Cisco Service Control Engine:
Gestione del Traffico per l'abilitazione di nuovi servizi

17 Maggio 2005

Guido Motta
Cisco Systems Italia
gmotta@cisco.com

© 2004 Cisco Systems, Inc. All rights reserved.

Agenda

- Introduzione al “Service Control”
- Esempi
- Descrizione della soluzione
- Considerazioni per il deployment
- Gestione e Integrazione

© 2004 Cisco Systems, Inc. All rights reserved.

Architettura Cisco IP NGN

APPLICATION LAYER

VoD / HDTV GAMING



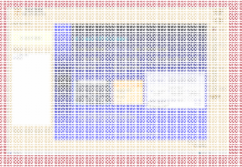
STORAGE



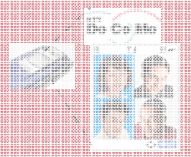
COMM



WEB SERVICES



MOBILE APPS

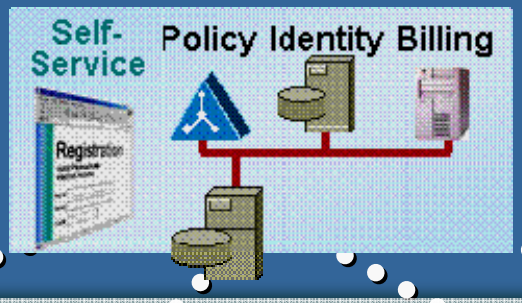


IP CONTACT CENTER



SERVICE CONTROL LAYER

Service Control



Struttura aperta per l'abilitazione del "Triple Play On The Move"

(Dati, Voce, Video, Mobilità)

OPERATIONAL LAYER

SECURE NETWORK LAYER

Customer Element

Access / Aggregation

Intelligent Edge

Multiservice Core

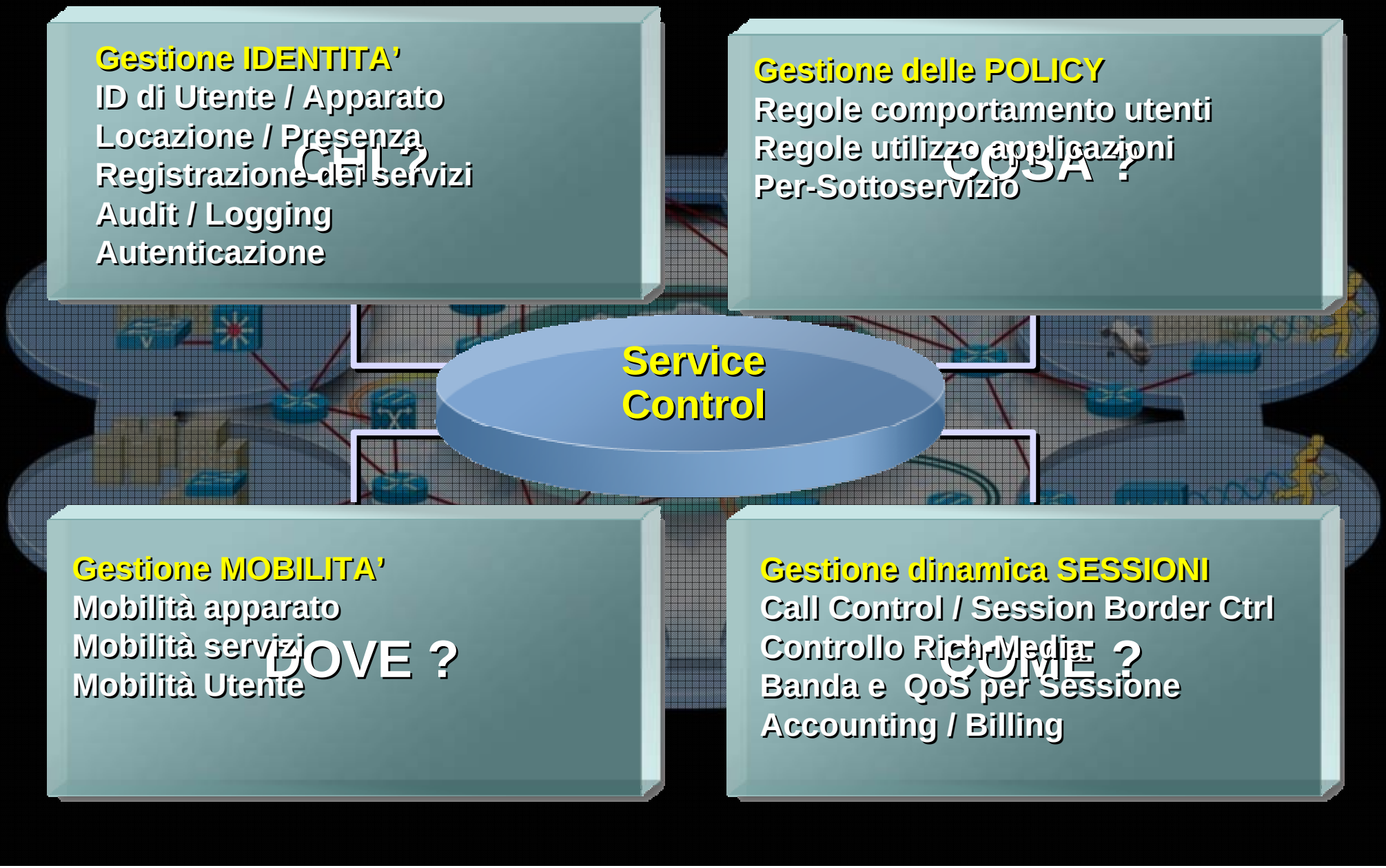
Transport

INTELLIGENT NETWORKING

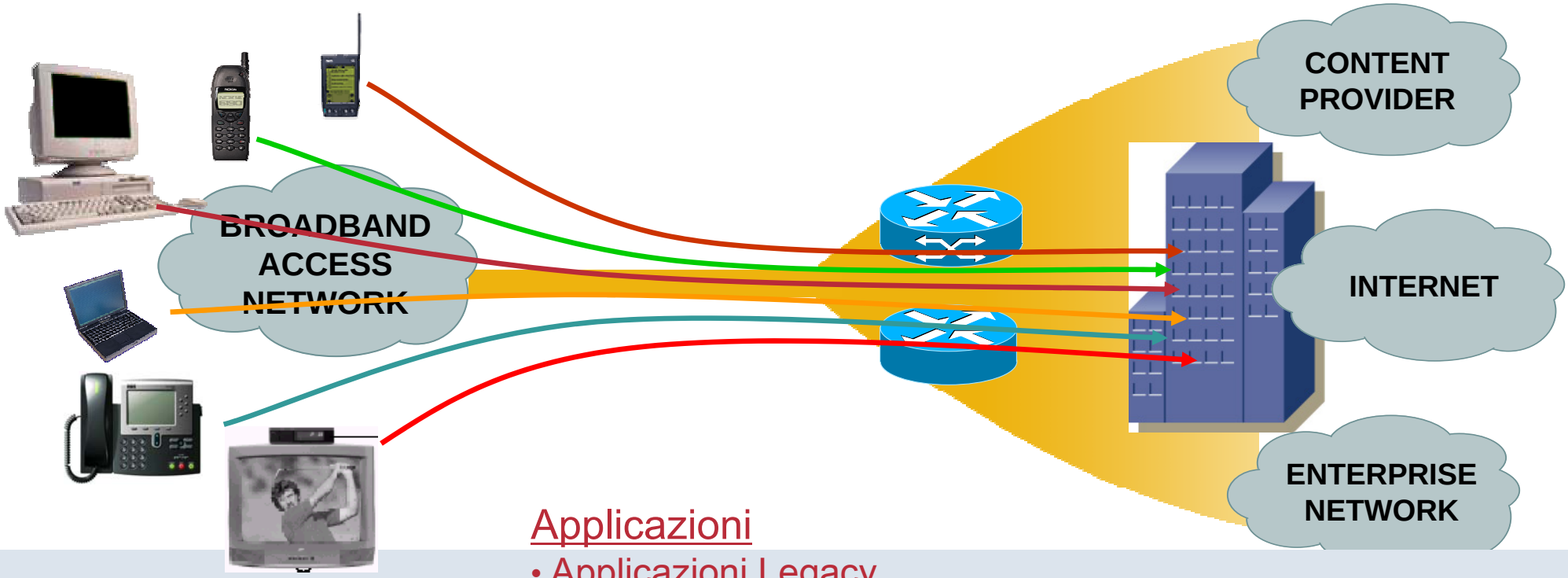
© 2004 Cisco Systems, Inc. All rights reserved.

Struttura “Service Control”

