Cisco Service Exchange Framework and Policy Management

March 2006

Agenda

Service Provider Market
and the Service Exchange

Cisco Service Control Engine
Review and update

Service Exchange Framework
Policy Management and services

SP Business Model Dilemma

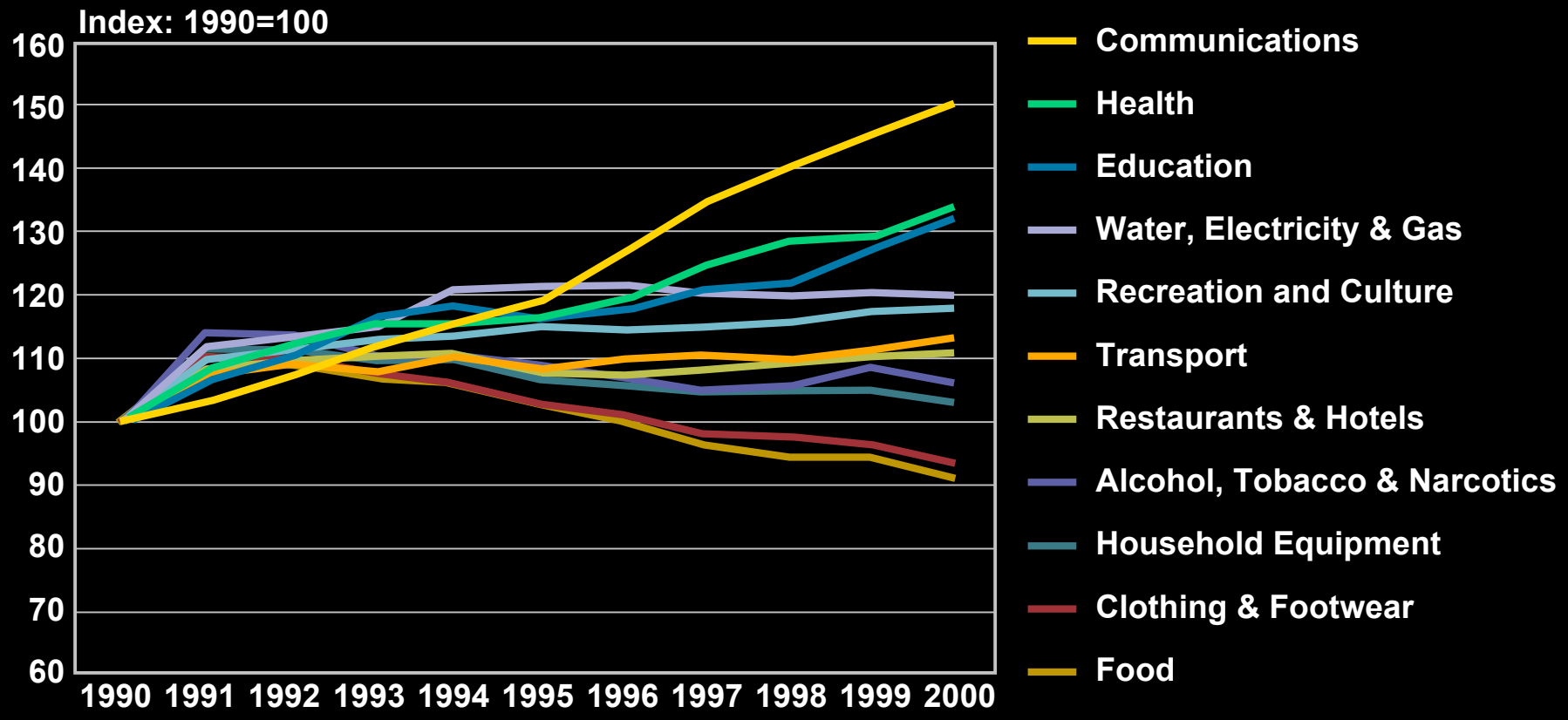
Source: Gartner 2003

Service Providers are Turning to New Service Platforms for Business Growth

Market is Primed…

Consumers are Spending Heavily on Communications

Evolution of Household Spending in OECD Countries, 1990–2000



Source: OECD 2003

…And are Willing to Pay More for Valued Services

Security
Simplicity
Integration
Personalization
Control

Speed	Voice	Wired
Reliability	Data	Wireless
Low Cost	Video	

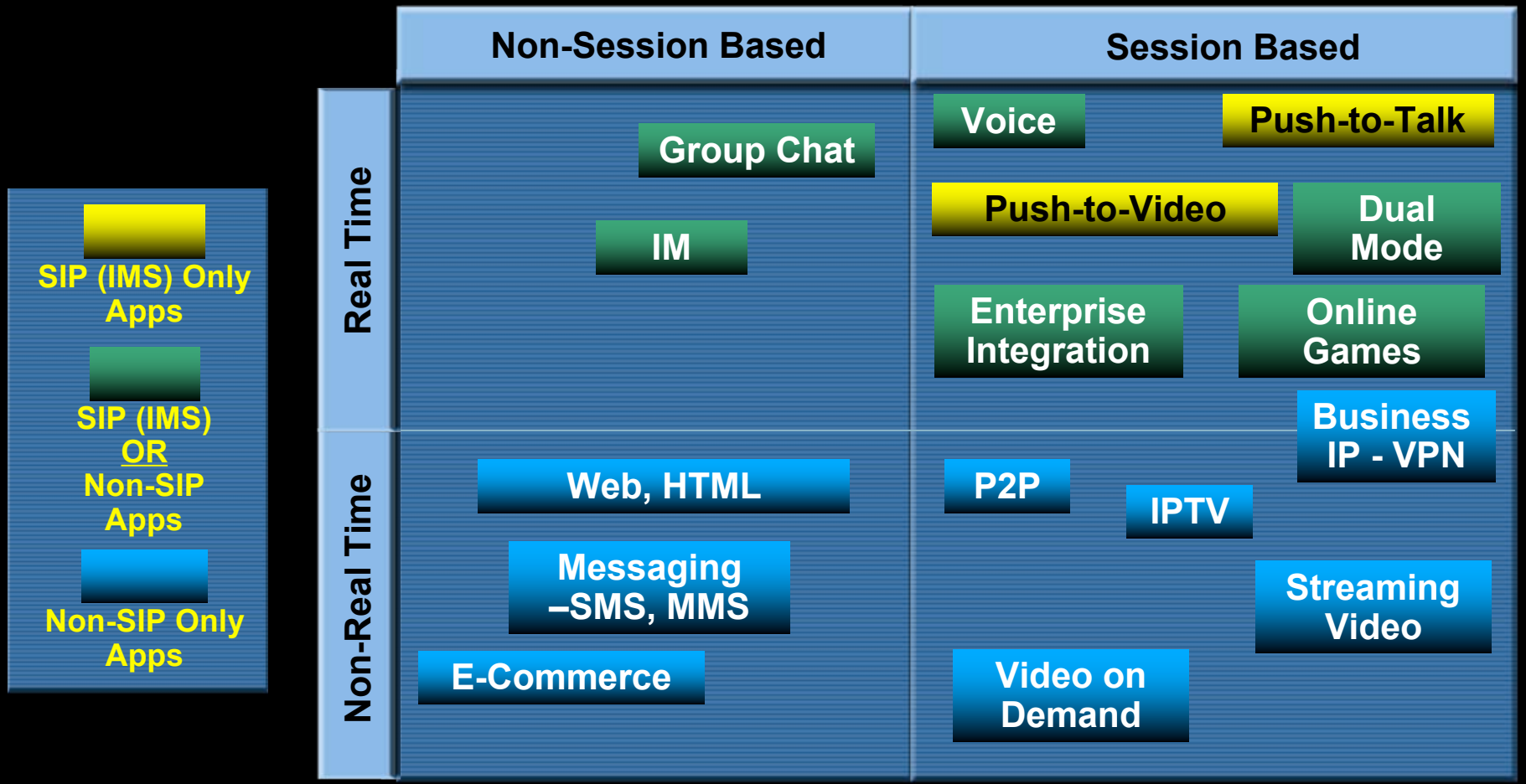
Innovation

Share households spent on communications rose by 50% in developed countries over the past decade

More Than Just Revenue
Other Tangible Benefits Can Be Measured

Market Share	Competitive Position	Customer Retention	Advancing Up the Value Chain with the Customer
Services crossing over into other segments traditional areas	Deploying services as defensive move versus competitors	More services per customer reduces churn	Deploying unique services fends against commoditization or being relegated to 'only transport' for application providers

Today's Universe of Applications
Requires Support for SIP and Non-SIP Applications



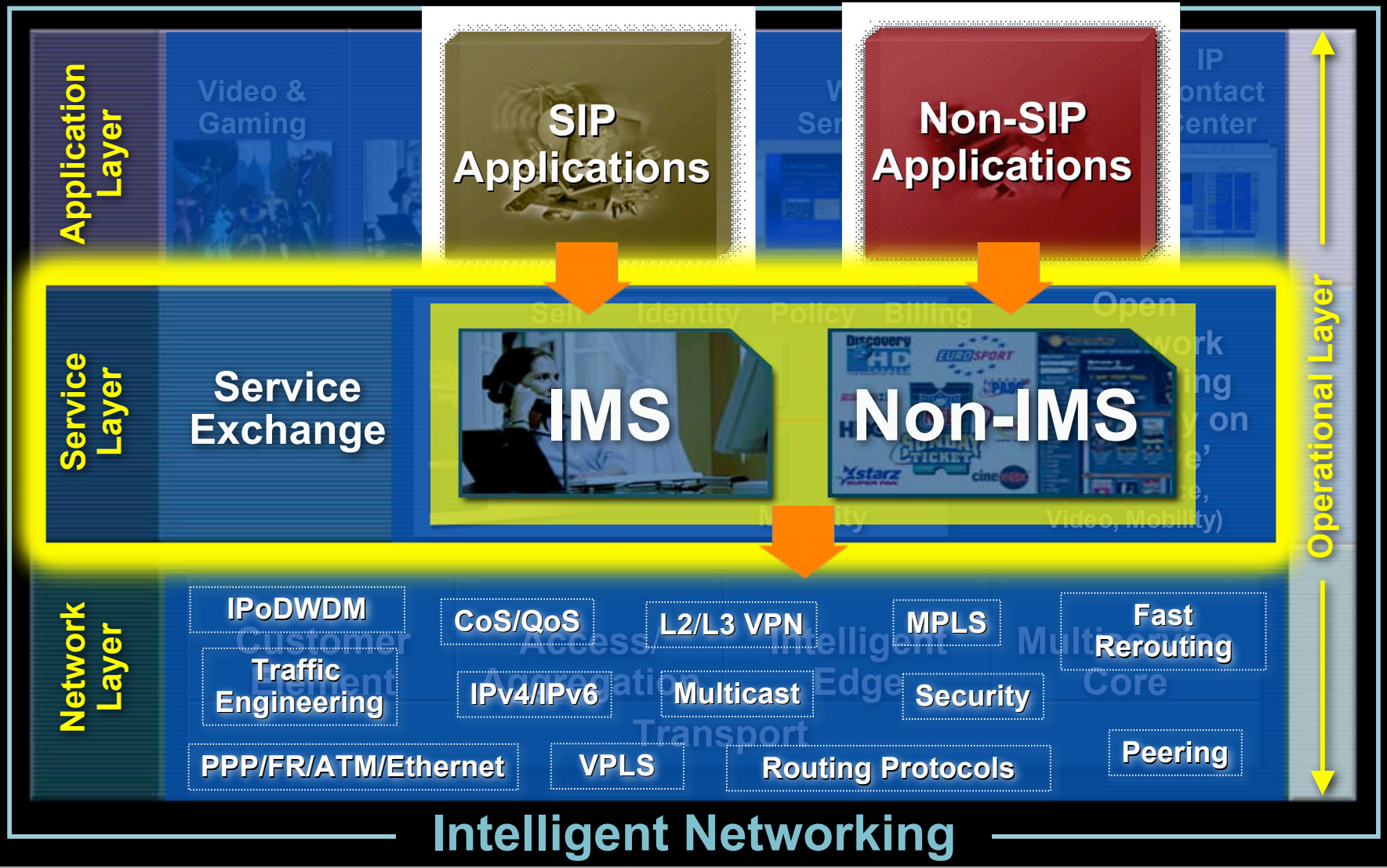
What is IP Multimedia Subsystem (IMS)?

A standards-based effort developed as a means for voice-centric mobile operators to more efficiently deploy and handle SIP services

- Layered architecture—separates transport, control and application functions
- Access-agnostic—initially defined for mobile carriers, but allows convergence of fixed and mobile networks and applications
- Real-time IP applications—Enhances and "blends" SIP-based services

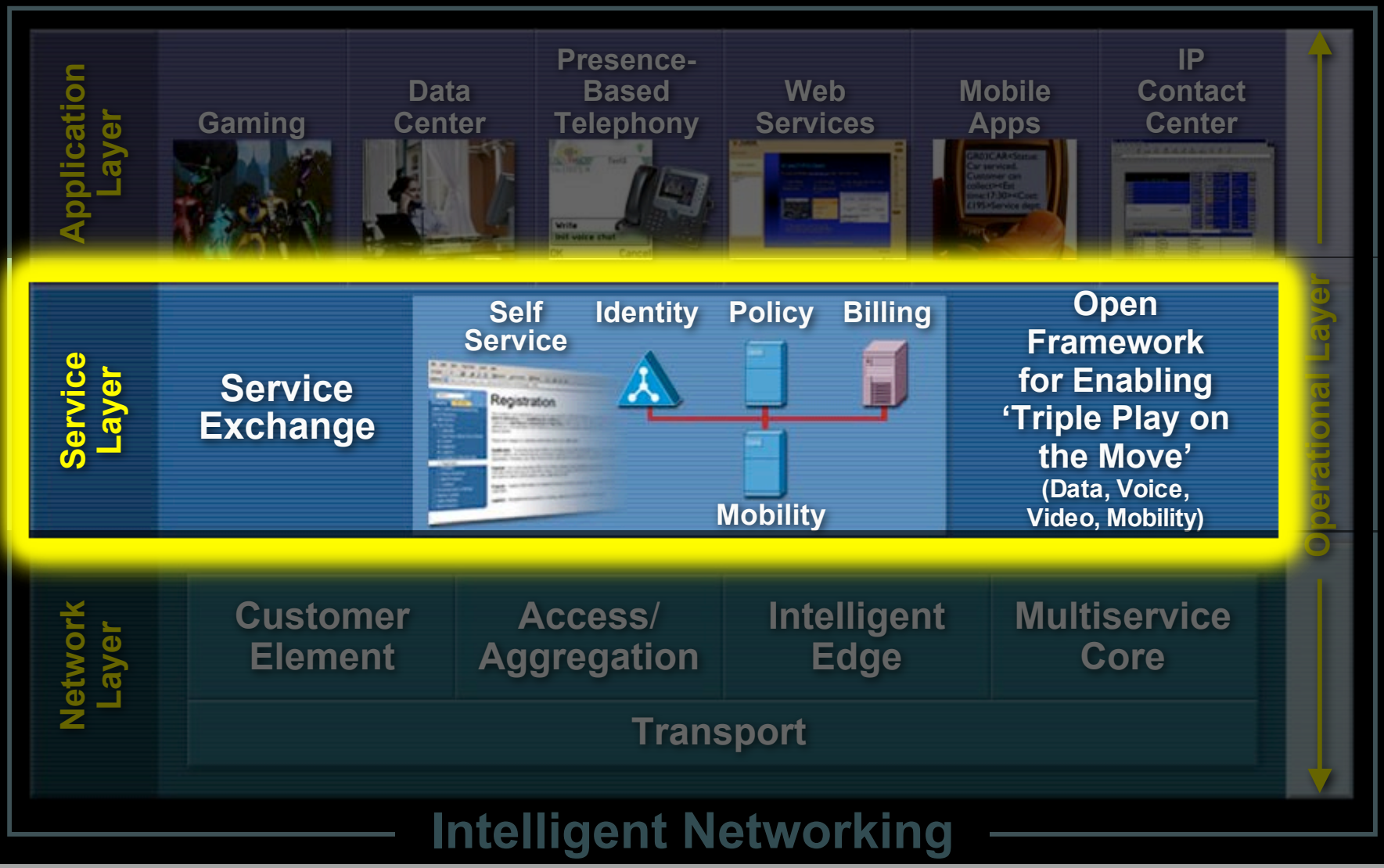
Service Exchange Framework

Comprehensive Support for BOTH IMS and Non-SIP Apps



Cisco IP NGN Architecture

Achieving a Whole Greater Than the Sum of the Parts



Service Exchange Framework
Enabling Personalized Rich Media Services

Who?

