AT&T IP Flexible Reach Service and AT&T IP Toll-Free on AT&T VPN Service

Customer Edge Router

Customer Configuration Guide for

AT&T Certified IP-PBX Solutions

November 12, 2015

Version 2.5

.

1 Introduction

This Customer Configuration Guide ("CCG") provides recommended guidelines for configuring the Customer-managed Customer Edge Router (CER) for use with AT&T IP Flexible Reach Service (including Enhanced Features Service) and/or AT&T IP Toll-Free on AT&T VPN Service ("AT&T VPN") as the Underlying Transport Service, specific to the various AT&T Certified IP-PBX Solutions defined below in Table 1. CERs can be utilized for either one of those services or for both services simultaneously. This CCG is to be used in conjunction with the *AT&T IP Flexible Reach Service and AT&T IP Toll-Free on AT&T VPN Service Customer Edge Router CCG*, which covers the additional configurations required for use with this service including, but not limited to, the various access types and interfaces, Class of Service.

Please ensure your system set-up is consistent with the recommended specifications provided in this document. AT&T reserves the right to modify or update its guidelines at any time without notice, so please check the following link to be sure you have the latest version of this document (***http://www.corp.att.com/bvoip/avpn/implementation/*** *(login: att, password: attvoip)*). You may also wish to consult with your AT&T technical sales representative to have them verify that you have the latest document.

AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free over AT&T VPN Service currently support the following IP PBX systems:

Table 1: AT&T Certified IP-PBX Solutions for use with AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free over AT&T VPN Service

IP-PBX Vendor / Version **Documentation Link**	**SBC Vendor / Version** **Documentation Link, if not included in IP-PBX CCG**	**BVoIP Service Certified** **i.e. IP Flexible Reach, IP Toll Free**
AASTRA		
Clearspan IP PBX Release R17sp4 **http://www.aastrausa.com/index.htm**	**Acme Packet (SBC) Net-Net OS-E Version E3.6.0.M4P5**	**IP Flexible Reach**
AudioCodes		
Genesys Voice Platform Release 8.1	**AudioCodes Mediant 3000 E-SBC Release 6.4** **http://www.audiocodes.com/att**	**IP Flexible Reach**
AVAYA		
Aura Communications Manager 6.2 and Aura Session Manager 6.2 **https://devconnect.avaya.com/public/download/dyn/SM62CM62SBCEFR.pdf** **https://devconnect.avaya.com/public/download/dyn/SM62CM62SBCIPTF.pdf**	**Avaya SBCE Release 4.0.5**	**IP Flexible Reach (Enhanced)** **IP Toll Free / Transfer Connect**

IP-PBX Vendor / Version Documentation Link	SBC Vendor / Version Documentation Link, if not included in IP-PBX CCG	BVoIP Service Certified i.e. IP Flexible Reach, IP Toll Free
Aura Communication Manager 6.0.1 **http://support.avaya.com/css/P8/documents/100124841**	**ACME Net-Net 6.2, Model: 3800/4250/4500**	**IP Flexible Reach (Enhanced)**
Aura Communication Manager 6.0.1 with Session Manager 6.1 https://devconnect.avaya.com/public/download/dyn/SM60CM60SBCIPFR.pdf **https://devconnect.avaya.com/public/download/dyn/SM61CM601APIPTF.pdf**	**ACME Net-Net 6.x (x=1 or 2), Model: 3800/4250/4500**	**IP Flexible Reach (Enhanced)** **IP Toll Free**
Aura Communication Manager 6.0.1 with Session Manager 6.1 https://devconnect.avaya.com/public/download/dyn/CMSMAASBC60IPFR.pdf **https://devconnect.avaya.com/public/download/dyn/SM61CM601AAIPTF.pdf**	**Aura SBC 6.0, Model: OEM ACME 2600**	**IP Flexible Reach** **IP Toll Free**
Aura Communication Manager 6.0.1 with Session Manager 6.1 **https://devconnect.avaya.com/public/download/dyn/CM601SM61SipAtt.pdf**	**Sipera Systems E-SBC R4.0.4**	**IP Flexible Reach**
Aura Communication Manager 6.0.1 with Session Manager 6.1.1 **http://support.avaya.com/css/P8/documents/100109078**	**Sonus NBS5200 R2.00.x** **http://www.sonus.net/att**	**IP Flexible Reach** **IP Toll Free**
Aura Communication Manager 6.0.1 with Session Manager 6.1.1 **http://support.avaya.com/css/P8/documents/100109078**	**Sonus SBC5x00 (v3.0)** **http://www.sonus.net/att**	**IP Flexible Reach (Enhanced)**
Aura Communication Manager 6.2 **https://devconnect.avaya.com/public/download/dyn/SM62CM62SBCEFR.pdf**	**Avaya SBCE 4.0.5 Q02 (formerly Sipera)**	**IP Flexible Reach (Enhanced)**
Aura Communication Manager 6.0 **http://support.avaya.com/css/P8/documents/100124841**	**ACME Net-Net 6.2.0, Model: 3800/4250/4500**	**IP Flexible Reach**
Aura Communication Manager 6.0 with Session Manager 6.0 https://devconnect.avaya.com/public/download/dyn/CMSMAASBC60IPFR.pdf	**Aura SBC 6.0, Model: OEM ACME 2600**	**IP Flexible Reach**
Aura Communication Manager 6.0 with Session Manager 6.0 https://devconnect.avaya.com/public/download/dyn/SM60CM60SBCIPFR.pdf	**Acme Net-Net 6.1.0, Model: 3800/4250/4500**	**IP Flexible Reach**
Aura Communication Manager 6.0 with Session Manager 6.1	**Avaya SBCE 4.0.5 Q02 (formerly Sipera)**	**IP Toll Free / Transfer Connect**

IP-PBX Vendor / Version Documentation Link	SBC Vendor / Version Documentation Link, if not included in IP-PBX CCG	BVoIP Service Certified i.e. IP Flexible Reach, IP Toll Free
Aura Communication Manager 5.2.1 with Session Manager 6.2 **https://devconnect.avaya.com/public/download/dyn/CM521SM62APEFR.pdf**	**Acme Net-Net 6.2.0, Model: 3800/4250/4500**	**IP Flexible Reach (Enhanced)** **IP Toll Free / Transfer Connect**
Aura Communication Manager 5.2.1 with Session Manager 6.2 **https://devconnect.avaya.com/public/download/dyn/SM62CM521SBCEFR.pdf**	**Avaya SBCE 4.0.5**	**IP Flexible Reach (Enhanced)**
Aura Communication Manager 5.2.1 with Session Manager 6.1 https://devconnect.avaya.com/public/search/d_sprofile.jsp?s=5641&l=upload/2262-1.gif	**Acme Net-Net 6.2.0, Model: 3800/4250/4500**	**IP Flexible Reach**
Aura Communications Manager 5.2.1 with Session Manager 6.1 **https://devconnect.avaya.com/public/download/dyn/SM61CM521AAIPFR.pdf** **https://devconnect.avaya.com/public/download/dyn/SM61CM521AAIPTF.pdf**	**Aura SBC 6.0**	**IP Flexible Reach** **IP Toll Free**
Aura Communications Manager 5.2.1 with Session Manager 6.0 https://devconnect.avaya.com/public/search/d_sprofile.jsp?s=5641&l=upload/2262-1.gif	**Acme Net-Net 6.2.0, Model: 3800/4250/4500**	**IP Flexible Reach**
Aura Communications Manager 5.2.1 with Session Manager 6.1.1	**Sonus SBC 5x00 (v 03.x)** **http://www.sonus.net/att**	**IP Flexible Reach(Enhanced)** **IP Toll Free**
Aura Communication Manager 5.2.1 https://devconnect.avaya.com/public/download/dyn/ACM521AcmeIPFR.pdf	**Acme Net-Net 6.2.0, Model: 3800/4250/4500**	**IP Flexible Reach**
Aura Communication Manager 5.2.1 **https://devconnect.avaya.com/public/download/dyn/ACM521AASBCIPFR.pdf** **https://devconnect.avaya.com/public/download/dyn/ACM521AASBCIPTF.pdf**	**Aura SBC R6.0.2**	**IP Flexible Reach** **IP Toll Free**
Aura Communication Manager 5.2.1 with Session Manager 5.2 https://devconnect.avaya.com/public/search/d_sprofile.jsp?s=5326&l=upload/2262-1.gif	**Acme Net-Net OS-E 3.6.0 , Model: 2600**	**IP Flexible Reach**
Aura Communication Manager 5.2.1 with Session Manager 5.2 https://devconnect.avaya.com/public/flink.do?f=/public/download/dyn/ACM521SM52ATT_Flex.pdf	**Acme Net-Net , Model: 3800/4250/4500**	**IP Flexible Reach**
Aura Communication Manager 5.1.2 with SES 5.1.2	**N/A**	**IP Flexible Reach**

IP-PBX Vendor / Version Documentation Link	SBC Vendor / Version Documentation Link, if not included in IP-PBX CCG	BVoIP Service Certified i.e. IP Flexible Reach, IP Toll Free
https://devconnect.avaya.com/public/search/d_sprofile.jsp?s=4156&l=upload/2262-1.gif		
Aura Communication Manager 5.2 with SES 5.2 https://devconnect.avaya.com/public/search/d_sprofile.jsp?s=4156&l=upload/2262-1.gif	**N/A**	**IP Flexible Reach**
(Nortel) Business Communication Manager (BCM) 50 & 450 Release 6. http://support.avaya.com/css/P8/documents/100122475	**N/A**	**IP Flexible Reach**
(Nortel) CS 1000 Release 7.0 https://support.avaya.com/css/P8/documents/100129069	**Acme Net-Net 6.2.0, Model: 3800/4250/4500**	**IP Flexible Reach**
Nortel CS1000 Release 7.5 with Aura Session Manager 6.1 https://devconnect.avaya.com/public/download/dyn/CS1KSMASBCIPFR.pdf	**Aura SBC 6.0**	**IP Flexible Reach**
CS1000 Release 7.5 with Aura Session Manager 6.1 **http://downloads.avaya.com/css/P8/documents/100162360**	**Avaya Enterprise SBC (formerly Sipera) Release 4.0.5**	**IP Flexible Reach** **IP Toll Free**
Avaya IP Office 8.1 **https://devconnect.avaya.com/public/download/dyn/IPOR81BIBEIPFR.pdf**	**N/A**	**IP Flexible Reach (Enhanced)** **IP Toll Free**
Avaya IP Office 8.0 **https://devconnect.avaya.com/public/download/dyn/IPOR8IPFR.pdf**	**N/A**	**IP Flexible Reach** **IP Toll Free**
Avaya IP Office 7.0 http://support.avaya.com/css/P8/documents/100147339	**N/A**	**IP Flexible Reach**
Avaya IP Office 6.1 https://devconnect.avaya.com/public/download/dyn/IPO61IPFR.pdf		**IP Flexible Reach**
Aura Experience Portal 6.0, Aura Communication Manager 6.0.1, Aura Session Manager 6.1 **https://downloads.avaya.com/css/P8/documents/100159029**	**Acme Net-Net 6.2.0**	**IP Toll Free**
Aura Experience Portal 6.0, Aura Communication Manager 6.0.1 **https://devconnect.avaya.com/public/download/dyn/EP60CM601APTF.pdf**	**Acme Net-Net 6.2.0**	**IP Toll Free**
Voice Portal 5.1, Aura Communication Manager 5.2.1 **https://support.avaya.com/css/P8/documents/100160304**	**ACME Net-Net 6.2.0, Model: 3800/4250/4500**	**IP Toll Free**
Voice Portal 5.1, Aura Communication Manager 5.2.1, Aura	**ACME Net-Net 6.2.0, Model: 3800/4250/4500**	**IP Toll Free**

IP-PBX Vendor / Version Documentation Link	SBC Vendor / Version Documentation Link, if not included in IP-PBX CCG	BVoIP Service Certified i.e. IP Flexible Reach, IP Toll Free
Session Manager 6.1 https://support.avaya.com/css/P8/documents/100157001		
Avaya Notification Solution 1.2 https://devconnect.avaya.com/public/download/dyn/ANS20APIPFR.pdf	ACME Net-Net 6.2.0, Model: 3800/4250/4500	IP Flexible Reach
CISCO		
CUCM 9.0 http://www.cisco.com/en/US/solutions/ns340/ns414/ns728/networking_solutions_products_genericcontent0900aecd805bd13d.html	CUBE 9.0 Model: ISR G2 (Standard or High Availability)	IP Flexible Reach
CUCM 8.6 (now covers CUCM 8.x per AT&T/Cisco agreement) http://www.cisco.com/en/US/solutions/ns340/ns414/ns728/networking_solutions_products_genericcontent0900aecd805bd13d.html	CUBE 8.8 Model: ISR G2 (Standard or High Availability)	IP Flexible Reach
CUCM 8.5.1 or CUCM 8.6 http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns833/1001797.pdf	CUBE 8.6, Model: ISR G1/G2 (Standard or High Availability)	IP Flexible Reach (Enhanced) IPTF (8.6/8.6 only)
CUCM 8.5.1 (now covers CUCM 8.x per AT&T/Cisco agreement) http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns833/1033136.pdf	CUBE 8.5, Model ISR G2 (Standard or High Availability)	IP Flexible Reach IPXC added for INFOPACK only
CUCM 8.5.1 or CUCM 8.6 http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns833/1001797.pdf	Sonus Network Border Switch 5200 (NBS5200) Rel.02.00.X http://www.sonus.net/att	IP Flexible Reach
CUCM 8.5.1 or CUCM 8.6 http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns833/1001797.pdf	Sonus SBC 5x00 Rel.3.00.X http://www.sonus.net/att	IP Flexible Reach (with Enhanced)
CUCM 8.5.1 or CUCM 8.6 http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns833/1001797.pdf	Sonus Network Border Switch 9000 (NBS9000) Rel 8.4.2 http://www.sonus.net/att	IP Flexible Reach
CUCM 8.5.1 or CUCM 8.6 http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns833/1001797.pdf	ACME Net-Net 6.2, Model: 3800/4250/4500 https://support.acmepacket.com	IP Flexible Reach (including Enhanced)
CUCM 8.6 http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns833/1087031.pdf	CUBE Service Provider Edition (SP) 3.3 or 3.4.1s or 3.5.2s, Model: ASR 1000 Series	IP Flexible Reach

IP-PBX Vendor / Version Documentation Link	SBC Vendor / Version Documentation Link, if not included in IP-PBX CCG	BVoIP Service Certified i.e. IP Flexible Reach, IP Toll Free
CUCME 8.5 http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns833/1001136.pdf	N/A	IP Flexible Reach
CUCME 7.0 https://communities.cisco.com/docs/DOC-9523	N/A	IP Flexible Reach
CUCM 8.0 with CUSP 8.5.1 http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns784/951698_1.pdf	CUBE 1.4, Model: ISR G1/G2	IP Flexible Reach
CUCM 8.x http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns833/1024986.pdf	CUBE 1.4, Model: ASR 1000 Series	IP Flexible Reach
CUCM 7.1.5	Sonus SBC5x00 (v03.00.X) http://www.sonus.net/att	IP Flexible Reach (including Enhanced)
CUCM 8.0 http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns784/951698_1.pdf	CUBE 1.4 or CUBE 8.6, Model: ISR G1/G2 (8.6 may use High Availability)	IP Flexible Reach
CUCM 7.1 http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns784/841251_2.pdf	CUBE 1.4 or CUBE 8.6, Model: ISR G1/G2	IP Flexible Reach
CUCM 7.1	Acme , Model: 3800/4250/4500 https://support.acmepacket.com	IP Flexible Reach
CUCM 6.1 http://www.corp.att.com/bvoip/avpn/docs/CCG_Cisco_UCM_6.1_with_CUBE_1.4.doc	CUBE 1.4 or CUBE 8.6, Model: ISR G1/G2	IP Flexible Reach
CVP 8.0(1) http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns833/962469.pdf	CUBE 1.4, Model: ASR 1000 Series	IP Toll-Free (includes IPXC)
Cisco Business Edition 3000 Release 8.6.4 http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns833/1173808.pdf	CUBE Lite Release 8.8	IP Flexible Reach
INTERACTIVE INTELLIGENCE		
Interaction Center 4.0	Acme 3xxx, 4xxx, v6.x	IP Flexible Reach IP Toll Free (with IC R4.1 only) IPXC for INFOPACK use only
Interaction Center 3.0	ACME Session Director 5.0	IP Transfer Connect only with Infopack

IP-PBX Vendor / Version Documentation Link	SBC Vendor / Version Documentation Link, if not included in IP-PBX CCG	BVoIP Service Certified i.e. IP Flexible Reach, IP Toll Free
Interaction Center 4.1	**Interactive SIP Proxy Release 4.1**	**IP Toll Free**
Microsoft		
Lync Server 2013 (Wave 15) **http://lync.microsoft.com/En-us/Pages/default.aspx**	**AudioCodes Mediant E-SBC R6.6** **http://www.audiocodes.com/att**	**IP Flexible Reach (including Enhanced)**
Lync Server 2010 **http://lync.microsoft.com/En-us/Pages/default.aspx**	**CUBE 8.6, Model: ISR G1/G2** **http://www.corp.att.com/bvoip/ipflex/docs/MS_Lync2010_CUBE8_6_IPFlex_CCG.doc**	**IP Flexible Reach** **IP Toll Free**
Lync Server 2010 **http://lync.microsoft.com/En-us/Pages/default.aspx**	**CUBE 1.4** **Model: ASR 1000 Series** **http://www.corp.att.com/bvoip/avpn/implementation/MS_Lync2010_Combined_or_Cascaded_ASR_CUBE_IPFlex_CCG.PDF**	**IP Flexible Reach**
Lync Server 2010 **http://lync.microsoft.com/En-us/Pages/default.aspx**	**CUBE 8.8, Model: ISR G2** **http://www.corp.att.com/bvoip/tollfreeavpn/implementation/MS_Lync2010_CUBE8.8_IPTollFree_CCG.PDF**	**IP Flexible Reach** **IP Toll Free**
Lync Server 2010 **http://lync.microsoft.com/En-us/Pages/default.aspx**	**ACME Net-Net 6.x, Model: 3800/4250/4500** **https://support.acmepacket.com**	**IP Flexible Reach** **IP Toll Free**
Lync Server 2010 **http://lync.microsoft.com/En-us/Pages/default.aspx**	**Sonus SBC 5100, Release 03.00.x** **http://www.sonus.net/att**	**IP Toll Free**
Lync Server 2010 **http://lync.microsoft.com/En-us/Pages/default.aspx**	**AudioCodes Mediant E-SBC R6.6** **http://www.audiocodes.com/att**	**IP Flexible Reach (including Enhanced)**
Lync Server 2010 **http://lync.microsoft.com/En-us/Pages/default.aspx**	**AudioCodes 6.x, (x >= 2), Model: Mediant 800 &1000 (MSBG) and 3000 (ESBC)** **http://www.audiocodes.com/att**	**IP Flexible Reach** **IP Toll Free (v6.4 only)**
Lync Server 2010 **http://lync.microsoft.com/En-us/Pages/default.aspx**	**NET VX R 4.7.5** **Model: VX1200 VX1800** **http://www.sonus.net/att**	**IP Flexible Reach (Enhanced)**
Lync Server 2010 **http://lync.microsoft.com/En-us/Pages/default.aspx**	**NET UX Release 2.0.1** **http://www.sonus.net/att**	**IP Flexible Reach (Enhanced)**
Office Communication Server (OCS) 2007 R2 http://www.microsoft.com/communicationsserver/en/us/product-documentation.aspx	**CUBE 1.4, Model: ISR G1** **http://infosphere.labs.att.com/s**	**IP Flexible Reach**

IP-PBX Vendor / Version Documentation Link	SBC Vendor / Version Documentation Link, if not included in IP-PBX CCG	BVoIP Service Certified i.e. IP Flexible Reach, IP Toll Free
	ites/2/bvoipvit/Public/CCG%27s/Microsoft/Microsoft-OCS-CUBE-CCG-Flexreach.doc	
Office Communication Server (OCS) 2007 R2 http://www.microsoft.com/communicationsserver/en/us/product-documentation.aspx	**NET VX R 4.x (x is 7 or greater), Model: VX1200 VX1800** **http://www.sonus.net/att**	**IP Flexible Reach**
Office Communication Server (OCS) 2007 R2 http://www.microsoft.com/communicationsserver/en/us/product-documentation.aspx	**Acme Net-Net 6.0, Model: 3800/4250/4500** **https://support.acmepacket.com**	**IP Flexible Reach**
MITEL		
Mitel 3300 MCD v5.0	**N/A**	**IP Flexible Reach (Enhanced)**
SAGEMCOM		
Xmedius Fax **http://xmediusfax.sagemcom.com/downloads/at_t/ATT_vendor_configuration_guide_XMediusFAX_7_0.pdf**	**N/A**	**IP Flexible Reach**
ShoreTel		
ShoreTel version 11.1 / 11.2	**InGate v4.9.1 & Shoretel Mobile Router** **http://www.shoretel.com/partners/tech_developers/ecosystem/att.html**	**IP Flexible Reach**
ShoreTel ShoreGear Release 12.x	**Ingate SIParator Release 4.9.2** **http://www.shoretel.com/partners/tech_developers/ecosystem/att.html**	**IP Flexible Reach**
SIEMENS		
OpenScape Voice V5, V6 and V7 **https://partnerdialog.siemens-enterprise.com/go.php/2623/11362/2623**	**OpenScape SBC V1 (with Voice 5 and 6), V2 (with Voice 5 and 6) and V7 (with Voice 7)**	**IP Flexible Reach** **IP Toll Free**
TOSHIBA Leading Innovation		
IPedge R1.0 and 1.1 **http://fyi.tsd.toshiba.com/cgi-bin/tsd/fy/fy_home.jsp**	**N/A**	**IP Flexible Reach** **IP Toll Free**

IP-PBX Vendor / Version Documentation Link	SBC Vendor / Version Documentation Link, if not included in IP-PBX CCG	BVoIP Service Certified i.e. IP Flexible Reach, IP Toll Free
(requires username and password)		
		
Communigate SIP Proxy	Prophecy SBC (version 11)	IP Toll Free

2 Overview

AT&T IP Flexible Reach and/or AT&T IP Toll-Free Service, over AT&T VPN as the Underlying Transport Service are AT&T Business Voice over IP (BVoIP) Services.

This document should be used solely as a general configuration guideline. The Customer is solely responsible for determining the appropriate configuration for their specific environment; AT&T provides resources to assist with that configuration. Please contact your AT&T technical support representative for assistance if needed.

Configuration examples in this guide are provided for informational purposes only. The example configurations may be mapped to a variety of vendor implementations, check with your AT&T technical support representative if you have any questions.

Note: The configuration examples provided in this document are based upon Cisco IOS features, however, the features are NOT described in their entirety; and may vary across hardware platforms and versions of IOS. Please refer to the appropriate Cisco documentation relative to your IOS features.

3 Special Considerations

- The following TCP/IP ports must not be blocked by firewall or access lists:
  - AT&T IP Border Element signaling and media addresses.
  - SIP signaling traffic (UDP port 5060).
  - RTP/RTCP traffic (UDP port range 16384-32767).
- The configuration information in this CCG assumes a single primary CER. Any alternate routing configurations or remote branch connectivity to other sites, within the same or other AT&T VPN, requires proper configuration of the signaling and media paths. Routing configurations in all customer routers need to be set up to assure that the routing in the primary CER is not affected.
- cRTP (Compressed RTP) is not supported with Avaya Communications Manager version 5.1.2 or 5.2
- NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

4 Customer Edge Router Configurations for various IP-PBX Solutions

This section will assist in configuring the Customer Edge Router (CER) properly to insure interoperability with AT&T Certified IP-PBX solutions for use on AT&T IP Flexible Reach and/or AT&T IP Toll-Free, Service on AT&T VPN transport. Please review the section below that is applicable to your environment.

Each IP-PBX section covers:

- Basic Solution Network Topology
- Configuration for the Standard Solution
- Configuration for the Optional NAT Solution (if applicable)

In some cases there are more than one supported solutions covered within a single IP-PBX section (i.e. Avaya Aura Communication Manager with Avaya Aura Session Manager is covered under the same section as Avaya Communication Server 1000).

Important Note: The IP-PBX solutions below make reference to IP Border Element (IPBE) IP Addresses, Signaling IP Address and Media IP Address, which are provided to the Customer prior to the scheduled Pre-test date in a letter AT&T will send titled *Customer Router Configuration Shipping/Confirmation*. The Signaling IP Address and the Media IP Address can be Customer supplied or AT&T provided.

Throughout this document, AT&T provided IP Address is synonymous with IP Flexible Reach IP Address

4.1 Standard IP-PBX with a cascaded SBC

This IP-PBX solution must work in conjunction with a cascaded SBC (see the appropriate CCG for the IP-PBX and SBC configurations). The certifications covered by this chapter is:

- Aastra Clearspan Release 17sp4 and ACME Net-Net OS-E Release 3.6.0.M4P5
- Genesys Voice Platform Release 8.1 with AudioCodes Mediant 3000E-SBC R6.4

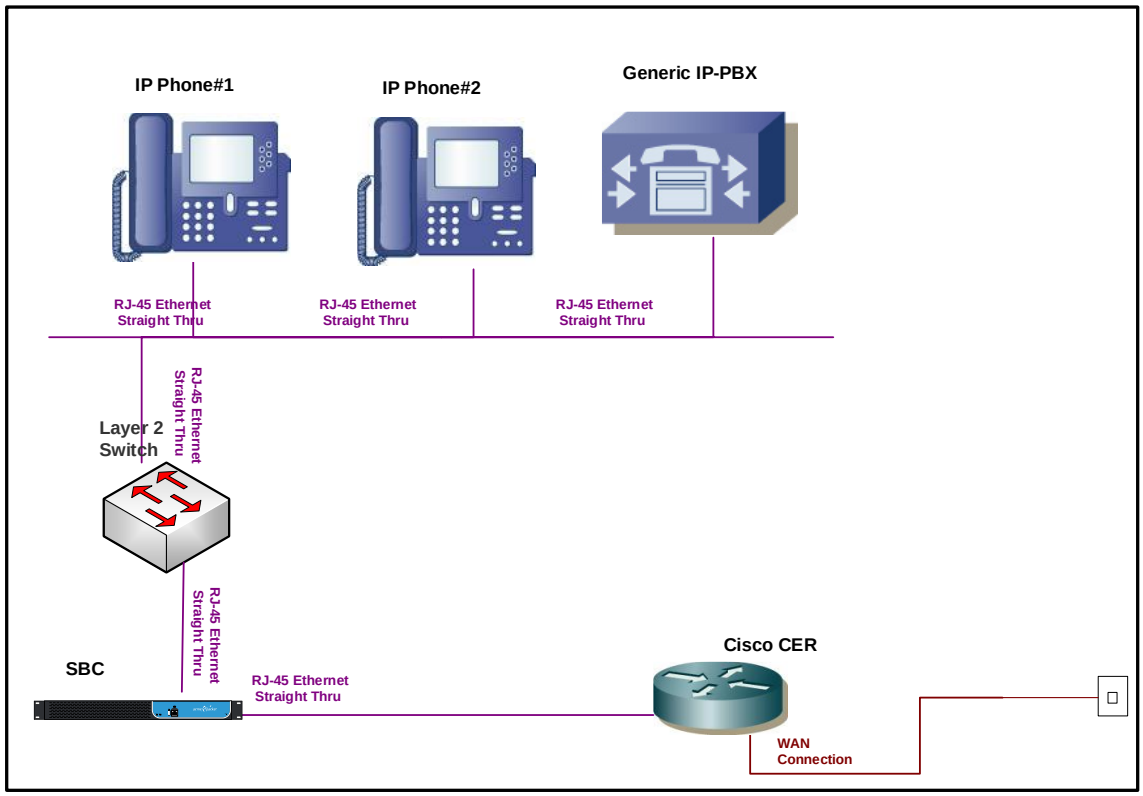
4.1.1 Topology

Following is a sample diagram of a network topology for a site with a standard IP-PBX and a cascaded SBC. In this design, the CER and the SBC are two separate routers. The AT&T VPN CSU-Probe is a AT&T managed device.

Note:

- The AT&T VPN CSU-Probe is optional.

AT&T BVoIP on AT&T VPN Site with IP-PBX with cascaded SBC
(CPE Site Design – Physical view)



4.1.2 Standard Solution

The SBC LAN interface (facing the CER) will be configured with the Signaling IP Address. Note: the SBC LAN interface provisioned for signaling will also be used for the media traffic. Therefore, all voice and signaling traffic destined for AT&T will be sourced from a single LAN interface on the SBC. The Media IP Address (assigned to you in the *Customer Router Configuration Shipping/Confirmation* letter*)* will be used to configure the CER LAN interface (facing the SBC) although it is not actually used for media traffic.

Step 1: Configure LAN interface facing the SBC

The CER interface which faces the SBC will be assigned the Media IP Address and the SBC interface which faces the CER will be assigned the Signaling IP Address. For example, if AT&T assigns a Media IP Address of 32.21.150.17, then that address will be configured on the CER LAN interface facing the SBC. If AT&T assigns a Signaling IP

Address of 32.21.150.18, then that address will be configured on the SBC's LAN interface facing the CER.

Note: The IP Address on the SBC interface is the assigned Signaling IP Address (although it is used for media as well) and must be the IP Address which has been provisioned as such in the AT&T Network. Note: AT&T prefers to assign the address space for the SIP Signaling/Media, but does offer to use existing customer addressing if required. Using a customer provided address space may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer's IP-PBX network is required for site-to-site calls.

```
ip route <customer voice network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

The Signaling IP Address and voice network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

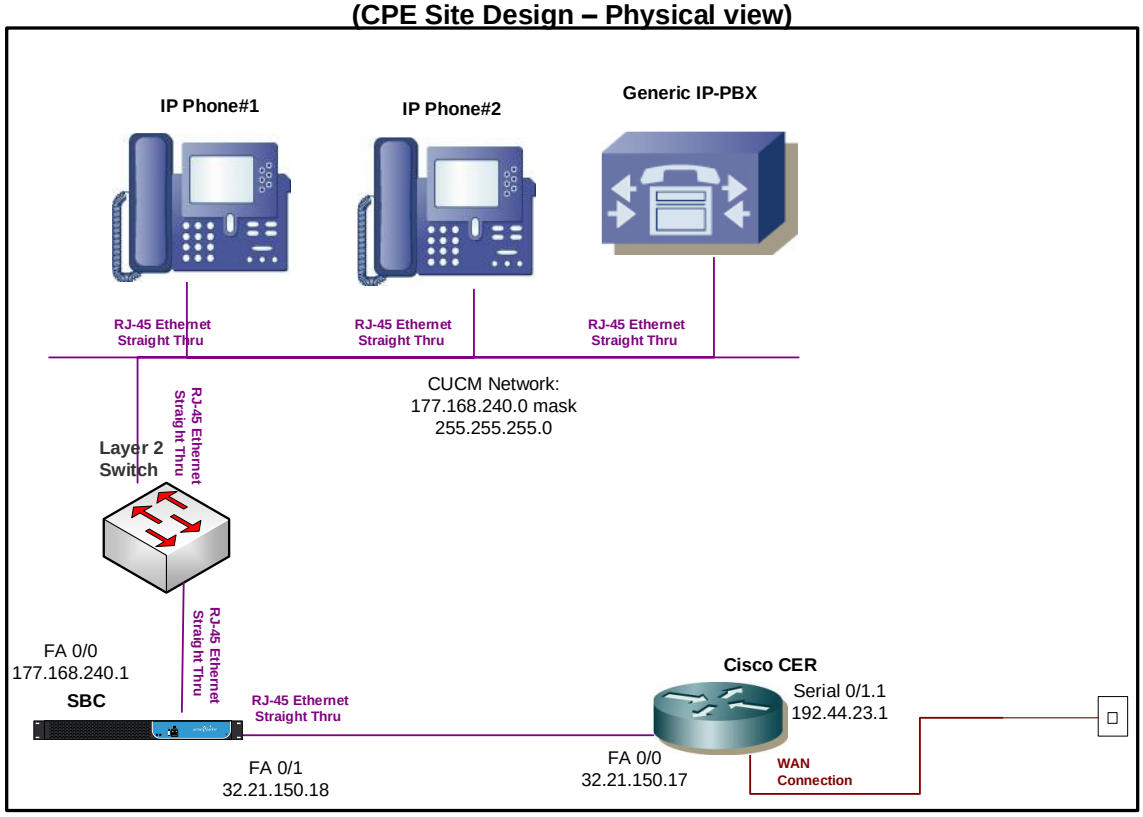
```
router bgp <your AS number>
no synchronization

bgp log-neighbor-changes
network <Signaling IP  Address network> mask 255.255.255.248
network <customer voice network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
neighbor <PER IP address>  allowas-in
no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where the IP-PBX resides. The 32.21.150.18 is the LAN address of the SBC facing the CER (this is the Signaling IP Address – which will also be used for media). The 32.21.150.17 is the LAN address of the CER (this is the Media IP Address – although it is not actually used for media).

AT&T BVoIP on AT&T VPN Site with standard IP-PBX with a cascaded SBC

(CPE Site Design – Physical view)



interface FastEthernet0/0

description LAN interface facing the SBC

ip address 32.21.150.17 255.255.255.248

duplex full

speed 100

ip route 177.168.240.0 255.255.255.0 32.21.150.18
router bgp 65000
no synchronization
bgp log-neighbor-changes
network 32.21.150.16 mask 255.255.255.248
network 177.168.240.0 mask 255.255.255.0
neighbor 192.44.23.2 remote-as 37383
neighbor 192.44.23.2 allowas-in
no auto-summary

4.1.3 Optional NAT Solution (non-standard configuration)

If the SBC uses a private Signaling/Media IP Address, then that address must be NAT'd to a public Signaling IP Address on the CER. However this is not recommended due to degraded CPU performance with NAT enabled.

The CER loopback interface used for NAT will be configured with the public Signaling IP Address. The CER loopback interface will also be used for the media traffic. Therefore all voice and signaling traffic will be sourced from a single loopback interface on the CER.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing the SBC

Configure a LAN interface on the CER for the same network as one of the SBC interfaces.

Step 2: Define Loopback Interface

Assign the public Signaling IP Address to a loopback interface on the CER (this same address will also be used for media).

```
interface Loopback <#>
  ip address  <Signaling IP Address> 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private signaling/media IP address to the public Signaling IP Address (the same address will also be used for media).

```
ip nat inside source static <private Signaling/Media IP Address> <public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside: statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the SBC.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing the SBC
 ip address <ip address> <mask>
 ip nat inside


interface WAN #  **Always use subinterface when available**
 description WAN interface facing AVPN
 ip address <ip address> <mask>
 ip nat outside
```

Step 5: Configure Static Routes

A static route is required for the customer voice network. The route will point at the SBC.

```
ip route <customer voice network> <appropriate subnet> <private Signaling/Media IP Address>
```

Step 6: Configure BGP

The public Signaling IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private signaling/media IP address). The CER will need to be configured with a network statement for the public Signaling IP Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address > mask 255.255.255.255
network <Customer voice network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The SBC LAN address (private signaling/media IP address) will be translated to a public Signaling IP Address (which is defined as a loopback interface on the CER). Continuing the example from section 4.4.2 (assume now that the SBC uses a private signaling/media IP address), the SBC private signaling/media address of 32.21.150.18 will be translated to a public Signaling IP Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255

interface FastEthernet0/0
```

```
 description LAN interface facing the SBC
 ip address 32.21.150.17 255.255.255.248
 ip nat inside
 duplex full
 speed 100


interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T
 bandwidth 1459
 ip address 192.33.20.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF


ip nat inside source static 32.21.150.18 135.16.180.66


router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

4.2 Cisco Unified Communications Manager Express (CME) with Cisco Unity Express (CUE)

The Cisco Unified Communications Manager Express solution will use a cascaded CME router (see appropriate CCG for CME configuration provided by Cisco). Voice and signaling traffic will be sourced from a LAN interface on the CME router.

CME does not support the periodic transmission of RTCP sender report to provide statistics of RTP flow. Therefore, **RTCP is not supported**.

4.2.1 Topology

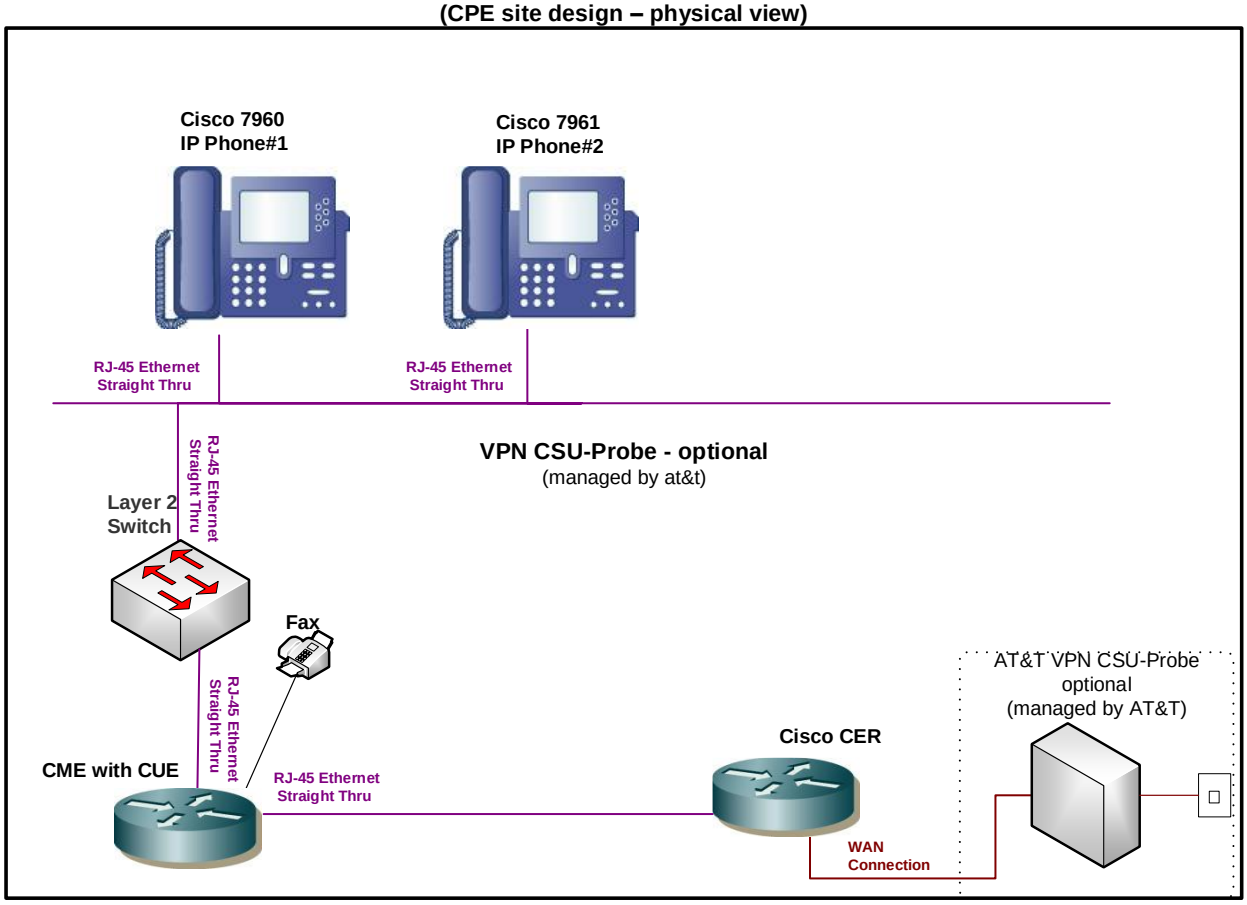
Following is a sample diagram of a network topology for a site with a Cisco Unified Communications Manager Express with Cisco Unity Express and Cisco Unified Border Element (CUBE) function for connectivity to AT&T SIP trunk service.

In this design, the CER and Cisco UCME are two separate routers. The AT&T VPN CSU-Probe is a AT&T managed device.

Note:

- The AT&T VPN CSU-Probe is optional.
- Cisco UCME does not support the periodic transmission of RTCP sender report to provide statistics of RTP flow. Therefore, **RTCP is not supported**.

AT&T BVoIP on AT&T VPN site
with VPN CSU-Probe, CME with CUE
(CPE site design – physical view)



4.2.2 Standard Solution

The CME LAN interface (facing the CER) will be configured with the Signaling IP Address. Note: The CME LAN interface provisioned for signaling will also be used for the media traffic. Therefore, all voice and signaling traffic destined for AT&T will be sourced from a single LAN interface on the CME router. The Media IP Address will be used to configure the CER LAN interface (facing the CME) although it is not actually used for media traffic.

Step 1: Configure CER LAN interface facing CME

The Signaling and Media IP Addresses will be used for the network between the CER and CME router. The CER interface, which faces the CME, will be assigned the Media IP Address and the CME router interface which faces the CER will be assigned the Signaling IP address. For example, if AT&T provides a media address 32.21.150.17, this address will be configured on the CER LAN interface facing the CME router. If AT&T provides a signaling address or 32.21.150.18, this address will be configured on the CME LAN interface facing the CER.

Note: The IP Address on the CME router interface is the Signaling IP Address (although it is used for media as well) and must be the IP Address which has been provisioned as such in the AT&T NETWORK. Note: AT&T prefers to provide the Signaling and Media IP Addresses, but does offer to use customer supplied IP addresses if required. Using a customer supplied address may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer's IP Phone network is required for site-to-site calls.