Controllo Servizi multimediale per convergenza Wireline/Wireless



Reti d'accesso moderne

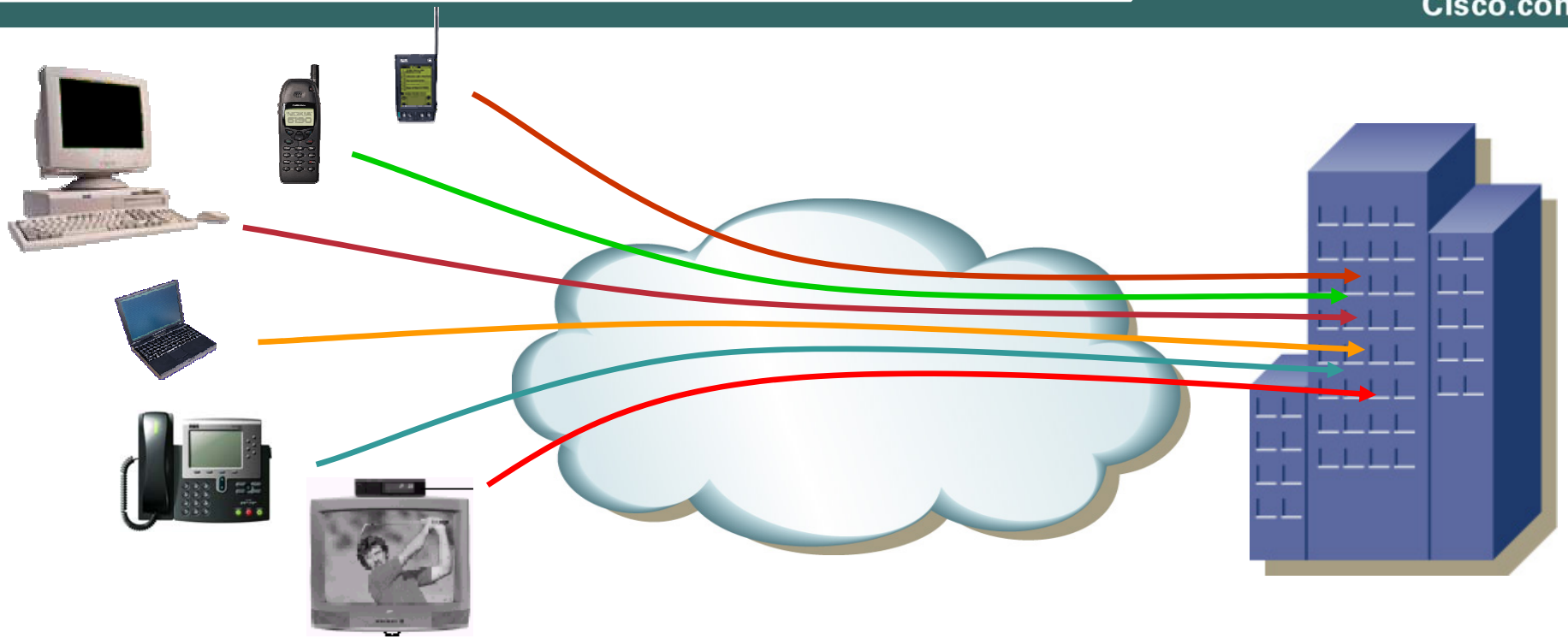


Utenza
- Postazioni di lavoro
- Laptop
- IPPhone
- Video
- Palmari

Applicazioni
- Applicazioni Legacy
- SNA/DLSW
- Web Based HTTPS
- E-learning
- Voice/Video over IP
- Internet
- P2P
- Streaming
- Network Management

Centro Servizi
- Servizi Centralizzati
- Infrastruttura ridondata
- Continuità dei servizi
- Accessi condivisi

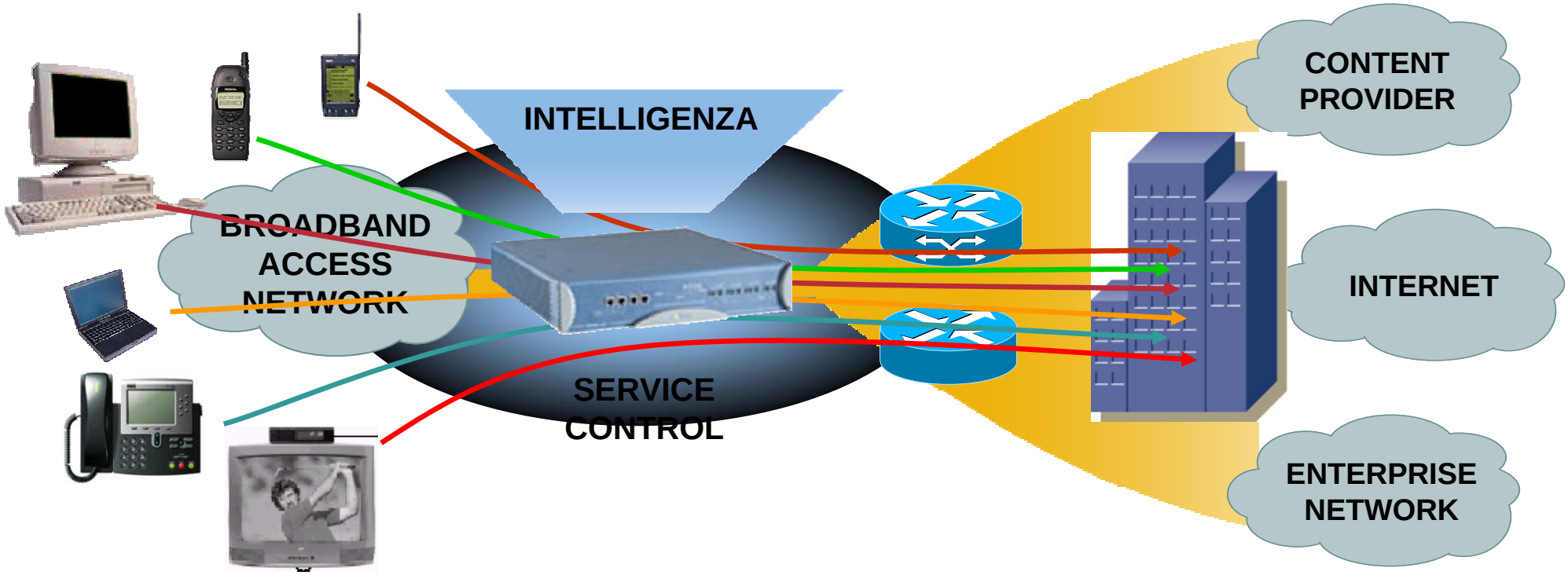
Esigenze del Cliente



- Visibilità in tempo reale delle applicazioni in rete
- Analisi e controllo per singolo utente e gruppi di utenti
- Analisi e controllo per applicazioni e servizi
- Prioritizzazione e differenziazione del traffico
- Garanzia per le applicazioni mission-critical
- Limitazione e blocco per servizi e utenti

© 2004 Cisco Systems, Inc. All rights reserved.

La soluzione: Una rete intelligente in grado di erogare “Servizi Controllati”



Reti abilitate al CONTROLLO dei SERVIZI

- I servizi messi a disposizione dalla rete vengono gestiti o eventualmente fatturati nel modo più appropriato agli utenti che ne hanno usufruito maggiormente
- Viene offerto un controllo granulare su bande differenziate, con capacità di controllo per-sessione e per applicazione, gestione QoS …

Cosa è il “Controllo dei Servizi”?

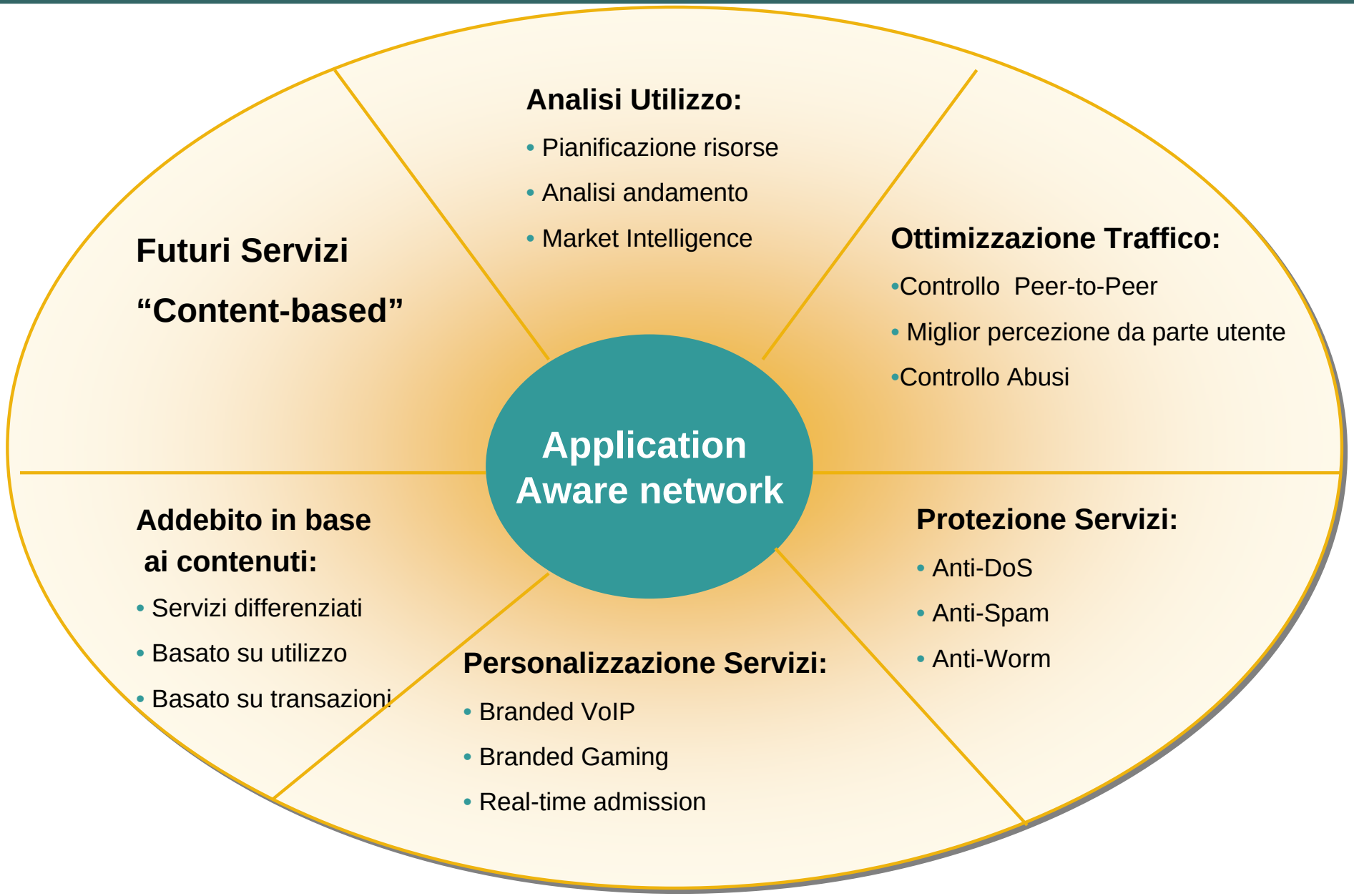
Tecnologia	Requisti
Conoscenza Applicazioni	Stateful deep-packet application inspection
Conoscenza degli Utenti	Gestione dello stato dell’utente (Gestione banda per-utente, quota e integrazione OSS (via DHCP e Radius)
Controllo in tempo reale	Dimensionamento della banda delle applicazioni a livello di sessione, blocco, redirezione (HTTP, RSTP, SIP)
Flessibilità dei Servizi	Programmabilità per supportare nuove applicazioni e nuove esigenze di business

ASPETTI FONDAMENTALI:

- **ALTE PRESTAZIONI: Gestione a livello Applicazione e controllo a velocità multi-Gigabit senza impatto sulle prestazioni**
- **INDIPENDENZA DAL TRASPORTO: Funziona con qualsiasi rete e abilita servizi basati su QoS**
- **INTEGRAZIONE OSS: API aperte per facile integrazione con sistemi OSS (es. Policy service, AAA, ecc.)**
- **PROGRAMMABILE: Facilità di integrazione e supporto nuovi protocolli o applicazioni**

© 2004 Cisco Systems, Inc. All rights reserved.

