Netflow/cflow - ulubionym narzędziem operatorów SP

Krzysztof Mazepa

CCIE No. 18662, Service Provider, kmazepa@cisco.com

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Abstract

Netflow/cflow – zapewne każdy z nas zetknął się z tym pojęciem. Czy jednak wszyscy wiemy gdzie i jak Netflow jest wykorzystywany w nowoczesnych sieciach IP/MPLS ? Czy zdajemy sobie sprawę, **jakie są jego możliwości** i **jakie aplikacje** mogą z niego skorzystać?
Przykładem niech będą:
- **monitorowanie sieci** (aplikacje i użytkownicy),
- **planowanie sieci**,
- **identyfikowanie ataków i innych zagrożeń** (wirusy, DoS)
- **wykorzystanie w systemach bilingowych**
- **analiza ruchu na styku operatorów** (traffic engineering).

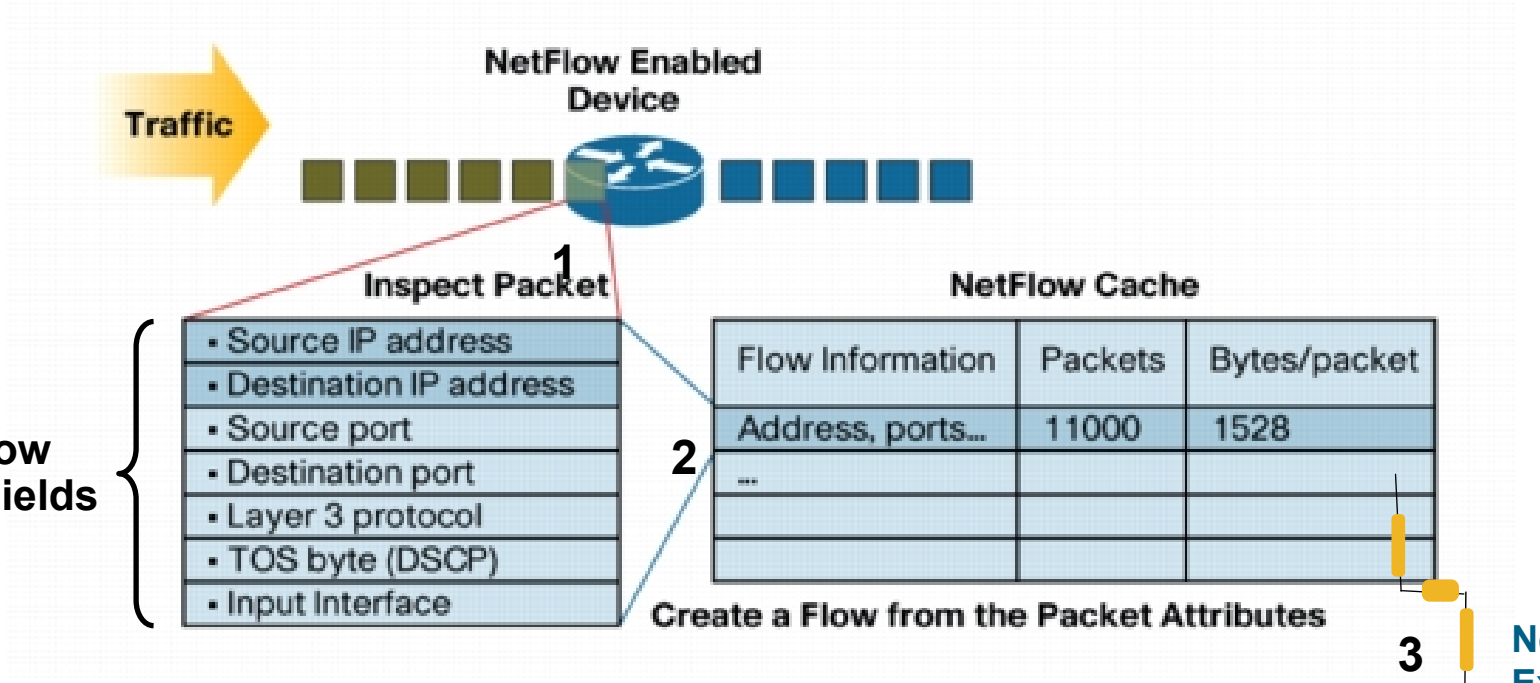
Celem sesji jest pokazanie **korzyści stosowania mechanizmów Netflow/cflow przez operatorów SP/Enterpise** i wywołanie dyskusji na temat wykorzystania Netflow/cflow w tych sieciach.

 © 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Co to jest Netflow ?

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

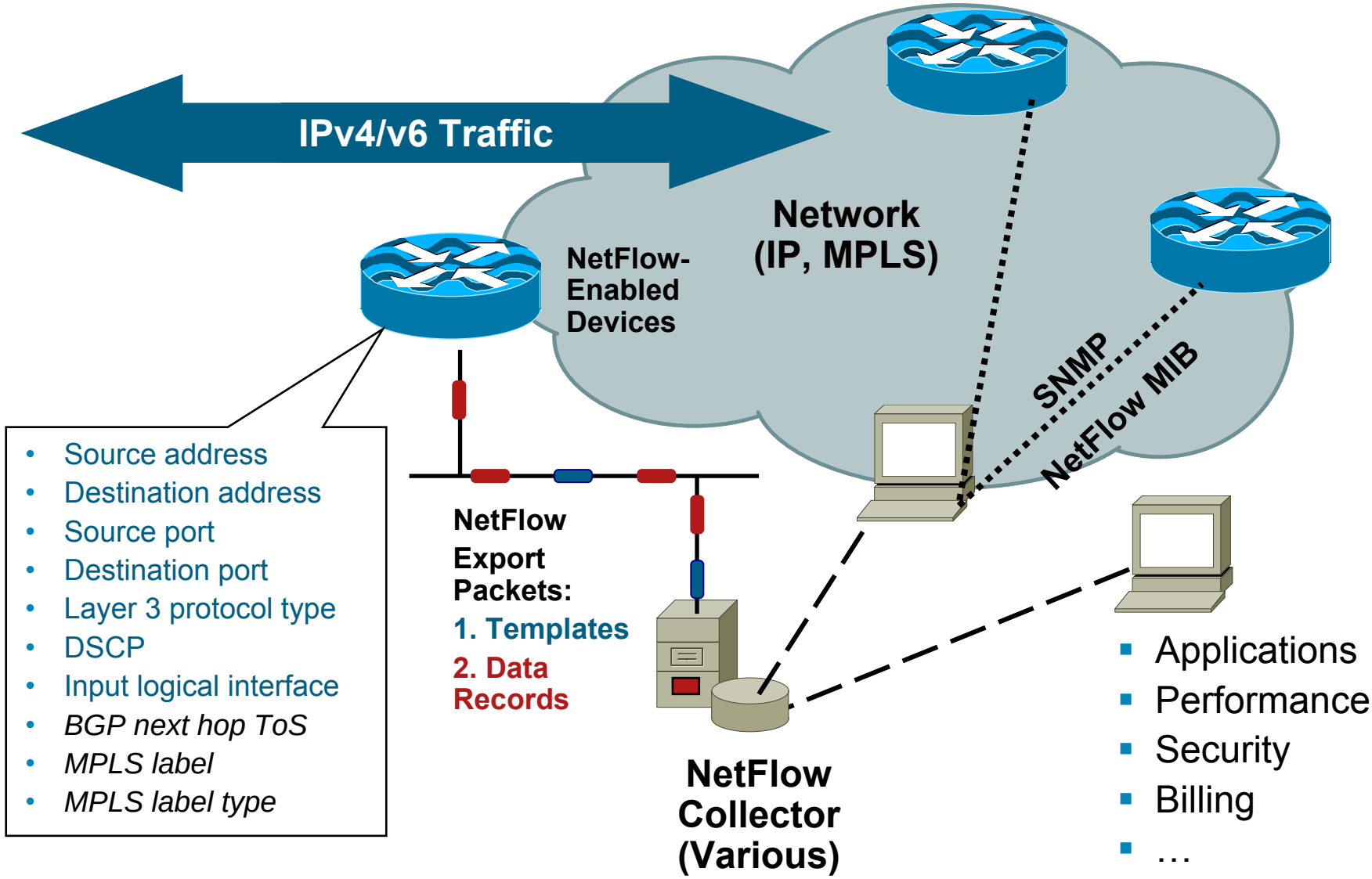
What Is a Traditional IP Flow?