```
ip route <customer IP Phone network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

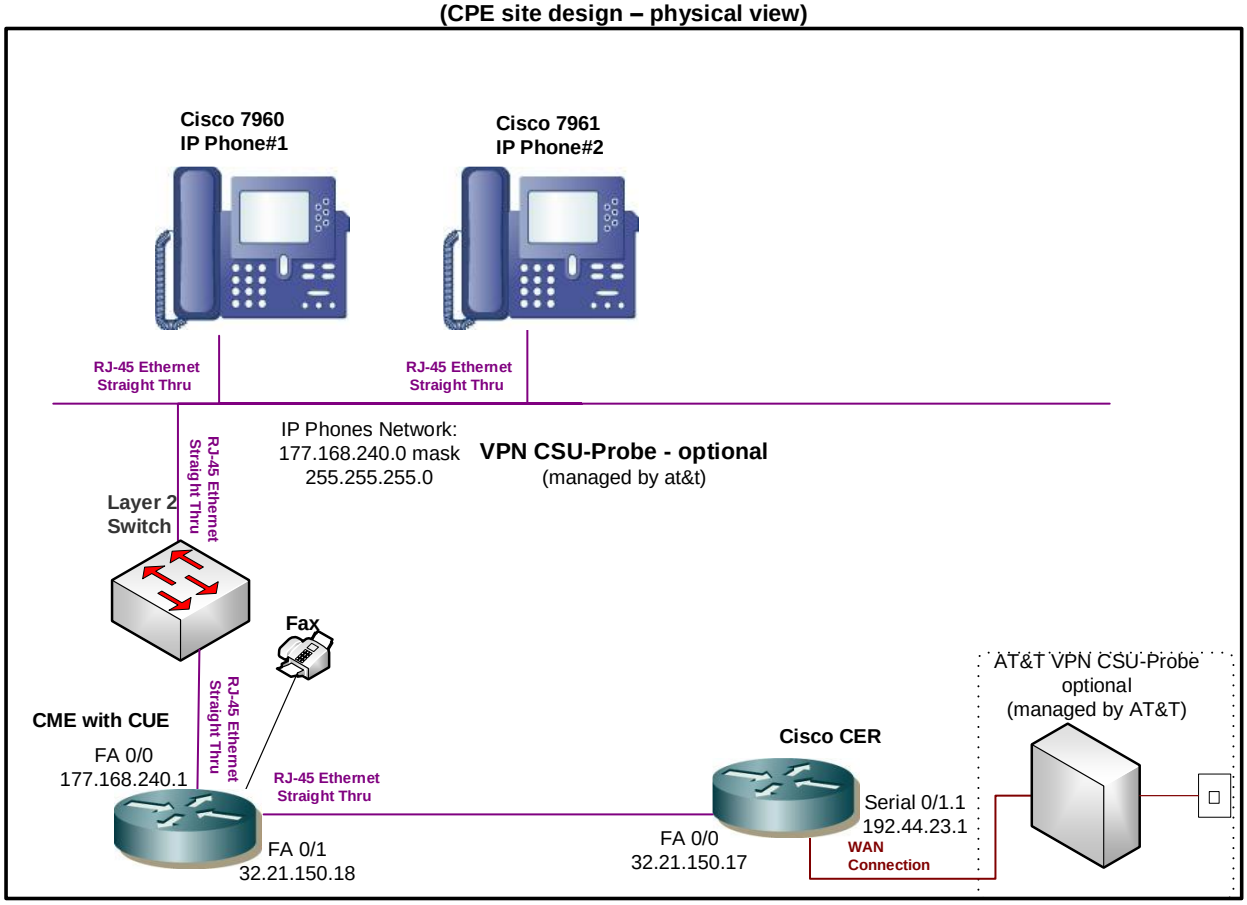
The Signaling IP Address network and customer IP phone network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

```
router bgp <your AS number>
no synchronization

bgp log-neighbor-changes
network <Signaling IP Address network> mask 255.255.255.248
network <customer IP Phone network > mask <use  appropriate mask>

neighbor <PER IP address>  remote-as  <remote AS>
neighbor <PER IP address>  allowas-in
no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where the customer IP phones reside. 32.21.150.18 is the LAN IP address of the CME router facing the CER (this is the Signaling IP Address – which will also be used for media). 32.21.150.17 is the LAN IP address of the CER (this is the Media IP Address – although it is not actually used for media).

AT&T BVoIP on AT&T VPN site
with VPN CSU-Probe, CME with CUE
(CPE site design – physical view)




```
interface FastEthernet0/0
 description LAN interface facing CME
 ip address 32.21.150.17 255.255.255.248
 duplex full
 speed 100
ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

```
router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 32.21.150.16  mask 255.255.255.248
network 177.168.240.0  mask 255.255.255.0
neighbor 192.44.23.2  remote-as  37383
 neighbor 192.44.23.2  allowas-in
 no auto-summary
```

4.2.3 Optional NAT Solution (non-standard configuration)

If the CME router uses a private IP address for signaling/media, that address may be NAT'd to a public Signaling IP Address on the CER. However, this is not recommended due to degraded CPU performance with NAT enabled.

The CER loopback interface used for NAT will be configured with the public Signaling IP Address. The CER loopback interface will also be used for the media traffic. Therefore all media and signaling traffic will be sourced from a single loopback interface on the CER.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing ACME

Configure a LAN interface of the CER in the same network as the CME interface facing the CER.

Step 2: Define Loopback Interface

Assign the public Signaling IP Address to a loopback interface on the CER (this address will also be used for media).

```
interface Loopback <#>
  ip address  <public Signaling IP Address > 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private CME Signaling/Media IP Address to the public IP Signaling Address (the same address will also be used for media).

```
ip nat inside source static <private CME Signaling/Media Address> < public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the CME router.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing CME
 ip address <ip address> <mask>
 ip nat inside

interface WAN #  **Always use subinterface when available**
 description WAN interface facing ATT
 ip address <ip address> <mask>
 ip nat outside
```

Step 5: Configure Static Routes

A static route is required for the customer IP Phones network. The route will point at the CME router.

```
ip route <customer IP Phones network> <appropriate subnet> <private CME Signaling/Media Address>
```

Step 6: Configure BGP

The public Signaling/Media IP Address must be distributed to the network via BGP (you will **not** need to redistribute the private CME Signaling/Media IP Address). The CER will need to be configured with a network statement for the public Signaling/Media Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling/Media IP Address > mask 255.255.255.255
network <customer IP Phones network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The CME LAN address used for Signaling/Media (private addressing) will be translated to a public Signaling IP

Address (which is defined as a loopback interface on the CER). Continuing the example from section 4.1.2 (assume now that the CME uses a private address), the CME private Signaling/Media IP address of 32.21.150.18 will be translated to a public Signaling Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255

interface FastEthernet0/0
 description LAN interface facing CME
 ip address 32.21.150.17 255.255.255.248
 ip nat inside
 duplex full
 speed 100


interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing ATT
 bandwidth 1459
 ip address 192.33.20.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF


ip nat inside source static 32.21.150.18 135.16.180.66


router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

4.3 Cisco Unified Communications Manager (CUCM) with Cisco Unified Border Element (CUBE) [Includes Cisco Customer Voice Portal (CVP) in an IPTF solution!]

The Cisco Unified Communications Manager solution must work in conjunction with a cascaded CUBE router (see the appropriate CCG for CUCM and CUBE configurations). AT&T recommends using the CUBE loopback interface for the public Signaling Address (media will also be sourced from the same loopback interface). Therefore, all voice and signaling traffic will be sourced from the loopback interface of the CUBE.

Although AT&T recommends using the loopback interface for the public Signaling Address to make configuration and troubleshooting easier, the customer may prefer to use "default binding" on the CUBE. Default binding uses the physical interfaces for media and signaling instead of a loopback interface. This alternate solution is shown below as a non-standard solution, section 4.2.3.

Note:

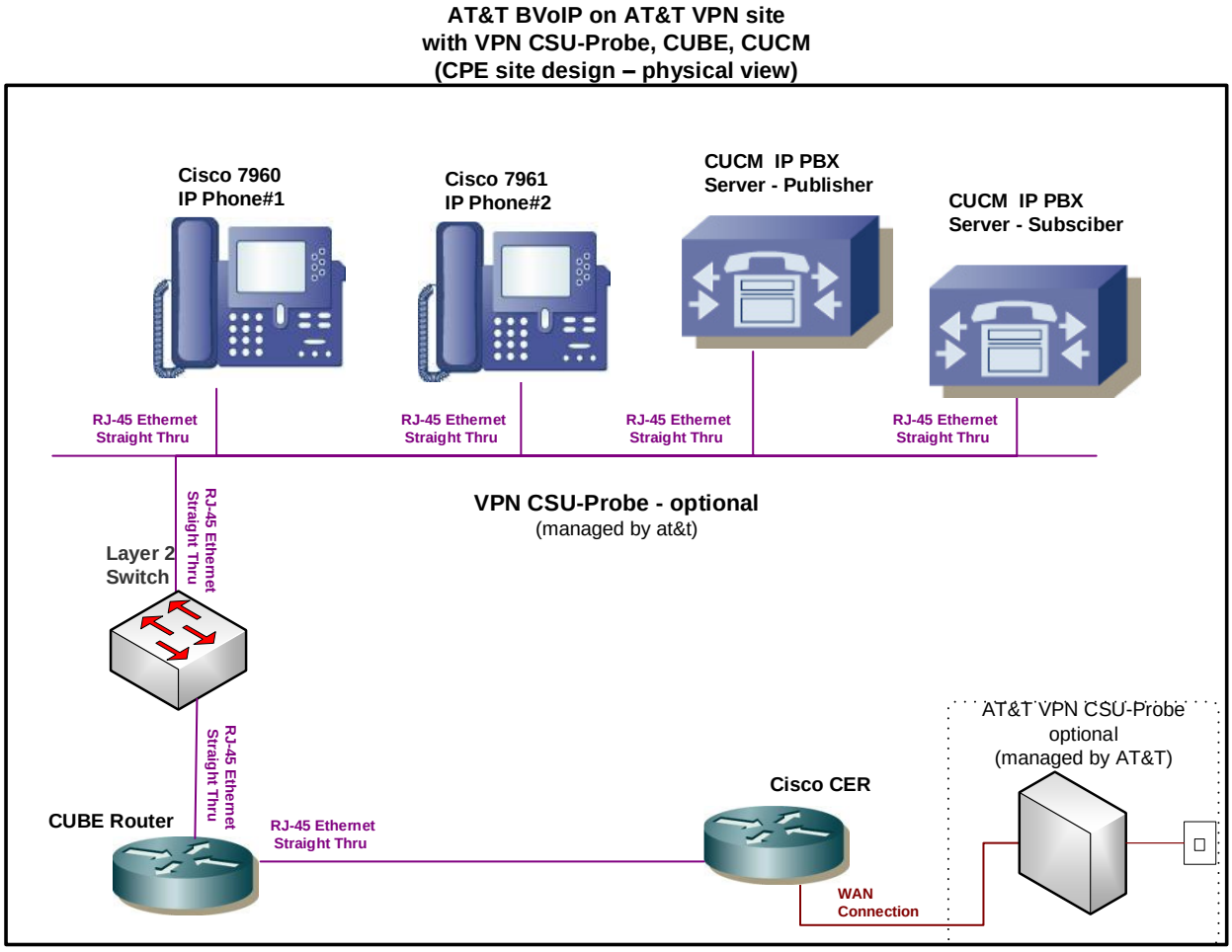
- Remote sites with a CUBE are supported (aka: Direct Media). The remote site IP phones register across the WAN to a central site where the CUCM resides. The configurations in this section can be used for both central and remote sites.
- This section also covers the CER configuration required to support Cisco CVP, certified only for IP Toll-Free Service. References to CVP are not made throughout this section to avoid confusion being that CVP is transparent, sitting behind the CUBE SBC.

4.3.1 Topology

Following is a sample diagram of a network topology for a site with a Cisco Unified Communications Manager (CUCM) and Cisco Unified Border Element (CUBE). In this design, the CER and CUBE are two separate routers (referred to as a "cascaded CUBE"). The AT&T VPN CSU-Probe is a AT&T managed device.

Note:

- The AT&T VPN CSU-Probe is optional.



4.3.2 Standard Solution (binding signaling/media to a loopback interface)

Step 1: Configure LAN interface facing CUBE

Configure a LAN interface of the CER on the same network as one of the CUBE interfaces.

Step 2: Configure static routes

The CER must be configured with static routes for the CUBE loopback address (Signaling IP Address) and the LAN where the CUCM and/or IP phones reside.

Route to the CUBE loopback interface:
Syntax: ip route <Signaling IP Address> 255.255.255.255 <CER facing LAN port of CUBE router>
Route to the CUCM and/or IP phones LAN:

Syntax: ip route <CUCM LAN network> <appropriate subnet> <CER facing LAN port of CUBE router>

Step 3: Configure network statements in BGP

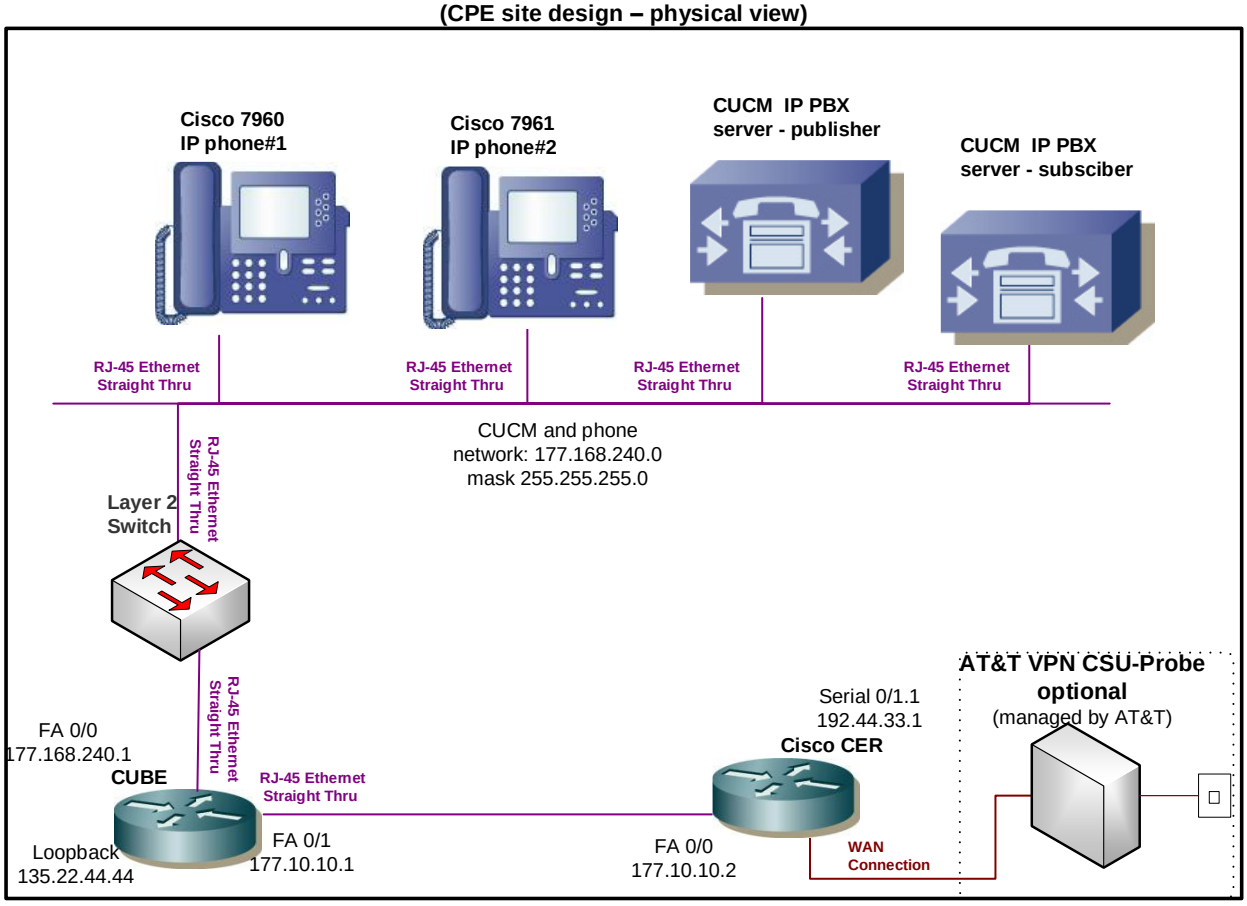
Next, the CUBE loopback address (Signaling IP Address) and LAN network address of the CUCM and/or IP phones must be advertised via BGP.

```
router bgp <your AS number>
no synchronization
bgp log-neighbor-changes
network <Signaling IP Address> mask 255.255.255.255
network <LAN address of CUCM and/or IP phones> mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
neighbor <PER IP address>  allowas-in
no auto-summary
```

Example:

In this example, 177.168.240.0 is the LAN where the Unified Communications Manager and IP phones reside. The 177.10.10.1 address is the LAN interface address of the CUBE (facing the CER). The CUBE sits in between the CER and the Unified Communications Manager/IP phones LAN. The 135.22.44.44 is the loopback address of the CUBE (Signaling IP Address).

**AT&T BVoIP on AT&T VPN Site
with AT&T VPN CSU-Probe, CUBE, CUCM
(CPE site design – physical view)**



Router configuration output:

```
interface FastEthernet0/0
 description LAN interface facing CUBE
 ip address 177.10.10.2  255.255.255.0
duplex full
speed 100
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
network 135.22.44.44 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.44.33.2  remote-as  37383
```

```
neighbor 192.44.33.2  allowas-in
no auto-summary
ip route 135.22.44.44 255.255.255.255 177.10.10.1
ip route 177.168.240.0 255.255.255.0 177.10.10.1
```

4.3.3 Non-Standard Solution (binding signaling/media to physical interfaces)

The CUBE LAN interface (facing the CER) will be configured with the Signaling IP Address. Note: the CUBE LAN interface provisioned for signaling will also be used for the media traffic. Therefore, all voice and signaling traffic destined for AT&T will be sourced from a single LAN interface on the CUBE. The Media IP Address (assigned to you in the *Customer Router Configuration Shipping/Confirmation* letter*)* will be used to configure the CER LAN interface (facing the CUBE) although it is not actually used for media traffic.

Step 1: Configure LAN interface facing CUBE

The CER interface which faces the CUBE will be assigned the Media IP Address and the CUBE router interface which faces the CER will be assigned the Signaling IP Address. For example, if AT&T assigns a Media IP Address of 32.21.150.17, then that address will be configured on the CER LAN interface facing the CUBE. If AT&T assigns a Signaling IP Address of 32.21.150.18, then that address will be configured on the CUBE's LAN interface facing the CER.

Note: The IP Address on the CUBE interface is the assigned Signaling IP Address (although it is used for media as well) and must be the IP Address which has been provisioned as such in the AT&T NETWORK. Note: AT&T prefers to assign the address space for the SIP Signaling/Media, but does offer to use existing customer addressing if required. Using a customer provided address space may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer's CUCM network is required for site-to-site calls.

```
ip route <CUCM network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

The Signaling IP Address network and customer IP phone network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a single network statement. This statement is derived by subtracting one from the

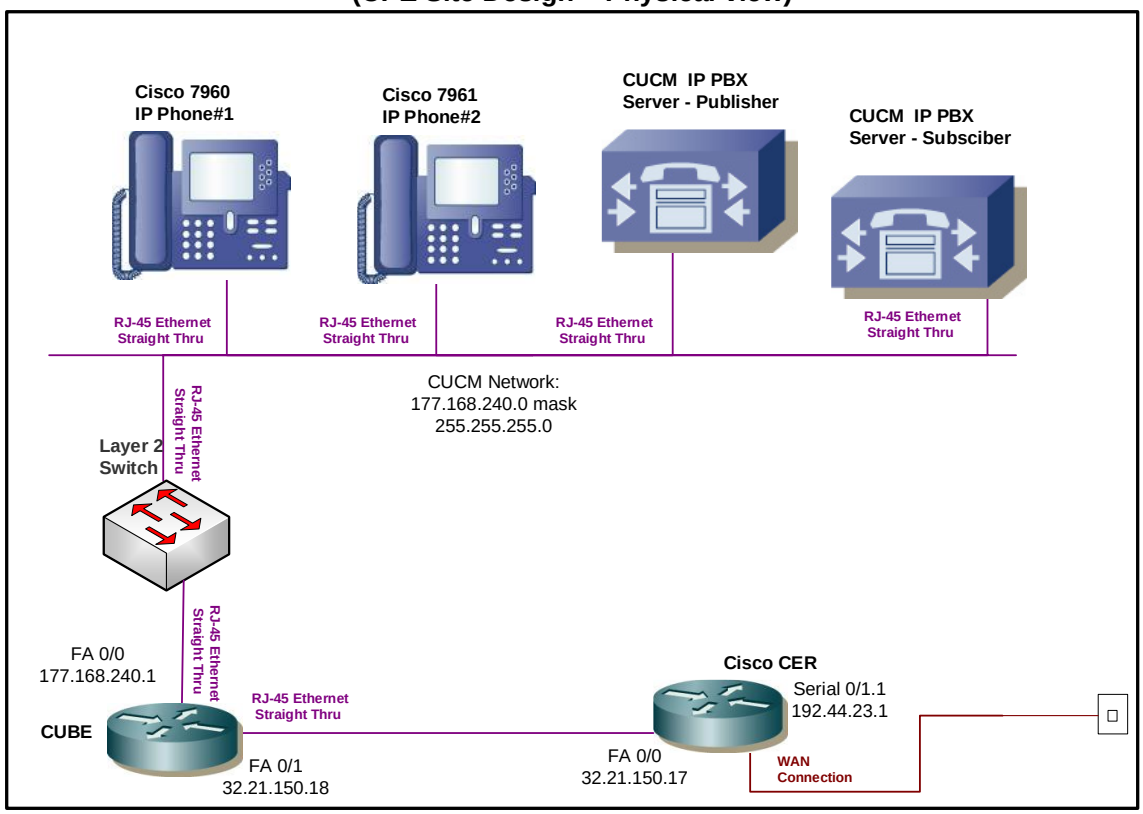
assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

```
router bgp <your AS number>
no synchronization

bgp log-neighbor-changes
network <Signaling IP Address network> mask 255.255.255.248
network <customer ip phone network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
neighbor <PER IP address>  allowas-in
no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where the CUCM resides. The 32.21.150.18 is the LAN address of the CUBE facing the CER (this is the Signaling IP Address – which will also be used for media). The 32.21.150.17 is the LAN address of the CER (this is the Media IP Address – although it is not actually used for media).

AT&T BVoIP on AT&T VPN Site with CUCM and CUBE SBC
(CPE Site Design – Physical view)



```
interface FastEthernet0/0
 description LAN interface facing CUBE
 ip address 32.21.150.17 255.255.255.248
 duplex full
 speed 100


ip route 177.168.240.0 255.255.255.0 32.21.150.18

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 32.21.150.16  mask 255.255.255.248
network 177.168.240.0  mask 255.255.255.0
neighbor 192.44.23.2  remote-as  37383
 neighbor 192.44.23.2  allowas-in
 no auto-summary
```

4.3.4 Optional NAT Solution - binding signaling/media to a loopback interface (non-standard configuration)

The CUBE loopback interface (used for the signaling and media) may be NAT'd at the CER. However, this is not recommended due to degraded CPU performance resulting from enabling NAT.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing CUBE

Configure a LAN interface on the CER in the same network as one of the CUBE interfaces.

Step 2: Define loopback interface

Assign the public Signaling IP Address to a loopback interface on the CER.

```
interface Loopback <#>
  ip address  <public Signaling IP Address> 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the CUBE loopback (private Signaling IP Address) to the CER loopback (public Signaling IP Address).

```
ip nat inside source static <CUBE loopback- private Signaling IP Address> <CER loopback – public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside" statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the CUBE router.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing CUBE
 ip address <ip address> <mask>
 ip nat inside

interface WAN #  **Always use subinterface when available**
 description WAN interface facing ATT
  ip address <ip address> <mask>
 ip nat outside
```

Step 5: Configure static routes

A static route is required for the CUCM and IP Phone network. The route will point to the CUBE router.

```
Route to the CUCM and IP phones LAN:
Syntax: ip route <CUCM LAN network> <appropriate subnet> <LAN port of CUBE router>
```

Step 6: Configure BGP

The NAT'd public Signaling IP Address must be distributed to the network via BGP (the CUBE loopback interface will **not** need to be redistributed). The CER will need to be configured with a network statement for the NAT'd address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <CER loopback interface IP - public Signaling IP Address> mask 255.255.255.255
network <LAN address of CUCM and/or IP phones> mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The CUBE loopback will be translated to a public Signaling IP Address (which is defined as a loopback interface on the CER). Continuing the example from section 4.2.2, (assume now that the CUBE

uses a private Signaling IP Address), the CUBE loopback address of 135.22.44.44 will be translated to a public Signaling IP Address of 135.16.180.66.

```
interface Loopback6
ip address 135.16.180.66 255.255.255.255


interface FastEthernet0/0
 description LAN interface facing CUBE
 ip address 177.10.10.2  255.255.255.0
 ip nat inside
 duplex full
 speed 100


interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T  VPN
 bandwidth 1459
 ip address 192.44.33.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF
ip nat inside source static 135.22.44.44 135.16.180.66


router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.44.33.2 remote-as  32733
 neighbor 192.44.33.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 177.10.10.1
```

4.3.5 Optional NAT Solution - binding signaling/media to physical interfaces (non-standard configuration)

If the CUBE uses a private Signaling/Media IP Address, then that address must be NAT'd to a public Signaling IP Address on the CER. However this is not recommended due to degraded CPU performance with NAT enabled.

The CER loopback interface used for NAT will be configured with the public Signaling IP Address. The CER loopback interface will also be used for the media traffic. Therefore all voice and signaling traffic will be sourced from a single loopback interface on the CER.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing CUBE

Configure a LAN interface on the CER for the same network as one of the CUBE interfaces.

Step 2: Define Loopback Interface

Assign the public Signaling IP Address to a loopback interface on the CER (this same address will also be used for media).

```
interface Loopback <#>
  ip address  <Signaling IP Address> 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private signaling/media IP address to the public Signaling IP Address (the same address will also be used for media).

```
ip nat inside source static <private Signaling/Media IP Address> <public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside: statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the CUBE.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing CUBE
 ip address <ip address> <mask>
 ip nat inside


interface WAN #  **Always use subinterface when available**
```

```
description WAN interface facing AVPN
ip address <ip address> <mask>
ip nat outside
```

Step 5: Configure Static Routes

A static route is required for the CUCM network. The route will point at the CUBE router.

```
ip route <CUCM network> <appropriate subnet> <private Signaling/Media IP Address>
```

Step 6: Configure BGP

The public Signaling IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private signaling/media IP address). The CER will need to be configured with a network statement for the public Signaling IP Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address > mask 255.255.255.255
network <CUCM network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The CUBE LAN address (private signaling/media IP address) will be translated to a public Signaling IP Address (which is defined as a loopback interface on the CER). Continuing the example from section 4.4.2 (assume now that the CUBE uses a private signaling/media IP address), the CUBE private signaling/media address of 32.21.150.18 will be translated to a public Signaling IP Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255

interface FastEthernet0/0
 description LAN interface facing CUBE
 ip address 32.21.150.17 255.255.255.248
 ip nat inside
 duplex full
 speed 100
```

```
interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T
 bandwidth 1459
 ip address 192.33.20.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF

ip nat inside source static 32.21.150.18 135.16.180.66

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

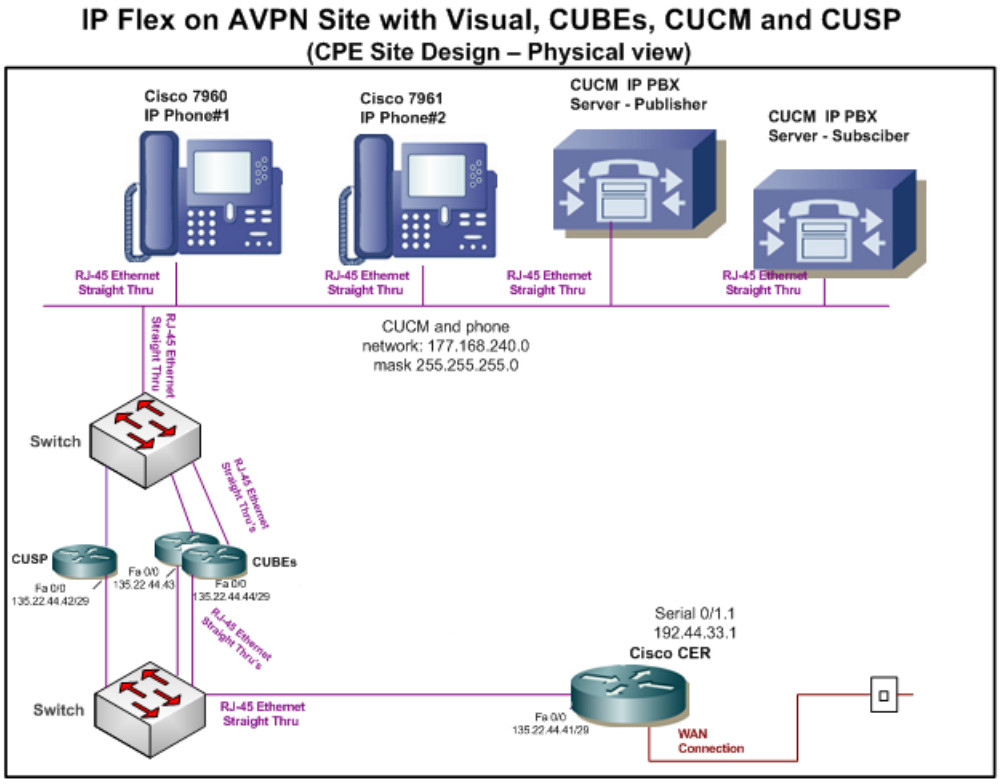
4.4 Cisco Unified Communications Manager (CUCM) with Cisco Unified Border Element (CUBE) and Cisco Unified SIP Proxy (CUSP)

Cisco Unified SIP Proxy (CUSP) can be implemented with or without NAT, without NAT being the preferred configuration with AT&T VPN Transport. Using either method, CUSP will be assigned a SIP Signaling IP Address and each CUBE will be assigned a Media IP Address. If CUSP is not used, then the standard solution of supporting one CUBE applies (see earlier section in this document for the non-CUSP solution).

Note: AT&T provides addressing with a 29 bit subnet mask (/29) allowing for six host addresses. With the non-NAT solution, the first host address (Media IP Address) is assigned to the LAN interface of the CER, the second host address (Signaling IP Address) is assigned to the CUSP module, and the remaining four host addresses are available for CUBEs. There is a limitation of **four** CUBEs for the non-NAT solution. For the NAT solution, the LAN interface of the CER will not use one of the AT&T provided addresses. Therefore, the second host address (Signaling IP Address) will be assigned to the CUSP and the remaining host addresses, including the first, can be assigned to the CUBEs. There is a limitation of **five** CUBEs for the NAT solution. The CUBE number limitations go on the assumption that AT&T Multiple IP's (MIPS) feature is **not** provisioned.

4.4.1 Topology

Following is a sample diagram of a network topology for a site with a Cisco Unified Communications Manager (CUCM) and Cisco Unified Border Element(s) (CUBE) with Cisco Unified SIP Proxy (CUSP). CUSP is optional and offered for media server scalability. In this design, the CER and CUBE(s) are separate routers (cascaded). The AT&T VPN CSU-Probe is a AT&T Managed Device. All other equipment is managed by the customer.



4.4.2 Standard Solution

Follow these steps to configure the CER without NAT (standard solution):

Step 1: Configure LAN interface facing CUBEs and CUSP

Configure a LAN interface on the CER for the same network as for the CER facing interfaces of the CUSP (Signaling IP Address) and CUBEs (Media IP Addresses). **The first AT&T host address (Media IP Address) provided will be assigned to this interface.**

Step 2: Configure Static routes

The CER must be configured with static routes for the customer LAN where the CUCM and IP phones reside.

Route to the CUCM and/or IP Phones LAN:

Syntax: ip route <CUCM LAN network> <appropriate subnet> <Signaling IP Address>*

**assuming the CUSP is the default gateway to the CUCM environment*

Step 3: Configure network statements in BGP

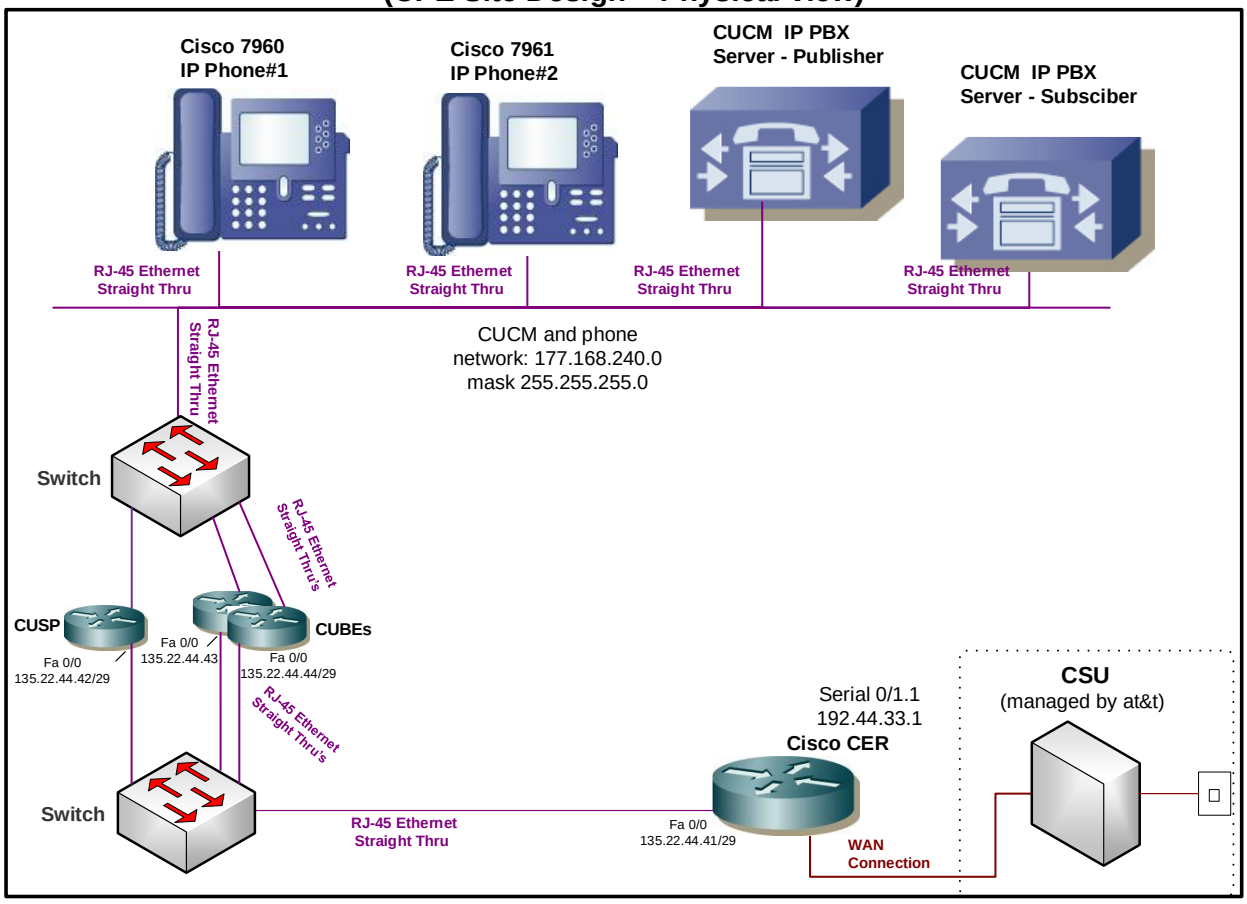
Next, the **Signaling IP Address**, **Media IP Addresses** and the **LAN network address of the CUCM and IP phones** must be advertised via BGP. Add additional network statements if more CUBEs are required. Please note that the Signaling and Media IP Addresses are advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

```
router bgp <your AS number>
no synchronization

bgp log-neighbor-changes
network <CUSP Signaling IP Address and CUBE Media IP Address network> mask 255.255.255.248
network <LAN address of CUCM and/or IP Phones> mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>

neighbor <PER IP address>  allowas-in
no auto-summary
```

Example:

In this example, 177.168.240.0 is the LAN where the Unified Communications Manager and IP phones reside. The 135.22.44.42 address (Signaling IP Address) is the LAN interface address of the CUSP (facing the CER). The 135.22.44.43 and 135.22.44.44 addresses (Media IP Addresses) are the LAN interface addresses of the CUBEs (facing the CER). The CUSP and CUBEs sit between the CER and the Unified Communications Manager/IP Phones LAN.

AT&T BVoIP on AVPN Site with Visual, CUBEs, CUCM
(CPE Site Design – Physical view)



interface FastEthernet0/0

description LAN interface facing CUBE and CUSP [assigned the first Media Address]

ip address 135.22.44.41 255.255.255.248

duplex full

speed 100

router bgp 65000
no synchronization
bgp log-neighbor-changes
network 135.22.44.40 mask 255.255.255.248
network 177.168.240.0 mask 255.255.255.0
neighbor 192.44.33.2 remote-as 37383
neighbor 192.44.33.2 allowas-in
no auto-summary
ip route 177.168.240.0 255.255.255.0 135.22.44.42

4.4.3 Optional NAT Solution (non-standard configuration)

The CUSP Signaling IP Address and CUBE Media IP Addresses may be NAT'd at the CER. However, this is not recommended due to degraded CPU performance observed with NAT enabled.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing CUBEs and CUSP

Configure a LAN interface on the CER for the same network as for the CER facing interfaces on the CUSP and CUBEs. Since we are using NAT in this configuration, the addressing used here will be from private addressing network space.

Step 2: Define Loopback Interface

Assign the public Signaling and Media IP Addresses to loopback interfaces on the CER. Additional CUBEs will require additional loopback interfaces.

