutdown
!
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line 67
 access-class 67 in
 login authentication MODULE
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 access-class 55 in
 transport preferred none
 transport input ssh
line vty 5 15
 access-class 55 in
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
end
```

Remote-Site with Distribution Layer (RS200)

```
version 15.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS200-3925-1
!
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
crypto pki token default removal timeout 0
!
no ipv6 cef
ipv6 spd queue min-threshold 62
```

```
ipv6 spd queue max-threshold 63
!
!
ip nbar protocol-pack flash0:/pp-adv-isrg2-152-4.M1-13-5.1.0.pack
!
!
flow record Record-FNF
 description Flexible NetFlow with NBAR Flow Record
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 match flow direction
 match application name
 collect routing source as
 collect routing destination as
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source prefix
 collect ipv4 source mask
 collect ipv4 destination mask
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
flow exporter Export-TNF-Solarwinds
 description TNF v9
 destination 10.4.48.173
 source Loopback0
 output-features
 transport udp 2055
!
!
flow exporter Export-FNF-Plixer
 description IPFIX-NBAR2
 destination 10.4.48.171
 source Loopback0
 output-features
 transport udp 4739
 export-protocol ipfix
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-FNF-Prime20
 description FNF-NBAR2
 destination 10.4.48.35
 source Loopback0
 output-features
 transport udp 9991
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-FNF-LiveAction
 description FNF-NBAR2
 destination 10.4.48.178
 source Loopback0
 output-features
 transport udp 2055
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-FNF-SevOne
 description FNF-NBAR2
 destination 10.4.48.172
 source Loopback0
 output-features
 transport udp 9996
 option interface-table
 option application-table
 option application-attributes
!
!
flow exporter Export-FNF-Lancope
 description FNF-NBAR2
 destination 10.4.48.174
 source Loopback0
 output-features
 transport udp 2055
 option interface-table
 option application-table
option application-attributes
!
!
flow monitor Monitor-TNF
 description TNF Traffic Analysis
 record netflow ipv4 original-input
 exporter Export-TNF-Solarwinds
 cache timeout active 60
!
!
flow monitor Monitor-FNF
 description FNF Traffic Analysis
 record Record-FNF
 exporter Export-FNF-SevOne
 exporter Export-FNF-Lancope
 exporter Export-FNF-LiveAction
 exporter Export-FNF-Prime20
 exporter Export-FNF-Plixer
 cache timeout active 60
!
ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
ip domain name cisco.local
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAE password 7 0508571C22431F5B4A
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAE password 7 130646010803557878
!
multilink bundle-name authenticated
!
voice-card 0
!
license udi pid C3900-SPE100/K9 sn FOC14415C5Q
hw-module sm 2
!
!
!
username admin password 7 070C705F4D06485744
!
redundancy
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
 match  dscp af21
class-map match-any BGP-ROUTING
 match protocol bgp
class-map match-any INTERACTIVE-VIDEO
 match  dscp cs4  af41
class-map match-any CRITICAL-DATA
 match  dscp cs3  af31
class-map match-any VOICE
 match  dscp ef
class-map match-any SCAVENGER
 match  dscp cs1  af11
class-map match-any NETWORK-CRITICAL
 match  dscp cs2  cs6
!
!
policy-map MARK-BGP
 class BGP-ROUTING
  set dscp cs6
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
  service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0
 class class-default
  shape average 50000000
  service-policy WAN
!
!
!
```

```
interface Loopback0
 ip address 10.255.251.200 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel1
 description EtherChannel link to RS200-D4507
 no ip address
 hold-queue 150 in
!
interface Port-channel1.50
 description R1 routed link to distribution layer
 encapsulation dot1Q 50
 ip address 10.5.0.1 255.255.255.252
 ip wccp 61 redirect in
 ip pim sparse-mode
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF output
 ip flow monitor Monitor-TNF output
 !
interface Port-channel1.99
 description Transit net
 encapsulation dot1Q 99
 ip address 10.5.0.9 255.255.255.252
 ip pim sparse-mode
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF output
 ip flow monitor Monitor-TNF output
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 bandwidth 50000
 ip address 192.168.3.17 255.255.255.252
 ip wccp 62 redirect in
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF output
 ip flow monitor Monitor-TNF output
 duplex auto
 speed auto
 no cdp enable
 service-policy output WAN-INTERFACE-G0/0
 !
```

```
interface GigabitEthernet0/1
 description RS200-D4507 Ten3/1
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface GigabitEthernet0/2
 description RS200-D4507 Ten4/1
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface SM2/0
 ip address 10.5.0.17 255.255.255.252
 service-module ip address 10.5.0.18 255.255.255.252
 !Application: running
 service-module ip default-gateway 10.5.0.17
!
interface SM2/1
 description Internal switch interface connected to Service Module
 no ip address
!
interface Vlan1
 no ip address
!
!
router eigrp 100
 default-metric 25000 100 255 1 1500
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface Port-channel1.50
 no passive-interface Port-channel1.99
 eigrp router-id 10.255.251.200
!
router bgp 65511
 bgp router-id 10.255.251.200
 bgp log-neighbor-changes
 network 10.5.1.0 mask 255.255.255.0
 network 10.5.2.0 mask 255.255.255.0
 network 10.5.3.0 mask 255.255.255.0
 network 10.5.4.0 mask 255.255.255.0
 network 10.255.251.200 mask 255.255.255.255
 network 192.168.3.16 mask 255.255.255.252
 network 192.168.3.17 mask 255.255.255.255
 aggregate-address 10.5.0.0 255.255.248.0 summary-only
 neighbor 192.168.3.18 remote-as 65401
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list standard WAE
 permit 10.5.7.8
 permit 10.5.7.9
!
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq tacacs any
 deny   tcp any any eq tacacs
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any
!
ip sla responder
logging 10.4.48.35
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 04680E051D2458650C00
!
```

```
!
!
control-plane
!
!
!
mgcp profile default
!
!
gatekeeper
 shutdown
!
!
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line 131
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
end
```

Appendix C: Changes

This appendix summarizes the changes to this guide since its last edition.

- Added support for NBAR-2, to include installation of protocol packs.
- Added support for IPFIX export.
- Added support for Cisco Prime 2.0 Netflow Collection.

Feedback

Please use the feedback form to send comments and suggestions about this guide.

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

B-0000130-1 12/13