Esempi di Servizi



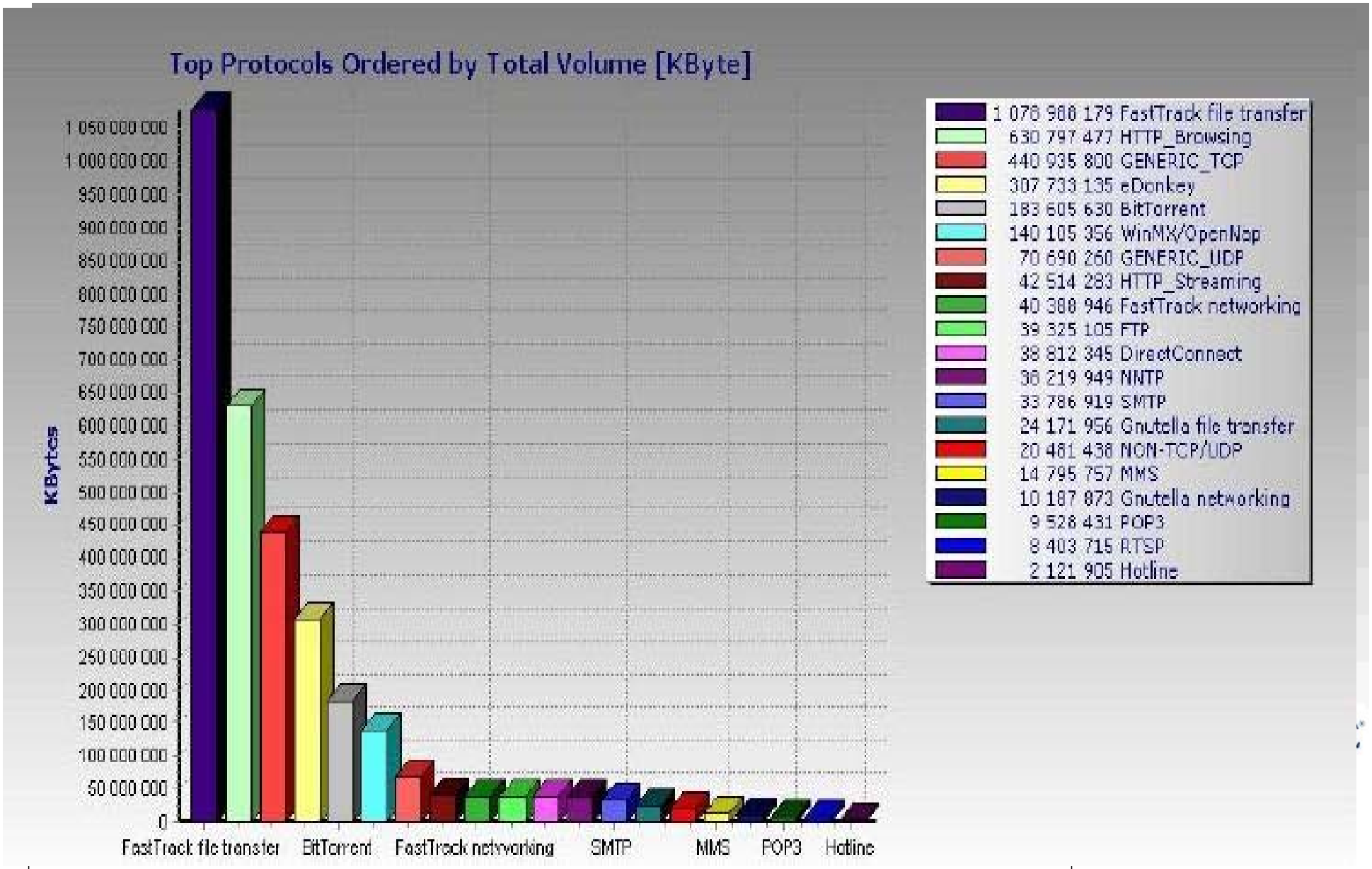
© 2004 Cisco Systems, Inc. All rights reserved.

Esempio: Controllo utilizzo applicazioni

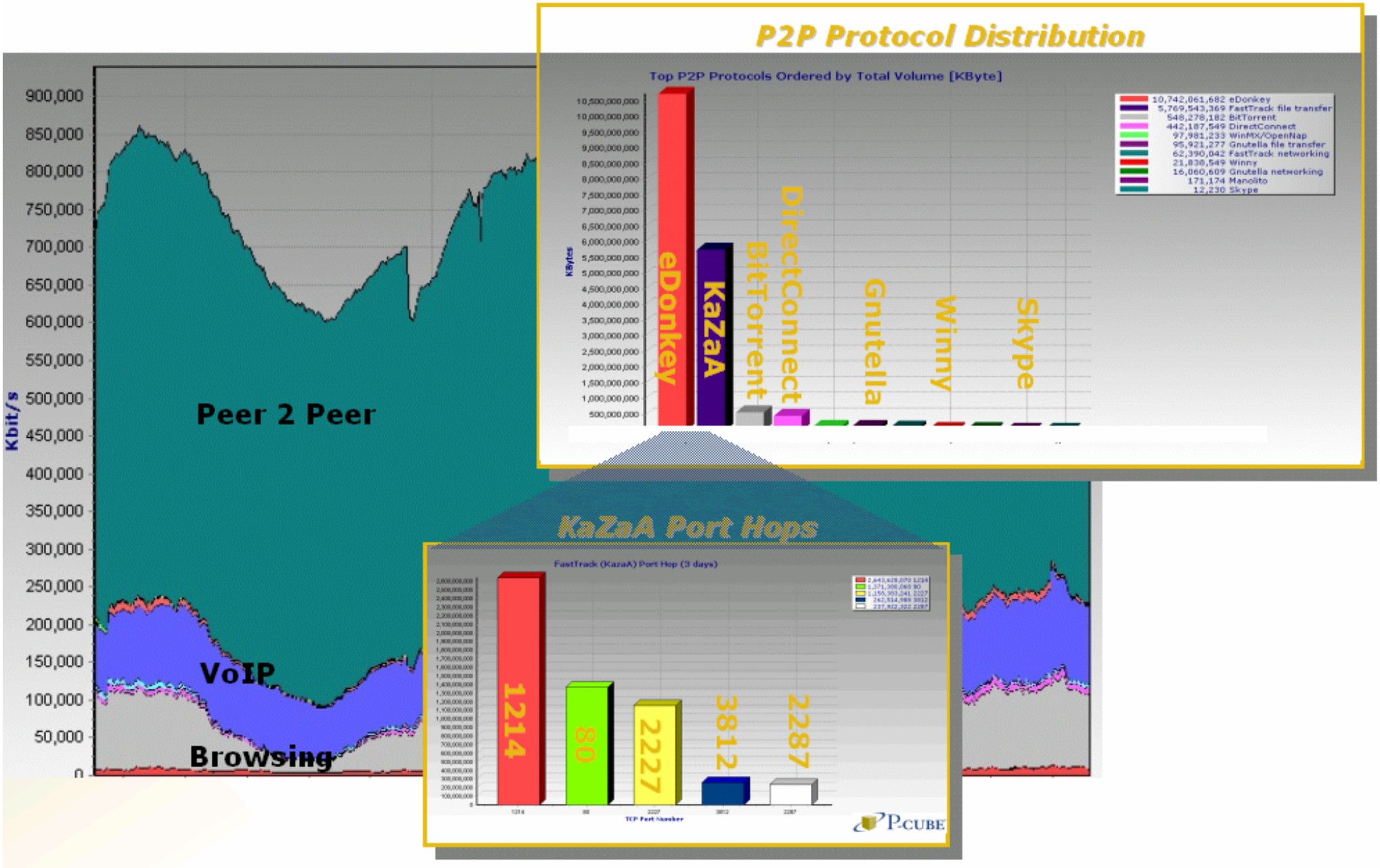
- **Visibilità Applicazioni e utenti**
  - **Applicazioni più utilizzate, top 10, picchi di utilizzo**
  - **Viste globali e per singolo utente**
  - **Maggiori utilizzatori per applicazione, distribuzione demografica**
- **Benefici**
  - Pianificazione risorse intelligente**: Quando c'è veramente bisogno di maggiore banda? Come si può ottimizzare?**
  - Rilevamento abusi**: Identificazione utenti che abusano delle risorse a disposizione**
  - Maggior sensibilità**: Quali sono le killer-apps? Quali servizi interessano o servono maggiormente agli utenti?**
  - Gestione costi**: Fatturazione per volume, sessione e contenuti**

© 2004 Cisco Systems, Inc. All rights reserved.