```
interface Loopback <#1>
  ip address  <public Signaling IP Address – for CUSP> 255.255.255.255
interface Loopback <#2>
  ip address  <public Media IP Address - for CUBE#1 > 255.255.255.255
interface Loopback <#3>
  ip address  <public Media IP Address - for CUBE#2 > 255.255.255.255
```

Step 3: Create NAT statement

Define the static NAT statement to translate the private Signaling and Media IP Addresses (CUSP and CUBE interfaces, respectfully) to the public Signaling and Media IP Addresses (CER loopback interfaces). Additional statements are required for additional CUBEs.

```
ip nat inside source static <private Signaling IP Address> <public Signaling IP Address>
ip nat inside source static <private Media IP Address #1> <public Media IP Address #1>
ip nat inside source static <private Media IP Address #2> <public Media IP Address #2>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside" statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the CUSP and CUBEs.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing CUSP and CUBEs
 ip address <ip address> <mask>
 ip nat inside

interface WAN #  **Always use sub-interface when available**
 description WAN interface facing AVPN
  ip address <ip address> <mask>
 ip nat outside
```

Step 5: Configure Static routes

The CER must be configured with static routes for the customer LAN where the CUCM and/or IP phones reside.

Route to the CUCM and/or IP Phones LAN:

Syntax: ip route <CUCM LAN network> <appropriate subnet> <<private Signaling IP Address>*

**assuming the CUSP is the default gateway to the CUCM environment*

Step 6: Configure BGP

The NAT'd public Signaling and Media IP Addresses must be distributed to the network via BGP (you will **not** need to redistribute the private Signaling and Media IP Addresses). The CER will need to be configured with a network statement for the NAT'd IP addresses.

```
router bgp <your AS number>
no synchronization
bgp log-neighbor-changes
 network <public Signaling IP Address > mask 255.255.255.255
 network <public Media IP Address #1> mask 255.255.255.255
 network <public Media IP Address #2> mask 255.255.255.255
 network <LAN address of CUCM and/or IP Phones> mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

The following is an example of a NAT configuration on the CER. The CUSP and CUBE addresses will be translated to public Signaling and Media IP Addresses (defined as loopback interfaces on the CER). Continuing the example from section 4.3.2, (assume now that the CUBE and CUSP use private addressing), the CUSP and CUBE private addresses 135.22.44.42 - 44 will be translated to public addresses in the range of 135.16.180.66 - 68, respectively.

```
interface Loopback6
description public Signaling IP Address
 ip address 135.16.180.66 255.255.255.255
interface Loopback7
description public Media Address -  CUBE#1
 ip address 135.16.180.67 255.255.255.255
interface Loopback8
description public Media Address – CUBE#2
 ip address 135.16.180.68 255.255.255.255

interface FastEthernet0/0
 description LAN interface facing CUSP and CUBEs
 ip address 135.22.44.41 255.255.255.0
 ip nat inside
 duplex full
 speed 100

interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AVPN
 bandwidth 1459
 ip address 192.44.33.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF

ip nat inside source static 135.22.44.42 135.16.180.66
ip nat inside source static 135.22.44.43 135.16.180.67
```

```
ip nat inside source static 135.22.44.44 135.16.180.68

router bgp 65000

no synchronization
bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 135.16.180.67 mask 255.255.255.255
network 135.16.180.68 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.44.33.2 remote-as  32733
 neighbor 192.44.33.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 135.22.44.42
```

4.5 Cisco Unified Communications Manager (CUCM) with Cisco Unified Border Element (CUBE) in a High Availability Configuration

This Cisco Unified Communications Manager solution must work in conjunction with two cascaded CUBE routers in a High Availability (HA) configuration using Hot Standby Routing Protocol (HSRP). Please see the appropriate CCG for CUCM and CUBE HA configurations.

Although AT&T recommends using the loopback interface for the signaling address for most CUBE topologies, **this solution requires using "default binding" on the CUBE for Signaling and Media**. Default binding uses the physical interfaces for media and signaling instead of a loopback interface.

Note:

- Remote sites with a CUBE are supported (aka: Direct Media). The remote site IP phones register across the WAN to a central site where the CUCM resides. The configurations in this section can be used for both central and remote sites.

4.5.1 Standard Solution (default binding of Signaling IP Address)

The CUBEs will be configured for High Availability using HSRP with a Virtual IP Address for the Signaling IP Address. Note: the CUBE provisioned signaling IP Address will also be used for the media traffic. Therefore, all voice and signaling traffic destined for AT&T will be sourced from a single virtual interface on the CUBE. The Media IP Address (assigned to you in the *Customer Router Configuration Shipping/Confirmation* letter*)* will be used to configure the CER LAN interface (facing the CUBE) although it is not actually used for media traffic. The third and fourth assigned IP Addresses (see example below for clarification) will be used for the Physical CUBE interfaces.

Step 1: Configure LAN interface facing CUBEs

The CER interface which faces the CUBEs will be assigned the Media IP Address, the CUBE router HSRP Virtual IP Address will be assigned the Signaling IP Address, and the next two IP Addresses will be assigned to the physical interface of the CUBEs. For example, if AT&T assigns a Media IP Address of 32.21.150.17, then that address will be configured on the CER LAN interface facing the CUBE. If AT&T assigns a Signaling IP Address of 32.21.150.18, then that address will be configured as the CUBE Virtual IP Address, and the next two IP addresses, 32.21.150.19-20 will be assigned to the LAN interface of each CUBE facing the CER.

Note: The Virtual IP Address on the CUBE is the assigned Signaling IP Address (although it is used for media as well) and must be the IP Address which has been provisioned as such in the AT&T NETWORK. Note: AT&T prefers to assign the address space for the SIP Signaling/Media, but does offer to use existing customer addressing if required. Using a customer provided address space may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer's CUCM network is required for site-to-site calls.

```
ip route <CUCM network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

The Signaling IP Address network and customer IP phone network must be advertised via BGP network statements. Please note that the Signaling IP Address and CUBE interfaces IP Addresses are advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

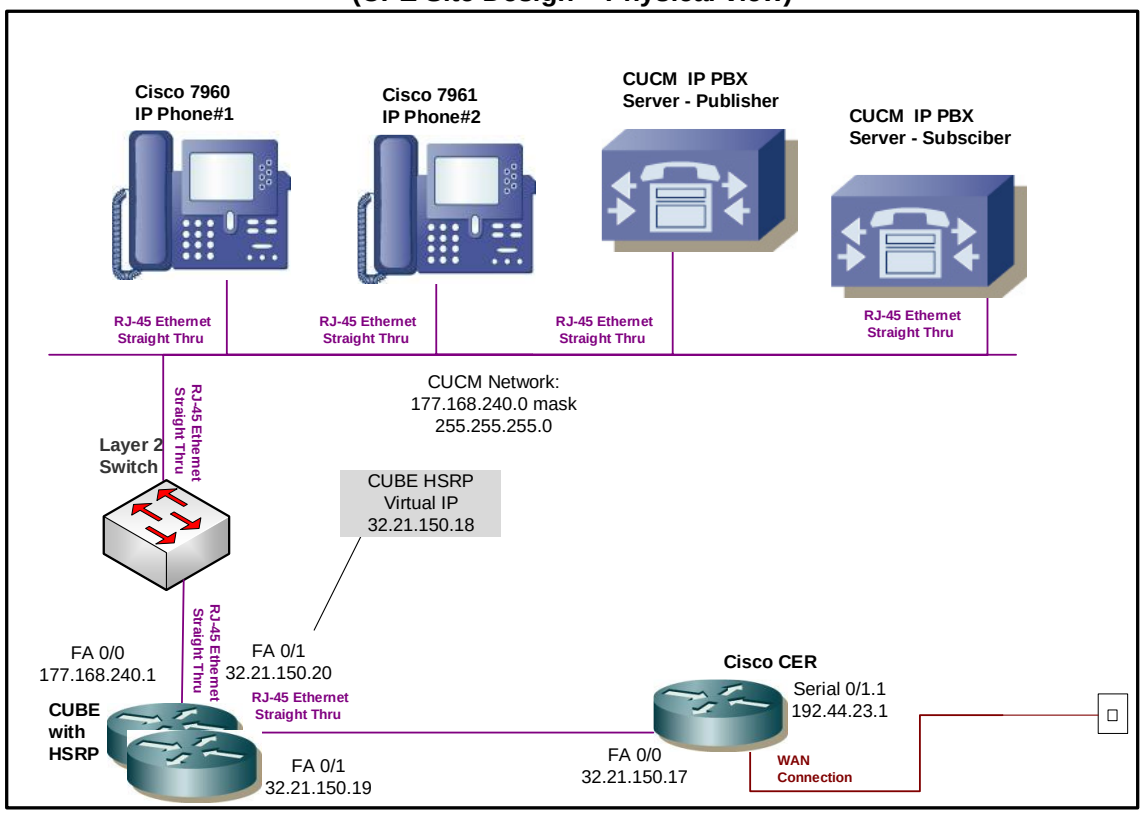
```
router bgp <your AS number>
no synchronization

bgp log-neighbor-changes
network <Signaling IP Address network> mask 255.255.255.248
network <customer ip phone network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
neighbor <PER IP address>  allowas-in
no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where the CUCM resides. 32.21.150.18 is the Virtual IP Address of the CUBE (this is the Signaling IP Address –

which will also be used for media). 32.21.150.17 is the LAN address of the CER (this is the Media IP Address – although it is not actually used for media). 32.21.150.19 and 32.21.150.20 are assigned to the CUBE physical interfaces facing the CER.

AT&T BVoIP on AT&T VPN Site with CUCM and CUBE SBC
(CPE Site Design – Physical view)



interface FastEthernet0/0

description LAN interface facing CUBE

ip address 32.21.150.17 255.255.255.248

duplex full

speed 100

ip route 177.168.240.0 255.255.255.0 32.21.150.18

router bgp 65000
no synchronization
bgp log-neighbor-changes
network 32.21.150.16 mask 255.255.255.248
network 177.168.240.0 mask 255.255.255.0

```
neighbor 192.44.23.2  remote-as  37383
 neighbor 192.44.23.2  allowas-in
 no auto-summary
```

4.5.2 Optional NAT Solution – default binding of Signaling IP Address

If the CUBE uses a private Signaling/Media IP Address, then that address must be NAT'd to a public Signaling IP Address on the CER. However this is not recommended due to degraded CPU performance with NAT enabled.

The CER loopback interface used for NAT will be configured with the public Signaling IP Address. The CER loopback interface will also be used for the media traffic. Therefore all voice and signaling traffic will be sourced from a single loopback interface on the CER.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing CUBE

Configure a LAN interface on the CER for the same network as one of the CUBE interfaces.

Step 2: Define Loopback Interface

Assign the public Signaling IP Address to a loopback interface on the CER (this same address will also be used for media).

```
interface Loopback <#>
  ip address  <Signaling IP Address> 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private signaling/media IP address to the public Signaling IP Address (the same address will also be used for media).

```
ip nat inside source static <private Signaling/Media IP Address> <public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside: statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the CUBE.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing CUBE
 ip address <ip address> <mask>
 ip nat inside

interface WAN #  **Always use subinterface when available**
 description WAN interface facing AVPN
 ip address <ip address> <mask>
 ip nat outside
```

Step 5: Configure Static Routes

A static route is required for the CUCM network. The route will point at the CUBE router.

```
ip route <CUCM network> <appropriate subnet> <private Signaling/Media IP Address>
```

Step 6: Configure BGP

The public Signaling IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private signaling/media IP address). The CER will need to be configured with a network statement for the public Signaling IP Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address > mask 255.255.255.255
network <CUCM network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The CUBE Virtual IP Address (private signaling/media IP address) will be translated to a public Signaling IP Address (which is defined as a loopback interface on the CER). Continuing the example from section 4.4.2 (assume now that the CUBE uses a private signaling/media

IP address), the CUBE private signaling/media address of 32.21.150.18 will be translated to a public Signaling IP Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255
interface FastEthernet0/0
 description LAN interface facing CUBE
 ip address 32.21.150.17 255.255.255.248
 ip nat inside
 duplex full
 speed 100

interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T
 bandwidth 1459
 ip address 192.33.20.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF

ip nat inside source static 32.21.150.18 135.16.180.66

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

4.6 Cisco Unified Communications Manager (CUCM) with ACME Packet Session Border Controller (SBC) or Sonus NBS5200/9000

The CUCM solution can work in conjunction with an SBC (ACME or Sonus NBS5200/9000) (see appropriate CCG for CUCM and ACME SBC or Sonus NBS5200/9000 configurations).

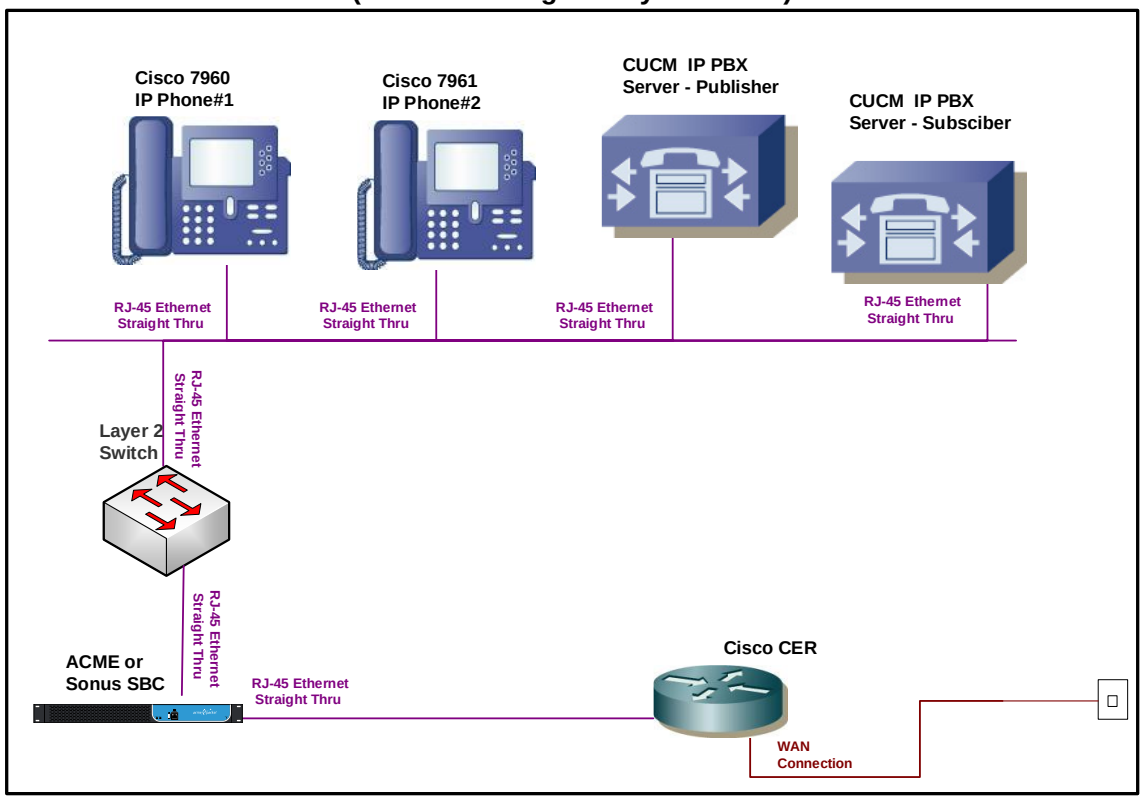
4.6.1 Topology

Following is a sample diagram of a network topology for a site with a Cisco Unified Communications Manager (CUCM) and an ACME Packet Net-Net SBC or Sonus NBS5200/9000. In this design, the CER and the SBC are two separate routers. The AT&T VPN CSU-Probe is a AT&T managed device.

Note:

- The AT&T VPN CSU-Probe is optional.

AT&T BVoIP on AT&T VPN Site with CUCM and ACME/Sonus SBC (CPE Site Design – Physical view)



4.6.2 Standard Solution

The ACME LAN interface (facing the CER) will be configured with the Signaling IP Address. Note: the SBC LAN interface provisioned for signaling will also be used for the media traffic. Therefore, all voice and signaling traffic destined for AT&T will be sourced from a single LAN interface on the SBC. The Media IP Address (assigned to you in the *Customer Router Configuration Shipping/Confirmation* letter*)* will be used to configure the CER LAN interface (facing the SBC) although it is not actually used for media traffic.

Step 1: Configure LAN interface facing the SBC

The CER interface which faces the SBC will be assigned the Media IP Address and the SBC interface which faces the CER will be assigned the Signaling IP Address. For example, if AT&T assigns a Media IP Address of 32.21.150.17, then that address will be configured on the CER LAN interface facing the SBC. If AT&T assigns a Signaling IP Address of 32.21.150.18, then that address will be configured on the SBC's LAN interface facing the CER.

Note: The IP Address on the SBC interface is the assigned Signaling IP Address (although it is used for media as well) and must be the IP Address which has been provisioned as such in the AT&T Network. Note: AT&T prefers to assign the address space for the SIP Signaling/Media, but does offer to use existing customer addressing if required. Using a customer provided address space may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer's CUCM network is required for site-to-site calls.

```
ip route <CUCM network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

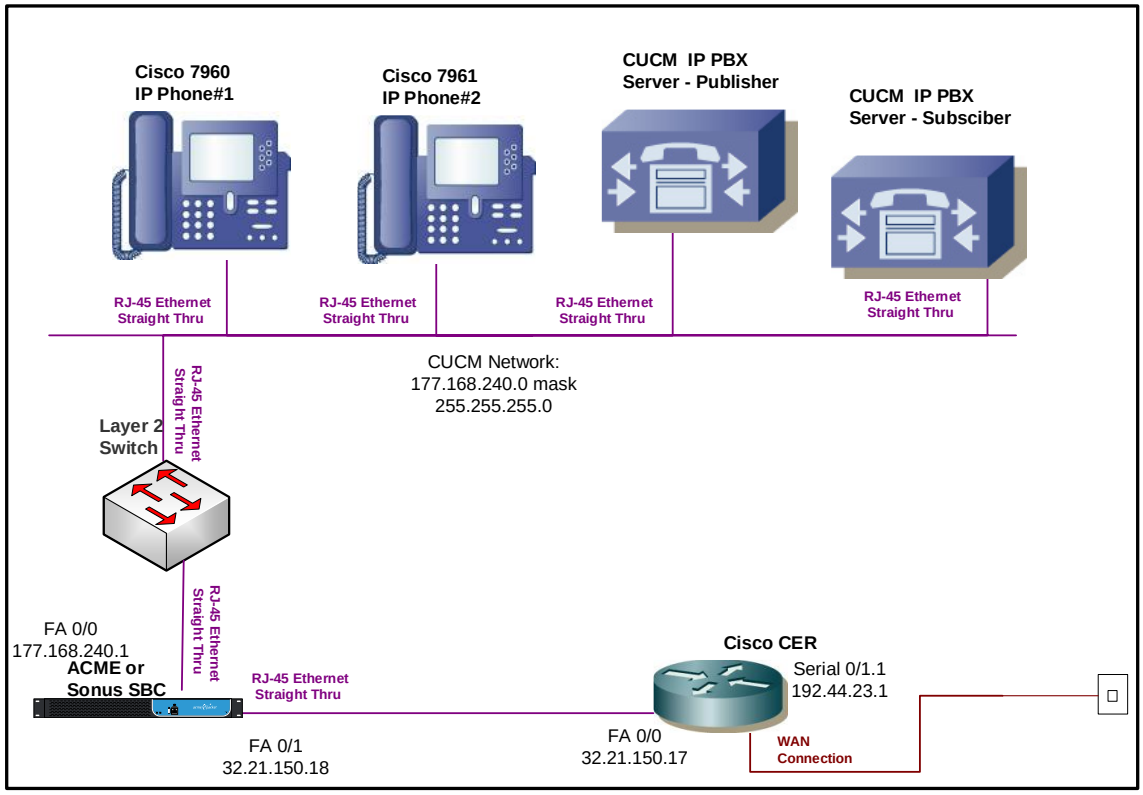
The Signaling IP Address and CUCM network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

```
router bgp <your AS number>
no synchronization

bgp log-neighbor-changes
network <Signaling IP  Address network> mask 255.255.255.248
network <CUCM network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
neighbor <PER IP address>  allowas-in
no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where the CUCM resides. The 32.21.150.18 is the LAN address of the SBC facing the CER (this is the Signaling IP Address – which will also be used for media). The 32.21.150.17 is the LAN address of the CER (this is the Media IP Address – although it is not actually used for media).

AT&T BVoIP on AT&T VPN Site with CUCM and ACME or Sonus SBC
(CPE Site Design – Physical view)



interface FastEthernet0/0

description LAN interface facing the SBC

ip address 32.21.150.17 255.255.255.248

duplex full

speed 100

ip route 177.168.240.0 255.255.255.0 32.21.150.18
router bgp 65000
no synchronization
bgp log-neighbor-changes
network 32.21.150.16 mask 255.255.255.248

```
network 177.168.240.0  mask 255.255.255.0
neighbor 192.44.23.2  remote-as  37383
 neighbor 192.44.23.2  allowas-in
 no auto-summary
```

4.6.3 Optional NAT Solution (non-standard configuration)

If the SBC uses a private Signaling/Media IP Address, then that address must be NAT'd to a public Signaling IP Address on the CER. However this is not recommended due to degraded CPU performance with NAT enabled.

The CER loopback interface used for NAT will be configured with the public Signaling IP Address. The CER loopback interface will also be used for the media traffic. Therefore all voice and signaling traffic will be sourced from a single loopback interface on the CER.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing the SBC

Configure a LAN interface on the CER for the same network as one of the SBC interfaces.

Step 2: Define Loopback Interface

Assign the public Signaling IP Address to a loopback interface on the CER (this same address will also be used for media).

```
interface Loopback <#>
  ip address  <Signaling IP Address> 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private signaling/media IP address to the public Signaling IP Address (the same address will also be used for media).

```
ip nat inside source static <private Signaling/Media IP Address> <public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside: statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the SBC.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing the SBC
 ip address <ip address> <mask>
 ip nat inside

interface WAN #  **Always use subinterface when available**
 description WAN interface facing AVPN
 ip address <ip address> <mask>
 ip nat outside
```

Step 5: Configure Static Routes

A static route is required for the CUCM network. The route will point at the SBC.

```
ip route <CUCM network> <appropriate subnet> <private Signaling/Media IP Address>
```

Step 6: Configure BGP

The public Signaling IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private signaling/media IP address). The CER will need to be configured with a network statement for the public Signaling IP Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address > mask 255.255.255.255
network <CUCM network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The SBC LAN address (private signaling/media IP address) will be translated to a public Signaling IP Address (which is defined as a loopback interface on the CER). Continuing the example from section 4.4.2 (assume now that the SBC uses a private signaling/media IP address), the SBC private signaling/media address of 32.21.150.18 will be translated to a public Signaling IP Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255

interface FastEthernet0/0
 description LAN interface facing the SBC
 ip address 32.21.150.17 255.255.255.248
 ip nat inside
 duplex full
 speed 100


interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T
 bandwidth 1459
 ip address 192.33.20.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF


ip nat inside source static 32.21.150.18 135.16.180.66


router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

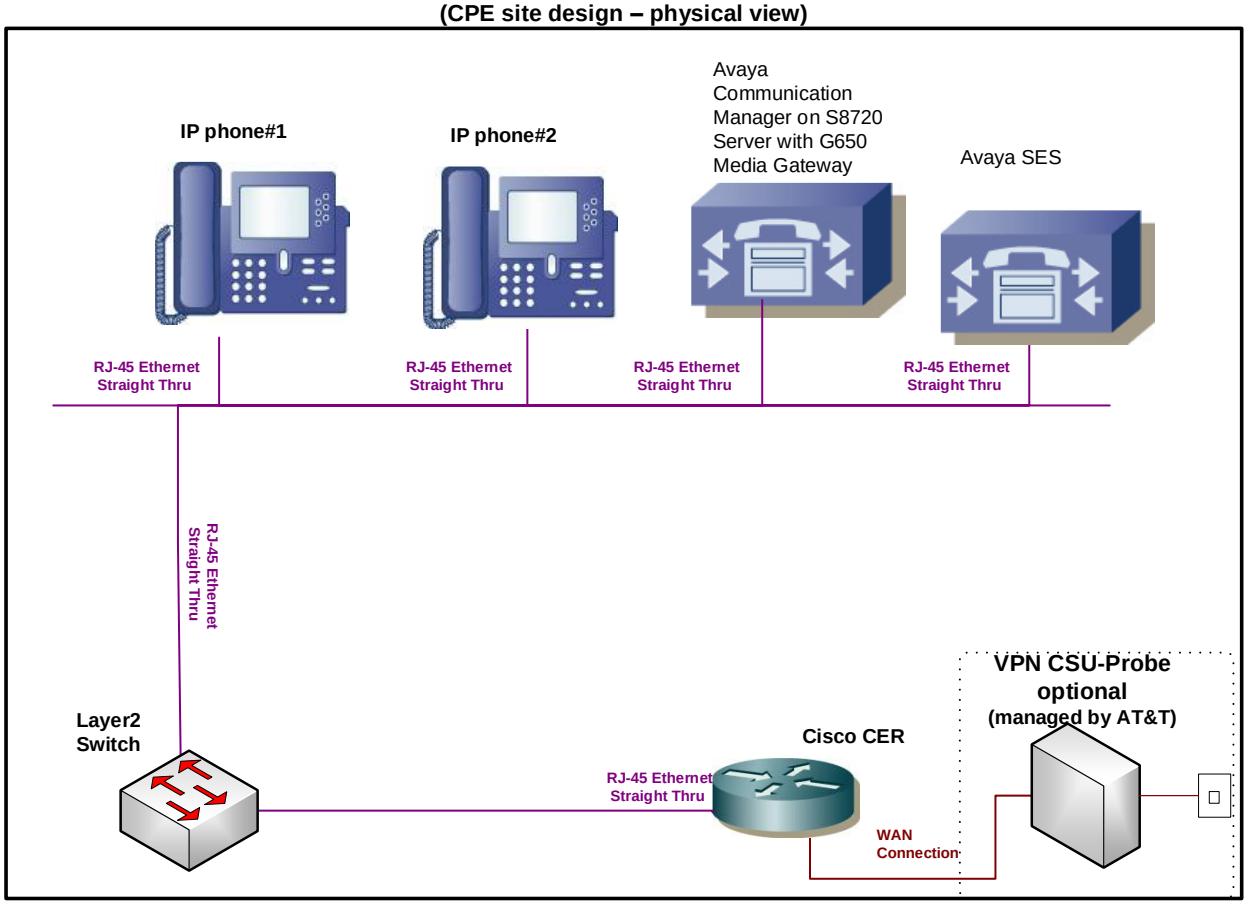
4.7 Avaya Communications Manager (without an SBC)

The Avaya Communications solution with SES is a supported solution (see appropriate CCG for IP PBX configurations).

4.7.1 Topology

Following is a sample diagram of a network topology for a site with an Avaya Communications Manager without an SBC. The AT&T VPN CSU-Probe is a AT&T managed device. Note: The AT&T managed VPN CSU-Probe is optional.

**AT&T BVoIP on AT&T VPN site
with AT&T VPN CSU-Probe, Avaya CM and SES
(CPE site design – physical view)**



4.7.2 Standard NAT/PAT Solution (required)

- The SES-Edge (when the SES-Edge and SES-Home are separate) or SES (when SES-Edge and SES-Home are combined) must be NAT'd to a registered AT&T IP address (which will be a loopback interface on the CER).
- The IP endpoints (IP Telephones, Soft phones, etc.) and the MedPro (media resources) must be PAT'd to a different registered loopback interface address (for media traffic).
- The C-LAN(s) and SES-Home(s) (when the SES-Edge and SES-Home(s) are separate) must retain its private addresses and must not be PAT'd.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing Avaya Communications Manager

Configure a LAN interface of the CER for the same network space as the Avaya Communications Manager and phones network.

Step 2: Define loopback interfaces

Define one loopback address as the Signaling IP Address. This will be the address that the SES is NAT'd to.

Define a second loopback address as the Media IP Address. This will be the address that the IP phones and MedPro are PAT'd to.

```
interface Loopback <X>
  ip address  <Signaling IP Address – NAT for SES > 255.255.255.255

interface Loopback <Y>
  ip address  <Media IP Address – PAT for IP phones/MedPro > 255.255.255.255
```

Step 3: Create NAT/PAT statements

PAT is required for the IP phones and the MedPro. An access list is used to define the addresses eligible for PAT. The SES and CLAN address will not be PAT'd (therefore, the access list will deny these addresses). The SES will have a separate NAT statement.

PAT statement:

```
ip nat inside source list <ACL # > interface LoopbackY overload

access-list <ACL#> deny   <Private IP address of SES>
access-list <ACL#> deny   <Private IP address of CLAN>
access-list <ACL#> permit <Private LAN address space of phones and Medpro> <appropriate mask>
```

NAT statement:

```
ip nat inside source static <Private IP address of SES>  <public Signaling IP Address>
```

Step 4: Configure BGP

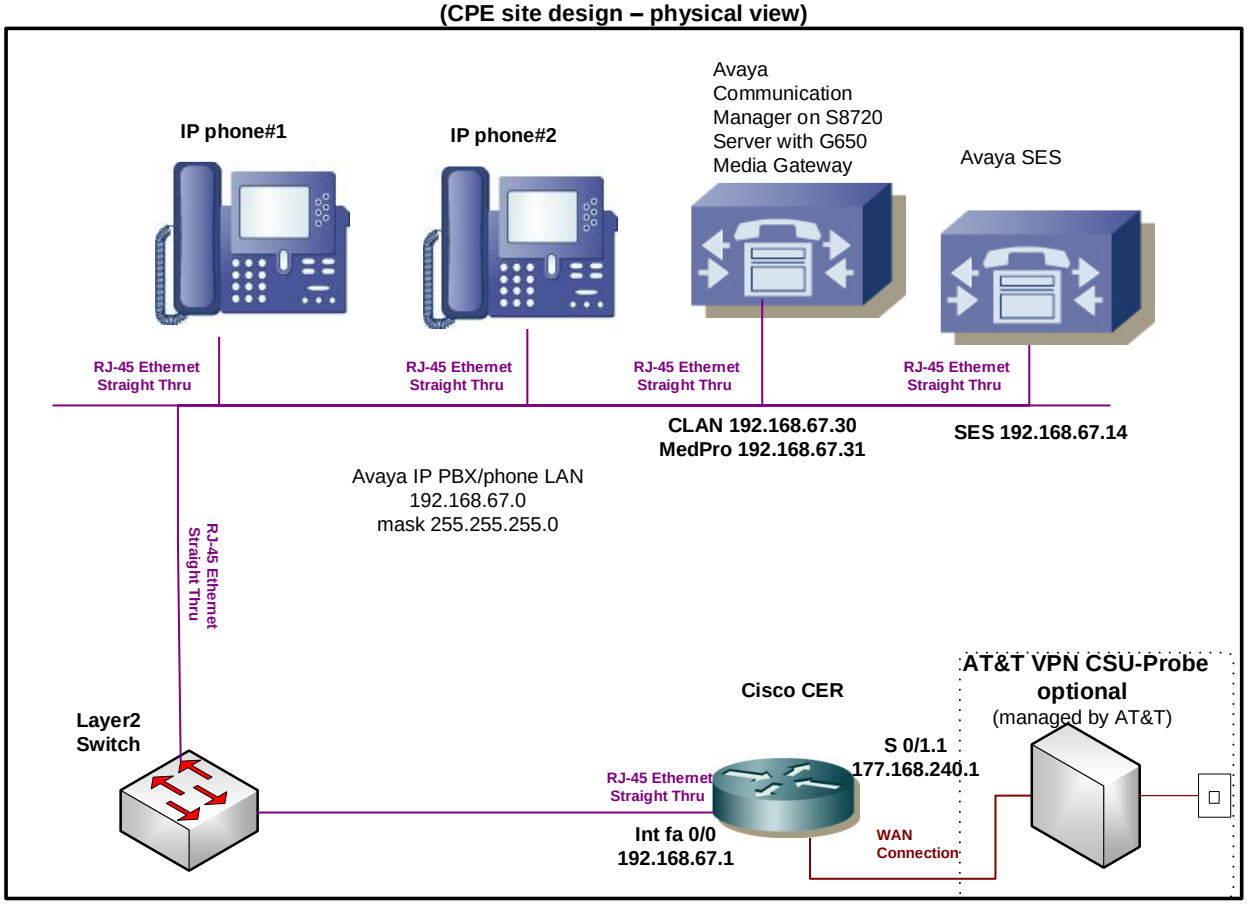
The AT&T NAT and PAT addresses (public Signaling and Media IP Addresses) must be distributed to the AT&T network via BGP. The network address of the Avaya IP PBX and phones should also be distributed.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address> mask 255.255.255.255
network <public Media IP Address> mask 255.255.255.255
network <Network address of Avaya IP PBX/phones > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

In this example, the SES address is 192.168.67.14, the CLAN IP address is 192.168.67.30 and the MedPro address is 192.168.67.31.

**AT&T BVoIP on AT&T VPN Site
with AT&T VPN CSU-Probe, Avaya CM and SES
(CPE site design – physical view)**




```
interface Loopback6
 ip address 135.16.170.55 255.255.255.255
!
interface Loopback7
 ip address 135.16.170.250 255.255.255.255
!
interface FastEthernet0/0
 description LAN interface facing Avaya Communications Manager
 ip address 192.168.67.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex full
 speed 100


interface Serial0/1/0:0.1 point-to-point
```

```
description WAN interface facing AT&T VPN
bandwidth 1459
ip address 192.166.202.1 255.255.255.252
ip nat outside
no ip virtual-reassembly
frame-relay class shape1536
frame-relay interface-dlci 239 IETF

ip nat inside source list 10 interface Loopback7 overload  (PAT for phones and Medpro)
ip nat inside source static 192.168.67.14 135.16.170.55      (NAT for SES)

access-list 10 deny   192.168.67.14     (Deny SES address)
access-list 10 deny   192.168.67.30     (Deny CLAN address)
access-list 10 permit 192.168.67.0 0.0.0.255  (Allow LAN address space of phones and Medpro)

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.170.55 mask 255.255.255.255
network 135.16.170.250 mask 255.255.255.255
network 192.168.67.0 mask 255.255.255.0
neighbor 177.168.240.2  remote-as  37383
neighbor 177.168.240.2  allowas-in
 no auto-summary
```

4.8 Avaya (Nortel) Business Communication Manager (BCM) Release 6.0 (without an SBC)

The Avaya BCM is a supported solution (see appropriate CCG for IP PBX configurations).

