

SECURING THE NETWORK



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

78

Service Provider Security Issues

Cisco.com

- **Prevent unauthorized control of their voice and data CPE or gateways, or call control or other elements inside their network**
- **Prevent Denial Of Service (DOS) attacks**
- **Prevent Unauthorized Monitoring**
- **Prevent Installation of unauthorized configuration and/or firmware**
- **Prevent eavesdropping on conversations**
- **Protecting the call signaling**
- **Fraudulent use of PSTN and other services**

VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

79

Cisco NAT/PIX and ALG

Cisco.com

- Cisco implements a set of products to protect SP and customer IP and voice networks:
PIX FW, IOS FW, PIX NAT, IOS NAT
- To support voice these products has a feature called Application Layer Gateway (ALG):
ALG main function is to look inside the voice signaling packet and changes the Transport address in SDP (Session Description Protocol) or H.245
- Recommend a separate secured management network

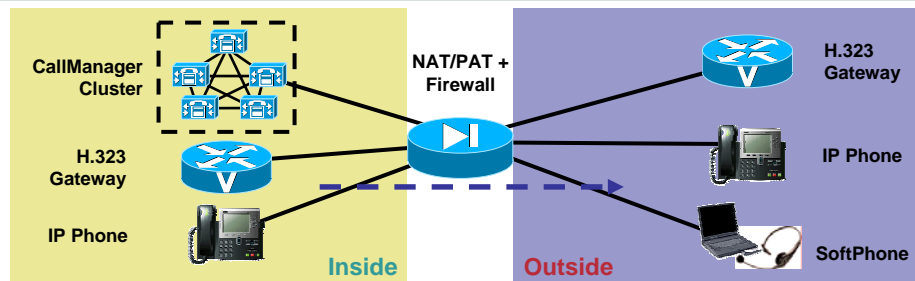
VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

80

NAT/PAT + Firewall + Voice Protocols

Cisco.com



- NATs work at layer 3
- NATs modify the source IP address
- NATs don't modify L4/L5/L6/L7 addresses, yet voice protocols (SCCP, H.323) embed IP address at L4-L7
- Embedded L4-L7 addresses become non-routable, so applications will not work
- Application Layer Gateway (ALG) required on NAT device to "fixup" voice protocol

VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

81

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

82

Cisco.com

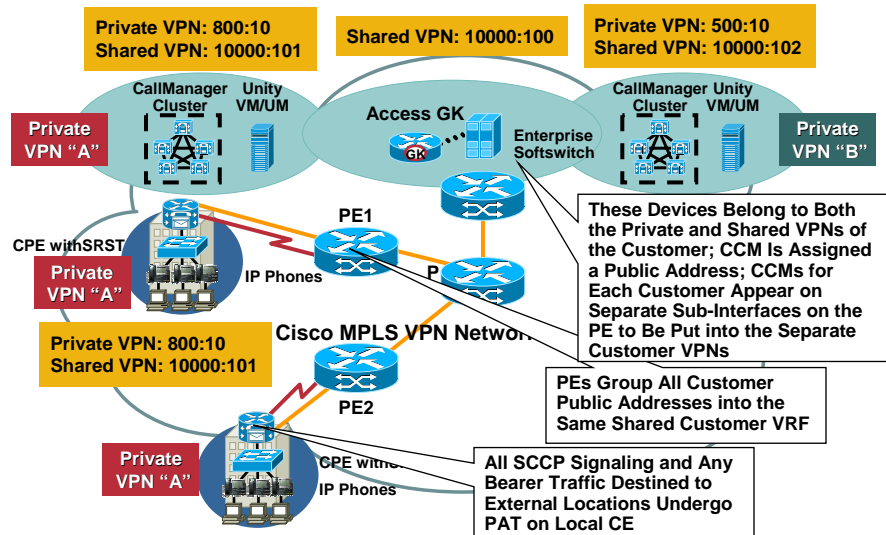
VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