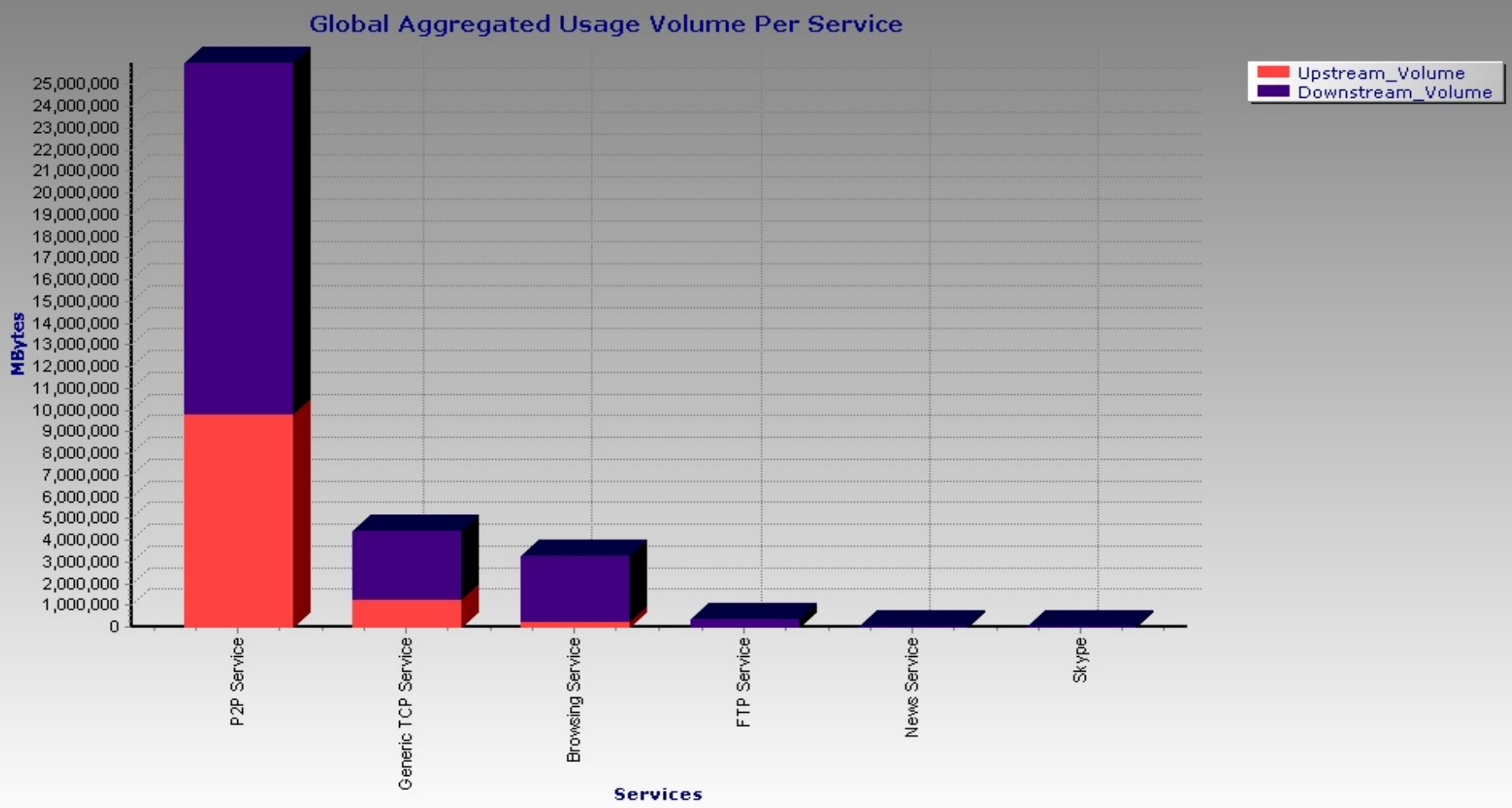
Completa analisi utilizzo applicazioni



Completa analisi utilizzo applicazioni



Analisi aggregata applicazioni per POP



Over 25 Terabytes of P2P traffic in 7 Days!

© 2004 Cisco Systems, Inc. All rights reserved.

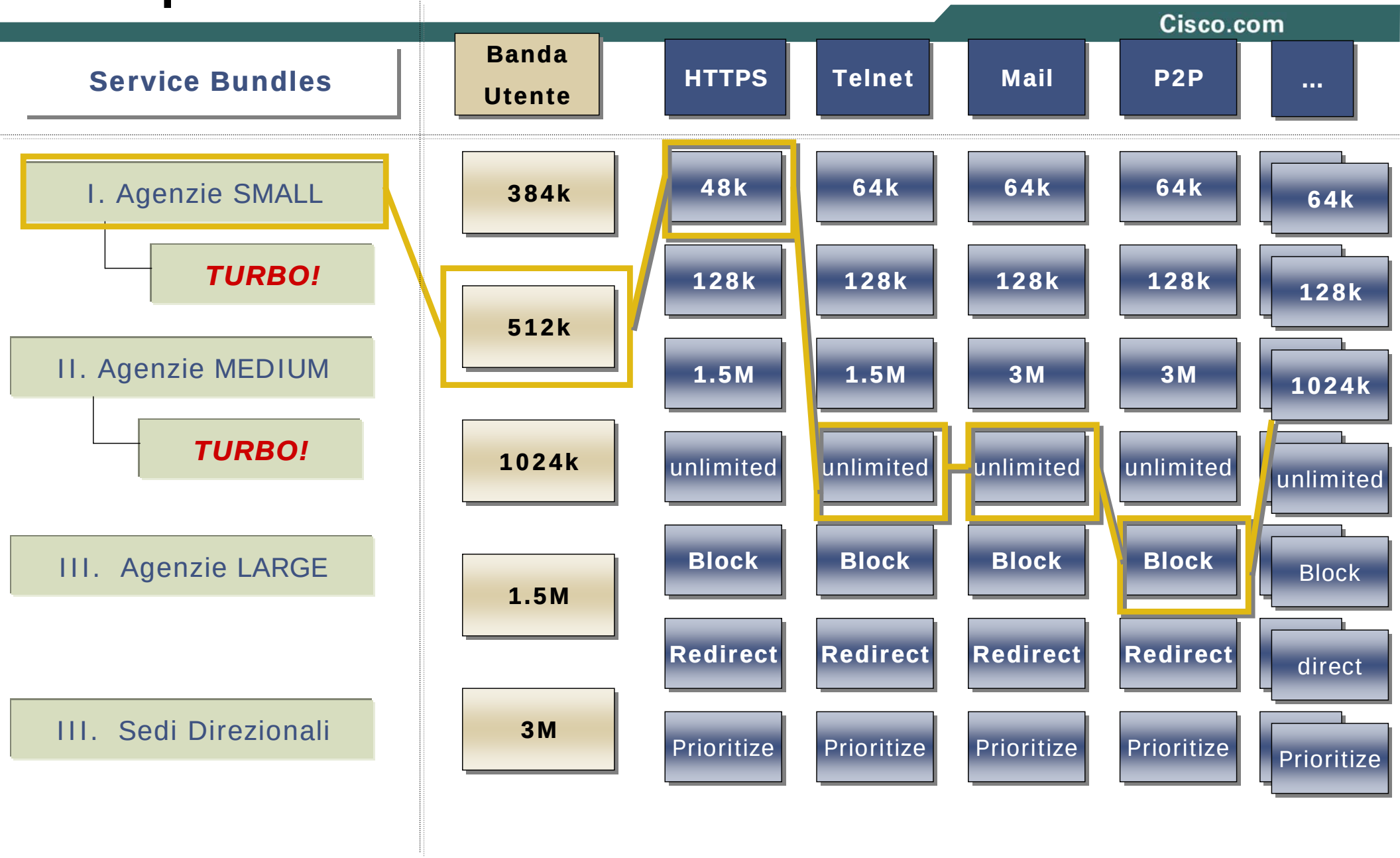
Esempio: Controllo della banda

- **Controllo e Prioritizzazione della banda**
  - Globale
  - Gruppo di utenti
  - Utente
  - Sessione applicativa
- **Regole Dinamiche**
  - Basate sul Tempo/Destinazione/Applicazione
  - Basate sulla quota utente

- **Esempio**
  - Turbo Boost per applicazione – es. Solo Http o RTSP
  - Abbassa priorità P2P durante le ore di picco
  - Abbassa priorità P2P dopo x MByte/g per utente

© 2004 Cisco Systems, Inc. All rights reserved.

Esempio: Controllo della banda



© 2004 Cisco Systems, Inc. All rights reserved.

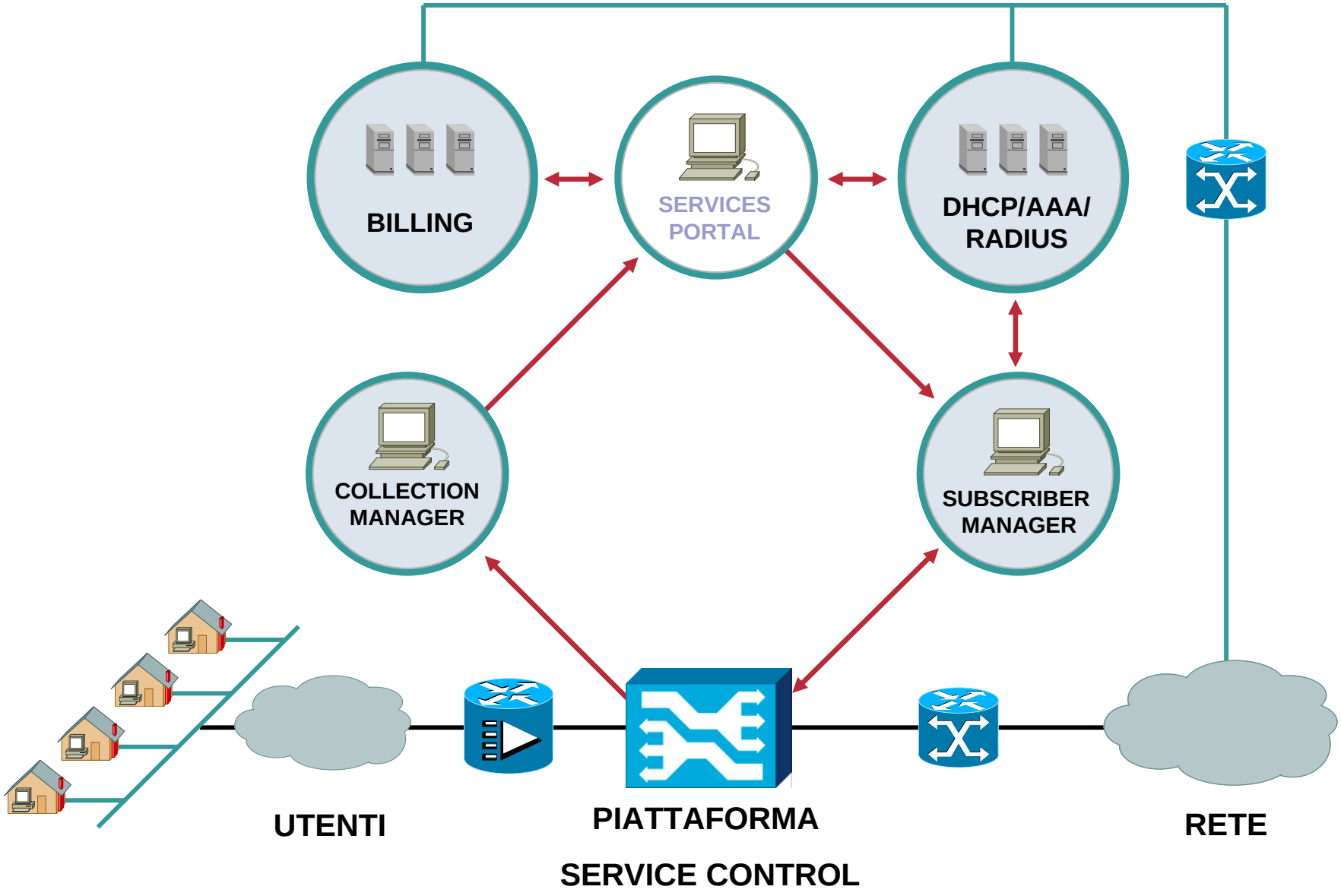
Esempio: Gestione Quote

- **Gestione completa delle “quote”**
  - **Multiple quote simultanee per utente**
  - **Tracciamento accurato di utilizzzo**
- **Integrazione OSS**
  - **Invia informazione a OSS in seguito a superamento quota**
  - **Controllo automatico e dinamico dei cambiamenti delle regole d’utente**

Piano	Quota per Accesso al Servizio	Quota specifica per Applicazione	Azione	Commenti
A	5GB	Gaming: 500min	Ridurre banda a velocità dialup	Contenuto “Premium” e applicazioni escluse da quote
B	5GB	P2P: 1GB	Applicare costo aggiuntivo	Contenuto “Premium” e applicazioni escluse da quote
C	Nessuna	Nessuna	N/A	Servizio critico non ha limite

© 2004 Cisco Systems, Inc. All rights reserved.

