Supporting CCME Remote Phones over IPSec VPNs

Application Note

March 30, 2005
Cisco Systems Inc.

Table of Contents

1 Introduction

1.1 Objective

This application note describes how remote IP phones may be supported by CCME for teleworkers working out of their homes over an IPSec VPN.

1.2 Scope

This application note provides the necessary information for the deployment of remote phones over IPSec VPN in two deployment models, Standalone CCME/CUE Teleworker Extension and CCME PBX Teleworker Extension. The CME teleworker solution should only be positioned for remote teleworkers, who access the PSTN and VM at a head-end CME. TAC will not support any implementations that deviate from these requirements.

If any of the following criteria are a required, Cisco CallManager centralized call processing or distributed CCME at each site must be used:

1. PSTN trunk (BRI, PRI, T1/E1 or analog FXO) is required at remote site
2. Distributed voicemail needs to be supported at remote site
3. E911 or emergency responder is required at remote site
4. Partitions and Calling Search Space functionality is required at remote site
5. Full Survivable Remote Site Telephony (SRST) required at remote site

For the purposes of this document, a "Remote IP phone" indicates an IP phone that is running a skinny phone load that registers across the WAN to a CCME router.

1.3 Audience

This document is targeted at Systems Engineers and other personnel who assist in design of voice over VPNs or Teleworker applications.

1.4 References

1. Voice and video enabled VPN (V3PN) solutions:
   http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns241/networking_solutions_sub_solution_home.html
2. Cisco Business Ready Teleworker solution:
   http://www.cisco.com/en/US/netsol/ns340/ns394/ns430/networking_solutions_packages_list.html
3. Call Manager Express Documentation:
   http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/itscdc/itsph.htm
4. Cisco AVVID Network Infrastructure Enterprise Quality of Service Design:
   http://www.cisco.com/application/pdf/en/us/guest/netsol/ns17/c649/ccmigration_09186a00800d67ed.pdf

2 Overview

This solution extends IP voice services out to Teleworkers using Cisco CallManager Express (CCME) over an IPSec QoS-enabled VPN (a.k.a., V^3PN). This CCME remote phone solution should not be considered a low-end replacement of the CallManager centralized call processing solution but as an additional capability of CCME that has limited support for remote phones for teleworkers. This solution is a culmination of the best practices from three existing solutions, Business Ready Teleworker (formally known as Enterprise Class Teleworker), Voice and Video Enabled IPSec VPN (V^3PN), and the CCME/CUE for the branch or small business.

There are two deployment models that CCME may be used to provide Teleworker voice services. CCME can provide the sole call processing, PSTN gateway and voice mail functions for the local and Teleworker IP phones (Figure 1) or an adjunct call processing agent to an existing PBX providing Teleworker IP phones a gateway to the corporate voice network (Figure 2).