83

NAT for SP Hosted Cisco CallManager with SRST

Cisco.com



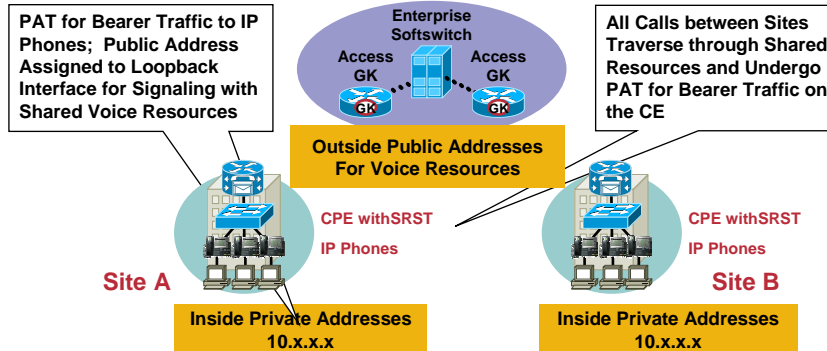
VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

84

MPLS Customer Network: SRST/CME/Cisco IOS Gateway

Cisco.com



- Loopback interface on CPE is in the public address space
- IP phones are PATed to the loopback interface
- On-net bearer traffic remains within the customer's VPN
- Off-net traffic is routed through the SP's off-net infrastructure

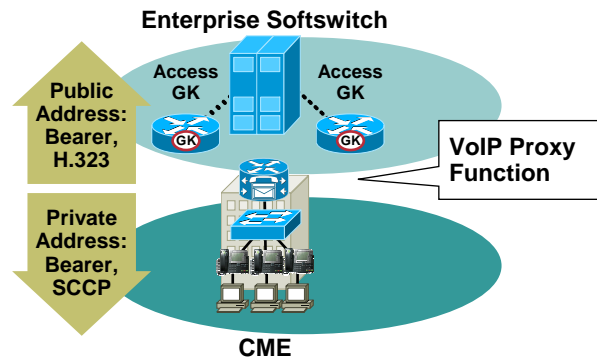
VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

85

CME Built in NAT/Proxy Functionality

Cisco.com



- CME has eFXS (emulated FXS ports)
- CME perceives the IP phones behind it as FXS ports
- Calls from the IP phones are sourced from the interface to which H.323 is bound
- IP phones speak skinny protocol to the CME

VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

86

NAT Order of Operations

Cisco.com

INSIDE-TO-OUTSIDE

- If IPsec then check input access list decryption—for CET (Cisco Encryption Technology) or IPsec
- Check input access list
- Check input rate limCME
- Input accounting
- Policy routing
- **Routing**
- Redirect to web cache
- **NAT inside to outside (local to global translation)**
- Crypto (check map and mark for encryption)
- Check output access list
- Inspect (Context-based Access Control [CBAC])
- TCP intercept
- Encryption

OUTSIDE-TO-INSIDE

- If IPsec then check input access list
- Decryption—for CET or IPsec
- Check input access list
- Check input rate limCME
- Input accounting
- **NAT outside to inside (global to local translation)**
- Policy routing
- **Routing**
- Redirect to web cache
- Crypto (check map and mark for encryption)
- Check output access list
- Inspect CBAC
- TCP intercept
- Encryption

VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

87

VOICE QUALITY AND QUALITY OF SERVICE



VVT-2021
9919_06_2004_X

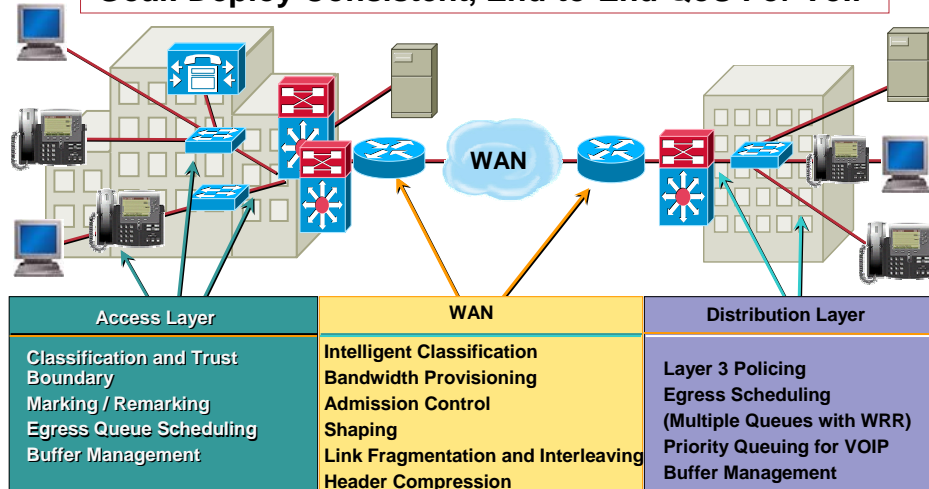
© 2004 Cisco Systems, Inc. All rights reserved.

