Cisco Systems

poweredbycisco. networkers 2005

NMS-3132

Advanced Netflow Usage

Michael De Leo
mdeleo@cisco.com

Recuerde siempre:

- **Apagar su teléfono móvil/pager, o usar el modo “silencioso”.**

- **Completar la evaluación de esta sesión y entregarla a los asistentes de sala.**

- **Ser puntual para asistir a todas las actividades de entrenamiento, almuerzos y eventos sociales para un desarrollo óptimo de la agenda.**

- **Completar la evaluación general incluida en su mochila y entregarla el miércoles 8 de Junio en los mostradores de registración. Al entregarla recibirá un regalo recordatorio del evento.**

This Tutorial Is...

- **NOT about**
  - An introduction to NetFlow
  - A level 1 type of presentation
  - Marketing slides
  - The NetFlow Collector (NFC) details
  - The Ecosystem partners applications and mediations
  - Many platform specific details
- **About**
  - New features
  - Advanced information
  - And scenario…
    assuming the NetFlow basics are known

Agenda

- Introduction
- NetFlow MIB
- NetFlow Version 9
- NetFlow Sampling and Filtering
  - Sampled NetFlow
  - Input Filters
  - Research on the NetFlow Sampling Accuracy
- NetFlow for Security
  - NetFlow L2 and Security Monitoring
  - NetFlow MIB and Top Talkers
- NetFlow for Capacity Planning
  - BGP Next Hop TOS Aggregation
  - MPLS Aware NetFlow
- New Features
  - Egress NetFlow
  - NetFlow and IPv6
- Platforms Specific
- NetFlow and IETF Interaction

INTRODUCTION

NetFlow Flow Keys on the Router

- **By default, the flow keys are:**

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

- **The NetFlow aggregation allows to reduce/change the number of flow keys**

  Example: source prefix aggregation: source network, source interface

  Can be seen as a different view of the main cache

- **Egress NetFlow, MPLS Aware NetFlow, etc…**

  Will specify new flow keys

- **On the Catalyst®, we speak of the flow mask**

  Define the flow keys

Flow Keys on the Catalyst 6500/7600
The Flow Mask

Full-Interface

VLAN	SRC IP	DST IP	IP Protocol	Src Port	Dst Port

Full

VLAN	SRC IP	DST IP	IP Protocol	Src Port	Dst Port

Destination-Source-Interface

VLAN	SRC IP	DST IP	IP Protocol	Src Port	Dst Port

Source-Only

VLAN	SRC IP	DST IP	IP Protocol	Src Port	Dst Port

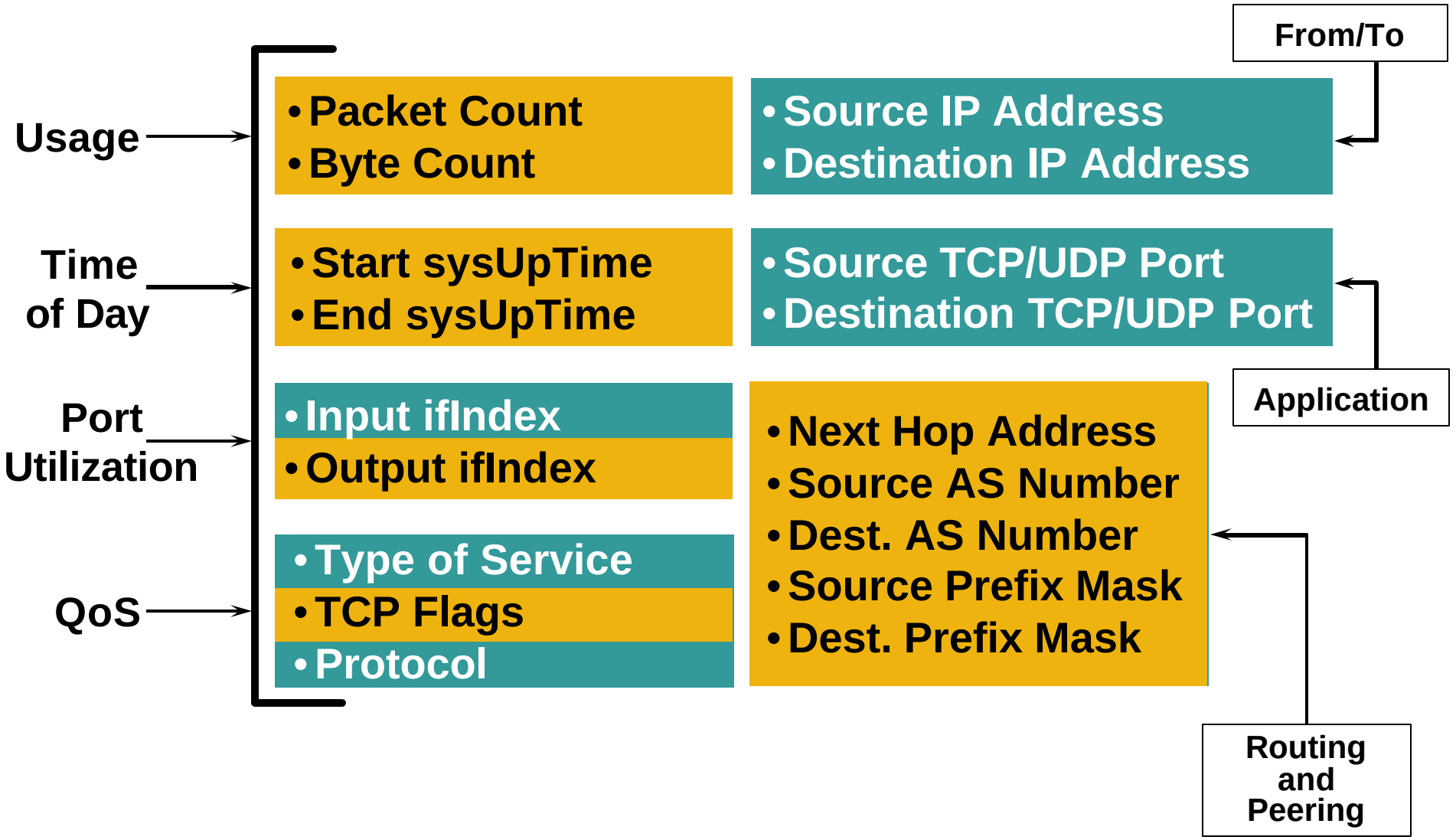
Destination-Only

VLAN	SRC IP	DST IP	IP Protocol	Src Port	Dst Port

Destination-Source

VLAN	SRC IP	DST IP	IP Protocol	Src Port	Dst Port

Version 5 Flow Format



NetFlow Cache Example

Cisco.com

1. Create and update flows in NetFlow cache

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	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	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	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

Aggregated Flows—Export Version 8 or 9

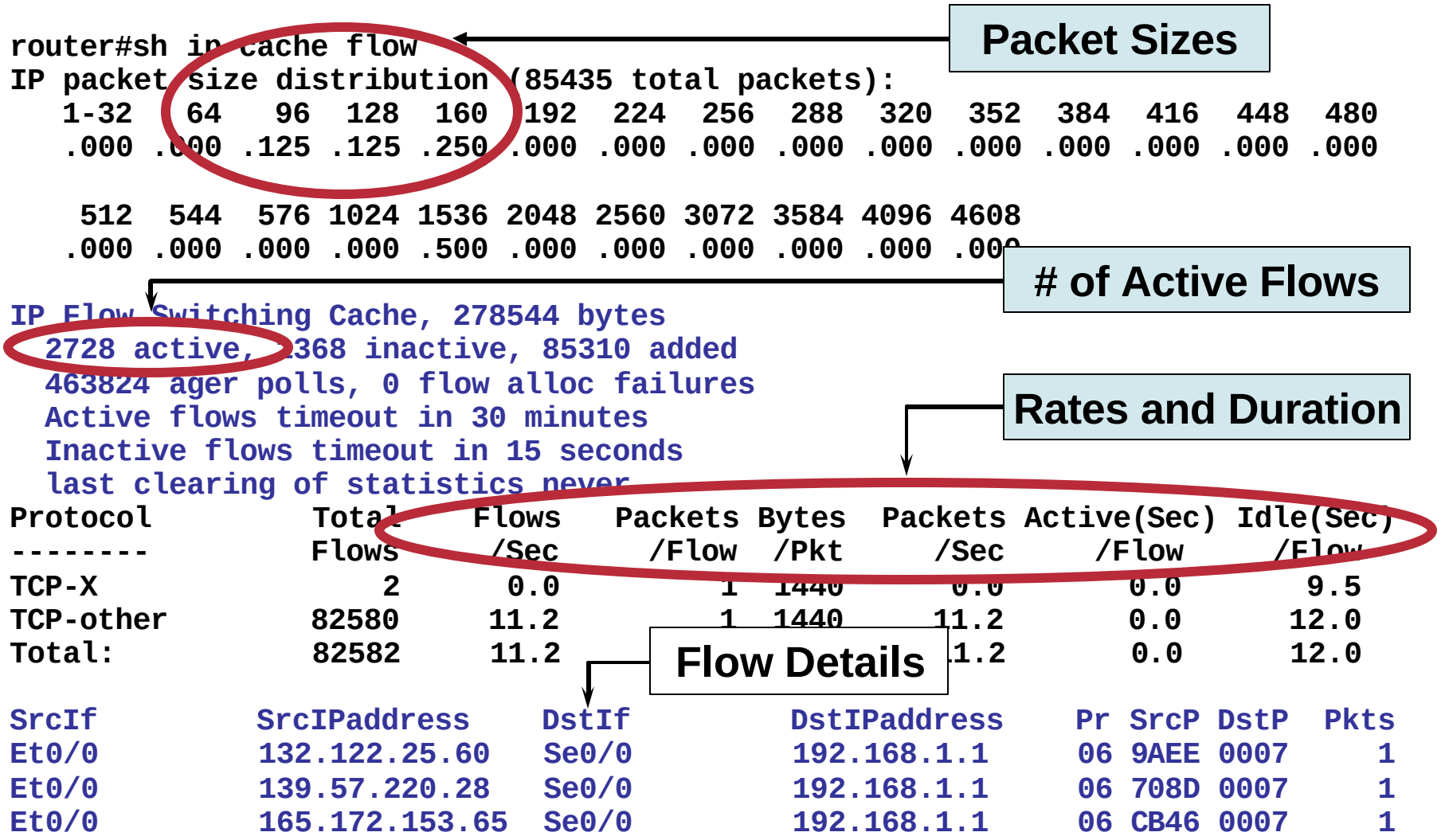
4. Export version

Non-Aggregated Flows—Export Version 5 or 9

5. Transport protocol

Export Packet

‘show ip cache flow’



‘show ip cache verbose flow’


```
router#sh ip cache verbose flow
IP packet size distribution (23597 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1323 active, 2773 inactive, 23533 added
  151644 ager polls, 0 flow alloc f
  Active flows timeout in 30 minut
  Inactive flows timeout in 15 sec
  last clearing of statistics neve
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           3.1         1  1440      3.1       0.0      12.9
Total:               3.1         1  1440      3.1       0.0      12.9

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr TOS Flgs Pkts
Port Msk AS                   Port Msk AS    NextHop             B/Pk  Active
Et0/0         216.120.112.114 Se0/0         192.168.1.1     06 00  10        1
5FA7 /0  0                    0007 /0  0     0.0.0.0              1440     0.0
Et0/0         175.182.253.65  Se0/0         192.168.1.1     06 00  10        1
```

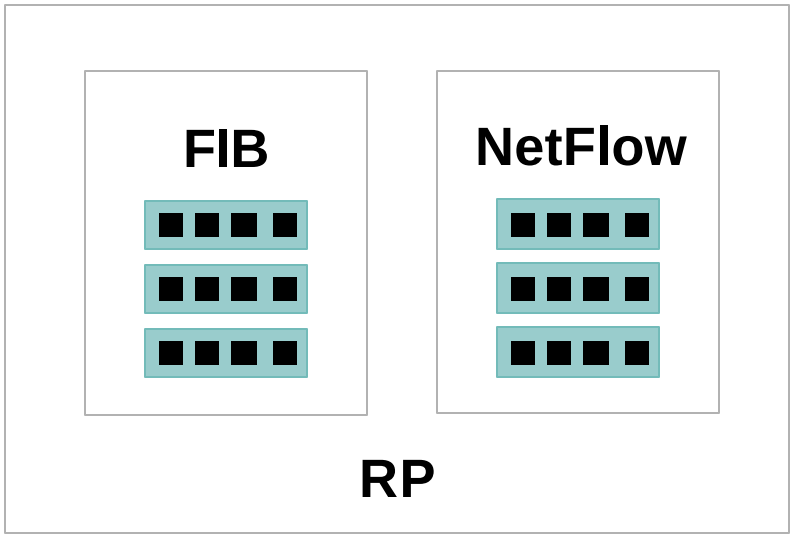
Flow Rate and Duration

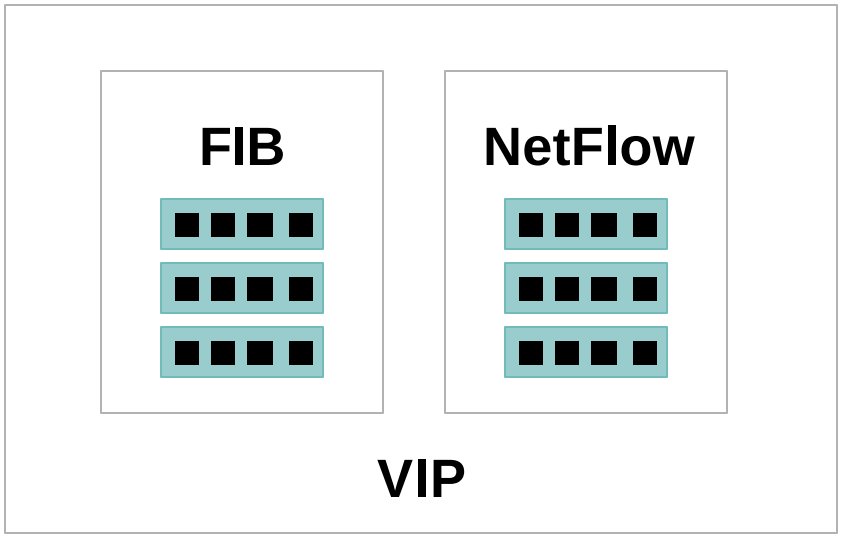
Destination Information

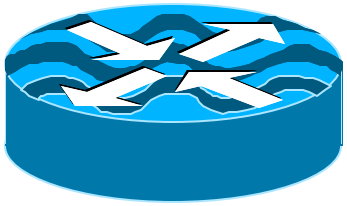
ToS Byte and TCP Flags

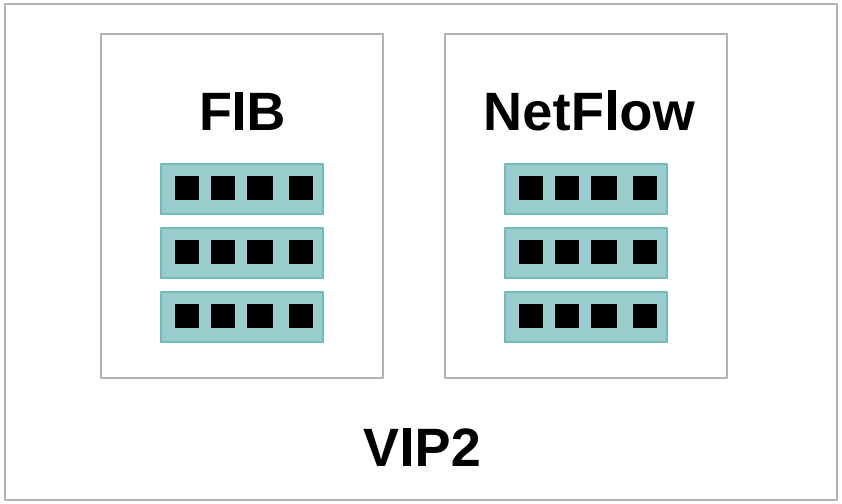
Source Mask and AS

Main Cache(s) with VIP and Line Card

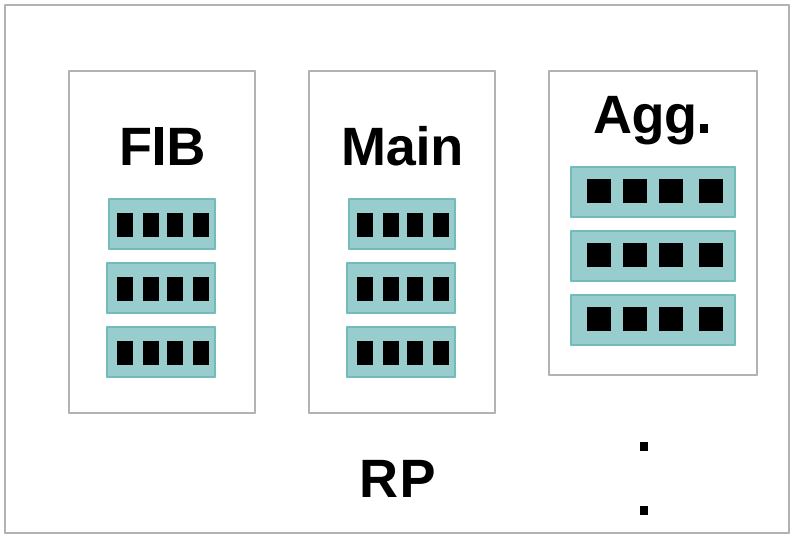


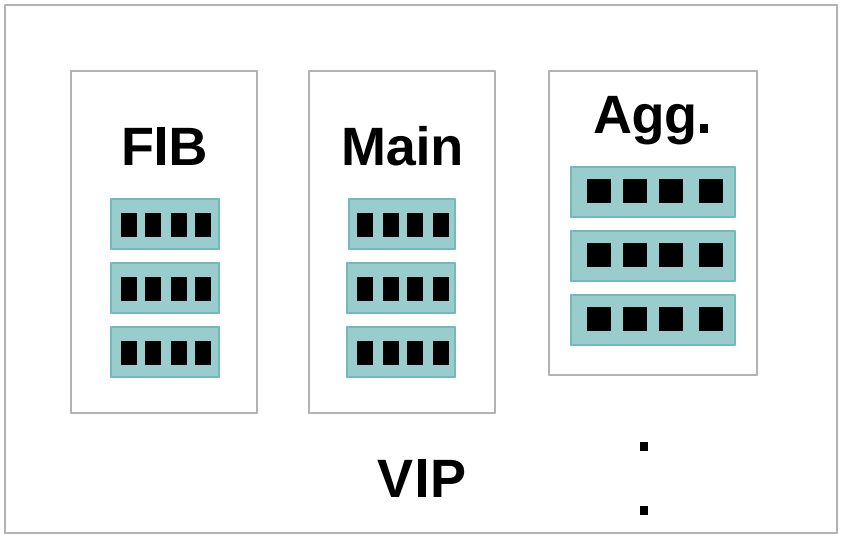


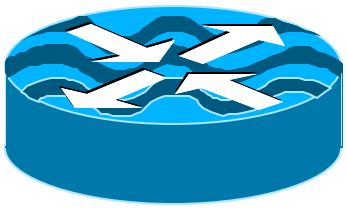


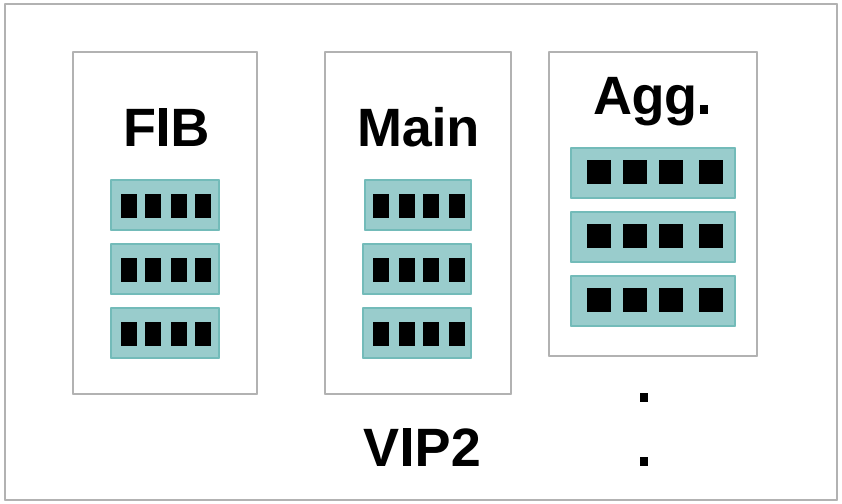


Aggregation Cache(s) with VIP and Line Card

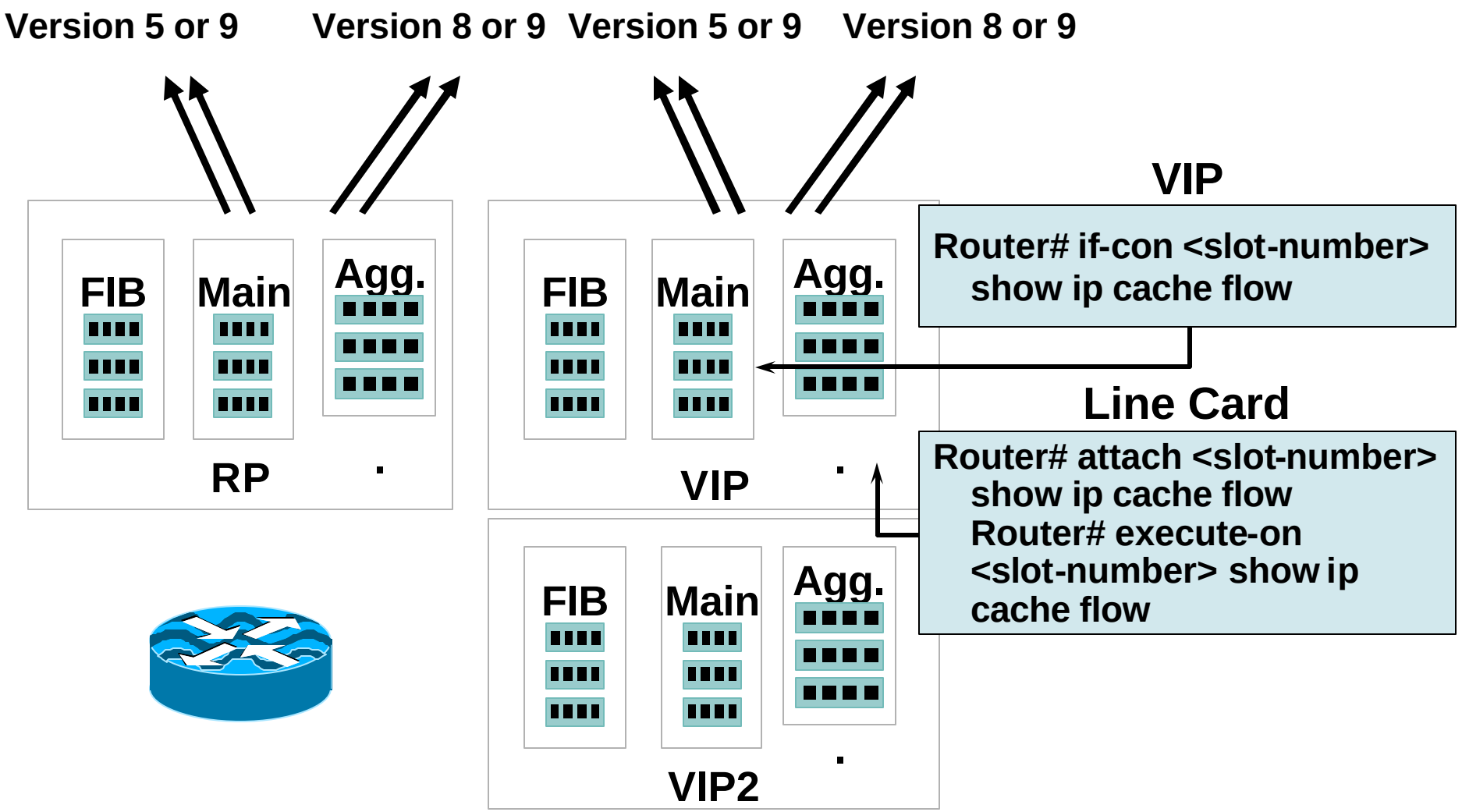








Aggregation Cache(s) with VIP and Line Card



NetFlow on Sub-Interface

- **“ip route-cache flow” enables NetFlow on the main interface and all the sub-interfaces**
- **Allow to enable NetFlow on selected sub-interfaces**

```
Router(config-if)# ip flow ingress
```