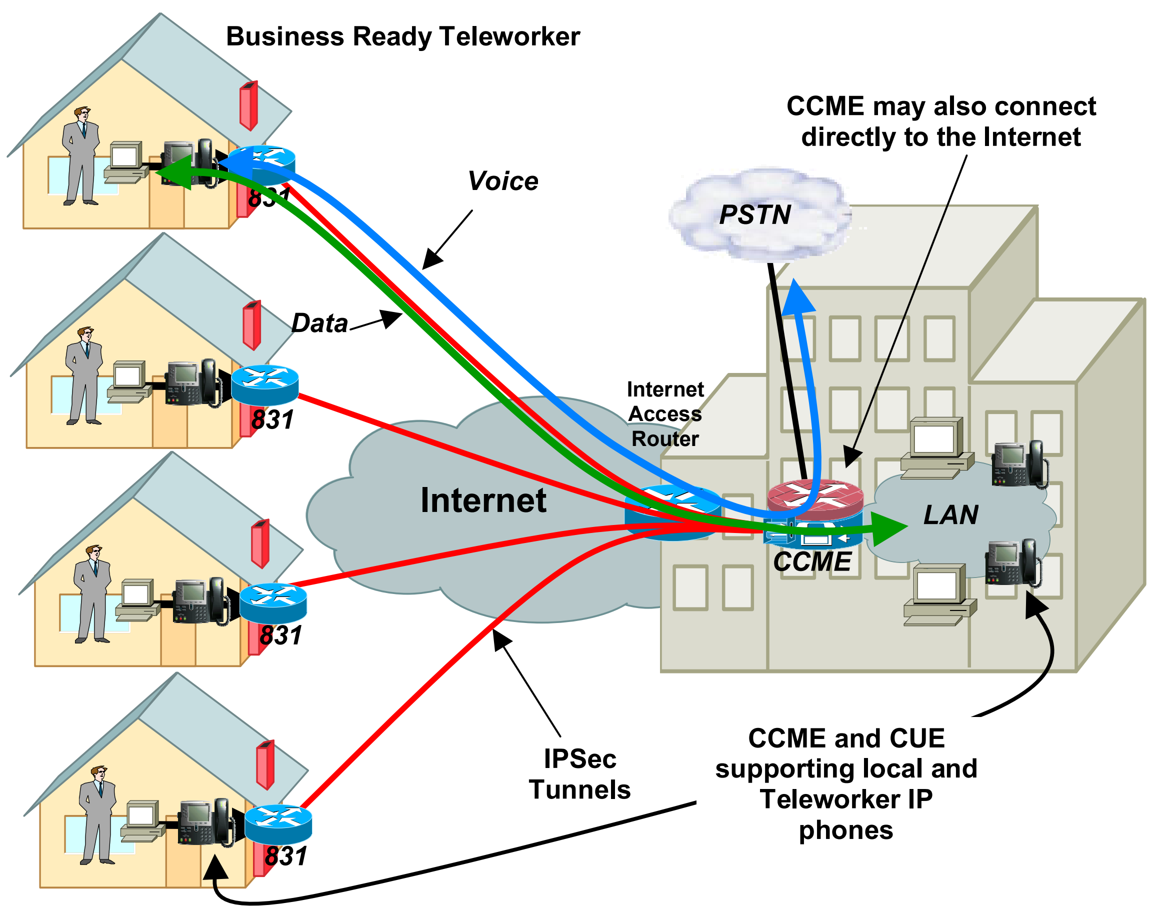

Figure 1 - Standalone CCME for Teleworkers

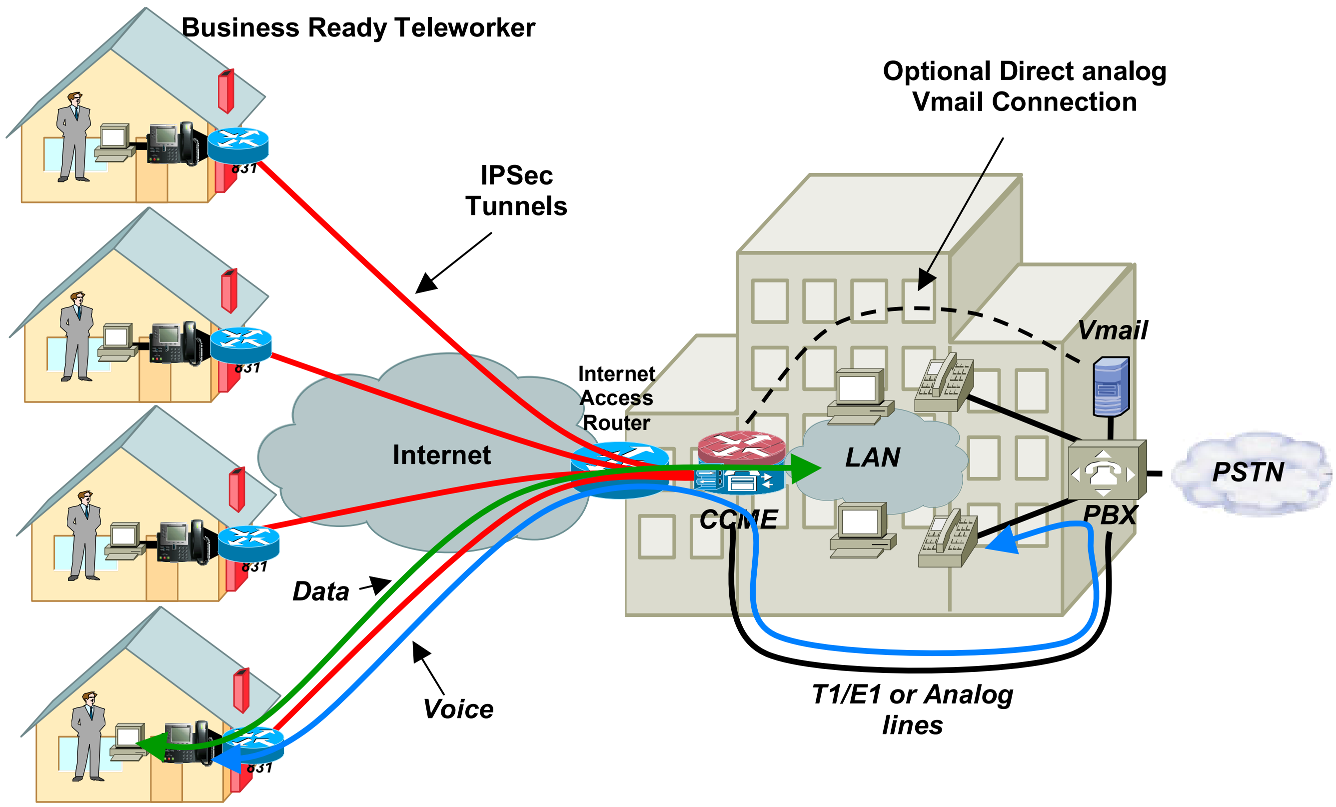

Figure 2 - CCME PBX Extension to Teleworkers

2.1 Benefits

Below are some of the benefits this CCME remote phone solution has to offer.

- Provides a cost-effective starter kit for a voice and data enabled teleworker solution.
- Provides a single device solution for voice, data, and Teleworker VPN.
- Provides fully encrypted voice and data between the Central and Teleworker remote sites.
- Provides centralized voice mail for all phones.
- Supports dynamic IP addresses on the remote sites.
- Supports full routing between the central and remote sites.

2.2 Recommendations and Restrictions

Below are some of the recommendations and restrictions when deploying this CCME remote phone solution.

Restrictions:
Remote skinny client control protocol (SCCP) phones connected across WAN links are subject to the following restrictions:

- Cisco TAC will not handle any voice or signaling issues for remote IP phones, unless the same issue can be replicated for LAN phones.
- E911 or emergency calls are not supported from the remote Teleworker IP phones.
- For inbound or outbound calls, remote IP phones cannot failover to a PSTN connection. Remote phones must use the WAN for all calls, even if available bandwidth is not sufficient to guarantee voice quality.
- GRE is required for remote teleworker sites. Calls from remote phones to PSTN/CUE will receive one-way audio if GRE is not used.
- Remote IP phones do not support Network Address Translation (NAT). All Cisco CME phones must use IP addresses that are routeable to and from Cisco CME. Remote IP phones must be able to access the IP addresses that are used for all other local and remote phones.
- All calls made to and from remote IP phones must use G.711. Cisco CME does not support the ability to specify G.729 codec for remote IP phones
- Cisco CME does not support Call Admission Control (CAC) for remote SCCP phones, so voice quality can degrade if a WAN link is oversubscribed.
- High-bandwidth data applications used over a WAN can cause degradation of voice quality for remote IP phones.

Recommendations:

- The recommended minimum bandwidth of one T1 (1.536 Mbps) or E1 (2.048Mbps) of bandwidth at the hub site
- Because only G.711 is supported, the minimum upload bandwidth of 256Kbps and download bandwidth of 1.4 Mbps for each remote site is recommended. Note that this bandwidth recommendation does not equate to the voice-only bandwidth requirement but is a minimum bandwidth recommendation for both voice and data based on lab testing and production field experience.
- Blocking 911 calling via Class of Restriction (COR) or Time-of-day call blocking is recommended to restrict teleworker 911 calling while allowing central site 911 calling. Both configurations are shown in Section 3.2. A precaution such as placing stickers on the remote phone that clearly states that 911 or emergency number dialing or training personnel to be wary of this limitation is recommended.
- Due to the 911 call restrictions mentioned above, Time-of-day call blocking may be used to configure shared line appearances between central and remote site IP phones. This will allow the sharing of a common phone number while blocking 911 calls from the Teleworker IP phone and allowing 911 calls from the central site phone.