1. Inspect a packet's seven key fields and identify the values
2. If the set of key field values is unique create a flow record or cache entry
3. When the flow terminates export the flow to the collector

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

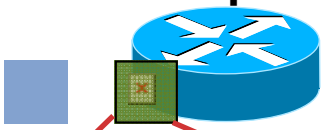
NetFlow Architecture



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

NetFlow Key Fields Creating Flow Records

Example 1



Inspect Packet

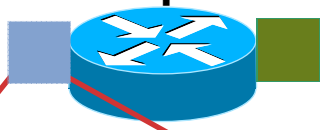
Key Fields	Packet 1
Source IP	1.1.1.1
Destination IP	2.2.2.2
Source Port	23
Destination Port	22078
Layer 3 Protocol	TCP - 6
ToS Byte	0
Input Interface	Ethernet 0

Create Flow Record in the Cache

Source IP	Dest. IP	Dest. I/F	Protocol	ToS	…	Pkts
1.1.1.1	2.2.2.2	E1	6	0	…	11000

1. Inspect packet for key field values
2. Compare set of values to NetFlow cache
3. If the set of values are unique create a flow in cache
4. Inspect the next packet

Example 2



Inspect Packet

Key Fields	Packet 2
Source IP	3.3.3.3
Destination IP	2.2.2.2
Source Port	23
Destination Port	22079
Layer 3 Protocol	TCP - 6
ToS Byte	0
Input Interface	Ethernet 0

Add New Flow to the NetFlow Cache

Source IP	Dest. IP	Dest. I/F	Protocol	ToS	…	Pkts
3.3.3.3	2.2.2.2	E1	6	0	…	11000
1.1.1.1	2.2.2.2	E1	6	0	…	11000

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

NetFlow Flow Fields

- NetFlow maintains per flow data in flow records
  - Key fields

    Key fields define the flow record

    An attribute in the packet used to create a flow record

    If the set of key field values is unique a new flow is created

  - Nonkey fields are used not to define a flow, instead they provide additional information

    Value fields

    These are additional fields and counters, such as packet and byte counter, start and stop time stamps

    Lookup fields

    These are additional information that are added to the flow, such as next hop address, source/destination AS number, etc.

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

NetFlow Cache Example

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 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

4. Export version

Non-aggregated flows—export version 5 or 9

5. Transport protocol

Export Packet

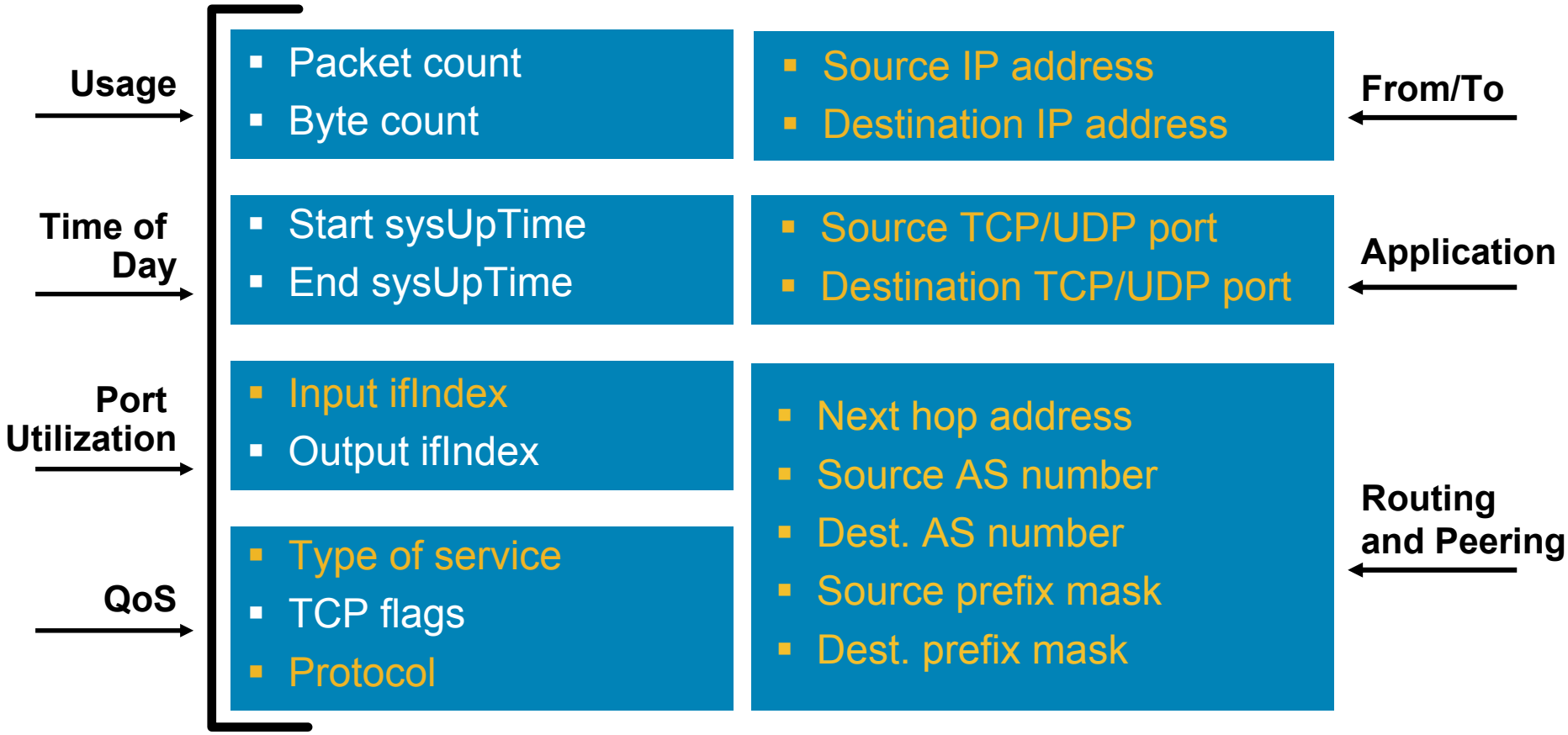
E.g. Protocol-Port Aggregation Scheme Becomes

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

Aggregated Flows—Export Version 8 or 9

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Version 5—Fixed Export Format



Version 5 Used Extensively Today

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Version 8—Fixed Aggregation Format

- 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
- Several aggregations can be enabled simultaneously

Note:
NetFlow Version 9 Can Be Used for Router-Based Aggregation and Is Recommended if Collector Supports v9

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Show NetFlow Information 'show ip cache flow'

For Your Reference

```
router_A#sh ip cache flow
IP packet size distribution (85435 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
  2728 active, 3368 inactive, 85310 added
  463824 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-X                2      0.0         1  1440      0.0      0.0       9.5
TCP-other        82580     11.2         1  1440     11.2      0.0      12.0
Total:           82582     11.2         1  1440     11.2      0.0      12.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         132.122.25.60   Se0/0         192.168.1.1     06 9AEE 0007     1
Et0/0         139.57.220.28   Se0/0         192.168.1.1     06 708D 0007     1
Et0/0         165.172.153.65  Se0/0         192.168.1.1     06 CB46 0007     1
```