88

Voice Quality

Cisco.com

Goal: Deploy Consistent, End-to-End QoS For VoIP



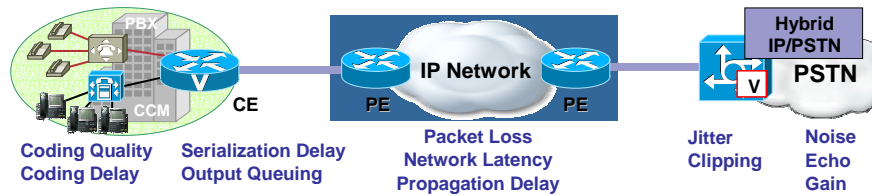
VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

89

Voice Quality

Cisco.com



- **Cisco DSPs:** G.729 packet loss concealment; adjustable packetization to lower coding delays; adjustable gain/loss per IP phone/port to reduce echo, clipping, and noise; dynamic jitter buffer to reduce delay and clipping; enhanced echo cancellation (G.168); SAA may kick off CAC
- **Edge QoS:** IP Precedence, RSVP, LLQ (CBWFQ withPQ), MLPPP LFI, 802.1p/q LAN COS, Auxilliary VLANs for policy management, WAN traffic shaping, Auto QoS on switches and routers for simpler provisioning
- **Core QoS:** WRED, MPLS traffic engineering for customized policy routing, MDRR round robin scheduling technique in core router

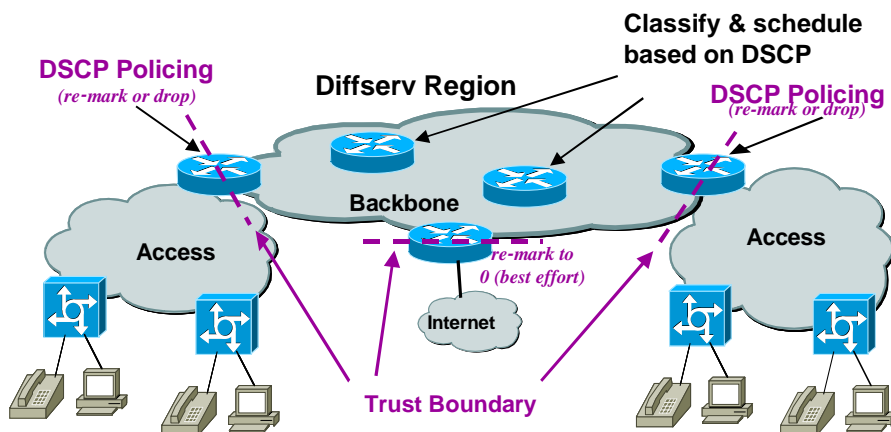
VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