- Who is the user?
  - Devices
  - Profile
  - Location
  - Presence

How?

- How can I dynamically control resources?
  - Interwork & provide rich media control
  - Monitor & charge on a per service / per user basis
  - Enable application awareness

What?

- What can the user do?
  - Within what timeframe
  - To what extent
  - Under what rules

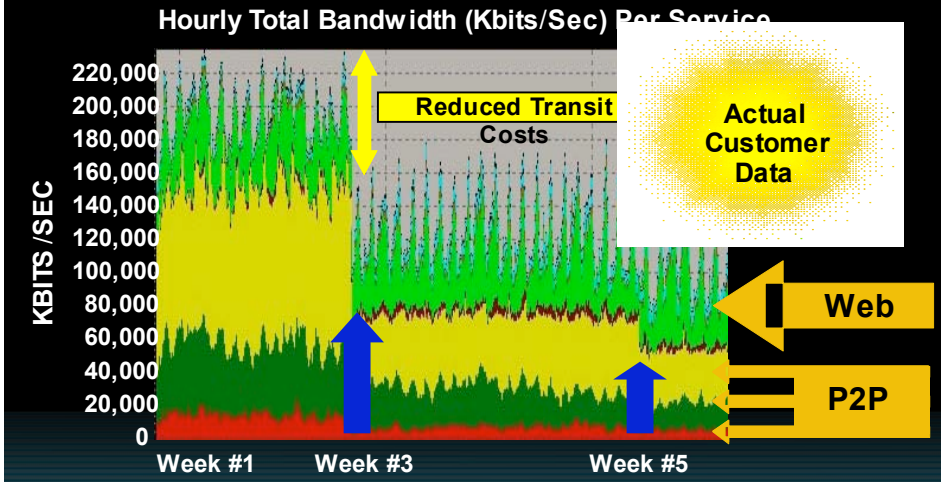
Where?

- Where can the user roam?
  - Track/recognize user devices across carriers
  - Maintain user sessions across multiple networks
  - Offer all services in all locations

Cisco Service Exchange Framework
Case Studies

Greater Efficiencies

Service Prioritization via Deep Packet Inspection



Efficient Management of Video Oversubscription

Managing P2P Applications

- Enable new business models between content and service providers
  - Detect and manage affiliated applications and align QoS
  - Co-branding and fee sharing

Video Call Admission Control

- Preserves quality of experience
- Provides network-based graceful busy signal when demand exceeds capacity
- In trials at major MSO, critical for IPTV

Cisco Service Exchange Framework
Case Studies

Better Control

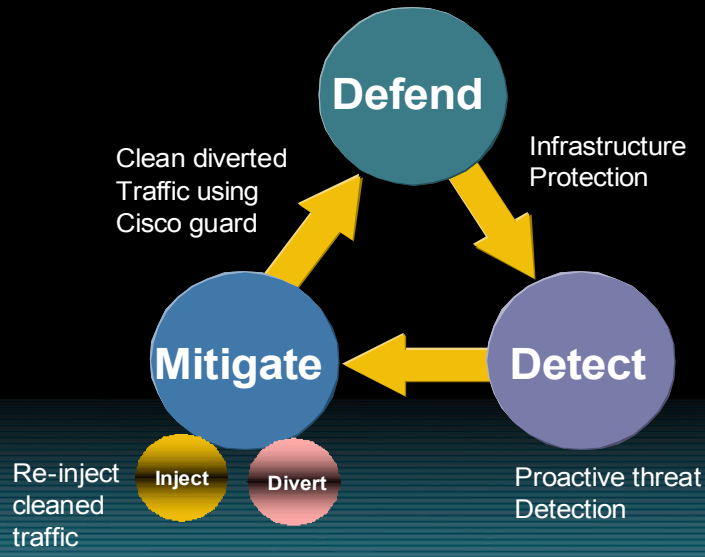
Implement Fair Use Policy

- Eliminates bandwidth bottlenecks
- Enhanced user experience

Usage	less than 2.8 GB	less then 4.2 GB	less then 5.6 GB	over 5.6 GB
e-mail + WWW	No Limit	No Limit	256 kbps	256 kbps
audio /video streaming	No Limit	128 kbps	65 kbps	48 kbps
P2P	48 kbps	28 kbps	28 kbps	16 kbps

User quota based on 7-day timeframe

Enhanced Security- DDoS Protection



Enhanced Security Services

- DDoS service provider infrastructure protection
- Peering edge DDoS protection
- Managed service models

Sprint

AT&T

COLT

Typical Tiered Service Model Pricing Example

Adding Value to Differentiate Services

Better Control

	MEMBER SERVICE	FAMILY SERVICE	BUSINESS SERVICE
	• One IP Address • 2MB Down • 512K Uplink	• One IP Address • 4MB Down • 512K Uplink	• Three IP Addresses • 6MB Down • 1MB Uplink
NEW	• Email • Basic Internet • P2P Marked	• Email / Video • Full Internet • 100 TCP Sessions • P2P Traffic Marking • Child-safe Internet • Pop-up Blocker	• Email / Video / Voice • Wireless Internet • No TCP Limits • P2P Traffic • Firewall • IPSEC VPN Speed Up
	• 500 Minutes paid	• Unlimited	• Unlimited
	$29.95	$39.95	$69.95

Enhanced VoBB Service Examples

Improving the Quality and Control of the User Experience

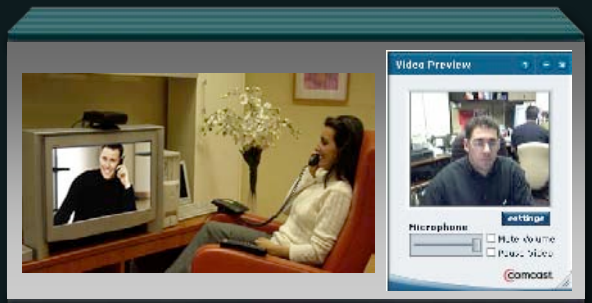
Better Control

Managed Video Applications

Broadcast Television

Video on Demand
TV on Demand / nPVR

Video Communications Services



Video Phone /
Video Conferencing

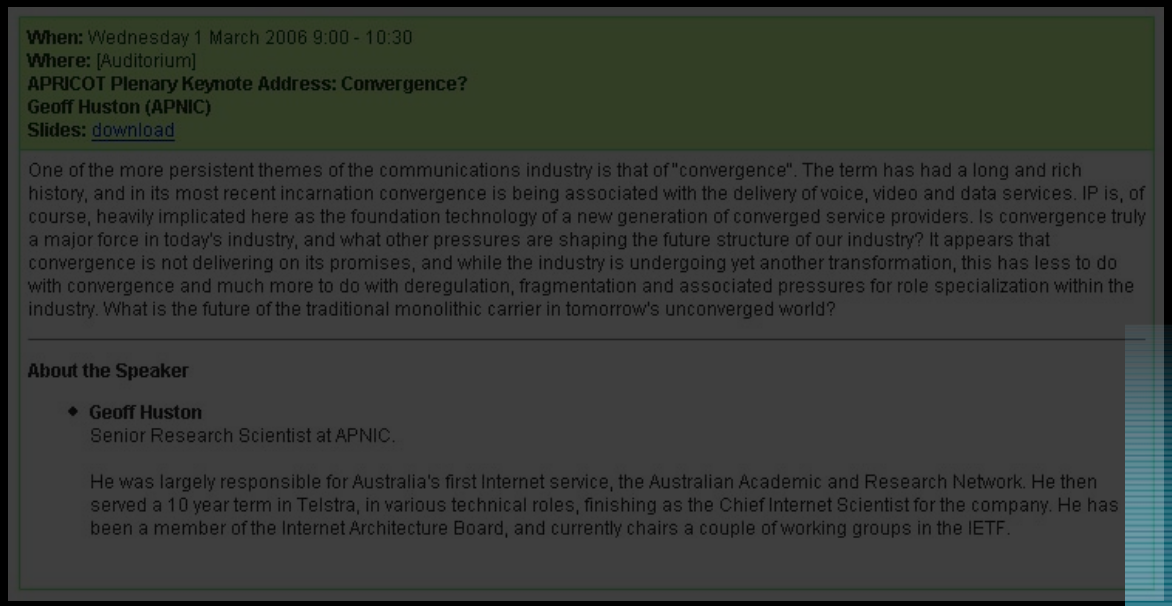
Gaming / Interactive TV

"Over the Top" Video

Video Streaming

Video to Other Devices

Apricot 2006 (http://www.apricot.net/)



When: Wednesday 1 March 2006 9:00 - 10:30
Where: [Auditorium]
APRICOT Plenary Keynote Address: Convergence?
Geoff Huston (APNIC)
Slides: download

One of the more persistent themes of the communications industry is that of "convergence". The term has had a long and rich history, and in its most recent incarnation convergence is being associated with the delivery of voice, video and data services. IP is, of course, heavily implicated here as the foundation technology of a new generation of converged service providers. Is convergence truly a major force in today's industry, and what other pressures are shaping the future structure of our industry? It appears that convergence is not delivering on its promises, and while the industry is undergoing yet another transformation, this has less to do with convergence and much more to do with deregulation, fragmentation and associated pressures for role specialization within the industry. What is the future of the traditional monolithic carrier in tomorrow's unconverged world?

About the Speaker

- **Geoff Huston**
  Senior Research Scientist at APNIC.

  He was largely responsible for Australia's first Internet service, the Australian Academic and Research Network. He then served a 10 year term in Telstra, in various technical roles, finishing as the Chief Internet Scientist for the company. He has been a member of the Internet Architecture Board, and currently chairs a couple of working groups in the IETF.

- Geoff talk at latest Apricot meeting in Perth.
- Can large incumbent implement a converged NGN network?
- Are they able to innovate?
- Unfortunately, SP EMEA perspective is missing from this presetnation...
- Also listen to Geoff speach at NANOG: http://www.nanog.org/mtg-0510/huston.futures.html

Apricot 2006 (http://www.apricot.net/)

When: Thursday 2 March 2006 9:00-10:30
Where: [Ballroom 1]
Session: Routing/Operations: Service Control Technologies for peer-to-peer traffic in next generation networks
Speakers: Teruyuki Hasegawa (KDDI R&D Labs) & Lior Gendel (Cisco)
Slides: download, download2

"Service Control Technologies Peer-to-peer traffic in next generation networks", Lior Gendel, Oren Raboy, Mallik Tatipamula, Cisco systems; Atsushi Tagami, Teruyuki Hasegawa, Shigehiro Ano, Toru Hasegawa, KDDI labs.

Peer-to-peer (P2P) traffic consumes network resources without creating additional revenue. It is allegedly estimated that 70 percent or more of broadband bandwidth is consumed by downloads of music, games, video, and other content. Consumption will increase as P2P downloads multiply because of increases in subscriber adoption and file sizes.

Identifying P2P applications is complex. Sophisticated P2P protocols can dynamically hop to different ports, making them difficult to detect, monitor, and control. Many existing devices and unsophisticated service control technologies lack the ability to detect changing P2P protocols, hampering a service provider's ability to cope with P2P application traffic.

This paper discusses the problems associated with the growing popularity of P2P applications and presents two kinds of service control technologies. First one is deep packet inspection, which enables accounting and controlling traffic with application awareness to attain the bandwidth fairness among subscribers. This approach is effective but needs some consideration about the deepness of inspection not to infringe the privacy of communications. Second one is P2P cache inducing P2P traffic to local destinations, which can mitigate inter-domain traffic. This caching architecture is P2P protocol independent but provides only rough traffic control. We also address the possibility of harmonized service control architecture for next generation network infrastructure.

About the Speakers

- **Teruyuki Hasegawa**
  KDDI R&D Labs

  Teruyuki Hasegawa received the B.E. and M.E. Degrees of electrical engineering from Kyoto University, Japan, in 1991 and 1993, respectively. Since joining KDD (now KDDI) in 1993, he has been working in the field of high speed communication protocol and multicast system.

