CISCO IOS NETFLOW OVERVIEW

ITD PRODUCT MANAGEMENT

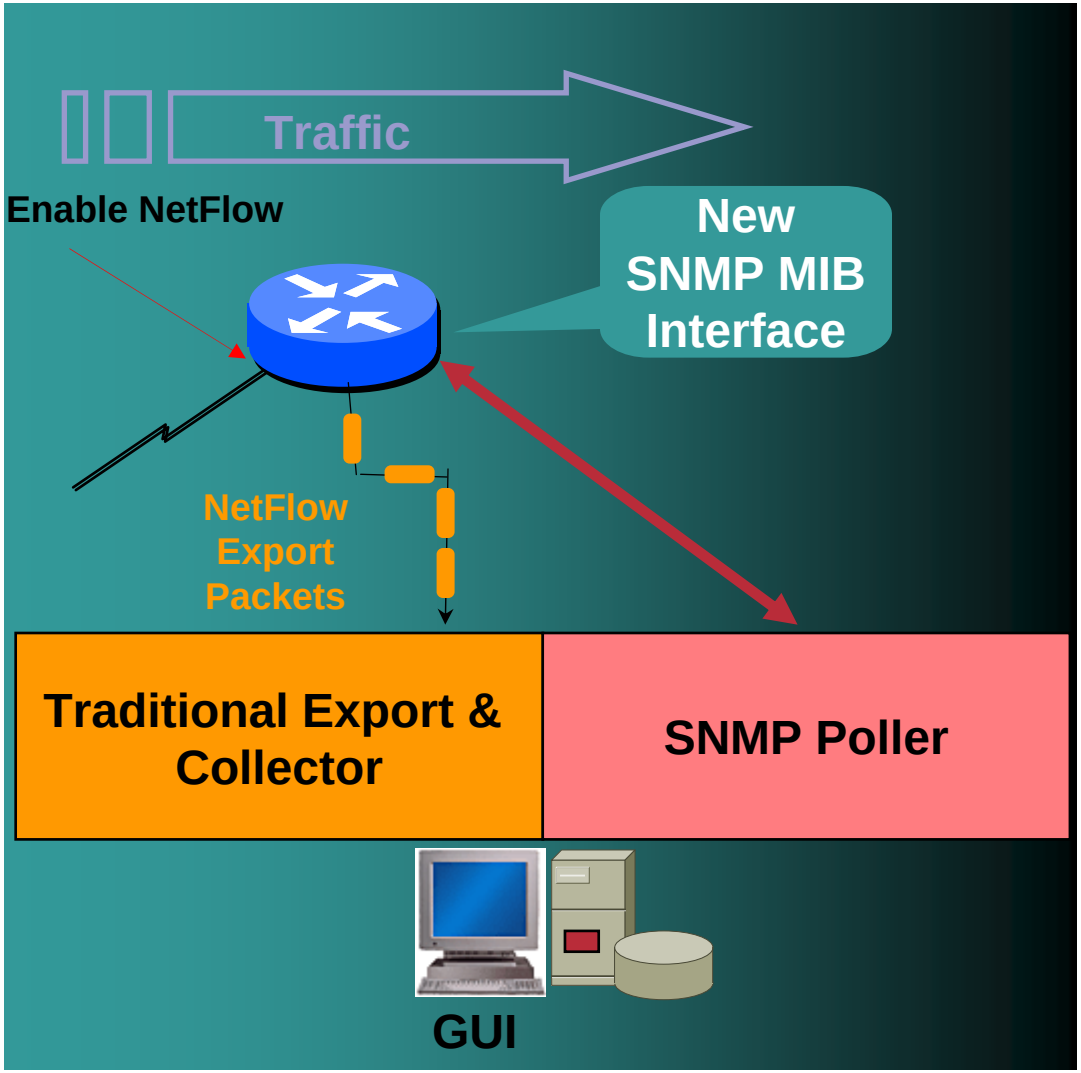
FEBRUARY 2004

Cisco IOS NetFlow Origination

- Developed and patented at Cisco® Systems in 1996
- NetFlow is now the primary network accounting technology in the industry
- Answers questions regarding IP traffic: who, what, where, when, and how
- Provides a detailed view of network behavior

