Cisco Networkers 2009
January 26-29 Barcelona, Spain

NGN Service Interconnect and SIP Trunking Architectures and Scenarios

BRKBBA-2015

Mark Rankin

Maurice Duault

Housekeeping

- We value your feedback- don't forget to complete your online session evaluations after each session & complete the Overall Conference Evaluation which will be available online from Thursday
- Visit the World of Solutions
- Please remember this is a 'non-smoking' venue!
- Please switch off your mobile phones
- Please make use of the recycling bins provided
- Please remember to wear your badge at all times including the Party

Abstract

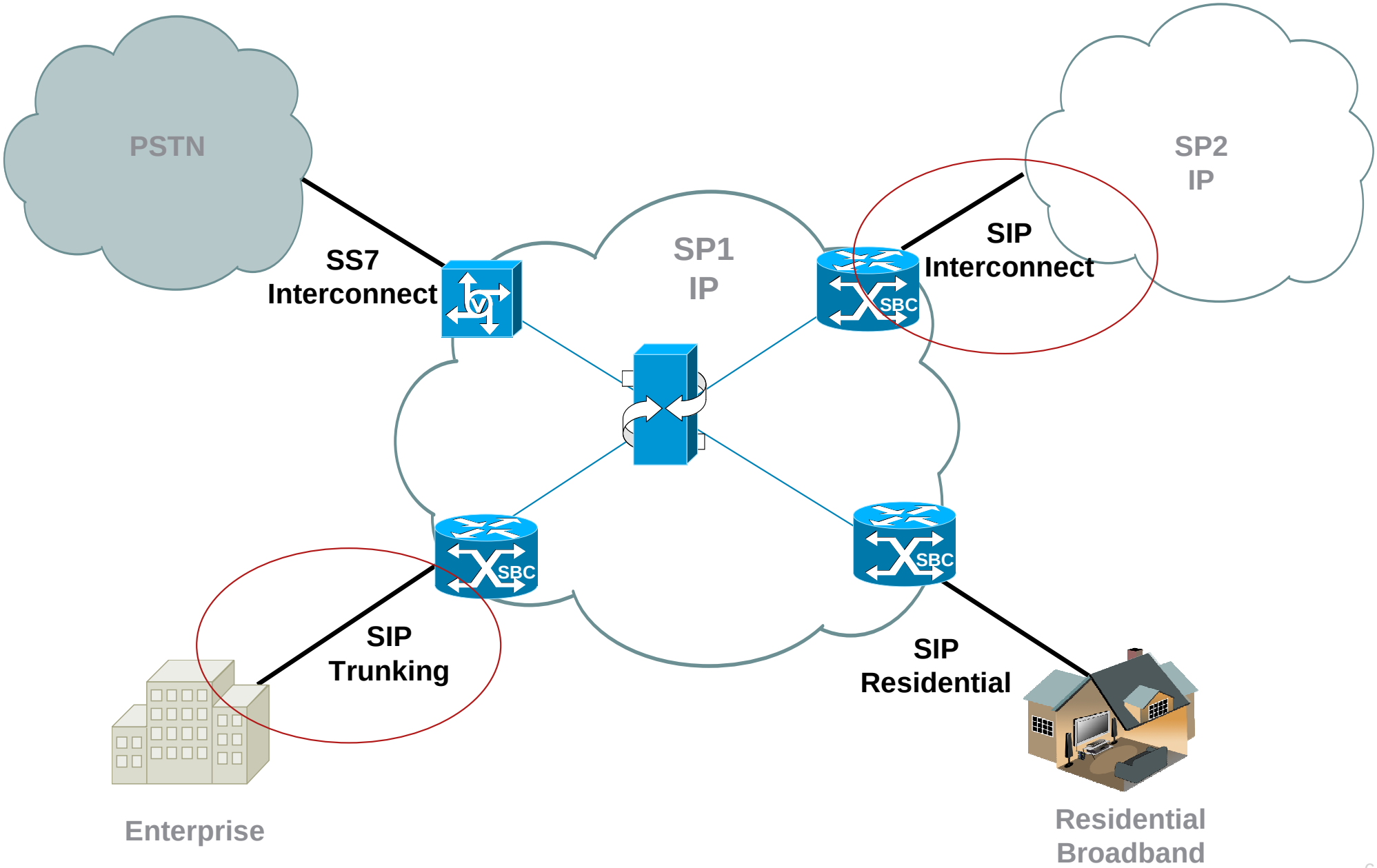
“This intermediate session is aimed mainly at service providers, applications service providers, (and) partners and integrators who deal with service providers. As more and more end users are migrating to Voice over IP and Multimedia over IP services both in the enterprise and consumer space traditional TDM based UNI (User Network Interface) and NNI (Network Network Interface) connectivity models become more and more impractical, not least due to the fact that they limit potential service offerings. There is a general trend in the industry, backed by national and international standards and industry bodies, to move toward native IP interconnectivity for all services. This INTERMEDIATE session will cover two important aspects of the move towards IP based service interconnects - The move towards a "SIP" Trunk for enterprise/SMB connectivity replacing the traditional BRI/PRI and the move to native IP peering replacing the traditional SS7/C7 interface. This session will cover the various standards involved in each of these (SIP Connect, IMS/TISPAN, IPX etc), market trends, use cases and the relevant Cisco solutions. This session is technical in nature and will cover technologies such as Session Border Controllers, Softswiches, Routing platforms, etc and will deal with key fundamental concepts around how protocols such as SIP, ENUM, SCTP and H.323 will be used to provide reachability information and transport service information. (Key technologies covered will include Session Border Controllers (SBCs), Call Servers/Softswitches, routing engines and the session will focus mainly on SIP as an underlying service protocol but will also touch upon the use of ENUM, SCTP and H.323.) “

Agenda

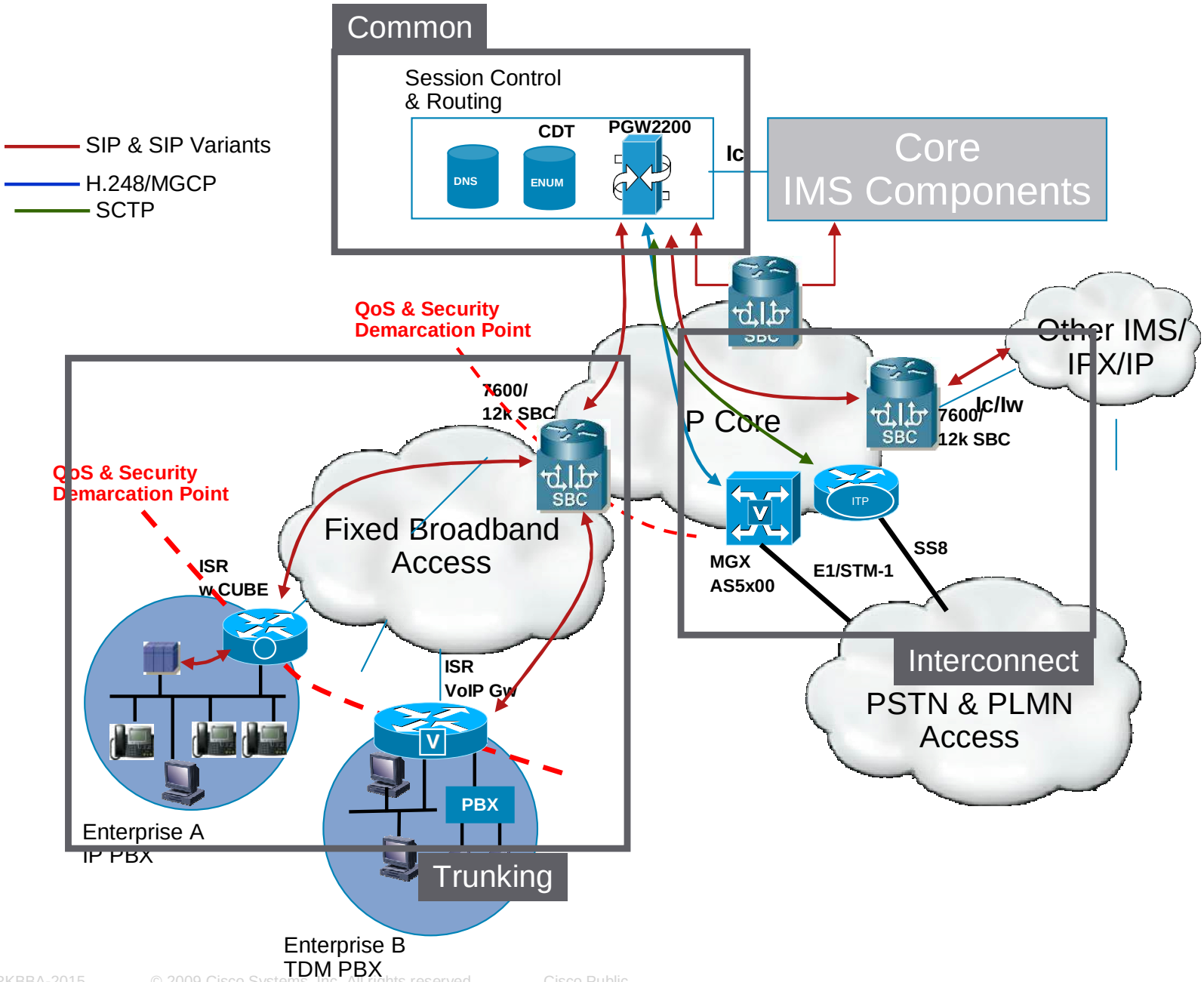
- Introduction
- SIP Trunking
  - Market Dynamics
  - Standards
  - Architecture & Deployment Scenarios
- NGN Interconnect
  - Market Dynamics
  - Standards
  - Interconnect Architecture & Key Attributes
- Summary

Introduction

What Is SIP Trunking & Interconnect



Architectural Diagram



Session Border Controller platforms

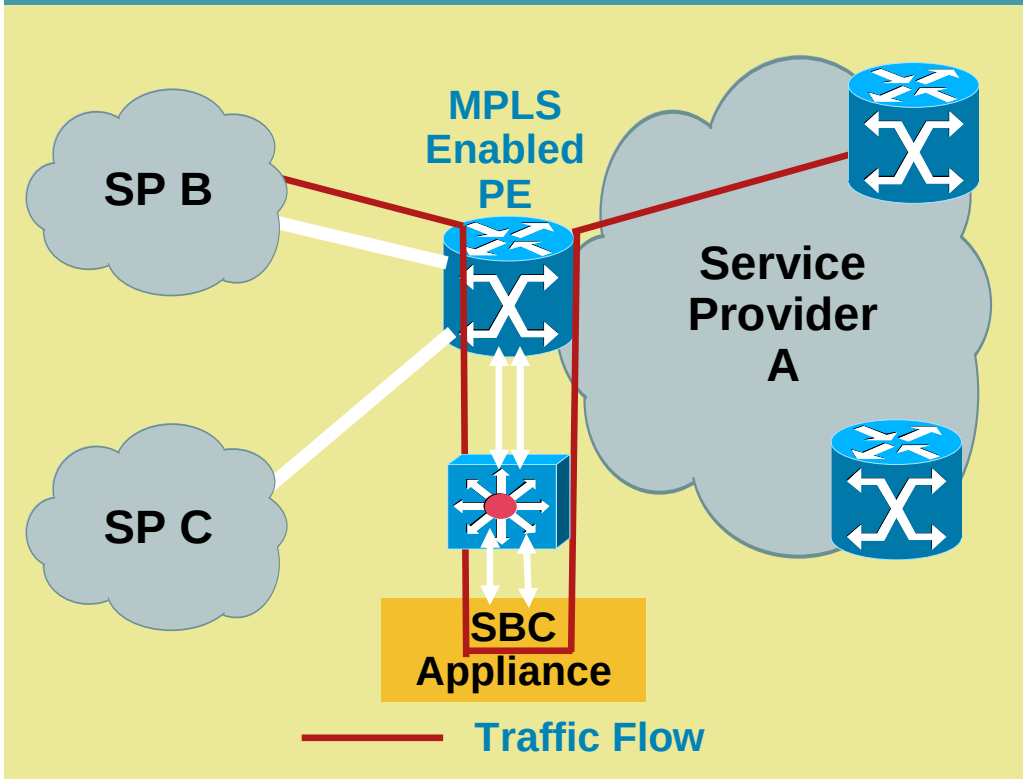
- GSR XR composed SBC
- 20K sessions per MSB card
- 300K sessions per chassis

- 7600 composed SBC
- 8K sessions per ACE card
- 120K sessions per chassis.

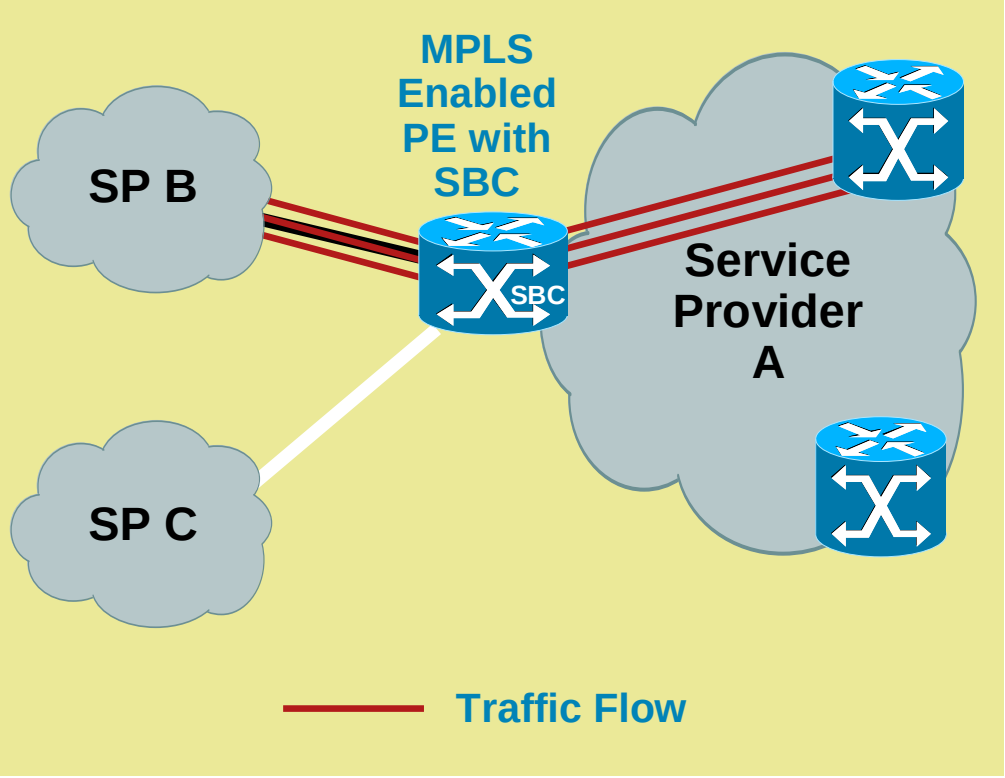
- ASR DBE
- Up to 32K sessions with RP1 & ESP10 Combination
- No additional card

What are the benefits for the Integrated SBC solution?

Appliance Based SBC Solution



Cisco's Integrated SBC Solution



- Seamless integration
- Eliminate overlay networks
- Array of QoS and security features on ingress/egress interfaces
- Integration with other L2/L3 services (eg: MPLS PE + SBC, FW + SBC)

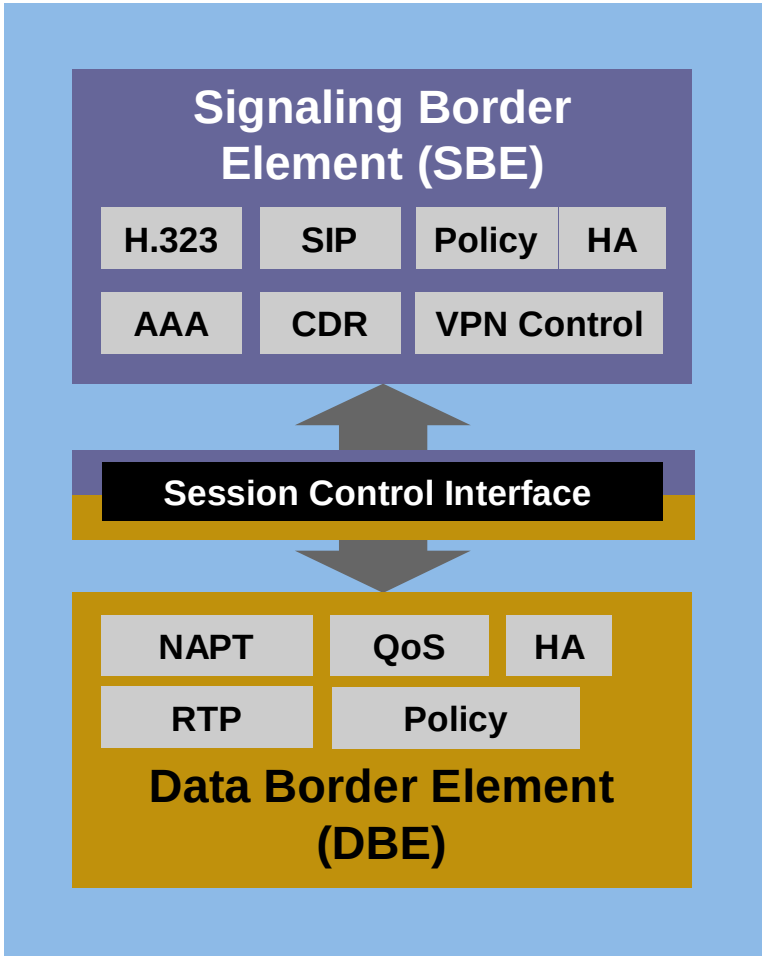
SBC Architecture Building Blocks

DBE = Data Border Element (Also Known as: Media Proxy)

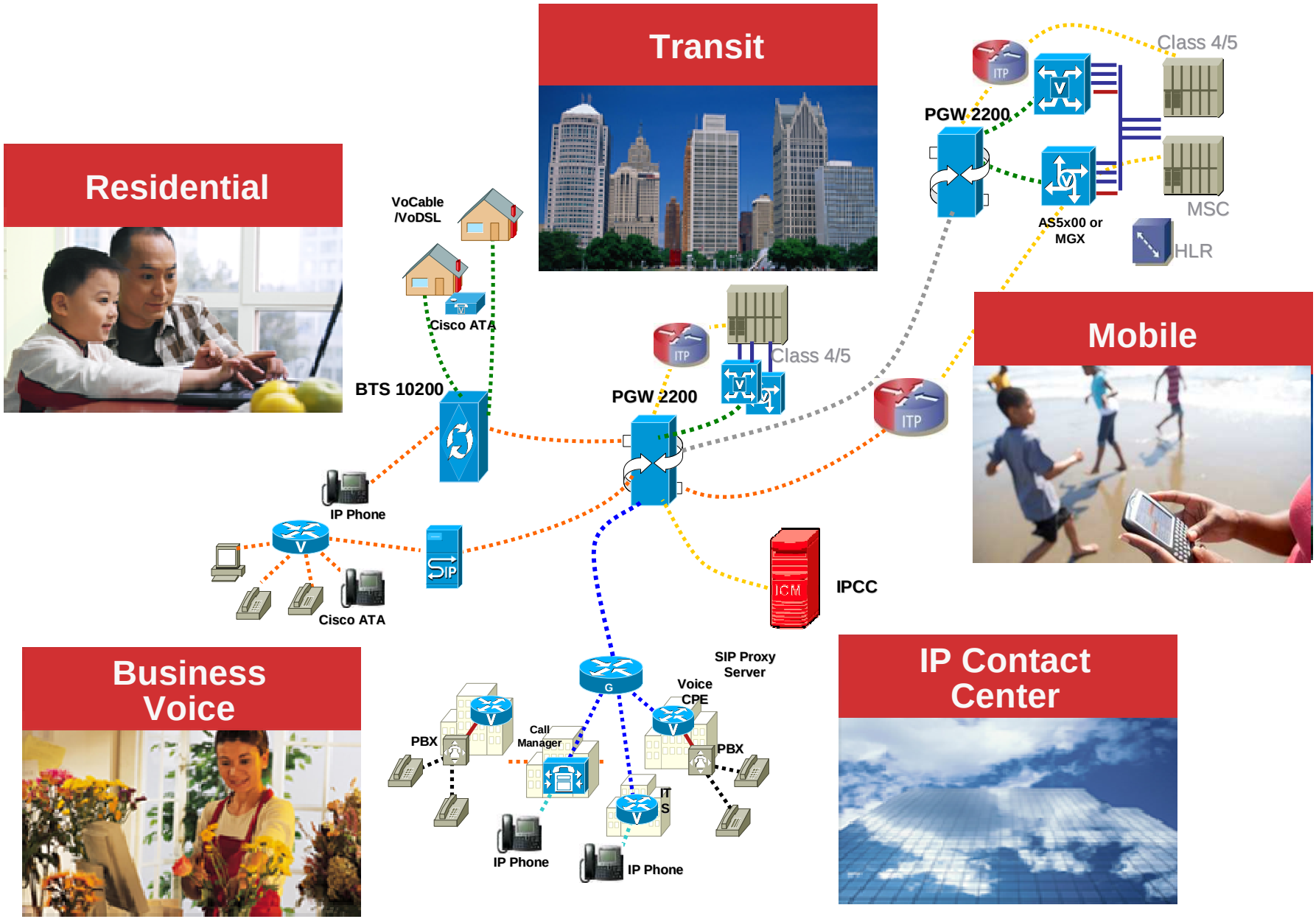
SBE = Signaling Border Element (Also Known as: Signaling Proxy)

- **Ground-up design for unified and distributed signaling deployment**
  - –Logical split into signaling and data border elements (SBE and DBE)
    - SBE handles all call processing (SIP, H.323, etc.)
    - DBE handles all media processing (RTP, RTCP, etc.)
  - **–Open industry standard (H.248) interface between the SBE and DBE**

SBC Architecture



PGW 2200 Softswitch Applications

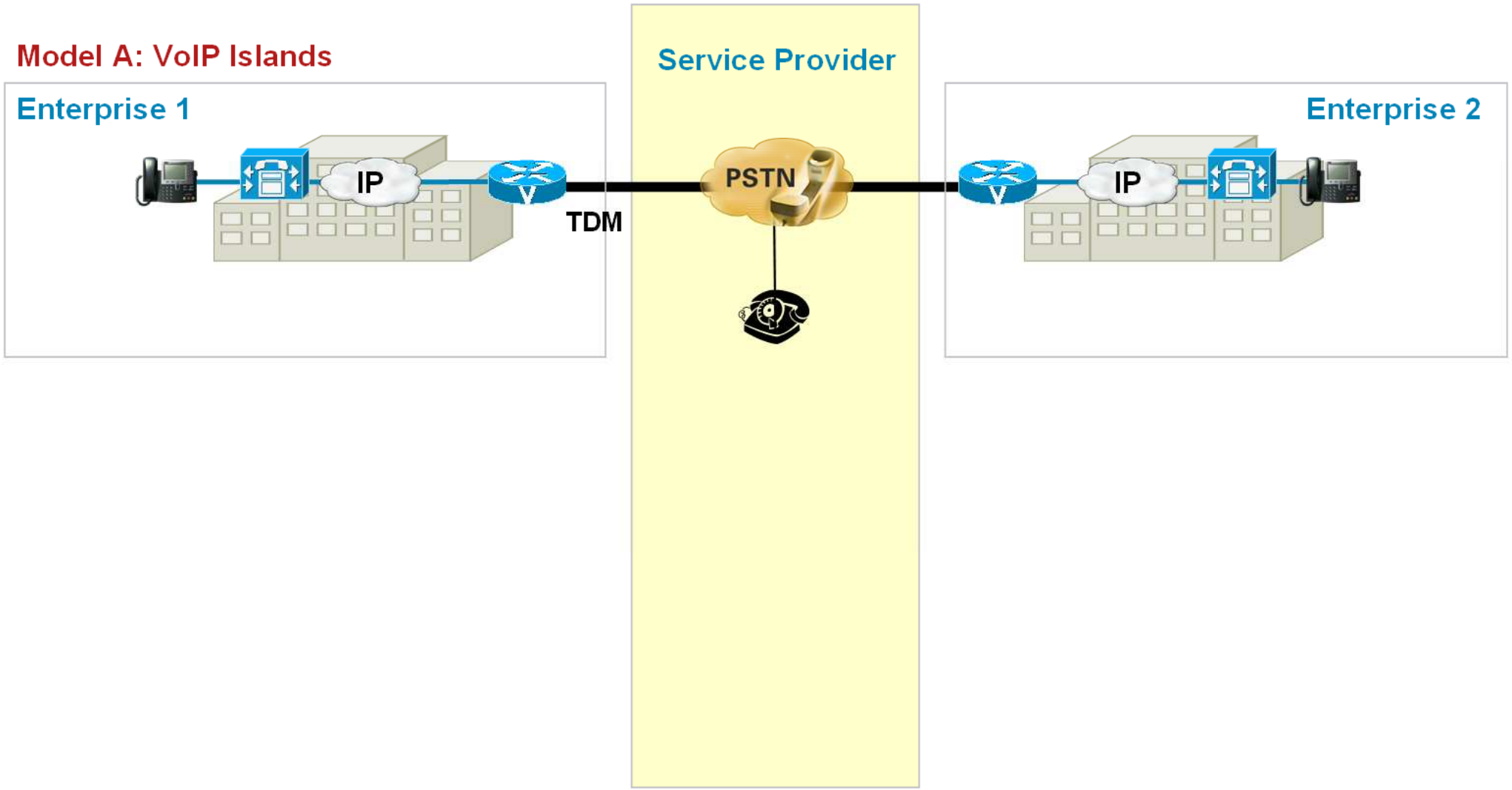


Cisco Networkers 2009
January 26-29 Barcelona, Spain

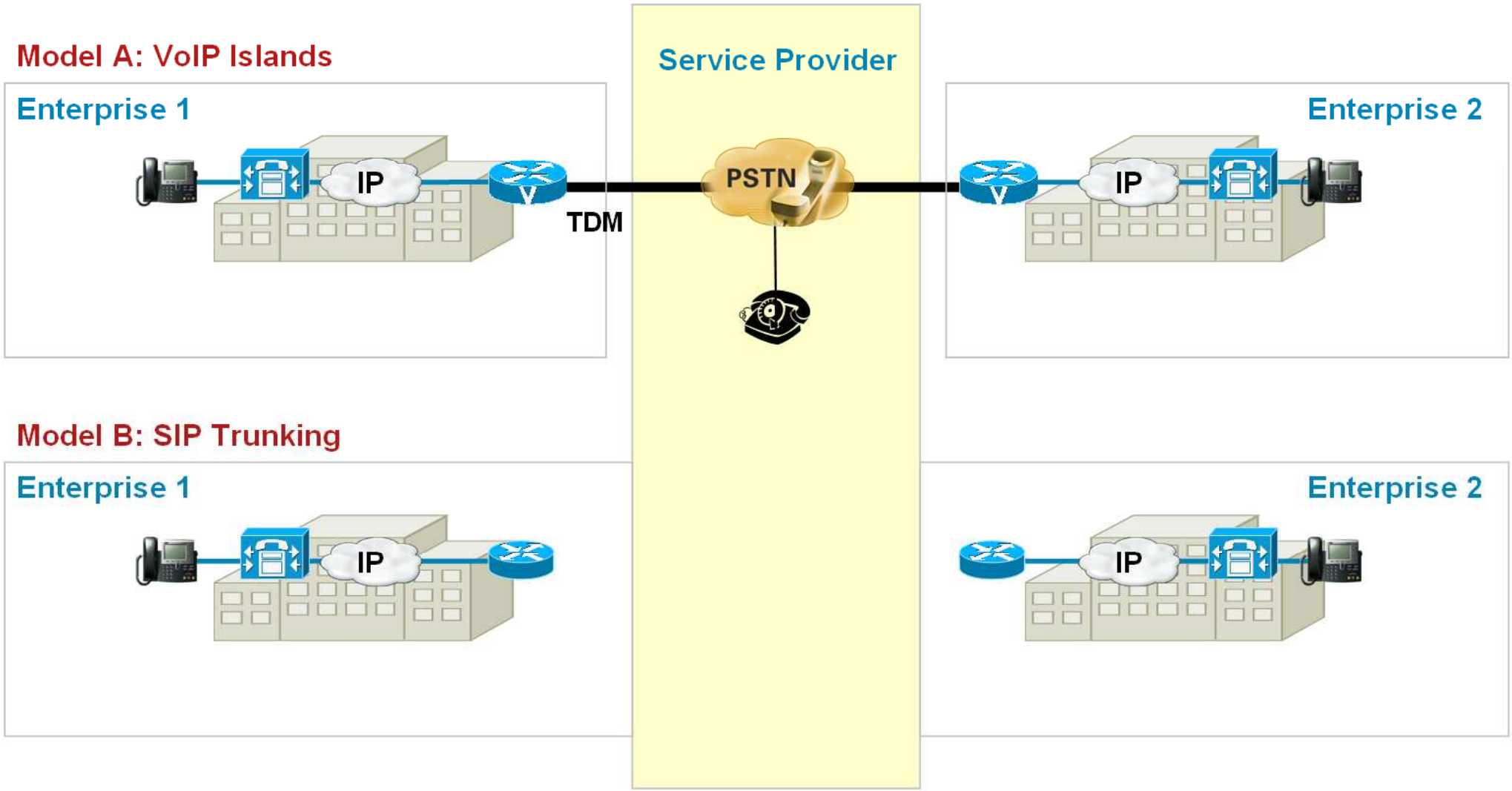
SIP Trunking

Market dynamics

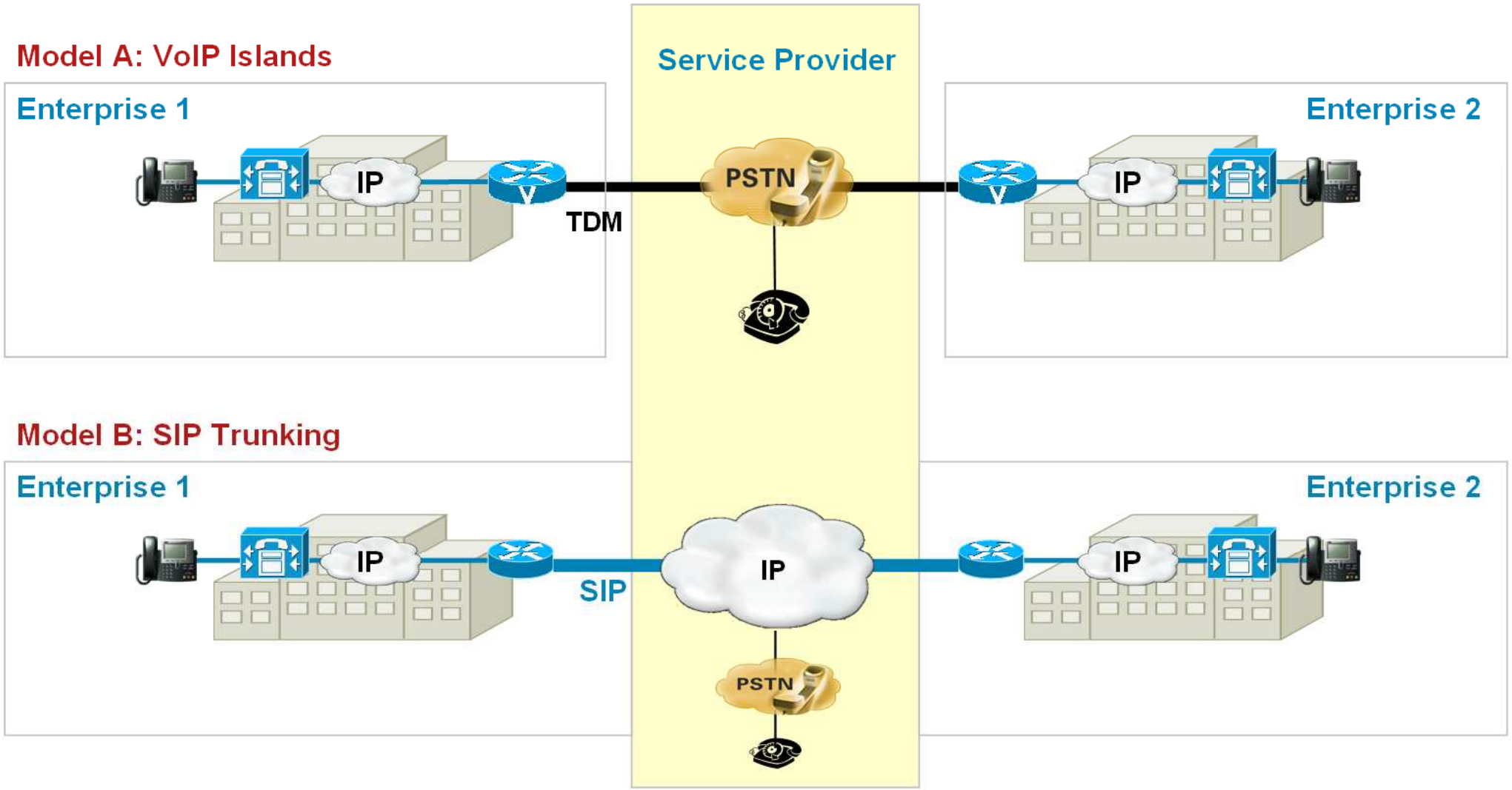
What is SIP trunking?



