



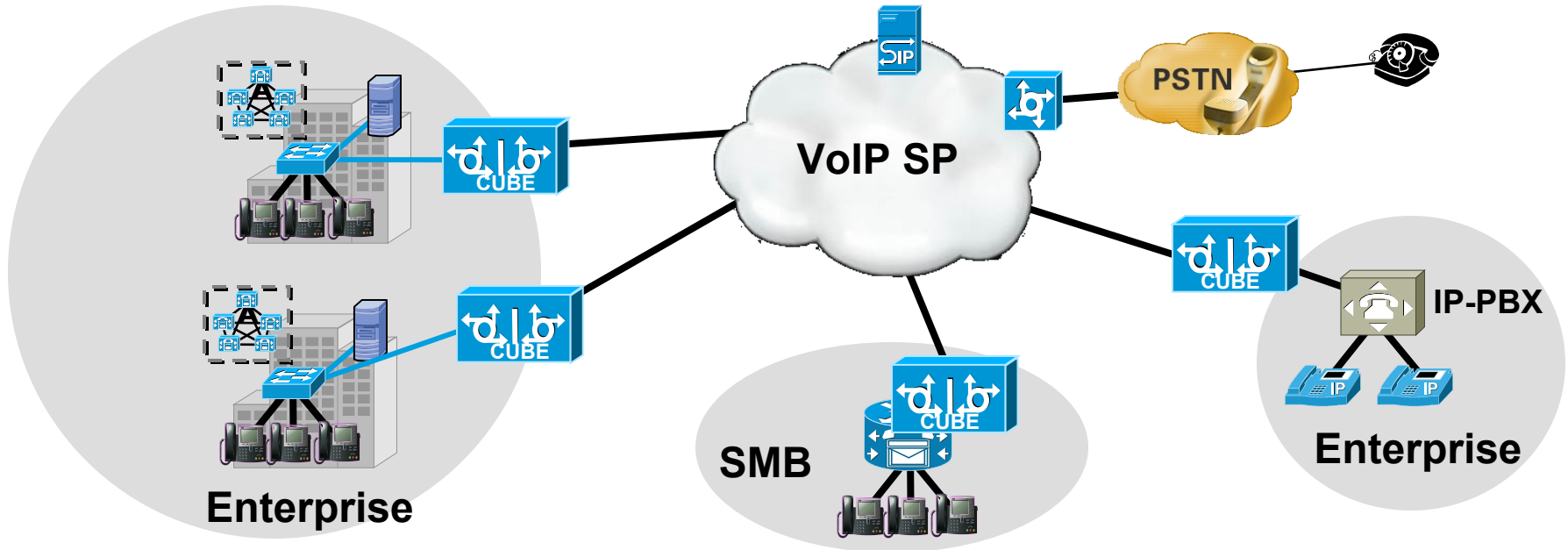
Cisco Expo
2009

Načrtovanje IP glasovnih omrežij



Aleksander Kocelj

Scope of This Seminar



1. Understand **the challenges** when interconnecting disparate VoIP networks
2. Learning **the features** the Cisco Unified Border Element provides as a session border controller to resolve UC network interconnects
3. Understand **how and where to deploy** session border controllers in your UC network

Agenda



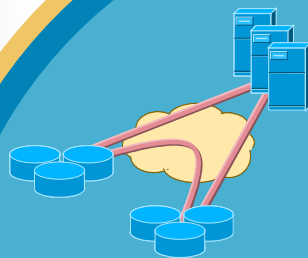
Cisco Unified Border Element Overview

Interconnecting UC Networks

Key Challenges

Session Mgmt

- Real-time session Mgmt
- Call Admissions Control
- Ensuring QoS
- PSTN GW Fallback
- Statistics and Billing
- Redundancy/Scalability



Interworking

- H.323 and SIP
- SIP Normalization
- DTMF Interworking
- Transcoding
- Codec Filtering
- Fax/Modem Support



Demarcation

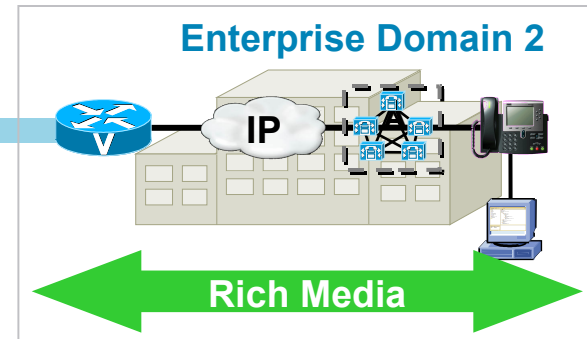
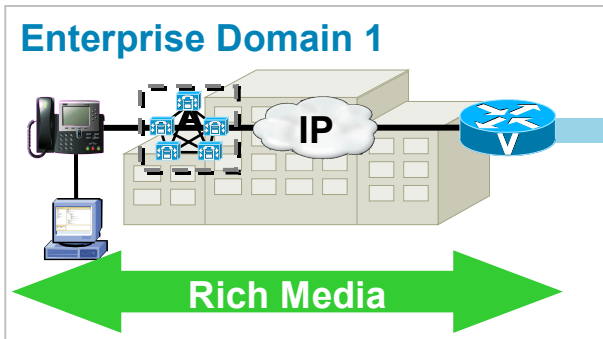
- Fault isolation
- Topology Hiding
- Network Borders
- L5/L7 Protocol Demarc
- Statistics and Billing

Security

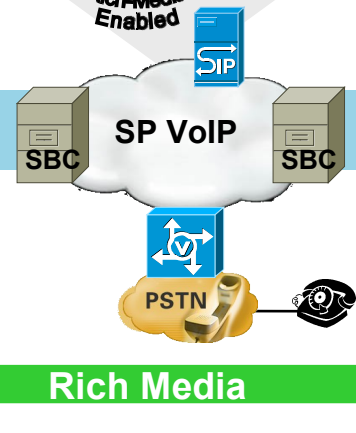
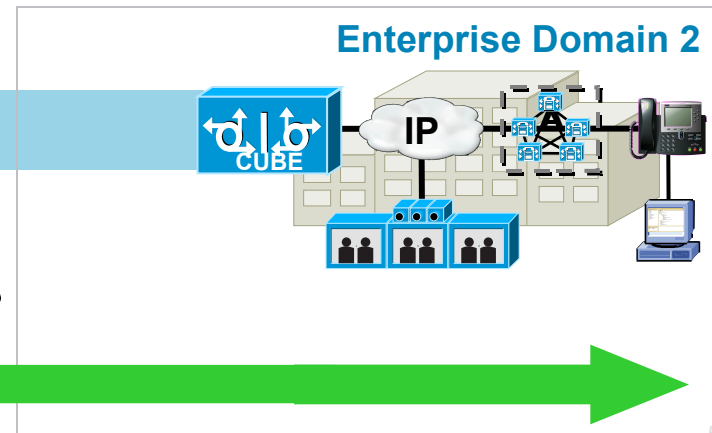
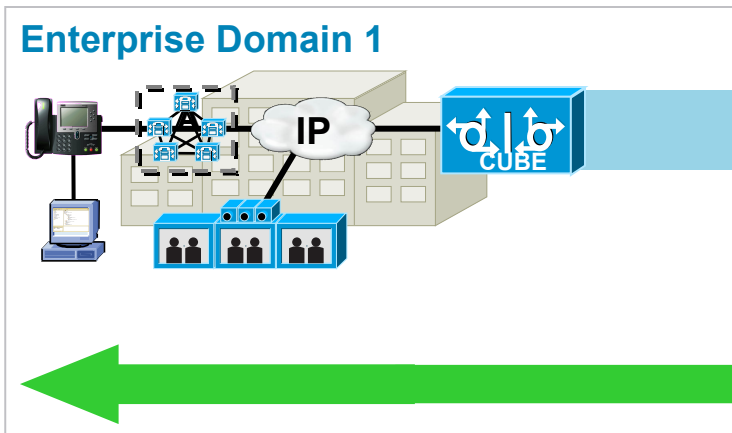
- Encryption
- Authentication
- Registration
- SIP Protection
- FW Placement
- Toll fraud