Flow Is Defined By Seven Unique Keys

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- TOS byte (DSCP)
- Input logical interface (ifIndex)



NetFlow Cache Example

1. Create and update flows in NetFlow Cache

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	SrcPort	SrcMsk	SrcAS	DstPort	DstMsk	DstAS	NextHop	Bytes/Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A1	/24	180	00A1	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

2. Expiration

- **Inactive timer expired (15 sec is default)**
- **Active timer expired (30 min (1800 sec) is default)**
- **NetFlow cache is full (oldest flows are expired)**
- **RST or FIN TCP Flag**

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	SrcPort	SrcMsk	SrcAS	DstPort	DstMsk	DstAS	NextHop	Bytes/Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

3. Aggregation?

No

Yes

e.g. Protocol-Port Aggregation Scheme becomes

Protocol	Pkts	SrcPort	DstPort	Bytes/Pkt
11	11000	00A2	00A2	1528

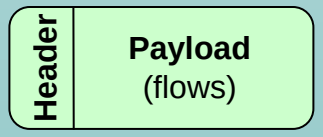
4. Export Version

Non-Aggregated Flows – export **Version 5 or 9**

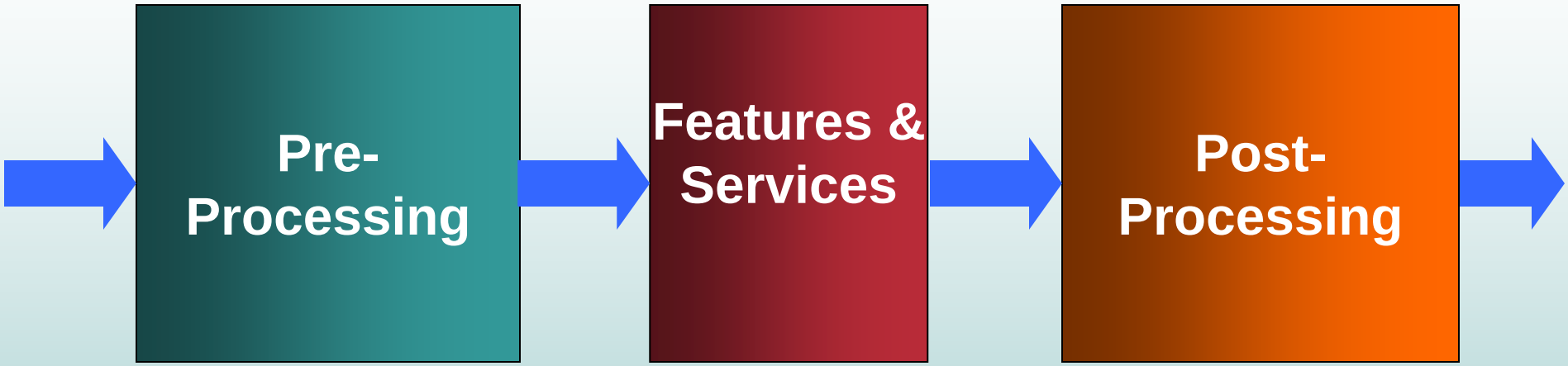
Aggregated Flows – export **Version 8 or 9**