Packet Sizes

# of Active Flows

Rates and Duration

Flow Details Cache

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Extensibility and Flexibility Requirements Phases Approach

- Traditional NetFlow with the v5, v7, or v8 NetFlow export
  - New requirements: build something flexible and extensible
- Phase 1: NetFlow version 9
  - Advantages: extensibility
    - Integrate new technologies/data types quicker (MPLS, IPv6, BGP next hop, etc.)
    - Integrate new aggregations quicker

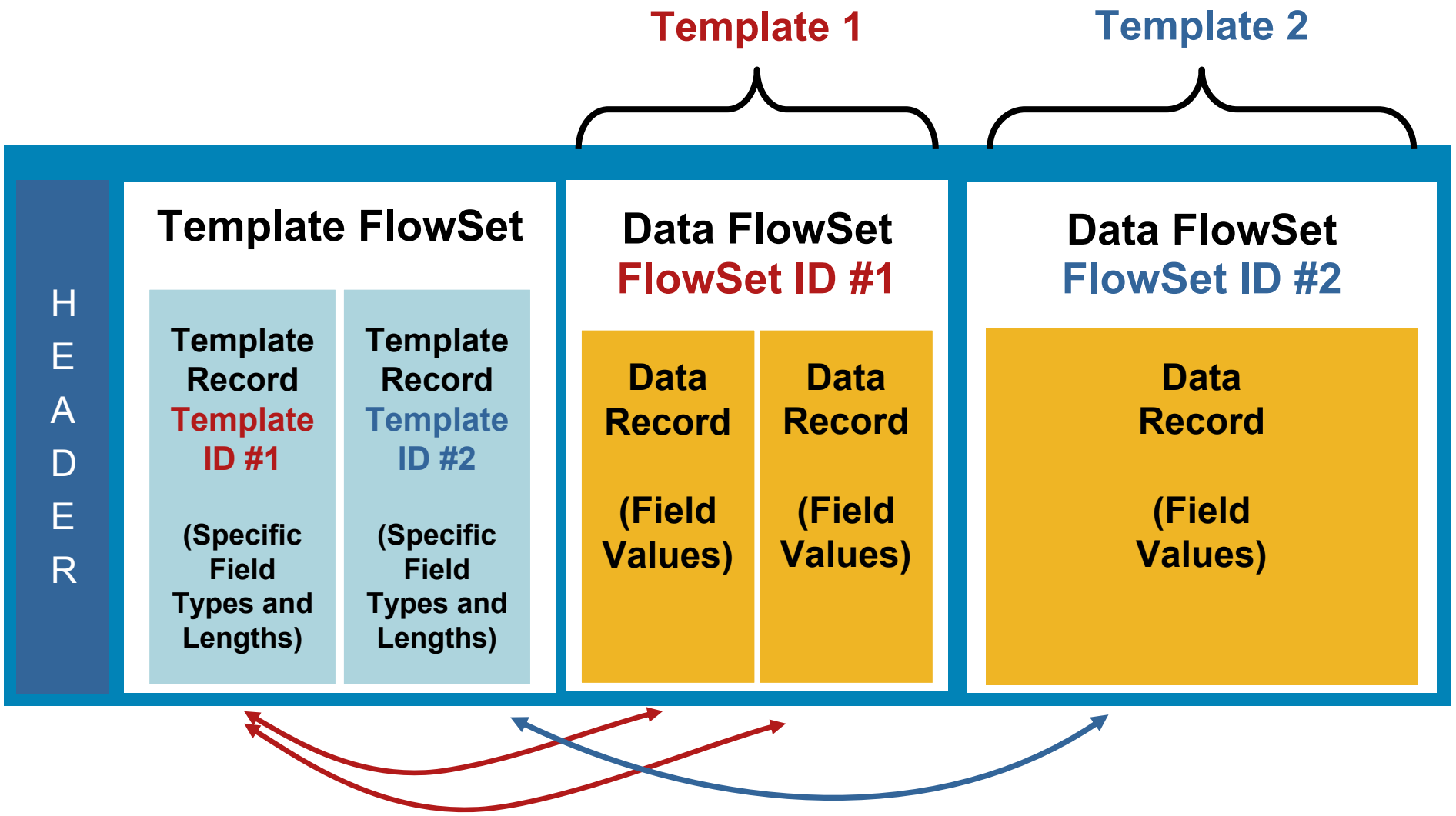
Exporting Process

- Phase 2: Flexible NetFlow
  - Advantages: cache and export content flexibility
    - User selection of flow keys
    - User definition of the records

Metering Process

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

NetFlow Version 9 Export Packet



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Flexible NetFlow
High-Level Concepts and Advantages

- Flexible NetFlow feature allows user configurable NetFlow record formats, selecting from a collection of fields:
  - Key, Non-key, Counter, Timestamp
- Advantages:
  - Tailor a cache for specific applications, not covered by existing NetFlow features
  - Different NetFlow caches: per sub-interface, per direction (ingress, egress), per sampler, per …
  - Better scalability since flow record customization for particular application reduces number of flows to monitor

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

NetFlow Configuration Example (IOS XR)

For Your Reference

Step 1. Create and configure an exporter map.

An exporter map contains user network specification and transport layer details for the NetFlow export packet.

Step 2. Create and configure a monitor map and a sampler map.

A monitor map contains name references to the flow record map and flow exporter map. The following monitor maps atributes can be configured: number of entries in the flow cache, type of cache (permanent or normal), active flow timeout, inactive flow timeout, update timeout, default timeouts, record type of packets sampled and collected

Step 3. Apply the monitor map and sampler map to an interface.

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

NetFlow Configuration Example (IOS XR)

For Your Reference

```
flow exporter-map FEM
   destination 10.1.1.1
   source Loopback 0
   transport udp 1024
   dscp 10
   version v9

flow monitor-map FMM
   record ipv4
   exporter FEM
   cache entries 10000
   cache timeout active 30
   cache timeout inactive 15

sampler-map FSM
   random 1 out-of 1000

interface TenGigE 0/0/0/0
   flow ipv4 monitor FMM sampler FSM ingress
```


© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Configure a User-Defined Flow Record

Configure the Exporter

```
Router(config)# flow exporter my-exporter
Router(config-flow-exporter)# destination 1.1.1.1
```

Configure the Flow Record

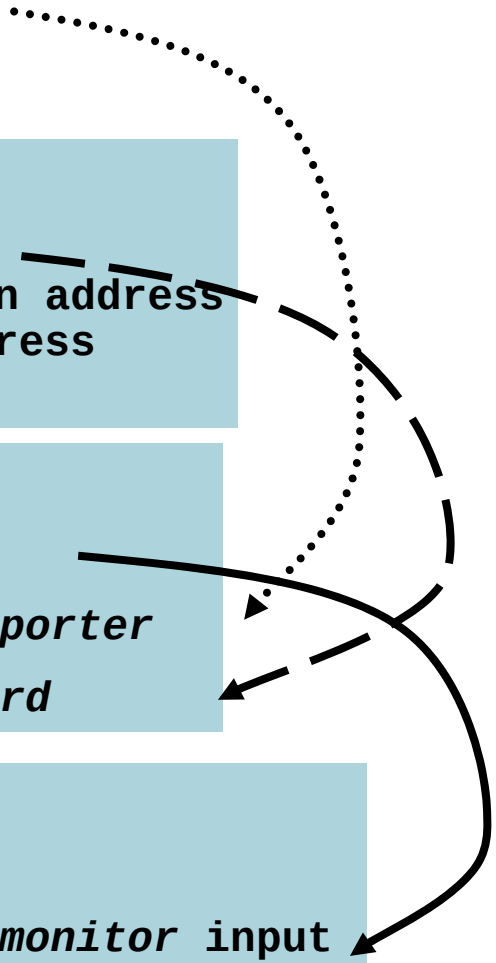
```
Router(config)# flow record my-record
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match ipv4 source address
Router(config-flow-record)# collect counter bytes
```