- The use of hardware encryption is recommended in all platforms for consistent voice quality. Currently when running CCME in the VPN headend 37xx routers, EPII and HPII VPN AIMs must be used. This solution has been only tested with 2691 as the CCME/VPN headend combination.
- For calls destined to AA or VoiceMail it is recommended that VAD be turned off.
- Quality of Service and Oversubscription - The Low-latency Queue (LLQ) on the headend CCME router should be allocated no more than 33% of the total headend Internet bandwidth. This will determine the number of simultaneous intra-teleworker and central site calls that can be made over the VPN with high quality. Exceeding the number of calls the LLQ is provisioned for could result in poor voice quality for all calls in progress.
- Although high voice quality can be achieved by deploying QoS on the edge devices (i.e., CCME and remote routers), guaranteeing high quality voice requires QoS to deployed throughout the whole network which includes the Enterprise Internet edge router and the SP networks between the CCME and remote Teleworker routers.

2.3 Minimum System Requirements

The following are the minimum system requirements for CCME teleworker solution which has been validated.

Standalone CCME/CUE Teleworker Extension

- Platform: 37xx, 2691 with NM-CUE, AIM-voice, T1/E1 VIC and AIM-VPN/EPII
- CUE release 1.0.1 or higher
- CCME router IOS version, 12.3.(4)T Advanced IP Services or higher
- Cisco 831 with IOS IP/FW/PLUS 3DES 12.2.13ZH, or 17xx, 26xx, 37xx with IP/FW/PLUS 3DES 12.2.15T or higher as remote router

CCME PBX Teleworker Extension

- Platform: 37xx, 2691 with FXO/FXS or T1/E1 voice modules and AIM-VPN/EPII
- CCME router IOS version, 12.3.(4)T Advanced IP Services or higher
- Cisco 831 with IOS IP/FW/PLUS 3DES 12.2.13ZH, or 17xx, 26xx, 37xx with IP/FW/PLUS 3DES 12.2.15T or higher as remote router

3 Deployment Models & Configurations

There are two deployment models described in this application note. These are:

- ***Standalone CCME/CUE Teleworker Extension*** where CCME provides the sole call processing, PSTN gateway and voice mail for the local and Teleworker IP phones.
- ***CCME PBX Teleworker Extension*** where CCME an adjunct call processing agent to an existing PBX providing Teleworker IP phones a gateway to the corporate voice network.

The following sections describe the configuration required to implement each of these deployment models.

3.1 Common Configuration

This section describes the common configuration required for both deployment models. Three primary features are configured, IPSec-protected GRE which includes the support for remote site dynamic IP addressing, Quality of Service (QoS) for insuring high quality voice and Basic Security which includes access control lists and IOS Firewall. IOS Firewall may be configured on the CCME router if the Enterprise places CCME directly on the Internet.

3.1.1 IPSec-protected GRE

In its current form, this solution requires the use of Generic Route Encapsulation (GRE) when using IPSec to the remote Teleworker site. Figure 3 illustrates how GRE is used in this application.

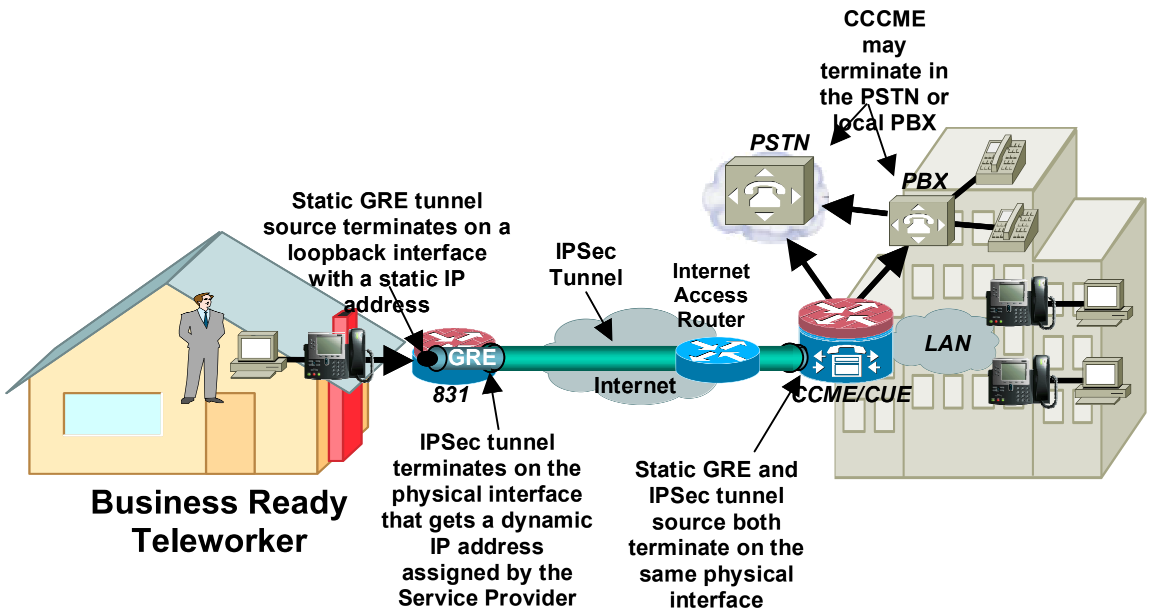

Figure 3 - IPSec-protected GRE Overview

3.1.1.1 Dynamic GRE

One of the misconceptions is that GRE can't be used with dynamically addressed endpoints due to the static nature of the source and destination configuration of the GRE tunnel interface. This can be worked around by using a static address of a loopback interface on the remote site as the GRE tunnel source verses the dynamically addressed physical interface. The remote site's IPSec source IP address is still tied to the physical interface and is dynamically assigned a publicly routable IP address by the Service Provider. Traffic from the remote site routing protocol initiates the IPSec tunnel to the Hub site. Once this IPSec tunnel is established the GRE tunnel then comes up and traffic can flow between the remote and the central site. Routing information is exchanged between the remote and central site and reachability is established between the IP phones and CCME. The IP phones then register and download their configuration including their extension number, speed dials, and any other configured features. Below are example configurations for the IPSec-protected GRE on both the remote and central site routers.