90

QoS Architecture

Cisco.com



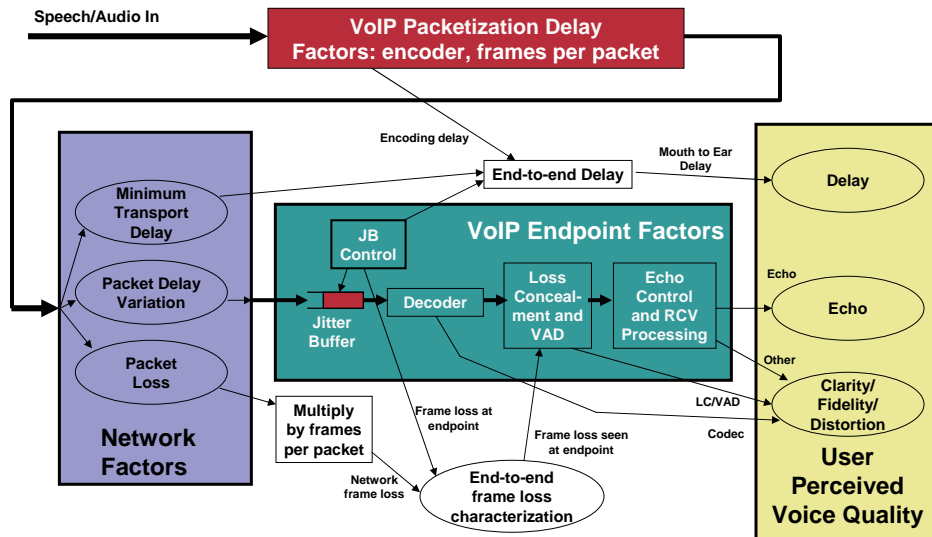
VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

91

Impairments Affecting Speech Quality (End-to-End Perspective)

Cisco.com



Recommendations for Loss, Delay, Jitter (End-to-End Perspective)

Cisco.com

- VoIP networks are typically designed for 0 packet loss
 - PLC (Packet Loss Concealment) techniques of codecs
 - Only real loss is due to Layer 2 bitter errors or network failures
- Delay design is currently based upon ITU-T G.114 recommendation (under investigation)
 - 150 msec one-way delay mouth to ear
 - Delay budget must include propagation, congestion, serialization, and service (codec, de-jitter buffer) delays
- “Jitter” can mean the maximum tolerated jitter or the jitter buffer setting recommendation
 - Cisco VoIP adaptive jitter (play-out) buffer can increase and decrease dynamically without affecting voice quality. So, jitter does not need to be separately defined as long as end-to-end delay budget is met
 - Other VoIP systems may place constraints on the network such that an explicit jitter maximum needs to be defined

VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

93

SCALING THE ENDPOINTS AND THE NETWORK



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

94

CISCO CALLMANAGER



VVT-2021
9919_06_2004_X

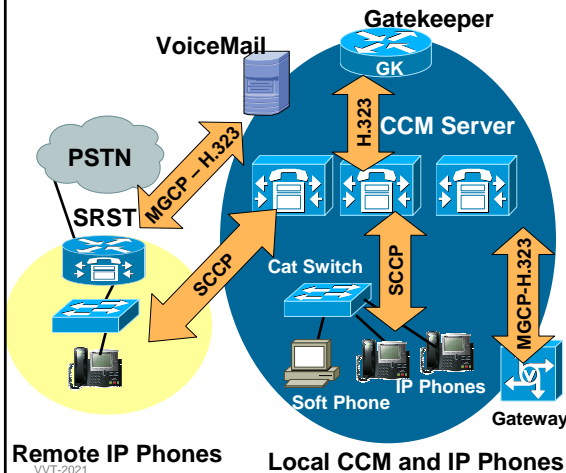
© 2004 Cisco Systems, Inc. All rights reserved.

95

Basic CallManager Components

Cisco.com

CallManager Components are Comprised of the Following:



- H.323 Gatekeeper
- CallManager Server
- Catalyst In-line powered switches
- IP Phones
- Gateways for fax and “black phones”
- Softphones
- SRST for backup to centralized CCM
- Voicemail Server

Remote IP Phones

Local CCM and IP Phones

VVT-2021
9919_06_2004_X

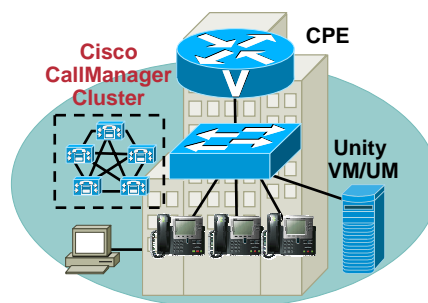
© 2004 Cisco Systems, Inc. All rights reserved.