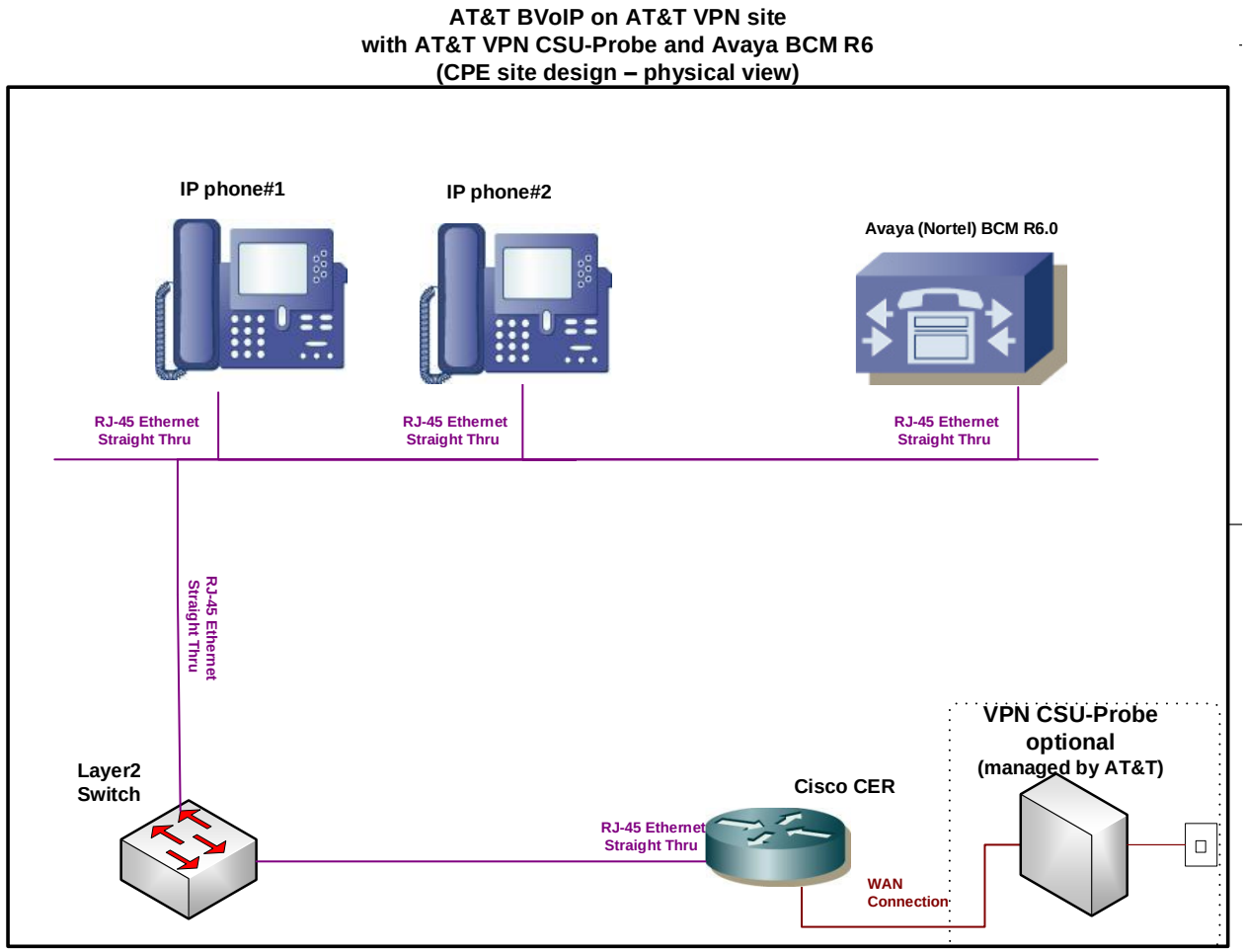
4.8.1 Topology

Following is a sample diagram of a network topology for a site with an Avaya BCM without a Session Border Controller (SBC). The AT&T VPN CSU-Probe is a AT&T managed device.

Note:

When using the AT&T VPN transport, a 30 byte payload with the G.729 CODEC is recommended for the maximum number of concurrent calls. This is especially

important with international customers using low bandwidth circuits. BCM does not support a 30 byte payload in both directions for any call scenarios, even when configured as such. Asymmetric payload size will **not** adversely affect call quality, but must be taken into consideration when calculating the maximum number of concurrent calls on a given circuit based on the bandwidth per call calculation.



4.8.2 Standard NAT/PAT Configuration (required)

- The BCM must be NAT'd to a registered public Signaling IP Address (which will be a loopback interface on the CER).
- The IP endpoints (IP Telephones, Soft phones, etc.) must be PAT'd to a different registered loopback interface address (for media traffic).

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing Avaya BCM

Configure a LAN interface of the CER for the same network as the Avaya BCM and phones network.

Step 2: Define loopback interfaces

Define one loopback address for the public Signaling IP Address. This will be the address the BCM is NAT'd to.

Define a second loopback address for the public Media IP Address. This will be the address the IP phones are PAT'd to.

```
interface Loopback <X>
  ip address  <public Signaling IP Address – NAT for BCM > 255.255.255.255

interface Loopback <Y>
  ip address  <public Media IP Address – PAT for IP phones > 255.255.255.255
```

Step 3: Create NAT/PAT statements

PAT is required for the IP phones. An access list is used to define the addresses eligible for PAT. The BCM will have a separate NAT statement.

PAT statement:

```
ip nat inside source list <ACL # > interface LoopbackY overload
access-list <ACL#> permit <Private LAN address space of phones> <appropriate mask>
```

NAT statement:

```
ip nat inside source static <private Signaling IP Address - on BCM>  <public Signaling IP Address>
```

Step 4: Configure BGP

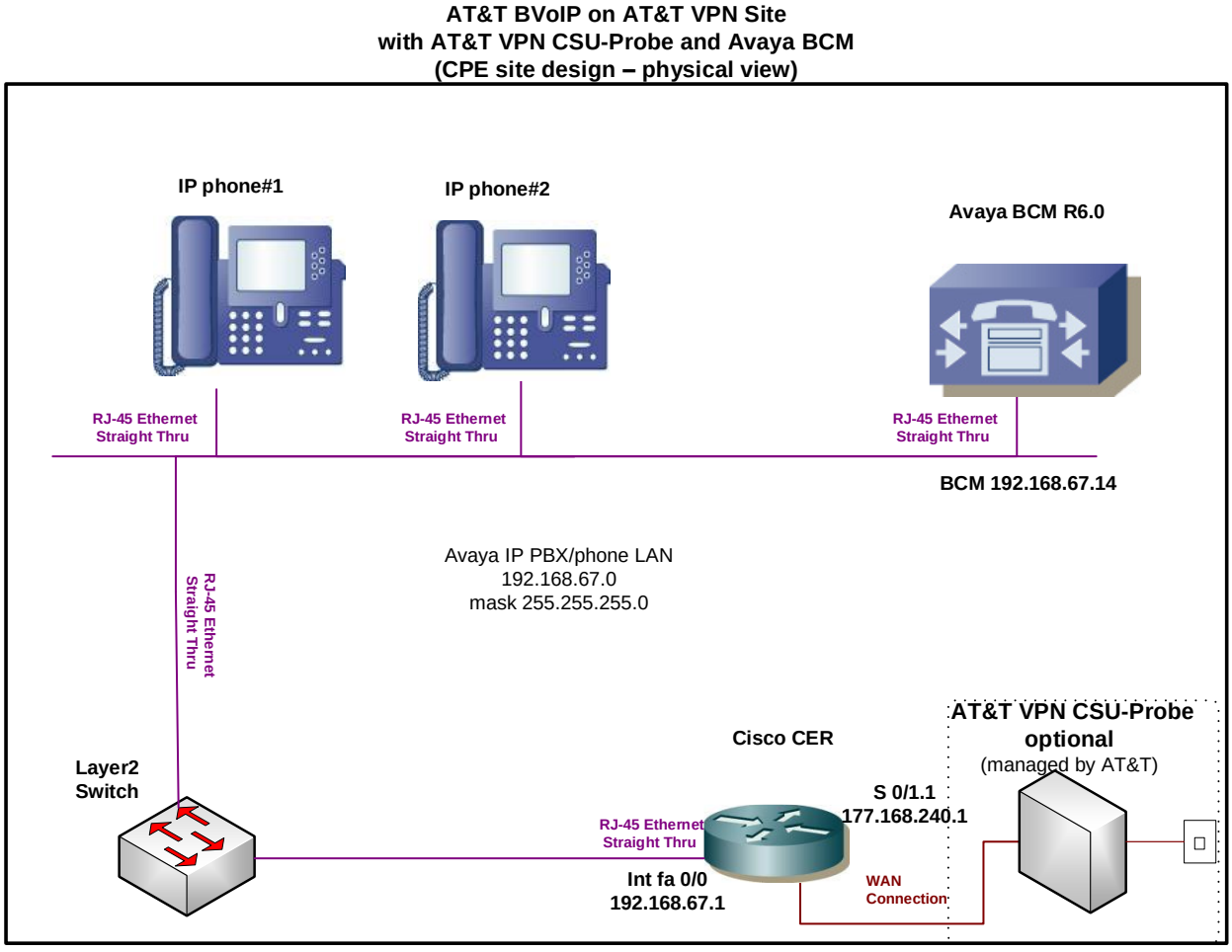
The public Signaling and Media IP Addresses must be distributed to the AT&T network via BGP. The network address of the Avaya IP PBX and phones should also be distributed.

```
router bgp <your AS number>
```

```
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address> mask 255.255.255.255
network <public Media IP Address> mask 255.255.255.255
network <Network address of Avaya IP PBX/phones > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

In this example, the BCM address is 192.168.67.14




```
interface Loopback6
 ip address 135.16.170.55 255.255.255.255
!
interface Loopback7
 ip address 135.16.170.250 255.255.255.255
!
```

```
interface FastEthernet0/0
 description LAN interface facing Avaya BCM
 ip address 192.168.67.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex full
 speed 100

interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T VPN
 bandwidth 1459
 ip address 192.166.202.1 255.255.255.252
 ip nat outside
 no ip virtual-reassembly
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF

ip nat inside source list 10 interface Loopback7 overload  (PAT for phones)
ip nat inside source static 192.168.67.30 135.16.170.55      (NAT for BCM)

access-list 10 permit 192.168.67.0 0.0.0.255  (Allow LAN address space of phones)

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.170.55 mask 255.255.255.255
network 135.16.170.250 mask 255.255.255.255
network 192.168.67.0 mask 255.255.255.0
neighbor 177.168.240.2  remote-as  37383
neighbor 177.168.240.2  allowas-in
 no auto-summary
```

4.9 Avaya IP Office (without an SBC)

This section applies to the Avaya IP Office solution (see appropriate CCG for IP Office configuration information).

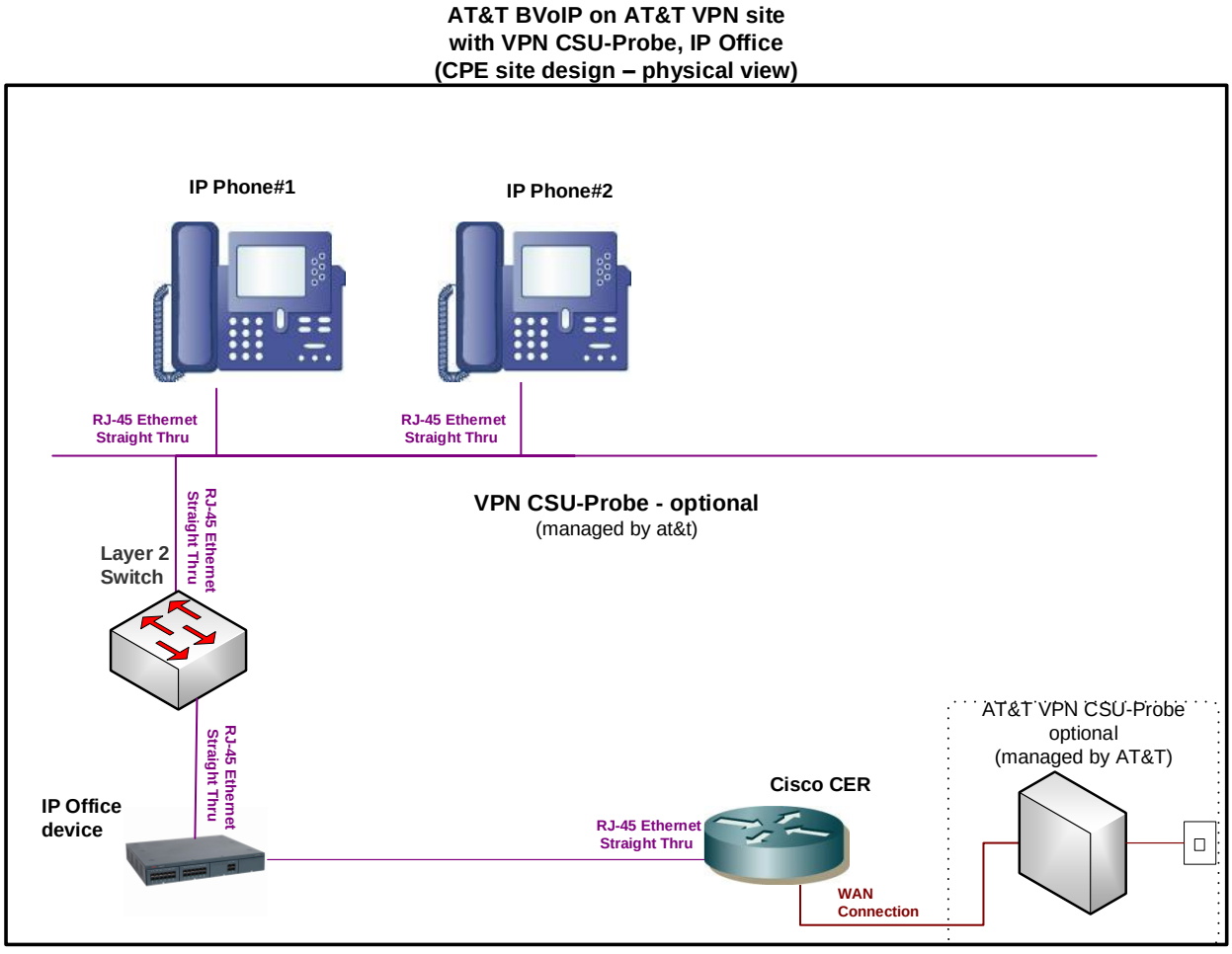
4.9.1 Topology

Following is a sample diagram of a network topology for a site with Avaya IP Office.

The AT&T VPN CSU-Probe is a AT&T managed device.

Note:

- The AT&T VPN CSU-Probe is optional.



4.9.2 Standard Solution

The IP Office LAN interface (facing the CER) will be configured with the Signaling IP Address. Note: The IP Office LAN interface provisioned for signaling will also be used for the media traffic. Therefore, all voice and signaling traffic destined for AT&T will be sourced from a single LAN interface on the IP Office device. The Media IP Address will be used to configure the CER LAN interface (facing the IP Office device) although it is not actually used for media traffic.

Step 1: Configure CER LAN interface facing IP Office

The Signaling and Media IP Addresses will be used for the network between the CER and IP Office device. The CER interface, which faces the IP Office device, will be assigned the Media IP Address and the IP Office device interface which faces the CER will be assigned the Signaling IP address. For example, if AT&T provides a media address 32.21.150.17, this address will be configured on the CER LAN interface facing the IP Office device. If AT&T provides a signaling address or 32.21.150.18, this address will be configured on the IP Office device LAN interface facing the CER.

Note: The IP Address on the IP Office device interface is the Signaling IP Address (although it is used for media as well) and must be the IP Address which has been provisioned as such in the AT&T NETWORK. Note: AT&T prefers to provide the Signaling and Media IP Addresses, but does offer to use customer supplied IP addresses if required. Using a customer supplied address may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer voice network is required for site-to-site calls.

```
ip route <customer voice network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

The Signaling IP address and customer voice network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

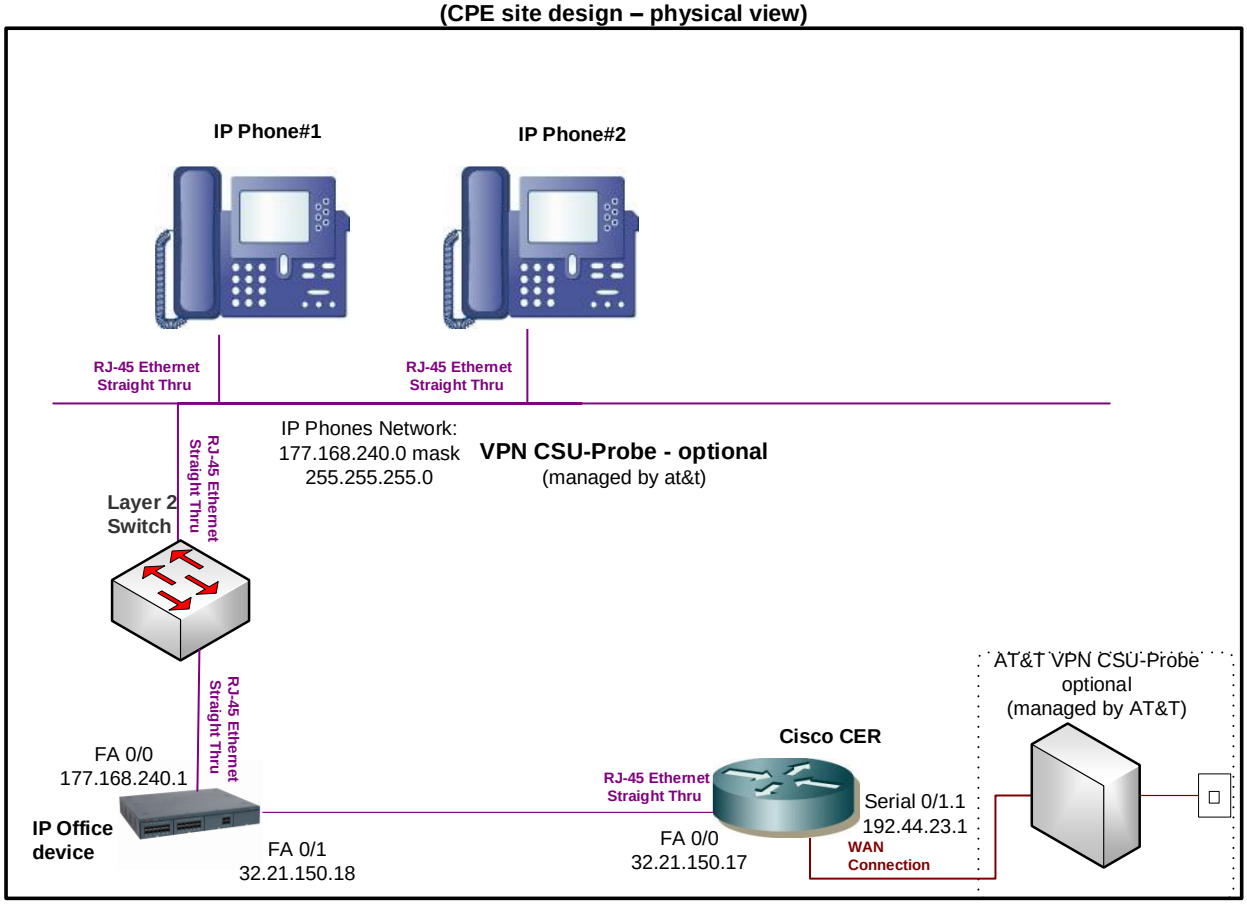
```
router bgp <your AS number>
no synchronization

bgp log-neighbor-changes
network <Signaling IP Address network > mask 255.255.255.248
network <customer voice network > mask <use  appropriate mask>

neighbor <PER IP address>  remote-as  <remote AS>
```

```
neighbor <PER IP address>  allowas-in
no auto-summary
```

Example:

In the following example, 177.168.240.0 is the customer voice network where the customer IP phones reside. 32.21.150.18 is the LAN IP address of the IP Office device facing the CER (this is the Signaling IP Address – which will also be used for media). 32.21.150.17 is the LAN IP address of the CER (this is the Media IP Address – although it is not actually used for media).

AT&T BVoIP on AT&T VPN site with VPN CSU-Probe, IP Office (CPE site design – physical view)




```
interface FastEthernet0/0
 description LAN interface facing IP Office
 ip address 32.21.150.17 255.255.255.248
 duplex full
 speed 100
ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

```
router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 32.21.150.16  mask 255.255.255.248
network 177.168.240.0  mask 255.255.255.0
neighbor 192.44.23.2  remote-as  37383
 neighbor 192.44.23.2  allowas-in
 no auto-summary
```

4.9.3 Optional NAT Solution (non-standard configuration)

If the IP Office device uses a private IP address for signaling/media, that address may be NAT'd to a public Signaling IP Address on the CER. However, this is not recommended due to degraded CPU performance with NAT enabled.

The CER loopback interface used for NAT will be configured with the public Signaling IP Address. The CER loopback interface will also be used for the media traffic. Therefore all media and signaling traffic will be sourced from a single loopback interface on the CER.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing IP Office

Configure a LAN interface of the CER in the same network as the IP Office interface facing the CER.

Step 2: Define Loopback Interface

Assign the public Signaling IP Address to a loopback interface on the CER (this address will also be used for media).

```
interface Loopback <#>
  ip address  <public Signaling IP Address > 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private IP Office Signaling/Media IP Address to the public IP Signaling Address (the same address will also be used for media).

```
ip nat inside source static <private IP Office Signaling/Media Address> < public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the IP Office device.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing IP Office
 ip address <ip address> <mask>
 ip nat inside


interface WAN #  **Always use subinterface when available**
 description WAN interface facing ATT
 ip address <ip address> <mask>
 ip nat outside
```

Step 5: Configure Static Routes

A static route is required for the customer IP Phones network. The route will point at the IP Office device.

```
ip route <customer IP Phones network> <appropriate subnet> <private IP Office Signaling/Media Address>
```

Step 6: Configure BGP

The public Signaling/Media IP Address must be distributed to the network via BGP (you will **not** need to redistribute the private IP Office Signaling/Media IP Address). The CER will need to be configured with a network statement for the public Signaling/Media Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling/Media IP Address > mask 255.255.255.255
network <customer IP Phones network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The IP Office LAN address used for Signaling/Media (private addressing) will be translated to a public Signaling IP Address (which is defined as a loopback interface on the CER). Continuing the example from section 4.1.2 (assume now that the IP Office device uses a private address), the IP Office private Signaling/Media IP address of 32.21.150.18 will be translated to a public Signaling Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255

interface FastEthernet0/0
 description LAN interface facing IP Office
 ip address 32.21.150.17 255.255.255.248
 ip nat inside
 duplex full
 speed 100


interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing ATT
 bandwidth 1459
 ip address 192.33.20.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF


ip nat inside source static 32.21.150.18 135.16.180.66


router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

4.10 Avaya Communications Manager or Avaya Communication Server 1000 or Aura Experience Portal or Voice Portal with an SBC (ACME Packet Net-Net SBC/Aura SBC/Sipera E-SBC) and optional Avaya Session Manager for certain scenarios

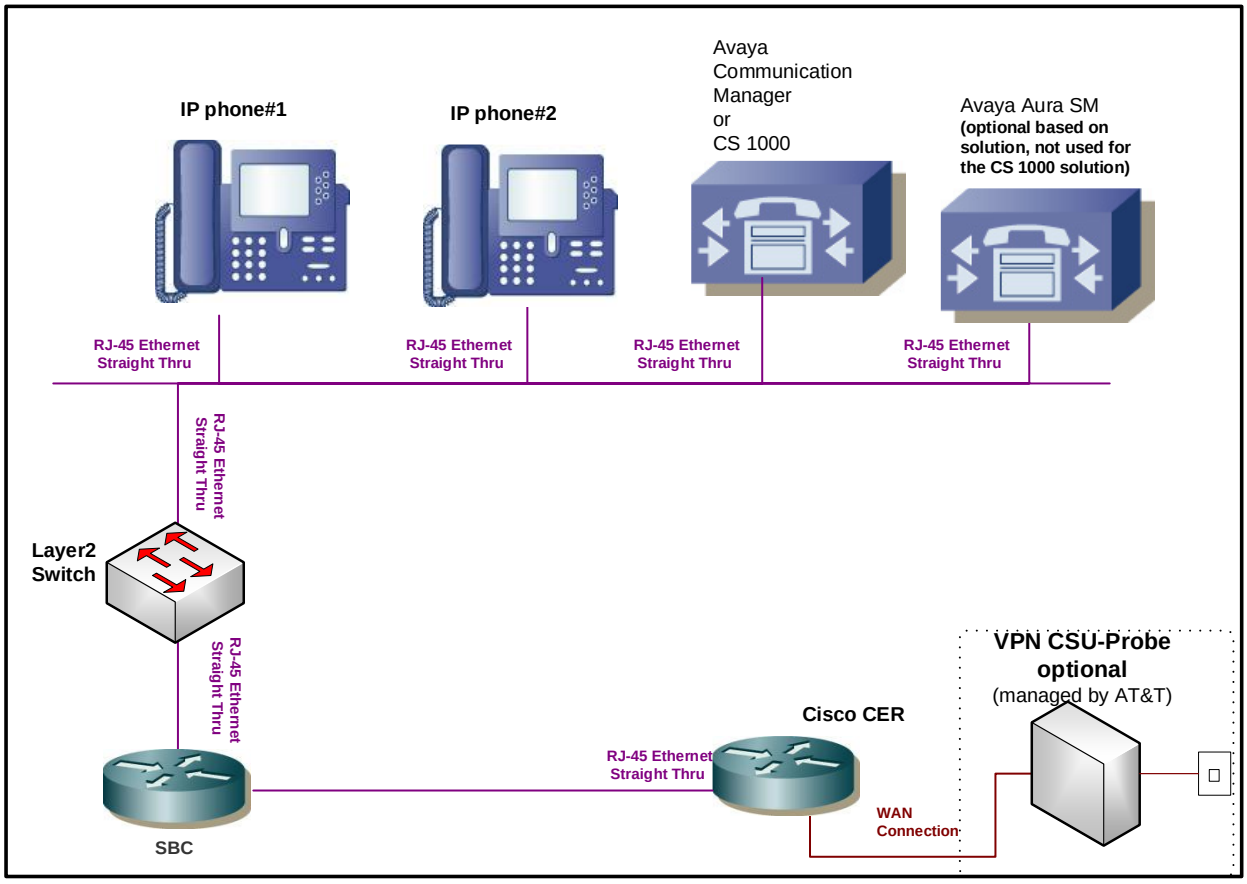
This section covers the following scenarios (see appropriate CCG for IP PBX configurations):

- Avaya Communications Manager with Avaya Session Manager and ACME Packet Net-Net SBC
- Avaya Communications Manager with Avaya Session Manager and Avaya Aura SBC
- Avaya CS1000 with an ACME Packet Net-Net SBC
- Avaya CS1000 with Avaya Session Manager and Avaya Aura SBC
- Avaya Communications Manager with Avaya Session Manager and Sipera™ Systems E-SBC
- Aura Experience Portal 6.0, Aura Communication Manager 6.0.1, Aura Session Manager 6.1 (Certified for IP Toll-Free Service only)

4.10.1 Topology

Following is a sample diagram of a network topology for a site with an Avaya Communications Manager or Communication Server 1000 (CS 1000) with an SBC. The AT&T VPN CSU-Probe is a AT&T managed device. Note: The AT&T VPN CSU-Probe is optional.

AT&T BVoIP on AT&T VPN site
with AT&T VPN CSU-Probe, Avaya Communications Manager or Avaya CS 1000
(CPE site design – physical view)



4.10.2 Standard Solution

Avaya Communications Manager or Avaya CS 1000 works in conjunction with an SBC (see appropriate CCG for Avaya Communications Manager and SBC configurations). All voice and signaling traffic will be sourced from the SBC.

Note: Avaya Aura Communication Manager (CM) 5.2.1 with Aura Session Manager (SM) 5.2 and the **ACME Packet Net-Net 3800/4250/4500** is certified **without** cRTP. cRTP testing has not been done, therefore, is **not** supported.

Step 1: Configure LAN interface facing the SBC

The SIP Signaling/Media address range assigned by AT&T will be used for the network between the CER and SBC. The CER LAN interface which faces the SBC will be assigned the Media IP Address and the SBC LAN interface which faces the CER will be assigned the Signaling IP Address. For example, if AT&T assigns

32.21.150.17 for the Media IP Address, this address will be configured on the CER (on the LAN interface facing the SBC). If AT&T assigns 32.21.150.18 for the Signaling IP Address, this address will be configured on the SBC (on the LAN interface facing the CER).

Note: The IP Address on the SBC interface is the SIP Signaling/Media IP address and must be the IP Address which has been provisioned as such in the AT&T Network. Note: AT&T prefers to assign the address space for the SIP Signaling/Media, but does offer to use existing customer Addressing if required.

Step 2: Configure static route statement

A static route statement to the customer's Avaya IP PBX and phone network is required.

```
ip route <Avaya IP PBX & phone network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

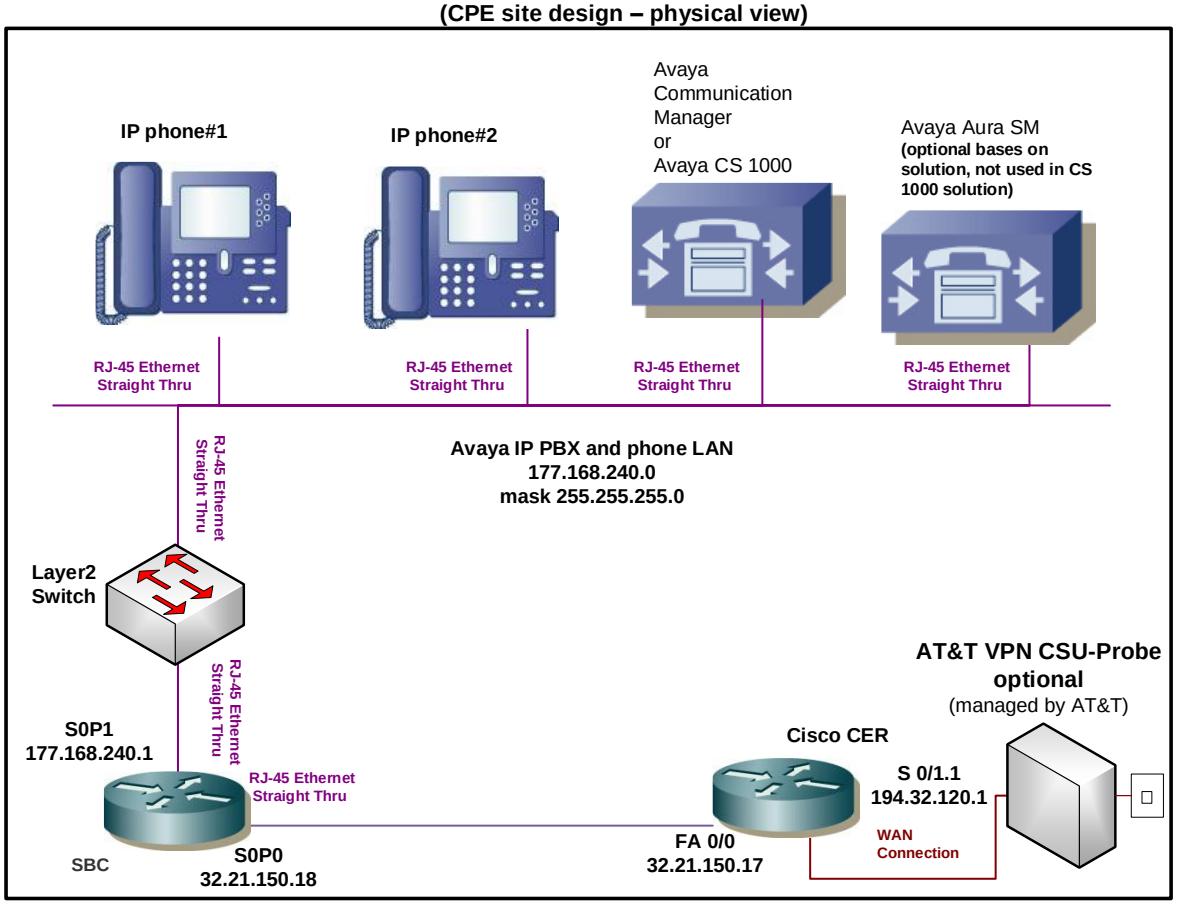
The Signaling IP Address and Avaya IP PBX/phone network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes


network <Signaling IP Address network> mask 255.255.255.248
network <Avaya IP PBX/phone network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where the Avaya IP PBX and phones reside. 32.21.150.18 is the LAN address of the SBC facing the CER (Signaling IP Address). 32.21.150.17 is the LAN address of the CER facing the SBC (Media IP Address).

AT&T BVoIP on AT&T VPN Site
with AT&T VPN CSU-Probe, Avaya Communications Manager or CS 1000
(CPE site design – physical view)




```
interface FastEthernet0/0
 description LAN interface facing SBC
 ip address 32.21.150.17 255.255.255.248
 duplex full
 speed 100
ip route 177.168.240.0 255.255.255.0 32.21.150.18

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 32.21.150.16  mask 255.255.255.248
network 177.168.240.0  mask 255.255.255.0
neighbor 194.32.120.2  remote-as  37383
 neighbor 194.32.120.1  allowas-in
 no auto-summary
```

4.10.3 Optional NAT Solution (non-standard configuration)

A private signaling/media address on the SBC may be NAT'd to a public Signaling

IP address on the CER. However, this is not recommended due to degraded CPU performance with NAT enabled.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing SBC

Configure a LAN interface of the CER for the same network as one of the SBC interfaces.

Step 2: Define loopback interface

Assign the public Signaling IP Address to a loopback interface on the CER.

```
interface Loopback <#>
  ip address  <public Signaling IP Address > 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private SBC signaling/media IP address to the public Signaling IP Address.

```
ip nat inside source static <private Signaling/Media IP Address> <public Signaling IP Address – CER loopback interface>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the “ip nat inside” and “ip nat outside: statements to the appropriate interfaces.

The “ip nat inside” statement will be applied to the LAN interface that is facing the SBC.

The “ip nat outside” statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing SBC
 ip address <ip address> <mask>
 ip nat inside

interface WAN #  **Always use subinterface when available**
 description WAN interface facing AT&T  VPN
```

```
ip address <ip address> <mask>
ip nat outside
```

Step 5: Configure static route statement

A static route statement to the customer's Avaya IP PBX and phone network is required.

```
ip route <Avaya IP PBX & phone network> <appropriate subnet> <private signaling/media IP address – SBC LAN interface>
```

Step 6: Configure BGP

The public Signaling IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private signaling/media address). The CER will need to be configured with a network statement for the public Signaling IP Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address> mask 255.255.255.255
network <Avaya IP PBX/phone LAN > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Continuing the example from section 4.7.2 (assume now that the SBC uses a private signaling/media address). 32.21.150.18 is the SBC private signaling/media IP address and it will be translated to the public Signaling IP Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255


interface FastEthernet0/0
 description LAN interface facing SBC
 ip address 32.21.150.17 255.255.255.248
 ip nat inside
 duplex full
 speed 100
interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T  VPN
 ip address 192.150.23.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF
```

```
ip nat inside source static 32.21.150.18 135.16.180.66


router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0  mask 255.255.255.0
neighbor 194.32.120.2  remote-as  37383
 neighbor 194.32.120.2  allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

Avaya Notification Solution (ANS) is a software only solution that runs on Linux server. It provides real-time multimedia notification and response capabilities to IP Phones, Cell phones, and digital/analog phones. It provides intelligent notification features such as notification cascading, acknowledgement gathering, and conference. It can be applied to emergency broadcast and system alarming.

We are certifying the ANS with Acme Net-Net SD for the IP FR service. The testing was done with a VMware vSphere ESX4.0 running ANS 1.2 on a 32-bit Redhat Enterprise Linux 5.4

The following is certified -

Avaya Notification Solution 1.2
Acme Packet Net-Net SD SCX6.2.0 MR-6 Patch 5 (Build 916)

4.11 Avaya Notification Solution (ANS) with ACME Packet Net-Net SBC

This solution will use the same configuration as show in the previous section "*Avaya Communications Manager or Avaya Communication Server 1000 or Aura Experience Portal or Voice Portal with an SBC (ACME Packet Net-Net SBC/Aura SBC/Sipera E-SBC) and optional Avaya Session Manager for certain scenarios*".

Avaya Notification Solution (ANS) is a software only solution that runs on Linux server. It provides real-time multimedia notification and response capabilities to IP Phones, Cell phones, and digital/analog phones. It provides intelligent notification features such as notification cascading, acknowledgement gathering, and conference. It can be applied to emergency broadcast and system alarming.

We are certifying the ANS with Acme Net-Net SD for the IP FR service. The testing was done with a VMware vSphere ESX4.0 running ANS 1.2 on a 32-bit Redhat Enterprise Linux 5.4

The following is certified -

Avaya Notification Solution 1.2
Acme Packet Net-Net SD SCX6.2.0 MR-6 Patch 5 (Build 916)

4.12 Microsoft Lync Server 2010 or Microsoft Office Communication Server 2007 R2 with Cisco Unified Border Element (CUBE)

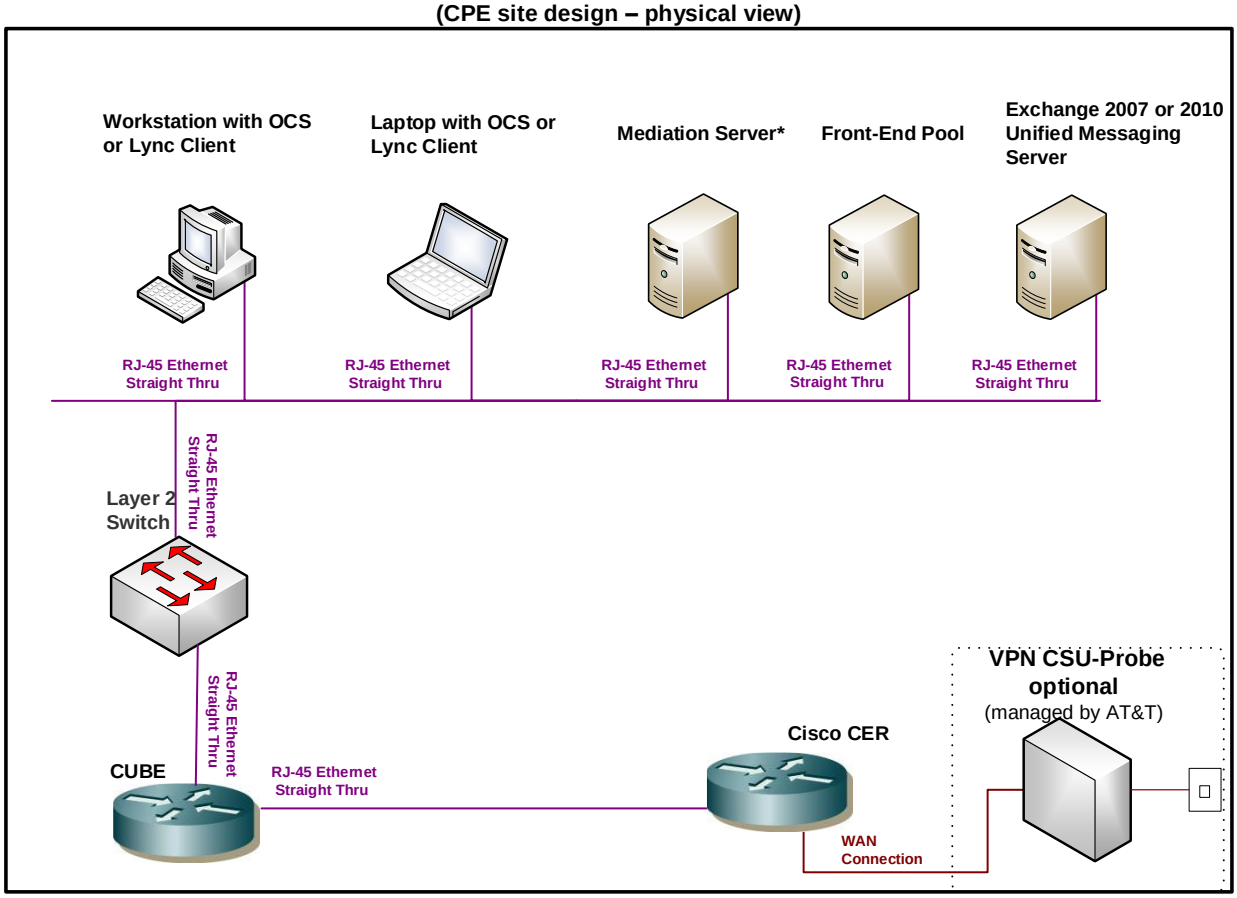
The Microsoft Lync Server 2010 or Microsoft Office Communication Server (OCS) solution can work in conjunction with a cascaded CUBE router (see the appropriate CCG for MS Lync or MS OCS and CUBE configurations). Voice and signaling traffic will be sourced from a single LAN interface CUBE.