Remote Site VPN Configuration	**Central Site VPN Configu**
crypto isakmp policy 1 encr 3des authentication pre-share group 2 crypto isakmp key bigsecret address 192.168.1.1 crypto isakmp keepalive 10 ! crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac ! crypto map static-map 10 ipsec-isakmp set peer 192.168.1.1 set transform-set vpn-test match address dyn-crypto qos pre-classify ! interface FastEthernet0/0 ip address dhcp crypto map static-map ! interface Loopback0 ip address 10.64.0.17 255.255.255.255 ! interface Tunnel1 ip address 10.0.7.5 255.255.255.252 qos pre-classify tunnel source Loopback0 tunnel destination 192.168.1.1 ! ip access-list extended dyn-crypto permit gre host 10.64.0.17 host 192.168.1.1	crypto isakmp policy 10 encr 3des authentication pre-share group 2 crypto isakmp key bigsecret crypto isakmp keepalive 10 ! crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac ! crypto dynamic-map dmap 10 set transform-set vpn-test qos pre-classify ! crypto map dynamic-map 10 ipsec-isakmp dynamic dmap ! crypto map dmap local-address FastEthernet0/0 ! interface Tunnel1 ip address 10.0.7.6 255.255.255.252 tunnel source FastEthernet0/0 tunnel destination 10.64.0.17 ! interface FastEthernet0/0 ip address 192.168.1.1 255.255.255.240 crypto map dynamic-map

A wild-card preshared key is shown and used during testing. The use of Digital Certificates is recommended for authentication.

Private IP address that was used for lab testing. In a production deployment this would be a publicly routable IP address

3.1.2 Firewall

Basic Security is implemented on the remote router that includes IOS firewall, Port Address Translation (PAT) and Access Control Lists to protect the teleworker and the connected Enterprise network. The firewall design follows the best practices found at the following URL http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_implementation_design_guide09186a00800fd670.html

The configuration below shows the basic security implemented on the remote and central site routers. Portions are highlighted to show the relationship between the different parts of the configuration. The following configurations show a split-tunnel configuration at the remote site to allow direct access to the Internet. The Central Site configuration only allows IPSec and GRE tunnels in from the remote sites.

The configuration below assumes CCME is behind an Enterprise's Internet access router and firewall. Although not shown in this configuration, CCME may connect directly to the Internet in which case would use IOS Firewall and split-tunneling similar to that shown in the remote site firewall configuration.

Remote Site Firewall Configuration	**Central Site Firewall Configuration**
ip inspect name firewall tcp ip inspect name firewall udp ip inspect name firewall rtsp ip inspect name firewall netshow ip inspect name firewall ftp ip inspect name firewall sqlnet ! interface Loopback0 ip address 10.64.0.17 255.255.255.255 ! interface FastEthernet0/0 description Internet-facing interface ip address dhcp ip nat outside ip access-group INPUT_ACL in ! interface FastEthernet0/1 description Local LAN ip address 10.2.1.65 255.255.255.192 ip nat inside ip inspect firewall in ! ip nat inside source list split-tunnel interface FastEthernet0/0 overload ! ip access-list extended INPUT_ACL remark Allow IKE and ESP from the headend router permit udp host 192.168.1.1 any eq isakmp permit esp host 192.168.1.1 any remark Allow GRE tunnel permit gre host 192.168.1.1 host 10.64.0.17 remark Allow DHCP address from ISP permit udp any any eq bootpc permit icmp any any unreachable permit icmp any any echo-reply permit icmp any any packet-too-big permit icmp any any time-exceeded remark Allow DNS name lookup from router permit udp any eq domain any	interface FastEthernet0/0 description Internet-facing interface ip address 192.168.1.1 255.255.255.240 ip access-group INPUT_ACL in ! interface FastEthernet0/1 description Local LAN ip address 10.2.20.65 255.255.255.192 ! ip access-list extended INPUT_ACL remark Allow IKE and ESP from spoke routers permit udp any eq isakmp host 192.168.1.1 eq isakmp permit esp any host 192.168.1.1 remark Allow GRE tunnels from spokes permit gre any host 192.168.1.1 permit icmp any host 192.168.1.1 unreachable permit icmp any host 192.168.1.1 echo-reply permit icmp any host 192.168.1.1 packet-too-big permit icmp any host 192.168.1.1 time-exceeded remark Allow DNS name lookup from router permit udp any eq domain any deny ip any any !

deny ip any any ! ip access-list extended split-tunnel permit ip 10.2.1.64 0.0.0.63 any deny ip any any	

3.1.3 Quality of Service

Quality of Service is required to minimize voice packet delay, variation in delay (jitter) and packet loss to consistently to provide high-quality voice. The existing methods include traffic classification, prioritization, shaping, and fragmentation/interleaving. The example below is based on the best practices described in the existing V3PN and SOHO QoS design guides.

Note: QoS must be implemented throughout the network to guarantee high quality voice. QoS strategies described in the CCME router configuration should also be implemented in the Enterprise's Internet access router where the transition from a high-speed interface (e.g., Fast Ethernet) to a lower-speed interface (e.g., T1/E1) occurs. This is where congestion would occur and where priority queuing of voice is most likely to be needed.

For information on QoS specifics to encrypted site-site voice and SOHO deployments please see the V^3PN and SOHO QoS SRNDs, both at:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns430/networking_solutions_packages_list.html

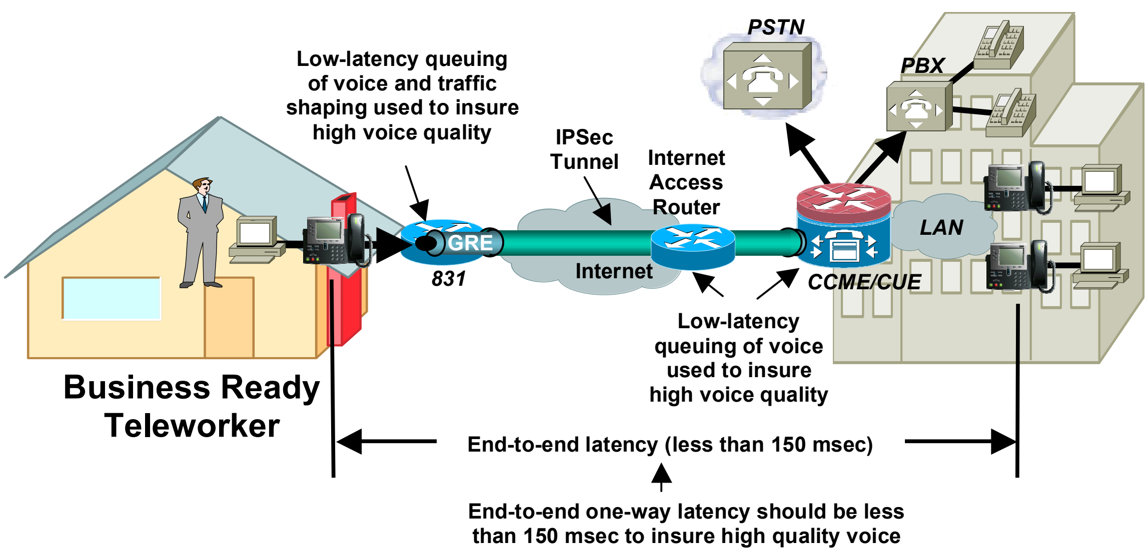

Figure 4 - End-to-end QoS

3.1.3.1 Classification and Queuing

Voice traffic must be classified and be queued with high priority to support high quality. Low-latency (LLQ) bandwidth should not exceed approximately 33% of the available Internet bandwidth to support voice RTP streams (i.e., audio streams). A single encrypted G.711 audio stream requires approximately 120 Kbps when deployed in this CCME remote phone solution. Note the LLQ bandwidth is configured to support 4 simultaneous G.711 calls on a T1, or 5 simultaneous calls on a E1 so that approximately 1/3 of the bandwidth on a T1 or E1 is consumed.