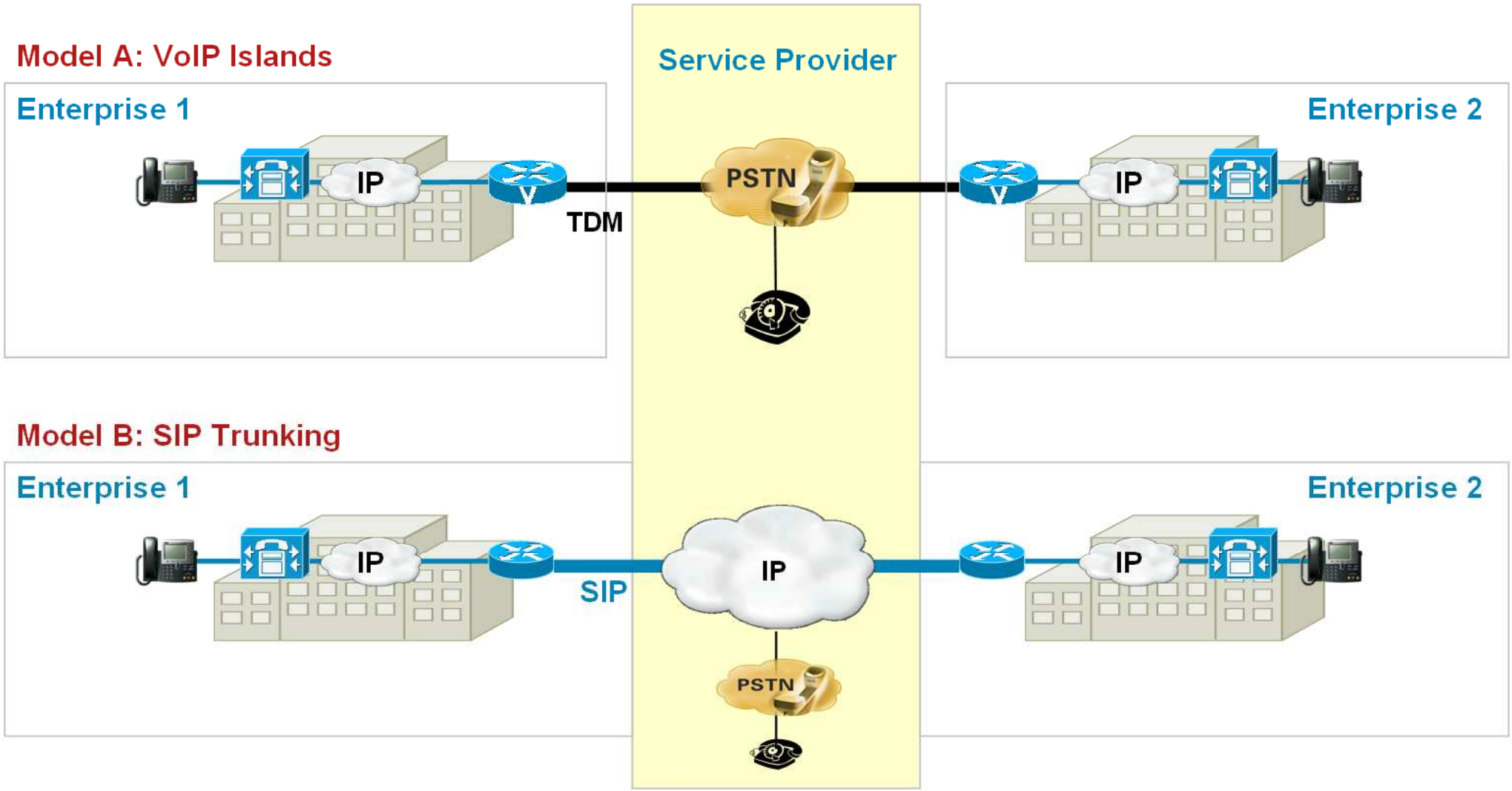
What is SIP trunking?



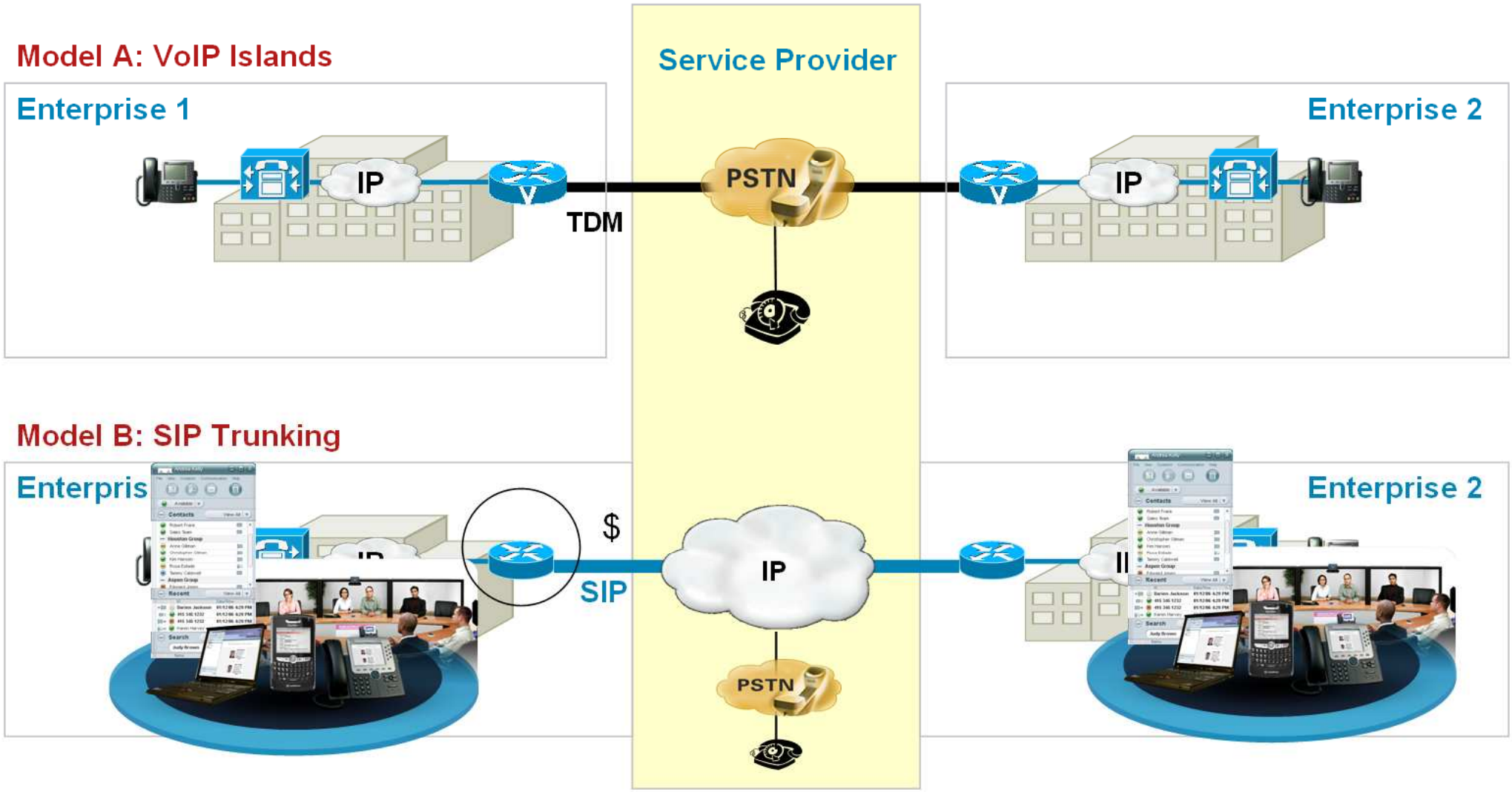
What is SIP trunking?



What is motivating enterprises?



What is motivating enterprises?



Spending less for more value

What is motivating Service Providers?

New players

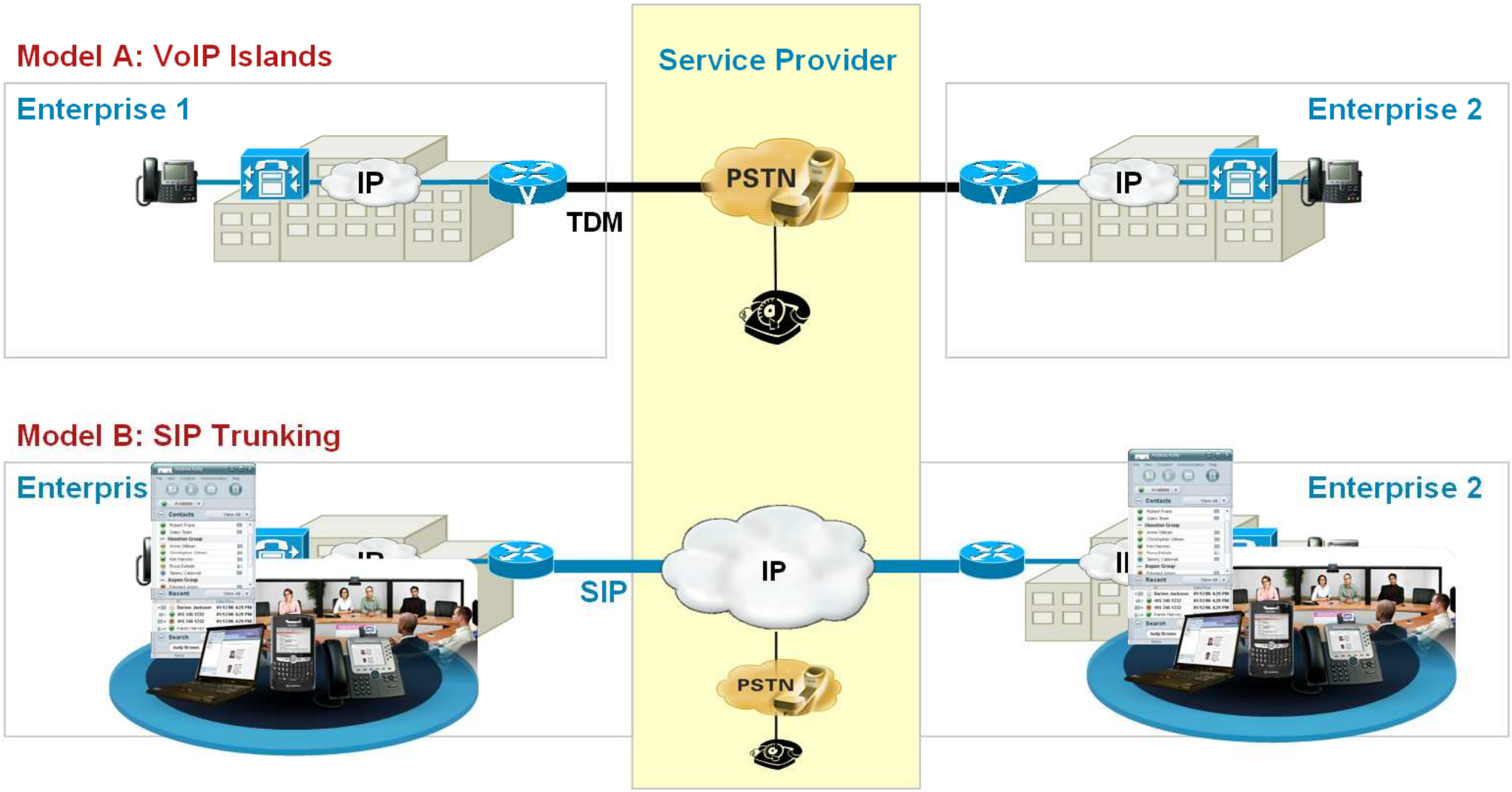
- Capture the business voice minutes revenue
- Expand managed data services with voice and multimedia services
- Enlarge geographic and global footprint

Incumbent

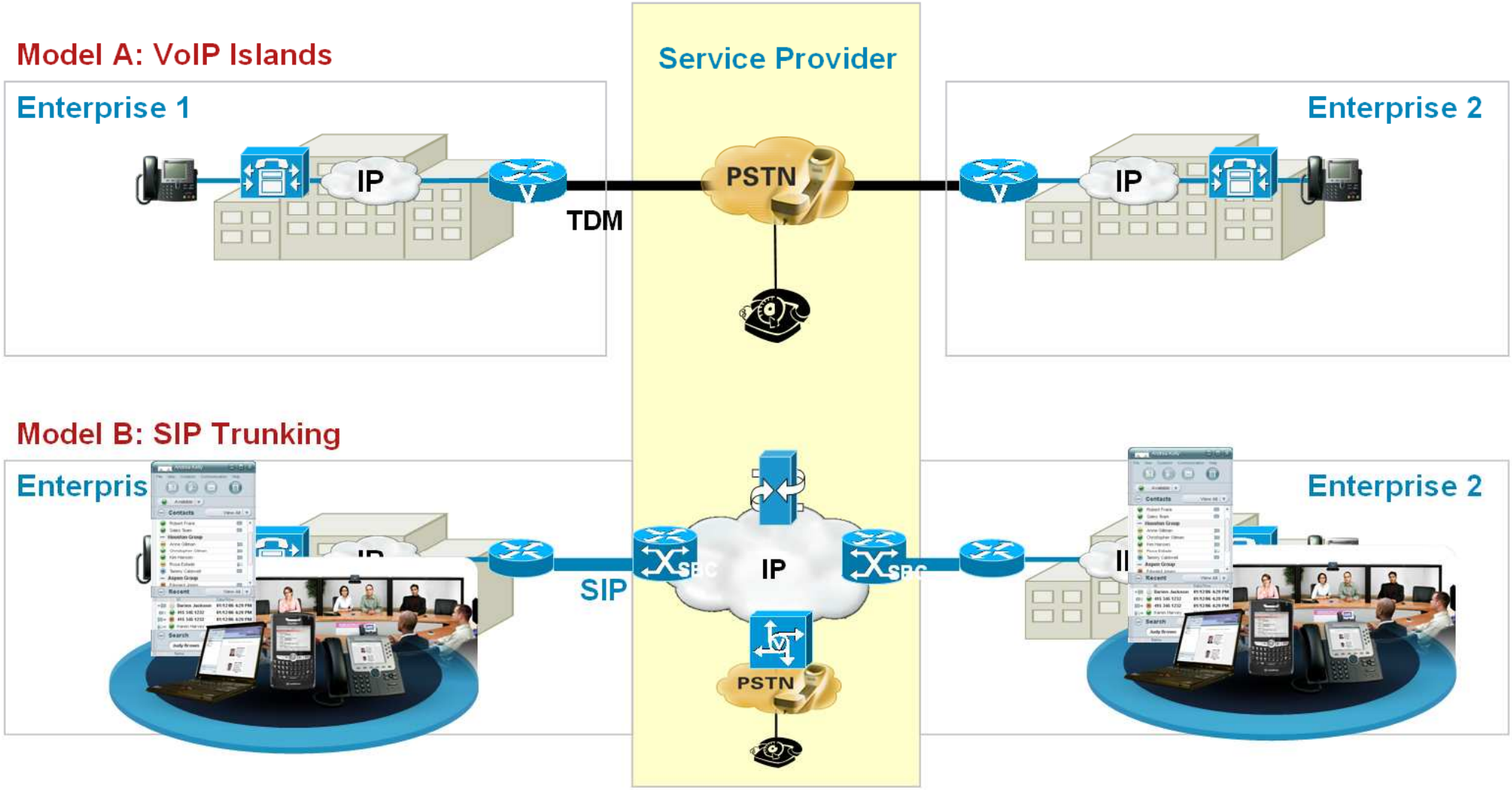
- Migrate current enterprise customer base
- Compensate the decrease of TDM revenue with new services
- Keep smaller competitors

Capture the transition from ISDN to SIP

Why did it take so long?



Why did it take so long?

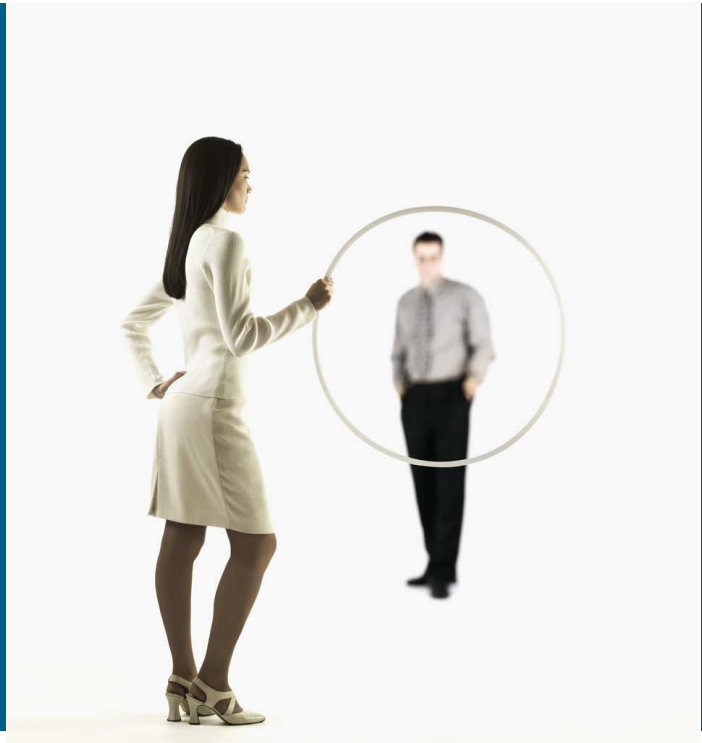


Interworking between domains is complex

Is SIP Trunking cheaper than ISDN?

Price of voice minutes	~ equal
Price per channel	~ equal
# channels needed	Less with centralization
# interfaces	Less (high speed converged with data)
Time to provision in SP network	Less
# devices in SP & enterprise network	Less
Other cost savings for enterprise	Pooling of DIDs, free BW for data, rich media…

SIP Trunking standards



Main standard organizations for SIP trunking

- IETF: SIP protocol
- ECMA: defines NGCN and UNI requirements
- SIP Forum SIP connect: defines very high level functional UNI. Published March 2006.
- ETSI TISPAN:

  -Specifies the NGN for fixed network operators.

  -Business Communications activity started in TISPAN R2 at beg. 2007

  -WG 1 specified Business Communications requirements (TS 181 019)

  -WG 2 specified Business Communication architecture:

  -Enterprise interactions scenarios (TS 182 023).

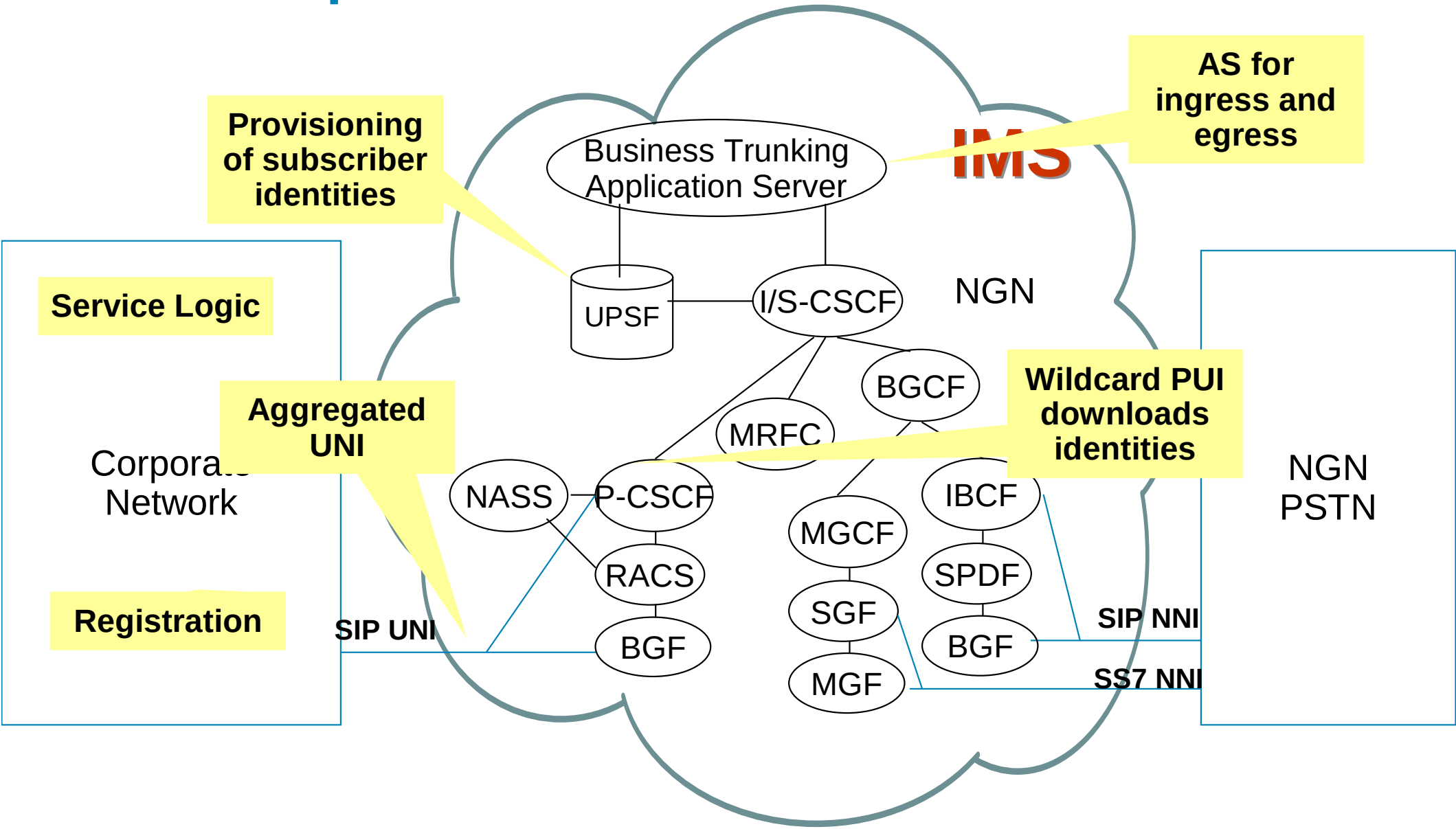
  -TISPAN Hosted Enterprise Services (TS 182 024)

  -TISPAN Business Trunking (TS 182 024)

2 models for ETSI TISPAN Business Trunking

	Subscription based	Peering based
IP PBX	Registration	No registration
Extends	Residential	Transit
Core functions	IMS and AS	Routing

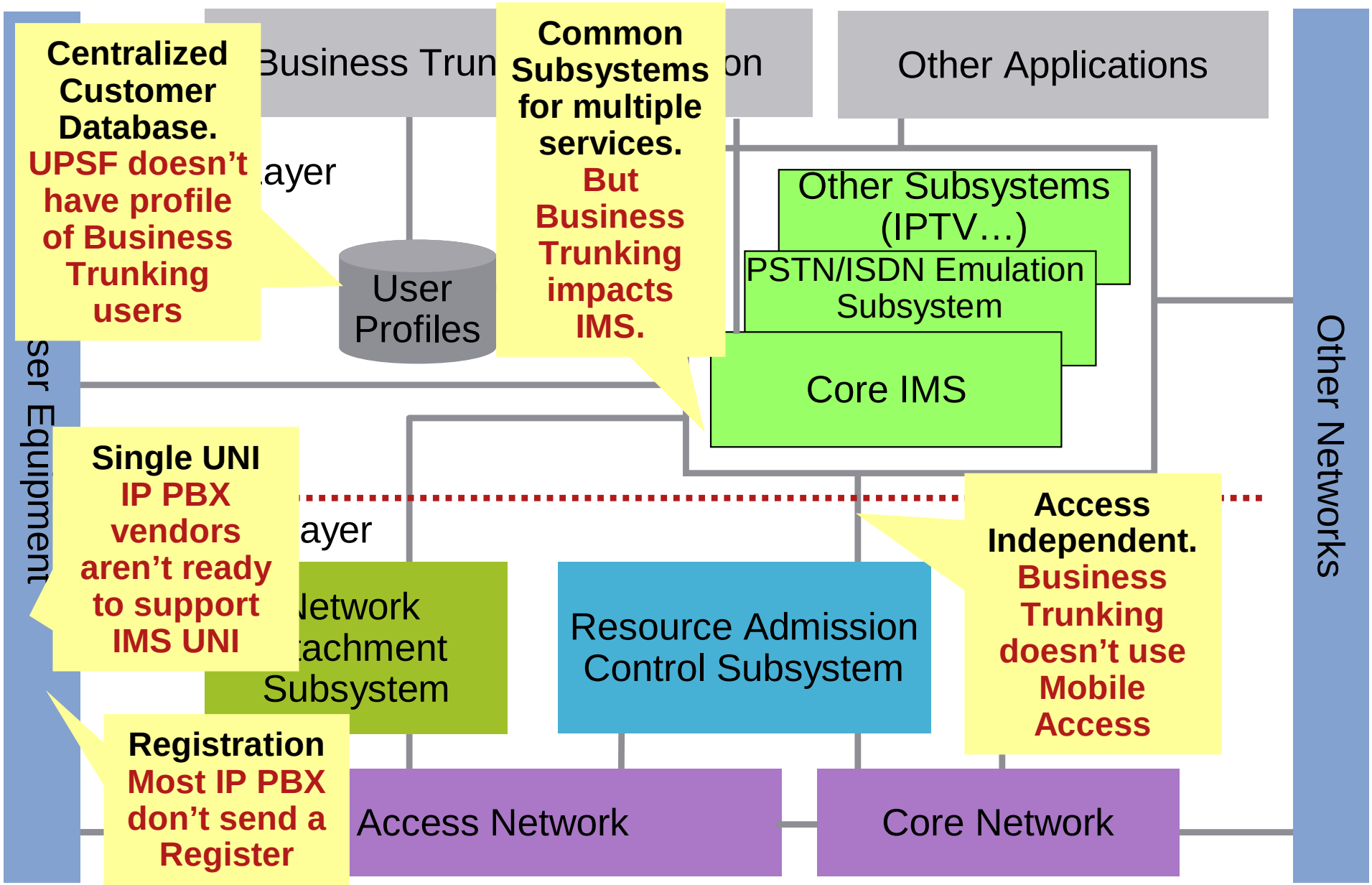
ETSI TISPAN Business Trunking Subscription Based architecture



Subscription based model characteristics

- Registration of NGCN site (surrogate registration out of scope)
- Identification of NGCN site with a private and public identity
- Implicit registration of NGCN users with wildcard Public User Identity (PUI) configured in UPSF and loaded in P-CSCF. Requires 3GPP R8 modifications.
- Insertion of Private-Network-Indicator header for break-in private network traffic
- Insertion of P-Asserted-Identity header based on P-Preferred Identity, P-Asserted-Identity or From header information
- Signaling transparency for private network traffic
- Emergency call: geolocation provided by the NGCN site or by the P-CSCF with P-Access-Network header
- Open issues: NAT traversal, impact on core IMS

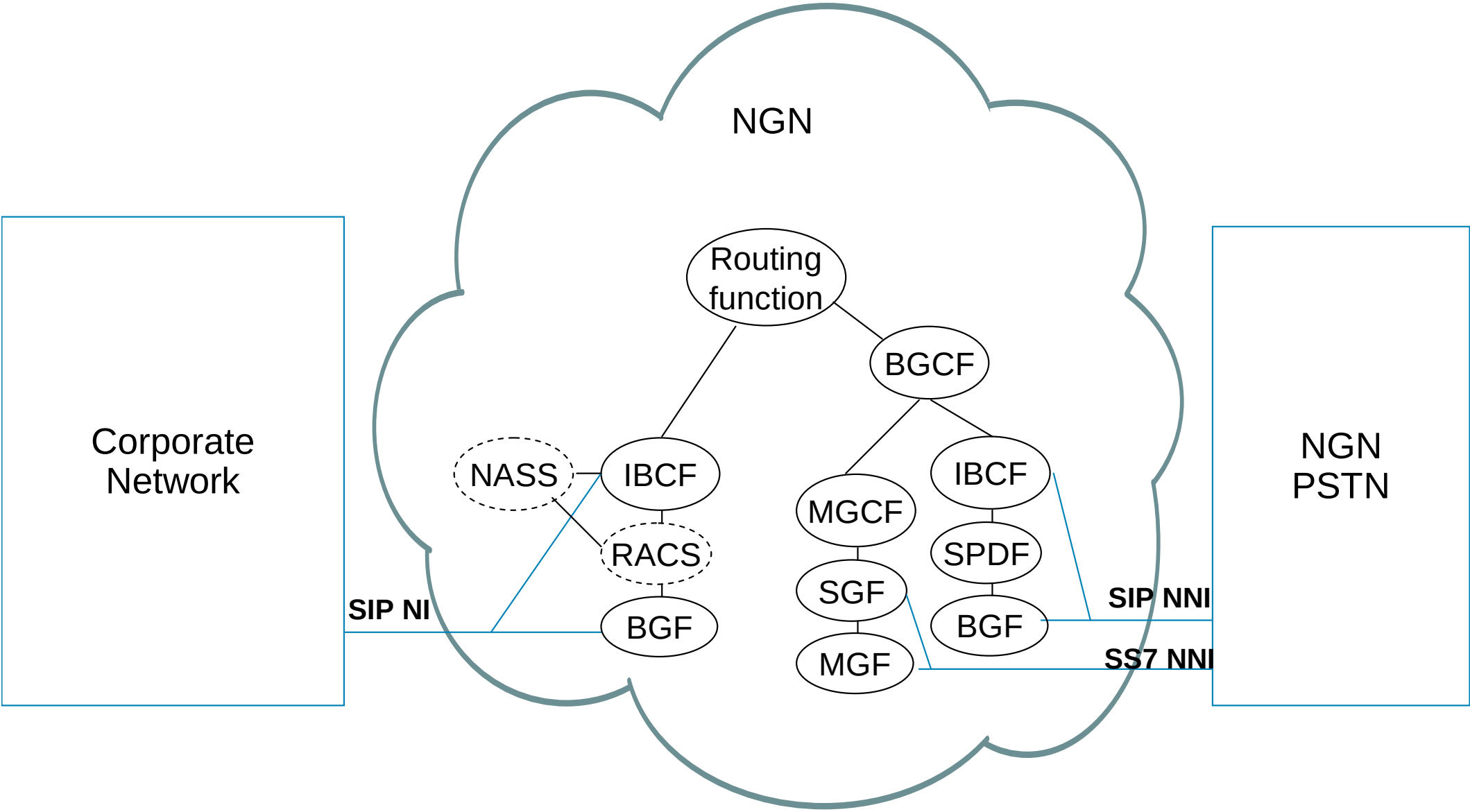
Do the drivers for TISPAN IMS subscription based model fit?



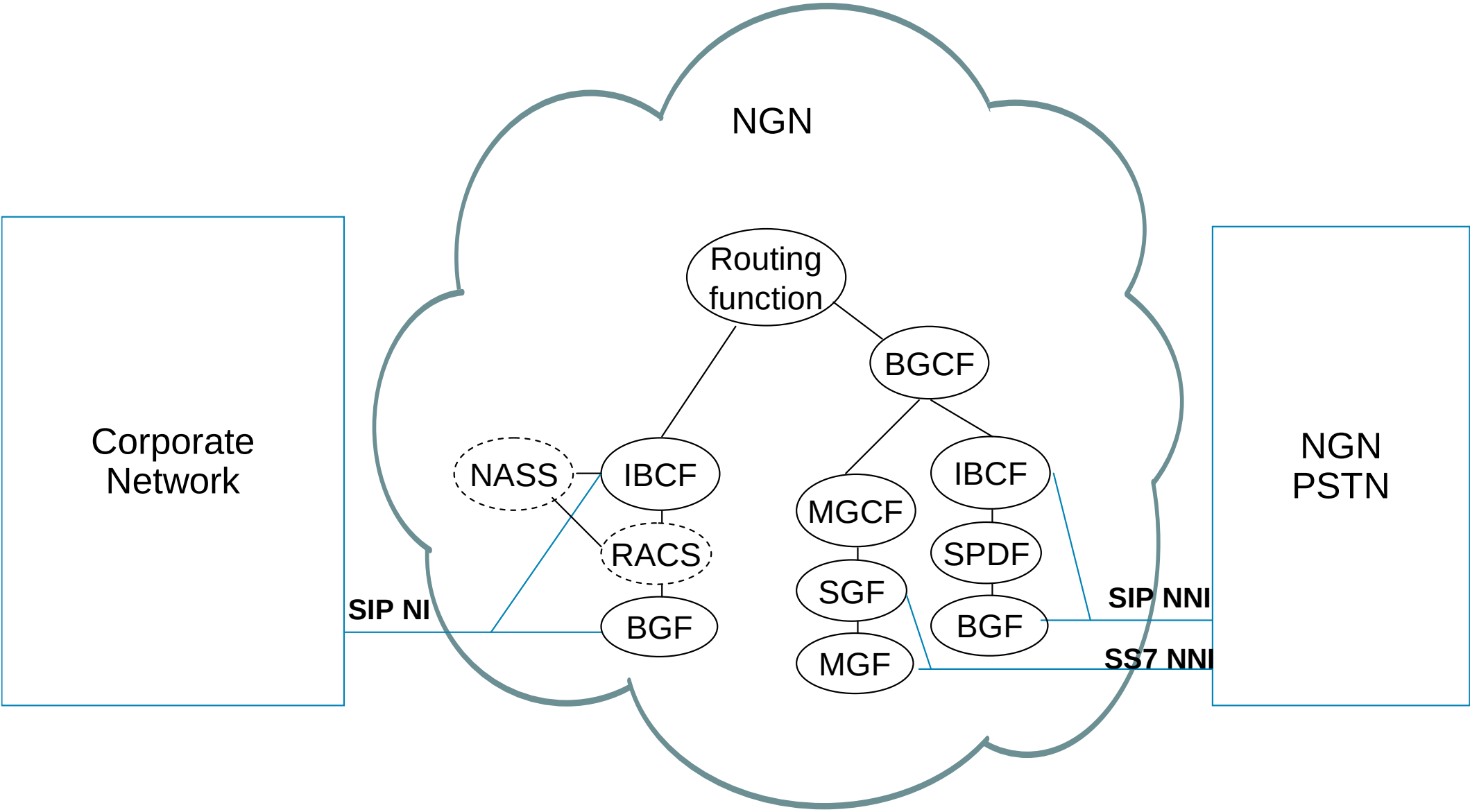
Is registration required?