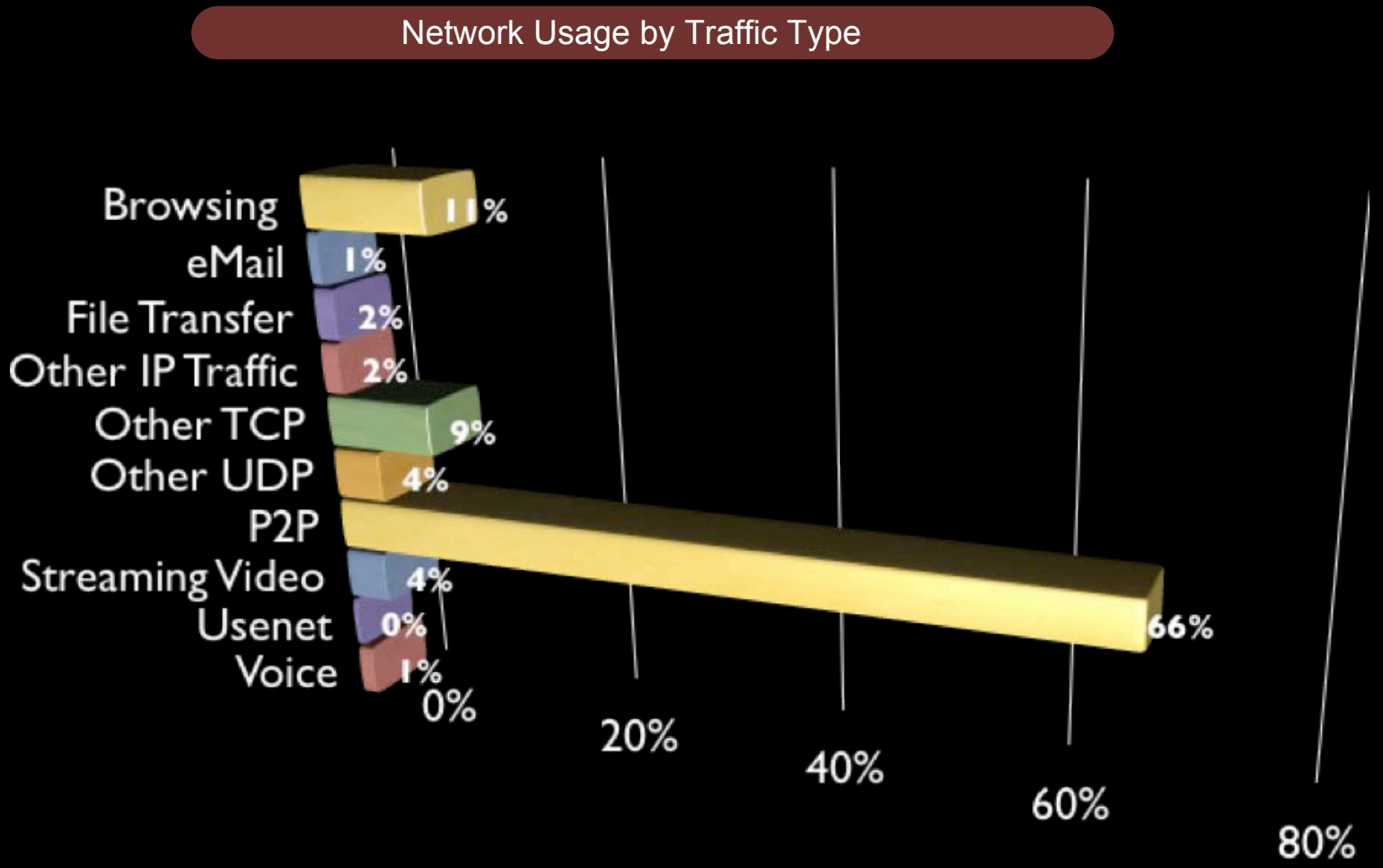
  He is currently a senior research engineer of IP Communication Quality Lab. in KDDI R&D Laboratories Inc. He received The Meritorious Award on Radio of ARIB in 2003.

- **Lior Gendel**
  Cisco

  LIOR GENDEL is Managing Technical Marketing team in Cisco Systems. Prior to joining Cisco he designed and implemented public IP networks. After joining Cisco in 1996 he participated in the design of many private and public IP networks, in particular in Europe. His latest activity in Cisco includes a study of applications response over large IP networks and architecture of Cisco NG products. He holds a B.Sc. in computer engineering, B.A. computer science and an M.Sc. in computer science from Ben-Gurion University, Israel.

- **Service Control talk at Apricot 2006 meeting in Perth.**
- **Exponential increase in peering bandwidth and transit costs.**
- **Need for P2P optimization.**

Traffic Distribution Patterns

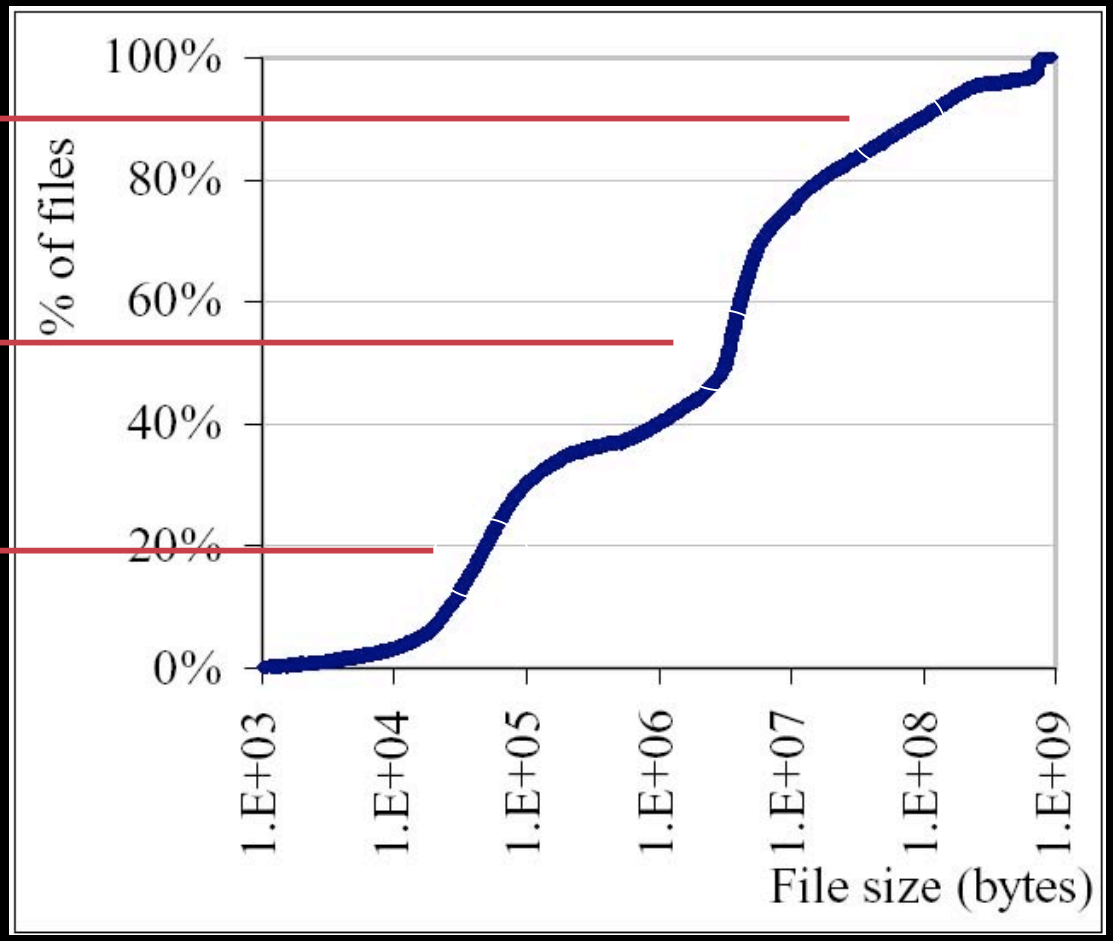


What Do We Download?

Movies

Songs

Images



Source: Leibowitz, N., Ripeanu, M., Wierzbicki, A.
"Desconstructing the KaZaA network"

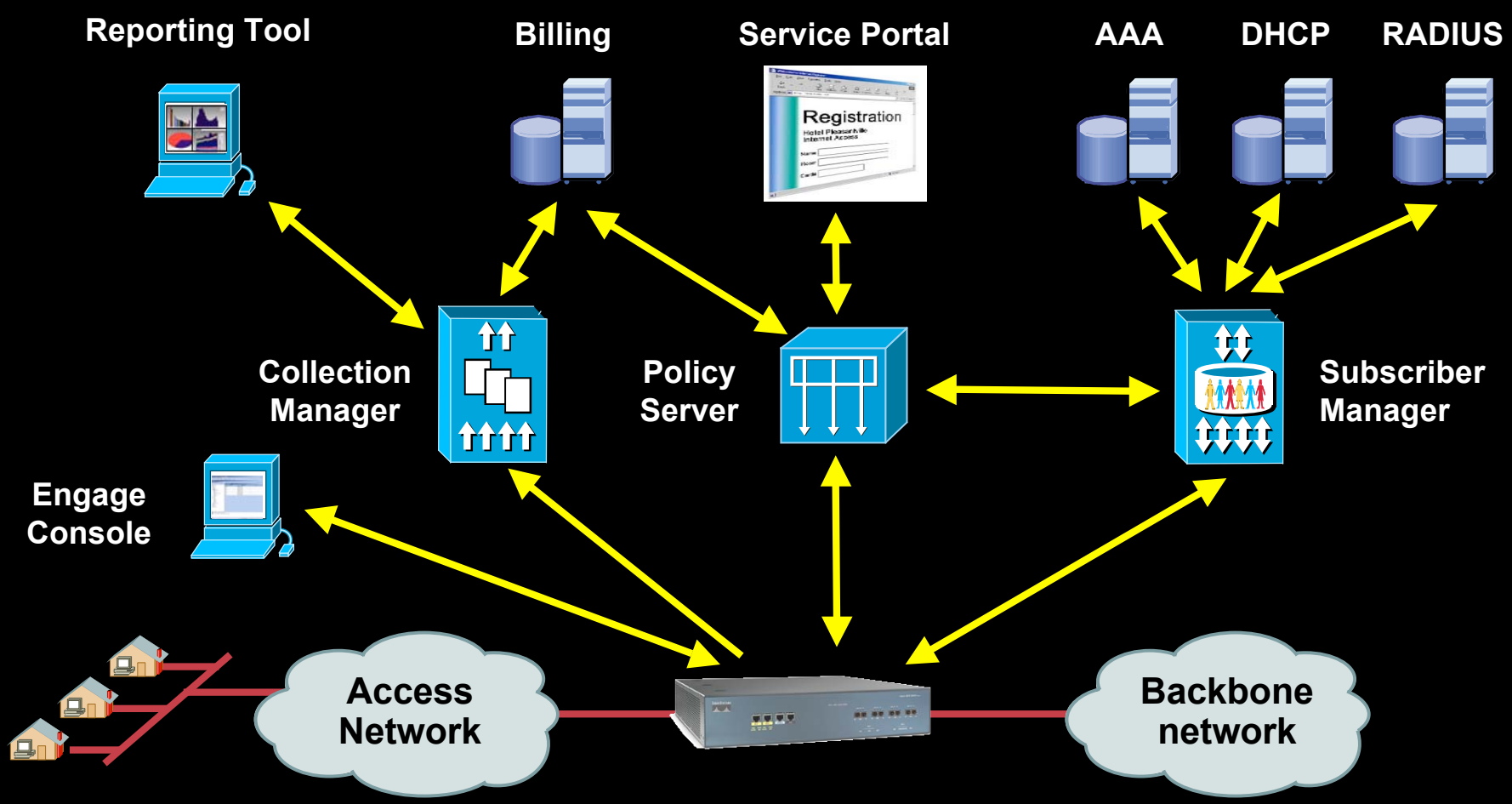
Agenda

Service Provider Market
and the Service Exchange

Cisco Service Control Engine
Review and update

Service Exchange Framework
Policy Management and services

Service Control – Solution Components

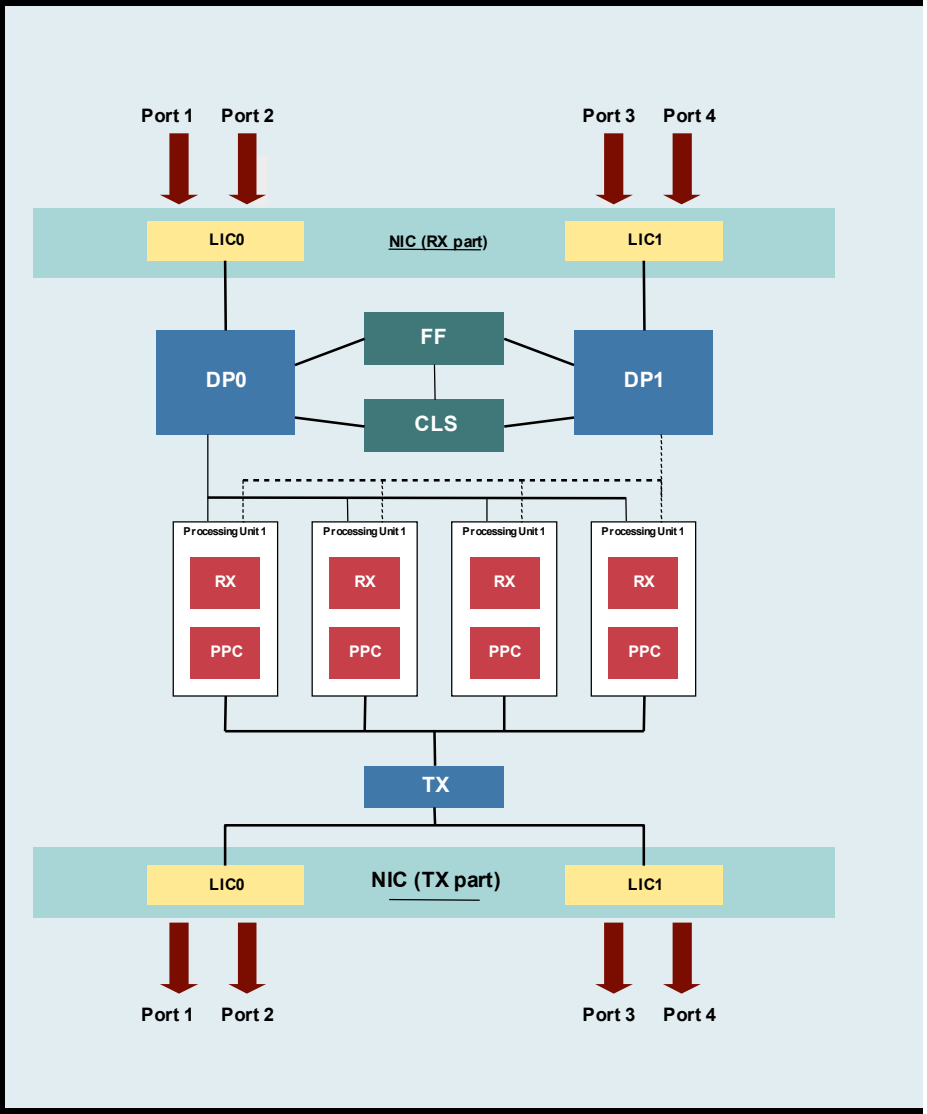


SCE 1000 and SCE 2000

	SCE1010	SCE2020-4GBE	SCE2020-4/8FE
Interfaces	2 x GE • SX (850 nm) • LX (1310 nm)	4 x GE • SX (850 nm) • LX (1310 nm)	8 x FE RJ-45
Management	2 x Eth 10/100 RJ-45	2 x 10/100/1000 RJ-45	2 x 10/100/1000 RJ-45
Max throughput	2 Gbps	4 Gbps	4 Gbps
Max # subscribers	40,000	100,000	100,000
Max flows (unidir)	2,000,000	2,000,000	2,000,000

