Cisco IOS NetFlow and Service Assurance Agent

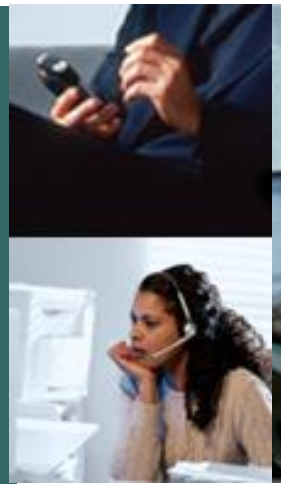
Paul Kohler

ITD Product Marketing

The Five Facets of Proper Network Management

- Addresses the network management applications that reside upon the NMS
- OSI model categorizes five areas of function (sometimes referred to as the FCAPS model):
  - Fault
  - Configuration
  - Accounting
  - Performance
  - Security

Cisco IOS NetFlow



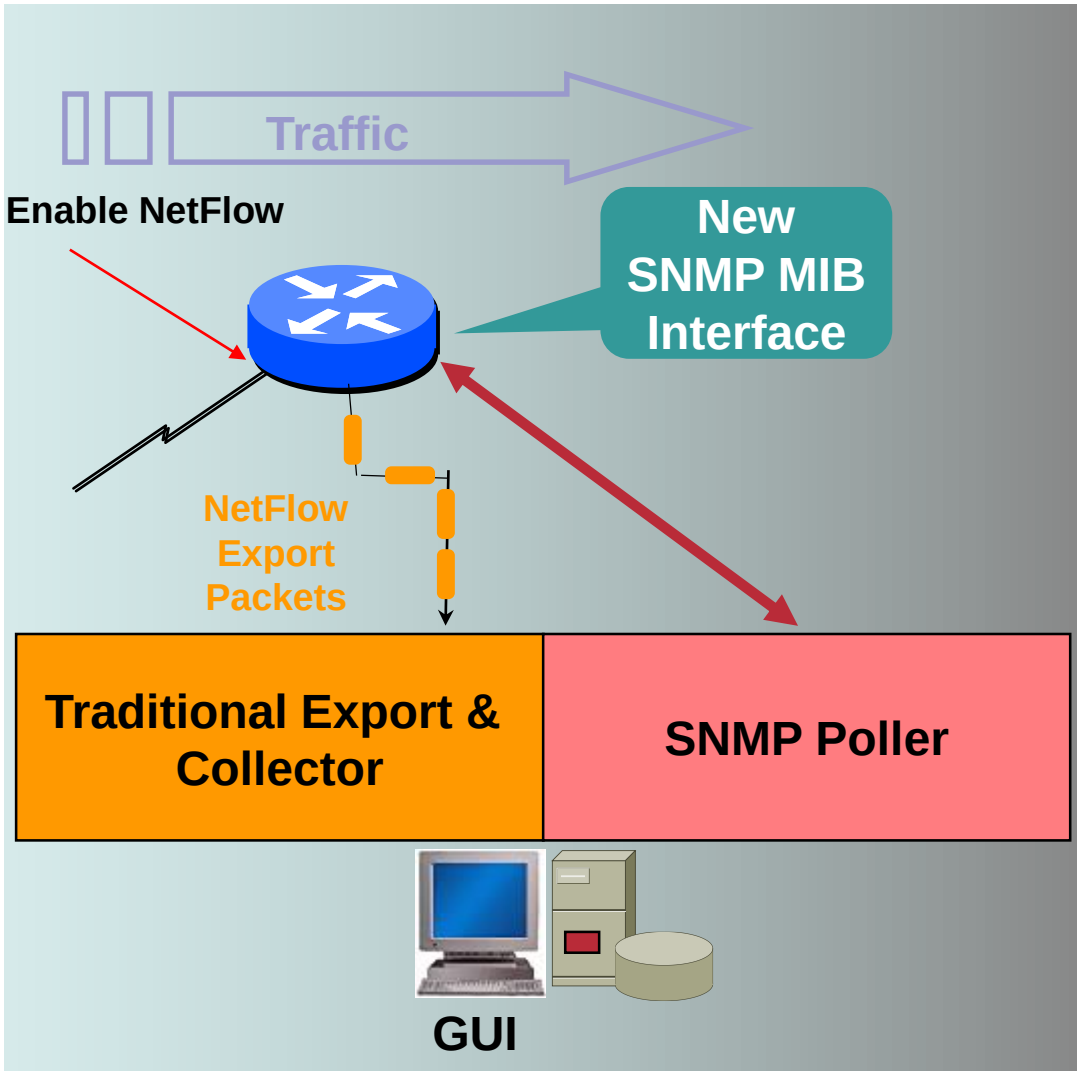
NetFlow Origination

- 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
- A detailed view of network behaviour

What is a Flow ?