5. Transport Protocol

Export Packet



NetFlow Processing Direction



- Packet Sampling
- Filtering

- IP
- Multicast
- MPLS
- IPv6

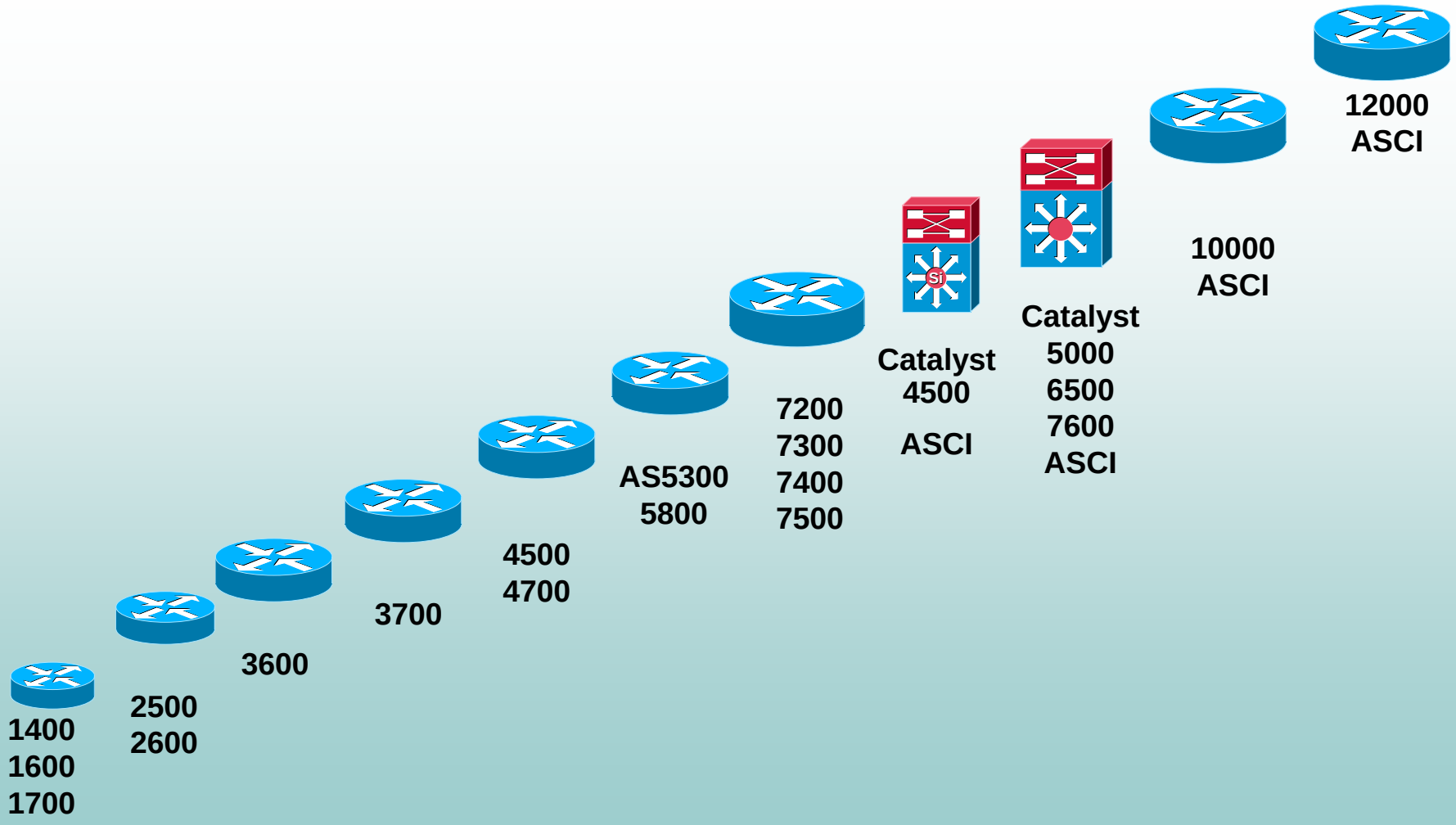
- Aggregation schemes
- Export

NetFlow Principles

- Inbound traffic only today
- Unidirectional flow
- Accounts for both transit traffic and traffic destined for the router
- Works with Cisco Express Forwarding or fast switching
  - Not a switching path
- Supported on all interfaces and Cisco IOS Software hardware products
- Returns the sub-interface information in the flow records