This solution only supports G.711 for RTP. Only access speeds of full T1 and greater will be supported with this solution. Fax is not supported.

4.12.1 Topology

Following is a sample diagram of a network topology for a site with Microsoft Lync Server 2010 or Microsoft Office Communications Server (OCS) 2007 R2 and Cisco Unified Border Element (CUBE). In this design, the CER and CUBE are two separate routers. The AT&T VPN CSU-Probe is a AT&T managed device. Note: The AT&T VPN CSU-Probe is optional.

**AT&T BVoIP on AT&T VPN site
with AT&T VPN CSU-Probe, CUBE, MS OCS or Lync 2010
(CPE site design – physical view)**



*** Lync Server 2010 offers the option to collocate the Mediation Server on the Front-End Server.**

4.12.2 Standard Solution

Step 1: Configure LAN interface facing CUBE

The SIP Signaling/Media address range assigned by AT&T will be used for the network between the CER and CUBE router. The CER interface which faces the CUBE will be assigned the Media IP Address (although it's not technically used to source the media traffic) and the CUBE router interface which faces the CER will be assigned the Signaling IP Address. For example, if AT&T assigns 32.21.150.17 as the Media IP Address, this address will be configured on the CER (LAN interface facing the CUBE). If AT&T assigns 32.21.150.18 as the Signaling IP Address, this address will be configured on the CUBE Router (LAN interface facing the CER).

Note: The IP Address on the CUBE interface is the SIP signaling address and must be the IP Address which has been provisioned as such in the AT&T NETWORK (although

this same address is technically also used for the media traffic). Note: AT&T prefers to assign the address space for the SIP Signaling/Media, but does offer to use existing customer addressing if required. Using a customer provided address space may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer's Microsoft Lync/OCS network is required for this solution (required for site-to-site calls).

```
ip route <MS Lync or OCS network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

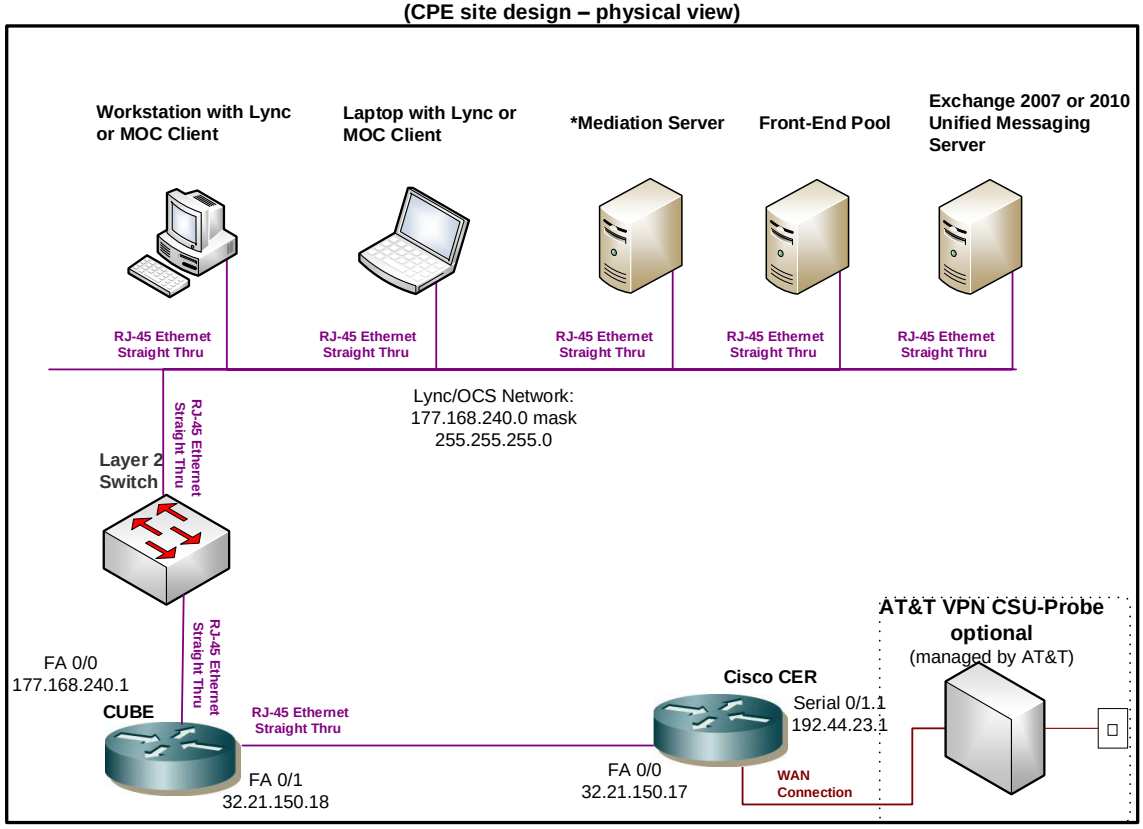
The Signaling IP Address and the MS Lync/OCS network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes

network <Signaling IP Address network> mask 255.255.255.248
network <MS Lync or OCS network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where MS Lync/OCS resides. The 32.21.150.18 is the LAN address of the CUBE router facing the CER (Signaling IP Address). 32.21.150.17 is the LAN address of the CER (Media IP Address).

AT&T BVoIP on AT&T VPN Site
with AT&T VPN CSU-Probe, CUBE, MS Lync or OCS
(CPE site design – physical view)



*** Lync Server 2010 offers the option to collocate the Mediation Server on the Front-End Server**

```
interface FastEthernet0/0
 description LAN interface facing CUBE
 ip address 32.21.150.17 255.255.255.248
 duplex full
 speed 100

ip route 177.168.240.0 255.255.255.0 32.21.150.18

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 32.21.150.16  mask 255.255.255.248
network 177.168.240.0  mask 255.255.255.0
neighbor 192.44.23.2  remote-as  37383
 neighbor 192.44.23.2  allowas-in
 no auto-summary
```

4.12.3 Optional NAT Solution (non-standard configuration)

If CUBE uses a private address for the signaling/media, that address may be NAT'd to a public Signaling IP Address on the CER. However this is not recommended due to degraded CPU performance with NAT enabled.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing CUBE

Configure a LAN interface of the CER for the same network as one of the CUBE interfaces.

Step 2: Define loopback interface

Assign the public Signaling IP Address to a loopback interface on the CER.

```
interface Loopback <#>
  ip address  <public Signaling IP Address > 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private CUBE signaling/media IP address to the public Signaling IP Address.

```
ip nat inside source static <private signaling/media IP address> <public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside: statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the CUBE router.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing CUBE
 ip address <ip address> <mask>
 ip nat inside
```

```
interface WAN #  **Always use subinterface when available**
 description WAN interface facing AT&T  VPN
 ip address <ip address> <mask>
 ip nat outside
```

Step 5: Configure static routes

A static route is required for the MS Lync/OCS network. This route will point to the CUBE router.

```
ip route <MS Lync or OCS network> <appropriate subnet> <private signaling/media IP address>
```

Step 6: Configure BGP

The public Signaling IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private CUBE signaling/media IP address). The CER will need to be configured with a network statement for public Signaling IP Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address > mask 255.255.255.255
network <MS Lync or OCS network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The CUBE private signaling/media IP Address interface will be translated to a public Signaling IP Address (which is defined as a loopback interface on the CER). Continuing the example from section 4.8.2 (assume now that the CUBE uses a private address), the private CUBE signaling/media address of 32.21.150.18 will be translated to the public Signaling IP Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255

interface FastEthernet0/0
 description LAN interface facing CUBE
 ip address 32.21.150.17 255.255.255.248
 ip nat inside
 duplex full
 speed 100
```

```
interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T  VPN
 bandwidth 1459
 ip address 192.33.20.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF

ip nat inside source static 32.21.150.18 135.16.180.66

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

4.13 Microsoft Office Communication Server (OCS) 2007 R2 with Network Equipment Technologies (NET) VX 1200/1800 Gateway

The Microsoft Office Communication Server solution can work in conjunction with a NET VX Gateway (see appropriate CCG for OCS and NET VX Gateway configurations). All voice and signaling traffic will be sourced from the NET VX Gateway.

This solution only supports G.711 for RTP. Fax messages cannot be received into a Microsoft Exchange mailbox. Fax messages can be received and transmitted from analog fax machines connected to a Quintum Tenor gateway (not shown). Note that problems have been encountered when faxing to a Cisco TDM gateway using T38 when the Fax machines at both sides are Super G3. This issue can be overcome by configuring the Quintum Tenor gateway to use the G711 codec instead of T38 for FAX calls.

Only access speeds of full T1 and greater will be supported with this solution.

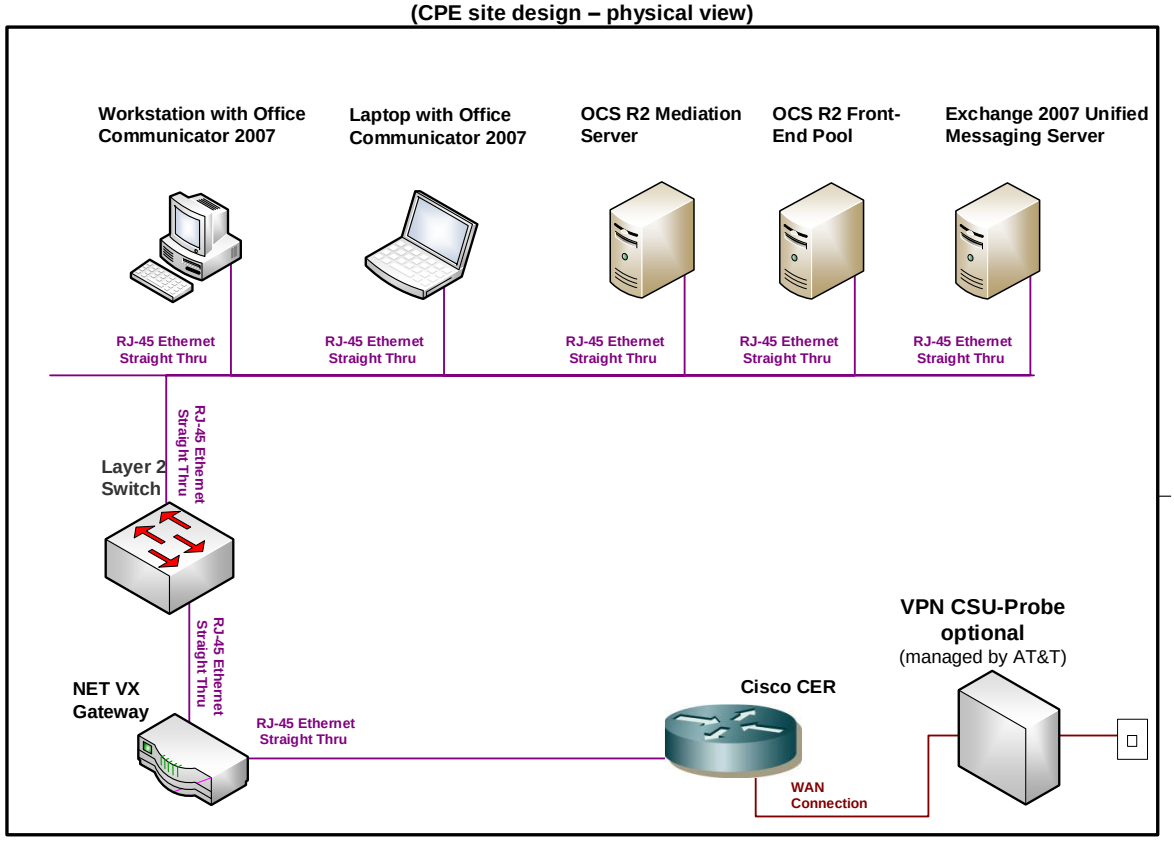
4.13.1 Topology

Following is a sample diagram of a network topology for a site with Microsoft Office Communications Server (OCS) 2007 R2 and NET's VX 1200/1800 Gateway. The AT&T VPN CSU-Probe is a AT&T managed device.

Note:

- The AT&T VPN CSU-Probe is optional. All other equipment is managed by the customer.
- This solution only supports G.711 for RTP.
- Fax messages cannot be received into a Microsoft Exchange mailbox. Fax messages can be received and transmitted from analog fax machines connected to a Quintum Tenor gateway (not shown).
- Problems have been encountered when faxing to a Cisco Voice Gateway using T38 when the FAX Machines at both sides are Super G3. This issue can be overcome by configuring the Quintum Tenor gateway to use the G711 codec instead of T38 for FAX calls.
- Only access speeds of full T1 and greater will be supported with this solution.

AT&T BVoIP on AT&T VPN Site
with AT&T VPN CSU-Probe, NET VX 1200/1800, MS OCS
(CPE site design – physical view)



4.13.2 Standard Solution

Step 1: Configure LAN interface facing NET VX Gateway

The SIP Signaling/Media IP Address range provided by AT&T will be used for the network between the CER and NET VX Gateway router. The CER interface which faces the NET VX Gateway will be assigned the Media IP Address (although it will not be used for media). The NET VX Gateway interface which faces the CER will be assigned the Signaling IP Address. For example, if AT&T assigns a 32.21.150.17 Media IP Address, this address will be configured on the CER (LAN interface facing the NET VX Gateway). If AT&T assigns 32.21.150.18 as the Signaling IP Address, this address will be configured on the NET VX Router (LAN interface facing the CER).

Note: The IP Address on the NET VX Gateway interface is the assigned Signaling IP Address (used for both signaling and media) and must be the IP Address which has been provisioned as such in the AT&T NETWORK. Note: AT&T prefers to assign the Signaling and Media IP Addresses, but does offer to use existing customer addressing if required. Using a customer provided address space may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer's MS OCS network is required for this solution (required for site-to-site calls).

```
ip route <MS OCS network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

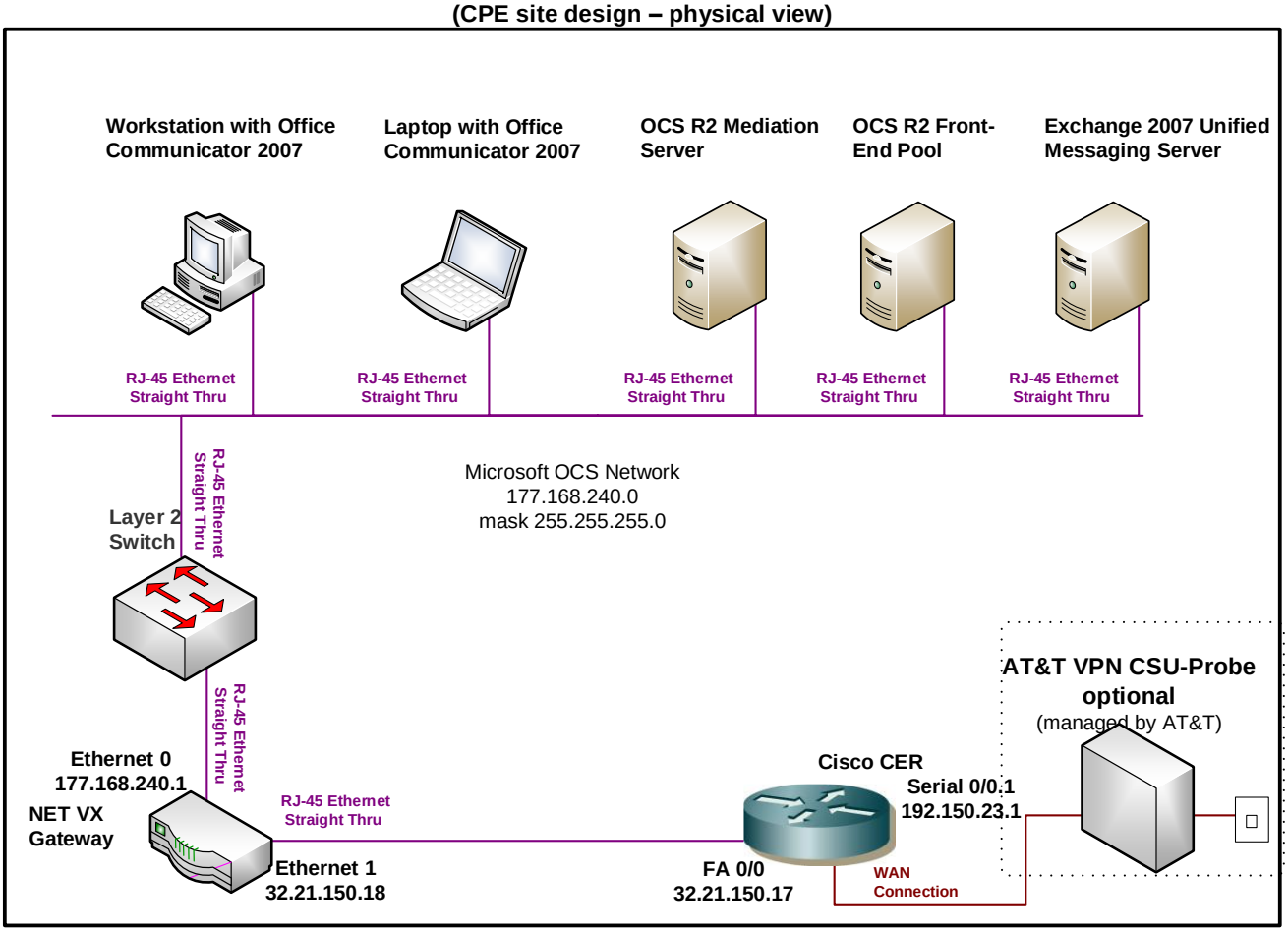
The Signaling IP Address and the MS OCS network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <Signaling IP Address network> mask 255.255.255.248
network <MS OCS network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where MS OCS resides. 32.21.150.18 is LAN address of the NET VX Gateway facing the CER (Signaling IP Address). 32.21.150.17 is the LAN address of the CER facing the NET VX Gateway (Media IP Address).

AT&T BVoIP on AT&T VPN Site
with AT&T VPN CSU-Probe, NET VX 1200/1800, MS OCS
(CPE site design – physical view)




```
interface FastEthernet0/0
 description LAN interface facing NET VX Gateway
 ip address 32.21.150.17 255.255.255.248
 duplex full
 speed 100

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

```
router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 32.21.150.16  mask 255.255.255.248

network 177.168.240.0  mask 255.255.255.0
neighbor 192.44.23.2  remote-as  37383
 neighbor 192.44.23.2  allowas-in
 no auto-summary
```

4.13.3 Optional NAT Solution (non-standard configuration)

The AT&T Signaling IP Address (NET VX Gateway interface that faces the CER) may be NAT'd at the CER. However this is not recommended due to degraded CPU performance with NAT enabled.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing NET VX Gateway

Configure a LAN interface of the CER for the same network as the NET VX Gateway interface.

Step 2: Define loopback interface

Assign the public Signaling IP Address to a loopback interface on the CER.

```
interface Loopback <#>
  ip address  <public Signaling IP Address > 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private NET VX Gateway signaling/media IP address to the public Signaling IP Address.

```
ip nat inside source static <private Signaling/Media IP Address> <public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside: statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the NET VX Gateway.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing NET VX Gateway
 ip address <ip address> <mask>
 ip nat inside


interface WAN #  **Always use subinterface when available**
 description WAN interface facing AT&T  VPN
 ip address <ip address> <mask>
 ip nat outside
```

Step5: Configure static route statement

A static route statement to the customer's MS OCS network is required for this solution (required for site-to-site calls).

```
ip route <MS OCS network> <appropriate subnet> <private Signaling/Media IP address>
```

Step 6: Configure BGP

The public Signaling IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private NET VX Gateway signaling/media address). The CER will need to be configured with a network statement for the public Signaling IP Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address> mask 255.255.255.255
network <MS OCS network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Continuing the example from section 4.9.2 (assume now that the NET VX Gateway uses a private signaling/media IP address). 32.21.150.18 is the NET VX Gateway

private signaling/media IP address (NET VX Gateway's router interface that faces the CER) and it will be translated to the public Signaling IP Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255

interface FastEthernet0/0
 description LAN interface facing NET VX Gateway
 ip address 32.21.150.17 255.255.255.248
 ip nat inside
 duplex full
 speed 100


interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T  VPN
 bandwidth 1459
 ip address 192.150.23.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF


ip nat inside source static 192.168.55.12 135.16.180.66


router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.80.66  mask 255.255.255.255
network 177.168.240.0  mask 255.255.255.0
neighbor 192.150.23.2  remote-as  37383
 neighbor 192.150.23.2  allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

4.14 Microsoft Lync Server 2010/Microsoft Office Communication Server 2007 R2 with ACME Packet Net-Net SBC or Sonus SBC

The Microsoft Lync Server 2010 (Lync) and Microsoft Office Communication Server (OCS) solution can work in conjunction with a cascaded ACME Packet Net-Net SBC or Sonus SBC (see appropriate CCG for MS Lync or MS OCS with the certified SBC combination). Voice and signaling traffic will be sourced from a LAN interface on the ACME Packet Net-Net.

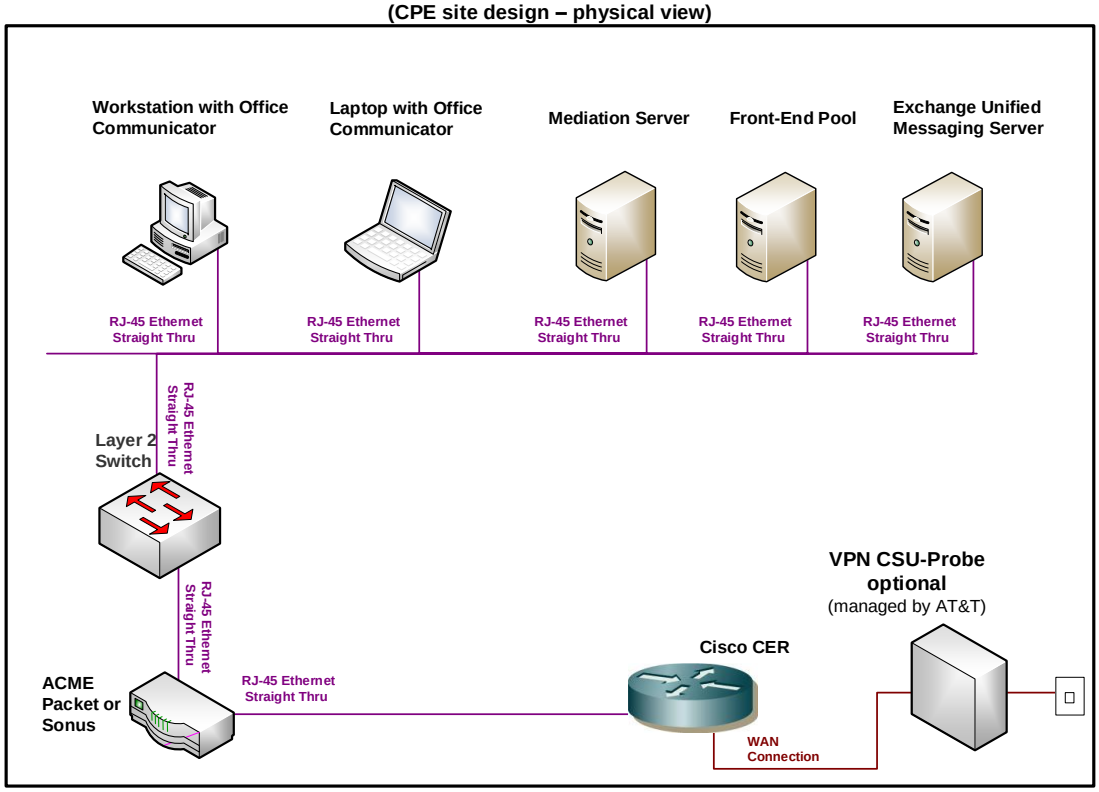
Certified solutions:
MS OCS with ACME SBC
MS Lync 2010 with ACME SBC
MS Lync 2010 with Sonus SBC

4.14.1 Topology

Following is a sample diagram of a network topology for a site with Microsoft Lync Server 2010 or Microsoft Office Communications Server 2007 R2 and ACME Packet Net-Net SBC or Sonus SBC. The AT&T VPN CSU-Probe is a AT&T managed device.

- The AT&T VPN CSU-Probe is optional. All other equipment is managed by the customer.
- G.711 is the only supported codec
- Fax is not supported.
- Only access speeds of full T1 and greater will be supported with this solution.

AT&T BVoIP on AT&T VPN site
with AT&T VPN CSU-Probe, ACME Packet Net-Net or Sonus, MS Lync/OCS
(CPE site design – physical view)



4.14.2 Standard Solution

Step 1: Configure the LAN interface facing the SBC

The SIP Signaling/Media address range assigned by AT&T will be used for the network between the CER and the SBC. The CER interface (which faces the SBC) will be assigned the Media IP Address (although this interface will not be used for media). The SBC interface (which faces the CER) will be assigned the Signaling IP Address. For example, if AT&T assigns 32.21.150.17 as the Media IP Address, this address will be configured on the CER (LAN interface facing the SBC). If AT&T assigns 32.21.150.18 as the Signaling IP Address, this address will be configured on the SBC (LAN interface facing the CER).

Note: The IP Address on the SBC interface, which faces the CER, is the Signaling IP Address (used for media traffic also) and must be the IP Address which has been provisioned as such in the AT&T Network. Note: AT&T prefers to assign the address space for the SIP Signaling/Media, but does offer to use existing customer addressing if required. Using a customer provided address space may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer's MS Lync/OCS network is required for this solution (required for site-to-site calls).

```
ip route <MS Lync/OCS network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

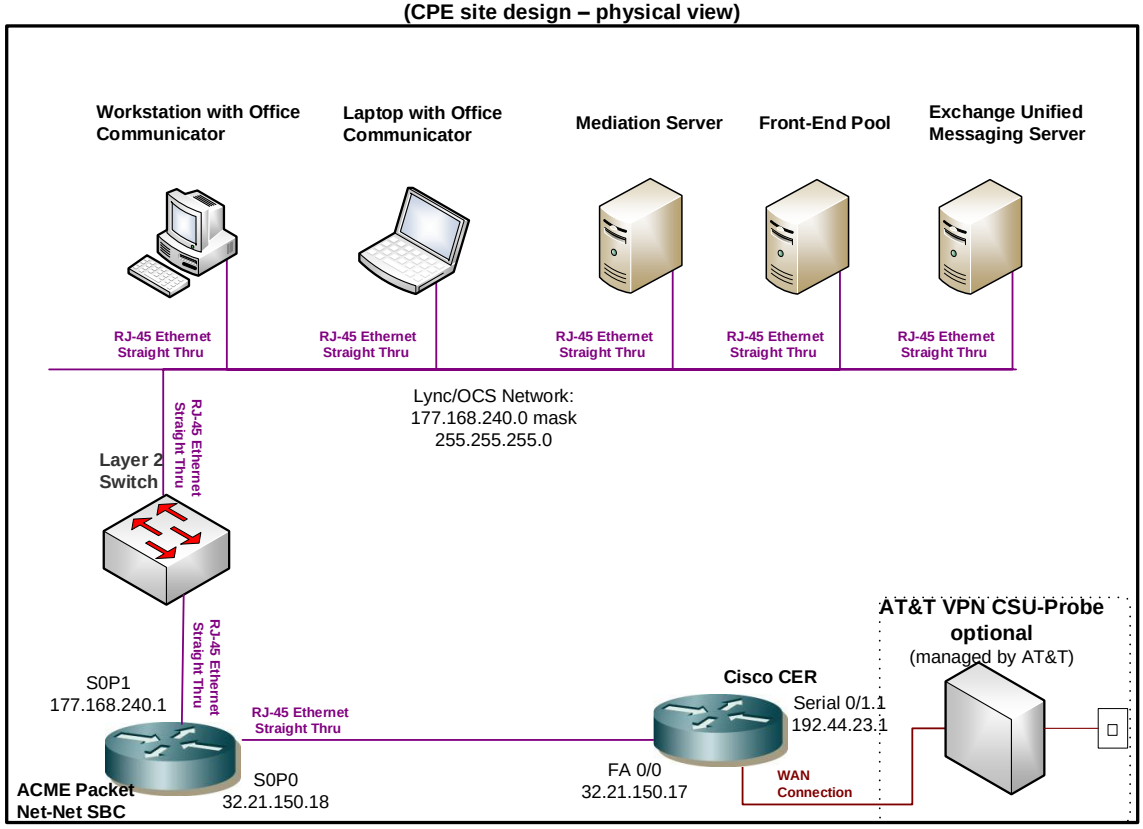
The Signaling IP Address and the MS Lync/OCS network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <Signaling IP Address network> mask 255.255.255.248
network <MS Lync/OCS network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where the OCS resides. 32.21.150.18 is the LAN address of the SBC interface facing the CER (Signaling IP Address). 32.21.150.17 is the LAN address of the CER (assigned Media IP Address).

AT&T BVoIP on AT&T VPN Site
with AT&T VPN CSU-Probe , ACME Packet Net-Net, MS Lync/OCS
(CPE site design – physical view)



interface FastEthernet0/0

description LAN interface facing the SBC

ip address 32.21.150.17 255.255.255.248

duplex full

speed 100

ip route 177.168.240.0 255.255.255.0 32.21.150.18

router bgp 65000
no synchronization
bgp log-neighbor-changes
network 32.21.150.16 mask 255.255.255.248
network 177.168.240.0 mask 255.255.255.0
neighbor 192.44.23.2 remote-as 37383
neighbor 192.44.23.2 allowas-in
no auto-summary

4.14.3 Optional NAT Solution (non-standard configuration)

If the SBC uses a private address for signaling/media, that address may be NAT'd to a public Signaling IP Address on the CER router. However this is not recommended due to degraded CPU performance with NAT enabled.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing the SBC

Configure a LAN interface of the CER router for the same network as one of the CUBE interfaces.

Step 2: Define loopback interface

Assign the public Signaling IP Address to a loopback interface on the CER.

```
interface Loopback <#>
  ip address  <public Signaling IP Address> 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private SBC signaling/media IP address to the public Signaling IP address.

```
ip nat inside source static <private signaling/media IP address> <public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside: statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the SBC.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing the SBC
 ip address <ip address> <mask>
 ip nat inside

interface WAN #  **Always use subinterface when available**
```

```
description WAN interface facing AT&T  VPN
ip address <ip address> <mask>
ip nat outside
```

Step 5: Configure Static Routes

A static route is required for the MS Lync/OCS network. The route will point at the SBC (private signaling/media IP address.

```
ip route <MS Lync/OCS network> <appropriate subnet> <private signaling/media IP address>
```

Step 6: Configure BGP

The public Signaling IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private SBC signaling/media address). The CER will need to be configured with a network statement for the public Signaling IP Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address> mask 255.255.255.255
network <MS Lync/OCS network> mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The SBC private signaling/media address will be translated to a public Signaling IP Address (which is defined as loopback interface on the CER). Continuing the example from section 4.10.2 (assume now that the SBC uses a private IP address), the private SBC signaling/media IP address of 32.21.150.18 will be translated to a public Signaling address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255

interface FastEthernet0/0
 description LAN interface facing the SBC
 ip address 32.21.150.17 255.255.255.248
```

```
 ip nat inside
 duplex full
 speed 100

interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T  VPN
 bandwidth 1459
 ip address 192.33.20.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF

ip nat inside source static 32.21.150.18 135.16.180.66

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

4.15 Microsoft Lync Server 2010 with AudioCodes SBC

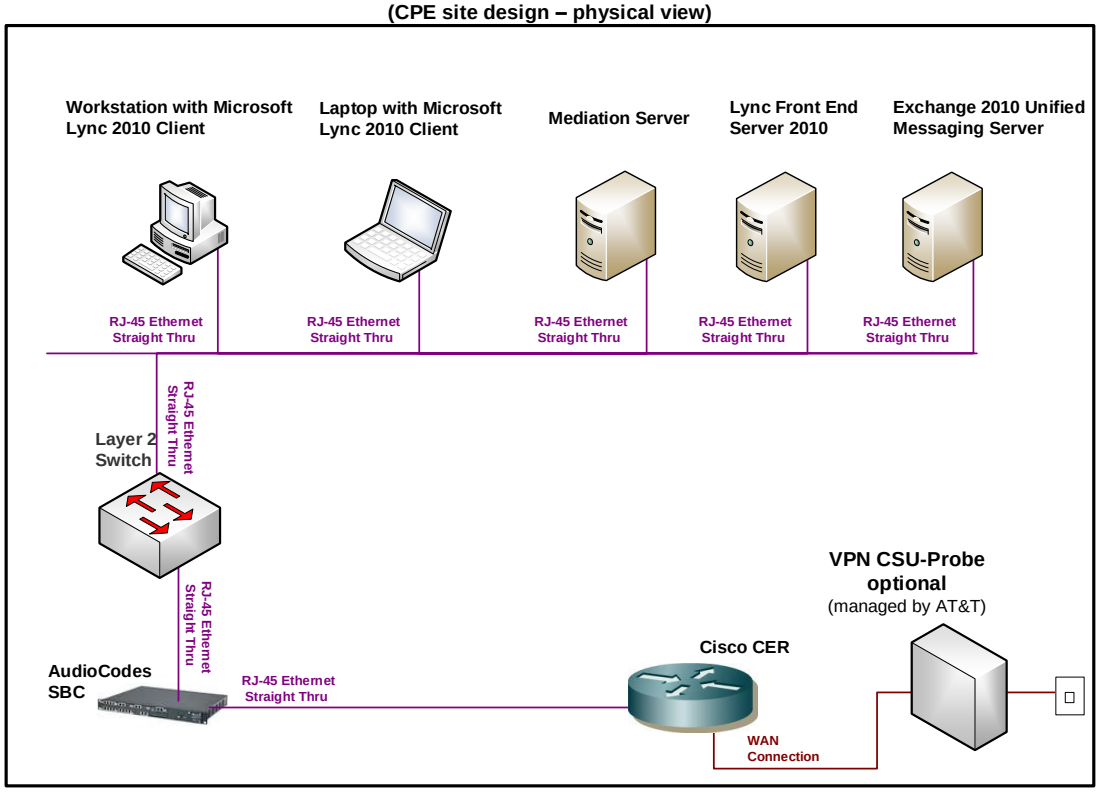
The Microsoft Lync Server 2010 solution can work in conjunction with a cascaded AudioCodes SBC (see appropriate CCG for Lync and AudioCodes configurations). Voice and signaling traffic will be sourced from a LAN interface on the AudioCodes SBC.

4.15.1 Topology

Following is a sample diagram of a network topology for a site with Microsoft Lync Server 2010 and AudioCodes SBC. The AT&T VPN CSU-Probe are AT&T managed device.

- The AT&T VPN CSU-Probe is optional. All other equipment is managed by the customer.
- G.711 is the only supported codec
- Fax is not supported.
- Only access speeds of full T1 and greater will be supported with this solution.

AT&T BVoIP on AT&T VPN site
with AT&T VPN CSU-Probe, AudioCodes SBC, MS Lync 2010 Server
(CPE site design – physical view)



4.15.2 Standard Solution

Step 1: Configure LAN interface facing AudioCodes SBC

The SIP Signaling/Media address range assigned by AT&T will be used for the network between the CER and AudioCodes SBC. The CER interface (which faces the AudioCodes) will be assigned the AT&T address for media, although it will not be used for media. The AudioCodes interface (which faces the CER) will be assigned the Signaling IP Address. For example, if AT&T assigns 32.21.150.17 as the Media IP Address, this address will be configured on the CER (LAN interface facing the AudioCodes). If AT&T IP assigns 32.21.150.18 as the Signaling IP Address, this address will be configured on the AudioCodes (LAN interface facing the CER).

Note: The IP Address on the AudioCodes interface is the Signaling IP address (used for both signaling and media) and must be the IP Address which has been provisioned as such in the AT&T NETWORK. Note: AT&T prefers to assign the address space for the SIP Signaling/Media, but does offer to use existing customer addressing if required. Using a customer provided address space may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer Lync environment is required for this solution (required for site-to-site calls).