La soluzione “Service Control”



© 2004 Cisco Systems, Inc. All rights reserved.

Service Control Engine



SCE2020

- 4 GBE or 4/8 FE
- HA Cascade
- 2 External Bypass



SCE1010

- 2 GBE
- 1 External Bypass

© 2004 Cisco Systems, Inc. All rights reserved.

Piattaforme Service Control

	SCE1010 	SCE2020 
Interfacce	2-GBE (fiber SX/LX)	4-GBE (fiber SX/LX) 8-FE*
Interfaccia Mgmt.	10/100 FE	2 x 10/100 FE **
Memoria Processore	768MB	1.5GB
N. Max. Flussi	2M flussi applicativi concorrenti unidirezionali	2M flussi applicativi concorrenti unidirezionali
N. Max. Contesti Utenti	40,000	100,000
Configurazione di Rete	- Receive-only - Inline	- Receive-only - Inline - Cascade

* Versione futura

** Oggi non usata

© 2004 Cisco Systems, Inc. All rights reserved.

Service Control Application

Collector Manager

- Raccoglie i dati generati dal SCE Row Data Records
- Memorizza i dati a database oppure su CSV file
- Bundle Edition viene fornito con database Sybase ASE
- Client Reporter per la generazione dei report da database
- Sistemi operativi supportati Solaris e Linux

Subscriber Manager

- Gestione degli utenti, necessario in architetture Subscriber Aware
- Memorizza gli utenti e il profilo in un database
- Sincronizza la registrazione degli utenti sui dispositivi SCE (PUSH/PULL)
- Integrazione con server Radius e DHCP

© 2004 Cisco Systems, Inc. All rights reserved.

Protocol Support

- The table shows the most relevant protocols supported by the Service Control Engine.
- Protocols are periodically updated by Cisco.
- Customers can also define additional signatures.

•HTTP	•Gnutella	•SIP
•FTP	•eDonkey	•H323
•NNTP	•BitTorrent	•Skype
•SMTP	•DirectConnect	•RTSP
•POP3	•SoulSeek	•MMS
•Any IP	•KazaA	•XBOX
•Any TCP port	•Manilito	•Vonage
•Any UDP port	•WinMX	
	•Winny	
	•Share	
	•Filetopia	
	•Suribada	
	•Kuro	
	•iTune	
	•Mute	
	•NodeZilla	
New protocols added periodically		

© 2004 Cisco Systems, Inc. All rights reserved.

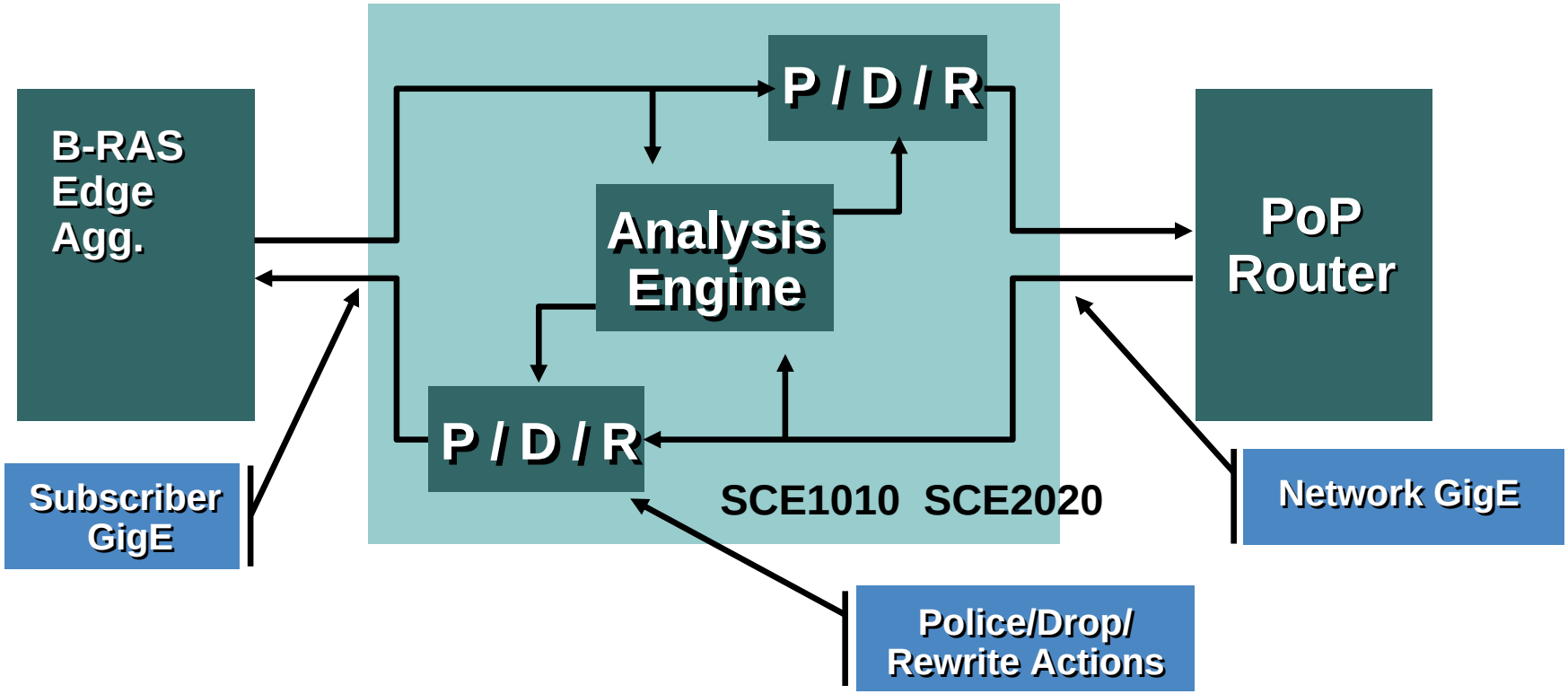
SCA: funzionalità

LA SOLUZIONE SI BASA SULLA DEFINIZIONE:

- dei **Servizi IP** per classificare il traffico in base a:
  - applicazione utilizzata (**P2P, Streaming, Browsing** …)
  - Protocollo e porta (**TCP 8080,UDP 53..)**
  - Server di destinazione
  - Fasce orarie
- degli **Utenti** in base all'indirizzo IP statico o dinamico
- dei **Profili utenti** per associare Utenti e Servizi IP in base a:
  - permessi di utilizzo
  - allocazione della banda
  - limitazione della banda

© 2004 Cisco Systems, Inc. All rights reserved.

Schema a blocchi



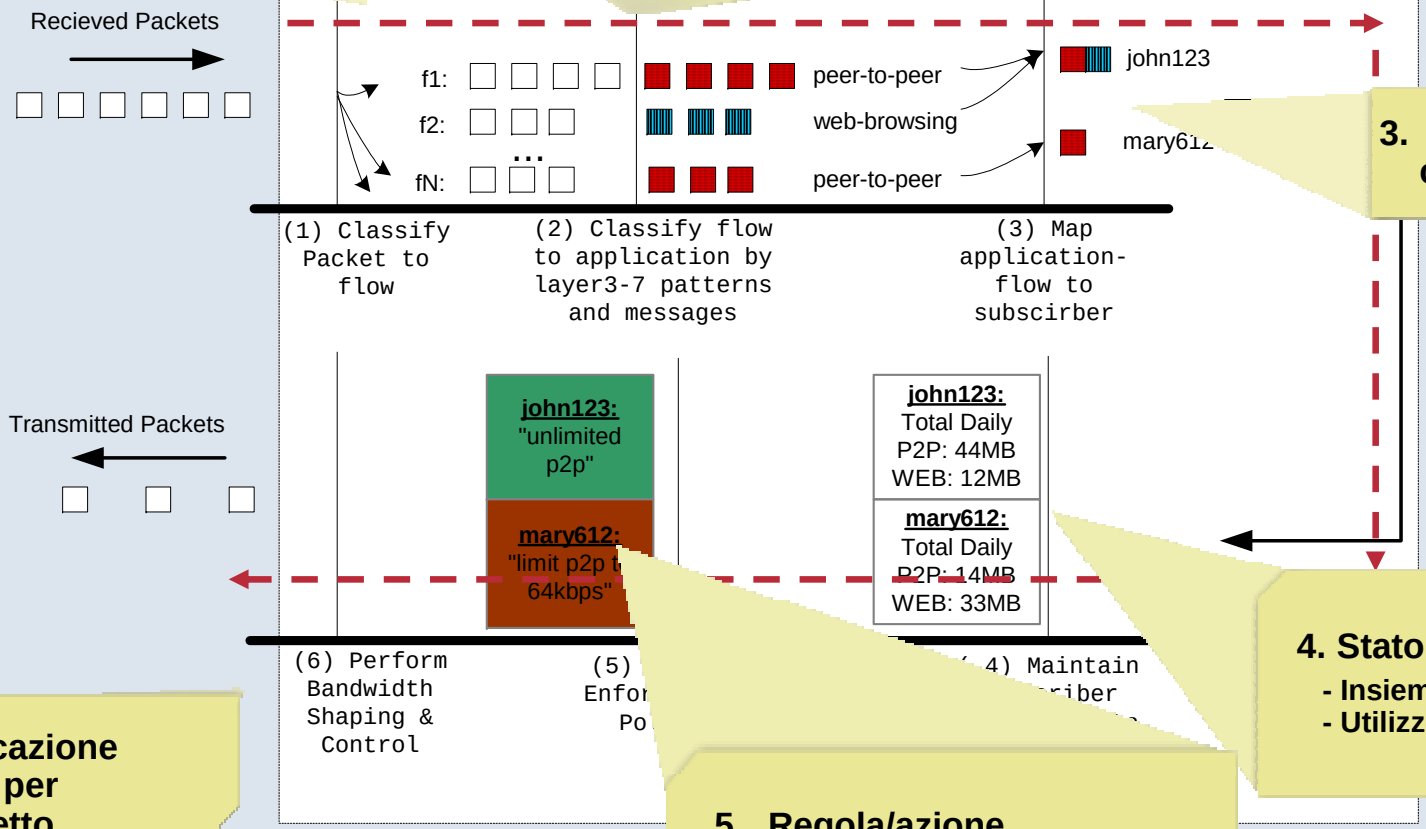
- **“Stateful Analysis Engine” con capacità di riconoscimento delle applicazioni — vede tutti I pacchetti in entrambe le direzioni**
- **Analysis Engine impiega Regole di Business attraverso la Dynamic Control Policy su base utente (es. rate policing, scarto pacchetti o riscrittura header)**
- **Pacchetti non instradati nè commutati; I pacchetti dall’interfaccia utente vanno sempre alla corrispondente interfaccia rete, e vice-versa**

© 2004 Cisco Systems, Inc. All rights reserved.