Migration to End-to-End VoIP

Enabling Business-to-Business Interconnect

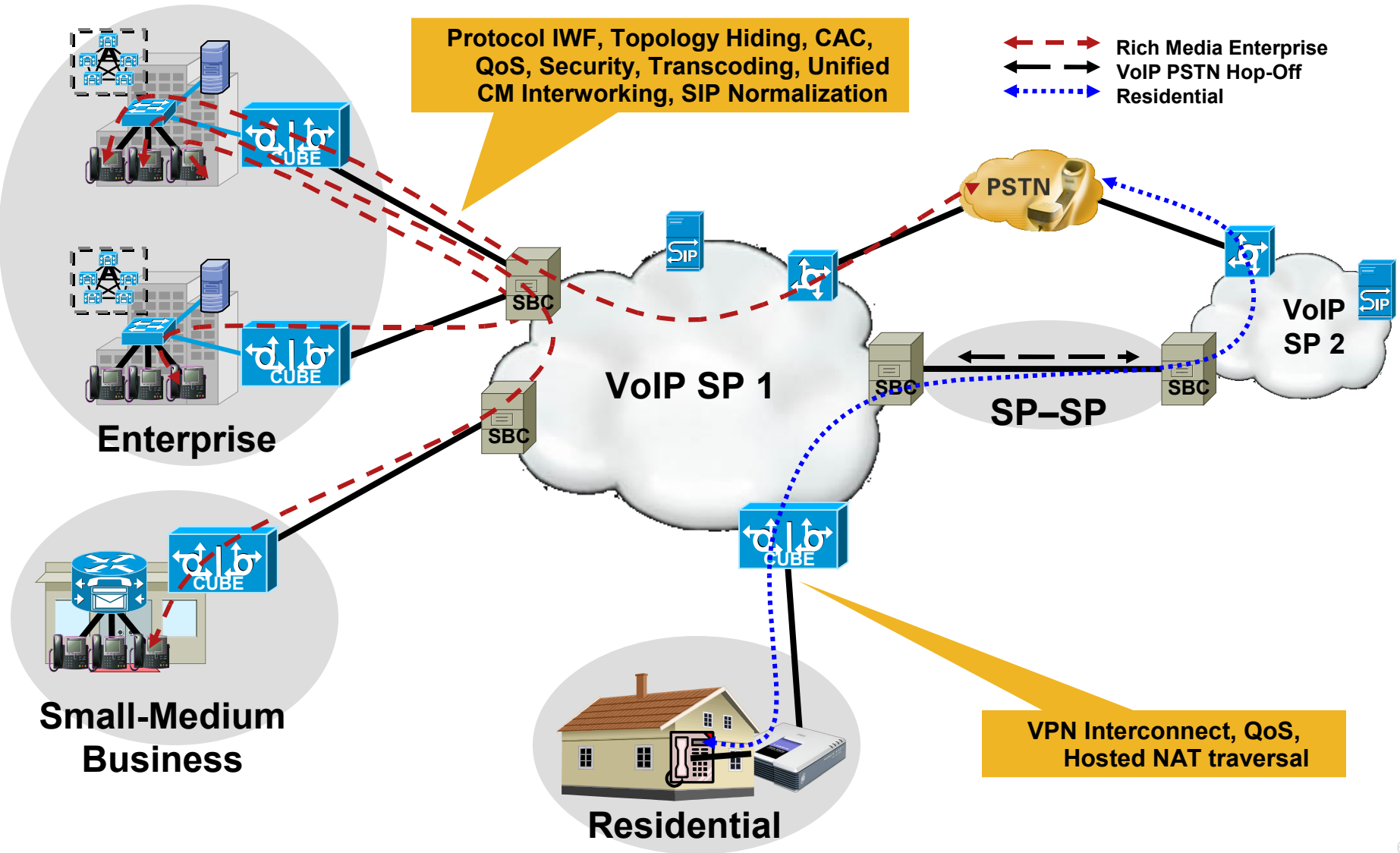


- Extend rich-media collaboration to vendors, partners and customers
- A Cisco Unified Border Element provides b2b interconnectivity for secure rich-media services



1. Changing Landscapes – VoIP Islands to VoIP Interconnects
2. Unified communications SIP Trunks to destinations beyond the Enterprise

Common VoIP Network Interconnects



Cisco Unified Border Element Architecture

Formerly the Cisco Multiservice IP-to-IP Gateway

1. Actively involved in the call treatment, signaling and media streams

SIP B2B User Agent

2. Signaling is terminated, interpreted and re-originated

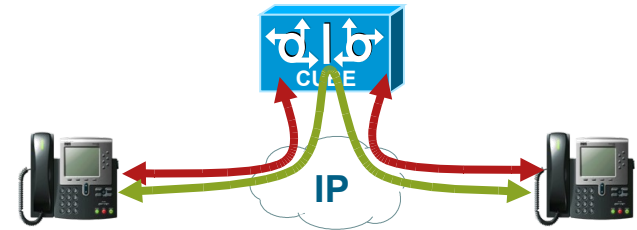
Provides full inspection of signaling, and protection against malformed and malicious packets

3. Media is handled in two different modes

Media Flow-Through

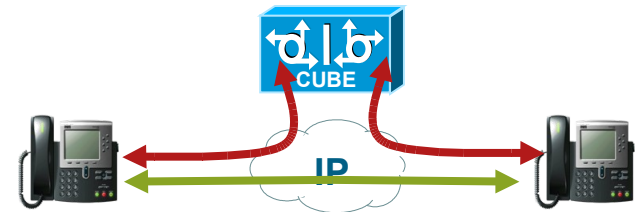
Media Flow-Around

4. Digital Signal Processors (DSPs) are required for transcoding (calls with dissimilar codecs)



Media Flow-Through

- Signaling and media terminated by the Cisco Unified Border Element
- Transcoding and complete IP address hiding require this model



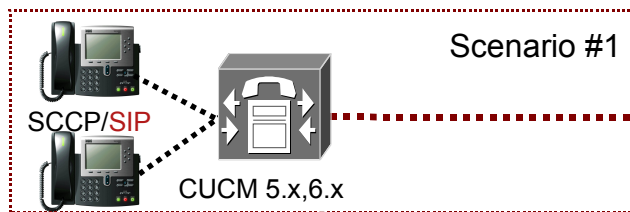
Media Flow-Around

- Signaling and media terminated by the Cisco Unified Border Element
- Media bypasses the Cisco Unified Border Element

CUBE Configuration Overview

1. Easy to configure as CUBE uses the regular IOS CLI
2. Enabling IP-to-IP Calls
 - voice service voip
 - allow-connections h323 to h323
 - allow-connections h323 to sip
 - allow-connections sip to h323
 - allow-connections sip to sip
3. Incoming and Outgoing VoIP Dial-peers with required parameters like Protocol, Transport, Codec, CAC, QoS, etc.
4. CUBE functionality requires Voice-capable images
 - Tiers of functionality from IP Voice to the IVS images

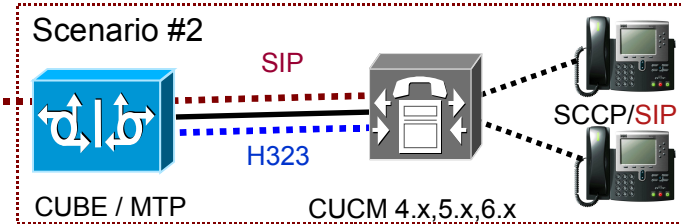
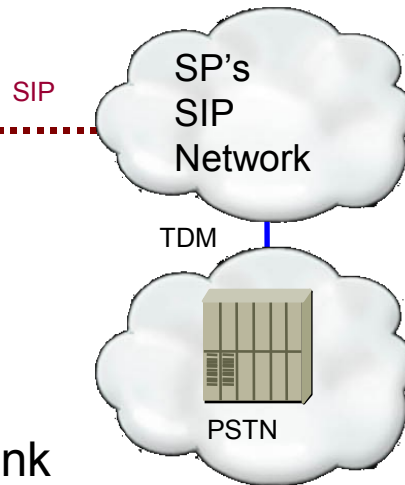
Direct SIP Trunk to CUCM versus SIP Trunk fronted by CUBE



NOT RECOMMENDED

Scenario #1 – Direct SIP Trunk

- Requires CUCM 5.x or 6.x, no 4.x support
- Need network reachability between Enterprise voice subnet & SP
- No SIP message normalization possible for SP UNI requirements (adding +, SIP hostname, etc)
- Troubleshooting would be cumbersome with no demarc
- Provisioning is based on CUCM version in Enterprise
- Still requires MTP for Early Offer outbound calls (hence still require a GW)
- No support for SIP Register
- No support for outbound OPTIONS for keepalive

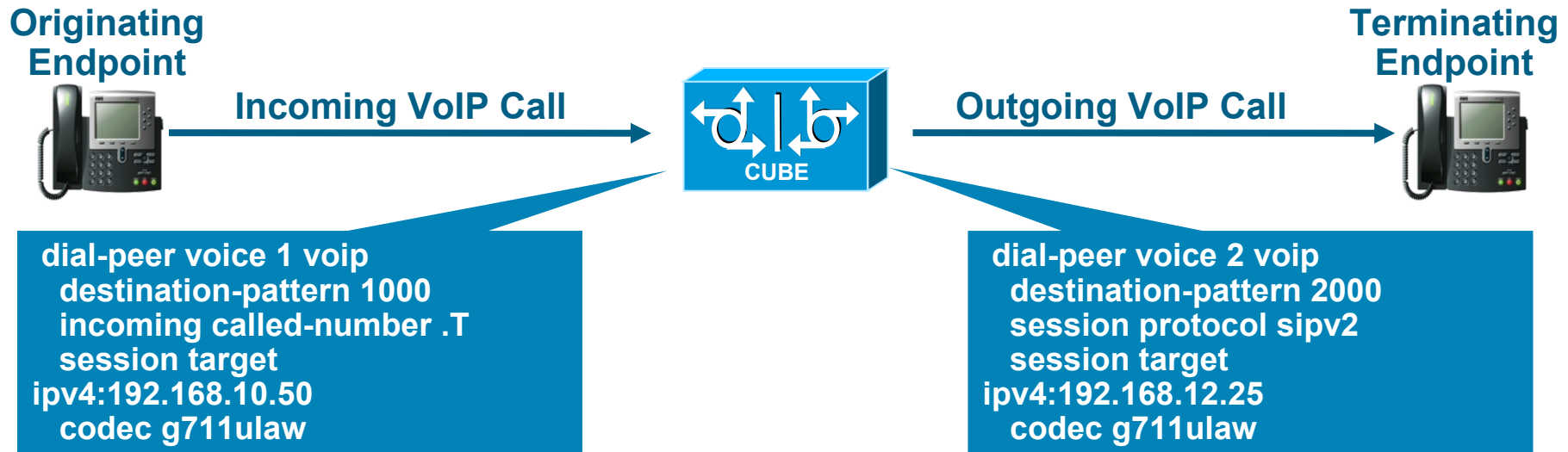


STRONGLY RECOMMENDED

Scenario #2 – SIP Trunk fronted by CUBE

- CUCM version can be 4.x, 5.x or 6.x
- Provides security via topology / IP address hiding & signaling / media protection
- Provides SIP message normalization & H.323 – SIP interworking for interop to SP
- Clear demarc for troubleshooting & QoS SLA
- Provides Call Admission Control
- Can act as MTP, TDM GW & SRST GW as well
- Supports SIP Register
- Supports sending in-dialog OPTIONS as keepalive