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

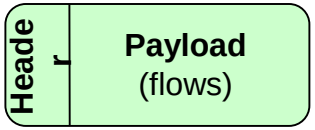
4. Export Version

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

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

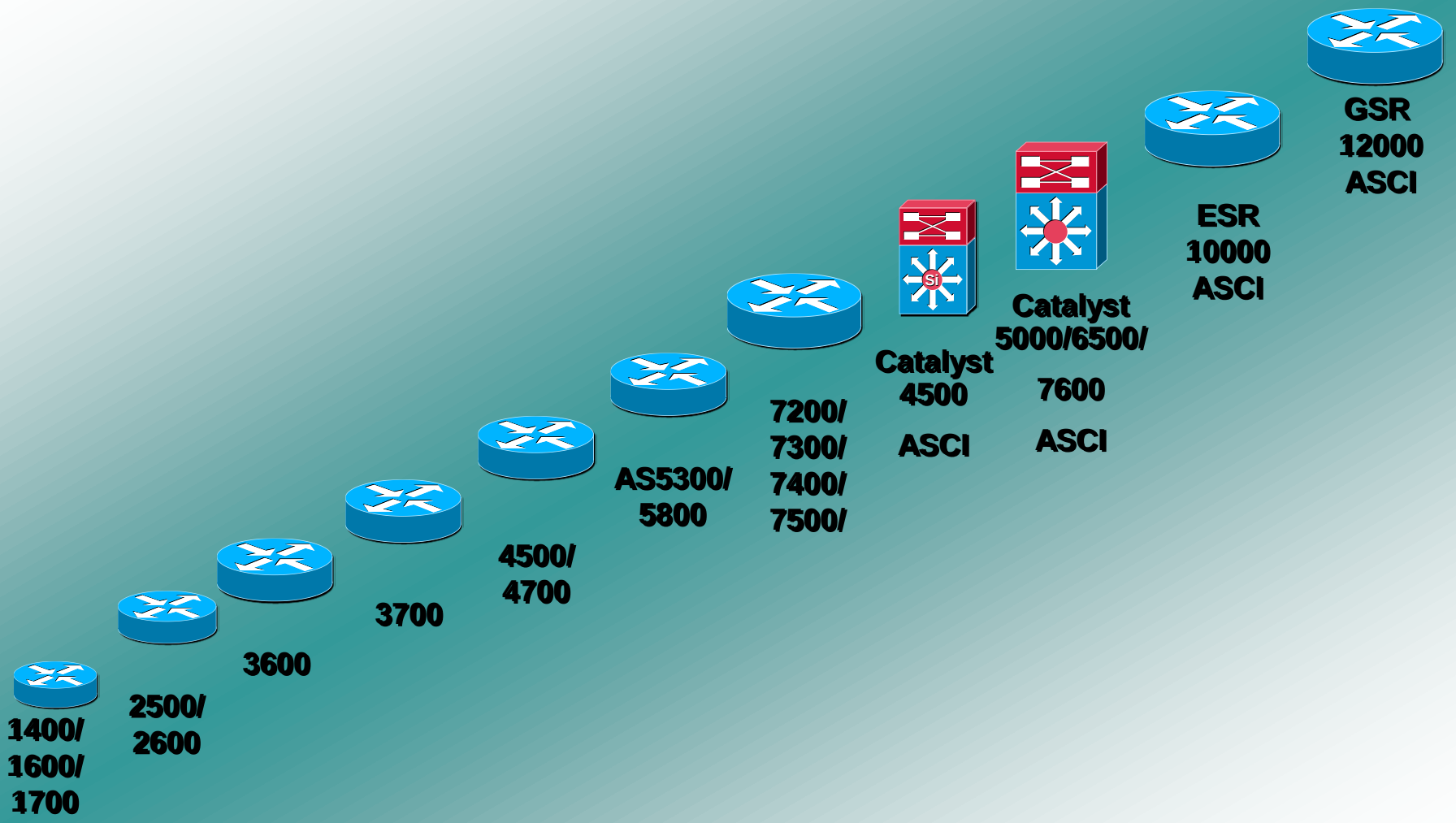
5. Transport Protocol

Export Packet



Comprehensive Platform Support

Cisco.com



Principle Netflow Benefits

Service Provider

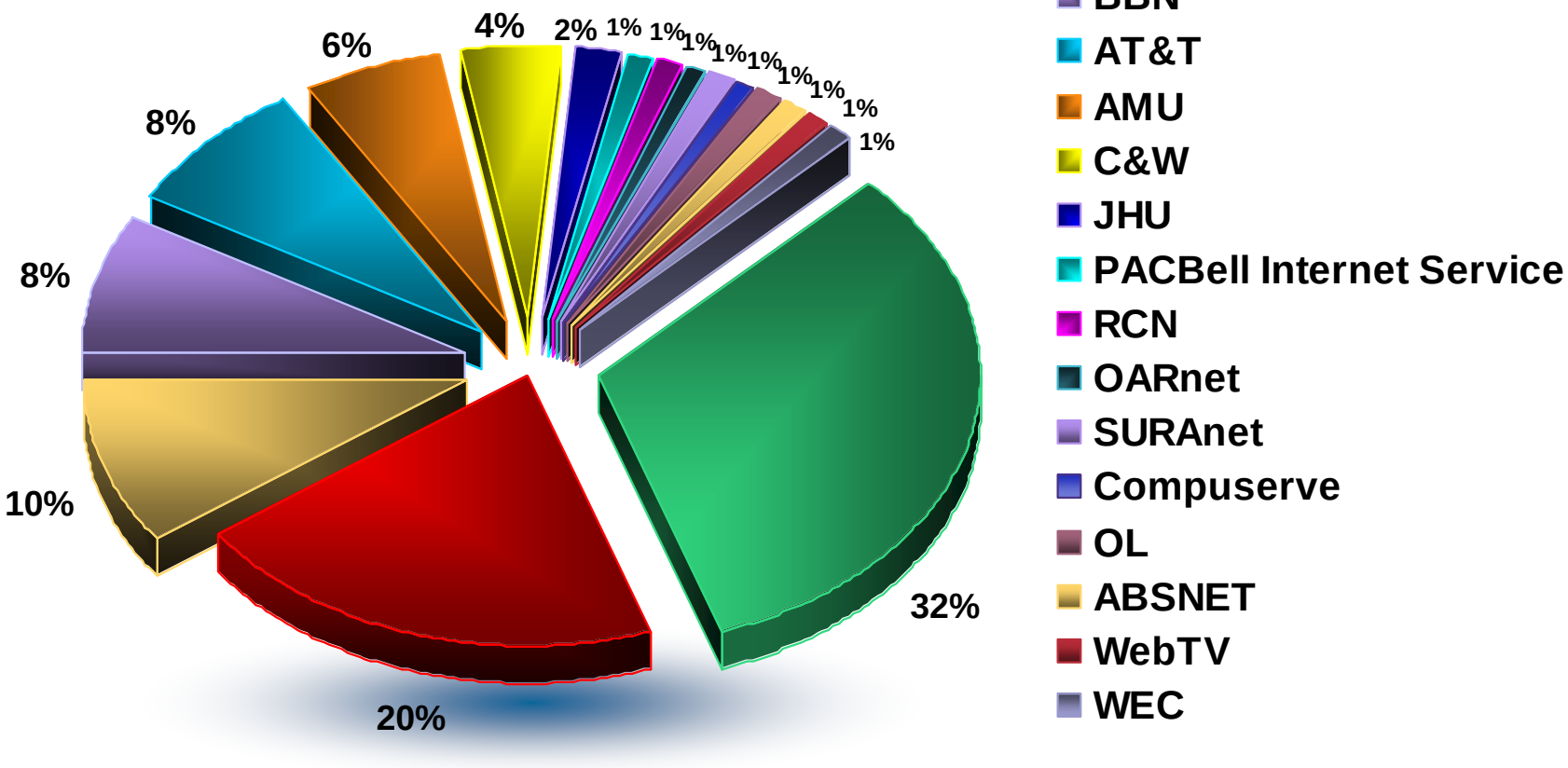
- Peering arrangements
- Network Planning
- Traffic Engineering
- Accounting and billing
- Security Monitoring