Key Advantage – Hardware Accelerated Platform

- Hardware only processing of most traffic (80%)
- Flexibility through CPUs and intelligent interaction with hardware
- Load balanced CPUs with zero processor wait-states
- *Fast-path* for delay sensitive (e.g. voice) traffic. Average delay of less than 30micro-seconds
- 4Gbps of processing
- No sampling; full processing of every packet
- Programmable inspection and policies
- Performance not dependant on policy complexity



Reliability

Component Reliability	• Redundant Power Supplies and fans • Field replaceable PSU / FAN • AC / DC power dual-feeds • Redundant management port • No HD • MTBF 80,890
System redundancy	• Electrical / Optical bypass • 1+1 Cascade redundancy • N+1 Cluster redundancy
Traffic filtering	• L3/4 traffic filter (isolate traffic)

Key Advantage: Programmability

- Flexible, bi-directional multi packet signatures
- Programmable device core
- Dedicated team of experts focused on service-provider requirements

Examples:

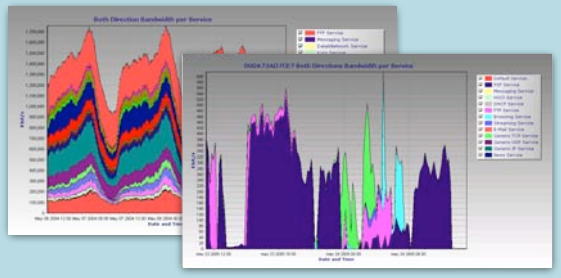
Protocol: Winny (popular Japanese P2P application)

- Development time: 3 weeks
- Signature update after application 'morphed': 1 day

Protocol: Skype (P2P VoIP Application)

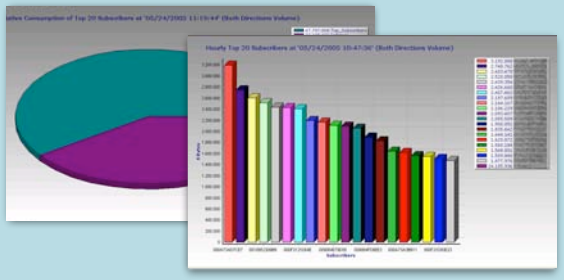
- First signature release: 1 week
- Final signature: 4 weeks

Network Analysis and Subscriber Intelligence



Bandwidth/Capacity Reports

- What is eating up my network resources?
- When do I need a capacity upgrade?
- What is causing congestion?



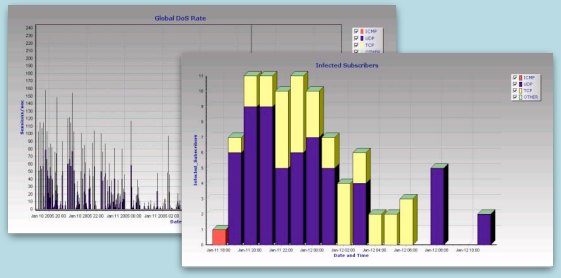
Subscriber Demographic Reports

- What percentage is using P2P/gaming application?
- What are the usage patterns of different subscriber groups?
- What is the cost-impact of my top subscribers?

Server Activity

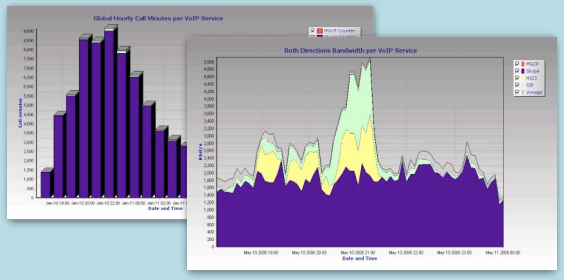
- What are the popular web-hosts used?
- What are the popular streaming sites?

Network Analysis and Subscriber Intelligence



Security Reports

- Which subscribers are infected and attacking others?
- Which subscribers are spamming?
- Which subscriber is attacking network resources?



Voice Reports

- Quality of experience of VoIP calls
- Minutes spent on VoIP services
- Total and concurrent calls per VoIP service
- Compare managed vs. non-facility service

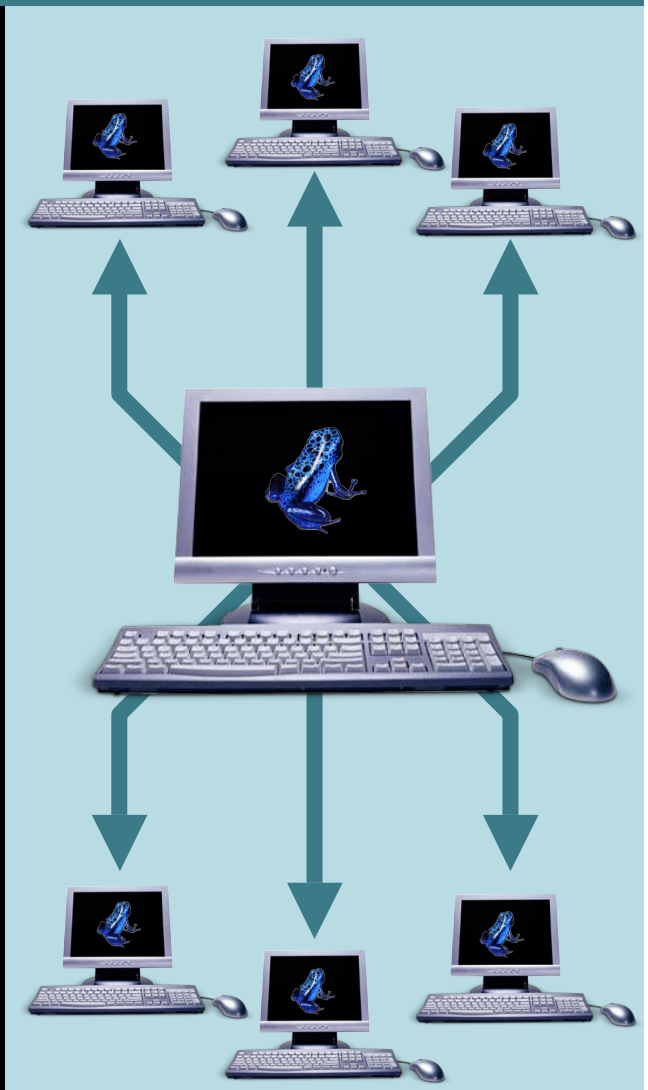
Robust Collection Environment

- Efficient and reliable usage export protocol
- Stand alone of integrated into upstream management or billing systems
- Scaleable collection software
- Powerful and easy to use, template-driven reporting tool

Intelligent Flow Management: BitTorrent Dormant Flows

- **BitTorrent multiple connections**
  - Single client creates 100's of concurrent flows
  - Flow are frequently revisited but not always used
  - BitTorrent signature only available on first client contact (flow start)
  - Order of magnitude more than other P2P applications
- **DPI dilemma: How to manage flows?**
  - Slow aging: Exhaust DPI engine flow-table (1,000 active BT clients can consume hundred of thousand flows)
  - Quick aging: Loose classification accuracy of most popular P2P application
- **A choice between two "bad options"?**

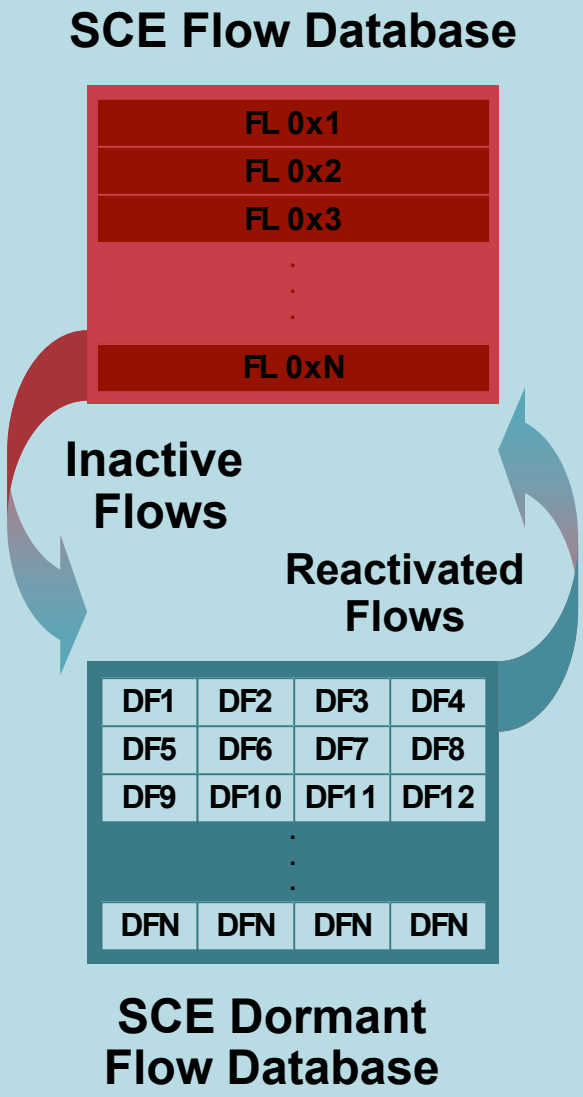
Available as part of 2.5.6 and 3.0



Intelligent Flow Management—BitTorrent Dormant Flows

- Cisco SCE Solution: Dormant Flow Repository
- Main flow database holds active flows
- Compressed dormant flows db used to age inactive flows
  - Dormant DB holds flow classification history
  - Flow reactivated when more packets are seen
  - Allows for quick aging without loss of classification information
- Result:
  - Flow efficiency of quick aging
  - Classification accuracy of slow aging

Available as part of 2.5.6 and 3.0



Intelligent Flow Management: BitTorrent Dormant Flows

- Dormant flow database supports 1M dormant flows in addition to main flow database (1M flows)
- Unique Cisco solution and infrastructure
  - Useful for other aggressive applications
- BitTorrent popularity necessitates approach to maintain effectiveness of P2P solution
  - Other solutions forced to loose accuracy or cannot scale

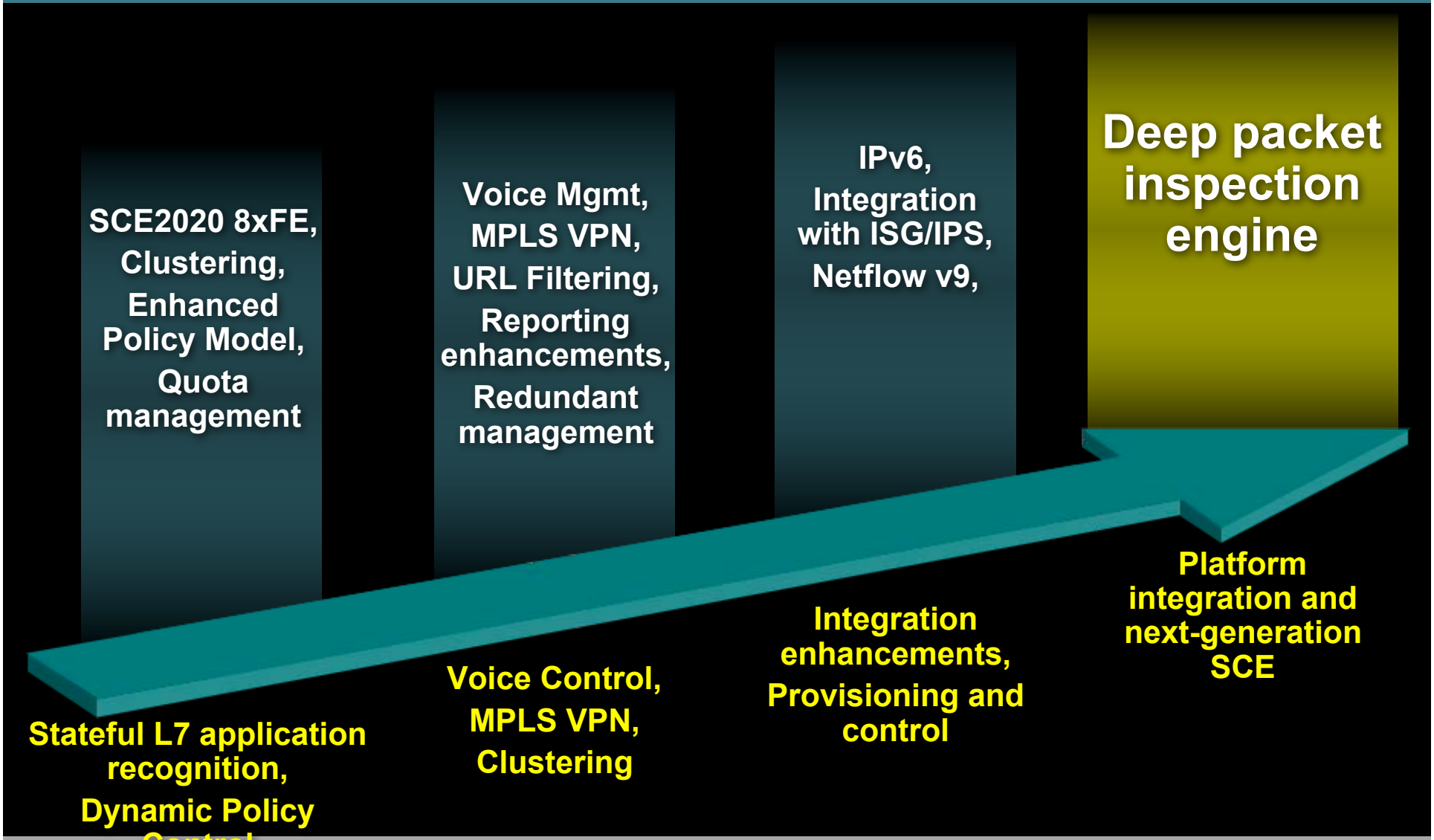
Available as part of 2.5.6 and 3.0

	DF Disabled 60min BT Aging	DF Disabled 5min BT Aging	DF Enabled
Avg. Active Flows	640,000	240,000	240,000
BT Classified Traffic	45%	29% (15% Misclassified as "Generic")	47%