- **“ip flow ingress” introduced in 12.2(14)S, 12.2(15)T, 12.0(22)S, for the 7200, 7400 and 7500**

  http://www.cisco.com/go/fn

- **“ip route-cache flow” should not be used anymore**

NETFLOW MIB

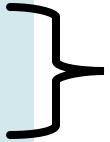
CISCO-NETFLOW-MIB

Cisco.com

- **Managed objects to configure the following NetFlow information:**
  - **Flow cache, Interface, Export**
- **Managed objects to monitor the following NetFlow information:**
  - **Configuration information, general statistics**
- **Example objects available:**
  - **Packet size distribution, Number of Bytes exported per second, Number of flows/UDP datagrams exported, Number of template active, etc…**
- **The CISCO-NETFLOW-MIB.my is NOT:**
  - **A replacement for the traditional method of exporting a flow cache**
  - **A way to retrieve all the flow records**
- **Note that CISCO-SWITCH-ENGINE-MIB, on the catalyst, allows to query the Multi Layer Switching Flow records**
- **Introduced in 12.2(25)S and 12.3(7)T**

NetFlow MIB
NetFlow Configuration


```
Router(config)# interface <slot/port>
Router(config-if)# ip flow ingress
Router(config-if)# ip flow egress
```



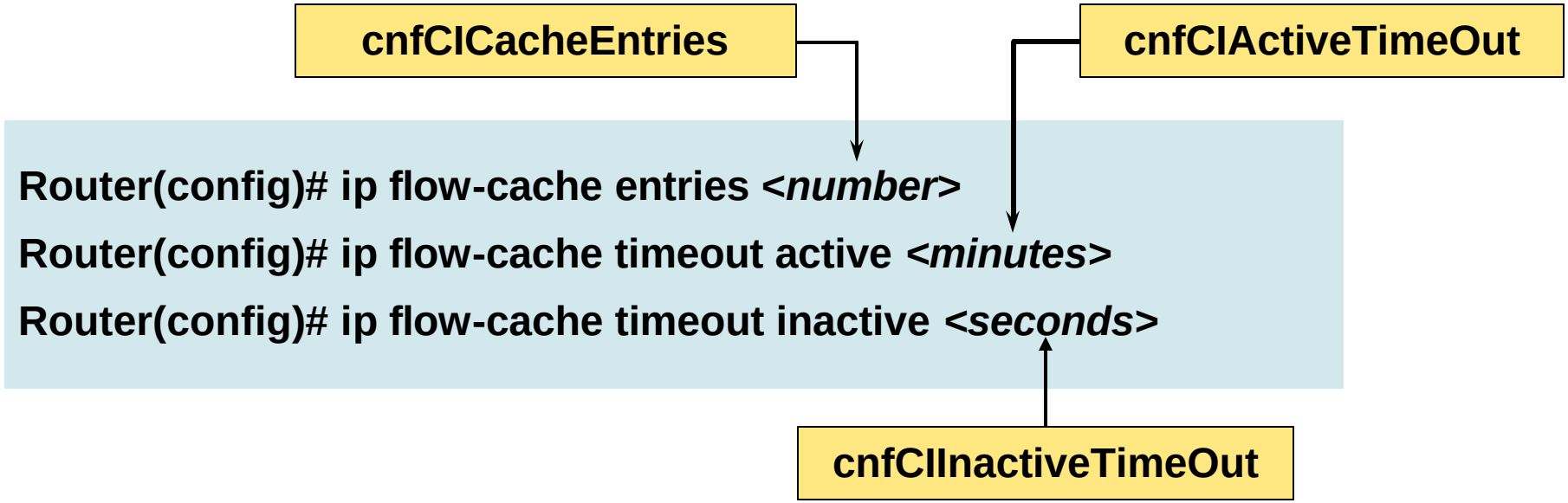
cnfCINetflowEnable

cnfCINetflowEnable

- Values for ingress, egress, ingress + egress, none
- Indexed by interface (ifIndex)
- Read-Write MIB variable
- Which sub-interfaces is NetFlow enabled on

NetFlow MIB
Main Cache Configuration

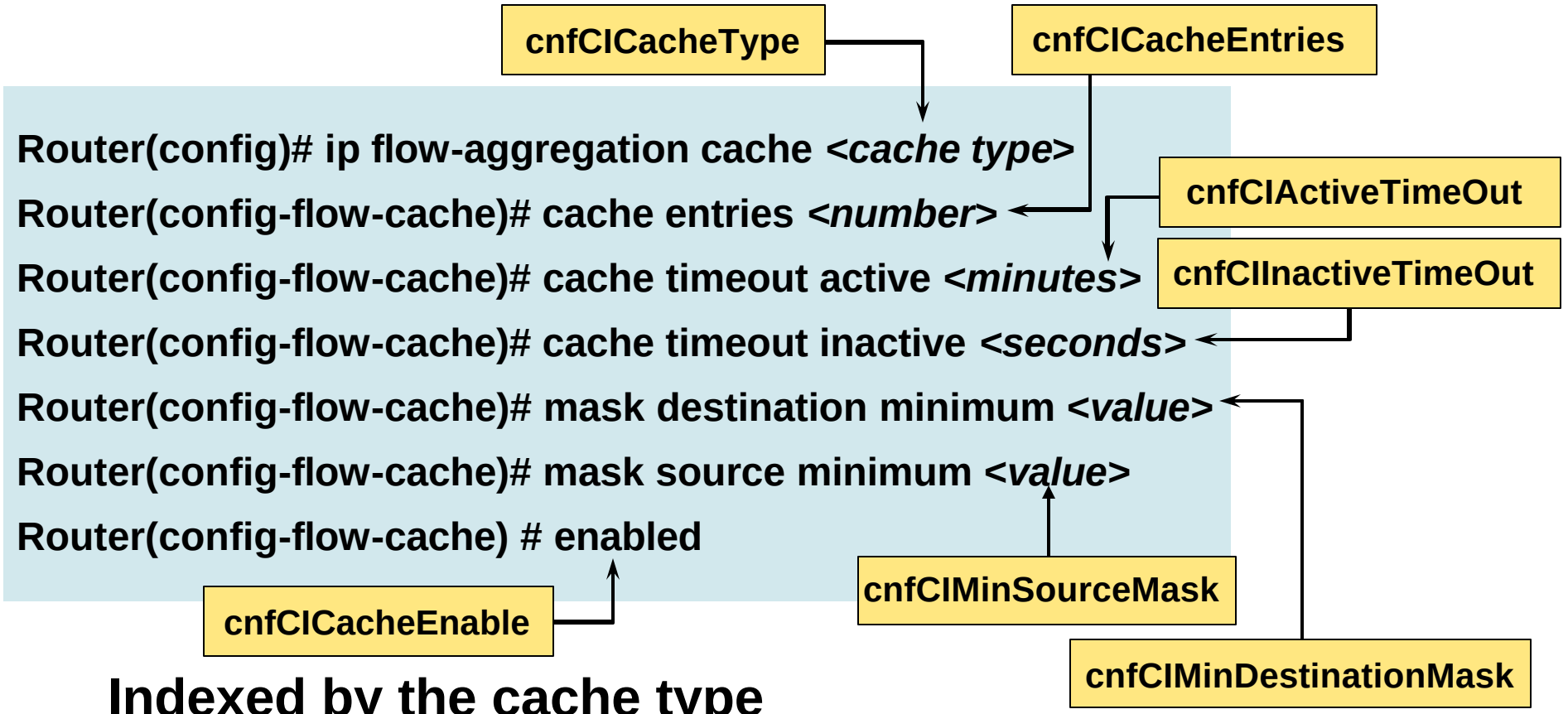
Cisco.com



Indexed by the cache type cnfClCacheType

- cnfClCacheType = 0 means the main cache

NetFlow MIB
Aggregation Cache Configuration



Indexed by the cache type

- As many cnfCICacheType values as aggregation cache types:
- main(0), as(1), protocolPort(2), sourcePrefix(3), etc…

NetFlow MIB
Main Cache Export Configuration


```
Router(config)# ip flow-export version 9 peer-as bgp-nexthop
Router(config)# ip flow-export destination 10.10.10.10 1234

Router # show ip flow export
Flow export v9 is enabled for main cache
  Exporting flows to 10.10.10.10 (1234)
  Exporting using source interface Loopback0
  Version 9 flow records, peer-as
```

cnfEIExportInfoTable

- **cnfEIExportInfoEntry**
  - **INDEX cnfCICacheType**
  - **cnfEIExportVersion**
  - **cnfEIPeerAS**
  - **cnfEIOriginAS**
  - **cnfEIBgpNextHop**

cnfEICollectorTable

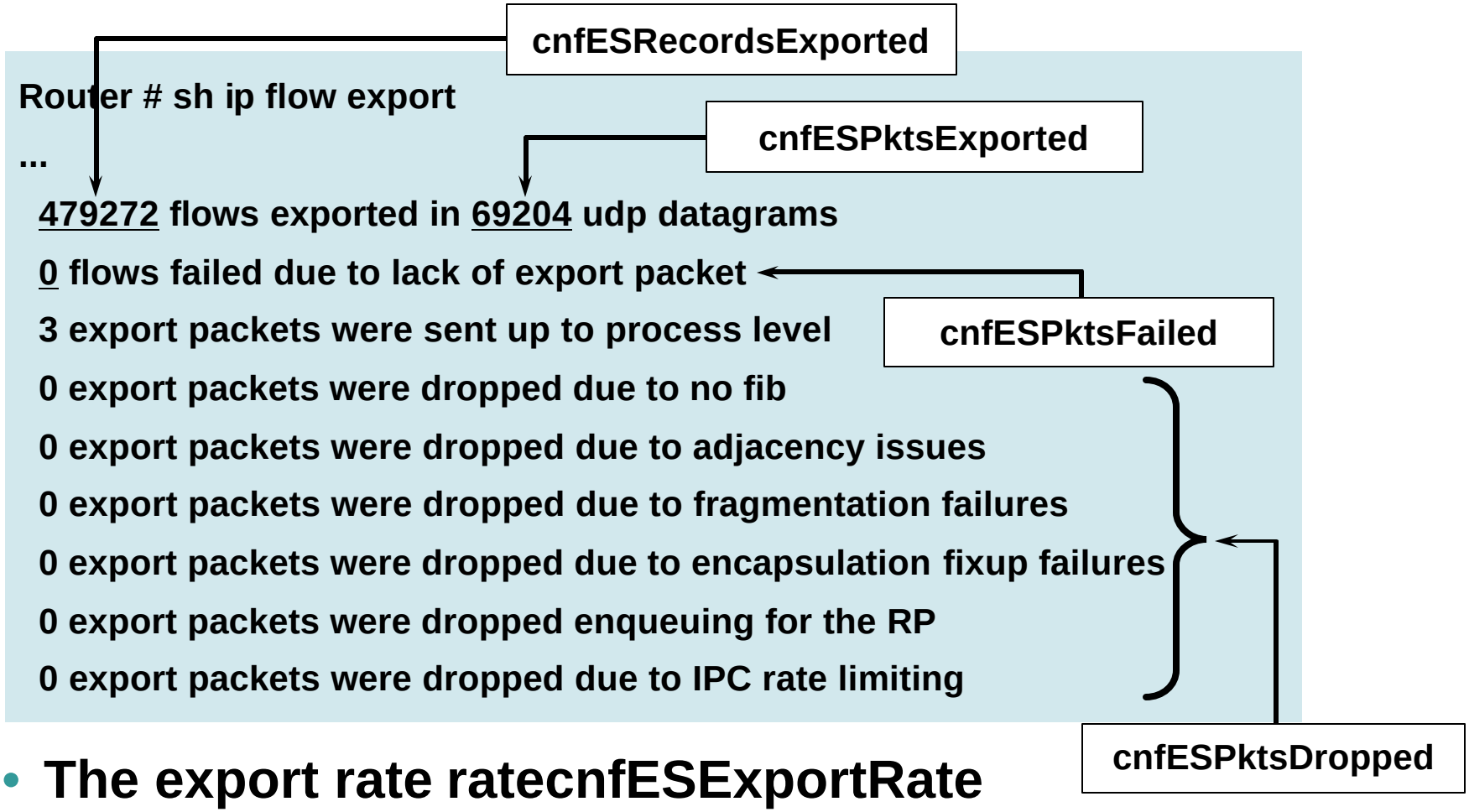
- **cnfEICollectorEntry**
  - **INDEX cnfCICacheType**
  - **cnfEICollectorAddressType**
  - **cnfEICollectorAddress**
  - **cnfEICollectorPort**
  - **cnfEICollectorStatus**

NetFlow MIB
Aggregation Cache Export Configuration


```
Router(config)# ip flow-aggregation cache <cache type>
Router(config-flow-cache)# export version 9
Router(config-flow-cache)# export destination 10.10.10.10 1234

Router # show ip flow export
...
Cache for <cache type> aggregation:
   Exporting flows to 10.10.10.10 (1234)
   Exporting using source IP address 192.2.1.5
```

- **Same principle, indexed by cnfCICacheType for the cache type**

NetFlow MIB Monitoring



- **The export rate ratecnfESExportRate**
  - **Useful to estimate the required bandwidth**