```
ip route <Lync 2010 network> <appropriate subnet> <LAN port of AudioCodes SBC>
```

Step 3: Configure BGP

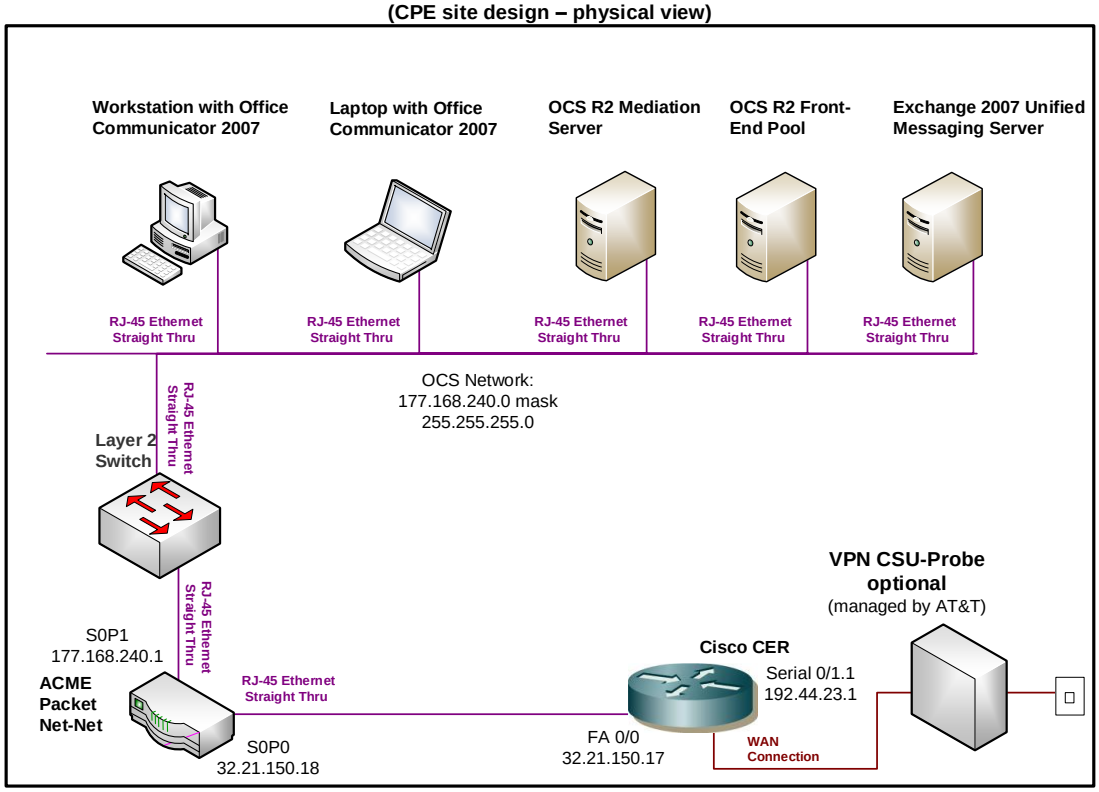
The Signaling IP Address and Lync 2010 network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <Signaling IP Address network> mask 255.255.255.248
network <Lync 2010 network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where Lync 2010 resides. 32.21.150.18 is the LAN address of the AudioCodes SBC interface facing the CER (the Signaling IP Address). 32.21.150.17 is the LAN address of the CER (the Media IP Address).

AT&T BVoIP on AT&T VPN site
with AT&T VPN CSU-Probe, ACME Packet Net-Net, MS OCS
(CPE site design – physical view)



interface FastEthernet0/0

description LAN interface facing AudioCodes
ip address 32.21.150.17 255.255.255.248
duplex full
speed 100

ip route 177.168.240.0 255.255.255.0 32.21.150.18

router bgp 65000
no synchronization
bgp log-neighbor-changes
network 32.21.150.16 mask 255.255.255.248
network 177.168.240.0 mask 255.255.255.0
neighbor 192.44.23.2 remote-as 37383
neighbor 192.44.23.2 allowas-in
no auto-summary

4.15.3 Optional NAT Solution (non-standard configuration)

If the AudioCodes SBC uses a private address for signaling/media, that address may be NAT'd to the public Signaling IP Address on the CER router. However this is not recommended due to degraded CPU performance with NAT enabled.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing AudioCodes SBC

Configure a LAN interface of the CER router for the same network as one of the AudioCodes interfaces.

Step 2: Define loopback interface

Assign the public Signaling IP Address to a loopback interface on the CER.

```
interface Loopback <#>
  ip address  <public Signaling IP Address> 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private AudioCodes signaling/media IP address to the public Signaling IP Address.

```
ip nat inside source static <private signaling/media IP address> <public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside: statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the AudioCodes SBC.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing AudioCodes
 ip address <ip address> <mask>
 ip nat inside

interface WAN #  **Always use subinterface when available**
 description WAN interface facing AT&T  VPN
```

```
ip address <ip address> <mask>
ip nat outside
```

Step 5: Configure Static Routes

A static route is required for the Lync 2010 network. The route will point to the AudioCodes SBC (private signaling/media IP address).

```
ip route <Lync network> <appropriate subnet> <private signaling/media IP address>
```

Step 6: Configure BGP

The Signaling IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private AudioCodes signaling/media IP address). The CER will need to be configured with a network statement for the public Signaling IP Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address > mask 255.255.255.255
network <Lync network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The AudioCodes private signaling/media IP address will be translated to a public Signaling IP Address (which is defined as loopback interface on the CER). Continuing the example from section 4.11.2 (assuming now that the AudioCodes uses a private IP address), the AudioCodes private signaling/media address of 32.21.150.18 will be translated to a public Signaling IP Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255


interface FastEthernet0/0
 description LAN interface facing AudioCodes
 ip address 32.21.150.17 255.255.255.248
 ip nat inside
```

```
 duplex full
 speed 100

interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T  VPN
 bandwidth 1459
 ip address 192.33.20.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF

ip nat inside source static 32.21.150.18 135.16.180.66

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

4.16 ShoreTel IP-PBX with Ingate Session Border Controller (SBC)

The ShoreTel solution works in conjunction with an Ingate SBC (see appropriate CCG for this configuration).

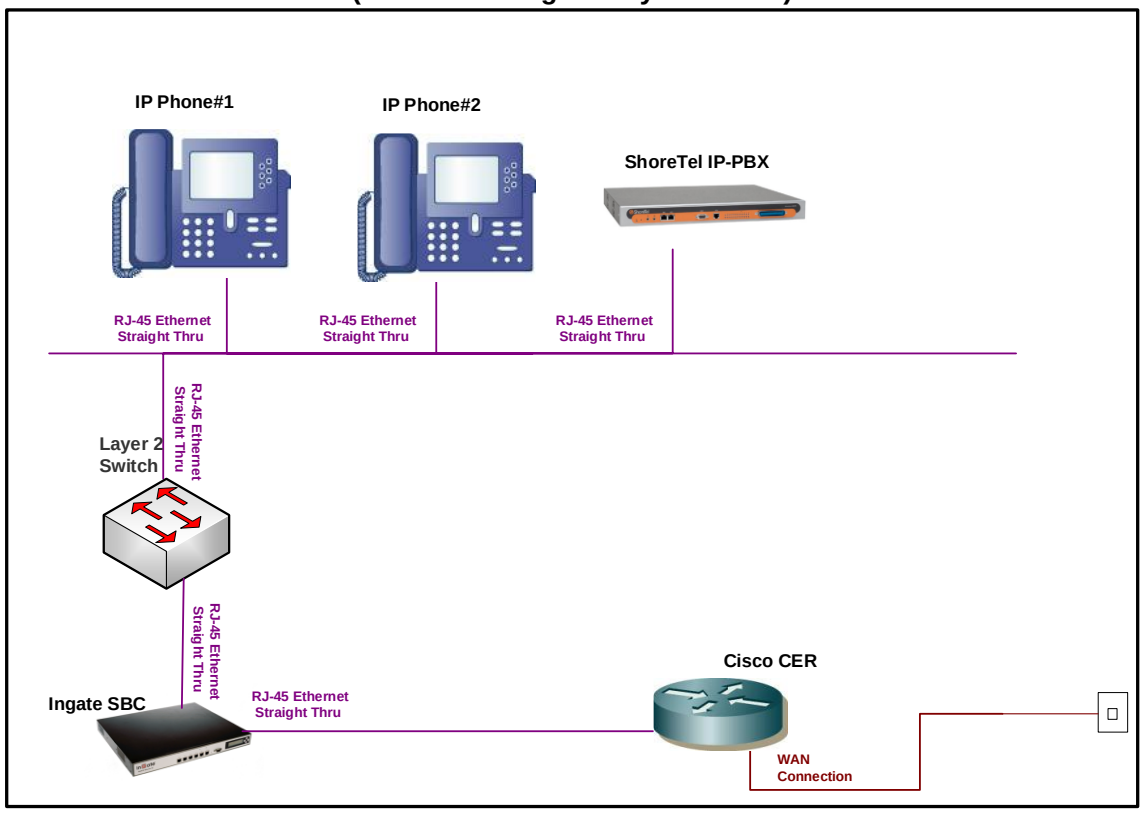
4.16.1 Topology

Following is a sample diagram of a network topology for a site with a Shoretel IP-PBX and an Ingate SBC. In this design, the CER and Ingate SBC are two separate devices. The AT&T VPN CSU-Probe is a AT&T managed device.

Note:

- The AT&T VPN CSU-Probe is optional.

AT&T BVoIP AT&T VPN Site with ShoreTel and Ingate SBC
(CPE Site Design – Physical view)



4.16.2 Standard Solution

The Ingate LAN interface (facing the CER) will be configured with the Signaling IP Address. Note: the Ingate LAN interface provisioned for signaling will also be used for the media traffic. Therefore, all voice and signaling traffic destined for AT&T will be sourced from a single LAN interface on the Ingate. The Media IP Address (assigned to you in the *Customer Router Configuration Shipping/Confirmation* letter*)* will be used to configure the CER LAN interface (facing the Ingate SBC) although it is not actually used for media traffic.

Step 1: Configure LAN interface facing Ingate SBC

The CER interface which faces the Ingate will be assigned the Media IP Address and the Ingate interface which faces the CER will be assigned the Signaling IP Address. For example, if AT&T assigns a Media IP Address of 32.21.150.17, then that address will be configured on the CER LAN interface facing the Ingate. If AT&T assigns a Signaling IP Address of 32.21.150.18, then that address will be configured on the Ingate LAN interface facing the CER.

Note: The IP Address on the Ingate interface is the assigned Signaling IP Address (although it is used for media as well) and must be the IP Address which has been provisioned as such in the AT&T NETWORK. Note: AT&T prefers to assign the address space for the SIP Signaling/Media, but does offer to use existing customer addressing if required. Using a customer provided address space may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer voice network is required for site-to-site calls.

```
ip route <customer voice network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

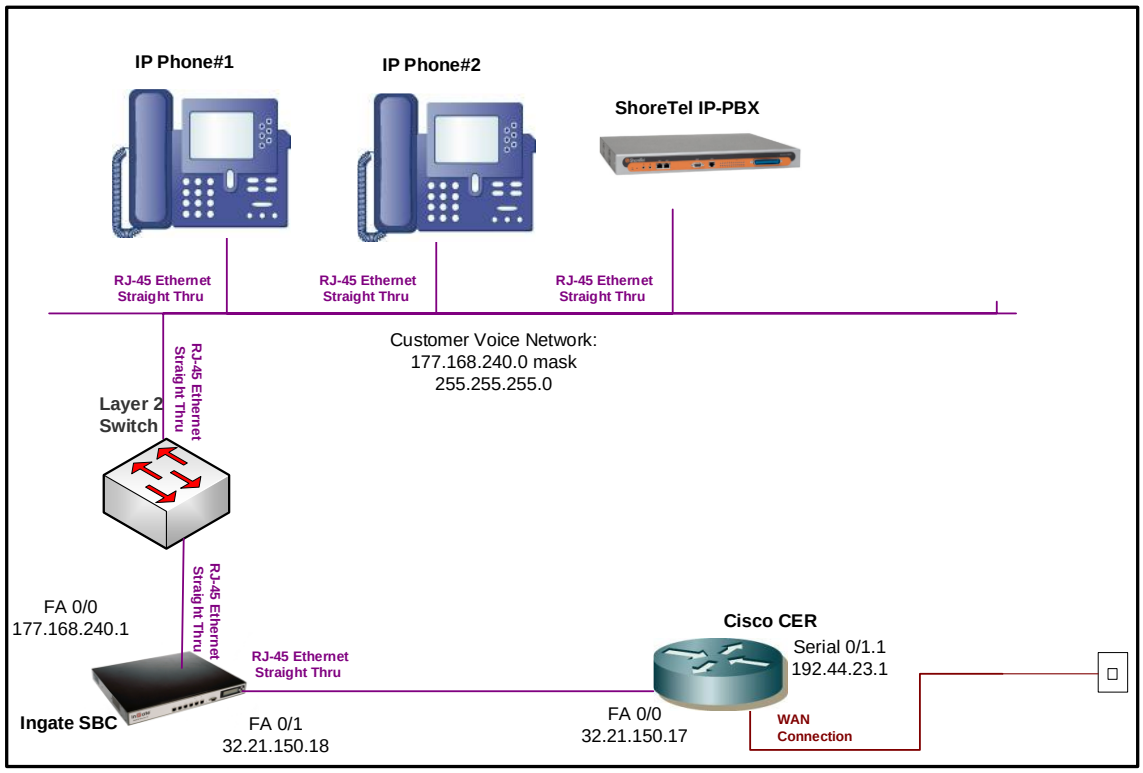
The Signaling IP Address and voice network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

```
router bgp <your AS number>
no synchronization

bgp log-neighbor-changes
network <Signaling IP Address network> mask 255.255.255.248
network <customer voice network > mask <use  appropriate mask>

neighbor <PER IP address>  remote-as  <remote AS>
neighbor <PER IP address>  allowas-in
no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where the ShoreTel IP-PBX resides. The 32.21.150.18 is the LAN address of the Ingate SBC facing the CER (this is the Signaling IP Address – which will also be used for media). The 32.21.150.17 is the LAN address of the CER (this is the Media IP Address – although it is not actually used for media).

AT&T BVoIP on AT&T VPN Site with ShoreTel IP-PBX and Ingate SBC
(CPE Site Design – Physical view)



interface FastEthernet0/0

description LAN interface facing Ingate SBC

ip address 32.21.150.17 255.255.255.248

duplex full

speed 100

ip route 177.168.240.0 255.255.255.0 32.21.150.18
router bgp 65000
no synchronization
bgp log-neighbor-changes
network 32.21.150.16 mask 255.255.255.248
network 177.168.240.0 mask 255.255.255.0
neighbor 192.44.23.2 remote-as 37383
neighbor 192.44.23.2 allowas-in
no auto-summary

4.16.3 Optional NAT Solution (non-standard configuration)

If the Ingate SBC uses a private Signaling/Media IP Address, then that address must be NAT'd to a public Signaling IP Address on the CER. However this is not recommended due to degraded CPU performance with NAT enabled.

The CER loopback interface used for NAT will be configured with the public Signaling IP Address. The CER loopback interface will also be used for the media traffic. Therefore all voice and signaling traffic will be sourced from a single loopback interface on the CER.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing Ingate SBC

Configure a LAN interface on the CER for the same network as one of the Ingate SBC interfaces.

Step 2: Define Loopback Interface

Assign the public Signaling IP Address to a loopback interface on the CER (this same address will also be used for media).

```
interface Loopback <#>
  ip address  <Signaling IP Address> 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private signaling/media IP address to the public Signaling IP Address (the same address will also be used for media).

```
ip nat inside source static <private Signaling/Media IP Address> <public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside: statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the Ingate SBC.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing Ingate SBC
 ip address <ip address> <mask>
 ip nat inside


interface WAN #  **Always use subinterface when available**
 description WAN interface facing AVPN
 ip address <ip address> <mask>
 ip nat outside
```

Step 5: Configure Static Routes

A static route is required for the customer voice network. The route will point at the Ingate SBC.

```
ip route <customer voice network> <appropriate subnet> <private Signaling/Media IP Address>
```

Step 6: Configure BGP

The public Signaling IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private signaling/media IP address). The CER will need to be configured with a network statement for the public Signaling IP Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address > mask 255.255.255.255
network <customer voice network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The Ingate SBC LAN address (private signaling/media IP address) will be translated to a public Signaling IP Address (which is defined as a loopback interface on the CER). Continuing the example from section 4.4.2 (assume now that the Ingate SBC uses a private signaling/media IP address), the Ingate SBC private signaling/media address of 32.21.150.18 will be translated to a public Signaling IP Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255

interface FastEthernet0/0
```

```
 description LAN interface facing Ingate SBC
 ip address 32.21.150.17 255.255.255.248
 ip nat inside
 duplex full
 speed 100


interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T
 bandwidth 1459
 ip address 192.33.20.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF


ip nat inside source static 32.21.150.18 135.16.180.66


router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

4.17 Siemens OpenScape Voice V5 with Siemens OpenScape SBC V1

The Siemens OpenScape solution can work in conjunction with an OpenScape SBC (see appropriate CCG for OpenScape Voice with OpenScape SBC configurations).

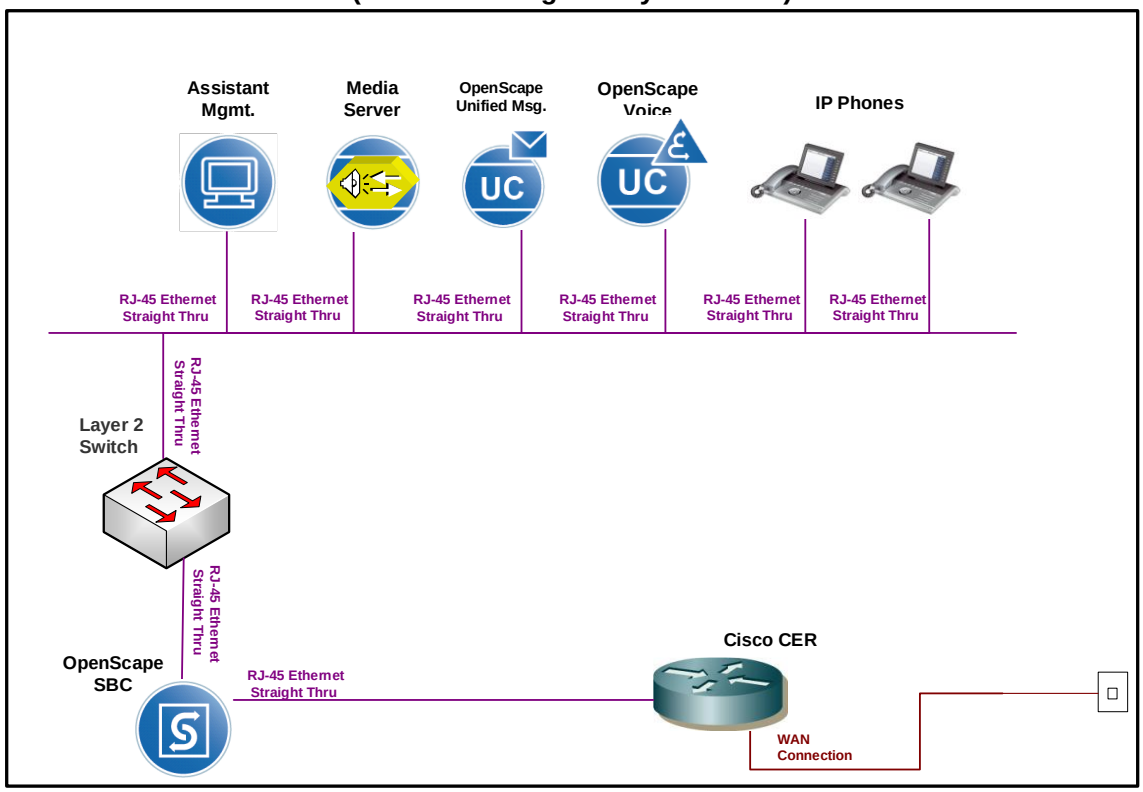
4.17.1 Topology

Following is a sample diagram of a network topology for a site with a Siemens OpenScape Voice and OpenScape SBC. In this design, the CER and OpenScape SBC are two separate devices. The AT&T VPN CSU-Probe is a AT&T managed device.

Note:

- The AT&T VPN CSU-Probe is optional.

AT&T BVoIP on AT&T VPN Site with Siemens OpenScape Voice and Siemens OpenScape SBC
(CPE Site Design – Physical view)



4.17.2 Standard Solution

The OpenScape SBC LAN interface (facing the CER) will be configured with the Signaling IP Address. Note: the OpenScape SBC LAN interface provisioned for signaling will also be used for the media traffic. Therefore, all voice and signaling traffic destined for AT&T will be sourced from a single LAN interface on the OpenScape SBC. The Media IP Address (assigned to you in the *Customer Router Configuration Shipping/Confirmation* letter*)* will be used to configure the CER LAN interface (facing the OpenScape SBC) although it is not actually used for media traffic.

Step 1: Configure LAN interface facing OpenScape SBC

The CER interface which faces the OpenScape SBC will be assigned the Media IP Address and the OpenScape SBC interface which faces the CER will be assigned the Signaling IP Address. For example, if AT&T assigns a Media IP Address of

32.21.150.17, then that address will be configured on the CER LAN interface facing the OpenScape SBC. If AT&T assigns a Signaling IP Address of 32.21.150.18, then that address will be configured on the OpenScape SBC LAN interface facing the CER.

Note: The IP Address on the OpenScape SBC interface is the assigned Signaling IP Address (although it is used for media as well) and must be the IP Address which has been provisioned as such in the AT&T NETWORK. Note: AT&T prefers to assign the address space for the SIP Signaling/Media, but does offer to use existing customer addressing if required. Using a customer provided address space may require the use of NAT (see following section).

Step 2: Configure static route statement

A static route statement to the customer's voice network is required for site-to-site calls.

```
ip route <customer voice network> <appropriate subnet> <Signaling IP Address>
```

Step 3: Configure BGP

The Signaling IP Address and customer voice network must be advertised via BGP network statements. Please note that the Signaling IP Address is advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

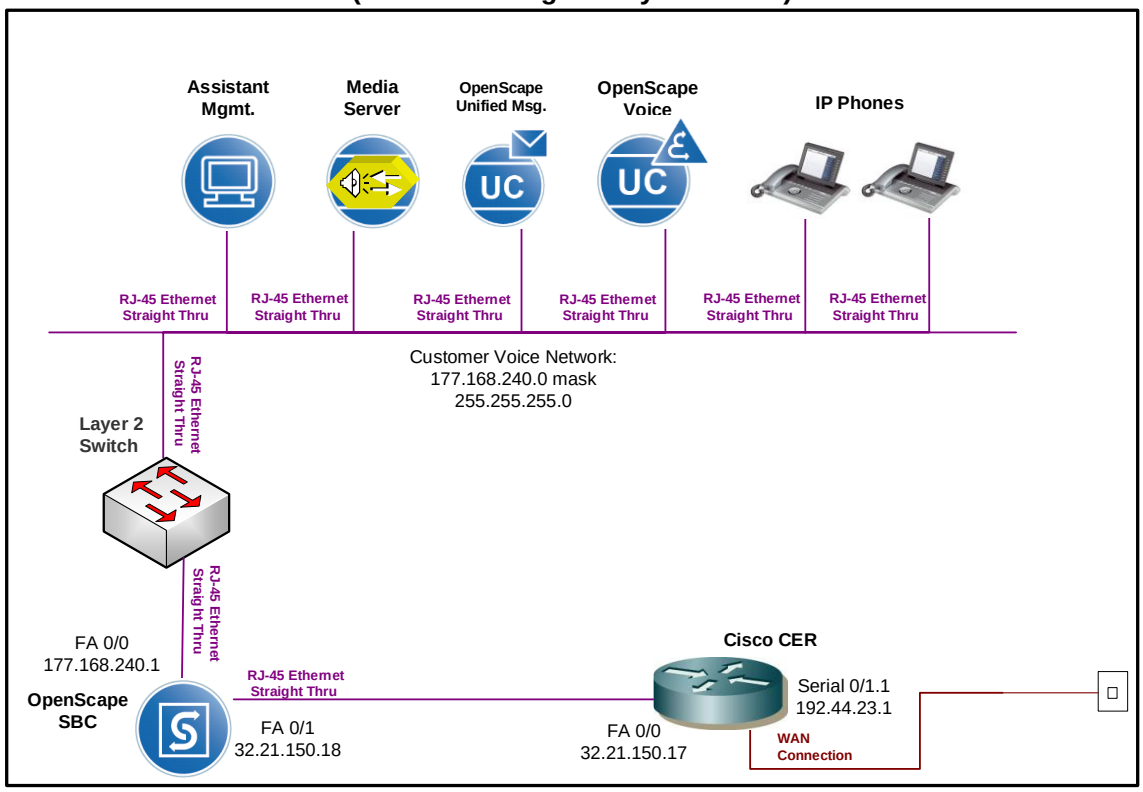
```
router bgp <your AS number>
no synchronization

bgp log-neighbor-changes
network <Signaling IP Address network> mask 255.255.255.248
network <customer voice network > mask <use  appropriate mask>

neighbor <PER IP address>  remote-as  <remote AS>
neighbor <PER IP address>  allowas-in
no auto-summary
```

Example:

In the following example, 177.168.240.0 is the customer voice network where the OpenScape Voice device resides. The 32.21.150.18 is the LAN address of the OpenScape SBC facing the CER (this is the Signaling IP Address – which will also be used for media). The 32.21.150.17 is the LAN address of the CER (this is the Media IP Address – although it is not actually used for media).

AT&T BVoIP on AT&T VPN Site with Siemens OpenScape Voice and Siemens OpenScape SBC

(CPE Site Design – Physical view)



interface FastEthernet0/0

description LAN interface facing OpenScape SBC

ip address 32.21.150.17 255.255.255.248

duplex full

speed 100

ip route 177.168.240.0 255.255.255.0 32.21.150.18
router bgp 65000
no synchronization
bgp log-neighbor-changes
network 32.21.150.16 mask 255.255.255.248
network 177.168.240.0 mask 255.255.255.0
neighbor 192.44.23.2 remote-as 37383
neighbor 192.44.23.2 allowas-in
no auto-summary

4.17.3 Optional NAT Solution (non-standard configuration)

If the OpenScape SBC uses a private Signaling/Media IP Address, then that address must be NAT'd to a public Signaling IP Address on the CER. However, this is not recommended due to degraded CPU performance with NAT enabled.

The CER loopback interface used for NAT will be configured with the public Signaling IP Address. The CER loopback interface will also be used for the media traffic. Therefore all voice and signaling traffic will be sourced from a single loopback interface on the CER.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing OpenScape SBC

Configure a LAN interface on the CER for the same network as one of the OpenScape SBC interfaces.

Step 2: Define Loopback Interface

Assign the public Signaling IP Address to a loopback interface on the CER (this same address will also be used for media).

```
interface Loopback <#>
  ip address  <Signaling IP Address> 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statement to translate the private signaling/media IP address to the public Signaling IP Address (the same address will also be used for media).

```
ip nat inside source static <private Signaling/Media IP Address> <public Signaling IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the "ip nat inside" and "ip nat outside: statements to the appropriate interfaces.

The "**ip nat inside**" statement will be applied to the LAN interface that is facing the OpenScape SBC.

The "**ip nat outside**" statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing OpenScape SBC
 ip address <ip address> <mask>
 ip nat inside


interface WAN #  **Always use subinterface when available**
 description WAN interface facing AVPN
 ip address <ip address> <mask>
 ip nat outside
```

Step 5: Configure Static Routes

A static route is required for the customer voice network. The route will point at the OpenScape SBC device.

```
ip route <customer voice network> <appropriate subnet> <private Signaling/Media IP Address>
```

Step 6: Configure BGP

The public Signaling IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private signaling/media IP address). The CER will need to be configured with a network statement for the public Signaling IP Address.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address > mask 255.255.255.255
network <customer voice network > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The OpenScape SBC LAN address (private signaling/media IP address) will be translated to a public Signaling IP Address (which is defined as a loopback interface on the CER). Continuing the example from section 4.4.2 (assume now that the OpenScape SBC uses a private signaling/media IP address), the OpenScape SBC private signaling/media address of 32.21.150.18 will be translated to a public Signaling IP Address of 135.16.180.66.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255

interface FastEthernet0/0
```

```
description LAN interface facing OpenScape SBC
ip address 32.21.150.17 255.255.255.248
ip nat inside
duplex full
speed 100

interface Serial0/1/0:0.1 point-to-point
description WAN interface facing AT&T
bandwidth 1459
ip address 192.33.20.1 255.255.255.252
ip nat outside
frame-relay class shape1536
frame-relay interface-dlci 239 IETF

ip nat inside source static 32.21.150.18 135.16.180.66

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.180.66 mask 255.255.255.255
network 177.168.240.0 mask 255.255.255.0
neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary

ip route 177.168.240.0 255.255.255.0 32.21.150.18
```

4.18 Mitel 3300 MCD Version 5.0 (without an SBC)

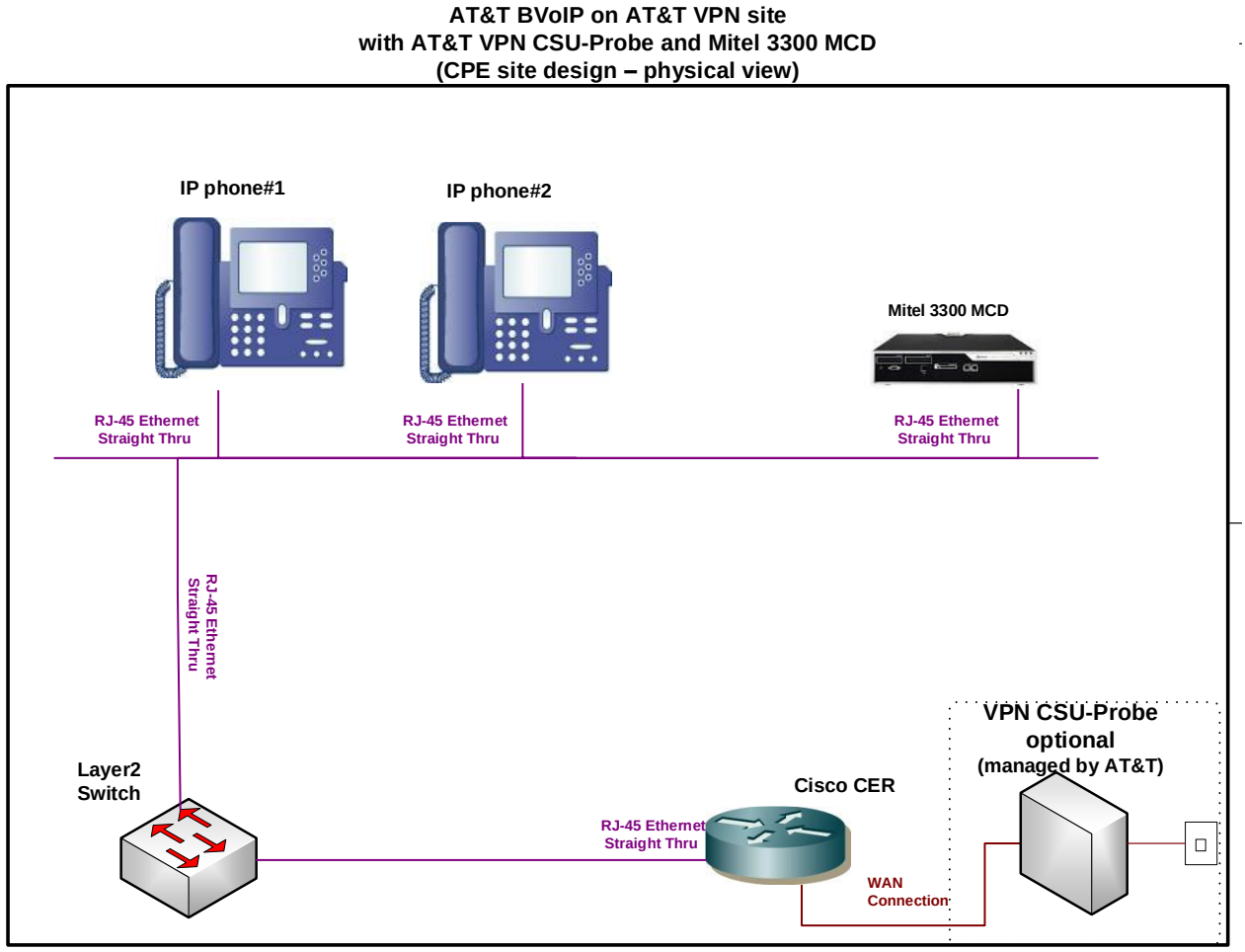
The Mitel 3300 MCD solution is supported without and SBC(see appropriate CCG for IP PBX configurations).

4.18.1 Topology

Following is a sample diagram of a network topology for a site with a Mitel 3300 without a Session Border Controller (SBC). The AT&T VPN CSU-Probe is a AT&T managed devices. Note: The AT&T managed VPN CSU-Probe is optional.

The RTP port range of 50000 – 50511 is used for Media. This is the port range per IP address that is streaming audio. The MCD does not anchor SDP as other CPEs devices

do. RTP is streamed directly to/from the end point in the call. Therefore, the RTP port range in the CER route must be changed to accommodate this.



4.18.2 Standard NAT/PAT Configuration (required)

- The Mitel 3300 must be NAT'd to a registered AT&T IP address (which will be a loopback interface on the CER).
- The IP endpoints (IP Telephones, Soft phones, etc.) must be PAT'd to a different registered loopback interface address (for media traffic).

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing Avaya BCM

Configure a LAN interface of the CER for the same network as the MItel 3300 and phones network.

Step 2: Define loopback interfaces

Define one loopback address for the public Signaling IP Address. This will be the address the Mitel 3300 is NAT'd to.

Define a second loopback address for the public Media IP Address. This will be the address the IP phones are PAT'd to.

```
interface Loopback <X>
  ip address  <public Signaling IP Address – NAT for Mitel 3300 > 255.255.255.255

interface Loopback <Y>
  ip address  <public Media IP Address – PAT for IP phones > 255.255.255.255
```

Step 3: Create NAT/PAT statements

PAT is required for the IP phones. An access list is used to define the addresses eligible for PAT. The Mitel 3300 will have a separate NAT statement.

PAT statement:

```
ip nat inside source list <ACL # > interface LoopbackY overload
access-list <ACL#> permit <Private LAN address space of phones> <appropriate mask>
```

NAT statement:

```
ip nat inside source static <private Signaling IP Address - on Mitel 3300>  <public Signaling IP Address>
```

Step 4: Configure BGP

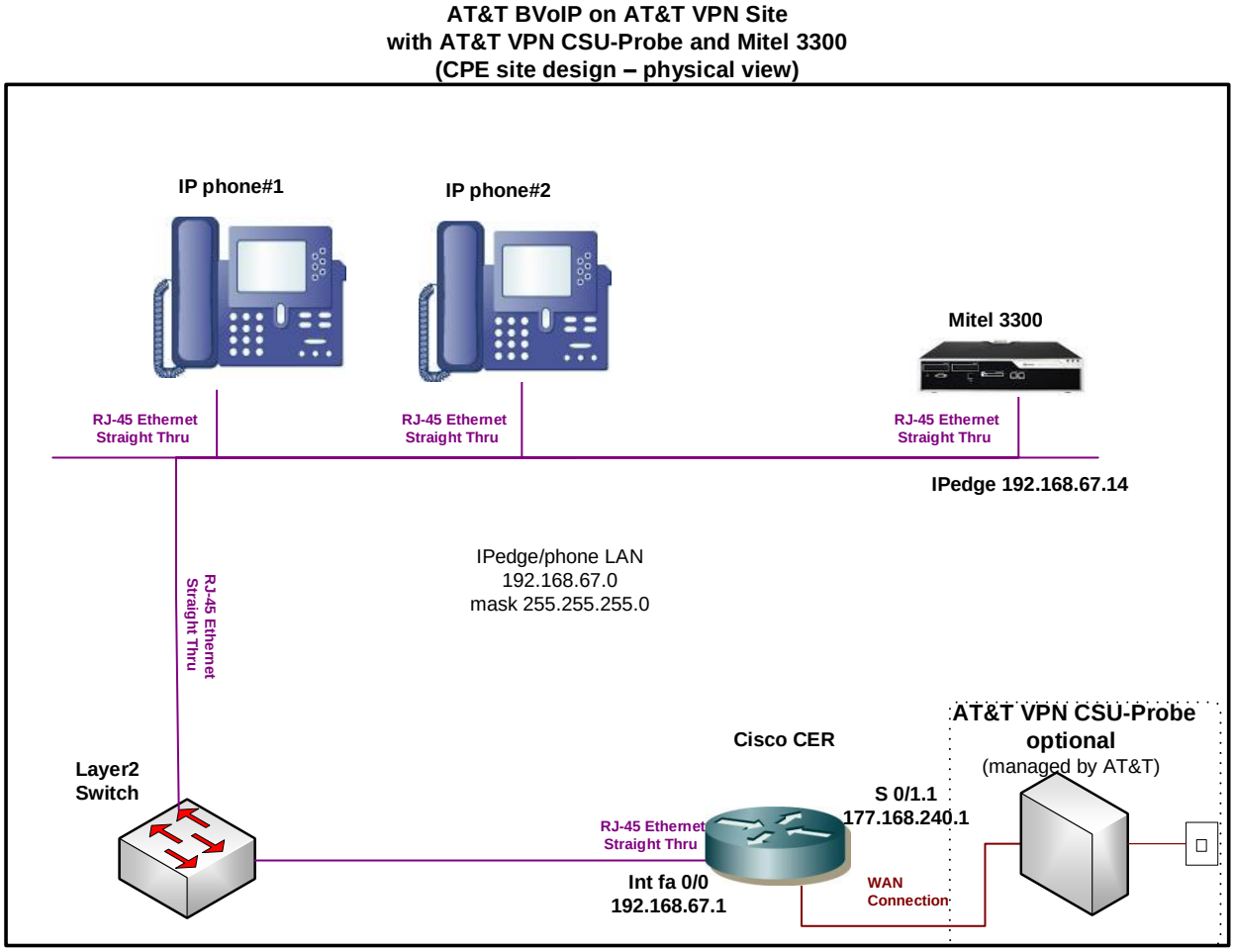
The public Signaling and Media IP Addresses must be distributed to the AT&T network via BGP. The network address of the Mitel 3300 and phones should also be distributed.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address> mask 255.255.255.255
network <public Media IP Address> mask 255.255.255.255
network <Network address of Mitel/phones > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
```

```
no auto-summary
```

Example:

In this example, the Mitel 3300 address is 192.168.67.14




```
interface Loopback6
 ip address 135.16.170.55 255.255.255.255
!
interface Loopback7
 ip address 135.16.170.250 255.255.255.255
!
interface FastEthernet0/0
 description LAN interface facing Mitel 3300
 ip address 192.168.67.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
```

```
 duplex full
 speed 100


interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T VPN
 bandwidth 1459
 ip address 192.166.202.1 255.255.255.252
 ip nat outside
 no ip virtual-reassembly
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF


ip nat inside source list 10 interface Loopback7 overload  (PAT for phones)
ip nat inside source static 192.168.67.30 135.16.170.55      (NAT for Mitel 3300)


access-list 10 permit 192.168.67.0 0.0.0.255  (Allow LAN address space of phones)


router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.170.55 mask 255.255.255.255
network 135.16.170.250 mask 255.255.255.255
network 192.168.67.0 mask 255.255.255.0
neighbor 177.168.240.2  remote-as  37383
neighbor 177.168.240.2  allowas-in
 no auto-summary
```

4.19 Toshiba IPedge Release 1.0 (without an SBC)

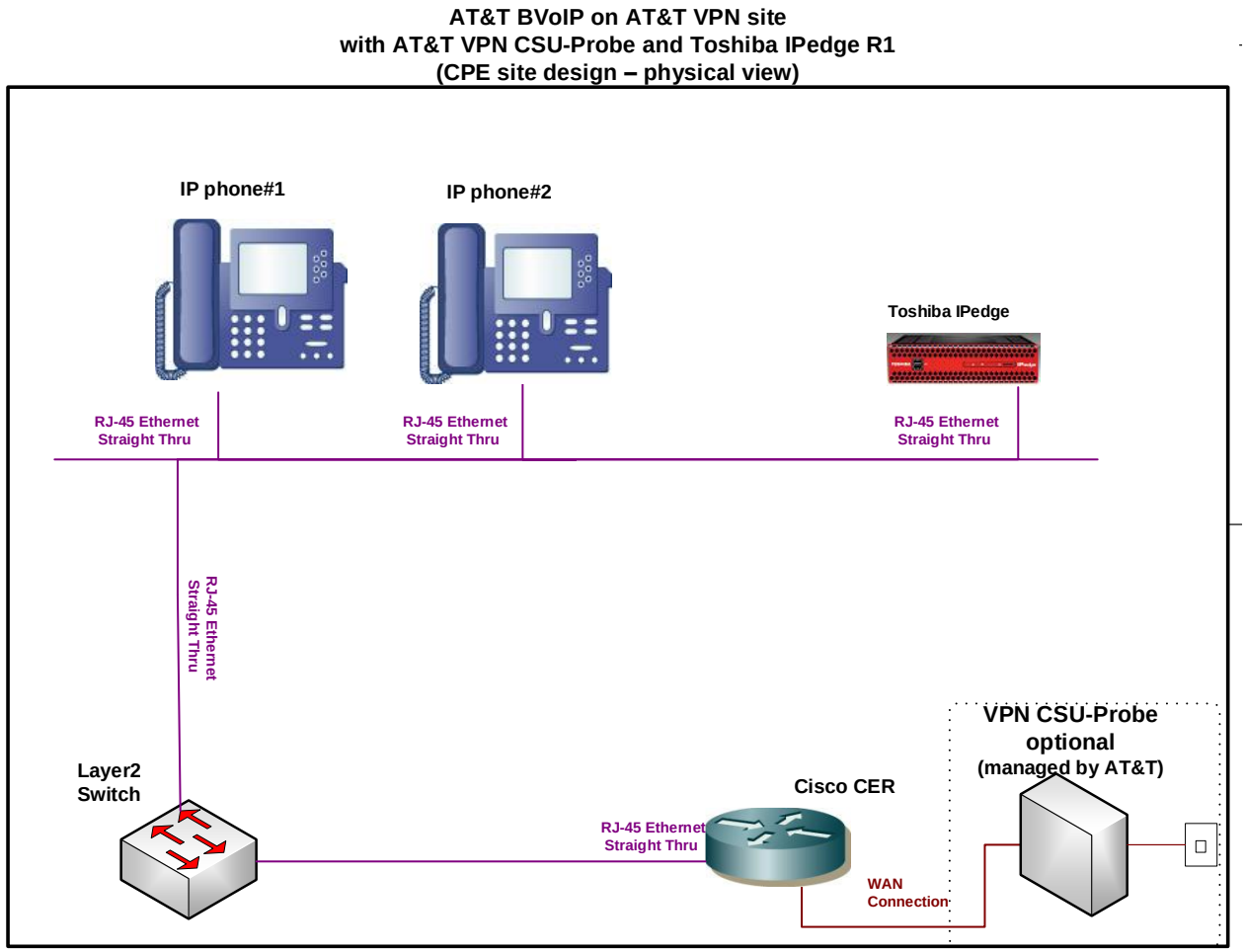
The Toshiba IPedge solution is supported (see appropriate CCG for IP PBX configurations).