Cisco Unified Border Element Basic Call Flow



1. Incoming VoIP setup message from originating endpoint to the Cisco Unified Border Element
2. This matches inbound VoIP dial peer 1 for characteristics such as codec, VAD, DTMF method, protocol, etc.
3. The Cisco Unified Border Element then looks up the called number in the call setup and matches outbound VoIP dial peer 2
4. Outgoing VoIP setup message from the Cisco Unified Border Element to terminating endpoint

Call Admissions Control

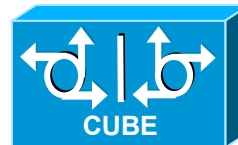
1. Requirement

Control **number of calls** based on resources and bandwidth

2. The Cisco Unified Border Element can provide six different CAC mechanisms

Total calls, CPU, Memory, GK IP call capacity, max-conn, RSVP

Total Calls, CPU, Memory



High Water Mark
Low Water Mark

```
call threshold global [total-calls | cpu-5sec | cpu-avg | total-mem | low <low-threshold> high <high-threshold>
```

```
call treatment on
```

```
call treatment cause-code ?
```

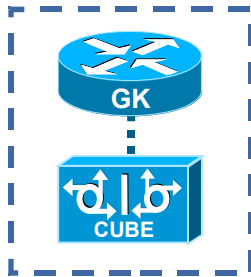
```
busy      Insert cause code indicating the GW is busy (17)
```

```
no-QoS    Insert cause code indicating the GW can't provide QoS (49)
```

```
no-resource Insert cause code indicating the GW has no resource (47)
```

Call Admissions Control

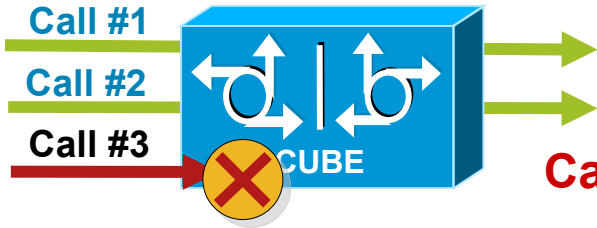
GK IP Call Capacity



```
gatekeeper
endpoint circuit-id h323id IPIPGW1 AA max-calls 500
```

```
voice service voip
allow-connections h323 to h323
h323
ip circuit max-calls 1500
ip circuit carrier-id AA reserved-calls 1000
```

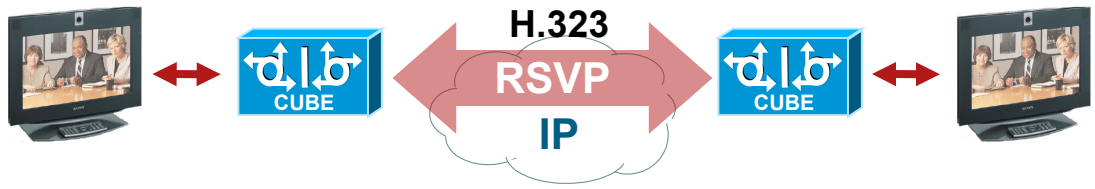
max-connections



```
dial-peer voice 1 voip
max-conn 2
```

Call #3 Rejected by the Cisco Unified Border Element

RSVP



```
interface FastEthernet0/0
ip rsvp bandwidth 1000 1000

dial-peer voice 10 voip
destination-pattern 2...
session target ras
req-qos guaranteed-delay audio
req-qos guaranteed-delay video
acc-qos guaranteed-delay audio
acc-qos guaranteed-delay video
```

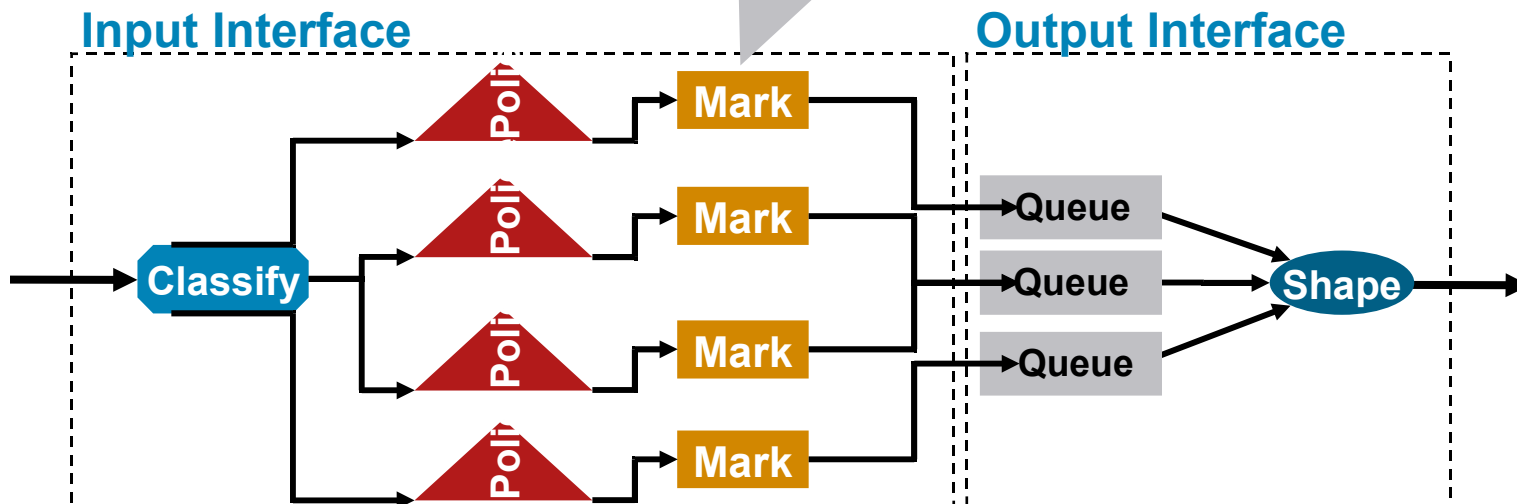
Quality of Service (QoS)

1. Requirement

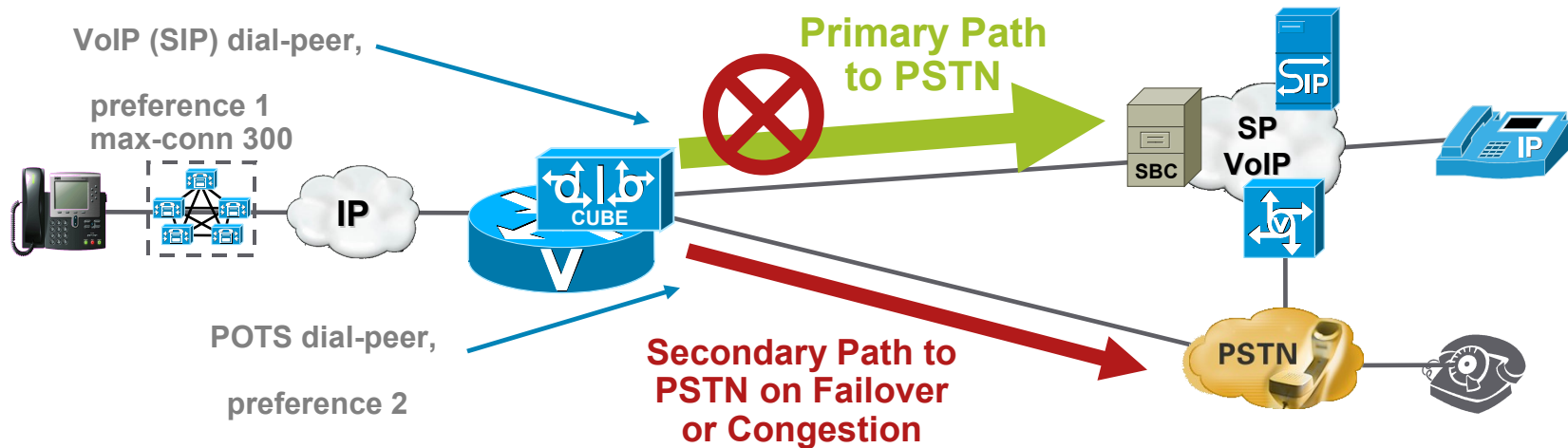
Ensure traffic adheres to **QoS policies** within each network