Enterprise

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

NetFlow – Peering Agreement

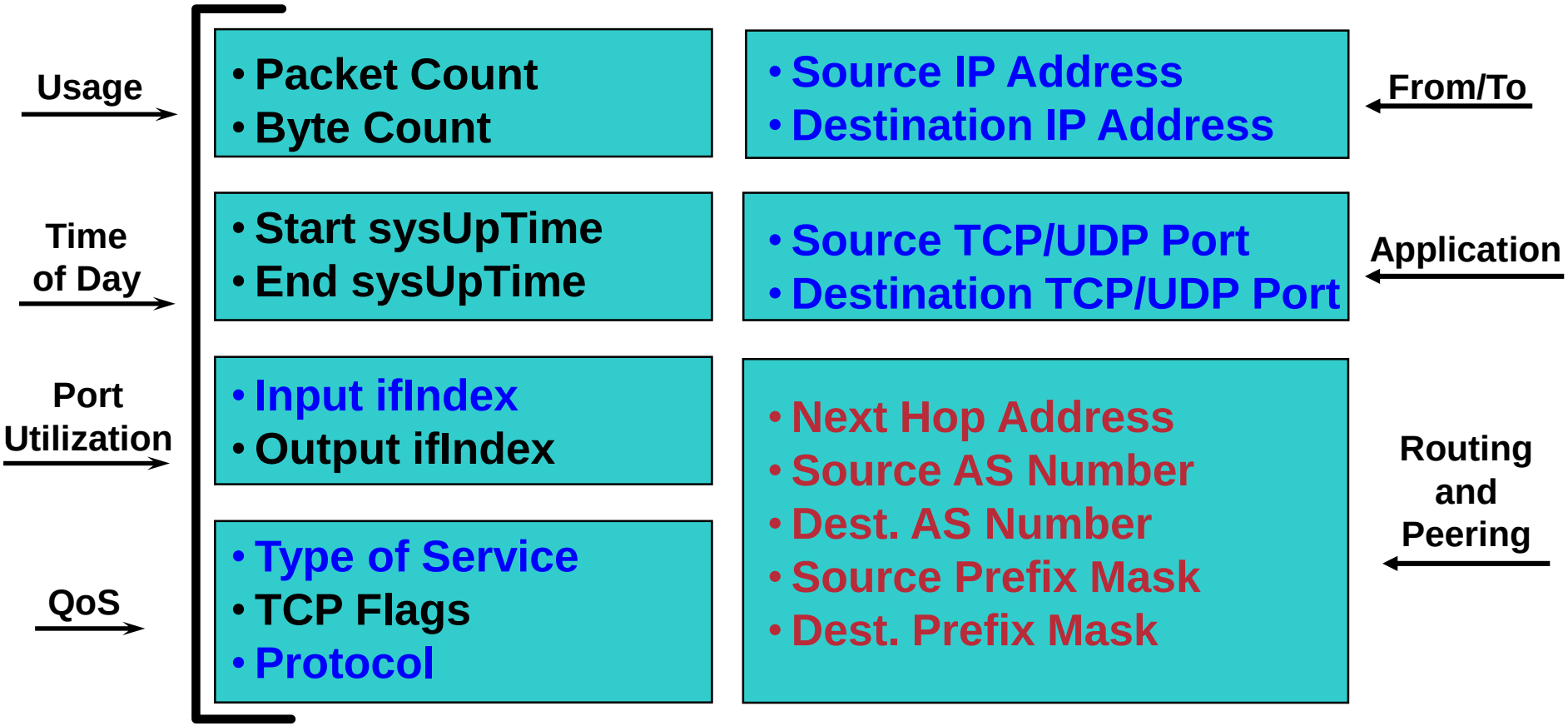
Public Routers 1, 2, 3 Month of September—Outbound Traffic



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

Version 5 - Flow Export Format



Version 5 used extensively today

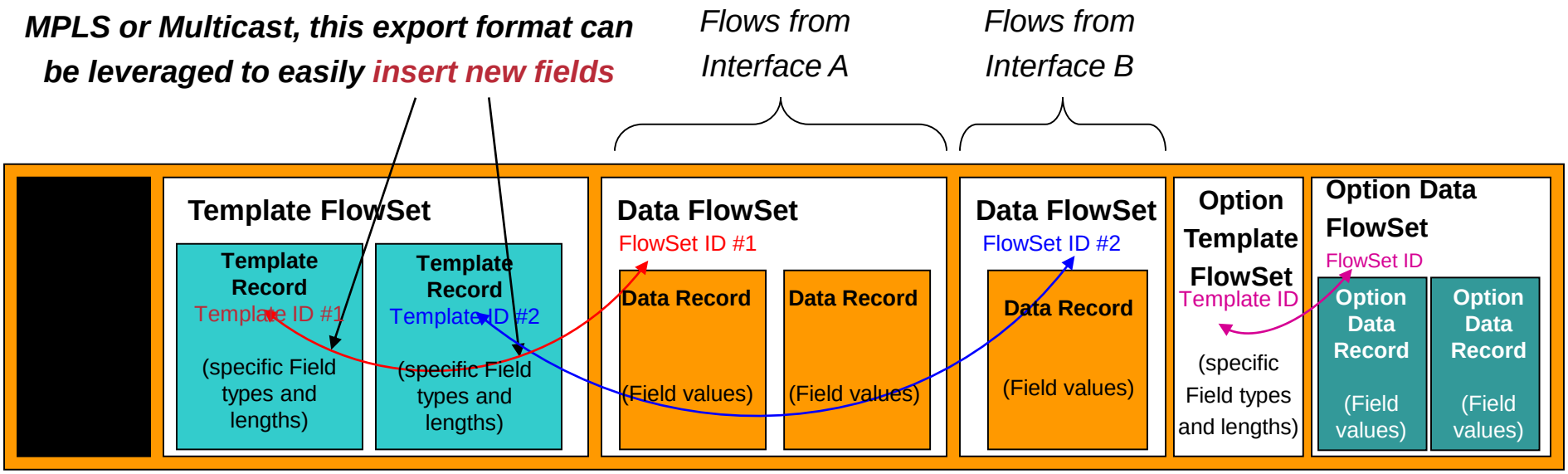
Why a New Version 9?