* Based on Production Network Data

Conclusion:
40% Resource Saving with No Sacrifices to Classification

Solution Strategy and Evolution

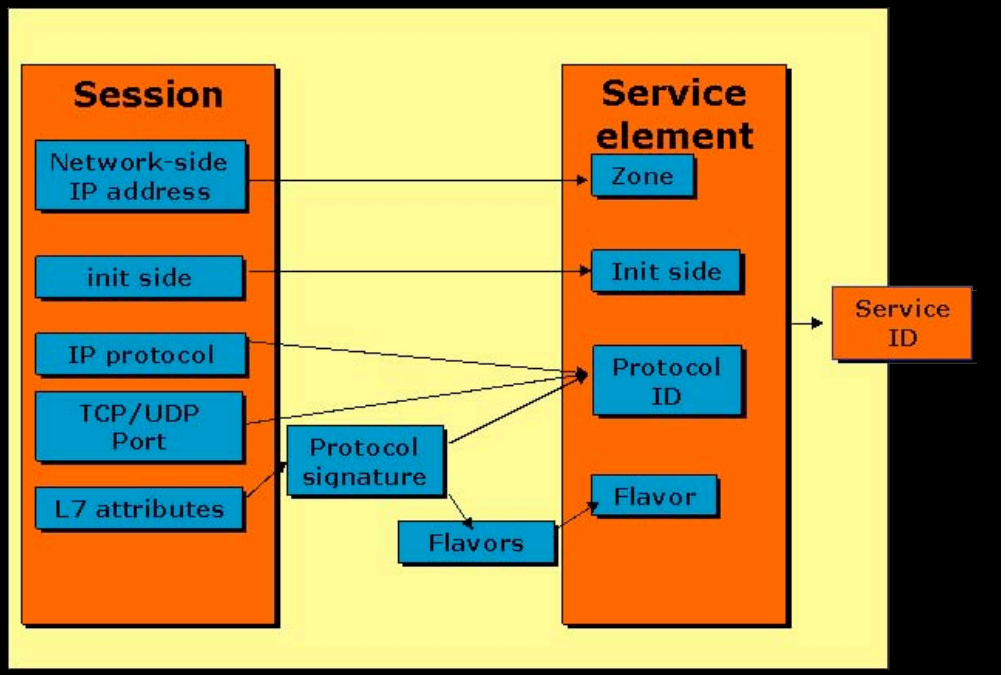


New and Enhanced Classification model

- Structured, rich and flexible classification process

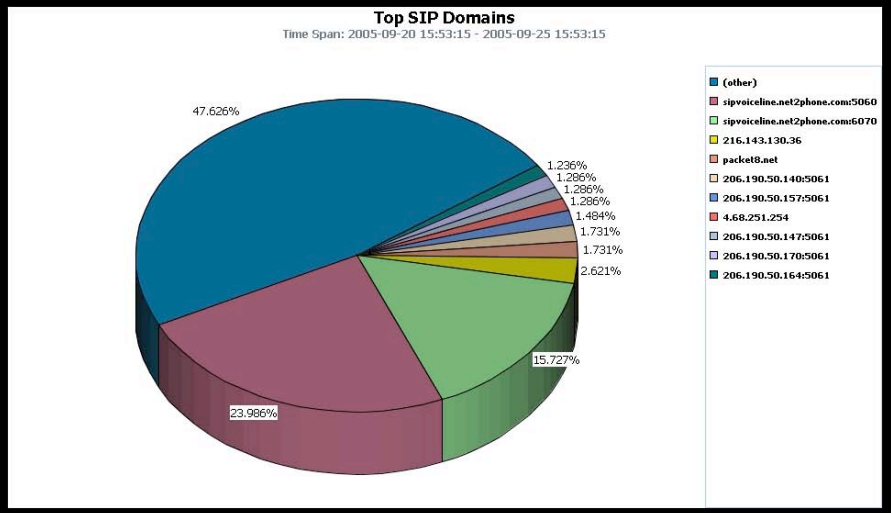
  Protocol Signature, ports, zones and flavors → all used for determining a service

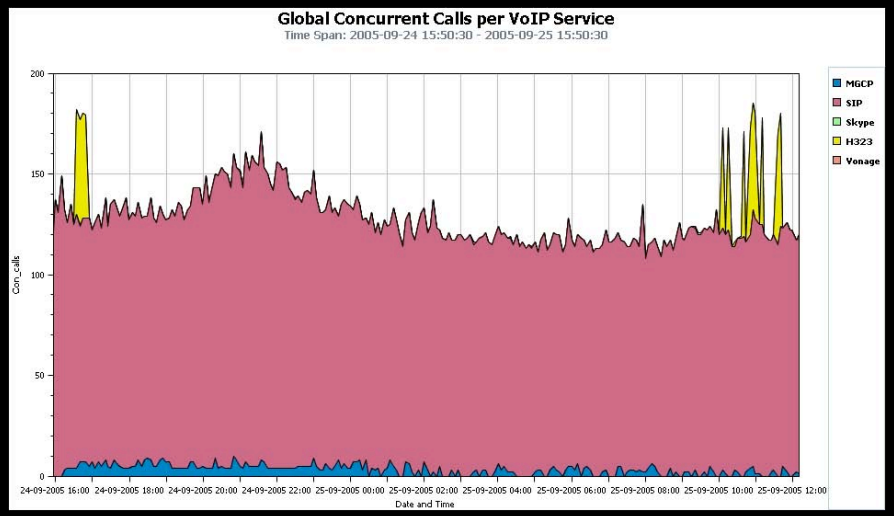
- Protocol signature lookup on all traffic (not restricted by port)



VoIP Functionality

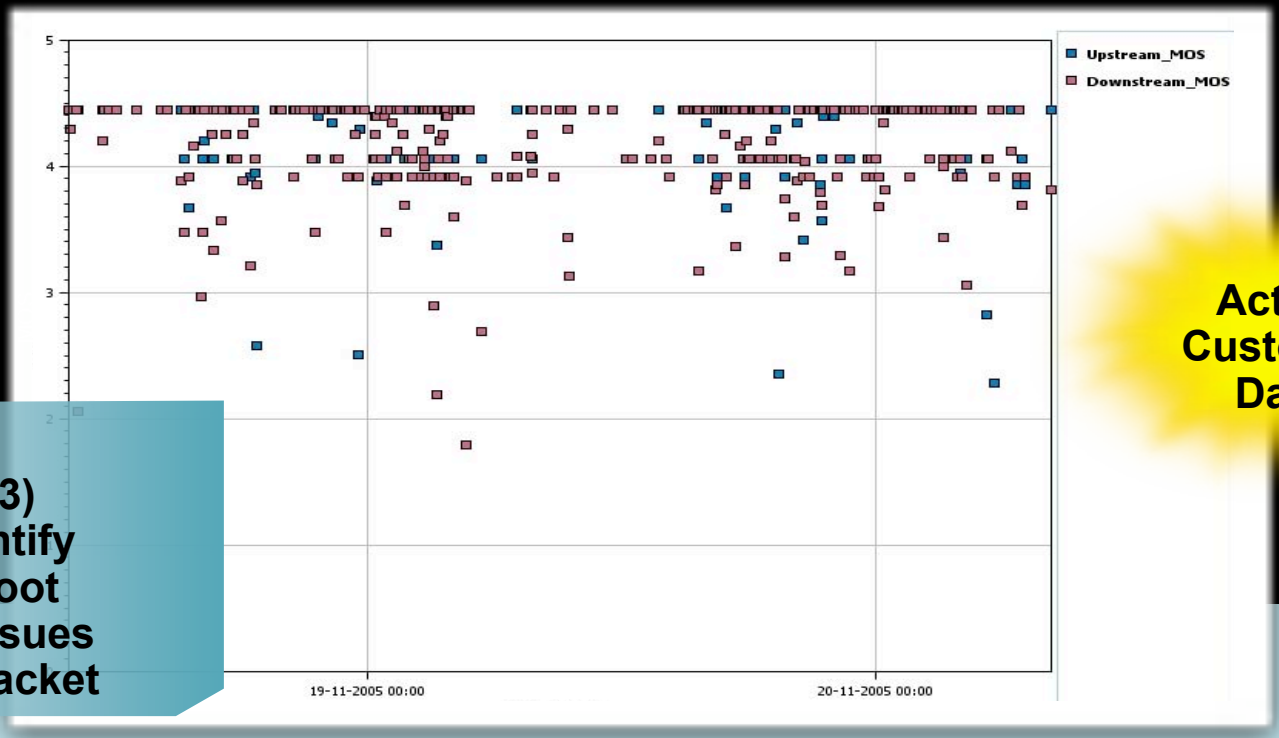
- Continuing the momentum from 2.5.5
  - Enhanced protocol support
  - Support for Transaction Usage RDRs for MGCP and SIP sessions using the same SCA BB VoIP RDR template used for the H.323 protocol.
  - SIP domain based classification





Reporting—Global VoIP MOS

Highlight:
VoIP Service Is Operating Well... Most Hours of the Day



Actual Customer Data

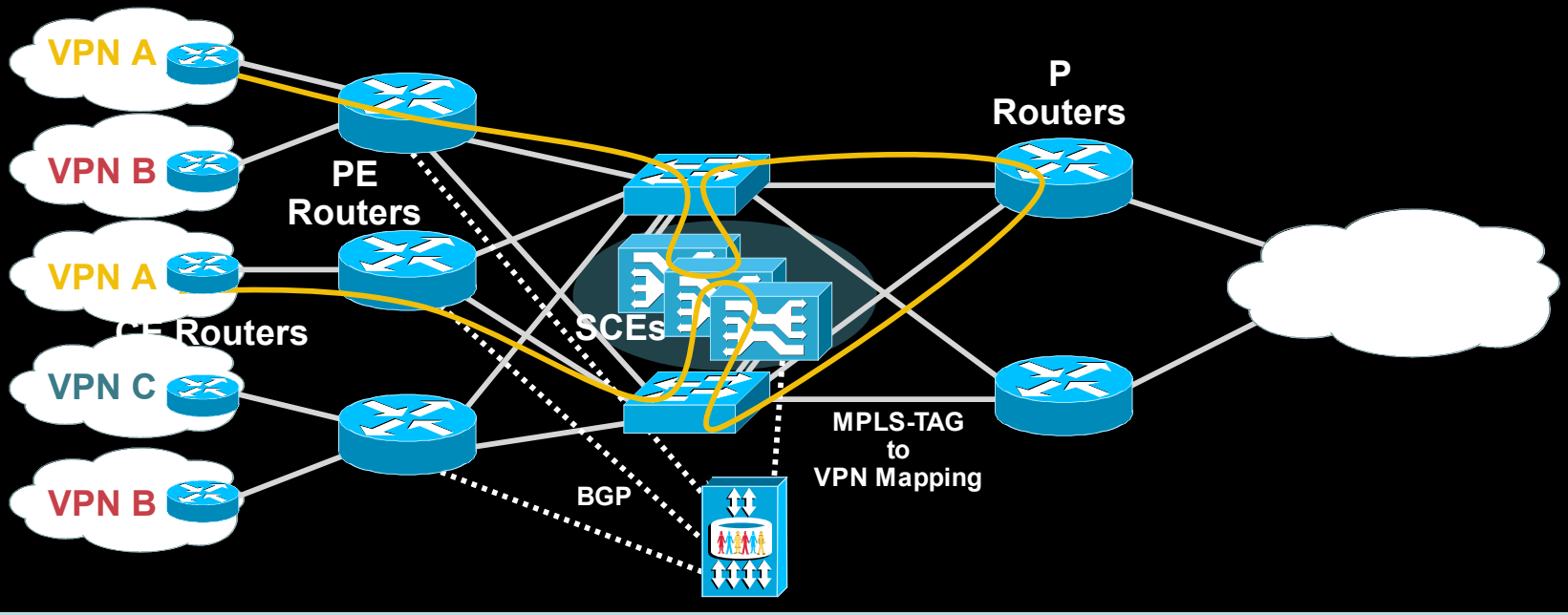
New!
(Available: 3.0.3) Reports to identify and Troubleshoot VoIP Quality Issues (MOS, Jitter, Packet Loss)

Global VoIP MOS

Time Span: 1998-03-03 09:50:43—2005-11-28 15:50:43

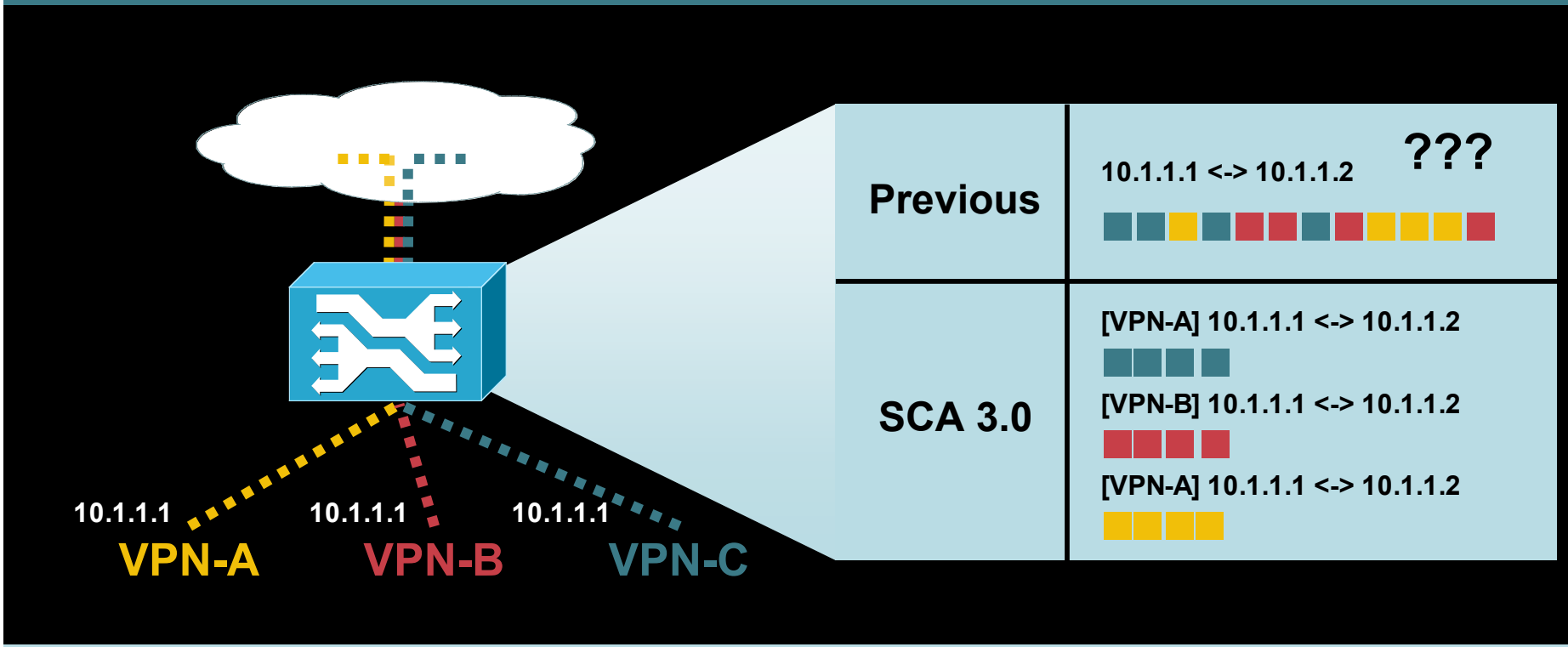
MPLS-VPN—Per VRF DPI

Example Network—Managed Corporate VPNs



- SCA BB 3.0 supports insertion into MPLS-VPN with overlapping private IP address spaces
- Each VPN (A, B,C) managed separately—VPN as a “subscriber”
- MPLS-VPN packet tags automatically extracted from PE BGP
- Flow concept is extended to contain MPLS tag—ensures consistency of packet to flow mapping