96

Customer Deployments Functional Area: Cisco CallManager

Cisco.com

- Cisco CallManager offers medium to large enterprise customers an IP PBX solution
- Cisco CallManager may reside on premise (distributed) or remain hosted in the service provider network (centralized)
- SCCP (Skinny) protocol for client signaling and control
- H.323 for RAS and trunk side signaling and control
- MGCP support for gateway signaling and control
- Can perform digit manipulation at endpoint



VVT-2021
9919_06_2004_X

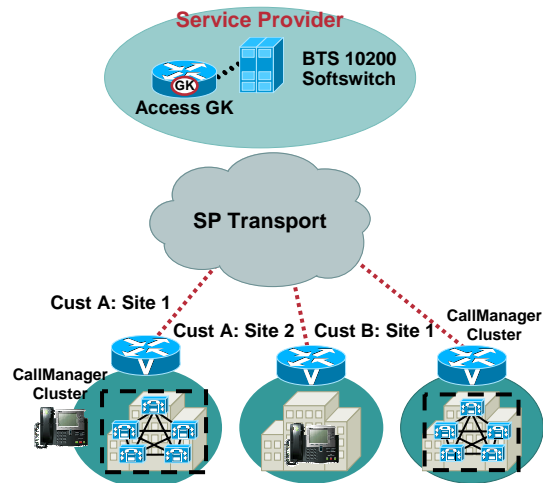
© 2004 Cisco Systems, Inc. All rights reserved.

97

Customer Deployment CCM at the Customer Premise

Cisco.com

- Cisco CallManager clusters are deployed at the customer premise
- Customer may choose to manage the devices, or outsource remote management to service provider
- Multisite businesses can use a centralized deployment (i.e., branch IP phones to corporate CallManager cluster)



VVT-2021
9919_06_2004_X

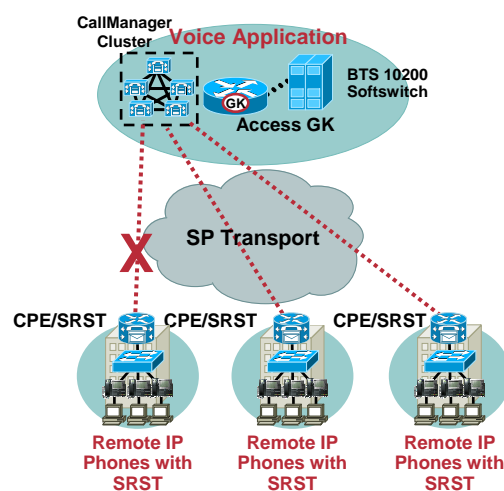
© 2004 Cisco Systems, Inc. All rights reserved.

98

Customer Deployment CCM at the Service Provider

Cisco.com

- A single CCM cluster is allotted for each customer
- Hosting in the service provider NOC eliminates CCM NMS access issues
 - NMS has no awareness of MPLS tags to overlapping IP addresses
- Requires backup mechanism in the event that WAN transport link goes down



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

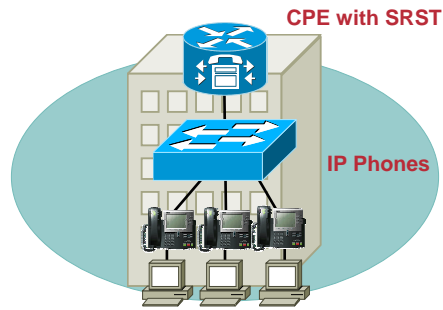
99

Customer Deployments Functional Area: Remote IP Phones (SRST)

Cisco.com

- Capability in branch office routers for IP telephony redundancy
- Provides backup call control to remote site in the event that CallManager connectivity is lost (i.e., WAN failure)
- Designed for centralized CallManager deployment
- CE router can support SRST functionality on same platform
- Supports 24 to 480 users dependent based on platform performance and feature license
- Can perform digit manipulation at endpoint

Survivable Remote Site Telephony (SRST)



VVT-2021
9919_06_2004_X

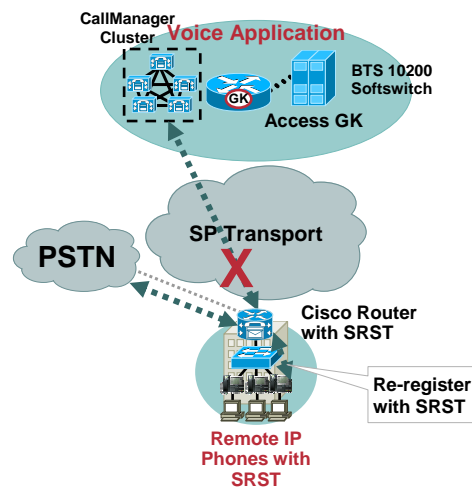
© 2004 Cisco Systems, Inc. All rights reserved.