2. The Cisco Unified Border Element can remark ToS/DSCP QoS parameters on signaling and media packets between networks

```
dial-peer voice 100 voip
ip qos dscp ef media
ip qos dscp af31
signaling
```



SIP Trunk to PSTN Failover



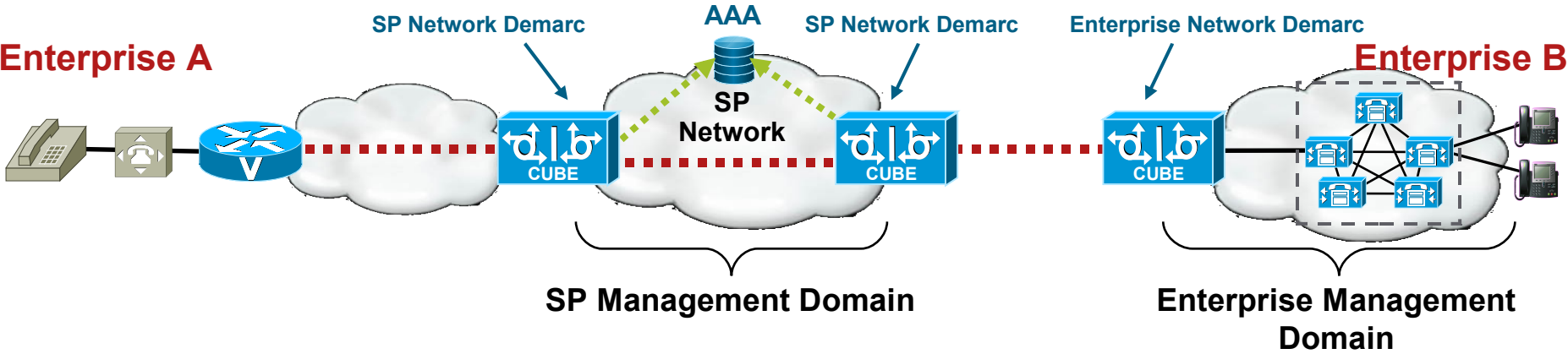
1. Collocated Cisco Unified Border Element (SIP trunks) and TDM GW (PSTN trunks)

Easy SIP trunk migration—Cisco Unified Border Element platform can also host TDM PSTN trunks for alternate or failover call routing

2. Integrated Cisco Unified Border Element and TDM GW platform can also provide many other integrated services to the site

MTP, SRST, RSVP Agent, Routing and security

Voice Call Statistics and Billing



1. VoIP performance statistics and billing collected within mgmt domains

2. The Cisco Unified Border Element generates CDR records

Radius VSAs or syslog

Conference ID is unique on both call legs

Call-ID is included in the CDR

```
show call active voice  
[compact]  
show voip rtp connections  
show call active voice [brief]  
show voice statistics csr
```

3. The Cisco Unified Border Element provides voice quality and call statistics

IP SLA monitoring

Cisco IOS CLI (“show call active voice”)

SNMP (POP-MGMT-MIB and CALL-HISTORY-MIB)

Voice CSR Statistics “show voice statistics csr”

Voice Call Statistics Sample Output

```
CUBE#sh call active voice compact
```

```
<callID>  A/O FAX T<sec> Codec      type      Peer Address      IP R<ip>:<udp>
Total call-legs: 10
  1  ANS      T13      g711ulaw  VOIP      P14085411001     9.13.25.101:6000
  2  ORG      T13      g711ulaw  VOIP      P14085414001     9.13.25.102:6000
  3  ANS      T13      g711ulaw  VOIP      P14085411002     9.13.25.101:6004
  4  ORG      T13      g711ulaw  VOIP      P14085414002     9.13.25.102:6004
  5  ANS      T12      g711ulaw  VOIP      P14085411003     9.13.25.101:6008
  6  ORG      T12      g711ulaw  VOIP      P14085414003     9.13.25.102:6008
  7  ANS      T11      g711ulaw  VOIP      P14085411004     9.13.25.101:6012
  8  ORG      T11      g711ulaw  VOIP      P14085414004     9.13.25.102:6012
  9  ANS      T10      g711ulaw  VOIP      P14085411005     9.13.25.101:6016
 10  ORG      T10      g711ulaw  VOIP      P14085414005     9.13.25.102:6016
```

```
CUBE#sh voip rtp connections
```

```
VoIP RTP active connections :
```

No.	CallId	dstCallId	LocalRTP	RmtRTP	LocalIP	RemoteIP
1	1	2	22336	6000	9.13.25.21	9.13.25.101
2	2	1	19280	6000	9.13.25.21	9.13.25.102
3	3	4	24154	6004	9.13.25.21	9.13.25.101
4	4	3	18316	6004	9.13.25.21	9.13.25.102
5	5	6	20710	6008	9.13.25.21	9.13.25.101
6	6	5	17190	6008	9.13.25.21	9.13.25.102
7	7	8	19640	6012	9.13.25.21	9.13.25.101
8	8	7	19820	6012	9.13.25.21	9.13.25.102
9	9	10	18024	6016	9.13.25.21	9.13.25.101
10	10	9	24018	6016	9.13.25.21	9.13.25.102

```
Found 10 active RTP connections
```

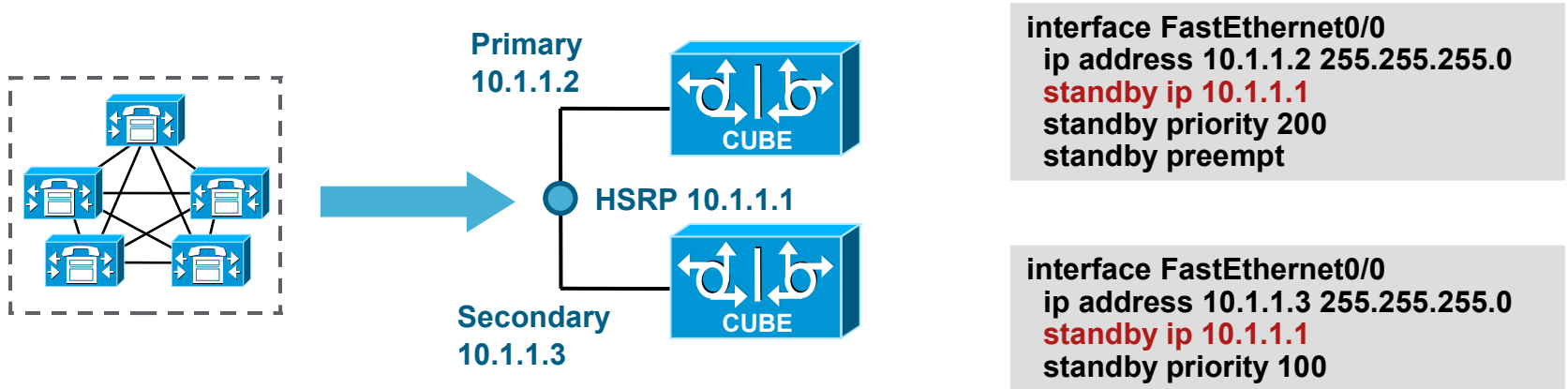
```
CUBE#sh call active voice brief
```

```
...
Telephony call-legs: 0
SIP call-legs: 10
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 10
...
```

Redundancy and Scalability

Method	Redundancy	Scalability	Notes
HSRP	✓		<ul style="list-style-type: none"> ▪ All Protocols ▪ Source IP Addresses May Be Interface Address
CUCM Route Lists	✓	✓	<ul style="list-style-type: none"> ▪ Application Server Alternate Routing ▪ H.323 and SIP
DNS	✓	✓	<ul style="list-style-type: none"> ▪ All Protocols ▪ May Affect PDD Depending on Network Design
Gatekeeper	✓	✓	<ul style="list-style-type: none"> ▪ H.323 Only

HSRP



1. Endpoints point towards the Virtual HSRP IP Address
2. Calls would normally be handled by the primary Cisco Unified Border Element
3. If the Primary fails, the secondary Cisco Unified Border Element handles new calls
4. Active/Standby—redundancy only, no scalability
5. Some outbound SIP messages from Cisco Unified Border Element may carry interface IP address, not the HSRP address

Cisco Unified Communications Manager Route Lists

1. Cisco Unified Communications Manager Route Lists

One Route Group to each Cisco Unified Border Element

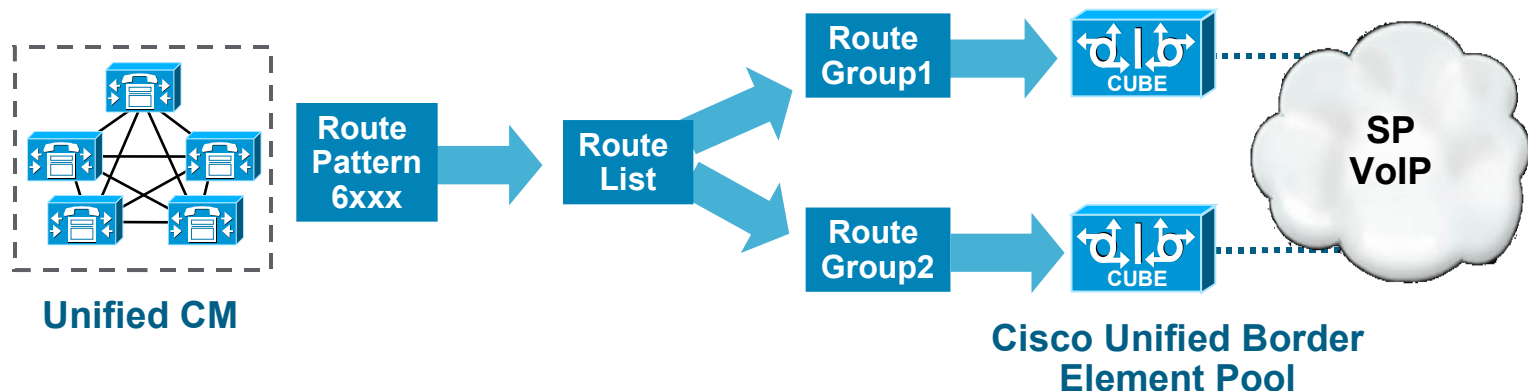
One Route List to aggregate all Route Groups