NetFlow MIB Monitoring


```
Router# sh ip cache flow
IP packet size distribution (311656 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .356 .316 .144 .115 .004 .003 .000 .007 .001 .000 .002 .017 .018 .009 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

cnfPSPacketSizeDistribution

cnfPSProtocolStatTable

…

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	33	0.0	65	40	0.0	18.4	10.0
TCP-WWW	3	0.0	5	45	0.0	3.0	1.2
TCP-BGP	5343	0.0	2	47	0.0	5.1	11.1
TCP-other	411	0.0	2	48	0.0	1.0	10.9
UDP-other	98614	0.4	2	76	0.9	2.1	10.8
ICMP	9519	0.0	9	71	0.4	21.3	11.5
Total:	113923	0.5	2	73	1.4	3.8	10.9

NetFlow MIB Applications

- NetFlow Configuration
- Checking NetFlow Configuration
  - Ex: peer-as or origin-as
- Monitoring and Security
  - Export Statistics
  - Protocol Statistics
  - Top Flows Information (More on this later ☺)
- Thresholding with the RMON event/alarm or the EVENT-MIB

NETFLOW VERSION 9

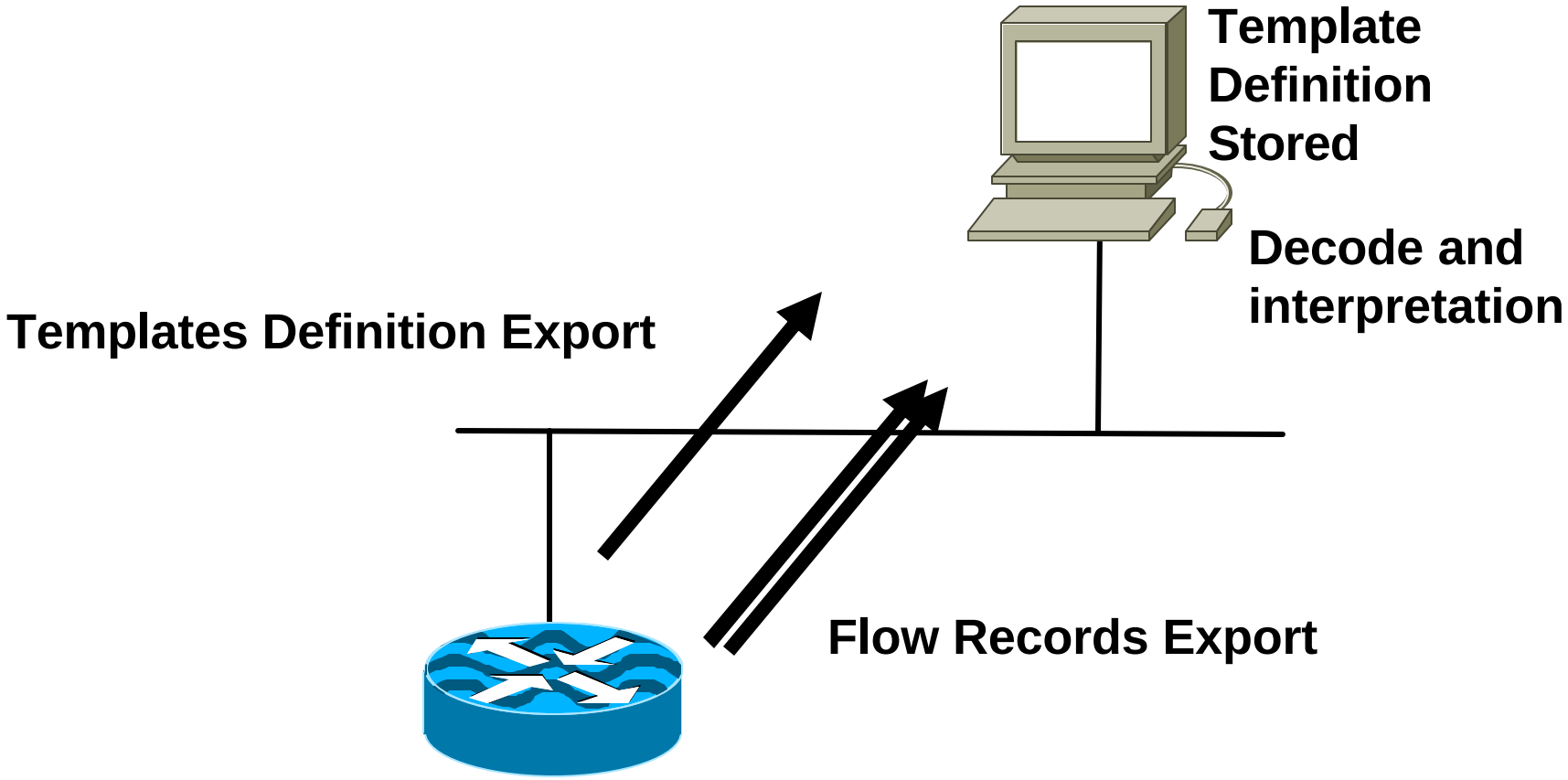
NetFlow Version 9

- **Version 9 is an export protocol**
  - **No changes to the metering process**
- **Version 9 based on templates and separate flow records**
  - **Templates composed of type and length**
  - **Flow records composed of template ID and value**
  - **Sent the template regularly (configurable), because of UDP**
- **Independent of the underlying protocol, it is ready for any reliable protocol (i.e. TCP, SCTP)**
  SCTP: Stream Control Transport Protocol
- **RFC 3954 "Cisco Systems NetFlow Services Export Version 9"**
- **12.0(24)S, 12.3(1), 12.2(18)S for the 800, 1700, 1800, 2600, 2800, 3600, 7200, 7300, 7500, 12000**
  - **Catalyst 6500 support soon**
  - **10000 support soon (with BGP next hop)**

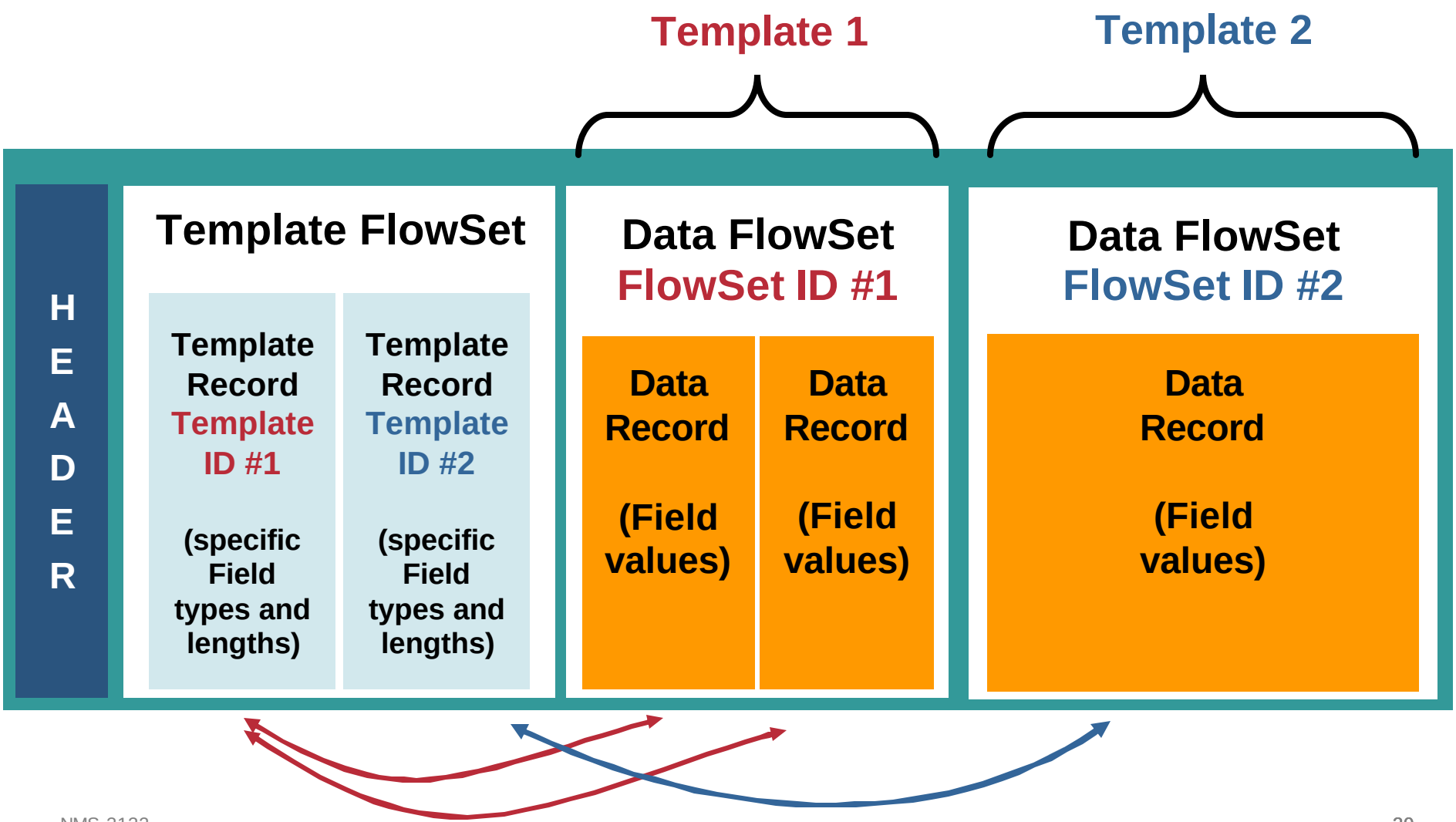
Extensibility and Flexibility Phases Approach

- **Why a new export protocol?**
  - Build a flexible and extensible export format!
  - Advantage: we can add new technologies/data types very quickly
    - Example: MPLS, IPv6, BGP next HOP
- **Phase 1: NetFlow Version 9, completed**
  - Advantages: extensibility
    - Integrate new technologies/data types quicker
    - Integrate new aggregations quicker
  - Note: for now, the template definitions are fixed!
- **Phase 2: User defined templates, under investigation**
  - Advantages: cache and export content flexibility
    - Selection of a subset of the 7 flow keys
    - Selection of the data types to export

NetFlow Version 9 Scenario #1

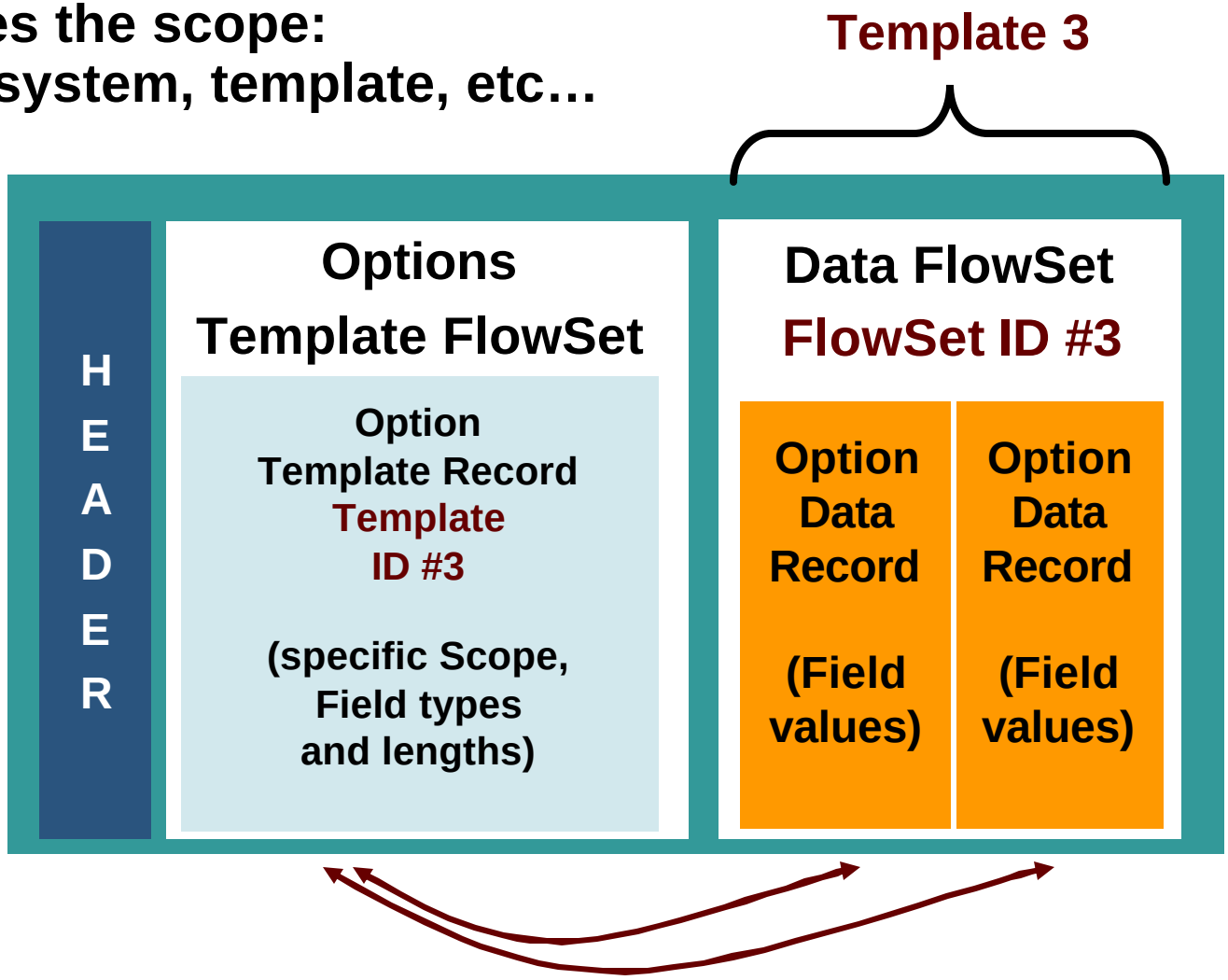


NetFlow Version 9 Export Packet

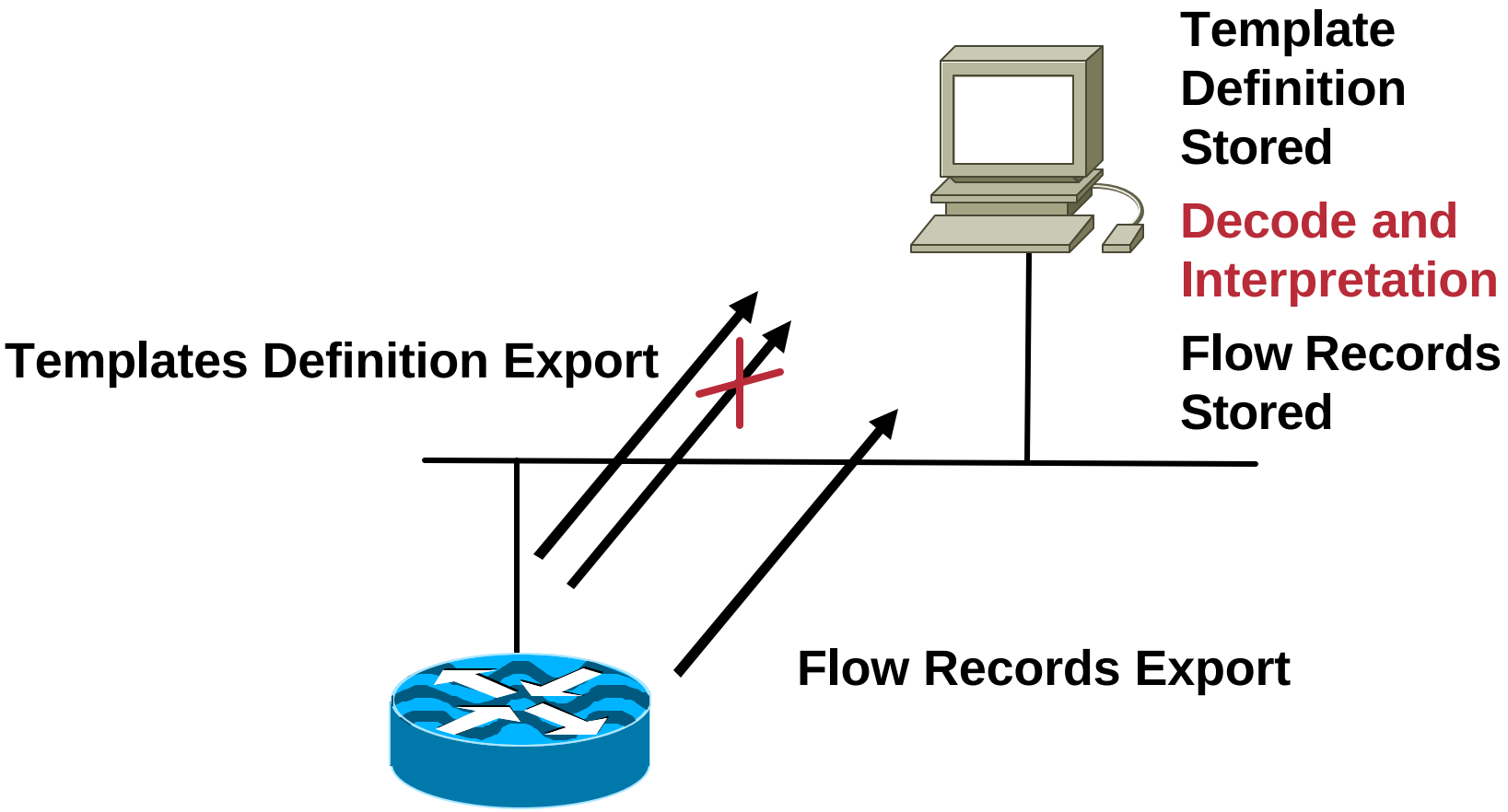


NetFlow Version 9 Export Packet

Options Template FlowSet specifies the scope: cache, system, template, etc…



NetFlow Version 9 Scenario #2

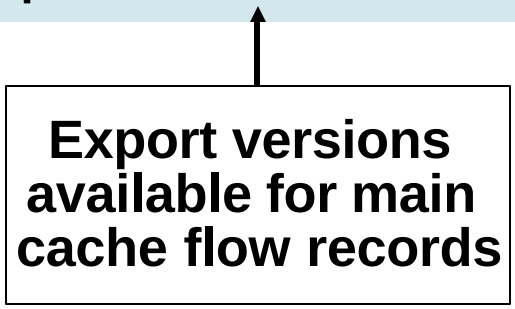


- The NetFlow collector should store the flow record and decode it after the template definition is received

NetFlow Version 9 Configuration

- **Main cache configuration**

```
router(config)# ip flow-export version 9 [origin-as|peer-as] [bgp-nexthop]
router(config)# ip flow-export template options export-stats
router(config)# ip flow-export template options timeout 30
router(config)# ip flow-export template refresh-rate 20
router(config)# ip flow-export destination 10.10.10.10 9996
```



Should you export from the main cache with NetFlow Version 5 or Version 9?

NetFlow Version 9 Configuration

Aggregation Cache Configuration

```
router(config)# ip flow-aggregation cache bgp-nexthop-tos
router(config-flow-cache)# enabled
router(config-flow-cache)# export destination 11.11.11.11 9999
  destination Specify the Destination IP address
  version configure aggregation cache export version
router(config-flow-cache)# export version ?
  8  Version 8 export format
  9  Version 9 export format
router(config-flow-cache)# export version 9
```

Sometimes available: in this case we have only Version 9. Why?

NetFlow Template Record Template for the BGP Next HOP ToS Aggregation

Cisco.com

New data template from 10.49.157.204: id=257, fields=11

field id=21 (LAST_SWITCHED), offset=0, len=4

field id=22 (FIRST_SWITCHED), offset=4, len=4

field id=1 (BYTES_32), offset=8, len=4

field id=2 (PKTS_32), offset=12, len=4

field id=10 (INPUT_SNMP), offset=16, len=2

field id=14 (OUTPUT_SNMP), offset=18, len=2

field id=5 (TOS), offset=20, len=1

field id=3 (FLOWS), offset=21, len=4

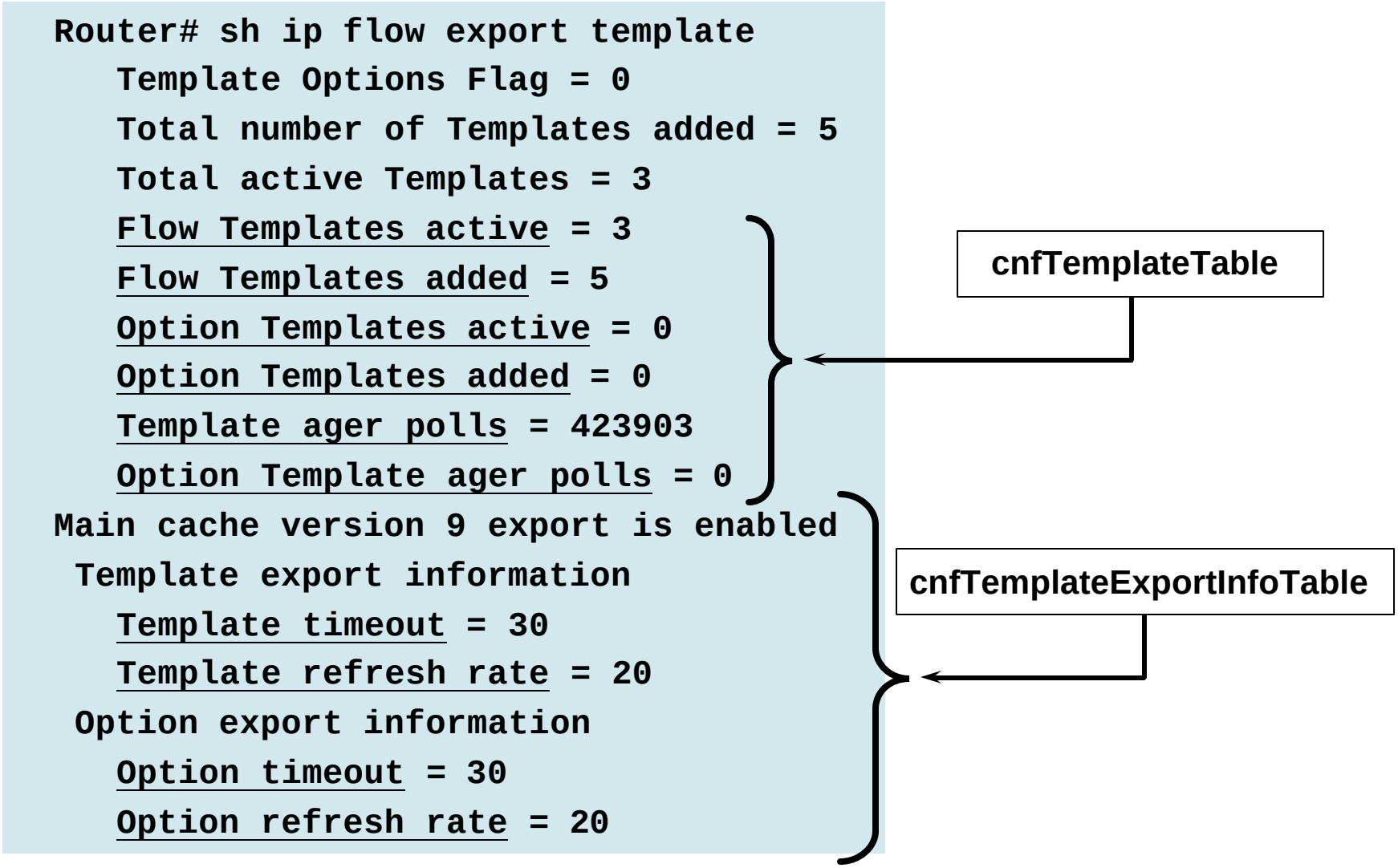
field id=17 (DST_AS), offset=25, len=2

field id=18 (BGP_NEXT_HOP), offset=27, len=4

field id=16 (SRC_AS), offset=31, len=2

NetFlow Version 9 Monitoring


```
Router# sh ip flow export template
   Template Options Flag = 0
   Total number of Templates added = 5
   Total active Templates = 3
   Flow Templates active = 3
   Flow Templates added = 5
   Option Templates active = 0
   Option Templates added = 0
   Template ager polls = 423903
   Option Template ager polls = 0
Main cache version 9 export is enabled
 Template export information
   Template timeout = 30
   Template refresh rate = 20
 Option export information
   Option timeout = 30
   Option refresh rate = 20
```

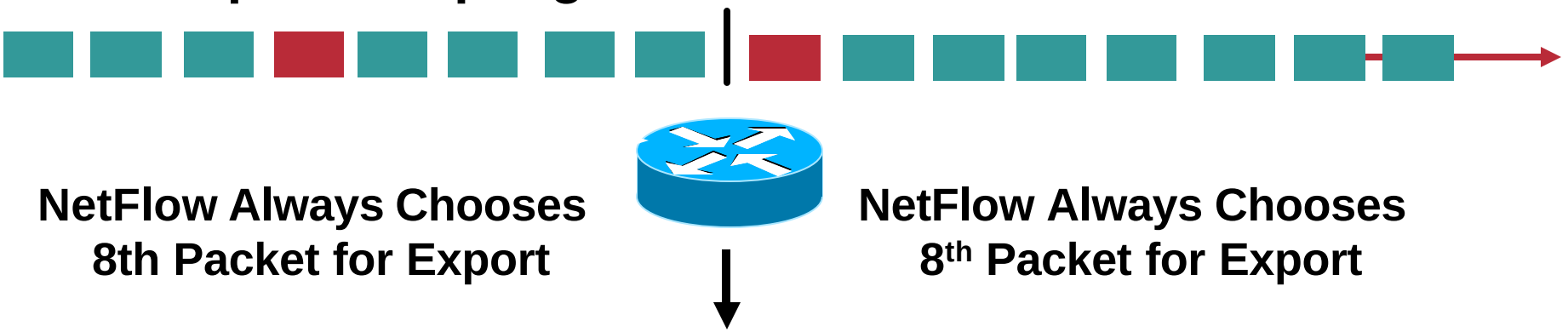


NETFLOW SAMPLING and FILTERING

Deterministic Sampled NetFlow

Deterministic Sampled NetFlow
Also Call Systematic Sampled NetFlow

Example: Sampling 1 out of 8 Packets

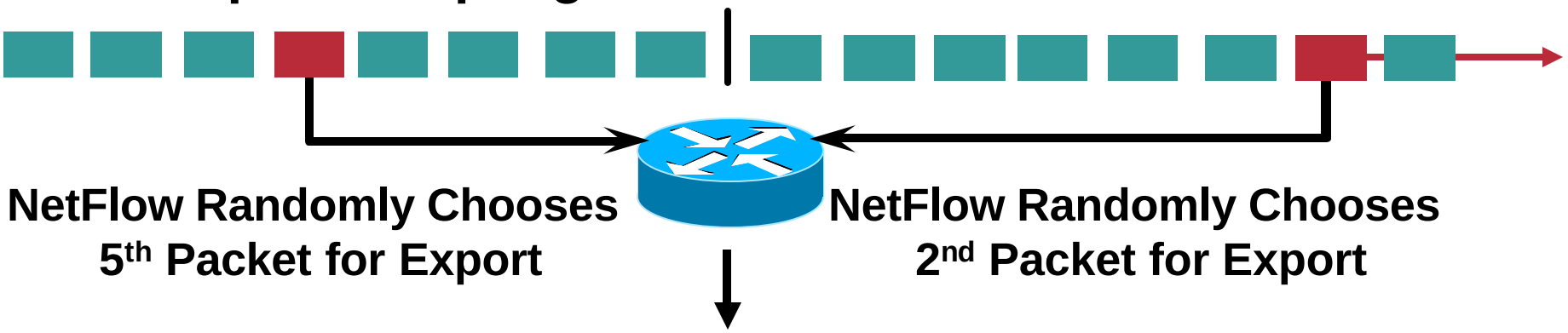


Potential Bias:
If Traffic Repetition = Multiple of Sampling Rate

Random Sampled NetFlow

Random Sampled NetFlow

Example: Sampling 1 Out of 8 Packets



No Traffic Repetition Issue

Sampled NetFlow

- Capacity planning may not need every packet per Flow
- Sampling will reduce CPU consumption
- Random (select packet to export per statistical principles)
  - Cisco IOS Software Releases 12.0(26)S, 12.2(18)S, and 12.3(1)T
  - Software platforms 7xxx, 37xx, 36xx, 26xx…
  - Cisco 12000 series: deterministic sampling today
  - Catalyst 6000: no packet sampling but flow sampling

Random Sampled NetFlow