Comprehensive Hardware Support

Cisco.com



Principle Netflow Benefits

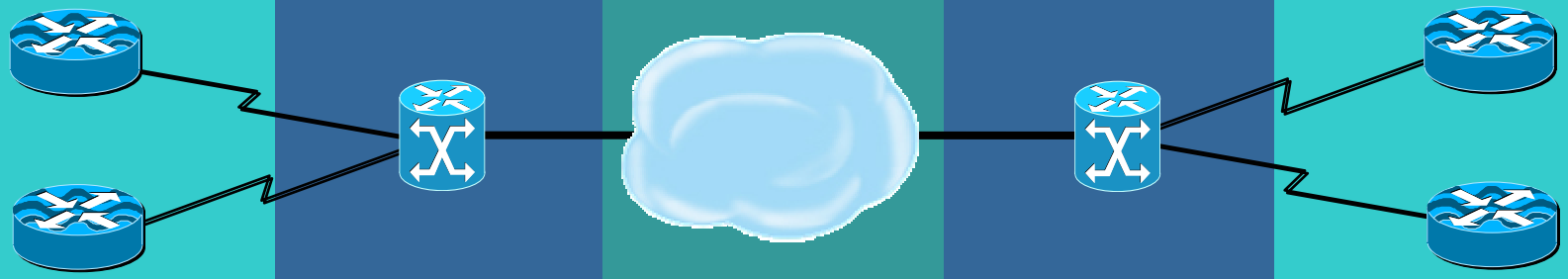
Service Provider

- Peering arrangements
- Network Planning
- Traffic Engineering
- Accounting and billing
- Security Monitoring

Enterprise

- Internet access monitoring (protocol distribution, where traffic is going/coming)
- User Monitoring
- Application Monitoring
- Charge Back billing for departments
- Security Monitoring

NetFlow Uses

	Access	Distribution	Core	Distribution	Access
Network Layer					
Applications	• Attack Mitigation • User (IP) monitoring • Application monitoring	• Billing • Chargeback • AS Peer Monitoring	• Traffic Engineering • Traffic Analysis	• Billing • Chargeback • AS Peer Monitoring	• Attack Mitigation • User (IP) monitoring • Application monitoring
NetFlow Features	• Aggregation Schemes (v8) • “show ip cache flow” command • Arbor Networks	• NetFlow MPLS Egress Accounting • BGP Next-hop (v9) • Multicast NetFlow (v9)	• MPLS Aware NetFlow (v9) • BGP Next-hop (v9) • Sampled NetFlow	• NetFlow MPLS Egress Accounting • BGP Next-hop (v9) • Multicast NetFlow (v9)	• Aggregation Schemes (v8) • “show ip cache flow” command • Arbor Networks

Tracking Users

Who are the top users?
How long are the users on the network?

What Internet sites do they use?
Where do the users go on the network?

What percentage of traffic do they use?
What applications do they use?
What are the user usage patterns?