Configure Route List under Route Pattern

2. Cisco Unified Border Element

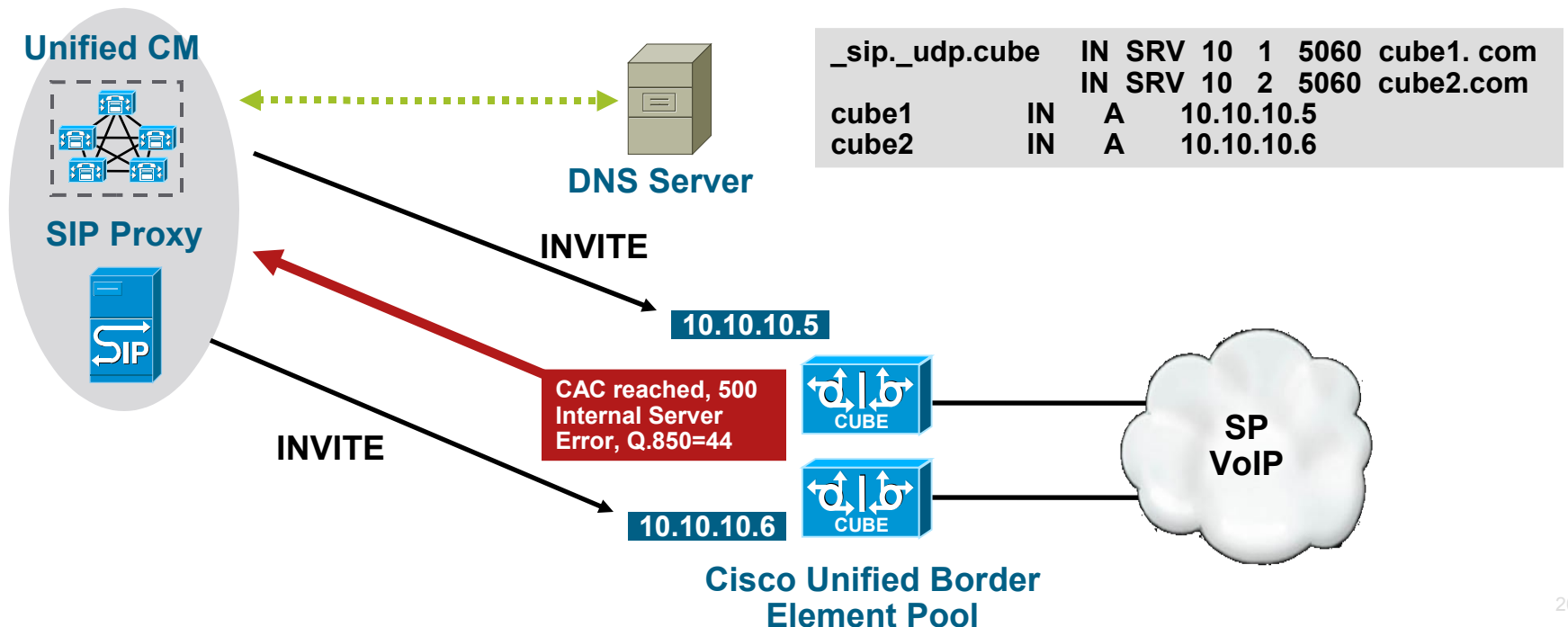
Option 1: Configure max-conn under the Cisco Unified Border Element dial-peers

Option 2: Set the Global Call Threshold/Treatment for total-calls



DNS SRV

1. Define CAC using total calls or max-conn on the Cisco Unified Border Element
2. When number of calls exceeded, server error 500 is sent back
3. SIP Proxy/Unified CM chooses the next IP Address provided by the DNS SRV record
4. Call is now sent to the next Cisco Unified Border Element in the DNS SRV record

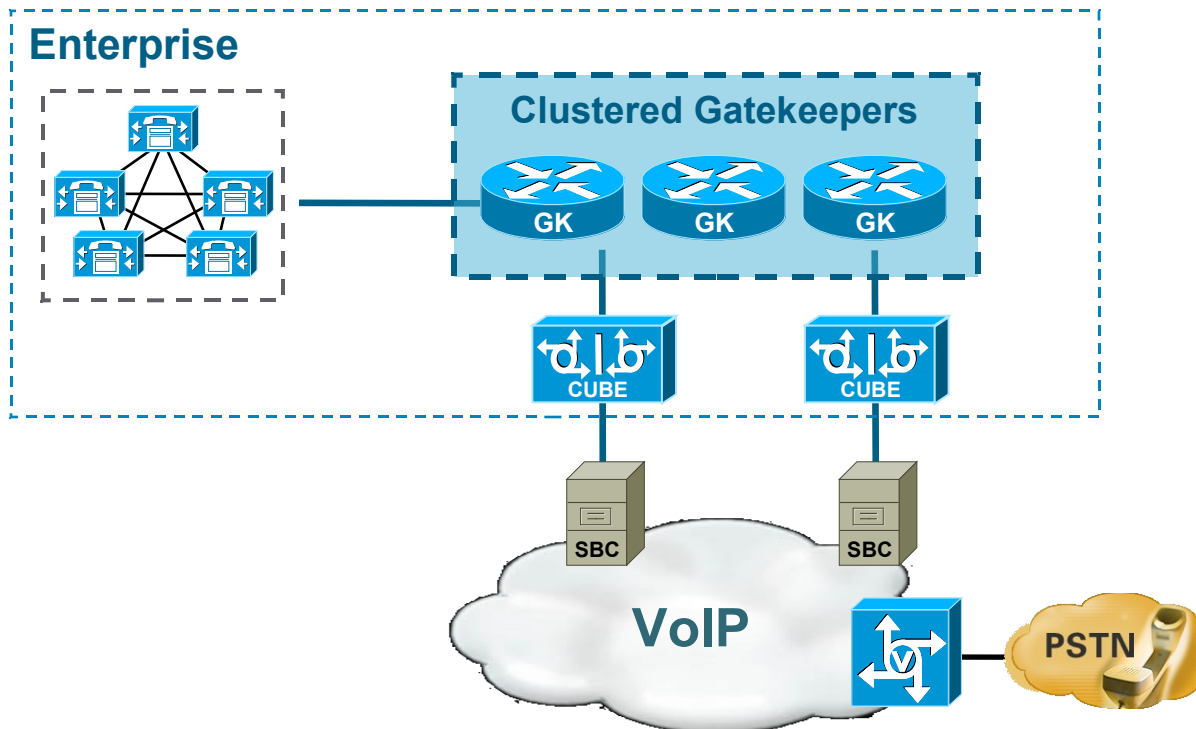


H.323 Gatekeeper

1. Load-Balancing across the Cisco Unified Border Elements in H.323 networks can be done

Round Robin algorithm

Percentage Based algorithm



H.323 and SIP Interworking

1. Requirement

Large installed base of H.323 applications, with an increasing number of SIP applications in the same enterprise network

Connect H.323 and SIP applications to SP SIP trunks

Incompatibilities and variations within same protocol

2. The Cisco Unified Border Element supports H.323-H.323, SIP-SIP and H.323-SIP interworking

Voice supported for all combinations

Video supported for H.323-H.323 and SIP-SIP

3. Define incoming and outgoing VoIP dial-peers with required parameters like protocol, transport, codec, CAC, QoS, etc.

```
voice service voip  
  allow-connections h323 to h323  
  allow-connections h323 to sip  
  allow-connections sip to h323  
  allow-connections sip to sip
```

H.323 and SIP Interworking

H.323-H.323



In Leg	Out Leg	Support
Fast Start	Fast Start	Bi-Directional
Slow Start	Slow Start	Bi-Directional
Fast Start	Slow Start	Bi-Directional

SIP-SIP



In Leg	Out Leg	Support
Early Offer	Early Offer	Bi-Directional
Delayed Offer	Delayed Offer	Bi-Directional
Delayed Offer	Early Offer	Uni-Directional