Flusso Logico

1.Pacchetti classificati in flussi bi-direzionali

2.Flussi classificati per applicazioni/contenuti:
- **TCP state machine,**
- **Signature detection,**
- **Tracciamento/classificazione Applicazioni**



3. Flussi mappati sul contesto utente

4. Stato dell'Utente:
- **Insieme di Regole**
- **Utilizzo/Quota**

5. Regola/azione selezionata:

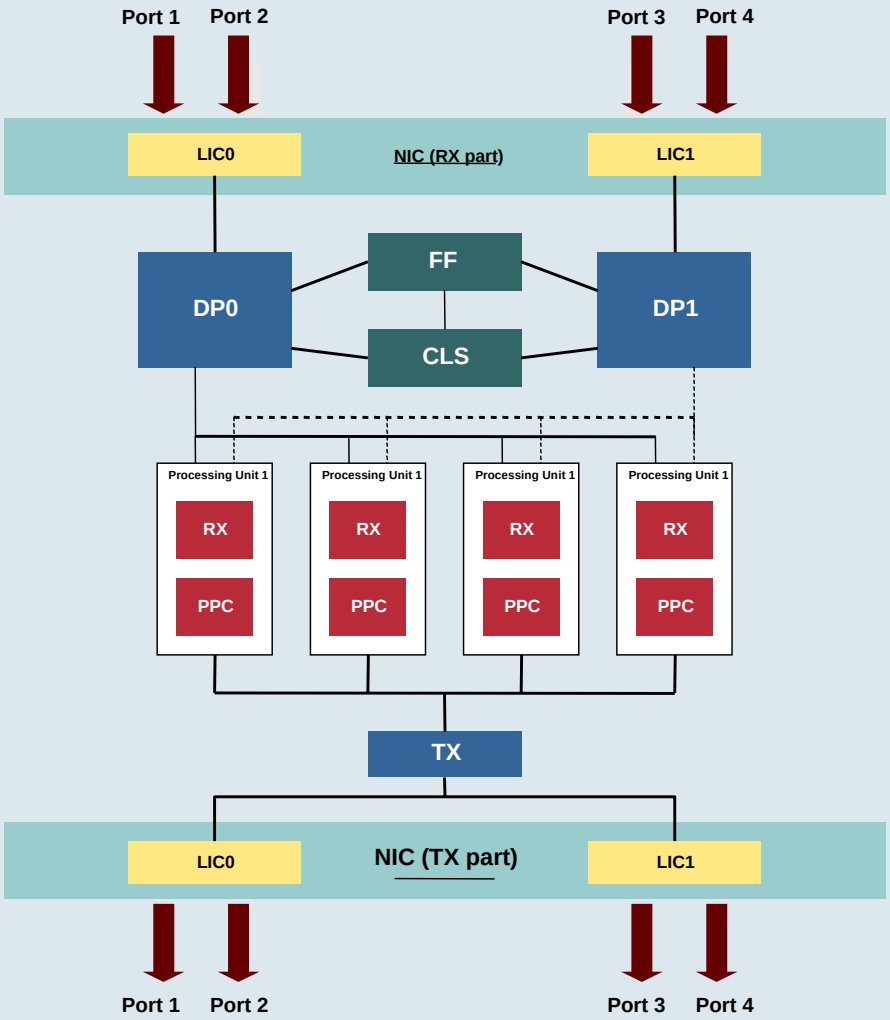
Blocco, redirezione, controllo bandl, coda, marcatura, rapporto

6. Applicazione regole per pacchetto

© 2004 Cisco Systems, Inc. All rights reserved.

Flusso dei pacchetti— Piattaforma Hardware Accelerata

- La maggior parte dei pacchetti (70-80%) sono processati in Hardware
- Le CPU sono usate quando viene richiesta ulteriore capacità di processo (ma bypassate se non richiesto)
- Bilanciamento “Stateful” assicura assenza “stati d’attesa” tra multiple (4) CPU che condividono il carico di processo
- Nessun campionamento; processo completo di ogni pacchetto
- Ispezione pacchetti e decisioni basate su regole programmabili



© 2004 Cisco Systems, Inc. All rights reserved.

Classificazione/Policy in azione

Flow tuple	End-User	Protocol	Service	Subscriber	Package	*Action*
TCP, 128.33.1.1, 61.2.3.4, 3122, 80		HTTP	General Browsing	Default	Default	*None*
TCP, 128.33.1.6, 61.2.3.4, 4321, 80		HTTP	Browsing-List1	maggie_simpson	Kids	*Redirect to: www.xxx.com*
TCP, 128.33.1.44, 61.2.3.66, 13142, 80		eDonkey	P2P	Default	Default	*Global Control: 30mbps/120mbps (no limit between 1am-4am)*
TCP, 128.33.1.7, 61.2.3.4, 3122, 25		SMTP	SMTP-Offnet	128.33.1.7@grp1	spam	*Alert if more than 3,000 / hour*
TCP, 128.33.1.99, 61.2.3.4, 3211, 5060		SIP	SIP-Offnet	Default	Default	*Set Priority = 1*
UDP, 128.33.1.99, 61.2.3.4, 3031, 30223		RTP (bind to F:104)	SIP-OffNet	Default	Default	*Set Priority = 1*

© 2004 Cisco Systems, Inc. All rights reserved.

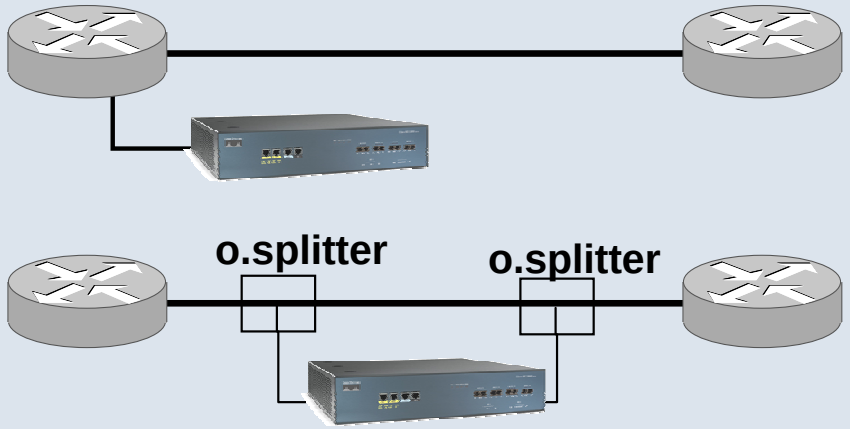
Deployment
Configurazioni Inline e Receive-only