```
router(conf)# flow-sampler-map mysampler1
Router(config-sampler)# mode random one-out-of 100

Router(config)# interface ethernet 1
Router(config-if)# flow-sampler mysampler1

Router(config)# ip flow-export template options sampling

Router# show flow-sampler
Sampler : mysampler1, id : 1, packets matched : 10
  mode : random sampling mode
  sampling interval is : 100
```

Must explicitly configure it on sub-interfaces

Sampling NetFlow on the Catalyst Flow Sampling

- **Not packet sampling but flow sampling**

  Reason: NetFlow in hardware on the catalyst

- **Time based flow sampling**

  Take a snapshot of the NetFlow cache at different time

- **Packet based flow sampling**

  At each Delta_T, export the flows with minim values of packet M

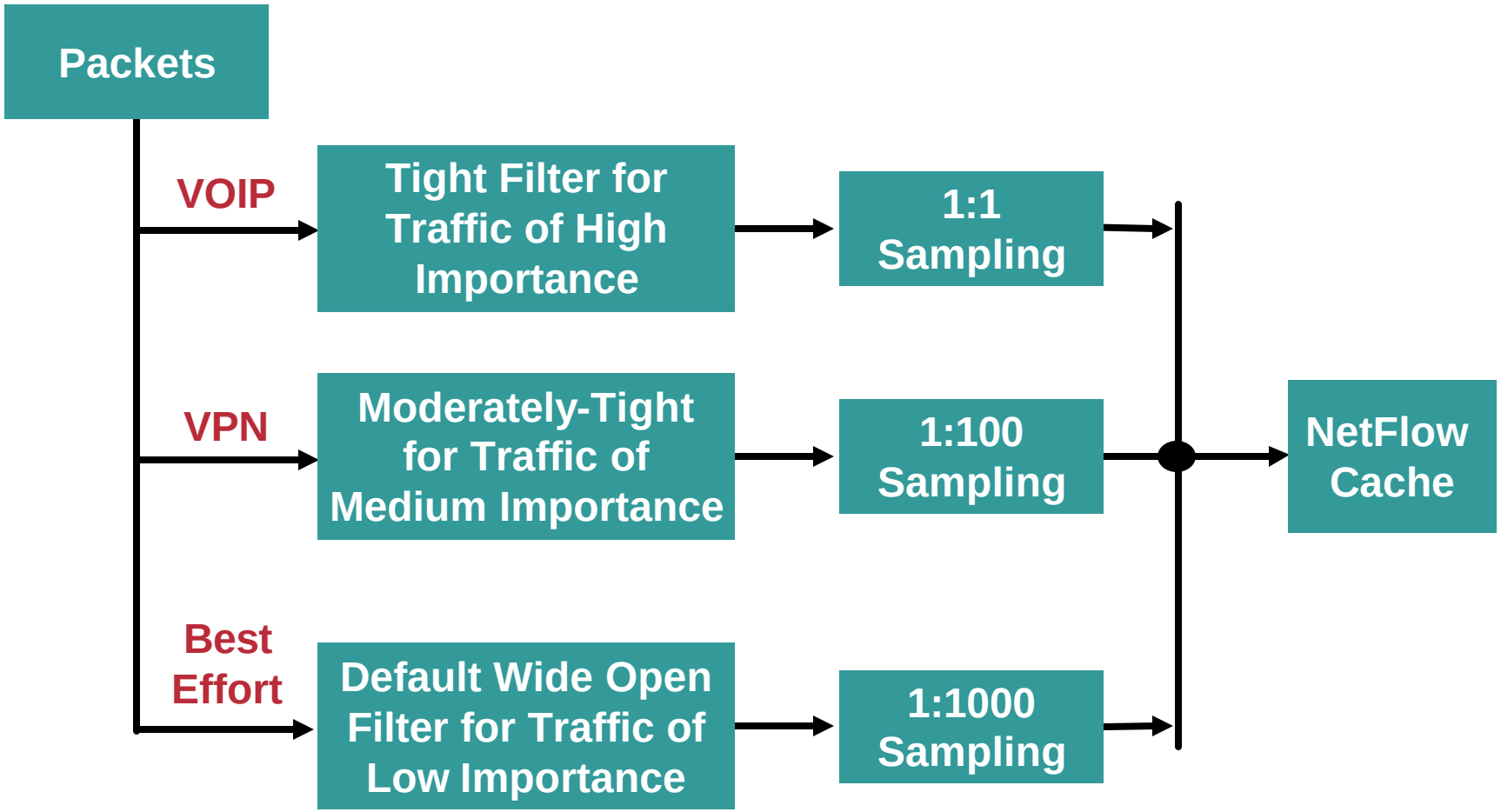
  For flows with packet count < M, packet counts will be summed up, and one flow will be sent

NetFlow Input Filters

Cisco.com

- **Support prefiltering for traffic for NetFlow processing**
- **Modular QoS Command Line (MQC) will provide the filtering mechanism for NetFlow**
  - **Classification by IP source and destination addresses, Layer 4 protocol and port numbers, Incoming interface, MAC address, DSCP**
  - **Layer 2 information such as Frame Relay DE bits, Ethernet 802.1p bits**
  - **Network Based Application recognition (NBAR)**
- **Ability to sample filtered data at different rates, depending on how interesting the traffic is**
- **12.3(4)T, 12.2(25)S**

NetFlow Input Filters Example



NetFlow Input Filters Configuration


```
Router(config)# class-map high_importance_class
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config)# class-map medium_importance_class
Router(config-cmap)# match access-group 102
Router(config-cmap)# exit
```

Define Traffic Classes (MQC)

```
Router(config)# flow-sampler-map high_sampling
Router(config-sampler-map)# mode random one-out-of 1
Router(config-sampler-map)# exit
Router(config)# flow-sampler-map medium_sampling
Router(config-sampler-map)# mode random one-out-of 100
Router(config-sampler-map)# exit
Router(config)# flow-sampler-map low_sampling
Router(config-sampler-map)# mode random one-out-of 1000
Router(config-sampler-map)# exit 18
```

Define NetFlow Samplers

NetFlow Input Filters Configuration


```
Router(config)# policy-map mypolicy
Router(config-pmap)# class high_importance_class
Router(config-pmap-c)# flow-sampler high_sampling
Router(config-pmap-c)# exit
Router(config-pmap)# class medium_importance_class
Router(config-pmap-c)# flow-sampler medium_sampling
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# flow-sampler low_sampling
Router(config-pmap-c)# exit
```

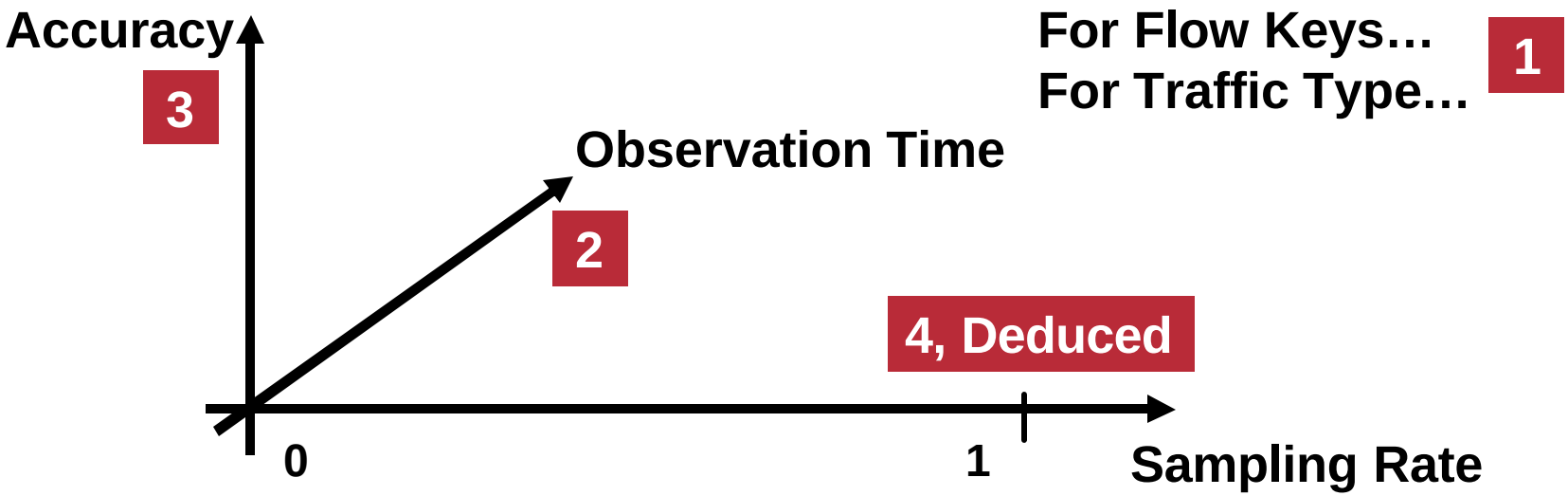
Define Policy with NetFlow Sampling Actions

```
Router(config)# interface POS1/0
Router(config-if)# service-policy input mypolicy
Router(config-if)# exit
Router(config)# interface ATM2/0
Router(config-if)# service-policy input mypolicy
```

Applying Policy with Netflow Sampling Actions to Interface

Accuracy of Sampled NetFlow

- What is the accuracy of sampled NetFlow? That is: is the estimated number of bytes per flow record accurate?
- Which sample rate should be used?
- No easy answer

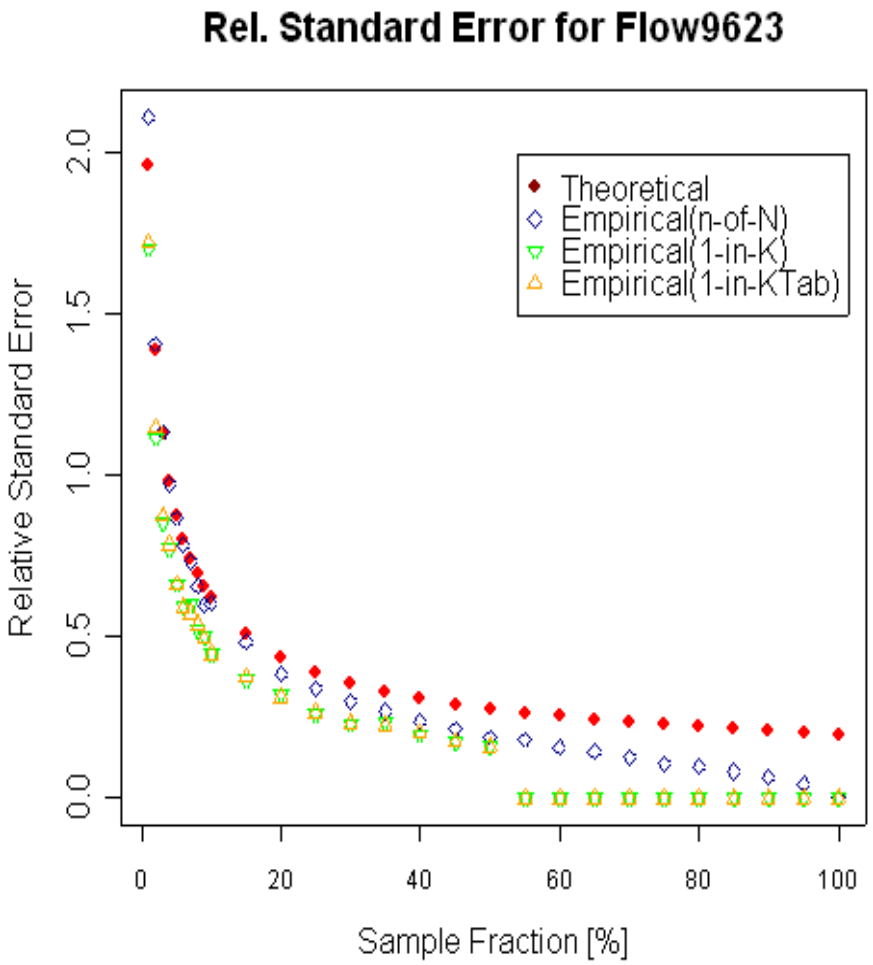


Accuracy of Sampled NetFlow Research Project

- Cisco funded an research by an external company
- State of the art analysis
  - Analysed many sampling researcher whitepapers
- Developed an mathematical model
  - This model is only valid for random sampled NetFlow!
  - Systematic sampled NetFlow would require some knowledge about the traffic patterns
  - A patent is in process of being filed

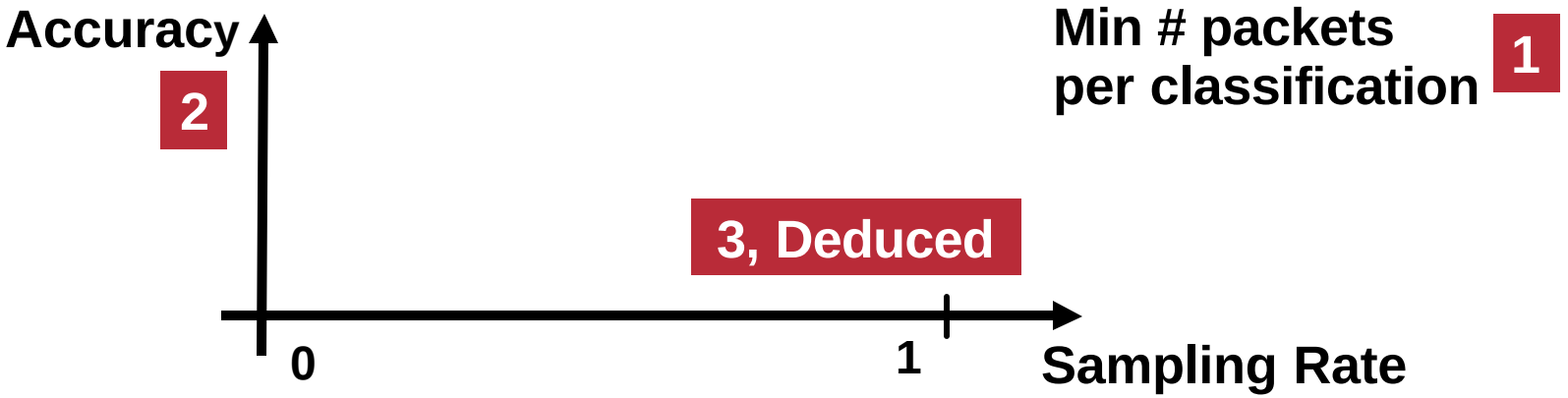
Accuracy of Sampled NetFlow Research Project

- **Empirical testing with real live testing**
  - **Mathematical model validity**
  - **Mathematical model assumptions**
  - **Results confidence interval**
  - **Graph the results**
- **Higher accuracy for flows with**
  - **Many packets**
    - **Flow proportion is high**
    - **Observe longer (AND characteristics remain)**
  - **Large packet size mean**
  - **Small packet size variation**



Accuracy of Sampled NetFlow Research Project

- What is the accuracy of sampled NetFlow?
  1. Depends on the sampling rate? ➔ Yes
  2. Depends on the flow definition? ➔ Not directly
  3. Depends on the traffic type (IPv4 versus MPLS)? ➔ Depends on traffic (flow characteristics)
  4. Depends on the observation period ➔ Yes, if characteristics remain
- Whitepaper will be published soon
- Next Step…Hope to get such a graph



NETFLOW FOR SECURITY

How to Identify a Security Attack?

- Suddenly highly-increased overall traffic in the network
- Higher CPU and memory utilization of network devices
- Unexpectedly large amount of traffic generated by individual hosts
- Increased number of accounting records generated
- Multiple accounting records with abnormal content, like one packet per flow record (e.g. TCP SYN flood)
- A changed mix of traffic applications, e.g. a sudden increase of “unknown” applications
- An increase of certain traffic types and messages, e.g. TCP resets or ICMP messages
- An increasing number of ACL violations

What Does a DoS Attack Look Like?