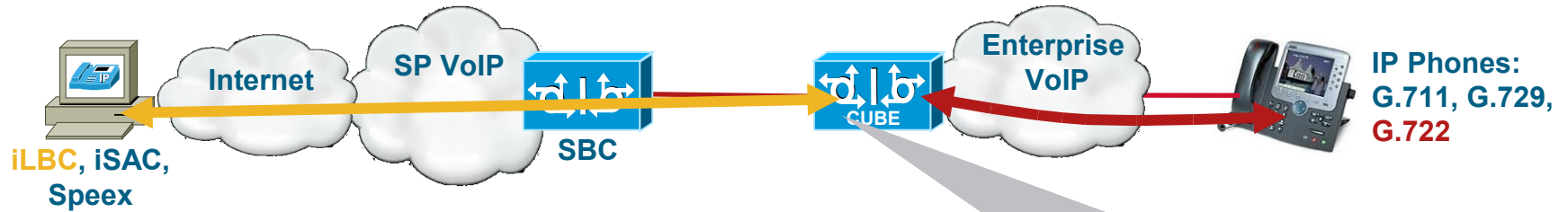


H.323-SIP



In Leg	Out Leg	Support
Fast Start	Early Offer	Bi-Directional
Slow Start	Delayed Offer	Bi-Directional

Media Transcoding



Transcoding: G.711, G.723.1, G.726, G.728, G.729/a, iLBC, G.722

1. Cisco Unified Border Element supports universal transcoding

Any voice codec to any other codec
 E.g. iLBC to G.711 or iLBC to G.729
 Voice transcoding only (not video)

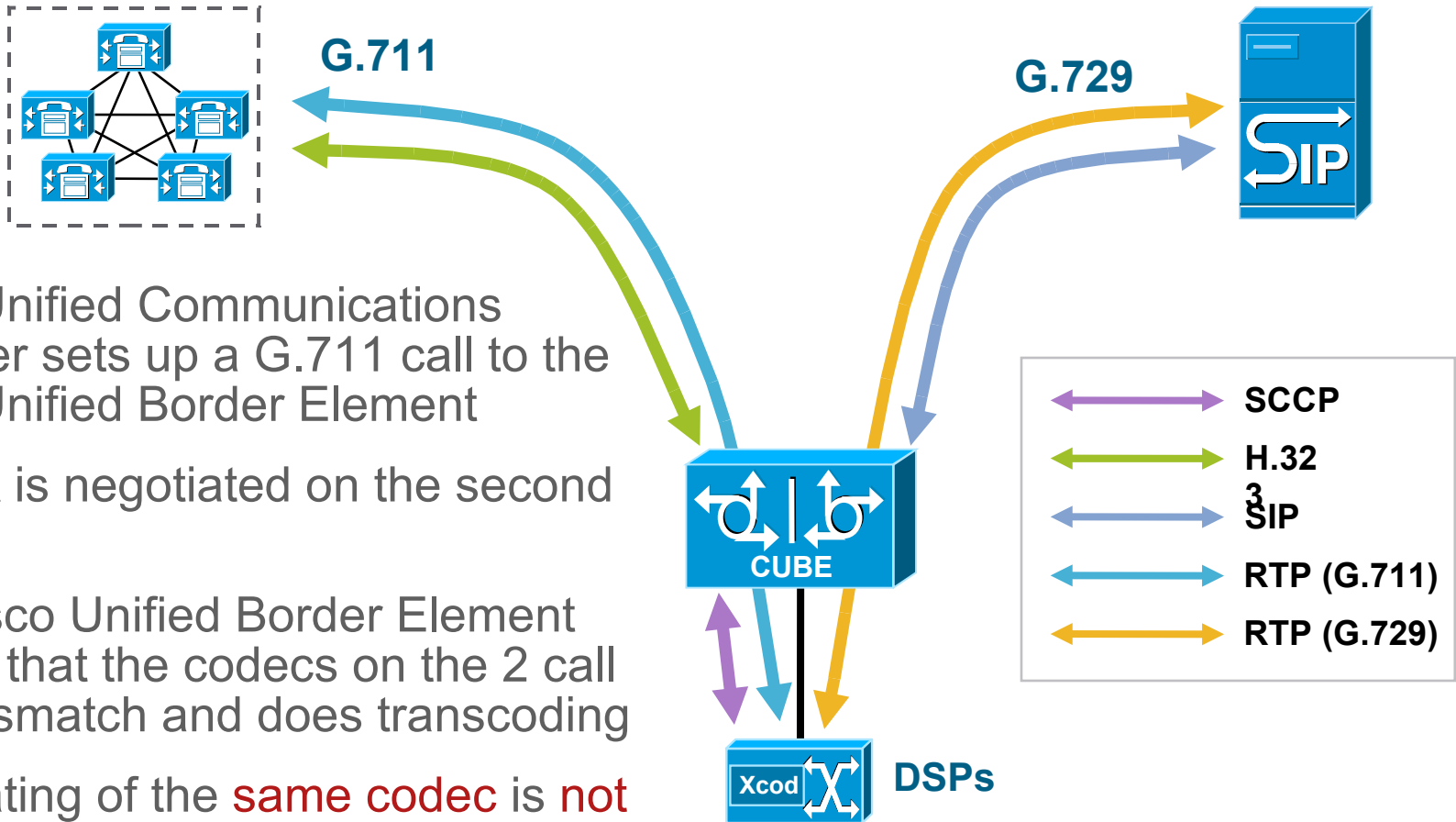
2. Transrating (different packetizations):

- ✓ – Supported: Transrating of **different** codecs
 e.g. G.711 a-law 20ms ↔ G.711 μ-law 10ms
 G.711 20ms ↔ G.729A 30ms
- ✗ – Not supported: Transrating of **the same** codec
 e.g. G.729A 20ms ↔ G.729A 30ms

Supported Codecs*	Release
G.711 a-law 64 Kbps	12.4(11)XW
G.711 μlaw 64 Kbps	12.4(11)XW
G.723—5.3 and 6.3 Kbps	12.4(11)XW
G.729, G.729A 8 Kbps	12.4(11)XW
G.729B, G.729AB 8 Kbps	12.4(11)XW
iLBC—13.3 and 15.2 Kbps	12.4(11)XW
G.722—64 Kbps	12.4(15)XY

*Note: Only voice codecs are supported with transcoding—no video codecs

Transcoding Call Flow

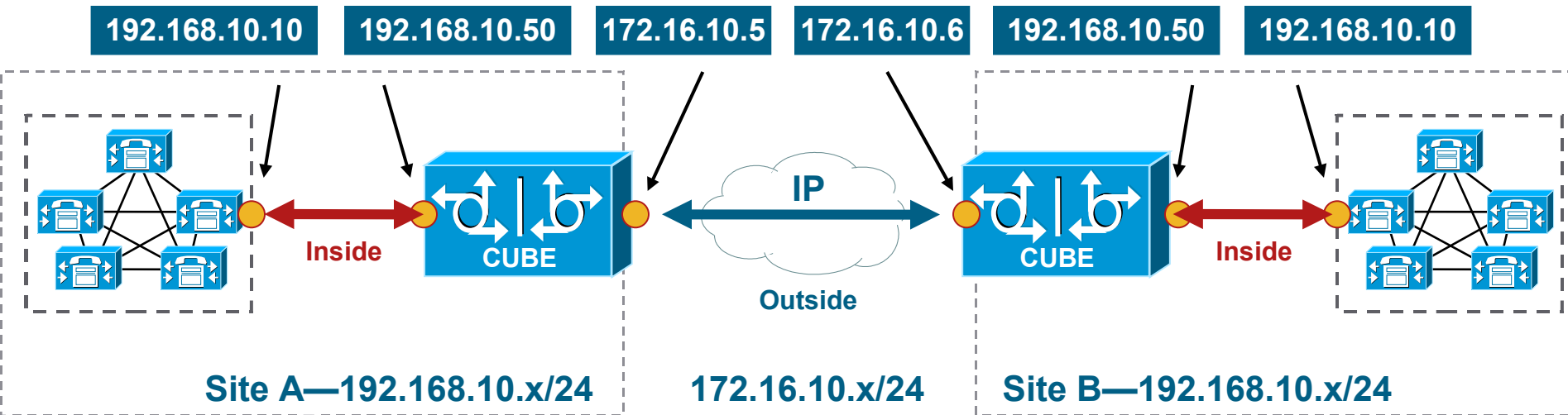


1. Cisco Unified Communications Manager sets up a G.711 call to the Cisco Unified Border Element
2. G.729A is negotiated on the second leg
3. The Cisco Unified Border Element detects that the codecs on the 2 call legs mismatch and does transcoding
4. Transrating of the **same codec** is **not** supported

Configuration example at:

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/prod_configuration_examples_list.html

Topology/Address Hiding



1. Requirements

Maintain connectivity without exposing the IP network details

Interconnect networks that have overlapping IP Addresses

2. B2BUA provides complete topology hiding on signaling and media

Maintains security and operational independence of both networks

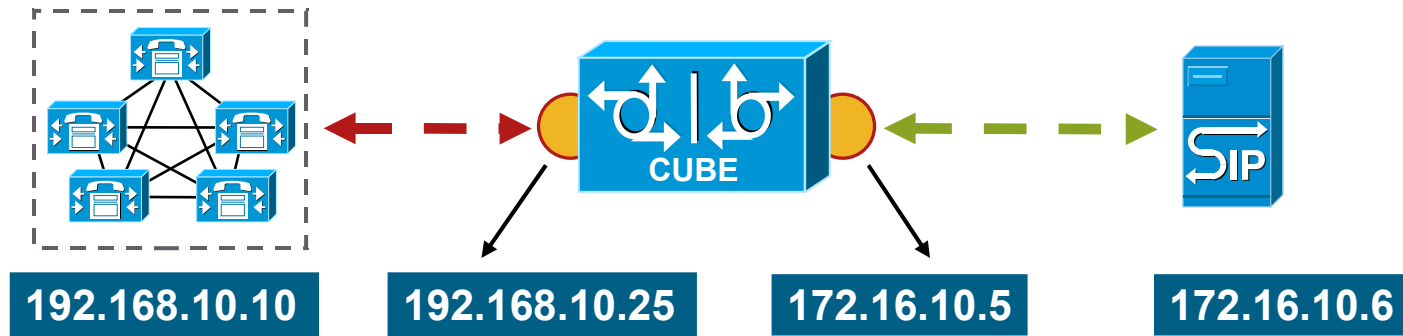
Provides implicit NAT service by substituting Cisco Unified Border Element IP addresses on all traffic