- A small IP PBX (e.g. CUCME) may register:
  - -Behaves like a large phone with multiple lines
  - -Imbedded in mobile or wireless routers
- A large IP PBX (e.g. CUCM) does not and should not register:
  - -A trunk is a peer protocol
  - -Trunks groups (parallel trunks for 1 network attachment)
  - -Multiple network attachments to one NGN
  - -Multiple network attachments to multiple NGN
  - -SIP proxy between multiple IP PBX and the NGCN
- Other mechanisms must handle detection of link failure, NAT traversal, user identity validation and trunk selection with mobility

ETSI TISPAN Business Trunking Peering Based architecture



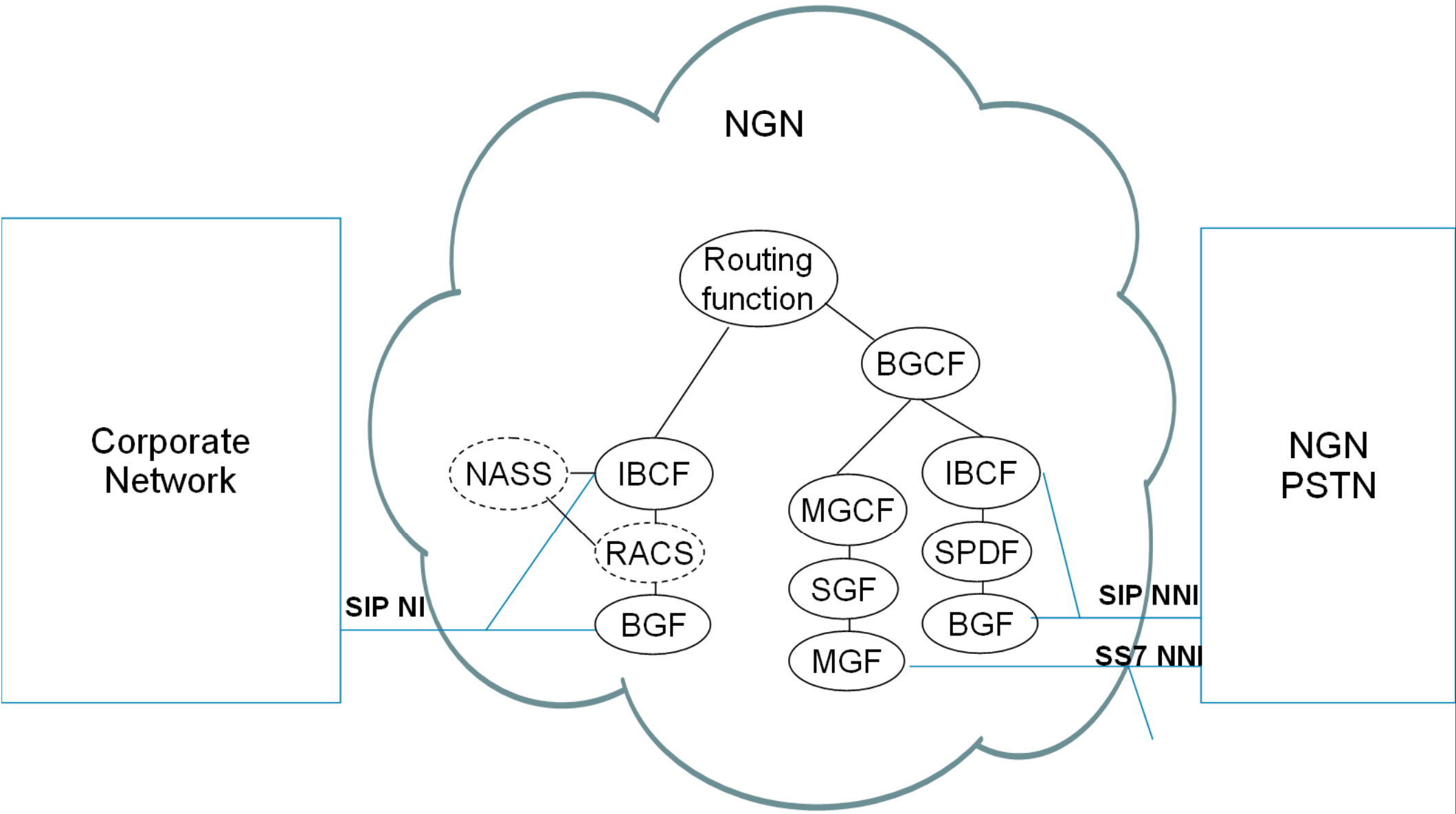
ETSI TISPAN Business Trunking Peering Based architecture



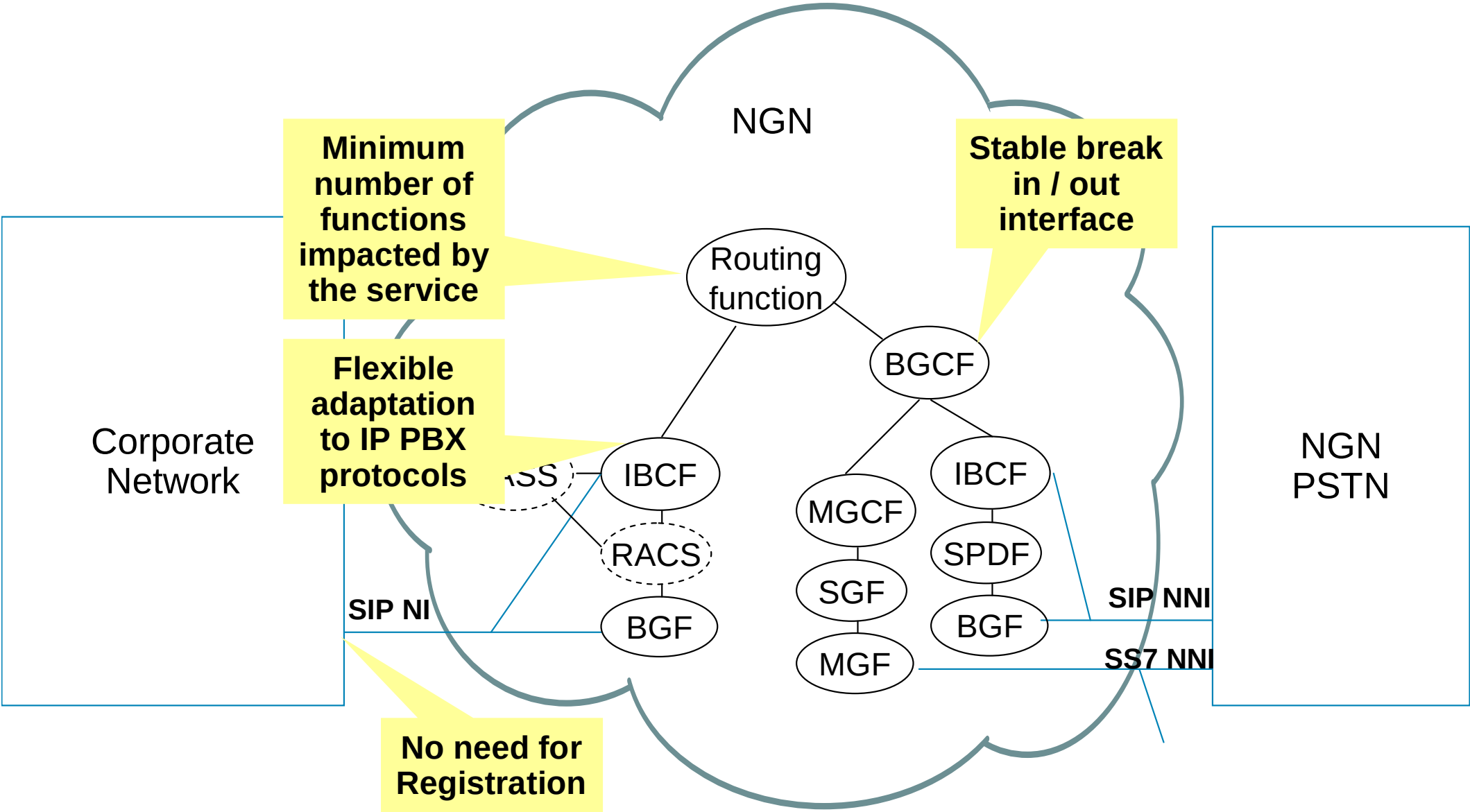
Peering based model characteristics

- No registration of NGCN site
- Business trunking application in the intelligent routing function
- Insertion of Private-Network-Indicator header for break-in private network traffic
- Insertion of a default identity in the P-Asserted-Identity header configured in the IBCF if there is an untrusted relationship between the NGN and NGCN
- Signaling transparency for private network traffic
- Emergency call: geolocation provided by the NGCN site
- Open issues: NAT traversal, charging, AoC

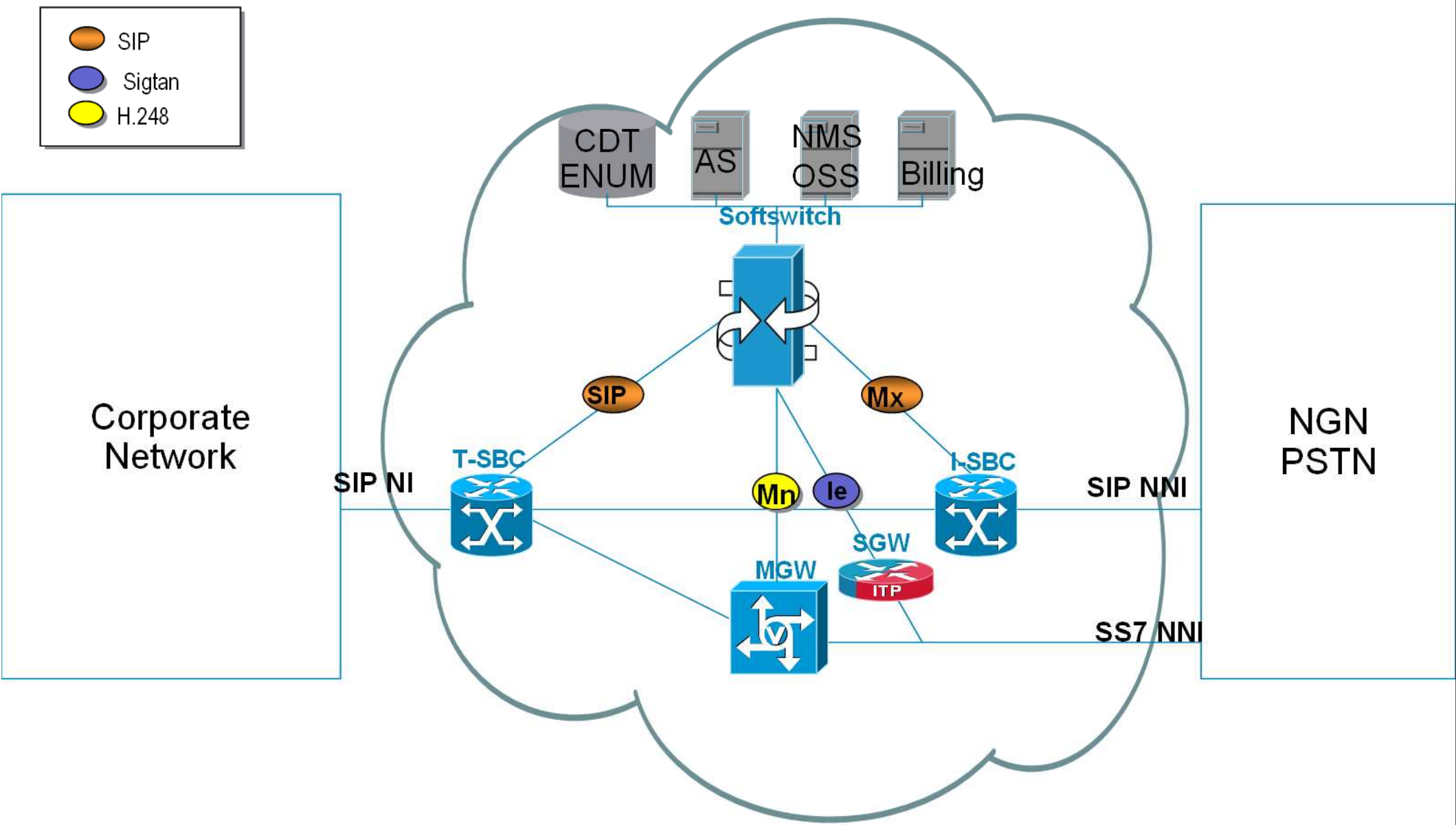
What are the benefits of the Peering Based model?



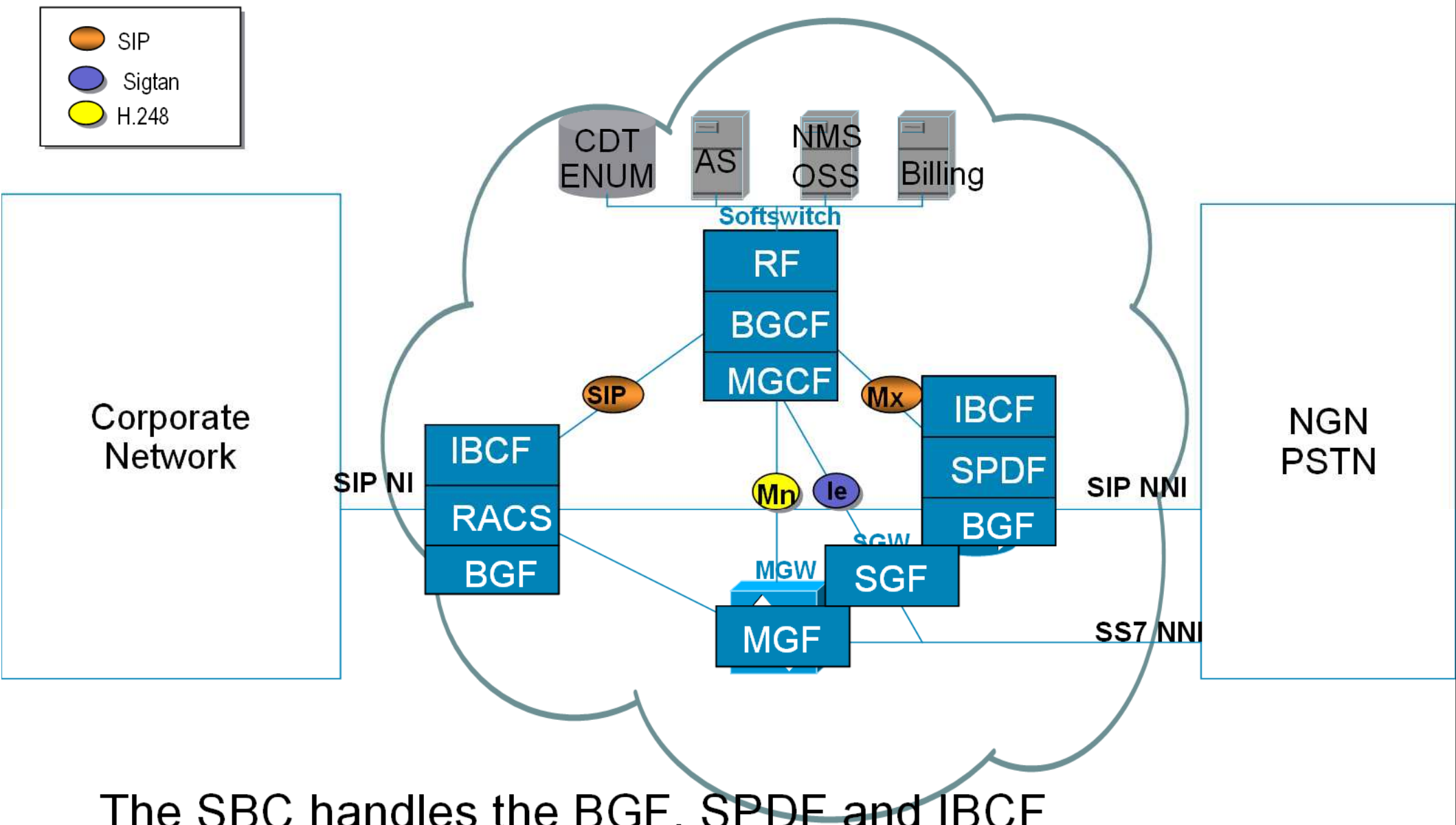
What are the benefits of the Peering Based model?



Peering Based model product mapping



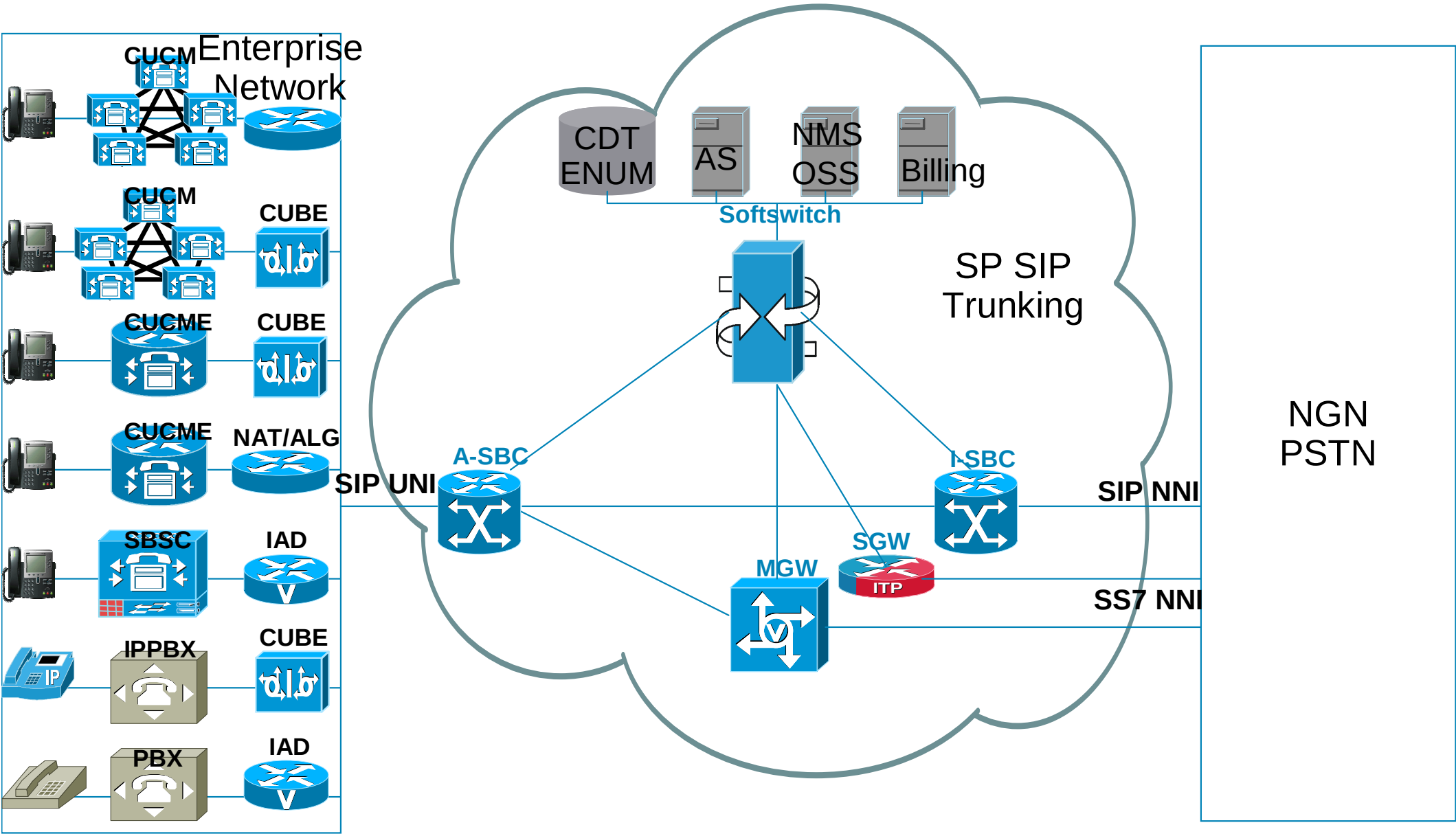
Peering Based model product mapping



The SBC handles the BGF, SPDF and IBCF

Architecture and deployment scenarios

SIP trunking system configuration



What are the important SIP trunking functions?

Addressed in BRKUCT-2001

- Offer method
- DTMF transport methods
- Fax transport methods
- Transport of Voice Band Data
- Supplementary Service options
- Call Admission Control
- Authentication and encryption
- Enterprise deployment methods

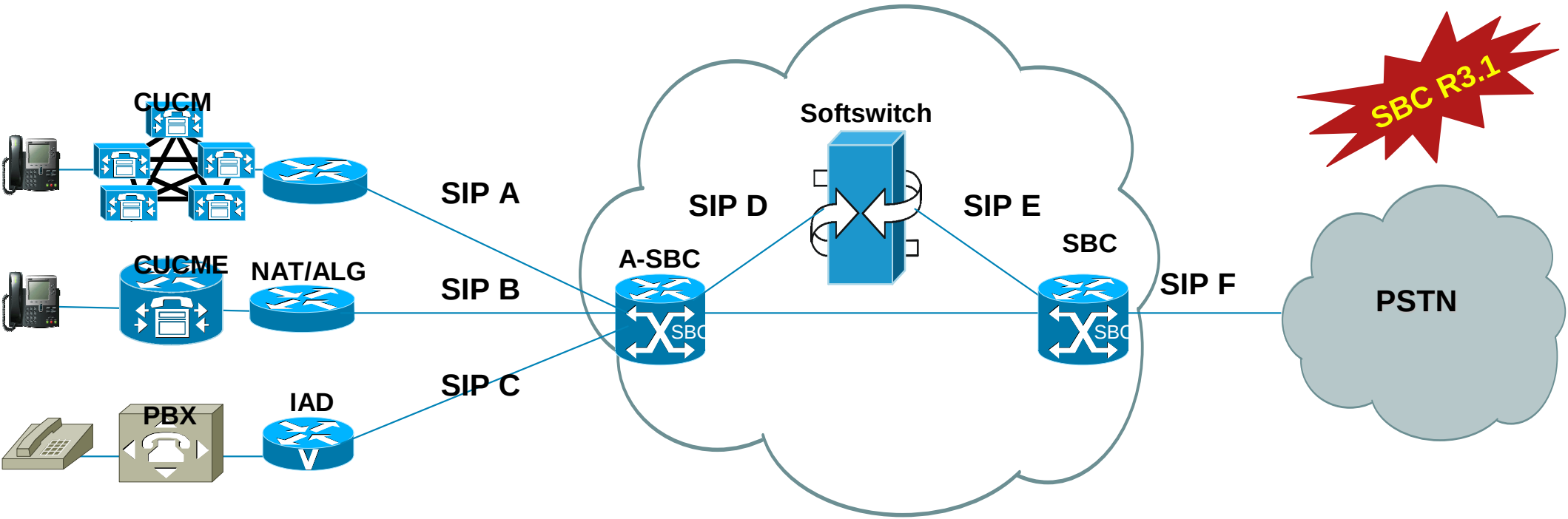
Addressed in this session

- Signaling
- Transcoding
- Lawful Interception
- Provisioning
- Rich media
- Testing
- Interconnection with SP services
- DoS and DDoS attacks

Examples of SIP signaling incompatibilities

- **Rejecting an unknown header** (value or parameter) instead of ignoring it
- **Sending incorrect data** in SIP
- **Not implementing** (or incorrectly) **protocol procedures**
- Expecting an **optional header** value/parameter which can be **implemented in multiple ways**
- Sending a **value/parameter that must be changed or suppressed** (“normalized”) before it leaves/enters the enterprise to comply with policies
- **Variations in the SIP standards** of how to achieve certain functions

SBC SIP header and parameter manipulation

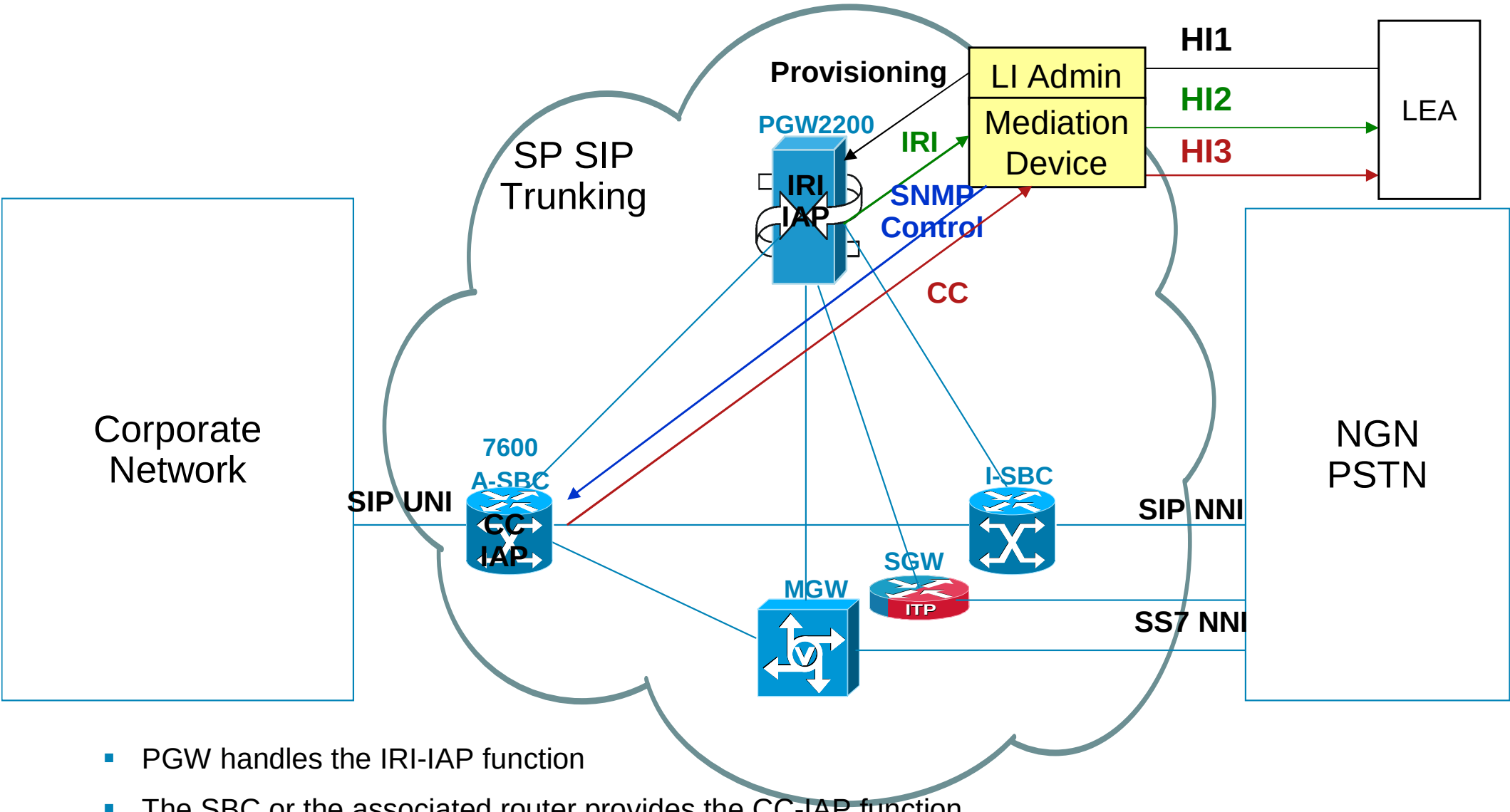


- Conditionally add/remove and replace headers and parameters from specific requests and responses
- Method Profile: contains Pass/reject indication plus one or more method names each of which may reference a parameter profile and/or a header profile. Supports status/response code mapping
- Header Profile: contains one or more header names which can be passed through (white list), removed (black list), conditionally removed, renamed, content changed, added (conditionally or unconditionally), reference a parameter or any combination of the above. Complex conditions can be constructed using boolean operators
- Parameter Profile: contains one or more URI parameter names that can be stripped, added or replaced. Applies only to Request, To, From and contact headers

PGW SIP Profiles

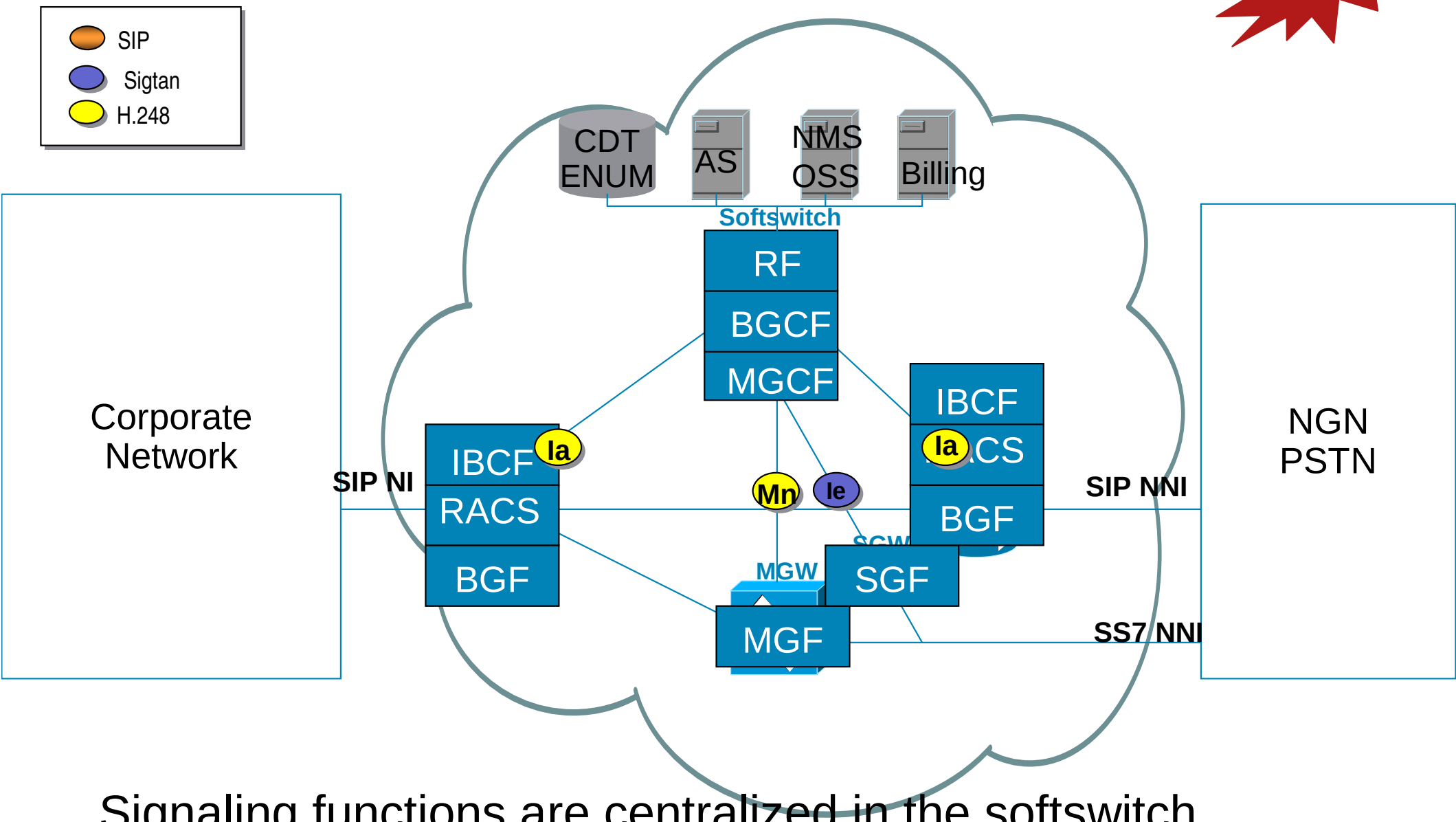
- The full SIP B2BUA mode isolates call legs
- Manipulation of SIP headers with SIP header tables
- A SIP profile applies at trunk group level for SIP & EISUP
- It optionally applies at a domain of SIP URI level

Lawful Interception



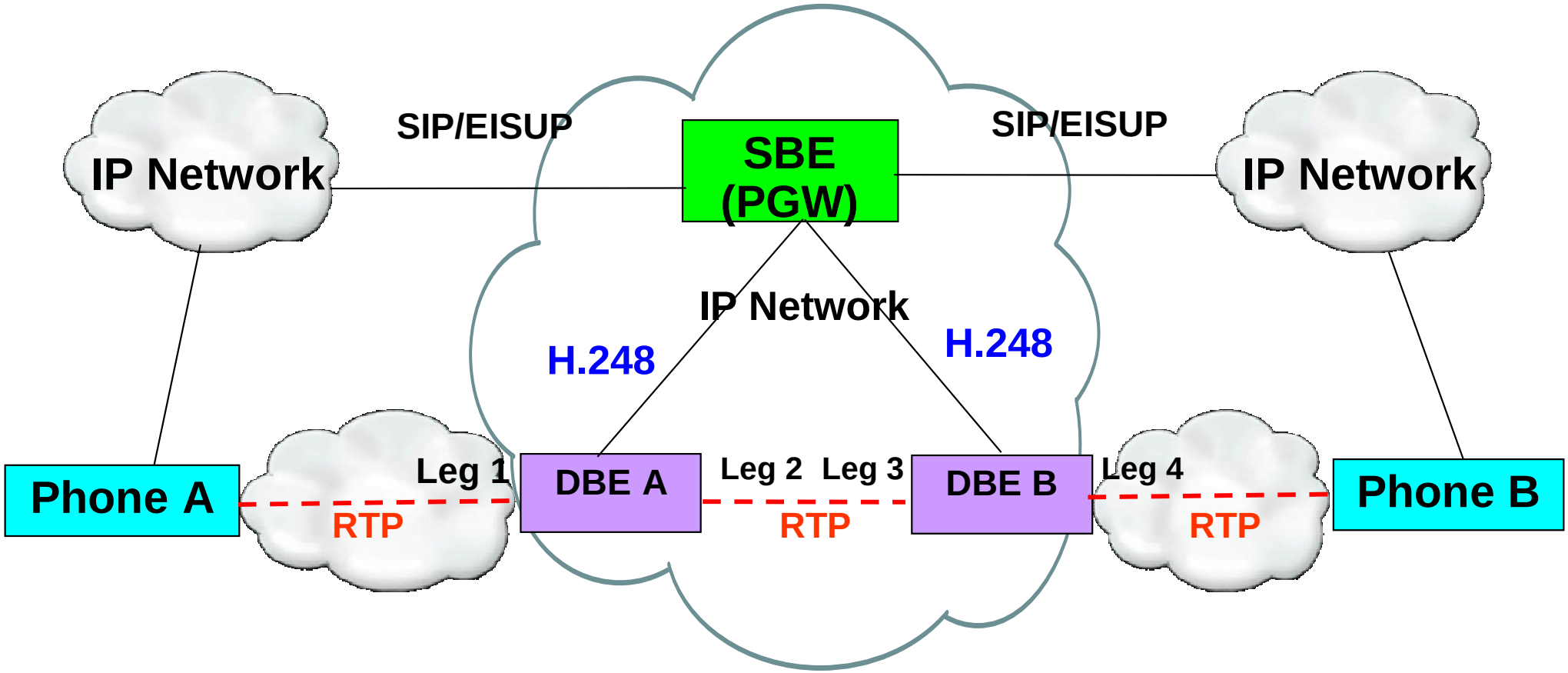
- PGW handles the IRI-IAP function
- The SBC or the associated router provides the CC-IAP function
- A Cisco partner provides the Mediation

Peering based model with distributed SBC



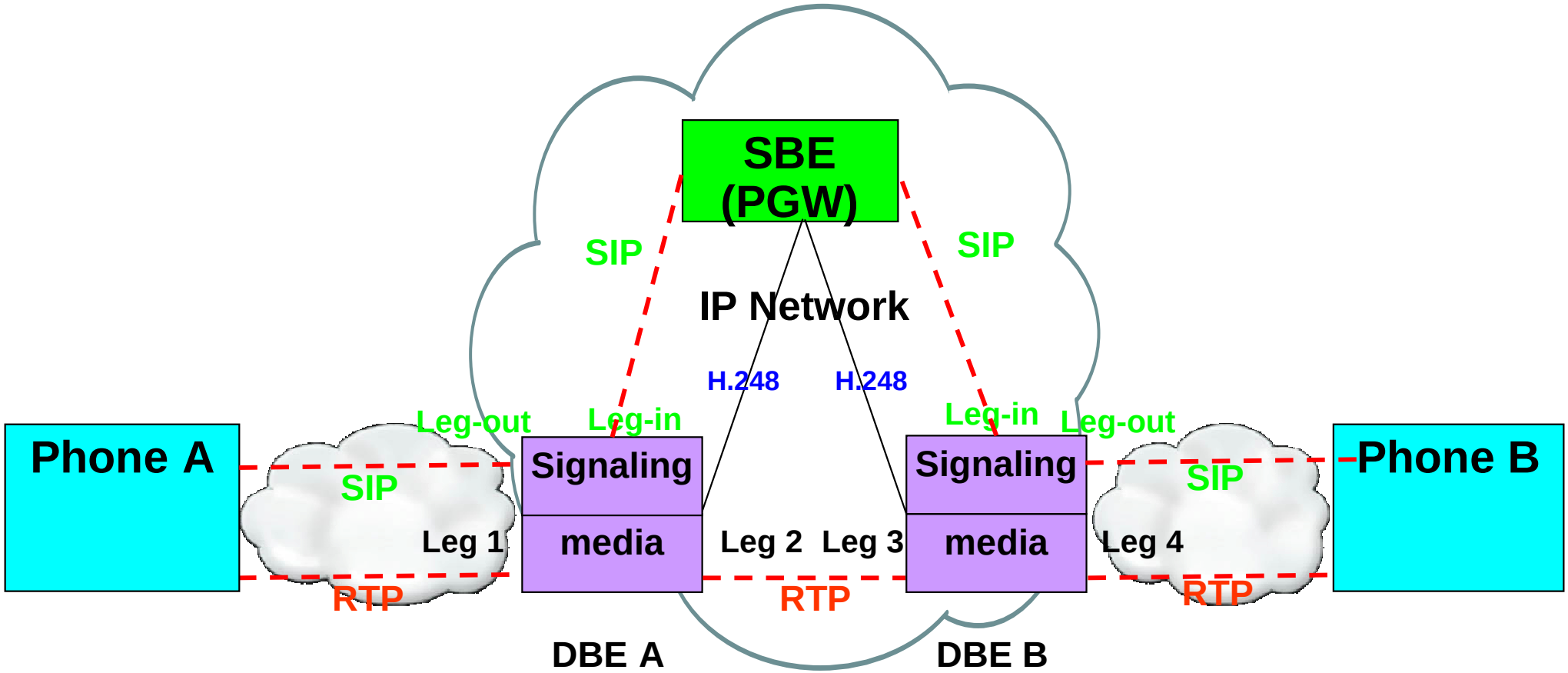
Signaling functions are centralized in the softswitch

PGW SBE



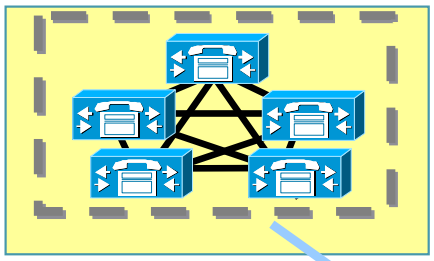
DBE handles the media plane only

What is signaling pinhole in DBE?