4.19.1 Topology

Following is a sample diagram of a network topology for a site with a Toshiba IPedge device without a Session Border Controller (SBC). The AT&T VPN CSU-Probe is a AT&T managed device. Note: The AT&T managed VPN CSU-Probe is optional.

When using the AT&T VPN transport, a 30 byte payload with the G.729 CODEC is recommended for the maximum number of concurrent calls. This is especially

important with international customers using low bandwidth circuits. IPedge does not support a 30 byte payload in both directions for any call scenarios, even when configured as such. Asymmetric payload size will **not** adversely affect call quality, but must be taken into consideration when calculating the maximum number of concurrent calls on a given circuit based on the bandwidth per call calculation.



4.19.2 Standard NAT/PAT Configuration (required)

- The IPedge must be NAT'd to a registered AT&T IP address (which will be a loopback interface on the CER).
- The IP endpoints (IP Telephones, Soft phones, etc.) must be PAT'd to a different registered loopback interface address (for media traffic).

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing Avaya BCM

Configure a LAN interface of the CER for the same network as the IPedge and phones network.

Step 2: Define loopback interfaces

Define one loopback address for the public Signaling IP Address. This will be the address the IPedge is NAT'd to.

Define a second loopback address for the public Media IP Address. This will be the address the IP phones are PAT'd to.

```
interface Loopback <X>
  ip address  <public Signaling IP Address – NAT for IPedge > 255.255.255.255

interface Loopback <Y>
  ip address  <public Media IP Address – PAT for IP phones > 255.255.255.255
```

Step 3: Create NAT/PAT statements

PAT is required for the IP phones. An access list is used to define the addresses eligible for PAT. The IPedge will have a separate NAT statement.

PAT statement:

```
ip nat inside source list <ACL # > interface LoopbackY overload
access-list <ACL#> permit <Private LAN address space of phones> <appropriate mask>
```

NAT statement:

```
ip nat inside source static <private Signaling IP Address - on IPedge>  <public Signaling IP Address>
```

Step 4: Configure BGP

The public Signaling and Media IP Addresses must be distributed to the AT&T network via BGP. The network address of the IPedge and phones should also be distributed.

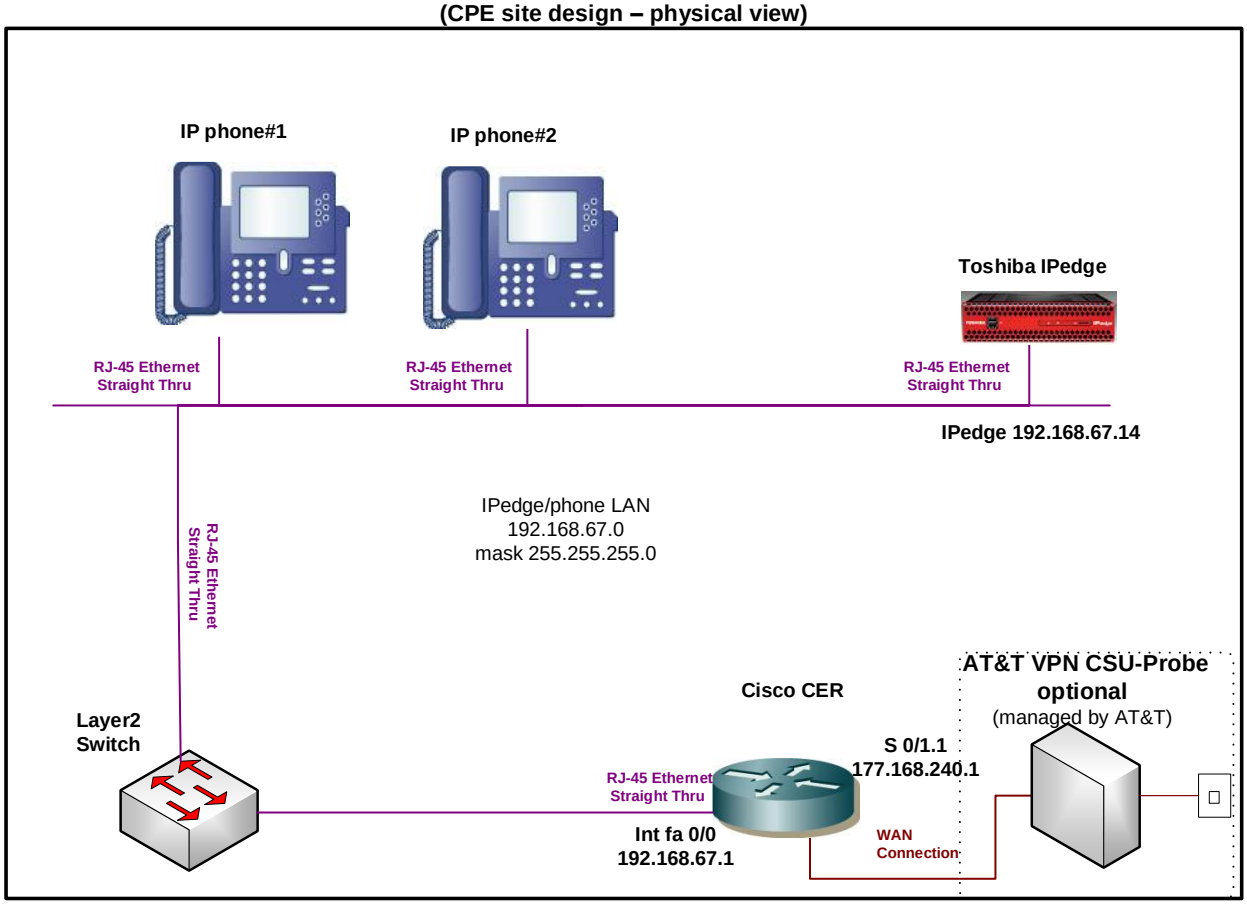
```
router bgp <your AS number>
no synchronization
```

```
 bgp log-neighbor-changes
network <public Signaling IP Address> mask 255.255.255.255
network <public Media IP Address> mask 255.255.255.255
network <Network address of IPedge/phones > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

In this example, the IPedge address is 192.168.67.14

AT&T BVoIP on AT&T VPN Site
with AT&T VPN CSU-Probe and Toshiba IPedge
(CPE site design – physical view)




```
interface Loopback6
 ip address 135.16.170.55 255.255.255.255
!
interface Loopback7
 ip address 135.16.170.250 255.255.255.255
!
interface FastEthernet0/0
```

```
 description LAN interface facing IPedge
 ip address 192.168.67.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex full
 speed 100

interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T VPN
 bandwidth 1459
 ip address 192.166.202.1 255.255.255.252
 ip nat outside
 no ip virtual-reassembly
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF

ip nat inside source list 10 interface Loopback7 overload  (PAT for phones)
ip nat inside source static 192.168.67.30 135.16.170.55      (NAT for IPedge)

access-list 10 permit 192.168.67.0 0.0.0.255  (Allow LAN address space of phones)

router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.170.55 mask 255.255.255.255
network 135.16.170.250 mask 255.255.255.255
network 192.168.67.0 mask 255.255.255.0
neighbor 177.168.240.2  remote-as  37383
neighbor 177.168.240.2  allowas-in
 no auto-summary
```

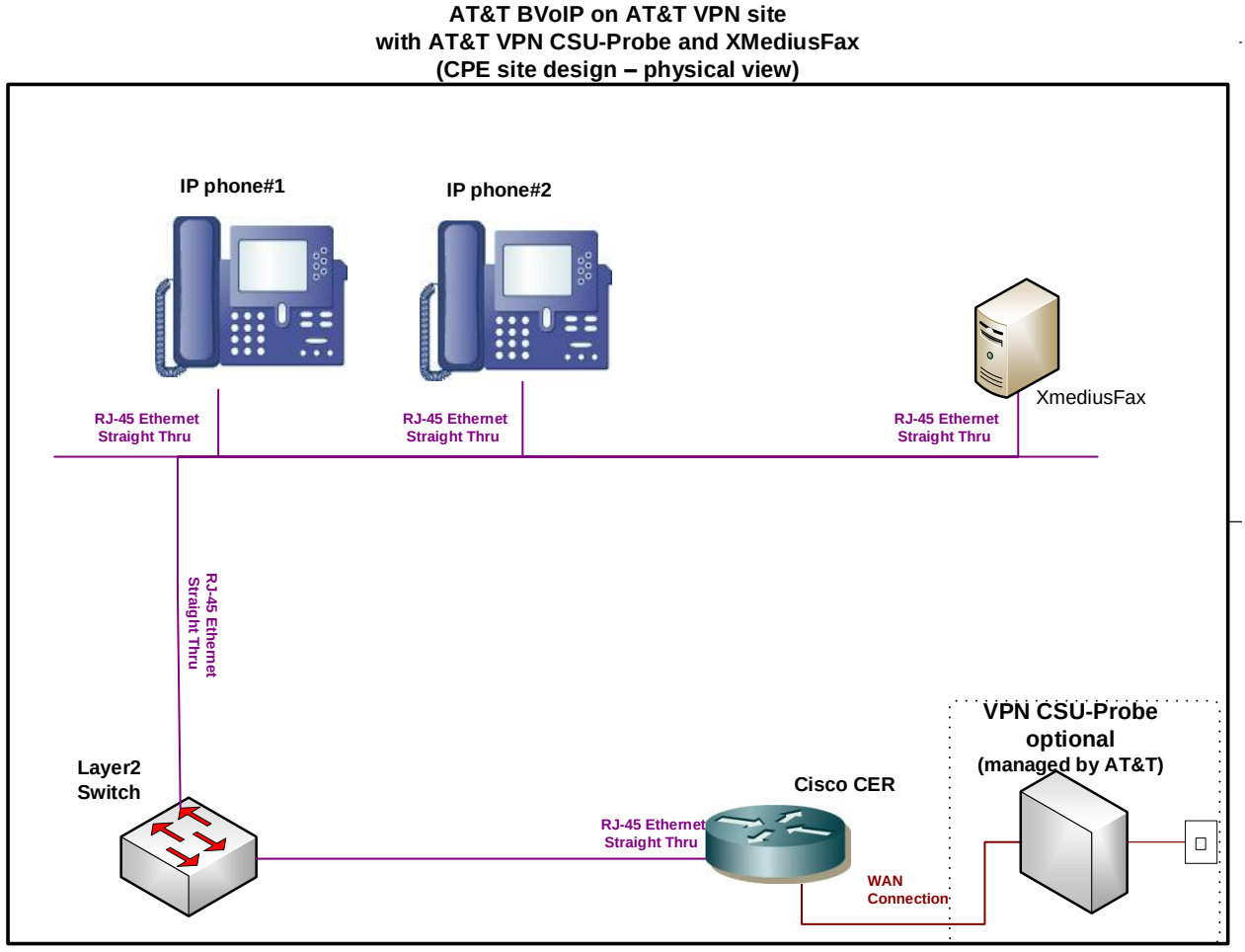
4.20 **Sagemcom XMediusFax (without an SBC)**

The Sagemcom XMediusFax solution is supported (see appropriate CCG for IP PBX configurations).

4.20.1 Topology

Following is a sample diagram of a network topology for a site with a Sagemcom XMediusFax device without a Session Border Controller (SBC). The AT&T VPN CSU-Probe is a AT&T managed device. Note: The AT&T managed VPN CSU-Probe is optional.

When using the AT&T VPN transport, a 30 byte payload with the G.729 CODEC is recommended for the maximum number of concurrent calls. This is especially important with international customers using low bandwidth circuits. Asymmetric payload size will **not** adversely affect call quality, but must be taken into consideration when calculating the maximum number of concurrent calls on a given circuit based on the bandwidth per call calculation.



4.20.2 Standard NAT Configuration (required)

- The Sagemcom XMediusFax must be NAT'd to a registered AT&T IP address (which will be a loopback interface on the CER).

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing XMediusFax

Configure a LAN interface of the CER for the same network as the Sagemcom XMediusFax and phones network.

Step 2: Define loopback interfaces

Define one loopback address for the public Signaling IP Address. This will be the address the Sagemcom XMediusFax is NAT'd to.

```
interface Loopback <X>
  ip address  <public Signaling IP Address – NAT for XMediusFax > 255.255.255.255
```

Step 3: Create NAT statements

The Sagemcom XMediusFax will have a separate NAT statement.

NAT statement:

```
ip nat inside source static <private Signaling IP Address - on XMediusFax>  <public Signaling IP Address>
```

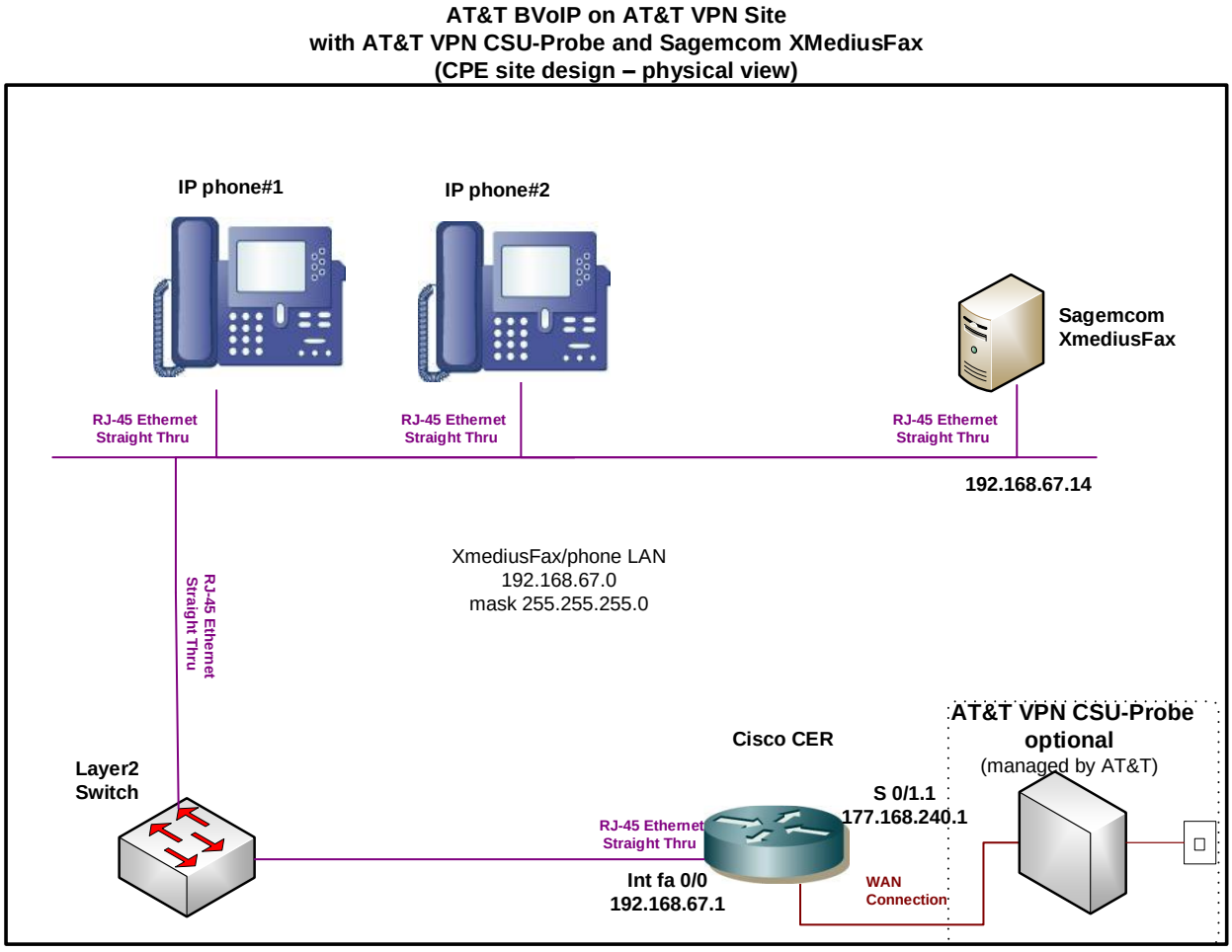
Step 4: Configure BGP

The public Signaling and Media IP Addresses must be distributed to the AT&T network via BGP. The network address of the Sagemcom XMediusFax and phones should also be distributed.

```
router bgp <your AS number>
no synchronization
 bgp log-neighbor-changes
network <public Signaling IP Address> mask 255.255.255.255
network <Network address of XMediusFax /phones > mask <use  appropriate mask>
neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

In this example, the Sagemcom XMediusFax address is 192.168.67.14




```
interface Loopback6
 ip address 135.16.170.55 255.255.255.255
!
interface FastEthernet0/0
 description LAN interface facing Sagemcom XMediusFax
 ip address 192.168.67.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex full
 speed 100


interface Serial0/1/0:0.1 point-to-point
```

```
description WAN interface facing AT&T VPN
bandwidth 1459
ip address 192.166.202.1 255.255.255.252
ip nat outside
no ip virtual-reassembly
frame-relay class shape1536
frame-relay interface-dlci 239 IETF


ip nat inside source static 192.168.67.30 135.16.170.55      (NAT for Sagemcom XMediusFax)
router bgp 65000
no synchronization
 bgp log-neighbor-changes
network 135.16.170.55 mask 255.255.255.255
network 135.16.170.250 mask 255.255.255.255
network 192.168.67.0 mask 255.255.255.0
neighbor 177.168.240.2  remote-as  37383
neighbor 177.168.240.2  allowas-in
 no auto-summary
```

4.21 Voxeo Prophecy Release 11 with Communigate SIP Proxy

The Voxeo Prophecy SBC solution works in conjunction with a Communigate SIP Proxy (see appropriate CCG from Voxeo for this configuration). This solution will require the customer to have an AT&T VPN circuit installed at the Voxeo data center, rather than at the customer site.

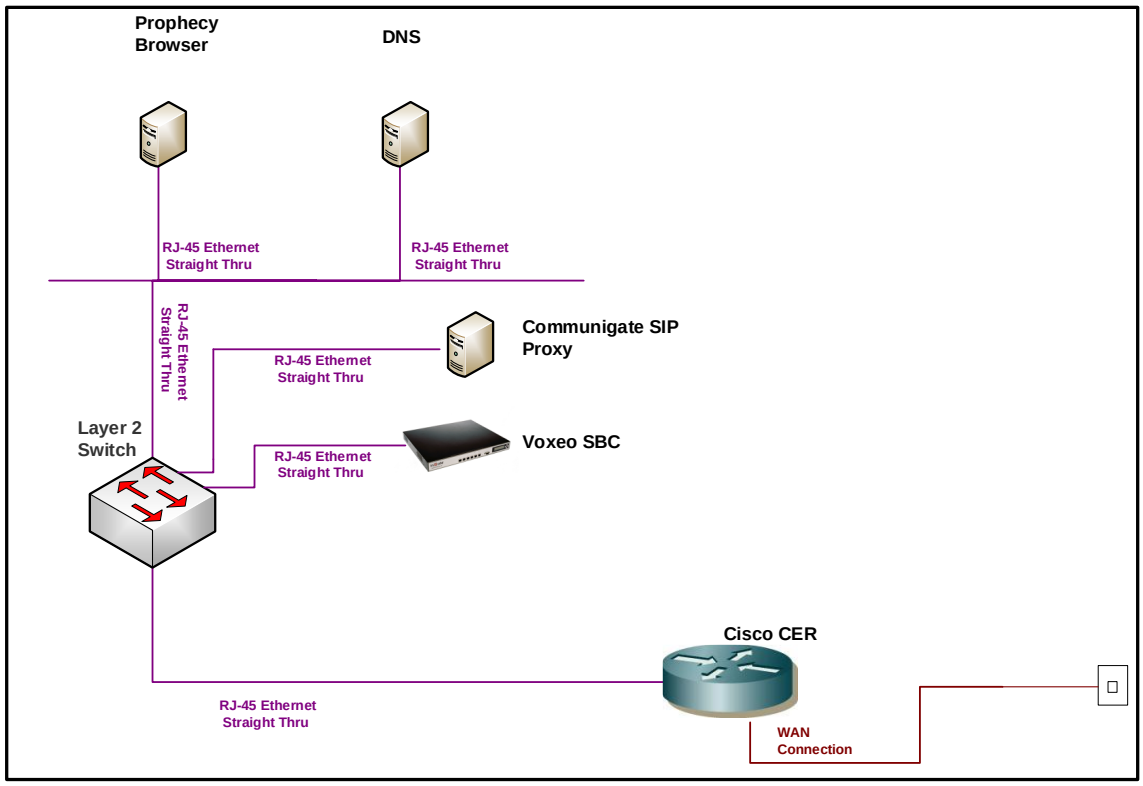
4.21.1 Topology

Following is a sample diagram of a network topology for a site with a Voxeo Prophecy SBC and a Communigate SIP Proxy. In this design, the CER, Prophecy SBC and Communigate SIP Proxy all connect to the same network switch.

Note:

- The CER and SBC are all connected to a network switch.
- The AT&T VPN CSU-Probe is optional.

AT&T BVoIP AT&T VPN Site with Voxeo SBC and Communigate SIP Proxy
(CPE Site Design – Physical view)



4.21.2 Standard Solution

The Communigate SIP Proxy LAN interface will be configured with the Signaling IP Address. The Voxeo SBC LAN interface will be configured with the Media IP Address. The third available host IP address in the AT&T provided network (assigned to you in the *Customer Router Configuration Shipping/Confirmation* letter*)* will be used to configure the CER LAN interface.

Step 1: Configure LAN interface facing customer network

The CER interface which faces the customer network will be assigned the third host IP address, and the SIP Proxy and SBC will be assigned the Signaling IP Address and Media IP Address, respectively. For example, if AT&T assigns a Media IP Address of 32.21.150.17 and Signaling IP Address of 32.21.150.18, the CER LAN interface will be assigned 32.21.150.**19**.

- Media IP Address assigned to Voxeo SBC (32.21.150.**17**)
- Signaling IP Address assigned to Communigate SIP Proxy (32.21.150.**18**)

- CER LAN interface assigned third available host (32.21.150.**19**)

Note: AT&T prefers to assign the address space for the SIP Signaling/Media, but does offer to use existing customer addressing if required. Using a customer provided address space may require the use of NAT (see following section).

Step 4: Configure BGP

The Signaling IP Address and Media IP Address must be advertised via BGP network statements. Please note that the Signaling IP Address and Media IP Address are advertised with a single network statement. This statement is derived by subtracting one from the assigned Media IP Address. For example, if a Media IP Address of 32.21.150.17 is provided, the network statement will use 32.21.150.**16**. The network mask for this network statement will be 255.255.255.248.

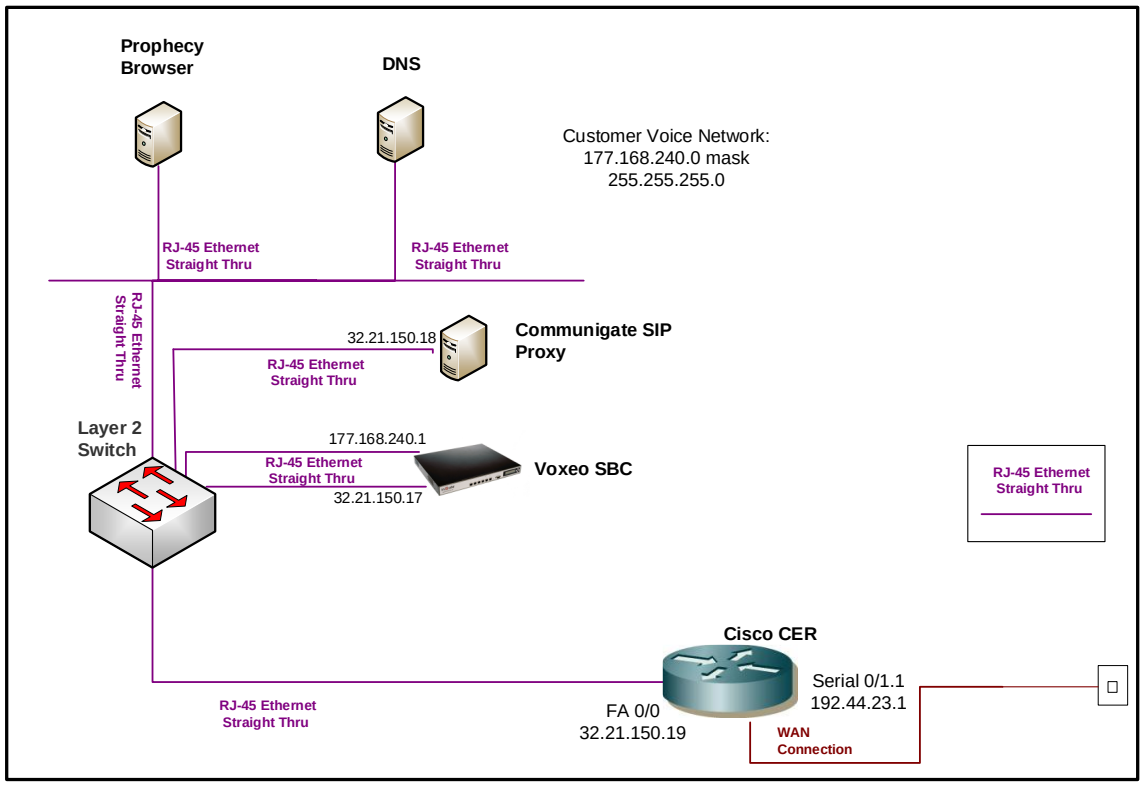
```
router bgp <your AS number>
no synchronization

bgp log-neighbor-changes
network <Signaling IP Address network> mask 255.255.255.248
neighbor <PER IP address>  remote-as  <remote AS>
neighbor <PER IP address>  allowas-in
no auto-summary
```

Example:

In the following example, 177.168.240.0 is the network where the customer network resides. 32.21.150.17 is the LAN address of the Voxeo SBC, 32.21.150.18 is the LAN address of the SIP Proxy interface facing the CER (this is the Signaling IP Address), and 32.21.150.19 is the LAN address of the CER.

AT&T BVoIP AT&T VPN Site with Voxeo SBC and Communigate SIP Proxy

(CPE Site Design – Physical view)




```
interface FastEthernet0/0
 description LAN interface facing customer SBC
 ip address 32.21.150.19 255.255.255.248
 duplex full
 speed 100

router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 network 32.21.150.16  mask 255.255.255.248
 neighbor 192.44.23.2  remote-as  37383
 neighbor 192.44.23.2  allowas-in
 no auto-summary
```

4.21.3 Optional NAT Solution (non-standard configuration)

If the SBC and SIP Gateway use a private Signaling and Media IP Address, then these addresses must be NAT'd to the public Signaling and public Media IP Addresses on the

CER. However this is not recommended due to degraded CPU performance with NAT enabled.

The CER loopback interfaces used for NAT will be configured with the public Signaling and public Media IP Addresses. All voice and signaling traffic will be sourced from two separate loopback interfaces on the CER.

NOTE: NAT and/or PAT of the signaling and media addresses is not supported with Cisco ASR routers running Cisco IOS-XE Release 2.4.3 (IOS 12.2.33XND3).

Step 1: Configure LAN interface facing the SBC

Configure a LAN interface on the CER for the same network as one of the SBC interfaces.

Step 2: Define Loopback Interfaces

Assign the public Signaling IP Address and public Media IP Address to loopback interfaces on the CER.

```
interface Loopback <#>
  ip address  <Signaling IP Address> 255.255.255.255
interface Loopback <#>
  ip address  <Media IP Address> 255.255.255.255
```

Step 3: Create NAT statement

Next, define the static NAT statements to translate the private signaling and media IP addresses to the public Signaling IP Address and public Media IP Address.

```
ip nat inside source static <private Signaling IP Address> <public Signaling IP Address>
ip nat inside source static <private Media IP Address> <public Media IP Address>
```

Step 4 : Define the NAT inside and outside interfaces

Apply the “ip nat inside” and “ip nat outside: statements to the appropriate interfaces.

The “**ip nat inside**” statement will be applied to the LAN interface that is facing the Ingate SBC.

The “**ip nat outside**” statement will be applied to the appropriate WAN interface.

```
interface LAN #
 description LAN interface facing the SBC
 ip address <ip address> <mask>
 ip nat inside


interface WAN #  **Always use subinterface when available**
 description WAN interface facing AVPN
 ip address <ip address> <mask>
 ip nat outside
```

Step 5: Configure BGP

The public Signaling IP Address and Public Media IP Address must be distributed to the AT&T network via BGP (you will **not** need to redistribute the private signaling/media IP address). The CER will need to be configured with a network statement for the public Signaling IP Address and public Media IP Address as shown below.

```
router bgp <your AS number>
 no synchronization
 bgp log-neighbor-changes
 network <public Signaling IP Address > mask 255.255.255.255
 network <public Media IP Address > mask 255.255.255.255
 neighbor <PER IP address>  remote-as  <remote AS>
 neighbor <PER IP address>  allowas-in
 no auto-summary
```

Example:

Following is an example of a NAT configuration on the CER. The SBC LAN IP address will be translated to a public Media IP Address (which is defined as a loopback interface on the CER). The SIP Proxy LAN IP Address will be translated to the public Signaling IP Address (also defined as a loopback interface on the CER). Continuing the example from section 4.19.2 (assume now that the SBC uses a private media IP address and the SIP Proxy uses a private signaling IP address), the SBC private media IP address of 32.21.150.17 will be translated to a public Media IP Address of 135.16.180.66 and the SIP Proxy private signaling IP address of 32.21.150.18 will be translated to the public Signaling IP address of 135.16.180.67.

```
interface Loopback6
 ip address 135.16.180.66 255.255.255.255

interface Loopback7
 ip address 135.16.180.67 255.255.255.255
```

```
interface FastEthernet0/0
 description LAN interface facing the SBC
 ip address 32.21.150.19 255.255.255.248
 ip nat inside
 duplex full
 speed 100

interface Serial0/1/0:0.1 point-to-point
 description WAN interface facing AT&T
 bandwidth 1459
 ip address 192.33.20.1 255.255.255.252
 ip nat outside
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF

ip nat inside source static 32.21.150.17 135.16.180.66
ip nat inside source static 32.21.150.18 135.16.180.67


router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 network 135.16.180.66 mask 255.255.255.255
 network 135.16.180.67 mask 255.255.255.255
 neighbor 192.33.20.2 remote-as  37383
 neighbor 192.33.20.2 allowas-in
 no auto-summary
```

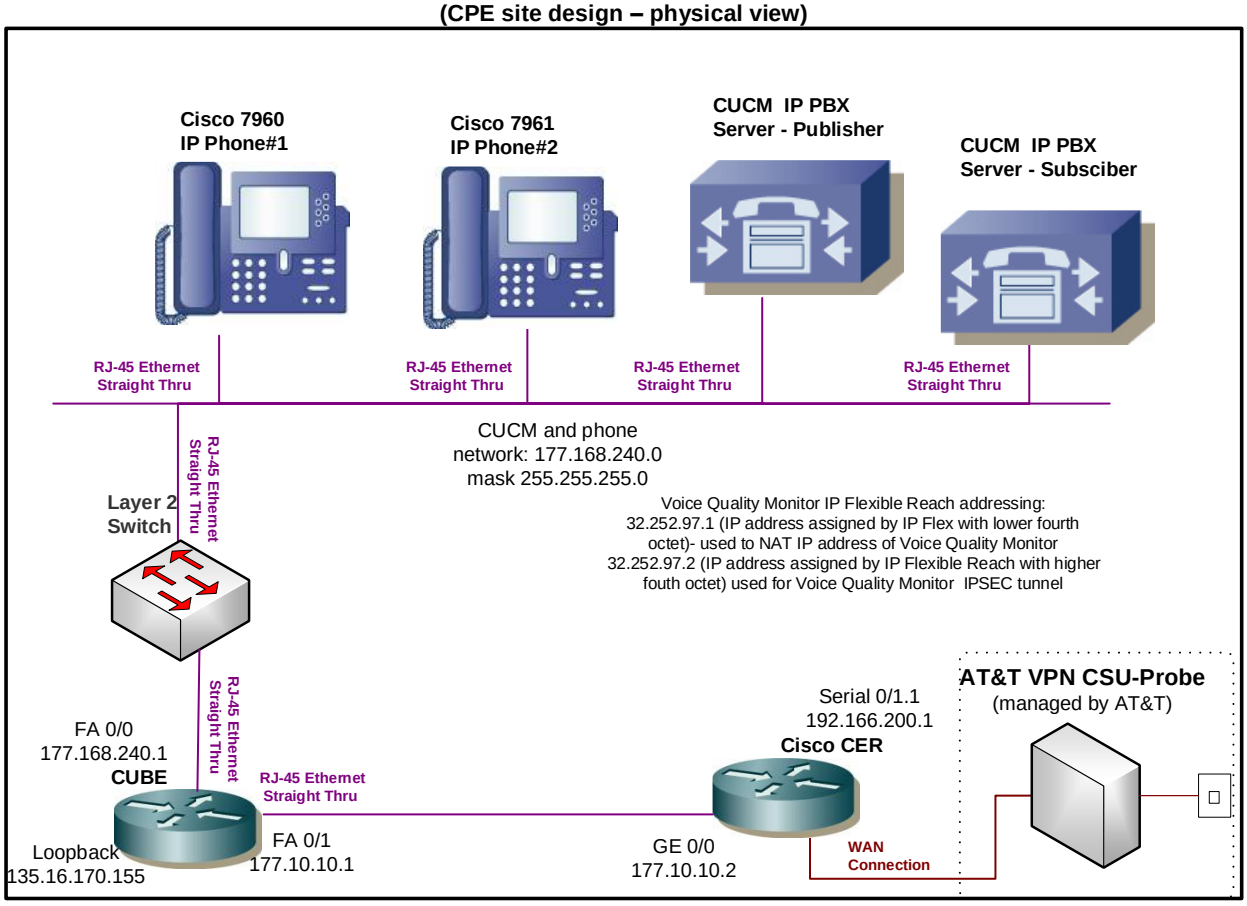
5 CER Sample Configurations

5.1 Sample Config: Customer Edge Router in conjunction with a Cisco Unified Communications Manager (CUCM) and Cisco Unified Border Element (CUBE)

Following is an example of a CER configured on a standard Frame Relay interface.

Note: This standard configuration can also be used for remote sites with IP phones only (with or without a CUBE at a remote site).