- Fixed export formats are not flexible and adaptable
- With each new version Cisco creates new export fields

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



- **Matching ID #s is 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 e.g. unicast traffic can be combined with multicast records**
- **If exported flows have different fields then they can't be contained in the same Template Record e.g. BGP next-hop can't be combined with MPLS Aware NetFlow records**

NetFlow v9 and IETF

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

  http://ipfix.doit.wisc.edu/

- **Netflow version 9 is the basis for the standard in the IETF**
- **Informational RFC on NetFlow version 9**
  http://www.ietf.org/internet-drafts/draft-bclaise-netflow-9-00.txt

Features using NetFlow Version 9

- Multicast NetFlow using Version 9 (Now - 12.3M)
  - Ingress Accounting of replicated multicast packets
  - Egress Per user accounting of multicast packets
- MPLS Aware NetFlow using Version 9 (8/2003 – 12.0(26)S)
  - Label and prefix export information
- BGP Next Hop Version 9 (Now – 12.3M)
  - Edge to Edge Traffic Matrix
  - BGP traffic destination information
- NetFlow for IPv6 (Now – 12.3(7)T)
  - Export IPv6 source and destination information

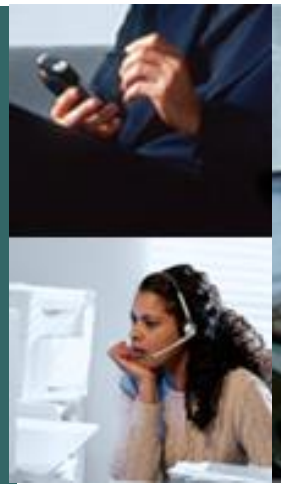
NetFlow Product Update

- **Sampled NetFlow (12.0(26)S)**
  - **Random Sampling of packets per flow with reduce CPU**
- **NetFlow MIB (12.3(7)T)**
  - **Top N Talker in MIB**
  - **NetFlow configuration using MIB**
- **Input Flow Filters (12.3(4)T)**
  - **QOS MQC based Filtering entering NetFlow**

New Features to be released
NetFlow Product Update

- **Egress NetFlow (Q3CY2004)**
  - **Egress Accounting of NetFlow**
- **NetFlow Security Enhancements (Q4CY2004)**
  - **New exports and show commands for security monitoring**
- **Flexible Flow Keys (Q1CY2005)**
  - **Allow user defined flow keys and aggregation with v.9**
- **Reliable and Congestion Aware Export (Q1CY2005)**
  - **SCTP protocol NetFlow export**

Cisco IOS Service Assurance Agent



Cisco IOS SAA Today

Cisco.com

Applications

- Availability
- Network Performance Monitoring
- VoIP Monitoring
- Service Level Agreement (SLA) Monitoring
- Network Assessment
- MPLS Monitoring
- Trouble Shooting

Measurement Metrics

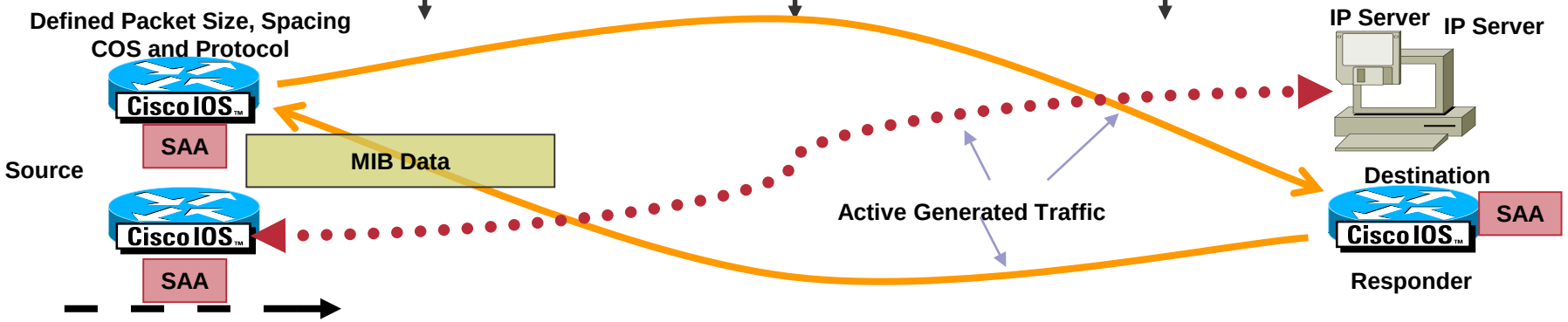
- Round Trip Time
- Packet Loss
- Network Jitter
- Uni-directional Measurements
- Connectivity