3. Allows for NAT and Firewall (FW) traversal

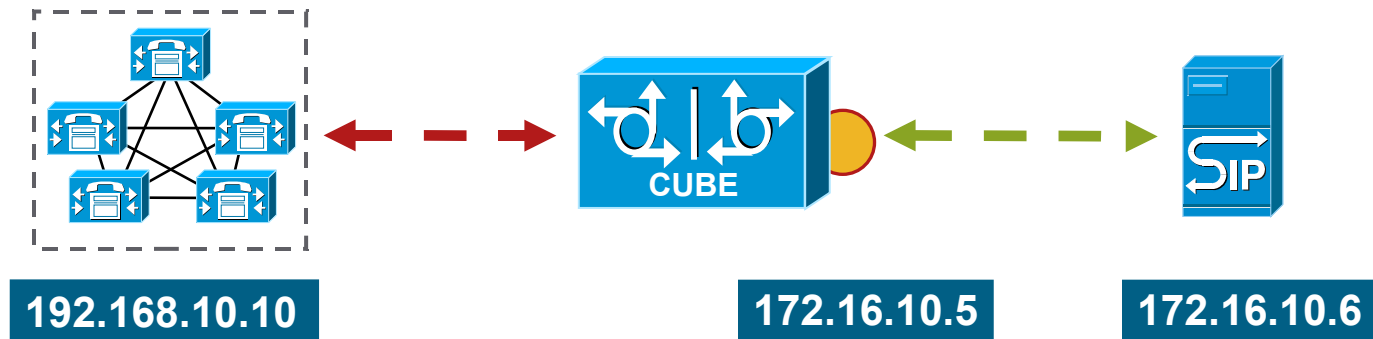
Address Hiding: Configuration Options

1. Both sides of the network talk only to the Cisco Unified Border Element

Two Physical Interfaces

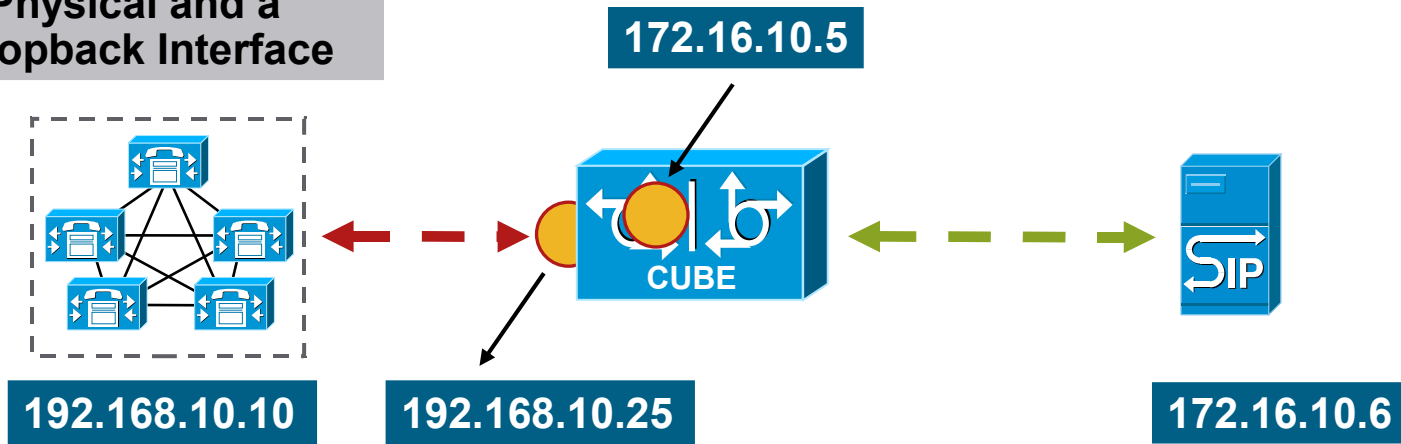


Single Physical Interface

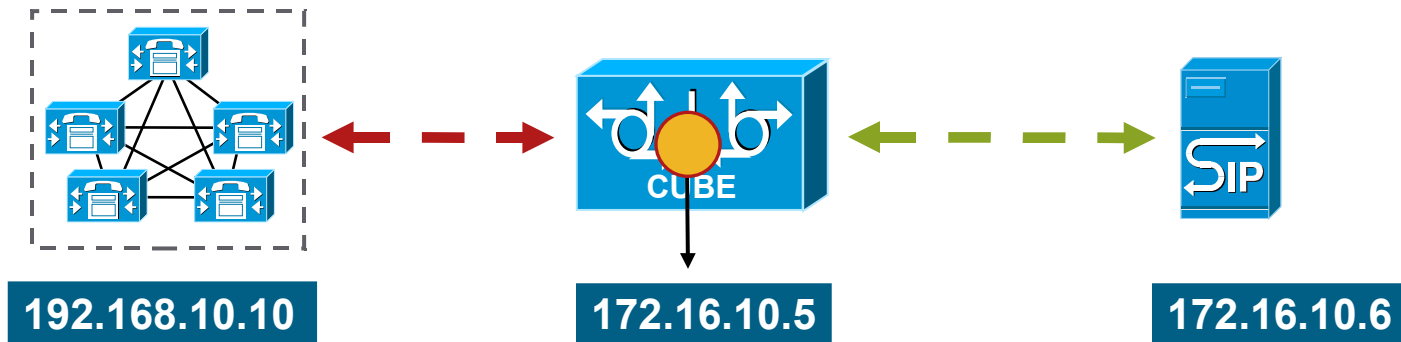


Address Hiding: Configuration Options

A Physical and a Loopback Interface

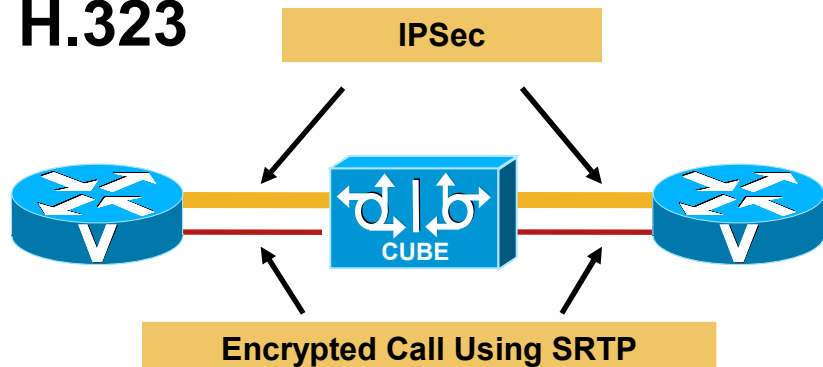


Single Loopback Interface



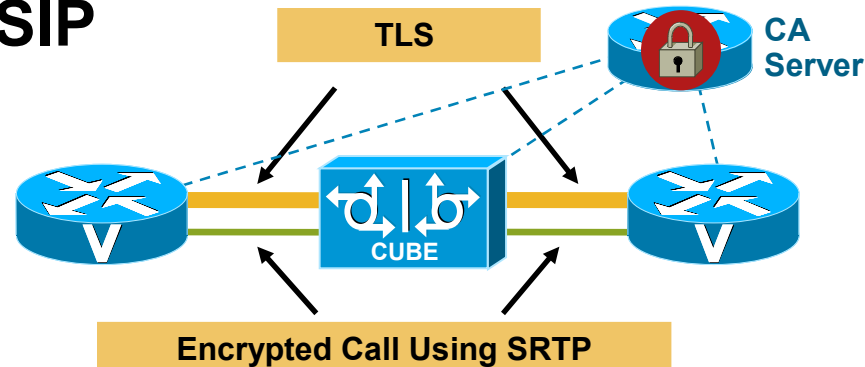
Authentication and Encryption

H.323



1. **IPSec**—Signaling Authentication and Encryption
2. **SRTP**—Media authentication and encryption
3. Keys sent transparently across

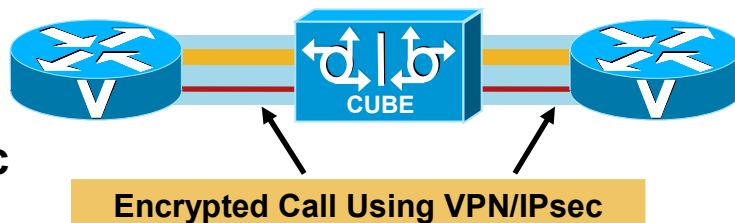
SIP



1. **TLS**—Signaling Authentication and Encryption
2. **SRTP**—Media authentication and encryption
3. **NonTLS**—TLS interworking

More information at: www.cisco.com/go/cube > Configure > Configuration Examples and TechNotes