Note:

1. The amount of bandwidth reservable for the LLQ is variable, yet if the LLQ is over-provisioned, the overall effect will be a dampening of QoS functionality. This is because the scheduling algorithm that decides how packets exit the device will be predominantly FIFO (which is essentially "no QoS"). Over-provisioning the LLQ defeats the purpose of enabling QoS at all. For this reason, it is recommended that you not provision more than 33% of the link's capacity as a LLQ

2. The 33% limit for LLQ is a design recommendation. There may be cases where specific business needs cannot be met while holding to this recommendation. In such cases, the enterprise must provision queueing according to their specific requirements and constraints.

Below are the example configurations of implementing QoS in both the remote and central site routers.

Remote Site QoS Configuration	**Central Site QoS Configuration (e.g., 4 remote sites)**
class-map match-all VOICE match ip dscp ef class-map match-any CALL-SETUP match ip dscp af31 match ip dscp cs3 class-map match-any INTERNETWORK-CONTROL match ip dscp cs6 class-map match-all TRANSACTIONAL-DATA match ip dscp af21 !! policy-map split-tunnel-spoke description 1 G.711 GRE/IPSec Tunnel mode call class VOICE priority 120 class CALL-SETUP bandwidth percent 2 class INTERNETWORK-CONTROL bandwidth percent 5 class TRANSACTIONAL-DATA bandwidth percent 22 class class-default fair-queue random-detect dscp-based policy-map split-tunnel-shaper class class-default shape average 360000 3660 0 service-policy split-tunnel-spoke ! interface Tunnel1 ip address 10.0.7.5 255.255.255.252 qos pre-classify tunnel source Loopback0 tunnel destination 192.168.1.1 ! interface FastEthernet0/0 bandwidth 384 ip address dhcp ip access-group INPUT_ACL in ip nat outside service-policy output split-tunnel-shaper load-interval 30 duplex auto speed auto crypto map static-map Traffic shaping is used to throttle traffic down to upload speed to avoid congestion upstream in the SP network	class-map match-all VOICE match ip dscp ef class-map match-any CALL-SETUP match ip dscp af31 match ip dscp cs3 class-map match-any INTERNETWORK-CONTROL match ip dscp cs6 class-map match-all TRANSACTIONAL-DATA match ip dscp af21 !! policy-map split-tunnel-hub description 4 G.711 GRE/IPSec Tunnel mode calls class VOICE priority 480 class CALL-SETUP bandwidth percent 2 class INTERNETWORK-CONTROL bandwidth percent 5 class TRANSACTIONAL-DATA bandwidth percent 22 class class-default fair-queue random-detect dscp-based ! interface Tunnel1 ← Other tunnel interfaces not shown description GRE tunnel to Teleworker1 bandwidth 384 ip address 10.0.7.6 255.255.255.252 load-interval 30 tunnel source Serial0/0 tunnel destination 10.64.0.17 ! interface FastEthernet0/0 description Internet-facing interface behind Internet access router ip address 192.168.1.1 255.255.255.240 ip nat outside service-policy output split-tunnel-hub no ip mroute-cache load-interval 30 duplex auto speed auto crypto map dynamic-map

3.1.3.2 Call Admission Control

Call admission control (CAC) is an important mechanism to prevent the central site's Internet connection from being oversubscribed and unable to maintain the level of service required for high quality voice. A specific amount of LLQ bandwidth for voice must be provisioned on the Internet connection. ***CCME currently does not support CAC so very conservative oversubscription ratios of the number of remote IP phones to the number of calls supported by the configured LLQ bandwidth must be used.***

The required configuration for this CCME remote phone solution is the deployment of no more than 10 remote IP phones with a requirement of at least a T1 (1.536 Mbps) or E1 (2.048Mbps) of Internet bandwidth. In the case of a T1, this provides a 2.5:1 oversubscription ratio of remote IP phones (10) to the number of calls supported (4) by the configured LLQ bandwidth (i.e., 4 calls at 120 Kbps/call = 480 Kbps, 10 IP phones/4 calls = 2.5 phones per number of calls supported.)
In the case of an E1, this provides a 2:1 oversubscription ratio of remote IP phones (10) to the number of calls (5) supported by the configured LLQ bandwidth (i.e., 5 calls at 120 Kbps/call = 600 Kbps, 10 IP phones/5 calls = 2 phones per number of calls supported .)

Note: The marketing restriction of 10 remote sites with 1 IP phone at each site still applies even if there is sufficient bandwidth to support more than 4 or 5 calls G.711 calls.

Although typical Enterprises provision at (4 or 5):1 phones to PSTN voice trunks, careful consideration needs to be made when designing for specific customer traffic patterns. Exceeding the number of calls the LLQ is provisioned for could result in poor voice quality for all calls in progress.