Operations

Jitter | FTP | Path Jitter | DNS | DHCP | DLSW | ICMP | UDP | TCP | HTTP | LDP

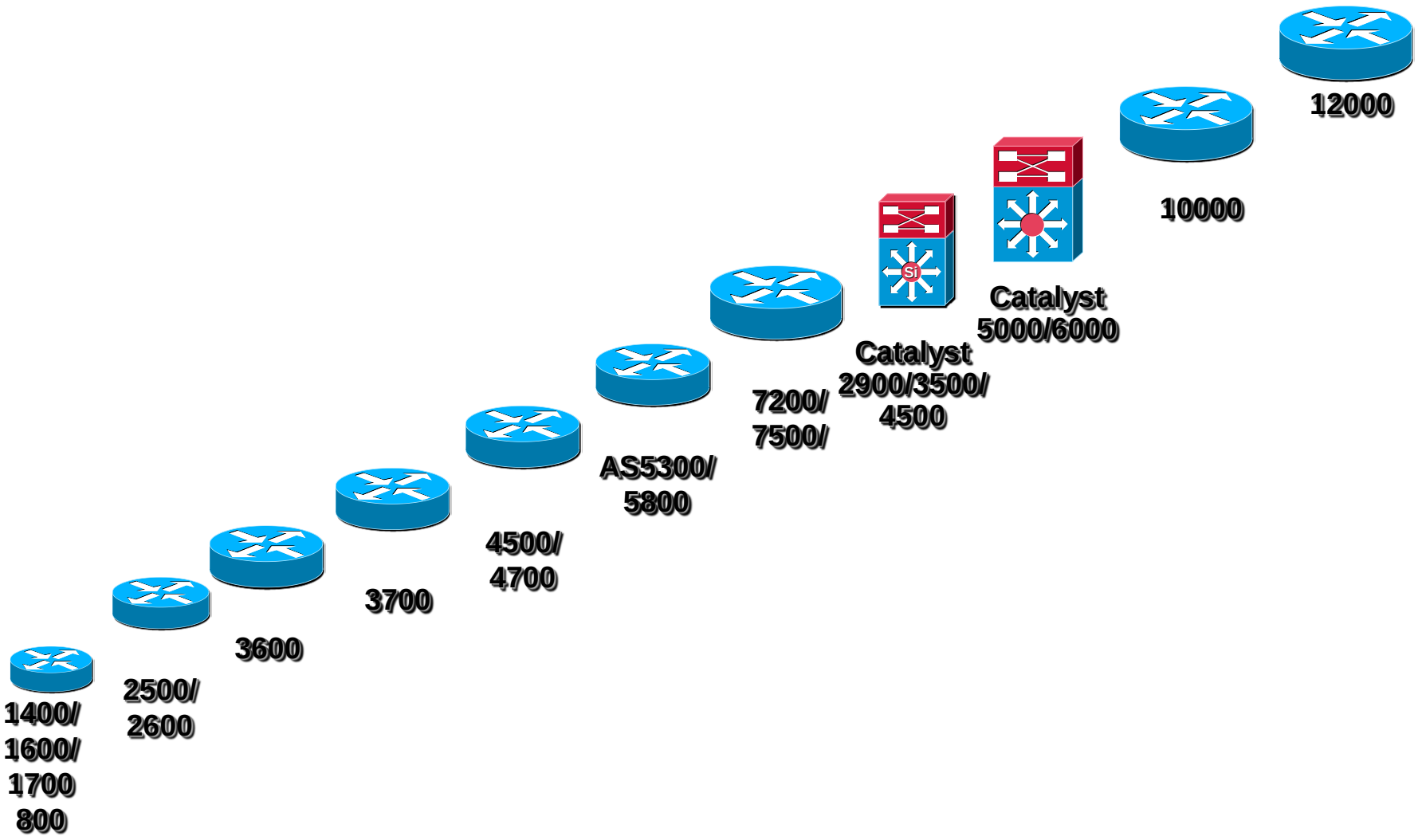
Soon

H323 | SIP | RTP



SAA Comprehensive Hardware Support

Cisco.com

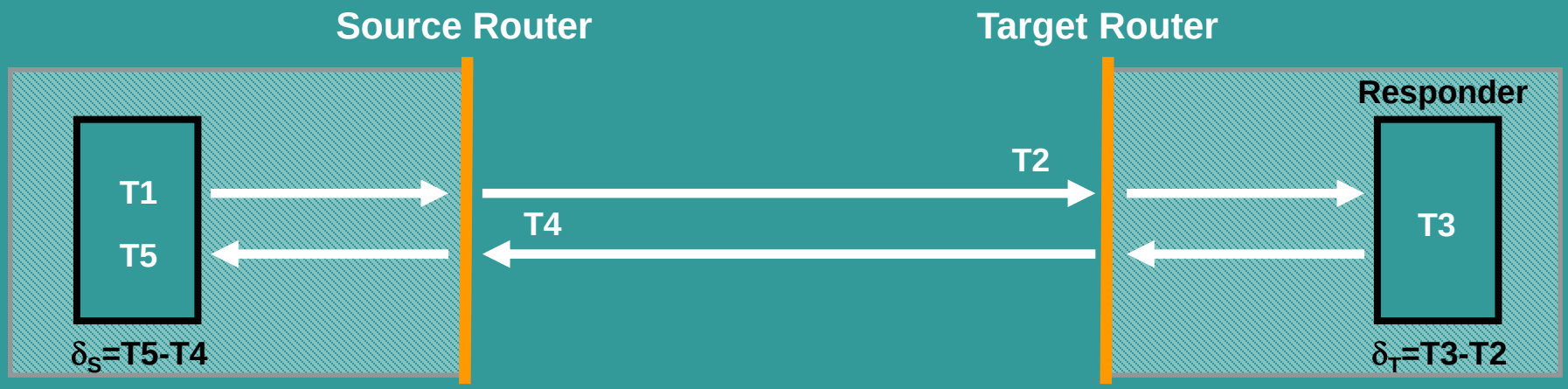


Cisco IOS SAA Source and Responder

- **Source Router**
  - Cisco IOS Software router that sends data from probe
  - Target may or may not be Cisco IOS Software
  - Some operations require the target to run the SAA responder
- **Responder**
  - Responds to SAA packets
  - User defined UDP/TCP ports
  - SAA Control Protocol
  - MD 5 Authentication
  - Accurate measurements

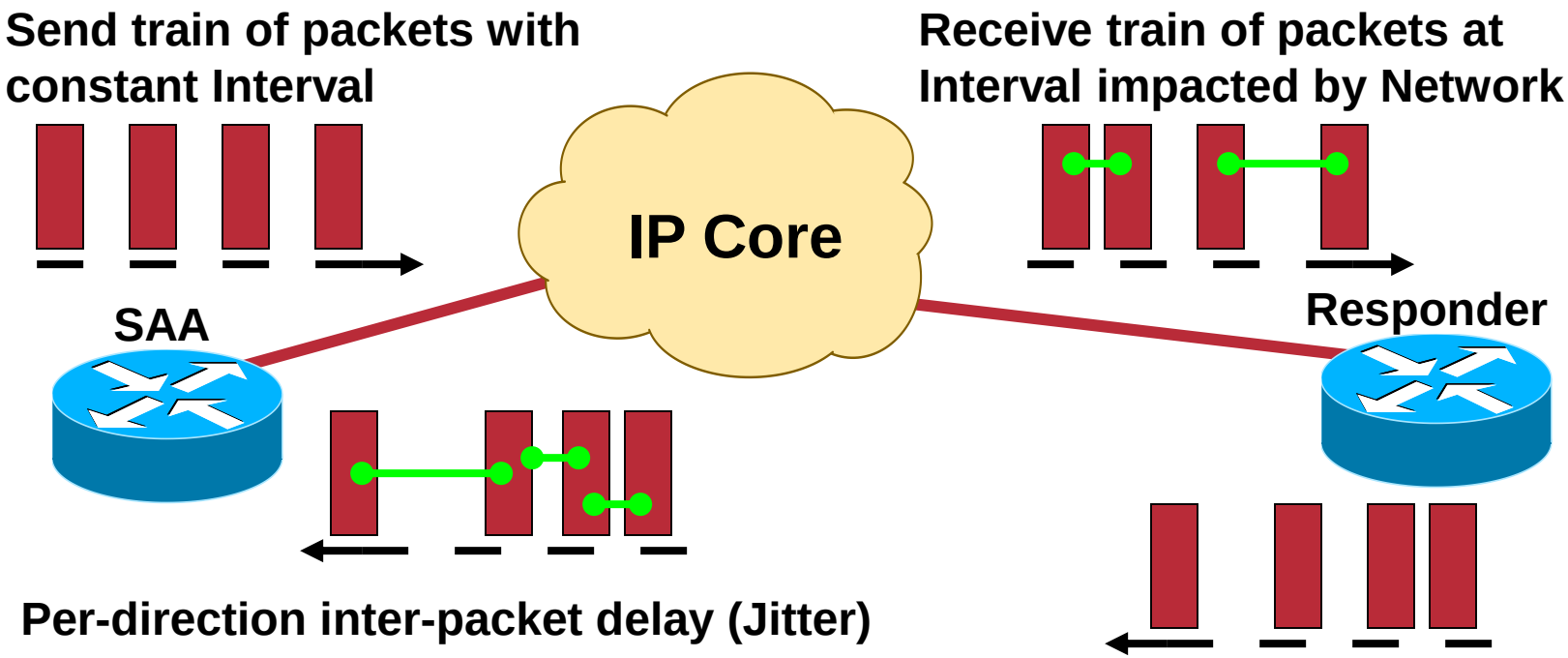
Cisco IOS SAA UDP-based Probe Round Trip Time Calculation