```
Router# show ip cache flow
…
SrcIf  SrcIPaddress SrcP  SrcAS  DstIf DstIPaddress  DstP  DstAS   Pr Pkts B/Pk
29     192.1.6.69     77    aaa     49   194.20.2.2  1308   bbb   6    1   40
29     192.1.6.222  1243    aaa     49   194.20.2.2  1774   bbb   6    1   40
29     192.1.6.108  1076    aaa     49   194.20.2.2  1869   bbb   6    1   40
29     192.1.6.159   903    aaa     49   194.20.2.2  1050   bbb   6    1   40
29     192.1.6.54    730    aaa     49   194.20.2.2  2018   bbb   6    1   40
29     192.1.6.136   559    aaa     49   194.20.2.2  1821   bbb   6    1   40
29     192.1.6.216   383    aaa     49   194.20.2.2  1516   bbb   6    1   40
29     192.1.6.111    45    aaa     49   194.20.2.2  1894   bbb   6    1   40
29     192.1.6.29   1209    aaa     49   194.20.2.2  1600   bbb   6    1   40
```

- **Typical DoS attacks have the same (or similar) entries:**
  - **Input Interface (SrcIf)**
  - **Destination IP (DstIf)**
  - **1 Packet per flow (Pkts)**
  - **Bytes per packet (B/Pk)**

Tracing DoS Attack with NetFlow 1/2

1. **To show high rate flows**

   router# show ip cache flow | include (K|M)

2. **To show all flows to one destination leverage**

   “router# sh ip cache (verbose) flow | include <destination>”

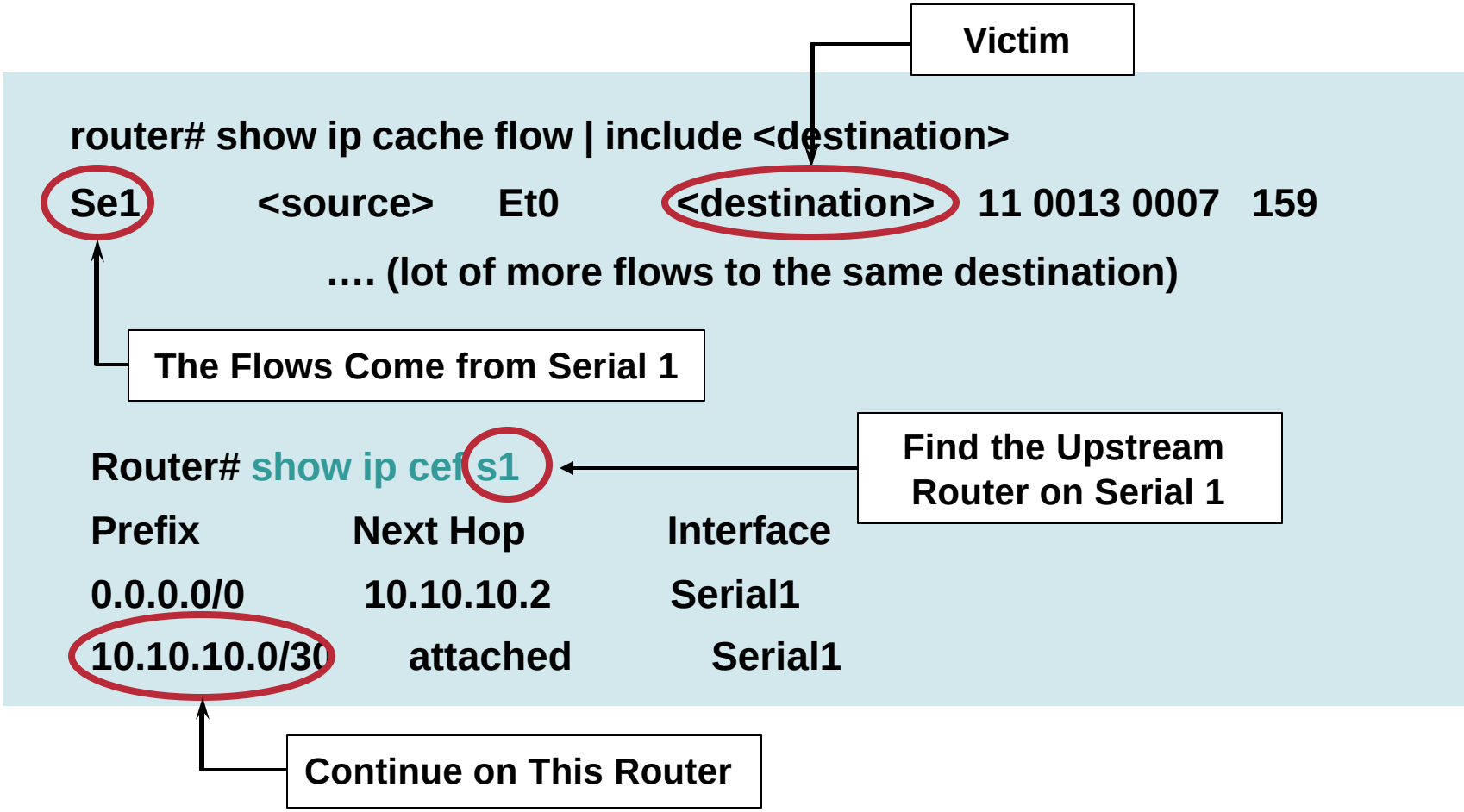
```
router# sh ip cache flow | include 194.20.2.2
…
SrcIf  SrcIPaddress  SrcP  SrcAS  DstIf DstIPaddress  DstP  DstAS Pr Pkts  B/Pk
29     192.1.6.69    77      aaa     49   194.20.2.2  1308  bbb    6    1    40
29     192.1.6.222   1243    aaa     49   194.20.2.2  1774  bbb    6    1    40
29     192.1.6.108   1076    aaa     49   194.20.2.2  1869  bbb    6    1    40
29     192.1.6.159   903     aaa     49   194.20.2.2  1050  bbb    6    1    40
…          …             …       …      …       …          …  …        …   …       ……
```

3. **To look for known attack signatures e.g. if we know of an attack using UDP port 666 (Hex 029A) we run**

   router# show ip cache flow | include 029A

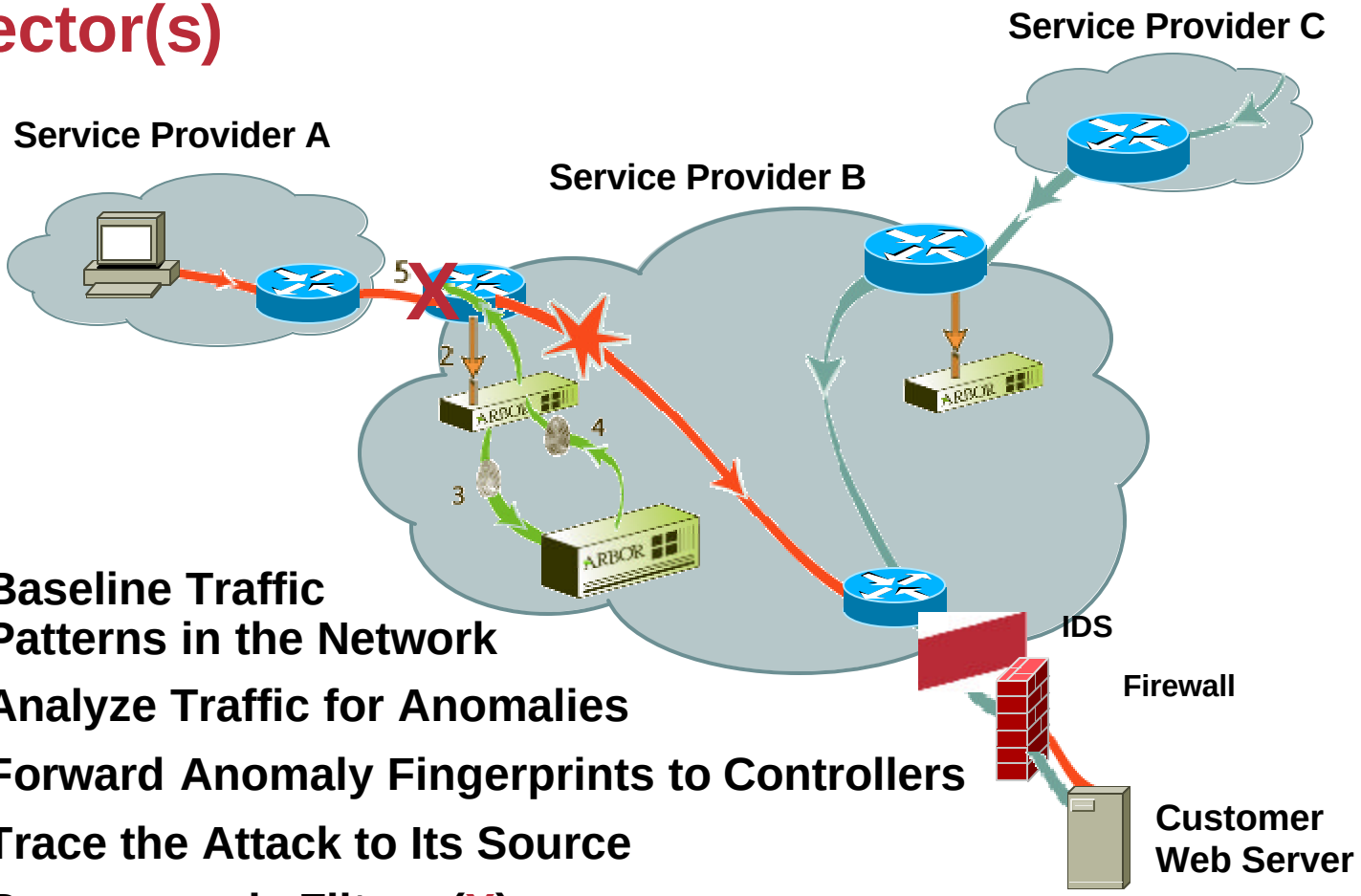
Tracing DoS Attack with NetFlow 2/2

- **Enable NetFlow on relevant routers/switches**



DoS Attack Example: Arbor Networks

Configure NetFlow Export to Arbor DoS Collector(s)



1. **Profile:** Baseline Traffic Patterns in the Network
2. **Monitor:** Analyze Traffic for Anomalies
3. **Detect:** Forward Anomaly Fingerprints to Controllers
4. **Trace:** Trace the Attack to Its Source
5. **Filter:** Recommends Filters (X)

Protego Networks Tracing Attack

Cisco.com

Incident Graph-245738986

Previous | Next | Toggle Topology

Session ID:
S:266156411

Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:

ICMP Ping Network Sweep

Session ID:
S:266156412

Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:

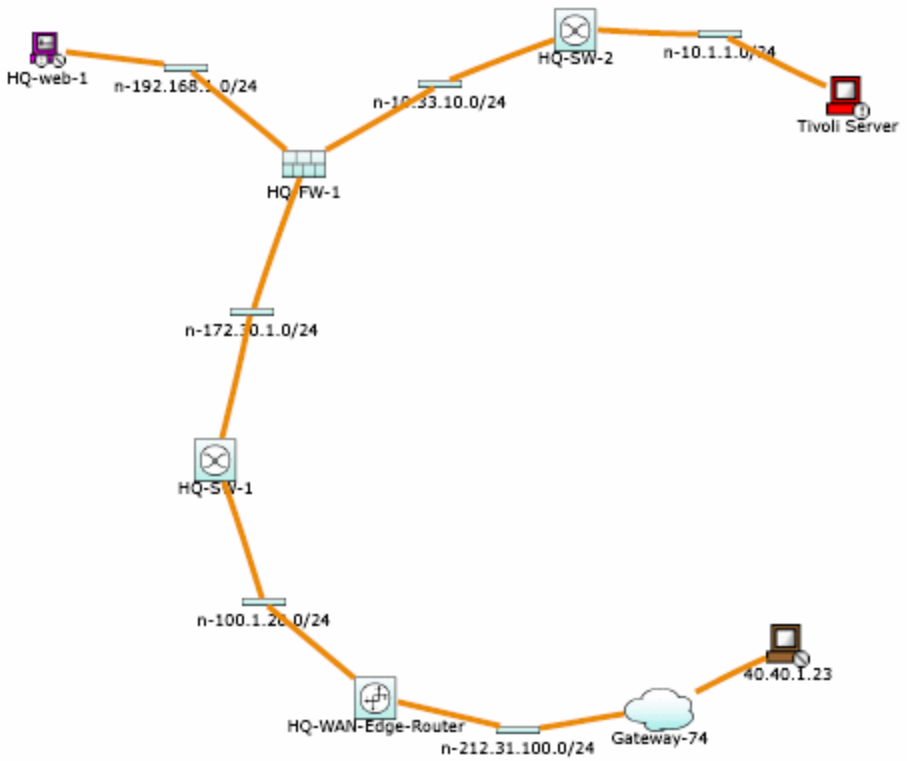
ICMP Ping Network Sweep

Session ID:
S:266156461

Src: 40.40.1.23/2500
Dest: 192.168.1.10/80
Event Types:

WWW IIS .ida Indexing Service Overflow

Session ID:
S:266167384



NetFlow L2 and Security Monitoring

Cisco.com

- **Layer 2 IP header fields**
  - **Source MAC address field from frames that are received by the NetFlow router**
  - **Destination MAC address field from frames that are transmitted by the NetFlow router**
  - **Received VLAN ID field (802.1q and Cisco's ISL)**
  - **Transmitted VLAN ID field (802.1q and Cisco's ISL)**
- **Extra Layer 3 IP header fields**
  - **Time-to-Live field**
  - **Identification field**
  - **Packet length field**
  - **CMP type and code**
- **Targeted for security: to help identify network attacks and their origin**
- **Introduced in 12.3(14)T on the low-end routers**

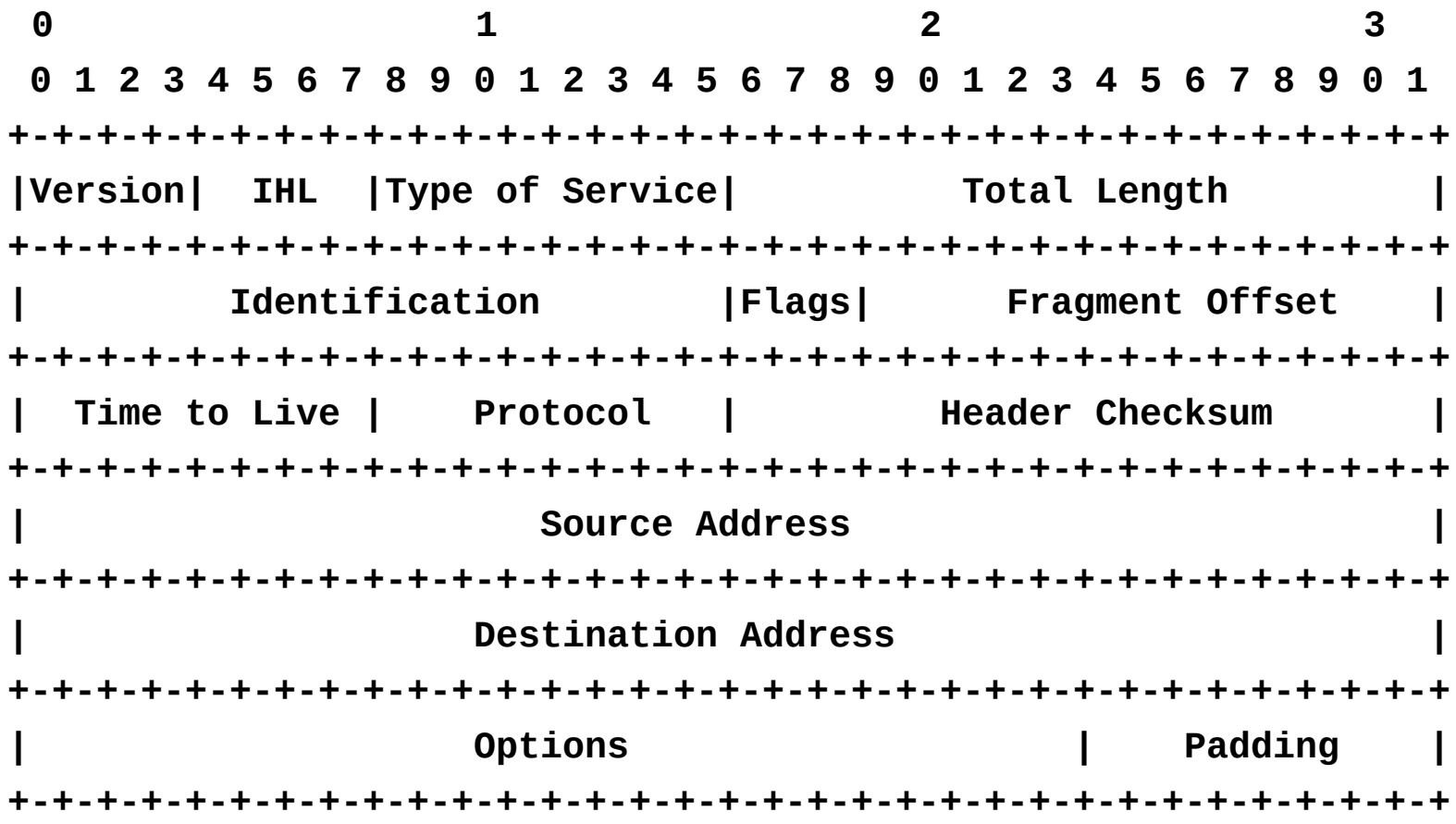
NetFlow L2 and Security Monitoring


```
Router(config)# ip flow-capture icmp
Router(config)# ip flow-capture ip-id
Router(config)# ip flow-capture mac-addresses
Router(config)# ip flow-capture packet-length
Router(config)# ip flow-capture ttl
Router(config)# ip flow-capture vlan-id
```

- **Not flow keys, the value of the first packet of the flow**
  - **Exception for packet length: min/max**
  - **Exception for the TTL: min/max**
- **Complete the main cache, not the aggregation caches**
  - **Info lost if an aggregation cache is used**

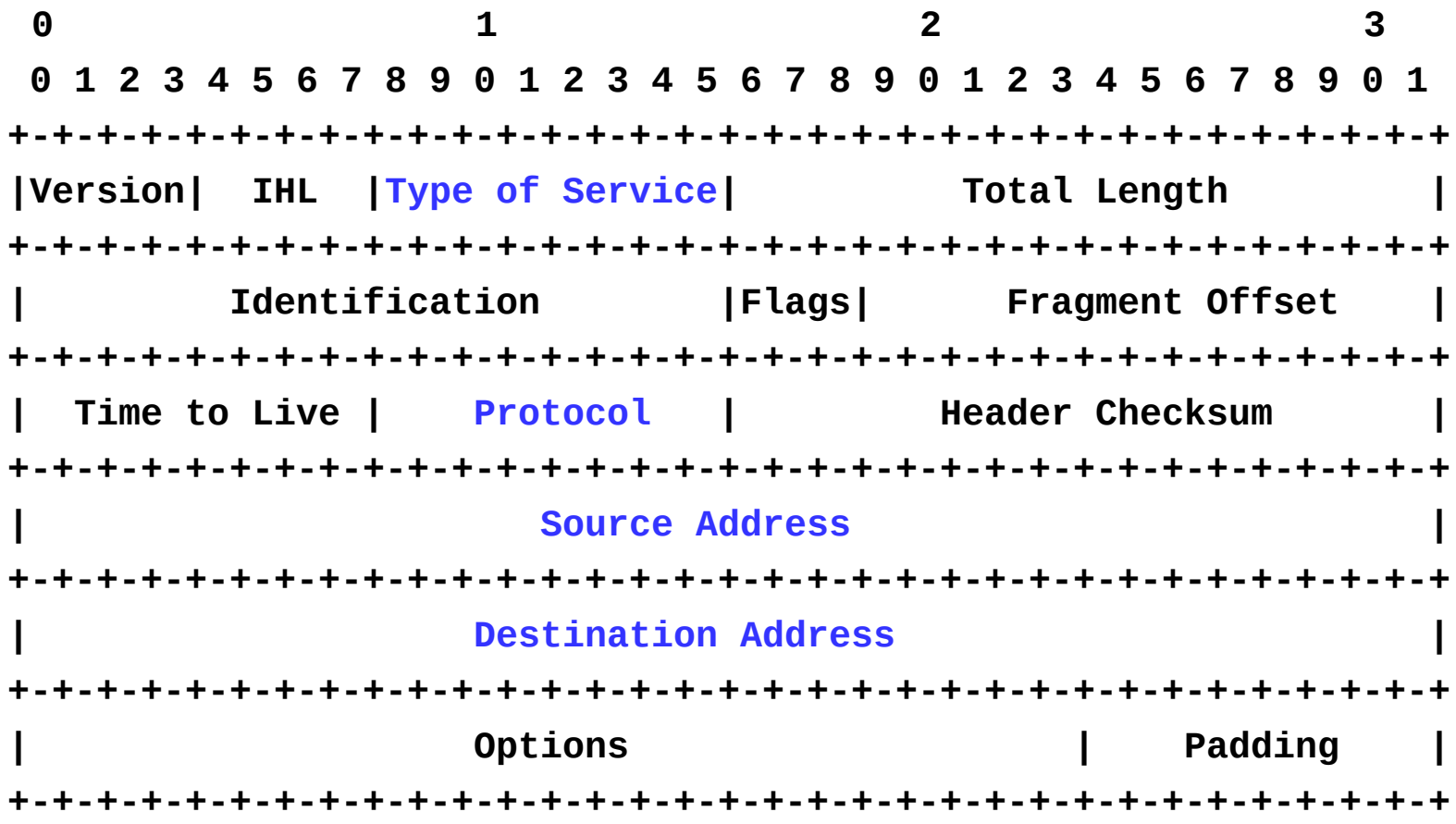
NetFlow L2 and Security Monitoring L3 Packet Format

Cisco.com



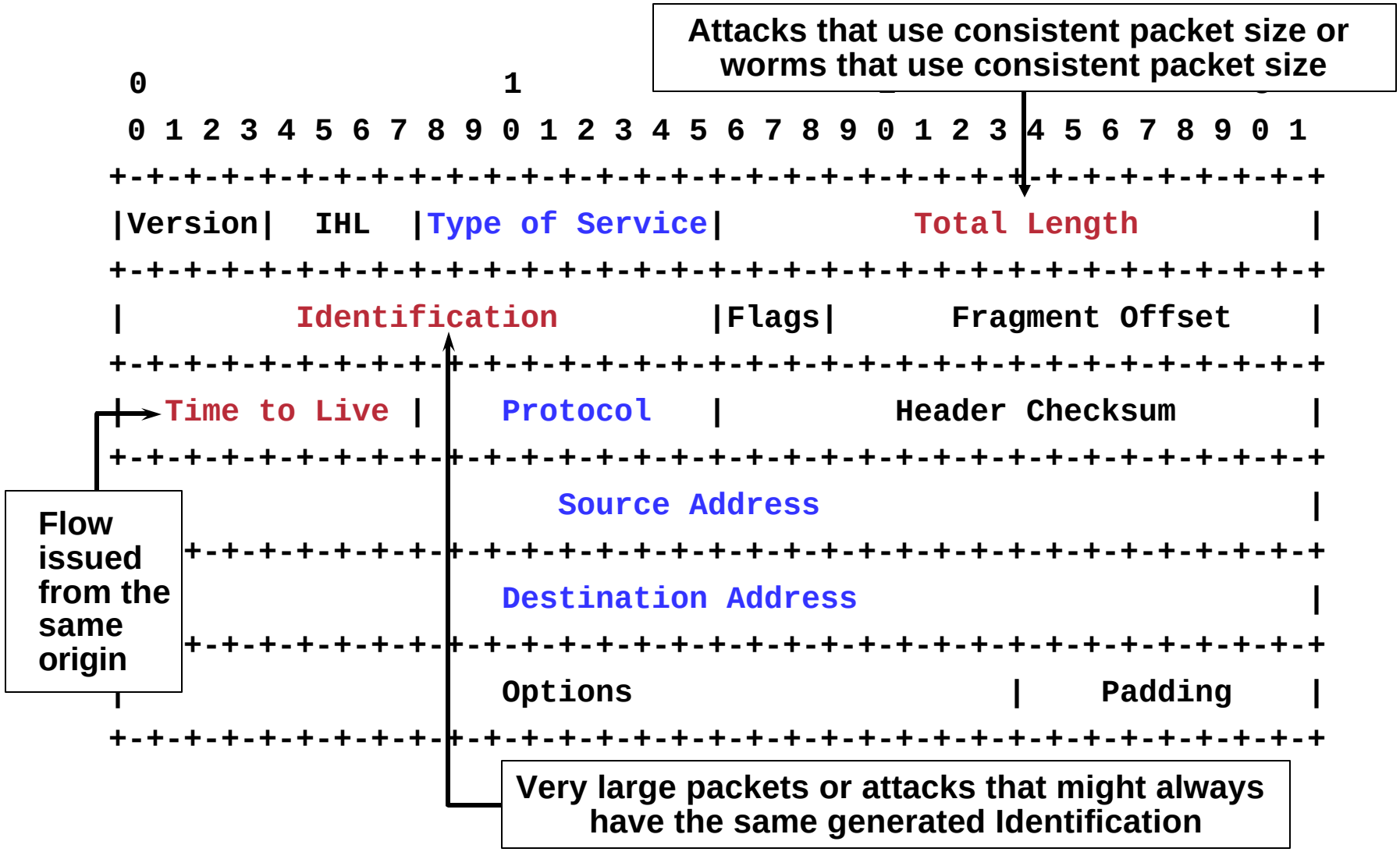
NetFlow L2 and Security Monitoring Current NetFlow L3 Fields

Cisco.com



NetFlow L2 and Security Monitoring Extra NetFlow L3 Fields

Cisco.com



NetFlow L2 and Security Monitoring


```
Router# show ip cache verbose flow
…
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active

Et0/0.1        10.251.138.218  Et1/0.1        172.16.10.2     06 80  00      65
0015 /0  0                     0015 /0  0     0.0.0.0               840    10.8
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      840                            Max plen:       840
Min TTL:        59                            Max TTL:         59
IP id:           0
```

One flow entry

NetFlow and ICMP Reminder

- ICMP is the protocol Identifier 1

```
Router# show ip cache flow
SrcIf   SrcIPaddress    DstIf   DstIPaddress   Pr   SrcP  DstP  Pkts
Fa1/0   144.254.12.209  Local   172.17.246.9   01   0000  0800   1
```

- The destination port number reported: (ICMP type * 256) + (the ICMP code)

  ICMP type = 8, ICMP code = 0

  Port = 8 * 256 + 0 = 2048 = 800 hexa

- Only for the routers

NetFlow L2 and Security Monitoring


```
Router# show ip cache verbose flow
…
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active