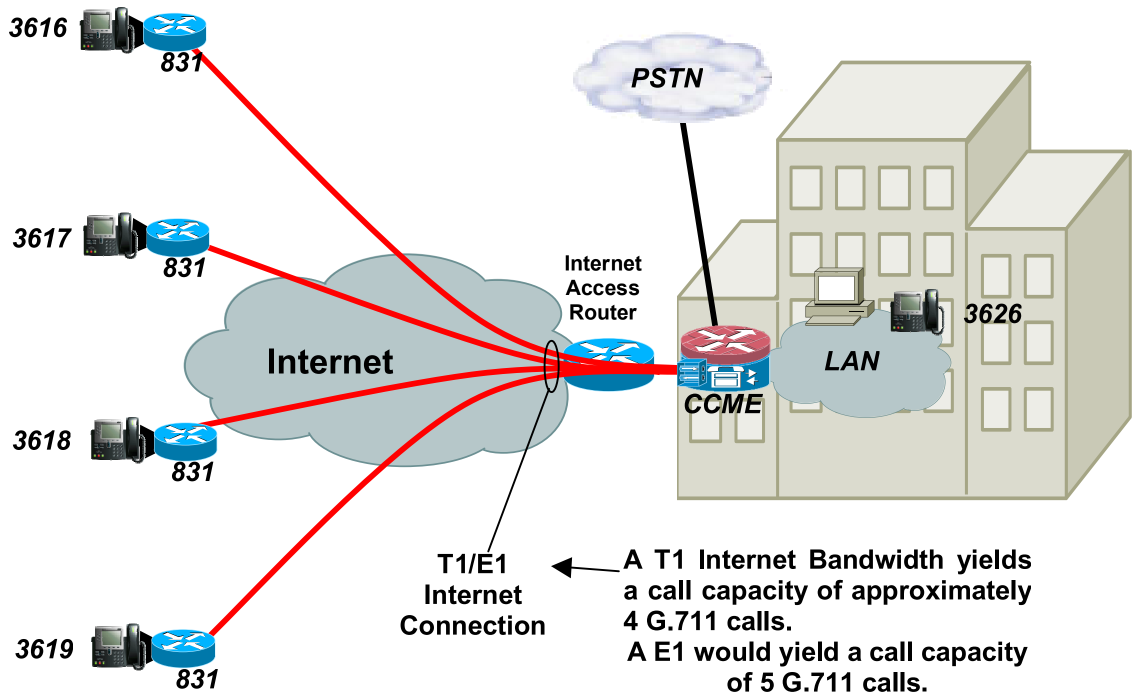

Figure 5 - CAC and the Number of Supported Remote Sites

3.2 Voice

The following sections describe how CCME and CUE are configured for each of the deployment models. The deployment models are as follows:

- Standalone CCME/CUE Teleworker Extension where CCME provides the sole call processing, PSTN gateway and voice mail for the local and Teleworker IP phones.
- CCME PBX Teleworker Extension where CCME an adjunct call processing agent to an existing PBX providing Teleworker IP phones a gateway to the corporate voice network.

3.2.1 Standalone CCME and CUE Teleworker Extension

This deployment model requires both CCME and CUE to provide full voice services. The table below shows both CCME and CUE configurations. Refer to Figure 1 for an illustration of this deployment model.

CCME Configuration	**CUE Configuration**
interface FastEthernet0/1 ip address 10.2.20.65 255.255.255.192 ! interface Service-Engine4/0 ip unnumbered FastEthernet0/1 service-module ip address 10.2.20.126 255.255.255.192 service-module ip default-gateway 10.2.20.65 hold-queue 60 out ! voice-port 3/0/0 ring number 10 ! voice-port 3/0/1 ! voice-port 3/1/0 ! voice-port 3/1/1 ! mgcp profile default ! dial-peer voice 10 pots description local calls destination-pattern 9[2-9]..[2-9]...... port 3/0/0 ! dial-peer voice 11 pots description LD calls destination-pattern 91[2-9]..[2-9]...... port 3/0/0 prefix 1 ! dial-peer voice 12 pots destination-pattern 911 no digit-strip port 3/1/1 !	se-10-73-14-6# sh run Generating configuration: ! Timezone Settings clock timezone America/New_York ! host name hostname se-10-73-14-6 ! domain name ip domain-name localdomain ! DNS Servers ip name-server 10.59.138.4 ntp server 10.73.14.5 groupname Administrators create username steve create username sschuber create username schubby-do create username steves create username stevester create username sschuber phonenumberE164 "4073133626" username schubby-do phonenumberE164 "4073133615" username steves phonenumberE164 "4073133625" username stevester phonenumberE164 "4073133616" username sschuber phonenumber "3626" username schubby-do phonenumber "3615" username steves phonenumber "3625" username stevester phonenumber "3616" groupname Administrators member steve backup server url "ftp://127.0.0.1/ftp" username "" password ""

```
dial-peer voice 100 voip
 description voice mail
 destination-pattern 360.
 session protocol sipv2
 session target ipv4:10.2.20.126
 codec g711ulaw
 no vad
!
telephony-service
 fxo hook-flash
 load 7910 P00403020209
 load 7960-7940 P00303020214
 max-ephones 48
 max-dn 48
 ip source-address 10.2.20.65 port 2000
 auto assign 1 to 48
 create cnf-files version-stamp 7960 Dec 11 2003 09:53:51
 voicemail 3600
 max-conferences 8
 moh music-on-hold.au
 web admin system name steve password cisco
 dn-webedit
 time-webedit
 transfer-system full-consult
 transfer-pattern 3...
 secondary-dialtone 9
!
ephone-dn  1  dual-line
 number 3625
 pickup-group 1
 description CentralSite phone1
 name steves
 call-forward busy 3600
 call-forward noan 3600 timeout 18
!
ephone-dn  2  dual-line
 number 3626
 pickup-group 1
 description CentralSite phone2
 name sschuber
 call-forward busy 3600
 call-forward noan 3600 timeout 18
!
ephone-dn  3  dual-line
 number 3615
 pickup-group 1
 description Teleworker phone1
 name schubby-do
 call-forward busy 3600
 call-forward noan 3600 timeout 18
!
ephone-dn  4  dual-line
 number 3616
 pickup-group 1
 description Teleworker phone2
 name stevester
```

```

ccn application autoattendant
 description "autoattendant"
 enabled
 maxsessions 4
 script "aa.aef"
 parameter "MaxRetry" "3"
 parameter "operExtn" "0"
 parameter "welcomePrompt" "AAWelcome.wav"
 end application

ccn application ciscomwiapplication
 description "ciscomwiapplication"
 enabled
 maxsessions 4
 script "setmwi.aef"
 parameter "strMWI_OFF_DN" "8001"
 parameter "strMWI_ON_DN" "8000"
 parameter "CallControlGroupID" "0"
 end application

ccn application voicemail
 description "voicemail"
 enabled
 maxsessions 4
 script "voicebrowser.aef"
 parameter                                  "logoutUri"
"http://localhost/voicemail/vxmlscripts/mbxLogout.jsp"
 parameter                                        "uri"
"http://localhost/voicemail/vxmlscripts/login.vxml"
 end application

ccn engine
 end engine

ccn subsystem sip
 gateway address "10.2.20.65"
 end subsystem

ccn trigger sip phonenumber 3600
 application "voicemail"
 enabled
 locale "en_US"
 maxsessions 4
 end trigger


 application "autoattendant"
 enabled
 locale "en_US"
 maxsessions 4
 end trigger

voicemail default mailboxsize 21180
voicemail mailbox owner "schubby-do" size 21180
 end mailbox
```