- Patented Control Protocol for UDP operation to Cisco router
- Requires responder for accurate results
- Processing delays subtracted on both source and destination



Cisco IOS SAA Jitter Operation Example

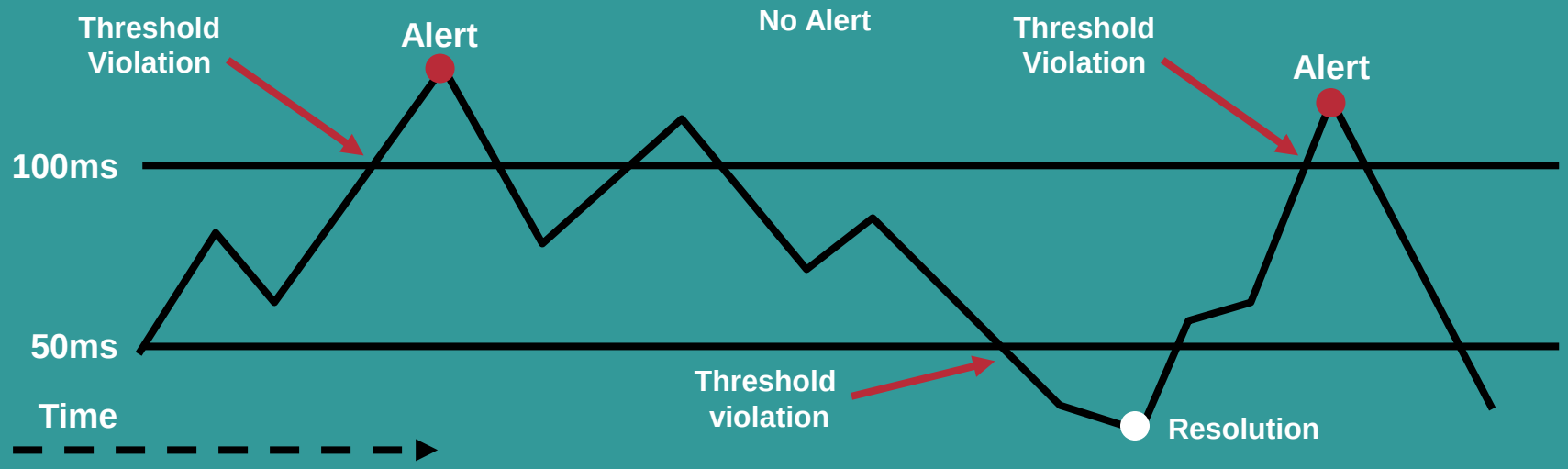
Cisco.com



Cisco IOS SAA Reaction Conditions

- **Reaction Trigger to Events**
  - **Can send SNMP traps for certain "triggering" events**
    - **Connection Loss and Timeout**
    - **Round Trip Time Threshold**
    - **Average Jitter Threshold**
    - **Unidirectional packet loss, latency, jitter, MOS Scores**
  - **Can trigger another SAA operation for further analysis**

Trigger
- **Immediate**
- **Consecutive**
- **X of Y times**
- **Average Exceeded**



Cisco IOS SAA for VoIP

Cisco IOS SAA VoIP Probes Current Functionality

Verify the network is ready for VoIP	Verify QoS setup using DSCP bits in probe traffic
UDP based SAA probe	Jitter, packet loss, RTT measurements
Threshold mechanism	Round trip time, average jitter, and timeout traps
Path probes	Path probes used for trouble shooting
Activate secondary probes based on thresholds	Trigger pat probe based on high jitter value

Cisco IOS IP SLA VoIP Operations

- **Phase 1 – Today Release Nov 2003 (12.3(4)T & 12.2(RLS5)S)**
  - **VoIP Codec Simulations using Cisco IOS IP SLA active monitoring**
    - **G.711 ulaw and alaw, G.729 Codec's**
  - **Voice Quality Scoring**
    - **Industry standard voice quality measurements built into Cisco IOS Software**
    - **G.113 ICPIF and G.107 MOS Voice Quality measurement**
- **Phase 2 – Today Release March 2004 (12.3(7)T)**
  - **New Threshold traps, one-way packet loss, jitter, latency and MOS**
- **Phase 3 – Q4CY2004**
  - **H323 and SIP Post Dial Delay, Gatekeeper delays**
- **Phase 4 – Q1CY2005**
  - **Voice Gateway DSP Integration with active test calls and VoIP statistic**