DBE transport media and signalling

Rich Media
TelePresence SP Solution Architecture



Unified Communications Manager (CUCM)

Session Border Controller:

Secure Inter-Enterprise Connectivity

SIP

SIP

SIP

SIP

IP/MPLS

CTS 3000

Cisco TelePresence Endpoints

Purpose Built Room

- **Up to 3 audio Speakers**
- **Up to 3 Microphones**
- **Up to 3 Video Cameras**
- **TelePresence Furniture**

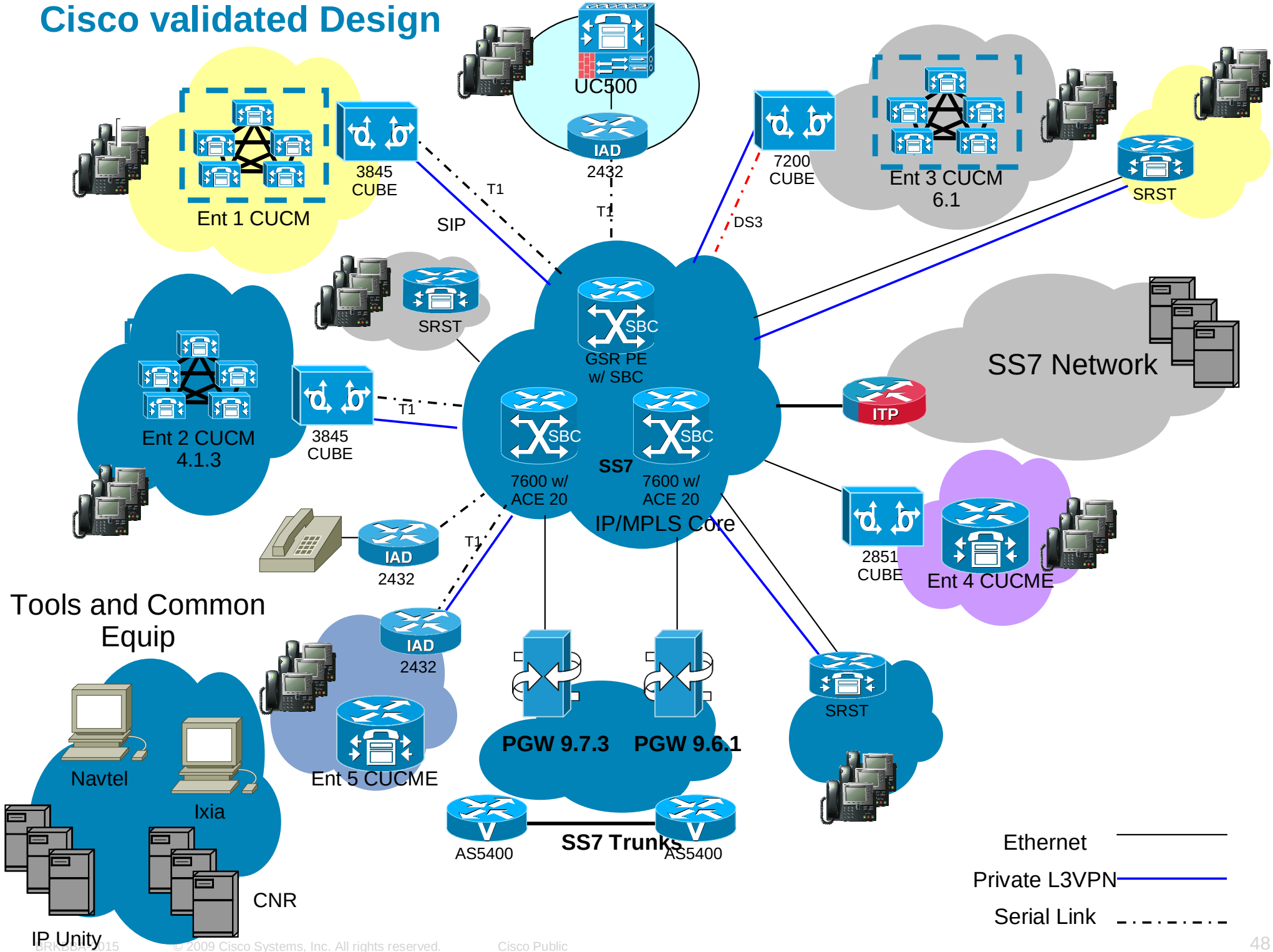
ENUM

Microsoft Exchange

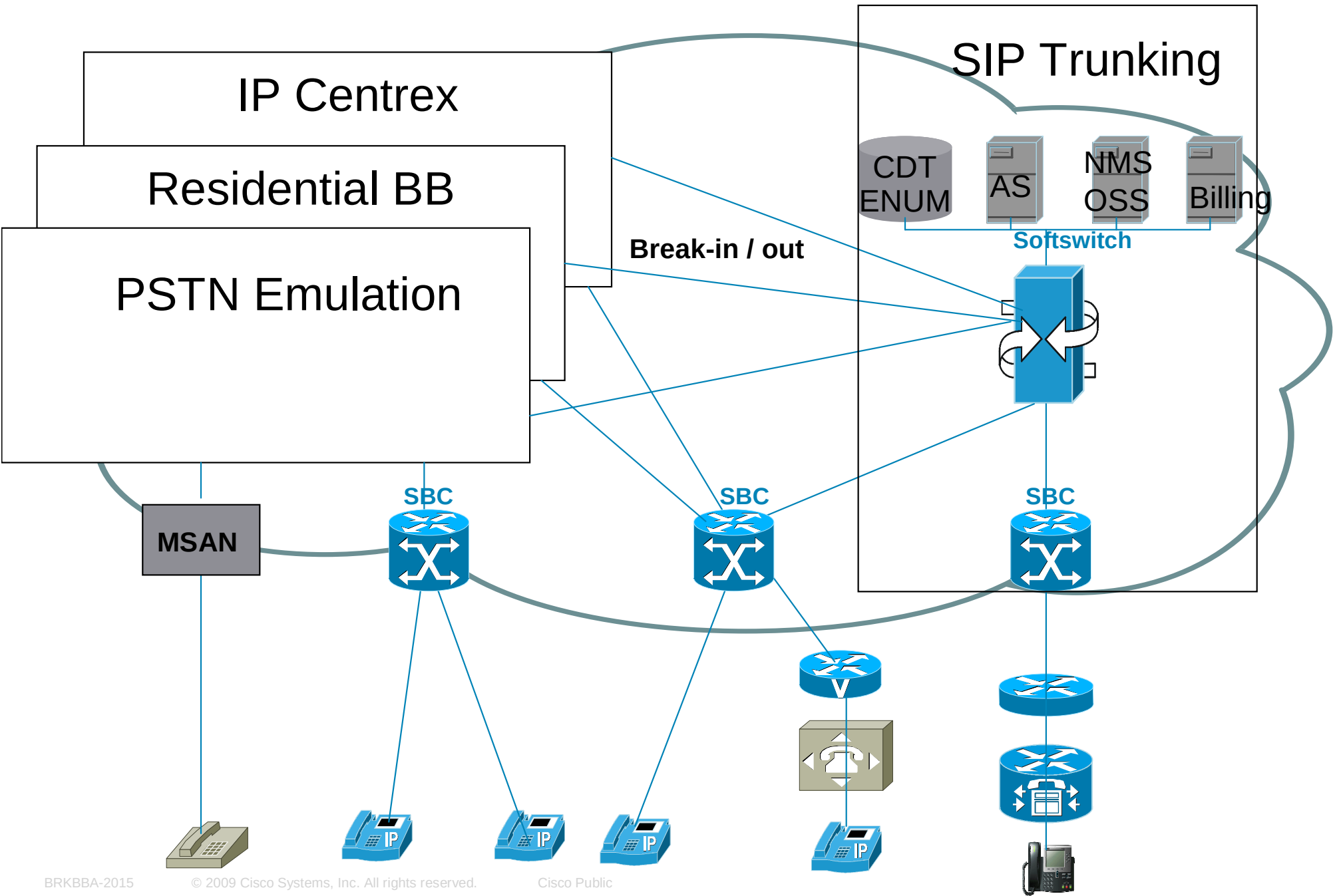
Microsoft Active Directory

TelePresence Scheduling Server

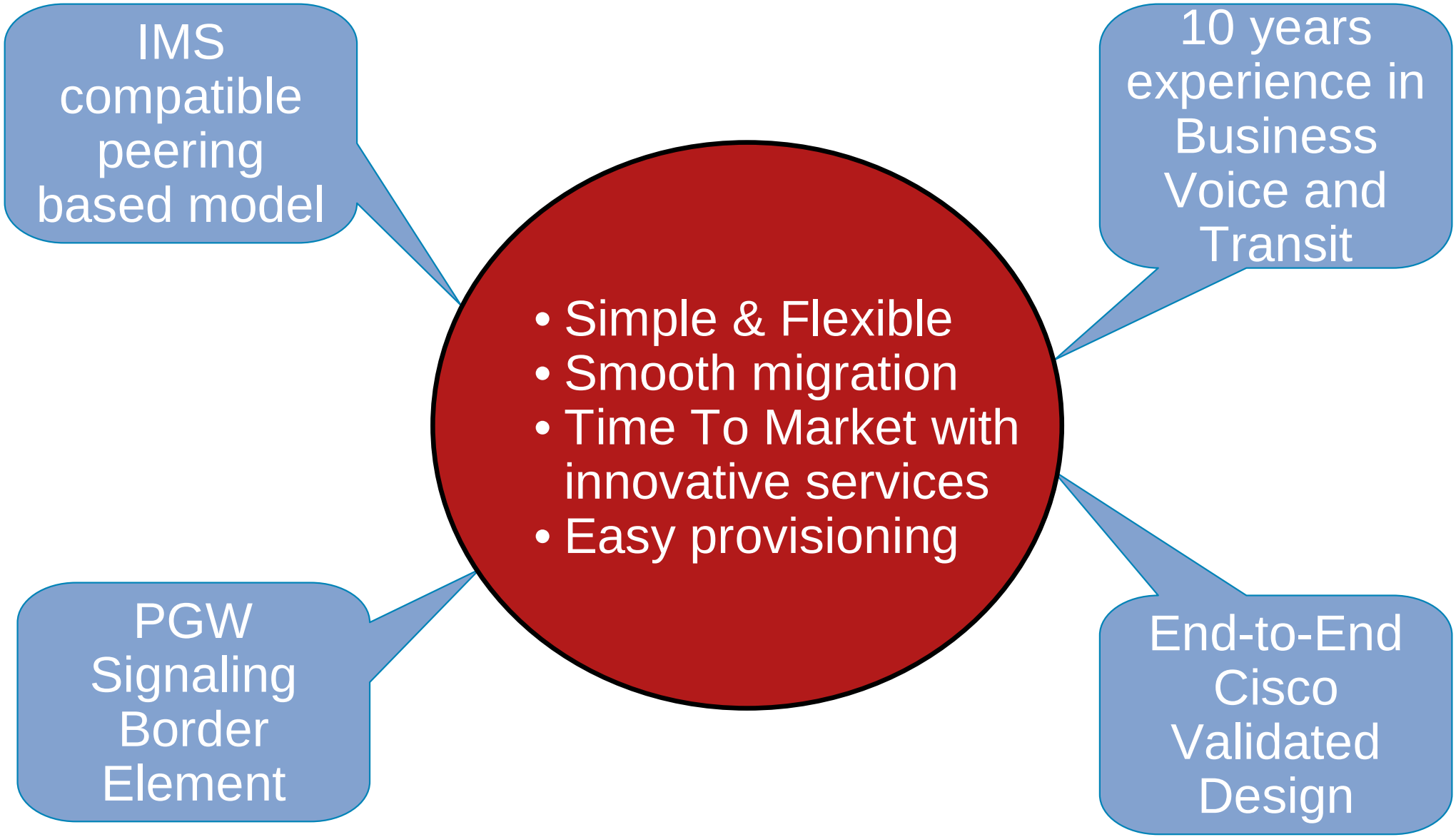
Cisco validated Design



Interconnection between services



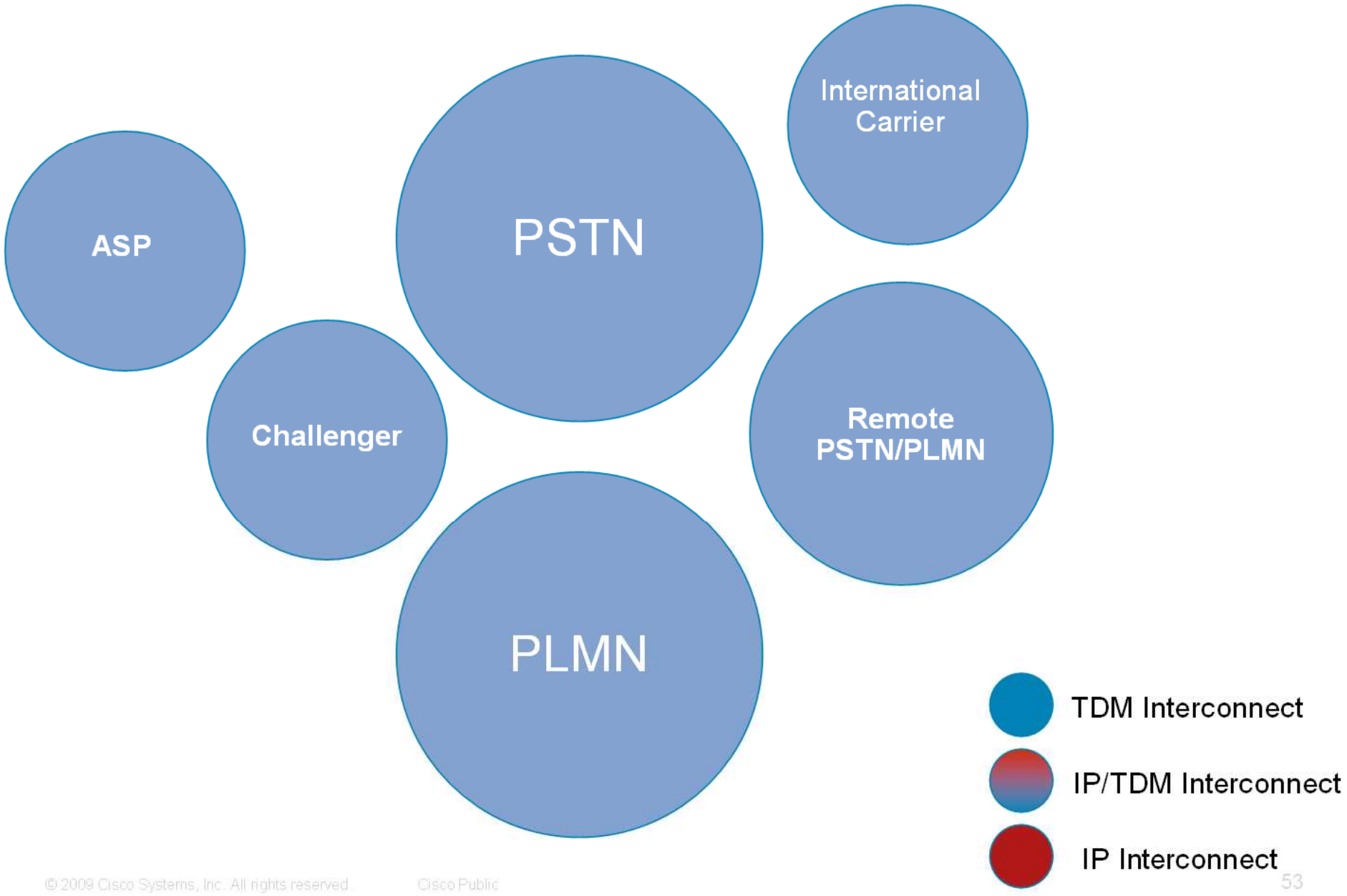
Cisco SIP trunking benefits for you



Cisco Networkers 2009
January 26-29 Barcelona, Spain

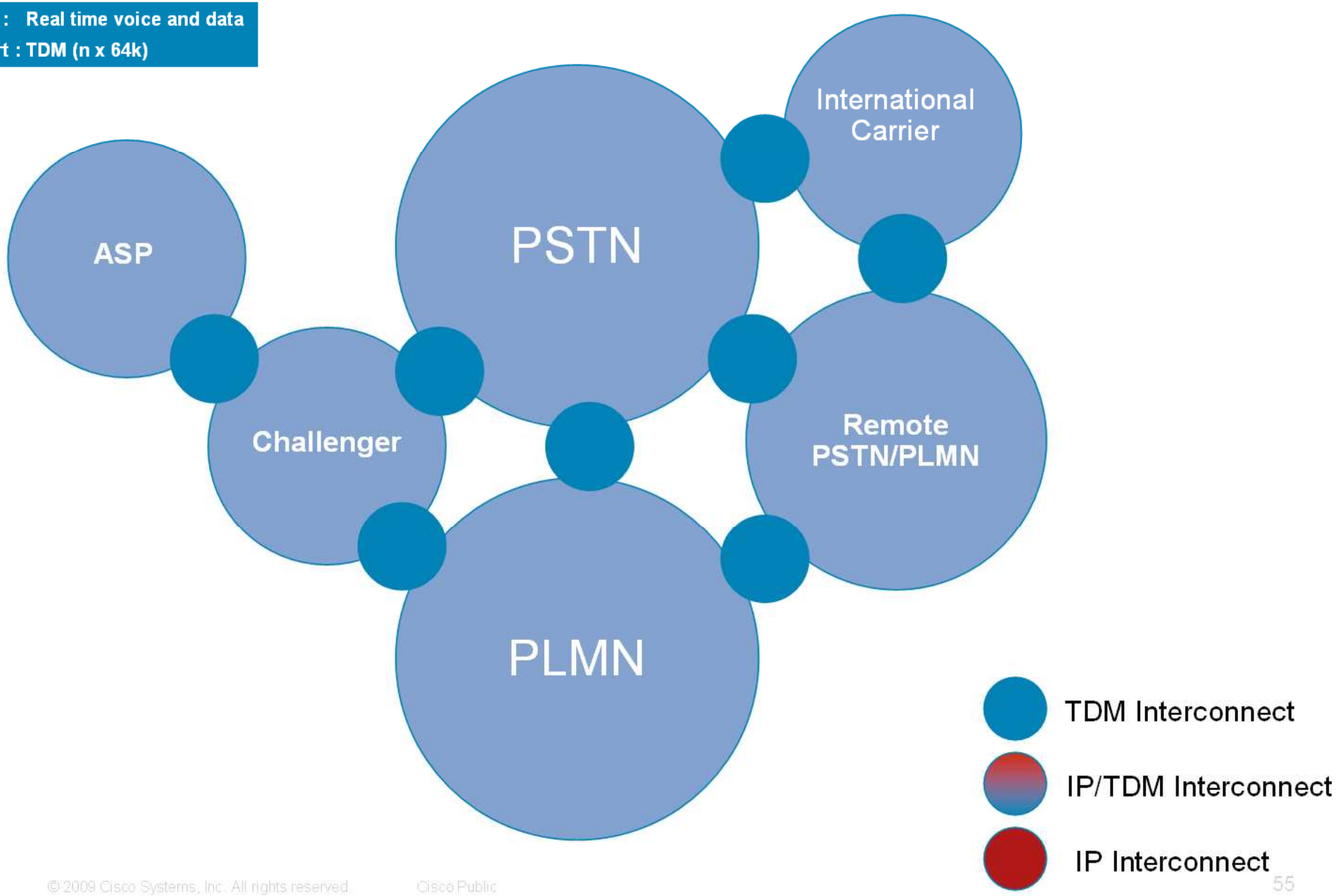
Interconnect Market Dynamics

The dynamics behind peering



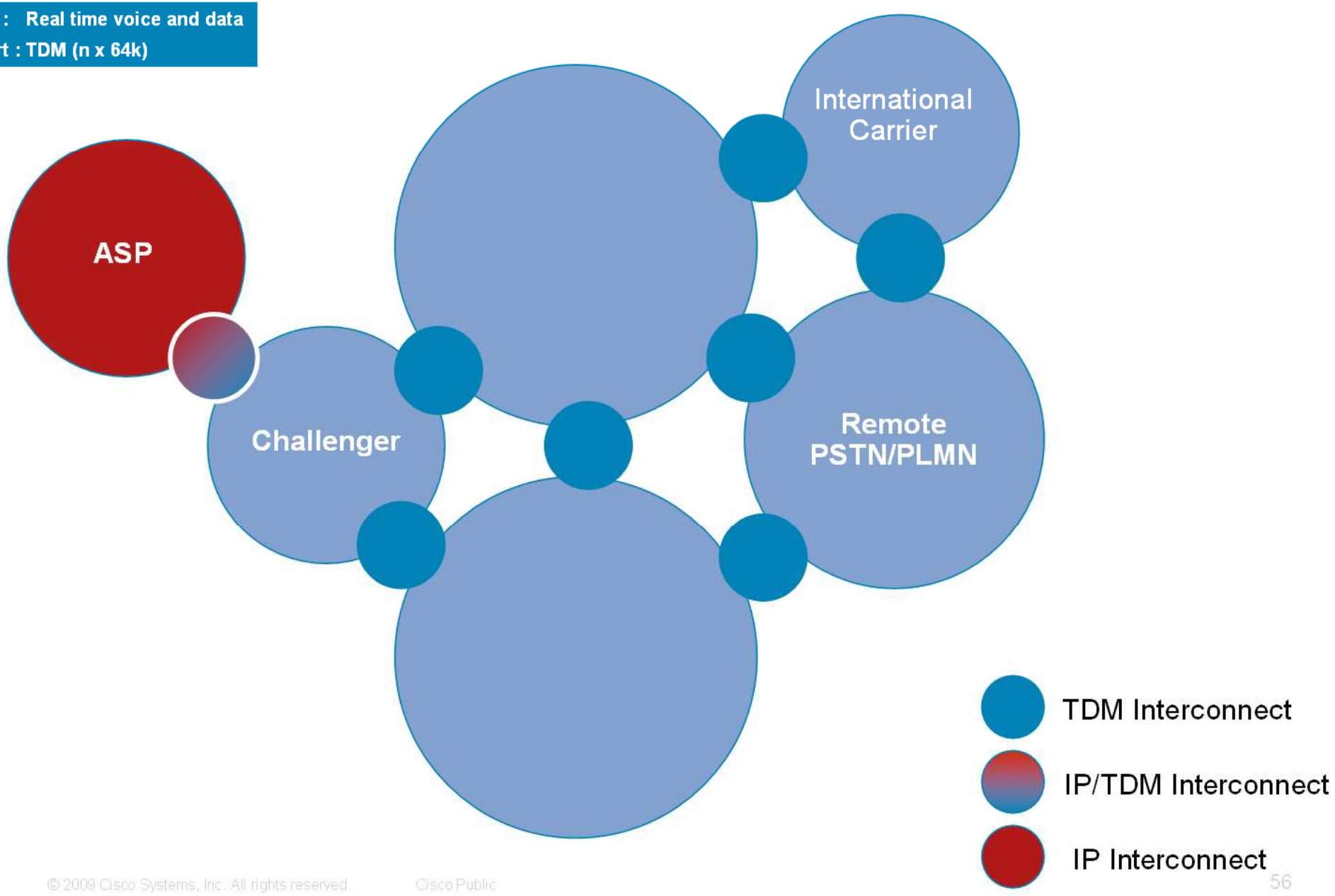
The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)



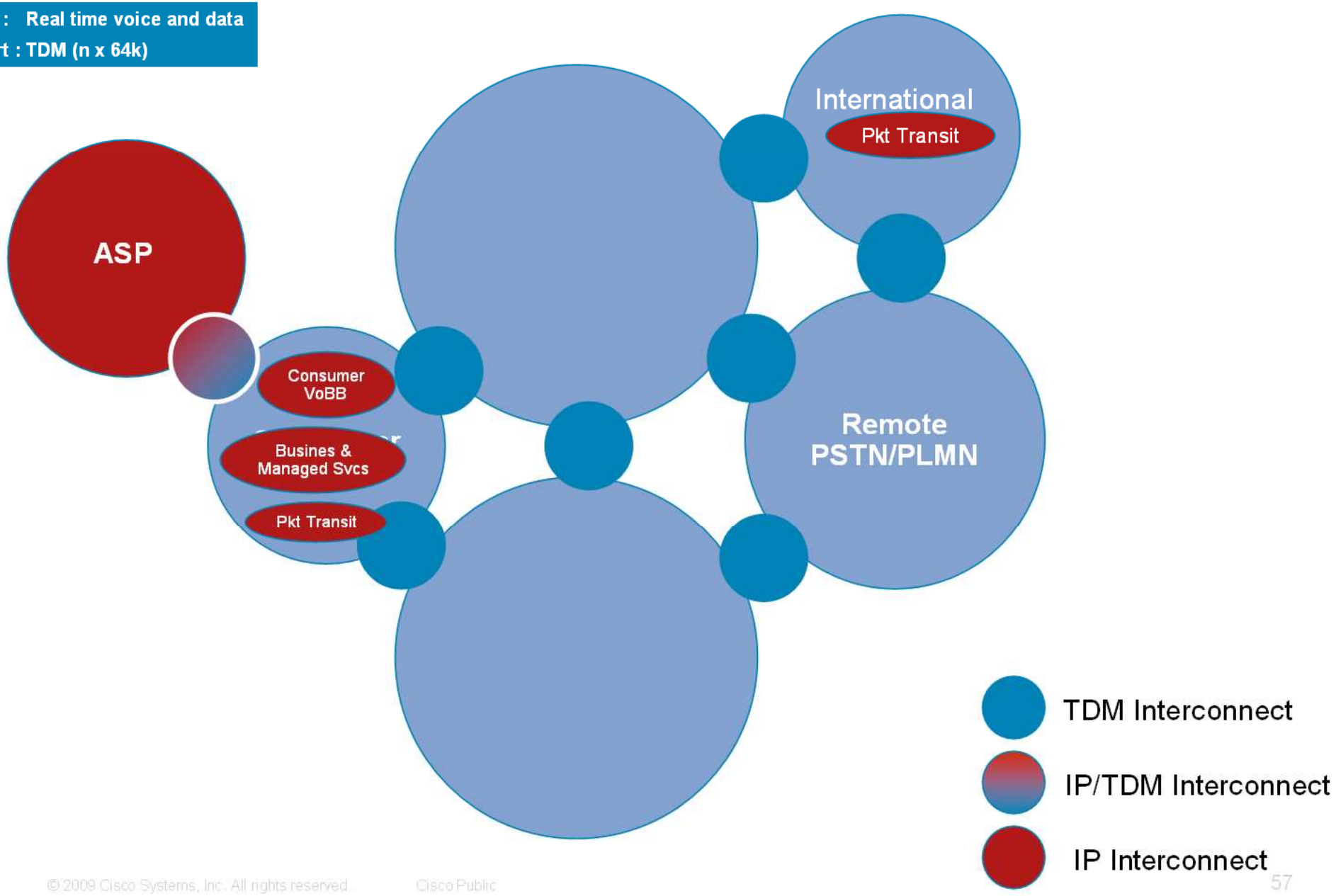
The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)



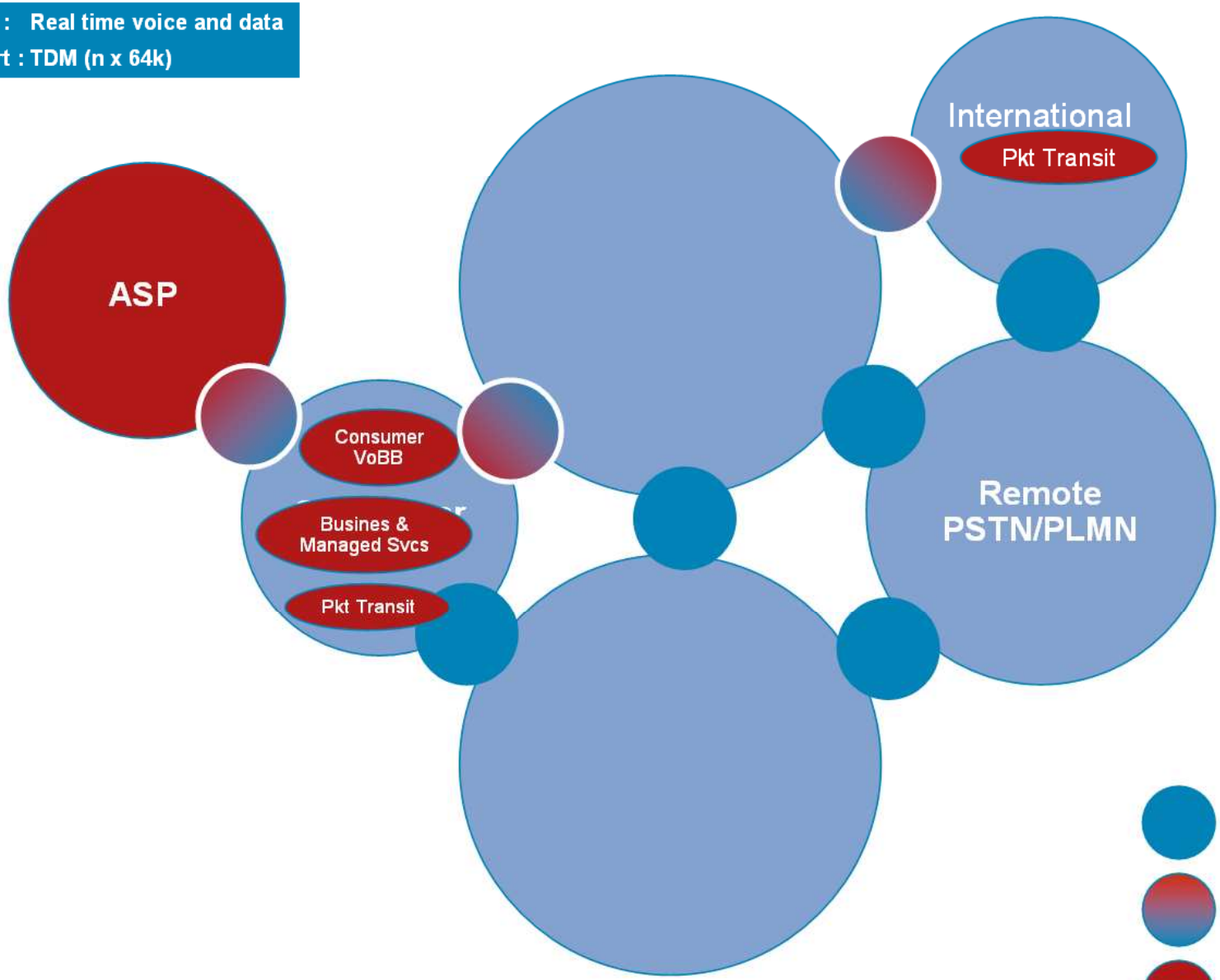
The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)