100

Customer Deployment Survivable Remote Site Telephony Backup

Cisco.com

- IP Phones exchange keepalive messages and call processing messages with centrally located Cisco CallManager (CCM)
- WAN link fails—IP phones lose contact with CCM
- IP Phones register with local router as router of last resort
- Router queries phones for configuration and auto-configures CME/elf
- Router provides call processing for duration of failure via PSTN
- Upon restoration of WAN, IP Phones revert back to CCM



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

101

CISCO CALLMANAGER EXPRESS



VVT-2021
9919_06_2004_X

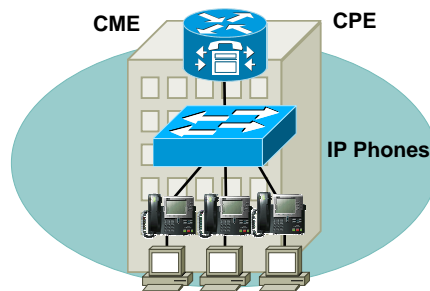
© 2004 Cisco Systems, Inc. All rights reserved.

102

Customer Deployments Functional Area: CallManager Express (CME)

Cisco.com

- Software feature added to Cisco IOS CPE to provide call processing for IP phones using SCCP
- Performs local IP telephony call control
- Offers IP telephony for small offices (up to 120 users)
- End customer uses VoIP for internal, site-to-site, and PSTN off-net calling
- Supports trunk side H.323, SIP and MGCP
- Can perform digit manipulation at endpoint



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

103

Cisco CallManager Express Platform Density

Cisco.com

Platform	Supported Phone Density
1751, 1760, IAD24xx	24
261xXM, 262xXM	36
265xXM, 3640	48
2691	72
AGM, 3725	96
3745, 3660	120

VVT-2021
9919_06_2004_X

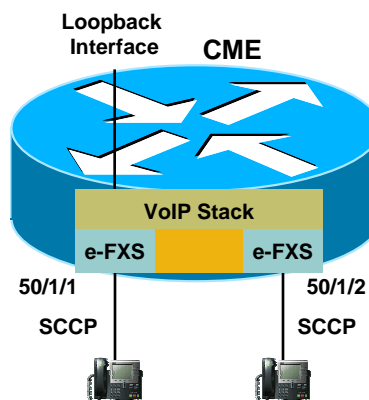
© 2004 Cisco Systems, Inc. All rights reserved.

104

Cisco IOS Telephony Service (CME) Architecture

Cisco.com

- CME sees IP phones as emulated fxs phones or “e-fxs ports”
- To the GK, CME appears as an analog GW
- Like analog GWs, CME will register its individual dial peer destination patterns (E.164)
- GK should not use these E.164 addresses for routing; turn off E.164 address registration
- Loopback address bound to RTP and signaling using “bind” command



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

105

GW WITH PBX



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

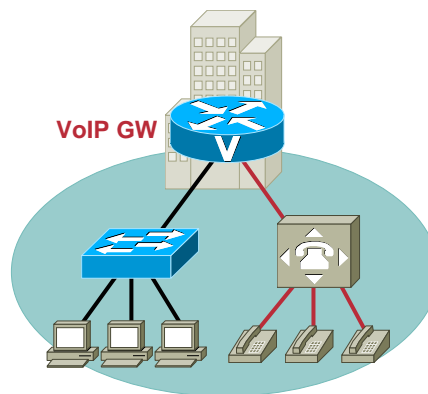
106

SAS Section 2.2.2.4

Customer Deployments Functional Area: Cisco IOS Gateway with PBX

Cisco.com

- Cisco IOS GW CPE front-ends a traditional PBX via FXS, FXO, T1/E1, T3/STM-1, Cable, DSL
- Enables migration of existing TDM PBX (ISDN, Q.SIG, DPNSS) customer to IP data/voice convergence with minimal investment
- Branch offices use VoIP for PBX tie-line and PSTN off-net calling
- Customers may upgrade to IP telephony (IP PBX) when ready
- GWs: AS5000s, MGX8000s range from ~200 to ~8000 DS0s