- **Configurazione Receive-only**

  GIG-E: Usando Optical Splitters /Port-Span

  FE: Port-Span

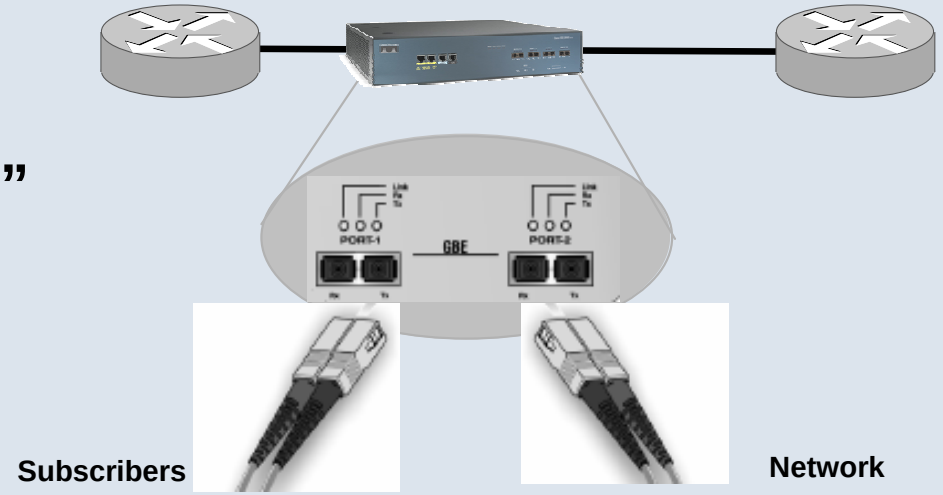
  Solo monitoraggio del traffico



- **Configurazione Inline**

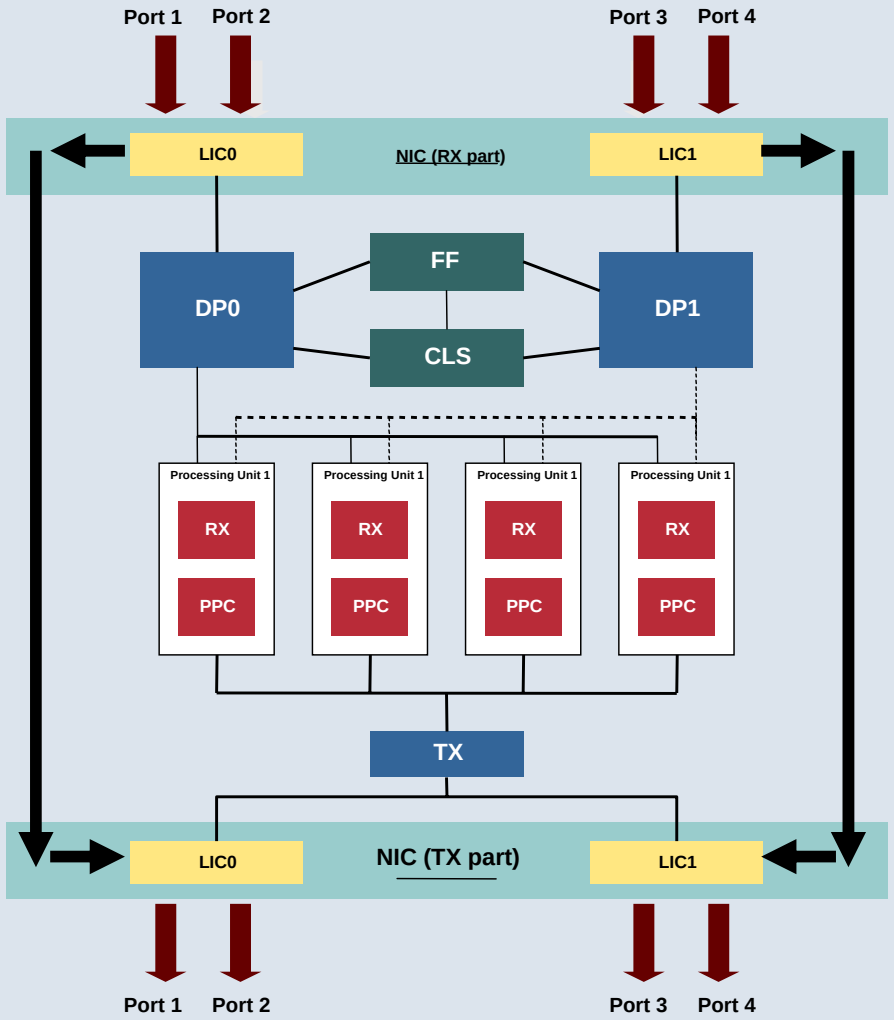
  Engine installato nel “data-path”

  Monitoraggio e controllo del traffico



Deployment
Service Engine Bypass

- **Hardware bypass interno**
- **Converte l'apparato in un "filo"**
  - **Bypass per ogni SCE 'monopath'**
- **Test Watchdog per problemi HW/SW**
- **Modalità configurabile**
  - **Fail Closed = Cut link on failure**
  - **Fail Opened = Bypass traffic on failure**
- **Differenti configurazioni si applicano a differenti topologie**

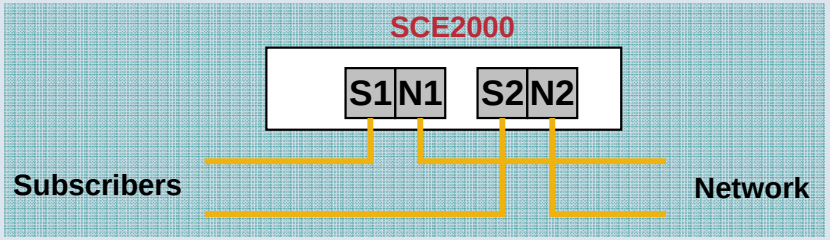


**** Optical bypass esterni disponibili per ovviare a problemi di alimentazione***

© 2004 Cisco Systems, Inc. All rights reserved.

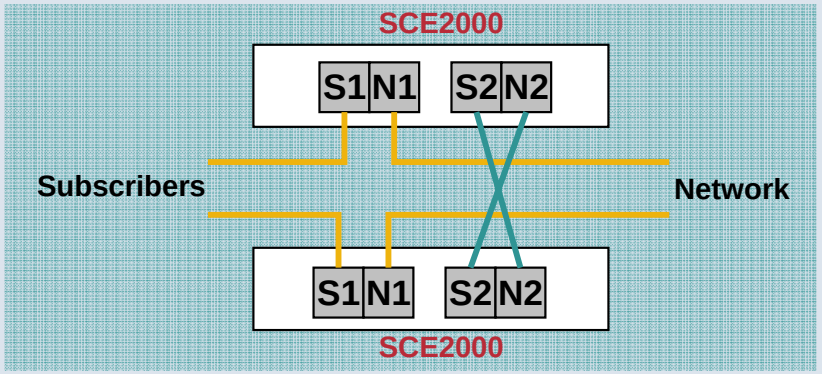
Deployment
Topologie trasparenti

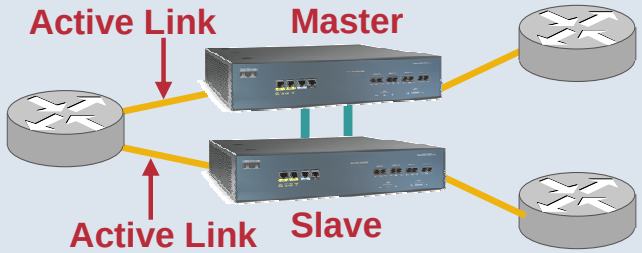
- **Due Monopath**
  - **Singolo SCE2000 su 2 link**
  - **Bypass config: Fail Closed**





- **Asimmetrico 1+1**
  - **Active/Active. SCE su ogni link**
  - **SCE2000 cascade risolve problema routing asimmetrico**
  - **Bypass config: Fail Open**





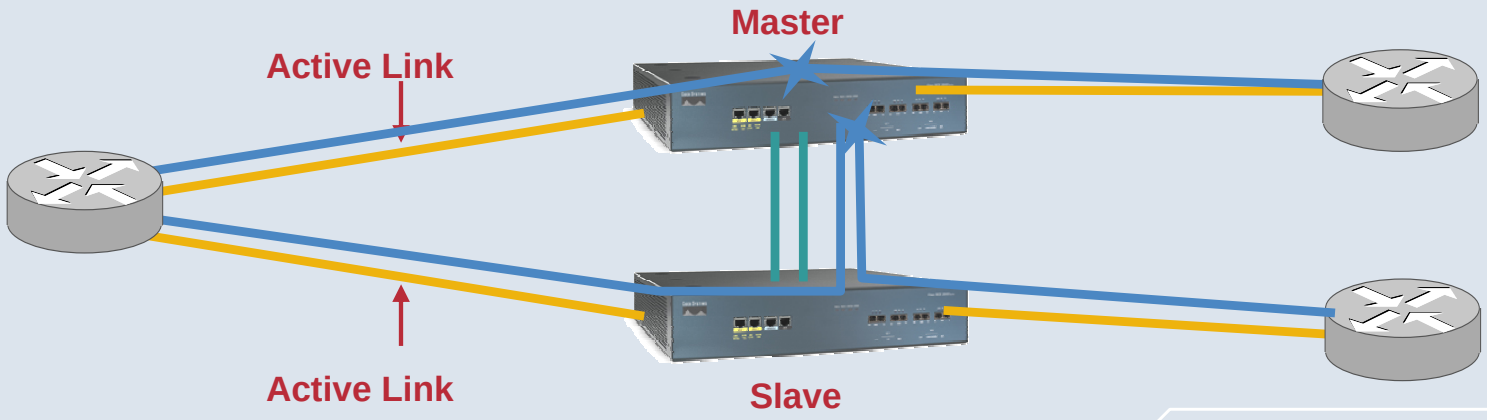
Deployment
SCE2000 “Cascade” per Alta Affidabilità

- **Risolve problema split flow tra due link**
- **La funzionalità SCE2000 cascade assicura la consistenza dei flussi**

  Slave inoltra tutto il traffico al Master per il processo dei dati

  Master aggiorna lo Slave con informazioni sullo Stato/regole per utente

  I ruoli cambiano in caso di problema sul percorso primario

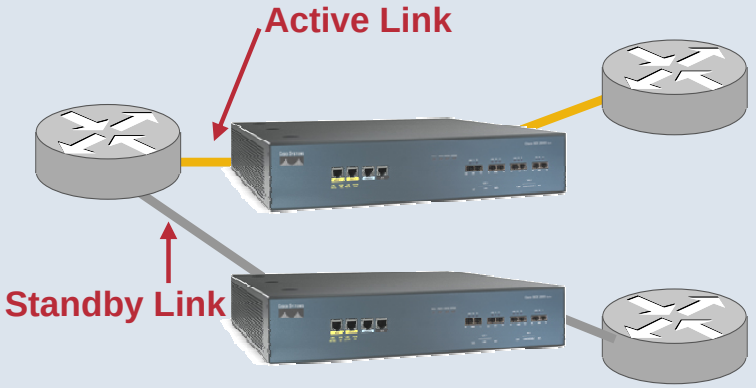


Active / Standby Schemes

- **1+0 (SCE1000, SCE2000)**
  - Active/Standby. SCE sul link attivo
  - In caso di problema, la rete utilizza il percorso alternativo
  - No ridondanza di servizio
  - Bypass config: Fail opened



- **1+1 (SCE1000, SCE2000)**
  - Active/Standby. SCE su ogni link
  - In caso di problema, la rete utilizza il percorso alternativo
  - SCE in Standby riprende il servizio
  - Bypass config: Fail opened



© 2004 Cisco Systems, Inc. All rights reserved.

Gestione e Integrazione

	Network Management	Configurazione Policy/Servizi	Gestione Utente	Raccolta Dati
Descrizione	FCAPS	Definizione di policy e propagazione agli apparati SCE	Gestione dinamica dei contesti utente	Raccolta dati di utilizzo per report e addebito
Protocolli e Tool	SNMP, CLI, SSH	SC-API GUI, Scripts XML	SM API Radius	RDR-Protocol
Moduli Software Esterni	N/A	Service Control Application Suite GUI	Subscriber Manager	Collection Manager

© 2004 Cisco Systems, Inc. All rights reserved.