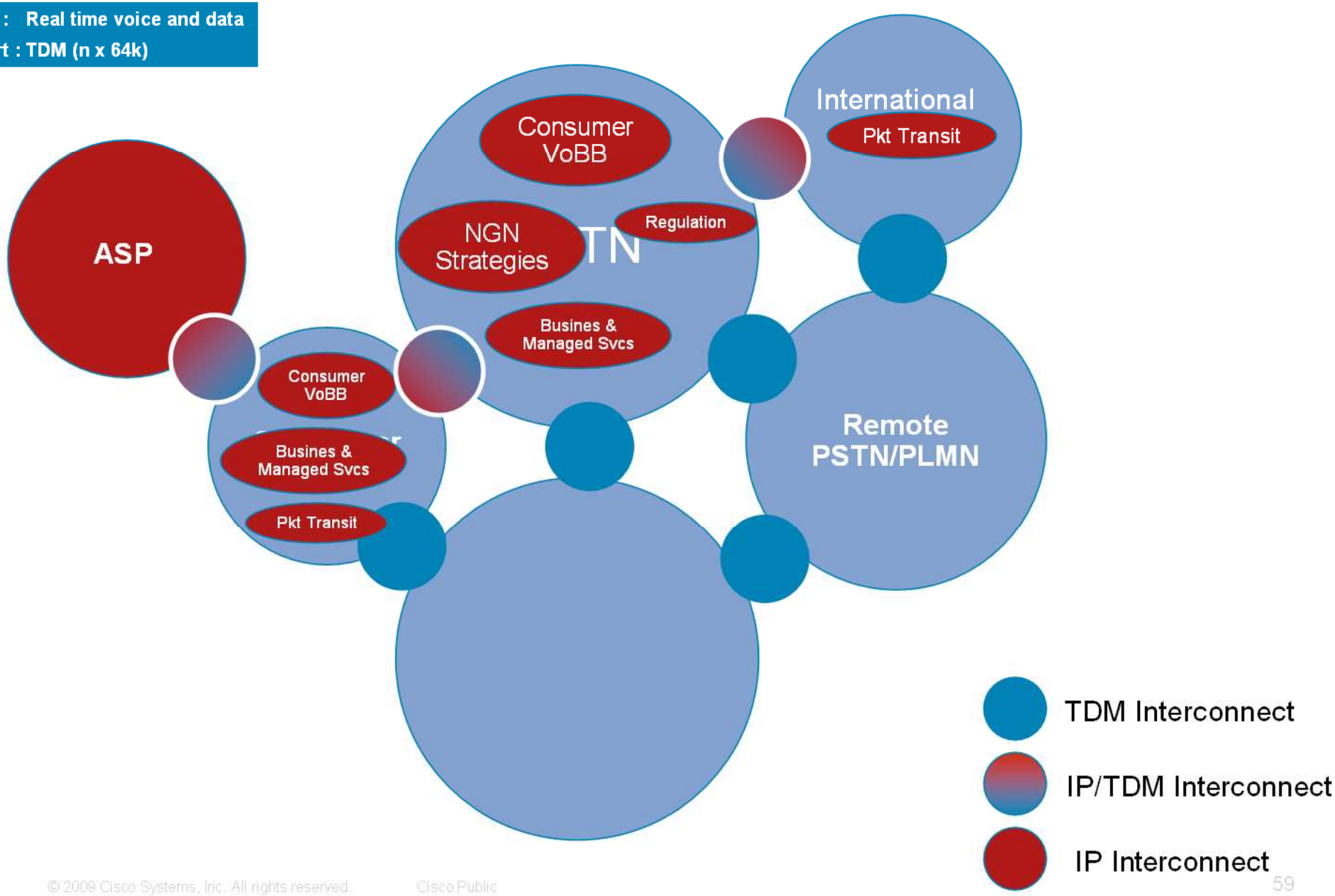
The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)



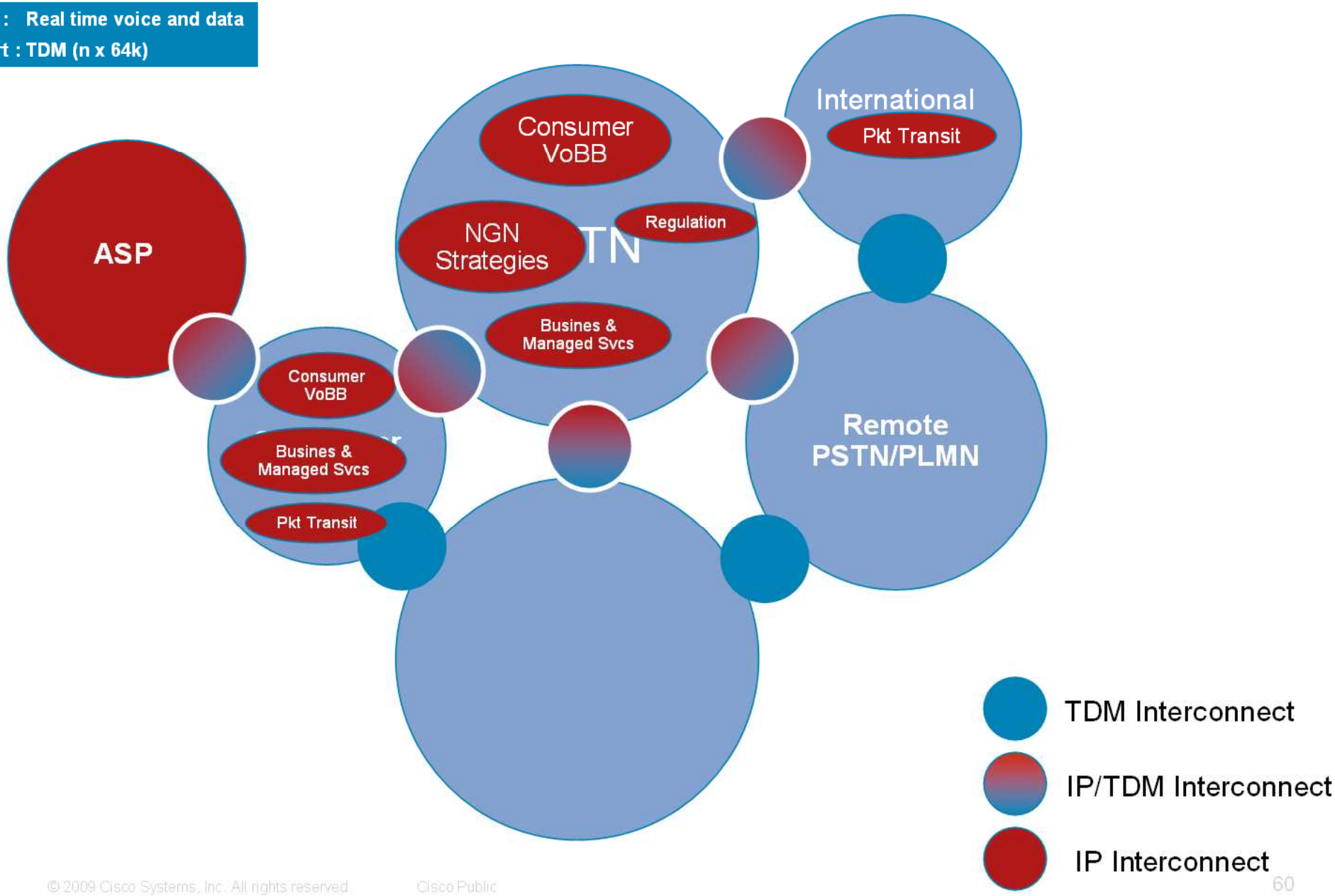
The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)



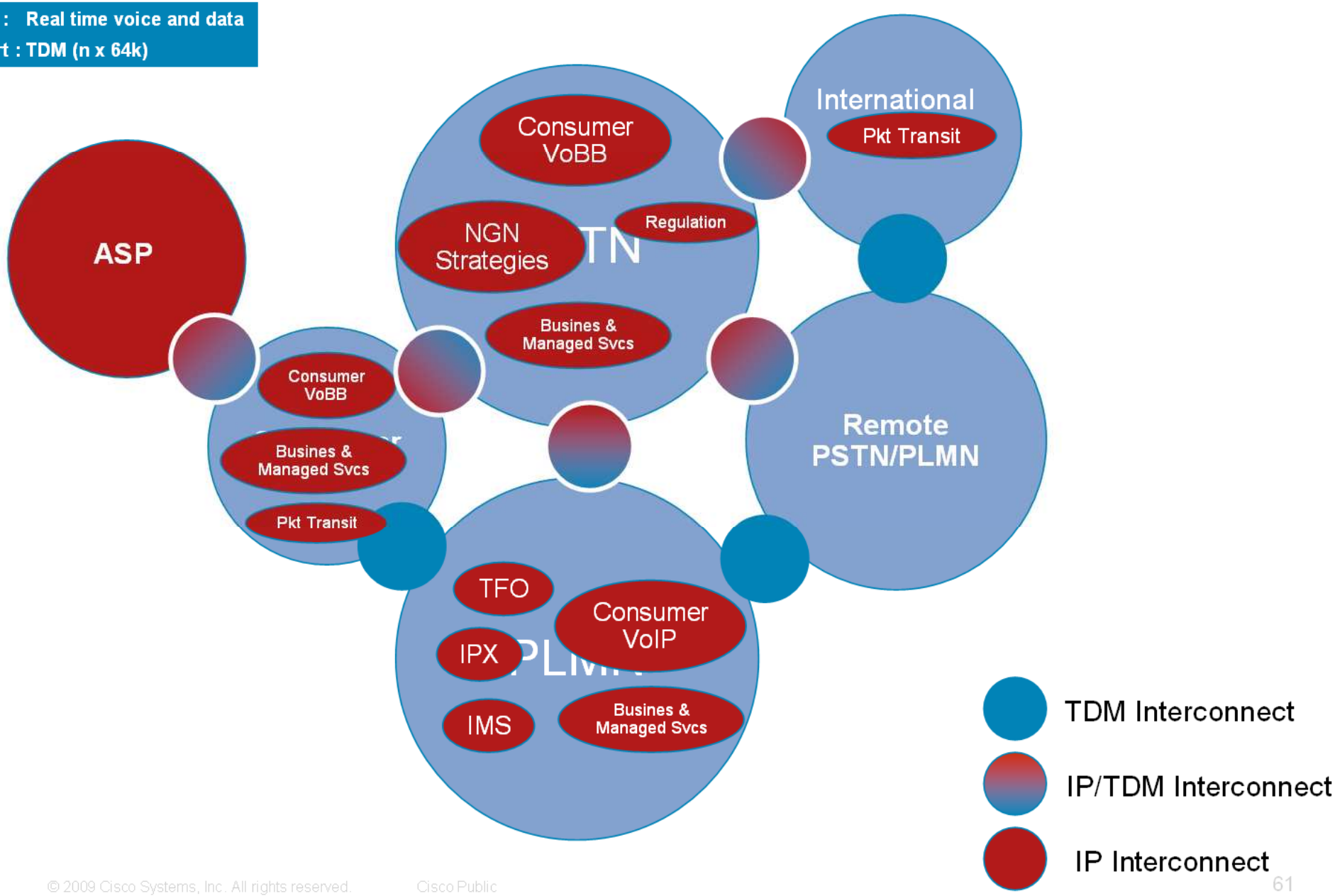
The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)



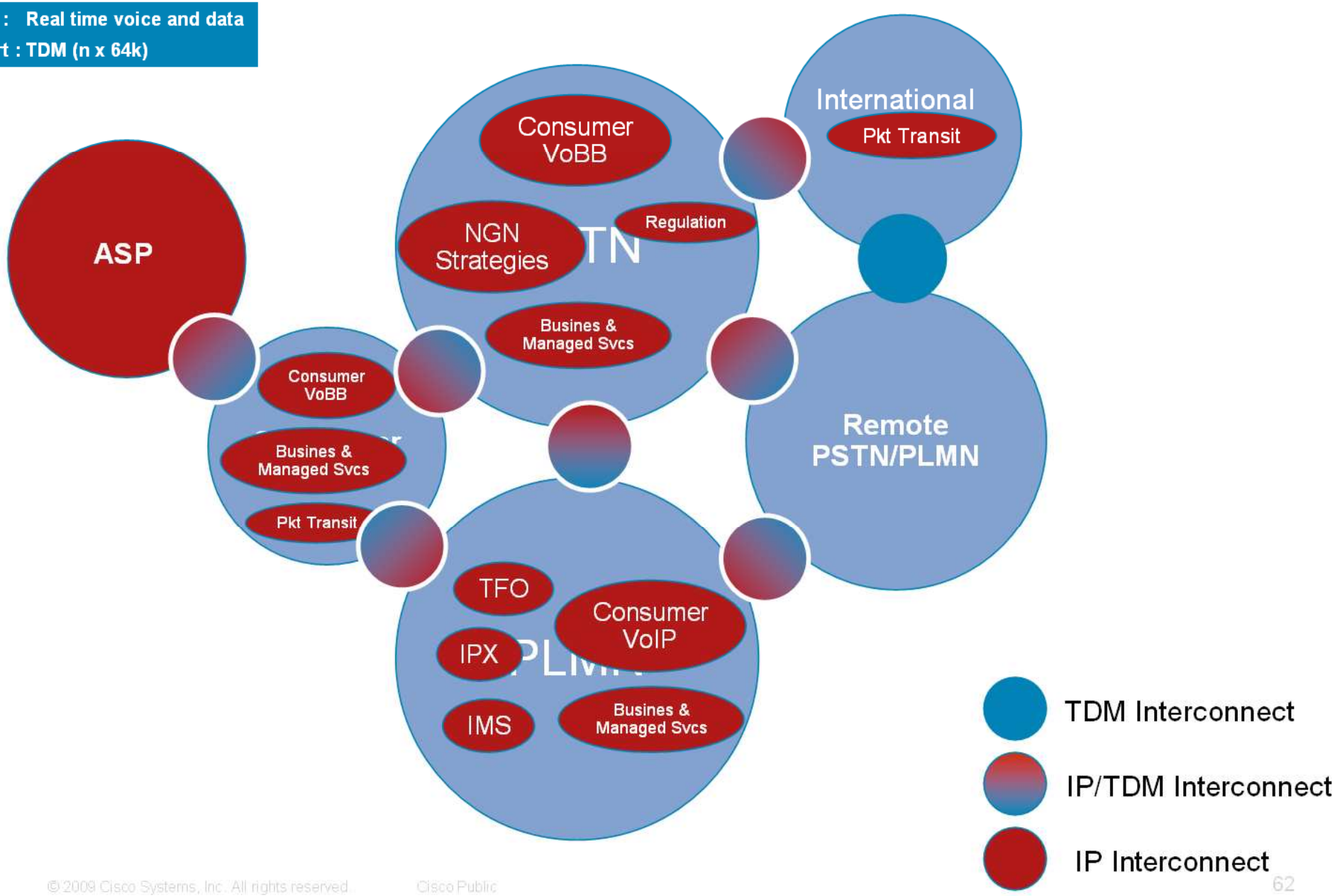
The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)



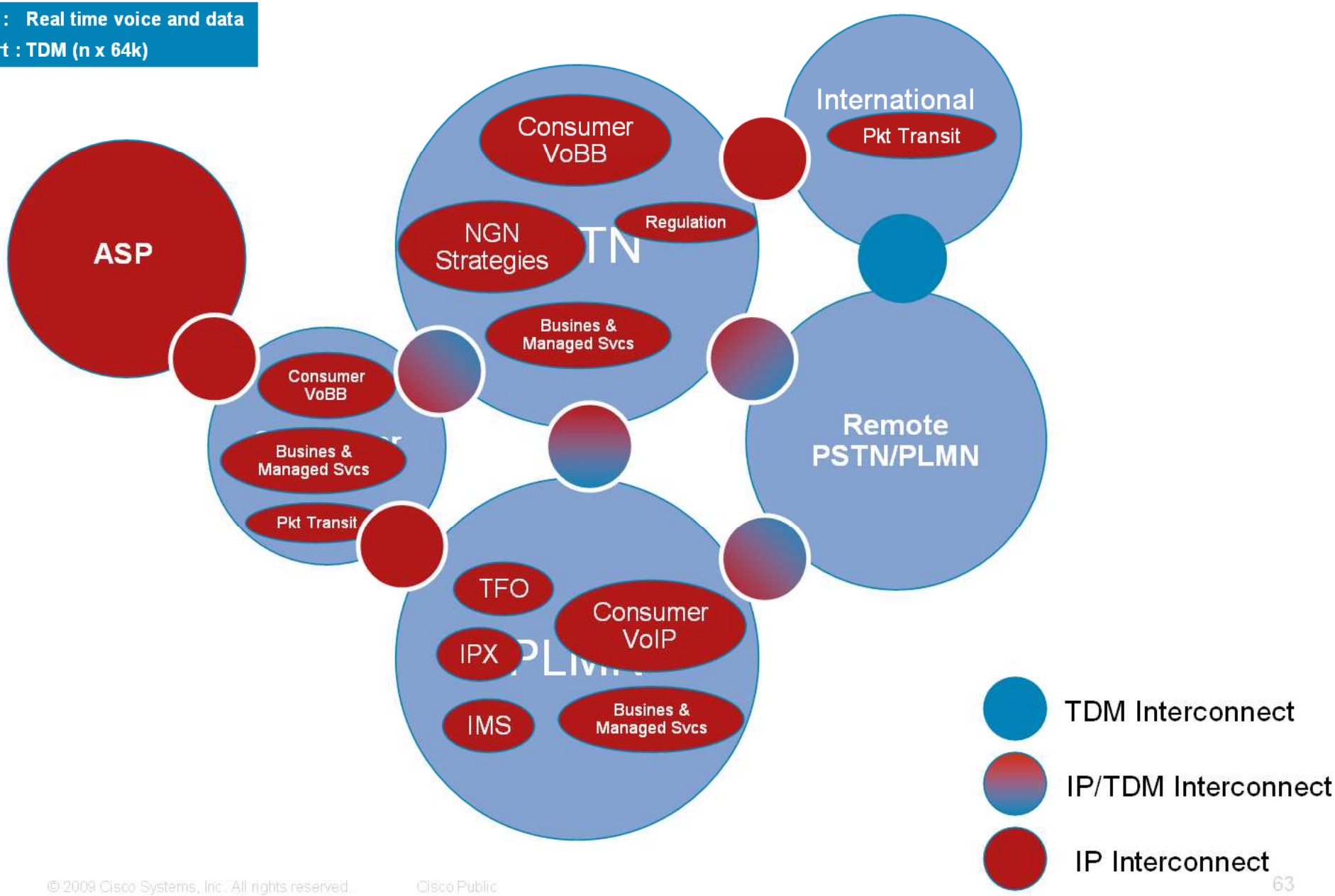
The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)



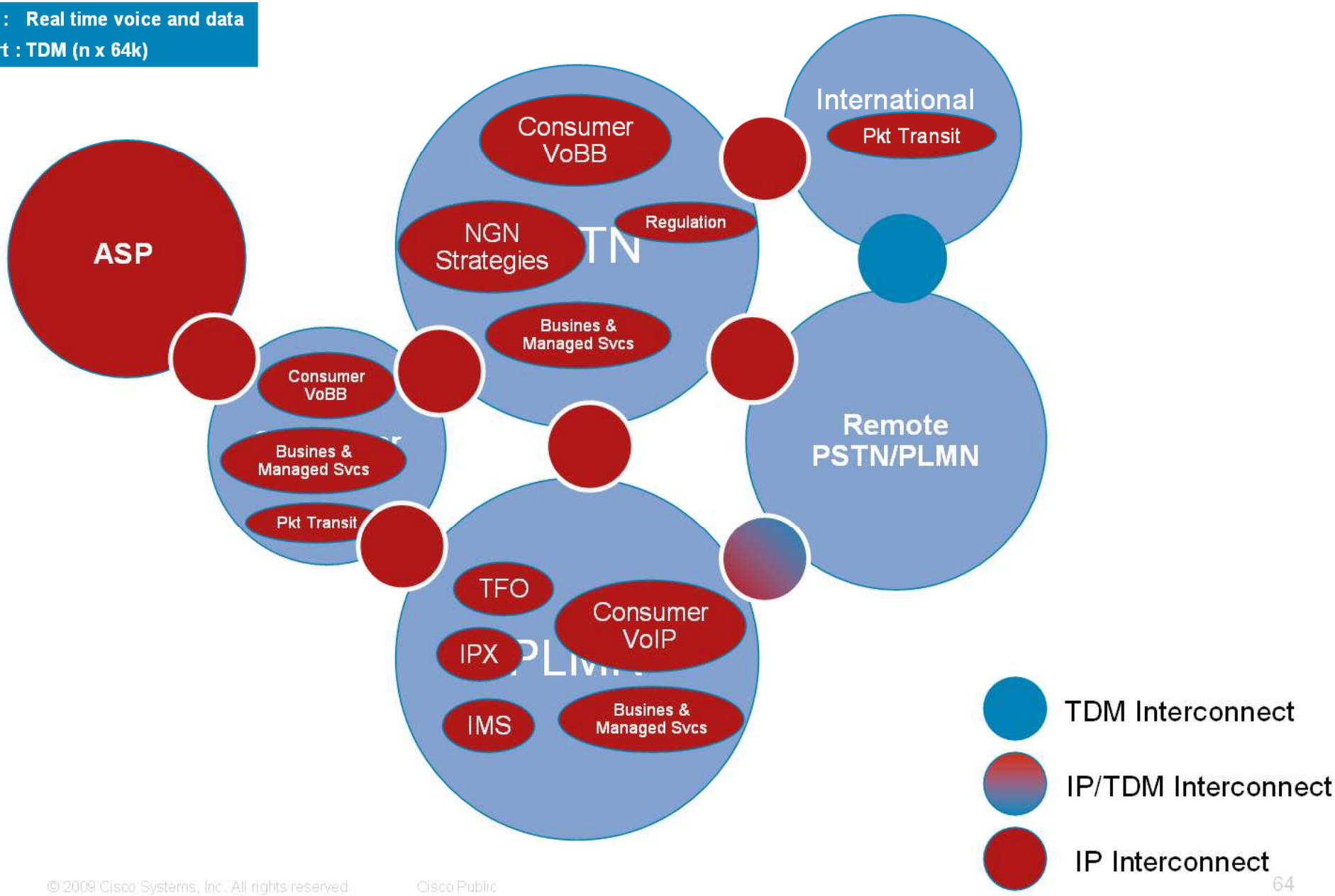
The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)



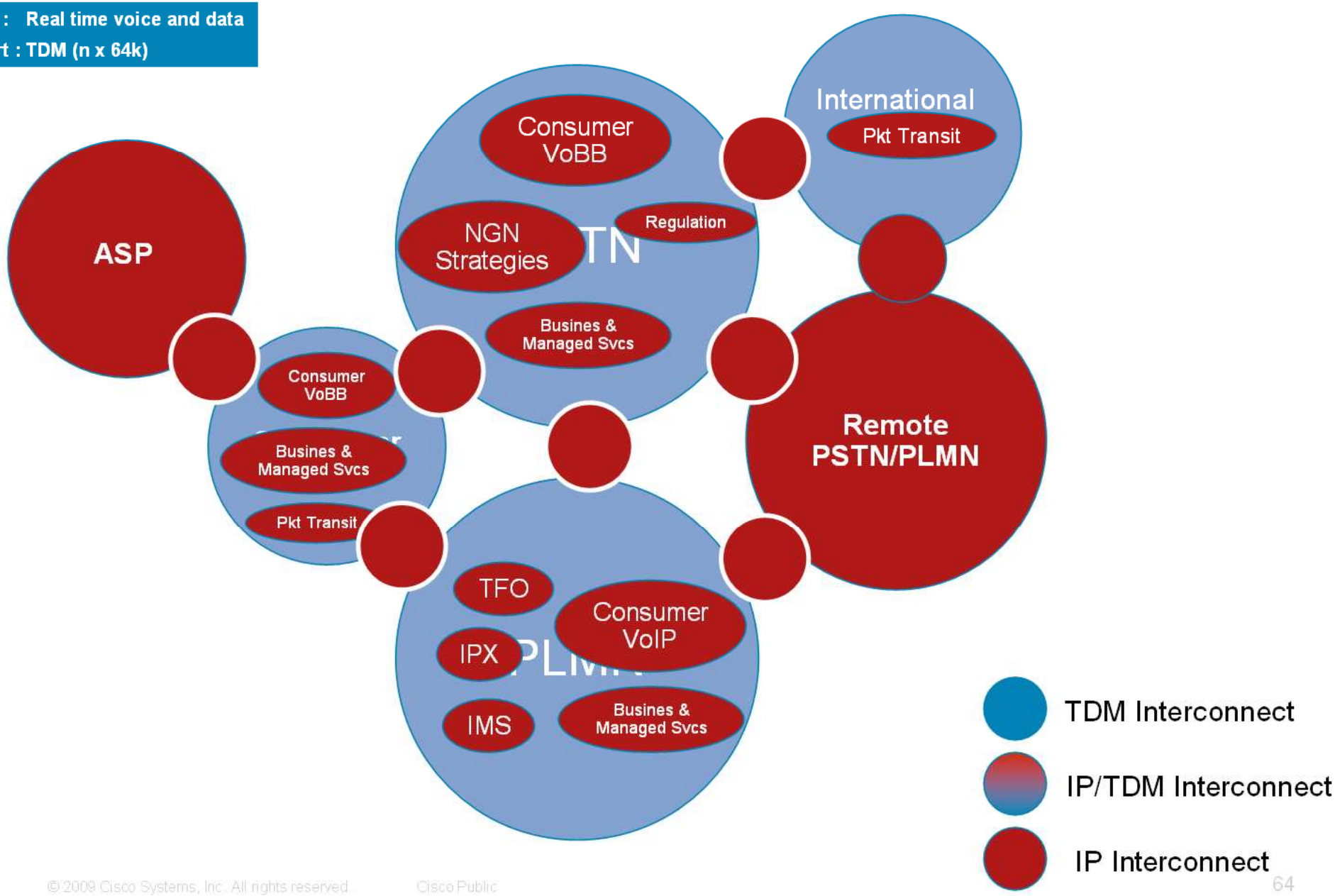
The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)



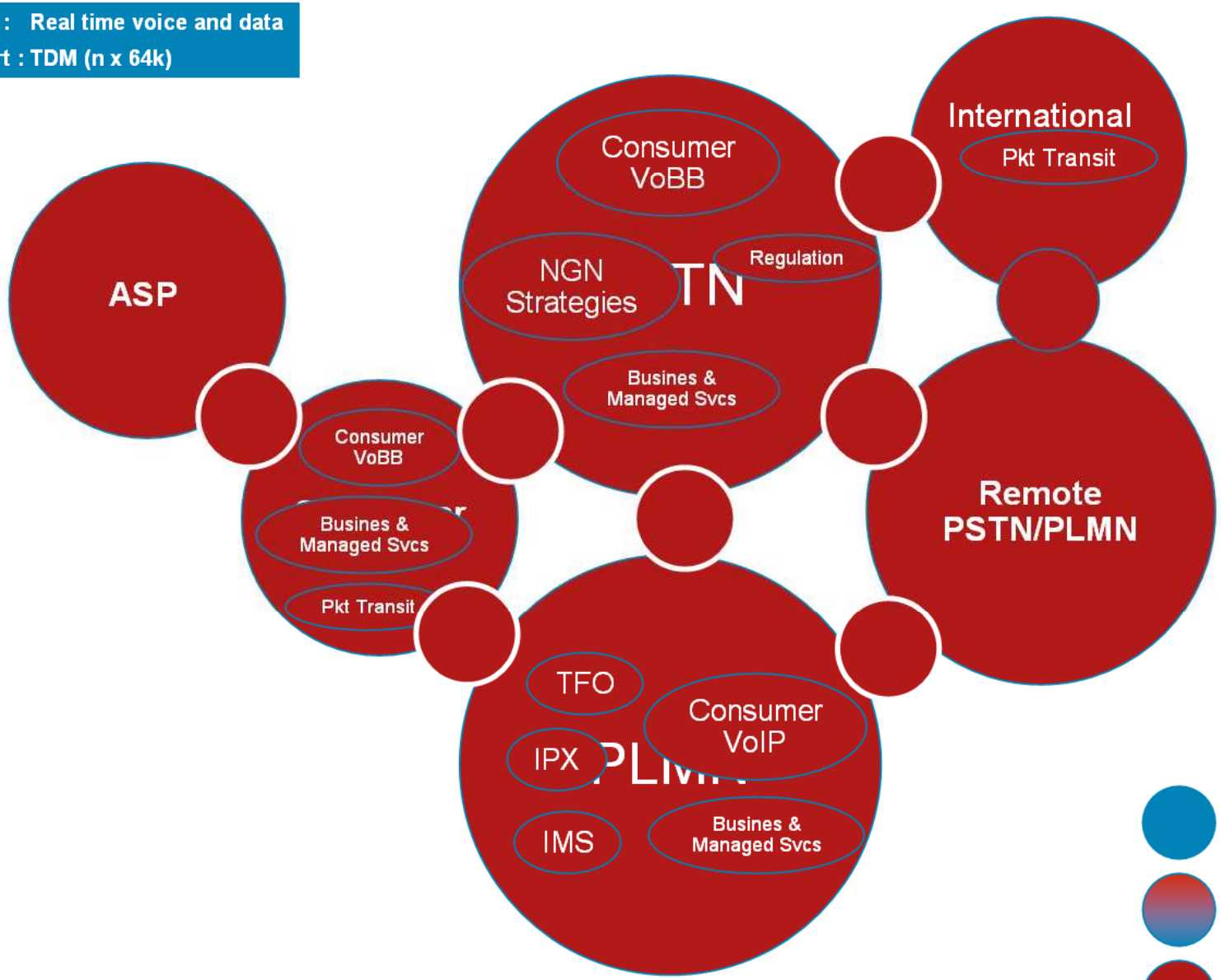
The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)

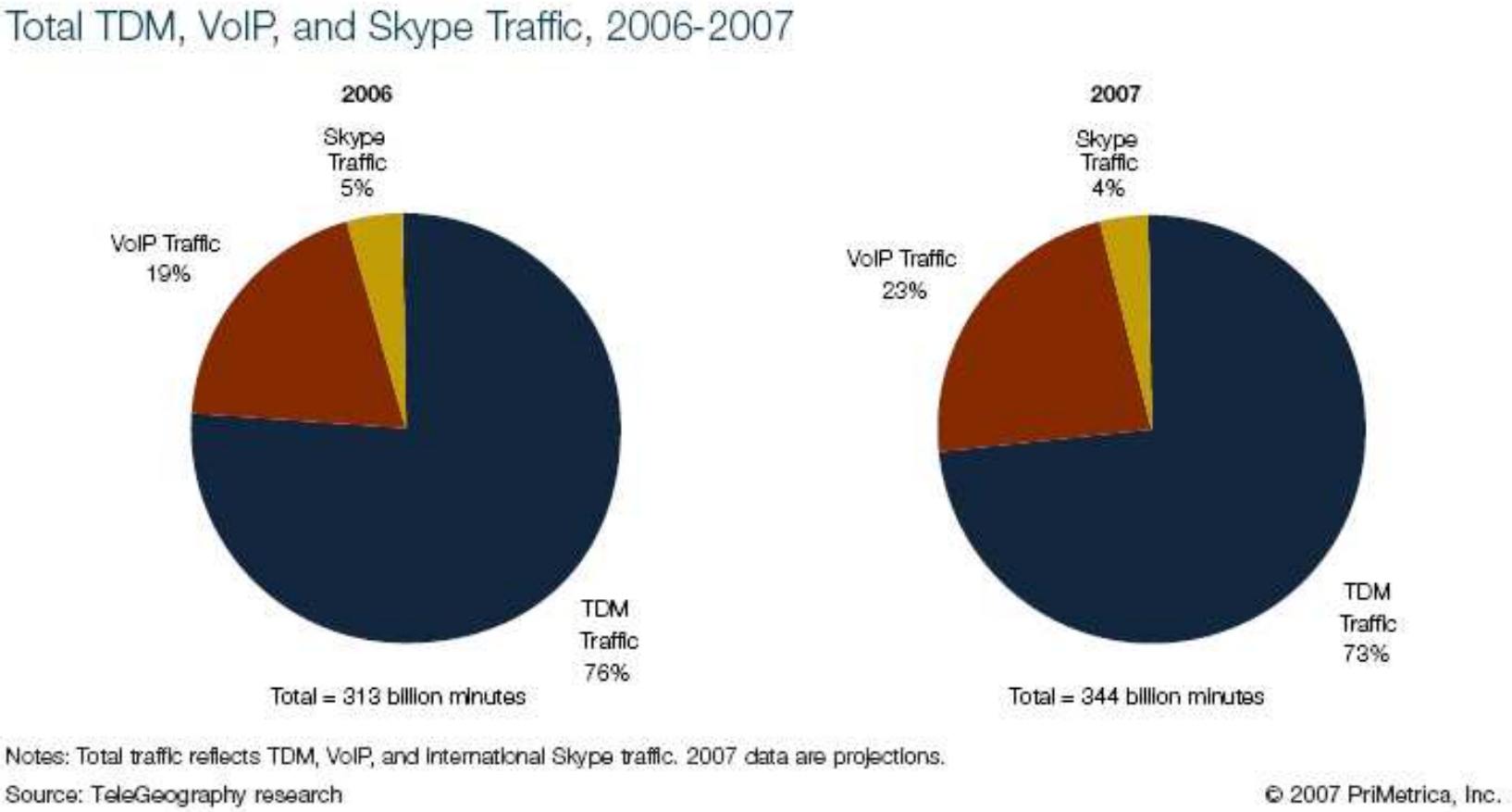


The dynamics behind peering

Services : Real time voice and data
Transport : TDM (n x 64k)

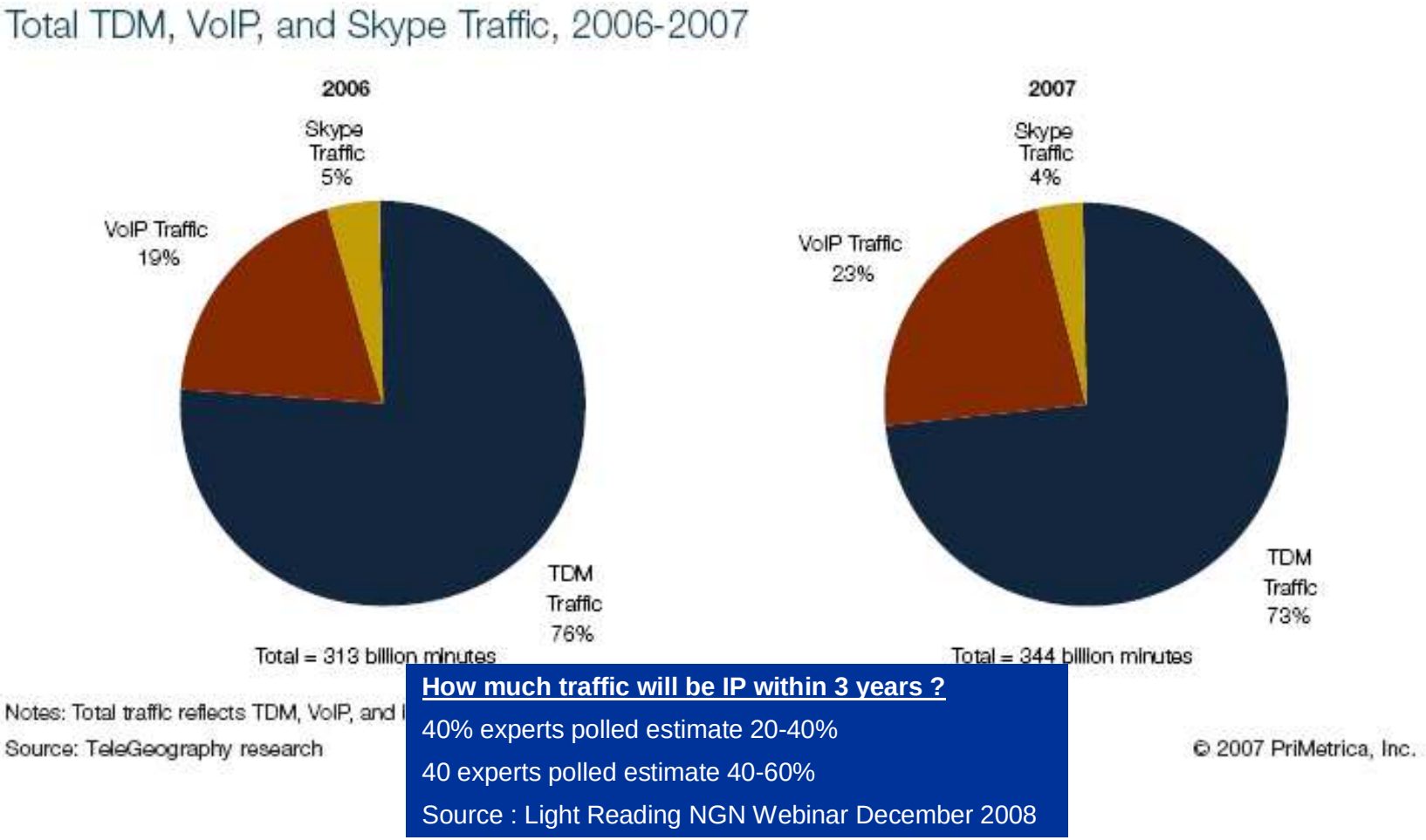


Changing nature of voice interconnect traffic…



An increasing percentage of voice traffic is native VoIP, but we are still some years away from an inflection point (VoIP traffic equaling TDM traffic). There will be lots of TDM infrastructure around for the foreseeable future, and a need to connect to both IP and TDM networks.