**AT&T IP Flexible Reach on AT&T VPN Site
with AT&T VPN CSU-Probe, CUBE, CUCM
(CPE site design – physical view)**




```
Building configuration...

Current configuration : 12372 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname 2821
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.124-15.T13a.bin
!
logging buffered 51200 warnings
```

```
enable password 7 0820585A05180704
!
no aaa new-model
!
resource policy
!
ip tcp path-mtu-discovery
!
!
ip cef
!
!
no ip domain lookup
ip domain name hawaii
!
!
!
class-map match-any BGP
 match access-group name BGP
class-map match-any COS1
 match access-group name RTP
 match access-group name SIP
 match access-group name SCCP
class-map match-any COS2
 match access-group name COS2-Traffic
 match access-group name BGP
class-map match-any COS3
 match access-group name COS3-Traffic
!
!
policy-map MARK-BGP
 class BGP
  set ip dscp cs6
policy-map COS
 class COS1
  priority 616 77000
  set ip dscp ef
 class COS2
  bandwidth remaining percent 40
  set ip dscp af31
  service-policy MARK-BGP
 class COS3
  bandwidth remaining percent 30
  set ip dscp af21
 class class-default
  bandwidth remaining percent 30
  set ip dscp default
!
!
interface GigabitEthernet0/0  **Facing CUBE**
 ip address 177.10.10.2 255.255.255.0
 ip virtual-reassembly
 duplex full
 speed 10
```

```
 no keepalive
!
!
interface Serial0/2/0
 no ip address
 encapsulation frame-relay IETF
 load-interval 30
 tx-ring-limit 2
 tx-queue-limit 2
 no fair-queue
 frame-relay traffic-shaping
 max-reserved-bandwidth 100
 hold-queue 32 out
!
interface Serial0/2/0.1 point-to-point
 bandwidth 1459
 ip address 192.166.200.1 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 frame-relay class shape1536
 frame-relay interface-dlci 236 IETF
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 2000000
!
router bgp 65000
 no synchronization
 bgp router-id 192.168.200.1
 bgp log-neighbor-changes
 network 135.16.170.155 mask 255.255.255.255
 network 177.168.240.0 mask 255.255.255.0
 network 32.252.97.1 mask 255.255.255.255
 network 32.252.97.2 mask 255.255.255.255
 neighbor 192.166.200.2 remote-as 13979
 neighbor 192.166.200.2 allowas-in
 no auto-summary
!
ip route 135.16.170.155 255.255.255.255 177.10.10.1
ip route 177.168.240.0 255.255.255.0 177.10.10.1
!
!
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip access-list extended BGP
 permit tcp any eq bgp any
 permit tcp any any eq bgp
ip access-list extended RTP
 permit udp any range 16384 32767 any range 16384 32767
```

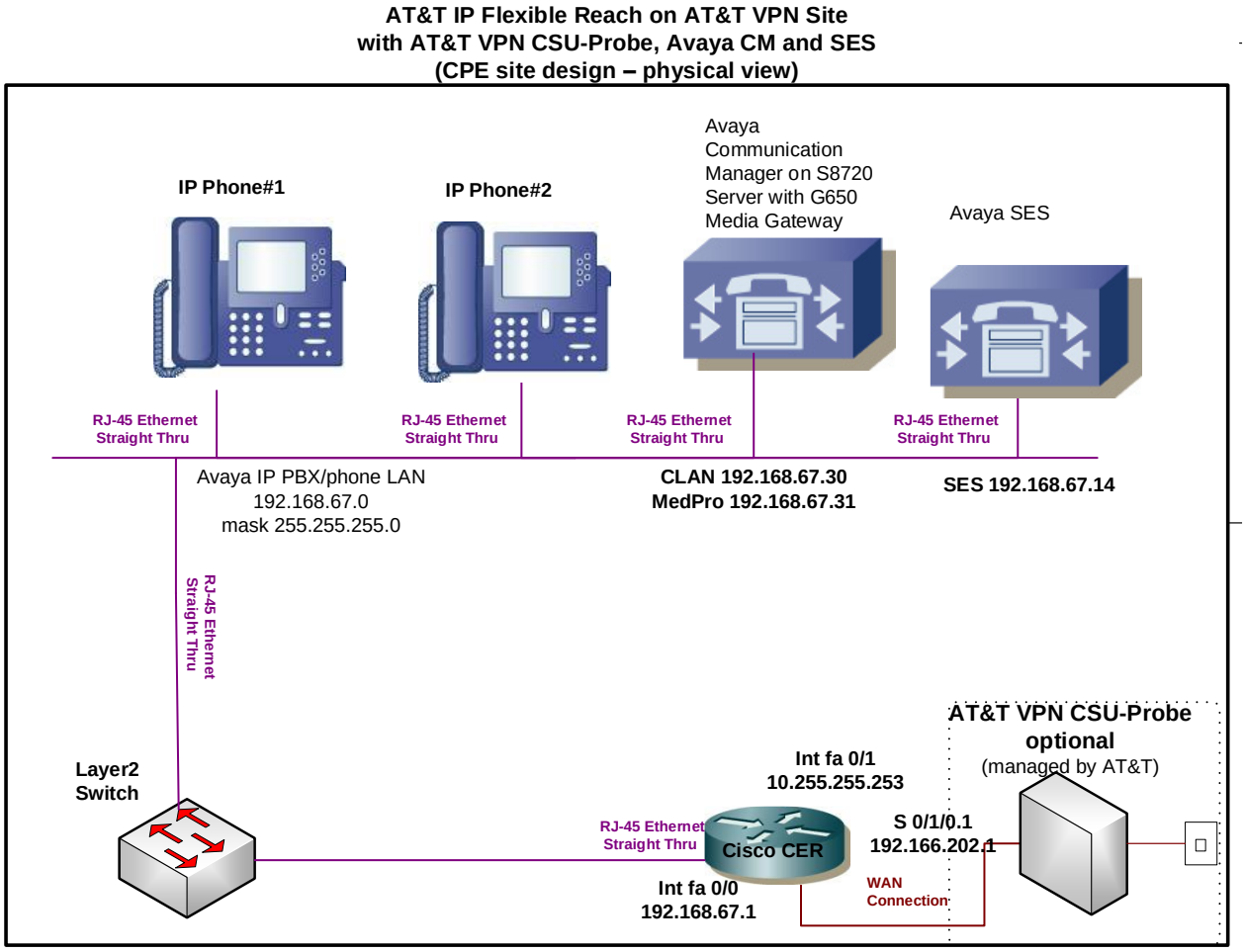
Note: Static routes required for CUBE loopback (135.16.170.155) address and private address of LAN (where IP PBX resides

```
ip access-list extended SIP
 permit udp any eq 5060 any
 permit udp any any eq 5060
ip access-list extended SCCP
 permit tcp any range 2003 2003 any
 permit tcp any any range 2000 2003
ip access-list extended COS2-Traffic
 permit udp any any eq 2082
 permit udp any eq 2082 any
ip access-list extended COS3-Traffic
 permit udp any any eq 2083
 permit udp any eq 2083 any
!
!
map-class frame-relay shape1536
 frame-relay cir 1459000
 frame-relay bc 14590
 frame-relay be 0
 frame-relay mincir 1459000
 service-policy output COS
!
banner login ^C
----------------------------------------------------------------------
Cisco Router and Security Device Manager (SDM) is installed on this device.
This feature requires the one-time use of the username "cisco"
with the password "cisco". The default username and password have a privilege level of 15.

Please change these publicly known initial credentials using SDM or the IOS CLI.
Here are the Cisco IOS commands.

username <myuser>  privilege 15 secret 0 <mypassword>
no username cisco

Replace <myuser> and <mypassword> with the username and password you want to use.

For more information about SDM please follow the instructions in the QUICK START
GUIDE for your router or go to http://www.cisco.com/go/sdm
----------------------------------------------------------------------
^C
alias exec CONFIGURED WITH ALL IN ONE CALCULATOR v2fi 02-08-2007 14:29:55
!
line con 0
line aux 0
 session-timeout 120
 exec-timeout 120 0
line vty 0 4
 exec-timeout 300 0
 password 7 00050712085A0915
 login local
 transport input ssh
!
scheduler allocate 20000 1000
!
webvpn context Default_context
```

```
 ssl authenticate verify all
 !
 no inservice
!
!
end
```

5.2 Sample Config: Customer Edge Router with Avaya Communications Manager without SBC

Following is an example of a full CER router configuration on a standard Frame Relay interface with an Avaya Communications Manager and Avaya SIP Enablement Services.




```
sh run
Building configuration...

Current configuration : 8781 bytes
!
version 12.4
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
service password-encryption
!
hostname Oslo
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.124-15.T13a.bin
boot-end-marker
!
logging buffered 51200 warnings
enable password 7 11080D111B13091F
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
no ip domain lookup
ip domain name hawaii
ip ssh authentication-retries 5
ip ssh version 2
!
username cisco privilege 15 secret 5 $1$pwCJ$4rzb68OzCfX/BW0/Z02rY0
username admin password 7 00050712085A0915
archive
 log config
  hidekeys
!
!
!
class-map match-any BGP
 match access-group name BGP
class-map match-any COS1
 match access-group name RTP
 match access-group name SIP
class-map match-any COS2
 match access-group name COS2-Traffic
 match access-group name BGP
class-map match-any COS3
 match access-group name COS3-Traffic
!
!
policy-map MARK-BGP
 class BGP
  set ip dscp cs6
policy-map COS
 class COS1
  priority 616 77000
  set ip dscp ef
 class COS2
```

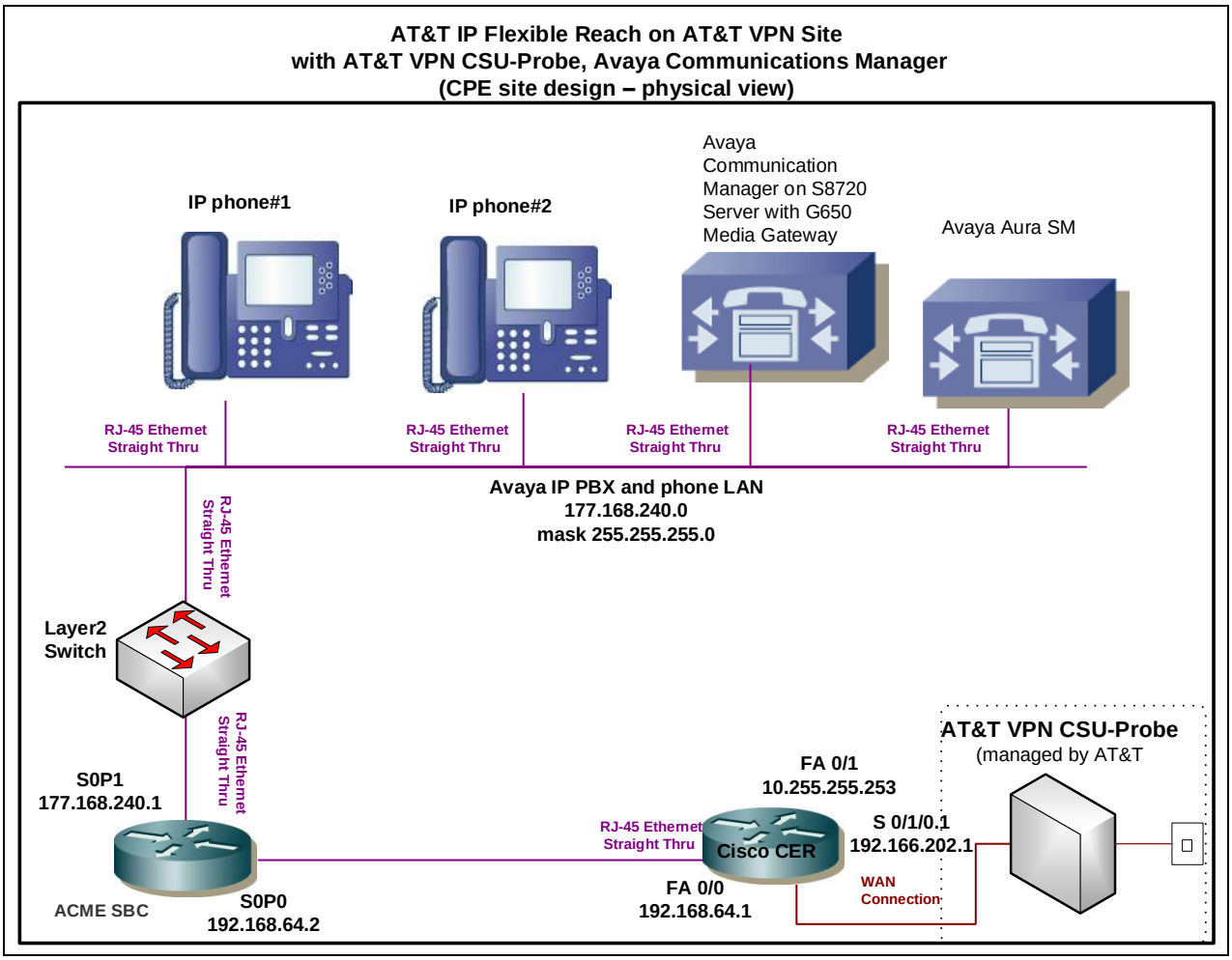
```
  bandwidth remaining percent 40
  set ip dscp af31
  service-policy MARK-BGP
 class COS3
  bandwidth remaining percent 30
  set ip dscp af21
 class class-default
  bandwidth remaining percent 30
  set ip dscp default
!
!
interface Loopback6  **NAT address for SES signaling**
 ip address 135.16.170.55 255.255.255.255
!
interface Loopback7  **PAT address for IP  phones/MedPro media**
 ip address 135.16.170.250 255.255.255.255
!
interface FastEthernet0/0  ** Facing IP PBX **

 ip address 192.168.67.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex full
 speed 100
!
!
interface Serial0/1/0
 no ip address
 encapsulation frame-relay IETF
 load-interval 30
 no fair-queue
 frame-relay traffic-shaping
 max-reserved-bandwidth 100
!
interface Serial0/1/0.1 point-to-point
 bandwidth 1459
 ip address 192.166.202.1 255.255.255.252
 ip nat outside
 no ip virtual-reassembly
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF
!
router bgp 65000
 no synchronization
 bgp router-id 192.166.202.1
 bgp log-neighbor-changes
 network 32.252.97.1 mask 255.255.255.255
 network 32.252.97.2 mask 255.255.255.255
 network 135.16.170.55 mask 255.255.255.255
 network 135.16.170.250 mask 255.255.255.255
 network 192.168.67.0 mask 255.255.255.0
 neighbor 192.166.202.2 remote-as 13979
 neighbor 192.166.202.2 allowas-in
 no auto-summary
```

```
!
!
ip nat inside source list 10 interface Loopback7 overload
ip nat inside source static 192.168.67.30 135.16.170.55
!
ip access-list extended BGP
 permit tcp any eq bgp any
 permit tcp any any eq bgp
ip access-list extended RTP
 permit udp any range 16384 32767 any range 16384 32767
ip access-list extended SIP
 permit udp any eq 5060 any
 permit udp any any eq 5060
 ip access-list extended COS2-Traffic
 permit udp any any eq 2082
 permit udp any eq 2082 any
ip access-list extended COS3-Traffic
 permit udp any any eq 2083
 permit udp any eq 2083 any
!
!
map-class frame-relay shape1536
 frame-relay cir 1459000
 frame-relay bc 1459
 frame-relay be 0
 frame-relay mincir 1459000
 service-policy output COS
!
access-list 10 deny   192.168.67.14
access-list 10 deny   192.168.67.30
access-list 10 permit 192.168.67.0 0.0.0.255
!
!
control-plane
!
!
line con 0
 login local
line aux 0
line vty 0 4
 exec-timeout 300 0
 privilege level 15
 password 7 15131F18082B2937
 login local
 transport input telnet
line vty 5
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
line vty 6 15
 access-class 23 in
 privilege level 15
 login local
```

```
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
!
end
```

5.3 Sample Config: Customer Edge Router with Avaya Communications Manager with ACME SBC

Following is an example of a full CER router configuration on a standard Frame Relay interface with an Avaya Communications Manager with ACME SBC.




```
sh run
Building configuration...

Current configuration : 8781 bytes
!
version 12.4
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
service password-encryption
!
hostname Oslo
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.124-15.T13a.bin
boot-end-marker
!
logging buffered 51200 warnings
enable password 7 11080D111B13091F
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
no ip domain lookup
ip domain name hawaii
ip ssh authentication-retries 5
ip ssh version 2
!
username cisco privilege 15 secret 5 $1$pwCJ$4rzb68OzCfX/BW0/Z02rY0
username admin password 7 00050712085A0915
archive
 log config
  hidekeys
!
!
!
class-map match-any BGP
 match access-group name BGP
class-map match-any COS1
 match access-group name RTP
 match access-group name SIP
class-map match-any COS2
 match access-group name COS2-Traffic
 match access-group name BGP
class-map match-any COS3
 match access-group name COS3-Traffic
!
!
policy-map MARK-BGP
 class BGP
  set ip dscp cs6
policy-map COS
 class COS1
  priority 616 77000
  set ip dscp ef
 class COS2
```

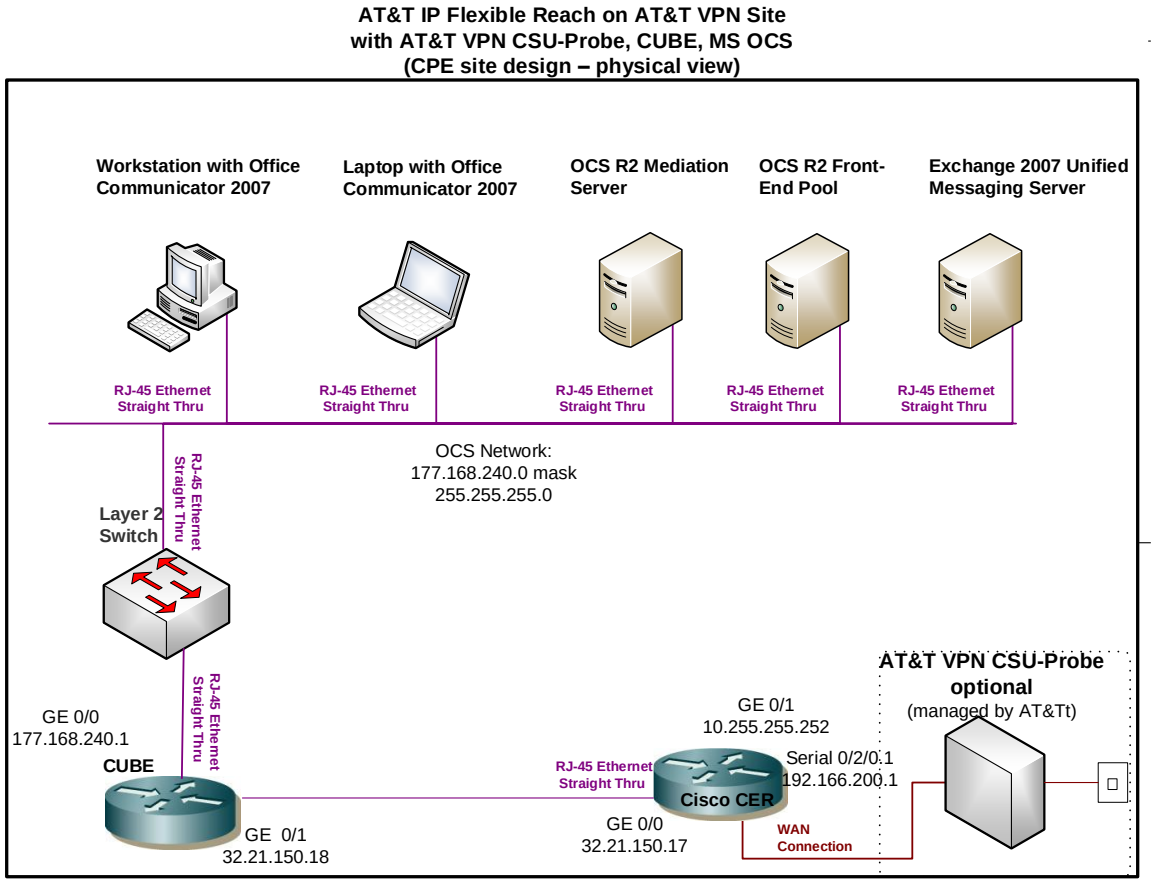
```
  bandwidth remaining percent 40
  set ip dscp af31
  service-policy MARK-BGP
 class COS3
  bandwidth remaining percent 30
  set ip dscp af21
 class class-default
  bandwidth remaining percent 30
  set ip dscp default
!
!
!
!
interface FastEthernet0/0  ** Facing ACME **

 ip address 192.168.64.1 255.255.255.252
 ip virtual-reassembly
 duplex full
 speed 100
!
!
interface Serial0/1/0
 no ip address
 encapsulation frame-relay IETF
 load-interval 30
 no fair-queue
 frame-relay traffic-shaping
 max-reserved-bandwidth 100
!
interface Serial0/1/0.1 point-to-point
 bandwidth 1459
 ip address 192.166.202.1 255.255.255.252
 ip nat outside
 no ip virtual-reassembly
 frame-relay class shape1536
 frame-relay interface-dlci 239 IETF
!
router bgp 65000
 no synchronization
 bgp router-id 192.166.202.1
 bgp log-neighbor-changes
 network 32.252.97.1 mask 255.255.255.255
 network 32.252.97.2 mask 255.255.255.255
 network 177.168.240.0 mask 255.255.255.0
 network 192.168.64.0 mask 255.255.255.248
 neighbor 192.166.202.2 remote-as 13979
 neighbor 192.166.202.2 allowas-in
 no auto-summary
!
!
ip route 177.168.240.0 255.255.255.0. 192.168.64.2  ** Route to IP PBX LAN**
!
!
ip access-list extended BGP
```

```
 permit tcp any eq bgp any
 permit tcp any any eq bgp
ip access-list extended RTP
 permit udp any range 16384 32767 any range 16384 32767
ip access-list extended SIP
 permit udp any eq 5060 any
 permit udp any any eq 5060
 ip access-list extended COS2-Traffic
 permit udp any any eq 2082
 permit udp any eq 2082 any
ip access-list extended COS3-Traffic
 permit udp any any eq 2083
 permit udp any eq 2083 any
!
access-list 1 deny 32.95.217.109 0.0.0.0
access-list 1 deny 10.255.255.252 0.0.0.3
access-list 1 permit any
!
map-class frame-relay shape1536
 frame-relay cir 1459000
 frame-relay bc 1459
 frame-relay be 0
 frame-relay mincir 1459000
 service-policy output COS
access-list 10 deny   192.168.67.14
access-list 10 deny   192.168.67.13
access-list 10 deny   192.168.67.30
access-list 10 permit 192.168.67.0 0.0.0.255
!
!
control-plane
!
!
line con 0
 login local
line aux 0
line vty 0 4
 exec-timeout 300 0
 privilege level 15
 password 7 15131F18082B2937
 login local
 transport input telnet
line vty 5
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
line vty 6 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
```

```
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
!
end
```

5.4 Sample Config: Customer Edge Router in conjunction with Microsoft Office Communication Server (OCS) 2007 R2 and Cisco Unified Border Element (CUBE)

Following is an example of a full CER router configuration on a standard Frame Relay interface with Microsoft OCS 2007 R2 with CUBE.



Sample Router Configuration:

```
Building configuration...

Current configuration : 12372 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname 2821
!
```

```
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.124-15.T13a.bin
!
logging buffered 51200 warnings
enable password 7 0820585A05180704
!
no aaa new-model
!
resource policy
!
ip tcp path-mtu-discovery
!
ip cef
!
no ip domain lookup
ip domain name hawaii
!
class-map match-any BGP
 match access-group name BGP
class-map match-any COS1
 match access-group name RTP
 match access-group name SIP
class-map match-any COS2
 match access-group name COS2-Traffic
 match access-group name BGP
class-map match-any COS3
 match access-group name COS3-Traffic
!
!
policy-map MARK-BGP
 class BGP
  set ip dscp cs6
policy-map COS
 class COS1
  priority 616 77000
  set ip dscp ef
 class COS2
  bandwidth remaining percent 40
  set ip dscp af31
  service-policy MARK-BGP
 class COS3
  bandwidth remaining percent 30
  set ip dscp af21
 class class-default
  bandwidth remaining percent 30
  set ip dscp default
!
!
!
interface GigabitEthernet0/0  **Facing CUBE**
 ip address 32.21.150.17 255.255.255.252
 ip virtual-reassembly
 duplex full
 speed 10
```

```
 no keepalive
!
!
!
interface Serial0/2/0
 no ip address
 encapsulation frame-relay IETF
 load-interval 30
 tx-ring-limit 2
 tx-queue-limit 2
 no fair-queue
 frame-relay traffic-shaping
 max-reserved-bandwidth 100
 hold-queue 32 out
!
interface Serial0/2/0.1 point-to-point
 bandwidth 1459
 ip address 192.166.200.1 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 frame-relay class shape1536
 frame-relay interface-dlci 236 IETF
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 2000000
!
router bgp 65000
 no synchronization
 bgp router-id 192.168.200.1
 bgp log-neighbor-changes
 network 32.21.150.16 mask 255.255.255.248
 network 177.168.240.0 mask 255.255.255.0
 network 32.252.97.1 mask 255.255.255.255
 network 32.252.97.2 mask 255.255.255.255
 neighbor 192.166.200.2 remote-as 13979
 neighbor 192.166.200.2 allowas-in
 no auto-summary
!
ip route 177.168.240.0 255.255.255.0 32.21.150.18
!
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip access-list extended BGP
 permit tcp any eq bgp any
 permit tcp any any eq bgp
ip access-list extended RTP
 permit udp any range 16384 32767 any range 16384 32767
```

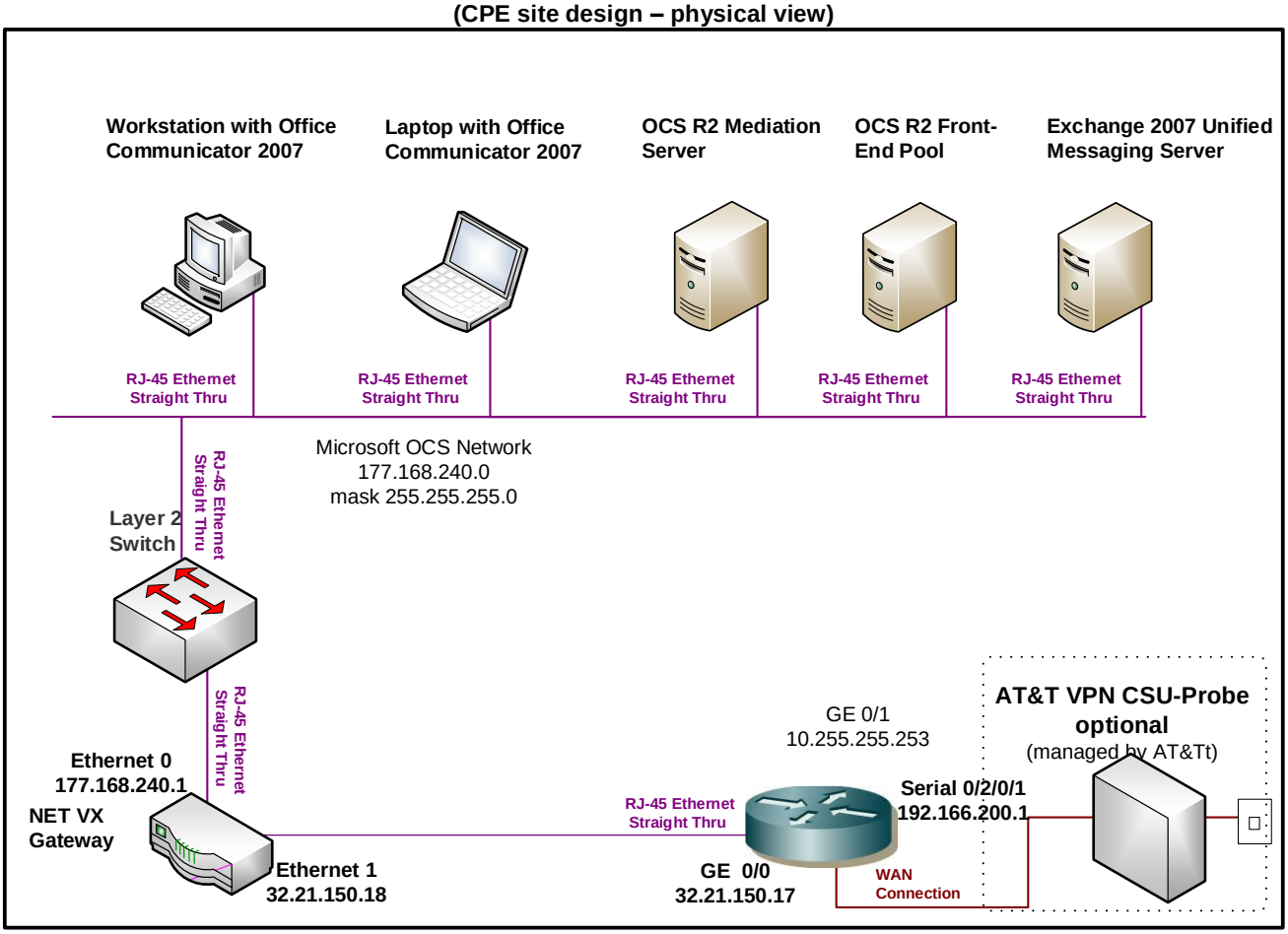
Note: Static routes required for private address of LAN (where IP PBX resides 177.168.240.0). Points to local CUBE interface.

```
ip access-list extended SIP
 permit udp any eq 5060 any
 permit udp any any eq 5060
ip access-list extended COS2-Traffic
 permit udp any any eq 2082
 permit udp any eq 2082 any
ip access-list extended COS3-Traffic
 permit udp any any eq 2083
 permit udp any eq 2083 any
!
map-class frame-relay shape1536
 frame-relay cir 1459000
 frame-relay bc 14590
 frame-relay be 0
 frame-relay mincir 1459000
 service-policy output COS
!
alias exec CONFIGURED WITH ALL IN ONE CALCULATOR v2fi 02-08-2007 14:29:55
!
line con 0
line aux 0
 session-timeout 120
 exec-timeout 120 0
line vty 0 4
 exec-timeout 300
 login local
 transport input ssh
!
scheduler allocate 20000 1000
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end
```

5.5 Sample Config: Customer Edge Router in conjunction with Network Equipment Technologies (NET) VX 1200/1800 Gateway

Following is an example of a full CER router configuration on a standard Frame Relay interface with a NET VX 1200 Gateway.

AT&T IP Flexible Reach on AT&T VPN Site
with AT&T VPN CSU-Probe, NET VX 1200/1800, MS OCS
(CPE site design – physical view)



Sample Router Configuration:

```
Building configuration...

Current configuration : 12372 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```

```
!
hostname 2821
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.124-15.T13a.bin
!
logging buffered 51200 warnings
enable password 7 0820585A05180704
!
no aaa new-model
!
resource policy
!
ip tcp path-mtu-discovery
!
!
ip cef
!
!
no ip domain lookup
ip domain name hawaii
!
!
!
class-map match-any BGP
 match access-group name BGP
class-map match-any COS1
 match access-group name RTP
 match access-group name SIP
class-map match-any COS2
 match access-group name COS2-Traffic
 match access-group name BGP
class-map match-any COS3
 match access-group name COS3-Traffic
!
!
policy-map MARK-BGP
 class BGP
  set ip dscp cs6
policy-map COS
 class COS1
  priority 616 77000
  set ip dscp ef
 class COS2
  bandwidth remaining percent 40
  set ip dscp af31
  service-policy MARK-BGP
 class COS3
  bandwidth remaining percent 30
  set ip dscp af21
 class class-default
  bandwidth remaining percent 30
  set ip dscp default
!
```

```
!
interface GigabitEthernet0/0  **Facing NET VX Gateway **
 ip address 32.21.150.17 255.255.255.252
 ip virtual-reassembly
 duplex full
 speed 100
 no keepalive
!
!
interface Serial0/2/0
 no ip address
 encapsulation frame-relay IETF
 load-interval 30
 tx-ring-limit 2
 tx-queue-limit 2
 no fair-queue
 frame-relay traffic-shaping
 max-reserved-bandwidth 100
 hold-queue 32 out
!
interface Serial0/2/0.1 point-to-point
 bandwidth 1459
 ip address 192.166.200.1 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 frame-relay class shape1536
 frame-relay interface-dlci 236 IETF
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 2000000
!
router bgp 65000
 no synchronization
 bgp router-id 192.168.200.1
 bgp log-neighbor-changes
 network 32.21.150.16 mask 255.255.255.248
 network 177.168.240.0 mask 255.255.255.0
 network 32.252.97.1 mask 255.255.255.255
 network 32.252.97.2 mask 255.255.255.255
 neighbor 192.166.200.2 remote-as 13979
 neighbor 192.166.200.2 allowas-in
 no auto-summary
!
!
ip route 177.168.240.0 255.255.255.0 32.21.150.18
!
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
```

Note: Static routes required for private address of LAN (where IP PBX resides 177.168.240.0). Points to local NET interface.

```
!
ip access-list extended BGP
 permit tcp any eq bgp any
 permit tcp any any eq bgp
ip access-list extended RTP
 permit udp any range 16384 32767 any range 16384 32767
ip access-list extended SIP
 permit udp any eq 5060 any
 permit udp any any eq 5060
ip access-list extended COS2-Traffic
 permit udp any any eq 2082
 permit udp any eq 2082 any
ip access-list extended COS3-Traffic
 permit udp any any eq 2083
 permit udp any eq 2083 any
!
!
map-class frame-relay shape1536
 frame-relay cir 1459000
 frame-relay bc 14590
 frame-relay be 0
 frame-relay mincir 1459000
 service-policy output COS
!
banner login ^C
----------------------------------------------------------------------
Cisco Router and Security Device Manager (SDM) is installed on this device.
This feature requires the one-time use of the username "cisco"
with the password "cisco". The default username and password have a privilege level of 15.

Please change these publicly known initial credentials using SDM or the IOS CLI.
Here are the Cisco IOS commands.

username <myuser>  privilege 15 secret 0 <mypassword>
no username cisco

Replace <myuser> and <mypassword> with the username and password you want to use.

For more information about SDM please follow the instructions in the QUICK START
GUIDE for your router or go to http://www.cisco.com/go/sdm
----------------------------------------------------------------------
^C
alias exec CONFIGURED WITH ALL IN ONE CALCULATOR v2fi 02-08-2007 14:29:55
!
line con 0
line aux 0
 session-timeout 120
 exec-timeout 120 0
line vty 0 4
 exec-timeout 300 0
 password 7 00050712085A0915
 login local
 transport input ssh
!
```

```
scheduler allocate 20000 1000
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
!
end
```

6 Acronyms

Acronym	Translation
ADSL	Asymmetric Digital Subscriber Line
AIM	Advanced Integration Module A
AS	Autonomous System
ATM	Asynchronous Transfer Mode
AT&T VPN	AT&T Virtual Private Network
BC	Committed Burst
BE	Excess Burst or Best Effort
BGP	Border Gateway Protocol
BH	Bursty High
BL	Bursty Low
BOE	Branch Office Extension
CAS	Channel Associated Signaling
CBWFQ	Class Based Weighted Fair Queuing
CCG	Customer Configuration Guide
CCS	Common Channel Signaling
CDR	Committed Data Rate
CEF	Cisco Express Forwarding
CER	Customer Edge Router
CHAP	Challenge Handshake Authentication Protocol
CIR	Committed Information Rate
CLI	Command Line Interface
CM	Communications Manager
COS	Class of Service
CPE	Customer Premise Equipment
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRTP	Compress Real Time Protocol
CSU/DSU	Channel Service Unit / Data Service Unit
CUBE	Cisco Unified Border Element
CUCM	Cisco Unified Communications Manager
DID	Direct Inward Dial
DS	Down Stream
DSCP	Differentiated Service Code Point
DSL	Digital Subscriber Line
DSP	Digital Signal Processors
DTMF	Dual Tone Multi Frequency
E&M	Ear & Mouth

Acronym	Translation
EF	Expedient Forwarding
ePVC	Enhanced Permanent Virtual Circuit
FR	Frame Relay
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station
GSM FR	Global System for Mobile communications Full Rate
HDV	High Density Voice
HWIC	High-speed WAN Interface Card
IAR	Inbound Alternate Routing
IETF	Internet Engineering Task Force
IMA	Inverse Multiplexing over ATM
IOS	Internetwork Operation System
IP	Internet Protocol
IPBE	Internet Protocol Border Element
IPSEC	Internet Protocol Security
ISR	Integrated Services Router
ITU-T	International Telecommunication Union - Telecommunications
GW	Gateway
LAN	Local Area Network
LFI	Link Fragmentation and Interleaving
LLQ	Low Latency Queuing
LD	Long Distance
MLPPP	Multi-Link Point-to-Point Protocol
MM	Multi Media
MOW	Most Of World
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NET	Network Equipment Technologies
NM	Network Module
NPE	Network Processing Engine
OAM	Operation Administration & Maintenance
OCS	Office Communication Server
PA	Port Adapter
PAT	Port Address Translation
PBX	Private Branch Exchange
PC	Personal Computer
PCR	Peak Cell Rate
PER	Provider Edge Router
POS	Packet over SONET
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol

Acronym	Translation
PQ	Priority Queue
PRI	Primary Rate Interface
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
PVDM	Packet Voice DSP Module
QOS	Quality of Service
QSIG	Q Signaling
RC	Receive
RFC	Request for Comment
RT	Real Time
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SBC	Session Border Controller
SCCP	Skinny Call Control Protocol
SCR	Sustainable Cell Rate
SHDSL	Single-Pair High-Speed Digital Subscriber Line
SIP	Session Initiation Protocol
SM	Session Manager
SPE	Synchronous Payload Envelope
TAC	Technical Assistance Center
TC	Time Interval
TDM	Time Division Multiplexing
TN	Telephone Number
TX	Transmit
UDP	User Datagram Protocol
US	Up Stream or United States
VAD	Voice Activity Detection
VCI	Virtual Circuit Identifier
VLAN	Virtual Local Area Network
VNI	Voice Network Infrastructure
VoIP	Voice over Internet Protocol
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VT	Virtual Template
WAN	Wide Area Network
WFQ	Weighted Fair Queuing
WIC	WAN Interface Card

This Customer Configuration Guide ("CCG") is offered as a convenience to AT&T's customers. The specifications and information regarding the product in this CCG are subject to change without notice. All statements, information, and recommendations in this CCG are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided “AS IS”. Users must take full responsibility for the application of the specifications and information in this CCG.

In no event shall AT&T or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage arising out of the use or inability to use this CCG, even if AT&T or its suppliers have been advised of the possibility of such damage.