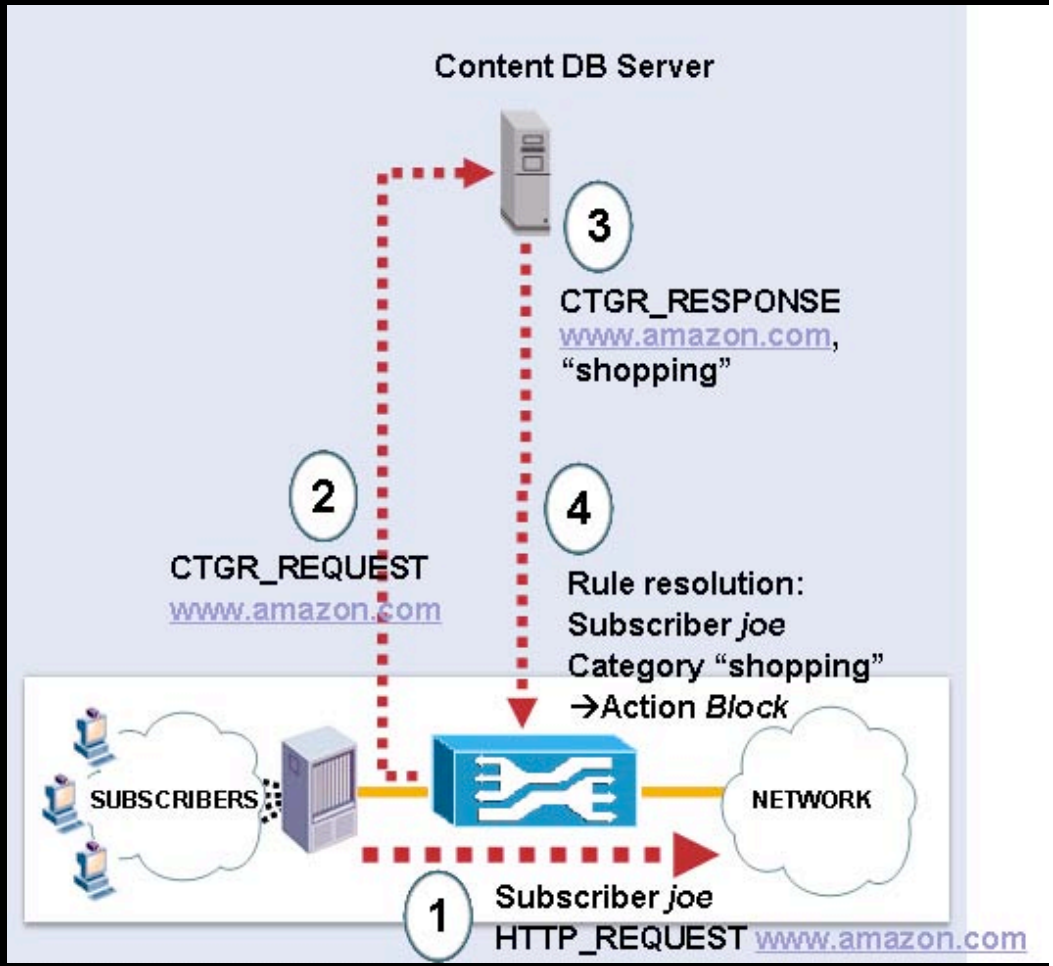
MPLS-VPN—Per VRF DPI



- DPI support for private/overlapping IP address spaces
- Upstream/downstream VPN-tags mapped through flow tracking
  - SCE identifies new flow from VPN-A, and correlates return packet's VPN tag

URL Filtering – General Approach

- API's for dynamically integrating with URL DB vendors
  - In addition to the built in URL lists mechanism
- Allows the solution to limit a subscriber's access to web sites based on "categorization" of content
- Useful for
  - Value added service for subscribers
  - Legal purposes (in some countries legislation requires that certain content is blocked)



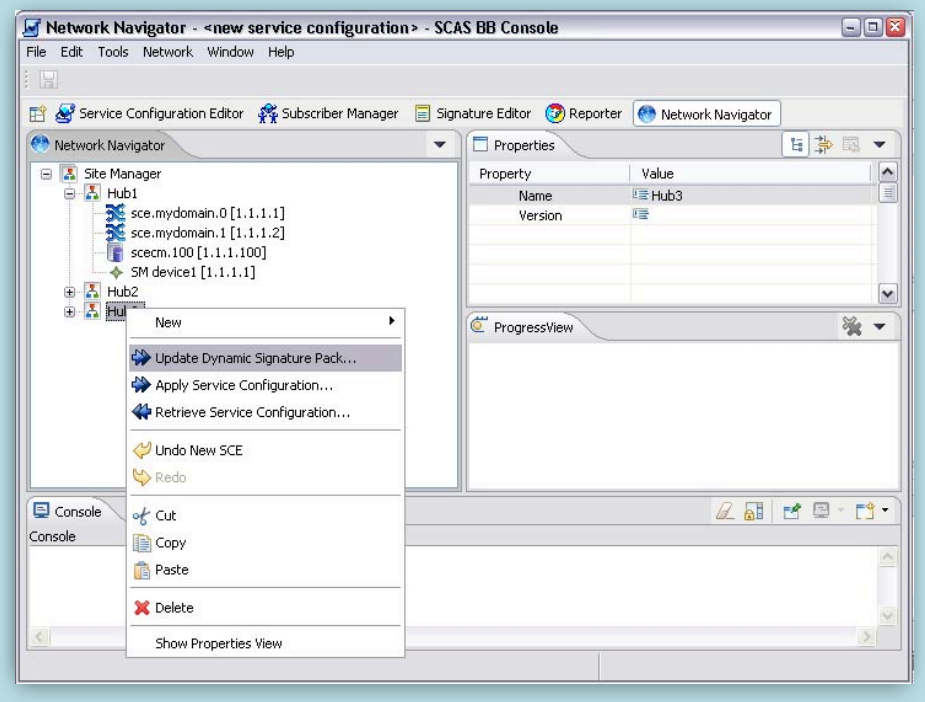
Dual link BW control

- In 2.x release global controllers for 2 GBE links were separated for each link
  - In order to enforce 300Mbps limit on upstream P2P traffic, the user had to configure 2 global-controllers, one for each link, while each enforces the P2P to 150Mbps
- On 3.0 a new mode is introduced, where the SCE enforces the global controllers policy on the aggregate traffic from the 2 ports
  - A user can define a single P2P global-controller that will enforce aggregate of 300M limit for the upstream P2P traffic
- The old mode is still supported for backward compatibility purposes

Management—Network Navigator

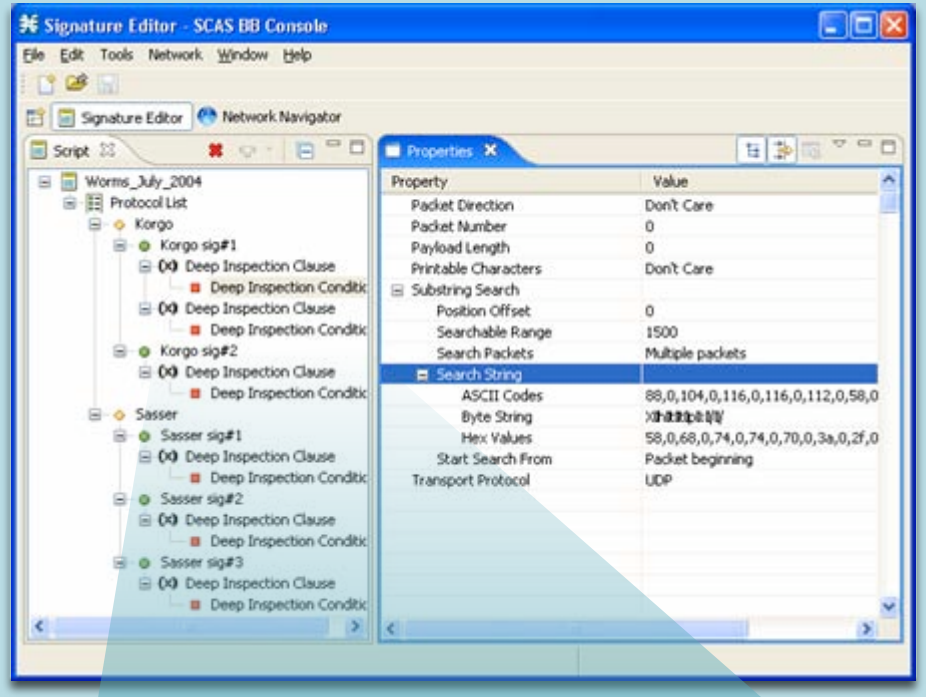
Single Interface to Manage All Solution Components

- Group devices into sites
  - SCE, CM, SM, database
- Batch management of devices/sites
  - Apply configuration
  - Update signatures
  - Update software
- Common management operations
  - View device status
  - Retrieve log
  - Activate/bypass



Signature Editor

- Customer defined signatures
- GUI based
- Rich signature language

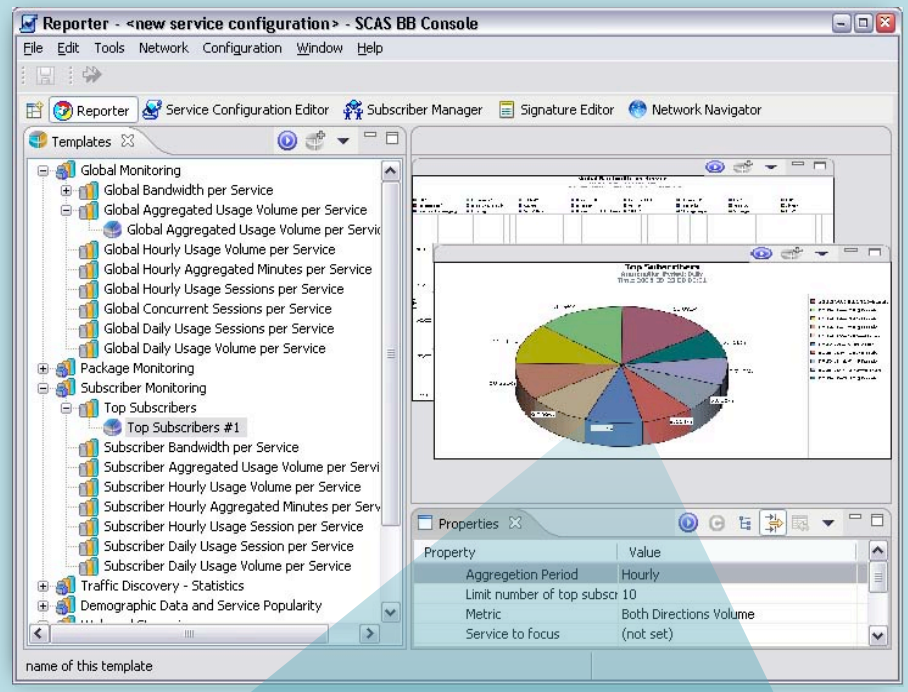


Multi-packet, Bi-Directional Patterns, Binary Characters, String-Match, HTTP User-Agent, HTTP X-Header

Integrated Reporter

- Integrated Java-based reporting tool
- Works with Oracle, MySQL or Sybase CM backend
- Context sensitive

  Drill down between reports and configuration

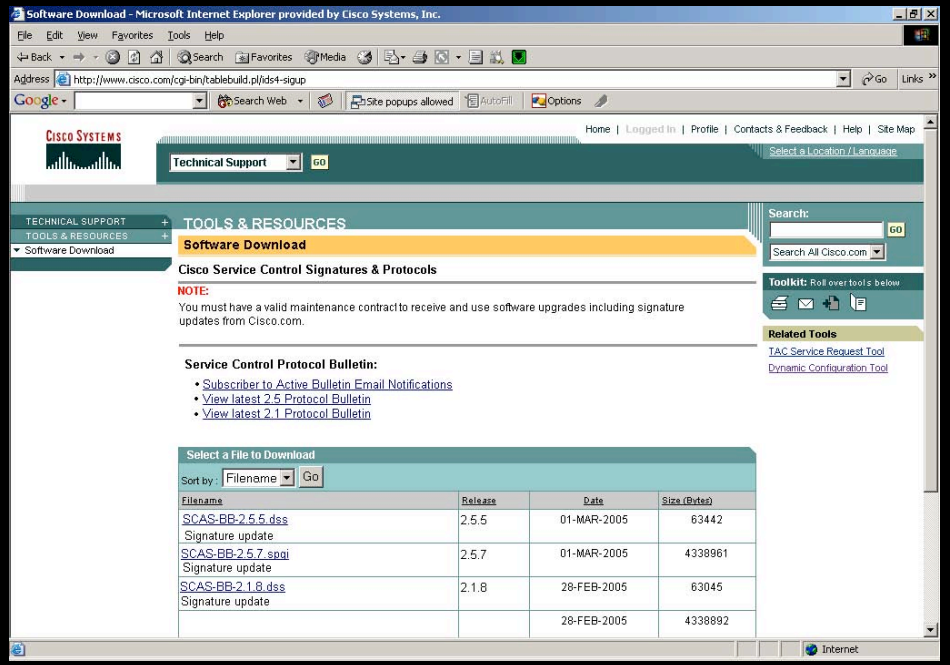


INTERACTIVE: Click on Top Subscriber to Activate Subscriber Real-Time Report

Hitless Upgrade (3.03)