Changing nature of voice interconnect traffic…



How much traffic will be IP within 3 years ?

40% experts polled estimate 20-40%

40 experts polled estimate 40-60%

Source : Light Reading NGN Webinar December 2008

An increasing percentage of voice traffic is native VoIP, but we are still some years away from an inflection point (VoIP traffic equaling TDM traffic). There will be lots of TDM infrastructure around for the foreseeable future, and a need to connect to both IP and TDM networks.

Mobile networks/handsets - evolution

- Mobile phones overtook the number of fixed-line phones worldwide in 2002 – currently about 70% of the world's telephone lines are mobile
- Mobile LTE (long-term evolution) architecture implies voice calls from handset will natively be VoIP in the future
- GSM Association promoting IPX service architecture to handle IP interconnect for this (and other IP) traffic between mobile (and fixed) carriers - more details on this later in the presentation

Cisco Networkers 2009
January 26-29 Barcelona, Spain

Interconnect Standards Overview

TDM Interconnect Standards

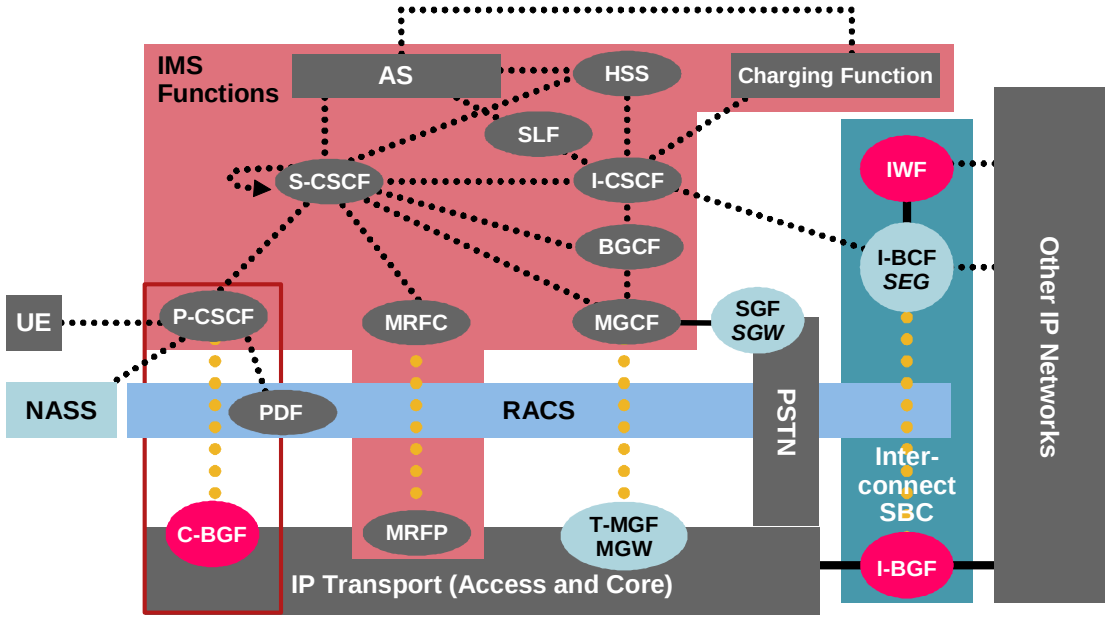
- TDM Connectivity
  - Well established TDM Interfaces & protocols – SS7, PRI etc
  - Well defined international standards from ITU/ETSI with national variations
  - Regulated interconnects – specified from a technical and commercial perspective. Typically mandatory for incumbent to offer
  - Unregulated interconnects – technical and commercial model established on a bi-lateral basis
- Cisco's established TDM/VoIP solution is the most widely deployed solution amongst all industry players

NGN Interconnect Standards

- IP Peering standards
  - Still evolving in most cases
  - Current peering mostly based on bi-lateral technical and commercial models
  - Three areas in play
    - International standards : ETSI/3GPP IMS & TISPAN
    - Industry architecture : GSMA IPX
    - National Standards: NICC

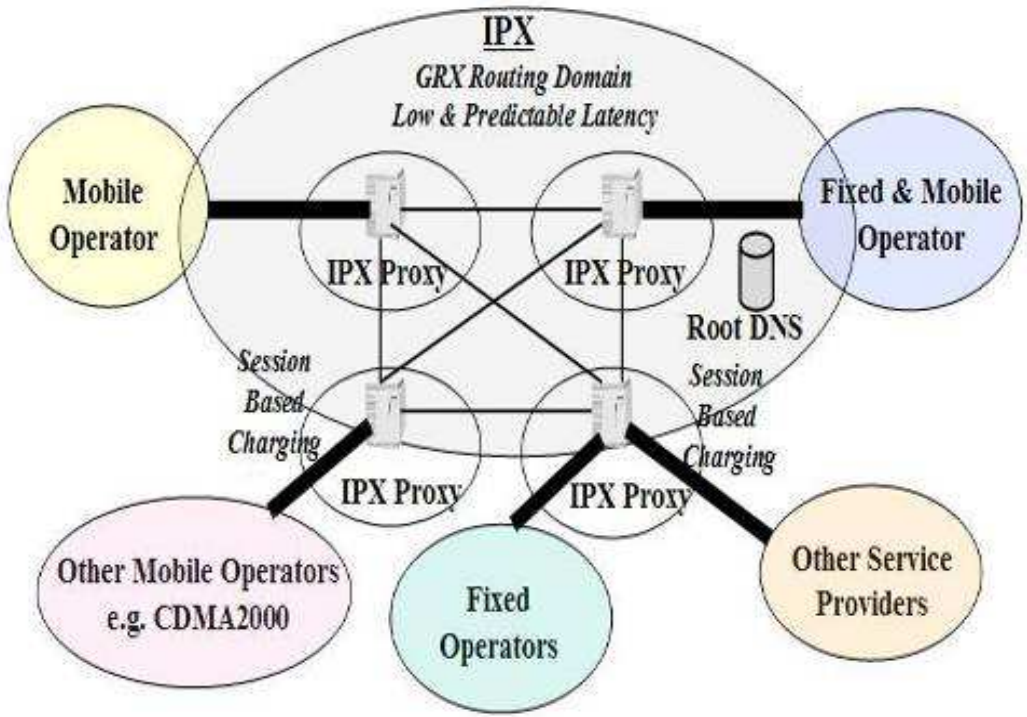
IMS & TISPAN

- 3GPP & ETSI defined blueprint for NGN architecture
- Being used by mobile operators and Tier 1s as basis for service evolution
- Uses SIP as underlying protocol
- Highly complex and requires SI capability
- Incorporates a discrete TDM & IP interconnect component which can be separated from core and access components.



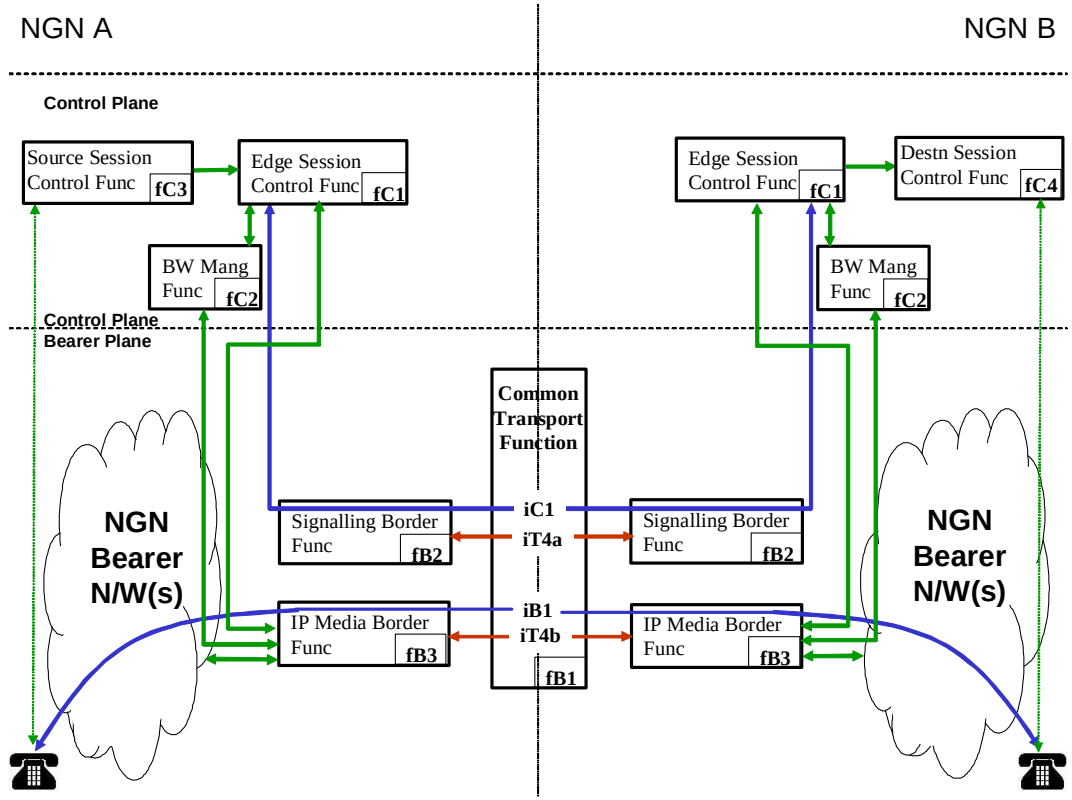
IP Packet Exchange (IPX)

- IPX builds on top of GRX adding:
  - Connectivity to non-GSM SPs
  - New charging models (beyond volume)
  - End-to-end QoS
  - Service interworking
  - Multilateral support
- Multiple options incl
  - Transport Only
  - Transport and Services
- Multiple Services incl
  - IP Voice
  - IP Video
  - Presence
  - Instant Messaging
- **SBC Provides typical NNI functionality (Network Connectivity, QoS, Security, Billing)**



National Standards

- Slow to develop – linked to large scale PTT NGN evolution
- UK NICC
  - A UK standards organisation compriding operators, vendors and regulators
  - Responsible for defining the “regulated” interconnects in the UK
  - Defined a IP/IP interconnect for BT 21CN
  - Based on SS7 and IMS concepts – ND1612
  - www.nicc.org.uk



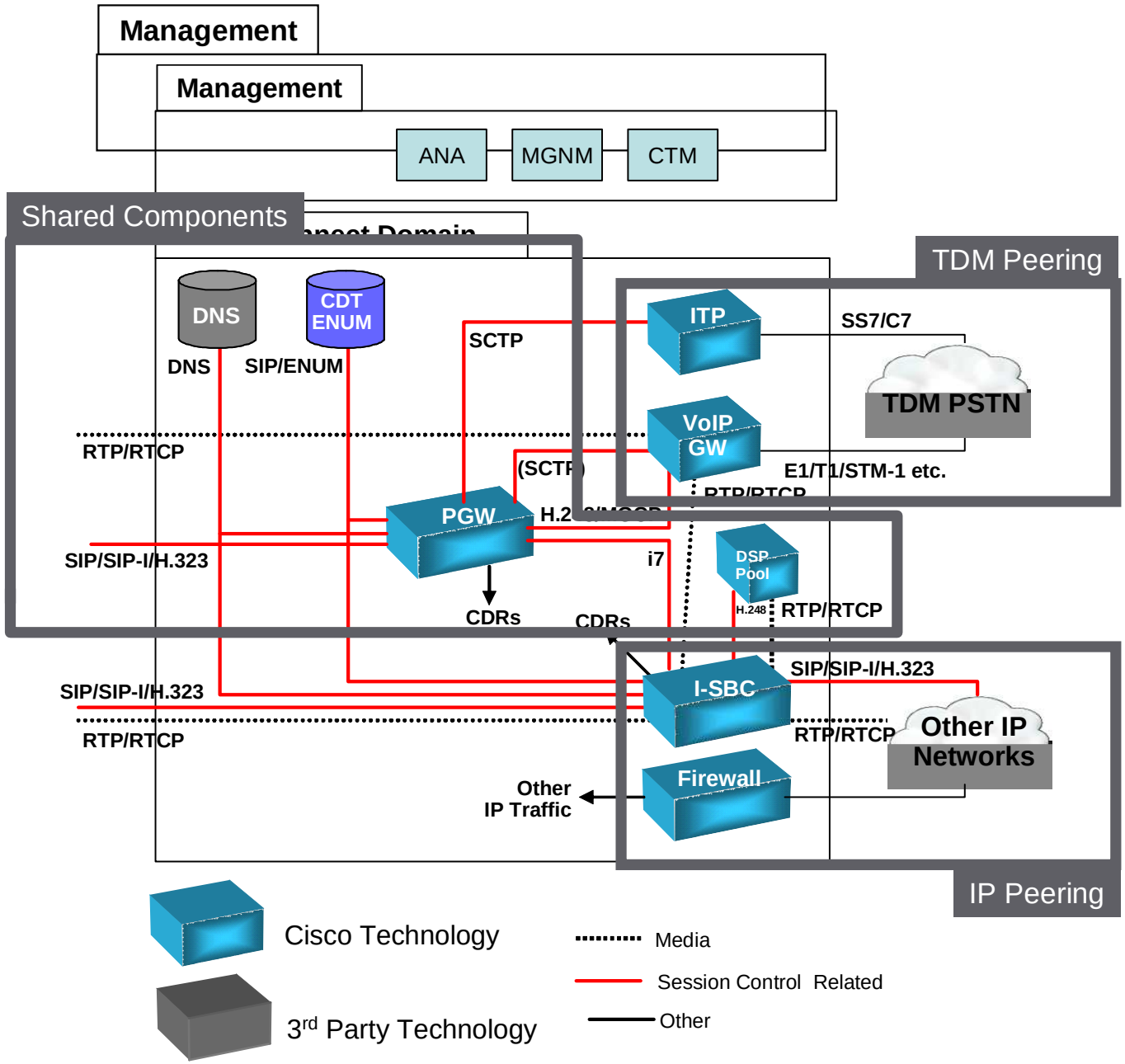
Cisco Networkers 2009
January 26-29 Barcelona, Spain

Interconnect Architecture & Key Attributes

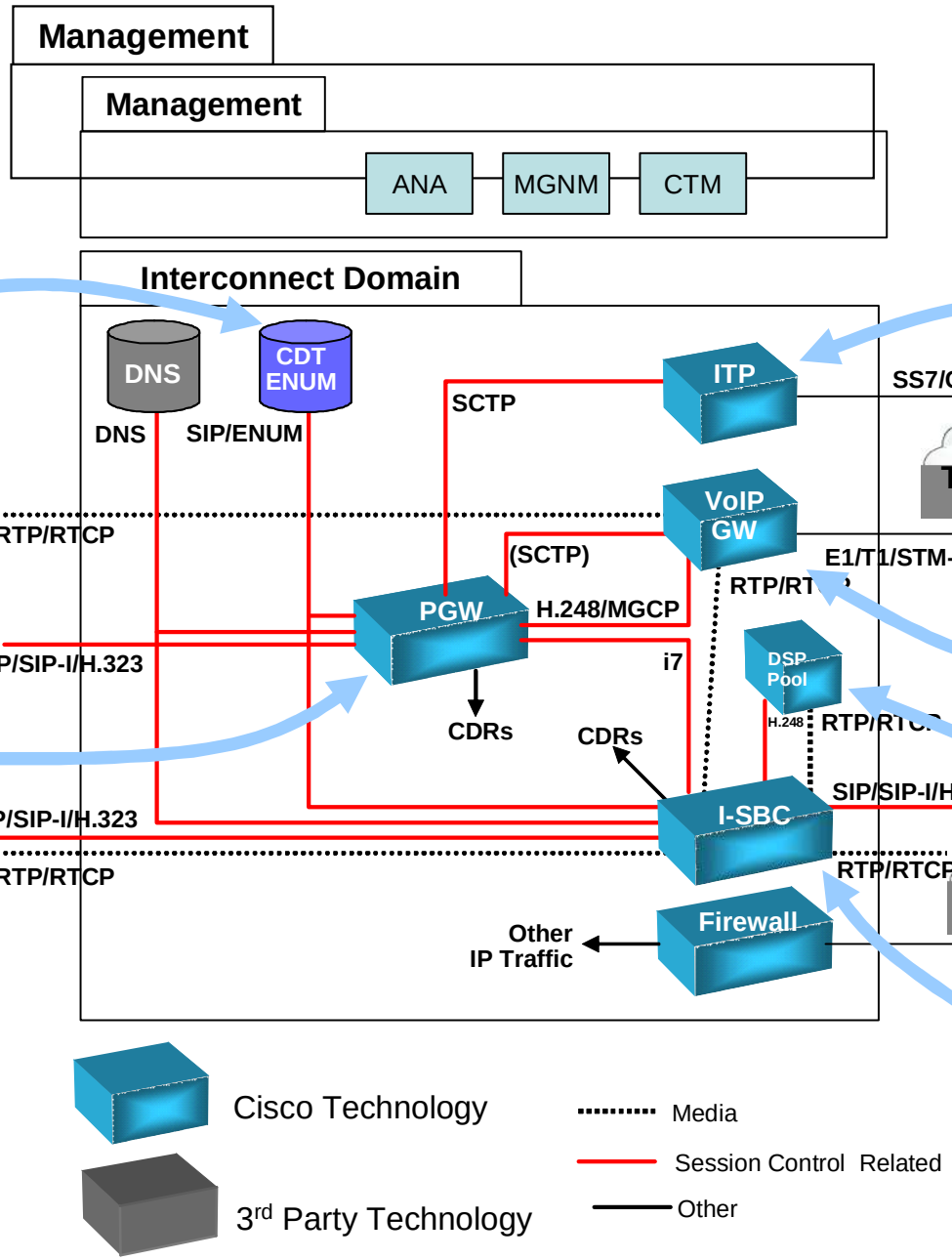
Anatomy of an Interconnect

- A peering relationship between carriers consists of both technical and comercial frameworks
- Key aspects that technical framework
  - Signalling
  - Addressing
  - Routing
  - Security
  - Availability
  - Accounting
  - Transcoding

Cisco Interconnect Architecture



Cisco Interconnect Architecture



CDT

Carrier ENUM platform that can be used as a central address translation database (for services such as freephone or LNP) or as a centralised routing database.

PGW2200

Cisco multiprotocol softswitch technology provides interworking between TDM and IP protocols as well as a highly scaleable and flexible routing engine

Internet Tranfer Point (ITP)

Provides signalling mediation function between TDM SS7 and SSoIP (SIGTRAN compliant node

MGX or AS5x00

Cisco media gateway technology provides best in class TDM to VoIP interworking for many voice "services".

MGX

Transcoding resource

Cisco SBC

Cisco Carrier Class SBC technology provides a media mediation function between IP networks.

- Signalling
- Addressing & Ruting
- Security
- Availability
- Accounting
- Transcoding

Signalling

Addressing & Ruting

Security

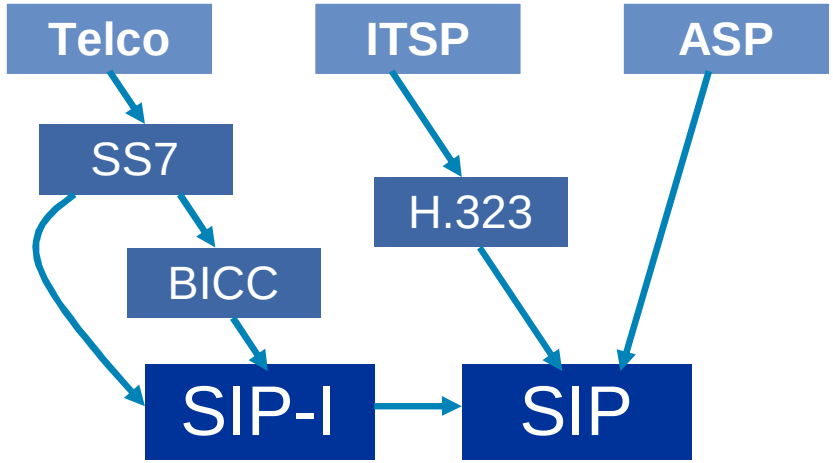
Availability

Accounting

Transcoding

Interconnect : Signalling Plane

- Application Layer
  - ITU-T & ETSI SS7
  - ITU-T Q.1901 BICC – evolved ISUP to cater for packet transport
  - ITU-T H.323 used by most early adopters
  - Session Initiation Protocol
    - IETF RFC3261 base SIP - (obsoletes RFC 2543/ updated by RFC 3853,RFC 4320) + many more*
    - ITU-T/ETSI define implementation specifics
      - Q.1912.5 Profile C – SIP-I
      - ETSI SIP-I *(Insert Ref)*
      - TS 124 229 – IMS SIP



* For a list of the IETF related SIP RFCs: **http://www.sipknowledge.com/SIP_RFC.htm**

SIP-I vs SIP

- SIP-I essentially uses SIP to "transport" ISUP signalling which is used to drive the session
  - SIP-T SIP for Telephony – RFC3372 (defines mime encapsulation of telephony signalling)
  - ITU-T Q.1912.5 SIP ISUP & BICC Interworking – more specifically defined than SIP-T
    - Profile A – 3GPP SIP ISUP Mapping no encapsulation
    - Profile B – IETF SIP ISUP Mapping no encapsulation
    - Profile C (SIP-I) – as per prfile B but with ISUP encapsulation (multipart MIME attachment)

Generic SIP INVITE

SIP Header

```
INVITE sip:23198@172.17.207.91:5060 SIP/2.0
Via: SIP/2.0/UDP 10.80.17.134:5060
Via: SIP/2.0/UDP 172.18.192.232:5060;branch=1FV1xhfvxGJOK9rWcKdAKOA
To: <sip:23198@172.18.192.232>;tag=abc
From: <sip:15691@10.80.17.134>;tag=a73kszlfl
Call-ID: c2943000-50405d-6af10a-382e3031@10.80.17.134
CSeq: 100 INVITE
Contact: sip:15691@10.80.17.134:5060
Expires: 180
Content-Type: application/sdp
Content-Length: 219
User-Agent: Cisco IP Phone/ Rev. 1/ SIP enabled
Accept: application/sdp
Record-Route: <sip:23198@172.18.192.232:5060;maddr=172.18.192.232>
```

body

```
v=0
o=CiscoSystemsSIP-IPPhone-UserAgent 17045 11864 IN IP4 10.80.17.134
s=SIP Call
c=IN IP4 10.80.17.134
t=0 0
m=audio 29118 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
```

SIP-I vs SIP

- SIP-I essentially uses SIP to "transport" ISUP signalling which is used to drive the session
  - SIP-T SIP for Telephony – RFC3372 (defines mime encapsulation of telephony signalling)
  - ITU-T Q.1912.5 SIP ISUP & BICC Interworking – more specifically defined than SIP-T
    - Profile A – 3GPP SIP ISUP Mapping no encapsulation
    - Profile B – IETF SIP ISUP Mapping no encapsulation
    - Profile C (SIP-I) – as per prfile B but with ISUP encapsulation (multipart MIME attachment)

SIP-I INVITE

SIP Header

```
INVITE sip:23198@172.17.207.91:5060 SIP/2.0
Via:  SIP/2.0/UDP 10.80.17.134:5060
Via: SIP/2.0/UDP 172.18.192.232:5060;branch=1FV1xhfvxGJOK9rWcKdAKOA
To:  <sip:23198@172.18.192.232>;tag=abc
From:  <sip:15691@10.80.17.134>;tag=a73kszlfl
Call-ID:  c2943000-50405d-6af10a-382e3031@10.80.17.134
CSeq:  100 INVITE
Contact:  sip:15691@10.80.17.134:5060
Expires: 180
Content-Type: multipart/mixed;boundary="testing"
Content-Length: 299
Record-Route: <sip:23198@172.18.192.232:5060;maddr=172.18.192.232>
```

body

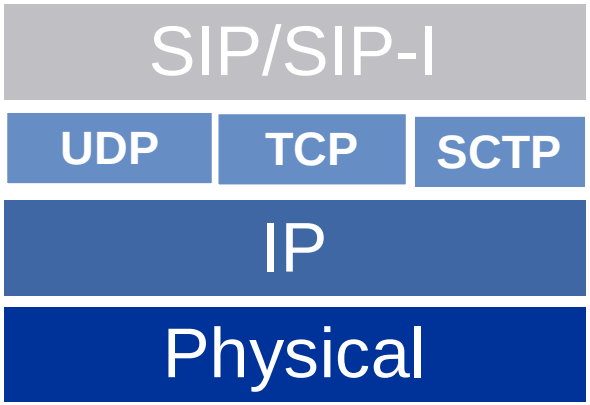
```
MIME-Version: 1.0
--testing
Content-Type: application/sdp
v=0
o=- 2890844526 2890844526 IN IP4 10.11.30.4
s=-
c=IN IP4 10.11.30.4
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
--testing
Content-Type: application/isup; base=ansi88; version=ansi
01 00 00 00 00 03 0f 16 0c d0 18 10 98 9e !,` c0 c6 e6 07 03 10 t'"00 10
07 03 10 t17 11 00 10 00
--testing-
```

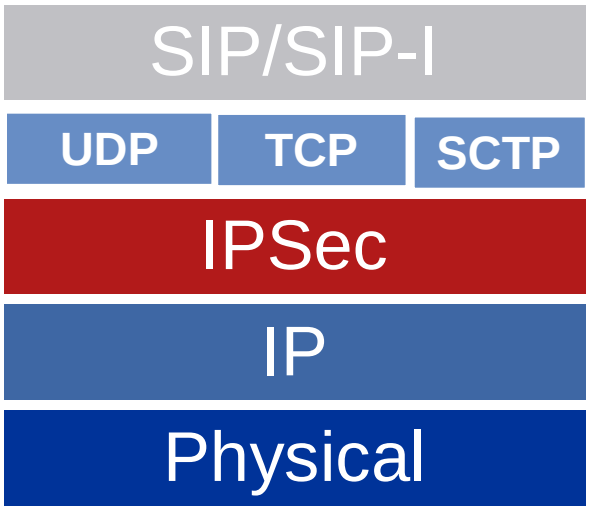
MIME encapsulated SDP

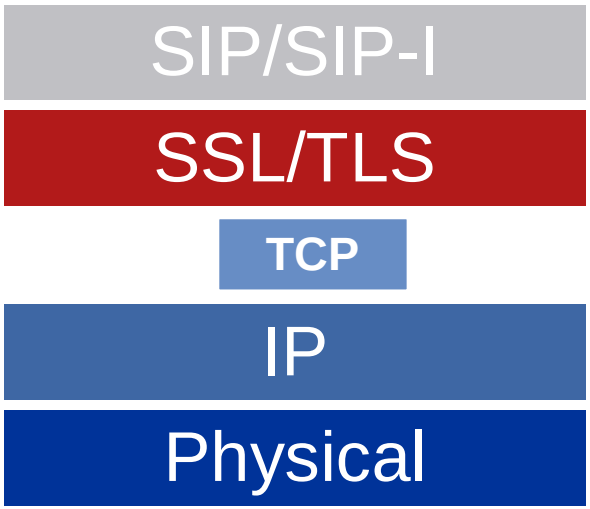
MIME encapsulated ISUP

Interconnect : SIP Transport

- Transport Later
  - UDP currently most common
  - SCTP includes multi path redundancy and heartbeat mechanism
- Encryption
  - TLS (SIPS URI)
  - IPSec







Interconnect : Media Plane

- Media described by Session Description Protocol (SDP) – RFC 2327
- Media Transport
  - Real Time Protocol/Real Time Control Protocol (RTP/RTCP)
    - RFC 3550 (replaces 1889)
    - RFC 2833 payload for DTMF
    - RFC 3711 – Secure RTP (sRTP)
  - Others
    - MSRP RFC 4975 (Message Session Relay Protocol)
    - RTSP RFC 2326 – Real Time Streaming Protocol

Signalling

Addressing & Ruting

Security

Availability

Accounting

Transcoding

Addressing for Multimedia Services

- Currently most services and applications are using numberic E.164 based addresses as this is supported by the vast majority of devices
- Moving forward URI based addressessing is predominantly the focus
- Peering points will need to cater ofr multiple addressing formats and be required to normalise and interwork between differering formats.