Configure the Flow Monitor

```
Router(config)# flow monitor my-monitor
Router(config-flow-monitor)# exporter my-exporter
Router(config-flow-monitor)# record my-record
```

Configure the Interface

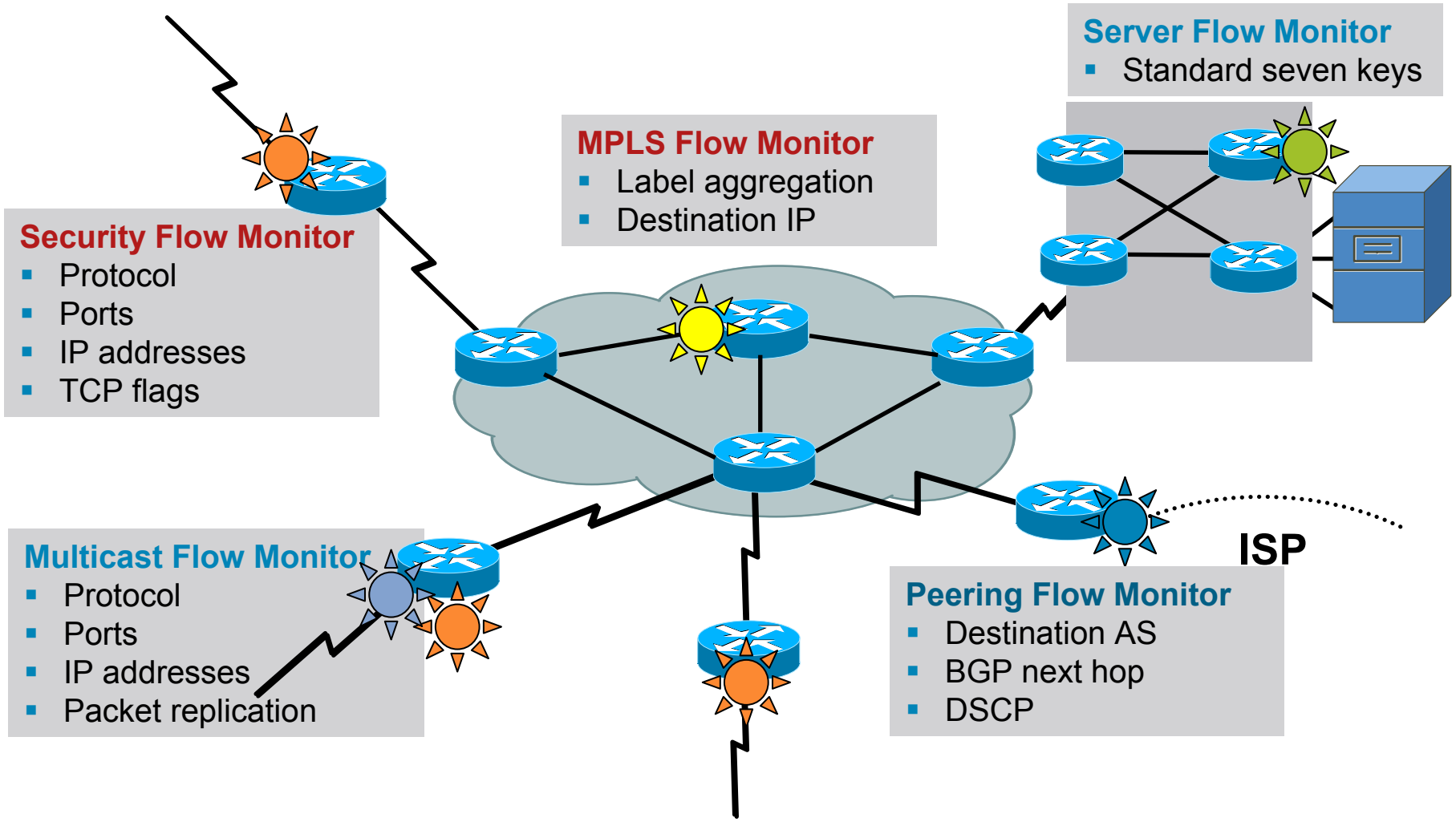
```
Router(config)# interface s3/0
Router(config-if)# ip flow monitor my-monitor input
```



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Flexible NetFlow Tracking Data With Flow Monitors

Different Flow Monitors for Different Applications



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco Applications and Partners

Traffic Analysis

OPNET
AdventNet Excellence Matters
Cisco Systems Empowering the Internet Generation NetFlow Collector
IBM
CRANNOGSOFTWARE now part of Fluke Networks
FLUKE networks
hp invent
InfoVista
isarNet Professional Networking
NetQoS Performance Experts
wiredcity a division of OSIsoft, Inc.
Valencia Systems
netusage
PAESSLER
concord | ca
SOLARWINDS
Caligare
ARBOR NETWORKS
net monitor
plixer International
COMPUWARE
IdeaData Group

Denial of Service

Cisco Systems Empowering the Internet Generation CS-Mars
Lancope®
ARBOR NETWORKS

Billing

EVIDENT SOFTWARE
PORTAL
NetQoS Performance Experts

More info: http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/commercial/

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

NetFlow Open Source Tools

Product Name	Primary Use	Comment	OS
Cflowd	Traffic Analysis	No longer supported	UNIX
Flow-tools	Collector Device	Scalable	UNIX
Flowd	Collector Device	Support V9	BSD, Linux
FlowScan	Reporting for Flow-Tools		UNIX
IPFlow	Traffic Analysis	Support V9, IPv4, IPv6, MPLS, SCTP, etc..	Linux, FreeBSD, Solaris
NetFlow Guide	Reporting Tools		BSD, Linux
NetFlow Monitor	Traffic Analysis	Supports V9	UNIX
Netmet	Collector Device		Linux
NTOP	Security Monitoring		UNIX
Panoptis	Security Monitoring		UNIX
Stager	Reporting for Flow-Tools		UNIX

Different Costs: Implementation and Customization

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Wykorzystanie Netflow

© 2006 Cisco Systems, Inc. All rights reserved.

Potencjalne wykorzystanie Netflow

1. Monitorowanie sieci (aplikacje i użytkownicy)
2. Planowanie sieci
3. Identyfikowanie ataków i innych zagrożeń (wirusy, DDoS)
4. Wykorzystanie w systemach bilingowych
5. Analiza ruchu na styku operatorów (traffic engineering)

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Monitorowanie sieci (aplikacje i użytkownicy)

Pytania:

- Jakiego rodzaju ruch (aplikacje) występują w naszej sieci ?
- Kto z moich użytkowników / klientów generuje najwięcej/najmniej ruchu ?
- Kto jest użytkownikiem mojej sieci i jaki generuje ruch (wielkość i rodzaj ruchu) ? Jaki jest kierunek tego ruchu ?
- Kiedy dany rodzaj ruchu pojawia się w sieci (rano, a może coś dzieje się w nocy) ?
- Czy dany rodzaj ruch przesyłany jest na odpowiednim łączu (vide planowanie sieci) ?

Czy netflow ma pod tym kątem ograniczenia ? Jakie ?