call-forward busy 3600 call-forward noan 3600 timeout 18 ! ephone 1 description 3625 username "steves" password null mac-address 0030.94C3.E77E type 7960 button 1:1 ! ephone 2 description 3626 username "sschuber" password null mac-address 0050.3EFF.DAD1 type 7960 button 1:2 ! ephone 3 description 3615 username "schubby-do" password null mac-address 0030.94C3.A1BC type 7960 button 1:3 ! ephone 4 description 3616 username "stevester" password null mac-address 0009.E847.0019 type 7960 button 1:4	voicemail mailbox owner "sschuber" size 21180 end mailbox voicemail mailbox owner "steve" size 21180 end mailbox voicemail mailbox owner "steves" size 21180 end mailbox voicemail mailbox owner "stevester" size 21180 end mailbox end

3.2.2 CCME PBX Teleworker Extension

In this deployment model CCME provides the call processing and connection to an existing PBX and voice mail system to support the remote IP phones in the Teleworker's home office. The CCME router is connected to the PBX via digital or analog trunks for calling into the existing corporate voice network. DTMF signaling is used by CCME and the voice mail system for accessing user mailboxes and lighting the IP phone's Message Waiting Indicator (MWI). This signaling may traverse the PBX to the Voice Mail system or run directly between the CCME router and the Voice Mail system via an analog voice line. Figures 6 and 7 illustrate these optional configurations.

When accessing the Voice Mail system via the PBX without a direct connection to the Voice Mail system, the CCME router configuration is very similar to the one shown in the previous section less the CUE configuration plus additional dial-peer statements routing PSTN and central site phone traffic to the PBX.

If connecting directly to the Voice Mail system, see the configuration examples in the CCME documentation:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/cme31sa/cme31vml.htm

Considerations when integrating CCME with a legacy PBX and Voice Mail system

- The PBX must have either digital T1/E1 or analog FXS and FXO ports available for routing calls between the IP phones and the existing PBX-connected phones and Voice Mail System.
- The PBX may require a Centralized Voice Mail feature to properly handle DTMF signaling across a trunk port to the CCME router for lighting the IP phone's Message Waiting Indicator.
- An optional configuration would be to directly connect the CCME router to the Voice Mail system via an analog port, therefore requiring this additional analog port be available on the Voice Mail system.
- The Digital T1/E1 and/or analog FXO/FXS Voice Interface Cards (VICs) are required in CCME router for interconnection to the PBX. Note this requirement when evaluating the CCME platform for the necessary slot capacity.

Note: The direct connection to the Voice Mail System is optional and depends on the features enabled in the existing PBX for sending DTMF MWI codes across a trunk port.

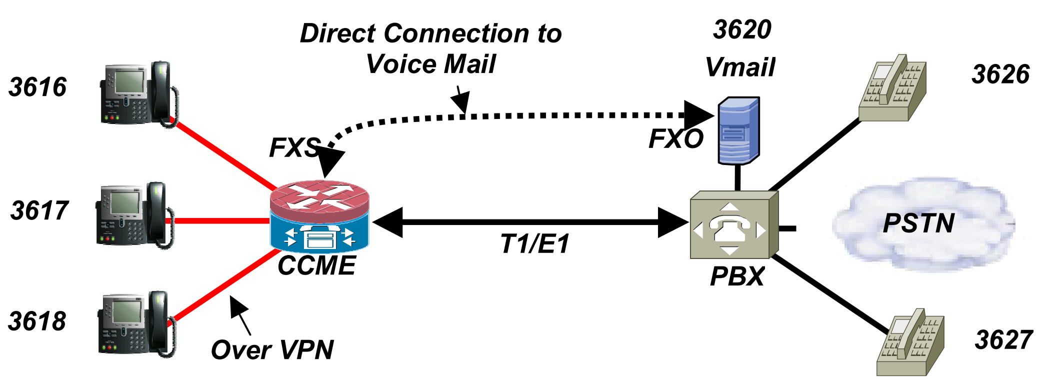

Figure 6 - Digital T1/E1 connection to the PBX with optional analog Voice Mail connection

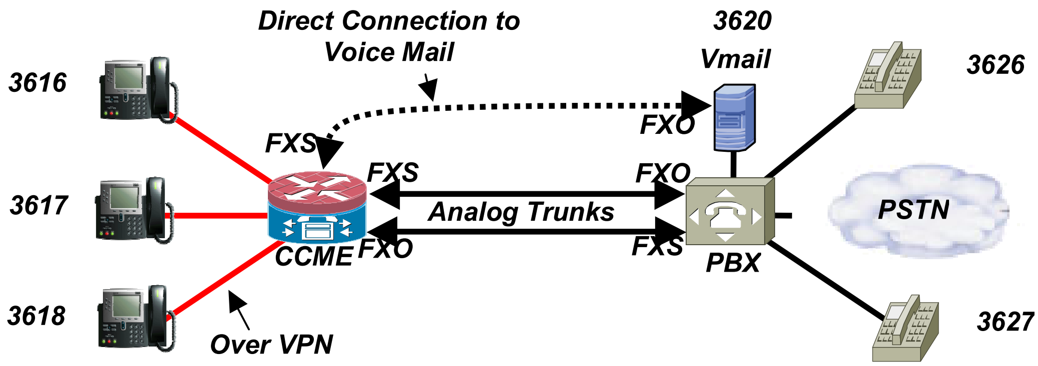

Figure 7 - Analog connection to the PBX with optional analog Voice Mail connection

3.2.3 911 Call Blocking

Remote site 911 calling is not supported in this solution so proper 911 call routing must be configured to ensure that remote IP phones are restricted from 911 calling while local IP phones are not. The next two sections describe two ways to implement Teleworker 911 call blocking using Class of Restriction and Time-of-day call blocking.

3.2.3.1 Class of Restriction (COR) 911 Call Blocking

Class of Restriction (COR) may be used to restrict specific IP phone directory numbers (ephone-dn) access to a 911 dial-peer.

Note: COR is used on ephone-dns and therefore blocking 911 calling on shared line appearances is not supported.

Below is a diagram and example configuration of using COR for restricting remote IP phone 911 calling while allowing local IP phone 911 calling.