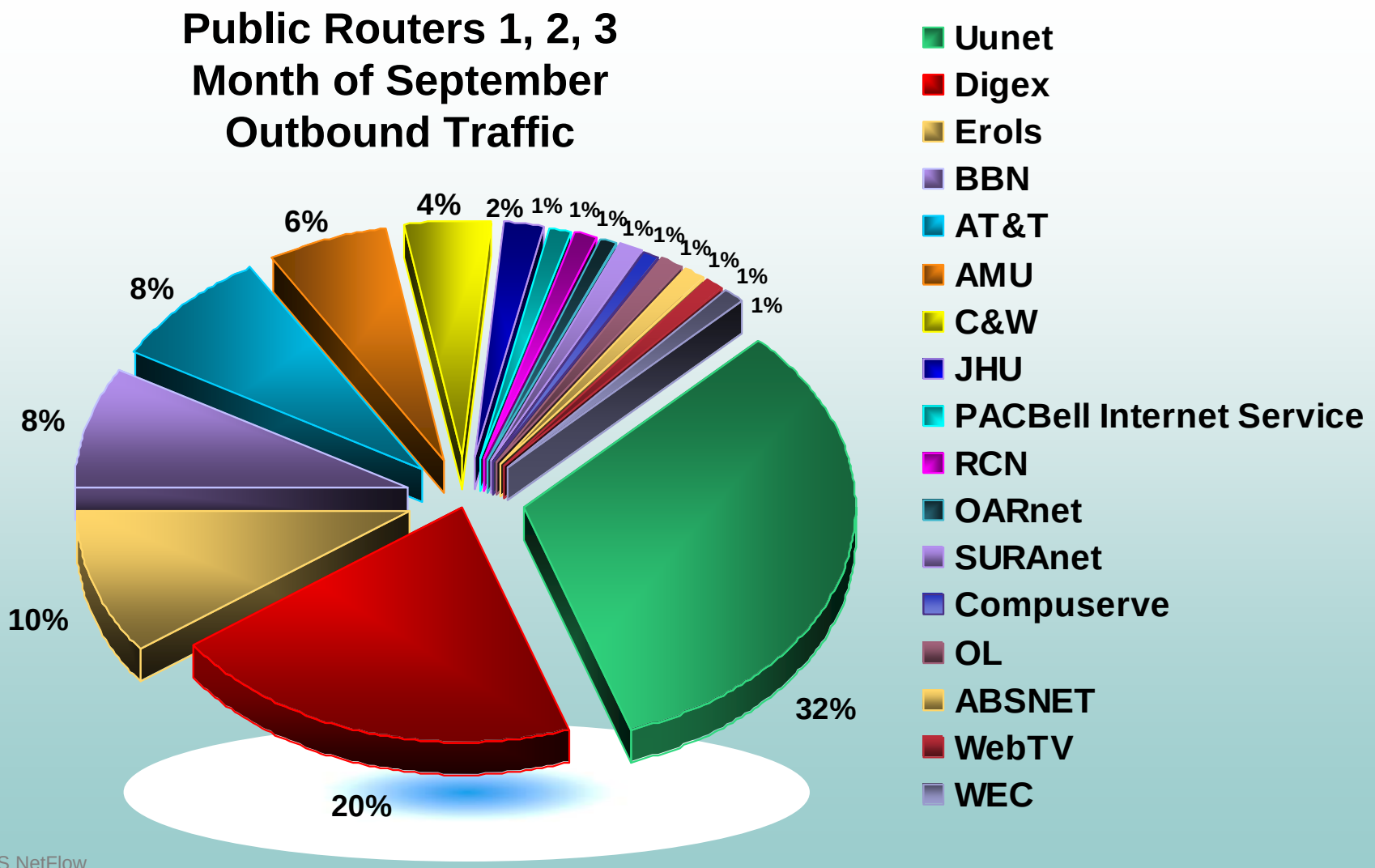
NetFlow for Security: Flow Information Helps Mitigate Attacks

- **Identify the attack**
  - **Count the Flows**
  - **Inactive flows signal a worm attack**
- **Classify the attack**
  - **Small size flows to same destination**
  - **What is being attacked and origination of attack**
- **Cisco IT prevented SQL slammer at Cisco by watching flows per port**

Billing

- **Flat-rate billing does not necessarily scale**
  - **Competitive pricing models can be created with usage-based billing**
- **Usage-based billing considerations**
  - **Time of day**
  - **Within or outside of the network**
  - **Application**
  - **Distance-based**
  - **Quality of Service (QoS) / Class of Service (CoS)**
  - **Bandwidth usage**
  - **Transit or peer**
  - **Data transferred**
  - **Traffic class**

NetFlow – Peering Agreement



“Capacity planning is the process of determining the network resources required to prevent a performance or availability impact on business-critical applications.”