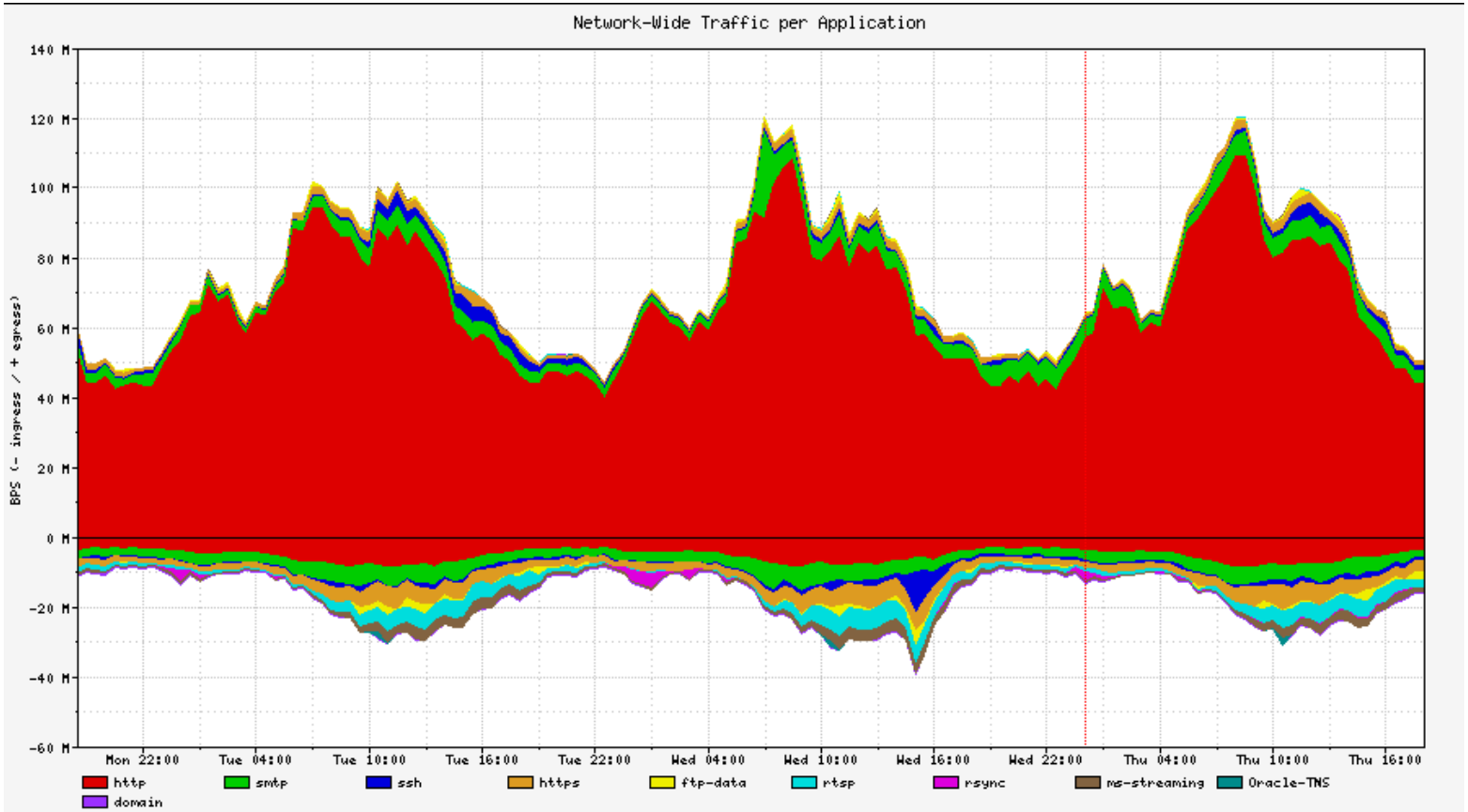
© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Monitorowanie sieci (aplikacje i użytkownicy)

- „*Network Monitoring*—NetFlow data enables extensive near real time network monitoring capabilities. Flow-based analysis techniques may be utilized to visualize traffic patterns associated with individual routers and switches as well as on a network-wide basis (providing aggregate traffic or application based views) to provide proactive problem detection, efficient troubleshooting, and rapid problem resolution”.
- „*Application Monitoring and Profiling*—NetFlow data enables network managers to gain a detailed, time-based, view of application usage over the network. This information is used to plan, understand new services, and allocate network and application resources (e.g. Web server sizing and VoIP deployment) to responsively meet customer demands”.
- User monitoring is performed by monitoring the IP addresses of the devices that users are running applications on.

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Pytanie – ile lat temy był zrobiony poniższy diagram ?



source - Cisco IT NetFlow Success Story
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_case_study0900aecd80311fc2.pdf

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Dynamic Top Talkers

Show ip flow top <N> <aggregate-field> <sort-criteria> <match-criteria>

Top 10 Protocols Currently Flowing Through the Router router#show ip flow top 10 aggregate protocol
Top 10 IP Addresses Which Are Sending the Most Packets router#show ip flow top 10 aggregate source-address sorted-by packets
Top 5 Destination Addresses to Which We're Routing Most Traffic from the 10.0.0.1/24 Prefix router#show ip flow top 5 aggregate destination-address match source-prefix 10.0.0.1/24
50 VLANs Which We're Sending the Least Bytes To router#show ip flow top 10 aggregate destination-vlan sorted-by bytes ascending
Top 20 Sources of One-Packet Flows router#show ip flow top 10 aggregate source-address match packets one

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Planowanie sieci

Pytania:

- W jaki sposób śledzić i przewidywać rozwój naszej sieci ?
- Czy potrzebuje w swojej sieci wprowadzić mechanizmy QoS ? Czy umiem odpowiedzieć na pytanie dlaczego moja firma ma wydać pieniądze na tego typu wdrożenie ?
- Czy zasoby mojej sieci są wykorzystywane optymalnie (sieci enterprise / sieci SP) ? Czy ja rzeczywiście rozbudowuję sieć pod główny ruch pod jaki sieć została zaprojektowana (rodzaje ruchu – sieć wielousługowa ☺) czy też „ktoś zjada moje zasoby”.
- **Co się stanie z ruchem w mojej sieci gdy nastąpi usterka jednego z łączy** ?

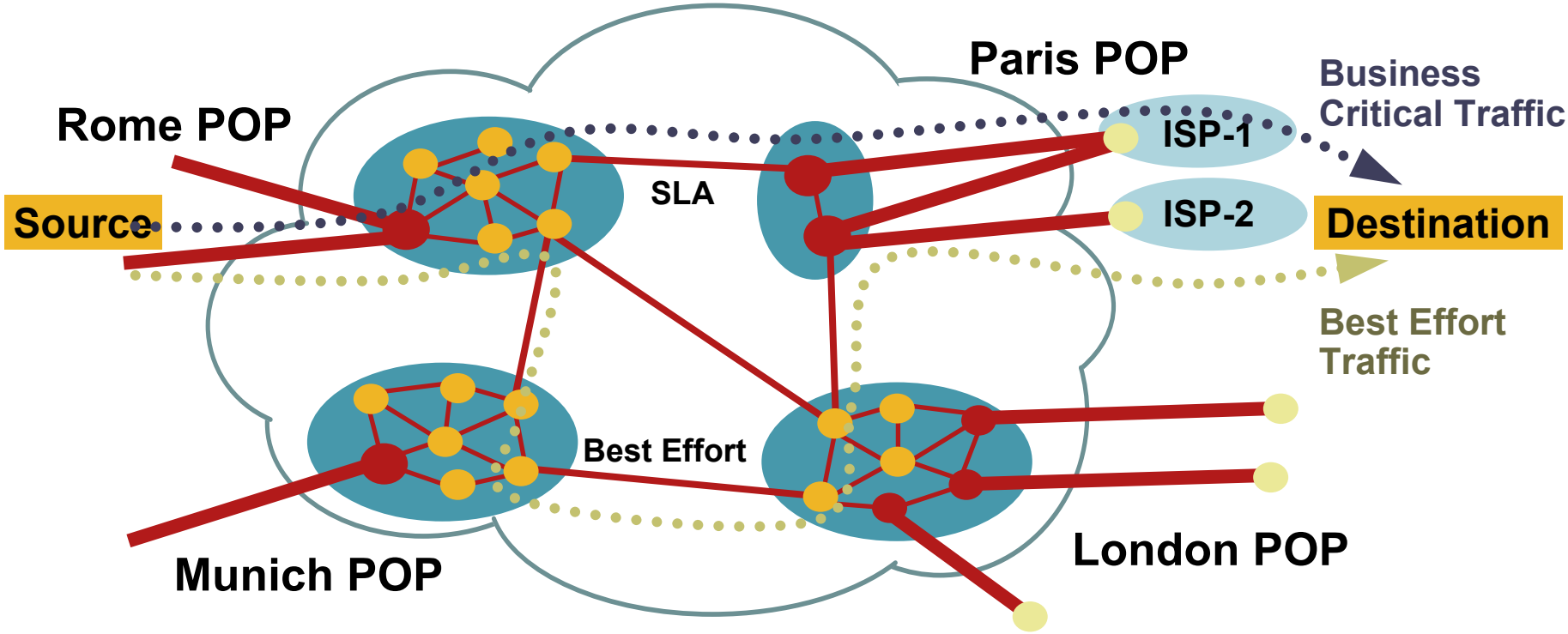
© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Core Capacity Planning