Et0/0.1        10.251.138.218  Et1/0.1        172.16.10.2     01 80  00       65
0015 /0  0                     0015 /0  0     0.0.0.0                840    10.8
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      840                           Max plen:       840
Min TTL:        59                           Max TTL:         59
ICMP type:       0                           ICMP code:       0
IP id:           0
```

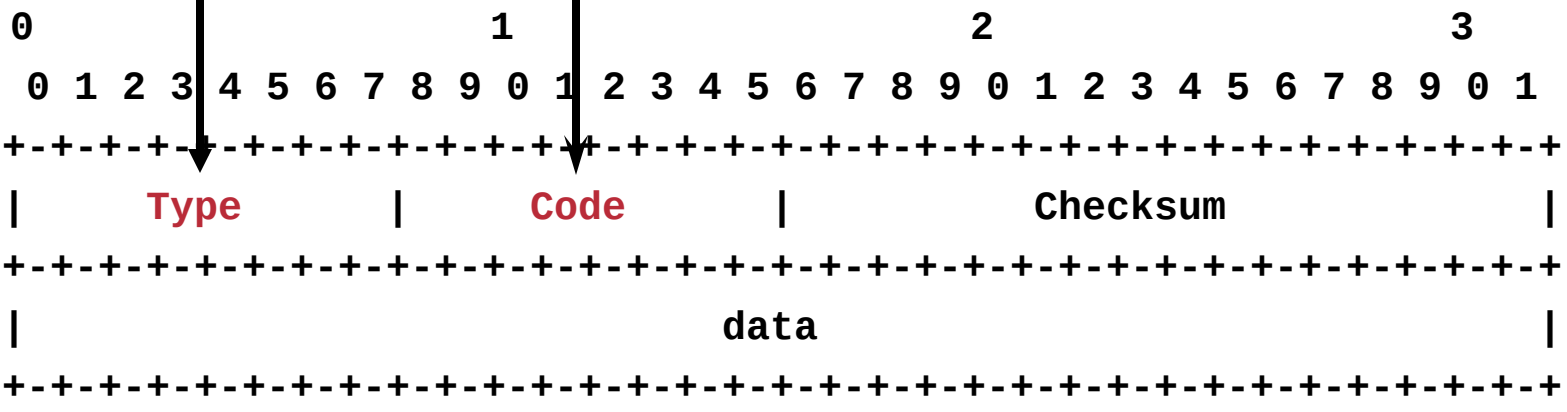
ICMP type 0, ICMP code 0: Echo Reply

NetFlow L2 and Security Monitoring ICMP Type and Code

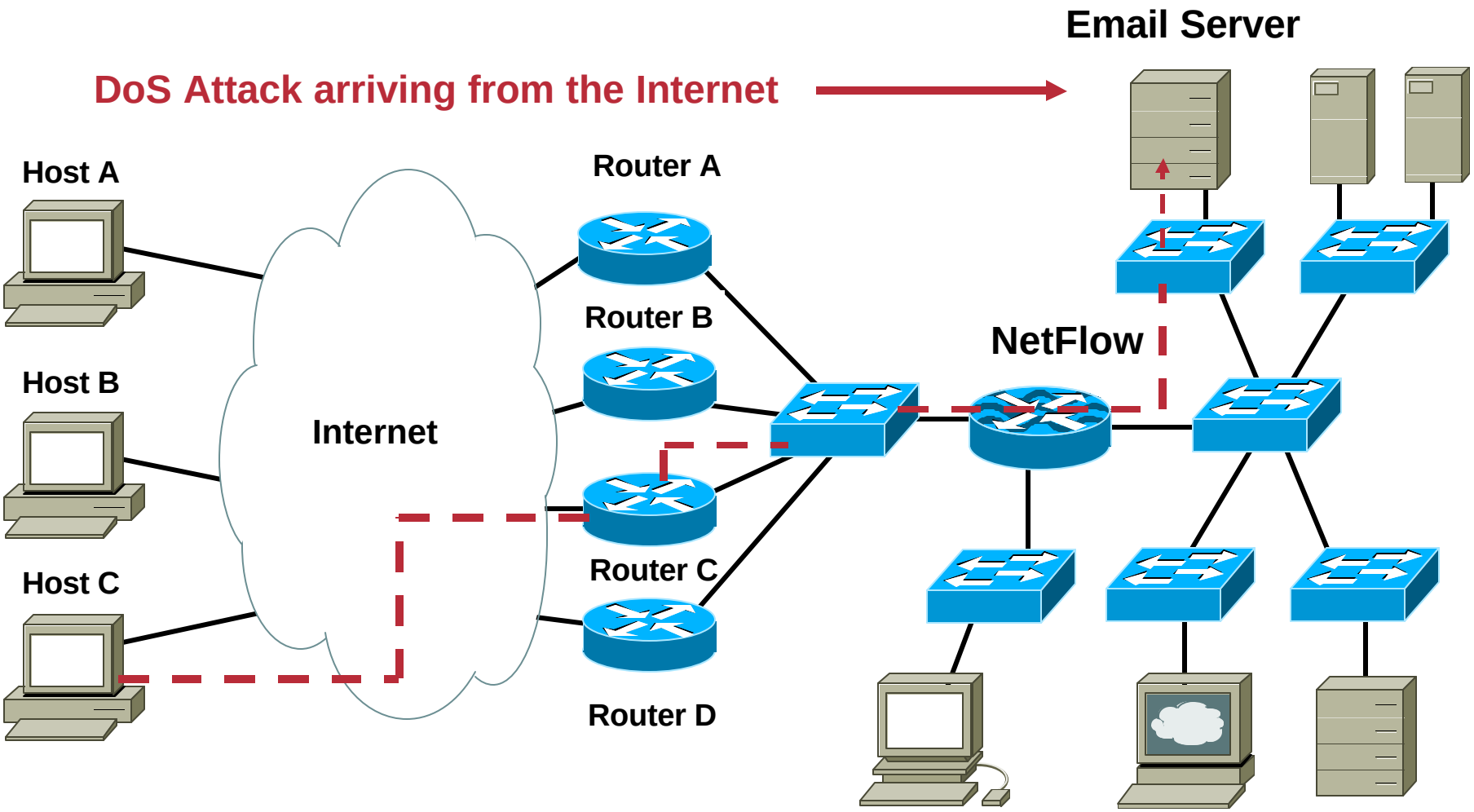
Cisco.com

Echo reply
Destination unreachable
Source quench
Redirect
Time Exceeded
Parameter problem
Etc…

1. Host unreachable
2. Protocol unreachable
3. Port unreachable
4. Fragmentation needed and DF bit set
5. Source route failed
6. Destination network unknown
7. Destination host unknown
8. Source host isolated
9. Communication with destination network is administratively prohibited
10. Communication with destination host is administratively prohibited
11. Destination network unreachable for TOS
12. Destination host unreachable for TOS



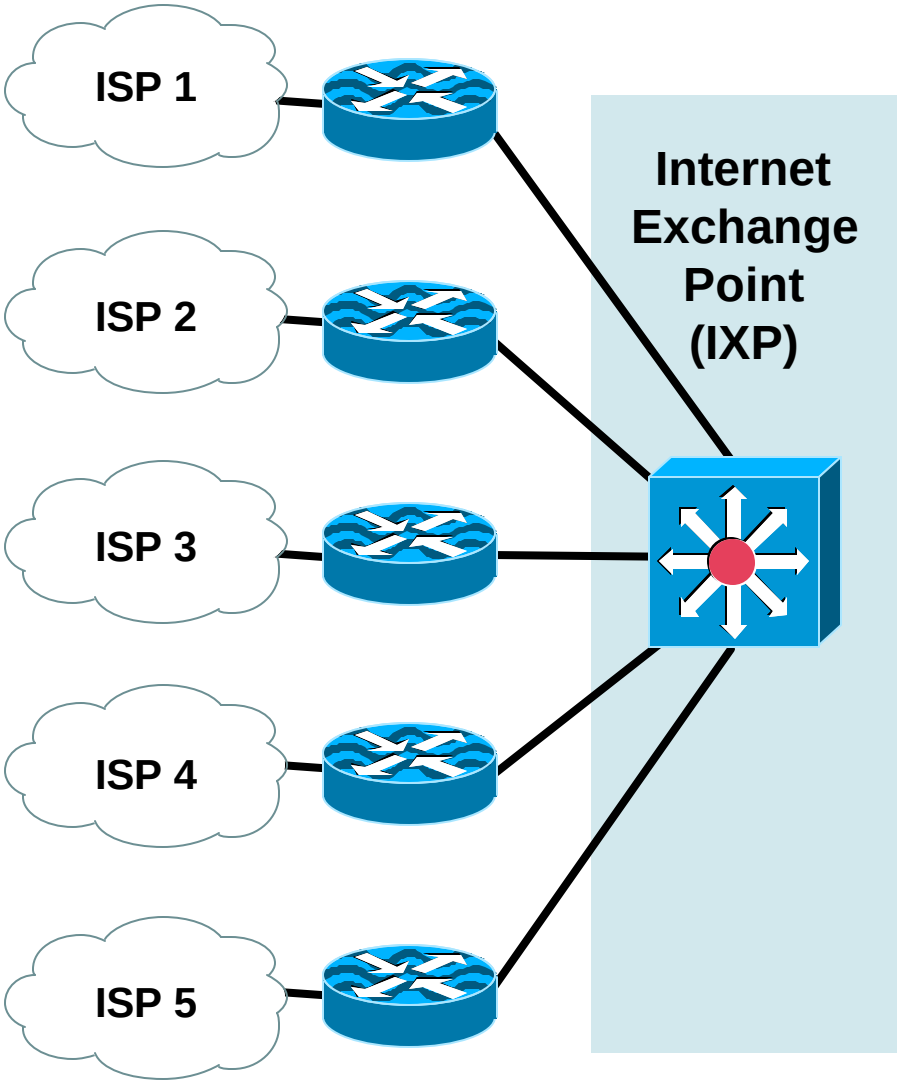
NetFlow L2 and Security Monitoring Source MAC Address



Report the MAC address for ethernet, fastethernet, and GigEthernet

NetFlow L2 and Security Monitoring Internet eXchange Point

- Internet Exchange Points require the accounting per MAC address:
  - Incoming
  - Outgoing
- NetFlow solution is more granular than the “IP accounting MAC address” feature



NetFlow MIB and Top Talkers

Cisco.com

- The flows that are generating the heaviest traffic are known as the "top talkers"
- Allows flows to be sorted by either of the following criteria:
  - By the total number of packets in each top talker
  - By the total number of bytes in each top talker.
- Match criteria for the top talkers: specific flow field values
  - Work like a filter
- A new separate cache
  - Similar output of the show ip cache flow or show ip cache verbose flow command
  - Generated on the fly
  - Frozen for the “cache-timeout” value
- Introduced in 12.2(25)S and 12.3(11)T on the low-end routers

NetFlow MIB and Top Talkers Configuration


```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# top 50
Router(config-flow-top-talkers)# sort-by <packets | bytes>
Router(config-flow-top-talkers)# cache-timeout 2000
```

```
Router# show ip flow top-talkers verbose

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
IPM: OPkts    OBytes
Fa1/0          10.48.71.9      Local          10.48.71.9      01 C0  10      56
0000 /24 0                     0303 /24 0     0.0.0.0                56   171.6
ICMP type:       3                            ICMP code:        3

Se0/0          192.1.1.97      Se0/3          192.1.1.110     01 00  00      12
0000 /30 0                     0000 /30 0     192.1.1.108          1436     2.8
ICMP type:       0                            ICMP code:        0
```

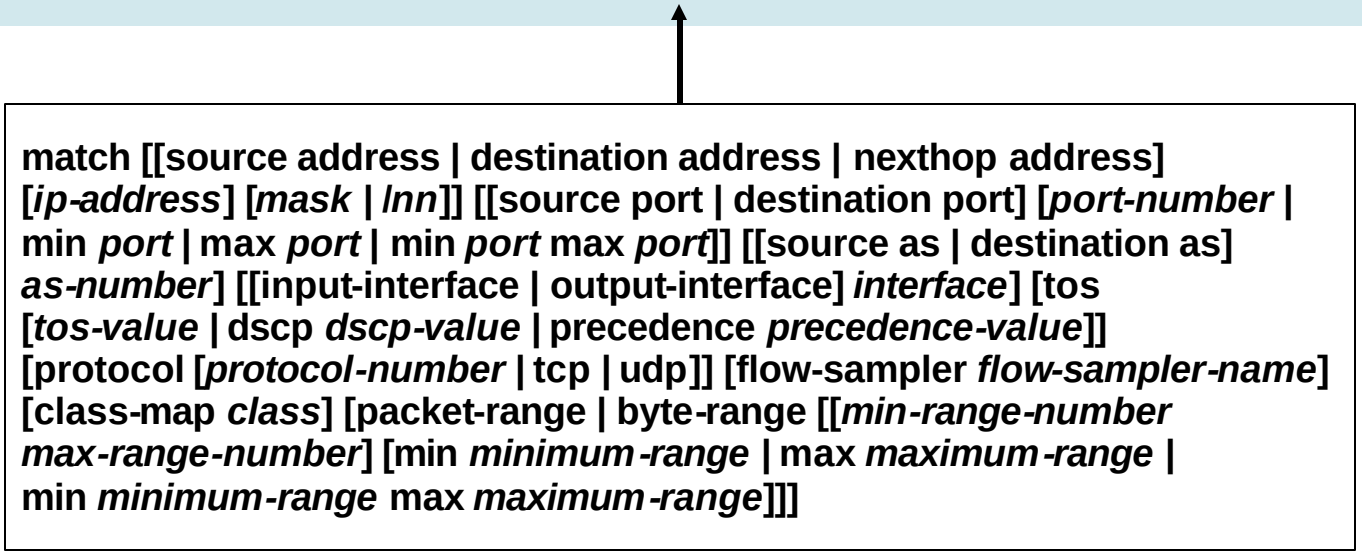
NetFlow MIB and Top Talkers Example 2


```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# top 50
Router(config-flow-top-talkers)# sort-by packets
Router(config-flow-top-talkers)# cache-timeout 2000
Router(config-flow-top-talkers)# match source address 192.1.1.97/32
Router(config-flow-top-talkers)# match destination address 192.1.1.110/32
```

```
Router# show ip flow top-talkers verbose

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active

Se0/0          192.1.1.97      Se0/3          192.1.1.110     01 00  00      12
0000 /30 0                     0000 /30 0     192.1.1.108          1436     2.8
ICMP type:       0                            ICMP code:         0
```

NetFlow MIB and Top Talkers Example 2


```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# top 50
Router(config-flow-top-talkers)# sort-by packets
Router(config-flow-top-talkers)# cache-timeout 2000
Router(config-flow-top-talkers)# match source address 192.1.1.97/32
Router(config-flow-top-talkers)# match destination address 192.1.1.110/32
```



NetFlow MIB and Top Talkers

- **The top talkers can be configured via SNMP with the CISCO-NETFLOW-MIB**
- **The top talkers can be retrieved via the MIB**

  cnfTopFlowsTable

- **No really a trending tool unless we compare all the flow key values**

  cnfTopFlowsIndex represents the top flow index but this is not keeping any correlation from the cnfTopFlowsIndex in the previous of next polling interval

NetFlow MIB and Top Talkers Applications

- **Security**

  List of top talkers to see if traffic patterns consistent with a denial of service (DoS) attack are present in your network.

- **Traffic analysis**

  The top talkers whose destination IP address is my web server

- **Capacity planning**

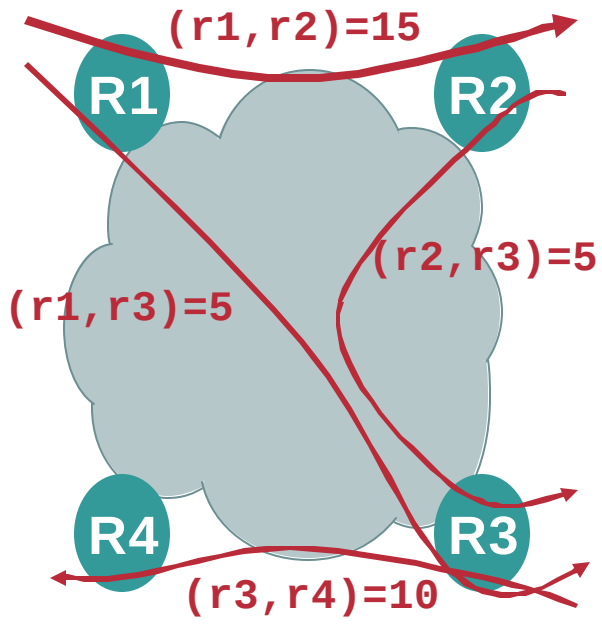
  The top talkers whose destination is the BGP AS X

- **Etc…**

NETFLOW FOR CAPACITY PLANNING

What Is the Traffic Matrix?

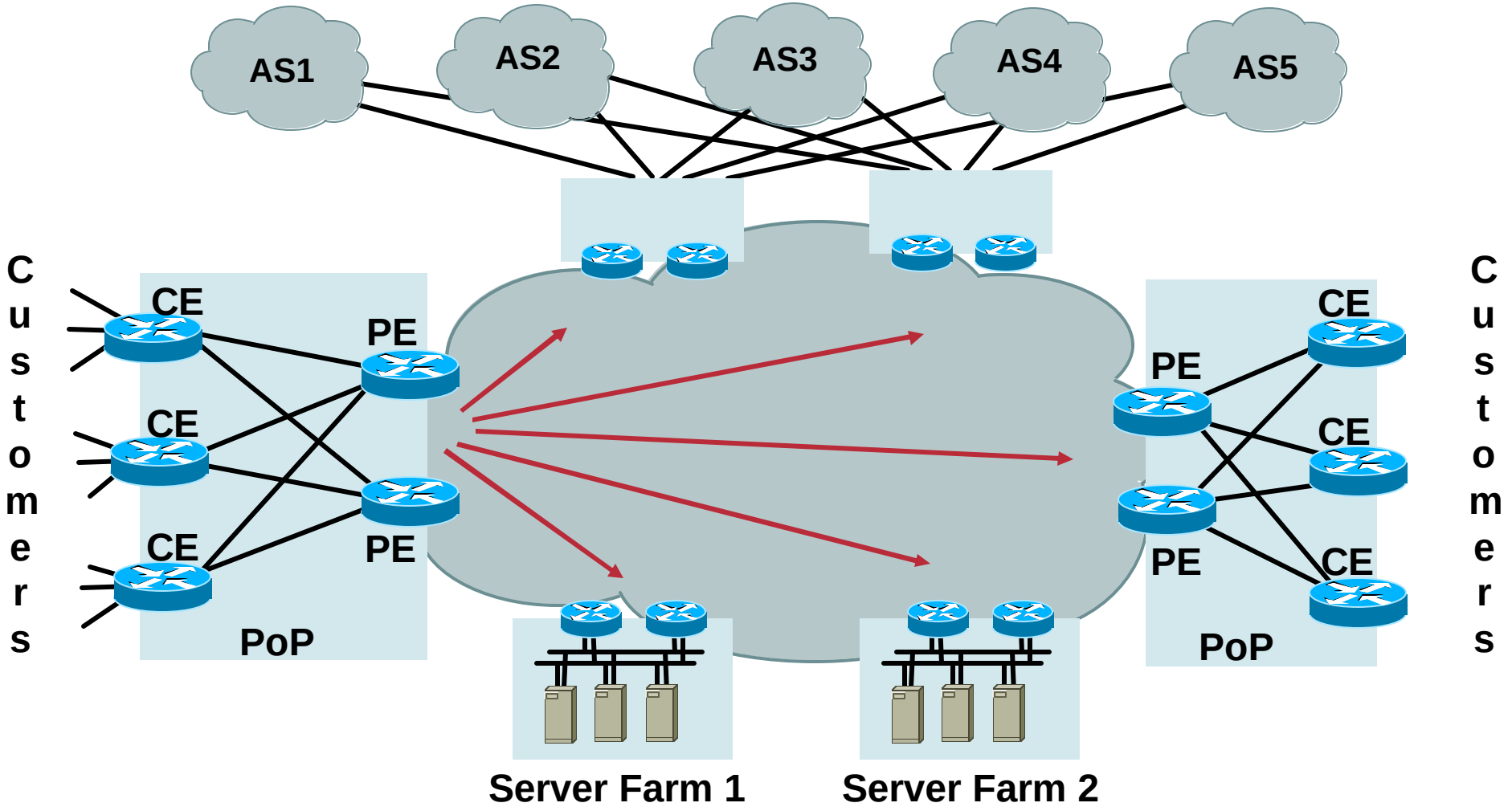
From / To	R1	R2	R3	R4
R1	0	15	5	0
R2	0	0	5	0
R3	0	0	0	10
R4	0	0	0	0



Core Capacity Planning
The Big Picture

1. The ability to offer SLAs is dependent upon ensuring that core network bandwidth is adequately provisioned
2. Adequate provisioning (without gross over provisioning) is dependent upon accurate core capacity planning
3. Accurate core capacity planning is dependent upon understanding the core traffic matrix and flows and mapping these to the underlying topology
4. A tool for “What if” scenarios

We Need the Core Traffic Matrix



"PoP to PoP": Access Router (AR) or Core Router (CR

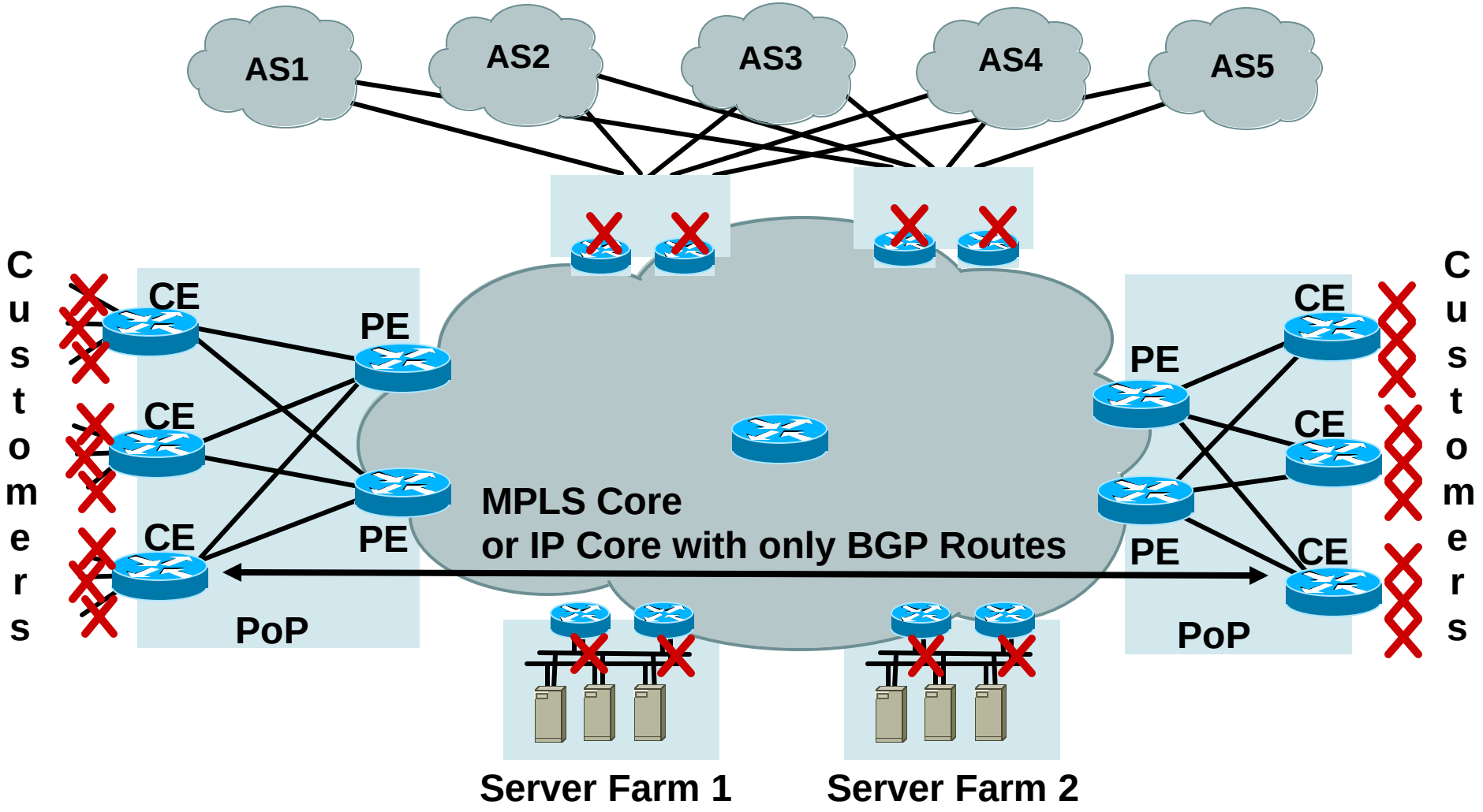
NetFlow BGP Next Hop TOS Aggregation

Cisco.com

- Lets you measure network traffic on a per BGP next hop basis, per TOS
- Lets you track which service provider the traffic is going through (exit point)
- Configure on ingress interface
- Leverages the new NetFlow Version 9 export format
- Support with sampled and non sampled NetFlow
- 12.0(26)S, 12.2(18)S and 12.3 for the low-end routers

  12.0(27)S for the 12000

BGP Next Hop TOS Aggregation Typical Example



NetFlow BGP Next Hop TOS Aggregation Flow Keys

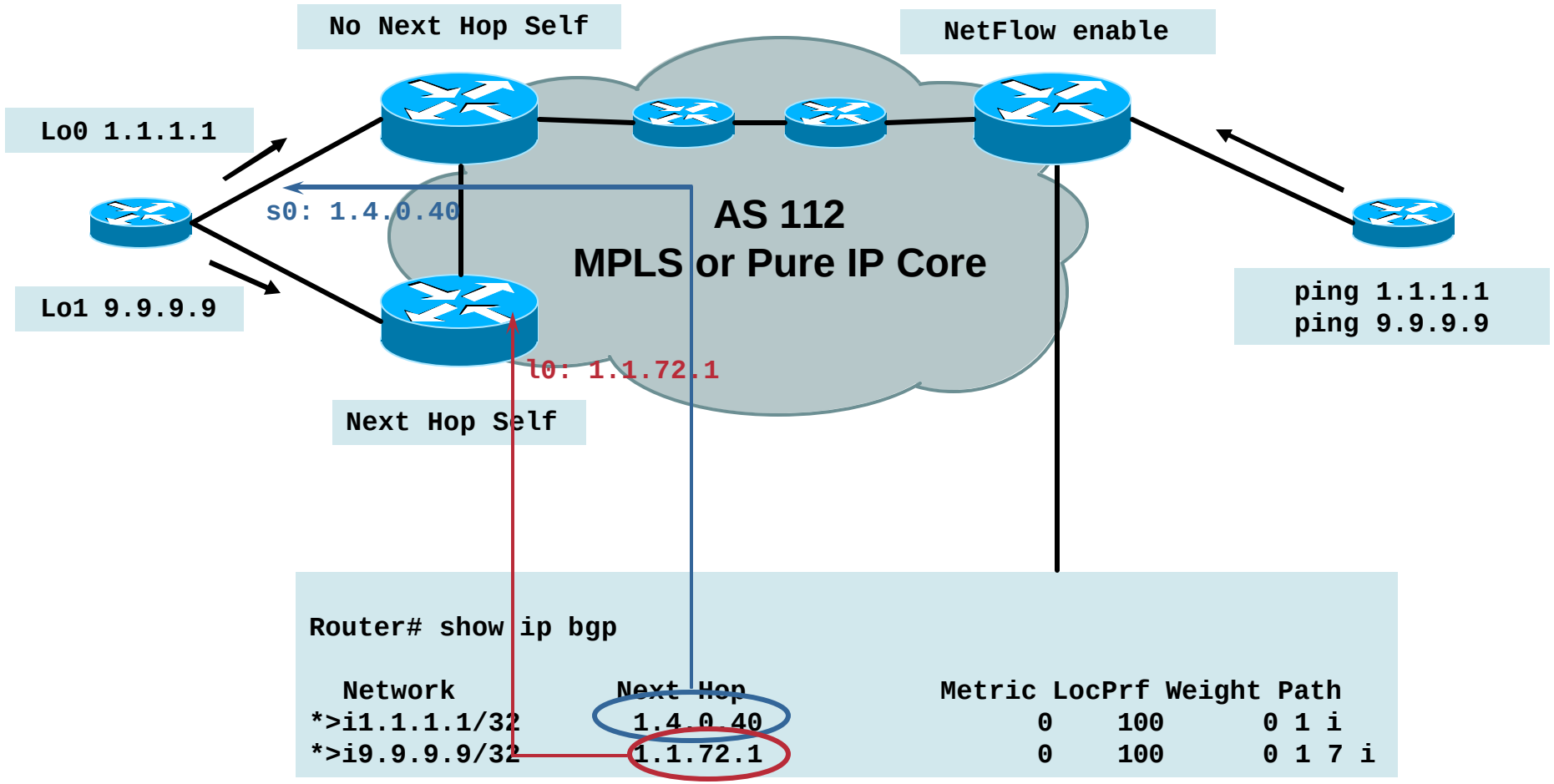
Key Fields (Uniquely Identifies the flow)	Additional Export Fields
• Origin AS	• Flows
• Destination AS	• Packets
• Inbound Interface	• Bytes
• Output Interface	• First SysUptime
• ToS/DSCP (*)	• Last SysUptime
• Next BGP Hop	

(*) before any re-coloring

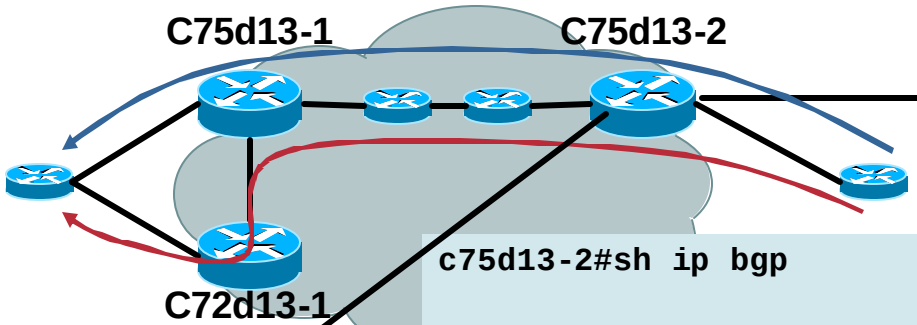
NetFlow BGP Next Hop TOS Aggregation Configuration