Capacity Planning

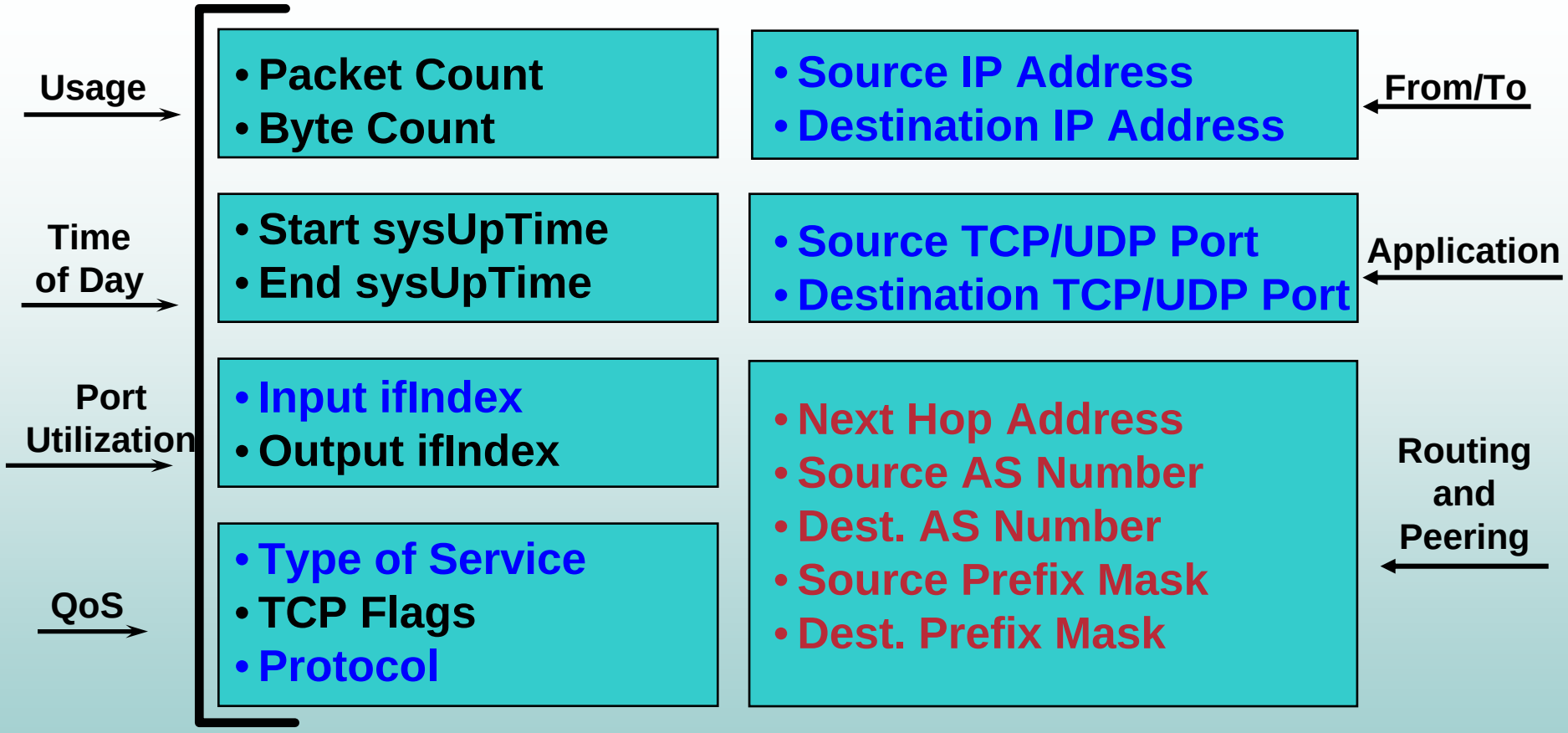
- **Key areas to monitor**
  - **Application usage**
  - **Identify which applications consume bandwidth**
  - **Who are the top ten nodes that consume bandwidth**
- **Output data circuit forecasts**
- **Current network utilization and capacity being used**

NetFlow Versions

NetFlow Version	Comments
1	Original
5	Standard and most common
7	Specific to Cisco Catalyst 6500 and 7600 Series Switches Similar to Version 5, but does not include AS, interface, TCP Flag & TOS information
8	Choice of eleven aggregation schemes Reduces resource usage
9	Flexible, extensible file export format to enable easier support of additional fields & technologies; coming out now MPLS, Multicast, & BGP Next Hop

Cisco Catalyst 6500 Series Router will support versions 5 & 8 in Cisco IOS Software Release 12.1(13)E

Version 5 - Flow Export Format



Version 5 used extensively today

Version 8

- Router-based aggregation
- Enables router to summarize NetFlow data
- Reduces NetFlow Export data volume
- Decreases NetFlow Export bandwidth requirements
- Currently 11 aggregation schemes
  - Five original schemes
  - Six new schemes with the TOS byte field
- Available in Cisco IOS Software Releases 12.0(15)S and 12.2(1)T
- Several aggregations can be enabled simultaneously

Why a New Version 9?