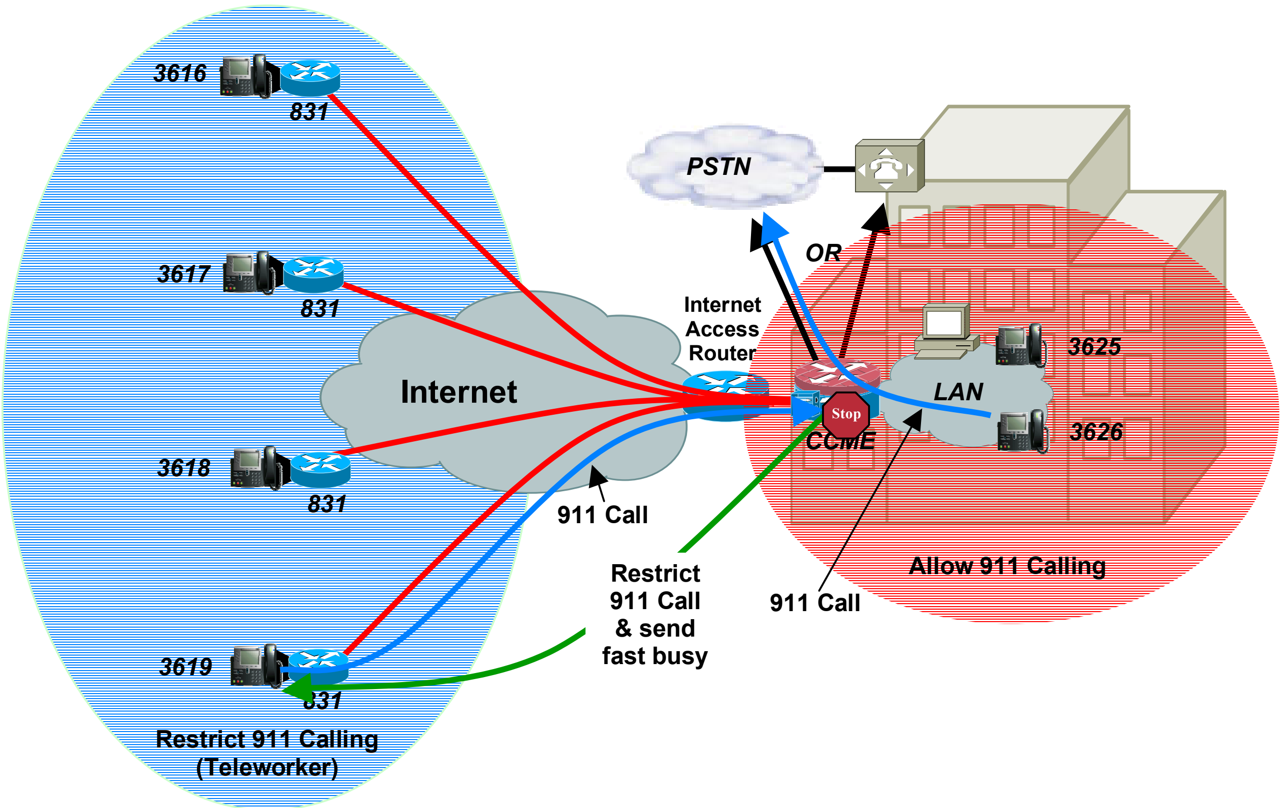

Figure 8 - 911 Call Routing

CCME Configuration

```
dial-peer cor custom
 name 911
!
dial-peer cor list call911
 member 911
!
dial-peer cor list Teleworker
!
dial-peer voice 10 pots
 description local calls
 destination-pattern 9[2-9]..[2-9]......
 port 3/0/0
!
dial-peer voice 11 pots
 description LD calls
 destination-pattern 91[2-9]..[2-9]......
 port 3/0/0
 prefix 1
!
dial-peer voice 100 voip
 description voice mail
 destination-pattern 360.
 session protocol sipv2
 session target ipv4:10.2.20.126
 codec g711ulaw
 no vad
!
dial-peer voice 911 pots
 corlist outgoing call911
 destination-pattern 911
 no digit-strip
 port 3/1/1
!
ephone-dn  1  dual-line
 number 3625
 pickup-group 1
 description CentralSite phone1
 name steves
 call-forward busy 3600
 call-forward noan 3600 timeout 18
!
ephone-dn  3  dual-line
 number 3615
 pickup-group 1
 description Teleworker phone1
 name schubby-do
 call-forward busy 3600
 call-forward noan 3600 timeout 18
 cor incoming Teleworker
```

Two COR lists are created to identify the 911 pots peer and the Teleworker ephone.

The Teleworker cor list is not a member of the 911 class so calls are not routed to the 911 pots peer and a fast busy is returned.

Any dial-peers or ephone-dns that are not assigned a COR are considered unrestricted and accessible by any other dial-peer or ephone.

3.2.3.2 Time-based Call Blocking

Time-based call blocking may be used to restrict specific IP phones (ephones) access to 911 calling. This requires the blocking of 911 calling and exempting central site IP phones. Below is an example configuration of using Time-based call blocking for restricting remote IP phone 911 calling while allowing local IP phone 911 calling. More configuration information on Time-based call blocking can be found at the following URL.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/itsv30/its30blk.htm#2175219

CCME Configuration

```
telephony-service
 fxo hook-flash
 load 7910 P00403020209
 load 7960-7940 P00303020214
 max-ephones 48
 max-dn 48
 ip source-address 10.2.20.65 port 2000
 auto assign 1 to 48
 create cnf-files version-stamp 7960 Dec 11 2003 09:53:51
 voicemail 3600
 max-conferences 8
 moh music-on-hold.au
 web admin system name steve password cisco
 dn-webedit
 time-webedit
 transfer-system full-consult
 transfer-pattern 3...
 secondary-dialtone 9
 after-hours block pattern 1 911 7-24
 after-hours block pattern 2 9911 7-24
!
ephone  1
 description Central Site 3625
 after-hour exempt
 username "steves" password null
 mac-address 0030.94C3.E77E
 type 7960
 button  1:1
!
ephone  3
 description Teleworker shared line 3625
 username "schubby-do" password null
 mac-address 0030.94C3.A1BC
 type 7960
 button  1:1
!
```

911 Call blocking is configured for 7 days a week,- 24 hours a day (7-24)

Central Site phones are exempted from 911 call blocking.

The 3625 shared line appearance on Teleworker phone is blocked from 911 calling.