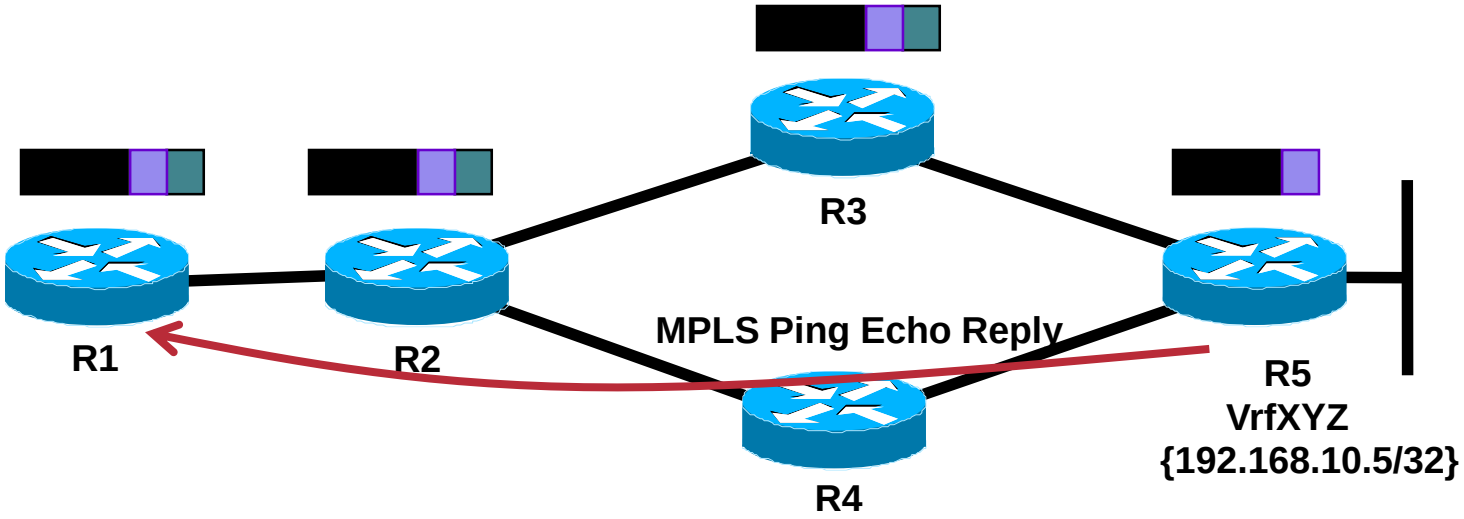
Cisco IOS SAA MPLS Monitoring

Cisco SAA Layer 3 MPLS VPN Operations Today

- VRF Aware monitoring
- L3 MPLS VPN SLA measurement
- PE router, Multi-VRF CE or dedicated SAA router
- Availability
  - Release 12.2(11)T
  - Release 12.0(26)S
  - Release 12.2(20)S

MPLS LSP Ping: Packet Flow For Testing a VPN Address

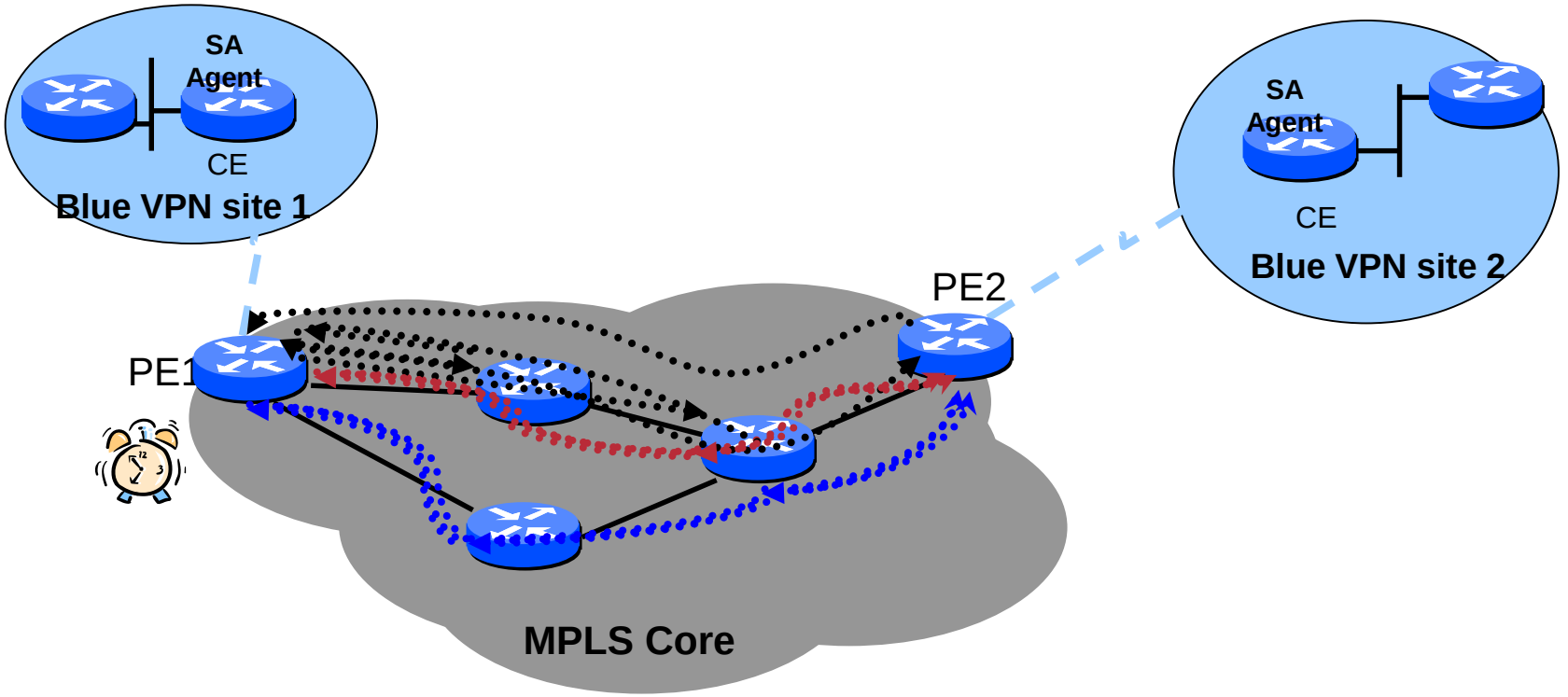
- R1# ping mpls vrf vpnXYZ vpnv4 192.168.10.5/32
- Label Switched at R2, R3
- R3 pops IGP label off
- R5 processes packet, returns reply to R1



Auto Cisco IOS SAA MPLS Layer 3 VPN Embedded Tool

- Automatic connectivity testing of label switch paths
- BGP Discovery automates SAA operation creation
- Proactive monitoring of equal cost traffic paths between the edges
- Troubleshooting and MPLS forwarding problem isolation
- Combined end to end testing for latency and connectivity utilizing LSP ping and MPLS trace route

Putting The Tools Together
SAA with ECMP Tree Trace



- Two Equal Cost paths are available from PE1 to PE2
- ECMP tree trace will discover these paths using a series of echo requests
- An automated LSP ping is setup for each discovered path verifying connectivity and the delivery of all customer traffic between PE1 to PE2

Cisco Auto SAA MPLS Phases

- **Auto SAA MPLS L3 VPN Phase 1 – Release 12.2(Rls6)S**
  - **Support echo and path probes**
  - **Auto-creation of SAA probes based on BGP neighbour discovery**
  - **Use of LSP ping infrastructure for active monitoring**
  - **Timeout, connectivity threshold support**
- **Auto SAA MPLS L3 VPN Phase 2 – Release 12.2(Rls7)S**
  - **Equal Cost Multi-path support (ECMP)**
- **Auto SAA MPLS Phase 3 – Radar**
  - **VCCV and LSP ping PWE connectivity and performance testing**
  - **VRF verify, automatic verification of PE-CE link performance**

Cisco IOS IP SLA Initiative

SLA Challenges

Delivering service levels is an increasingly complex task

Today's SLA's may not guarantee services

- ✓ **Lack of strict SLA metrics means decreased service differentiation and service quality**

No clear understanding of what metrics need monitoring in multi-service networks

- ✓ **Standardized jitter measurement is not established**
- ✓ **Best practices for measurement parameters not established**