3.03

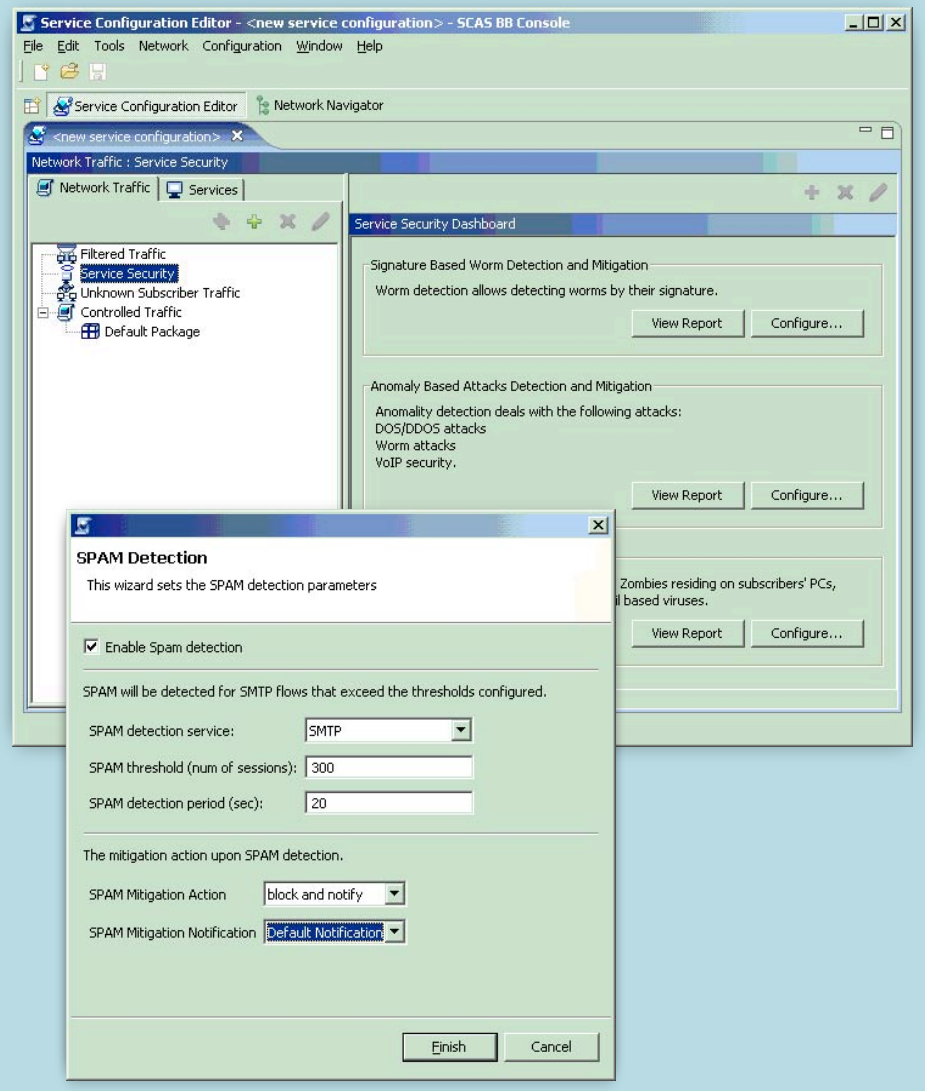
- Graceful phase-in of new protocol pack is supported by the SCOS infrastructure
- This Complements the Service Control framework for ongoing protocol support
  - Protocol upgrades are posted periodically on CCO (since 2.5.7)
  - No service downtime is incurred to the operator during upgrade



Service Security Dashboard

- Integrated console to manage service security functionality
  - View/load/edit signatures
  - Configuration identification thresholds
  - Setup mitigation actions
  - View reports

Availability: 3.0.3

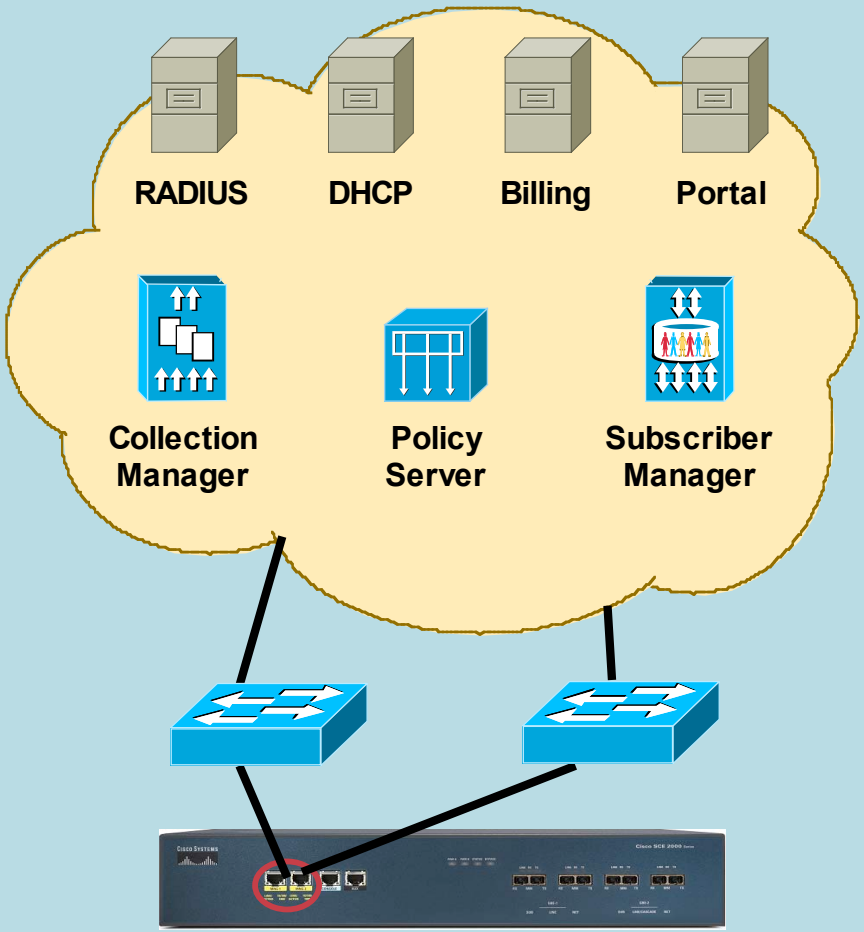


Redundant Management Ports

Critical High-Availability for Service Creation Scenarios

- SCE2020/1010 management interface redundancy
- Protects from physical failure or network partition
- Active/standby ports
- Transparent—Same IP/MAC for both ports
- 300 ms failure detection with active ARP to expedite recovery

Not Available on SE1010 1.5U Hardware (“P-Cube Box”)

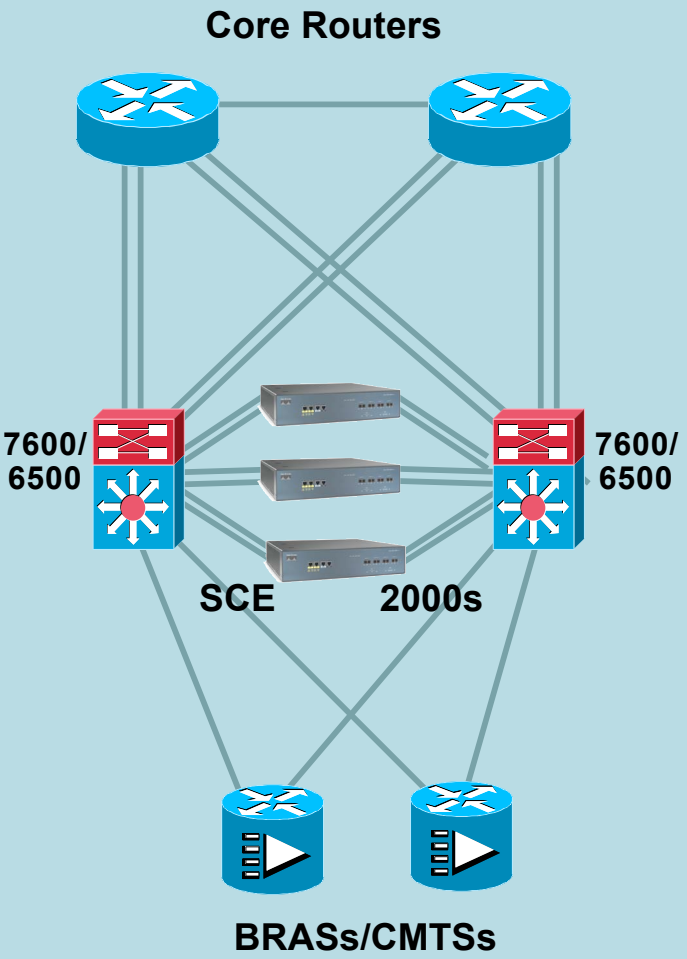


Subscriber Management

- "Subscriber-aware" solutions
- Manages Subscriber-contexts
  - Subscriber-ID: ID of subscriber-context
  - Network-ID: IP addresses used to map traffic to context
  - Policy-ID: ID of policy (package) defining rules
  - Subscriber-quotas: set/add/read usage quota buckets
- Integration into back-office/AAA
  - RADIUS AAA
  - Policy Control Systems (Tazz Networks)
- Cisco Subscriber Manager (CSM) serves as integration point

Multi-Gig Cluster Solution

- Split flows between more than two GBE links
- SCE(s) are hair pinned to redundant 6500/7600 matching EtherChannels on 6500/7600 ensure traffic of single subscriber flows to same SCE
  - Can use PBR as well
- Support for N+1 configuration through EC failover