URI Based Addressing

- Fully-Qualified Domain Names
  sip:jdoe.cisco.com
- SMTP-style Domain Names
  sip:jdoe@cisco.com
- E.164 style addresses
  sip:14085551234@gateway.com; user=phone
  user=phone means this is a gateway
  (gateway.com is the FQDN of the egress IP gateway)
- Mixed addresses
  sip:14085551234@10.1.1.1; user=phone
  sip:jdoe@10.1.1.1
- Secure address:
  sips:mi5@uk.govt.biz **(mandatory for TLS)**
- Telephone URI
  tel:+358-555-1234567
  tel:1234567;phone-context=+358-555
  'phone-context' is the parameter used to specify the local context in which the Tel URI is valid.
  tel: +1-800-234-5678;cic=2345
  CIC is carrier id code

Session Routing

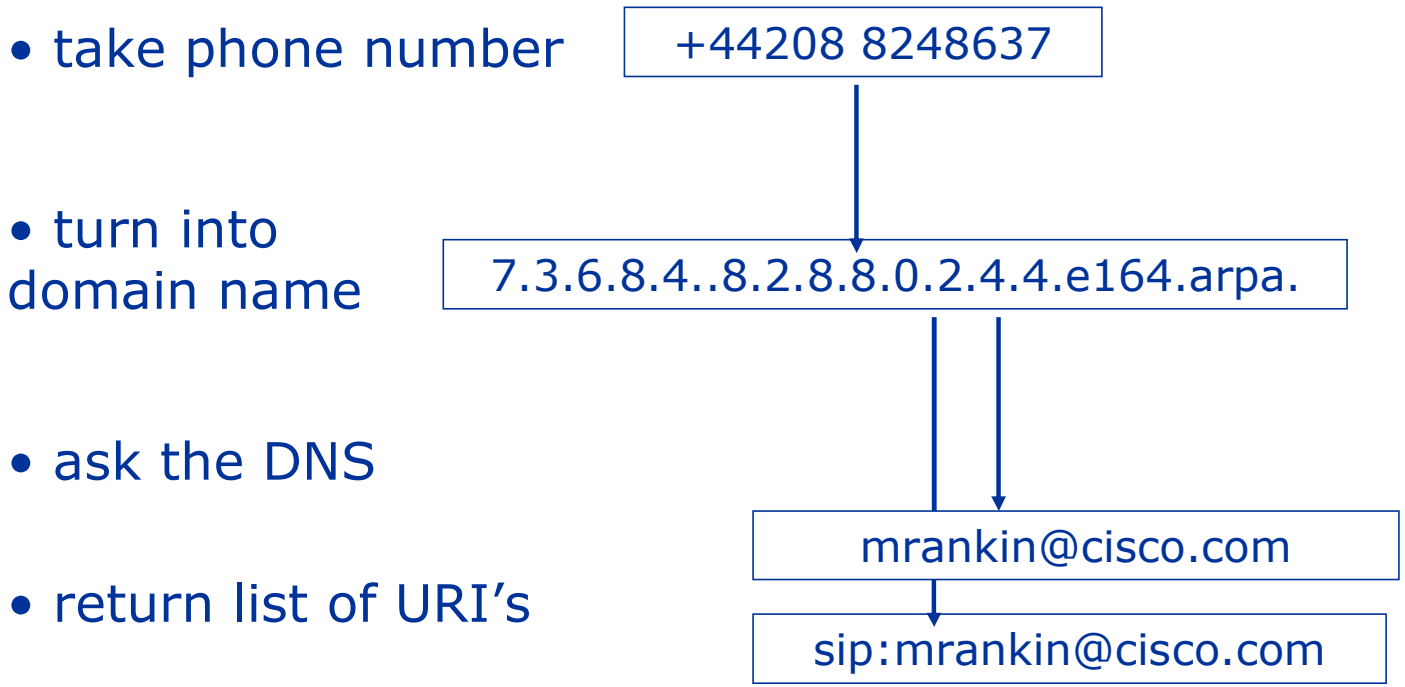
- Historically and currentlky most route determination is done by digit analysis of an E.164 numbers – essentially matching patterns against predefined destinations (or dets of destinations)
- As URI based addressing becomes widespread then additional options become available

  Simple domain name routing – i.e. change analysis to match on domain part of URI either via DNS or via local logic

  ENUM
- Using these later techniques however means that complex route selections such as Least Cost, Time of Day, ASR etc must be implemented mostly in the “database” layer

ENUM

- General ENUM
  - IETF RFC 3761
  - Essentially applies DNS techniques to resolving numeric addresses
  - Intended to be used to link subscribers and provide simple one address reach capabilities
- “Carrier ENUM”
  - is being used internally by many SPs for Number Portability and routing purposes (e.g. LCR etc)
  - Can be used to link carriers – i.e. determine which carriers are hosting a given e.164 numeric address (requires linking)

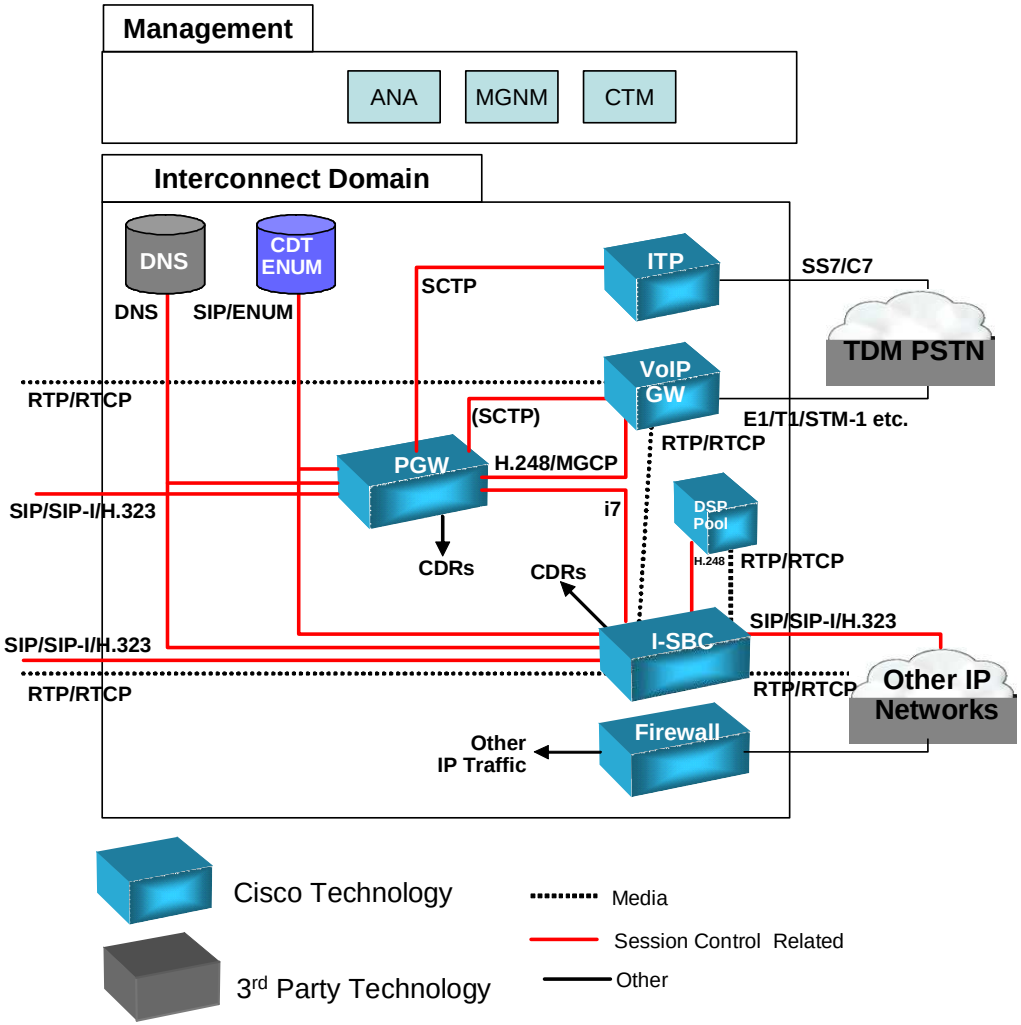


Cisco support

- Cisco Database for Telephony (CDT)
- Clients

  PGW 2200 Rel 9.8

  SBC Rel 3.2 (can use INVITE/3xx REDIRECT now)



Signalling

Addressing & Ruting

Security

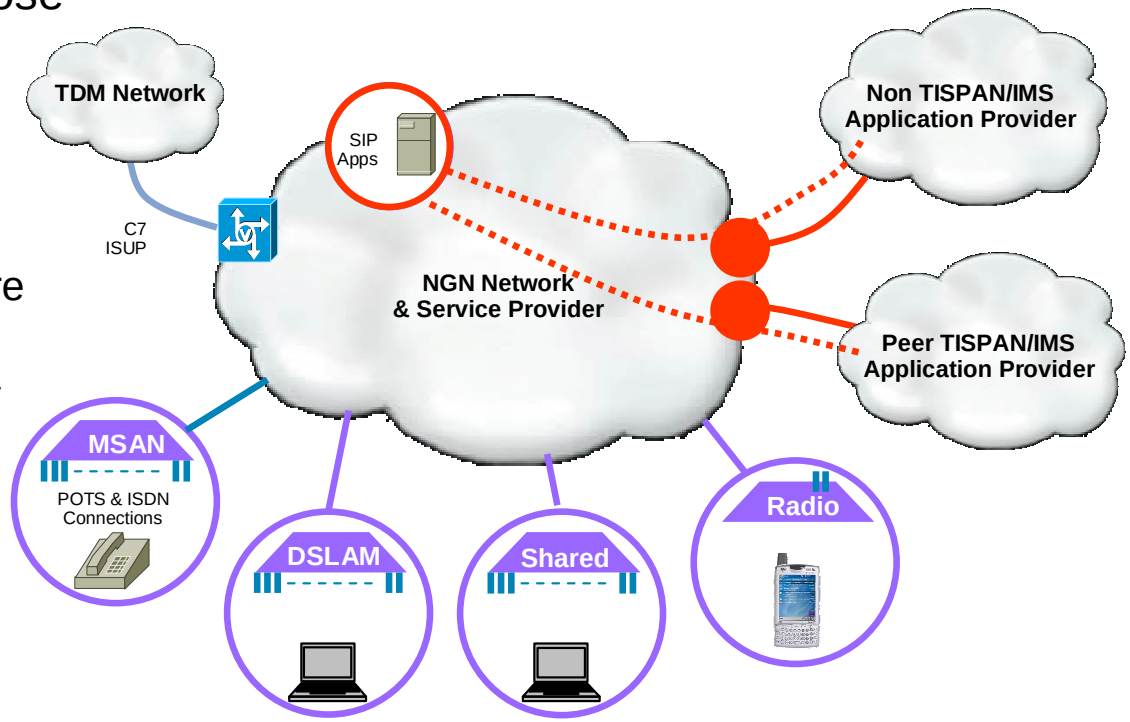
Availability

Accounting

Transcoding

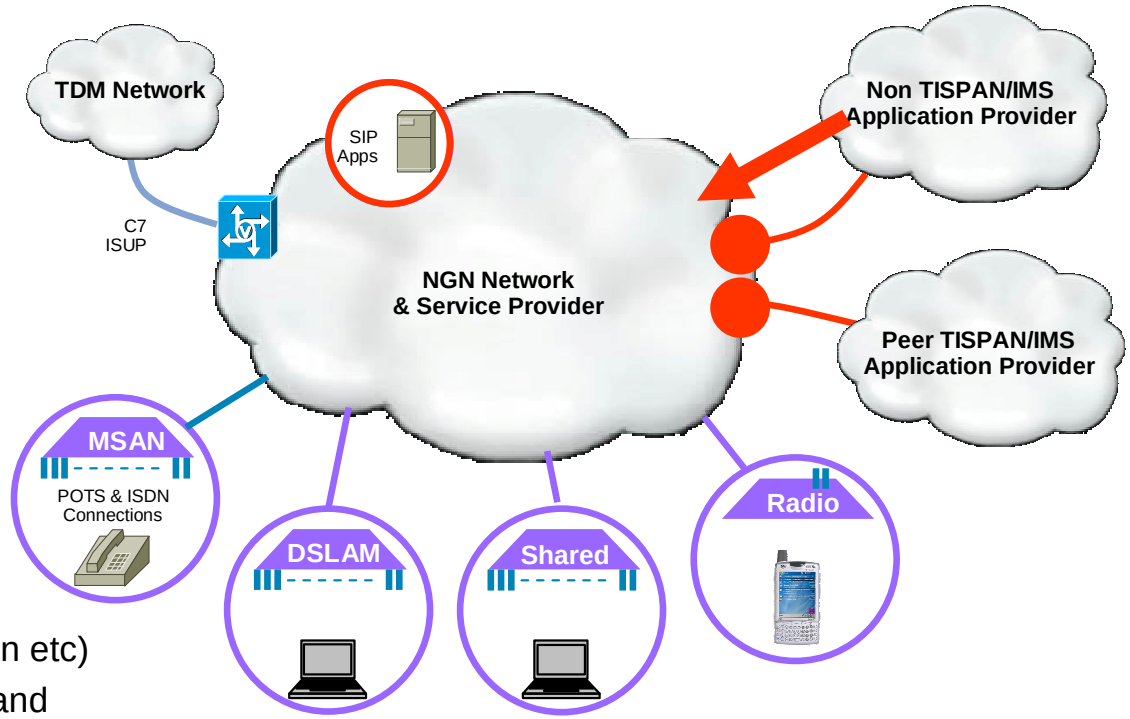
Peer Network Risks

- POTS/ISDN “legacy” interfaces pose no increase in risk
- Risk Introduced as IP-IP peering provided
  - Predicted to be many such interconnects as hardware/software costs may be lower
  - Cannot trust peer network security capabilities
- VoIP Risk Categories
  - DoS/DDoS
  - Theft of Service
  - SPAM/SPIT



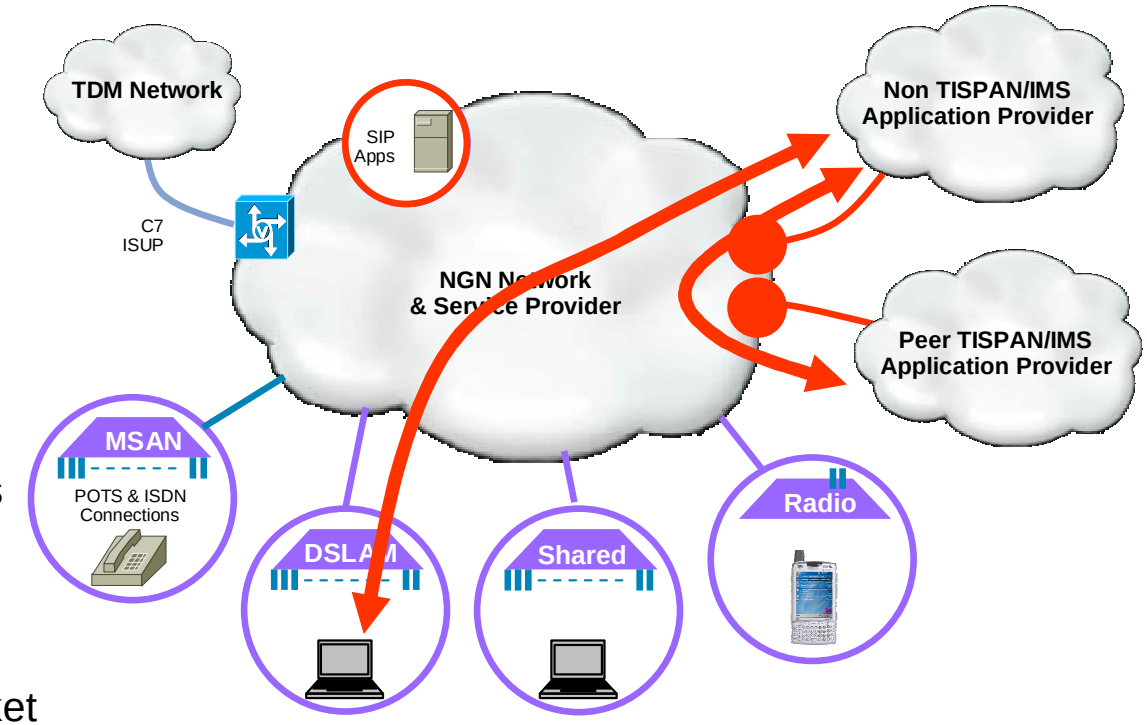
Peer Network Risks : DoS & DDoS

- Types of threat
  - Protocol Level (malformed, large, fragmented SIP)
  - Traffic Load towards SIP/RTP ports
- Targets
  - Interconnect Point/Points
- Source
  - Usually “trusted” source
  - Unexpected source(s)
- Risk Mitigated by
  - Secure & Encrypted Signalling to known peers only (IPSec. SCTP)
  - General IP Security concepts and techniques (ACLs, DoS, DDoS protection etc)
  - SIP policing, RTP pinhole opening Call and message based overload controls (SBC or decomposed model)



Peer Network Risks : Theft of Service

- For peer network connectivity theft of service would typically be limited to bandwidth theft at the point of interconnect
  - Sessions to a hosted subscriber
  - Sessions to another peer
  - Requires pre-arrangement and software hacks but doable – negotiate one codec and use a higher bit rate.
- Risk Mitigated by
  - Lockdown signalling relationships to know peers and securing and encrypting them
  - Dynamic RTP pinhole opening
  - Media policing – i.e. enforce packet stream to confirm to negotiated profile (SBC media border element)



Peering Security

- IP Peering introduces many new aspects to securing the service layer
- We have the concept of untrusted and (more) trusted peering relationships
- Need to cater for
- IP Layer Attacks
  - Classic Attacks targeted at the platform
- Application Protocol Level Attacks
  - Signalling Plane – SIP/H.323 protocol level attacks (load, corrupt, spoofing etc) – Codenomicon tests and load tests
  - Media Plane Attacks – attacks at open and closed media addresses (bandwidth/ptime, spoofing, scanning etc)
- Load Based Attacks
  - Simple message rate overload attacks – can be both session initiation attempts or individual SIP messages related to information passing
  - Can be height volume from single source or low volume from many sources
  - Can be intentional/malicious, caused by a network failure or a mass call event

Some Basic Protocol Level Risks

- **Legal but likely not implemented**
- whitespace everywhere (around colons, around semicolons);
- **no** space after colons;
- continuation lines: everywhere there can be whitespace (including around colons, around semicolons, after colons, in the middle of things like CSeq and Via);
- case: cAmEl CaSe headers, other case-insensitive fields;
- empty values in unstructured headers (e.g. Subject);
- unknown Require/Proxy-Require headers;
- Surprising header ordering (Via last, Via in the middle);
- Comma-separated values;
- Mixed comma-separated and header-separated values for the same header;
- Expires after 2000, after 2038, after 9999 (five-digit years aren't legal, but the implementation shouldn't crash);
- Expires: 1;
- Unknown schemes in Request-URI, To, From, Contact (is this really legal for INVITE)?
- Unknown header field names;
- Unknown parameters of known headers;
- Check how header formatting gets through a proxy;
- INVITE Requests with Accept: but not listing application/sdp;
- INVITE Requests without application/sdp payloads;
- INVITE to a multicast session;
- INVITE with "blank" SDP (e.g., for H.323 interop);
- Unknown methods (for proxies);
- Unknown authentication schemes;
- Multiple requests in a UDP packet;
- Extra bytes at end of UDP packet;
- Christmas-tree Via headers;
- Dozens of Via headers (there should be no limit, beyond message size constraints, to the number of Via headers understood);
- Very long messages, up to UDP maximum packet size (i.e., including fragmentation and reassembly);
- Short-form, long-form, both for the same header field;
- Evil quoting games: "This ends with a backslash: \\" "This ends with a backslash and a quote: \\\""
- Extra whitespace between requests (this is legal!)
- versions other than SIP/2.0
- Extremely long URLs, To and From fields (to make sure SIP implementations don't become vehicles for buffer overrun attacks)
- URLs containing semicolons in the "user" part

- **SDP**
- Various charsets.
- Future sessions.
- Several session dates and repeats, as in sdr.
- **Not Likely to be Implemented Yet**
- MIME multipart
- **Illegal but shouldn't crash you:**
- CSeq out of order
- missing any or all of To/From/Call-ID/CSeq
- multiple of any or all of To/From/Call-ID/CSeq
- multiple of other non-repeatable headers
- empty values or parameters (,, or ;;)
- CSeq method and Header method disagree
- gibberish in Request-URI
- broken Date fields; syntactically or semantically
- case-sensitive fields in the wrong case (E.g., invite sip://foo)
- Via: 255.255.255.255
- Via: 127.0.0.1
- Via: nonexistenthost.example.com
- wrong Content-length
- garbage after request
- un-terminated quotes
- un-terminated < in Contact
- splitting request and response across TCP connections
- out-of-range status code (e.g., 704)
- appropriate handling of unexpected protocols (e.g. "GET /~hgs/sip/ HTTP/1.1")
- **Undefined Behavior**
- multicast requests that require authentication (401)

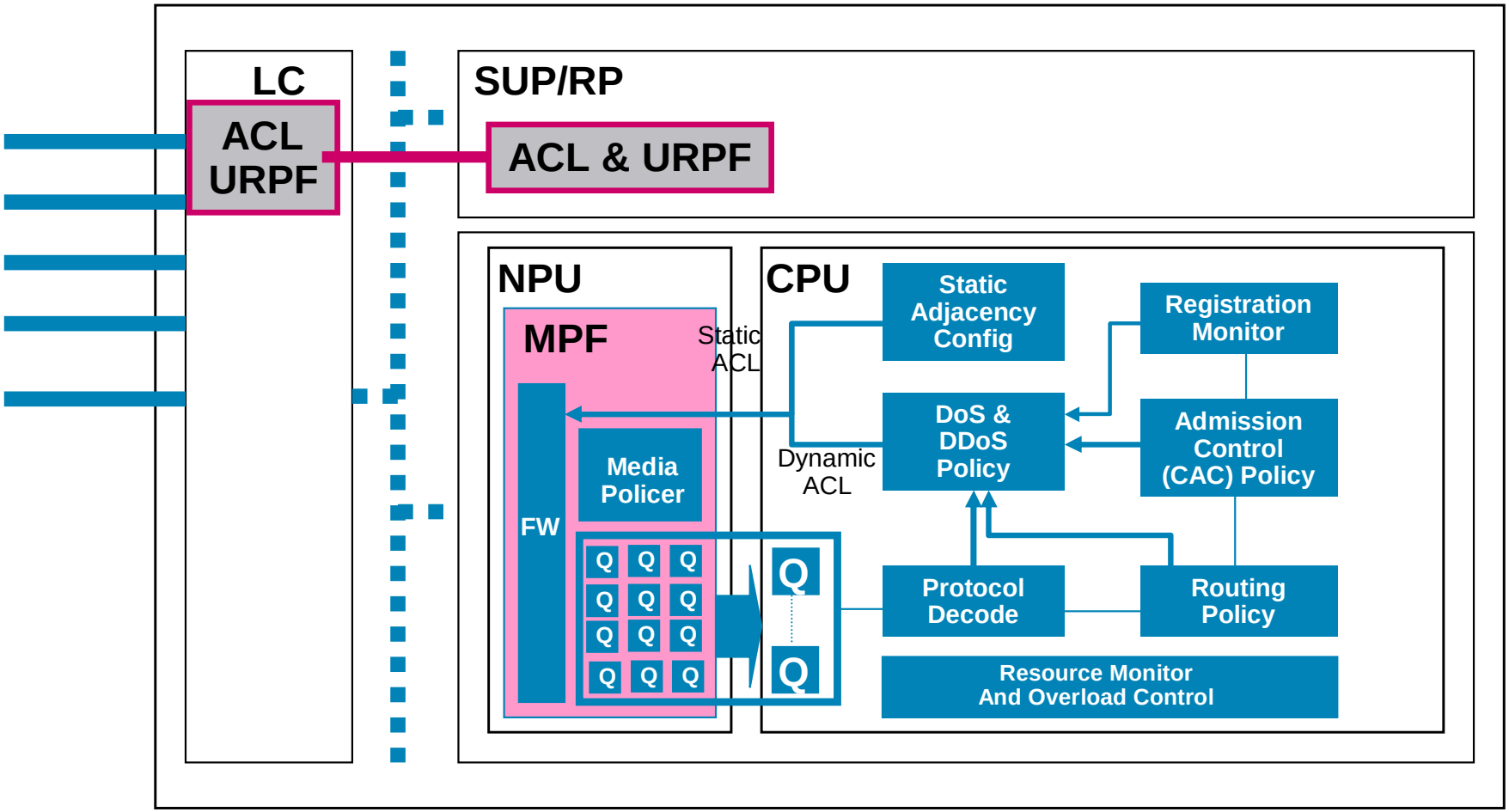
RFC 4475 ‘sip-torture-tests’

Addressing the risks

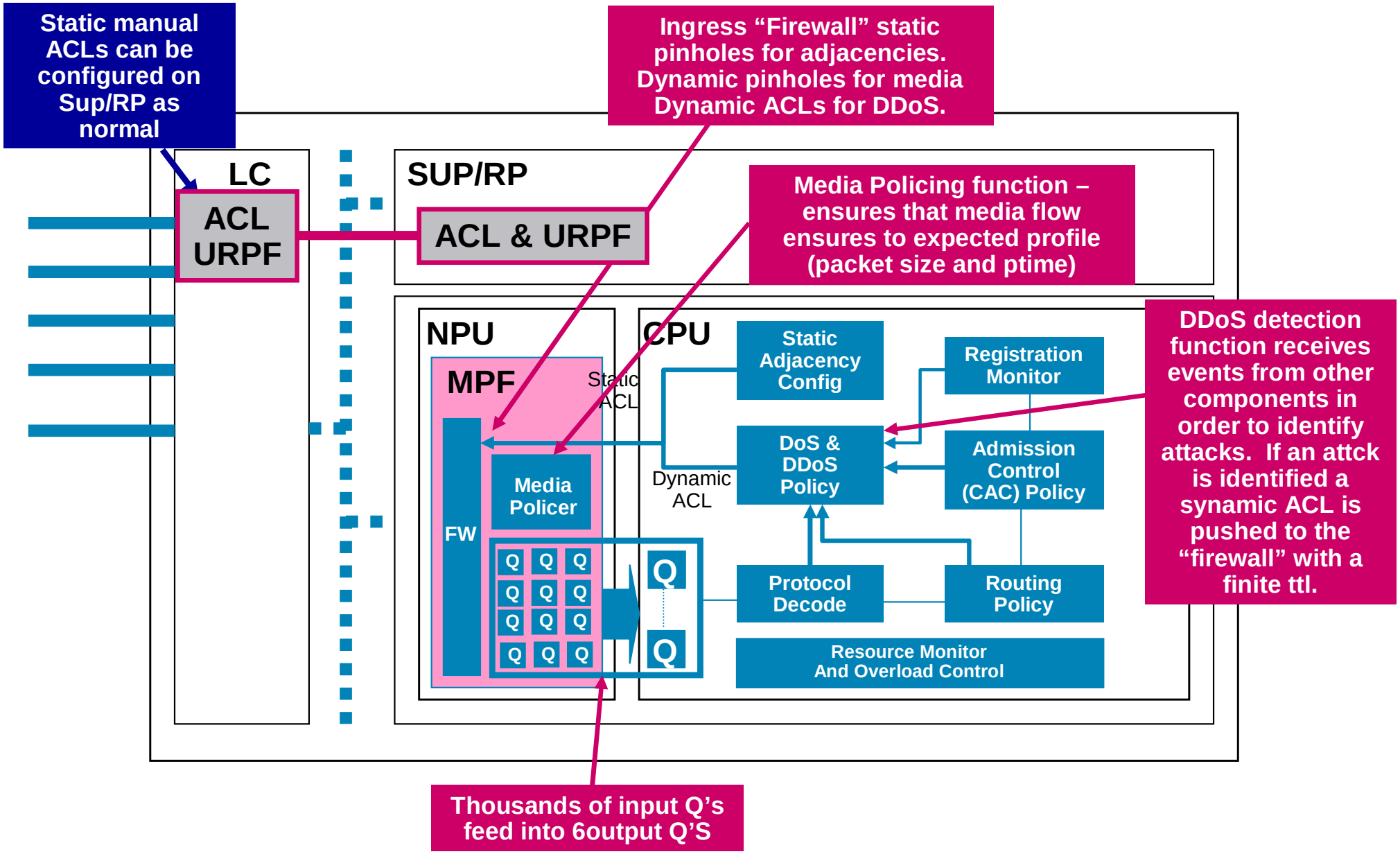
A numer of security technologies can play a role in addressing the issues – it just depends what you are concerned about…..

Risk	Firewall	SBC	Other	Notes
Network Topology Hiding	P	Y	ALG	**Obscure identies and addresses of infrastructure equipment**
Theft of Service	N	Y		**Enforce negotiated media flows**
Protocol Normalisation	N	Y		**Only allow standard messages and paramters**
Signalling Security	P	Y		**Encrypt signalling and potentially media**
DoS/DDoS	P	Y		**Mittigate all forms of mallicious or unintentional attack**