1. The ability to offer SLAs is dependent upon ensuring that core network bandwidth is adequately provisioned
2. Adequate provisioning (without gross overprovisioning) 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

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Network planning - The Core Traffic Matrix

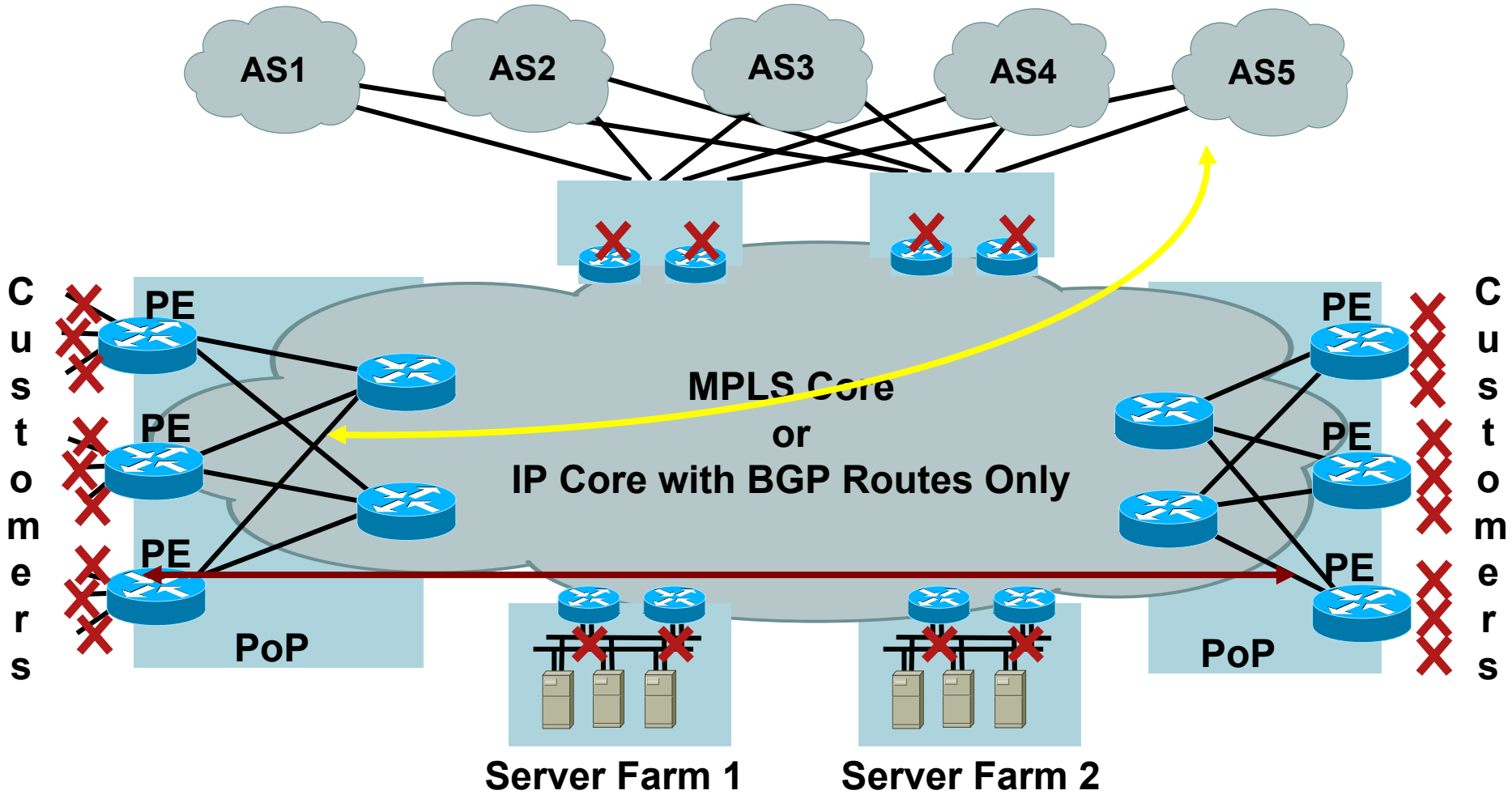


	Rome Exit Point	Paris Exit Point	London Exit Point	Munich Exit Point
Rome Entry Point	NA (*)	…Mb/s	…Mb/s	…Mb/s
Paris Entry Point	…Mb/s	NA (*)	…Mb/s	…Mb/s
London Exit Point	…Mb/s	…Mb/s	NA (*)	…Mb/s
Munich Exit Point	…Mb/s	…Mb/s	…Mb/s	NA (*)

(*) Potentially Local Exchange Traffic

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

BGP Next Hop TOS Aggregation Typical Example



Internal Traffic: “PE to PE”

External Traffic Matrix PE to BGP AS

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Identyfikowanie ataków i innych zagrożeń (wirusy, DDoS)

Pytania:

- Czy mogę zauważyć atak i inne zagrożenie korzystając z Netfow ? Jak mogę ustalić rodzaj zagrożenia ?
- Czy jestem w stanie przedstawić w czasie historię ataku ?