- Fixed export formats are not flexible and adaptable
- With each new version Cisco creates new export fields
- Partners need to re-engineer for each new version

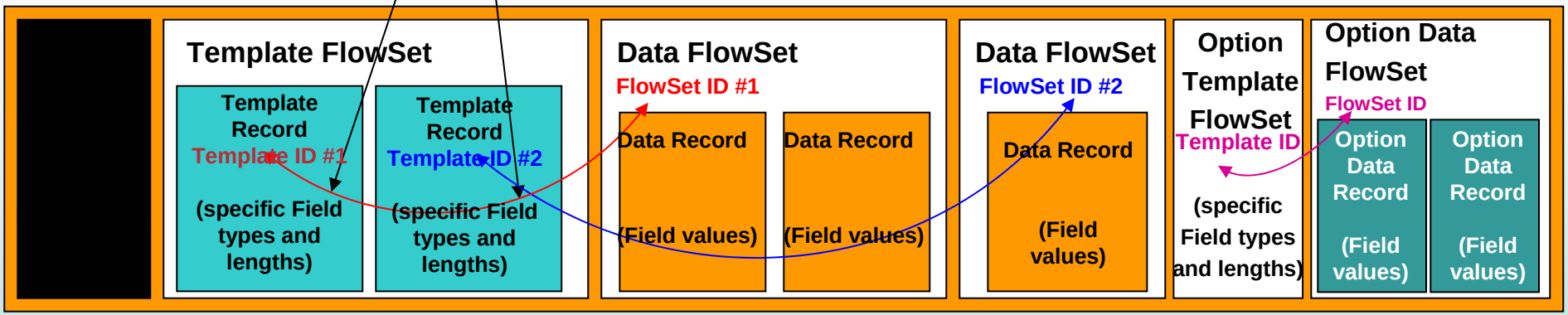
Solution: Build a flexible and extensible export format called version 9!

NetFlow v9 Export Packet

To support technologies such as MPLS or Multicast, this export format can be leveraged to easily insert new fields

Flows from Interface A

Flows from Interface B



- Matching ID numbers are the way to associate template to the Data Records
- The Header follows the same format as prior NetFlow versions so Collectors will be backward compatible
- Each data record represents one flow
- If exported flows have the same fields, then they can be contained in the same Template Record (ie: unicast traffic) can be combined with multicast records
- If exported flows have different fields, then they cannot be contained in the same Template Record (ie: BGP next-hop cannot be combined with MPLS Aware NetFlow records)

NetFlow v9 and IETF

- **Internet Protocol Flow Information eXport (IPFIX) is an IETF Working Group**

  ipfix.doit.wisc.edu/

- **Netflow version 9 is the basis for the standard in the IETF**
- **Informational RFC on NetFlow version 9**

  www.ietf.org/internet-drafts/draft-bclaise-netflow-9-00.txt

NEW FEATURES

NetFlow Version 9 Features

- **Multicast NetFlow version 9**
  - **Availability: Major Release 12.3**
  - **Ingress Accounting of replicated multicast packets**
  - **Egress Per user accounting of multicast packets**
- **MPLS Aware NetFlow version 9**
  - **Availability: Release 12.0(26)S**
  - **Label and prefix export information**
- **BGP Next Hop version 9**
  - **Availability: Releases 12.3 and 12.0(26)S**
  - **Edge to Edge Traffic Matrix**
  - **BGP traffic destination information**
- **NetFlow for IPv6**
  - **Availability: Release 12.3(7)T**
  - **Export IPv6 source and destination information**

NetFlow Product Update

- **Sampled NetFlow**
  - **Availability: Releases 12.0(26)S, 12.3(2)T, and 12.2(18)S**
  - **Random Sampling of packets per flow with reduce CPU**
- **NetFlow MIB**
  - **Availability: Release 12.3(7)T**
  - **Top N Talker in MIB**
  - **NetFlow configuration using MIB**
- **Input Flow Filters**
  - **Availability: Release 12.3(7)T**
  - **QOS MQC based Filtering entering NetFlow**

References

- **Cisco IOS NetFlow**

  www.cisco.com/go/netflow

- **Cisco Network Accounting Services**

  Comparison of Cisco NetFlow versus other available accounting technologies

  www.cisco.com/warp/public/cc/pd/iosw/prodlit/nwact_wp.htm