```
Router (config) # ip flow-export version 9 [origin-as | peer-as] [bgp-nexthop]
Router (config) # ip flow-export destination <dest IP> <dest udp-port>
Router (config) # ip flow-export source <interface>

Router (config) # ip flow-aggregation cache bgp_nexthop_tos
Router (config-flow-cache)# export destination <dest IP > <dest udp-port>
Router (config-flow-cache)# enabled

Router (config-if)# ip flow ingress
```

NetFlow BGP Next Hop TOS Aggregation Testing



NetFlow BGP Next Hop TOS Aggregation Testing




```
c75d13-2#sh ip bgp

  Network          Next Hop            Metric LocPrf Weight Path
*>i1.1.1.1/32      1.4.0.40                 0    100      0 1 i
*>i9.9.9.9/32      1.1.72.1                 0    100      0 1 7 i
```

FOR A PING TO 1.1.1.1

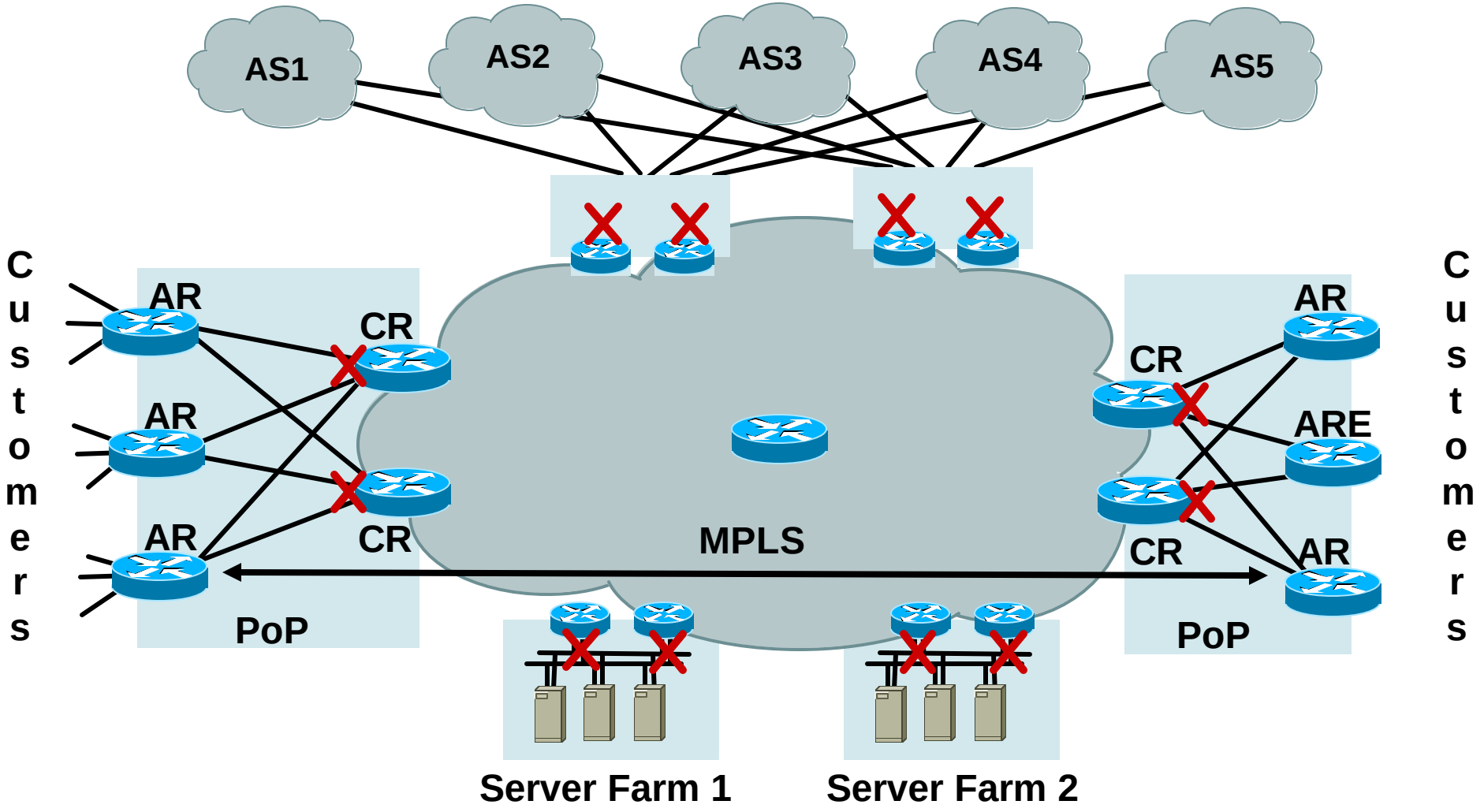
```
sh ip cache verbose flow aggregation bgp-nexthop-tos

Src If         Src AS  Dst If         Dst AS  TOS Flows   Pkts  B/Pk  Active
BGP NextHop
Et1/0/1         2      Et1/0/2         1      00     1      5    100     0.0
BGP  1.4.0.40

Src If         Src AS  Dst If         Dst AS  TOS Flows   Pkts  B/Pk  Active
BGP NextHop
Et1/0/1         2      Et1/0/2         1      00     1      5    100     0.0
BGP  1.1.72.1
```

FOR A PING TO 9.9.9.9

MPLS Aware NetFlow Description

- **Provides flow statistics per MPLS and IP packets**
  - **MPLS packets:**
    - **Labels information**
    - **And NetFlow V5 fields for underlying IP packet**
  - **IP packets:**
    - **Regular IP NetFlow records**
- **Leverages the new NetFlow Version 9 export format**
- **Configure on ingress interface**
- **Supported on sampled/non sampled NetFlow**
- **12.0(26)S1, 12.2(18)S and 12.3 for the low-end routers**
  - **12000: 12.0(24)S, 12.2(18)S and 12.3**

MPLS Aware NetFlow Typical Example



MPLS Aware NetFlow Top Label Aggregation

Key Fields (Uniquely Identifies the Flow)

- Input Interface (ifIndex)
- THE TOP incoming MPLS labels with experimental bits and end-of-stack bit

Additional Export Fields

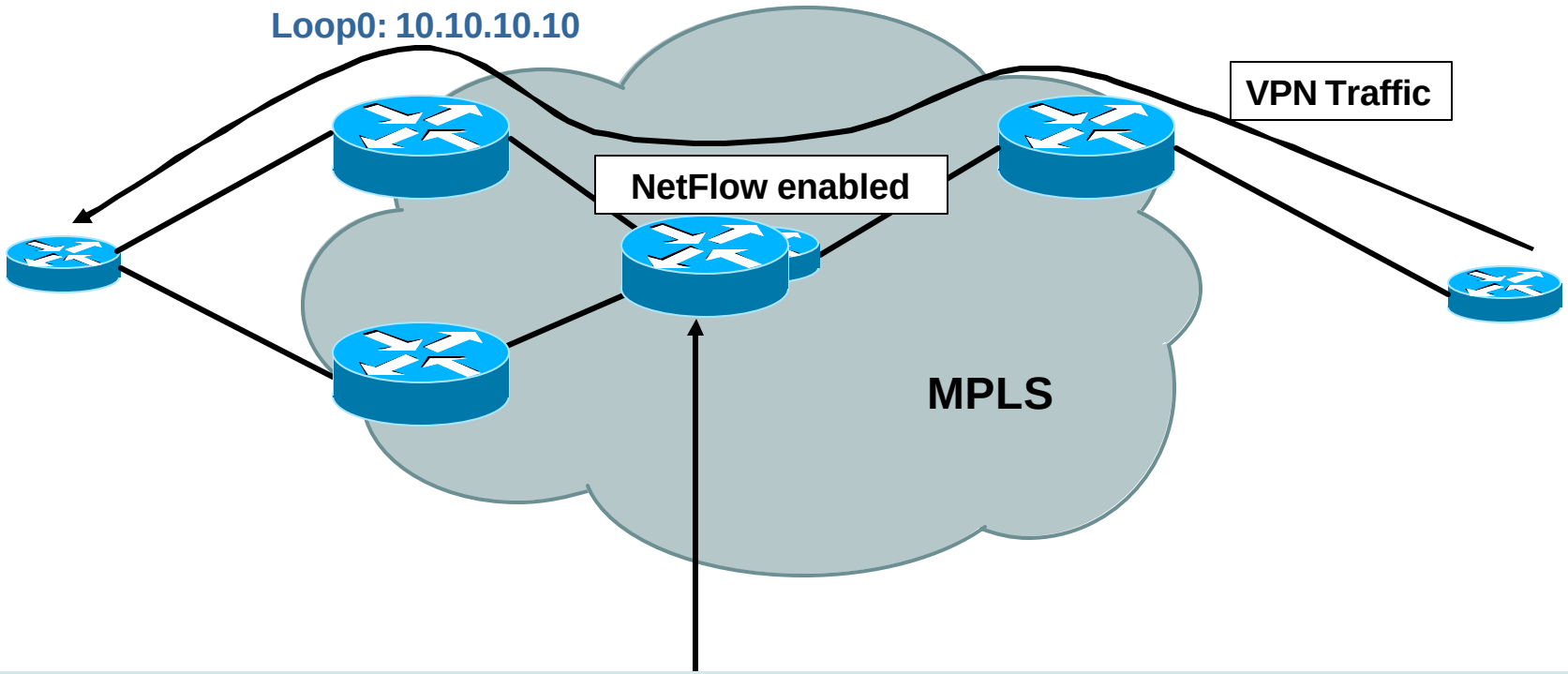
- Flows
- Packets
- Bytes
- First Timestamp (SysUptime)
- Last Timestamp (SysUptime)
- Output Interface
- NetFlow Version 5 fields of the underlying IP packet (TCP flags, etc…)
- Type of the top label: LDP, BGP, VPN, ATOM, TE Tunnel MID-PT, unknown
- The Forwarding Equivalent Class mapping to the top label

MPLS Aware NetFlow Configuration

Cisco.com

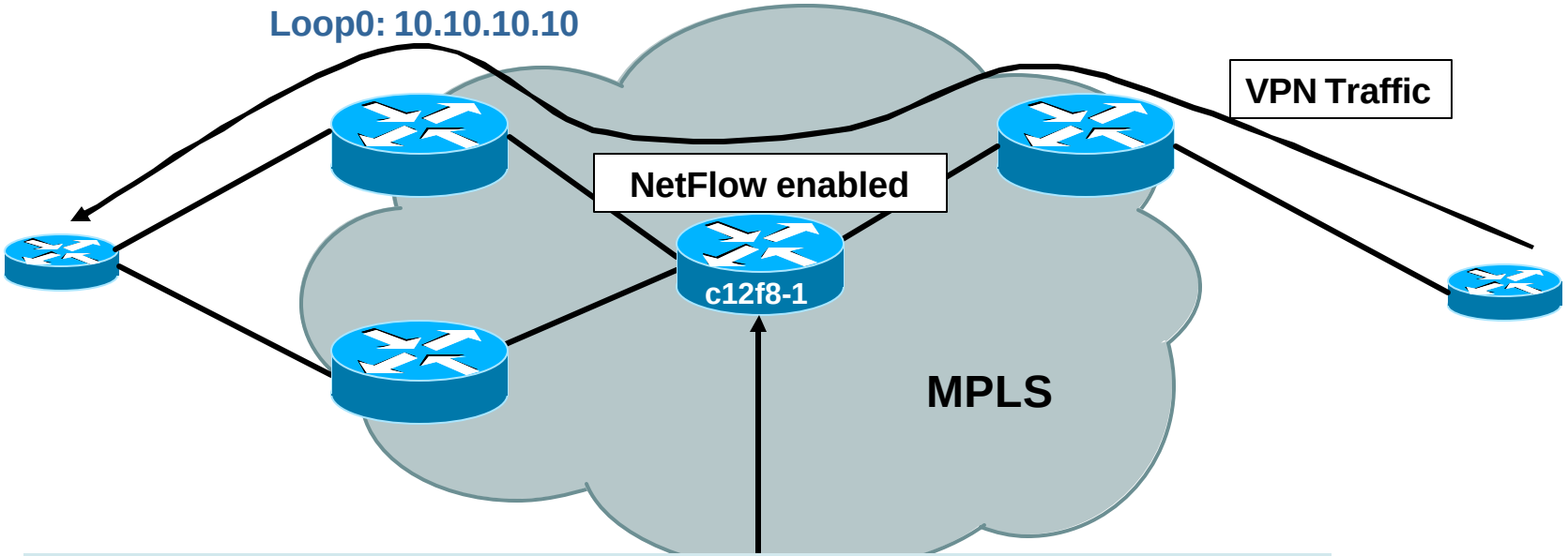
```
Router(config)#ip flow-cache mpls label-positions 1 no-ip-fields mpls-length
Router(config-if)# ip route-cache flow sampled
Router(config)# ip flow-export version 9
Router(config)# ip flow-export template options export-stats
Router(config)# ip flow-export template options sampling
Router(config)# ip flow-sampling-mode packet-interval 100
```

NetFlow MPLS Aware Testing




```
Router# show mpls forwarding 10.10.10.10
Local  Outgoing    Prefix            Bytes tag      Outgoing    Next Hop
tag    tag or VC   or Tunnel Id      switched       interface
486    Pop tag     10.10.10.10/32  1696244602516  PO3/0       point2point
```

NetFlow MPLS Aware Testing




```
Router# show ip flow verbose cache
…
SrcIf  SrcIPaddress DstIf  DstIPaddress  Pr  TOS  Flgs  Pkts
Port  Msk  AS  Port  Msk  AS  NextHop  B/Pk  Active