Standard Cisco IOS VPN Technology Can Also Be Used to Protect VoIP Traffic



Note: Using PKI on Cisco IOS requires the router clock to be synchronized with the network time to ensure proper validation of certificates

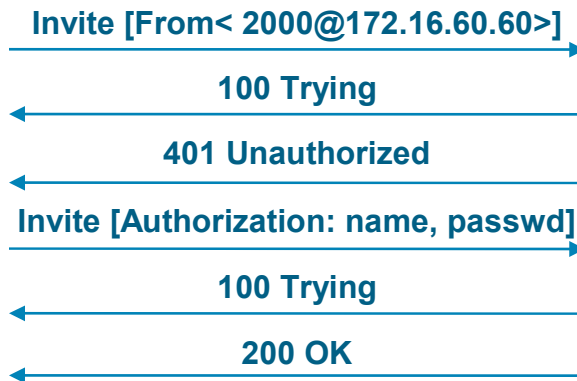
SIP Protection

Digest Authentication

```

sip-ua
authentication username xxx password yyy
  
```

1. SIP Proxy challenges INVITEs from the Cisco Unified Border Element to check endpoint validity with 401 Unauthorized
2. The Cisco Unified Border Element responds with INVITE including credentials



Hostname Validation

- Initial INVITEs with a hostname URI are compared to a configured list of up to 10 hostnames
- If there is no a match to the INVITE, the Cisco Unified Border Element returns a "400 Bad Request—Invalid Host"

```

sip-ua
permit hostname dns:example1.sip.com
permit hostname dns:example2.sip.com
permit hostname dns:example3.sip.com
permit hostname dns:example4.sip.com
  
```

SIP Protection

SIP Listening Port

1. Default SIP Listen ports are 5060 (UDP/TCP) and 5061 (TLS)
2. These ports are well-known and can be the target of attacks
3. Change the SIP Listen port to a different setting that is not well-known

```
voice service voip
  sip
    shutdown
```

```
voice service voip
  sip
    listen-port non-secure 2000 secure 2050
```

Registration

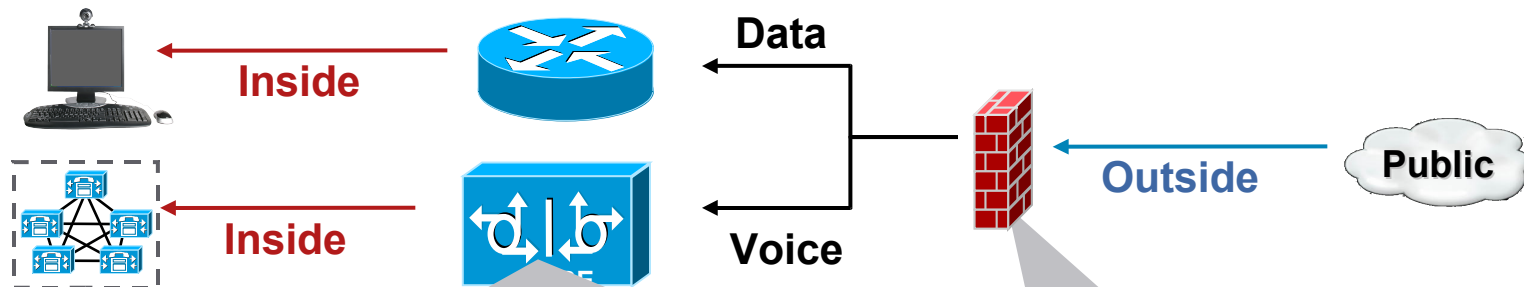
- The Cisco Unified Border Element can send SIP REGISTER messages with credentials to a proxy
- Register statically on behalf of endpoints behind the Cisco Unified Border Element that do not register

```
x(config)#sip-ua
x(config-sip-ua)#credentials username 1001
password cisco realm cisco.com
```

```
sip-ua
  registrar ipv4:172.16.193.97 expires 3600
  credentials username 1001 password
  0822455D0A16 realm cisco.com
```

Firewall Placement

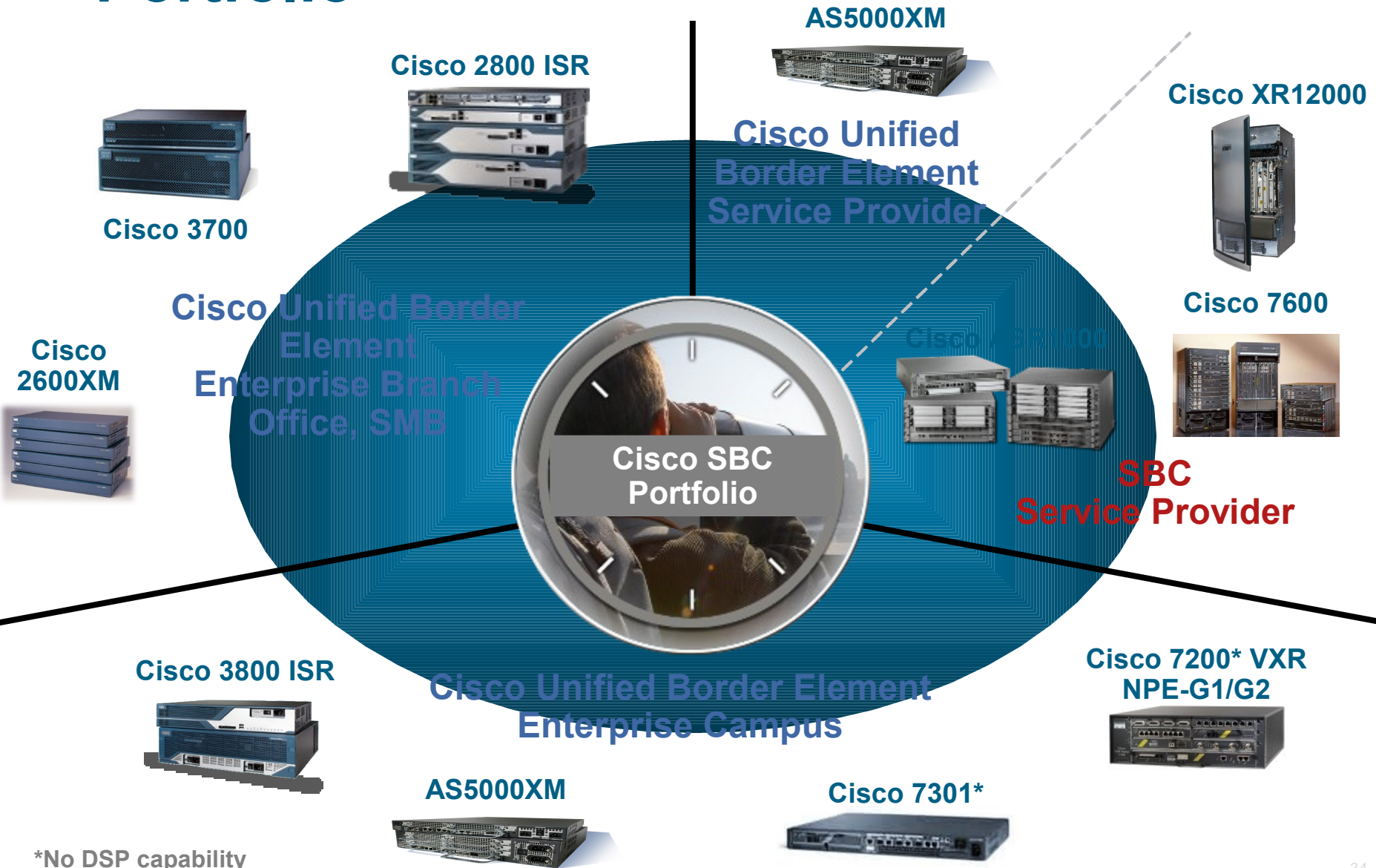
1. Security is a layered approach
2. FW is a general traffic security device, the Cisco Unified Border Element is a voice-application demarcation and security device



- L5 / L7 SIP Validation:
- Reject non-allowed calls, generate CDR
- Call limiting (only accept certain number of calls)
- Codec limiting (only accept certain codecs)
- Call admission control – BW protection
- ACLs – valid source/destination call agents
- Complete rogue/malformed SIP packet protection
- Digest authentication and hostname validation
- SIP registration
- SIP listening port configuration

- L2/L3 Inspection:
- Black hole routing
- Mitigation through TCP window control, drop UDP packets
- ACLs – traffic correct and allowed
- DOS protection
- Optional SIP ALG for cursory SIP rogue/malformed packet inspection

Cisco Session Border Controller Portfolio



*No DSP capability

CUBE Capacity Recommendations

Platform	Cisco Unified Border Element	
	Flow-through Calls	Flow-around Calls
AS5000XM	1000	3000
7301, 7200-NPE-G1	800	2,000
7200-NPE-400	500	1,250
3845	750	750
3825	600	750
3745	500	750
3725	250	750
2851	600	750
2821	400	600
2811	200	400
2801	100	350
2651XM	100	350
2621XM	75	250
2611XM	65	200

Based on 12.4.9T, Basic Calls, VAD On, AAA Enabled, CPU measured at 75%

CUBE Memory Recommendations

Platform	Flash	DRAM
2800/3800	64M	256M
7x00	64M	1G
5400XM	128M	1G



CISCO