  Packet size, packet spacing, measurement frequency…

Cisco IP SLA Functionality

Automate SLA measurements for IP Services, MPLS, VPN, VoIP and Video

Define SLA metrics and methodology

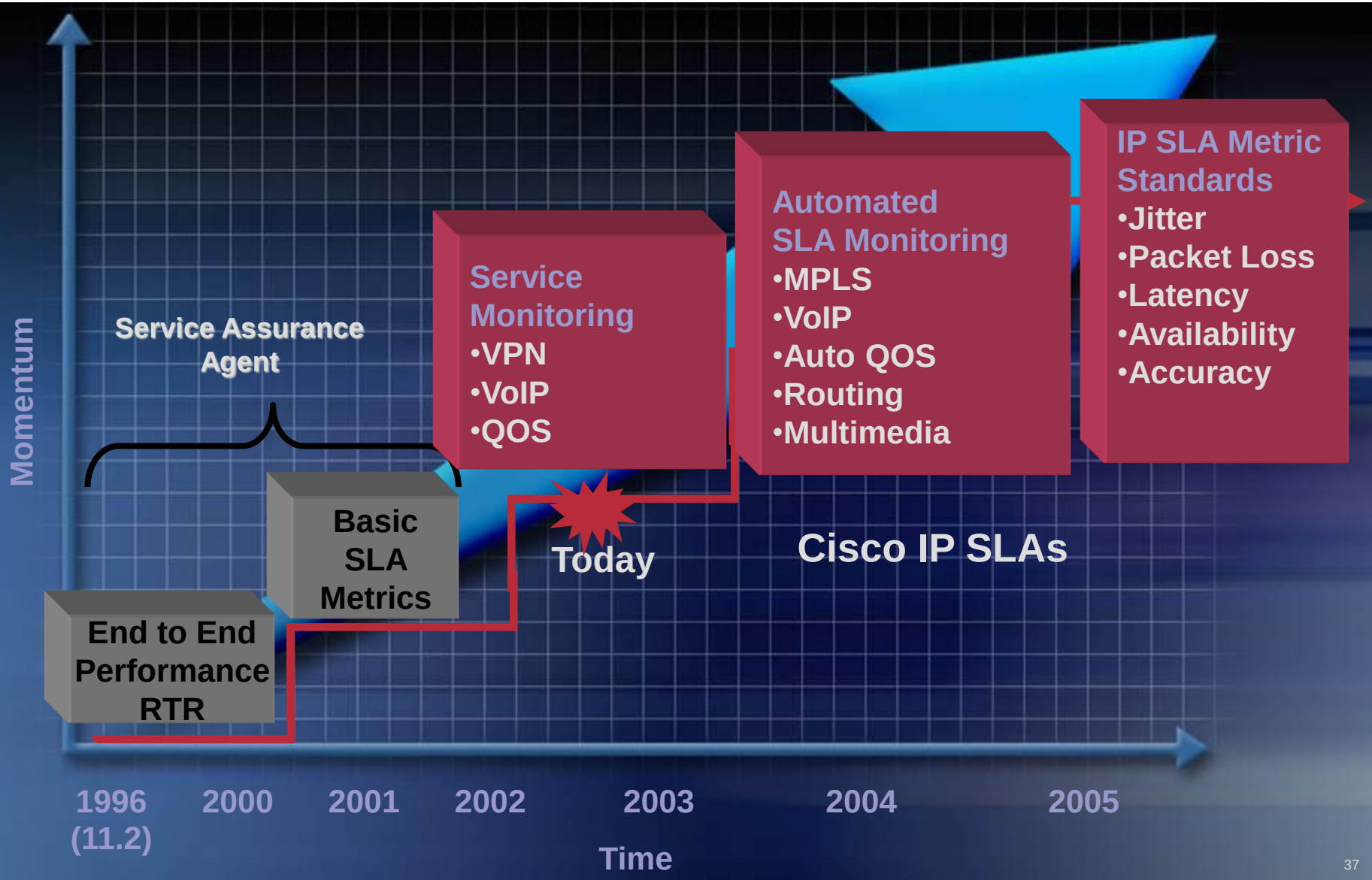
- ✓ Standardized jitter measurement
- ✓ Best practices for measurement parameters
- ✓ Packet size, packet spacing, measurement frequency…
- ✓ NTP designs for unidirectional measurements

Standardize how to measure the SLA metrics

- ✓ New research for SLA metrics including work in IETF

High accuracy and highly granular measurements

IP SLA Building Momentum



References

- **NetFlow**

  www.cisco.com/go/netflow

- **SAA**

  www.cisco.com/go/saa

- **QoS**

  www.cisco.com/go/qos

SAA Performance – CPU Load by platform

(Jitter probe running Phase 1 – 500 active probes – Cisco IOS® 12.2(8)T5 and 12.0S)

Cisco.com

Probes/ second	Probes/ minute	2600	2650XM	3640	3725	7200/225	7500/ RSP8
4	240	8	8	8	1	1	3
8	480	20	7	12	1	1	3
12	720	34	13	21	3	2	3
16	960	46	27	28	4	3	3
20	1200	57	32	35	6	4	3
24	1440	66	39	42	9	5	3
28	1680	77	45	49	16	6	4
32	1920	88	52	56	25	7	6
36	2160	96	59	58	29	10	9
40	2400		65	64	34	15	14
44	2640		71	70	40	21	19
48	2880		77	76	41	23	22
52	3120		82	81	45	27	23
56	3360		96	95	56	31	25
60	3600				57	35	27

Jitter probes are activated sequentially with this testing.

SAA Performance with Phase 2 — CPU Load by Platform

(Jitter Probe Running Infra 2 — 2000 Active Probes — Cisco IOS 12.3(3))

Probes/ Second	Probes/ Minute	2600	2620XM	3640	3725	7200VXR NPE225
4	240	14	7	6	2	4
8	480	20	8	9	3	3
12	720	29	12	13	2	3
16	960	35	15	17	3	3
20	1200	41	19	22	2	3
24	1440	48	24	25	3	3
28	1680	56	27	28	3	3
32	1920	63	28	31	2	4
36	2160	67	31	35	2	3
40	2400		34	38	3	7
44	2640		38	43	4	8
48	2880		42	47	5	8
52	3120		46	49	5	10
56	3360		48	43	6	11
60	3600		52	58	6	11

SAA Memory Usage new versus old infrastructure

Engine 2 reduce the memory usage by a factor 2 to 5.

	Phase1 12.2(8)T5	Phase2 12.2(13)T
UDP Jitter	< 24 KB	< 12KB
UDP Echo	< 19 KB	< 3.5KB
ICMP Echo	< 17 KB	< 3.2 KB