PO2/0  0.0.0.0      PO3/0  0.0.0.0       00  00   10    1729
0000  /0   0   0000  /0   0   0.0.0.0   792  14.6
Pos:Lbl-Exp-S 1:486-4-0 (LDP/10.10.10.10)
```

Exported as 7784, EXP in NFC 5.0

NEW FEATURES

Egress NetFlow Accounting

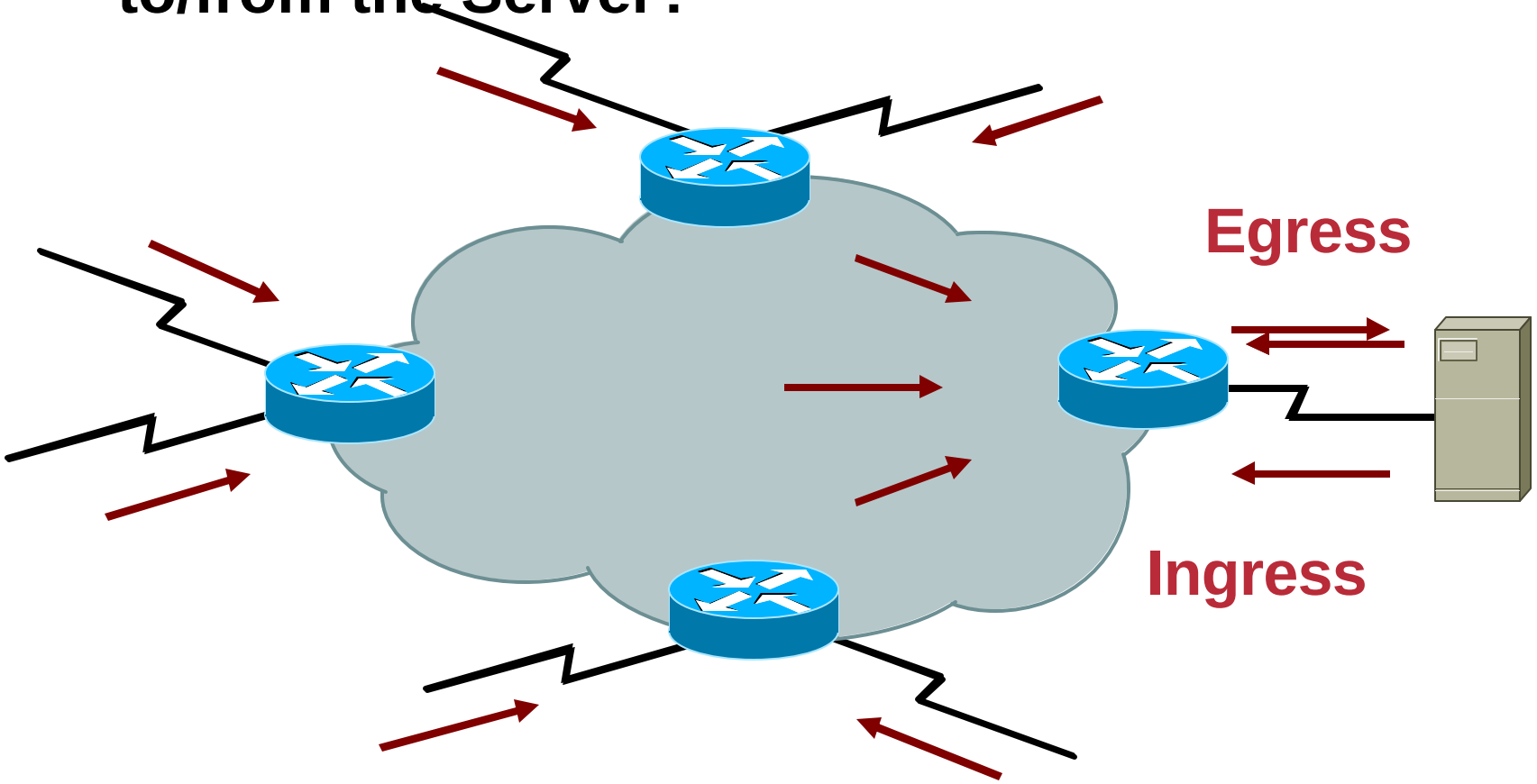
Cisco.com

- The NetFlow Egress Support feature allows NetFlow accounting to be implemented for egress (outgoing) traffic on an interface or sub-interface
- Locally generated traffic (traffic that is generated by the router on which the NetFlow Egress Support feature is configured) will not be counted
- The NetFlow Egress feature captures NetFlow statistics for IP traffic only; MPLS statistics are not captured
- 12.3(11)T for the low-end routers

```
Router(config-if)# ip flow egress
```

Egress NetFlow Accounting

How to Account the Traffic to/from the Server?



Attention to Double Count the Flow Records!

Egress NetFlow Accounting


```
Router# show ip cache flow
…
SrcIf  SrcIPaddress DstIf  DstIPaddress  Pr SrcP DstP  Pkts
Et0/0 10.0.0.1     Et0/0* 10.0.1.1      01 0000 0000    5
Et0/1 10.0.0.2     Et0/1  10.0.1.2      01 0000 0000    5
```

- A flow is identified by the output interface (amongst other), by default with egress NetFlow

```
Router(config)# ip flow-egress input-interface
```

Egress NetFlow and Top Talkers


```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# match source address 192.1.1.97/32
Router(config-flow-top-talkers)# match direction ?
        egress   Match egress flows
        ingress  Match ingress flows
```

- The direction match statement added
- The “direction” is a new information element
  - Egress value added in the Template
  - Egress value not added for the aggregation caches
  - Existing ingress templates are not modified

NetFlow and IPV6

Cisco.com

- Monitors the IPv6 traffic
- Based on NetFlow Version 9
- For both ingress and egress traffic
- Non sampled
- No data export over IPV6; Still IPv4
- NetFlow L2 and Security Monitoring available for IPv6:

  ICMP, IP Identification, mac-addresses, packet-length, TTL, vlan-id

- 12.3(4)T, 12.2(25)S for low-end platform (3600, 7200, 7500, etc…)

NetFlow and IPV6


```
Router#show ipv6 flow cache
…
SrcAddress    InpIf DstAddress     OutIf Prot SrcPrt DstPrt Pkts
2001:400::2   Local 2001:400::1    Et3/0 0x3A 0x0000 0x8100 5
2001:300::2   Local 2001:300::1    Et3/0 0x3A 0x0000 0x8100 5
2001:200::2   Local 2001:200::1    Et3/0 0x3A 0x0000 0x8100 5
2001:300::1   Et3/0 FF02::1:FF00:2 Local 0x3A 0x0000 0x8700 2
2001:400::1   Et3/0 FF02::1:FF00:2 Local 0x3A 0x0000 0x8700 2
2001:400::1   Et3/0 2001:400::2    Local 0x06 0x2B00 0x0017 88
```

- **Exactly the same commands as for IPv4 for configuration and monitoring, except that “ip” is replaced by “ipv6”**
- **New NetFlow Version 9 information elements**

NetFlow Enabled Interfaces

Cisco.com

```
Router# show ip flow interface
Serial0/0
  ip route-cache flow
Serial0/0.1
  ip flow egress
Serial0/3
  ip route-cache flow
FastEthernet1/0
  ip flow ingress
  flow-sampler benoit egress
```

Introduced in 12.3(7)T for low-end routers

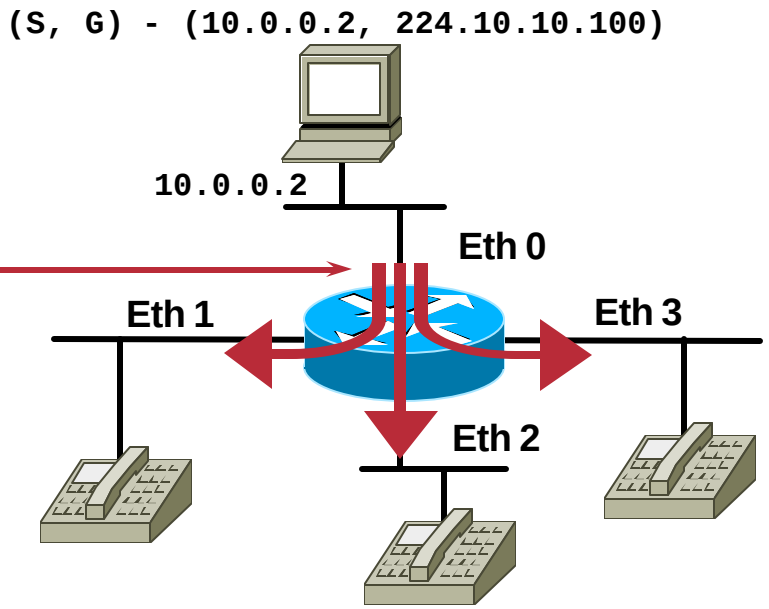
Multicast NetFlow

Cisco.com

- **Three types of NetFlow implementations for Multicast traffic:**
  - **Traditional NetFlow**
  - **Multicast NetFlow Ingress**
  - **Multicast NetFlow Egress**
- **Support**
  - **Cisco IOS software releases 12.0(27)S, 12.2(18)S and 12.3(1)**
  - **Not supported in 12000**
  - **C6500/7600 support in a future supervison**

Multicast: Traditional NetFlow


```
Interface Ethernet 0
    ip route-cache flow

ip flow-export version 9
ip flow-export destination x.x.x.x <port>
```



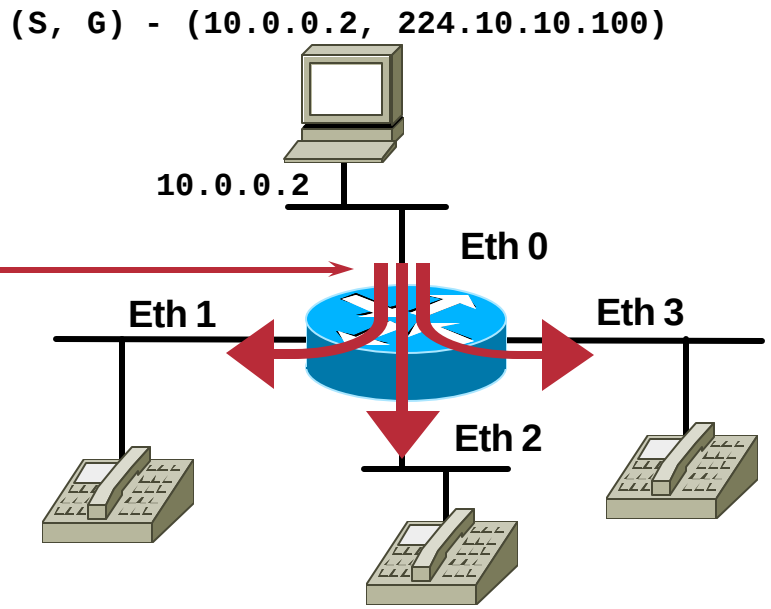
SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	SrcPort	SrcMsk	DstPort	DstMsk	NextHop	Bytes	Packets	Active	Idle
Eth 0	10.0.0.2	Null	224.10.10.100	11	80	10	00A2	/24	00A2	/24		23100	21	1745	4

- There is only one flow per NetFlow configured input interface
- The 7 Key fields that define a unique flow are marked in red
- Destination interface is marked as “Null”
- Bytes and Packets are the incoming values

Multicast NetFlow Ingress

Cisco.com

```
Interface Ethernet 0
    ip multicast netflow ingress

ip flow-export version 9
ip flow-export destination x.x.x.x <port>
```

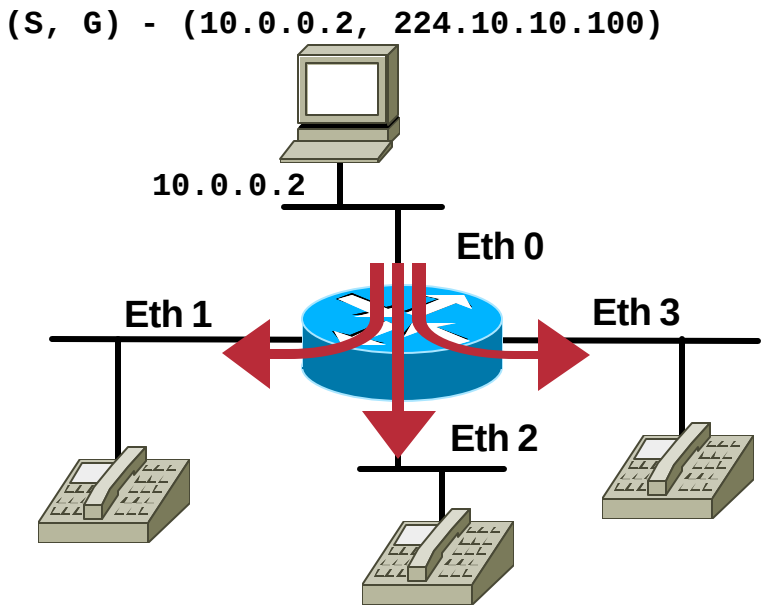


SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	SrcPort	SrcMsk	DstPort	DstMsk	NextHop	Bytes	Packets	Active	Idle
Eth 0	10.0.0.2	Null	224.10.10.100	11	80	10	00A2	/24	00A2	/24		69300	63	1745	4

- There is only one flow per NetFlow configured input interface
- The 7 Key fields that define a unique flow are marked in red
- Destination interface is marked as “Null”
- Bytes and Packets are the incoming values

Multicast NetFlow Egress


```
Interface Ethernet 0
Interface Ethernet 1
   ip multicast netflow egress
Interface Ethernet 2
   ip multicast netflow egress
Interface Ethernet 3
   ip multicast netflow egress

ip flow-export version 9
ip flow-export destination x.x.x.x <port>
```



SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	SrcPort	SrcMsk	DstPort	DstMsk	NextHop	Bytes	Packets	Active	Idle
Eth 0	10.0.0.2	Eth 1	224.10.10.100	11	80	10	00A2	/24	00A2	/24		23100	21	1745	4
Eth 0	10.0.0.2	Eth 2	224.10.10.100	11	80	10	00A2	/24	00A2	/24		23100	21	1745	4
Eth 0	10.0.0.2	Eth 3	224.10.10.100	11	80	10	00A2	/24	00A2	/24		23100	21	1745	4

- There is one flow per Multicast NetFlow Egress configured output interface
- One of the 7 Key fields that define a unique flow has changed from Source Interface to Destination Interface
- Bytes and Packets are the outgoing values

PLATFORMS SPECIFIC

NetFlow on the Cisco 12000 Router

- Engine 0—Software support
- Engine 1—Software support
- Engine 2—Supported in ASICs (but lower priority so beware if running many other features)
- Engine 3—Version 5 support in software, Version 8 support in ASICs
- Engine 4—Not supported
- Engine 4+—Supported in ASICs

Cisco Catalyst 6500 and Cisco 7600 Series Versions and Features

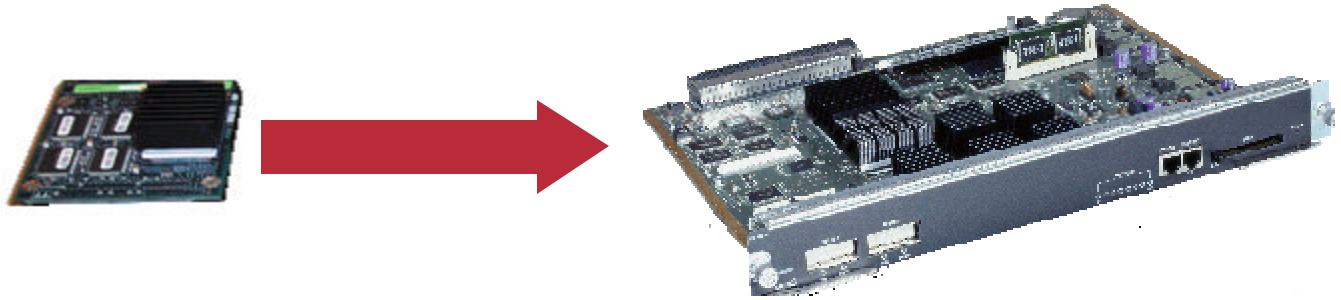
- **Cisco IOS Software Release 12.1(13)E1**
  - **PFC2 Source/destination interface information (Hybrid 6.3(6))**
  - **PFC2 Source/destination AS information**
  - **PFC2 Support for V5 NetFlow data export (Hybrid 7.5(1))**
  - **Flow sampling is available on PFC in Cisco IOS**
- **Cisco IOS Software Release 12.2(14)SX**
  - **Version 8 in native mode**
- **Dual export support Sup2 12.2(17d)SXB**

Cisco Catalyst 6500 and Cisco 7600 Series Versions and Features

- **PFC3b and 3bXL (Sup720) cards**
  - **input ToS field**
- **Hybrid Catalyst OS 7.2(1)**
  - **L2 switched traffic (vlan x to vlan y) support (doesn't require MSFC)**
- **Hybrid Catalyst OS 7.3(1) and 6.3(6)**
  - **Destination and source IfIndex export**
- **Hybrid Catalyst OS 8.4**
  - **Per VLAN NetFlow Configuration**
- **Under Development now**
  - **Multicast NetFlow and Version 9 (Q3CY'05)**
  - **NetFlow IPV6 NetFlow (Q4CY'05)**

Catalyst 4000/4500 NetFlow

- **NetFlow services card in Supervisor 4:**
  - **12.1(13)EW supports Version 5 without interface tracking**
  - **12.1(19)EW supports Version 5 (with interface tracking) and Version 8**
- **NetFlow services card in Supervisor 5:**
  - **12.2(18)EW supports Version 5 and 8**
- **Prior card was NetFlow Feature Card (NFFC) (now end of sale)**



NETFLOW and IETF INTERACTION

IETF: IP Flow Information Export WG (IPFIX)

- **IPFIX web site for the charter, email archive, drafts, etc. http://ipfix.doit.wisc.edu/**
- **IPFIX is an effort to:**
  - **Define the notion of a "standard IP flow"**
  - **Devise data encoding for IP flows**
  - **Consider the notion of IP flow information export based upon packet sampling**
  - **Identify and address any security privacy concerns affecting flow data**
  - **Specify the transport mapping for carrying IP flow information (IETF approved congestion-aware transport protocol)**

IETF: IP Flow Information Export WG (IPFIX)

- **RFC3954 "Cisco Systems NetFlow Services Export Version 9"**
  - **Published as Informational RFC**
  - **NetFlow Patent: Intellectual Property Right statement on the IETF web site**

    https://datatracker.ietf.org/public/ipr_detail_show.cgi?&ipr_id=10

- **RFC 3917 "Requirements for IP Flow Information Export (IPFIX)“**
  - **Published as an Informational RFC**
  - **Gathers all IPFIX requirements for the IPFIX evaluation process**

IETF: IP Flow Information Export WG (IPFIX)

- **NetFlow Version 9 has been selected as a basis for the IPFIX protocol**
  - **Out of 5 existing protocols: CRANE from Xacct, LFAP from Riverstone, Diameter (RADIUS extension), IPDR (ipdr.org)**
  - **Based on the requirements drafts RFC 3917**
- **RFC3955 "Evaluation of Candidate Protocols for IP Flow Information Export (IPFIX)“**
  - **Published as an Informational RFC**
  - **Shows that NetFlow Version 9 is better suited for the IPFIX requirements**

IETF: IPFIX Drafts

- **IPFIX Protocol Specifications, standard track**

  draft-ietf-ipfix-protocol-12.txt

  Changed in terminology but same NetFlow Version 9 principles.

  Improvements versus NetFlow Version 9: SCTP-PR, security, variable length information element, IANA registration, etc…

  Generic streaming protocol, not flow-centric anymore

- **IPFIX Architecture, informational**

  draft-ietf-ipfix-arch-07.txt

  Same architecture as NetFlow

IETF: IPFIX Drafts

- **IPFIX Information Model, standard track**

  draft-ietf-ipfix-info-06.txt

  Most NetFlow Version 9 information elements ID are kept

  Proprietary information element specification

- **IPFIX Applicability Statement, informational**

  draft-ietf-ipfix-as-04.txt

- **All drafts are in last-call**

IETF: Packet SAMPling WG (PSAMP)

- **PSAMP is an effort to:**
  - **Specify a set of selection operations by which packets are sampled**
  - **Specify the information that is to be made available for reporting on sampled packets**
  - **Describe protocols by which information on sampled packets is reported to applications**
  - **Describe protocols by which packet selection and reporting configured**
- **PSAMP web site for the charter, email archive, drafts, etc. http://psamp.ccrle.nec.de/**
- **Agreed to use IPFIX for export protocol**
  - **Good news for NetFlow Version 9**

IETF: PSAMP Drafts

- **A framework for Packet Selection and Reporting**

  draft-ietf-psamp-framework-10.txt

- **Sampling and Filtering Techniques for IP Packet Selection**

  draft-ietf-psamp-sample-tech-06.txt

  To be compliant with PSAMP, we must implement at least one of the mechanisms:

  Sampled NetFlow

  NetFlow Input Filters

IETF: PSAMP Drafts

- **Packet Sampling (PSAMP) Protocol Specifications**

  draft-ietf-psamp-protocol-00.txt

  Waiting for the IPFIX protocol draft to complete

- **Definition of Managed Objects for Packet Sampling**

  draft-ietf-psamp-mib-03.txt

  Waiting for the PSAMP framework and sampling techniques drafts

- **Information Model for Packet Sampling Export**

  draft-ietf-psamp-info-04.txt

  Extension of the IPFIX information model

  Waiting for the PSAMP framework and sampling techniques drafts

CONCLUSION

NetFlow Summary and Conclusion

- NetFlow is a mature Cisco IOS feature (in Cisco IOS since 1996)
- NetFlow provides input for Accounting, Performance, Security, and Billing Applications
- Cisco has IETF and industry leadership
- NetFlow v9 eases the exporting of additional fields
- A lot of new features have been added
- Stay tuned for more ☺

References

- **NetFlow**

  http://www.cisco.com/go/netflow

- **Cisco Network Accounting Services**

  Comparison of Cisco NetFlow versus other available accounting technologies

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

- **Cisco IT Case Study**

  http://business.cisco.com/prod/tree.taf%3Fasset_id=106882&IT=104252&public_view=true&kbns=1.html

- **A complete white paper**

  http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.htm

Complete Your Online Session Evaluation!

Cisco.com

Por favor, complete el formulario de evaluación.

Muchas gracias.

Session ID: NMS-3132

Advanced Netflow Usage