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

107

MANAGED IADs



VVT-2021
9919_06_2004_X

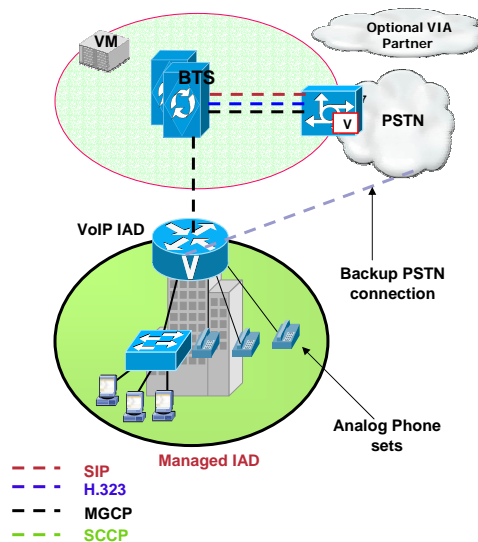
© 2004 Cisco Systems, Inc. All rights reserved.

108

Centralized Call Control IAD/ATA

Cisco.com

- SP offering for small and medium business needs
- IAD24xx provides up to 24 analog ports for analog phones, FAX, etc.
- VG248 for use with CCM to support analog devices
- ATA-186 provides 2 analog ports
- ATA-188 provides 2 analog ports and 1 ethernet port
- Coming soon: Linksys ATA



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

109

ON-PREMISE SIP PHONES



VVT-2021
9919_06_2004_X

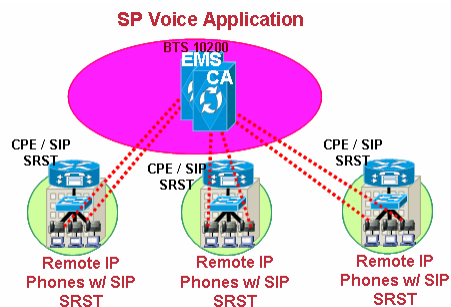
© 2004 Cisco Systems, Inc. All rights reserved.

110

SIP Phone with SIP SRST

Cisco.com

- Targeted toward small and medium business that requires limited voice features set
- Centralized call control or Hosted IP telephony with SIP as the signaling protocol used by the BTS10200 to communicate with the IP phones
- BTS10200 functions as a SIP B2BUA and a registrar
- BTS10200 is fully partitionable and uses its Centrex features to provide features and service to the IP phones. For FAX, customer may choose to have a separate ATA gateway with FXS ports or add FXS ports on the data access router. In both cases the fax ports will be controlled by BTS10200
- PSTN access (for DID/DOD) is provided by the SP VoIP PSTN infrastructure. SP provides voice mail services through third-party servers
- SIP SRST as a feature that runs on IOS router is used. The IP phones would do dual registration (with the BTS10200 and the IOS SRST)



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

111

SCALING THE BUSINESS VOICE SOLUTION



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

112

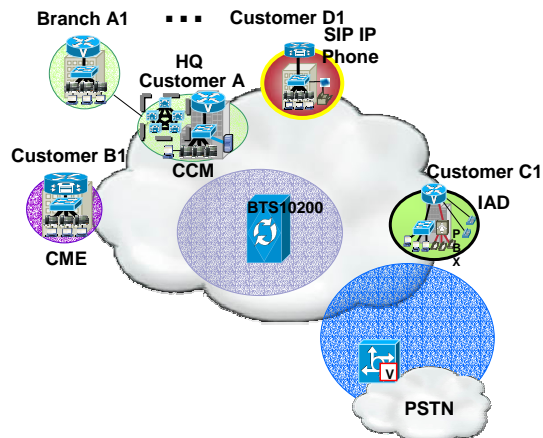
Scaling Deployments: Small

Cisco.com

- **Small scale**

CPE: CCM for large sites clustered as enterprises grow in size (30000), CME or IAD for small sites (<120), GW for legacy PBX sites or SIP IP Phone for small office or home office