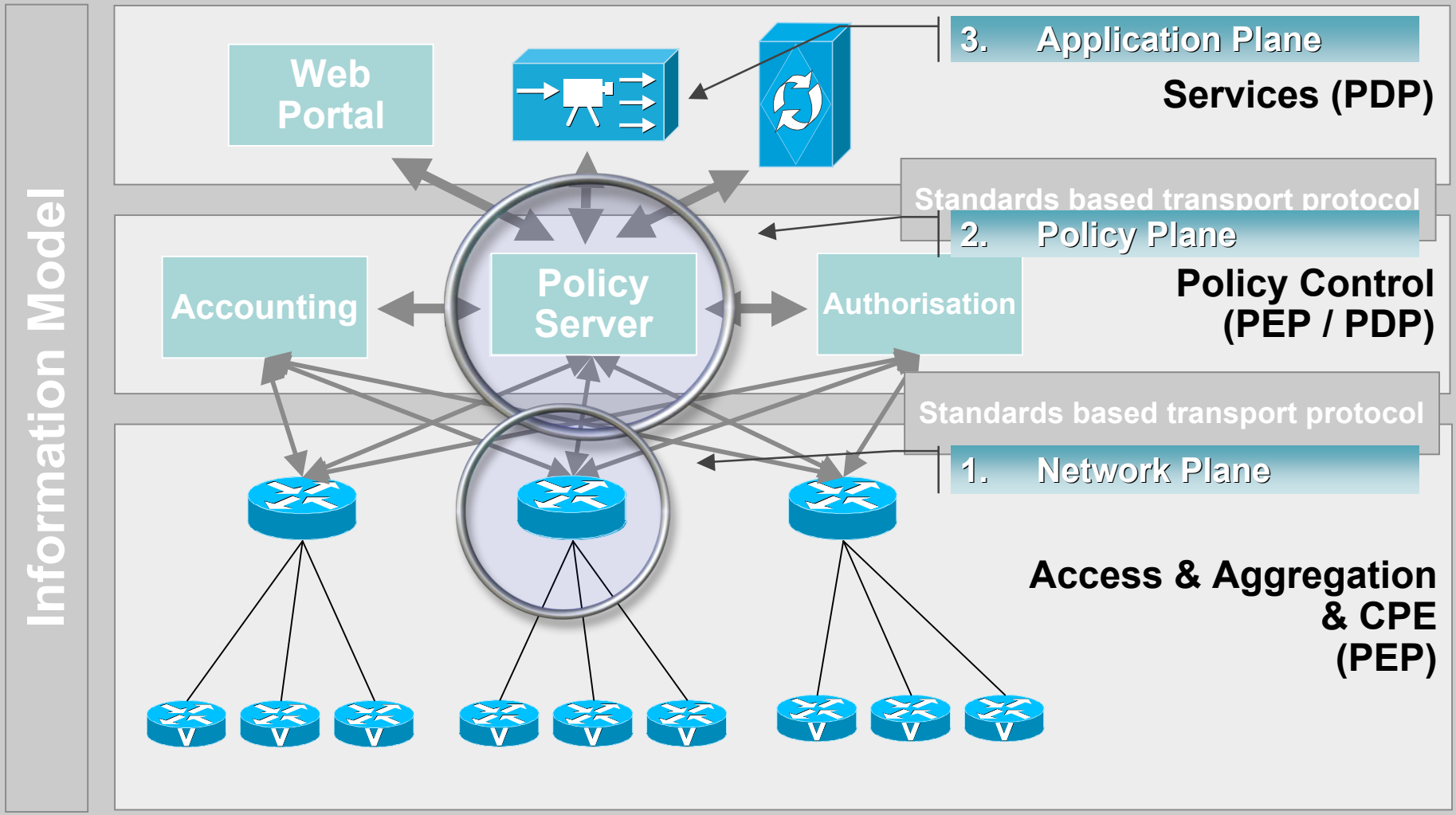
Agenda

Service Provider Market
and the Service Exchange

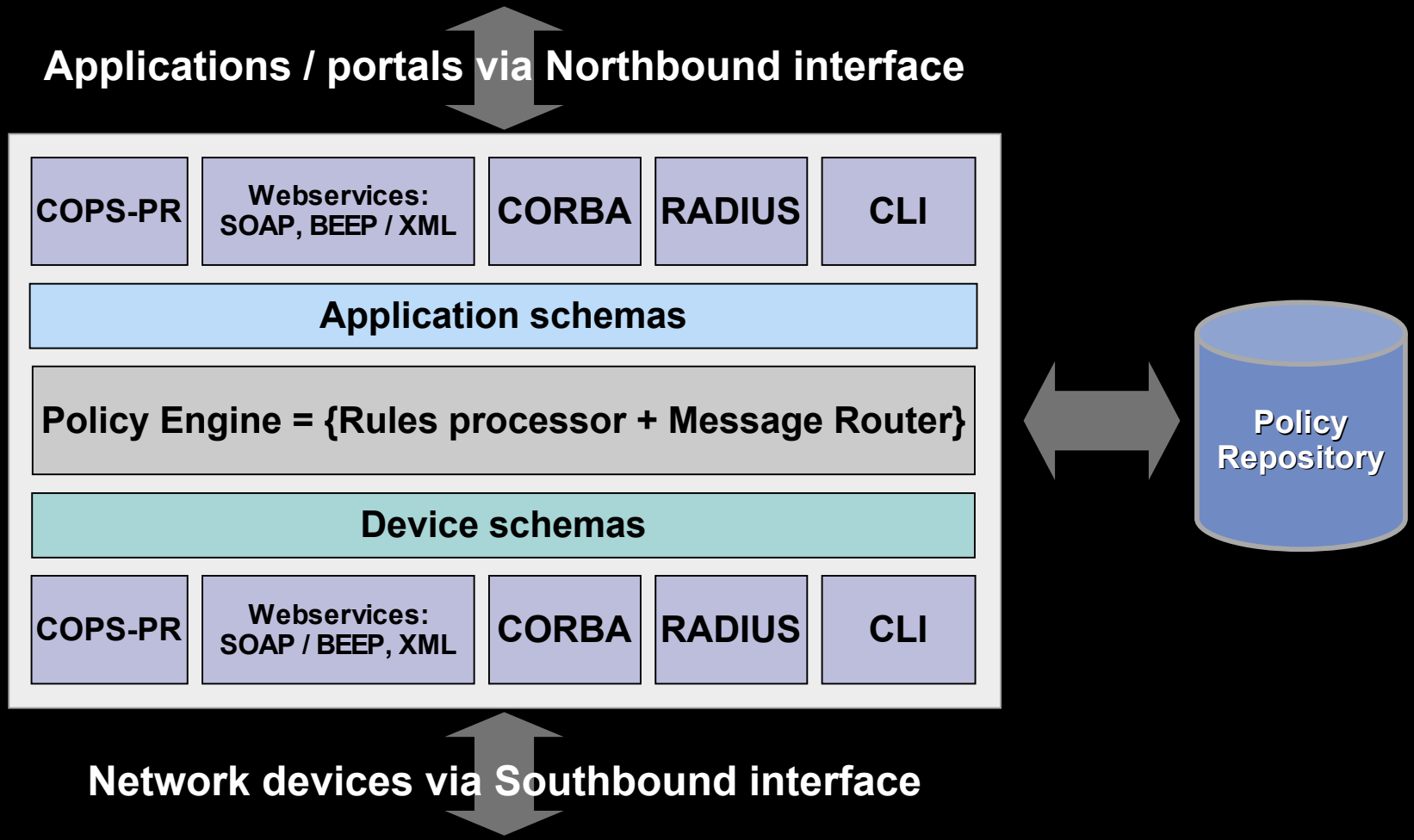
Cisco Service Control Engine
Review and update

Service Exchange Framework
Policy Management and services

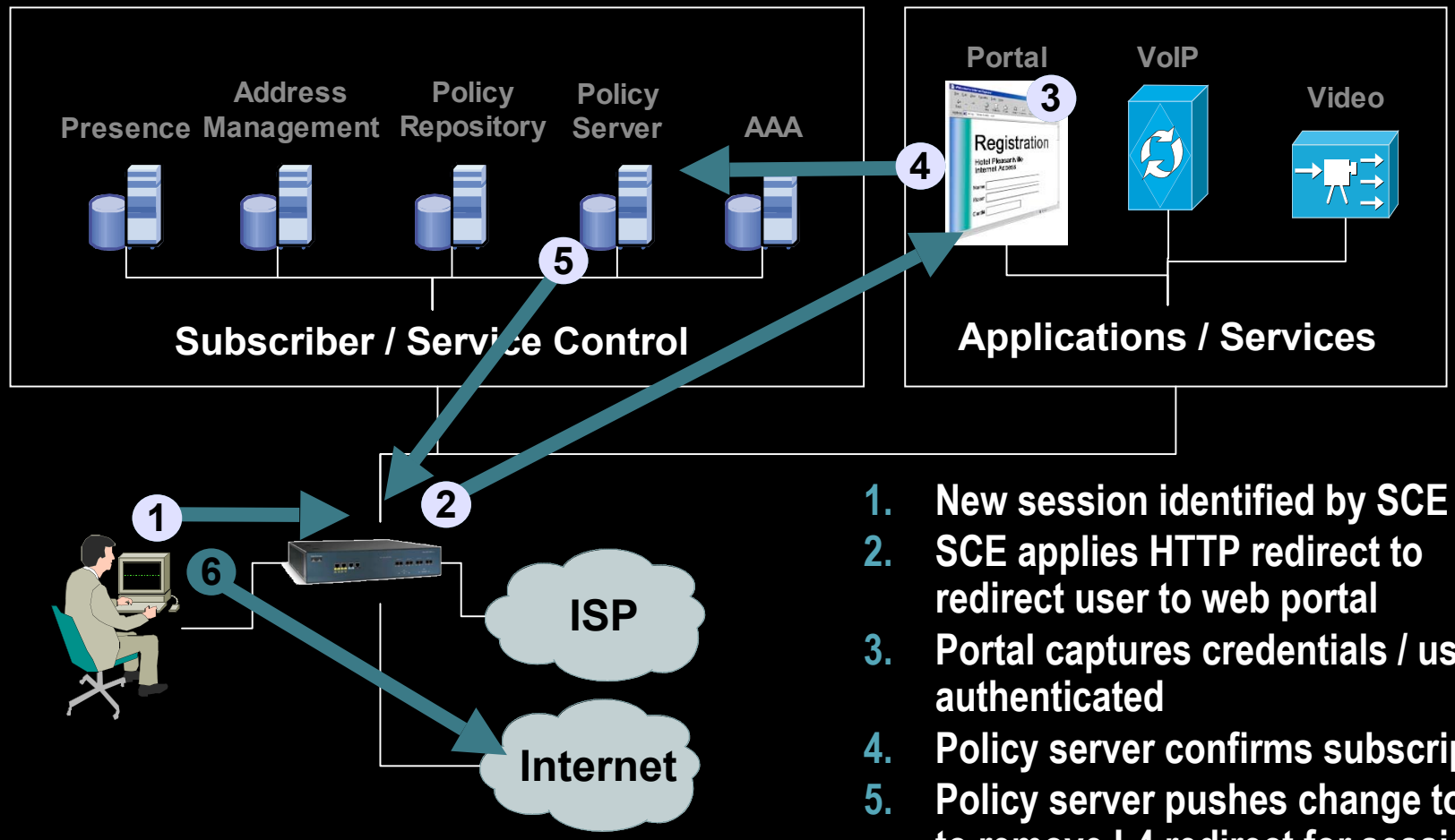
Policy Control Framework



Policy Server Components

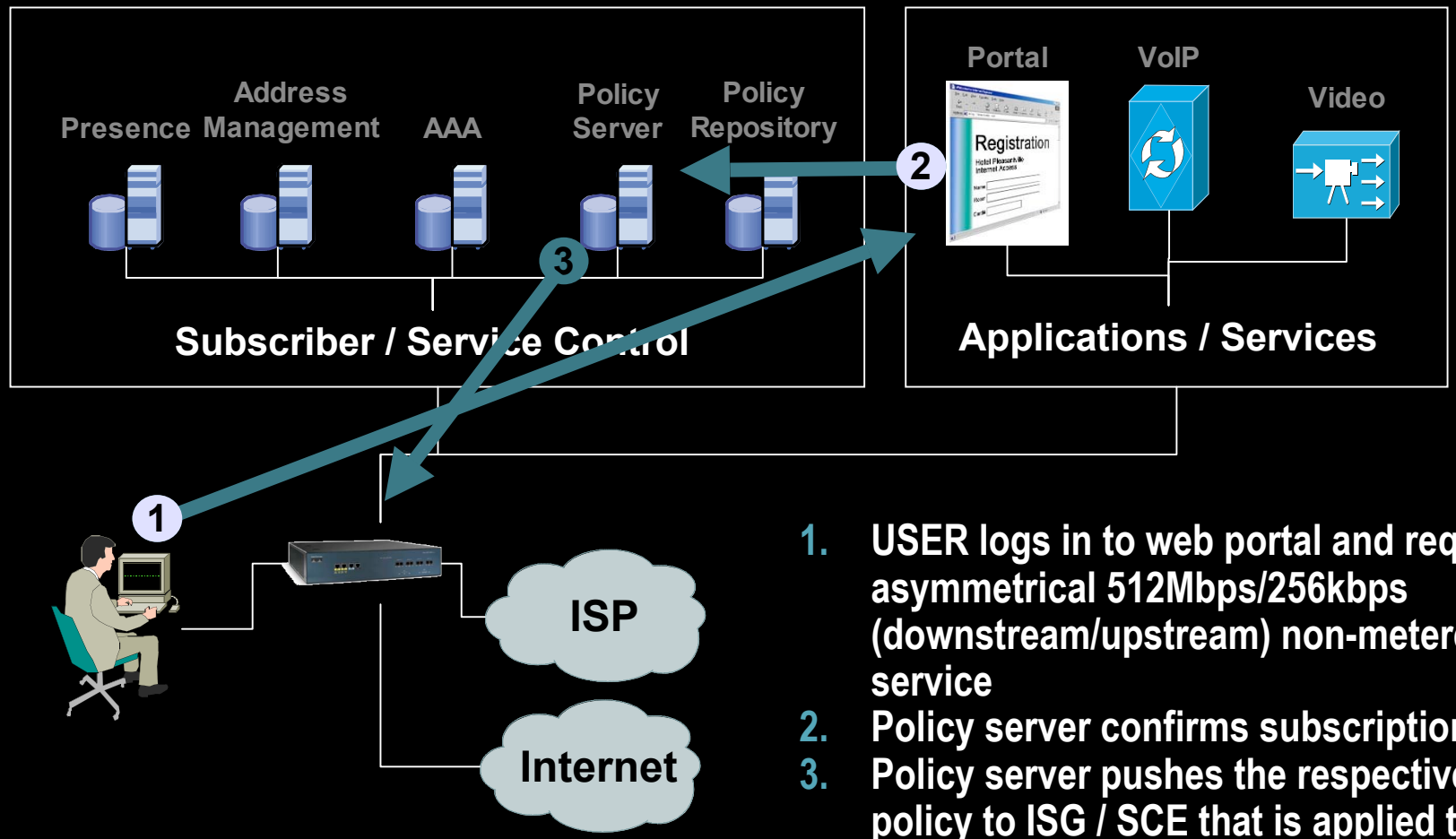


A. User self subscription with redirection



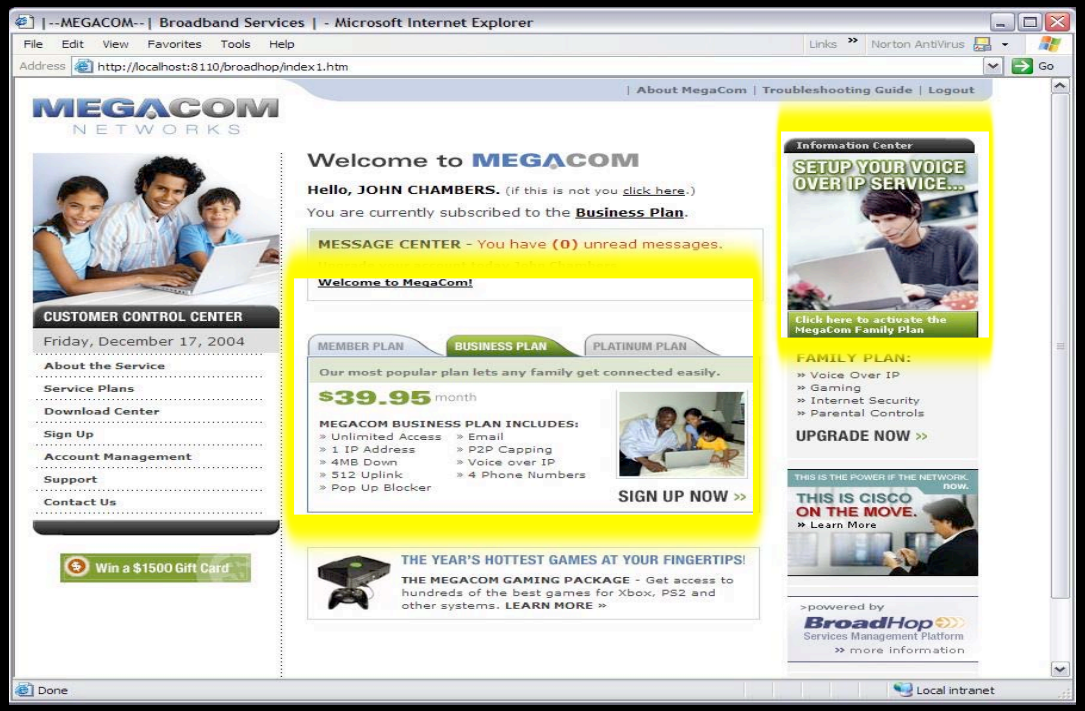
1. New session identified by SCE
2. SCE applies HTTP redirect to redirect user to web portal
3. Portal captures credentials / user authenticated
4. Policy server confirms subscription
5. Policy server pushes change to SCE to remove L4 redirect for session
6. User now has Internet access

B. User bandwidth selection



1. USER logs in to web portal and requests an asymmetrical 512Mbps/256kbps (downstream/upstream) non-metered service
2. Policy server confirms subscription
3. Policy server pushes the respective QOS policy to ISG / SCE that is applied to the user session

Customer self-provisioning



- Customer subscribed to an-entry-level profile.
- All customer's access lines are identically provisoned (i.e. DSL profile at max access speed).
- Service exchange enforces current customer speed and traffic profile.
- Customers can dynamically change profiles with no manual intervention.
- Profile change can be permanent (new tariff plan) or time-limited (turbo button, promotional offers).

To conclude …

- Cable, mobile, and DSL standards bodies are defining the need for policy server functionality
- Policy control layer is of growing importance and is being defined in all evolving access technologies
  - Significant commonality between evolving access technologies
  - Adds intelligence to base network transport solution - the equivalent to the Intelligent Networks (IN) capability in the voice world
- Policy control layer server is becoming the access agnostic service convergence plane
- Cisco Systems' Service Exchange Framework provides the service/application convergence layer for next generation networks