Collection Manager

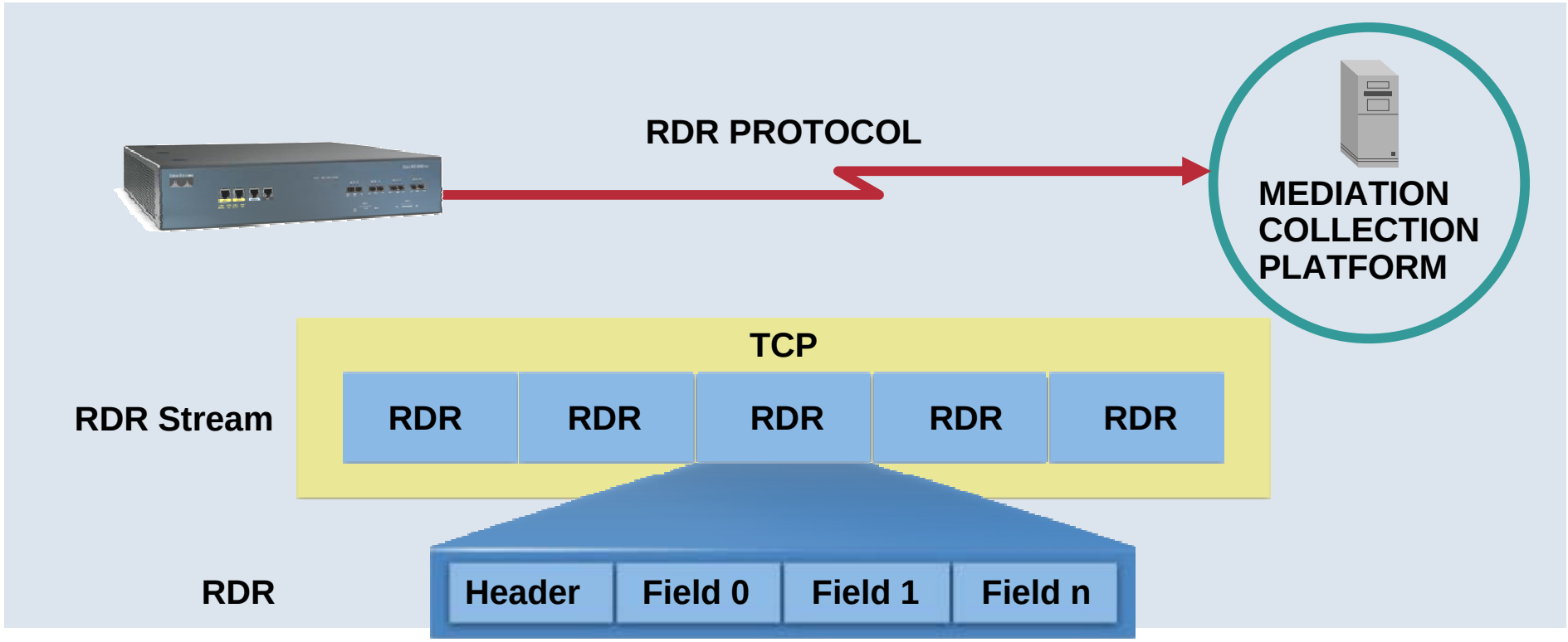
- **Le funzioni di analisi e processo dei dati dell’ SCE producono i Raw Data Records (RDRs)**
- **RDR sono inviati al “Collection Manager” dove sono elaborati**
  - **Cisco Collection Manager**
  - **Third party**
- **Granularità dei dati configurabile**
  - **Intervallo tra RDR**
  - **Parametri di campionamento**



© 2004 Cisco Systems, Inc. All rights reserved.

Collection Manager—RDR Protocol

- I dati sull'utilizzo sono inviati dall'apparato tramite il protocollo RDR
  - TCP, codificato in binario
  - Supporto di multiple destinazioni, failover
- RDR-Protocol integrato direttamente in sistemi di terze parti
  - Policy-Control, Mediation, Home grown customer



© 2004 Cisco Systems, Inc. All rights reserved.

Collection Manager Software

- **CM-Software**

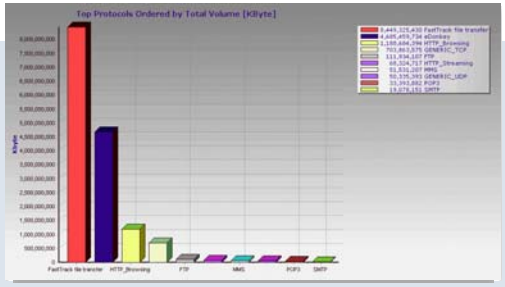
  Unix (Solaris, Linux) Java software

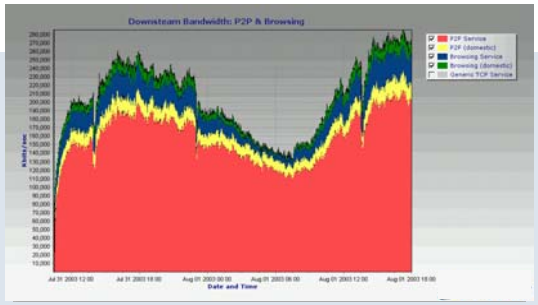
  Collection software memorizza I dati in qualsiasi database JDBC

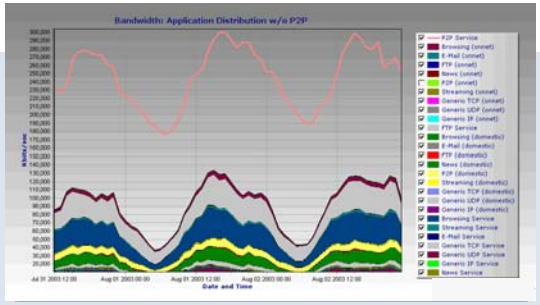
  Qualsiasi strumento di report di terze parti può essere usato per interrogare il DB e generare report

- **CM-Bundle**

  Cisco offre una versione software pre-pacchettizata con un DB (Sybase) e Reporting tool (con 50 report)







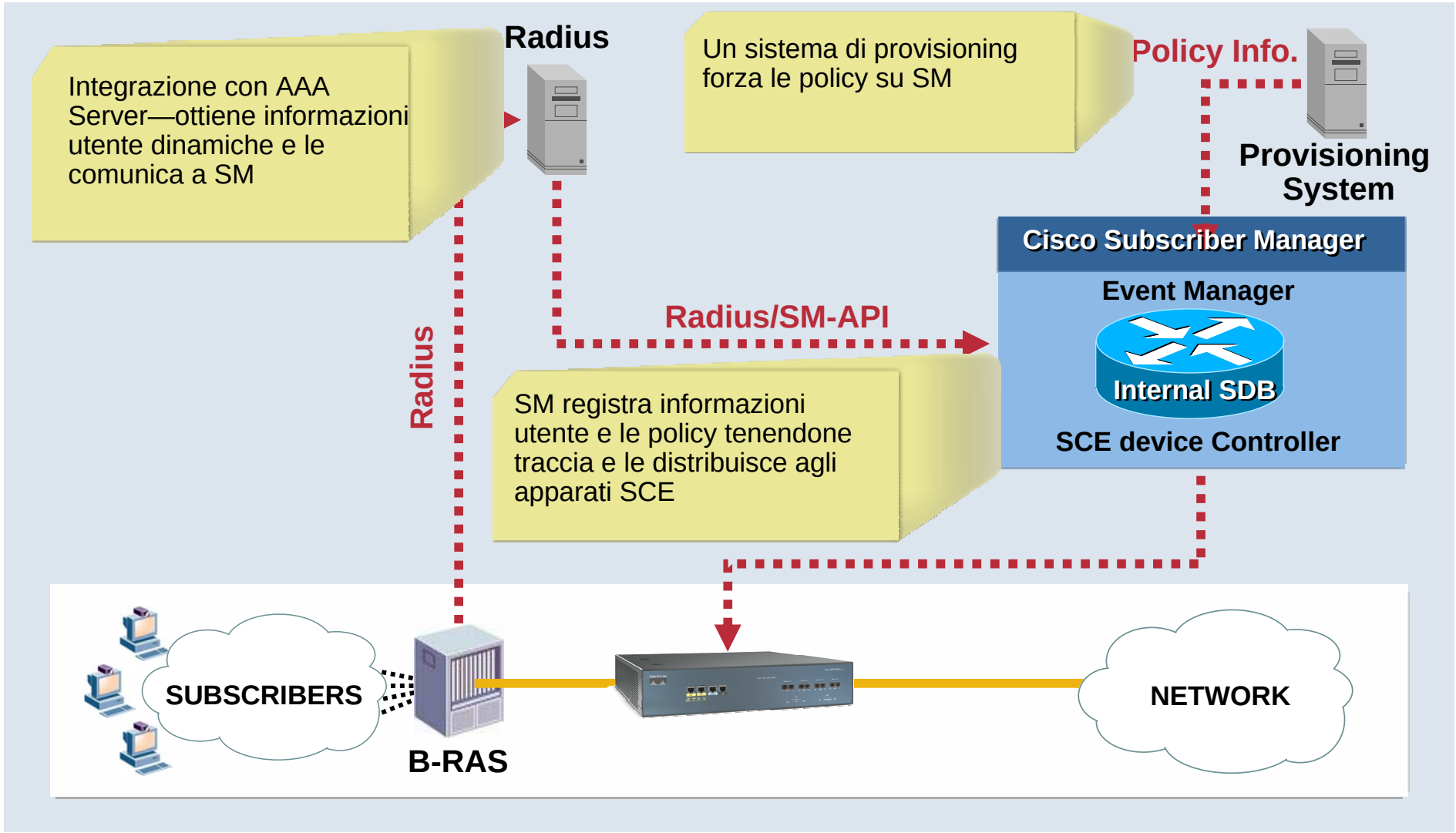
Subscriber Management

- Soluzione “Subscriber-aware”
- Gestisce Contesti-Utente
  - Subscriber-ID
  - Network-ID
  - Policy-ID
  - Subscriber-quotas
- Integrazione back-office/AAA
  - Radius AAA
  - Policy Control Systems (Tazz Networks)
- Cisco Subscriber Manager (CSM) serve come punto di integrazione



© 2004 Cisco Systems, Inc. All rights reserved.

Subscriber Manager



© 2004 Cisco Systems, Inc. All rights reserved.

Sommario

- La rete evolve e può includere maggiore “intelligenza” per l’abilitazione e il controllo di servizi
- No impatto sulle prestazioni
- Integrazione con realtà esistente
- Capacità di :
  - Analisi
    Identificazione utenti / applicazioni / profili
  - Controllo
    Garanzia apps Mission Critical /Limite abusi /identificazione traffico anomalo
  - Report
    Report dettagliati per utente / applicazione / sessione

© 2004 Cisco Systems, Inc. All rights reserved.



© 2004 Cisco Systems, Inc. All rights reserved.