PSTN: non-SS7 GW (analog to T1/E1 interfaces)



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

113

Scaling Deployments: Medium

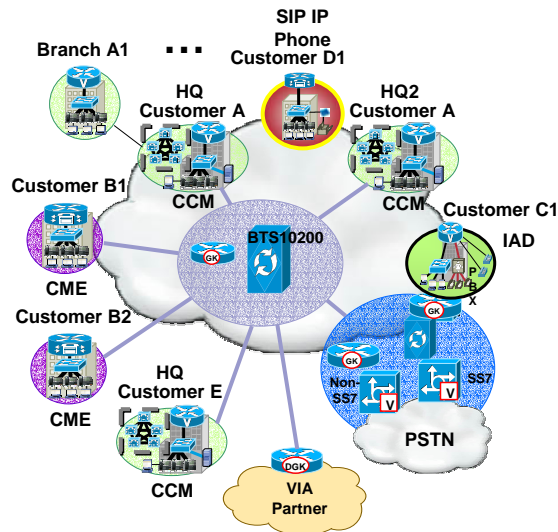
Cisco.com

- **Medium scale**

CPE: Inter-cluster trunking

Core: Add centralized routing (BTS and AGK) to accommodate customer volume

PSTN: Add GWs and GK, add SS7, 8850 large GWs, VIA partner



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

114

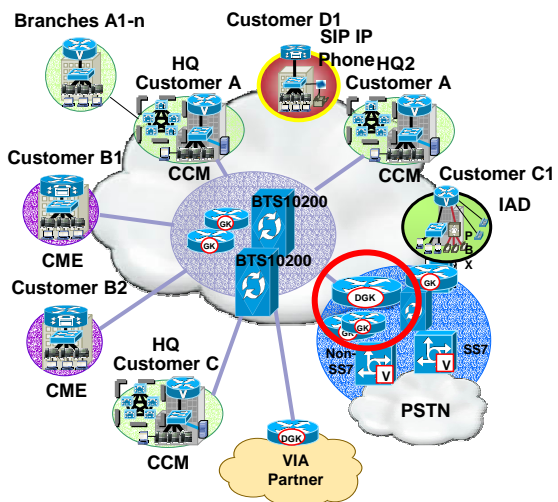
Scaling Deployments: Large

Cisco.com

- **Large scale**

Core: Cluster AGKs, additional BTS and load balance with AGKs

PSTN: DGK, cluster PSTN GKs



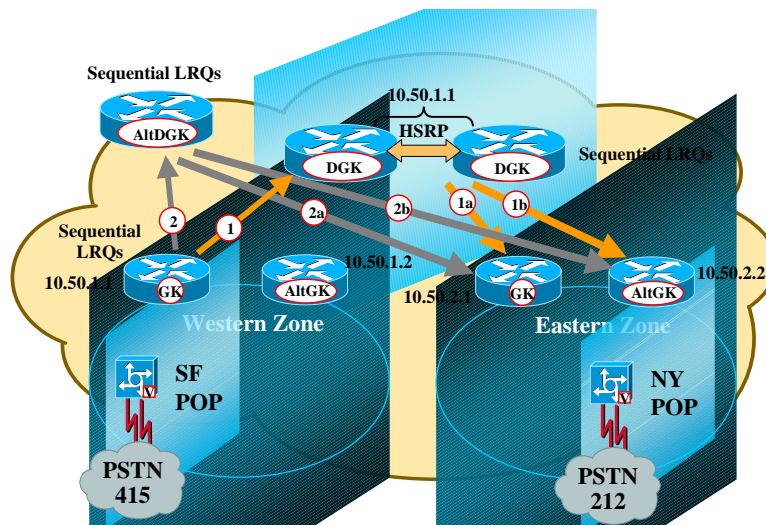
VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

115

Gatekeeper Scaling and Redundancy

Cisco.com



VVT-2021
9919_06_2004_X

© 2004 Cisco Systems, Inc. All rights reserved.

116