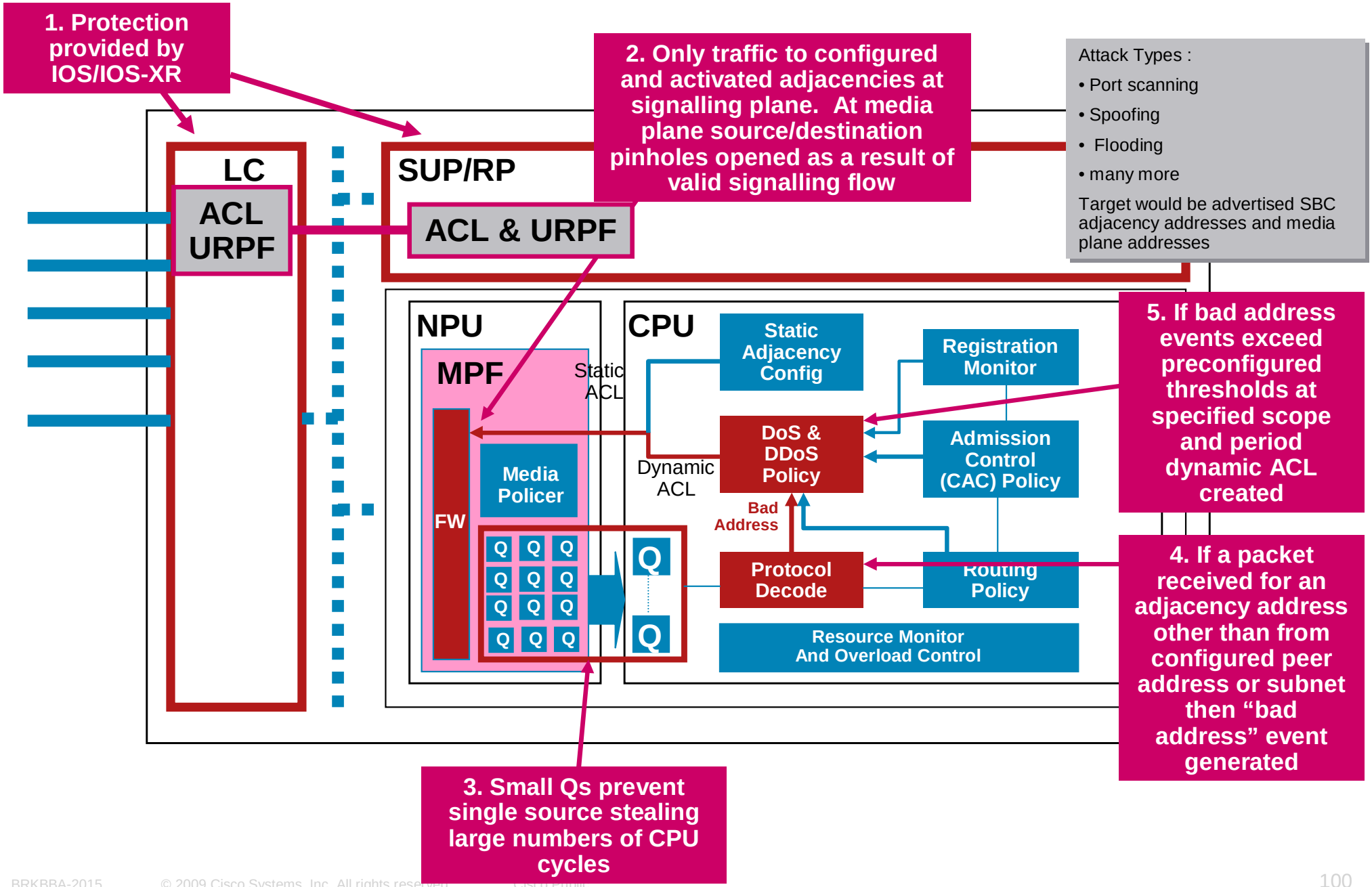
Cisco SBC Protection Points



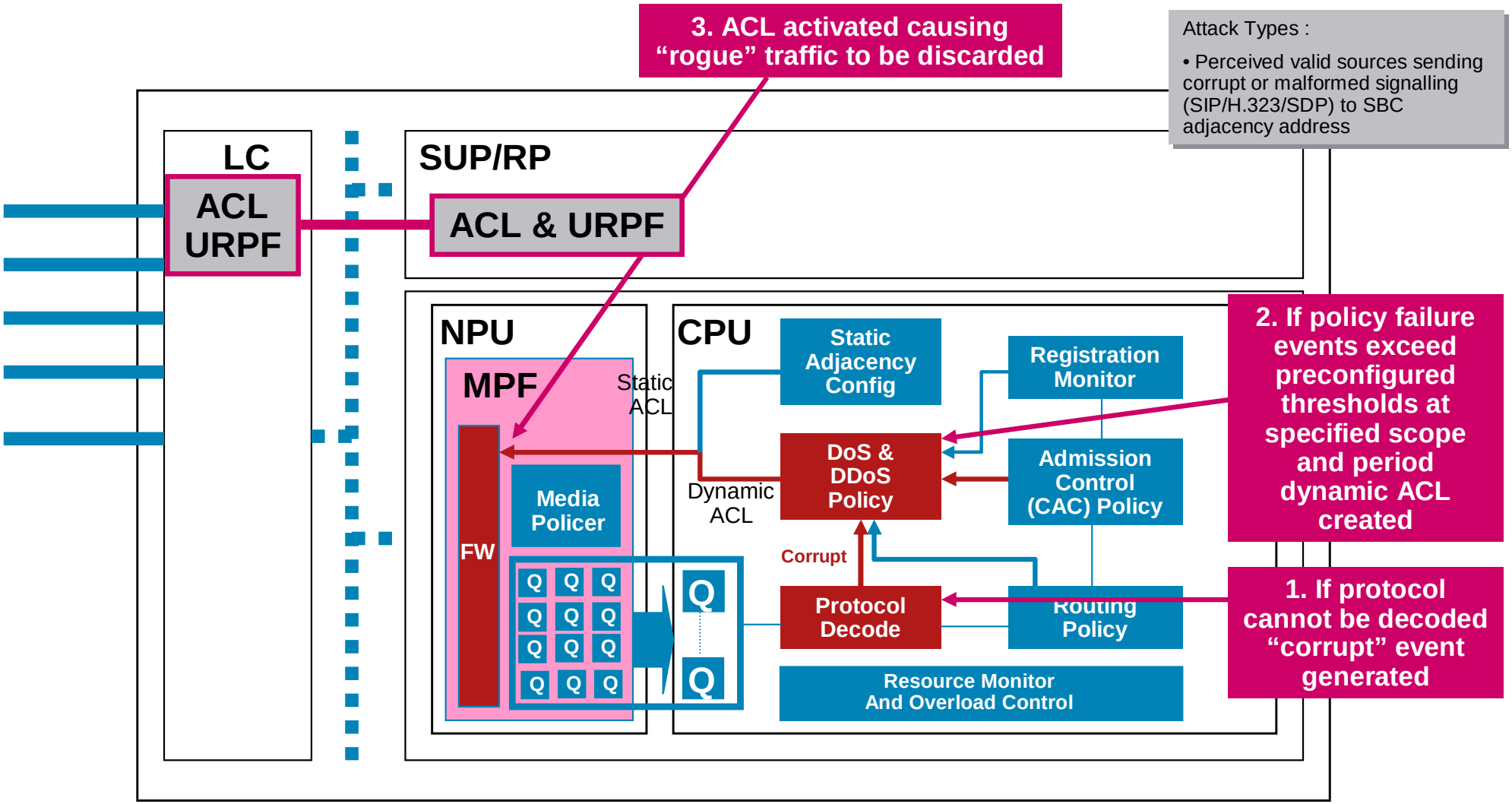
Cisco SBC Protection Points



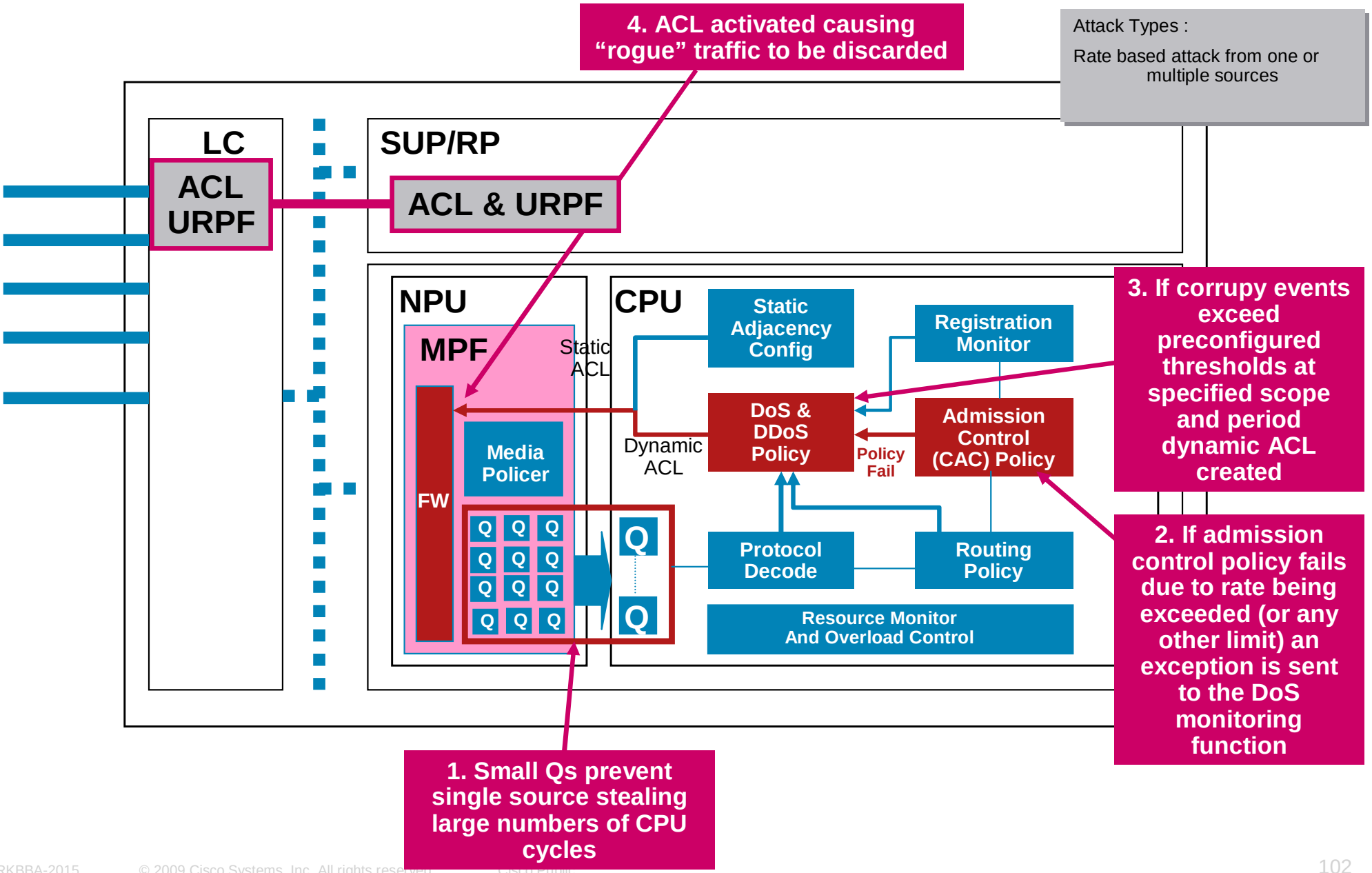
IP Level Attacks



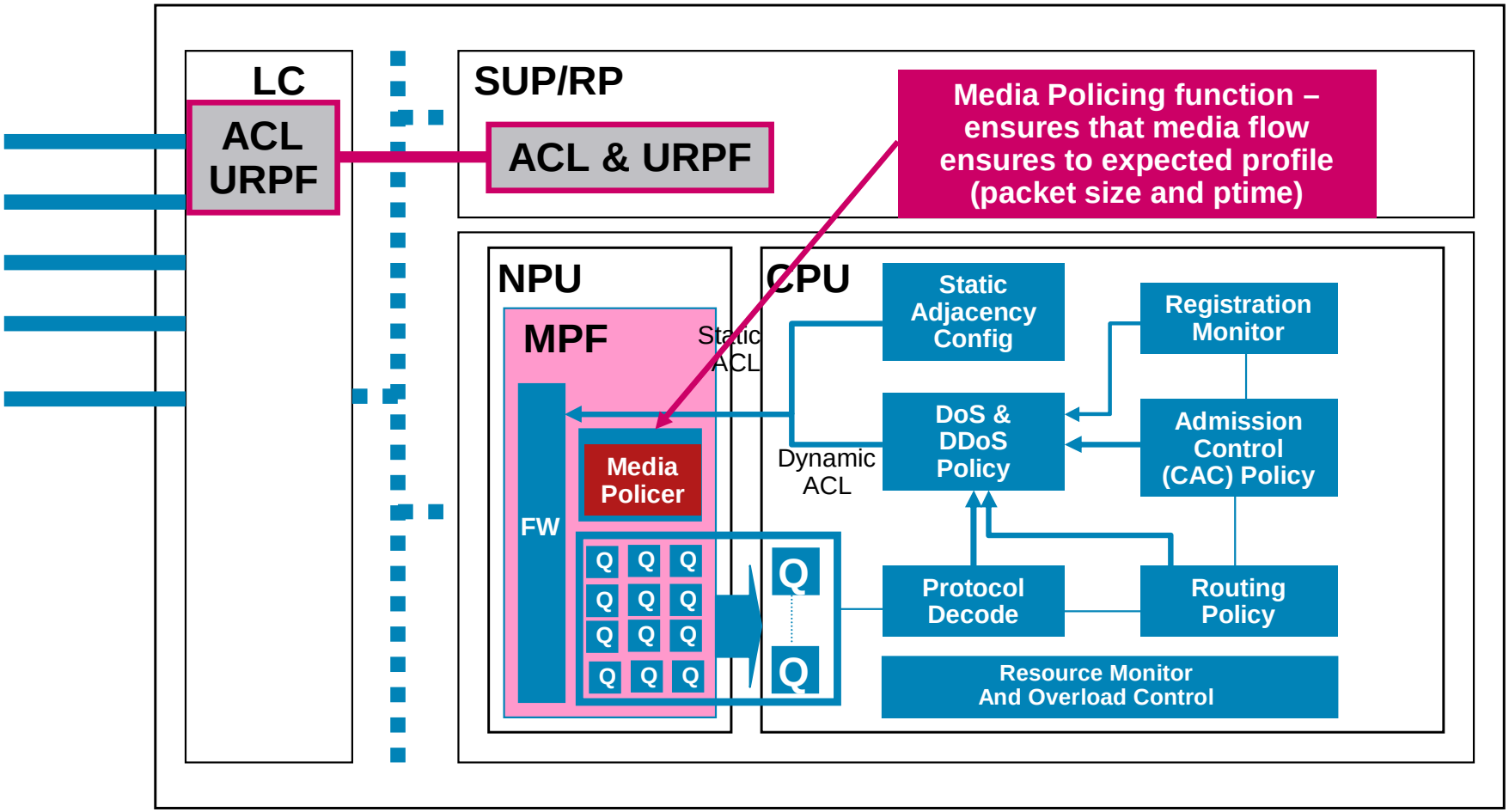
Signalling Plane Attack : Protocol Corruption



Signalling Plane Attack :Load



Media Plane Attack : Load & Malformed



Signalling

Addressing & Ruting

Security

Availability

Accounting

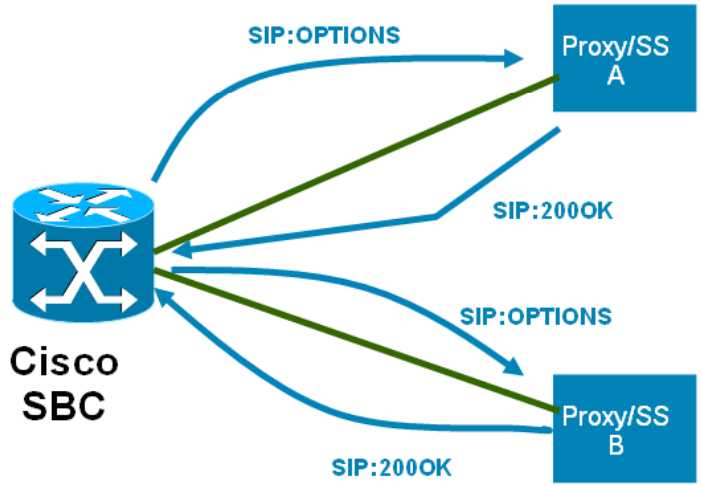
Transcoding

Availability Detection

- Signalling Plane
  - SIP does not include any “availability” check mechanism at the application layer, instead it relies on typically long times
  - Reliance is on transport layer – most common transport UDP does not support
  - A SIP “PING” mechanism is comonly used - OPTIONS - draft-fwmiller-ping-03.txt
- Media Plane
  - Issue if media and signalling sepated (as per IMS/TISPAN)
  - Media timeouts can be long and still allow new calls

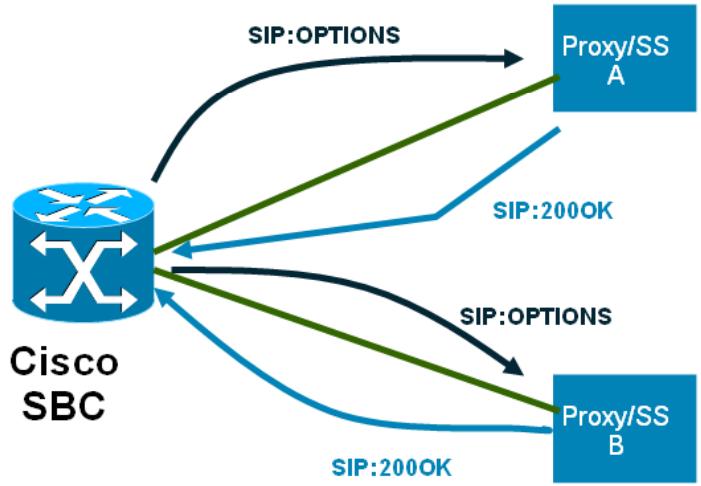
Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



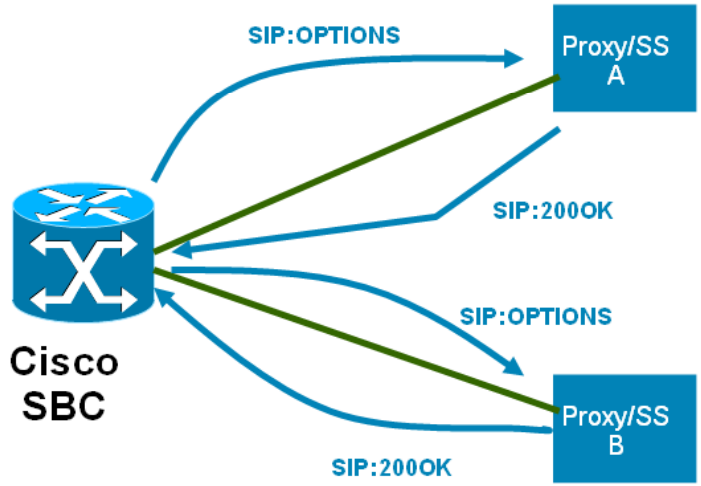
Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



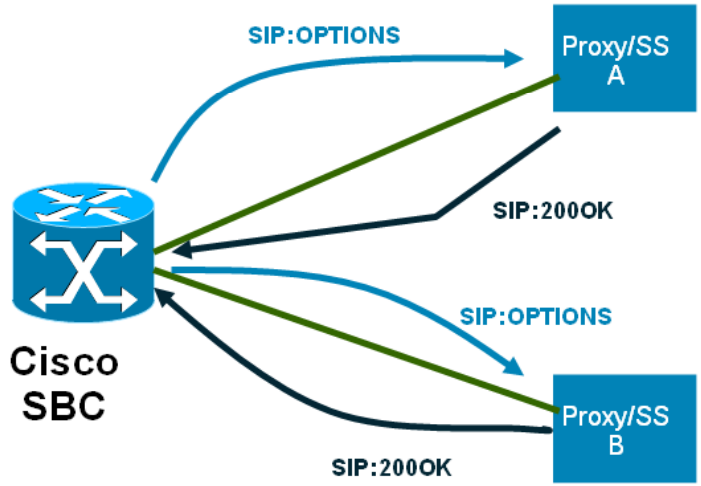
Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



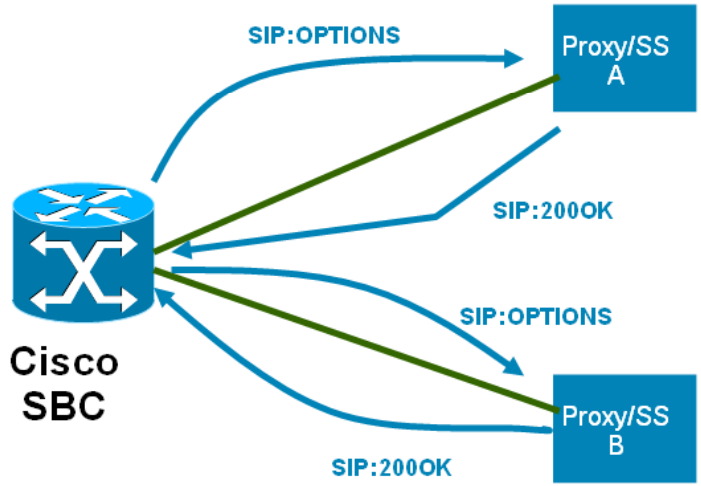
Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



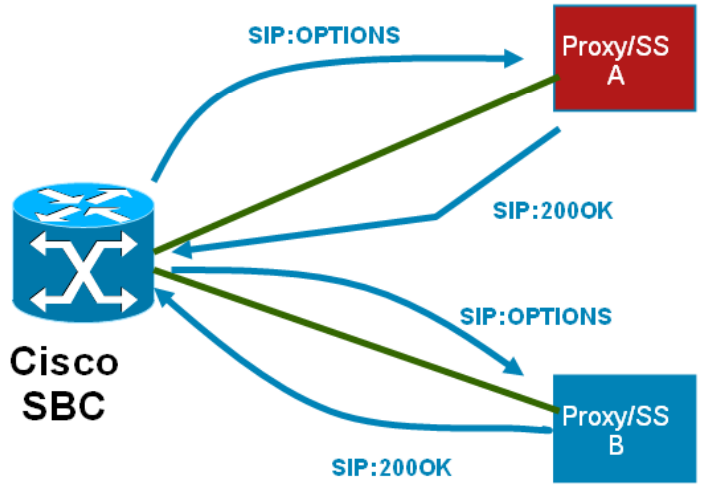
Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



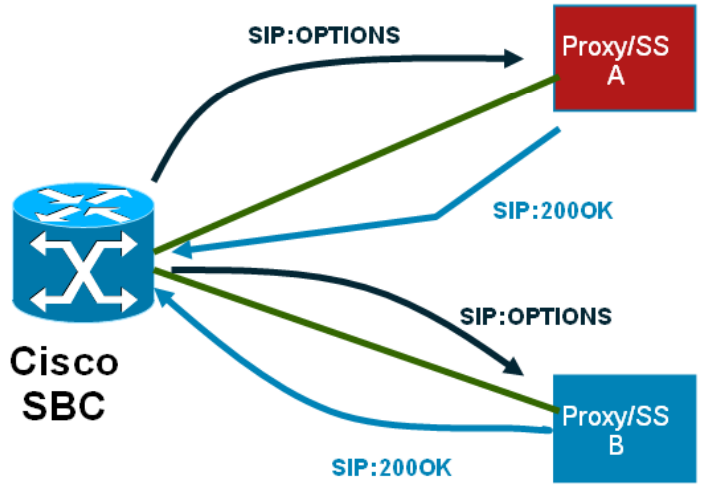
Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



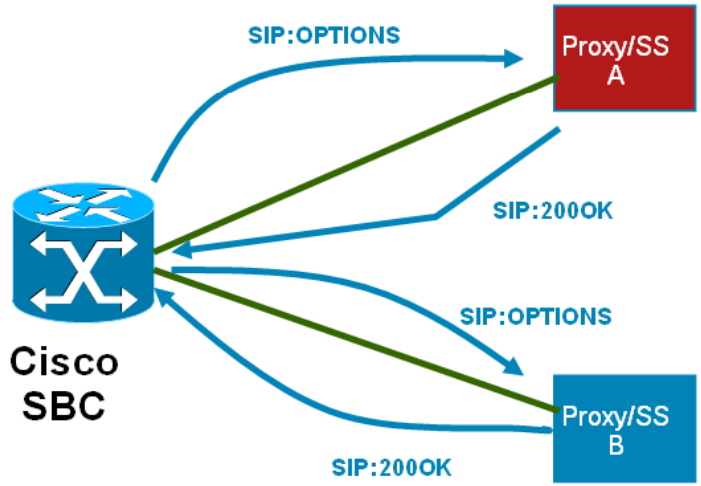
Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



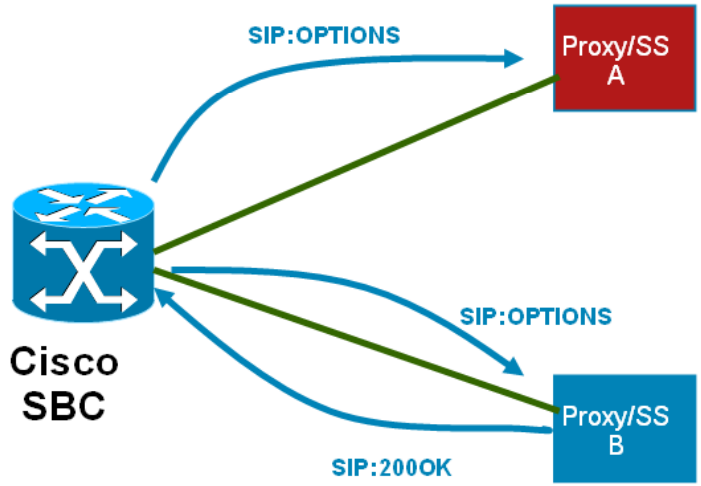
Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



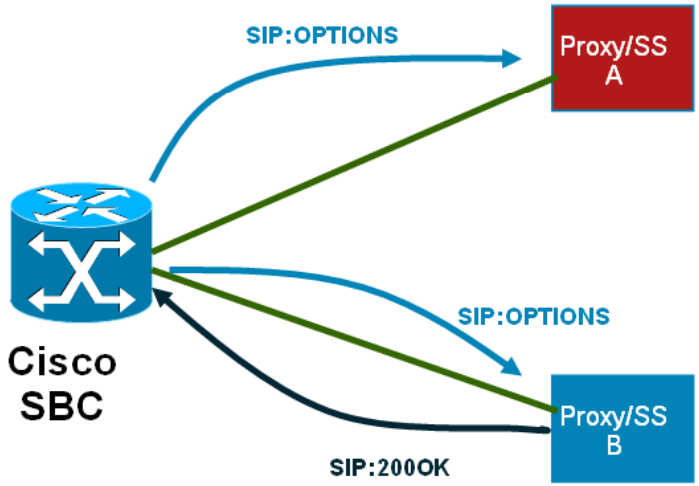
Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



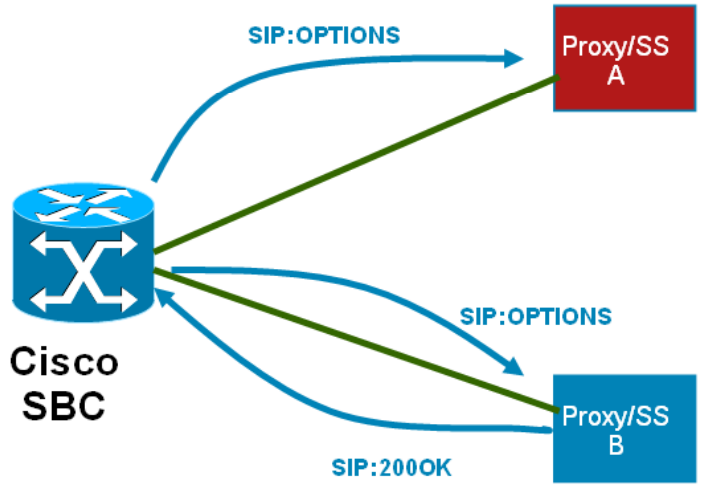
Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



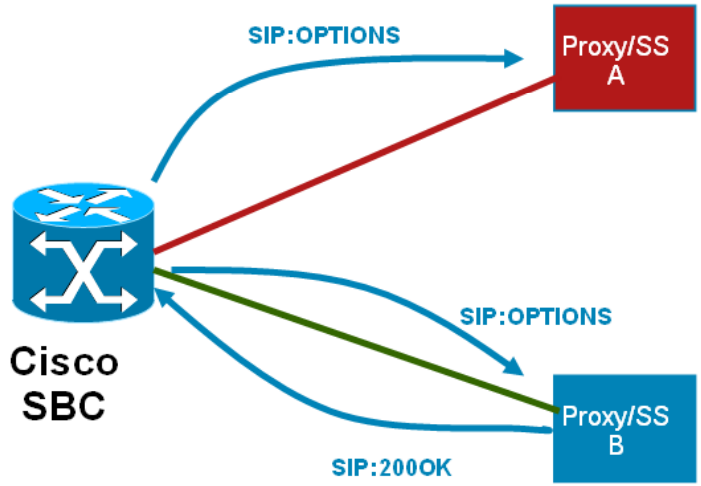
Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



Availability via SIP OPTIONS

- Cisco SBC Supports avalability check via OPTIONS
  - Define multiple routes with associated weighting
  - Enable “health probe” on each path
    - Frequency
    - TTL
    - Failure detection count



- Signalling
- Addressing & Ruting
- Security
- Availability
- Accounting
- Transcoding

Interconnect Accounting

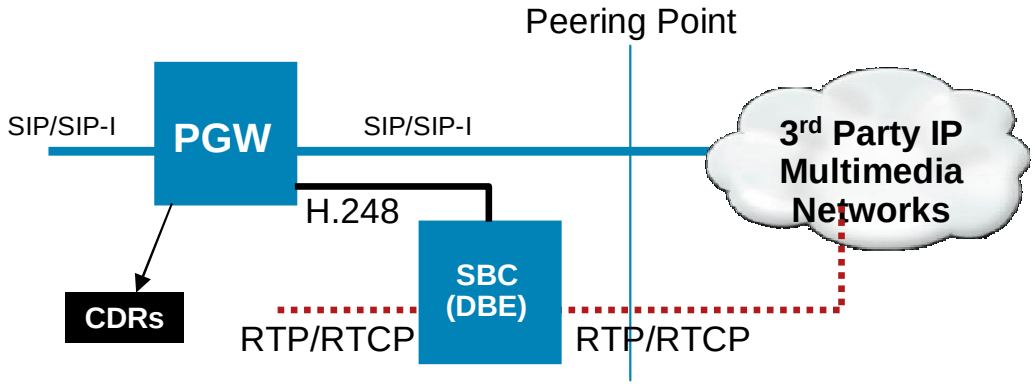
- Accounting models and rules for TDM peering well defined
- For IP Peering can adopt same strateegy as TDM or there are other possibilities

Traditional Address Based	Both PGW and SBC provide To/From information in numer or alpha format for text URI support. If SIP-I used PGW provides additional ISUP parameters in CDRs that can be used for traditional billing models
Packet/Octet Based	Both PGW and SBC CDRs provide packet and Octet counts that would potentially allow for bandwidth based accounting if desired. The data provided also gives values for packets lost/jitter/latency that can give an indication of QoS for a session but this is not ideal as it applies to the whole duration of the call – enhancements in this space of being investigated
QoS Based	SBC has ability to directly affect the DSCP markings of the signalling and media for a given session **– need to verify that thes values can be sent to CDR**. It is however possible to provide some forma of charging based on the call statistics in terms of packets lost/delay/jitter if desired
Codec Based	During a multimedia session multiple codecs may be used either simultaneouly or one at a time – changhing codecs mid session. It should be possible to differentially bill for sifferent codecs used **however** this may need to be combined with some form of packet flow metrics as some devices establish multiple parallel codecs but only use one.

Billing Models

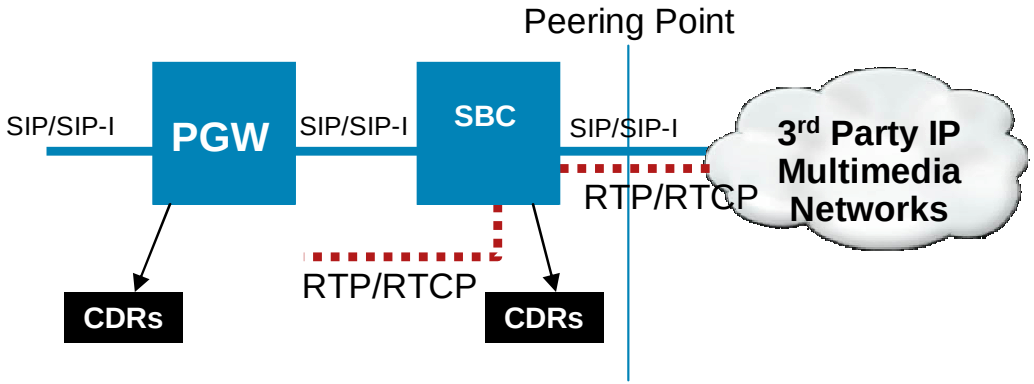
Model 1

PGW is session control platform and controls media plane directly via H.248. PGW only generates CDRs



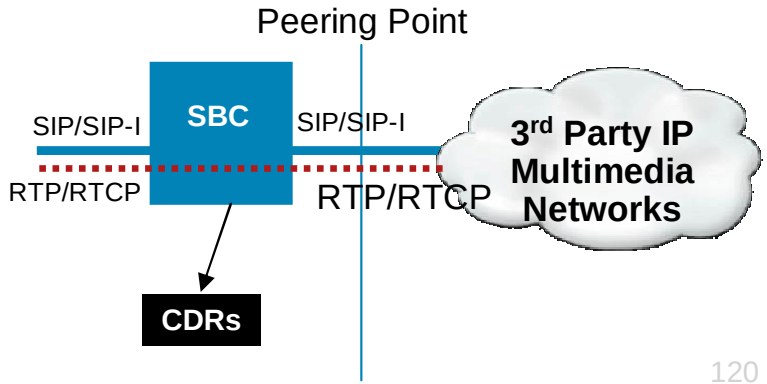
Model 2

Session control layer is provided by both PGW and SBC in series. Both platforms will generate records that can be correlated by a dowstream system.



Model 3

SBC provides both session and media control and there is no reliance on any CDR data produced by PGW.



Cisco PGW & SBC Billing

PGW2200

SBC

PGW220 produces CDRs via two mechanisms

- **"Traditional" CDRs that are stored on local disk and can be pulled via FTP/sFTP. These CDRs are produced for *all* session attempts whether effective or ineffective and are in the form of one or more CDBs (Call Detail Blocks). A CDR is typically written at the end of the session however partial CDRs are available for long duration sessions**
- **RADIUS CDRs can be issued to a RADIUS server at the end of a session – this currently only supports IP-TDM calls controlled by PGW**

Note that a Billing Mediation platform called BAMS is available to consiolidate PGW CDR output and reformat records

For full details of the PGW2200 Billing capabilities please refer to http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/billing/guide/r9chap1.html

The Cisco SBC currently produces CDRs are currently in the format or RADIUS event records as defined by PKT-SP-EM1.5-I01-050128

These records are pushed by the SBC to one or more RADIUS server farms (for redundancy(

A single session will typically gennerate multiple RADIUS event records a defined points in session such as call start, call end, and media-type changes

Signalling

Addressing & Ruting

Security

Availability

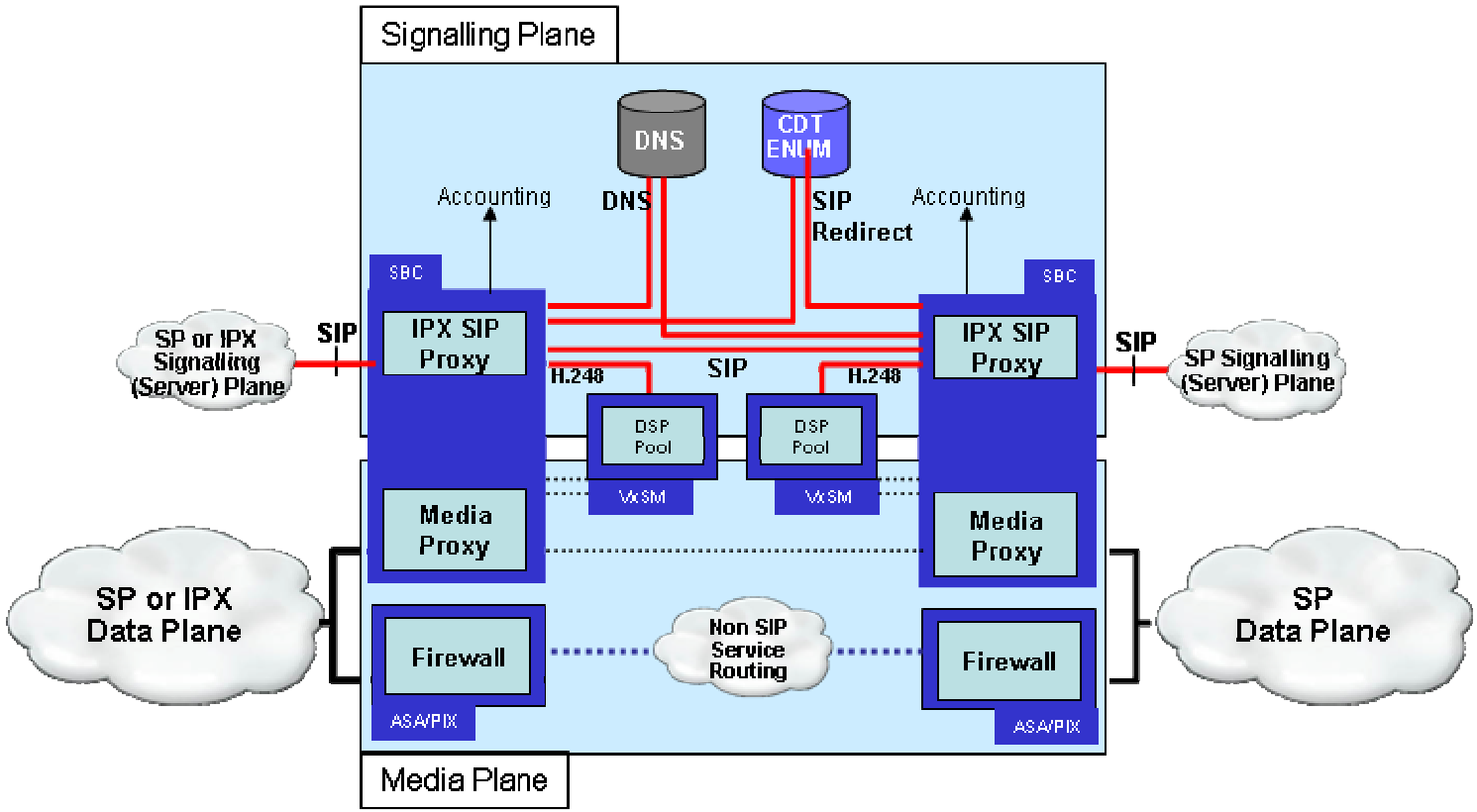
Accounting

Transcoding

Transcoding Drivers

- May be required for a number of reasons
  - CPE Support limitations
  - Standardised network codec (e.g. G.711 at 10ms)
  - Proprietary codecs used (e.g. Microsoft RTAudio)
  - Mobile to “fixed”
- Not typically an issue in TDM interconnects as gateways typicallyu support many codecs

Transcoding in the Cisco Architecture



- H.248 DSP Pool on MGX gateway used for transcoding currently allowing for re-use of TDM gateway resources
- DSP pools can be located anywhere in IP network – either local to SBC PoP or remote
- SBC can engage transcoding via two methods
  - Failed initial CODEC offer
  - Preconfigured/hardcoded
- SBC will offer configurable set of CODECs in a configurable order of preference
- **Cisco SBC can provide transrating – i.e. ptime change without the use of the external DSP resources**

Summary

Key Takeaways

- Cisco can provide comprehensive, standards based and feature rich solutions in both the SIP trunking & NGN Peering spaces
- Cater for multimedia application not just voice – driving Unified Communication
- Our approach re-uses and evolves existing components and technologies wherever possible (e.g. PGW2200 and MGX)
- The Cisco solutions will evolve over in line with standards and application innovation

We want to help you ACCELERATE your SIP deployments

Cisco Networkers 2009
January 26-29 Barcelona, Spain

Q & A

Related sessions

- BRKUCT-2001 SIP Trunking for SP Access

  And some that you might not directly associate with this topic
- BRKAPP-2002 Server Load Balancing Design
- BRKAPP-1009 Introduction to Web Application Security

Product Links

Cisco Session Border Controller

http://www.cisco.com/en/US/netsol/ns759/networking_solutions_sub_sub_solution.html

Cisco PGW2200

http://www.cisco.com/en/US/products/hw/vcallcon/ps2027/index.html

Cisco ITP & CDT (LNP/ENUM)

http://www.cisco.com/en/US/products/sw/wirelssw/ps1862/index.html

Cisco Universal Gateways & Access Servers

http://www.cisco.com/en/US/products/hw/iad/index.html

Cisco MGX Media Gateways

http://www.cisco.com/en/US/products/hw/gatecont/ps3869/index.html

Meet The Expert

To make the most of your time at Cisco Networkers 2009, schedule a Face-to-Face Meeting with a top Cisco Expert.

Designed to provide a "big picture" perspective as well as "in-depth" technology discussions, these face-to-face meetings will provide fascinating dialogue and a wealth of valuable insights and ideas.

Visit the Meeting Centre reception desk located in the Meeting Centre in World of Solutions

Recommended Reading

- There are currently no Cisco Press Books recommended for this Presentation - please browse the Cisco Company Store for suitable titles