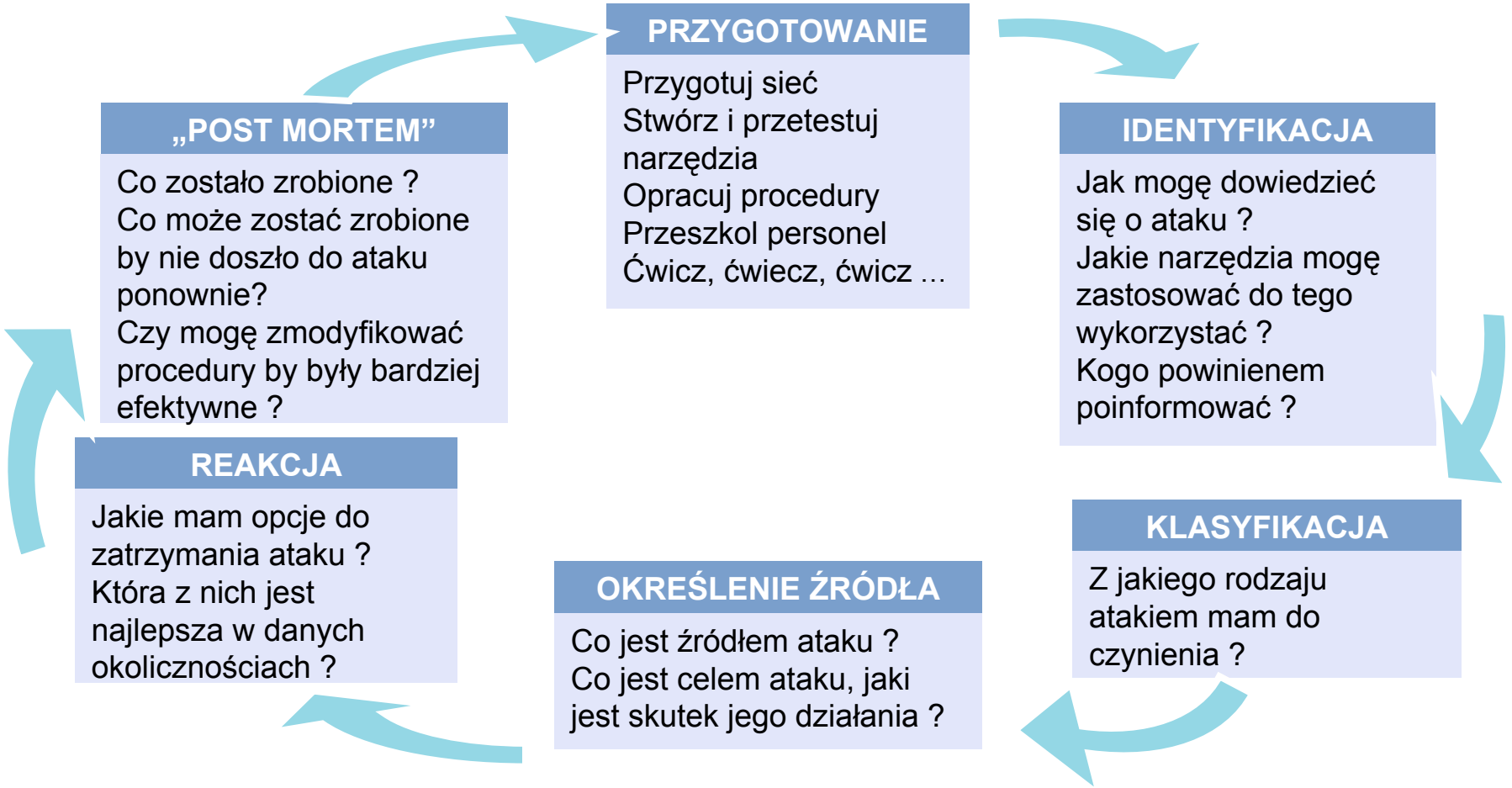
Określenie normalnego zachowania się sieci.

- Netflow na brzegu sieci
- Próbkowany netflow w szkielecie sieci
- Wyszukiwianie anomalii, określenie skąd przyszedł atak i odpowiednie reagowanie używając innych narzędzi…

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Identyfikowanie ataków i innych zagrożeń (wirusy, DDoS)

Bądź przygotowany na incydenty związane z bezpieczeństwem twojej sieci.



„Bezpieczeństwo infrastruktury sieciowej operatorów telekomunikacyjnych”, Krzysztof Mazepa, Cisco Forum Zakpoane 2008

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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, destination IP, one packet per flow, constant bytes per packet (B/Pk)
- Don’t forget “show ip cache verbose flow | include …”
- Export to a security oriented collector: CS-MARS, Lancope, Arbor

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Tracing Back with Netflow

- Routers need Netflow to be enabled

Victim

```
router1#sh ip cache flow | include <destination>
Se1        <source>      Et0        <destination>    11 0013 0007   159
...(lots more flows to the same destination)
```

The flows come from serial 1

```
router1#sh ip cef se1
Prefix              Next Hop          Interface
0.0.0.0/0           10.10.10.2        Serial1
10.10.10.0/30       attached          Serial1
```

Find the upstream router on serial 1

Continue on this router

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

NetFlow Top Talkers

- The flows that are generating the heaviest traffic in the cache are known as the “top talkers”; prefer “top flows”
- 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, work like a filter
- The top talkers can be retrieved via the CISCO-NETFLOW-MIB (cnfTopFlowsTable)
- 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

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

NetFlow Top Talkers

```
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   171.0
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
```


© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

NetFlow Dynamic Top Talkers

- Somehow similar to the top talkers
  - But dynamic, done on the fly with show commands
  - But does not require modifications to the router config
  - But does not create a new cache
  - But no available with the MIB—obviously
- Even more useful than top talkers for security
- “show ip flow top” command:
  - show ip flow top <N> <aggregate-field> <sort-criteria> <match-criteria>

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Dynamic Top Talkers

Show ip flow top <N> <aggregate-field> <sort-criteria> <match-criteria>

Top 10 Protocols Currently Flowing Through the Router router#show ip flow top 10 aggregate protocol
Top 10 IP Addresses Which Are Sending the Most Packets router#show ip flow top 10 aggregate source-address sorted-by packets
Top 5 Destination Addresses to Which We're Routing Most Traffic from the 10.0.0.1/24 Prefix router#show ip flow top 5 aggregate destination-address match source-prefix 10.0.0.1/24
50 VLANs Which We're Sending the Least Bytes To router#show ip flow top 10 aggregate destination-vlan sorted-by bytes ascending
Top 20 Sources of One-Packet Flows router#show ip flow top 10 aggregate source-address match packets one

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Wykorzystanie w systemach bilingowych

Netflow jest jednym z narzędzi accountingu

„NetFlow data provides fine-grained metering (e.g. flow data includes details such as IP addresses, packet and byte counts, timestamps, type-of-service and application ports, etc.) for highly flexible and detailed resource utilization accounting. Service providers may utilize the information for billing based on time-of-day, bandwidth usage, application usage, quality of service, etc. Enterprise customers may utilize the information for departmental charge-back or cost allocation for resource utilization”.

Rozwiązania

- Volume based billing (broadband access, transit and peering agreement)
- Transit and peering agreements (service provider interconnect)
- Destination-sensitive billing
- Enterprise department charge back

Jakie są wasze oczekiwania ? Doświadczenia ?

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

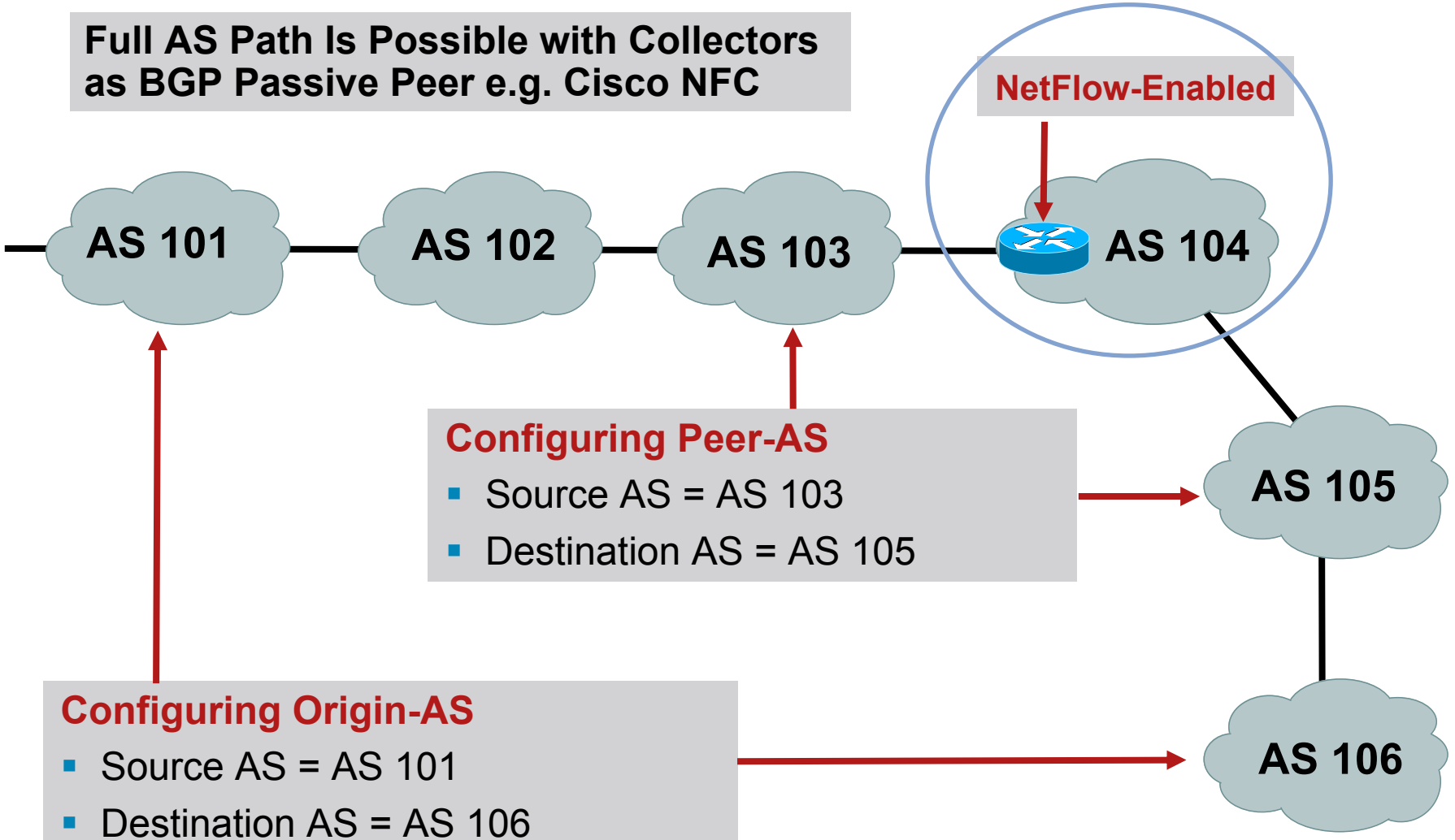
Analiza ruchu na styku operatorów (traffic engineering).

Pytania:

- Czy używam optymalnie swoją sieć (hot potato) ?
- Jaki jest poziom ruchu do/od innych operatorów w punkcie peeringowym ?
- Czy zachowane są warunki na jakich zgodziłem wymieniać się ruchem z innym operatorem ?

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

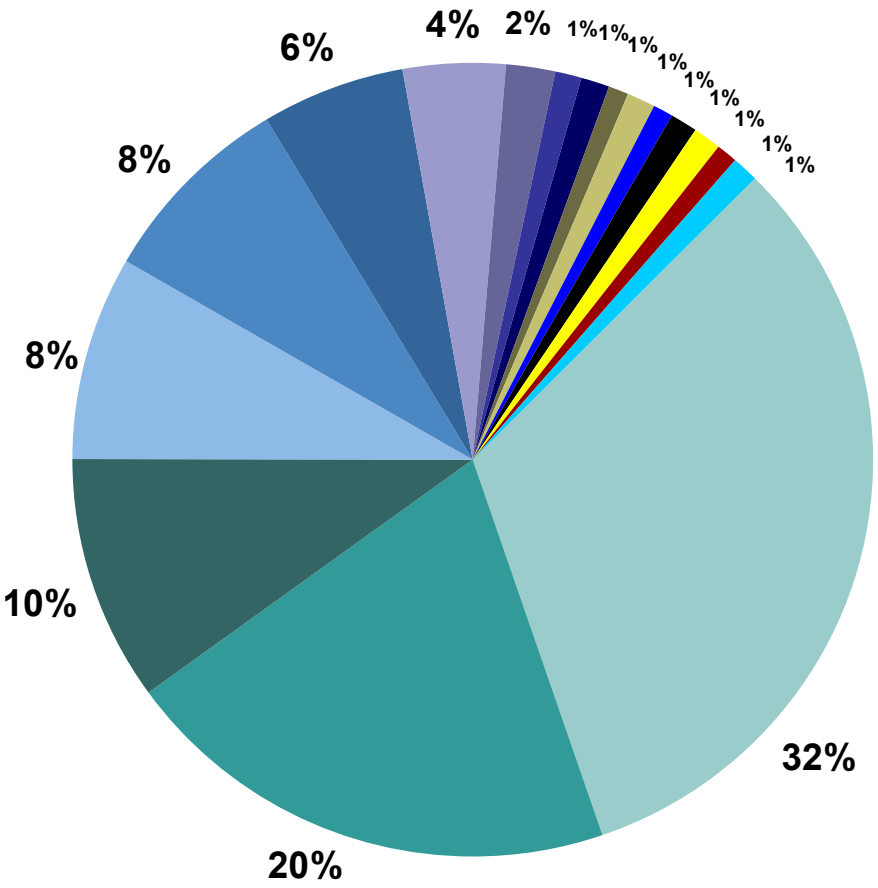
BGP Tracking with Peer and Origin AS



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

NetFlow: Peering Agreement

Public Routers 1, 2, 3 Month of September—Outbound Traffic



- Uunet
- Digex
- Erols
- BBN
- AT&T
- AMU
- C&W
- JHU
- PACBell Internet Service
- RCN
- OARnet
- SURAnet
- Compuserve
- OL
- ABSNET
- WebTV
- WEC

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Podsumowanie - potencjalne wykorzystanie aplikacji Netflow

1. Monitorowanie sieci (aplikacje i użytkownicy)
2. Planowanie sieci
3. Identyfikowanie ataków i innych zagrożeń (wirusy, DDoS)
4. Wykorzystanie w systemach bilingowych
5. Analiza ruchu na styku operatorów (traffic engineering)

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Gdzie szukać dalszych informacji ?

Netflow

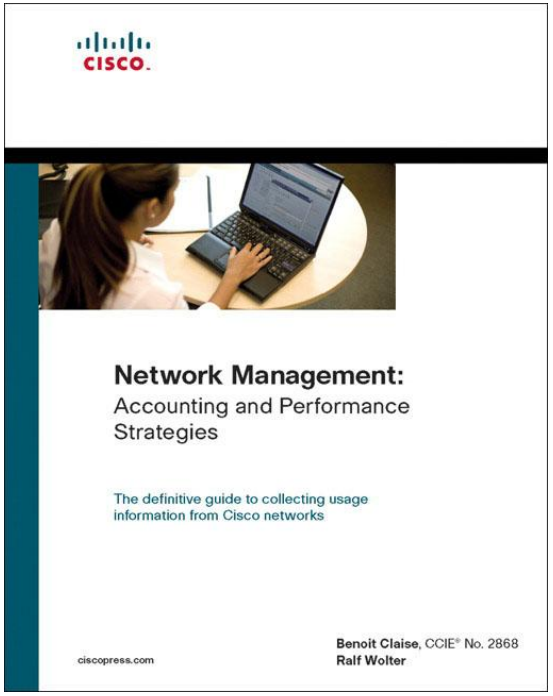
www.cisco.com/go/netflow

Cisco IOS NetFlow Introduction white paper

www.cisco.com/en/US/products/ps6601/products_white_paper0900aecd80406232.shtml

NetFlow solutions guide—technical deployment information

http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Dziękuję za uwagę, komentarze i pytania

kmazepa@cisco.com

 © 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential