



RECEIVED

2018 NOV 27 AM 11:04

WV PURCHASING  
DIVISION

**AT&T Response to State of West Virginia's RFP # CRFP  
0212 SWC1900000001 for VOIP Hosted Services**



**AT&T Business**



816 Lee Street  
Charleston, WV 25301

Office: 304.690.0140  
Mobile: 304.690.0140  
[ef8030@att.com](mailto:ef8030@att.com)  
[www.att.com](http://www.att.com)

November 21, 2018

Mark Atkins  
Department of Administration, Purchasing Division  
State of West Virginia  
2019 Washington Street East  
Charleston WV 25305-0130

Re: West Virginia's Request for Proposals for Managed and Hosted Voice Services, #0212  
SWC1900000001, dated August 29, 2018 (the "RFP")

Dear Mr. Atkins:

On behalf of AT&T Corp. ("AT&T"), I would like to thank the State of West Virginia (the "State") for the opportunity to submit this response to the RFP (the "Response"). As a leading provider of telecommunications and related services to government institutions, AT&T is uniquely positioned to meet the State's service and product needs.

In that regard, please understand that AT&T is submitting the Response pursuant to the responses, answers, clarifications and supplemental terms and conditions set forth in and/or incorporated into the Response.

Notwithstanding anything to the contrary in the RFP, neither AT&T nor the State is under any obligation with respect to the RFP until both parties have agreed upon a mutually acceptable final terms and conditions.

AT&T looks forward to working with you in the event AT&T is selected as your vendor of choice. Please do not hesitate to call me for assistance at any time.

Sincerely,

Beth Spradlin  
Client Solutions Executive



## Connecting Your World

### AT&T Response to State of West Virginia's RFP CRFP # 0212 SWC1900000001 for VOIP Hosted Services

November 21, 2018

Beth Spradlin  
Client Solutions Executive  
AT&T  
816 Lee Street  
Charleston, WV 25301  
304.690.0140  
[ef8030@att.com](mailto:ef8030@att.com)



**Proposal Validity Period**—The information and pricing contained in this response (the "Response" or the "Proposal") is valid for a period of 90 days from the date written on the Proposal cover page, unless rescinded or extended in writing by AT&T. **Terms and Conditions**—Unless otherwise stated herein, this Proposal is conditioned upon negotiation of mutually acceptable terms and conditions. **Proposal Pricing**—Pricing proposed herein is based upon the specific product/service mix and locations outlined in this Proposal. Any changes or variations in the proposed terms and conditions, the products/services, length of term, locations, and/or design described herein may result in different pricing. Prices quoted do not include applicable taxes, surcharges, or fees. In accordance with the tariffs or other applicable service agreement terms, Customer is responsible for payment of such charges. **Providers of Service**—Subsidiaries and affiliates of AT&T Inc. provide products and services under the AT&T brand. AT&T Corp. is an AT&T company, is the proposer for itself and on behalf of its service-providing affiliates. **Software**—Any software used with the products and services provided in connection with this Response will be governed by the written terms and conditions applicable to such software. Title to software remains with AT&T or its supplier. Customer must comply with all such terms and conditions, and they will take precedence over any agreement between the parties as relates to such software. **Copyright Notice and Statement of Confidentiality**—©2018 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo, and all other marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. The contents of the Proposal (except for pricing applicable to E-rate funded services) are unpublished, proprietary, and confidential and may not be copied, disclosed, or used, in whole or in part, without the express written permission of AT&T Intellectual Property or affiliated companies, except to the extent required by law and insofar as is reasonably necessary in order to review and evaluate the information contained herein.



## Table of Contents

Executive Summary.....	3
RFP Response .....	5
SECTION 1: GENERAL INFORMATION .....	8
SECTION 2: INSTRUCTIONS TO VENDORS SUBMITTING BIDS.....	10
SECTION 3: GENERAL TERMS AND CONDITIONS .....	20
SECTION 4: PROJECT SPECIFICATIONS .....	64
SECTION 5: VENDOR PROPOSAL .....	163
SECTION 6: EVALUATION AND AWARD .....	165
AT&T Attachments.....	169







## AT&T'S GENERAL RESPONSE TO THE RFP ("AT&T's General Response")

AT&T Corp. ("AT&T") is submitting this response (the "Response") to this RFP pursuant to the responses, answers, clarifications and supplemental terms and conditions set forth in and/or incorporated into this Response. The State of West Virginia may be referred to as the "State" or "Customer" within this Response.

The terms and conditions contained within this RFP document do not contain the product- and service-related contractual terms necessary for AT&T to properly deliver the products and services described in the Response. Accordingly, AT&T is submitting the additional terms and conditions set forth below after General Terms and Conditions §44 (the "Additional Terms and Conditions"). The pricing submitted by and through this Response assumes full incorporation of the Response, including the Additional Terms and Conditions, as part of any final, negotiated contract between the parties. In the event AT&T is fortunate enough to be chosen as the State's vendor, AT&T is fully prepared to negotiate with the State in good faith on a final document.

Please note that included within AT&T's General Response, in an efficiency effort, are several statements that apply to several, similar provisions throughout the RFP and should be read as applicable to any and all such related provisions. In that regard, note that:

- AT&T clarifies that only the physical response materials become Customer property. Any other pre-existing or newly-developed intellectual property of AT&T, its suppliers or its third parties, provided in this Response or which is used or developed during the project remains the intellectual property of AT&T or its suppliers. AT&T would be willing to negotiate with Customer regarding rights to use that intellectual property.
- AT&T respectfully requests that information in this document be held confidential by Customer to the extent allowed under applicable law.
- AT&T clarifies that only the physical response materials become Customer property. Any other pre-existing or newly-developed intellectual property of AT&T, its suppliers or its third parties, provided in this Response or which is used or developed during the project remains the intellectual property of A
- AT&T will hold the prices quoted for a period of 90 days and will endeavor to extend this period to the length of time as requested by the RFP.
- The Response is a direct reflection of the entire scope of work as presented here, as of the date of submission. Acceptance of only part of the quote may require mutual agreement/adjustment to the final configuration, subsequent pricing and implementation schedule.



- Regarding any proposed waiver of informalities and irregularities, AT&T agrees, except to the extent the waiver of technicalities or informalities portions of this provision as used here and throughout this RFP implies AT&T waives rights to protest the award decision. To that end, AT&T reserves all protest rights afforded bidders/respondents participating in the contracting process.
- Any purchase orders issued for services as provided under the RFP must clearly provide that the purchase is made via the mutually agreed contract and not subject to the preprinted terms of that purchase order form.
- Any third-party software used with the services will be governed by the written terms and conditions of the third-party software supplier's software license documentation applicable to such software.
- Title to software remains with AT&T or its supplier. The Customer, as the licensee, will be bound to all such terms and conditions, and they will take precedence over any agreement between the parties as relating to such software.
- To the extent any portion of this project may be funded in whole or in part with grants, loans or payments made pursuant to the American Recovery and Reinvestment Act of 2009 ("ARRA"), AT&T and Customer will need to reach mutual agreement on AT&T's participation.
- The information and pricing submitted with this Response is subject to change on account of any error or omission in the information provided by Customer or upon further investigation(s) as to the exact requirements of any order. For the price(s) quoted herein, AT&T will provide the items of equipment and services specifically listed in its proposal. Work which is not shown or described in a proposal will require mutual agreement/adjustment to the final configuration, subsequent pricing and Implementation schedule.

Notwithstanding anything to the contrary set forth in the RFP, neither AT&T nor the State is under any obligation with respect to the RFP until both parties have agreed upon and executed a mutually acceptable final contract.

It is AT&T's goal to provide the best communications services at the best value for all of our customers using the highest ethical and legal standards. Given the long and successful history of AT&T, we are confident this will be a successful contracting process, leading to a successful project performance.



## Executive Summary

AT&T understands the primary goal of this procurement is to expand and modernize the telecommunication capabilities that will enable the State to meet the current and future technology needs of state government. We know that to provide quality public service, the State of West Virginia aims to improve efficiencies, upgrade to the latest technologies, and find ways to satisfy the changing business requirements to support state and local agencies, internal and external business partners and citizens throughout the State.

AT&T knows that in order to be successful in West Virginia, we have to understand the inter-relationships of each of the procurement efforts and align the solutions we are proposing in response to these RFP's directly with the State's goals to:

- Optimize Services
- Transform Government
- Empower the Workforce
- Foster Collaboration, Communication and Governance

We understand that the State has identified another essential component of the modernization of its telecommunications services as the delivery of Unified Communications & Voice Services throughout the state. The primary goal of this procurement is to obtain a comprehensive, secure, and cost-effective voice communications solution for State agencies.

AT&T Unified Communications Services consists of best of breed applications and services that are tailored to help support the delivery of new communications systems in an expedient and cost-effective manner. It consists of a set of proven core Unified Communications products and services that provide voice, video, mobility and unified messaging services that will be customized to meet the State's requirements.

With AT&T's integrated solution, we will be there to deliver or the answer the call regardless of the technology. AT&T will be providing holistic support model for interaction with new and existing service providers to provide proactive and reactive monitoring, management and MACD support for core network MPLS, integrated network transport, SIP, voice and collaboration services.

The AT&T Universal Help Desk will provide support for direct interaction with State end users and designated systems admins as required to maintain services. AT&T will also provide integrated network Security Operation Center providing proactive security



alerting, Intrusion prevention and detection services. AT&T will provide periodic security auditing and analysis to ensure optimal security for all State services.

AT&T provides common fabric of services that is useful and usable for all PA agencies and for other suppliers. Networks are changing, and AT&T is leading the way. This ongoing transformation will enable an intelligent, dynamic and on-demand infrastructure to support the continuing evolution of both telecommunications and business itself.


We are currently in the process of virtualizing our own network with 30% of the conversion completed. By 2020, we plan to virtualize and control over 75% of our network using these new software-defined architectures.

The software-defined network of the future will help AT&T deliver to the State some incredible benefits:

- Secure networking solutions to access corporate information across locations, connecting citizens, business partners, cloud providers, and mobile workers.
- Connect anywhere at any time to a business world that's mobile, unified and scalable for growth.
- The office will be everywhere. A smart network brings everything together. Devices can talk to one another. Applications can be accessed anywhere in one simple platform.



## RFP Response

	Purchasing Division 2019 Washington Street East Post Office Box 50138 Charleston, WV 25305-0138	State of West Virginia Request for Proposal 35 -- Telecomm
---	--	--

Proc Folder: 432803			
Doc Description: RFP for Managed and Hosted Voice Services (OT18027)			
Proc Type: Statewide MA (Open End)			
Date Issued	Solicitation Closes	Solicitation No	Version
2018-09-29	2018-10-24 13:30:00	CRFP 0212 SWC1900000001	1

BID RECEIVING LOCATION	
BID CLERK	
DEPARTMENT OF ADMINISTRATION	
PURCHASING DIVISION	
2019 WASHINGTON ST E	
CHARLESTON	WV 25305
US	

### VENDOR

ATT Corp., 816 Lee Street Charleston WV 25301, 3046900140

### FOR INFORMATION CONTACT THE BUYER

Mark A Atkins  
(304) 558-2307  
[mark.a.atkins@wv.gov](mailto:mark.a.atkins@wv.gov)

*Elizabeth Spadlin*

FEIN #  
134924710

DATE 11/23/18

All offers subject to all terms and conditions contained in this solicitation





### ADDITIONAL INFORMATION

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code 5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to provide Managed Voice Services for the State's Legacy VoIP Environment, while working to migrate those Legacy Environments to a Hosted VoIP Platform, included Hosted Contact Center Services per attached documents.

#### MANDATORY PRE-BID MEETING:

DATE: 09/26/2018

TIME: 2:30PM EDT

LOCATION: VW Office of Technology  
1900 Kanawha Blvd. E.,  
Building 5, 10th Floor  
Charleston, WV 25305

NOTE: Online responses to this solicitation are prohibited. Please see the Instructions to Bidders in Section 2 for proposal submission.

INVOICE TO		SHIP TO	
ALL STATE AGENCIES		STATE OF WEST VIRGINIA	
VARIOUS LOCATIONS AS INDICATED BY ORDER		VARIOUS LOCATIONS AS INDICATED BY ORDER	
No City	VW99999	No City	99999
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Managed and Hosted Voice Services	0.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81161700			

Extended Description:



See Attachment\_A Cost Sheet for proposal pricing.

Vendor shall use the Attachment\_A Cost Sheet for proposal pricing.

Note: online proposal submissions are prohibited.

Please see Section 5 Vendor Proposal Subsection 5.3 for further instructions.

#### SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Mandatory Pre-Bid Meeting @ 2:30pm EDT:	2018-09-26
2	Technical Questions due by 2:00pm EDT:	2018-10-05



## SECTION 1: GENERAL INFORMATION

### 1.1. Introduction:

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W.Va. Code S5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to provide Managed Voice Services for the State's Legacy VoIP Environment, while working to migrate those Legacy Environments to a Hosted VOIP Platform, included Hosted Contact Center Services.

The RFP is a procurement method in which vendors submit proposals in response to the request for proposal published by the Purchasing Division. It requires an award to the highest scoring vendor, rather than the lowest cost vendor, based upon a technical evaluation of the vendor's technical proposal and a cost evaluation. This is referred to as a best value procurement. Through their proposals, vendors offer a solution to the objectives, problem, or need specified in the RFP, and define how they intend to meet (or exceed) the RFP requirements.

#### AT&T Response:

AT&T has read and understands.

### 1.2. RFP Schedule of Events:

RFP Released to Public	08/29/2018
Mandatory Pre-bid Conference	09/26/2018 @ 2:30pm EDT
Vendor's Written Questions Submission Deadline	10/05/2018 by 2:00pm EDT
Addendum Issued	TBD
Technical Bid Opening Date	10/24/2018 at 1:30pm EDT
Technical Evaluation Begins	10/24/2018
Oral Presentation	TBD
Cost Bid Opening	TBD





Cost Evaluation Begins

TBD

Contract Award Made

TBD

**AT&T Response:**

AT&T has read and understands.





## SECTION 2: INSTRUCTIONS TO VENDORS SUBMITTING BIDS

Instructions begin on next page.



## INSTRUCTIONS TO VENDORS SUBMITTING BIDS

1. **REVIEW DOCUMENTS THOROUGHLY:** The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

### AT&T Response:

AT&T has read and understands.

2. **MANDATORY TERMS:** The Solicitation may contain mandatory provisions identified by the use of the words "must," "will," and "shall." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

### AT&T Response:

AT&T has read and understands. AT&T has taken exception where needed and is noted in the response.

3. **PREBID MEETING:** The item identified below shall apply to this Solicitation.

- ☐ A pre-bid meeting will not be held prior to bid opening
- ☐ A NON-MANDATORY PRE-BID meeting will be held at the following place and time:
- ☒ A MANDATORY PRE-BID meeting will be held at the following place and time:

DATE: 09/26/2018

TIME: 2:30pm EDT

LOCATION: West Virginia Office of Technology  
1900 Kanawha Blvd. E.,  
Building 5, 10th Floor  
Charleston, WV 25305

All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one person attending the pre-bid meeting may represent more than one Vendor.



An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. The State will not accept any other form of proof or documentation to verify attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.

Additionally, the person attending the pre-bid meeting should include the Vendor's E-Mail address, phone number, and Fax number on the attendance sheet. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

All Vendors should arrive prior to the starting time for the pre-bid. Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in, but are charged with knowing all matters discussed at the pre-bid.

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

#### AT&T Response:

AT&T has read and understands.

4. **VENDOR QUESTION DEADLINE:** Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below in order to be considered. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are nonbinding.

Submitted e-mails should have solicitation number in the subject line.

Question Submission Deadline: **October 05, 2018 due by 2:00pm EDT**

Submit Questions to: Mark Atkins, Senior Buyer  
2019 Washington Street, East  
Charleston, WV 25305

Fax: (304) 558-4115 (Vendors should not use this fax number for bid submission)

Email: [Mark.A.Atkins@wv.gov](mailto:Mark.A.Atkins@wv.gov)



**AT&T Response:**

AT&T has read and understands.

5. **VERBAL COMMUNICATION:** Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

**AT&T Response:**

AT&T has read and understands.

6. **BID SUBMISSION:** All bids must be submitted electronically through wvOASIS or signed and delivered by the Vendor to the Purchasing Division at the address listed below on or before the date and time of the bid opening. Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via e-mail. Acceptable delivery methods include electronic submission via wvOASIS, hand delivery, delivery by courier, or facsimile.

The bid delivery address is:

Department of Administration, Purchasing Division  
2019 Washington Street East  
Charleston, WV 25305-0130

A bid that is not submitted electronically through wvOASIS should contain the information listed below on the face of the envelope or the bid may be rejected by the Purchasing Division.:

SEALED BID: VOIP Hosted Services  
BUYER: Mark Atkins  
SOLICITATION NO.: CRFP 0212 SWC1900000001  
BID OPENING DATE: 10/24/2018  
BID OPENING TIME: 1:30pm EDT  
FAX NUMBER: 304-558-3970

The Purchasing Division may prohibit the submission of bids electronically through wvOASIS at its sole discretion. Such a prohibition will be contained and communicated in the wvOASIS system resulting in the Vendor's inability to submit





bids through wvOASIS. Submission of a response to an Expression of Interest or Request for Proposal is not permitted in wvOASIS.

**For Request For Proposal ("RFP") Responses Only:** In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal plus Five (5) convenience copies of each to the Purchasing Division at the address shown above. Additionally, the Vendor should identify the bid type as either a technical or cost proposal on the face of each bid envelope submitted in response to a request for proposal as follows:

BID TYPE: (This only applies to CRFP)

☒ Technical

☒ Cost

**AT&T Response:**

AT&T has read and understands.

7. **BID OPENING:** Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by wvOASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery).

Bid Opening Date and Time: **October 24, 2018 at 1.30pm EDT**

Bid Opening Location: Department of Administration, Purchasing Division

2019 Washington Street East  
Charleston, WV 25305-0130

**AT&T Response:**

AT&T has read and understands.

8. **ADDENDUM ACKNOWLEDGEMENT:** Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgment Form, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The



addendum acknowledgement should be submitted with the bid to expedite document processing.

**AT&T Response:**

AT&T has read and understands.

9. **BID FORMATTING:** Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

**AT&T Response:**

AT&T has read and understands.

10. **ALTERNATE MODEL OR BRAND:** Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand should clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items. Failure to provide information for alternate items may be grounds for rejection of a Vendor's bid.

☐ This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

**AT&T Response:**

AT&T has read and understands.

11. **EXCEPTIONS AND CLARIFICATIONS:** The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.



**AT&T Response:**

AT&T has read and understands.

**12. COMMUNICATION LIMITATIONS:** In accordance with West Virginia Code of State Rules #148-1-6.6, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

**AT&T Response:**

AT&T has read and understands.

**13. REGISTRATION:** Prior to Contract award, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the \$125 fee, if applicable.

**AT&T Response:**

AT&T has read and understands.

**14. UNIT PRICE:** Unit prices shall prevail in cases of a discrepancy in the Vendor's bid.

**AT&T Response:**

AT&T has read and understands.

**15. PREFERENCE:** Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § 5A-3-37, and should include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at:

<http://www.state.wv.us/admin/purchase/vrc/Venpref.pdf>





**AT&T Response:**

AT&T has read and understands.

15A. **RECIPROCAL PREFERENCE:** The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. A request form to help facilitate the request can be found at: <http://www.state.wv.us/admin/purchase/vrc/Venpref.pdf>

**AT&T Response:**

AT&T has read and understands.

16. **SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES:** For any solicitations publicly advertised for bid, in accordance with West Virginia Code # 5A-337(a)(7) and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women-owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors. Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR § 148-22-9.

**AT&T Response:**

AT&T has read and understands.

17. **WAIVER OF MINOR IRREGULARITIES:** The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules # 148-1-4.6.

**AT&T Response:**

AT&T has read and understands.





**18. ELECTRONIC FILE ACCESS RESTRICTIONS:** Vendor must ensure that its submission in wVOASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires, and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

**AT&T Response:**

AT&T has read and understands.

**19. NON-RESPONSIBLE:** The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules # 148-15.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform, or lacks the integrity and reliability to assure good-faith performance."

**AT&T Response:**

AT&T has read and understands.

**20. ACCEPTANCE/REJECTION:** The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules # 148-1-4,5, and # 148-1-6.4.b."

**AT&T Response:**

AT&T has read and understands.

**21. YOUR SUBMISSION IS A PUBLIC DOCUMENT:** Vendors entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code ## 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code ## 29B-1-1 et seq.



DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code # 47-22-1 et seq. All submissions are subject to public disclosure without notice.

**AT&T Response:**

AT&T has read and understands.

**22. INTERESTED PARTY DISCLOSURE:** West Virginia Code # 6D-1-2 requires that the vendor submit to the Purchasing Division a disclosure of interested parties to the contract for all contracts with an actual or estimated value of at least \$1 Million. That disclosure must occur on the form prescribed and approved by the WV Ethics Commission prior to contract award. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

**AT&T Response:**

This requirement does not apply to publicly traded companies listed on a national or international stock exchange.

**23. WITH THE BID REQUIREMENTS:** In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR # 148-1-4.6. This authority does not apply to instances where state law mandates receipt with the bid.

**AT&T Response:**

AT&T has read and understands.



## SECTION 3: GENERAL TERMS AND CONDITIONS

General Terms and Conditions begin on next page.

### AT&T Response:

See AT&T's General Response.





## GENERAL TERMS AND CONDITIONS:

1. **CONTRACTUAL AGREEMENT:** Issuance of a Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

### AT&T'S Response to General Terms and Conditions §1:

See AT&T's General Response. In addition, AT&T takes Exception to the portion of this provision that implies that bidder's mere execution and submission of the Response acts as an acceptance of the terms and conditions in the RFP. AT&T does not intend that the information described in the Response is to be the final expression between the parties. AT&T's proposal is submitted subject to the provisions of its Response; and AT&T reserves the right to negotiate the terms and conditions of the final contract.

2. **DEFINITIONS:** As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.
  - 2.1. "Agency" or "Agencies" means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.
  - 2.2. "Bid" or "Proposal" means the vendors submitted response to this solicitation.
  - 2.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.
  - 2.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.
  - 2.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.
  - 2.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.



- 2.7. "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.
- 2.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.
- 2.9. "Vendor" or "Vendors" means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

**AT&T Response:**

AT&T has read and understands.

**3. CONTRACT TERM; RENEWAL; EXTENSION:**

**AT&T'S Response to General Terms and Conditions §3:**

See AT&T's General Response. In addition, any renewal option would be exercisable only via mutual written consent.

The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

☒ Term Contract

Initial Contract Term: Initial Contract Term: This Contract becomes effective on Upon award and extends for a period of Four (4) year(s).

**Renewal Term:** This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to see below successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)



- ☒ **Alternate Renewal Term** — This contract may be renewed for Two (2) successive Two (2) year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

**Delivery Order Limitations:** In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

- ☐ **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within \_\_\_\_\_ days.
- ☐ **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within \_\_\_\_\_ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that maintenance, monitoring, or warranty services will be provided for \_\_\_\_\_ year(s) thereafter.
- ☐ **One Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.
- ☐ **Other:** See attached.

**AT&T Response:**

AT&T has read and understands.

4. **NOTICE TO PROCEED:** Vendor shall begin performance of this Contract immediately upon receiving notice to proceed unless otherwise instructed by the Agency. Unless otherwise specified, the fully executed Award Document will be considered notice to proceed.

**AT&T Response:**

AT&T has read and understands.



5. **QUANTITIES:** The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

- ☒ **Open End Contract:** Quantities listed in this Solicitation are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.
- ☒ **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.
- ☒ **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.
- ☒ **One Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

**AT&T Response:**

AT&T has read and understands.

6. **EMERGENCY PURCHASES:** The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute a breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One Time Purchase contract.

**AT&T Response:**

AT&T has read and understands.

7. **REQUIRED DOCUMENTS:** All of the items checked below must be provided to the Purchasing Division by the Vendor as specified below.





- ☐ **BID BOND (Construction Only):** Pursuant to the requirements contained in W. Va. Code 5-22-1 (c), All Vendors submitting a bid on a construction project shall furnish a valid bid bond in the amount of five percent (5%) of the total amount of the bid protecting the State of West Virginia. The bid bond must be submitted with the bid.
- ☐ **PERFORMANCE BOND:** The apparent successful Vendor shall provide a performance bond in the amount of 100% of the contract. The performance bond must be received by the Purchasing Division prior to Contract award.
- ☐ **LABOR/MATERIAL PAYMENT BOND:** The apparent successful Vendor shall provide a labor/material payment bond in the amount of 100% of the Contract value. The labor/material payment bond must be delivered to the Purchasing Division prior to Contract award.

In lieu of the Bid Bond, Performance Bond, and Labor/Material Payment Bond, the Vendor may provide certified checks, cashier's checks, or irrevocable letters of credit. Any certified check, cashier's check, or irrevocable letter of credit provided in lieu of a bond must be of the same amount and delivered on the same schedule as the bond it replaces. A letter of credit submitted in lieu of a performance and labor/material payment bond will only be allowed for projects under \$100,000. Personal or business checks are not acceptable. Notwithstanding the foregoing, West Virginia Code 5-22-1 (d) mandates that a vendor provide a performance and labor/material payment bond for construction projects. Accordingly, substitutions for the performance and labor/material payment bonds for construction projects is not permitted.

- ☐ **MAINTENANCE BOND:** The apparent successful Vendor shall provide a two (2) year maintenance bond covering the roofing system. The maintenance bond must be issued and delivered to the Purchasing Division prior to Contract award.
- ☐ **LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits prior to Contract award, in a form acceptable to the Purchasing Division.

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications prior to Contract award regardless of whether or not that requirement is listed above.

#### AT&T Response:

AT&T has read and understands.



8. **INSURANCE:** The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below and must include the State as an additional insured on each policy prior to Contract award.

**AT&T'S Clarification to General Terms and Conditions §8:**

"AT&T can agree to the insurance requirements as indicated by the modifications noted by AT&T."

The insurance coverages identified below must be maintained throughout the life of this contract. Ten (10) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor will provide at least 30 days' prior written notice to Agency of cancellation or non renewal of any required coverage that is not replaced. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether or not that insurance requirement is listed in this section. Vendor may self insure any required coverage.

Vendor must maintain:

- ☒ Commercial General Liability Insurance in at least an amount of: \$1,000,000.00 per occurrence and in the aggregate.
- ☒ Automobile Liability Insurance in at least an amount of: \$1,000,000.00 per occurrence.
- ☐ Professional/Malpractice/Errors and Omission Insurance in at least an amount of: \_\_\_\_\_ per occurrence.
- ☐ Commercial Crime and Third Party Fidelity Insurance in an amount of: \_\_\_\_\_ per occurrence.
- ☒ Cyber Liability Insurance in an amount of: \$3,000,000.00 per claim or wrongful act and in the aggregate.
- ☐ Builders Risk Insurance in an amount equal to 100% of the amount of the Contract.
- ☐ Pollution Insurance in an amount of \_\_\_\_\_ per occurrence.
- ☐ Aircraft Liability in an amount of: \_\_\_\_\_ per occurrence.



Notwithstanding anything contained in this section to the contrary, the Director of the Purchasing Division reserves the right to waive the requirement that the State be named as an additional insured on one or more of the Vendor's insurance policies if the Director finds that doing so is in the State's best interest.

**AT&T Response:**

AT&T has read and understands.

9. **WORKERS' COMPENSATION INSURANCE:** The apparent successful Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

**AT&T'S Clarification to General Terms and Conditions §9:**

"AT&T can agree to the insurance requirements as indicated by the modifications noted by AT&T."

10. [Reserved]

11. **LIQUIDATED DAMAGES:** This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

- ☐ \_\_\_\_\_ for \_\_\_\_\_
- ☐ Liquidated Damages Contained in the Specifications

**AT&T'S Response to General Terms and Conditions §11:**

See AT&T's General Response. In addition, AT&T takes exception to and does not agree to be bound by this Liquidated Damages provision. AT&T's liability responsibilities will be as provided in the Additional Terms and Conditions submitted with this Response.

12. **ACCEPTANCE:** Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless



otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

#### **AT&T'S Response to General Terms and Conditions §12:**

See AT&T's General Response. In addition, AT&T takes exception to the portion of this provision that implies a bidder's mere execution and submission of a proposal acts as an acceptance of the terms and conditions in the RFP. AT&T does not intend that the information described in the RFP is to be the final expression between the parties.

**13. PRICING:** The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification.

#### **AT&T Response:**

AT&T has read and understands.

**14. PAYMENT IN ARREARS:** Payment in advance is prohibited under this Contract. Payment may only be made after the delivery and acceptance of goods or services. The Vendor shall submit invoices, in arrears.

#### **AT&T Response:**

AT&T has read and understands.

**15. PAYMENT METHODS:** Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

#### **AT&T Response:**

Payment via electronic funds transfer can be arranged and set up with your assigned AT&T sales team. Credit card payments are accepted for some AT&T services.

**16. TAXES:** The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby.





The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

**AT&T Response:**

AT&T takes an exception. AT&T requests the State of West Virginia to submit the appropriate TAX Exempt forms. AT&T will then determine the taxes and surcharges that appear on your bill according to the services that you've purchased based upon the State of West Virginia's tax exemption status. Taxes vary greatly depending on your geographic location, and AT&T follows all jurisdictional tax laws.

17. **ADDITIONAL FEES:** Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

**AT&T Response:**

AT&T takes an exception. AT&T reserves the right to pass along additional charges, surcharges and fees imposed on AT&T by State or Federal regulations or laws and any cost incurred by AT&T in providing the services.

AT&T may add surcharges to certain services. For example, the Universal Connectivity Charge (UCC), Administrative Expense Fee (AEF), Property Tax Allotment (PTA), and Federal Regulatory Fee (FRF) apply to all regulated, interstate, and international/U.S. billed services. AT&T applies the surcharges to the net invoiced amount.

18. **FUNDING:** This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available.

**AT&T Response:**

AT&T has read and understands.





19. **CANCELLATION:** The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules # 148-1-5.2.b.

**AT&T Response:**

AT&T has read and understands.

20. **TIME:** Time is of the essence with regard to all matters of time and performance in this Contract.

**AT&T'S Response to General Terms and Conditions §20:**

See AT&T's General Response. AT&T clarifies that not all times are of the essence. AT&T is willing to look at specific times the State of West Virginia would like for AT&T to consider but does not agree that all times are critical.

21. **APPLICABLE LAW:** This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code or West Virginia Code of State Rules is void and of no effect.

**AT&T'S Response to General Terms and Conditions §21:**

AT&T's Response is submitted under applicable codes, laws and regulations current at the time of contract execution. AT&T shall comply with all codes, laws and regulations applicable to AT&T. Changes in codes, laws and regulations may require changes in pricing and performance.

22. **COMPLIANCE WITH LAWS:** Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

**SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws,



regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

#### AT&T'S Response to General Terms and Conditions §22:

See AT&T's General Response. The Response is submitted under applicable codes, laws and regulations current at the time of contract execution. AT&T shall comply with all codes, laws and regulations applicable to AT&T. Changes in codes, laws and regulations may require changes in pricing and performance.

23. **ARBITRATION:** Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

#### AT&T Response:

AT&T has read and understands.

24. **MODIFICATIONS:** This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

#### AT&T Response:

AT&T has read and understands.

25. **WAIVER:** The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.



**AT&T Response:**

AT&T has read and understands.

26. **SUBSEQUENT FORMS:** The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes Internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

**AT&T Response:**

AT&T has read and understands.

27. **ASSIGNMENT:** Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

**AT&T'S Response to General Terms and Conditions §27:**

See AT&T's General Response. AT&T reserves the right to assign its rights and obligations under any definitive agreement relating to services to be provided as proposed in this RFP and AT&T's Response to same -- to an AT&T affiliate, or subcontract to an affiliate or third party work to be performed -- but AT&T will in each such case remain financially responsible for the performance of such obligations.

28. **WARRANTY:** The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

**AT&T Response:**

AT&T has read and understands.





**29. STATE EMPLOYEES:** State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

**AT&T Response:**

AT&T has read and understands.

**30. PRIVACY, SECURITY, AND CONFIDENTIALITY:** The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in <http://www.state.wv.us/admin/purchase/privacy/default.html>

**AT&T Response:**

AT&T has read and understands.

**31. YOUR SUBMISSION IS A PUBLIC DOCUMENT:** Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code # 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code ## 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code 47-22-1 et seq. All submissions are subject to public disclosure without notice.

**AT&T Response:**

AT&T has read and understands.



**32. LICENSING:** In accordance with West Virginia Code of State Rules # 148-1-6.1 -e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

**SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

**AT&T Response:**

AT&T has read and understands.

**33. ANTITRUST:** In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

**AT&T'S Response to General Terms and Conditions §33:**

See AT&T's General Response. AT&T will work with the State of West Virginia to reach agreement on a mutually acceptable assignment of anti-trust claim provision.

**34. VENDOR CERTIFICATIONS:** By signing its bid or entering into this Contract, Vendor certifies (1) that its bid or offer was made without prior understanding, agreement,



or connection with any corporation, firm, limited liability company, partnership, person or entity submitting a bid or offer for the same material, supplies, equipment or services; (2) that its bid or offer is in all respects fair and without collusion or fraud; (3) that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; and (4) that it has reviewed this Solicitation in its entirety; understands the requirements, terms and conditions, and other information contained herein.

Vendor's signature on its bid or offer also affirms that neither it nor its representatives have any interest, nor shall acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency. The individual signing this bid or offer on behalf of Vendor certifies that he or she is authorized by the Vendor to execute this bid or offer or any documents related thereto on Vendor's behalf; that he or she is authorized to bind the Vendor in a contractual relationship; and that, to the best of his or her knowledge, the Vendor has properly registered with any State agency that may require registration.

#### **AT&T'S Response to General Terms and Conditions §34:**

See AT&T's General Response. The undersigned can affirm to the best of the undersigned's knowledge and belief that AT&T's Response to the RFP was not prepared in collusion with any other person or entity. In addition, AT&T is not aware of any material conflict of interest. AT&T is publicly owned, and with millions of shareholders, it is impossible for AT&T to determine whether any State employee or any member of his or her immediate family may be a shareholder in AT&T, Inc. Further, given AT&T and its affiliates' nearly 230,000 employees, it is not possible in any practical fashion and in the time available for this response to determine any possible connections between all AT&T employees and any employees of the State or any component office. AT&T will represent, however, that to the best of its knowledge and belief, after a reasonable inquiry, that none of the people involved in the preparation of this Response have a familial relationship with any employee of the State. However, the State should make such an inquiry of its own employees, directors, and officers prior to entering into an agreement with AT&T and take the necessary steps to ensure such individuals remain in compliance with these requirements.

**35. VENDOR RELATIONSHIP:** The relationship of the Vendor to the state shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating





any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

**AT&T Response:**

AT&T has read and understands.

- 36. INDEMNIFICATION:** The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

**AT&T'S Response to General Terms and Conditions §36:**

See AT&T's General Response. AT&T takes exception to this indemnification section and respectfully requests the opportunity to negotiate this provision to the parties' mutual satisfaction.

- 37. PURCHASING AFFIDAVIT:** In accordance with West Virginia Code #5A-3-10a and # 5-22-1 (i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. Vendors are required to sign, notarize, and submit the Purchasing Affidavit to the Purchasing Division affirming under oath that it is not in default on any monetary obligation owed to the state or a political subdivision of the state.



**AT&T Response:**

AT&T has read and understands. Added under AT&T Attachments.





**38. ADDITIONAL AGENCY AND LOCAL GOVERNMENT USE:** This Contract may be utilized by other agencies, spending units, and political subdivisions of the State of West Virginia; county, municipal, and other local government bodies; and school districts ("Other Government Entities"), provided that both the Other Government Entity and the Vendor agree. Any extension of this Contract to the aforementioned Other Government Entities must be on the same prices, terms, and conditions as those offered and agreed to in this Contract, provided that such extension is in compliance with the applicable laws, rules, and ordinances of the Other Government Entity. A refusal to extend this Contract to the Other Government Entities shall not impact or influence the award of this Contract in any manner.

**AT&T'S Response to General Terms and Conditions §38:**

See AT&T's General Response. AT&T is certainly willing to entertain the opportunity to provision to other entities. However, AT&T would need to know information including, but not limited to, which entities were being considered, how the billing and collection would work (e.g., who would ultimately be responsible for payment), any credit issues, and what services were involved. Once AT&T understood the details, AT&T would consider this opportunity.

**39. CONFLICT OF INTEREST:** Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

**AT&T Response:**

AT&T has read and understands.

**40. REPORTS:** Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

- ☒ Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.
- ☒ Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at [purchasing.requisitions@wv.gov](mailto:purchasing.requisitions@wv.gov)



#### AT&T Response:

AT&T has read and understands.

**41. BACKGROUND CHECK:** In accordance with W. Va. Code 15-2D-3, the Director of the Division of Protective Services shall require any service provider whose employees are regularly employed on the grounds or in the buildings of the Capitol complex or who have access to sensitive or critical information to submit to a fingerprint-based state and federal background inquiry through the state repository. The service provider is responsible for any costs associated with the fingerprint-based state and federal background inquiry.

After the contract for such services has been approved, but before any such employees are permitted to be on the grounds or in the buildings of the Capitol complex or have access to sensitive or critical information, the service provider shall submit a list of all persons who will be physically present and working at the Capitol complex to the Director of the Division of Protective Services for purposes of verifying compliance with this provision. The State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check.

Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

#### AT&T Response:

As part of conducting a background and/or criminal history investigation pursuant to Section 41, the State of West Virginia obtain information regarding AT&T employees or subcontractors, which includes, but is not limited to, name, address, telephone number, driver's license number, date of birth, health information, biometric data and other personal information obtained in connection with the investigation (collectively, "Sensitive Personal Information" or "SPI"). The State of West Virginia and its designee(s) shall consider SPI to be private, sensitive and confidential. SPI may be subject to certain privacy laws and regulations and requirements, including requirements of AT&T, and requires a high degree of protection. The State of West Virginia shall comply with all applicable privacy laws and regulations and must treat such SPI with the same degree of care as the State of West Virginia would treat SPI of its own employees and subcontractors including, without limitation:

1. Collect SPI only as needed for a background and/or criminal history investigation or otherwise as permissible under this Agreement;



2. Not use, disclose, or distribute any SPI except in connection with a background and/or criminal history investigation or otherwise as permissible under this Agreement;
3. Store and transmit SPI securely, including without limitation encrypting SPI when it is at rest and being transmitted;
4. Restrict access to SPI only to those employees of the State or its designee(s) that require access to perform the services under this Agreement;
5. Immediately notify AT&T if the State becomes aware that (a) any of the above provisions has been breached; (b) any disclosure of SPI to any third party not expressly permitted herein to receive or have access to SPI; or (c) any breach of, or other security incident involving, 's systems or network that could cause or permit access to SPI inconsistent with the above-referenced provisions. The State shall fully cooperate with AT&T in determining, as may be necessary or appropriate, actions that need to be taken including the full scope of the breach, disclosure or security incident, corrective steps to be taken by the State, the nature and content of any notifications, law enforcement involvement, or news/press/media contact etc., and the State shall not communicate directly with any AT&T employee or subcontractor without AT&T's consent, which such consent shall not be unreasonably withheld; and
6. Implement any other administrative, physical, and technical safeguards to ensure proper use, and protect against any unauthorized disclosure, of SPI.

42. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS: Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code # 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code # 5A-3-56. As used in this section:

- a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.
- b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more of such operations, from steel made by the open hearth, basic oxygen, electric furnace, Bessemer or other steel making





process. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

- c. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars (\$2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or
- d. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

**AT&T Response:**

AT&T has read and understands.

**43. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL:** In

Accordance with W. Va. Code # 5-19-1 et seq., and W. Va. CSR # 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars (\$50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This



provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

**AT&T Response:**

AT&T has read and understands.

**44. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE:** W. Va. Code 0-1-2 requires that for contracts with an actual or estimated value of at least \$1 million, the vendor must submit to the Agency a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-award interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

**AT&T Response:**

AT&T has read and understands.

**DESIGNATED CONTACT:** Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

Beth Spradlin, Client Solutions Exec 2 Integrated Mob\*

(Name, Title)

816 Lee Street, Charleston, WV 25301

(Address)

304.690.0140

(Phone Number) / (Fax Number)





[ef8030@att.com](mailto:ef8030@att.com)  
(email address)

## AT&T'S Additional Terms and Conditions:

As noted in AT&T's General Response, AT&T submits the Response subject to the Additional Terms and Conditions set forth immediately below. The pricing submitted in the Response assumes the use of these clauses as part of any final, negotiated contract.

### 1. INTRODUCTION

**1.1 Overview of Documents.** This Master Agreement and the following additional documents (collectively, the "Agreement") shall apply to all products and services AT&T provides Customer pursuant to this Agreement ("Services") and shall continue in effect so long as Services are provided under this Agreement:

- (a) **Pricing Schedules.** A "Pricing Schedule" means a pricing schedule (including related attachments) or other document that is attached to or is later executed by the parties and references this Master Agreement. A Pricing Schedule includes the Services, the pricing (including discounts and commitments, if applicable) and the pricing schedule term ("Pricing Schedule Term").
- (b) **Tariffs and Guidebooks.** "Tariffs" are documents containing the descriptions, pricing and other terms and conditions for a Service that AT&T or its Affiliates file with regulatory authorities. "Guidebooks" are documents (designated as Guidebooks or Price Lists) containing the descriptions, pricing and other terms and conditions for a Service that were but no longer are filed with regulatory authorities. Tariffs and Guidebooks can be found at [att.com/servicepublications](http://att.com/servicepublications) or other locations AT&T may designate.
- (c) **Acceptable Use Policy.** AT&T's Acceptable Use Policy ("AUP") applies to (i) Services provided over or accessing the Internet and (ii) wireless (i.e., cellular) data and messaging Services. The AUP can be found at [att.com/aup](http://att.com/aup) or other locations AT&T may designate.
- (d) **Service Guides.** The descriptions, pricing and other terms and conditions for a Service not covered by a Tariff or Guidebook may be contained in a Service Guide, which can be found at [att.com/servicepublications](http://att.com/servicepublications) or other locations AT&T may designate.

**1.2 Priority of Documents.** The order of priority of the documents that form this Agreement is: the applicable Pricing Schedule or Order; this Master Agreement;



the AUP; and Tariffs, Guidebooks and Service Guides; provided that Tariffs will be first in priority in any jurisdiction where applicable law or regulation does not permit contract terms to take precedence over inconsistent Tariff terms.

**1.3 Revisions to Documents.** Subject to Section 8.2(b) (Materially Adverse Impact), AT&T may revise Service Publications at any time.

**1.4 Execution by Affiliates.** An AT&T Affiliate or Customer Affiliate may sign a Pricing Schedule in its own name, and such Affiliate contract will be a separate but associated contract incorporating the terms of this Agreement. Customer and AT&T will cause their respective Affiliates to comply with any such separate and associated contract.

## **2. AT&T DELIVERABLES**

**2.1 Services.** AT&T will either provide or arrange to have an AT&T Affiliate provide Services to Customer and its Users, subject to the availability and operational limitations of systems, facilities and equipment. Where required, an AT&T Affiliate authorized by the appropriate regulatory authority will be the service provider. If an applicable Service Publication expressly permits placement of an order for a Service under this Master Agreement without the execution of a Pricing Schedule, Customer may place such an order using AT&T's standard ordering processes (an "Order"), and upon acceptance by AT&T, the Order shall otherwise be deemed a Pricing Schedule under this Master Agreement for the Service ordered.

**2.2 AT&T Equipment.** Services may be provided using equipment owned by AT&T that is located at the Site ("AT&T Equipment"), but title to the AT&T Equipment will remain with AT&T. Customer must provide adequate space and electric power for the AT&T Equipment and keep the AT&T Equipment physically secure and free from liens and encumbrances. Customer will bear the risk of loss or damage to the AT&T Equipment (other than ordinary wear and tear), except to the extent caused by AT&T or its agents.

**2.3 Purchased Equipment.** Except as specified in a Service Publication, title to and risk of loss of Purchased Equipment shall pass to Customer on delivery to the transport carrier for shipment to Customer's designated location.

**2.4 License and Other Terms.** Software, Purchased Equipment and Third-Party Services may be provided subject to the terms of a separate license or other agreement between Customer and either the licensor, the third-party service provider or the manufacturer. Customer's execution of the Pricing Schedule for





or placement of an Order for Software, Purchased Equipment or Third-Party Services is Customer's agreement to comply with such separate agreement. Unless a Service Publication specifies otherwise, AT&T's sole responsibility with respect to Third-Party Services is to place Customer's orders for Third-Party Services, except that AT&T may invoice and collect payment from Customer for the Third-Party Services.

### 3. CUSTOMER'S COOPERATION

**3.1 Access Right.** Customer will in a timely manner allow AT&T access as reasonably required for the Services to property and equipment that Customer controls and will obtain at Customer's expense timely access for AT&T as reasonably required for the Services to property controlled by third parties such as Customer's landlord. AT&T will coordinate with and, except in an emergency, obtain Customer's consent to enter upon Customer's property and premises, which consent shall not be unreasonably withheld. Access rights mean the right to construct, install, repair, maintain, replace and remove access lines and network facilities and the right to use ancillary equipment space within a building for Customer's connection to AT&T's network. Customer must provide AT&T timely information and access to Customer's facilities and equipment as AT&T reasonably requires for the Services, subject to Customer's reasonable security policies. Customer will furnish any conduit, holes, wireways, wiring, plans, equipment, space, power/utilities and other items as AT&T reasonably requires for the Services and will obtain any necessary licenses, permits and consents (including easements and rights-of-way). Customer will have the Site ready for AT&T to perform its work according to a mutually agreed schedule.

**3.2 Safe Working Environment.** Customer will ensure that the location at which AT&T installs, maintains or provides Services is a safe working environment, free of Hazardous Materials and reasonably suitable for the Services. "Hazardous Materials" mean any substance or material capable of posing an unreasonable risk to health, safety or property or whose use, transport, storage, handling, disposal or release is regulated by any law related to pollution, to protection of air, water or soil or to health and safety. AT&T shall have no obligation to perform work at a location that is not a suitable and safe working environment or to handle, remove or dispose of Hazardous Materials.

**3.3 Users.** "User" means anyone who uses or accesses any Service provided to Customer. Customer will cause Users to comply with this Agreement and is responsible for Users' use of any Service unless expressly provided to the contrary in an applicable Service Publication.



**3.4 Resale of Services.** Customer may not resell the Services or rebrand the Services for resale to third parties without AT&T's prior written consent.

#### **4. PRICING AND BILLING**

##### **4.1 Pricing and Pricing Schedule Term; Terms Applicable After End of Pricing**

**Schedule Term.** The prices listed in a Pricing Schedule are stabilized until the end of the Pricing Schedule Term and will apply in lieu of the corresponding prices set forth in the applicable Service Publication. No promotion, credit, discount or waiver set forth in a Service Publication will apply. Unless the Pricing Schedule states otherwise, at the end of the Pricing Schedule Term, Customer may continue Service (subject to any applicable notice or other requirements in a Service Publication for Customer to terminate a Service Component) under a month-to-month service arrangement at the prices, terms and conditions in effect on the last day of the Pricing Schedule Term. AT&T may change such prices, terms or conditions on 30 days' prior notice to Customer.

**4.2 Additional Charges and Taxes.** Prices set forth in a Pricing Schedule are exclusive of and Customer will pay all taxes (excluding those on AT&T's net income), surcharges, recovery fees, customs clearances, duties, levies, shipping charges and other similar charges (and any associated interest and penalties resulting from Customer's failure to timely pay such taxes or similar charges) relating to the sale, transfer of ownership, installation, license, use or provision of the Services, except to the extent Customer provides a valid exemption certificate prior to the delivery of Services. To the extent required by law, Customer may withhold or deduct any applicable taxes from payments due to AT&T, provided that Customer will use reasonable commercial efforts to minimize any such taxes to the extent allowed by law or treaty and will furnish AT&T with such evidence as may be required by relevant taxing authorities to establish that such tax has been paid so that AT&T may claim any applicable credit.

**4.3 Billing.** Unless a Service Publication specifies otherwise, Customer's obligation to pay for a Service Component begins upon availability of the Service Component to Customer. Customer will pay AT&T without deduction, setoff or delay for any reason (except for withholding taxes as provided in Section 4.2 - Additional Charges and Taxes or in Section 4.5 - Delayed Billing; Disputed Charges). At Customer's request, but subject to AT&T's consent (which may not be unreasonably withheld or withdrawn), Customer's Affiliates may be invoiced separately, and AT&T will accept payment from such Affiliates. Customer will be responsible for payment if Customer's Affiliates do not pay charges in accordance with this Agreement. AT&T may require Customer or its Affiliates to tender a deposit if AT&T determines, in its reasonable judgment, that Customer







or its Affiliates are not creditworthy, and AT&T may apply such deposit to any charges owed.

**4.4 Payments.** Payment is due within 30 days after the date of the invoice (unless another date is specified in an applicable Tariff or Guidebook) and must refer to the invoice number. Charges must be paid in the currency specified in the invoice. Restrictive endorsements or other statements on checks are void. Customer will reimburse AT&T for all costs associated with collecting delinquent or dishonored payments, including reasonable attorneys' fees. AT&T may charge late payment fees at the lowest of (a) 1.5% per month (18% per annum), (b) for Services contained in a Tariff or Guidebook at the rate specified therein, or (c) the maximum rate allowed by law for overdue payments.

**4.5 Delayed Billing; Disputed Charges.** Customer will not be required to pay charges for Services initially invoiced more than 6 months after close of the billing period in which the charges were incurred, except for calls assisted by an automated or live operator. If Customer disputes a charge, Customer will provide notice to AT&T specifically identifying the charge and the reason it is disputed within 6 months after the date of the invoice in which the disputed charge initially appears, or Customer waives the right to dispute the charge. The portion of charges in dispute may be withheld and will not be considered overdue until AT&T completes its investigation of the dispute, but Customer may incur late payment fees in accordance with Section 4.4 (Payments). Following AT&T's notice of the results of its investigation to Customer, payment of all properly due charges and properly accrued late payment fees must be made within ten (10) business days. AT&T will reverse any late payment fees that were invoiced in error.

**4.6 Credit Terms.** AT&T retains a lien and purchase money security interest in each item of Purchased Equipment and Vendor Software until Customer pays all sums due. AT&T is authorized to sign and file a financing statement to perfect such security interest.

**4.7 MARC.** Minimum Annual Revenue Commitment ("MARC") means an annual revenue commitment set forth in a Pricing Schedule that Customer agrees to satisfy during each 12-consecutive-month period of the Pricing Schedule Term. If Customer fails to satisfy the MARC for any such 12-month period, Customer will pay a shortfall charge in an amount equal to the difference between the MARC and the total of the applicable MARC-Eligible Charges incurred during such 12-month period, and AT&T may withhold contractual credits until Customer pays the shortfall charge.





#### 4.8 Adjustments to MARC.

- (a) In the event of a business downturn beyond Customer's control, or a corporate divestiture, merger, acquisition or significant restructuring or reorganization of Customer's business, or network optimization using other Services, or a reduction of AT&T's prices, or a force majeure event, any of which significantly impairs Customer's ability to meet a MARC, AT&T will offer to adjust the affected MARC to reflect Customer's reduced usage of Services (with a corresponding adjustment to the prices, credits or discounts available at the reduced MARC level). If the parties reach agreement on a revised MARC, AT&T and Customer will amend the affected Pricing Schedule prospectively. This Section 4.8 will not apply to a change resulting from Customer's decision to use service providers other than AT&T. Customer will provide AT&T notice of the conditions Customer believes will require the application of this provision. This provision does not constitute a waiver of any charges, including monthly recurring charges and shortfall charges, Customer incurs prior to amendment of the affected Pricing Schedule.
- (b) If Customer, through merger, consolidation, acquisition or otherwise, acquires a new business or operation, Customer and AT&T may agree in writing to include the new business or operation under this Agreement. Such agreement will specify the impact, if any, of such addition on Customer's MARC or other volume or growth discounts and on Customer's attainment thereof.

#### 5. CONFIDENTIAL INFORMATION

**5.1 Confidential Information.** Confidential Information means: (a) information the parties or their Affiliates share with each other in connection with this Agreement or in anticipation of providing Services under this Agreement (including pricing or other proposals), but only to the extent identified as Confidential Information in writing; and (b) except as may be required by applicable law or regulation, the terms of this Agreement.

**5.2 Obligations.** A disclosing party's Confidential Information will, for a period of 3 years following its disclosure to the other party (except in the case of software, for which the period is indefinite): (a) not be disclosed, except to the receiving party's employees, agents and contractors having a need-to-know (but only if such agents and contractors are not direct competitors of the other party and agree in writing to use and disclosure restrictions as restrictive as this Section 5) or to the extent authorized to be revealed by law, governmental authority or legal process (but only if such disclosure is limited to that which is so authorized





and prompt notice is provided to the disclosing party to the extent practicable and not prohibited by law, governmental authority or legal process); (b) be held in confidence; and (c) be used only for purposes of using the Services, evaluating proposals for new services or performing this Agreement (including in the case of AT&T to detect fraud, to check quality and to operate, maintain and enhance the network and Services).

**5.3 Exceptions.** The restrictions in this Section 5 will not apply to any information that: (a) is independently developed by the receiving party without use of the disclosing party's Confidential Information; (b) is lawfully received by the receiving party free of any obligation to keep it confidential; or (c) becomes generally available to the public other than by breach of this Agreement.

**5.4 Privacy.** Each party is responsible for complying with the privacy laws applicable to its business. AT&T shall require its personnel, agents and contractors around the world who process Customer Personal Data to protect Customer Personal Data in accordance with the data protection laws and regulations applicable to AT&T's business. If Customer does not want AT&T to comprehend Customer data to which it may have access in performing Services, Customer must encrypt such data so that it will be unintelligible. Customer is responsible for obtaining consent from and giving notice to its Users, employees and agents regarding Customer's and AT&T's collection and use of the User, employee or agent information in connection with a Service. Customer will only make accessible or provide Customer Personal Data to AT&T when it has the legal authority to do so. Unless otherwise directed by Customer in writing, if AT&T designates a dedicated account representative as Customer's primary contact with AT&T, Customer authorizes that representative to discuss and disclose Customer's customer proprietary network information to any employee or agent of Customer without a need for further authentication or authorization.

## **6. LIMITATIONS OF LIABILITY AND DISCLAIMERS**

### **6.1 Limitation of Liability.**

- (a) EITHER PARTY'S ENTIRE LIABILITY AND THE OTHER PARTY'S EXCLUSIVE REMEDY FOR DAMAGES ON ACCOUNT OF ANY CLAIM ARISING OUT OF AND NOT DISCLAIMED UNDER THIS AGREEMENT SHALL BE:
  - (i) FOR BODILY INJURY, DEATH OR DAMAGE TO REAL PROPERTY OR TO TANGIBLE PERSONAL PROPERTY PROXIMATELY CAUSED BY A PARTY'S NEGLIGENCE, PROVEN DIRECT DAMAGES;



- (ii) FOR BREACH OF SECTION 5 (Confidential Information), SECTION 10.1 (Publicity) OR SECTION 10.2 (Trademarks), PROVEN DIRECT DAMAGES;
  - (iii) FOR ANY THIRD-PARTY CLAIMS, THE REMEDIES AVAILABLE UNDER SECTION 7 (Third Party Claims);
  - (iv) FOR CLAIMS ARISING FROM THE OTHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, PROVEN DAMAGES; OR
  - (v) FOR CLAIMS OTHER THAN THOSE SET FORTH IN SECTION 6.1(a)(i)-(iv), PROVEN DIRECT DAMAGES NOT TO EXCEED, ON A PER CLAIM OR AGGREGATE BASIS DURING ANY TWELVE (12) MONTH PERIOD, AN AMOUNT EQUAL TO THE TOTAL NET CHARGES INCURRED BY CUSTOMER FOR THE AFFECTED SERVICE IN THE RELEVANT COUNTRY DURING THE THREE (3) MONTHS PRECEDING THE MONTH IN WHICH THE CLAIM AROSE.
- (b) EXCEPT AS SET FORTH IN SECTION 7 (Third Party Claims) OR IN THE CASE OF A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, RELIANCE OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOST PROFITS, ADVANTAGE, SAVINGS OR REVENUES OR FOR INCREASED COST OF OPERATIONS.
- (c) THE LIMITATIONS IN THIS SECTION 6 SHALL NOT LIMIT CUSTOMER'S RESPONSIBILITY FOR THE PAYMENT OF ALL PROPERLY DUE CHARGES UNDER THIS AGREEMENT.

**6.2 Disclaimer of Liability.** AT&T WILL NOT BE LIABLE FOR ANY DAMAGES ARISING OUT OF OR RELATING TO: INTEROPERABILITY, ACCESS OR INTERCONNECTION OF THE SERVICES WITH APPLICATIONS, DATA, EQUIPMENT, SERVICES, CONTENT OR NETWORKS PROVIDED BY CUSTOMER OR THIRD PARTIES; SERVICE DEFECTS, SERVICE LEVELS, DELAYS OR ANY SERVICE ERROR OR INTERRUPTION, INCLUDING INTERRUPTIONS OR ERRORS IN ROUTING OR COMPLETING ANY 911 OR OTHER EMERGENCY RESPONSE CALLS OR ANY OTHER CALLS OR TRANSMISSIONS (EXCEPT FOR CREDITS EXPLICITLY SET FORTH IN THIS AGREEMENT); LOST OR ALTERED MESSAGES OR TRANSMISSIONS; OR UNAUTHORIZED ACCESS TO OR THEFT, ALTERATION, LOSS OR DESTRUCTION OF CUSTOMER'S (OR ITS AFFILIATES', USERS' OR THIRD PARTIES') APPLICATIONS, CONTENT, DATA, PROGRAMS, INFORMATION, NETWORKS OR SYSTEMS.





**6.3 Purchased Equipment and Vendor Software Warranty.** AT&T shall pass through to Customer any warranties for Purchased Equipment and Vendor Software available from the manufacturer or licensor. The manufacturer or licensor, and not AT&T, is responsible for any such warranty terms and commitments. ALL SOFTWARE AND PURCHASED EQUIPMENT IS OTHERWISE PROVIDED TO CUSTOMER ON AN "AS IS" BASIS.

**6.4 Disclaimer of Warranties.** AT&T MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, SPECIFICALLY DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT AND SPECIFICALLY DISCLAIMS ANY WARRANTY ARISING BY USAGE OF TRADE OR BY COURSE OF DEALING. FURTHER, AT&T MAKES NO REPRESENTATION OR WARRANTY THAT TELEPHONE CALLS OR OTHER TRANSMISSIONS WILL BE ROUTED OR COMPLETED WITHOUT ERROR OR INTERRUPTION (INCLUDING CALLS TO 911 OR ANY SIMILAR EMERGENCY RESPONSE NUMBER) AND MAKES NO GUARANTEE REGARDING NETWORK SECURITY, THE ENCRYPTION EMPLOYED BY ANY SERVICE, THE INTEGRITY OF ANY DATA THAT IS SENT, BACKED UP, STORED OR SUBJECT TO LOAD BALANCING OR THAT AT&T'S SECURITY PROCEDURES WILL PREVENT THE LOSS OR ALTERATION OF OR IMPROPER ACCESS TO CUSTOMER'S DATA AND INFORMATION.

**6.5 Application and Survival.** The disclaimer of warranties and limitations of liability set forth in this Agreement will apply regardless of the form of action, whether in contract, equity, tort, strict liability or otherwise, of whether damages were foreseeable and of whether a party was advised of the possibility of such damages and will apply so as to limit the liability of each party and its Affiliates and their respective employees, directors, subcontractors and suppliers. The limitations of liability and disclaimers set out in this Section 6 will survive failure of any exclusive remedies provided in this Agreement.

## **7. THIRD PARTY CLAIMS –**

**7.1 AT&T's Obligations.** AT&T agrees at its expense to defend and either to settle any third-party claim against Customer, its Affiliates and its and their respective employees and directors or to pay all damages that a court finally awards against such parties for a claim alleging that a Service provided to Customer under this Agreement infringes any patent, trademark, copyright or trade secret, but not where the claimed infringement arises out of or results from: (a) Customer's, its Affiliate's or a User's content; (b) modifications to the Service by Customer, its Affiliate or a third party, or combinations of the Service with any non-AT&T services or products by Customer or others; (c) AT&T's adherence to Customer's





or its Affiliate's written requirements; or (d) use of a Service in violation of this Agreement.

**7.2 Customer's Obligations.** Customer agrees at its expense to defend and either to settle any third-party claim against AT&T, its Affiliates and its and their respective employees, directors, subcontractors and suppliers or to pay all damages that a court finally awards against such parties for a claim that: (a) arises out of Customer's, its Affiliate's or a User's access to or use of the Services and the claim is not the responsibility of AT&T under Section 7.1; (b) alleges that a Service infringes any patent, trademark, copyright or trade secret and falls within the exceptions in Section 7.1; or (c) alleges a breach by Customer, its Affiliate or a User of a Software license agreement.

**7.3 Infringing Services.** Whenever AT&T is liable under Section 7.1, AT&T may at its option either procure the right for Customer to continue using, or may replace or modify, the Service so that it is non-infringing.

**7.4 Notice and Cooperation.** The party seeking defense or settlement of a third-party claim under this Section 7 will provide notice to the other party promptly upon learning of any claim for which defense or settlement may be sought, but failure to do so will have no effect except to the extent the other party is prejudiced by the delay. The party seeking defense or settlement will allow the other party to control the defense and settlement of the claim and will reasonably cooperate with the defense. The defending party will use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim where relief against the party being defended is limited to monetary damages that are paid by the defending party under this Section 7.

**7.5** AT&T's obligations under Section 7.1 shall not extend to actual or alleged infringement or misappropriation of intellectual property based on Purchased Equipment, Software, or Third-Party Services.

## **8. SUSPENSION AND TERMINATION**

**8.1 Termination of Agreement.** This Agreement may be terminated immediately upon notice by either party if the other party becomes insolvent, ceases operations, is the subject of a bankruptcy petition, enters receivership or any state insolvency proceeding or makes an assignment for the benefit of its creditors.







**8.2 Termination or Suspension.** The following additional termination provisions apply:

- (a) **Material Breach.** If either party fails to perform or observe any material warranty, representation, term or condition of this Agreement, including non-payment of charges, and such failure continues unremedied for 30 days after receipt of notice, the aggrieved party may terminate (and AT&T may suspend and later terminate) the affected Service Components and, if the breach materially and adversely affects the entire Agreement, terminate (and AT&T may suspend and later terminate) the entire Agreement.
- (b) **Materially Adverse Impact.** If AT&T revises a Service Publication, the revision has a materially adverse impact on Customer and AT&T does not effect revisions that remedy such materially adverse impact within 30 days after receipt of notice from Customer, then Customer may, as Customer's sole remedy, elect to terminate the affected Service Components on 30 days' notice to AT&T, given not later than 90 days after Customer first learns of the revision to the Service Publication. "Materially adverse impacts" do not include changes to non-stabilized pricing, changes required by governmental authority, or assessment of or changes to additional charges such as surcharges or taxes.
- (c) **Internet Services.** If Customer fails to rectify a violation of the AUP within 5 days after receiving notice from AT&T, AT&T may suspend the affected Service Components. AT&T reserves the right, however, to suspend or terminate immediately when: (i) AT&T's suspension or termination is in response to multiple or repeated AUP violations or complaints; (ii) AT&T is acting in response to a court order or governmental notice that certain conduct must be stopped; or (iii) AT&T reasonably determines that (a) it may be exposed to sanctions, liability, prosecution or other adverse consequences under applicable law if AT&T were to allow the violation to continue; (b) such violation may harm or interfere with the integrity, normal operations or security of AT&T's network or networks with which AT&T is interconnected or may interfere with another customer's use of AT&T services or the Internet; or (c) such violation otherwise presents an imminent risk of harm to AT&T, AT&T's customers or its or their respective employees.
- (d) **Fraud or Abuse.** AT&T may terminate or suspend an affected Service or Service Component and, if the activity materially and adversely affects the entire Agreement, terminate or suspend the entire Agreement, immediately by providing Customer with as much advance notice as is reasonably practicable under the circumstances if Customer, in the course of breaching



the Agreement: (i) commits a fraud upon AT&T; (ii) uses the Service to commit a fraud upon another party; (iii) unlawfully uses the Service; (iv) abuses or misuses AT&T's network or Service; or (v) interferes with another customer's use of AT&T's network or services.

- (e) **Infringing Services.** If the options described in Section 7.3 (Infringing Services) are not reasonably available, AT&T may at its option terminate the affected Services or Service Components without liability other than as stated in Section 7.1 (AT&T's Obligations).
- (f) **Hazardous Materials.** If AT&T encounters any Hazardous Materials at the Site, AT&T may terminate the affected Services or Service Components or may suspend performance until Customer removes and remediates the Hazardous Materials at Customer's expense in accordance with applicable law.

### 8.3 Effect of Termination.

- (a) Termination or suspension by either party of a Service or Service Component does not waive any other rights or remedies a party may have under this Agreement and will not affect the rights and obligations of the parties regarding any other Service or Service Component.
- (b) If a Service or Service Component is terminated, Customer will pay all amounts incurred prior to the effective date of termination.

### 8.4 Termination Charges.

- (a) If Customer terminates this Agreement or an affected Service or Service Component for cause in accordance with the Agreement or if AT&T terminates a Service or Service Component other than for cause, Customer will not be liable for the termination charges set forth in this Section 8.4.
- (b) If Customer or AT&T terminates a Service or Service Component prior to Cutover other than as set forth in Section 8.4(a), Customer (i) will pay any pre-Cutover termination or cancellation charges set out in a Pricing Schedule or Service Publication, or (ii) in the absence of such specified charges, will reimburse AT&T for time and materials incurred prior to the effective date of termination, plus any third party charges resulting from the termination.
- (c) If Customer or AT&T terminates a Service or Service Component after Cutover other than as set forth in Section 8.4(a), Customer will pay applicable termination charges as follows: (i) 50% (unless a different amount is specified





in the Pricing Schedule) of any unpaid recurring charges for the terminated Service or Service Component attributable to the unexpired portion of an applicable Minimum Payment Period; (ii) if termination occurs before the end of an applicable Minimum Retention Period, any associated credits or waived or unpaid non-recurring charges; and (iii) any charges incurred by AT&T from a third party (*i.e.*, not an AT&T Affiliate) due to the termination. The charges set forth in Sections 8.4(c)(i) and (ii) will not apply if a terminated Service Component is replaced with an upgraded Service Component at the same Site, but only if the Minimum Payment Period or Minimum Retention Period, as applicable, (the "Minimum Period") and associated charge for the replacement Service Component are equal to or greater than the corresponding Minimum Period and associated charge for the terminated Service Component, respectively, and if the upgrade is not restricted in the applicable Service Publication.

- (d) In addition, if Customer terminates a Pricing Schedule that has a MARC, Customer will pay an amount equal to 50% of the unsatisfied MARC for the balance of the Pricing Schedule Term.

9. [RESERVED]

10. MISCELLANEOUS PROVISIONS

- 10.1 **Publicity.** Neither party may issue any public statements or announcements relating to the terms of this Agreement or to the provision of Services without the prior written consent of the other party.
- 10.2 **Trademarks.** Each party agrees not to display or use, in advertising or otherwise, any of the other party's trade names, logos, trademarks, service marks or other indicia of origin without the other party's prior written consent, which consent may be revoked at any time by notice.
- 10.3 **Independent Contractor.** Each party is an independent contractor. Neither party controls the other, and neither party nor its Affiliates, employees, agents or contractors are Affiliates, employees, agents or contractors of the other party.
- 10.4 **Force Majeure.** Except for payment of amounts due, neither party will be liable for any delay, failure in performance, loss or damage due to fire, explosion, cable cuts, power blackout, earthquake, flood, strike, embargo, labor disputes, acts of civil or military authority, war, terrorism, acts of God, acts of a public enemy, acts or omissions of carriers or



suppliers, acts of regulatory or governmental agencies or other causes beyond such party's reasonable control.

**10.5 Amendments and Waivers.** Any supplement to or modification or waiver of any provision of this Agreement must be in writing and signed by authorized representatives of both parties. A waiver by either party of any breach of this Agreement will not operate as a waiver of any other breach of this Agreement.

**10.6 Assignment and Subcontracting.**

- (a) Customer may, without AT&T's consent but upon notice to AT&T, assign in whole or relevant part its rights and obligations under this Agreement to a Customer Affiliate. AT&T may, without Customer's consent, assign in whole or relevant part its rights and obligations under this Agreement to an AT&T Affiliate. In no other case may this Agreement be assigned by either party without the prior written consent of the other party (which consent will not be unreasonably withheld or delayed). In the case of any assignment, the assigning party shall remain financially responsible for the performance of the assigned obligations.
- (b) AT&T may subcontract to an Affiliate or a third party work to be performed under this Agreement but will remain financially responsible for the performance of such obligations.
- (c) In countries where AT&T does not have an Affiliate to provide a Service, AT&T may assign its rights and obligations related to such Service to a local service provider, but AT&T will remain responsible to Customer for such obligations. In certain countries, Customer may be required to contract directly with the local service provider.

**10.7 Severability.** If any portion of this Agreement is found to be invalid or unenforceable or if, notwithstanding Section 10.11 (Governing Law), applicable law mandates a different interpretation or result, the remaining provisions will remain in effect and the parties will negotiate in good faith to substitute for such invalid, illegal or unenforceable provision a mutually acceptable provision consistent with the original intention of the parties.

**10.8 Injunctive Relief.** Nothing in this Agreement is intended to or should be construed to prohibit a party from seeking preliminary or permanent injunctive relief in appropriate circumstances from a court of competent jurisdiction.







- 10.9 **Legal Action.** Any legal action arising in connection with this Agreement must be filed within two (2) years after the cause of action accrues, or it will be deemed time-barred and waived. The parties waive any statute of limitations to the contrary.
- 10.10 **Notices.** Any required notices under this Agreement shall be in writing and shall be deemed validly delivered if made by hand (in which case delivery will be deemed to have been effected immediately), or by overnight mail (in which case delivery will be deemed to have been effected one (1) business day after the date of mailing), or by first class pre-paid post (in which case delivery will be deemed to have been effected five (5) days after the date of posting), or by facsimile or electronic transmission (in which case delivery will be deemed to have been effected on the day the transmission was sent). Any such notice shall be sent to the office of the recipient set forth on the cover page of this Agreement or to such other office or recipient as designated in writing from time to time.
- 10.11 **[RESERVED]**
- 10.12 **Compliance with Laws.** Each party will comply with all applicable laws and regulations and with all applicable orders issued by courts or other governmental bodies of competent jurisdiction.
- 10.13 **No Third-Party Beneficiaries.** This Agreement is for the benefit of Customer and AT&T and does not provide any third party (including Users) the right to enforce it or to bring an action for any remedy, claim, liability, reimbursement or cause of action or any other right or privilege.
- 10.14 **Survival.** The respective obligations of Customer and AT&T that by their nature would continue beyond the termination or expiration of this Agreement, including the obligations set forth in Section 5 (Confidential Information), Section 6 (Limitations of Liability and Disclaimers) and Section 7 (Third Party Claims), will survive such termination or expiration.
- 10.15 **Agreement Language.** The language of this Agreement is English. If there is a conflict between this Agreement and any translation, the English version will take precedence.

## 11. DEFINITIONS

**"Affiliate"** of a party means any entity that controls, is controlled by or is under common control with such party.





**"API"** means an application program interface used to make a resources request from a remote implementer program. An API may include coding, specifications for routines, data structures, object classes, and protocols used to communicate between programs.

**"AT&T Software"** means software, including APIs, and all associated written and electronic documentation and data owned by AT&T and licensed by AT&T to Customer. AT&T Software does not include software that is not furnished to Customer.

**"Customer Personal Data"** means information that identifies an individual, that Customer directly or indirectly makes accessible to AT&T and that AT&T collects, holds or uses in the course of providing the Services.

**"Cutover"** means the date Customer's obligation to pay for Services begins.

**"Effective Date"** of a Pricing Schedule means the date on which the last party signs the Pricing Schedule unless a later date is required by regulation or law.

**"MARC-Eligible Charges"** means the recurring and usage charges (including amounts calculated from unpaid charges that are owed under Section 8.4(c)(i)), after deducting applicable discounts and credits (other than outage or SLA credits), that AT&T charges Customer for the Services identified in the applicable Pricing Schedule as MARC-contributing. The following are not MARC-Eligible Charges: (a) charges for or in connection with Customer's purchase of equipment; (b) taxes; and (c) charges imposed in connection with governmentally imposed costs or fees (such as USF, PICC, payphone service provider compensation, E911 and deaf relay charges).

**"Minimum Payment Period"** means the Minimum Payment Period identified for a Service Component in a Pricing Schedule or Service Publication during which Customer is required to pay recurring charges for the Service Component.

**"Minimum Retention Period"** means the Minimum Retention Period identified for a Service Component in a Pricing Schedule or Service Publication during which Customer is required to maintain service to avoid the payment (or repayment) of certain credits, waived charges or amortized charges.

**"Purchased Equipment"** means equipment or other tangible products Customer purchases under this Agreement, including any replacements of Purchased Equipment provided to Customer. Purchased Equipment also includes any internal code required to operate such Equipment. Purchased Equipment does not include Software but does include any physical media provided to Customer on which Software is stored.

**"Service Component"** means an individual component of a Service provided under this Agreement.





**"Service Publications"** means Tariffs, Guidebooks, Service Guides and the AUP.

**"Site"** means a physical location, including Customer's collocation space on AT&T's or its Affiliate's or subcontractor's property, where AT&T installs or provides a Service.

**"Software"** means AT&T Software and Vendor Software.

**"Third-Party Service"** means a service provided directly to Customer by a third party under a separate agreement between Customer and the third party.

**"Vendor Software"** means software, including APIs, and all associated written and electronic documentation and data AT&T furnishes to Customer, other than AT&T Software.



**CERTIFICATION AND SIGNATURE:** By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein;

that I am submitting this bid, offer or proposal for review and consideration \*\*\*  
**SUBJECT TO THE EXCEPTIONS, CLARIFICATIONS, ADDITIONAL TERMS AND CONDITIONS, AND RESPONSES SPECIFIED IN AT&T'S PROPOSAL RESPONSE \*\*\***; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

ATT Corp  
(Company)  
Elizabeth Spradlin Elizabeth Spradlin, Client Solutions Executive  
(Authorized Signature) (Representative Name, Title)

Elizabeth Spradlin, Client Solutions Executive  
(Printed Name and Title of Authorized Representative)

11/27/18  
(Date)

304-690-0140  
(Phone Number) (Fax Number)

## DEFINITIONS, ABBREVIATIONS, ACRONYMS:

1. ANI, Automatic Number Identification
2. COS, Class of Service
3. DID, Direct Inward Dial
4. DNIS, Dialed Number Identification Service
5. E. 164, the International public telecommunication numbering plan





6. High Security, any use case where the Vendor's solution requires a higher security baseline standard. High security use cases are either the result of regulatory or legal compliance requirements and/or risk assessment indicates a higher level of security is warranted.
7. ID, Identification
8. IP, Internet Protocol
9. LAN, Local Area Network
10. LMS, Learning Management System
11. M/S, Millisecond
12. MACD, Move, Add, Change, Delete
13. Microsoft 0365, Microsoft Office 365
14. MPLS, Multiprotocol Label Switching
15. MWI, Message Waiting Indicator
16. PHI, Protected Health Information
17. P II, Personally Identifiable Information
18. PMBOK, Project Management Body of Knowledge
19. PMO, Project Management Office
20. POTS, Plain Old Telephone Service
21. PRI, Primary Rate Interface
22. PS/ALI, Private Switch/Automatic Location Identifier
23. PSAP, Public Safety Answering Point
24. PSTN, Public Switched Telephone Network
25. QoS, Quality of Service
26. SIP, Session Initiation Protocol
27. SOW, Statement of Work





- 28. SRST, Survivable Remote Site Telephony
- 29. Standard Security, any use case where the Vendor's solution does not require heightened security baseline standards. The standard security use case is delineated to provide the State a potentially lower cost option when a standard level of security provides an appropriate level of protection.
- 30. TCR, Telecommunications Change Request
- 31. UCaaS, Unified Communications as a Service
- 32. UCCaaS, Unified Communications and Collaborations as a Service
- 33. VoC, Virtual Contact Center
- 34. VLAN, Virtual Local Area Network
- 35. VoIP, Voice over Internet Protocol
- 36. WAN, Wide Area Network
- 37. WBS, Work Breakdown Structure
- 38. WVOT, West Virginia Office of Technology

**AT&T Response:**

AT&T has read and understands.





#### AT&T'S Response to RFP §§4, 5, and 6:

The State replaced the entirety of §§4 and 5 pursuant to an RFP amendment issued on or around November 2, 2018. AT&T's response to new §4 and new §5 are set forth in a separate document included with the Response. AT&T has deleted former §§4, 5, and 6 from this portion of the Response.





## SECTION 4: PROJECT SPECIFICATIONS

**4.1. Background and Current Operating Environment:** As outlined in the West Virginia State Code # 5A-6-4e "the Chief Technology Officer shall oversee telecommunications services used by state spending units for the purpose of maximizing efficiency to the fullest possible extent". Additionally, per State Code # 5A-6-4a (11), the Chief Technology Officer develops a "unified and integrated structure for information systems for all executive agencies." In pursuance of those objectives, the West Virginia Office of Technology is seeking proposals from Vendors to establish an open-end, Statewide Contract for Managed Voice Services and Hosted Voice over Internet Protocol ("VoIP") Services, encompassing Unified Communications as a Service ("UCaaS"), and Hosted Contact Center Services.

It is the State's intent to establish a contract with a single Vendor to provide maintenance, management, and support for the State's current IP Telephony platforms while working to migrate those telephony services to a fully managed and hosted VoIP solution. Additionally, the Vendor will be expected to provide daily management and operational support for multiple Contact Centers while working to migrate those Contact Centers to its hosted solution.

Currently, the State of West Virginia has an estimated 10,000 phones on multiple Cisco VoIP solutions — 3x Cisco Unified Call Manager and Unity Express, 4x Cisco Unified Call Manager and Unity, 7x Cisco Unified Call Manager and Unity Connection, 1 0x Cisco Unified Call Manager and Unity Connection, Cisco Call Manager Express, ten (10) Cisco Contact Center Version 7 sites, and a Hosted VoIP Solution with Verizon Business Solutions (UCaaS and Contact Center); it is anticipated all of those sites currently utilizing a VoIP solution will be migrated to the Vendor's proposed hosted solution. In addition to the current VoIP Agencies, the State also requires the flexibility to implement a VoIP solution at sites where one does not currently exist. Potentially, the State may leverage the awarded contract to implement another estimated 10,000 users where traditional telephony services exist.

The State of WV's current environments consist of the following:

- Cisco Unified Messaging
- Cisco Unity Connection
- Cisco Unity Express
- Cisco Call Manager Express
- Cisco Contact Center Express
- Cisco Expressway C&E
- Cisco Presence



- Cisco Jabber
- Cisco Gateways using VoIP Session Initiation Protocol ("SIP") Trunks, Primary Rate Interface ("PRI") Circuits, and Analog POTS ("Plain Old Telephone Service") lines
- Microsoft Skype for Business 2016
- Microsoft Active Directory
- Microsoft Office 365
- Cisco Survivable Remote Site Telephony ("SRST")
- Bridge Communications Operator Console
- SingleWire Informacast Paging
- Verizon hosted solution- Unified Communications and Collaborations as a Service (UCCaaS)
- Verizon hosted solution - Virtual Contact Center (VCC)

More information regarding the State's current telephony infrastructure can be found in **Appendix A**.

Meanwhile, the State's current Wide Area Network ("WAN") is undergoing a conversion from Switched Ethernet to Multiprotocol Label Switching ("MPLS") services, which may impact how the Vendor's proposed solution will be implemented. The WVOT is working with Verizon Business to migrate an estimated 500 data circuits across the State with a projected completion of December 2018. Thus far, approximately 275 circuits have been migrated, meaning that the proposed VoIP solution may be implemented at those sites using MPLS circuits to ensure quality of service. The State has deployed Cisco routers for WAN communications. Local Area Networks ("LANs") are comprised of various switches manufactured by Cisco, Hewlett Packard, Brocade, and Extreme.

#### AT&T Response:

AT&T has read and understands.

- 4.2. **Project Goals and Mandatory Requirements:** The State of West Virginia is seeking to establish a contract with a Vendor for the management of the State's current Legacy Environment and to migrate its Legacy Environment to a Hosted VoIP Solution, including Contact Center Services. Vendor should describe its approach and methodology to providing the service or solving the problem described by meeting the goals/objectives identified below. **Vendor's response should include any information about how the proposed approach is superior or inferior to other**





possible approaches as well as identify areas where the proposed solution exceeds the project expectations.

**AT&T Response:**

AT&T has read and understands.

4.2.1. Goals and Objectives — The project goals and objectives are listed below.

4.2.1.1 Voice Services

4.2.1.1.1 Managed Voice Services — Support of State's Legacy IP Environment

4.2.1.1.1.1 The State's goal is to contract with a single Vendor for all application, hardware, and MACD management, maintenance, and support of its current IP Telephony platforms (as described in **Appendix\_A**), with the goal of the Vendor migrating the State's current IP telephony infrastructure, excluding network infrastructure, to a unified, hosted IP platform within 24 months. The State further desires an economical monthly per phone cost for these support services. As such:

The State is proposing the following division of duties for the support of its Legacy IP Environment:

Vendor Duties:

1. Create an operational plan of the State's Legacy IP Environment for the State's review and approval
2. Daily management, operational support, and ongoing maintenance of the State's current telephony environment, as outlined in **Appendix\_A**.
3. MACD changes to the State's current telephony infrastructure.
4. Replacement of failed parts where feasible, outdated telephony equipment, or other telephony components. If the Vendor is unable to furnish parts or replace equipment, the State expects the Vendor to migrate that site to the Vendor's Hosted VoIP platform.





5. Set-up mutually agreed upon standing meetings with the State to address concerns, changes, service interruptions, and project progress.
6. The Vendor should alert the State points of contact after being notified of any service interruptions, in writing, that exceed sixty (60) minutes. The Vendor should provide updates to the State every sixty (60) minutes thereafter until the issue is resolved.

**AT&T Response:**

See AT&T's General Response. AT&T will endeavor to meet all mutually agreed contract obligations; however, AT&T shall not be liable for any problems caused by force majeure, delays due to any fault of the State and/or any contractor or subcontractor employed by the State, network delays, or for problems resulting from causes beyond the reasonable control of AT&T.

7. The Vendor should have a 24x7x365 operations center that includes Tier 1 support to receive trouble tickets and onsite operational support for critical failures.

**AT&T Response:**

See AT&T's General Response. AT&T will endeavor to meet all mutually agreed contract obligations; however, AT&T shall not be liable for any problems caused by force majeure, delays due to any fault of the State and/or any contractor or subcontractor employed by the State, network delays, or for problems resulting from causes beyond the reasonable control of AT&T.

**State Duties:**

1. Management of State's LAN/WAN Network Infrastructure
2. Ordering, disconnecting, and billing services

**AT&T Response:**

AT&T has read and understands.



4.2.1.1.1.2 The State desires the Vendor provide the State with its proposed Operations Plan within 30 calendar days of contract effective date, outlining its plan for managing, supporting, and maintaining the State's current IP telephony infrastructure. The Vendor's Operations Plan should include a strategy for assuming its duties, as outlined above. Please describe your company's experience and strategy in developing operations plans for supporting legacy environments.

**AT&T Response:**

See AT&T's General Response. AT&T will endeavor to meet all mutually agreed contract obligations; however, AT&T shall not be liable for any problems caused by force majeure, delays due to any fault of the State and/or any contractor or subcontractor employed by the State, network delays, or for problems resulting from causes beyond the reasonable control of AT&T.

4.2.1.1.1.3 The State desires that the State and Vendor finalize and agree upon an Operations Plan within 60 calendar days of contract effective date for the management, support, and maintenance of the State's current telephony infrastructure. Please describe your company's ability to deliver the finalized Operations Plan to the State within 60 calendar days of contract effective date with scheduling the appropriate meetings, making changes after State input, and meeting deadlines.

**AT&T Response:**

See AT&T's General Response. AT&T will endeavor to meet all mutually agreed contract obligations; however, AT&T shall not be liable for any problems caused by force majeure, delays due to any fault of the State and/or any contractor or subcontractor employed by the State, network delays, or for problems resulting from causes beyond the reasonable control of AT&T.

4.2.1.1.1.4 The State desires the Vendor to be fully managing its Legacy Environment within 90 calendar days of contract effective date and until all sites wishing to adopt these services have been migrated to a Hosted VoIP solution. Please describe your company's experience in providing support of a Legacy Environment, its experience in taking over existing





infrastructure, and provide a plan showing how this goal can be met.

**AT&T Response:**

See AT&T's General Response. AT&T will endeavor to meet all mutually agreed contract obligations; however, AT&T shall not be liable for any problems caused by force majeure, delays due to any fault of the State and/or any contractor or subcontractor employed by the State, network delays, or for problems resulting from causes beyond the reasonable control of AT&T.

4.2.1.1.1.5 It is the State's desire that the awarded Vendor of this contract will establish a local support system to continue support and maintenance of the State's Legacy IP systems. Please describe your company's ability to provide maintenance and support of the State's Legacy Environment.

**AT&T Response:**

AT&T provide support for remote monitoring and management with support for onsite maintenance when required. AT&T also provides hardware replacement leveraging Cisco Smartnet with a variety of maintenance options based on the critical nature of the equipment and location. Our proactive monitoring allows for alerts to detect equipment failures and coordinate replacement before they become major issue.

4.2.1.1.1.6 The State desires all application, hardware, and MACD support for the State's current telephony infrastructure will be entered via the Vendor's self-service web portal and/or a Vendor-provided toll-free number within 90 calendar days from contract effective date. If the Vendor determines that an issue or problem falls within the State's purview, the Vendor should notify the State's points of contact in writing within one hour of reaching this determination. Please describe your company's support offerings or its ability/plan to accomplish this.

**AT&T Response:**

See AT&T's General Response. AT&T will endeavor to meet all mutually agreed contract obligations; however, AT&T shall not be liable for any problems caused by force majeure, delays due to any fault of the State and/or any contractor or subcontractor





employed by the State, network delays, or for problems resulting from causes beyond the reasonable control of AT&T.

#### 4.2.1.1.2 Transition from the State's Legacy IP Environment to the Vendor's Hosted Solution

4.2.1.1.2.1 The State desires all sites listed in Appendix A be migrated to a Hosted VoIP solution within 730 calendar days from contract effective date. The State reserves the right to reprioritize this list as necessary. Please describe your company's plan to accomplish these migrations.

#### AT&T Response:

See AT&T's General Response. AT&T will endeavor to meet all mutually agreed contract obligations; however, AT&T shall not be liable for any problems caused by force majeure, delays due to any fault of the State and/or any contractor or subcontractor employed by the State, network delays, or for problems resulting from causes beyond the reasonable control of AT&T.

4.2.1.1.2.2 The Vendor should include site preparation and coordination services to implement a turn-key solution at various State locations, including simultaneous deployments to the Vendor's hosted solution. These services should be provided by Vendor personnel knowledgeable in both the Vendor's solution and legacy public switched telephone services. The State desires the Vendor perform site assessment and readiness work for the implementation of its hosted solution, at no additional cost, including a proposed division of duties (Vendor, State), which results in a Statement of Work for each site, as follows:

#### AT&T Response:

AT&T defines 'turnkey' to mean that AT&T will provide only the items of equipment and services specifically listed in this bid response. For the price(s) quoted herein, AT&T will provide the items of equipment and services specifically listed in this bid response. Any additional equipment or services beyond those listed in AT&T's response will be provided at additional charges. Our pricing is predicated on the requirements as set forth by the bid documents, and use of terms and phrases, such as "turn-key" or





"included even if not specifically listed," does not require AT&T to provide equipment or services beyond those specifically noted in our quote.

**VENDOR duties:**

- Gather site's end-user data in order to get site ready for Vendor's hosted solution;
- Provide list of equipment/specifications needed for site readiness, including cabling infrastructure requirements;
- Conduct review to move, at a minimum, existing telephony system to new environment;
- Provide the State with necessary ordering information for TCRs;
- The State owns all data gathered under the scope of the contract and is able to obtain copies of all configuration files gathered as part of this contract. The Vendor should update, maintain the data repository in a manner negotiated with the State upon award, and provide information upon request in an Excel or csv format;

**AT&T Response:**

All intellectual property in the Services shall be the sole and exclusive property of AT&T or its suppliers, as applicable. Each party shall retain all of its rights in its pre-existing intellectual property.

- Configure, tag, label, and drop-ship phones to site;

**STATE duties:**

- Confirm site readiness;
- Coordinate between the Agency, Vendor, and other applicable parties;
- Purchase, configure, update and refresh network hardware;
- Prepare, process, and submit TCR to Vendor based on information provided;
- Place physical phones.



The Vendor should describe its solution's capability to meet or exceed each of these objectives.

### AT&T Response:

AT&T provides the phased approach that includes the following steps

#### Project Planning/Kickoff

- Project kickoff meeting
- Gathering project contact information
- Creating escalation procedures
- Review preliminary project plan/migration schedule
- Review Project Management Tools
- Schedule recurring project status meeting
- Review CPE (BOM) bill of material
- Obtain documentation on current LAN/WAN/Telephony
- Identify **local** Team Sponsors for SRS data collection
- Schedule SRS data collection meeting
- Discuss SRS data collection information to be collected

#### Project Management – For UC Services

- Develop and manage detailed implementation Project Plan/issue tracker
- Develop and manage project migration schedule
- Develop and manage completion of site readiness checklist
- Develop and manage test plans/checklists
- Manage CPE inventory: confirm delivery, inventory and document receipt of hardware.
- Manage and lead recurring project status meetings - provide updated project plan/migration schedule and issue tracker

#### Design and Planning

- Outline and document key criteria that will need to be collected for completion of High Level Design (HLD) and Low Level design (LLD)
  - Review end user provided current state documentation:





- LAN network – validate POE, QoS, Voice VLANS
- WAN/PSTN network – obtain circuit information by location/Client numbers (DID/Toll Free)
- Discuss, review and validate future state design for UC services
- Implement LAN changes
  - PoE, Voice VLAN, QoS, etc.
- Define UC Services
  - Dial plan
  - CSS, Partition,
  - Call Routing design, 911, etc.
- Define Integration Points
  - Routers/Gateways to PSTN/WAN
  - Analog devices
  - Overhead paging/etc.
  - For UC services in Table 2
- Develop SRS and review collection of SRS data provided by end user
  - Build SRS template
  - Review data to be collected by end user
  - Obtain SRS / Finalize SRS
- Finalize Design
  - Define any identified risks or gaps
  - Review and modify future state design BOM (as required)
  - Submit design changes to end user for approval/order

#### **Develop Future State Low Level Design (LLD) and Site Survey**

- Review core requirements collected during discovery meetings
- Review and validate future state Bill of Material, if applicable.
- Identify any technical or functional constraints (product or timeline)
- Complete High Level Design (HLD) and Low Level design (LLD) for UC Services
- Conduct Site Surveys and audits to support capturing accurate up to date information on the existing network

#### **Build and Test**

- UC Service - Build, Test and Troubleshoot
  - UC Application Servers
    - Partitions/CSS
    - Dial Plans





- Call Routing Templates
- For UC services in Table 2
- Configure Routers/Gateways/Switches and UC Applications
- Validate and test

### **Configure Unified Communications Services**

- Provision Unified Communications Service as defined in Table 2
  - UC Applications
  - Routers, switches and analog gateways
  - Subscriber and user accounts (as defined in Table 2)
    - SRS Build
      - Review final SRS spreadsheets
      - Identify and correct missing data, errors or issue on SRS with end user
      - Obtain sign off on SRS
      - Convert final SRS to files
      - Import files to UC Services
      - Review and remediate conflicts for imports
      - Conduct testing of subscribers
    - Auto Attendants (AA)
      - Design Auto Attendant Call Flows
      - Obtain sign off on Auto Attendant Call flows
      - Build Auto Attendant scripts
      - Test Auto Attendant scripts

### **Migration to Unified Communications Services**

- Installation
  - Confirm Racks, Power, etc.
  - Confirm WAN/PSTN in locations
  - Conduct CPE installation
  - Conduct Telephone Placement
- Test Plan Execution
- Migration and Post Migration Support
  - Site Migrations
  - Post migration support
  - Migrated to UC Services Support Team
  - Provide Client Customer Service Manual (CSM) for UC Services Support





## Project Completion Meeting

This meeting is designed to ensure that all deliverables and expectations have been completed. This meeting will be facilitated by the UC Services project manager and should be attended by all individuals with project sign off responsibility. Topics to be covered during this meeting include but are not limited to:

- Review of original project deliverables
- Delivery of final project documentation
- Project Completion Form signoff

### 4.2.1.1.3 Hosted Voice Services

The State's goal is to obtain a reliable, customizable, and scalable UCaaS solution providing hosted voice-over-IP (VOIP) services for an estimated 10,000 state employees located at various sites throughout the State. The State desires these services be provided at no additional cost, except where noted in this section. To that end:

4.2.1.1.3.1 The Vendor's solution should offer four voice packages. These packages should include: A Basic Package with at least Ad Hoc Conferencing, Call Forwarding, Call History, Call Hold, Call Waiting, Caller ID, and Do Not Disturb; an Enhanced Package including at least all features in the Basic package plus Voice Mail (including Immediate Divert to Voicemail and Message Waiting Indicator); a Premium Package including at least all of the features in the Enhanced Package plus Extension Mobility; and an Analog line option. All packages should be available with high and standard security options. Equipment for the analog line package will not be required for this contract. Please describe your Company's offerings.

### AT&T Response:

AT&T UCaaS service user profiles provide a standard set of functionality and supported devices, sold on a Per Unit per Month basis. The bundles offered through AT&T UCaaS correspond to the licensing of UCaaS by Cisco. AT&T has created some additional bundles by combining Unified Messaging with Basic and Foundation licenses.

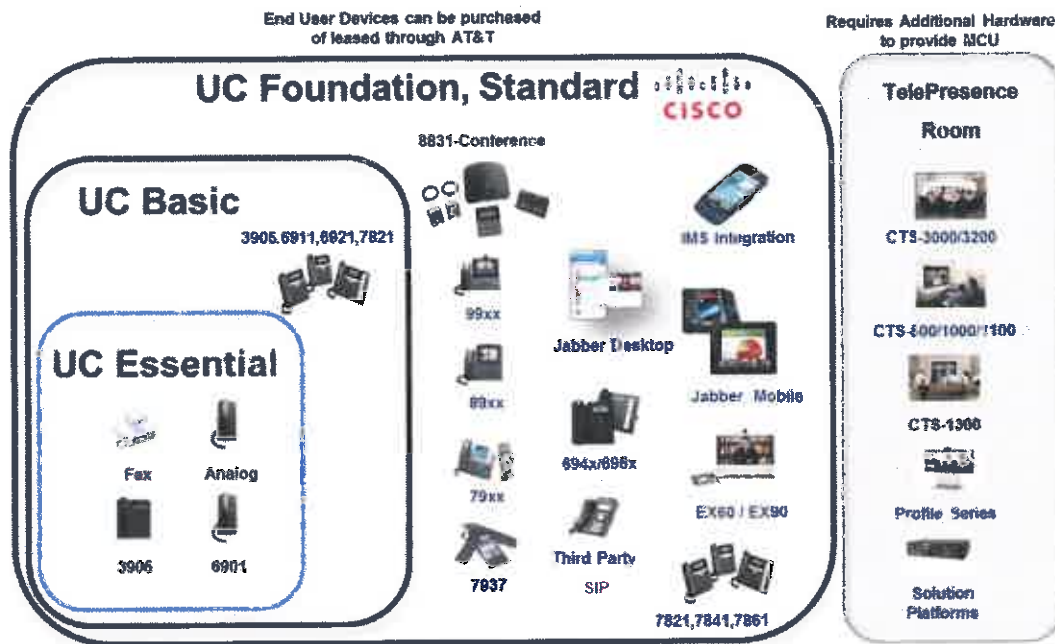
### UC Profile Definition





- UCaaS user profiles are priced per user or per port per month
- The UC Profile price include the end user license, 7X24X365 support, core Geo-Redundant IP PBX, Voice Mail, IM and Presence applications.

#### UC Profile and Cisco Device Options



#### UC Network Operations Support

- AT&T provide all upgrades and patches for security and performance as part of the solution
- Proactive monitoring and management and ticketing is also included
- Fault Isolation and 7X24X365 support for all AT&T contracted services and equipment

#### On Premise Equipment

- Customer can select from a broad range of Cisco IP Phone sets, PC and Mobile soft clients
- Support for analog gateways and local site survivability can also be provided as required
- All on premise equipment can be purchased or leased from AT&T



## Training

- AT&T can provide training on premise; web based and trains the trainer. Additional charges apply for on-site training
- Admin training and end user portal training are also provided as part of the overall deployment

## Enterprise UCaaS User Profiles

The UCaaS end user profiles matrix provides support for specific features and devices, features and options for Cisco Unified Communications Manager and Unity Connection. As new versions of CUCM are released, the UCaaS features and supported devices will be updated.

### Quick Glance UCaaS User Profiles

UC Profile	Functionality	Devices Supported
Essential	<ul style="list-style-type: none"><li>• Voice dial tone / Call Control for analog devices</li><li>• 1 Device</li></ul>	<ul style="list-style-type: none"><li>• Fax</li><li>• Analog</li><li>• 3905</li><li>• 6901</li></ul>
Basic	<ul style="list-style-type: none"><li>• Voice dial tone / Call Control</li><li>• Single Number Reach mobility</li><li>• 1 Device</li></ul>	<ul style="list-style-type: none"><li>• 6911</li><li>• 7821</li><li>• 6921</li><li>• 3905</li></ul>
Foundation	<ul style="list-style-type: none"><li>• Voice dial tone / Call Control</li><li>• Single Number Reach mobility</li><li>• Instant Messaging &amp; Presence</li><li>• Video Calling (point to point) without MCU</li><li>• Desktop Client License</li><li>• Mobile Device Client License</li><li>• Supports 1 Device</li></ul>	<ul style="list-style-type: none"><li>• 6911, 6921</li><li>• 79XX,88XX, 89XX, 99XX series</li><li>• 7800 series</li><li>• Jabber Desktop &amp; Mobile</li><li>• Third Party SIP</li><li>• EX60, EX90</li><li>• IMS Integration</li></ul>
Foundation + VM	<ul style="list-style-type: none"><li>• Voice dial tone / Call Control</li><li>• Single Number Reach mobility</li><li>• Instant Messaging &amp; Presence</li><li>• Video Calling (point to point ) without MCU</li><li>• Desktop Client License</li><li>• Mobile Device Client License</li><li>• Voice Mail</li><li>• Supports 1 Device</li></ul>	<ul style="list-style-type: none"><li>• 6911, 6921</li><li>• 79XX,88XX, 89XX, 99XX series</li><li>• 694X, 696X</li><li>• Jabber Desktop &amp; Mobile</li><li>• Third Party SIP</li><li>• EX60, EX90</li><li>• IMS Integration</li></ul>





UC Profile	Functionality	Devices Supported
Standard	<ul style="list-style-type: none"> <li>• Voice dial tone / Call Control</li> <li>• Single Number Reach mobility</li> <li>• Instant Messaging &amp; Presence</li> <li>• Video Calling</li> <li>• Desktop Client License</li> <li>• Mobile Device Client License</li> <li>• Unified Messaging</li> <li>• Supports up to 10 Devices</li> </ul>	<ul style="list-style-type: none"> <li>• 6911, 6921</li> <li>• 79XX, 88XX, 89XX, 99XX</li> <li>• 694X, 696X</li> <li>• 7800 series</li> <li>• Jabber Desktop &amp; Mobile</li> <li>• Third Party SIP</li> <li>• EX60, EX90</li> <li>• IMS Integration</li> <li>• Video End Points</li> </ul>

#### UCaaS Supported Devices, Features and Options

Collaboration Features	UCaaS Essential/Basic Features	UCaaS Foundation	UCaaS Foundation +VM Features	UCaaS Standard Features
<b>Call Features:</b>				
Coordinated dial plan	X	X	X	X
Barge: single button	X	X	X	X
Call Forward: All, Busy, No Answer.	X	X	X	X
Call Hold/Resume: includes Music on Hold, Tone on Hold	X	X	X	X
Call Park	X	X	X	X
Call Waiting	X	X	X	X
Call Pickup and Group Call Pickup	X	X	X	X
Call Transfer: Direct, Consultative, Blind, Complete transfer on hang up	X	X	X	X
Do not Disturb: do not ring, call reject	X	X	X	X
On-Hook and Off-Hook Dialing	X	X	X	X
Join across lines: allows user to join callers from different lines	X	X	X	X
Point to Point Video Calls	N/A	N/A	X	X
<b>Conferencing:</b>				
Ad hoc Conferencing (up to 8 participants)	X	X	X	X
Multi-Party Meet Me/Ad Hoc Conferencing: Dependent on phone,	X	X	X	X





Collaboration Features	UCaaS Essential/Basic Features	UCaaS Foundation	UCaaS Foundation +VM Features	UCaaS Standard Features
allows user to establish conference that attendees can direct dial into Limited to 10 participants per CUCM instance				
<b>Phone Features:</b>				
Audible and Visual Indication of Ringing Line: Indicator light on IP phone/handset, distinctive ring per line, distinctive ring (external vs. internal), User configurable ring settings (Requires specific phone model to support)	X	X	X	X
Call Status per Line: on Cisco IP phone showing connected state, number and timer of call duration	X	X	X	X
Standard Soft-Key Support	X	X	X	X
Answer/Release: soft key to answer/end call on Cisco IP phone	X	X	X	X
User configurable ring setting	X	X	X	X
Direct Outward Dial (DOD)	X	X	X	X
Abbreviated dialing: speed dialing (Requires specific phone model to support)	X	X	X	X
Multiple Line Appearances: number based on Cisco IP phone	N/A	X	X	X
<b>Incoming Call Routing:</b>				
Direct Inward Dial (DID)	X	X	X	X
Calling Line ID ( When Supported by PSTN)	X	X	X	X
Calling Name ID (When Supported by PSTN)	X	X	X	X
Dialed Number ID Service (DNIS): receipt/passing of dialed number	X	X	X	X
Multiple Calls Per Line: Depending on phone, can support up to 4 calls on a single line	X	X	X	X



Collaboration Features	UCaaS Essential/Basic Features	UCaaS Foundation	UCaaS Foundation +VM Features	UCaaS Standard Features
Hunt Groups: Longest Idle Hunting, Broadcast Hunting, Queuing with Music-on-Hold, Native Hunt Groups	X	X	X	X
Shared/Bridged Line Appearances: same number on multiple phones Note: (Not available when UC Central Client associated with user and device)	X	X	X	X
<b>Assistant/Manager Control:</b>				
Manager-Assistant Service: Assistant can answer calls for manager, configure preferences; managers can enable do not disturb, send all calls, immediate divert, transfer to voicemail, call intercept	N/A	N/A	N/A	X
<b>Web Attendant Console (separate product):</b>				
Department attendant console: Web app for up to 150 phones. (Some features require additional software, specific hardware and configuration to support.)	NA	NA	X	X
Business attendant console: Web app for up to 500 phones. (Some features require additional software, specific hardware and configuration to support.)	N/A	NA	X	X
Enterprise attendant console: Supports up to 25 attendants and 100,000 phones. (Some features require additional software, specific hardware and configuration to support.)	N/A	NA	X	X
Manager attendant console: Basic attendant console. (Some features require additional software, specific hardware and configuration to support.)	N/A	NA	X	X
<b>Phone Expansion Modules (7915, 7916, KEM)</b>				





Collaboration Features	UCaaS Essential/Basic Features	UCaaS Foundation	UCaaS Foundation +VM Features	UCaaS Standard Features
Attendant console side car models 7915 and 7916 provide up to 24 additional line appearances when connect to either a Cisco 7965 or 7962 IP Phone. Up to two sidecars can be combined per IP phone to provide up to 48 line appearances. 9971, 9951 utilizes KEM up to 133 lines.	N/A	N/A	N/A	X
The line keys can be programmed to provide Busy Lamp Fields (BLF) for use with executive assistance or receptionists desks. (Some features require additional software, specific hardware and configuration to support.)				
<b>Extension Mobility:</b>				
Extension Mobility -User can log onto IP phone within their organization and apply their user profile and number.	N/A	N/A	X	X
Advanced Extension Mobility: with Feature Safe and Extension Mobility across clusters	N/A	N/A	X	X
<b>Directories:</b>				
Personal Address Book: IP phone app which stores personal address book	N/A	X	X	X
Directories: On Cisco IP phone for corporate directory, missed calls, placed calls, received calls, personal directory	N/A	X	X	
<b>Video Telephony:</b>				
Cisco VT Advantage and Cisco 9800-9900 series phone with optional video camera) Point to Point Video only. EX-60 and EX-90	N/A	N/A	X	X
<b>IP Phones</b>				
69xx, 79xx, 9800, 9900, 8800, 7800, 8900 series phones	X	X	X	X



Collaboration Features	UCaaS Essential/Basic Features	UCaaS Foundation	UCaaS Foundation +VM Features	UCaaS Standard Features
<b>Single Number Reach</b>				
Single number reach: Call processing to customer defined devices. Up to 4 devices	X	X	X	X
Single number reach: with time of day access	X	X	X	X
<b>Conference IP Phones:</b>				
7935, 7937G, 8831 series as well as certified analog and SIP based conference units	N/A	X	X	X
<b>Voicemail:</b>				
Record up to five personal greetings: alternative, busy, internal, of hours or standard	N/A	N/A	X	X
Can specify after greeting action: callers can leave message, sign in, hang up or be sent to call handlers, directory handlers, interview handlers or other users	N/A	N/A	X	X
Can send notifications for messages from a particular user or phone number	N/A	N/A	X	X
Can create private distribution list and send messages to this list	N/A	N/A	X	X
<b>Security:</b>				
Password and PIN policy options: to enforce expiration, complexity, reuse and lockouts supported	N/A	N/A	X	X
Call restriction tables to prevent toll fraud	N/A	N/A	X	X
Secure private messaging: prevents playing of private messages forwarded outside of enterprise	N/A	N/A	X	X
Voice message aging policies: deletes messages beyond specified number of days for all users	N/A	N/A	X	X
Voice message aging policies: set on a user basis	N/A	N/A	X	X







Collaboration Features	UCaaS Essential/Basic Features	UCaaS Foundation	UCaaS Foundation +VM Features	UCaaS Standard Features
HTTPS for secure web access	N/A	N/A	X	X
SRTP, TLS and Secure SIP Port Support	N/A	N/A	X	X
<b>Voicemail Access:</b>				
Process messages: repeat, reply, record, forward, delete, save, mark as new, hear day or time stamp, skip to next message	N/A	N/A	X	X
Play messages: reverse, pause, or fast forward message, control volume, speed	N/A	N/A	X	X
Address message to multiple recipients	N/A	N/A	X	X
Remove introductions to forwarded messages	N/A	N/A	X	X
Search for messages by name, caller ID, phone number, extension	N/A	N/A	X	X
Mark message as regular, urgent, and private messages	N/A	N/A	X	X
Create secure messages: no playback when sent outside of company	N/A	N/A	X	X
Record message for future delivery	N/A	N/A	X	X
Request return receipt for recorded message	N/A	N/A	X	X
Live record conversation and have recording sent to mailbox	N/A	N/A	X	X
Live reply (Internal and external callers): immediately reply to messages from other users	N/A	N/A	X	X
Address message by extension or by name	N/A	N/A	X	X
Message delivery to non-subscribers or subscribers at non-office telephone numbers	N/A	N/A	X	X
<b>Unified Messaging via IMAP</b>				
View email, voicemail, fax messages together from an IMAP client: MS	N/A	N/A	N/A	X



Collaboration Features	UCaaS Essential/Basic Features	UCaaS Foundation	UCaaS Foundation +VM Features	UCaaS Standard Features
Outlook, IBM Lotus Notes, Entourage for Mac. (There may be additional cost to configure Lotus Notes or Entourage for Mac)				
Cisco View Mail for Outlook and Cisco View Mail for Notes plug-in allow user to compose, reply to, forward, play, rewind, or pause messages from mail client. (There may be additional cost to configure ViewMail for Outlook or Notes.)	N/A	N/A	N/A	X
IBM SameTime voicemail plug-in: view and play messages through IM client	N/A	N/A	N/A	X
<b>Visual Voicemail:</b>				
View voice message like email on Cisco IP phone display: view, listen, and respond to messages right from IP Phone display, without having to dial into your corporate voicemail box	N/A	N/A	N/A	X
<b>Auto Attendant :</b>				
Call Management: Call Handlers, Directory Handlers, Interview Handlers, Call Routing, Schedules & Holidays. Note: (Requires purchase of one voice mail port per call handler, directory handler or interview handler) VM port allows for up to 4 primary options to be created with each primary option having up to 4 sub options. Additional options beyond the 4X4 options or custom outbound dialer's requirements require additional cost to support. Additional cost will be based on time to setup beyond standard call handlers	N/A	N/A	X	X
<b>Desktop Client Support:</b>				
Cisco IP Communicator Soft phone for PC	X	X	X	X



Collaboration Features	UCaaS Essential/Basic Features	UCaaS Foundation	UCaaS Foundation +VM Features	UCaaS Standard Features
<b>Presence (dependent on phone):</b>				
Presence: Others can monitor real-time status of other parties/entities available from Busy Lamp Field/Speed Dial Buttons; Missed Call, Placed Call or Received Call Lists in directories window; Shared Directories. Requires UC Central Client or Jabber Client to support in addition to UCV port	N/A	N/A	X	X
<b>Fax/Modem Support:</b>				
Fax/Modem over IP: Fax Pass-Through, Cisco Fax-Relay, T.38 Fax-Relay, Modem Pass-Through, Cisco Modem Relay, SIP T.38	X	X	N/A	N/A
Features not specific to VoIP port option. Analog port on Cisco voice gateways maybe required				
<b>Analog Device Support:</b>				
Fax/Modem, Over-head paging system, analog phone, elevator phones. Requires separate analog voice gateway and selection of voice port	X	X	X	X
<b>Cisco Emergency Responder and Enhanced E911 support: Separate hardware and services required (Not part of UCaaS)#</b>				
Cisco Emergency Responder supports E911 location definitions that specify the end users location as well as caller line information for end users when accompanied by PS-ALL or Carrier locator ID services. Requires additional consulting services to setup and support. UCV Port required to support call processing for end user	X	X	X	X
<b>911 support #</b>				



Collaboration Features	UCaaS Essential/Basic Features	UCaaS Foundation	UCaaS Foundation +VM Features	UCaaS Standard Features
Basic 911 call processing is supported via PSTN network transport leveraging Cisco CUCM. UC Fusion end user phone number is provided to the Public Service Answering Point (PSAP) via the PSTN access circuit and primary leading DID number associated with the circuit servicing the customer location. (T1-PRI, E1-PRI, IP Flex with Branch office Exchange defined)	X	X	X	X

### 911 Services and Limitations

The UCaaS service is a Voice over Internet Protocol (VoIP) service that manages emergency service calls (911 or E911) in a different manner from traditional analog or digital emergency service calls. E911 service relies on the Customer to register physical locations associated with phone numbers so emergency calls can be routed to the proper Public Safety Answering Point (or Public Safety Access Point – PSAP). The Customer is responsible for updating registered locations associated with user devices to allow the correct automatic number information (ANI) and automatic location information (ALI) to be passed to a local emergency service operator. A Registered Location is a single physical location associated with each Customer device registered to the AT&T UCaaS service, consisting of a valid mailing address and any additional premise information required by applicable 911 or E911 laws or government regulations. Accurate location information cannot be guaranteed for mobile VoIP devices. AT&T also supports Cisco Emergency Responder (CER) and Intrado as part of solution offering when E911 with PS-ALI services is required to define specific floor space or location within a building.

### UCaaS Supported Device Options (Separately Priced as Options)

Supported Hardware	Description
Cisco Voice Gateways	Cisco 1800, 2800-2900, 3800-3900, 4300, 4400 AS-5400, 7200 series routers equipment with PVDM modules and all voice interface card types.



Supported Hardware	Description
Cisco Voice Interface Modules	Cisco analog voice interfaces for ISR routers all revisions ( VIC-2FXO, VIC-2FXS, VIC-4FXO, VIC4FXS, all high density analog router blades ) Note: Requires DSP PVDM resources on router
Cisco Analog Voice Gateways	Cisco Analog Gateways VG224, VG202, VG204 ATA-187, PIMG, TIMG, VG320
Cisco IP Phone Models	Cisco Unified IP Phone Series 6900 ( 6901, 6911,6921,6941,6961) Cisco Unified IP Phone Series 7900 ( 7941, 7961, 7942, 7962, 7945, 7965, 7970, 7975) Cisco Unified IP Phone Series 9900 (9971, 9951) Cisco Unified IP Phone Series 7800 Cisco Unified IP Phone Series 8800-8900
Cisco IP Conference Units	Cisco Unified IP Phone 7937G , 8831, Cisco certified SIP units are also supported
Video Support	Cisco CTS, EX, SX, Polycom , others via cloud bridging and third party units from Polycom

#### UCaaS Supported Application Options (Separately Priced as Options)

Applications Support	Description
Cisco IP Communicator	Soft Phone features support on PC. Requires coordination with end users and customer security team to ensure media and signaling ports are open to support call processing. Specific VPN clients may be required to support operation for remote users.
Cisco Jabber for Mobile	Requires use of Cisco Anyconnect client to support Jabber soft phone options for iPhone, IPAD, MAC, and Android. Blackberry requires separate MVS server not a part of UCaaS Services offering.
Cisco Jabber	Cisco Jabber for PC, iPhone and Android provide click to call as well as presence and IM. Requires selection for UC Voice port to support call processing.
Cisco Webex Conferencing	Cisco WebEx, providing shared desktop capabilities for presentations, shared whiteboard, and controlled sharing of a common desktop.
Video Conferencing (CMS)	Cloud video conferencing bridging support
Hosted Microsoft Exchange	Hosted Microsoft Exchange messaging, calendaring, and contact system.

#### UCaaS Supported Application Options (Separately Priced as Options)

Auto Attendant Support	Description
Call Handlers	Allows voice mail port to be configured to support inbound selectable call options with prompt defining each option. Upon selecting an option the inbound call is directed a specific end user or hunt group number. There are no queuing options or statistics for inbound calls provide with call handlers. Each voice mail port can be defined up to 4 primary options





Auto Attendant Support	Description
	with 4 sub options. Additional primary and sub options can be configured for additional cost based on the time required to configure.
Directory Handlers	Directory handlers allow for the selection of end user to call based directory number. Voice mail port is required to support directory handlers.
Interview Handlers	Interview handlers allow for a voice port to be configured and to have specific question defined and the ability to capture the response from the calling party. Interview handlers require purchase of voice mail port and call prompts to be recorded by the customer.
Call Routing, Time of day and Holiday schedulers	Call routing allows for voice mail port to be setup to support after hours, time of day and holiday call routing. These option can be applied to call handlers and requires purchase of voice mail port

#### Attributes of UCaaS

- Hardware, software and licensing to provide hosted UCaaS
- Maintenance for hardware, software and licensing
- Connectivity to SIP trunking, PSTN and LD usage are optional services priced separately.
- Datacenter facilities
- Private network connectivity from the client's network into the AT&T Data Centers is NOT included. Network Engineering services are available to help design and implement this connectivity is based on port access speed (1Gbps and 10Gbps). The customer may order and own the telecom service, or the customer may choose to order service through another telecom partner.

### 3.1 UC Global UC Network

AT&T leverages our Global UC Nodes and our AT&T IP Flex reach services as well as partnerships with other SIP trunk service providers to support centralized call processing to customer defined locations. AT&T provides managed voice gateway service to provide support for locations that require local PSTN access in countries with regulatory restrictions requiring local carrier PSTN access. The voice gateways will have SIP signaling control from our UC nodes with local TDM or SIP media within country. AT&T will develop a coordinated dial plan to support on-net and off net dialing with least cost call routing. The diagram below provides a high level view of our standard global UC services approach. Each AT&T UC node provides IPT, Video, IM, Contact Center, Voice Mail and Unified Messaging applications. The UC nodes are located in ASIA, North America and EMEA in order to provide reduction in round trip delay for voice and video applications and each UC node is equipped with redundant core LAN, WAN and Session Boarder control. This most of world access approach allows AT&T to provide services to





locations across the globe. We also provide unique back up solutions to ensure the locations are always accessible. AT&T in addition to MPLS can also deliver connectivity over SD-WAN with broadband or mobile 3G, 4G and LTE. AT&T provides end to end network connectivity via our AVPN network MPLS services.

4.2.1.1.3.2 The State desires six handset options for use under this contract: a 2-line phone, a 6-line phone with sidecar capabilities, a conference phone, a softphone, a wireless phone, and an ADA-compliant hardware option. The State further desires a leasing option for all handsets on this contract, by which the State will pay a monthly lease price to be added to the price of the monthly voice package. In the event that a phone is broken or stops functioning, the State desires the Vendor replace that phone, at no additional cost. Additionally, the State desires that the Vendor refresh equipment in-line with the Original Equipment Manufacturer's refresh program, at no additional cost. At the end of the contract, the State will own all of the phones. Please describe your company's leasing options, refresh programs, and ability to meet this goal.

#### AT&T Response:

AT&T provides options for the complete line of Cisco IP Phones, video end points and soft clients to support the States requirements. AT&T aligns with vendors end of sale and end of life programs and provides refresh programs for phones, gateways and includes all upgrades to core applications as part of the UC as a Service.

4.2.1.1.3.3 The State utilizes Cisco SRST and local voice services in case of data network failure. At the initial deployment of the site to the Vendor's hosted solution, if requested, the Vendor should work with an Agency to implement call control and PSTN connectivity, in case the data network fails at a State location. This should include the provisioning of at least one local phone line for 911 calling. The Vendor should include the provisioning of one failover line in the cost of its monthly package. If the site requests more than one failover line, the State understands there may be additional charges for that work. Please describe your solution's ability to meet this goal and any additional costs.



**AT&T Response:**

AT&T provides support for SRST configuration as well as new solutions that provide for Integrated SDWAN that can provide failover via Broadband and LTE reducing the cost of future deployment of SRST. AT&T will work with the State to demonstrate some new concepts for high availability.

4.2.1.1.3.4 The Vendor's solution should support station-to-station calling that remains "on-net" (on the State's private data network) at no additional cost. Please describe your solution's ability to meet this goal.

**AT&T Response:**

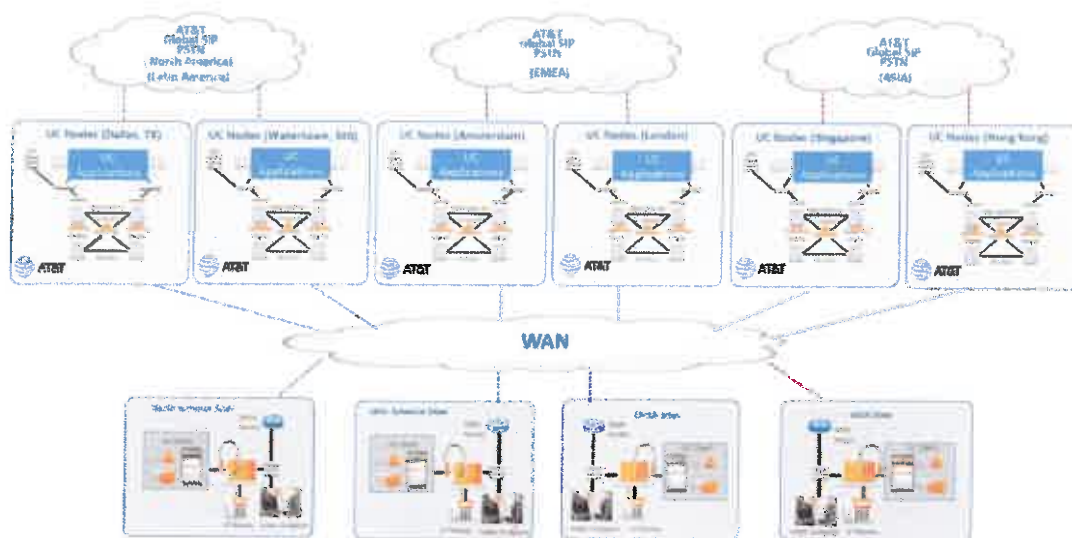
AT&T provide coordinated dial plans that ensure that calls placed between State locations utilize on-net connections to establish calls via least cost routing detection.

4.2.1.1.3.5 The Vendor's solution should provide at least two PSTN connections via SIP Trunks over secure private connections engineered for voice quality of service. These PSTN connections should adhere to the industry standard of 150 m/s latency or better, and jitter of 40 m/s or better. Please describe your network engineering architecture and your practices to continuously achieve these standards.

**AT&T Response:**

AT&T provides geo-redundant UC nodes that provide for redundant SBC and SIP trunking at each node to ensure high availability between core processing applications. Each UC node is also equipped with redundant applications and hardware with automatic alternate routing to support transition between network access as well as support PSTN access resiliency. AT&T UC as a Service is global service which can provide support for local user, but also for users that maybe traveling in North America, EMEA, ASIA, and Latin America. AT&T support access via MPLS, Broadband and Mobile.





4.2.1.1.3.6 The Vendor's solution should provide a MPLS network connection to Verizon's MPLS core to reduce and/or eliminate the backhaul of traffic to the State's core network. The State has provided a column on the Attachment a Cost Sheet for both one-time installation costs and for monthly recurring costs for these connections. Please describe your ability to meet this goal.

#### AT&T Response:

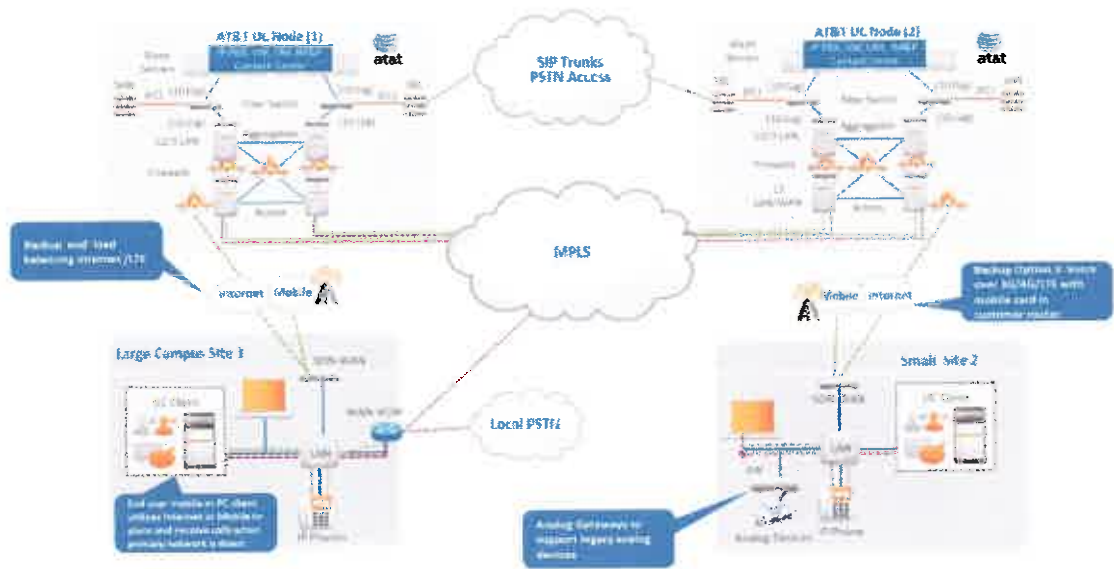
AT&T can support NNI as well as supporting direct extension of existing Verizon MPLS into our UC node data centers. This allows for the AT&T solution to look just like another site on the current State backbone network and utilize existing routing tables and extend State security boundaries.

4.2.1.1.3.7 As an option for small sites with non-private network handoffs, the State desires a solution utilizing public networking with the ability to securely transmit sensitive data. Please describe any offerings to support this goal.

#### AT&T Response:

AT&T provides our Integrated SDWAN that can support secure access from remote user sites utilizing our Secure Vector Routing protocol that is session aware and can support primary access as well as LTE services to connect small remote sites.





4.2.1.1.3.8 The Vendor's solution should include Caller ID services (inbound traffic) and custom number and naming (outbound traffic) that State Agencies may utilize to customize their displayed information. The Vendor should provide this capability at no additional cost. Please describe your solution's ability to provide these services.

#### AT&T Response:

All feature defined are provided as part of the standard AT&T services at no extra charge.

4.2.1.1.3.9 The Vendor's solution should include unlimited local and nationwide calling at no additional charge. Please describe your no cost offerings.

#### AT&T Response:

AT&T UC as a Service offers a full array of voice features, including mobile client, call forwarding, three-way calling, auto attendant, and music on hold, as well as unlimited local and long distance calling within the U.S. via our centralized SIP trunk services

4.2.1.1.3.10 The Vendor's solution should provide international calling. The State understands fees may be associated with international calling. The Vendor should provide it's per





minute international calling rates for Mexico, Canada, and Jamaica in the **Attachment Cost Sheet**. These will be used as part of the cost evaluation. The Vendor should also attach an appendix of its international calling rates for all countries. This appendix will be used to establish the international calling rates per country in the awarded contract and will be required prior to award. Please describe your solution's international calling offerings.

**AT&T Response:**

AT&T provides support for international calling as part of our global SIP services and included rates in the State provided pricing sheet

4.2.1.1.3.11 The Vendor's solution should provide comprehensive site coverage to meet the State's local and long-distance IP-based calling requirements. Please describe your coverage, as well as how you plan to meet the State's coverage needs.

**AT&T Response:**

AT&T centralized SIP services provide local, LD and International calling integrated with coordinated dial plan to direct calls on-net and local off-net dynamically using E.164 dial plan.

4.2.1.1.3.12 The Vendor's solution should provide load balancing for all traffic in-bound from the PSTN. Please describe your solution's ability to meet this goal.

**AT&T Response:**

AT&T provide load balancing as well as automatic alternate routing of traffic in the event of failure of primary path between our geo-redundant data centers as a standard component of our UC services.

4.2.1.1.3.13 The Vendor's solution should ensure 911 call delivery to the appropriate local PSAPS. Additionally, the State desires support for Private Switch/Automatic Location Identification (PS/ALI) services for 911 calls. Please describe your process for ensuring the accuracy of 911 call delivery, as well as the process to support PS/ALI.



**AT&T Response:**

AT&T provides support for E911 services as well as PS-ALI E911 to define location and accurately extend the caller ID mapping of information via ALI data base to the appropriate local PSAP as well as can support directing calls to security desk within specific facilities when required.

4.2.1.1.3.14 The Vendor's solution should support the following industry standard protocols: G.711 (uncompressed), G.729 (compression), and T.38 (fax). Please describe the protocols supported by your solution.

**AT&T Response:**

AT&T supports G.711, G.729, T.38, SIP TLS, SRTP, RTP and Secure Vector Routing.

4.2.1.1.3.15 The Vendor's solution should have the ability to scale the number of simultaneous concurrent calls on a monthly and/or seasonal basis at the State's request. Please describe your solution's ability and your process to accomplish this, including division of duties.

**AT&T Response:**

AT&T provides for dynamic bandwidth allocation from our UC nodes and our centralized SIP trunks and SBC clusters. As traffic volumes raise or fall the session awareness of the systems adjust dynamically without manual intervention.

4.2.1.1.3.16 The Vendor's solution should include interoperability with the following: IPv4 addressing (RFC 791), RFC 1918 for private IP addressing, and support SIP over TCP or UDP. Carrier NAT (RFC 6598), link-local IP addresses (RFC 3927), and Multicast addresses (RFC 3171) will not be accepted. Please describe your solution's interoperability to accomplish this goal.

**AT&T Response:**

AT&T support all standard protocols and RFC's defines by the state including Secure Vector Routing, SIP TLS, SRTP and WebRTC.





4.2.1.1.3.17 The Vendor's solution should provide the following quality and reliability standards: QoS tagging IEEE 802.1 Q-2011; not rewriting, marking, or remarking any VLAN tags affixed to packets by the State, without the State's expressed consent; at a minimum, one Class of Service (COS) marking per Ethernet service. Please describe your solution's ability to meet this goal.

**AT&T Response:**

You can use the AT&T Collaborate™ Class of Service (Coos) feature to help ensure that the network routes your voice traffic with top priority.

We recommend that you configure your routers to assign real-time handling to 90% of your traffic. You can do this by using a Differentiated Services Code Point (DSCP) marking of 46 for both Session Initiated Protocol (SIP) packets and Real-time Transport Protocol (RTP) packets.

4.2.1.1.3.18 The State desires a Unified Messaging solution; therefore, the Vendor's solution should fully integrate with Microsoft 0365, allowing users to listen, forward, and delete voicemails from both 0365 and the hosted environment. Voicemails should be retained in the solution for 15 days or longer. In addition, the Vendor's solution should be provisioned to fully integrate with the State's Active Directory and Active Directory Federated Services. Please describe your abilities to meet these goals.

**AT&T Response:**

AT&T supports native extension of Voice Mail to Unified messaging and support for 0365. Unity Connection accesses Office 365 mailboxes using a domain service account called the unified messaging services account. After you create the account, you grant it the rights necessary for Unity Connection to perform operations on behalf of the user.

4.2.1.1.3.19 Some State Agencies utilize paging and notification to the PC desktop, over-head paging, or through-the-phone speaker paging. The Vendor's solution should include an option for providing, maintaining, and supporting a paging solution, including any associated hardware, software, and licenses, and if requested by Agency, or integrate with an existing or



Agency-owned paging solution. The State understands there may be fees associated with this offering. Please describe your offerings with respect to these deployments.

#### AT&T Response:

AT&T will use due care, but AT&T does not assume responsibility for interactions with pre-existing systems.

4.2.1.1.3.20 The State desires an option for Agencies with high call volume and receptionist personnel that will utilize an Operator Console for fast and efficient call control. The State understands there may be fees associated with this offering. Please describe your solution's Operator Console offerings.

#### AT&T Response:

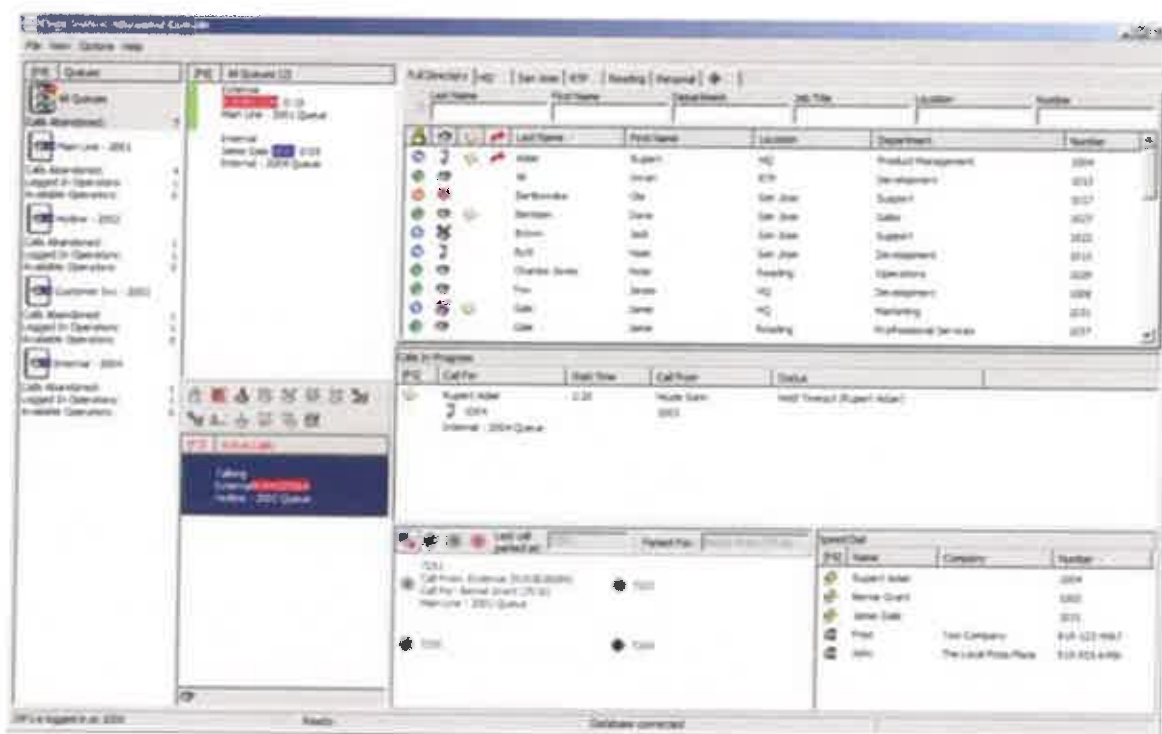
AT&T provided Cloud Attendant Console based on the quantity of users per location as part of the services based on a one time setup fee and MRC per attendant for softphone as well as IP Phone users with client desktop for attendant console. The service can be extended to all UC as a Service site.

Cisco® Unified Attendant Console Advanced gives users the tools required to confidently, efficiently, and professionally tend to incoming calls. Within the console client, users see all console queue activity, shared active call notes, and informative call tags for held, recalled, and parked calls. The customizable contact directory presents contact phone line (BLF), Cisco Jabber®, and Skype for Business status.

Cisco Unified Attendant Console Advanced







Cisco Unified Attendant Console Advanced uses a web-based administration utility to guide you through configuring and managing the application server. The attendant console client software is loaded onto each user's desktop PC.

Cisco Unified Attendant Console Advanced controls and monitors Cisco Unified IP Phones and Cisco Jabber soft phones registered with your Cisco Unified Communications Manager or Cisco Business Edition platform.

#### Features and benefits

Cisco Unified Attendant Console Advanced is built around the core competencies of a console user. Having all call controls, a searchable corporate directory, and queue visibility in a single user interface allows users to operate more efficiently and with a greater focus on the caller's experience.

Table 1 outlines an extended list of Cisco Unified Attendant Console Advanced features and benefits.





#### Features and benefits

Feature	Benefit
Queue features	
Support for 100 queues with prioritization	Configure queue names and priorities to match your call answering requirements. You can prioritize and answer calls out of order. For example, you might have a sales queue, a service queue, and a general business queue. Sales calls can be prioritized and answered first, before service or general business calls.
Operator queue assignment	In the web-based administration tool, you can assign one or more queues to each console user.
Queue view	View all calls within a specific queue or all queues. Empowered with this information, users can adjust their call handling times to deliver the best possible level of support to queued and active calls.
Queue statistics	Users can see the following details in real time for each queue: <ul style="list-style-type: none"><li>• Number of calls abandoned</li><li>• Number of operators logged in</li><li>• Number of operators available to answer calls</li></ul>
Queue overflow options (defined on a queue-by-queue basis)	<ul style="list-style-type: none"><li>• <b>Number of calls</b> overflow sends calls to the overflow destination when the queue is full.</li><li>• <b>No operator</b> overflow sends calls to the overflow destination when no operators are logged in to the queue.</li><li>• <b>Wait time</b> overflow sends calls to the overflow destination when a call has been waiting in a queue for a defined period of time.</li></ul>



Feature	Benefit
Queue salutations (displayed when a call is accepted from a configured queue)	Deliver the most appropriate greeting to each caller by providing a script to be read by the operator for each queue.
Music on hold (option to configure on a queue-by-queue basis)	Callers hear hold music through the Cisco Unified Communications Manager Music on Hold (MoH) function. The attendant console's queue device groups let you play different music to different queues.
Directory features	
Active Directory, Cisco Unified Communications Manager, iPlanet directory integration	You can synchronize contact data directly from your corporate directory. Console users have the option to update any contact field not belonging to the directory source.
Manually add contacts	Users may add individual contacts to the full directory and to shared and private directory groups from within the console. System administrators can add individual contacts to the full directory from within the web-based administration tool.
Bulk add, update, and delete contacts	System administrators can import, update, and delete contacts in bulk from the server's web-based administration tool.
Personal directory groups	Each user can create and share up to 100 custom directory groups, displayed as tabs across the top of the directory. Directory groups are populated by directory filters, by dragging and dropping contacts from the full directory, and by manual creation.



Feature	Benefit
Search options	Six directory search fields are provided. They allow the operator to find call destinations quickly and then dispatch calls quickly. Search options include last name, first name, department, extension, job title, and location, and they can be customized within each attendant console client.
Presence integration	With Cisco Jabber (Cisco IM & Presence and Cisco WebEx® Messenger) and Skype for Business integration, console users are able to see real-time availability for directory contacts.
Telephony features	
Operator handset ringing	When a call comes into a queue configured with operator handset ringing, the call is sent directly to the handset of the operator who has been logged in to that queue the longest. This feature lets operators answer the call from a wireless headset while away from their desks. (The wireless headset is not included.)
Transfer reversion (call recall)	Enables a transferred call to revert back to the operator so that it can be answered and then transferred to a new destination.
Call park	With call park, the operator can place a caller on hold while announcing that a call is on hold and waiting for a particular person or group. The call can be answered from any phone by dialing the park extension.
Call park recall	If a parked call is not answered, it reverts back to the operator so that it can be transferred to a new destination.



Feature	Benefit
Call toggle	Call toggle allows the operator to shift between callers.
Conference	The conference feature allows the operator to provide a third-party conference call.
Emergency Mode switch	Redirects all calls to another destination if an emergency such as a natural disaster or weather event occurs. This manual switch lets you stay in touch with callers or alert them that the business is closed until further notice.
Out-of-hours routing	For each queue, you can define specific blocks of time and where to send calls during that time. Create templates that you can apply to queues. Set up call routing for recurring holidays.
Additional client-side features	
Auto-unavailable on idle	If an operator's PC is idle for a specified period of time, the attendant console can automatically change their state to unavailable.
Server-based console preferences	All attendant console client preferences follow user login names, allowing users to enjoy the same user experience from any console client location.
Console client user single sign-on	Easy account management and user passphrase management
Adjustable font size	Changing the font size is one of the many ways in which individual users can tailor the Cisco Unified Attendant Console Advanced application to best suit their needs.



Feature	Benefit
Accessibility	The visually impaired can use the attendant console with JAWS screen reading software (English and Spanish scripts available).
Attendant console client localization	English, French, German, Italian, Portuguese, Spanish, Dutch, Swedish, Danish, Russian, Arabic, Korean, Japanese, Traditional Chinese, and Simplified Chinese are supported.
Additional server-side features	
Reports	Gain a better understanding of call volumes by operator and queue, the queues that have the most abandoned calls, and other important metrics through attendant console reports. Reports are easily accessible through the web-based administration tool.
High Availability (add-on option)	Provides an added layer of protection against system failures and convenience during maintenance efforts by adding a hot standby server. In the event of service interruption, console users and the calls they manage are automatically routed to the standby server until service is restored to the primary server.

4.2.1.1.3.21 If requested by an Agency, the State desires the ability to integrate a third-party call recording solution with the Vendor's hosted solution. Please describe your solution's ability to meet this goal.

#### AT&T Response:

AT&T support third party call recording applications that are certified via Cisco for use with Cisco CUCM. AT&T can also offer cloud call recording services for users and contact center agents.







4.2.1.1.3.22 The State desires that the Vendor use currently-owned State IP telephony handsets where the handset is still supported on the Vendor's solution. Please describe your company's ability to use the State's current handsets and its ability to meet this objective.

**AT&T Response:**

AT&T provides support for registration of existing IP Phones with the caveat that the device may have limitations based on end of support or end of life by the manufacturer. Some existing IP Phones may not be able to be upgraded to support new features. AT&T would work with the State to phase out any phones that become end of support as needed, but will support the existing devices that are deployed today.

**4.2.1.1.4 Hosted Contact Center Services**

4.2.1.1.4.1 The State's goal is to obtain a reliable, customizable, and scalable solution to provide hosted contact center services for an estimated twenty-five (25) individual contact center sites that works in conjunction with the Vendor's proposed Hosted VoIP solution. Certain sites require the capability to transmit and/or store call recordings that may contain sensitive data (such as PHI or PII). For ease of deployment and maintenance, the State prefers the contact center solution be web-based. The solution should provide the following capabilities:

- Ability for a simple, drag-and-drop, easy-to-understand interface to create customized call routing and role based queues that can be deployed to sites with nontechnical administration
- Should provide chat capabilities
- Should provide live data reporting
- If requested by an Agency, the solution should have the ability to interface with an Agency's database to populate information based on data provided by the caller
- If requested by an Agency, the solution should provide the flexibility for agents to use a public-switched telephone network (PSTN) phone to utilize the solution
- Should provide scalability for up to 800 agents and the ability to expand in the future



Please describe your solution and identify any areas in your solution that exceed the items requested above.

**AT&T Response:**

See AT&T's General Response. AT&T has configured the proposed system per the stated specifications but cannot guarantee compliance or compatibility with unknown future needs, technologies or operational requirements.

4.2.1.1.4.2 Some of the State's call centers operate on a 24x7x365 basis, delivering critical services to the communities. As such, the State prefers the Vendor's solution have inherent redundancy and survivability characteristics that will ensure minimal service disruptions, such as data centers in geographically diverse regions allowing for failover, equipment and power redundancies in those data centers, etc. Please describe your solution's redundancy and its ability to meet and/or exceed this goal.

**AT&T Response:**

We achieve geographic redundancy for AT&T Cloud Contact Center by using two geographically diverse data centers in fully active mode.

Each site is capable of handling all failover traffic from the other site. As an example, each site can handle 25,000 subscribers as its normal load and 50,000 subscribers if the other site fails.

4.2.1.1.4.3 The Vendor's solution should include enhanced features for Administrators, Supervisors, and Agents to effectively meet the needs of their customers. As such, the solution should provide the following capabilities:

- Agent and Supervisor client that provides Blended agents: Inbound and outbound capability
- Ability to monitor critical performance metrics allowing managers to coach, train, and encourage agent behavior
- Ability for Supervisors to change an agent's status
- Ability for Supervisors to silently monitor inbound and outbound calls





- Ability to interrupt an agent's call to interact with both the caller and the agent
- Ability for Supervisors to remove an agent from a call
- Ability to change an agent's skill profile in real time Please describe your solution and identify any areas in your solution that exceed the items requested above.

### AT&T Response:

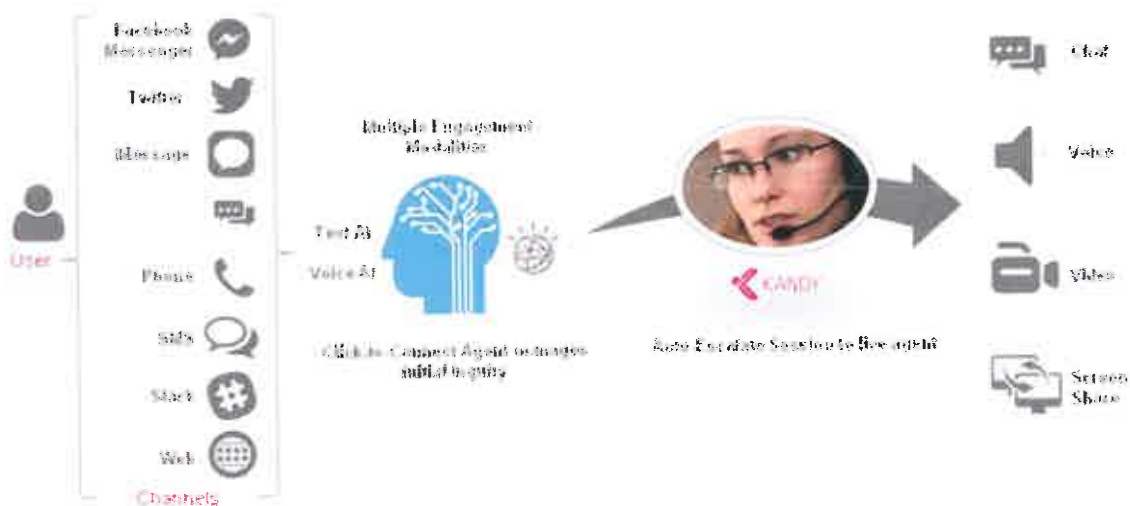
AT&T has developed a unique approach to the delivery of contact center services utilizing pre-defined agent profile options that can be mixed per location or group to meet feature requirements. Organizations can simple order the quantity profiles required and bring them on line via internet with WebRTC clients or utilize AT&T cloud IP Telephony with traditional IP handsets.

Basic Agent Profile	Standard Agent Profile	Enhanced Agent Profile
<ul style="list-style-type: none"><li>• Inbound Voice</li><li>• Outbound Voice</li><li>• Unlimited Sub-Tenants &amp; Roles</li><li>• Standard IVR</li><li>• Standard Reports</li><li>• Skills-Based Routing</li><li>• Configuration &amp; Administrative APIs</li></ul>	<ul style="list-style-type: none"><li>• Inbound Voice</li><li>• Outbound Voice</li><li>• Unlimited Sub-Tenants &amp; Roles</li><li>• Standard IVR</li><li>• Standard Reports</li><li>• Skills-Based Routing</li><li>• Configuration &amp; Administrative APIs</li><li>• Custom Reports &amp; Statistics</li><li>• Real-Time Reporting API</li><li>• Historical Reporting API</li><li>• Silent Monitoring &amp; Barge-in</li><li>• Queue Call Back</li><li>• Basic Scripting</li></ul>	<ul style="list-style-type: none"><li>• Inbound Voice</li><li>• Outbound Voice</li><li>• Unlimited Sub-Tenants &amp; Roles</li><li>• Standard IVR</li><li>• Standard Reports</li><li>• Skills-Based Routing</li><li>• Configuration &amp; Administrative APIs</li><li>• Custom Reports &amp; Statistics</li><li>• Real-Time Reporting API</li><li>• Historical Reporting API</li><li>• Silent Monitoring &amp; Barge-in</li><li>• Queue Call Back</li><li>• Basic Scripting</li><li>• Email Channel Functionality</li><li>• Chat Channel Functionality</li><li>• SMS Channel Functionality</li><li>• 3rd-Party Work Items</li><li>• Facebook Messenger Chat Integration</li><li>• Real-Time Adherence</li></ul>

AT&T provides the Advanced Flow Designer that utilizes drag and drop provisioning tools that allow organizations to develop calls flow effortlessly and without months of training. AT&T provides the initial support as part of our service to assist in constructing the call flows. Contact center administrators can then make additional changes as business requirements dictate without having to contact AT&T or requiring extensive training. Changes can be implemented real time.

Group's leaders and manager can add or remove staff to queues or assign skill levels and adjust skills based routing as needed without contacting AT&T or IT.

On average customers have reduced operational cost by 60% by leveraging AT&T cloud contact center provisioning tools along with AT&T proactive support services.



AT&T combines our CCaaS with AI to provide a holistic service model that can enhance customer service responsiveness and reduce over operation cost by providing more proactive support without having to add more staff. Multimodal capabilities provide more ways for customers to interact with support staff when required and AI provides access to databases and takes care of requests that can be automated. AT&T leverages pre-built AI front end processes that can self learn using IBM Watson. Customers can escalate conversations from Chat to Voice and then to Video when required.

AT&T can also apply our AI capabilities to existing contact center solution to enhance service interaction for older systems. AT&T builds customer specific AI capabilities that we refer to as Kandy Wrappers. These Kandy Wrappers can add AI IVR capabilities to add a level of pre call routing support to off load caller request that do not require direct human interaction. Callers can quickly escalate to live agent when required.

AT&T CCaaS and AI also assists with retention of agent staff by providing a way to off load work flows that are tedious or that could be answered more effectively via automated database look up. Easy to use agent desktop along with easy to manage call flows create a more favorable work environment





#### Rich Messaging Chat

Users can share images and videos with their support representative to better describe the issues that need resolution



#### Screen Sharing

Support experts can remotely assist users in real-time by activating screen sharing directly within the Live Support window



#### Works on Web & Mobile

Unlike other competing solutions, Live Support also works when your users access your website via their smartphone



#### Live Support & AI-IVR

Optional artificial intelligence chat bots with seamless escalation to a human customer service agent



#### Voice Call Promotion

Move a customer from a plain phone call to a full multimedia interaction with the click of a button



#### For Any Business Size

Micro businesses, SMBs, Enterprises and Large Contact Centers can benefit from Live Support as an overlay or fully integrated



#### WebRTC Enabled

Voice and Video calls directly from the website. Agents use web browser console or tablet app



#### Easy to Deploy

Use the back end portal to define the menu tree, create the button and generate the HTML embed code for your website

## Reports and Analytics

- Custom Statistics
  - Create widgets to visualize your data in bar charts, bubbles, columns, Stacked columns, donuts, gauges, lines, tables, or as a plain value.
- Custom Dashboards
  - Drag & drop your widgets to design your own custom dashboard so key performance indicators are front and center without having to run individual reports.
- Real -Time & Historical Reporting
  - Make sure every decision within your contact center is based on current &
  - Actionable data with real-time statistics, key performance indicators, and
  - Business analytics. Display contact center metrics such as call volume,
  - Service level, handle time, & wait time over any given time-period for
  - Data-driven decision making.
- Reporting APIs
  - readily access real-time and historical data and stream relevant statistics to third-party applications

## Simplified Agent Experience

- Customer Journey Mapping





- Full visibility into customer problems and historical interactions including notes,
- Call recordings, and chat / email transcripts that synchronize with each interaction so agents can focus on the customer rather than the tool.
- Reference Library
  - Link to a knowledge base, product catalog, or external website to draw from a limitless store of information while reducing the number of windows an agent must manage
- Performance Monitoring
  - Customizable agent metrics and presence states integrated directly into the global footer for real-time feedback and self-management of daily goals.

4.2.1.1.4.4 Some State agencies require the ability to utilize call recording, both on-demand and session-initiated. Certain call recordings will contain sensitive data (PHI, PII, etc.) and will require proper security protocols when transmitting or storing this information, with role-based access as defined by the State. Please describe your solution's call recording capabilities, and any additional requirements for the State in order to utilize these features.

#### AT&T Response:

AT&T supports both full time and on demand recording that can be enabled by the agent or controlled and the manager level. Recordings can be stored at AT&T highly secured data centers in SAN storage that is equipped with encryption for data at rest that meets and exceeds standards for most organizations for data storage. The following is utilized to secure call recordings within AT&T data centers. AT&T can also extend the recordings to customer provided storage or to end user desktop when required.

#### Security:

NIST FIPS 140-2 Level 3 via BeyondTrust appliance and applications

PCI-e Cryptographic Module embedded

Encryption card (validation in process)

#### Cryptography:

- AES, 3DES, DES, RSA (signatures and





Encryption), RC4, HMAC SHA-I – SHA512,

SEED encryption

- Asymmetric key sizes
- 1024, 2048, 3072, 4096
- Symmetric key sizes
- 128, 192, 256

### **Key Management Protocol**

OASIS KMIP (Key Management Interoperability  
Protocol) 1.0 Specification compliant

- NIST 800-57 Key Lifecycle support
- Symmetric Key, Asymmetric Key, Opaque,

Secret Data, Template

- Operations: Create, CreateKeyPair, Register, Get, GetAttribute, GetAttributeList, Locate, Query, Add/Delete/Modify Attributes

### **Role-based Management Control**

- • Multiple restricted roles can be defined for Each administrator
- • Automated, self-contained key management
- • Multi-credential administrative authorization

For sensitive security operations

### **Key Availability and Capacity**

- Secure key replication to multiple appliances
- Intelligent key sharing via key sharing groups

### **High Availability and Redundancy**

- Active-Active mode of clustering
- Multiple geographies
- Hierarchical clustering



## Supported Technologies

### API support

- iCAPI, KMIP, PKCS #11, JCE, MSCAPI, and
- .NET

### Network management

- SNMP (v1, v2, and v3), NTP, URL health check, signed secure logs & syslog, automatic log rotation, secured encrypted and integrity checked backups and upgrades, extensive statistics

### System administration

- Secure Web-based GUI, Secure Shell (SSH), and console Supported Directory.

4.2.1.1.4.5 The State may utilize an outbound predictive dialing campaign, at an Agency's request. Please describe your solution's capabilities in providing predictive dialing campaigns.

### AT&T Response:

AT&T Cloud Contact Center provides for fast and easy predictive dialing enablement predictive dialing and also integrates with outbound call dial databases via the advance flow designer that is included as part of the Advance Flow Design tool kit. Each agency can have the ability to enable predictive dial.

### 4.2.1.2 Security for Vendor's Hosted Solution

The State's goal is to ensure the Vendor's solution adheres to industry standard security practices and provides for sensitive data protection (where required) as it relates to cloud-based services. As such, the Vendor should:

4.2.1.2.1 Describe how its solution leverages high security standards associated with regulated data and/or high availability requirements, but also offers a cost-effective, standard-security solution option to the state.



### AT&T Response:

AT&T utilizes a layered approach to security. Each layer builds upon the next to ensure safeguards for our customers. We adhere to security standards that match or exceed the best practices outlined by AT&T chief Security Offices Information Security Standard and Center for Internet Security. We also follow best practices defined by equipment vendors and standards developed by AT&T Labs, AT&T Security Policy Requirements (ASPR) for data center security defining a layered security approach:

- **Secure the core switches:** Layer 2/Layer 3 switches build the data center core and aggregate links from other data centers. These switches are secured using the practices described in the Secure Network Foundation section of the SAFE Security Architecture design guide, Center for Internet Security best practices. Both are based on best practices for securing Cisco LAN switching environments
- **Segmentation of distribution switches:** Redundant distribution switches are responsible for aggregating the Layer 2/Layer 3 links connecting the access switches. Where a multilayer design is required, each layer is implemented as a separate VLAN that may span from distribution all the way to the access switches.
- **Stateful firewall deployment:** AT&T Security Architecture for Data Centers design uses stateful firewalls configured in failover mode to protect servers and help ensure segregation between application layers. The firewalls deep packet inspection mitigates DoS attacks and enforces protocol compliance. Web and UC applications are protected with a web applications firewall.
- **Traffic inspection and protection:** An IDS device is used to identify well-known attacks and suspicious activity. Complementary to the IDS, an anomaly detection system is also deployed at the web tier.
- **Server protection:** Servers residing at the different layers are protected with endpoint security software. Alerts and alarms generated by the IDS and endpoint security software are processed by a monitoring and analysis system.

**Switch hardening:** All switches are hardened using the procedures in the Cisco SAFE Security Architectures Secure Network Foundations section. This section is the bases for the Center for Internet Security best practices. Additionally, the access switches are configured with port security and other Layer 2 protection features.

### Network Functional Areas

AT&T UC Node network has been segmented into separate functional areas. Segmentation of the network allows control over the interactions between different sets of devices and users, and facilitates the deployment of control and monitoring



technologies, which are essential components of a secure network. Segmentation also allows containment of network attacks, for example should an attacker gain access to one of the network areas, or a worm outbreak occurs, the security filters between the areas can stop the attacker or worm reaching other parts of the network.

The following functional areas exist in relation to the UC Node network:

- The core AT&T IP network.
- Customer IP networks, which connect to the core AT&T UC Node IP network.
- Per-customer VRFs that carry customer traffic across the core IP network.
- Per-customer virtualised voice servers.
- USM voice management systems.
- UC Node management network that is logically separate from the user plane of the production service network.

### Monitoring

#### Intrusion Detection

The following describes the key aspects of intrusion detection on the HCS network at the four data centres:

- The Cisco IPS-4270 will be used as an Intrusion Detection System (IDS) will be used to monitor traffic for attack patterns at the following points on the HCS network:
  - Each customer's voice signalling traffic destined for their voice servers, on the 'inside' of their virtual firewall.
  - Each customer's 'command' traffic destined for the USM servers, on the 'USM' interface of their virtual firewall.
  - 'Command' traffic from the USM servers destined for the customer's voice servers, on the 'USM' interface of their virtual firewall.
- The Cisco Security Manager monitoring system located at the Watertown data center will be used to collect and analyse the alerts from the IDS.

#### Access Control

AT&T utilizes and established dedicated backbone network to support remote access from the Network Operations Center (NOC) and Security Operations Center (SOC) located in Atlanta, GA. UC Support Team (UCST) staff adhere to the following security process for access:





- All UCST staff members that will be accessing the UC Voice Federal platform will have the appropriate security clearances for access
- All UCST staff members will access the UC Voice Federal platform utilizing computers that have been approved for use by AT&T Chief Security Office (CSO).
- Remote access from the support staff requires the use of Two Factor RSA SecureID® Token Authentication
- VPN access for support from vendors and or remote work staff shall be provide through dedicated ASA 5510 firewalls defined with specific user access . The ASA 5510 shall be separate from ASA-5580 firewalls providing customer security and segmentation.
- Secure Access is provided via AT&T Jump Server
- Access to the network devices that the ACS servers are providing AAA service for will be via a dedicated management network.
- The following design details apply to AAA services for network device access:
  - ACS will also be used to authenticate user access to network devices for management and administration purposes.
  - A backup username and password will be configured on each device's local database, which will be used to authenticate a login if there is no response or an error is returned from the AAA Server.
  - AAA will be used as the access method for all devices on the network, and apart from the backup account, no user accounts will be configured locally on any device.
  - Each network administrator will have their own username and password for accessing network devices.
  - Different levels of access (authorization levels) will be granted to different groups of network administrators. For example, junior support engineers will not be allowed to reload devices, which is a feature that should only be granted to more experienced support personnel.
  - Accounting will be enabled on network devices, so that user login/logout times are recorded, along with each command that is entered, on the AAA server. This will provide valuable forensic information as all changes on the network will be logged in a central repository, along with the user who made the change.

## Management Plane Level

### Management Plane Level 1-2



Description: Services, settings and data streams related to setting up and examining the static configuration of the router, and the authentication and authorization of router administrators. Examples of management plane services include: administrative telnet and ssh, SNMP, TFTP for image file upload, and security protocols like RADIUS and TACACS+.

1. **AT&T provides AAA Service:** AT&T supports Authentication, authorization and accounting (AAA) systems for Local Console, Login, VTY, enable mode specific to Cisco IOS devices. AAA accounting supported
2. **AT&T provides local user encrypted password support:** All Cisco devices admin, user devices have encrypted passwords
3. **AT&T provides SSH for Remote Device Access/ VTY Transport SSH :** (SSH) access is configured on all management connections. Support for Automatic disconnect after 10 minutes.
4. **Auxiliary Port Disabled for core equipment:** Core LAN and routers are defined with "transport input none" to ensure prevention of un authorized connection
5. **Access Control Lists (ACL) for VTY:** IP address specific access for AT&T NOC users with configuration level access
6. **EXEC Banner Support:** Banner display security access restricted statement per AT&T standard for MOTD and login
7. **Password Rules:** AT&T Enable secrets use a strong, one-way cryptographic hash (MD5).
8. **Encrypted Line and User Passwords:** AT&T requires a password to be set on each line. Local usernames (level 1) or TACACS+ (level 2) line passwords are not used for authentication.
9. **SNMP Rules:** AT&T deploys SNMPv3 which utilizes authentication, authorization and data privatization encryption. No default SNMP community strings are utilized. SNMP control restricted by ACL to specific AT&T NOC administrators with configuration access level capabilities

## Control Plane Level

### Control Plane Level 1-2

The control plane covers monitoring, route table updates, and generally the dynamic operation of the router. Services, settings, and data streams that support and document the operation, traffic handling, and dynamic status of the router. Examples of control plane services include: logging (e.g. Syslog), routing protocols, status protocols like CDP and HSRP, network topology protocols like STP, and traffic security control protocols like





IKE. Network control protocols like ICMP, NTP, ARP, and IGMP directed to or sent by the router itself also fall into this area.

1. **Clock Time zone - UTC:** AT&T configures the devices clock time zone to coordinated universal time (UTC) explicitly.
2. **Cisco CDP:** AT&T disables Cisco Discovery Protocol (CDP) service at device level in the UC core. Specific management VLANs are defined where CDP is required.
3. **AT&T Default Disabled Services:** Finger Services, IP BOOTP server, Identification Service, IP HTTP Server, Remote Startup Configuration
4. **AT&T TCP Enabled Services:** TCP keepalives-in Service, TCP keepalives-out Service, TCP-small-servers
5. **Logging Rules:** AT&T supports logging buffers, logging to AT&T administered syslog server, Trap severity levels with time stamp in log messages
6. **Multilevel NTP:** AT&T provides Primary, Secondary and Tertiary Network Timing support from secure stratum level clocking sources.
7. **Loopback Rules:** AT&T supports Binding AAA, NTP, TFTP Services to Loopback Interface

## Data Plane Level

### Data Plane Level 1-2

Services and settings related to the data passing through the router (as opposed to direct to it). The data plane is for everything not in control or management planes. Settings on a router concerned with the data plane include interface access lists, firewall functionality (e.g. CBAC), NAT, and IPSec. Settings for traffic-affecting services like unicast RPF verification and CAR/QoS also fall into this area.

1. **Routing Rules :** AT&T default disabled routing components include; Directed Broadcast, IP source-route
2. **Border Router Filtering AT&T access restrictions:** Restrict Private Source Addresses from External Networks and External Source Addresses on Outbound Traffic
3. **Routing Protocol Neighbor Authentication Requirements:** Require Authentication for BGP, EIGRP, OSPF, and RIPV2 as required.
4. **Routing Rules Requirements:** Enable Unicast Reverse-Path Forwarding. Disable IP Proxy ARP and Tunnel Interfaces

## Virtual Platform Security



1. **VMware Management:** AT&T creates separate Management Network and data segments
2. **VMware Patches:** AT&T has three categories for patches: Security, Critical, and General. The patch # refers to KB (knowledge base) article number that goes into more detail. VMware will (usually) issue a KB article when they become aware of security vulnerabilities AT&T tests patches in it staging lab prior to implementing on production environments.
3. **BIOS Configuration:** AT&T disables the server's ability to boot off all non-hard disk devices, including floppy, CD-ROM, and USB.
4. **NTP Support:** AT&T enables system clock synchronization with Network Time Protocol (NTP) server(s). The Network Time servers are provided via AT&T network backbone that extends to the NTP platforms housed with the Watertown IDC in separate cage.
5. **System Access, Authentication, Authorization, and User Accounts:** Specific NOC administrators are allowed access using secure shell (SSH). AT&T does not enable Direct Root SSH. Do not enable direct su to root, only allow sudo .
6. **Password History:** AT&T retains a history of previous passwords used and configure the authentication controls to validate new passwords against greater than or equal to 10 recently used credentials

**Password Complexity:** Password strength requirements:

- Ignored when 1 character class is used.
- Ignored when 2 character classes are used.
- Ignore passphrases.
- Greater than or equal to 12 characters in length when 3 character classes are used.
- Greater than or equal to 8 characters in length when 4 character classes are used.
- Ignore reuse of any number of characters from the old password unless the new password is exactly the same as the old password.

**(Virtual Platform Security)**

1. **Failed Login Attempts :** AT&T sets the number of login attempts allowed before the account is locked / disabled to 3
2. **Maximum Days Before Password Change:** Set the maximum number of days before a password is required to be changed to 90 days





3. **Minimum Days before Password Change:** Set the minimum number of days a password must exist before it can be changed to: Greater than or equal to 7 days.
4. **Minimum Password Length:** Greater than or equal to 8 Characters
5. **Log Compression and Rotation:** Increase the file size 2096K and enable compression for the log files vmkernel and vmksummary
6. **Review Logs:** *Configure syslogd to Send Logs to a Remote LogHost are reviewed once a day by AT&T security team or when specific event dictate and are sent to an off box location to reduce being compromised*
7. **MAC Spoofing:** *AT&T protects Against MAC Address Spoofing, Forged Transmits, and Promiscuous mode by changing the flags to reject for the settings MAC Address*
8. **VMware Internal Firewall:** *AT&T configures the Firewall to Allow Only Authorized Traffic*
9. **Storage:** AT&T configures connections to iSCSI storage devices to use the CHAP protocol for authentication
10. **Warning Banners:** AT&T creates warning banners for console and remote access.
11. **Guest Interaction with the Host:** AT&T does not allow guests to control hardware devices outside of ESX or vCenter.
12. **AT&T Default Disables:** *Disable Group and Other Write File Permissions for .vmx Files, Disable Group and Other Read, Write and Execute File Permissions for .vmdk Files*

### IPSec VPN Termination

The following describes the key aspects of IPSec VPN termination on the HCS network:

- Customer traffic may be encrypted across the AT&T network, in which case it will be terminated at the AT&T router that connects to the Cisco ASA5580.
- Remote access to the environment will be through Cisco provided ASA5510 devices, enforcing strong authentication.
- The ASA5510 device will be configured for AAA using the ACS system. Cisco will be responsible for managing access to the HCS platform through the ASA5510 devices.
- AT&T will provide backup access to the HCS platform for Cisco through their IPSec VPN infrastructure.







4.2.1.2.2 Describe its policies and procedures for conducting sub-contractor assurance, validating both the capability of the vendor to fulfill contracted responsibilities and adhere to all applicable security & privacy policies and controls of all parties.

**AT&T Response:**

AT&T conducts a full background investigation on any subcontractors that are utilized to support services provided as part of the project. This may include full FBI background when requirements for CJIS standards are required. Financials are examined along with verification of previous work is conducted via our AT&T sourcing teams.

4.2.1.2.3 Describe its company's cyber security and privacy management program including an overview of the governance structure, cyber security strategy, and the experience of personnel in key security and privacy roles.

**AT&T Response:**

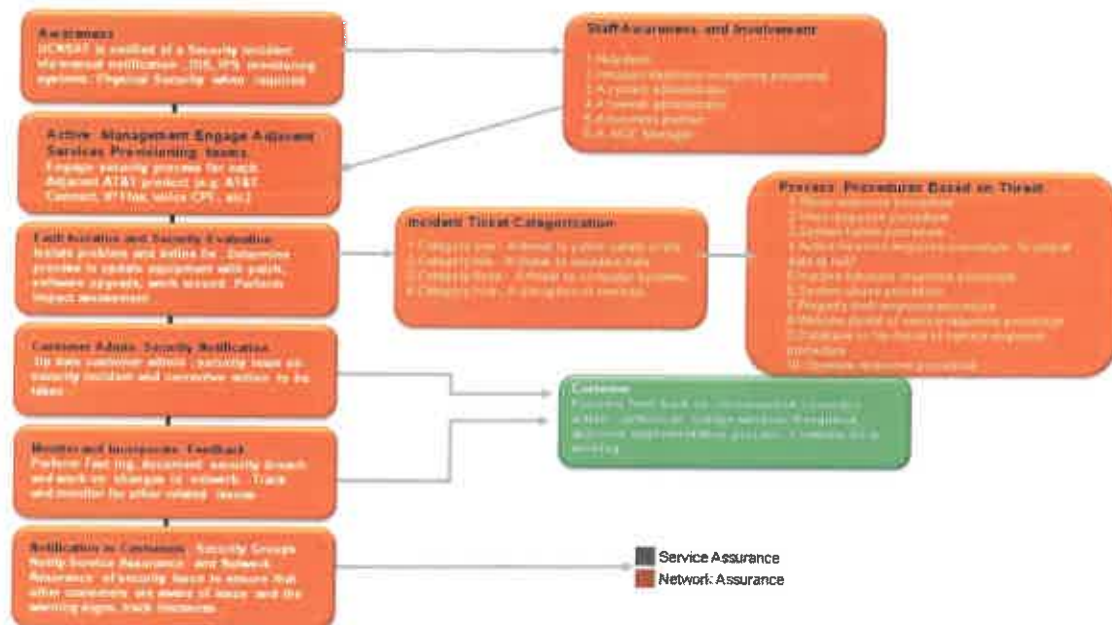
AT&T provides complete cyber security practice as part of our overall service approach. The attached link below defines the overall services and practices that AT&T delivers in support of our customer solutions. AT&T also operates one of the largest threat management and Security Operations Centers in the world.

<https://www.business.att.com/portfolios/cybersecurity.html>

**Security Incident Management**

AT&T utilizes IPS 4270 to capture details on inbound packets, IP address source and destination information. When traffic is determined to not match MAC, IP addresses defined in IPS for valid customers is tagged and an alert is generated by the IPS to the security incident management team for handling and quarantine. The following process flows demonstrates the security approach.





Page 2

## Security Incident Management

AT&T uses an RSA SecureID® token-based scheme for two factor authentication. Two factor authentication uses “something you have” and “something you know” to establish authenticity. For the UC Voice service, two factor authentications require possession of a token fob as well as knowledge of your Personal Identification Number (PIN).

AT&T has a separate pool of tokens used for administering security devices for all customers. Use of a common token pool simplifies overall token administration. A multiple (two) realm arrangement provides for separation of UC Voice users, servers and device data from Commercial customers’ data. Employing cross realm authentication an administrator can support multiple services with one token fob.

Each realm contains an independent database of the valid userids, PIN + token codes, servers and devices that are available for two factor authentications. (Some devices in UC Voices do not support two factor authentications.) UserIDs are designated as local (authentication performed completely in local realm) or remote (authentication performed in conjunction with remote home realm). When a remote realm is engaged, this process is called cross realm authentication.

AT&T’s commercial service administrators are provisioned in the NBFW realm. AT&T’s UC Voice service administrators are provisioned in the UC VOICE realm. The respective



realms are further divided into roles to further segregate administrators by specific function.

AT&T has deployed primary and replica servers for both realms. Either the primary or replica of a given realm is capable of authenticating a user.

Two factor authentications are processed as follows:

1. A potential administrator attempts to log in to a given server or device.
2. The administrator is prompted for a Passcode, which is a combination of their PIN + Token Code.
3. Upon submission of these credentials, the userID (login) is checked against the UC Voice realm.
4. If the userID is not found in the UC Voice realm, the login request is rejected. If the userID is provisioned in the UC Voice realm, the PIN and token code values are evaluated by that user's home realm for confirmation.
5. If the home realm produces a negative response for the PIN and token code, the login is rejected. If denied, the administrator must wait until the token's display has changed (thirty (30) seconds maximum) before making another attempt to authenticate. After a positive confirmation, the UC Voice authentication servers will permit access to the user's desired server or device.

An administrator must allow the token code to update prior to attempting to log in to another system. Note that a given token code can only be used once.

Authentication requests are logged. Local realm logging includes userID, server or device name, status (successful or failed) as well as a cross realm indication, if cross realm was attempted. Remote realms log userID, status (successful or failed) as well as the fact that a cross realm authentication was attempted. The server or device name from the local realm is not available to the remote realm to prevent sharing of local information.

#### 4.2.1.3 Service and Support for Vendor's Hosted Solution

The State's goal is to partner with a Vendor whose service and support structures allow the State to focus on its core services, while ensuring telephony and contact center systems are available to State Agencies, with certain Agency sites (hospitals, jails, etc.) operating critical services 24x7x365. The State desires a Vendor to provide all levels of tiered support, including Tier 1 support for end-users. To this end, the Vendor's service and support structure for the Vendor's hosted solution should provide for the following:





4.2.1.3.1 Performance monitoring, capacity planning, and real-time surveillance of the Vendor's network to ensure 99.9% availability of services and provide network utilization reports upon request. Please describe your company's process and ability for providing this information upon request, including any lead times needed and how the State submits these requests.

#### AT&T Response:

AT&T provides remote monitoring, management and MACD services as part of the Unified Communications infrastructure and support for contracted customer's premise equipment (CPE) using a suite of sophisticated management tools. The UC Network Operation Center (NOC) responds to alarms and alerts received from the core UC infrastructure and then triages the issues and works to resolve problems proactively.

In the event that there is a site related issue (loss of power to site, damage to premise cabling, accidental disconnection of cabling or equipment, or carrier issues) that causes an outage of devices or systems under management, the UC Services Support team will document the issue within the UC Services Support ticketing system, notify the end user designated contact(s), and manage the issue until resolution. The UC Services Support will close the ticket once the site related issue is remediated. When the ticket is closed, the end users designated contact will receive an email indicating that the site issue is resolved.

In the event that a contracted device has a component hardware failure, the UC Services Support will diagnose and attempt to resolve the issue remotely. If the hardware failure cannot be resolved remotely, the UC Services Support will begin dispatch of a replacement part. AT&T can leverage customer's existing site staff for dispatch or contact contracted vendor for on site hardware replacement. On site AT&T hardware support is not included with the core services and requires additional interaction with the customer to define what level of on site would be required. AT&T will setup add pricing for onsite support after further requirements are defined upon request from the customer.

### 2.1 Fault Management

The UC Services Support Fault Management consists of the following:

- **Fault** - A fault is defined as a failed device poll indicating the target device is not visible to the UC Services Support network management systems and tools. Also equipment generated alarms proactively alerting the support team to failure of a





system or components under AT&T monitoring and management within the network

- **24X&X365 Fault Management** - The UC Services Support will manage the contracted network devices for fault alarms and conditions. If a critical task or function turns off for some reason (up/down), the monitoring tools send out an alert and the UC Services Support will notify the end user designated contact(s) of the alarm. The UC Services Support will open a ticket and troubleshoot the alarm and resolve the issue. If the UC Services Support cannot fix the issue directly, the UC Services Support will open a ticket with the vendor (under a vendor maintenance support contract) and work with the vendor support team to resolve the issue. When a fault is identified, the UC Services Support will take ownership of the issue until it is resolved.
- **Problem Identification and Triage** - The UC Services Support will verify that an alert or alarm is valid and then notify the end user designated contact(s) of a detected problem according to the contact process provided by the end user and documented in the Customer Service Manual. The service will open a trouble ticket and start the remediation actions.
- **Event Management** - Most events that happen on a server are recorded in an event log. The UC Services Support monitors all of those logs. If a critical event occurs the UC Services Support monitoring tools sends out an alert and the UC Services Support will notify the end user designated contact(s) of the alarm. The UC Services Support engineers will open a ticket and troubleshoot the cause of the alarm. When the cause of the alarm is confirmed, the UC Services Support will resolve the issue. If the UC Services Support cannot fix the issue directly, the UC Services Support will open a ticket with the vendor (under a vendor maintenance support contract) and work with the vendor support team to resolve the issue, taking ownership until the issue is resolved.
- **Trap Monitoring** - For devices that can support traps, the UC Services Support can configure the traps to send critical event information to the network monitoring tools. These events can create alarms which trigger a trouble ticket. Corrective action will be taken by the UC Services Support depending on the nature of the alarm.
- **Ownership** of resolution of the problem on behalf of the end users and act as an agent for the end user under executed letters of agency.
- End user designated contact(s) notification of the progress of all faults per the end user provided contact(s) and escalation process.







- Safeguard end user's proprietary information and take all necessary precautions to ensure a secure connection from the UC Services Support into the end users network.
- Secure end user designated contact(s) web portal access to view the fault management alarms and event logs, open tickets and contact information.

## 2.2 Capacity Planning and Patch Management

- **Capacity Management** – The NOC monitoring tools and engineers will preemptively identify the need to add additional capacity to the hardware and carrier infrastructure in advance of experiencing issues.
- **Patch Management** – Patches are enhanced features or bug fixes released by product vendor or other vendors as required to maintain the most current release of code. As part of the service, the NOC will regularly review patches and upgrades that are available, then prioritize and schedule deployment, as required.
- **Scheduled Maintenance Window** – In order to ensure a stable and secure infrastructure, AT&T will work with the customer to develop maintenance windows that are required to maintain the core infrastructure patches and equipment upgrades as needed. While the window will only be used as needed, it is important to have an agreed upon monthly maintenance time. In the event that a maintenance window will be used, the NOC will inform the customer a minimum of three (10) days in advance so that the customers have time to notify internal users and plan to test after maintenance is completed.
- **Emergency Maintenance** – In the event that maintenance must be performed outside of the regularly scheduled maintenance window, AT&T will reach out to inform the customer of the issue and impact. This maintenance will be performed only when there is significant risk to the infrastructure that cannot be postponed to the next available scheduled window. We will work closely with the customer to mitigate any potential outages during the emergency maintenance window and perform tests after the fact to ensure success and stability.
- **Capacity Management** – The NOC monitoring tools and engineers will preemptively identify the need to add additional capacity to the hardware and carrier infrastructure in advance of experiencing issues.
- **Patch Management** – Patches are enhanced features or bug fixes released by product vendor or other vendors as required to maintain the most current release of code. As part of the service, the NOC will regularly review patches and



upgrades that are available, then prioritize and schedule deployment, as required.

- **Scheduled Maintenance Window** – In order to ensure a stable and secure infrastructure, AT&T will require maintenance windows to perform upgrades from time to time. While the window will only be used as needed, it is important to have an agreed upon maintenance time. In the event that a maintenance window will be used, the NOC will inform the customer a minimum of three (10) days in advance so that the customers have time to notify internal users and plan to test after maintenance is completed.
- **Emergency Maintenance** – In the event that maintenance must be performed outside of the regularly scheduled maintenance window, AT&T will reach out to inform the customer of the issue and impact. This maintenance will be performed only when there is significant risk to the infrastructure that cannot be postponed to the next available scheduled window. We will work closely with the customer to mitigate any potential outages during the emergency maintenance window and perform tests after the fact to ensure success and stability.

### 2.3 Configuration Management

- **Access Control and Monitoring** - For security and compliance reasons, this service provides Access Control giving UC Services Support secure and quick remote access to the managed equipment and keeps an audit trail of who has logged into the end user system and when logins occur.
- **Equipment Configuration Management** - The service scans the managed network equipment daily and stores all configuration changes. This feature allows the UC Services Support to quickly restore the last known good configuration of a critical device in case of hardware failure or an inadvertent command being placed in the device that would cause the device to not function as designed. Highlights of the configuration management service include:
  - Maintaining a log of network device configuration changes
  - Daily polling of each contracted network device to determine if configuration changes have occurred
  - Automatic notification of configuration changes
  - Capturing and archiving the most recent 30 device configuration changes
  - Ability to quickly provide the last good archived configuration to assist with rapid recovery in the event of configuration loss (including during any outage or disaster) or changes, or performance issues

### 2.3 Third Party Vendor Management





**The UC Services Support will manage vendors (thru letters of agency) for:**

- Replacement parts dispatch thru vendor maintenance contracts
- Vendor On-site technician dispatch thru vendor maintenance contracts
- Incident management with Telco's (PSTN or WAN)
- Vendor tickets

Note: Additional charge may apply depending on further details on third party support requirements.

**2.4 Web Portal Access**

- The UC Services Support can provide access into the ticketing system and monitoring tools via a secure WEB portal. The WEB portal is configured provide 24x7x365 read only access into the end users devices and tickets. The WEB portal can provide the following to the end user designated contact(s):
  - View open and closed tickets
  - Open a new S3 or S4 ticket
  - View end user (CPE) devices in real time using the UC Services Support monitoring tools
- Some of the information available thru the WEB portal includes:
  - Network Performance Information
    - Bandwidth utilization
    - Network latency
    - R-factor score
    - Jitter
    - Packet loss
    - Circuit status
  - Device and Application Performance Information
    - Device CPU utilization
    - Device memory utilization
    - Device buffer performance
    - Device queue performance
    - Gateway utilization
    - Storage utilization
    - RAID controllers
    - Power supplies
    - Fans
    - Temperature



- A list of authorized end user designated contact(s) will need to be provided to the UC Services Support for access into the WEB portal. The list can be identified in the Customer Service Manual provided at the end user kick off meeting. WEB portal training (usually 1 hour) for the end user designated contact(s) portal uses will be scheduled thru the UC Services Support.

## 2.5 Service Requests and MACD

A trouble tickets are generated automatically by the UC Services Support's monitoring tools when faults are detected in the core systems. The end user designated contact(s) can open a trouble tickets by sending an email to the UC Services Support, phone call into the UC Services Support. If a problem is critical (S1 or S2), the end user is urged to call into the UC Services Support via phone call. MACD requests can also be requested thru the UC Services Support. The following information is needed in order to open an UC Services Support trouble ticket:

- Contact name and telephone number of person making request.
- Model number and serial number of the equipment to be serviced.
- Site location address of equipment to be serviced.
- Description of the problem or MACD request.

### MACD (Moves, Adds, Changes & Deletions):

- **User Administration** - The UC Services Support will remotely add and remove people from your system, reset passwords, and assign new passwords as needed.
- This standard support agreement includes up to 750 MACDs per month, up to 50 MACDs can be submitted every 48 hours. In the event the end user requires more than 50 MACDs within 48 hours, the MACDs exceeding 50 will be completed under a revised service level objective of 5 business days for targeted completion.
- New site implementations are not supported as MACD and are classified as projects that require prior planning and coordination to implement. Large migrations of users from one physical location to another are also defined as projects and may require additional charges depending on the nature the equipment to be migrated.
- The MACDs will be performed remotely by the UC Services Support. The timeframe in which the UC Services Support will complete the remote MACDs varies based upon the quantities of activities requested. However, the UC





Services Support will complete most requested MACDs within 24 hours of receipt of the remote MACD request.

- Unless otherwise specified, remote MACDs will generally be handled Monday-Friday 8 a.m. to 8 p.m. EST. The end user designated contact(s) will submit a MACD request to the UC Services Support via email, email or phone call. Upon receipt of the request, the UC Services Support will verify submission, open a trouble ticket and provide the end user designated contact(s) with e-mail confirmation of receipt of the remote MACD and the trouble ticket information. The UC Services Support will follow all end user change procedures when performing a remote MACD on behalf of the end user. Upon completion of the remote MACD, the UC Services Support will verify the change was successful, update the documentation to reflect the change, notify the end user designated contact(s) and update and close the trouble ticket.
- Emergency MACD requests will be prioritized by working with the customer and review of current MACD in the queue. Designated customer admin will define the priority level and time for completion required.

## 2.6 Reports

The AT&T UC Service Support team will provide reports to help the customer understand the state of the managed CPE. A list of available reports is provided below:

### 2.6.1 Weekly Reports

**Weekly Reports** - These reports look at the summarizing the weekly ticket activity showing all tickets opened, closed and still active tickets.

### 2.6.2 Monthly Reports

**Monthly Reports** - These monthly reports look at the contracted infrastructure devices. The NOC will send out detailed reports each month to your designated contact person. The reports include statistics on:

- Network, device uptime and availability
- Fault history
- Trouble tickets
- MACD's used
- Professional Services hours used
- Configuration changes during the month





### 2.6.3 Strategic Reports

**Periodic Business Review** - Provides business intelligence information based on the data that the UC Service Support team gathers during the period under review. This information has potential business impacting information that reflects UC CPE network including the following elements: capacity planning, resource utilization, ticketing, compliance issues, best practice standards, security concerns and business continuity planning. The goal of this report is to:

- Characterize the existing managed environment
- Make specific recommendations for improvement
- Provide budgetary information to implement the recommendations
- The first category of recommendations will be referred to as **Immediate Impact** recommendations. These recommendations will provide an immediate impact on performance across the managed network. The second category of recommendations will be referred to as **High Impact** recommendations. The recommendations within this section will provide additional improvements in performance as well as increasing network management efficiency. The third category of recommendations will be referred to as **Strategic** recommendations. These recommendations will focus on ensuring that the network will scale to meet future business requirements and that the customer will be able to proactively monitor and manage network performance through the use of the NOC.
- **Performance Analysis** - Provides detailed information that reflects the overall performance of the managed network showing bottlenecks, areas of high utilization, areas of under- utilization, dropped packets, unusually high error rates and lowers than normal device uptime.

The reports that are included with monitoring and management package are reflected in the table below:

Report	Select Service Management
Weekly Report (fault/ticket summary)	X
Monthly Report	X
Fault History	X
Trouble Tickets	X
Device Uptime	X
Periodic Business Review	X
Fault History	X
Trouble Tickets	X



Report	Select Service Management
Device Uptime	X
MACD's Performed	X
Average PSTN Trunk Access Utilization	X
Professional Service Hours	X
Performance Analysis	X
Configuration Management Changes	X

## 2.7 Support Level Definitions

Support level definitions define the Service Level Agreements and Service Level Objective the AT&T UC service provides. Custom SLA and SLO are negotiated at the time of contracting when required.

### 2.7.1 Severity Support Level Definitions

Fault ID	Objective Description	Service Level Response
P1	Detection of Priority 1 (P1) events on the customer network	Within 15 Minutes
P2	Detection of Priority 2 (P2) events on the customer network	Within 15 Minutes
P3	Detection of Priority 3 (P3) events on the customer network	Within 1 hour
P4	Detection of Priority 4 (P4) events on the customer network	Within 2 Business Days

#### (P1) - Critical Priority:

Produces an emergency situation in which the network is inoperable, produces incorrect results, or fails catastrophically, or a mainline function of the network is inoperative (i.e. a critical application server), causing significant impact on the Client's business operations (i.e., the Customer's production network is down causing critical impact to business operations if service is not restored quickly). The NOC shall continue to work on the problem while it remains unresolved and no workaround has been provided. The NOC and the customer are willing to commit full-time resources around the clock to resolve the situation.

#### (P2) - High Priority:

Produces a serious situation in which the network is inoperable, produces incorrect results, or a mainline function of the network is inoperative (i.e. a critical application server), causing a major impact on the customer's business operations (i.e., the



customer's production network is severely degraded, impacting significant aspects of business operations). The NOC and the customer are willing to commit full-time resources during business hours to resolve the situation.

(P3) - Medium Priority:

Produces a non-critical situation in which the network produces incorrect results, or a feature of the network is inoperative, causing a minor impact on the Client's business operations (i.e., the customer's network performance is degraded; network functionality is noticeably impaired but most business operations continue). The NOC shall make reasonable efforts to resolve the problem or provide a workaround as agreed upon between the parties.

(P4) - Low Priority:

General questions, MACD requests and/or inquiries causing little or no impact on the customer's business operations. The remote management services makes reasonable efforts to resolve the problem or provide a workaround as agreed upon between the parties

## **2.8 Service Level Agreements**

UC Services Support Service has established Service Level Objectives/Service Level Agreements (SLOs/SLAs) for Unified Communications (UC) Services.

### **2.8.1 Service Level Agreements Eligibility**

The SLOs/SLAs apply only if the Customer's network meets the following criteria:

- End user has:
  - Deployed LAN switches that support required Quality of Service (QoS) capabilities.
  - Deployed wireless access points as required to support UC wireless devices with QoS.
  - Provided WAN access between at least one of the UC Services Support Service UC nodes and end user premise.
  - WAN access capable of providing class of service with prioritization for Real Time Transport Protocols and VoIP signaling. WAN access can be provided by AT&T via AT&T Virtual Private Network, AT&T Enhanced Virtual Private Network, AT&T Managed Internet Service, or AT&T Private Network Transport. Third-party transport services can also be utilized but must support Quality of Service (QoS) and provide 99.9% availability.





- The WAN transport SLOs are provided separately and are not a part of UC Services Support Service UC Services SLOs defined in this document.
- All LAN switches and WAN transport must support Quality of Service capabilities. The implementation and configuration of the IP Telephony, LAN, WAN and Wireless LAN Service meets the design criteria as proposed to the end user by UC Services Support Service.
- The IP Telephony, LAN and Wireless LAN Services service components are installed, tested and documented in the end user location(s) prior to implementation of UC Services Support Service UC Services solution. The UC Services Support Service requires review and must approve the LAN and WAN configurations prior to deployment of UC Services Support Service UC Services.

### 2.8.2 Response Time

The standard Time to respond objective provides that UC Services Support Service will strive to respond to Severity Levels in accordance with the timeframes described below. Time to Respond is the time elapsed from a trouble ticket's creation that a problem was detected or automatically generated by UC Services Support Service tools, to the time that an engineer takes ownership and begins steps to resolve. Troubles will be prioritized using Severity Levels as described in the *Definitions* section above.

UC Services Support Service will strive to respond to troubles in the timeframe described no less than 95% of the time in aggregate. Time to Respond Intervals:

Priority	Maximum Response Time	Mean Monthly Response Target	Maximum Resolution Time	Mean Monthly Resolution Target
P1 (Critical)	15 Minutes via customer contact via Phone	90%	4 hours	90%
	5 Minutes via automated ticket triggered by AT&T proactive monitoring tools			
P2	1 hour	90%	1 day	85%
P3	4 hours	90%	2 day	75%
P4	1 day	80%	5 day	75%
P5	2 days	80%	10 day	75%



### 2.8.3 Measurement Period

The time elapsed from a trouble ticket's creation, i.e. time-stamped by virtue of the trouble being reported to UC Services Support Service by the end user or by a trouble ticket being automatically generated by UC Services Support Service tools, to the time the trouble has been resolved or service has been otherwise restored, will be used for determining time to resolve for the purpose of this SLA or SLO. Upon resolution, the trouble ticket will be time-stamped accordingly. Internetwork Operating System (IOS) reloads are excluded from this metric. IOS reloads are defined as soft reloads. They are essentially a re-boot of specific hardware components either as part of the UC Services node or at the end user's premise. The Time to resolve objective is to meet the defined resolution intervals listed below at least 95% of the time in aggregate. Networking issues outside of the span of control of UC Services Support Service and times to dispatch will be excluded from the resolution time. Time to resolve is measured monthly. A trouble ticket will be included in the SLO/SLA metric in the month that the ticket was closed.

### 2.8.4 Process

UC Services Support Service will track the time between report of trouble and restoration of service to determine the Time to Resolve.

### 2.8.5 MACD SLO

MACD Service Requests will be completed by UC Services Support Service in accordance with the schedule set forth in the table immediately below or as mutually agreed in end user's service agreement. The following are not included in this measure: 1) Timeframes associated with the ordering, procurement or provisioning, and delivery of Service Components. The Service Level measurement begins once all Service Components (network transport and end user premise equipment (routers, LAN switches, Wi-Fi access points, computers, phone sets, mobile devices, end user provided applications) are in place.

Schedule of Cycle Times	
IPT/UC Service Request Type	Typical Cycle Time within (Completion period following acceptance of written request for change)
UC User Password Reset 1 MACD	2 hours
UC User Password Reset 2-10	4 hours
UC User Password Reset 11-50	1 business days
UC User Password Reset >50	Negotiated determine if there is a project related to changes





Schedule of Cycle Times	
IPT/UC Service Request Type	Typical Cycle Time within (Completion period following acceptance of written request for change)
UC Level 1 Soft MACD 1-10	Standard - 1 business day, 8x5xNBD Express - 4 business hours, 8x5x4
UC Level 1 Soft MACD 11-20	3 business days or agreed upon interval
UC Level 1 Soft MACD >20	Negotiated
UC Level 2 Soft MACD 1-10	3 business days or agreed upon interval
UC Level 2 Soft MACD 11-20	5 business days or agreed upon interval
UC Level 2 Soft MACD >20	Negotiated

### 2.8.6 Objective

The SLO commitment is for MACDs to be completed in accordance with the specified intervals at least 90% of the time during the measurement period. Performance will be measured at the aggregate of all completed end user MACDs within a calendar month.

### 2.8.7 Calculation

The calculation of On-Time Provisioning Performance for all categories is:

- $(\text{Sum of N divided by sum of T}) \times 100 = \_\% \text{ where, for a given month,}$
- "N" means the total number of MACDs that are completed on-time during the measurement period,
- "T" means the total number of MACDs that should have been completed on time during that measurement period as set forth below.

This metric excludes the following: (a) processing time for missing information, inaccurate information provided by the end user or time to resolve approval issues, (b) service requests that are rescheduled due to Equipment order and delivery process delays by the manufacturer, the supplier or vendor are excluded from the metric, (c) service requests that are rescheduled by an end user request after UC Services Support Service agreed upon scheduled completion date, and (d) delays due to force majeure events described in the *SLO Exceptions and Exclusions* section, below.

### 2.8.7 MACD Measurement Period



Provisioning Performance is measured monthly. A provisioning request will be included in the provisioning metrics in the month that the MACD activity is closed.

Example: a MACD that is submitted on the 28th day of a given month, with a two (2) day timeframe, will be measured and reported in the following month.

### 2.8.7 MACD Measurement Process

UC Services Support Service will record (1) the time of receipt of a complete request with all required approvals for a Service Request, (2) the agreed-upon scheduled completion date, and (3) the date and time of the completed request. A complete request includes all required information and approvals and does not conflict with existing information documented in the environment.

### 2.9 Service Availability SLA

Service Availability is the percentage of time the Service is available and usable by end user at an aggregate of all managed sites, subject to adjustment for exclusion(s) and exceptions set forth below. For the purposes of this SLA, the Service will be deemed to be unavailable if there is a failure in any UC services Device (this includes the UC Services node as well as any end user premise equipment (CPE) used in conjunction with the service, such as voice gateway routers and analog gateways which are managed and monitored by UC Services Support Service which renders end user unable to complete calls at any managed site (i.e., outages of Severity 1 or 2). The Service Availability SLA commitment is for the Service to be available 99.9% of the time during the scheduled operating hours of the managed sites in each calendar month, aggregated across all managed sites, subject to the exclusions and limitations set forth herein. The total scheduled minutes of availability for each managed site for any month shall be computed based upon the scheduled operating hours for such site during such month as designated by end user to UC Services Support Service prior to such month minus scheduled maintenance minutes.

Components not covered by the defined SLA's include the following

- Network Transport
- Failures in the Public Switched Telephone Network (PSTN) or connections to the PSTN.
- Customer Premise equipment (Existing Routers, LAN Switches, WIFI Access Points, Computers, Phone sets, mobile devices, end user provided applications
- Services beyond the scope of the UC Services Service





### 2.9.1 Calculation

The formula for calculating Service Availability is:

$M - S / A$ , where, for a given month:

- "M" denotes the cumulative sum of total scheduled minutes of availability for each managed site (defined in the UC Services service description. It is the core UC node plus the on premise voice gateway and support UC Services phone sets in the month,
- "S" denotes the cumulative sum total of actual minutes of unavailability for each managed site in the month,
- "A" denotes the cumulative sum total of scheduled minutes of availability for each managed site in the month.

Unavailability due to any of the causes set forth in the *SLA Exceptions and Exclusions* section, below, or occurring during any scheduled maintenance window for UC Services or at any managed site outside of the designated operating hours for such site, shall be excluded from this SLA and shall not constitute minutes of unavailability for the purposes of determining Service Availability.

### 2.9.2 Measurement Period

The Measurement Period for Service Levels in the aggregate shall be one calendar month. If performance by UC Services Support Service over the Measurement Period meets or exceeds the specified Service Level, no Credit will be due. If performance by UC Services Support Service does not meet such Service Level, a Service Level Credit will be due, as set forth in the *Credit Assessment Table*, below.

### 2.9.3 Credit Assessment Table

UC Services Support Service shall pay a Service Level Credit to the end user based on the table below if its performance does not meet the specified Service Level targets (subject to any applicable exclusion).

Service Level Agreement Credit Assessment			
Category	Component	Service Level	Credit
Service Availability	Aggregate	99.99%	10% of monthly recurring UC services fees for UC Services  If the SLA is missed in consecutive months, the following level of credits apply: <ul style="list-style-type: none"><li>• 2nd consecutive month – 15%</li></ul>



#### Service Level Agreement Credit Assessment

Category	Component	Service Level	Credit
			<ul style="list-style-type: none"><li>• 3rd consecutive month – 25%</li><li>• 4th consecutive month – 50%</li><li>• 5th (or higher) consecutive month – 100%</li></ul>

**Note:** UC Services Support Service shall credit end user such eligible credits as determined above subject to the condition that in no event will credits to the end user either alone or in combination with other credits UC Services Support Service may issue to the end user, exceed more than one hundred (100) percent of the monthly recurring service fees for the UC Services Support Service UC Services in any given month.

4.2.1.3.2 The State desires regularly scheduled meetings and/or calls to discuss the following areas:

- Architecture and Design
- Implementation
- Ordering and Billing
- Service and Support
- Project Management

Please describe your company's ability to hold regular meetings on each of these topics, as well as your company's implementation plans for starting these discussions.

#### AT&T Response:

AT&T provides full account stewardship with Strategic Account Management (SAM).

Your AT&T Service Manager holds monthly stewardship meetings with you to report on performance with provisioning, billing, service, and maintenance of your AT&T services. Your AT&T account team meets with you on site to understand your business needs, to recommend solutions, and to help ensure your overall experience with AT&T is meeting your expectations.

We hold annual meetings with you to create and review your account plan. In these meetings, your account team will review its plans to support you in the coming year. We design this plan to support your business objectives and determine where to focus sales and support efforts in the next year.



At least annually, we request briefings to refresh our understanding of your long-term plans and to present new technologies and services that may affect your business or industry. We schedule an annual Customer Satisfaction Survey meeting with you and your AT&T sales and service teams. We then review your feedback from the annual survey process to determine and develop action plans that address any service or support gaps.

With Strategic Account Management, we work with you to create, monitor, and adjust a specialized account plan.

4.2.1.3.3 Vendor should contact the State's engineering points of contact by phone within 30 minutes of a Vendor network outage that affects multiple sites on the State's network. This verbal notification should be followed with a written report that provides an explanation of the problem, the cause of the problem, the solution to the problem, the estimated time for recovery, and the steps taken or to be taken to prevent a recurrence. To that end, please describe your company's notification procedures in the case of an outage.

#### AT&T Response:

AT&T standard is contact within 15 minutes of a service impacting event and with automated updates until event is cleared. Followed by RCA within 24 hours.

4.2.1.3.4 Vendor should provide written notification of ten (10) business days or more in advance of any planned upgrades, modifications, etc. that may affect the State's customers to the State's engineering points of contact. Please describe your company's notification process for planned maintenance.

#### AT&T Response:

If a network outage is scheduled, AT&T will use reasonable efforts to give you at least 30 days' notice before the planned maintenance.

If the network requires emergency maintenance, we'll provide you with as much advance notice as possible, depending on the urgency of the maintenance. We may require emergency maintenance in situations where a critical network component fails, or is at risk of failing, that would have a negative impact on our ability to provide service to our customers or pose a risk to us or to our customers. Also, if we identify a network





vulnerability that requires a software upgrade or patch in advance of scheduled maintenance, we may perform emergency maintenance.

In all situations, we make every effort to notify the impacted customers within 24-48 hours prior to the maintenance activity. However, we retain the authority to implement emergency maintenance at any time to help ensure a secure, healthy, and stable network environment.

4.2.1.3.5 Vendor should provide notification of three (3) business days or more in advance of emergency maintenance. While the State understands emergency outages and/or unplanned maintenance windows occur, it is expected that these situations are kept to a minimum. Please describe your company's notification process for emergency maintenance and outages.

**AT&T Response:**

Please refer to the previous response. AT&T enables emergency protocol that would provide notification for security patches that may affect services within 48 hours of learning of the critical patch.

4.2.1.3.6 If the Vendor's work requires them to be at a State site, the Vendor should provide Agency at least 72 hours' notice before arriving at the site and comply with State law and all Agency policies, including but not limited to background checks for contractors, vendors, and visitors. Please describe your approach and methodology in your solution/response.

**AT&T Response:**

AT&T can provide 72 hours notification.

4.2.1.3.7 The Vendor's network operation support center should provide: all tiers of support, including end-user support, advanced technical expertise, be staffed with resources that are proficient in spoken and written English, maintain and take responsibility for trouble tickets reported by the State until resolved, and provide a tiered support escalation process. Please describe your network operation support center's structure, processes, and procedures for handling trouble tickets, resolving those tickets, and reporting back to the State's point of contacts.





### AT&T Response:

The AT&T Global Customer Support Center (GCSC) provides support for our customers and services.

The GCSC organizational structure provides focused management to deliver a complete customer care package that includes 24x7 support. Teams of analysts with tier 1 and tier 2 skills own and manage a problem from its beginning to resolution. As necessary, tier 3 analysts provide their experience and support.

Whenever possible, we monitor in-scope service components—including client routers, provider devices, and circuits. In monitoring components, we use our proprietary, state-of-the-art integrated Global Enterprise Management System (iGEMS) platform. iGEMS supports common, consistent management of enterprise Wide Area Network (WAN), Local Area Network (LAN), voice, and security services.

iGEMS tools can support reactive management (indication that something has failed), pro-active management (indication of imminent failure) and predictive management (prediction that failure will occur if trends continue). Our iGEMS tools, along with supplier tools that use integrated processes and methodologies, are central to our global network of 24x7 customer and network management centers.

We proactively manage Simple Network Management Protocol (SNMP) manageable devices. We up/down (ping) manage and/or reactively manage devices that aren't SNMP manageable. And, we work with you to discuss any additional SNMP traps you require.

After initial automated triage, correlation, and fact finding, the alarms and data that iGEMS generate flow directly to our support staff so we can take appropriate action. In addition, trending information is available to the AT&T Service Managers we assign to you who perform predictive fault resolution—whether that is re-balancing of traffic classes, upgrade/downgrade of a circuit, or a full redesign project.

When you have an issue that requires escalation, our Customer Operations team uses a 24x7 escalation process to increase focus and resources. In addition, we prefer to review your business-critical sites to better understand your specific escalation criteria for them.

We add Read Only (RO) and Read-Write SNMP Community Strings to managed devices for use with our monitoring and management systems in addition to customer-required RO strings. We monitor SNMP traps and Management Information Bases (MIBs) as necessary to monitor faults or detect abnormal behavior by device. If you require



additional SNMP traps and deem them to be non-intrusive to normal device behavior or performance, we can enable additional traps.

This means that we provide comprehensive care to help you keep your network running.

4.2.1.3.8 The Vendor's solution should include a documented support and escalation structure to address outages. The State prefers the severity of the issue/support problem to determine the average problem resolution response time, as outlined below:

- Severity Level 1 is defined as an urgent situation, where the customer's services are unavailable and the customer is unable to use/access the network. The Vendor should resolve Severity Level 1 problems as quickly as possible, which on average should not exceed two (2) business hours. If repair inside the 2-hour window is not feasible, then regular 1-hour updates are desired.
- Severity Level 2 is defined as significant outages and/or repeated failures resulting in limited effective use by the customer. The service may operate but is severely restricted (i.e. slow response, intermittent but repeated inaccessibility, etc.). The Vendor should resolve Severity Level 2 problems as quickly as possible, which on average should not exceed four (4) business hours. If repair inside the 4-hour window is not feasible, then regular 2-hour updates are desired.
- Severity Level 3 is defined as a minor problem that exists with the service, but most of the functions are still usable, and some circumvention may be required to provide service. The Vendor should resolve Severity Level 3 problems as quickly as possible, which on average should not exceed ten (10) business hours. If repair inside the 10-hour window is not feasible, then updates are desired at the start of the next business day and every day thereafter until repairs are complete.

Please describe your company's severity level structure, as well as your documented procedures for handling outages, including escalation processes, notification methods, and resolution times.

#### AT&T Response:

AT&T will adjust an incident's severity level at your request, depending on the business impact. Please see details response in section 4.2.1.3





If you incorrectly report the business impact, we can change the severity level; however, we avoid downgrading a severity level due to service restoration.

You can find the AT&T Service Assurance program procedures for reporting and escalating issues in the Customer Service Guides (CSGs).

Your AT&T service manager provides you with CSGs for your specific services. In these guides, you'll find the procedures to report and escalate troubles. In addition, your service manager will provide you with a link to the Service Assurance Escalation Portal (<https://ebiznet.att.com/engage/>).

This means that you'll have the specific directions you need to help us quickly resolve your service concerns.

4.2.1.3.9 The State desires the ability to place initial service orders, any changes with an associated charge, or to disconnect services, electronically and receive confirmation of receipt and subsequent order detail. The State desires details including the following data elements:

- Telecommunications Change Request (TCR) Form Number
- Date order was received
- Customer Name
- Customer on-site address
- Projected due date
- Rate element identifier (circuit ID or other)
- Additional order details

Additionally, the State prefers the Vendor's solution has a web portal for Agencies to enter moves, add, and changes that do not contain billing elements. MACD changes should be resolved by the same or next business day. Please describe your company's ability to accept, process, and report on electronic order submissions, as well as any requirements from the State needed to implement such a program.

#### AT&T Response:

AT&T provides an interactive portal that provides support for providing service level details defined.





4.2.1.3.10 The State maintains a Learning Management System (LMS) for training purposes. The State desires web-based training and training materials for all services offered under this contract. The State desires the Vendor to provide materials that can be uploaded into its LMS, initial Train the Trainer session(s), and documentation/reference materials that can be distributed to and used by end-users. The State intends to incorporate these materials into its LMS, as well. Additionally, the State desires training sessions, if requested by the Agency, and the Vendor should include a professional services rate for training that would be above and beyond the initial training included in the site deployment. The State expects the Vendor's training materials to be updated as necessary. The training services for the hosted voice services should be included in the monthly per package cost. Please provide information regarding your training program.

**AT&T Response:**

AT&T can provide written as well as web based training information to support the States requirements. AT&T updates all training material on an annual basis as well as when upgrades provide for new feature enhancement. The State can also schedule specific on site or web training as needed.

4.2.1.3.11 The State desires an hourly rate for Hosted Contact Center Training Services in the instance the State desires training sessions beyond the training provided at initial implementation. The training at initial implementation should be built into the one-time costs for the Contact Center. These training services should include training for all contact center roles and should be provided at the State's request. Please describe your Contact Center training offerings and your solution's ability to meet this goal.

**AT&T Response:**

AT&T provides three forms of training in order to support the States requirements.

- End user training provides support for up to 1 hour of training groups of end users up to 20 per class on site or up to 50 via web session. The cost for end user training is \$200.00 per hour
- Train the trainer training provides support for training customer staff that would be responsible for conducting ongoing training. The training session can cover







end user features and devices. Up to 20 participants can attend this type of training either on site or via web session. The costs is \$200.00 per hour.

- Contact center agent and manager training provides support for specific users that require contact center agent desktop or administration. The cost for this training is \$250.00 per hour.

**4.2.2. Mandatory Project Requirements** — The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.

#### 4.2.2.1 Managed Voice Services

**4.2.2.1.1** The Vendor must provide a turnkey technical support solution that ensures the continued operations and MACD needs of the State's existing telephony infrastructure, as defined in Appendix A, through the migration period to a Hosted VoIP solution. Additionally, the Vendor must, at the State's discretion, migrate any site to the hosted solution.

#### AT&T Response:

AT&T defines 'turnkey' to mean that AT&T will provide only the items of equipment and services specifically listed in this bid response. For the price(s) quoted herein, AT&T will provide the items of equipment and services specifically listed in this bid response. Any additional equipment or services beyond those listed in AT&T's response will be provided at additional charges. Our pricing is predicated on the requirements as set forth by the bid documents, and use of terms and phrases, such as "turn-key" or "included even if not specifically listed," does not require AT&T to provide equipment or services beyond those specifically noted in our quote.

#### 4.2.2.2 Hosted Voice Services

**4.2.2.2.1** The Vendor must agree the State owns all data gathered under the scope of this contract and the Vendor must produce and/or return the data upon the State's request in an editable format.



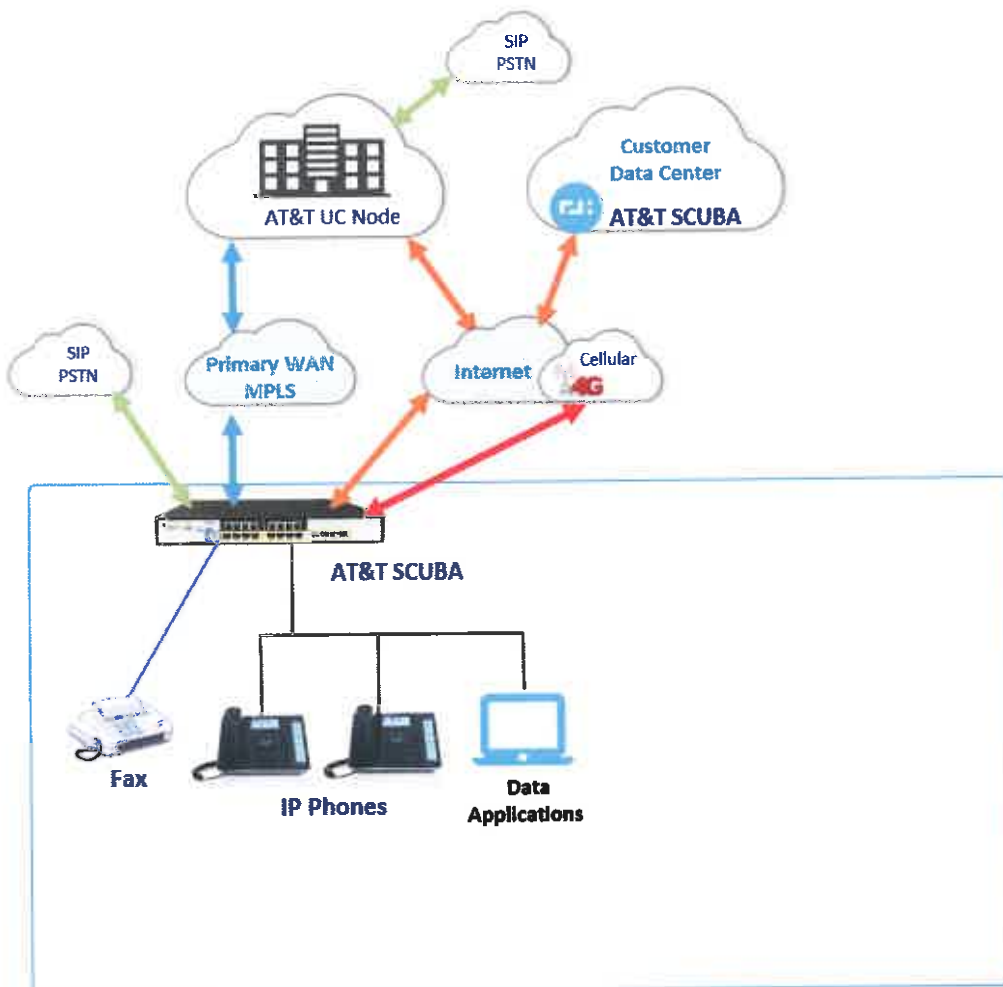
#### AT&T Response:

AT&T has read and will comply with this request.

4|2.2.2.2 Vendor's solution must provide support for local failover and/or survivability services, if requested by Agency, in the event the hosted service becomes inaccessible.

#### AT&T Response:

AT&T provides for local failover utilizing Cisco SRST, AT&T Integrated SDWAN services that provides up to three levels of local network failover. Example of local survivability.





4.2.2.2.3 Vendor's solution must provide local telephone numbers in West Virginia.

**AT&T Response:**

AT&T provides support for porting number in West Virginia.

4.2.2.2.4 Vendor's solution must support inbound Automatic Number Identification (ANI).

**AT&T Response:**

AT&T supports as standard feature.

4.2.2.2.5 Vendor's solution must include inbound Caller ID, outbound custom telephone number, and outbound custom name display.

**AT&T Response:**

AT&T provides support for inbound caller ID and can provide custom outbound call masking as part of our standard services.

4.2.2.2.6 Vendor's solution must support Dialed Number Information Services (DNIS) on 800 # toll-free telephone services.

**AT&T Response:**

AT&T provides this as a standard feature.

4.2.2.2.7 Vendor's solution must support rerouting of calls to an alternate site at the State's directive.

**AT&T Response:**

AT&T supports automatic alternate routing as well as directed call routing.

4.2.2.2.8 Vendor's solution must support 900/976 blocking.



**AT&T Response:**

AT&T support 900/976 and any other specific number blocking at trunk and user levels.

4.2.2.2.9 Vendor's solution must support x11 services (currently 211, 411, 511, 611, 811, 911).

**AT&T Response:**

AT&T support all standard service dialing numbers including currently 211, 411, 511, 611, 811, 911).

4.2.2.2.10 Vendor's solution must include Direct Inward Dial (DID) feature and service.

**AT&T Response:**

AT&T supports DID and DOD features for all users.

4.2.2.2.11 Vendor's solution must support Operator services.

**AT&T Response:**

AT&T support operator services.

4.2.2.2.12 Vendor's solution must support local number portability.

**AT&T Response:**

AT&T provides support for local number portability as part of our standard services.

4.2.2.2.13 Vendor's solution must provide unlimited free local and long-distance calling.

**AT&T Response:**

AT&T offers local and long distance packages that can also include international.





4.2.2.2.14 Vendor's hosting center(s) must be located within the continental United States.

**AT&T Response:**

AT&T provides services for our US customer from data centers located in Dallas, TX, Watertown, MA.

4.2.2.2.15 Vendor must provide Train the Trainer sessions for Hosted Voice Services implementations.

**AT&T Response:**

AT&T provides three types of training

- End user training provides support for up to 1 hour of training groups of end users up to 20 per class on site or up to 50 via web session. The cost for end user training is \$200.00 per hour
- Train the trainer training provides support for training customer staff that would be responsible for conducting ongoing training. The training session can cover end user features and devices. Up to 20 participants can attend this type of training either on site or via web session. The costs is \$200.00 per hour.
- Contact center agent and manager training provides support for specific users that require contact center agent desktop or administration. The cost for this training is \$250.00 per hour.

**4.2.2.3 Hosted Contact Center Services**

Vendor's Contact Center solution must support:

4.2.2.3.1 Automatic Call Distributor (ACD)

4.2.2.3.2 Computer telephony integration (CTI)

4.2.2.3.3 Call control

4.2.2.3.4 E. 164

4.2.2.3.5 Interactive voice response (IVR)

4.2.2.3.6 Voice Recording





4.2.2.3.7 High Availability with load balancing and built-in redundancy

4.2.2.3.8 Vendor must provide Train the Trainer sessions, encompassing all Hosted Contact Center roles — Administrator, Supervisor, and Agents.

**AT&T Response:**

AT&T Cloud Contact Center provides all listed features as well as Artificial Intelligence including training for contact center agents, administrators and Supervisors. See details in section 4.2.1.1.4.3.

**4.2.2.4 Security**

4.2.2.4.1 The proposed solution must adhere to the security and privacy baseline standards in accordance to the high-security and standard-security use-case requirements.

**AT&T Response:**

AT&T meets and exceeds the high security requirements defined by the State.

4.2.2.4.2 Must adhere to the State of West Virginia's Cyber Security & Privacy policies, procedures, and standards; these can be viewed at the following link: <https://technology.wv.gov/securityæages/policies-issued-by-thecto.aspx>

**AT&T Response:**

AT&T has read and conforms to the standards defined.

4.2.2.4.3 Must adhere to all applicable security and privacy standards and provide compliance for components and network segments that are subject to the following:

- Health Insurance Portability and Accountability Act (HIPAA) requirements as outlined in the attached Business Associate Addendum (BAA) (see **Attachment\_B**)
- Federal Information Security Management Act (FISMA), National Institute of Standards Technology's Special





Publication (NIST SP) 800-53, NIST SP 800-17 which serve as the baseline;

- Family Education Rights and Privacy Act (FERPA) requirements;
- Criminal Justice Information System (CIIS) requirements;
- Payment Card Industry Data Security Standards (PCI-DSS) requirements;
- Federal tax Information (FTI) and Internal Revenue Service publication 1075 (IRS 1075) requirements;
- Centers for Medicare & Medicaid (CMS) Services Information Security Policy requirements.
- Ensure network boundary and access control protection such as dual session boundary controllers and firewalls.
- Data-at-rest and data-in-transit encryption.
- Role-based access control for all applications which process and/or store sensitive data, to ensure need-to-know policies are enforceable.

**AT&T Response:**

AT&T UC as a Service meets all requirements defined for service security. Please see attachments ATT\_UCV\_SDD\_2017r2-7.

4.2.2.4.4 Vendor must draft a cyber risk management plan outlining the process, by which, cyber risk management activities are conducted to identify, assess, communicate, and manage shared cyber risk. The Vendor must provide this prior to the first implementation on the Vendor's hosted solution.

**AT&T Response:**

AT&T will work with the State to draft the cyber risk management plan to meet with the States requirements.

4.2.2.4.5 Vendor must draft an incident management plan aligned with NIST SP 800-61rev2, whereas both the State and Vendor must mutually approve. The plan must include the outlined scope, responsibility matrix, communications plan, procedures, and deliverables



associated with cyber security incident response. In addition, the plan must outline incident reporting requirements, semiannual security reports, and cyber threat intelligence sharing. The Vendor must provide this prior to the first implementation on the Vendor's hosted solution.

**AT&T Response:**

AT&T will leverage our advanced security assessment team to ensure alignment with NIST standards.

4.2.2.4.6 The Vendor must adhere to personnel security requirements for background checks in accordance with state law. The vendor is liable for all costs associated with ensuring staff meets all requirements.

**AT&T Response:**

AT&T will comply with requirements including required background checks.

4.2.2.4.7 Vendor must agree to drafting an audit management plan designed to assist the state with conducting internal and external compliance audits when the vendor-supplied solution is within the audit scope. At minimum, the plan must include:

- How the vendor will provide a NIST 800-53 security controls report, outlining organizational responsibilities (State, Vendor, or Shared), per each applicable control for each major application/information system within the audit scope.
- Plan of Action & Milestone documentation for non-compliant security & privacy controls when the vendor holds primary or shared control responsibility. The Vendor must provide this prior to the first implementation on the Vendor's hosted solution.

**AT&T Response:**

AT&T will comply with this request.

**4.2.2.5 Service and Support**





4.2.2.5.1 Vendor must provide a network operation support center(s) for all tiers of support, including end-user support, that is available 24x7x365 and is accessible via a toll-free number.

**AT&T Response:**

The AT&T Global Customer Support Center (GCSC) provides support for our customers and services.

The GCSC organizational structure provides focused management to deliver a complete customer care package that includes 24x7 support. Teams of analysts with tier 1 and tier 2 skills own and manage a problem from its beginning to resolution. As necessary, tier 3 analysts provide their experience and support.

Whenever possible, we monitor in-scope service components—including client routers, provider devices, and circuits. In monitoring components, we use our proprietary, state-of-the-art integrated Global Enterprise Management System (iGEMS) platform. iGEMS supports common, consistent management of enterprise Wide Area Network (WAN), Local Area Network (LAN), voice, and security services.

iGEMS tools can support reactive management (indication that something has failed), pro-active management (indication of imminent failure) and predictive management (prediction that failure will occur if trends continue). Our iGEMS tools, along with supplier tools that use integrated processes and methodologies, are central to our global network of 24x7 customer and network management centers.

We proactively manage Simple Network Management Protocol (SNMP) manageable devices. We up/down (ping) manage and/or reactively manage devices that aren't SNMP manageable. And, we work with you to discuss any additional SNMP traps you require.

After initial automated triage, correlation, and fact finding, the alarms and data that iGEMS generate flow directly to our support staff so we can take appropriate action. In addition, trending information is available to the AT&T Service Managers we assign to you who perform predictive fault resolution—whether that is re-balancing of traffic classes, upgrade/downgrade of a circuit, or a full redesign project.

When you have an issue that requires escalation, our Customer Operations team uses a 24x7 escalation process to increase focus and resources. In addition, we prefer to review your business-critical sites to better understand your specific escalation criteria for them.



We add Read Only (RO) and Read-Write SNMP Community Strings to managed devices for use with our monitoring and management systems in addition to customer-required RO strings. We monitor SNMP traps and Management Information Bases (MIBs) as necessary to monitor faults or detect abnormal behavior by device. If you require additional SNMP traps and deem them to be non-intrusive to normal device behavior or performance, we can enable additional traps.

This means that we provide comprehensive care to help you keep your network running.

4.2.2.5.2 The successful Vendor must assign an experienced and skilled Project Manager who will provide a high-level project management plan including key components such as a project charter, issue tracking, statements of work (SOW), work breakdown structures (WBS), implementation schedules, etc. in accordance with the Project Management Body of Knowledge (PMBOK) or other industry standard project management methodology stated in West Virginia State Code (SSA-6-4b). The link can be found at:

<http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=05a&art=6#06>

The project management plan must be submitted to and approved by the WVOT Project Management Office (PMO) prior to engaging the first agency for VoIP services implementation.

#### AT&T Response:

AT&T shall employ and make available at reasonable times an adequate number of appropriately qualified and trained personnel, familiar with Customer's operations and use of telecommunications services, to provide and support Customer's use of the Services in accordance with the terms of AT&T's response to this RFP. The identities and titles of specific persons and their availability to provide and support Customer's needs will be separately established by authorized representatives of AT&T upon award of the RFP to AT&T. If required after contract award, AT&T will supply documentation to authenticate technical expertise, within the parameters of confidentiality limits.

Due to the possibility of promotions or role reassignments, AT&T is unable to guarantee that assigned personnel will remain on the project for the duration of any resulting contract. However, AT&T understands the importance of consistent support and will work with the Customer to the greatest extent possible to minimize personnel transition







and to ensure that the performance of the personnel supporting the Customer and this project meets or exceeds the Customer's expectations.

4.2.2.5.3 The successful Vendor's Project Manager must track and report (via written status reports) the following: schedule, scope, budget, issues, risks, specified performance indicators, and other metrics determined appropriate throughout the project and each site implementation.

#### **AT&T Response:**

Project Management is a service provided by AT&T that provides you with professional project managers who work closely with your project team to develop and implement comprehensive project processes and plans. Project Management includes the Statement of Work, Master Schedule and site schedules, Project Acceptance Criteria, and other key deliverables that support your overall plan. Project Management provides a project or program manager who coordinates project resources including all project staff, other internal AT&T resources, WAN/remote access service providers, cabling contractors, and other 3rd party resources. They may be based onsite or work remotely depending on project requirements.

A project is a non-routine job with defined start and end dates, a scope, and a budget. In most cases, an ad-hoc organization executes a project and disbands once the project is over. Network integration projects require project management expertise. Our professional project managers in the World Wide Project Management Group are technical and logistical problem-solvers who are trained and experienced in planning and implementing integration projects.

Project Management capabilities are reinforced by our expertise in networking, structured cabling, inventory management, and global logistics. Project Management complements the LAN, WAN, and remote access equipment configuration, staging, installation, and on-going support services.

We can combine Project Management with many network implementation services to deliver any size or scope of Network Integration project. We have broad expertise in technology deployments including IP Telephony, WiFi, IP video, cabling, data center build-outs, national and international local area network/wide area network installation, PBX, video, call centers, and security systems.

We also provide multi-national Project Management services. We are your single point of contact for international deployment and integration projects. We can identify and



reduce the risks associated with multi-national deployments through the application of our established project management methodology.

Our multi-national project managers understand the intricacies of international cultures, business practices, and regulatory requirements. We take the domestic network lifecycle offshore and can manage all aspects of a multi-national project including procurement, staging, transportation and logistics, documentation, implementation, maintenance, and invoicing.

4.2.2.5.4 Vendor must work with the WVOT using the established Telecommunications Change Request (TCR) (Attachment\_C) procedures for ordering and implementing these telecommunications services.

**AT&T Response:**

AT&T will incorporate the TCR as part of our change request process.

4.2.2.5.5 Vendor billing errors must be credited back to the State from the effective date of the error. The State reserves the right to withhold payment until credit is received.

**AT&T Response:**

We manage bill disputes via AT&T BusinessDirect®.

If you discover a billing error, you should submit your dispute to AT&T's Customer Care Center via BusinessDirect. Once we receive it, our Customer Care Center will evaluate your request and put the disputed charges in a no-treat status while investigating the dispute.

A Customer Care representative will notify you of the resolved dispute via BusinessDirect. This notification will include details as to whether an adjustment was issued or charges are being sustained. If we're unable to resolve the dispute within 30 days, you can escalate the dispute to the Business Manager.

After we've resolved the dispute, you must pay the bill (consistent with the resolution) within ## days (as determined by your state's public utility commission) of AT&T's resolution notice. If you fail to pay within that timeframe, we may impose interest charges calculated from the date that payment was originally due, at the lower rate of





1.5% per month (18% per annum) or the maximum rate allowed by law, plus reasonable attorney's fees.

This means that, by using our online tool, we can quickly address and correct your billing disputes.

4.2.2.5.6 For auditing, billing, and support purposes, the State requires any service with an associated rate to be identified on its monthly bill. As such, the State must be provided, at a minimum, the following:

- Billing Month
- Billed Entity Name
- Customer Name/Account (if different from billed entity)
- Service Location
- Service Period
- Itemized Cost for Individual Billing Components
- Itemized Call Detail
- Itemized Cost for Any One-Time or Non-Recurring Charges
- Itemized Cost for Any Surcharges and Total Cost

The cost identified in the bill must match the contract rates for the specified services. The Vendor must provide the State's monthly bill in an editable format such as Excel and/or csv.

#### AT&T Response:

AT&T will endeavor to provide the State the requested information in an alternative media if cannot be provided on the physical invoice.

4.2.2.5.7 The Vendor must invoice on a consistent monthly billing cycle across all services. Services installed or disconnected for a partial month must be prorated based on the date the service is activated/accepted or disconnected. The Vendor must not bill the State of services until the services have been activated and accepted as functional. The Vendor shall not bill the State for services after the disconnect due date listed on the submitted TCR.



**AT&T Response:**

AT&T will make every effort to bill within two billing cycles of installation; however, AT&T reserves the right to invoice for new Services within 6 months. AT&T will invoice the State for individual Services once the Services is installed and turned up at a State location and not upon acceptance by the State. AT&T will provide consistent monthly billing and will assign billing specialists to support the States requirements.

4.2.2.5.8 The Vendor must provide and update a weekly status report and/or order log for submitted TCRs.

**AT&T Response:**

AT&T will comply with this request.

4.2.2.5.9 If, as part of its proposal, the Vendor submits appendices or other supplemental materials, the Vendor must denote specifically in those materials where the relevant information is located.

**AT&T Response:**

AT&T will denote.

4.2.2.5.10 The State expects full, complete, and timely cooperation in disentangling the relationship in the event the Agreement expires or terminates for any reason. In the event of expiration or termination, the State expects that the Vendor shall, among other things: return all State data and documentation to the State, including but not limited to configuration information; transfer ownership of all leased equipment at no cost to the State (other than the payments already received by the Vendor under the Agreement); and, allow the State or the replacement provider(s) continued access to all billing, ordering, and trouble ticketing systems, and processes that have been employed in servicing the State, in accordance with methods and procedures to be agreed upon and established in the Agreement. Please acknowledge your acceptance of this.

**AT&T Response:**

AT&T takes exception to the allowing of access to billing data directly. If the State chooses, the State can provide a user ID and passcode for others to access any billing







data or reports that may be available via the AT&T Business Direct Portal. AT&T can accept the remainder of this Section.

4.3. **Qualifications and Experience:** Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives were and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

#### **AT&T Response:**

##### **Staff biography**

Because the assignment(s) for specific tasks are not made until the contract is awarded, specific name(s) and biographical information for specific tasks cannot be supplied at this time. The required documentation will be furnished if AT&T is your vendor of choice.

AT&T is uniquely qualified to provide proficient technical service for the system proposed herein. Only manufacturer trained Technicians and Service Consultants perform installation, maintenance and training on the system. If required after contract award, AT&T will supply documentation to authenticate technical expertise, within the parameters of confidentiality limits.

##### **References**

During negotiations or presentations, your AT&T account team will secure customer references.

Most customers do not wish to be contacted directly as references. So, your account team will work to arrange contact or to supply you with direct contact information.

Consequently, we're unable to provide you with customer references until that time.

4.3.1. **Qualification and Experience Information:** Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.





4.3.1.1 Vendor should provide three (3) examples demonstrating at least three (3) years of experience in providing a Hosted VoIP solution of a similar size and scope — 15,000 users across 200 sites with one example being a public entity. Vendor should provide a summarization of each project including goals and objectives, total number of phones deployed per site, length of time deployment took, if still in service, and reference for each example.

#### AT&T Response:

AT&T has developed and provided solution for IBM with over 2000 location and over 200,000 users. AT&T provide support for migration of all existing Cisco and AVAYA phones, analog gateways and contact center agents to AT&T UC as a Service.

US Department of the Army for 1 Million users. AT&T created dedicated NOC and SOC and migrated users for over 4000 global locations including number porting and support for migration to Skype clients and variety of IP PBX's

Advanced Auto Parts for 6000 locations and over 50,000 devices. AT&T implemented dynamic local failover for each location with primary MPLS and LTE backup along with deploying IP phones and coordination number porting for over 50,000 phone numbers and testing and turn up with monitoring and management for core UC as a service and the voice gateways and IP Phones and contact center. Additional examples and reference available through prior authorization with our over 600 customers.

4.3.1.2 Vendor should provide at least one (1) example demonstrating at least three (3) years of experience in providing single/multiple Hosted Call Center solutions of a similar size and scope — 500 users across 20 sites. Vendor should provide a summarization the project including goals and objectives, total number of agents per site, length of time deployment took, if still in service, and reference for the example.

#### AT&T Response:

AT&T provides support for large financial institutions with between 20-70 locations with between 400- 1000 agents with centralized call processing and WebRTC agent desktop as well as IP phones at core contact centers and remote home office locations. AT&T provided the on site implementation as well as the call flow scripting and integration with CRM application such as Salesforce and Microsoft Dynamics and custom API applications.





4.3.1.3 The State desires an Account Team (including Account Support Representative, Technical Support Representative, Solution Implementation Support Representative, Contract Manager, Billing Support Representative, Security/Compliance Specialist, and Project Manager) for the winning solution and life of the contract. Vendor should describe in detail the responsibilities of key roles and staffs experience in working in these roles.

**AT&T Response:**

AT&T provides you with support under our Strategic Account Management (SAM) model.

We tailor support to meet your specific needs, and we provide local, regional, and global support, as needed. Account team members typically include a Global Account Director, a Regional Account Director, a Technical Solution Consultant, and a National Account Manager.

The AT&T account team adheres to a formal methodology to guide its interaction with you. This model dictates a collaborative approach to direct customer interaction and sales support in each major market in which you operate. We structure your AT&T account team to mirror your organizational makeup. We locate the account team lead near your corporate headquarters and support him or her with local and regional account teams and with our support organizations around the world.

AT&T uses its global governance model to successfully support many large multi-national corporations.

4.3.1.4 Vendor should describe its experience and process in conducting cyber risk management ensuring shared risk is identified, assessed, communicated, and managed.

**AT&T Response:**

AT&T has extensive experience as a provider of Managed Security Services.

We've long been a pioneer in developing cybersecurity capabilities. AT&T Labs and our Chief Security Office (CSO) have worked closely together to provide industry-leading technology, and security is at the core of our network and our goals.

The CSO maintains a global security organization that comprises more than 600 security professionals, and more than 1,400 additional security specialists work in our other



organizations. These security experts have an average 15 years of experience in the field.

4.3.1.5 Vendor should describe its experience and process for conducting NIST SP 80053 security assessment and authorization control families' activities, designed to ensure each vendor-provided solution implementation adheres to security and privacy requirements before being placed into production.

**AT&T Response:**

The sources we use to develop the AT&T Security Policy and Requirements (ASPR) include laws, industry standards, best practices, and our technical and business expertise.

Our ASPR framework helps us set objectives and provides direction and principles for action regarding information security. Via that framework, we maintain a set of security standards that draw upon and meet industry standards, such as the National Institute for Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), and the International Standards Organization (ISO) /International Electrotechnical Commission (IEC) 27001:2005.

4.3.1.6 Vendor should list all government or standards organization security certifications it currently holds that apply specifically to the vendor's proposal, as well as those in process at time of response. Specifically include HIPAA, CMS, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

**AT&T Response:**

AT&T has supported our services with CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171,

4.3.1.7 Vendor should provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp), and certifications relating to cybersecurity and privacy controls.

**AT&T Response:**

AT&T will provide prior to contracting and after down select process.





4.3.1.8 Vendor should describe its experience and capabilities in supporting their customers concerning compliance audits when the vendor-supplied solution is within the scope of audit.

**AT&T Response:**

AT&T support scheduled audits when requested by customer. AT&T conduct audits on security and operational aspects on an annual basis and for fee and upon request for additional request when required.

4.3.1.9 Vendor should describe its experience and provide an overview of their incident management process and cyber threat intelligence sharing process for incidents associated with the vendor provided solution.

**AT&T Response:**

AT&T has a well defined Problem Management process.

This process helps us identify problems and work to resolve them. Our goal is to minimize the adverse impact of incidents and problems within your infrastructure. After reducing the frequency and severity of impacts to your systems, we institute preventive action.

We begin the process by obtaining the following data from Incident Management:

- Incident details
- Any defined workaround
- Trend data

We complete the process by producing the following deliverables:

- Known errors
- A Request for Change (RFC)
- An updated problem record (including the solution and/or any available workaround)
- A closed problem record (for a resolved problem)
- A response from incident matching to problems and known errors



We use a Problem Management tool to identify and track root causes and create action plans to remove underlying errors. Our Problem Management process uses two key approaches: reactive and proactive. The reactive approach manages problems to closure to minimize adverse impacts. The proactive approach analyzes closed incidents for trends to identify problems and then executes preventive action to avoid adverse business impacts.

When you consider the importance of your systems and infrastructure, our Problem Management process is critical to reducing the frequency and severity of incidents that impact them.

4.4. Oral Presentations: The Agency will require oral presentations of all Vendors participating in the RFP process. The date of the presentations will be determined at a later time and all vendors will be notified in advance. During oral presentations, Vendors may not alter or add to their submitted proposal, but only clarify information. A description of the materials and information to be presented is provided below:

Materials and Information Requested at Oral Presentation:

- 4.4.1. Summary of solution, including product and support offerings, ability to deliver the solution in the specified timeframes, and experience in providing managed and hosted voice solutions.
- 4.4.2. The State will ask clarifying questions regarding the Vendor's submitted technical response.
- 4.4.3. Contact Center Presentation to see a live demonstration of Vendor's offering.

**AT&T Response:**

AT&T will support oral presentation as required to further details our capabilities to support the State.







## SECTION 5: VENDOR PROPOSAL

- 5.1. **Economy of Preparation:** Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.

**AT&T Response:**

AT&T has read and complies.

- 5.2. **Incurring Cost:** Neither the State nor any of its employees or officers shall be held liable for any expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.

**AT&T Response:**

AT&T has read and understands.

- 5.3. **Proposal Format:** Vendors should provide responses in the format listed below:

- 5.3.1. **Two-Part Submission:** Vendors must submit proposals in two received submitted in two distinct parts: technical and cost. Technical proposals must not contain any cost information relating to the project. Cost proposal must contain all cost information and must be sealed in a separate envelope from the technical proposal to facilitate a secondary cost proposal opening.
- 5.3.2. **Title Page:** State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature and date.
- 5.3.3. **Table of Contents:** Clearly identify the material by section and page number.
- 5.3.4. **Response Reference:** Vendor's response should clearly reference how the information provided applies to the RFP request. For example, listing the RFP number and restating the RFP request as a header in the proposal would be considered a clear reference.
- 5.3.5. **Proposal Submission:** All proposals must be submitted to the Purchasing Division prior to the date and time stipulated in the RFP as the opening date. All submissions must be in accordance with the provisions listed in Section 2: Instructions to Bidders Submitting Bids.



**AT&T Response:**

AT&T has read and understands.





## SECTION 6: EVALUATION AND AWARD

- 6.1. **Evaluation Process:** Proposals will be evaluated in two parts by a committee of three (3) or more individuals. The first evaluation will be of the technical proposal and the second is an evaluation of the cost proposal. The Vendor who demonstrates that it meets all of the mandatory specifications required, attains the minimum acceptable score and attains the highest overall point score of all Vendors shall be awarded the contract.

### AT&T Response:

AT&T has read and understands.

- 6.2. **Evaluation Criteria:** Proposals will be evaluated based on criteria set forth in the solicitation and information contained in the proposals submitted in response to the solicitation. The technical evaluation will be based upon the point allocations designated below for a total of 70 of the 100 points. Cost represents 30 of the 100 total points.

#### Evaluation Point Allocation:

##### Project Goals and Proposed Approach

Approach & Methodology to Goals/Objectives	55 Points Possible
• 4.2.1.1 Voice Services	(40 Points Possible)
• 4.2.1.2 Security of Solution's Services	(5 Points Possible)
• 4.2.1.3 Service and Support of Hosted Solution	(10 Points Possible)

Approach & Methodology to Compliance with Mandatory Project Requirements	0 Points Possible
--	-------------------

##### Qualifications and experience

Qualifications and Experience Generally	10 Points Possible
---	--------------------

- 4.3 Vendor Qualifications and Experience

Exceeding Mandatory Qualification/Experience Requirements	0 Points Possible
---	-------------------

Oral Presentation	5 Points Possible
-------------------	-------------------



Total Technical Score:

70 Points Possible

Total Cost Score:

30 Points Possible

**Total Proposal Score: 100 Points Possible**

**AT&T Response:**

AT&T has read and understands.

- 6.3. **Technical Bid Opening:** At the technical bid opening, the Purchasing Division will open and announce the technical proposals received prior to the bid opening deadline. Once opened, the technical proposals will be provided to the Agency evaluation committee for technical evaluation.

**AT&T Response:**

AT&T has read and understands.

- 6.4. **Technical Evaluation:** The Agency evaluation committee will review the technical proposals, assign points where appropriate, and make a final written recommendation to the Purchasing Division.

**AT&T Response:**

AT&T has read and understands.

- 6.5. **Proposal Disqualification:**

- 6.5.1. **Minimum Acceptable Score ("MAS"):** Vendors must score a minimum of 70% (49 points) of the total technical points possible in order to move past the technical evaluation and have their cost proposal evaluated. All vendor proposals not attaining the MAS will be disqualified.
- 6.5.2. **Failure to Meet Mandatory Requirement:** Vendors must meet or exceed all mandatory requirements in order to move past the technical evaluation and have their cost proposals evaluated. Proposals failing to meet one or more mandatory requirements of the RFP will be disqualified.

**AT&T Response:**

AT&T has read and understands.





- 6.6. **Cost Bid Opening:** The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.

**AT&T Response:**

AT&T has read and understands.

- 6.7. **Cost Evaluation:** The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

**Cost Evaluation Formula:** Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1:  $\text{Lowest Cost of All Proposals} / \text{Cost of Proposal Being Evaluated} = \text{Cost Score Percentage}$

Step 2:  $\text{Cost Score Percentage} \times \text{Points Allocated to Cost Proposal} = \text{Total Cost Score}$

Example:

Proposal 1 Cost is \$1, 000,000

Proposal 2 Cost is \$1, 100,000

Points Allocated to Cost Proposal is 30





Proposal 1: Step 1 -  $\$1,000,000/\$1,000,000$  = Cost Score Percentage of 1 (100%)

Step 2 -  $1 \times 30$  = Total Cost Score of 30

Proposal 2: Step 1-  $\$1,000,000/\$1,100,000$  Cost Score Percentage of 0.909091  
(90.9091%)

Step 2 —  $0.909091 \times 30$  = Total Cost Score of 27.27273

**AT&T Response:**

AT&T has read and understands.

- 6.8. **Availability of Information:** Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code #5A-3-11 (h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules # 148-1-6.3.d.

**AT&T Response:**

AT&T has read and understands.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration \*\*\* \*\*

**SUBJECT TO THE EXCEPTIONS, CLARIFICATIONS AND RESPONSES SPECIFIED IN AT&T'S PROPOSAL RESPONSE \*\*\***; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

**AT&T Corp.**

(Company)

**Beth Spradlin, Client Solutions Exec 2 Integrated Mob\***

(Representative Name, Title)

**304.690.0140**

(Contact Phone/Fax Number)

**11/26/2018**

(Date)





- 6.6. **Cost Bid Opening:** The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.

**AT&T Response:**

AT&T has read and understands.

- 6.7. **Cost Evaluation:** The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

**Cost Evaluation Formula:** Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1:  $\text{Lowest Cost of All Proposals} / \text{Cost of Proposal Being Evaluated} = \text{Cost Score Percentage}$

Step 2:  $\text{Cost Score Percentage} \times \text{Points Allocated to Cost Proposal} = \text{Total Cost Score}$

Example:

Proposal 1 Cost is \$1,000,000

Proposal 2 Cost is \$1,100,000

Points Allocated to Cost Proposal is 30



Proposal 1: Step 1 -  $\$1,000,000/\$1,000,000$  = Cost Score Percentage of 1 (100%)

Step 2 -  $1 \times 30$  = Total Cost Score of 30

Proposal 2: Step 1 -  $\$1,000,000/\$1,100,000$  Cost Score Percentage of 0.909091  
(90.9091%)

Step 2 —  $0.909091 \times 30$  = Total Cost Score of 27.27273

**AT&T Response:**

AT&T has read and understands.

- 6.8. **Availability of Information:** Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code #5A-3-11 (h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules # 148-1-6.3.d.

**AT&T Response:**

AT&T has read and understands.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions; and other information contained herein; that I am submitting this proposal for review and consideration \*\*\* \*\*

**SUBJECT TO THE EXCEPTIONS, CLARIFICATIONS AND RESPONSES SPECIFIED IN AT&T'S PROPOSAL RESPONSE \*\*\***; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

**AT&T Corp.**

(Company)

**Beth Spradlin, Client Solutions Exec 2 Integrated Mob\***

(Representative Name, Title)

**304.690.0140**

(Contact Phone/Fax Number)

**11/26/2018**

(Date)





- 6.6. **Cost Bid Opening:** The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.

**AT&T Response:**

AT&T has read and understands.

- 6.7. **Cost Evaluation:** The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

**Cost Evaluation Formula:** Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1:  $\text{Lowest Cost of All Proposals} / \text{Cost of Proposal Being Evaluated} = \text{Cost Score Percentage}$

Step 2:  $\text{Cost Score Percentage} \times \text{Points Allocated to Cost Proposal} = \text{Total Cost Score}$

Example:

Proposal 1 Cost is \$1, 000,000

Proposal 2 Cost is \$1, 100,000

Points Allocated to Cost Proposal is 30





Proposal 1: Step 1 -  $\$1,000,000/\$1,000,000$  = Cost Score Percentage of 1 (100%)

Step 2 -  $1 \times 30$  = Total Cost Score of 30

Proposal 2: Step 1-  $\$1,000,000/\$1,100,000$  Cost Score Percentage of 0.909091  
(90.9091%)

Step 2 -  $0.909091 \times 30$  = Total Cost Score of 27.27273

**AT&T Response:**

AT&T has read and understands.

6.8. **Availability of Information:** Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code #5A-3-11 (h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules # 148-1-6.3.d.

**AT&T Response:**

AT&T has read and understands.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration. \*\*\* \*\*

**SUBJECT TO THE EXCEPTIONS, CLARIFICATIONS AND RESPONSES SPECIFIED IN**

**AT&T'S PROPOSAL RESPONSE \*\*\***; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

AT&T Corp.

(Company)

**Beth Spradlin, Client Solutions Exec 2 Integrated Mob\***

(Representative Name, Title)

**304.690.0140**

(Contact Phone/Fax Number)

**11/26/2018**

(Date)







- 6.6. **Cost Bid Opening:** The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.

**AT&T Response:**

AT&T has read and understands.

- 6.7. **Cost Evaluation:** The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

**Cost Evaluation Formula:** Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1:  $\text{Lowest Cost of All Proposals} / \text{Cost of Proposal Being Evaluated} = \text{Cost Score Percentage}$

Step 2:  $\text{Cost Score Percentage} \times \text{Points Allocated to Cost Proposal} = \text{Total Cost Score}$

Example:

Proposal 1 Cost is \$1, 000,000

Proposal 2 Cost is \$1, 100,000

Points Allocated to Cost Proposal is 30



Proposal 1: Step 1 -  $\$1,000,000/\$1,000,000 =$  Cost Score Percentage of 1 (100%)

Step 2 -  $1 \times 30 =$  Total Cost Score of 30

Proposal 2: Step 1 -  $\$1,000,000/\$1,100,000$  Cost Score Percentage of 0.909091 (90.9091%)

Step 2 —  $0.909091 \times 30 =$  Total Cost Score of 27.27273

**AT&T Response:**

AT&T has read and understands.

- 6.8. **Availability of Information:** Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code #5A-3-11 (h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules # 148-1-6.3.d.

**AT&T Response:**

AT&T has read and understands.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration \*\*\* \*\*

**SUBJECT TO THE EXCEPTIONS, CLARIFICATIONS AND RESPONSES SPECIFIED IN**

**AT&T'S PROPOSAL RESPONSE \*\*\***; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

**AT&T Corp.**

(Company)

**Beth Spradlin, Client Solutions Exec 2 Integrated Mob\***

(Representative Name, Title)

**304.690.0140**

(Contact Phone/Fax Number)

**11/26/2018**

(Date)



## AT&T Attachments

- ATT-ICS-2018R6-CF-WV
- ATT\_Cloud\_Contact\_Center\_2018R3
- ATT-UCV-SDD-2017r2-8
- Addendum Acknowledgement Form
- Purchasing Affidavit

# AT&T Integrated Communications Services Overview

Presenter: Mark Beranek  
UC Solution Architect  
CCIE, BSEE, MCSE  
Date: Nov, 2018



# AT&T Collaboration Features (Smart Office Suite)

## WebRTC

Smart Office Collaboration Rooms  
Smart Office Desktop  
Smart Office Mobile

### Voice and Video

Click to call

Call logs

### Conferencing and Collaboration

Reservation-less Meet Me Conferencing

Multi-party video conferencing with screen share

### IM and Presence

Integrated with Global Directory

Presence includes "on the phone"

Integration with Skype for IM and Presence via API

### Directory Integration

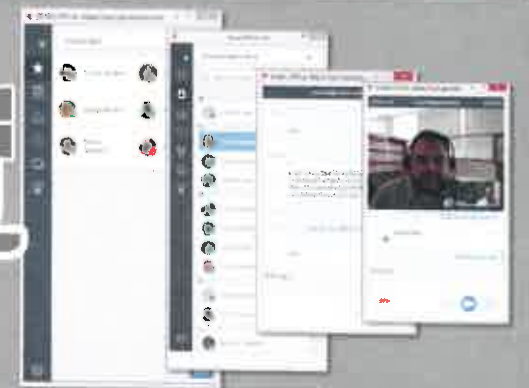
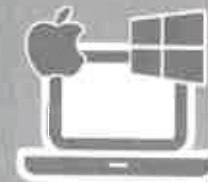
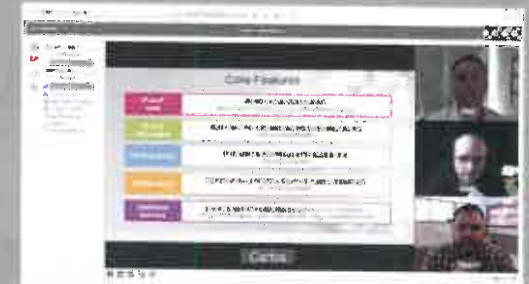
View corporate or system directories Microsoft AD and LDAP

### Value

Extends UC functionality wherever you may roam

Replace or complement desktop phone and mobile phone

Consistent experience on Windows, Mac and Mobile



© 2014 AT&T Affiliates

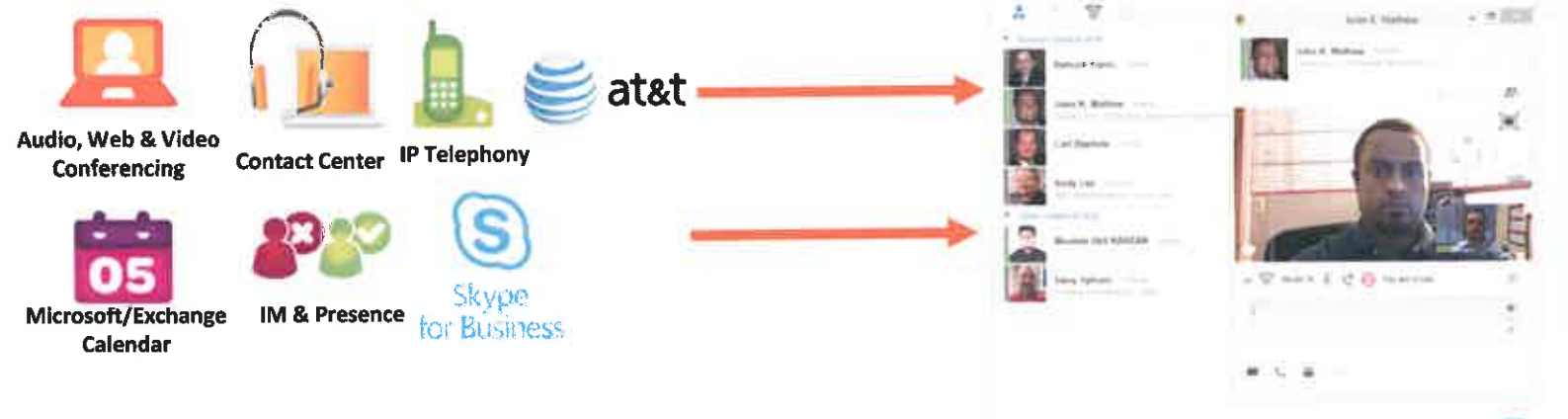


# Skype and Google Collaboration

The RTC client for Skype for Business or Google blends together the best of Microsoft Skype IM, Presence and Directory Access with the reliability and scale of AT&T voice, video and collaboration solutions.

AT&T leverages Omni client technology that uses an HTML5 client core with platform specific WebRTC-based agents. Omni clients look like a rich application to the user but deploy like a web client for the IT professional. Integration via AT&T API directly between client and Skype or Google applications instead of middleware integration.

- Maintain the features and reliability of a traditional PBX
- Eliminate the cost of new Microsoft licensing – no premium CALs or E5 required, leverage E3 license with AT&T provided call control
- Dramatically reduce the complexity of Google/Skype deployments – no new servers or gateways – clients use WebRTC and a browser on many devices/platforms



© 2018 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T company except under a written agreement.



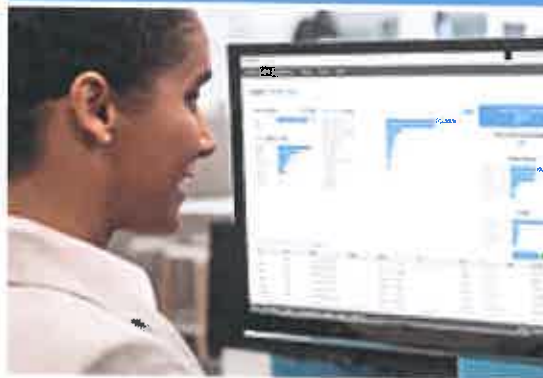
# AT&T Universal Help Desk

## Core Support Services



- 7X24X365 Monitoring, Management and MACD
- Core UC Applications Support
- Core Servers, SBC, Firewalls, LAN
- SBC, Voice Gateway Support
- IP Phone Management
- Video end point support
- Patch and upgrades
- Network access and SIP/PSTN
- SDWAN applications and hardware
- Ebonding Support

## Asset Management



- Track all end points in a common asset database
- Software upgrade support
- Track end device maintenance
- Take over of existing assets
- Third party services coordination

## Analytics



- Conference Bridge Utilization Reports
- Capacity planning
- Call Quality Reports
- PSTN utilization
- Call Detail Reports

Support for legacy and new voice, and collaboration services

© 2018 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.

 **AT&T Business**

# AT&T Network Monitoring and Management

End to end correlation of SIP signaling, media and event alerts.

AT&T provides proactive monitoring, management and MACD support

- Central pain of glass to view overall service performance
- Proactive alerts based on MOS scoring for voice quality
- RMA support for premise equipment replacement coordination
- AT&T UC Node core applications and hardware support
- Customer premise equipment monitoring and management
- Monitoring and management of existing LAN, WAN, WIFI

The UC Services Support will provide reports to help the Customer understand the overall status of the following services.

- PC to PC calling reports
- PC to PSTN calling reports
- IP Phone to IP Phone calling reports
- Analog voice gateway call quality
- Call volume reports
- Call Detail Reporting



# AT&T UC Service Dashboard

**Weekly Reports** - These reports look at the summarizing the weekly ticket activity showing all tickets opened, closed and still active tickets.

**Monthly Reports** - These monthly reports look at the contracted infrastructure devices. The UC Services Support will send out detailed reports each month to customer designated contact person. The reports include statistics on:

- Network, device uptime and availability
- Fault history
- Trouble tickets
- MACD's used
- Professional Services hours used
- Configuration changes during the month

**Quarterly Service Review** - Provides business intelligence information based on the data that the UC Services compiles. This information has potential business impacting information that reflects CPE network trends observed, capacity planning, resource utilization trends, ticketing trends, compliance issues, best practice standards, security concerns and business continuity planning.



AT&T, the AT&T logo, and the AT&T globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.





# AT&T UC Service Admin Portal

- Add new users
- Edit existing user information
- Edit features
- Reset user passwords
- Define Call Permission Levels
- Define and edit location information
- Configure voicemail, voice services, and conferencing settings
- Change user phone number

## AT&T UC SERVICES

Dashboard Account Provision Documentation

Site Deployment Structure
 Subscriber Provisioning
 Address Book Extension

### IDENTITY

First Name: John

Last Name: Doe

User ID: jdoe@attcenter.com

Password:

Confirm Password:

Site: Union Bank 1 (ub1)

Role:

### PRODUCTS

SKU	Name
ATT-UC-000	AT&T UC Standard
ATT-UC-001	AT&T UC Basic
ATT-UC-002	AT&T UC Standard
<input checked="" type="checkbox"/> ATT-UC-003	AT&T UC Enhanced
DEFAULT-004	Auto Attendant

### ACTIONS

SUSPEND USER

SHOW ADVANCED

USER PORTAL

SAVE USER

REMOVE USER

RETURN TO LIST

### SETTINGS

VoIP Numbers: 8043350995

Mobile Number: (Optional)

Home Number: (Optional)

Fax Number: (Optional)

E-mail: (Optional)

Voicemail E-Mails: Disabled

Voicemail PIN: 0995

Call Grab Number:

### ADVANCED

Time Zone: GMT-05:00 Eastern Standard Time

Location: Other

Call Permissions: PSTN

Call FWD Permissions: PSTN

Public Number: 8043350995

Alias: 0995

Conf Extn Number: 47008763

Mobility Profile: Default

Voicemail Service: Hosted

Device Password State: ☐ Site ☐ User ☒ None



# End User Portal

- Access voicemail and messages
- Edit personal address book and add contact from corporate directory to favorites
- Set up personal call routing rules
- Configure voicemail, voice services, and conferencing settings



# AT&T Complete Implementation Support



# Contact Center Support



# AT&T Cloud Contact Center

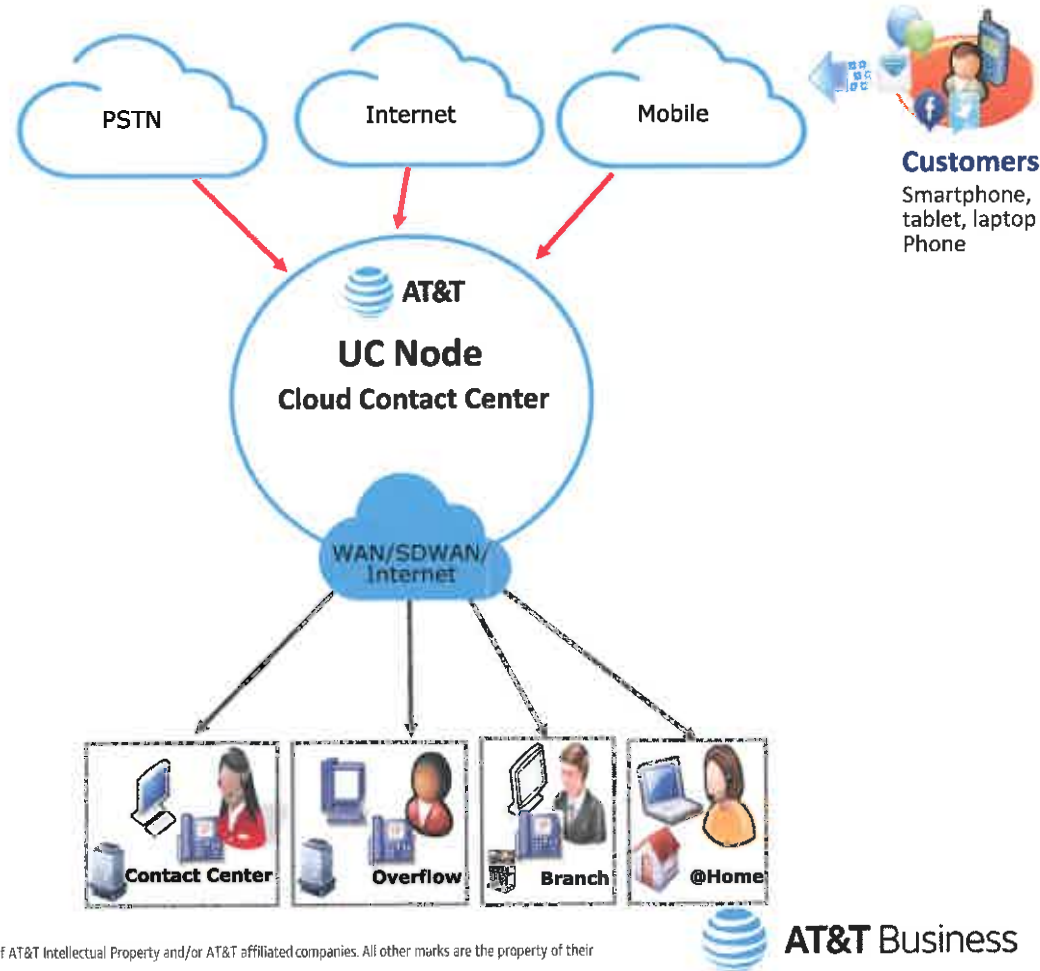
## One Virtualized Center

### Omni-Channel with fully integrated Contact Center feature suite

Agents can be anywhere, added as needed to drive business agility with elastic scale.

- At contact center locations, behind an existing PBX/Key system
- At home using local POTS lines, IP Phone, or IP Soft Client
- At remote offices with unique site-based auto attendant/menu and queue options tied into the formal contact centers
- At outsourcers for seasonal growth or cost savings with a flexible overflow results in one true CC Instance across your Enterprise.
- Overflow calls to any location and user trained as backup agent
- Interactive Voice Response
- Call Recording
- Work Force Optimization, Salesforce, CRM applications
- Artificial Intelligence and IBM Watson Integration

**No matter where the agents are physically, they are part of the solution - any contact can be delivered to any agent, anywhere at any time - with one set of business logic on a single Routing Engine providing full cradle to grave reporting across all interactions.**



# AT&T Cloud Contact Center

## Basic Agent Profile

- Inbound Voice
- Outbound Voice
- Unlimited Sub-Tenants & Roles
- Standard IVR
- Standard Reports
- Skills-Based Routing
- Configuration & Administrative APIs

## Standard Agent Profile

- Inbound Voice
- Outbound Voice
- Unlimited Sub-Tenants & Roles
- Standard IVR
- Standard Reports
- Skills-Based Routing
- Configuration & Administrative
- Custom Reports & Statistics
- Real-Time Reporting API
- Historical Reporting API
- Silent Monitoring & Barge-In
- Queue Call Back
- Basic Scripting

## Enhanced Agent Profile

- Inbound Voice
- Outbound Voice
- Unlimited Sub-Tenants & Roles
- Standard IVR
- Standard Reports
- Skills-Based Routing
- Configuration & Administrative APIs
- Custom Reports & Statistics
- Real-Time Reporting API
- Historical Reporting API
- Silent Monitoring & Barge-In
- Queue Call Back
- Basic Scripting
- Email Channel Functionality
- Chat Channel Functionality
- SMS Channel Functionality
- 3rd-Party Work Items
- Facebook Messenger Chat Integration
- Real-Time Adherence

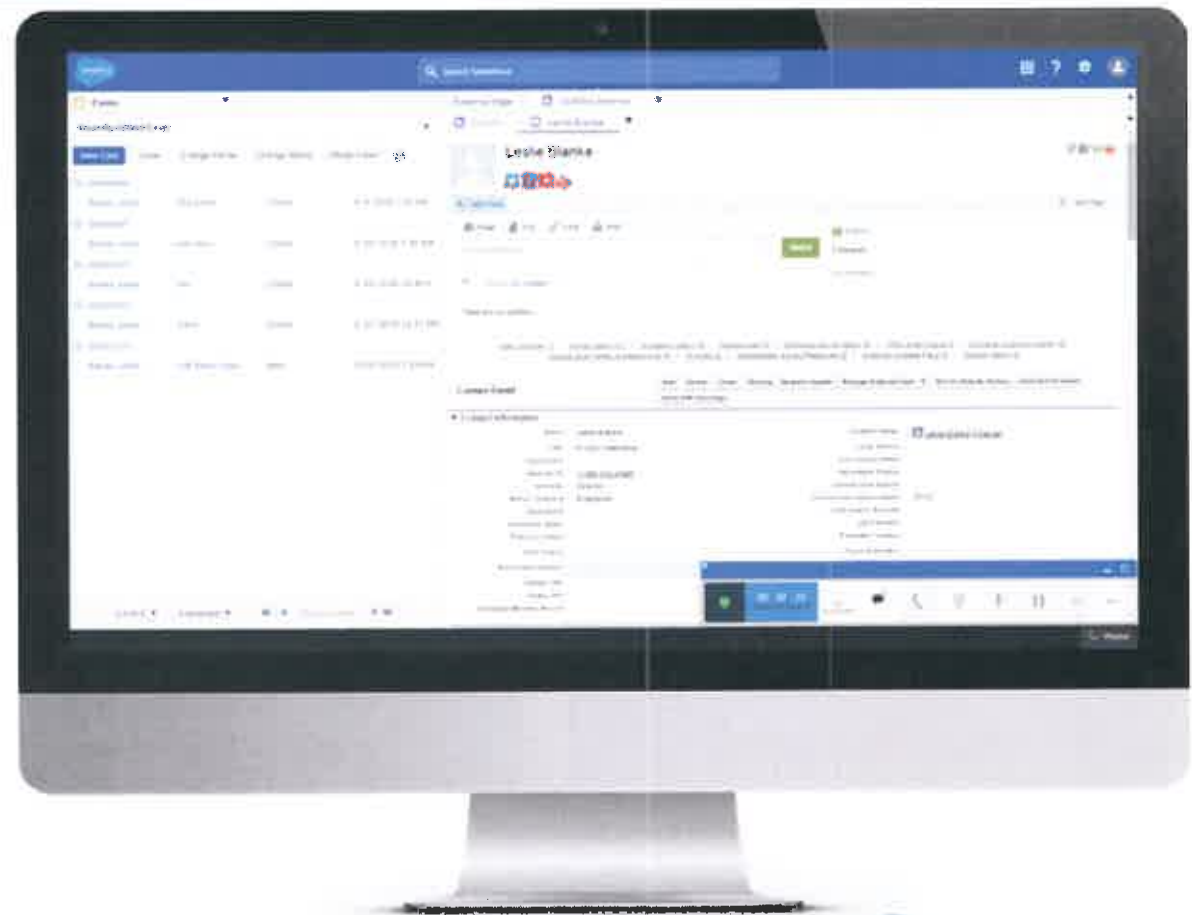




# Agent Desktop with Salesforce Integration

## Seamless Salesforce Contact Center Integration

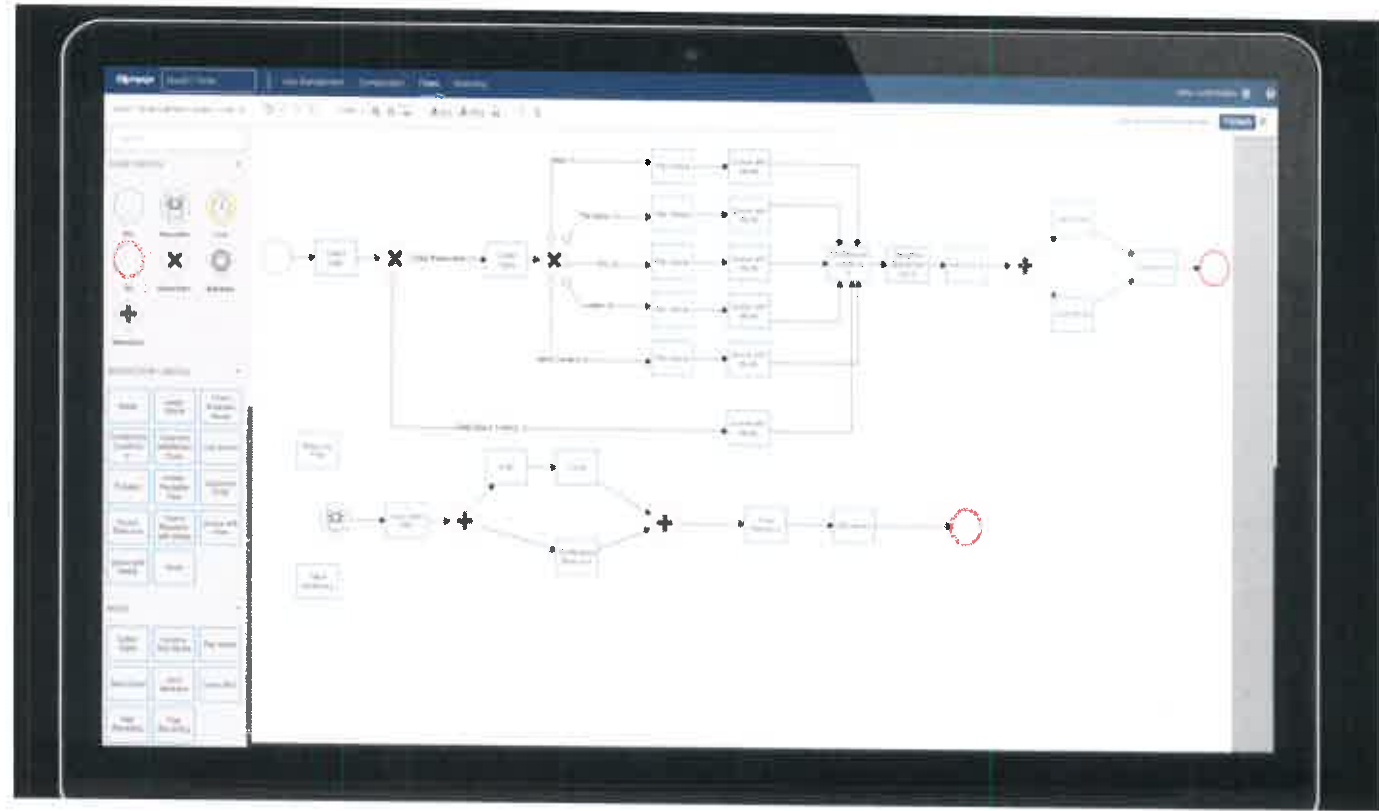
Native telephony app for Salesforce CRM using Open CTI to provide instant deployment of an end-to-end customer interaction solution.



# Administration (Advanced flow Designer)

Advanced Flow Designer  
Reduced IT Footprint  
Leverage an intuitive drag-and-drop interface to create sophisticated interaction Flows without complex programming.

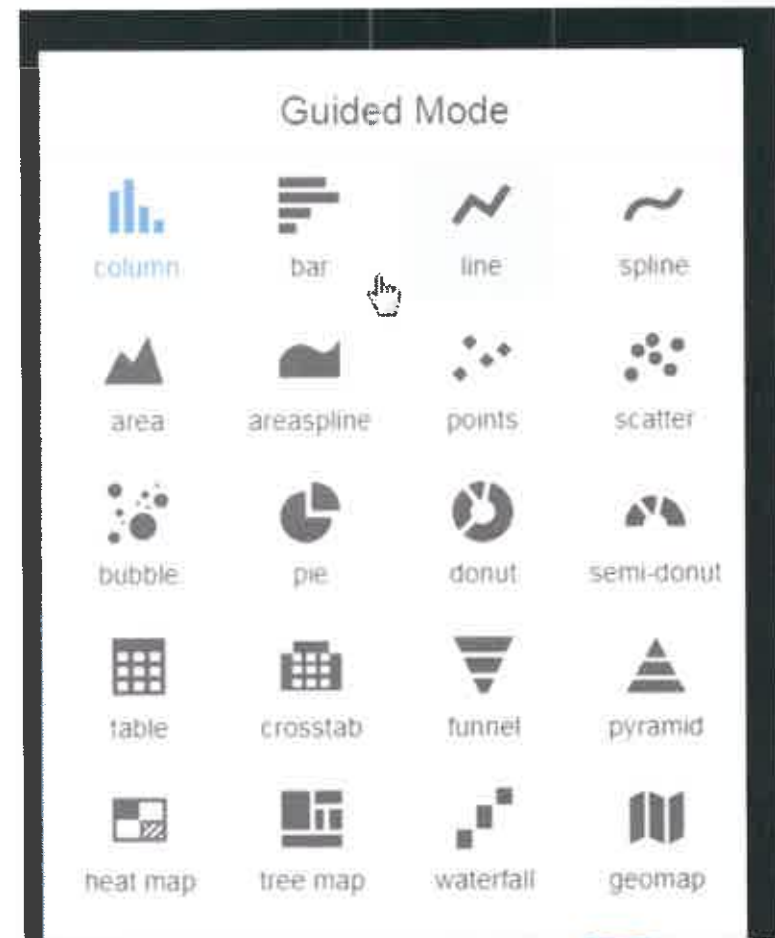
Quickly develop interaction  
Flows using re-usable templates  
provided by CxEngage or create Flow  
templates unique to your business for  
copy & paste-like functionality.



# Custom reports and Dashboard Widgets

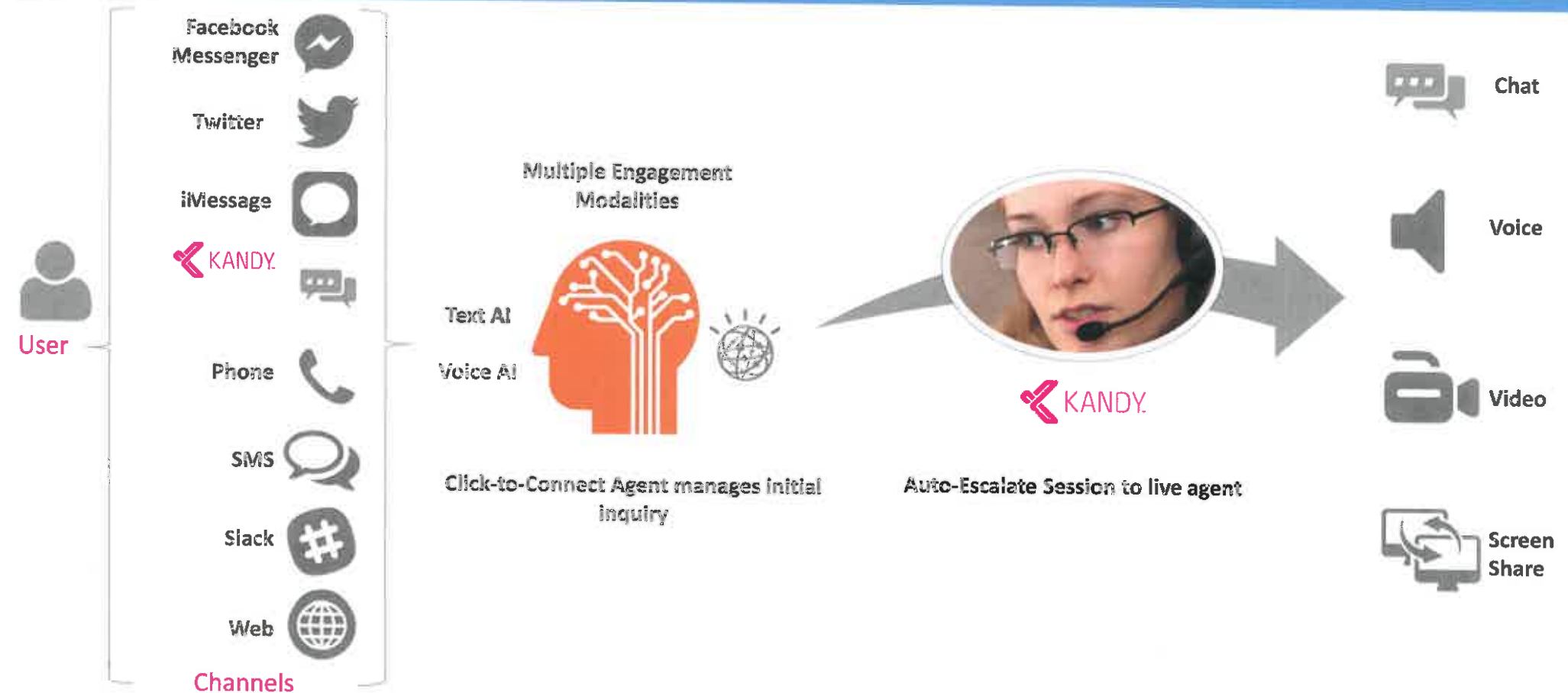
## Custom Reports and Dashboards

Design custom widgets, then drag and drop on the canvas to create your own custom reports and dashboards. Create widgets to visualize your data in bar charts, bubbles, columns, stacked columns, donuts, gauges, lines, tables, or as a plain value.



© 2018 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.

# Live Support with Digital Cognitive Agent (Powered by AI)



# Live Support Features



## Rich Messaging Chat

Users can share images and videos with their support representative to better describe the issues that need resolution



## Screen Sharing

Support experts can remotely assist users in real-time by activating screen sharing directly within the Live Support window



## Works on Web & Mobile

Unlike other competing solutions, Live Support also works when your users access your website via their smartphone



## Live Support & AI-IVR

Optional artificial intelligence chat bots with seamless escalation to a human customers service agent



## Voice Call Promotion

Move a customer from a plain phone call to a full multimedia interaction with the click of a button



## For Any Business Size

Micro businesses, SMBs, Enterprises and Large Contact Centers can benefit from Live Support as an overlay or fully integrated



## WebRTC Enabled

Voice and Video calls directly from the website. Agents use web browser console or tablet app

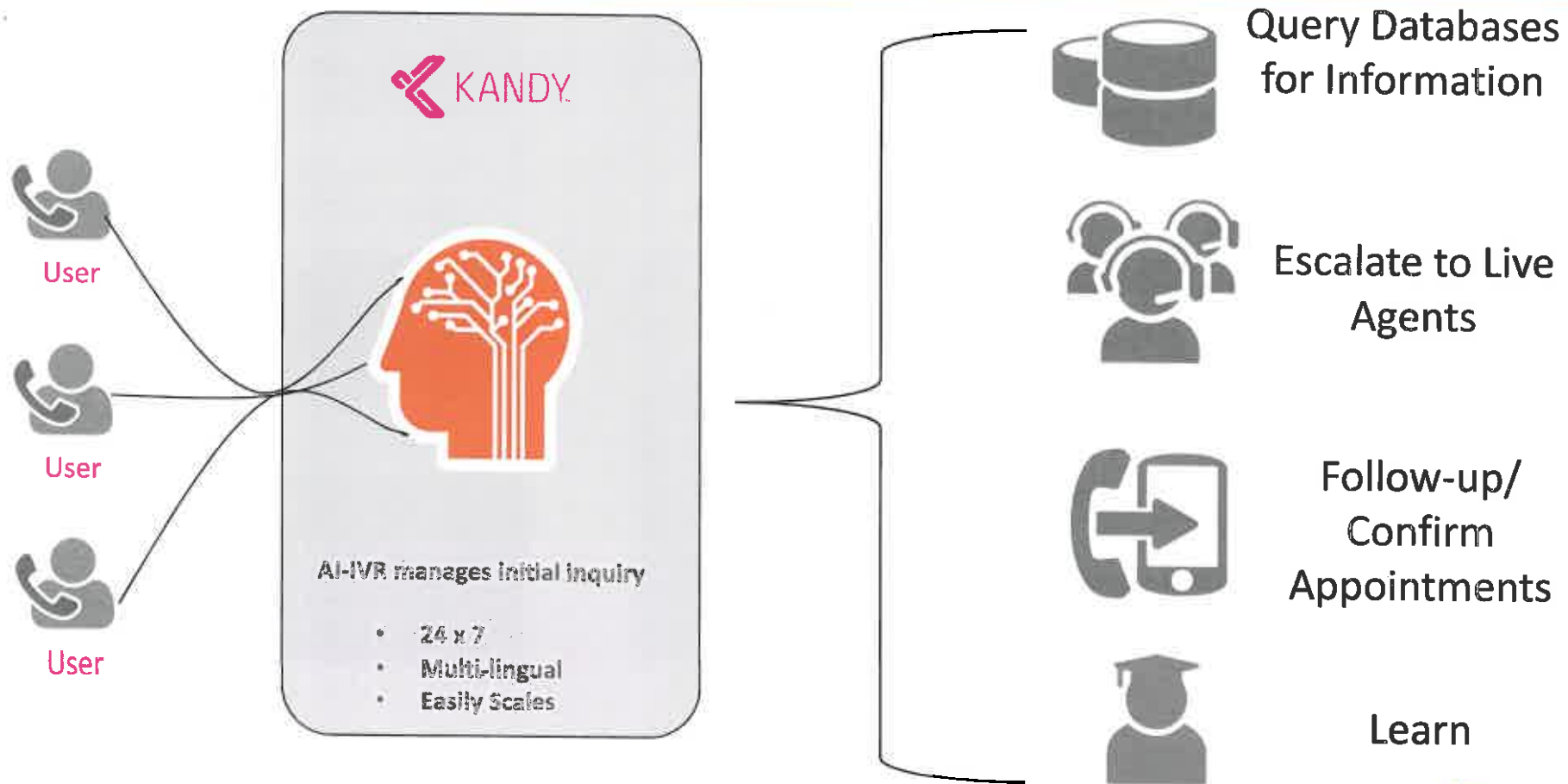


## Easy to Deploy

Use the back end portal to define the menu tree, create the button and generate the HTML embed code for your website



# AT&T Kandy - AI-IVR



# AT&T Video as a Service

## Video Services



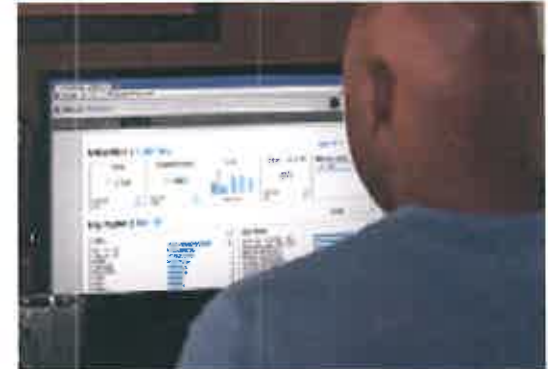
- 7X24X365 Help Desk Support
- Multiple Vendor Video Device Support
- Cloud Video Bridging Service
- Integrate new and existing video end point support
- White Glove Support for large meeting
- Video Federation support

## Asset Management



- Track all end points in a common asset database
- Software upgrade support
- Track end maintenance
- Take over of existing assets

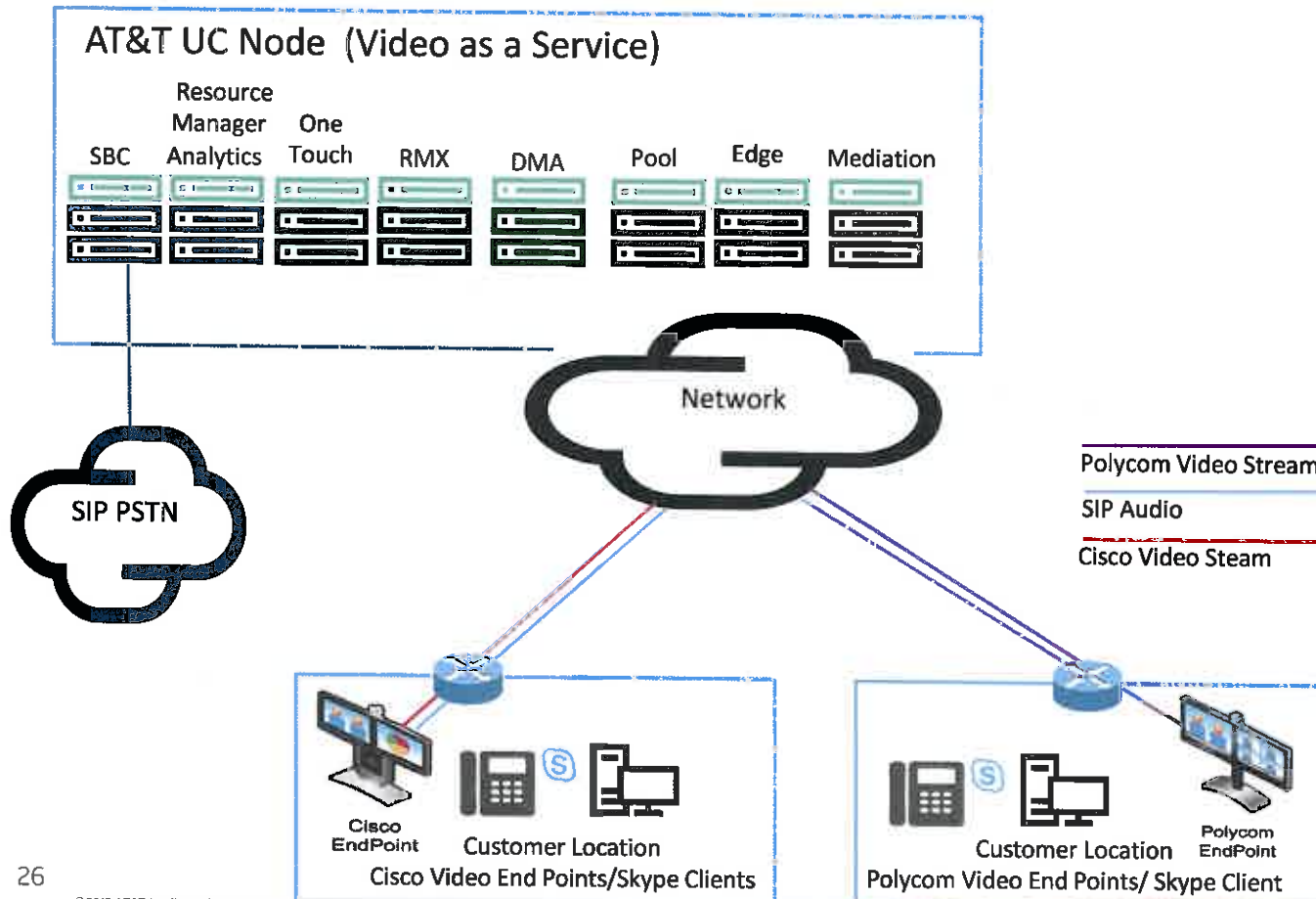
## Analytics



- Conference Bridge Utilization Reports
- Capacity planning
- Call Quality Reports

AT&T and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

## AT&T Video as a Service ( Mixed Video End Point Support)



### Notes

- Support Legacy Polycom, Cisco Video end points register to AT&T Video platform
- New Polycom end points migrate to Skype and Teams directly with AVMCU
- Support for One Touch application Scheduling across Cisco and Polycom end points
- Establish AT&T Global Voice SIP Services for PSTN access

# AT&T Managed Polycom Trio 8800

Ideal for mid-size or large conference rooms

## Broadest Interoperability

- Office 365
- Open SIP
- Bluetooth/NFC or USB speakerphone
- Hybrid registration

 Skype for Business

## Business-class videoconferencing (choice of camera)

- EagleEye 12x optical mPTZ
- USB web cam



## Legendary Voice Quality

- Up to 22kHz HD Voice
- 20ft/6m mic pick up
- NoiseBlock™ technology
- Optional expansion mics

## Future-proof options

- Polycom Trio Visual+ enables:

- Content Sharing
- Business-class videoconferencing

## Modern intuitive interface

- Stylish, award winning design
- 5.5" color touch display
- One-touch- join with Microsoft exchange
- Thoughtfully placed mute indicators
- Configurable UI
- Recognizable icons for easy navigation

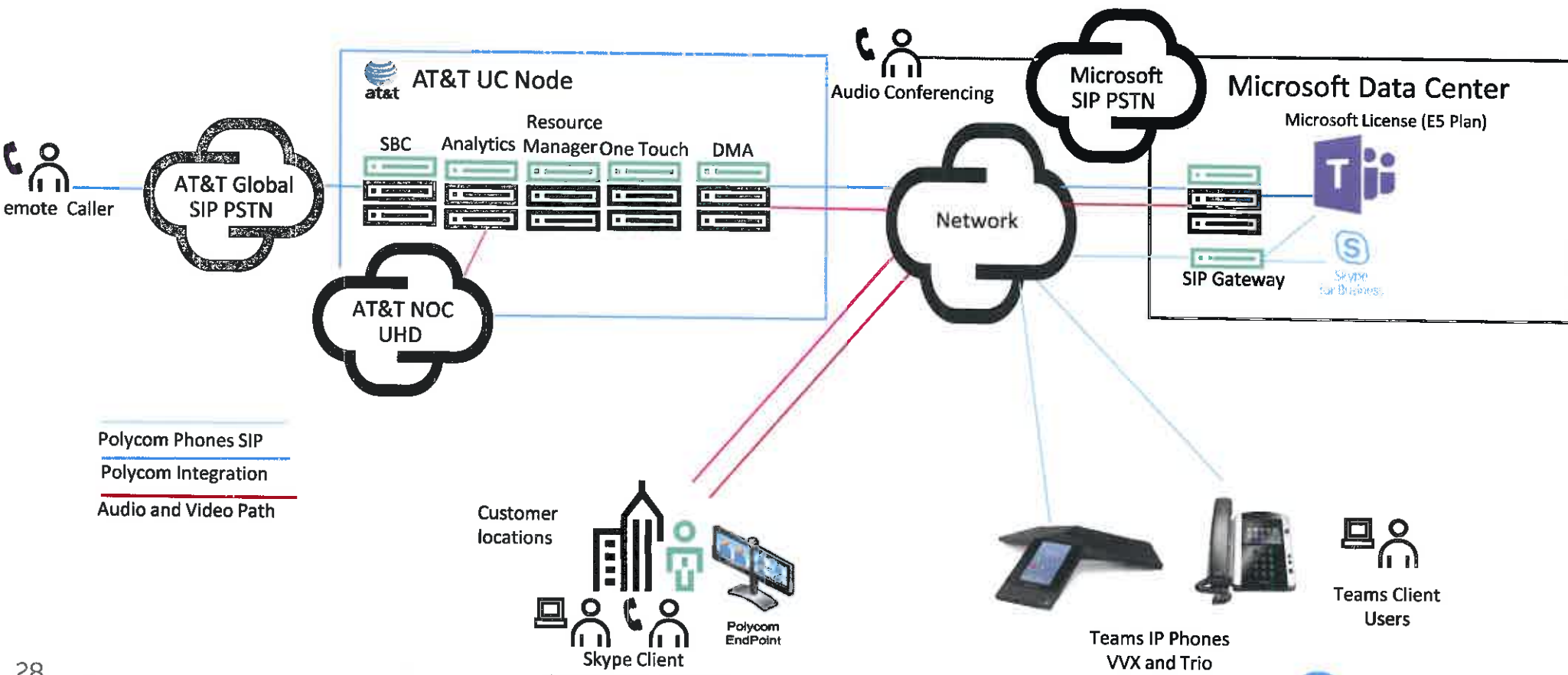
© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World are respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T

marks are the property of their





# Customer Transition to Teams with Video Support





# Integrated SDWAN Services

## HARDWARE / ACCESS

### Appliances

○○○○○  
**Blade Servers  
VM**

○○○○○  
**AudioCodes  
Appliances**

○○○○○  
**Lanner  
Appliances**

### Access



AT&T  
MPLS



AT&T/3<sup>rd</sup>  
Party  
Internet



3<sup>rd</sup> Party  
MPLS



Voice  
Interfaces



LTE

Supports TDM (T1, MLPPP to 3M), Ethernet and LTE access

## APPLICATIONS

### Routing

BGP, OSPF, STATIC

### SD-WAN

Secure Vector  
Routing

### Load Balancing

By Protocol

### Security

IDS/IPS Stateful  
Firewall

### Universal Management

Monitoring Tools

Embedded SDWAN, stateful Firewall, IDS/IPS, DDoS, and voice aware load balancing capabilities

## OFFERS/ COVERAGE

SDN Essential Data  
Only

SDN UC Basic Data  
& voice

SDN UC Standard Data  
& voice with  
High Availability

Package 4  
SDN Data Center  
Appliance or Virtual Machine



**AT&T  
UC Solutions**



**SDN  
Orchestration  
Portal**



**AT&T  
Universal  
Helpdesk**

End to end management and SDN packaged options

© 2018 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.



**AT&T Business**

# Analog Device Support (Gateways) and Integrated SDWAN

AT&T Support multiple options for analog Gateways that range from 2- 24 ports utilizing the Audiocodes MediaPak line MP 112- 124. The analog gateways can also support emergency pass through. AT&T has provided attachments with additional specifics on each gateway that can be utilized to support current and future analog requirements. AT&T can also examine the use of existing gateways that FCA may have in place today for reuse option.

Audiocodes M800 is utilized to support on site survivability, SDWAN, Voice Gateway functions

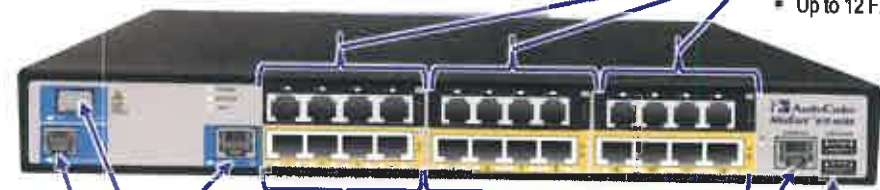
**MP-112- 114 Analog Gateways**



**MP-124 Analog Gateways**



**M800-Multi-function Appliance**



**WAN interfaces**  
Options (up to 3):

- GE Copper
- 100/1000 SFP
- ADSL2+/VDSL 2
- SHDSL
- T1/E1

**LAN interfaces**

- Up to 4 Gigabit Ethernet
- PoE

**LAN interfaces**

- Up to 8 Fast Ethernet
- PoE

RJ-45 port for RS-232 serial communication

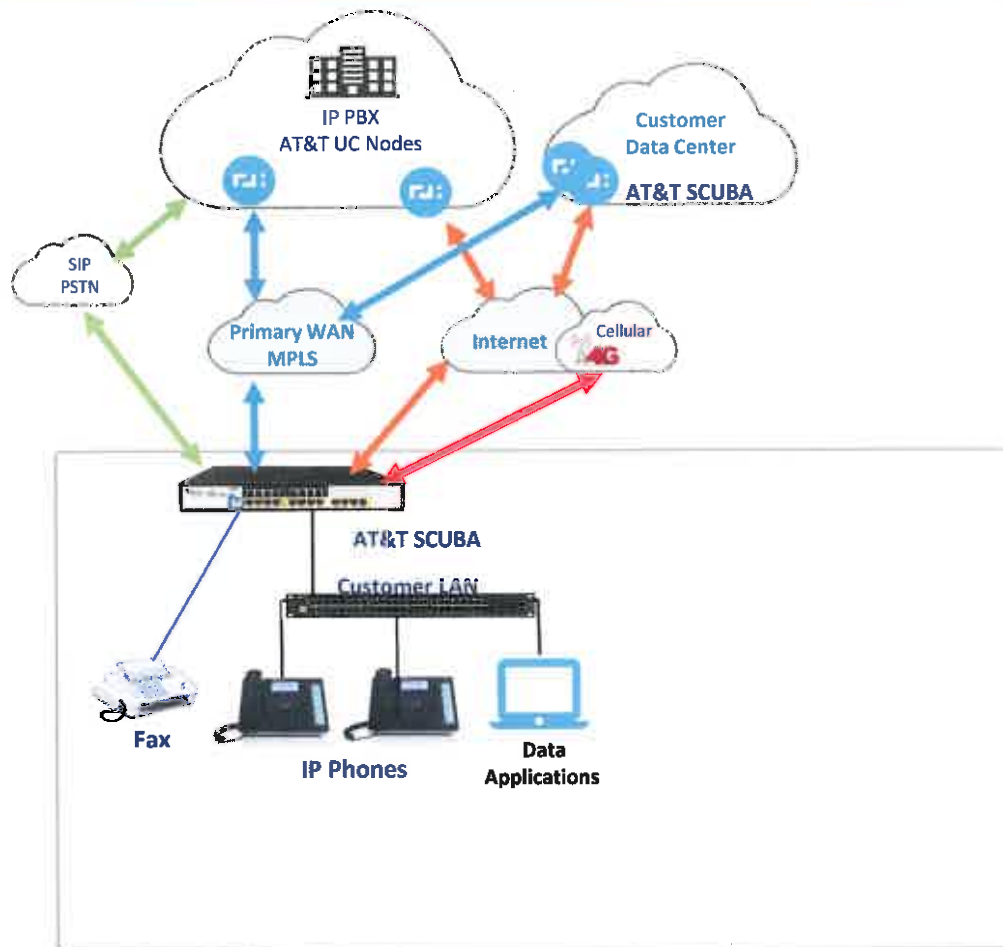
**Telephony interfaces**  
Options (120 voice channels):

- 2 x E1/T1
- Up to 8 BRI
- Up to 12 FXS
- Up to 12 FXO

**2 x USB2.0**

- 3G/4G mobile WAN modem
- External USB hard drive or flash disk (debug)

# Network High availability Option(Single SDWAN Appliance) Self Contained Unified Business Appliance (SCUBA)



## AT&T SDN (SCUBA)

- ✓ Single SCUBA
- ✓ Primary WAN MPLS
- ✓ Survivability based on Internet and LTE Backup support
- ✓ Backup both voice and data
- ✓ Built in SBC option for local PSTN access
- ✓ Enhanced SDWAN services:
  - ✓ WAN link resiliency (dual wan and 3G/4G)
  - ✓ LAN services (DHCP, DNS, LLDP, 802.1x)
    - ✓ Firewall
    - ✓ Port forwarding for GW/IPP management
  - ✓ QoS prioritization, VoIP Monitoring
  - ✓ END-END service management

respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.

Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their



# Security Compliance



March 21, 2017

To Whom It May Concern,

The purpose of this letter is to confirm that 128 Technologies has been a member of the Cryptocomp FIPS 140-2 validated encryption module from SafeLogic, CryptoComp v1.0, a validated module. The Cryptocomp encryption engine for servers, workstations, appliances, and mobile devices. The Cryptocomp engine supports the cryptographic functions and features listed in the Cryptocomp v1.0 specification. Cryptocomp v1.0 offers a secure key generation, distribution, and storage process, and secure encryption and decryption of data.

Cryptocomp Server has received FIPS 140-2 Certificate Number 3028, which can be found here: <https://csrc.nist.gov/groups/ST/toolkit/monitors/monitors/140-2/3028/3028.pdf>

128 Technologies will receive a FIPS 140-2 certificate, to verify the use of the Cryptocomp v1.0 encryption module. The Cryptocomp v1.0 encryption module is a validated encryption module, but we do not expect any issues with the validation process.

Please let us know if you or your customers have any questions.

Sincerely,

Mark Miller

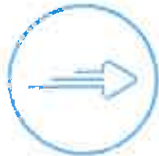
CEO, SafeLogic



- FIPS 140-2, Level 1
  - Leveraging certified encryption module from SafeLogic
  - NIST Validated Modules certificate
- ICSA Corporate Firewall Certification, compliance
- PCI Compliance by
- Nessus/Codenomicon compliance
- Passed penetration testing for use with Department of Defense
- FISMA with sponsorship

# Why AT&T UC Solutions?

## AT&T provides a holistic UC solution



### Network and PSTN Access

AT&T provides a SIP trunks, Emergency Services, MPLS, Broadband, Mobile and SDN-WAN services

+



### Network Simplification

AT&T provides 7X24X365 global proactive monitoring, management and MACD support for core UC services as well as for network access and coordination with third party vendors

+



### Future Proof and Flexible Solution

AT&T stays current and evolves as technology evolves including upgrades and service enhancement as part of the solution Support for multiple vendors equipment allowing for migration as required to support specific end user requirements



### Financial Stability

AT&T has been delivering communications solutions for over 139 years and continues to enhance technology via AT&T labs and partnerships with other leading technology suppliers



### Global Support

AT&T has over 40 data center across the globe providing data services. AT&T provides UC implementation services in over 70 countries. Most of world SIP PSTN access support. Local field services support teams in over 96 countries



### Skilled Staff

AT&T has over 360,000 employees focused on delivery and development of technology. AT&T has over 2500 engineers and focused on the design implementation and support of UC







**AT&T** Business



# Cloud Contact Center Solution

## AT&T

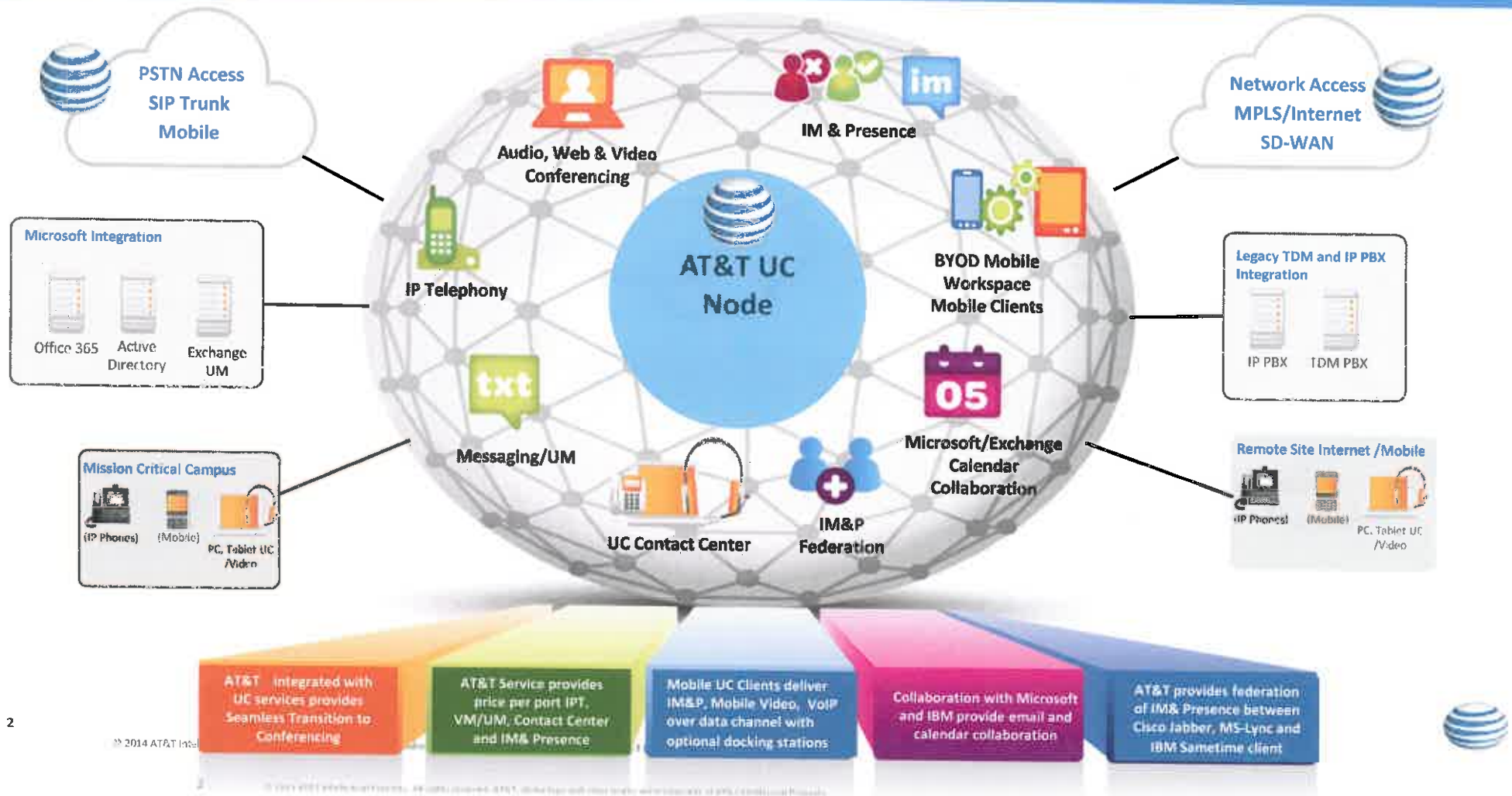
### Unified Communications Solution Session

Mark Beranek  
NI Unified Communications Architect  
CCIE, MCSE, BSEE  
Oct, 2018



© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

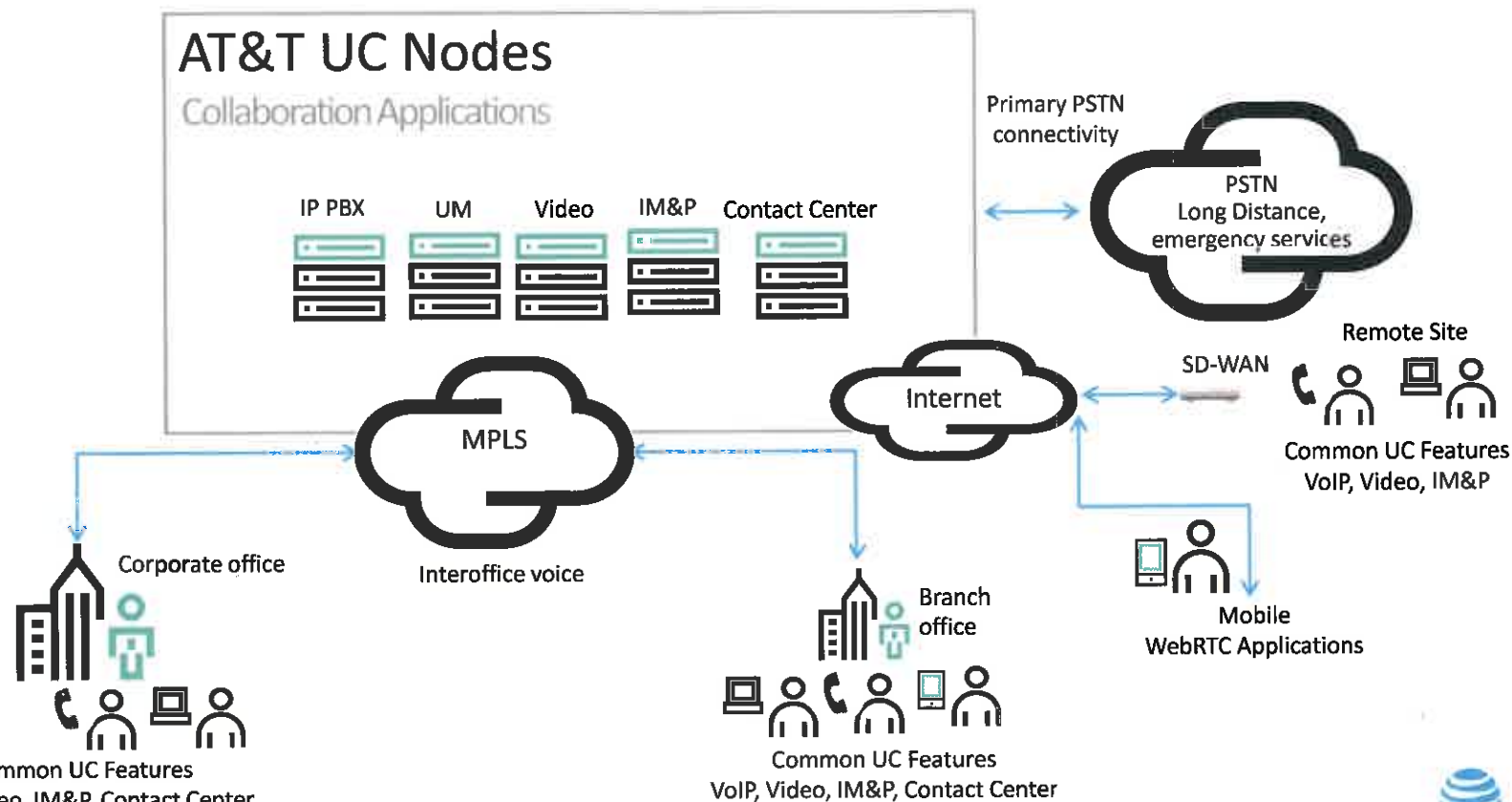
# AT&T Global UC Services Core Nodes



# AT&T UC Service Architecture and Cloud Contact Center

## Key benefits

- Unified Communications as a Service (UCaaS) service
- Operating expense (OPEX) financial model
- Cloud Contact Center
- Centralized SIP trunking option
- Internet Access support
- MPLS Access support
- Global Dial Plan Support
- Upgrades included
- Global 7X24X365 support
- Leverage Existing Phone Systems with Contact Center
- Combine with AT&T UC

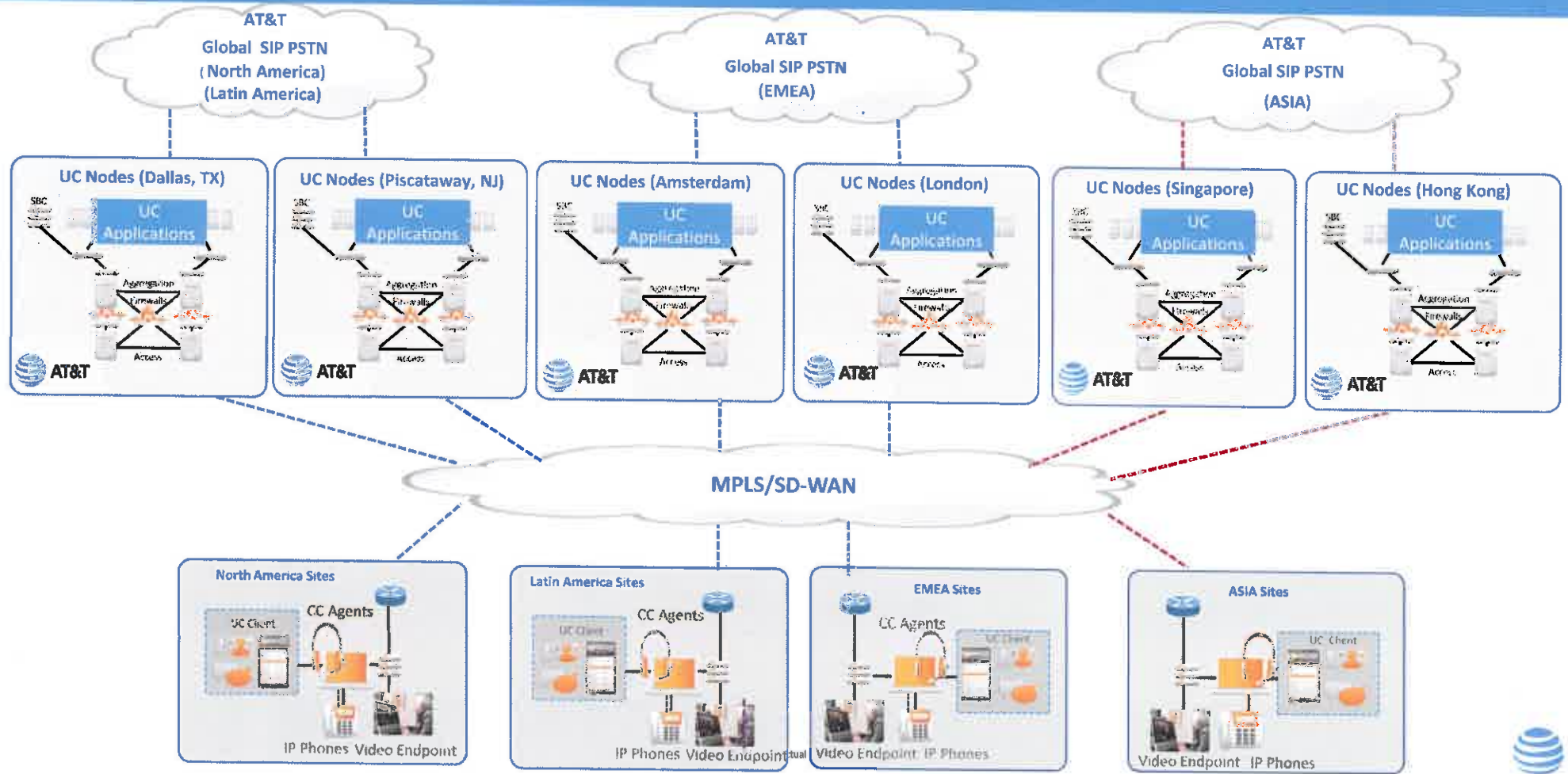


© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

Section 2



# AT&T Global Reach Approach





# Cloud Contact Center Profiles

## Basic Agent Profile

- Inbound Voice
- Outbound Voice
- Unlimited Sub-Tenants & Roles
- Standard IVR
- Standard Reports
- Skills-Based Routing
- Configuration & Administrative APIs

## Standard Agent Profile

- Inbound Voice
- Outbound Voice
- Unlimited Sub-Tenants & Roles
- Standard IVR
- Standard Reports
- Skills-Based Routing
- Configuration & Administrative APIs
- Custom Reports & Statistics
- Real-Time Reporting API
- Historical Reporting API
- Silent Monitoring & Barge-In
- Queue Call Back
- Basic Scripting

## Enhanced Agent Profile

- Inbound Voice
- Outbound Voice
- Unlimited Sub-Tenants & Roles
- Standard IVR
- Standard Reports
- Skills-Based Routing
- Configuration & Administrative APIs
- Custom Reports & Statistics
- Real-Time Reporting API
- Historical Reporting API
- Silent Monitoring & Barge-In
- Queue Call Back
- Basic Scripting
- Email Channel Functionality
- Chat Channel Functionality
- SMS Channel Functionality
- 3rd-Party Work Items
- Facebook Messenger Chat Integration
- Real-Time Adherence



# AT&T UC Profile Options

Monthly UC Port Charge Includes ( End User License, MACD Support, Core Hardware, Software upgrades, Monitoring and management support)

## UC Services

### UC Enhanced Profile



### UC Standard Profile



### UC Basic Profile



### UC Essential Profile



## Capabilities

### UC Enhanced High level Feature Overview

- Presence/IM Client for mobile, PC and Tablet
- IP Phone Support
- Client for PC , MAC, iPad
- Single Number Reach
- Fixed Mobile Convergence (Call Grabber)
- Voicemail
- Provides audio, web , multi-party video conferencing + content sharing
- Fax to desktop support

### UC Standard High Level Feature Overview

- Presence/IM Client for mobile, PC and Tablet
- IP Phone Support
- Single Number Reach
- Fixed Mobile Convergence
- Voice Mail
- Video Point to Point Call

### UC Basic High Level Feature Overview

- IP Phone Support
- Single Number Reach
- Fixed Mobile Convergence
- Voice Mail

### UC Essential High Level Feature Overview

- IP Phone and analog device support
- Common area phone features basic internal calling



# AT&T Cloud Contact Center

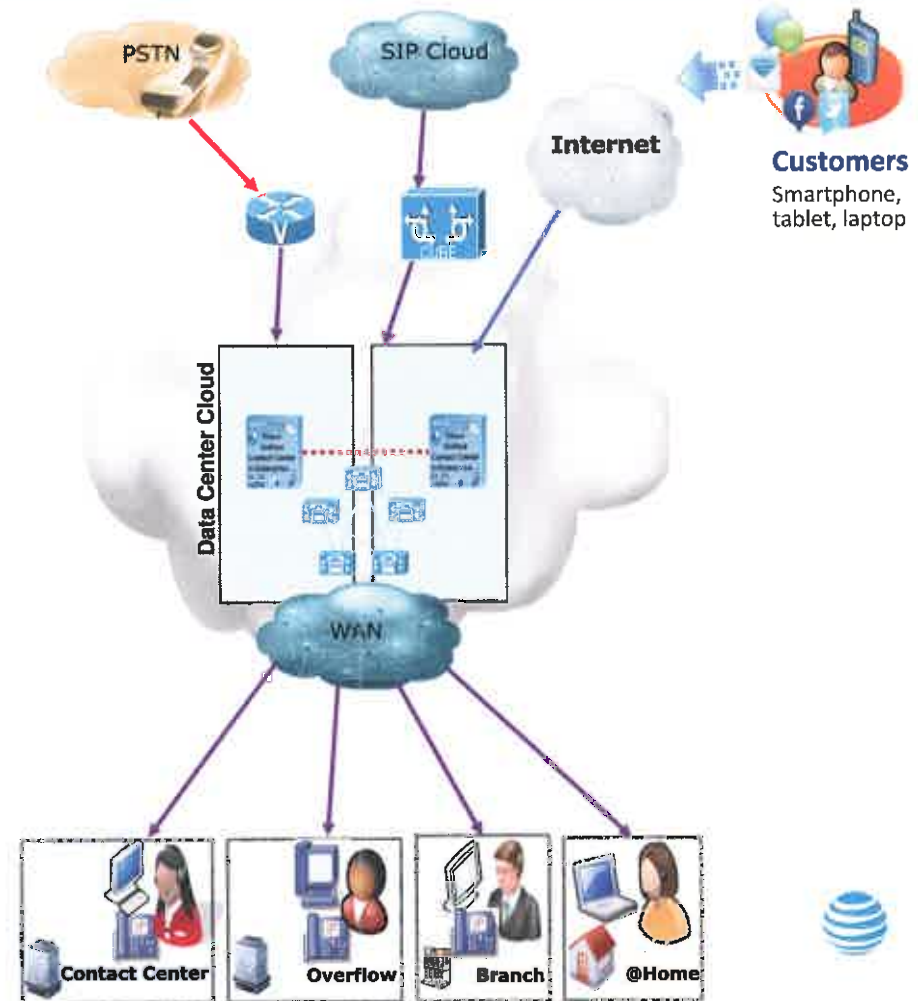
## One Virtualized Center

### Omni-Channel with fully integrated Contact Center feature suite

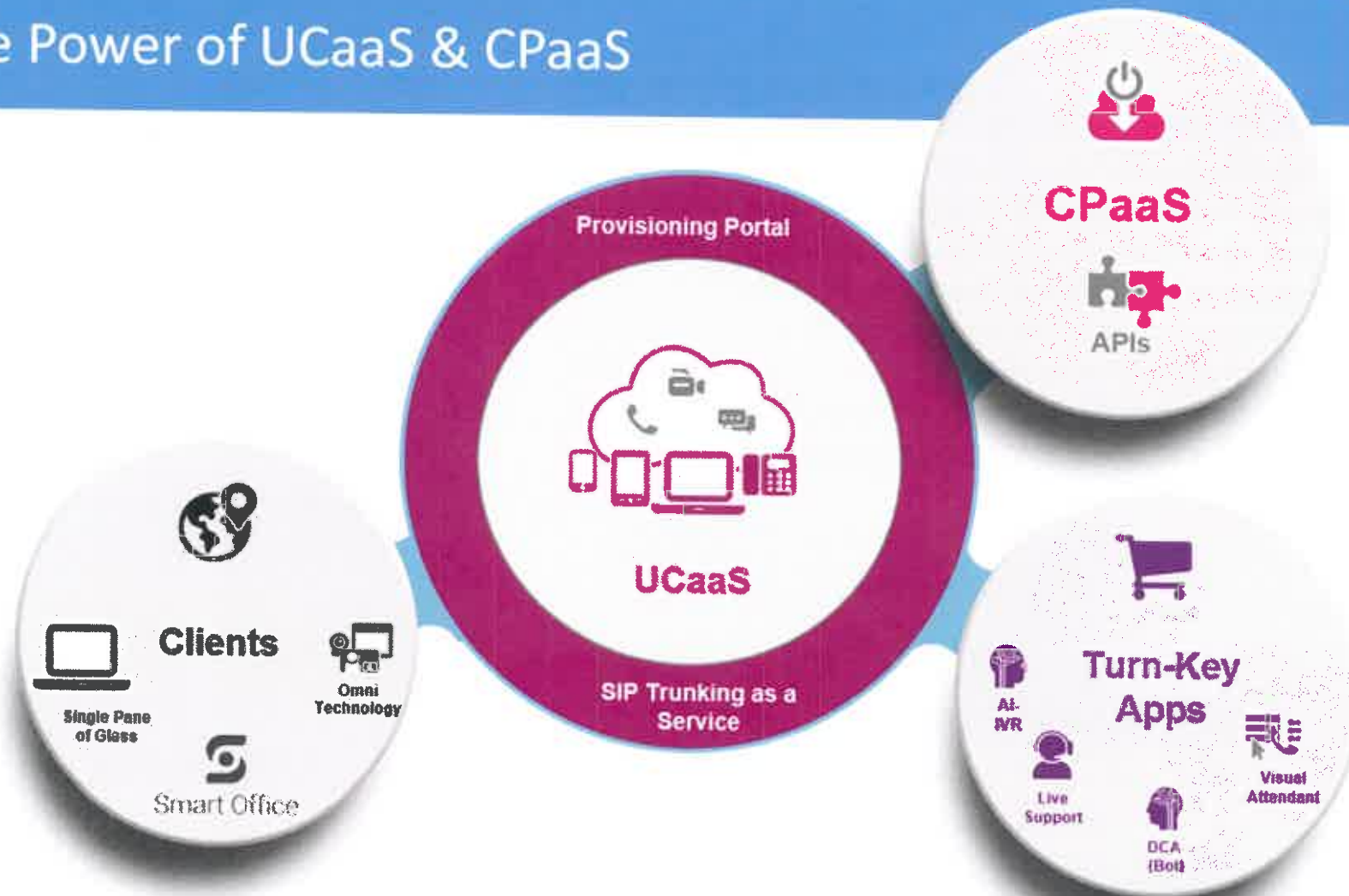
Agents can be anywhere, added as needed to drive business agility with elastic scale.

- At contact center locations, behind an existing PBX/Key system
- At home using local POTS lines, IP Phone, or IP Soft Client
- At remote offices with unique site-based auto attendant/menu and queue options tied into the formal contact centers
- At outsourcers for seasonal growth or cost savings with a flexible overflow results in one true CC Instance across your Enterprise.
- Overflow calls to any location and user trained as backup agent
- Interactive Voice Response
- Call Recording
- Work Force Optimization, Salesforce, CRM applications

**No matter where the agents are physically, they are part of the solution - any contact can be delivered to any agent, anywhere at any time - with one set of business logic on a single Routing Engine providing full cradle to grave reporting across all interactions.**



# The Power of UCaaS & CPaaS



© 2016 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.





# Cloud Contact Center Profiles (Bolt On)

## Bolt On Features

- Call Recording
- Screen Capture
- Salesforce Integration
- Microsoft Dynamics CRM
- WebRTC Client
- Custom API Integration Support



**Improve agent effectiveness and maximize every customer contact with 100% call recording, as well as the first truly cloud-enabled screen recording application in the market. Unlike traditional on-premise solutions, cloud-based LiveOps Recording can capture as many concurrent agent screen interactions as needed without any hardware or software limitations. And, all recordings are encrypted securely in LiveOps data centers and can be retrieved for playback from a web browser for up to 1 year.**





## • WebRTC Agent Desktop

- Customer Journey Mapping Performance Monitoring
- Simplified Agent Experience Full visibility into customer profiles and historical interactions including notes, call recordings, and chat / email transcripts that synchronize with each interaction. so agents can focus on the customer rather than the tool.
- Customizable agent metrics and presence states integrated directly into the global footer for real-time feedback and self-management of daily goals.
- Reference Library Link to a knowledge base, product catalog, or external website to draw from a limitless store of information while reducing the number of windows an agent must manage.
- Real-time scripting and messaging templates for voice, chat, SMS, & email.
- Less is More Fewer applications to switch between means greater agent productivity and the ability to support a higher volume of interactions.
- Data Exchange Sync contact information and interaction history with your CRM in real-time.



## WebRTC UC Clients

### Smart Office Collaboration Rooms

### Smart Office Desktop

### Smart Office Mobile

#### Voice and Video

Click to call

Call logs

#### Conferencing and Collaboration

Reservation-less Meet Me Conferencing

Multi-party video conferencing with screen share

#### IM and Presence

Integrated with Global Directory

Presence includes "on the phone"

Integration with Skype for IM and Presence via API

#### Directory integration

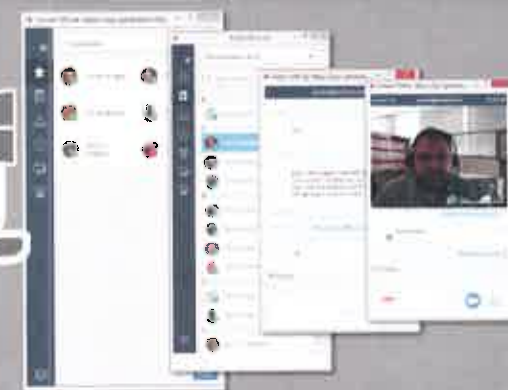
View corporate or system directories Microsoft AD and LDAP

#### Value

Extends UC functionality wherever you may roam

Replace or complement desktop phone and mobile phone

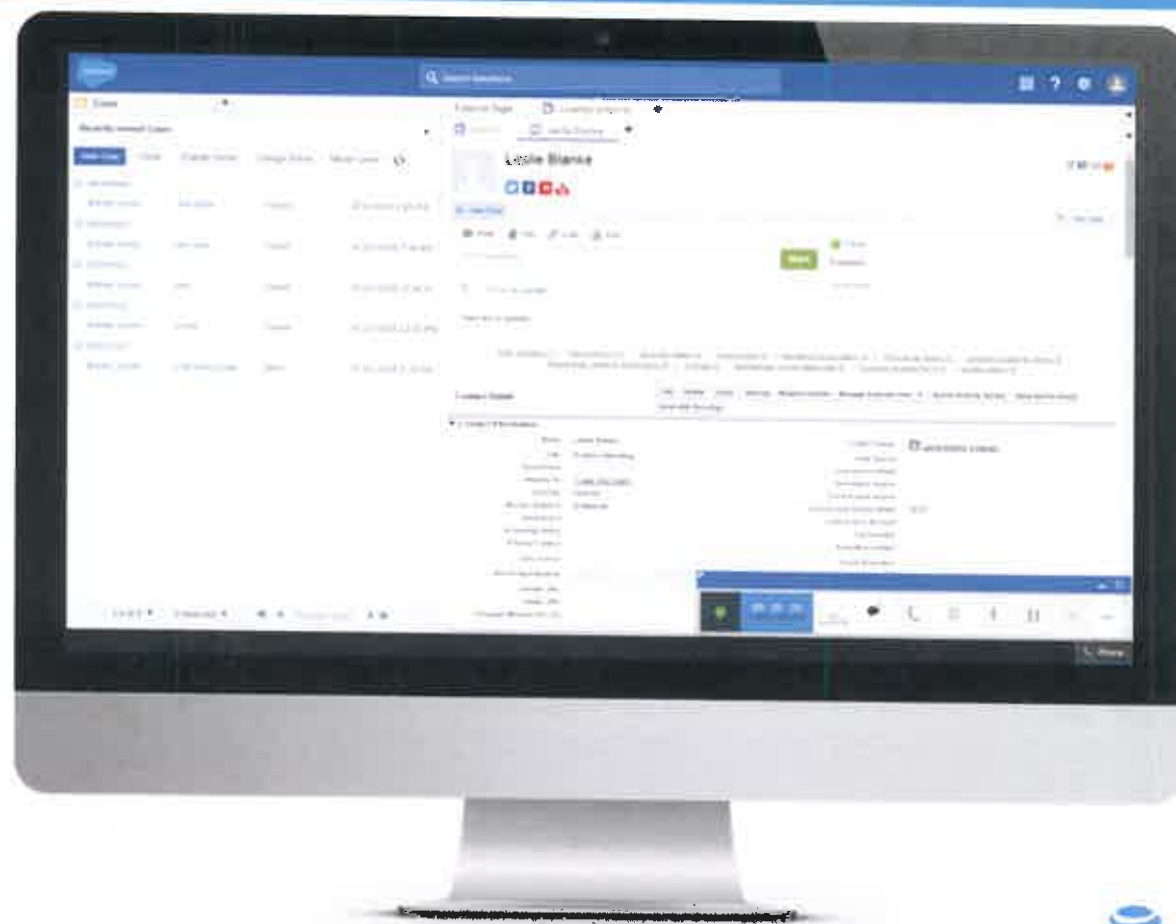
Consistent experience on Windows, Mac and Mobile



# Agent Desktop with Salesforce Integration

## Seamless Salesforce Contact Center Integration

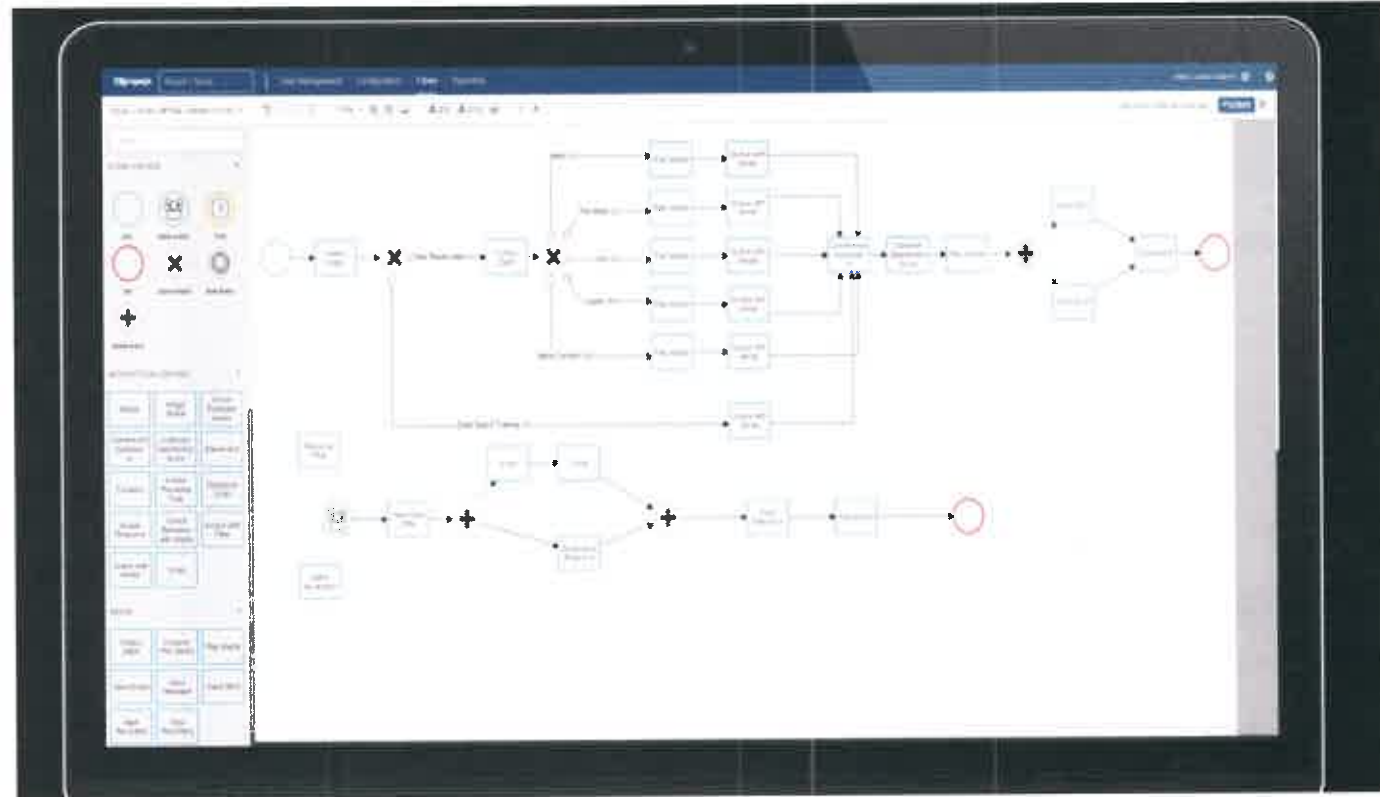
Native telephony app for Salesforce CRM using Open CTI to provide instant deployment of an end-to-end customer interaction solution.



# Administration (Advanced flow Designer)

Advanced Flow Designer  
Reduced IT Footprint  
Leverage an intuitive drag-and-drop interface to create sophisticated interaction Flows without complex programming.

Quickly develop interaction Flows using re-usable templates provided by CxEngage or create Flow templates unique to your business for copy & paste-like functionality.



# Social Omni-Channel

## Social Media Customer Care

- Social media campaign management
- Real-time capture of social media postings



- Enable proactive customer service by queuing and assigning social web posts and callback requests to appropriate staff
- Complement brand monitoring dashboards





# Reporting

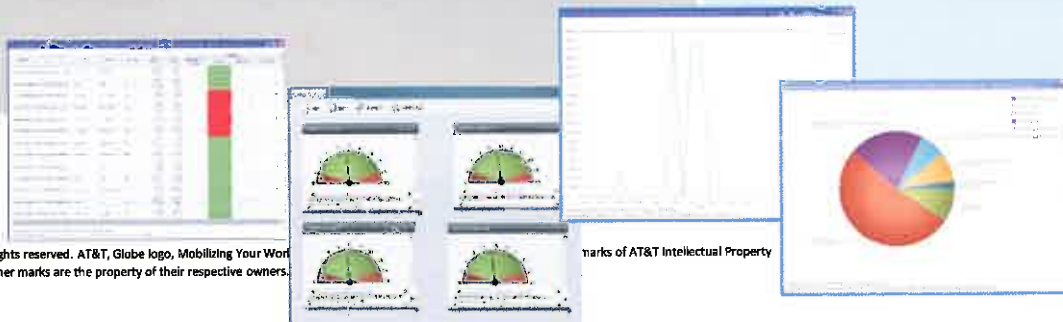
## Customizable Reporting

### Features

- Live Data reports (grid) with improved UI
- Real-time and historical dashboards include charts, grids, web content, notes to team
- Wizard-based interface to extend reporting to data sources inside and outside contact center
- Highly customizable look and feel
- User groups and access control to data, reports, and capabilities
- Thresholds and drill-downs
- Time zone preference

### Benefits

- Automate manual consolidation of data in a single dashboard
- Reduce customization costs via end-user access to some customization
- Increase speed to find preconfigured drill-down information



# Dashboard

## Single Data Pipeline

A single data pipeline for both real-time and historical reporting across all tenants means you have a sole source of truth, making it easy to understand your business performance.

## Real-Time Dashboards

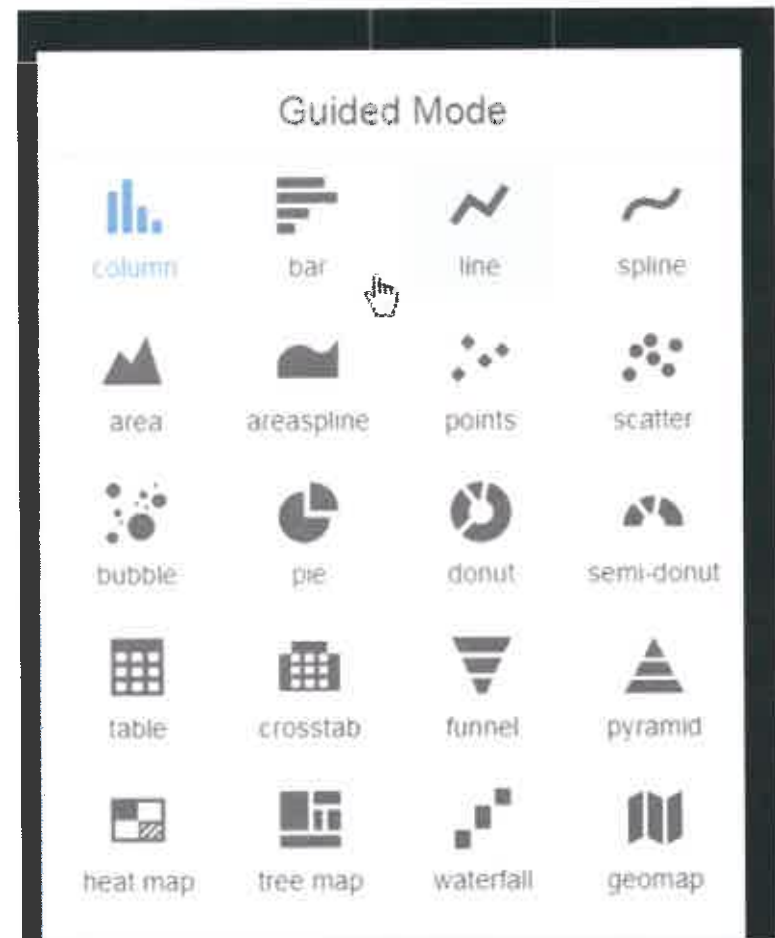
Make every decision based on current & actionable data with real-time statistics, KPIs, and business analytics.



# Custom reports and Dashboard Widgets

## Custom Reports and Dashboards

Design custom widgets, then drag and drop on the canvas to create your own custom reports and dashboards. Create widgets to visualize your data in bar charts, bubbles, columns, stacked columns, donuts, gauges, lines, tables, or as a plain value.

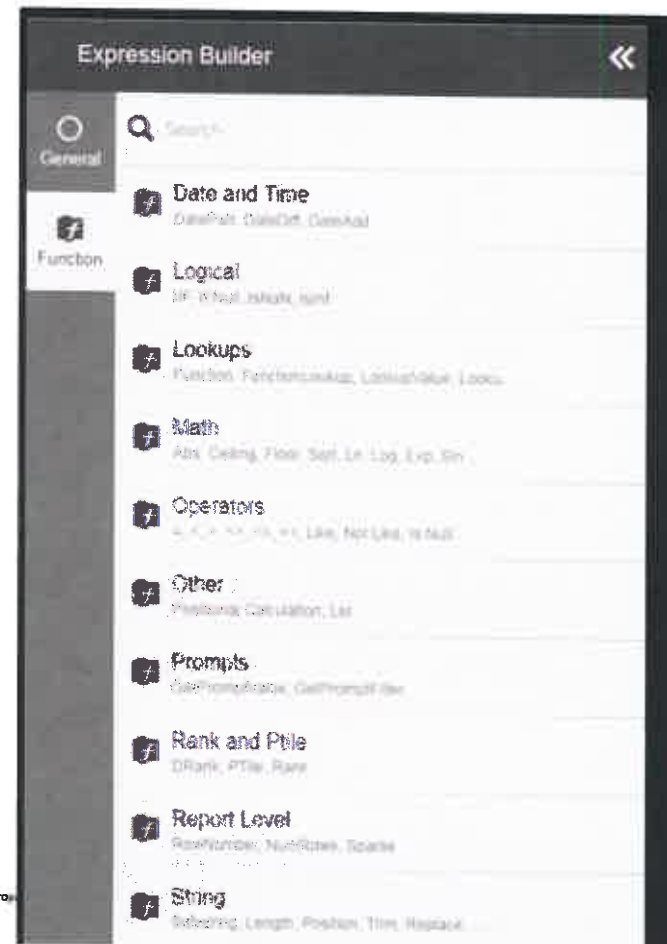


# Customize Statistics Builder

Need to modify or create unique statistics? With custom statistics, you can define statistics to measure what is important to you to use in both real-time and historical reporting.

You may create three types of custom statistics:  
Duration Calculates the time between two events.  
For example, the amount of time between when a conversation starts and when a conversation ends.  
Instance Tracks an event that occurs.

For example, a conversation starting.  
Score Calculates a percentage based on the value collected and the maximum possible value.  
For example, customer satisfaction score.



# Standard Reports (Over 50 Reports)

Field	Data Type	Unit	Description
Abandon	Char (1)	Fixed Values	Y = The caller was placed into queue but hung up before an agent was linked. N = The caller was either never queued or the caller was queued and was later handled by an agent.
Abandon_Cnt	Integer	Count	Number of contacts that abandoned (only calls that are placed in queue but are not handled by agents qualify as abandoned contacts). This field is calculated by counting all contact id in the database having an Abandoned contact state (Abandoned = 1).
Abandon_Time	Integer	Milliseconds	The duration of time the caller waited in queue before hanging up.
AbandonRate	Integer	Percentage	Percentage of queued contacts that terminated before being delivered to an agent. This field is calculated by dividing the total abandoned calls by the total queued calls times 100.
ACD_Outbound_Avail_Percent	Integer	Percent	A percentage of how much of the agent's time was spent in ACD, outbound, and available states. This is defined by ACD Duration + Outbound Duration + Available Duration divided by the Total Duration.
ACD_Time	Integer	Seconds	The total duration of time the agent spent in an ACD state (inbound). The calculation of the ACD Duration field consists on adding all the durations starting with the contact state Contact_State = 4 and Inbound = T and Outbound = F until the next Contact_State = 18.

AddDate	Date/Time	Timestamp	The date and time the station profile was created.
Agent_Cnt	Integer	Count	Count of instances that contacts were directed to an agent.
Agent_No	Integer	Identifier	Identifier for the last agent to handle this contact.
Agent_State_Code	Integer	Identifier	Identifier for the state in which the agent allocated time (available, ACD, break, etc.).
Field	Data Type	Unit	Description
Agent_Time	Integer	Milliseconds	The period of time between an agent joining a call until the agent leaves the call. (Usually an agent leaves a call simply by hanging up, but an agent can also transfer a caller or unlink which leaves the caller to continue to interact with an IVR). Can also be the duration of time agents spent in ACD for a particular skill. The calculation of the ACD Duration field consists on adding all the durations starting with the contact state Contact_State = 4 and Inbound = T and Outbound = F until the next Contact_State = 18.
Available_Time	Integer	Seconds	The total duration of time the agent spent in an available state. The calculation of the available duration field consists on adding all the durations starting with an available state until the next state.
Ave_ACD	Integer	Seconds	The average length of the agent's inbound calls. The calculation of the Average ACD Duration consists on the Total ACD Time divided by ACD Contacts.
Ave_Outbound	Integer	Seconds	The average length of the agent's outbound calls. The calculation of the Average Outbound Duration consists on the Total Outbound Time divided by Outbound Contacts.
AvgMinutes	Integer	Minutes	Average total duration of contacts delivered to this skill. This field is calculated by dividing the total time of active contacts since they enter the IVR with Prequeue contact state (Prequeue = 1) until they exit the system with an EndContact contact state (EndContact = 18), by the total number of contacts.
Callback_Time	Integer	Seconds	Duration of time the contact spent in a callback state.
Caller_ID	Varchar (128)	Label	The phone number that will be displayed on caller ID's on outbound calls.
Campaign_Name	Varchar (50)	Label	Name of the campaign.

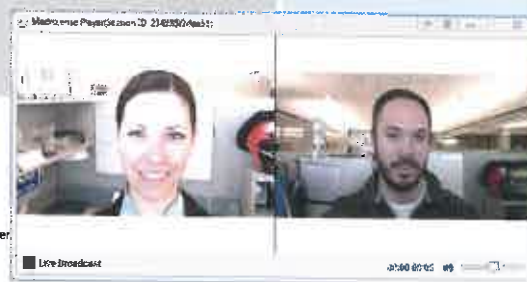




# Call Recording

## Omnichannel Recording and Streaming

Features	Benefits
<ul style="list-style-type: none"><li>• Network-based recording and streaming</li><li>• Audio and video recording</li><li>• On-demand and full-time recording</li><li>• Branch or multisite topologies</li><li>• Built-in Search and Play</li><li>• APIs for partner applications</li><li>• Integrated with customer care, unified communications solutions</li></ul>	<ul style="list-style-type: none"><li>• Uses existing network infrastructure</li><li>• One platform for all channels</li><li>• Supports regulatory compliance</li><li>• Support for live monitoring, videos on demand, video on hold, video IVR</li><li>• Enables optional third-party apps (advanced quality management [AQM], WFO, WFM, analytics)</li></ul>



# AT&T Universal Service Desk (USD)

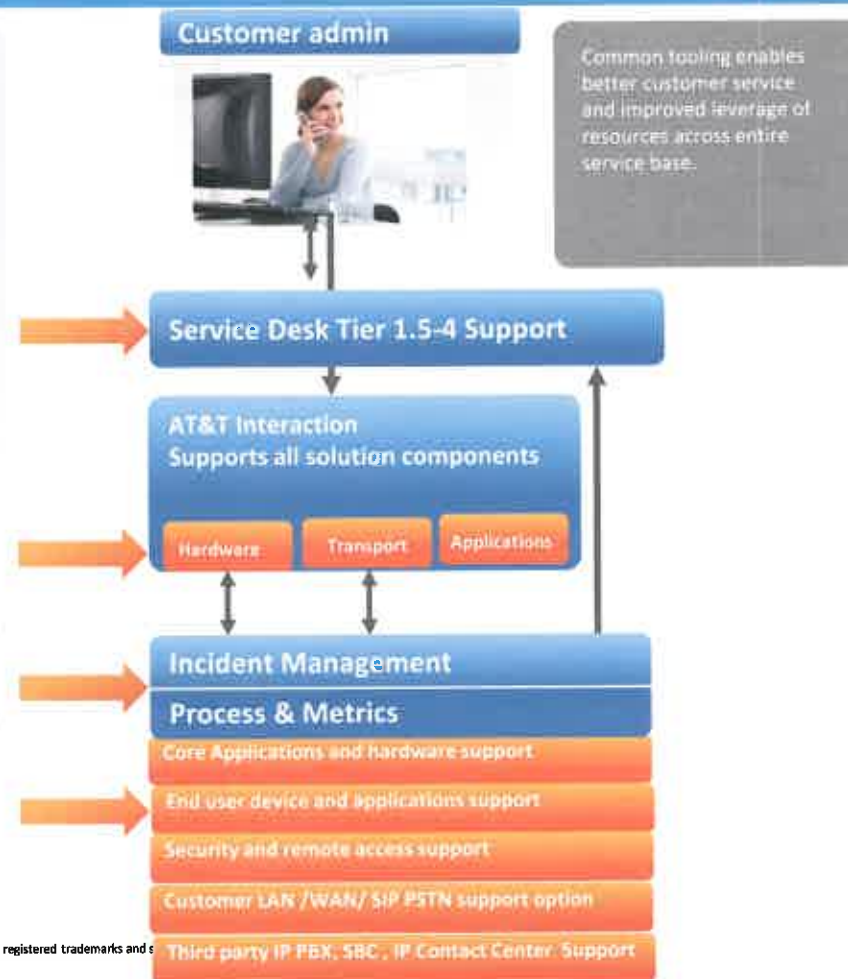
## AT&T UC Services Support

- Primary interface for all UC support questions
- Universal agents have robust tools to see entire customer environment and status
- Access UC support via phone, web, or chat
- Coordination with AT&T and Third party Field Services
- Standardized reports and SLA/SLO
- Quarterly network health assessment
- Customer Portal Access to view reports
- 7X24X365 Support
- MACD included with price per user port
- E-Bonding Support
- Multi language Support

## Specialized expertise aligned by Customer and Application

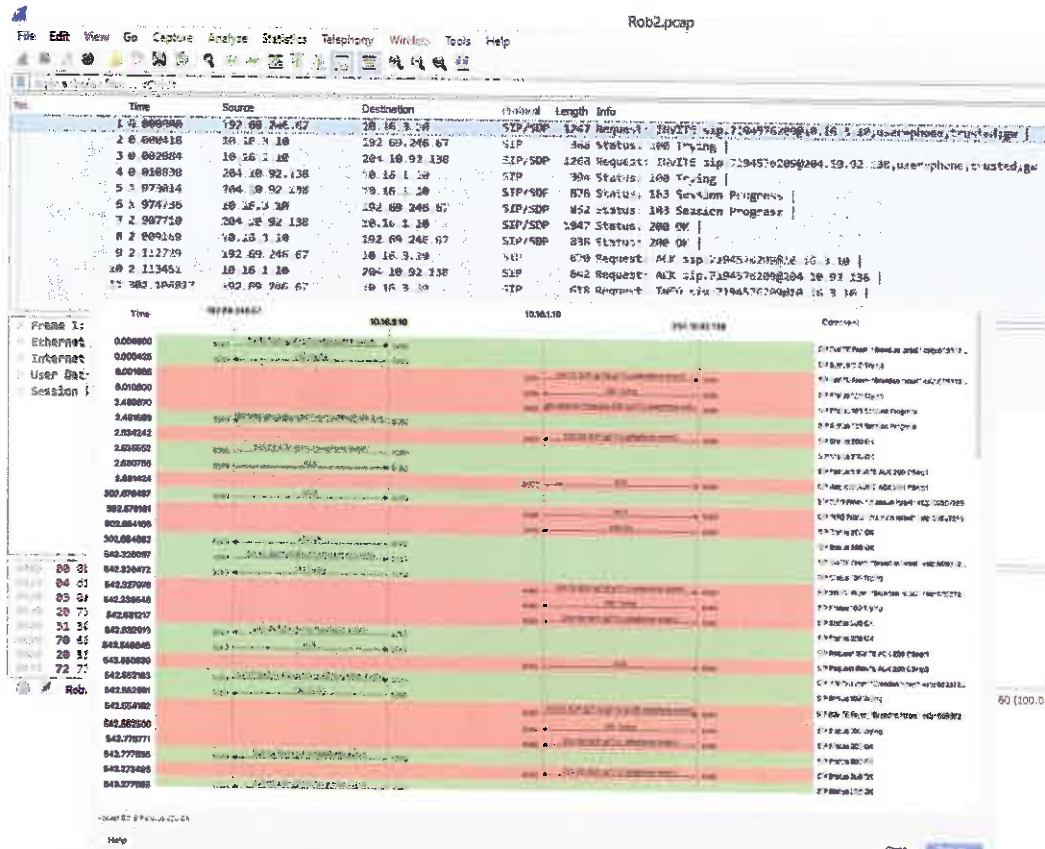
## Centralized and integrated process management

**NOC manages all aspects of the network Including: Network Transport, LAN, Security, Field Services, Core UC Applications and Security**



AT&T UC Services AVATAR 3.0

- ✓ Call Stitching: End to end correlation of SIP signaling, media and event alerts.



## AT&T UC Services AVATAR 3.0 QoE Dashboard

## Voice Quality Metrics / QoE Dashboard - Weekly/Monthly Dashboards



- Provides complete overview of performance of contract service components





# AVATAR Reports

## PSTN Calls – Session Analysis



- Provides complete overview of performance for user to user calls





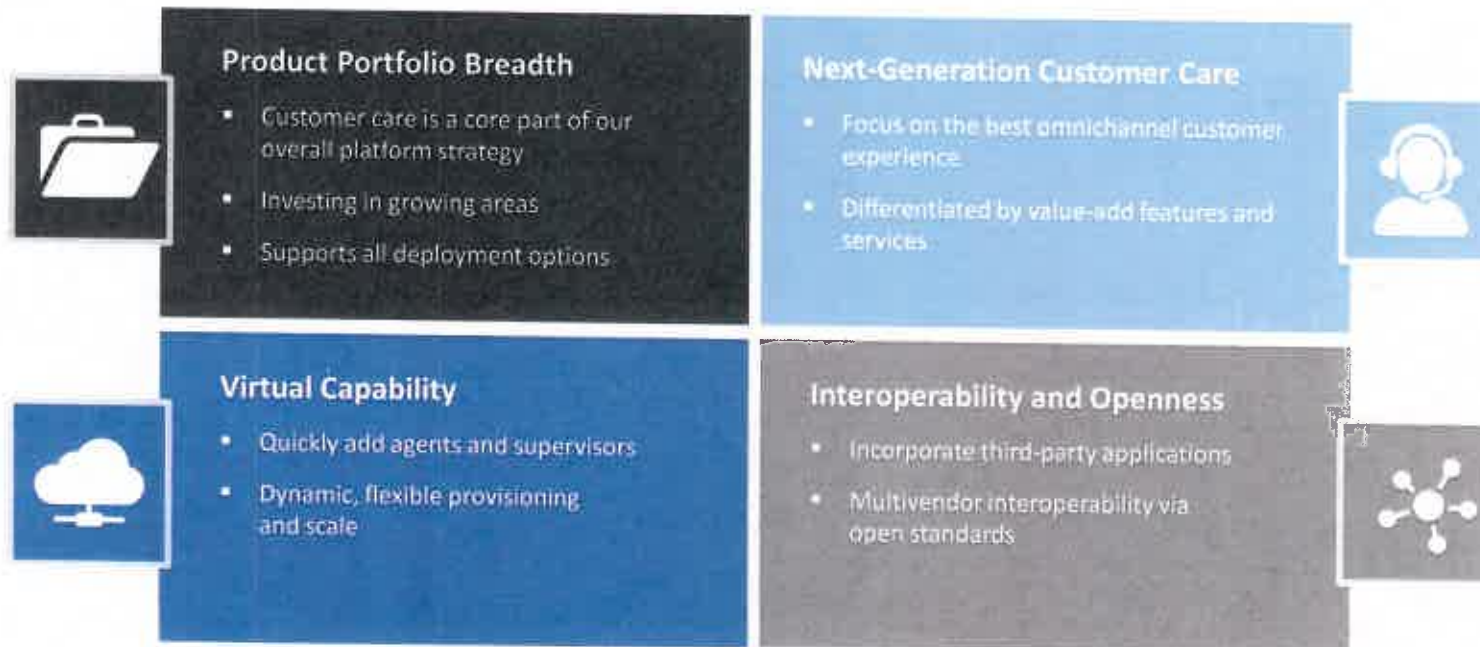
# AT&T Cloud Contact Center

Revolutionizing the Agent Experience

Features	Benefits
<ul style="list-style-type: none"><li>• Browser-based agent desktop</li><li>• Web gadget container<ul style="list-style-type: none"><li>– WebRTC Access Support</li><li>– Administrators define agent and supervisor layouts</li></ul></li><li>• Developer-friendly web API</li></ul>	<ul style="list-style-type: none"><li>• Single pane of glass for all agent information</li><li>• Easy management and upgrades</li><li>• Empowers agents via a user-centered design</li><li>• Flexible and expandable</li></ul>



# Why AT&T Customer Care Solutions?







# AT&T Unified Communications Services

## AT&T UC as a Service Services Design Document

**Version 2.7**

**Author: Mark Beranek**

**Revised 12/05/2017**



# Contents

---

<b>Contents</b>	<b>2</b>
<b>Tables</b>	<b>9</b>
<b>Figures</b>	<b>10</b>
<b>About This Service Design Document</b>	<b>13</b>
Document Purpose	13
Intended Audience	13
Document Usage Guidelines	13
Assumptions and Caveats	13
Related Source Documents	13
<b>Service Description Overview</b>	<b>15</b>
<b>Network Transport Services</b>	<b>17</b>
Wide Area Network Access	17
Network Transport Overview	17
Customer Network	18
AT&T Backbone Network Access	18
TDM PSTN Network	18
SIP PSTN Network	18
Remote Support Access	19
Network Access Boundaries	20
<b>Physical Site Information</b>	<b>22</b>
AT&T Internet Data Centers	22
Building	22
Building Access Security	22
Backup IDC	Error! Bookmark not defined.
<b>UC Node Architecture</b>	<b>24</b>
UC Node Overview	24
Network Access Layer	25
Routing Protocols	26
Border Gateway Protocol	26
Static Routes	27
VRF to VLAN Mapping	27
Physical Network Topology	28
Applications Layer	29



<b>NAT .....</b>	<b>30</b>
<b>Call Flows .....</b>	<b>31</b>
<b>Supported Features .....</b>	<b>36</b>
IP Telephony .....	36
Lawful Intercept .....	37
Number portability .....	38
Supplementary Voice Service .....	38
Video Telephony .....	38
Unified Messaging .....	38
Mobility Services .....	39
Presence .....	39
Call Detail Reporting .....	39
Emergency Services .....	40
<b>Compatibility of IP Phones with 911 capabilities. ....</b>	<b>40</b>
<b>C. Customer Responsibility and Indemnity .....</b>	<b>40</b>
<b>Contingency Planning .....</b>	<b>41</b>
<b>UC Node Redundancy .....</b>	<b>41</b>
CUCM Cluster Design .....	42
AT&T Utilizes Cisco best practices for deployment of Cisco Unified Communications Manager (CUCM) and Unity Connection for voice and voicemail services .....	42
Publisher .....	42
Subscriber .....	43
Call Processing Subscriber .....	43
TFTP Subscriber .....	43
<b>Alternate Site Redundancy .....</b>	<b>44</b>
Failover Prerequisites .....	45
Alternate Site Description .....	46
<b>Software Versions Watertown, MA and Allen, TX.....</b>	<b>47</b>
<b>Remote Access .....</b>	<b>48</b>
<b>Naming Convention .....</b>	<b>48</b>
<b>UCS-5108 Architecture .....</b>	<b>49</b>
General Overview .....	49
UCS Hardware/Firmware .....	49
UCS Connectivity .....	51
SAN .....	51
LAN .....	52
UCS Configuration Guidelines .....	54
UUID .....	54
MAC ADDRESS .....	54

WWNN and WWPN .....	54
Boot Policies .....	55
Management Policies .....	55
Network Control Policy .....	56
NPIV .....	56
NPV .....	56
<b>SAN Architecture .....</b>	<b>57</b>
<b>Hardware.....</b>	<b>57</b>
<b>Connectivity.....</b>	<b>57</b>
<b>Storage Requirements.....</b>	<b>58</b>
Latency.....	58
IOPS.....	58
Hot Spare .....	59
<b>Storage Overview.....</b>	<b>59</b>
<b>SafeNet Storage Security Overview.....</b>	<b>61</b>
<b>Storage Layout.....</b>	<b>63</b>
<b>Virtual SAN .....</b>	<b>63</b>
Port VSAN Membership.....	64
VSAN ID Scheme.....	64
<b>Zone and Zone Sets.....</b>	<b>64</b>
Zone .....	64
Zone Sets.....	65
Design .....	65
<b>RAID .....</b>	<b>65</b>
<b>LUN.....</b>	<b>65</b>
Overview .....	65
LUN Distribution per DAE.....	66
VM Distribution per LUN.....	67
<b>VMWare Architecture.....</b>	<b>68</b>
<b>VCenter Setup .....</b>	<b>68</b>
Logical Specifications.....	68
Physical Specifications .....	68
<b>ESXi .....</b>	<b>69</b>
Logical Specifications.....	69
Physical Specifications .....	69
Configuration and Optimization .....	70
<b>DVS Nexus 1000V .....</b>	<b>71</b>
Network Topology.....	72

Configuration .....	72
<b>Virtual Machine Setup .....</b>	<b>73</b>
VM Specifications per Application.....	73
VM Distribution per Blade per Chassis .....	75
<b>VMWare Features Support .....</b>	<b>76</b>
VMware High Availability (HA) .....	76
VMotion.....	77
SRM .....	77
Snapshots .....	77
VDR .....	77
FT.....	77
<b>UC Architecture .....</b>	<b>78</b>
<b>UC Feature Requirements.....</b>	<b>78</b>
<b>Overview .....</b>	<b>78</b>
<b>Technical Description of Components .....</b>	<b>79</b>
Clustering Across UCS Chassis/Data Centers .....	79
Call Processing Redundancy.....	80
TFTP Redundancy .....	81
Media Resources .....	81
<b>Dial Plan Overview .....</b>	<b>82</b>
Dial Plan Requirements .....	82
Inbound and Outbound Call Flows .....	84
Class of Service.....	84
<b>Network Quality of Service and Bandwidth Requirements for Voice.....</b>	<b>85</b>
Bearer Traffic .....	85
Signaling Traffic .....	85
<b>Voice Gateways and SRST.....</b>	<b>85</b>
Cisco Voice Gateway Types .....	85
Gateway Protocols .....	85
Site Remote Survivability Telephony (SRST) .....	85
Fax and Modem .....	86
<b>Call Admission Control .....</b>	<b>86</b>
Locations Based CAC.....	86
SBC Based CAC .....	86
<b>Features and Functions .....</b>	<b>86</b>
Emergency Call.....	86
<b>Unity Connection Architecture .....</b>	<b>87</b>
<b>Overview .....</b>	<b>87</b>

<b>Requirements for Installing Cisco Unity Connection on a Virtual Machine .....</b>	<b>87</b>
<b>Centralized Messaging and Centralized Call Processing.....</b>	<b>88</b>
<b>Redundancy.....</b>	<b>89</b>
<b>Deploying Cisco Unity Connection with Unified CM.....</b>	<b>89</b>
Managing Bandwidth.....	89
Cisco Unity Connection Operation .....	89
<b>Version .....</b>	<b>90</b>
<b>CUCM SIP Trunk Integration Guide for CUCxn Release 10.6.....</b>	<b>90</b>
Requirements .....	90
Call Information.....	91
Integration Functionality.....	91
<b>End-User Features .....</b>	<b>91</b>
Flexible User Interface.....	91
Automated Attendant Functionality .....	92
Dial Plan Flexibility: Partitions and Search Spaces .....	92
Languages .....	92
Access to Calendar, Meeting, and Contact Information.....	92
Desktop Message Access .....	92
Mobile Clients.....	93
Fax Messages .....	93
<b>Cisco Presence Architecture .....</b>	<b>94</b>
Overview .....	94
Cisco Unified Presence Components .....	95
Unified CM Presence Guidelines.....	96
Unified CM Presence Performance .....	96
CUP Single-Cluster Deployment .....	97
Cisco Unified Presence Cluster.....	99
Design Considerations for Cisco Unified Presence.....	99
<b>Mobility Architecture .....</b>	<b>101</b>
Overview .....	101
Features .....	101
Mobile Connect (SNR) .....	101
Mobile Connect Mid Call Features .....	101
Dual-Mode Phones and Clients.....	102
Design Considerations.....	102
Mobile Connect (SNR) .....	102
Mobile Connect Mid Call Features .....	104
Dual-Mode Phones and Clients.....	104

<b>Provisioning .....</b>	<b>109</b>
Mobile Connect (SNR) .....	109
Mobile Connect Mid Call Features .....	110
Dual-Mode Phones and Clients.....	110
<b>Management Architecture .....</b>	<b>111</b>
<b>AT&amp;T UC Node HCS Platform Management Overview.....</b>	<b>111</b>
Service Management Layer.....	112
Integration Layer.....	112
Domain Management Layer.....	112
Devices.....	112
<b>HCS Platform Management Services .....</b>	<b>113</b>
Vizgems Monitoring Application .....	113
Solar Winds Monitoring and Management .....	114
Domain Management Layer.....	115
<b>Multi-level administration.....</b>	<b>116</b>
<b>Management Network.....</b>	<b>120</b>
<b>Security Architecture.....</b>	<b>121</b>
<b>Overview .....</b>	<b>121</b>
<b>Network Functional Areas.....</b>	<b>121</b>
<b>Security Architecture.....</b>	<b>123</b>
Firewalling.....	123
Key Aspects.....	123
Firewall: Customer Phone to Customer Voice Servers .....	123
Firewall: Customer to USM Servers via Internal Network .....	124
Firewall: USM Servers to Customer Voice Servers .....	125
Monitoring .....	126
Intrusion Detection .....	126
Logging .....	127
Access Control.....	128
Management Plane Level.....	129
Control Plane Level .....	130
Data Plane Level.....	131
Virtual Platform Security .....	131
IPSec VPN Termination.....	132
Security Device Management .....	133
<b>Security Equipment .....</b>	<b>134</b>
ASA5500.....	134



ASA5580.....	134
ASA 5510.....	135
IPS 4270.....	136
Security Incident Management .....	137
Two Factor RSA Security ID Token Authentication .....	138
<b>Ports and Protocols .....</b>	<b>140</b>
Media and Signalling Protocols .....	140
<b>Data center requirements .....</b>	<b>143</b>
<b>CUCM requirements .....</b>	<b>143</b>
WAN Considerations .....	143
Intra-Cluster Communications .....	144
<b>Unity connection requirements .....</b>	<b>144</b>
<b>USM requirements .....</b>	<b>145</b>
<b>Network VLAN and Subnets .....</b>	<b>145</b>
<b>Appendix I Rack Elevation Diagrams.....</b>	<b>147</b>
<b>Glossary .....</b>	<b>148</b>
<b>About This Document.....</b>	<b>152</b>
<b>History .....</b>	<b>152</b>

# Tables

---

<b>Table 1</b>	<b>Software Versions</b>	<b>47</b>
<b>Table 2</b>	<b>UCS Hardware/Firmware</b>	<b>50</b>
<b>Table 3</b>	<b>SAN Hardware for Watertown, MA and Allen, TX</b>	<b>57</b>
<b>Table 4</b>	<b>IOPS Requirements Per Application</b>	<b>58</b>
<b>Table 5</b>	<b>Netapp Storage Component List</b>	<b>60</b>
<b>Table 6</b>	<b>SafeNet Storage Security Appliance</b>	<b>60</b>
<b>Table 7</b>	<b>VSAN Names and IDs</b>	<b>64</b>
<b>Table 8</b>	<b>vCenter Server Logical Specifications</b>	<b>68</b>
<b>Table 9</b>	<b>vCenter Server System Hardware Physical Specifications</b>	<b>68</b>
<b>Table 10</b>	<b>VMware ESX/ESXi Logical Specifications</b>	<b>69</b>
<b>Table 11</b>	<b>VMware ESX/ESXi Host Hardware Physical Specifications</b>	<b>69</b>
<b>Table 12</b>	<b>VM Specifications per Application (per VM)</b>	<b>74</b>
<b>Table 13</b>	<b>VMWare Features Support in HCS</b>	<b>76</b>
<b>Table 14</b>	<b>UC Feature Customer Requirement Against HCS Support</b>	<b>78</b>
<b>Table 15</b>	<b>Media Resources Support in HCS</b>	<b>82</b>
<b>Table 16</b>	<b>Codec Characteristics</b>	<b>89</b>
<b>Table 17</b>	<b>Supported Versions for CUCXN 8.x and CUCM</b>	<b>90</b>
<b>Table 18</b>	<b>CUP Server Platforms and Number of Users Supported</b>	<b>97</b>
<b>Table 19</b>	<b>USM server layout</b>	<b>115</b>
<b>Table 20</b>	<b>ASA5580 Capabilities and Capacities</b>	<b>134</b>
<b>Table 21</b>	<b>ASA5510 Capabilities and Capacities</b>	<b>135</b>
<b>Table 22</b>	<b>IPS4270 Capabilities and Capacities</b>	<b>136</b>

# Figures

---

<b>Figure 1</b>	<b>Network Topology Example Assumptions</b>	<b>17</b>
<b>Figure 2</b>	<b>Jump Server Topology</b>	<b>19</b>
<b>Figure 3</b>	<b>Network Boundaries Topology</b>	<b>20</b>
<b>Figure 4</b>	<b>AT&amp;T UC Node Architecture</b>	<b>25</b>
<b>Figure 5</b>	<b>IP Routing Network Access</b>	<b>26</b>
<b>Figure 6</b>	<b>Customer VRF to VLAN Mapping Topology</b>	<b>27</b>
<b>Figure 7</b>	<b>Physical Network Topology</b>	<b>28</b>
<b>Figure 8</b>	<b>VPN Integration</b>	<b>30</b>
<b>Figure 9</b>	<b>On-net Inter-Site VoIP Call</b>	<b>31</b>
<b>Figure 10</b>	<b>On-net Intra-Site VoIP Calls</b>	<b>32</b>
<b>Figure 11</b>	<b>Off-net calls to PSTN / Local Voice Gateway</b>	<b>33</b>
<b>Figure 12</b>	<b>Off-net calls to PSTN / Centralized SIP Network</b>	<b>34</b>
<b>Figure 13</b>	<b>Call processing in Survivable Remote Site Mode (SRST)</b>	<b>35</b>
<b>Figure 14</b>	<b>Voice Mail Access from IP Phone</b>	<b>36</b>
<b>Figure 15</b>	<b>CUCM Cluster Design</b>	<b>44</b>
<b>Figure 17</b>	<b>Alternate Site Allen Texas</b>	<b>46</b>
<b>Figure 20</b>	<b>Enterprise UC Node Backup Scenario</b>	<b>46</b>
<b>Figure 21</b>	<b>UCS Logical Connectivity</b>	<b>49</b>
<b>Figure 22</b>	<b>UCS and ESXi Connectivity</b>	<b>51</b>
<b>Figure 23</b>	<b>Blade Connectivity</b>	<b>52</b>
<b>Figure 24</b>	<b>Ethernet Mode</b>	<b>53</b>
<b>Figure 25</b>	<b>SAN Boot Policy</b>	<b>55</b>
<b>Figure 26</b>	<b>NPIV</b>	<b>56</b>
<b>Figure 27</b>	<b>NPV</b>	<b>56</b>
<b>Figure 28</b>	<b>SAN Connectivity</b>	<b>58</b>

<b>Figure 29</b>	<b>NetApp FAS 3270-R5</b>	<b>59</b>
<b>Figure 30</b>	<b>Example Allocation of Physical Drives In SAN</b>	<b>63</b>
<b>Figure 31</b>	<b>Virtual SAN</b>	<b>63</b>
<b>Figure 32</b>	<b>Zoning Concept Example</b>	<b>65</b>
<b>Figure 33</b>	<b>Logical Unity Number Concept</b>	<b>66</b>
<b>Figure 34</b>	<b>LUN Distribution per DAE</b>	<b>66</b>
<b>Figure 35</b>	<b>Cisco Nexus 1000V Network Topology</b>	<b>72</b>
<b>Figure 36</b>	<b>Example Layout of Applications per Chassis/Blade</b>	<b>75</b>
<b>Figure 37</b>	<b>Call Processing Redundancy</b>	<b>80</b>
<b>Figure 38</b>	<b>TFTP Redundancy</b>	<b>81</b>
<b>Figure 39</b>	<b>SRST</b>	<b>86</b>
<b>Figure 40</b>	<b>Centralized Messaging with Centralized Call Processing</b>	<b>88</b>
<b>Figure 41</b>	<b>Redundancy of Cisco Unity Connection Messaging</b>	<b>89</b>
<b>Figure 42</b>	<b>CUP 8.0 Architecture</b>	<b>95</b>
<b>Figure 43</b>	<b>CUP Components</b>	<b>96</b>
<b>Figure 44</b>	<b>Interactions Between CUP Components</b>	<b>97</b>
<b>Figure 45</b>	<b>Basic CUP Deployment</b>	<b>99</b>
<b>Figure 46</b>	<b>Mobile Connect Architecture</b>	<b>103</b>
<b>Figure 47</b>	<b>Dual-Mode Phone Architecture</b>	<b>106</b>
<b>Figure 48</b>	<b>Cisco Mobile Dual-Mode Hand-Out (WLAN-to-Mobile Voice Network)</b>	<b>107</b>
<b>Figure 49</b>	<b>Nokia Call Connect Dual-Mode Hand-Out (WLAN-to-Mobile Voice Network)</b>	<b>108</b>
<b>Figure 50</b>	<b>Nokia Call Connect Dual-Mode Hand-In (Mobile Voice Network-to-WLAN)</b>	<b>108</b>
<b>Figure 51</b>	<b>Cisco HCS Management Service Enablement</b>	<b>111</b>
<b>Figure 52</b>	<b>HCS Management Solution for AT&amp;T</b>	<b>113</b>
<b>Figure 53</b>	<b>AT&amp;T Vizgems Monitoring Topology</b>	<b>114</b>
<b>Figure 54</b>	<b>AT&amp;T HCS Network Functional Areas</b>	<b>122</b>
<b>Figure 55</b>	<b>Customer Phone to Customer Voice Servers Firewalling</b>	<b>124</b>
<b>Figure 56</b>	<b>Customer to USM Servers Firewalling via Internal Network</b>	<b>125</b>
<b>Figure 57</b>	<b>USM Servers to Customer Voice Servers</b>	<b>126</b>

<b>Figure 58 HCS Data Centre IDS Monitoring Points</b>	<b>127</b>
<b>Figure 59 Access Control Pat</b>	<b>129</b>
<b>Figure 60 IPSec Termination Points on the HCS Network</b>	<b>133</b>
<b>Figure 61 Security Incident Management</b>	<b>138</b>



# About This Service Design Document

---

## Document Purpose

The purpose of UC voice Service Design Document (SDD) is to define the Architecture, support services and identify security components located within the accreditation boundary of UC Voice information system (IS), which resides at the following location: Watertown, MA, Allen, TX, Singapore, Amsterdam, Piscataway, NJ (IDC). The UC Voice System Security Plan (SSP) in conjunction with the SDD describes, in detail, the security mechanics that are implemented and comprise the overall UC Voice design, provisioning, operation elements and system security framework.

## Intended Audience

This document is intended for use by AT&T design and designated internal and third party implementation staff, authorized system auditors and the end customer.

## Document Usage Guidelines

This SDD is not to be shared outside of AT&T without approval by UC product team Mark Beranek

## Assumptions and Caveats

This SDD only intends to cover the AT&T UC Voice core infrastructure and is not intended to provide detailed description of any existing external network connectivity. Descriptions on how network access is to be achieved are provided for conceptual overview of complete network capabilities and are not intended to reflect the actual implementation of network transport for the end customer locations. Billing and ordering systems are not part of the scope of this document.

## Related Source Documents

- [1] CUP installation, administration, and configuration guides  
[http://www.cisco.com/en/US/products/ps6837/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html)
- [2] Netapp SAN storage support edge secure for government
- [3] Netapp system implementation workbook
- [4] Presidential Directive HSPD-12
- [5] E-Government Act of 2002 - Public Law 107-347 Title III – FISMA
- [6] Office of Management and Budget Circular a-130
- [7] Appendix III - Security of Federal Automated Information Resources
- [8] NIST Special Publication 800-53 Revision 2, Recommended Security Controls for Federal Information Systems dated December 2007

- [9] NIST Special Publication 800-37 Revision 1, Security Authorization of Federal Information Systems, dated August 2002
- [10] Networx Statement of Work (SOW) Unified Connection Voice over IP Service (UC Voice) **For Official Use Only**, Amendment 004, November 18, 2008
- [11] Networx Statement of Work (SOW) Unified Connection Voice over IP Service (UC VOICE ), November 1, 2011

# Service Description Overview

---

AT&T's UC Voice Service provides an integrated user experience across a combination of real-time communication services including chat (instant messaging), presence information, IP telephony, audio/web conferencing, and non real-time communication services such as e-mail across multiple devices (desktop, mobile, and landline).

Users of AT&T UC Voice Services are able to communicate with their colleagues using a rich suite of IP telephony and unified messaging capabilities. AT&T UC Services is delivered as a set of features. The UC Voice Service components provide the foundation for the following features to meet Networkx services customers stated requirements to support:

- Voice Calling: UC Voice Desktop Phone Service
- Voice Calling: Local and Long Distance (requires connection of customer provided voice service)
- Soft Phone and Mobile Device Applications
- Voice Messaging
- Unified Messaging
- Empower the mobile worker
- Ability to have presence in the network regardless of actual location
- Ability to initiate conferences and collaboration sessions immediately
- Communication portability
- Integration of employee's tool
- Instant Message
- Electronic mail Collaboration
- Voice mail
- Cellular service
- Integration with Conferencing
- Integration with Mobility resources
- Utilize customer existing or new network transport

AT&T Unified Communications Voice is a dedicated hosted cloud-based service consisting of IP telephony (IPT), Presence, IM, conferencing and collaboration. AT&T utilizes unified communications nodes to support centralized call processing and integration with Presence, IM applications. AT&T UC Voice core hardware and applications are deployed in our highly secure and reliable AT&T Internet Data Centers (IDCs). The architecture is fully redundant with integration into customer's locations via existing and new dedicated network transport. AT&T utilizes 6 AT&T UC Node Data centers to provide Alternate-Site Redundancy services. AT&T manages the two centers 24x7x365 via our UC Support team located in Atlanta, GA, Schaumburg .IL, Piscataway, NJ and India.

AT&T UC Services has been designed to support high-availability requirements. The centralized architecture streamlines the ability to deploy productivity enhancing applications across a unified communications platform for all of end-customer locations.

AT&T UC Services is a complete unified communications solution that utilizes customers' existing LAN infrastructure, augmented with peripheral voice gateways, and a fully redundant unified messaging core. Network transport, services, and applications layers are implemented transparently, allowing transport infrastructure to be independent from the services and applications that run on top of it.

The AT&T UC Services architecture also enables easy evolution and incorporation of future applications as your business needs require. AT&T UC Services provides a seamless path to enhanced IP voice communications. The Networx customers can utilize a phased migration approach to move existing employees from legacy voice systems to complete unified communications at their own pace and as their requirements dictate.

AT&T will provide support for the migration of existing voice clients, utilizing the AT&T Unified Communications platform. The platform will allow for support of basic voice and voice mail communications as well as providing for next-generation unified messaging via IMAP integration with Microsoft Outlook or other IMAP-compatible email applications. AT&T UC Services provides for the scalability that you will likely require in the future, adding clients as needed to meet your expansion requirement.

AT&T UC Services solution also provides for complete network monitoring, management and on-site support to maintain the solution 24x7. AT&T network transport components provide a seamless one-stop support environment. AT&T can also offer implementation, training and project management support services as part of the overall solution.

The entire solution is delivered, managed and monitored by AT&T. AT&T provides options to perform all of the moves, adds and changes for end customers. The customers administration staff will also have the ability to use an online portal to open and track troubles or to request moves, adds and changes to the voice messaging system. AT&T Integrated Data Centers (IDC) that house the AT&T UC Nodes can be connected to customer data centers to support connectivity, security, and resiliency as required. The proposed AT&T solution for Networx customers has been engineered to deliver 99.999% reliability. *Please note:* Reliability refers to the AT&T provided services. The performance of your existing WAN or other equipment that is integrated into the overall solution may degrade the level of reliability.

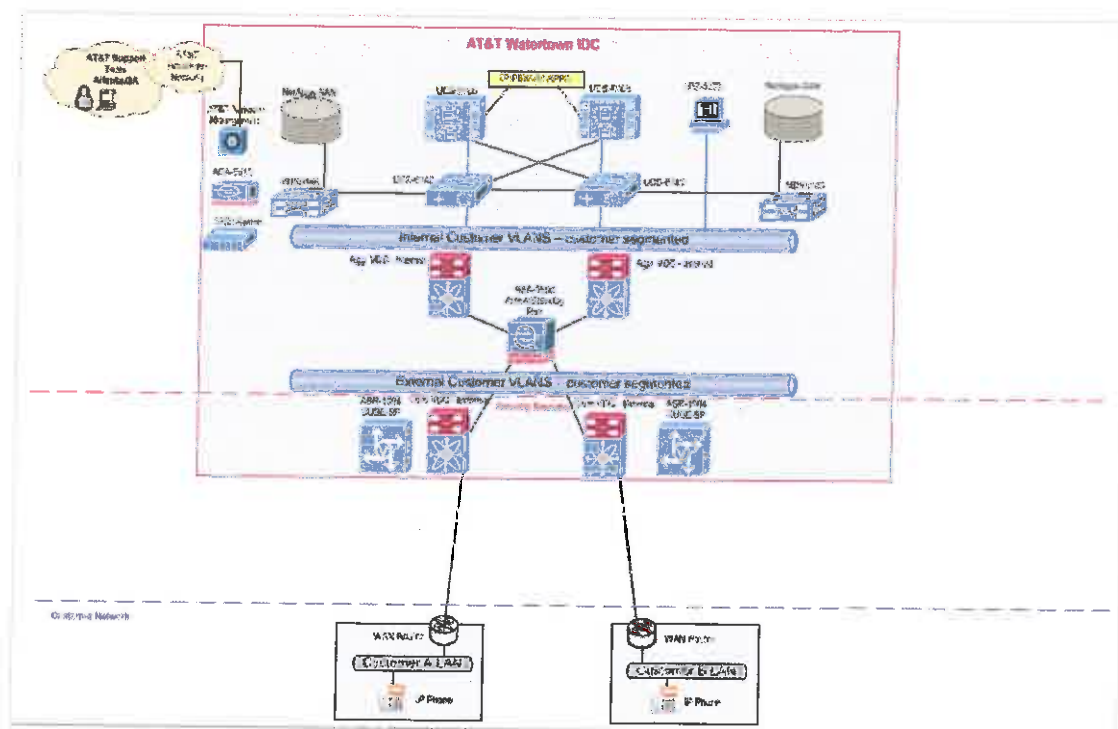
# Network Transport Services

## Wide Area Network Access

AT&T utilizes the customers' existing network transport to extend Unified Communications services including voice, messaging, presence, IM and messaging. Deployment of AT&T UC service for federal system customers is delivered via the customer existing or new network transport. High level description is provided to define how customers will access AT&T UC voice services and the interaction of WAN and network access with core UC Voice systems. AT&T supports access via Ethernet handoff to the Nexus 7010. Customer can elect to utilize other network transport such as Optical services, DS3, T1/E1 as long as the service provider provides management for the circuit termination device and the handoff from that device is Ethernet with connection speeds from 10Mbps to 1000Mbps.

## Network Transport Overview

AT&T transport overview section provides high level requirements and supported network access methods. The customer can elect to leverage other AT&T transport services or third party to establish connectivity to the UC service nodes.



**Figure 1** Network Topology Example Assumptions

The following assumptions are made regarding the delivery of AT&T UC Services over customer network transport



## Customer Network

AT&T provides the core call processing equipment as part of UC Voice services and the customer premise voice gateways and end user IP Phone devices as part of the service. AT&T relies on the end customer to provide the following:

Provide network access to the UC node centers via MPLS network transport

Provide Local Area Network IP addresses and voice VLAN information and configuration

Ensuring that routing information is exchanged with the customer network such that any phones or end devices establish connectivity to the hosted services via Boarder Gateway Routing Protocol version 4 (BGP4).

Since the UC applications are delivered within the existing customer's network, the bandwidth and latency requirements must be met within the customers' existing network. Network requirements are defined in the High Level Architecture chapter of this SDD.

## AT&T Backbone Network Access

AT&T utilizes an established dedicated backbone network to support remote access from the Network Operations Center (NOC) and Security Operations Center (SOC) located in Atlanta, GA.

The AT&T backbone network is also utilized to provide data backup capabilities between UC nodes.

## TDM PSTN Network

Where centralized SIP trunks are not available, T1 PRIs connected to on site voice gateways will provide PSTN access.

AT&T Solution Requirements document and Configuration Capture documents will be utilized to capture the specific PRI signaling information required for provisioning voice gateways. Customer will be responsible for ordering the local PSTN access either through AT&T or third party. PSTN access is defined as a regulated service and must be ordered and contracted separately from UC Voice service.

Calls delivered to the PSTN will not require any customer tagging or separation at PRI integration point. Emergency services are delivered as part of the regulated services and the PSTN provider selected by the customer. AT&T will define dialing rules within the IP PBX to support extending the calls to the carrier and emergency services. UC Voice is a hosted dedicated PBX platform and not an Interconnected VoIP carrier platform.

## SIP PSTN Network

Where SIP trunks are provided they may allow calls to be placed to one or more locations in the U.S.

SIP trunks will terminate into the AT&T IDC via circuit access Main Distribution Frames and then will be extended to the UC Node with the CUBE-SP acting as session border controller (SBC)

Calls delivered to the PSTN via SIP will be associated to the customer specific voice VLAN and associated to the CUBE-SP

Numbering information for service calls and emergency calls will be provided by AT&T as part of the customer specific dial plan.

SIP trunk are contracted separately as a regulated service and are not included in the UC Voice hosted dedicated IP PBX platform.

## Remote Support Access

Remote access is provided over dedicated network access through the AT&T secure network backbone. Access control is provided via the ASA5510 firewall appliance installed in each data center. The ASA5510 will be configured with specific source and destination access control lists along with authentication and password defined for use by designated support team staff. Access to specific applications is further controlled by use of Jump server. The designator for the jump server is HOP 21560 as defined in the rack elevation diagram included in this document

### HOP Server details:

Authentication by user ID with Pin + RSA SecureID Hard Token as password. HOP requires Active Directory user and password combination after successful Secure ID authentication.

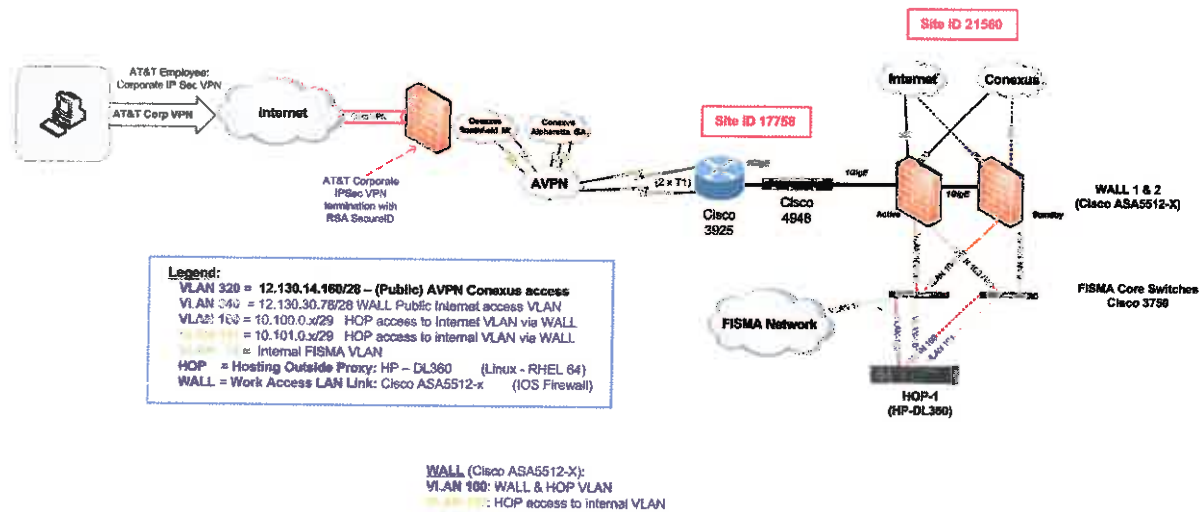


Figure 2 Jump Server Topology

## Network Access Boundaries

The network access boundaries are as follows:

### Carrier Network Transport:

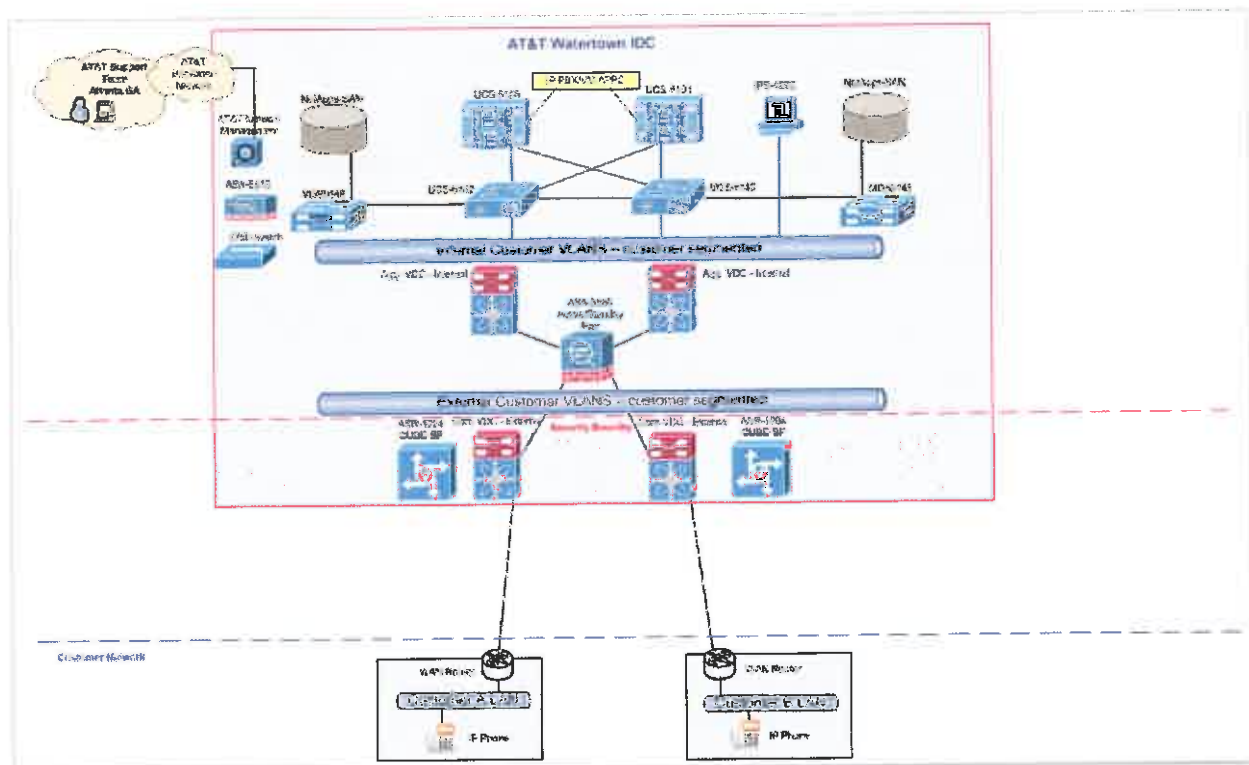
- TDM interfaces for PRI for local customer premise
- SBC interface for SIP trunks delivered to the AT&T IDC and UC Node

### AT&T UC Node Security Boundary

- Nexus switch for WAN connectivity between datacenter and remote customer sites
- Connectivity to a carrier provided access router
- Interface between south bound customer traffic and north bound UC applications
- AT&T backbone providing secure remote access to UC node applications and hardware

### Customer Network

- Provides Local Area Network (LAN) access to end user devices
- Provides LAN connectivity to on premise voice gateway for PSTN access



**Figure 3 Network Boundaries Topology**

June 15, 2015

AT&T UC Voice SDD

20

Company Confidential. A printed copy of this document is considered uncontrolled.

# Physical Site Information

---

## AT&T Internet Data Centers

AT&T UC Voice is deployed in highly secure, and reliable, AT&T Internet Data Centers (IDCs). Geographic redundancy, and thus high availability including disaster recovery, is achieved by deploying AT&T UC Voice across AT&T IDCs located in North America ASIA and EMEA. The IDC's provide primary power heating and air conditioning to sustain equipment operations within the center. Backup power generation is provided via battery subsystems and diesel generators. The IDC also provide dual path access for circuit delivery.

## Building

AT&T IDC's locations have raised floor and are rated to 150 lbs./sf (1000 lbs./rack). Racks greater than 1000 lbs require additional under floor supports. Sub-floor rating is 250 lb/sf. Heavier loads can be accommodated through an engineering review. AS will develop a Low Level Design (LLD) that will provide the detailed design for the project. There are 5 - 600 ton centrifugal chillers in a N+1 configuration at full building load. The raised floor is used as an air plenum. There are 68 diverse 30 ton CRAC units, configured as N+1. There is 3-16,000 gal onsite water storage tanks designed to support the cooling system at Maximum facility full load for 12 hours. There are 2-900 ton Heat exchangers. The fire alarm system is a VESDA (air sampling) smoke detection and alarm system. The data center area has a pre-action dry pipe fire suppression system.

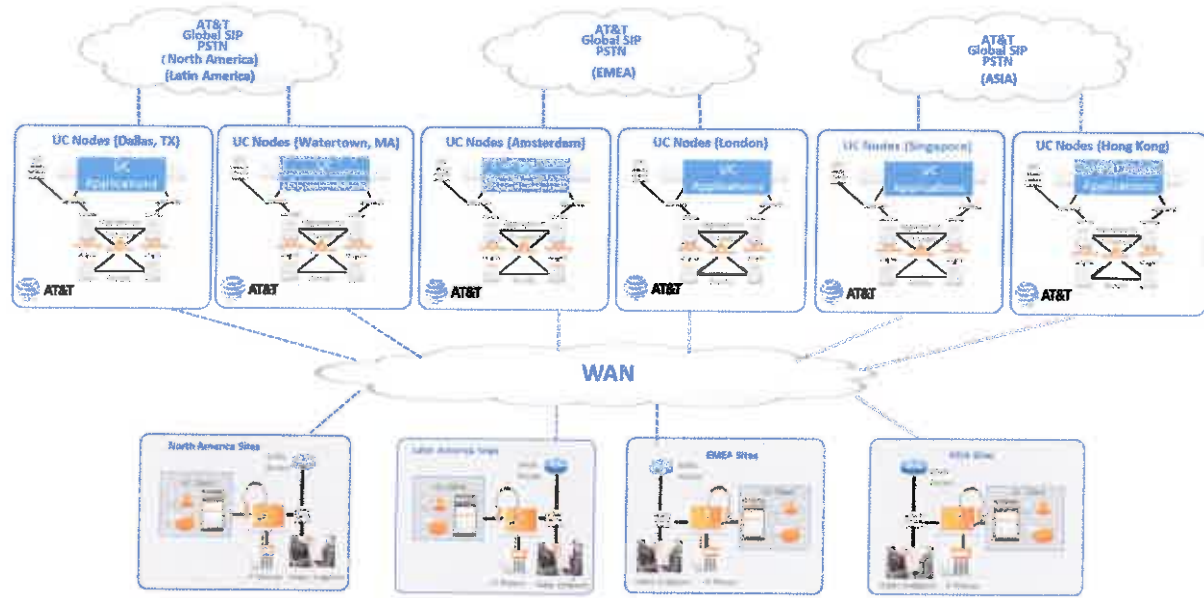
## Building Access Security

AT&T IDC provides security staffing is 24x7x365, closed circuit monitors, secure key-card access, biometrics scanner, a mantrap, and alarmed doors. Guards maintain access from the loading dock and access requires a card key. Security personnel also monitor the building. AT&T maintains a current list of authorized personnel. Monitoring is provided onsite and remotely.

- CCTV recording retention is 90 days at 3.5-7 frames per second.
- Shipping & Receiving: No unidentified packages will be accepted.
- Onsite security personnel monitor access to the loading docks and all cages and cabinets.

## Geo-Redundant Global UC Node Data Centers

A second IDC located in each region to provide backup for North America, ASIA, EMEA



AT&T UC Nodes are located per region to deliver real time applications without loss of call quality and also support requirements for in country regulatory requirements when required.



# UC Node Architecture

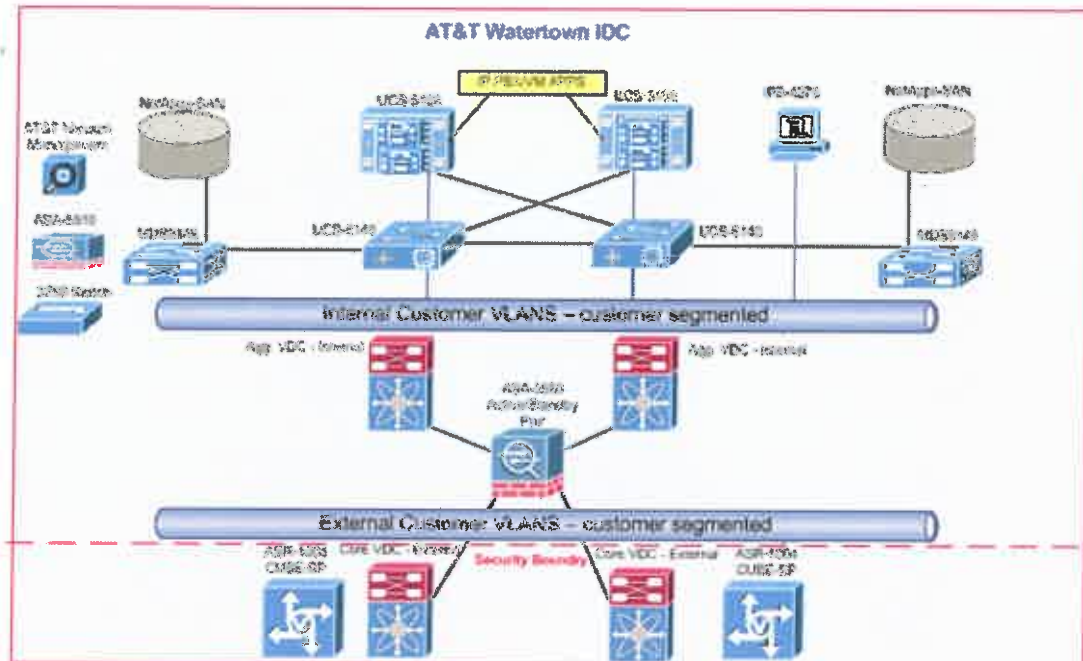
## UC Node Overview

AT&T leverages Cisco Hosted Collaboration Solution (HCS) architecture. Cisco HCS consists of the following platforms that will be described in detail throughout this SDD. The term UC Node is used to describe the deployment of HCS into an AT&T IDC. The Cisco Nexus 7010 is utilized to provide layer 2 and 3 routing and switching between the core applications and customer network access. Multiple 1 GIG layers three connections are established to ensure bandwidth level for support of traffic volumes and resiliency. Cisco UCS 5108 chassis are connected via multiple path fibre channel via redundant Cisco 6296 fibre switches with Nexus 1000v virtual switches built within the 5108 chassis performing segment connectivity into the UCS virtual Cisco Unified Communications Manager (CUCM) application instances. Netapp self-encrypting SAN storage is utilized to backup applications databases. Each CUCM instance has backup via redundant Netapps SAN and CUCM Publisher and Subscriber data base replication. Centralized management of the multiple CUCM instances is provided by Cisco Unified Domain Manager (CUCDM) application. The CUCDM application provides logical segmentation of customer provisioning attributes. AT&T Vizgems and Solar Winds applications provide support for monitoring and management and fault isolation. SNMP polling, and traps for all equipment reports to redundant AT&T AOTS platform. Cisco ASR 1004 provides hardware support for Cisco Unified Border Element Service Provider (CUBE-SP) software in support session border control functions. Two Cisco ASR1004 provides support for SIP trunk termination into the UC node when centralized call processing is required. Cisco ASA 5580 firewalls provide security border between network transport access and end user application. The ASA firewalls also provide segmentation along with VLAN ID between customers within the UC Node. Cisco IPS-4270 provides detection and intrusion prevention services. All hardware is deployed with redundancy within the UC Node.

AT&T utilizes Cisco Unified Communication Manager CUCM to support IP voice features. CUCM provides functions normally performed by a traditional PBX. It is a client/server application. The CUCM applications are deployed on VMware based Cisco UCS 5108 blade server platforms. The CUCM handles all call signaling, call processing, and device management and coordinates communications between its core call processing tasks utilizing Cisco Skinny Communications Control Protocol (SCCP) between IP Phones and CUCM. SIP is utilized to communicate with customer premise voice gateways and CUBE-SP. CUCM is integrated with AT&T UC applications utilizing the following protocols: SIP, JTAPI, XML and SOAP AXL.

CUCM provides call set-up and call processing between all voice devices. For example, CUCM will set up a call between two IP phones. The call can also be between an IP phone and a voice gateway for PSTN utilizing the customers premise voice gateways or via centralized SIP trunks delivered to the AT&T UC Nodes. The CUCM sets up the call, but then actual media traffic passes directly between the endpoints – between the IP phones or between the IP phone and the gateway. Call setup is handled using Cisco SCCP and voice path utilizes RTP/UDP protocol.

Cisco Unity Connection (CUCx) application provides support for voice mail. The CUCX application is delivered on the same UCS 5108 chassis that provide CUCM. Both applications are distributed across multiple blades to provide resiliency. Application and hardware resiliency are covered later in the SDD.



**Figure 4 AT&T UC Node Architecture**

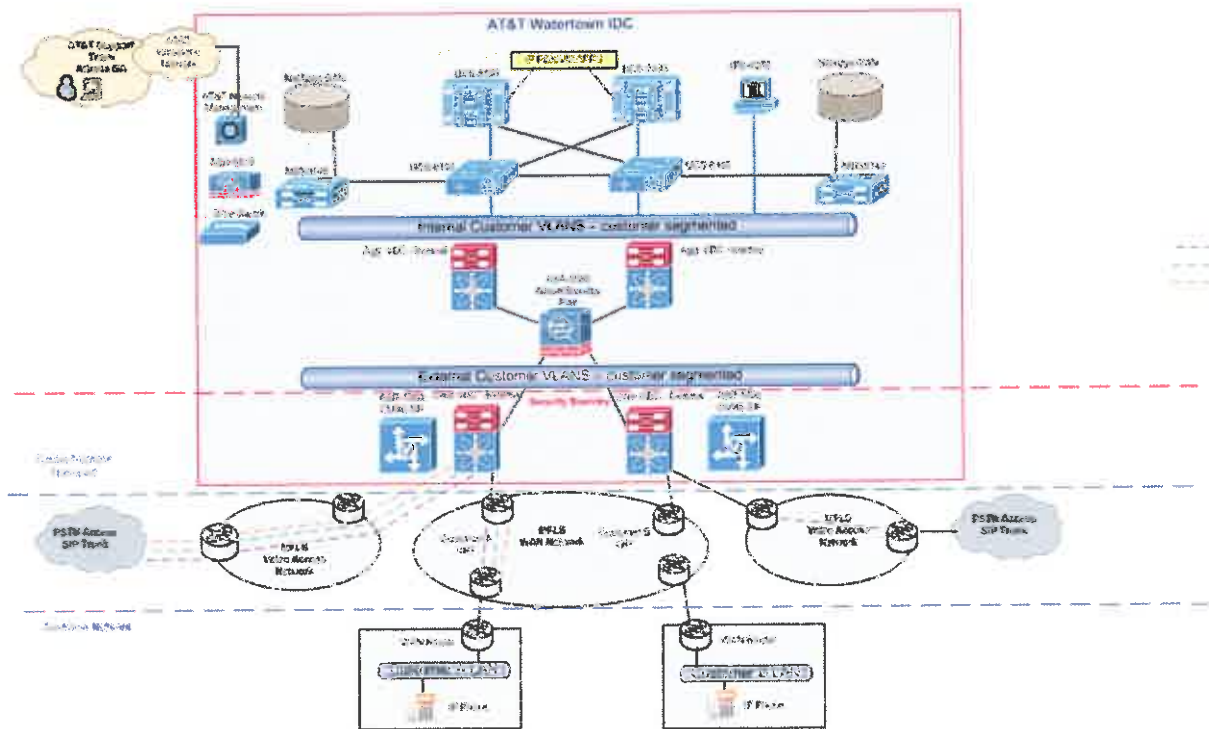
The UC Node architecture at AT&T will be based on 3 layers or building blocks, from bottom to top:

1. **Network Access Layer:**  
This layer provides access to and from customer network utilizing the Nexus 7010 layer 2/3 routing and switching capabilities. This is also Aggregation VDC. All internal Customer VLAN terminates at Agg VDC, Customer segmented through VLAN's. This layer includes the ASA 5580 firewall and access control policies, UCS 6296 provides provisioning support and Ethernet to fiber channel conversion. MDS 9148 provides integration to Netapp SAN storage. A unique VRF and multiple VLAN's are created per customer.
2. **Core Layer:**  
This layer contains all of the core infrastructure equipment include Nexus 7000 Core VDC. This layer includes the CUBE-SP and ARS1004 routers provide the termination point for SIP trunks.
3. **Applications Layer:**  
This layer contains all the virtualized instances of CUCM, CUCx, CUCDM, Solar Winds per customer running on the UCS 5108 chassis and B200M1 blades. Intrusion detection applications utilizing the IPS 4270 platform

## Network Access Layer

Watertown UC nodes use various routing protocols within the core infrastructure to transport IP traffic though the infrastructure. Figure 4 shows where these routing protocols are deployed. Layer 2 and Layer 3 IP routing is supported by the Cisco Nexus 7010 switches. Two Nexus 7010 switches are deployed in the UC node to provide resiliency. The Nexus Aggregation 7010 switches interact with other core hardware Nexus 7000 components to perform IP traffic routing. Border Gateway Protocol 4 (BGP4) is the primary protocol deployed for both internal and external routing updates. Static routes are defined for specific connection between UCS 5108 applications

and CUBE-SP. Other Static route are defined between Cisco ASA-5580 firewalls to allow specific traffic flows and to segment customer traffic like IPflex VPN etc.



**Figure 5 IP Routing Network Access**

## Routing Protocols

### Border Gateway Protocol

**BGP-4 (Border Gateway Protocol)** is used to communicate with customer existing network.

- External BGP4 routing
  - Peers to AT&T (MPLS) Routers and Nexus 7010 in the Watertown UC Node
  - Receives and distributes full Internet Routing Table
  - Advertises customer private networks to the AT&T (MPLS) Network router
  - Control default route injection into the agency VPN at the Virtual Route Forwarding (VRF) level
- Internal BGP4 routing
  - Exchanges routes between internal core UC Node equipment subnets
  - Controls static route injection between internal BGP4 equipment

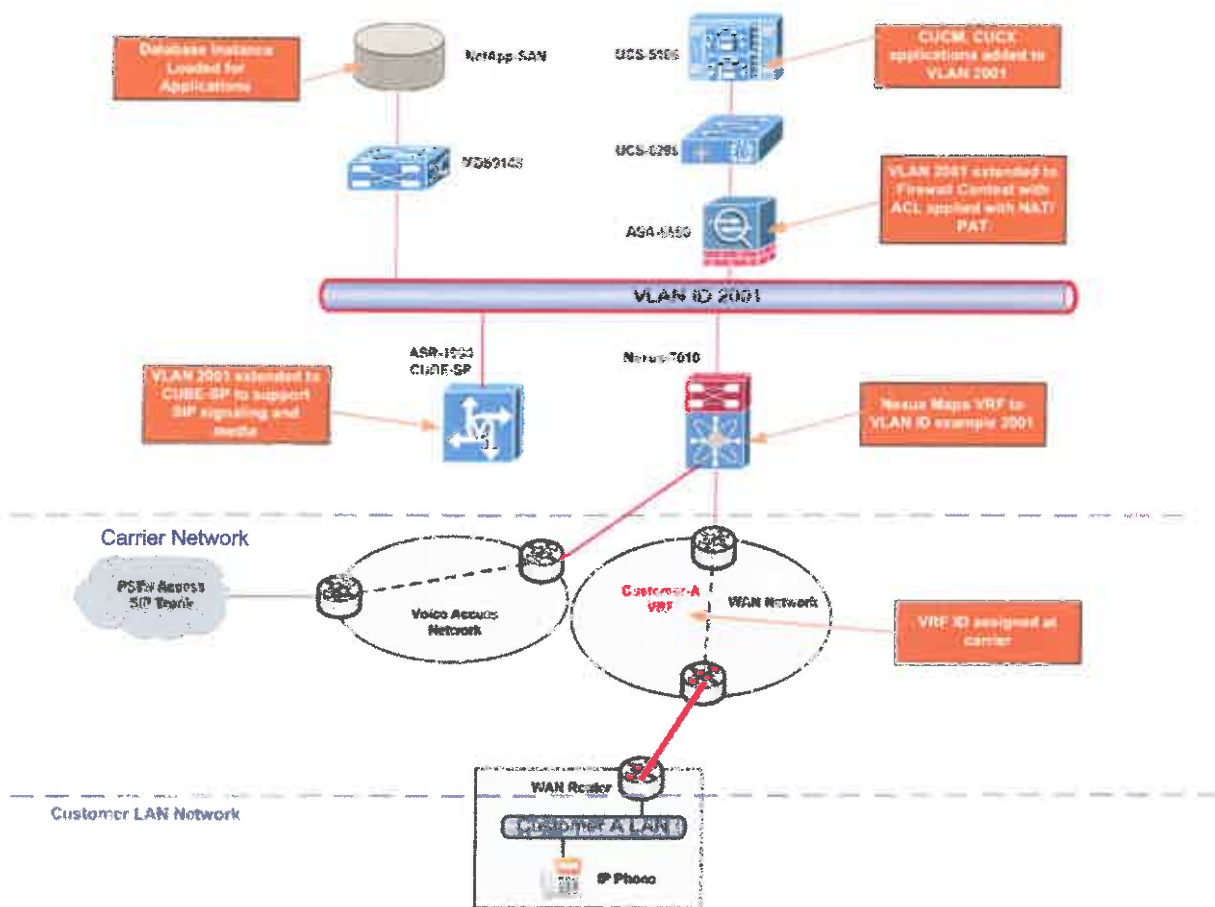
## Static Routes

- Utilized at the Core UCS Server Blades, Firewall and CUBE-SP
  - Use static routes to define specific customer information paths between CUCM/VM application servers and CUBE-SP

These protocols communicate routes in real-time to direct the flow of traffic. Under normal operations, traffic is directed through the Watertown UC node. In the event of a component or interface failure, these protocols automatically redirect the traffic.

AT&T has registered a public Autonomous System Number (ASN) for each UC Voice Watertown UC Node. The designation of each customer as a public Autonomous System (AS) allows AT&T to advertise subscribing agencies' ASNs

## VRF to VLAN Mapping

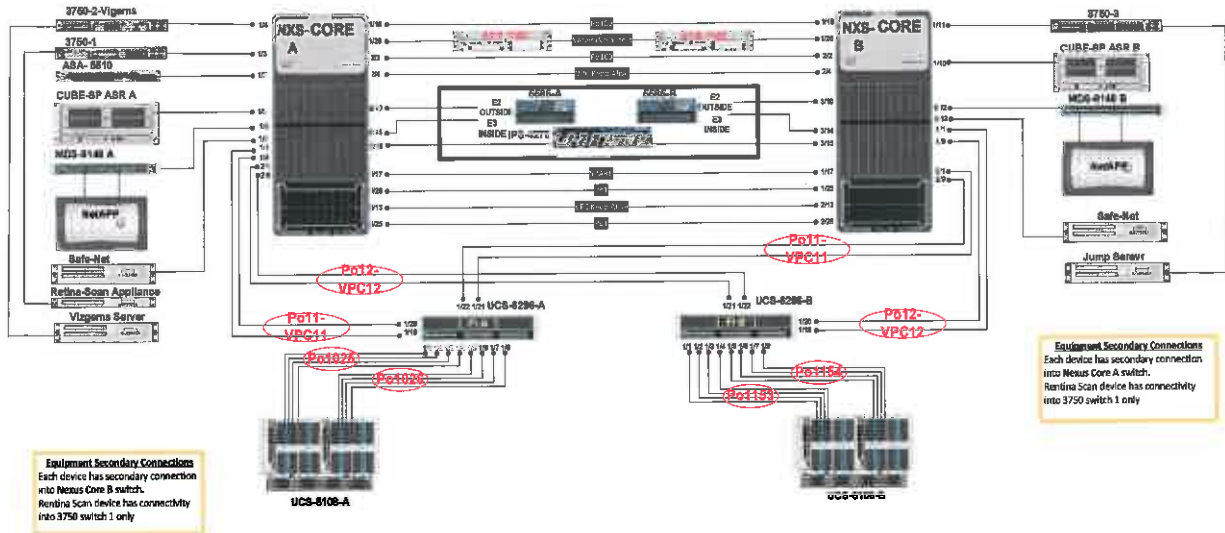


**Figure 6 Customer VRF to VLAN Mapping Topology**

AT&T maps the customer and carrier provided Virtual Route Forwarding (VRF) information to the Nexus 7010 physical switch port. The switch port is then assigned into a customer specific Virtual Local Area Network (VLAN). The VLAN is assigned a customer specific ID that is utilized to extend the customer network IP addresses and routing information up to the Cisco ASA Firewalls. The VLAN ID is mapped to the firewall virtual context that defines a specific customer firewall instance. The firewall context defines access control information to extend signalling and media to the CUCM and CUCX applications as well as the CUBE-SP.

It is assumed that the customer will provide DHCP, DNS and LDAP servers on premise.

## Physical Network Topology



**Figure 7 Physical Network Topology**

The AT&T UC Node is equipped and connected as follows:



- Multiple UCS 5108 chassis hosting UCS blades running distributed virtual switch (Nexus 1000V), VMware ESXi and virtual machines with applications. Connectivity is provided via Fiber Channel Over Ethernet to the Cisco 6296 Fabric interconnects
- Dual UCS fabric interconnects Cisco 6296 providing access for the virtual machines to the LAN/WAN (Nexus 7010 and MPLS VPN network) and to the SAN via Fiber Channel connections
- The SAN comprised of 2 SAN switches (MDS 9148) and an FC storage (NetApp)
- A central SBC (CUBE-SP SBC) aggregating the different customer VPN to provide address translation and anchor for call signaling and media, as well as access to the AT&T voice network via SIP and is connected via two Gig Ethernet connection per chassis to the Nexus 7010 layer 2/3 switches
- Two (2) ASA 5580 redundancy pair utilized to perform security barrier between inside and outside traffic as well as customer segmentation within the UC node. 4 connections per ASA establish segmentation between access and core networks
- An IPS-4270 for intrusion detection service appliance to monitor inbound traffic. There is one Gig Ethernet connect into each nexus 7010 switch

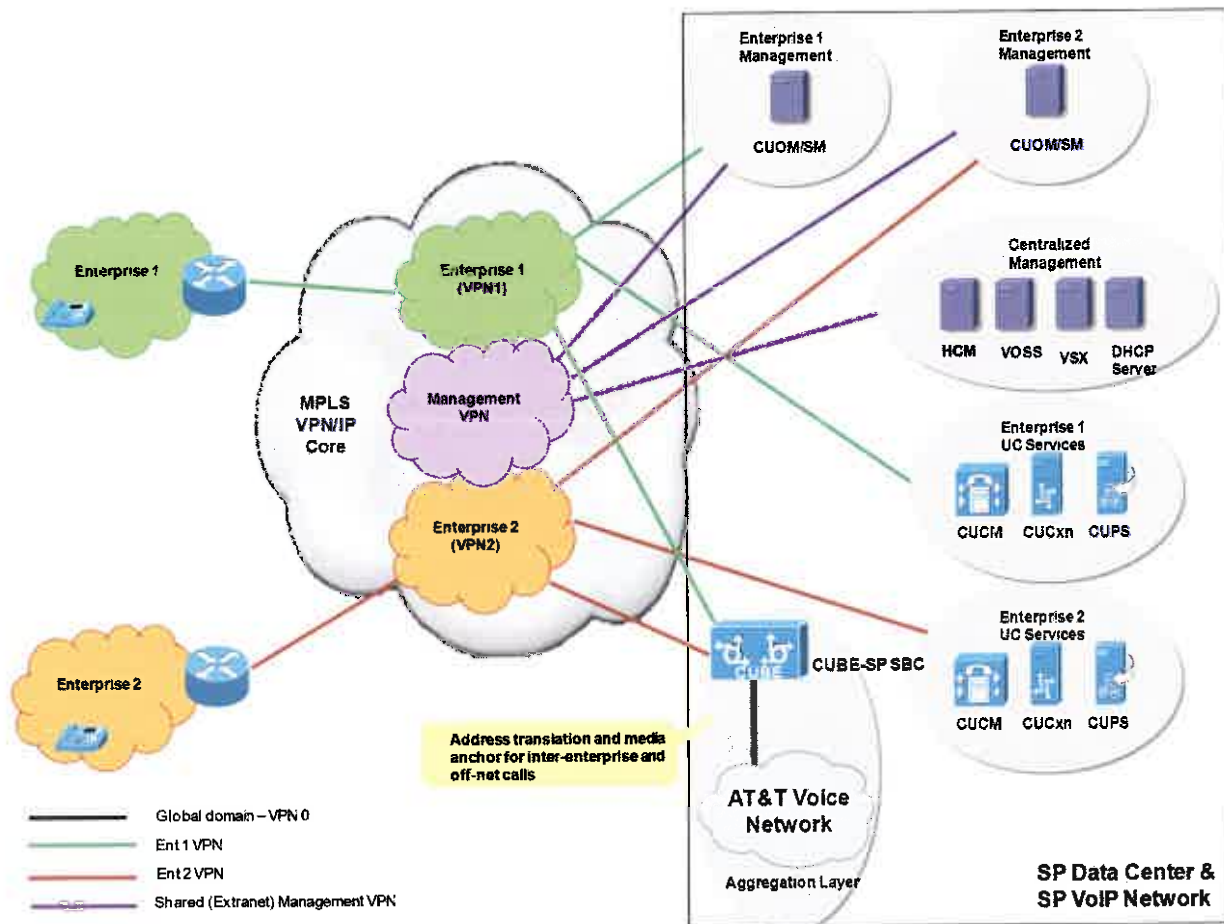
Outside the data center acting as the central site, are a number of remote sites belonging to AT&T end customers connecting to the AT&T network via the customers MPLS VPN network.

Each component is defined with software and hardware specification later in this document. Rack elevation diagram and power distribution can be found in appendix I.

## Applications Layer

The UC Voice solution will be deployed utilizing customers MPLS VPN network. The picture below defines which VPN each solution component will belong to:

- UC services (CUCM, CUCxn, CUPS) will belong to the customer VPN. The most common deployment for AT&T is to use a /24 from the customer IP addressing space.
- One ASA firewall or virtual firewall instance will be deployed per customer for topology hiding purposes. Each firewall will be part of the customer VPN, either located at the datacenter (preferably) or on customer premise. Note that if NAT/PAT is required to prevent IP address overlaps on the phone inventory, the ASA will perform this task.
- The centralized management services (VSX, and VOSS/CUCDM) will belong to the AT&T management VPN and have AT&T owned IP addresses. Hosted Collaboration Management (HCM) is the assigned AT&T name for all components working together to support provisioning and monitoring
- The aggregation layer service will be made of the CUBE-SP Session Border Controller (SBC). The SBC will aggregate all customer VPNs as part of per customer SIP trunks from the serving CUCM clusters. It will also interface, via SIP, the aggregation call control component located in the global AT&T voice network for off-net call purposes.



**Figure 8** VPN Integration

## NAT

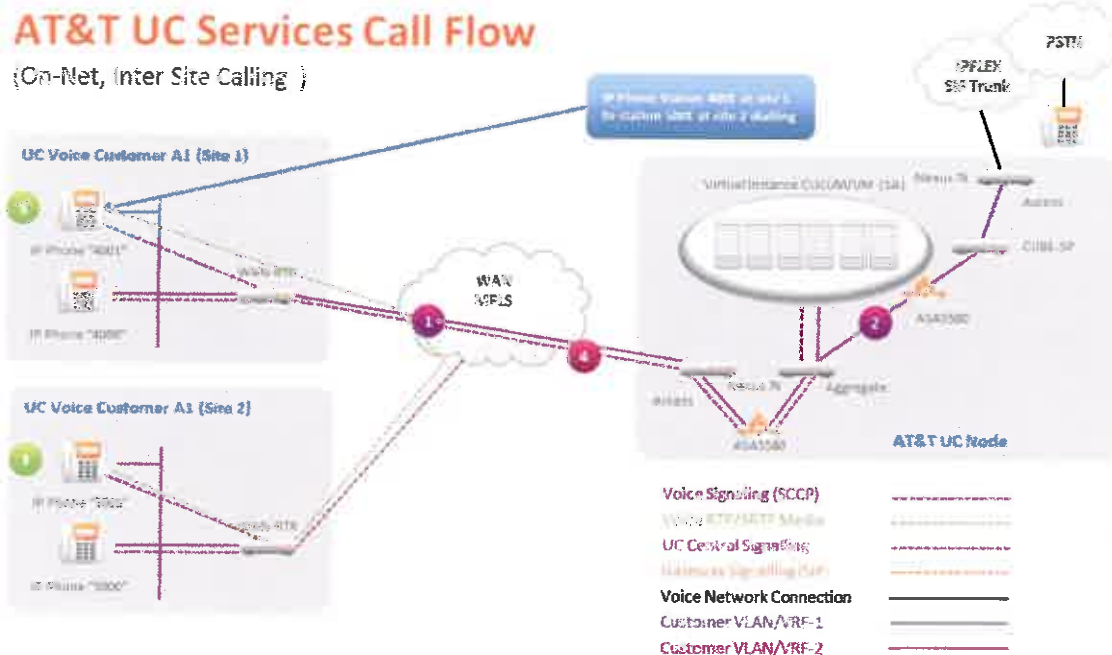
The customer VPN will be extended into the data centers incorporating the UC applications in the customer address space. Since the customer address space may be private address space and may overlap with other customers or AT&T infrastructure, the CUBE-SP will be used as a border element between the AT&T addresses common infrastructure and the customer addressed components. The CUBE-SP will therefore use customer address space for the customer side interfaces and AT&T address space in the AT&T infrastructure, mapping both signalling and media between the two VPN's

It is desirable to optimise media through the most direct route between the end customer IP phone or device and the gateway terminating media at the PSTN access point. If the SBC is located in one data center, then the media will flow via that data center even in the case that both the phone and gateway are both in another location. This is undesirable for reasons of bandwidth and delay, and therefore it is proposed that SBC's may be provided in more than one country in order to reduce the overhead. This requires that the instances of CUCM are able to route calls to the appropriate SBC based on the destination country.

## Call Flows

There are 6 types of basic call flows:

- On-net intra-site VOIP Calls
- On-net inter-site VOIP Calls
- Off-net calls to PSTN / Local Voice Gateway
- Off-net calls to PSTN / Centralized SIP Network
- Call processing in Survivable Remote Site Mode (SRST)
- Access to voice mail from IP Phone

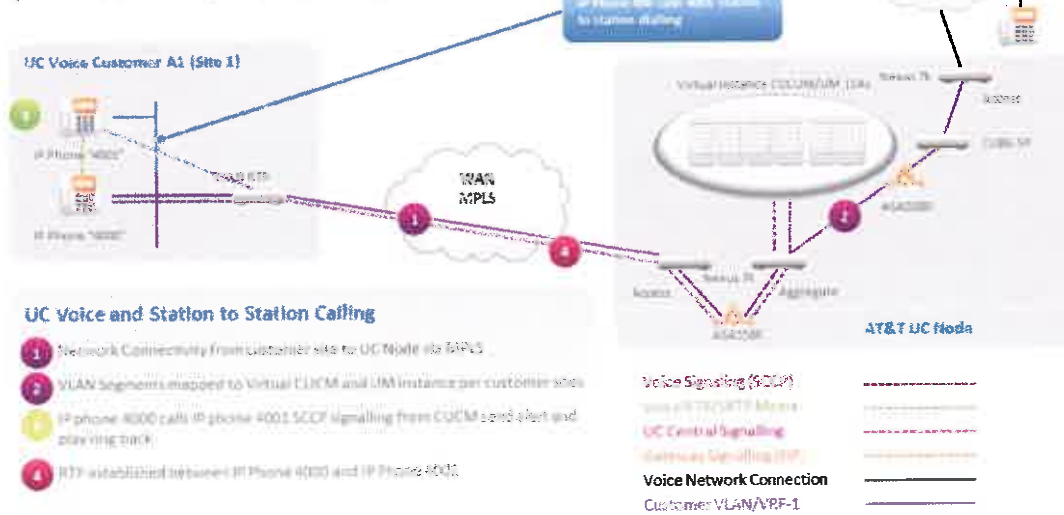


**Figure 9 On-net Inter-Site VoIP Call**

1. Call Control is established between CUCM and end user device via SCCP protocol
2. Device 4001 dials 5001 and SCCP extends information about the called number to CUCM
3. CUCM send alert via SCCP to 5001
4. 4001 and 5001 go off hook and RTP protocol establishes media stream between the two device
5. Device 4001 and 5001 go back on hook and call is disabled via SCCP

## AT&T UC Services Call Flow

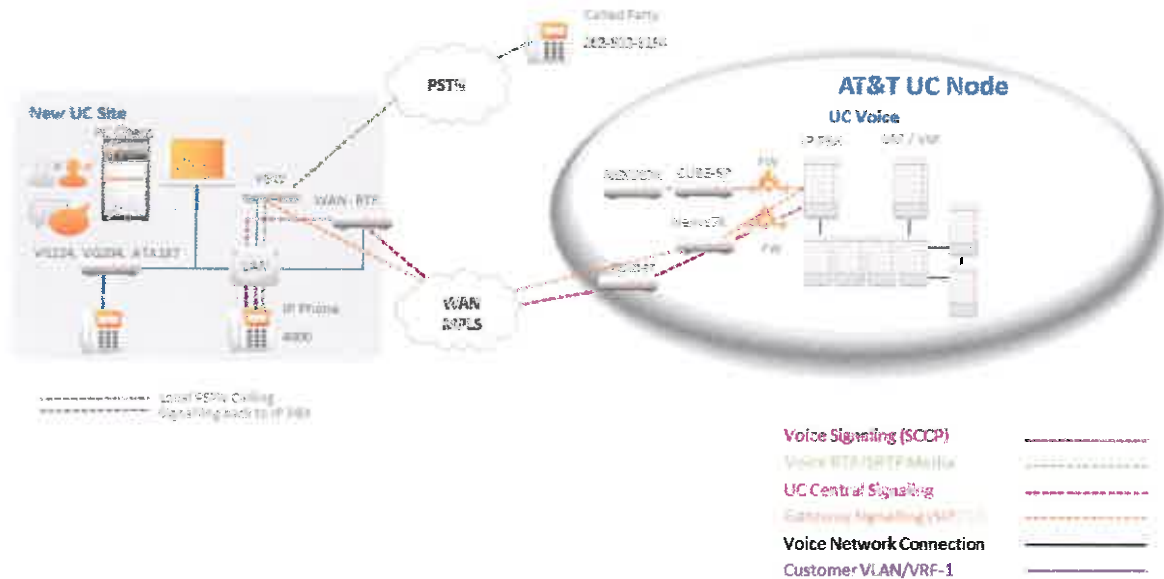
(Station to Station Intra Site Calling)



**Figure 10 On-net Intra-Site VoIP Calls**

1. Call Control is established between CUCM and end user device via SCCP protocol
2. Device 4000 dials 4001 and SCCP extends information about the called number to CUCM
3. CUCM send alert via SCCP to 4001
4. 4001 and 4000 go off hook and RTP protocol establishes media stream between the two device
5. Device 4001 and 4000 go back on hook and call is disabled via SCCP

## AT&T UC Services (Voice Gateway Signaling and Call Flow)



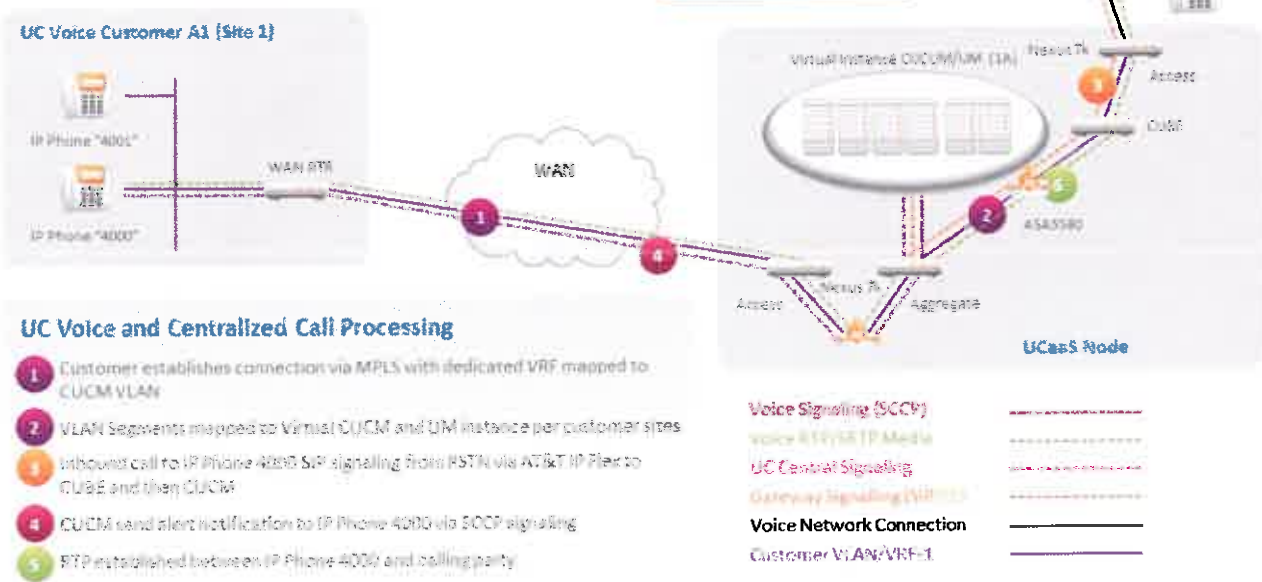
**Figure 11 Off-net calls to PSTN / Local Voice Gateway**

1. Call Control is established between CUCM and end user device
2. SIP Signalling for PSTN access control established between Voice Gateway (VGW)
3. Device 4000 dials off-net PSTN number 262-902-3194 SCCP carries the dial information to CUCM
4. CUCM send SIP signalling to local voice gateway to establish media path between IP Phone and VGW
5. Alerting sent to called party and calling party
6. Device 4000 and 262-902-3194 establish call via RTP and TDM voice path



## UC Services Call Flow

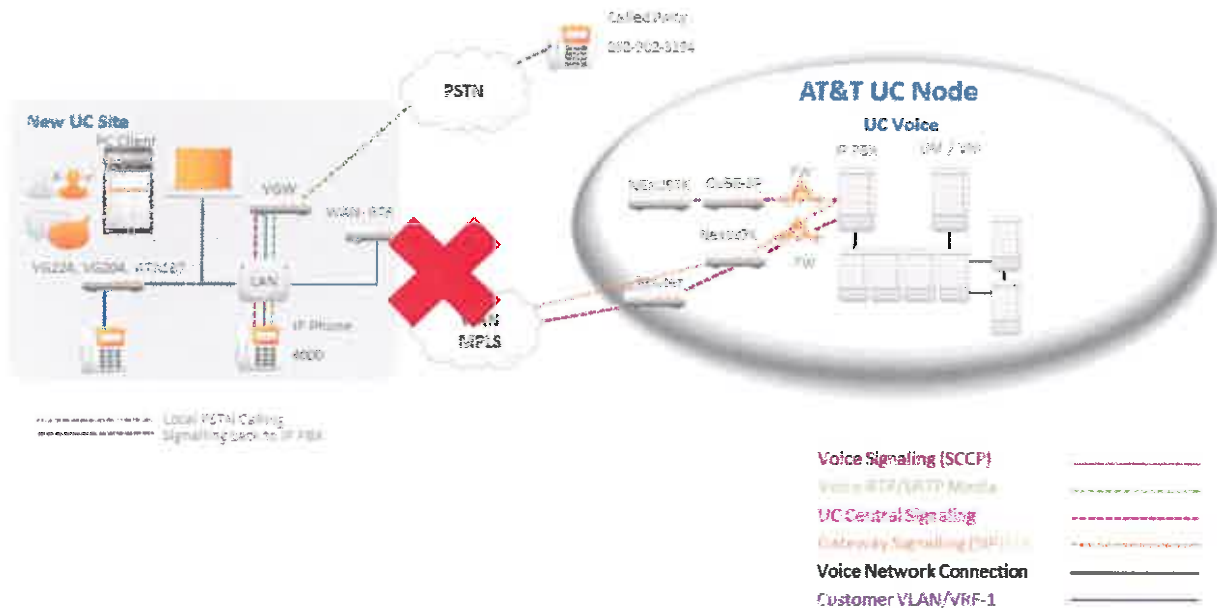
(UC Voice and UC Centralized Call Processing)  
Supporting RTP, SIP Secure TLS



**Figure 12 Off-net calls to PSTN / Centralized SIP Network**

1. Call Control is established between CUCM and end user device
2. SIP signalling for PSTN access control established between carrier and CUBE-SP
3. SIP trunk signalling also established from CUCM to CUBE-SP
4. Device 4000 dials off-net PSTN number 262-902-3194 SCCP carries the dial information to CUCM
5. CUCM send SIP signalling to CUBE-SP to establish media path between IP Phone and CUBE-SP
6. Alerting sent to called party and calling party
7. Device 4000 and 262-902-3194 establish call via RTP and SIP path to carrier

## AT&T UC Services (SRST Call Flows)



**Figure 13 Call processing in Survivable Remote Site Mode (SRST)**

1. Call Control is established between CUCM and end user device disrupted
2. SCCP signalling established between IP Phone and local voice gateway via SRST
3. Device registers with voice gateway
4. Device 4000 dials off-net PSTN number 262-902-3194 SCCP carries the dial information to local voice gateway in SRST mode
5. Voice gateway establishes RTP media path between IP phone and gateway and TDM path to PSTN
6. Alerting sent to called party and calling party
7. Device 4000 and 262-902-3194 establish call via RTP path to carrier



## Lawful Intercept

Lawful Intercept is the process by which law enforcement agencies (LEAs) conduct electronic surveillance as authorized by judicial or administrative order. Increasingly, legislation is being adopted and regulations are being enforced that require service providers (SPs) and Internet service providers (ISPs) to implement their networks to explicitly support authorized electronic surveillance. The types of SPs or ISPs that are subject to LI mandates vary greatly from country to country. LI compliance in the United States is specified by the CALEA.

SPs and ISPs are required to meet LI requirements for voice and data in a variety of countries worldwide. Communications Assistance for Law Enforcement Act (CALEA) is a public law that describes how telephony service and broadband access providers in the United States must support LI. In Europe there are a number of similar laws, including the Regulation of Investigatory Powers Act (RIPA) in the United Kingdom, the Telecom Act/Telekommunikations Überwachungsverordnung (TKUV) in Germany, the Telecom Act in France, the Criminal Code in Italy, and the Telecom Act in the Netherlands. Legal requirements and specific interfaces vary from country to country. Four specifications define the interface to the LEAs for the purposes of meeting the CALEA requirements:

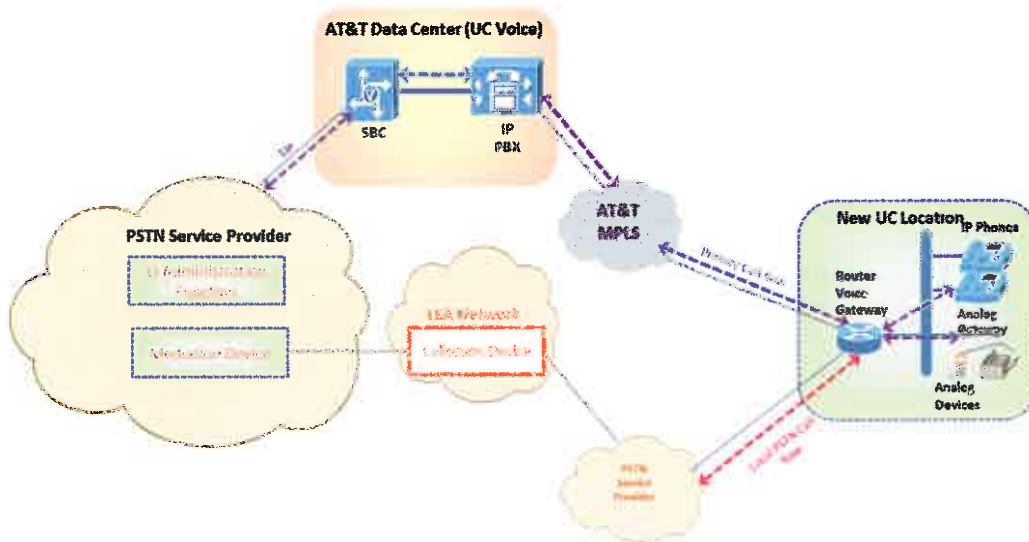
- The *Telephone Industry Association Lawfully Authorized Electronic Surveillance* standard developed by the Telephone Industry Association (TIA).
- The *PacketCable Electronic Surveillance Specification* standard.
- The *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technology in Wireline Telecommunications Networks* and *Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services* standards developed by American National Standards for Telecommunications.

Cisco supports two architectures for LI: PacketCable and Service Independent Intercept. The LI components by themselves do not ensure customer compliance with applicable regulations but rather provide tools that can be used by SPs and ISPs to construct an LI-compliant network.

UC Voice is classified as a hosted dedicated IP PBX and therefore not providing the circuit switched network.

PSTN access and the carrier switched network is order separately from the local carrier and therefore the responsibility for support of Lawful Intercept based on where the wire tap is invoked is provided and responsibility lies with the selected provider of PSTN carrier network. AT&T however can provide support when required to interact with the LEA when required to setup packet capture application to aid in the support of law enforcement utilizing supported third party applications that have been certified by Cisco.

High level view of Lawful Intercept Interaction with PSTN service provider and UC Voice provided defines the connectivity of the LEA network and collection device interaction with the PSTN service provider. Call intercept takes place at the PSTN service provider providing the SIP trunk and at the local PSTN level into provided voice gateways.



16

## Number portability

This will be provided by the Circuit Switched network via SIP trunks and local PSTN access and voice gateways as required. Number porting is a function of regulated services and must be order separately by the customer via third party or AT&T.

## Supplementary Voice Service

- Call Forward No Answer
- Call Park
- Call Transfer (Blind, Consultative)
- 3 Way Conference Call
- Call Waiting
- Call Hold/Resume
- Caller Line ID
- Extension Mobility

## Video Telephony

Intra Enterprise (ptp video) using, Cisco 9971, 9951 with video camera bolt on

## Unified Messaging

- Listening to Voice Message from Email
- Read Email Messages from VOIP Phone
- CFNA to VM
- Retrieving VM from PSTN
- Retrieving VM from Mobile phone



Retrieving VM from Phone Display  
Manage personal greetings

## Mobility Services

SNR (Single Number Reach)  
SNR: Desk Phone Pickup  
SNR: Remote Destination Pick Up  
Mid call transfer  
Mid Call Conference  
Mid Call Hold/Resume  
Call Park  
MWI Notification on the SIP Phone  
Dual Mode Mobility client (iPhone, Nokia)

## Presence

Services Use Cases  
Presence info (availability/location/phone status)  
Presence info change (availability/location/phone status)  
Click to Call  
Instant Messaging  
Telephone Status

## Call Detail Reporting

CUCM will provide Call Detail Reports (CDR) as required in .csv format to support requests for billing and call tracking. Support for malicious calltrace, 911 call placement and voice gateway calls are captured as part of the CDR records in Cisco Unified Communications Manager (CUCM). The CUCM is the hosted dedicated IP PBX. The raw CDR information data is provided to the customer for placement and analysis by the customer provided CDR analysis tool. The customer provided CDR tool extracts the raw data by way of SFTP protocol to ensure secure transfer of data. Any raw CDR data on the CUCM is secure via two part authentication with restricted access to only select AT&T UC service support team members. AT&T retains the data on CUCM for 30 days. Long term retention of CDR data is the responsibility of the customer.

## Emergency Services

### Compatibility of IP Phones with 911 capabilities.

*Please read this notice concerning compatibility of IP Phones with 911 capabilities.*

Two general areas of concern exist regarding the implementation and operation of 911 capabilities in an IP Telephony environment. The first is powering of the phone set and supporting systems and the second is routing and information exchange for processing a 911 call with accuracy.

(a) Many digital, ISDN and IP phone sets and related equipment, including the AT&T CPE provided as part this service require electrical power to operate. Customer should determine whether and how to include Uninterruptible Power Supply (UPS) devices in support of Customer's IP telephony environment to maintain electrical power during a commercial power outage. **THE FAILURE TO USE UPS PROTECTION PROPERLY MAY AFFECT USERS' ABILITY TO REACH 911.**

(b) Customer must have in place and maintain IP telephone gateways, a well-designed dialing plan, and backup Call Server support for accurate Emergency 911 call processing. Where only basic 911 service is available (enhanced 911 service is not available in all areas in the United States), Customer may be required to have a local IP telephony gateway at each site as well as a dialing plan that uses the local gateway for 911 calls. **OTHERWISE, THE 911 OPERATOR MAY NOT BE ACCESSIBLE OR THE CALL MAY BE ROUTED TO AN INCORRECT 911 OPERATOR.**

(c) If E911 service is available in Customer's area, it offers the capability to provide to the 911 operator the geographic location of the remote user. Customer must equip the IP Telephony gateway with an ISDN Primary Rate Interface (PRI) voice port, or a Foreign Exchange Office (FXO) port with an external Centralized Automatic Message Accounting (CAMA) translator box (or equivalent) to utilize the E911 functionality. Customer also must maintain a location database that maps the calling party telephone number to the physical location of the calling party (i.e., building/floor/room). The E911 system will use this database to provide location information to the 911 operator. The use of ShoreTel IP Telephony applications may require additional configurations to correctly implement E-911. **OTHERWISE, THE 911 OPERATOR MAY NOT BE ACCESSIBLE OR INCORRECT LOCATION INFORMATION MAY BE PROVIDED TO THE 911 OPERATOR.**

### C. Customer Responsibility and Indemnity.

(a) Customer is solely responsible for determining whether to equip their IP Telephony system with the functionality described within the SDD at its own expense. Customer is solely responsible for maintaining the location database and any other applicable configuration parameters, and for updating such database and parameters as may be necessary whenever the physical location of an IP Phone changes. Customer may be required by state law to purchase equipment or maintain databases to provide user-specific location information. Neither AT&T nor Cisco Systems can advise Customer as to what the legal obligations are in this respect. Customer should consult their attorney.

(b) Customer will indemnify, defend and hold harmless AT&T, its subcontractors (including ShoreTel Systems), their Affiliates and the employees of each of them against any all claims or losses based on any error affecting 911 functionality.

AT&T UC Voice is a hosted dedicated IP PBX and the services provided include the support for the core Cisco infrastructure defined in this SDD. 911 and E911 services with support of PS ALI are not included in the services and must be established with the PSTN provider as part of the contracting for regulated services. UC Voice support team will configure the dial plan attributed that will allow for calls to be placed to emergency services across the PSTN service provider network. The customer will work directly with the PSTN provider to define the location of end user and locations. AT&T as part of the test plan will confirm that emergency service calls are functioning prior to going into final production mode. AT&T UC support team will work with the PSTN service provider to correct any issues related to call failure as part of the test and trun up process. AT&T services assurance and service delivery team along with support from assigned project management will define the testing and confirm functionality prior to go live and perform periodic testing with PSTN service provide to ensure emergency services are operational. Testing should be conducted once a year as well as after any change to PSTN access or gateway replacement takes place.

## Contingency Planning

The Contingency Plan establishes procedures to recover the UC Voice System following a manmade or natural disruption. UCV-FED primary site is in Watertown IDC and plans in place to build an alternate site in Allen IDC. The following objectives have been established for this plan:

Maximize the effectiveness of contingency operations through an established plan that

Consists of the following phases:

- Notification/Activation phase to detect and assess damage and to activate the plan
  - Perform initial impact assessment answering the questions, who, what, where, why and how long
  - Determine if contingency plan need to be activated
  - Access internal/external partner/vendor list
  - Establish Command and Control for the organization
  - Review UCV-FED customer list(Geo Redundancy vs Non Geo Redundancy)
  - Assign someone to create an event log
  - Track Impact assessment information categories:
    - Customers
    - Network
    - Property
    - Platform and application
    - External factors if applicable
  - Provide information from the outage assessment to stakeholders
  - Notify internal/external vendors critical to restoration of service/system
- Recovery phase to restore temporary IT operations and recover damage done to the Original system
  - Identify Recovery location – Primary or Alternate location
  - Identify required resources to perform recovery procedures
  - Retrieve backup and system installation information
  - Implement failover operational plan
  - Confirm all UCV-Fed customers are operational at alternate site
  - Restore system capability
  - Restore damage as applicable
  - Resume operational capabilities
- Reconstitution phase to restore IT system-processing capabilities to normal operations.
  - Identify the activities, resources, and procedures needed to carry out UC services Processing requirements during prolonged interruptions to normal operations.
  - Assign responsibilities to designated UC Support team personnel and provide guidance For recovering during prolonged periods of interruption to normal operations.
  - Ensure coordination with other staff who will participate in the Contingency planning strategies. Ensure coordination with external points of contact and Vendors who will participate in the contingency planning strategies.

## UC Node Redundancy

The AT&T UC Node provides multiple levels of redundancy. All major hardware is deployed in a redundancy pair.

- UC Node Hardware

- UCS and Virtualization infrastructure – blades, chassis, SAN switching, and SAN storage
- UC applications are spread across blades, chassis
- ASA Firewalls deployed in redundancy pair
- ASR-1004 routers running CUBE-SP in redundancy mode
- Nexus 7010 layer 2/3 switching configured with cross connect and shared VLANs across platforms
- VMware Features - addresses node and virtual machine failures
  - VMware HA: Restart of an application in the case of host hardware failure.
  - Data Recovery : Centralized management for virtual machine backup and recovery
- UC Applications
  - UC utilizes current best practices for CUCM clustering architecture with Active and Standby Subscribers databases per customer, Clustering-over-WAN
  - Each customer CUCM application instance is built across at least two UCS 5108 chassis with a minimum of three CUCM instances in a standard Publisher and two subscriber CUCM model spread across multiple B200 blades
  - Unity Connection providing voice mail is also established utilizing two virtual instances spread across two UCS 5108 chassis and B200 blades.

## CUCM Cluster Design

AT&T Utilizes Cisco best practices for deployment of Cisco Unified Communications Manager (CUCM) and Unity Connection for voice and voicemail services

### Publisher

The publisher is a required server in all clusters, and as shown in Figure 14 there can be only one publisher per cluster. This server is the first to be installed and provides the database services to all other subscribers in the cluster. The publisher server is the only server that has full read and write access to the configuration database.

On larger systems with more than 1250 users, Cisco recommends a dedicated publisher to prevent administrative operations from affecting the telephony services. A dedicated publisher does not provide call processing or TFTP services running on the server. Instead, other subscriber servers within the cluster provide these services.

The choice of hardware platform for the publisher should be based on the desired scale and performance of the cluster. Cisco recommends that the publisher have the same server performance capability as the call processing subscribers. Ideally the publisher should also be a high-availability server to minimize the impact of a hardware failure.

## Subscriber

During installation of the Unified CM software, you can define two types of servers, publisher and subscriber. These terms are used to define the database relationship during installation. When the software is installed initially, only the database and network services are enabled. All subscriber nodes subscribe to the publisher to obtain a copy of the database information. However, in order to reduce initialization time for the Unified CM cluster, all subscriber servers in the cluster attempt to use their local copy of the database when initializing. This reduces the overall initialization time for a Unified CM cluster. All subscriber nodes rely on change notification from the publisher or other subscriber nodes in order to keep their local copy of the database updated.

As shown in Figure 15 multiple subscriber nodes can be members of the same cluster. Subscriber nodes include Unified CM call processing subscriber nodes, TFTP subscriber nodes, and media resource subscriber nodes that provide functions such as conferencing and music on hold (MoH).

## Call Processing Subscriber

A call processing subscriber is a server that has the Cisco Call Manager Service enabled. Once this service is enabled, the server is able to perform call processing functions. Devices such as phones, gateways, and media resources can register and make calls only to servers with this service enabled. As shown in Figure 14 multiple call processing subscribers can be members of the same cluster. In fact, Unified CM supports up to eight call processing subscriber nodes per cluster.

Each call processing subscriber node in a cluster requires its own server license in order to enable the Cisco Call Manager Service on that subscriber node. The Cisco Call Manager Service cannot be enabled on a server if the publisher is not available because the publisher acts as a licensing server and distributes the licenses needed to activate the Cisco Call Manager Service.

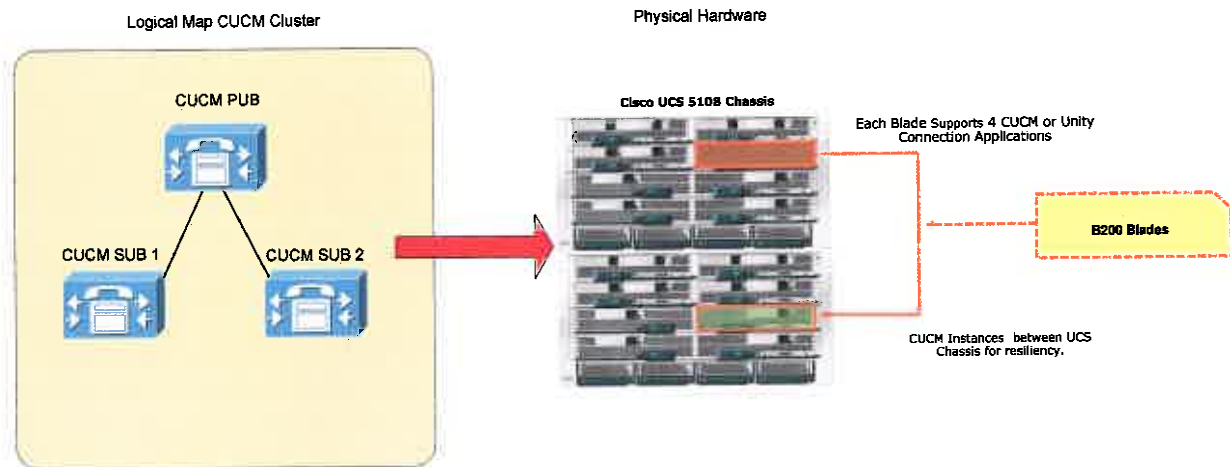
## TFTP Subscriber

A TFTP subscriber or server node performs two main functions as part of the Unified CM cluster:

- The serving of files for services, including configuration files for devices such as phones and gateways, binary files for the upgrade of phones as well as some gateways, and various security files
- Generation of configuration and security files, which are usually signed and in some cases encrypted before being available for download

The Cisco TFTP service that provides this functionality can be enabled on any server in the cluster. However, in a cluster with more than 1250 users, other services might be impacted by configuration changes that can cause the TFTP service to regenerate configuration files. Therefore, Cisco recommends that you dedicate a specific subscriber node to the TFTP service, as shown in Figure 14 for a cluster with more than 1250 users or any features that cause frequent configuration changes.





**Figure 15 CUCM Cluster Design**

## Alternate Site Redundancy

AT&T will utilize a second UC node to provide alternate site redundancy in order to recover from manmade or natural disasters. A connection from the customers Wide Area Network WAN network is required to be established into each UC node. The primary UC node is located in Watertown, MA and the secondary UC node will be located in Allen, Texas. Singapore, Japan and UK and Amsterdam nodes are linked via and AT&T backbone network. The backbone network is reserved for extending and backing up customer data between the two UC nodes and for access by AT&T support resources for testing. All customer media and signaling traffic flows through the customer provided network transport. The CUCM application pushes information down to each IP phone defining the primary, secondary and local Survivable Remote Site (SRST) gateway that also can provide on premise backup in addition to the primary and secondary UC nodes.

A keep alive, for the purposes of this document, is a TCP/SCCP packet sent from a phone to one or more CUCM nodes to which it is configured to register and communicate.

These keep lives are used by the phone for a couple of different reasons. First, the keep lives ensure that the TCP link to the CUCM node(s) is still viable. Second, the keep alive ensures that the Cisco Call Manager (CCM) Service is still functional, and able to process the phone's call control needs, and requests. While these may seem to be one in the same, they are actually slightly different in functionality, but both are obviously important with the SCCP connection to the CCM Service being reliant upon the TCP connection being connected for success. The implication of keep alive failure to either of these processes will be discussed in greater detail later on in this document.

By default, SCCP phones send a keep alive to their primary CUCM server every 30 seconds and to their failover node, which is the second node listed in the phone's Call Manager (CM) Group, every 60 seconds. The primary node will respond with a keep alive ACK confirming that both the TCP connection and the SCCP connection are both still valid. Alternatively, if the CCM Service on the primary node is down, the TCP connection may be ACK'd, but the SCCP aspect of the keep alive would not. This type of a response would signal to the phone that the TCP stack on the CUCM is still able to respond to inbound traffic, however the CUCM does not appear to be able to process calls at this time. Additionally, if the TCP

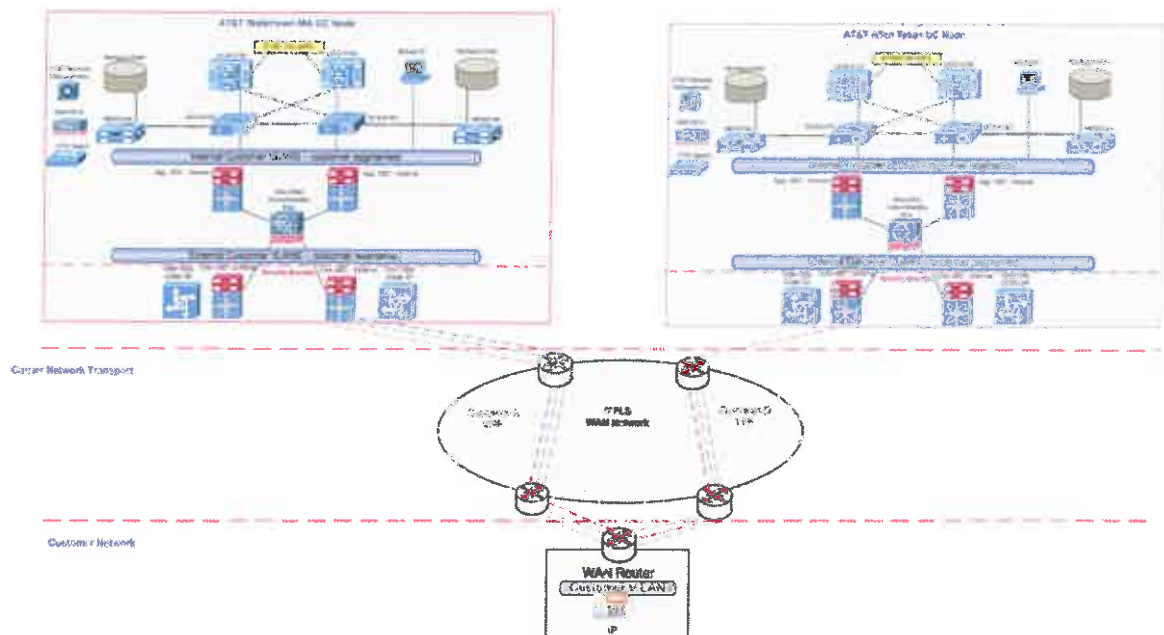
connection fails to respond, then the phone quickly recognizes that the link is broken and the failover process begins.

Cisco IP phones also send a SCCP keep alive to their secondary node. This is done to maintain and monitor a TCP connection between the phone and the secondary CUCM in order to facilitate a prompt and reliable failover should the need arise. The secondary CUCM, however, does not have a SCCP connection (as the phone has not registered to the secondary node at this point) and will therefore only ACK the TCP connection in response to the SCCP keeps alive sent by the phone.

## Failover Prerequisites

AT&T provides redundancy capabilities by supporting a split cluster capability that allows for an instance of the customer CUCM, Unity Connection applications to be built out in both Watertown, MA and Allen, TX nodes. Once the end IP Phones detect that they cannot reach the primary UC node the devices will automatically register to the secondary UC node. The CUCM and Unity cluster instances maintain real time updates between both nodes as all times. This action can take place when the following occurs:

- Loss of network connectivity from the customer provided WAN to the UC node
- Primary UC node is incapacitated by natural or manmade outage
- Primary UC node CUCM and Unity hardware or application failure



## Alternate Site Description

The Alternate site located in Allen, TX is maintained by the same support team utilized to support the FISMA platform in Watertown. The current Allen, TX location provides support for other customers as an alternate site. The current Allen, TX location is monitored and maintained by the same UC support team that will be maintaining the Watertown, MA FISMA platform. The same access control and security processes are utilized in Allen, TX today. The hardware deployed is also the same as the Watertown location with the exception being that there is more capacity at the Allen, TX location.

The diagram in figure 16 provides high level on the equipment that is in place today providing alternate site support. AT&T will be constructing a second FISMA platform in Allen, TX in 2014. The second FISMA platform will be constructed to be a complete replica in capacity and hardware to what is deployed in Watertown, MA today.

### ***Figure 16 Alternate Site Allen Texas***

The UC Node as it is deployed today with additional capacity and hardware.

### ***Figure 17 Enterprise UC Node Backup Scenario***

## Software Versions Watertown, MA and Allen, TX

**Table 1 Software Versions**

Device Name	Function		Software Version
<b>UC Applications</b>			
CUCM	Call Control		11.X
Unity Connection	Messaging		11.X
CUPS	Presence		11.X
<b>Customer Premises</b>			
Cisco 2800, 2900, 3900 series	On Premise SRST Gateway		15.1(1)T
<b>Service Fulfillment</b>			
VSX	Service Management Layer		1.0.1
DXSI	Management Integration Layer		8.4.1
vCenter	VM Provisioning Domain Manager		ESXi 5.X
USM	Provisioning Management		7.3
<b>Jump Server</b>			
HP DL 380	Remote Access Control		RHEL 5.9
FMS	SAN Switch Monitoring		5.0(1a)
DCNM	DC Switch Monitoring		5.0(3a)
vCenter	Virtual Machine Monitoring		ESXi 5.0
UCSM	Computing Infrastructure Monitoring		Latest 1.3(1)
CUSM	Call Quality Monitoring		8.6
CUOM	UC Application Monitoring		8.6
<b>Infrastructure</b>			
UCS 5108	Blade Server Chassis		Latest 1.3(1)
UCS U2104Xp	Fabric Extender		Latest 1.3(1)
UCS 6296XP	40 Port Fabric Interconnect		Latest 1.3(1)
UCS B6620-1: B200 M1	Server Blades		Latest 1.3(1)
VMware ESXi	Virtual Host		ESXi 5.0 (build 258902)
Nexus 7010	Collapsed distribution/core switch		n7000-s1-dk9.5.0.3.CCO.bin
Nexus 1000v or vSwitch	Virtual Access Switch		4.0(4)SV1(3b)
Cisco MDS 9148	SAN Switch		5.0.1a

Device Name	Function		Software Version
NetApp	FC Storage Area Network		SW-3270AONTAP8-C
<b>Aggregation</b>			
CUBE-SP	Aggregation SBC		03.01.00.S.150-1.S
ASR 1004	Router Platform for CUBE-SP		15.1
<b>Security</b>			
ASA-5580, 5510	Firewall		8.3(1)
IPS-4270	IDS		8.3(1)
<b>Monitoring/Management</b>			
Dell Power Edge (Vizgems)	SNMP Pulling and Trap Collection		RHEL 5.9
VMWare UCS B200 blade Solar Winds	SNMP Pulling, Voice Quality Monitoring, R Factors and Trap collection		<ul style="list-style-type: none"> <li>Network Configuration Manager – 7.0.2</li> </ul> OS-Windows Server 2008 R2 SP1,

## Remote Access

VPN access for support from vendors and or remote work staff shall be provide through dedicated ASA 5510 firewalls defined with specific source and destination access control lists. The ASA 5510 shall be separate from ASA-5580 firewalls providing customer security and segmentation

## Naming Convention

The following naming convention will be applied to all equipment and will define the equipment type, site location and sequential number.

Example: Nexus 7010 located in the Watertown, MA UC Node would be defined as follows:

*Device Name – Location-Sequential Number*

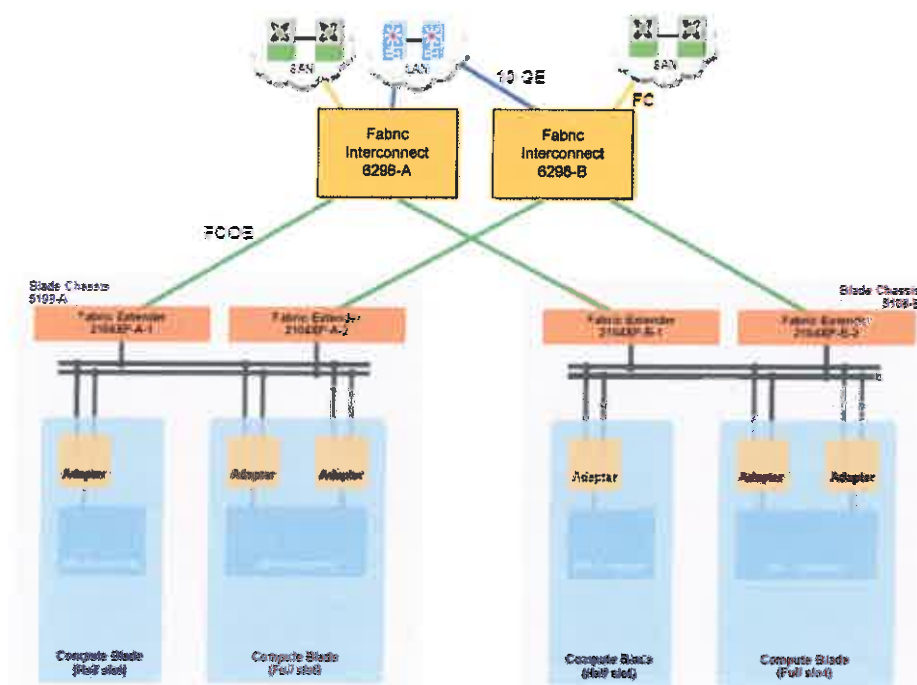
Device Information defined in command line = Nexus-7010-WT-1



# UCS-5108 Architecture

## General Overview

The picture below depicts the general architecture of UCS-5108 Chassis and SAN environment.



**Figure 18 UCS Logical Connectivity**

Inside the UCS 5108 chassis, are half slot B200M1 blades which are interconnected internally to two fabric extenders for redundancy purposes. Each fabric extender is connected to one fabric interconnect via one to four FC links. There are two fabric interconnects for redundancy purposes, each communicating with the SAN and LAN clouds.

To cope with blade chassis failure, a second chassis is introduced in a similar fashion. Cisco UCS is typically deployed in a High Availability clustered configuration for management plane redundancy and increased data plane bandwidth.

## UCS Hardware/Firmware

The table below lists the components that are deployed in the Watertown UC Node data centers.

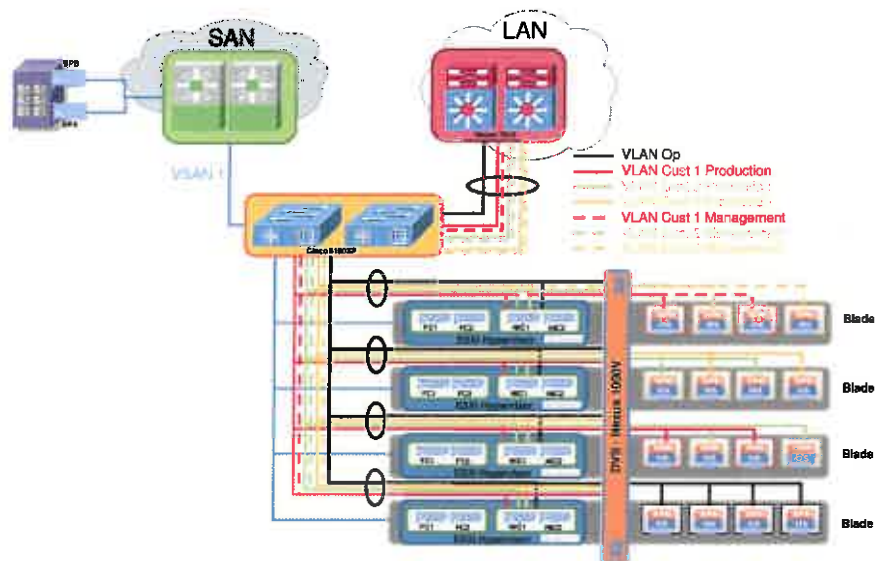
**Table 2 UCS Hardware/Firmware**

Cisco Device Name	Description	
<b>UCS Blade</b>		
N20-B6625-1	UCS B200 M2 Blade Server w/o CPU, memory, HDD, mezzanine	
A01-X0109	2.66GHz Xeon E5640 80W CPU/12MB cache/DDR3 1066MHz	
N01-M308GB2-L	8GB DDR3-1333MHz RDIMM/PC3-10600/dual rank/Low Voltage	
A03-D073GC2	73GB 6Gb SAS 15K RPM SFF HDD/hot plug/drive sled mounted	
N20-AC0002	UCS M81KR Virtual Interface Card/PCIe/2-port 10Gb	
N20-BHTS1	CPU heat sink for UCS B200 M1 Blade Server	
<b>UCS 5108 Chassis</b>		
N20-C6508	UCS 5108 Blade Server Chassis/0 PSU/8 fans/0 fabric extender	
N20-I6584	UCS 2104XP Fabric Extender/4 external 10Gb ports	
N20-PAC5-2500W	2500W power supply unit for UCS 5108	
SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter	
CAB-AC-2500W-US1	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	
<b>UCS Fabric Interconnect</b>		
N10-E0440	4-port 10 GE/4-port 4Gb FC/Expansion module/UCS 6100 Series	
N10-PAC2-750W	750W power supply unit for UCS 6140XP/100-240VAC	
N10-L001	UCS 6100 Series Fabric Interconnect 1 10GE port license	
DS-SFP-FC4G-SW	4 Gbps Fibre Channel-SW SFP, LC	
SFP-10G-SR	10GBASE-SR SFP Module	
N10-SACCB	Accessory kit for UCS 6140XP Fabric Interconnect	
N10-MGT005	UCS Manager v1.3	

# UCS Connectivity

## SAN

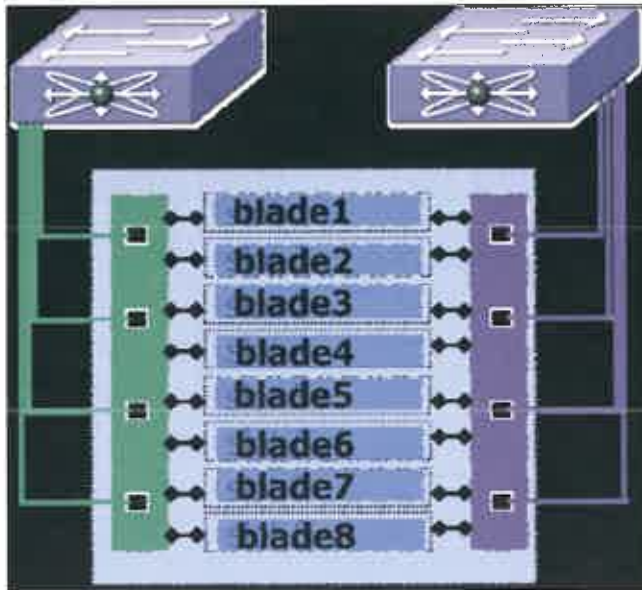
All VLANs will be trunked to each blade so that all VLANs are extended to the blade's DVS but only specific VLANs are connected to each application as required.



**Figure 19 UCS and ESXi Connectivity**

Note: If two IP addressing spaces are used per customer (one owned by the customer for the UC applications, one owned by AT&T for the UC management), there will be two VLANs per customer. Each customer has one production VLAN (for CUCM, CUCxn, CUP) and one management VLAN (CUOM).

To ensure the maximum throughput to the blade, 4 FCOE links will make the connectivity between the I/O module and fabric interconnect. Those links carry fibre channel and LAN traffic.



**Figure 20 Blade Connectivity**

The distribution of blades per FC uplink will be done dynamically. One fabric extender will be used as primary and one as secondary should the internal connection from the blade to primary fabric extender fail.

## LAN

### Ethernet End Host Mode

A UCS Fabric Interconnect operating in End Host Mode is called an EH-node. An EH-node appears to the external LAN as an end station with many adapters.

An EH-node has two types of ports (by configuration)

1. Border port (can be port channel) : connect to upstream L2 network
2. Server port: connect to servers

The EH-node does not participate in STP on the border ports, hence it reduces the scale of STP control plane.

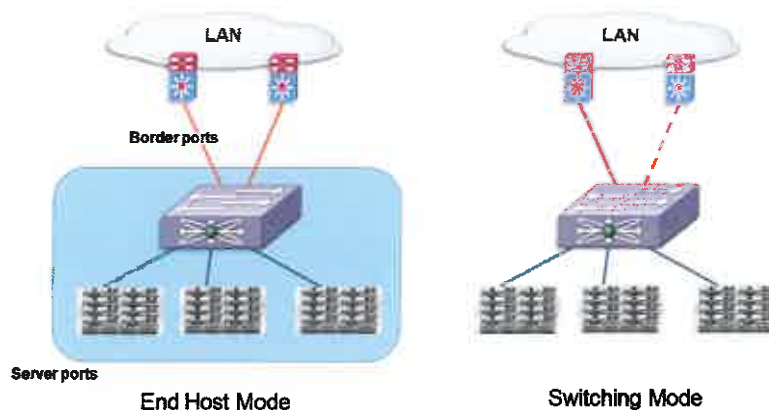
Traffic CANNOT be forwarded between border ports.

End-host mode is the default Ethernet switching mode, and should be used if either of the following are used upstream:

- Layer 2 switching for L2 Aggregation
- Virtual Switching System (VSS) aggregation layer

Switch mode is the traditional Ethernet switching mode. The switch runs STP to avoid loops, and broadcast and multicast packets are handled in the traditional way. Switch mode is not the default Ethernet switching mode, and should be used only if the switch is directly connected to a router, or if either of the following is used upstream:

- Layer 3 aggregation
- vLAN in a box



**Figure 21 Ethernet Mode**

The Ethernet mode used in HCS is the end host mode.

## Uplinks

The enabled Uplink Ethernet ports in UCS 6100 series switch are used to forward traffic to the next layer in the network.

## VLAN

In the Cisco UCS, a named VLAN creates a connection to a specific external LAN. The VLAN isolates traffic to that external LAN, which includes broadcast traffic. The name that you assign to a VLAN ID adds a layer of abstraction that you can use to globally update all servers associated with service profiles that use the named VLAN. You do not need to reconfigure servers individually to maintain communication with the external LAN.

Four options are available if two 6296 switches are configured in cluster:

- Global
- Fabric A only
- Fabric B only
- Both fabrics different destinations

**Note:** VLANs with IDs from 3968 to 4048. These VLAN IDs are reserved.

AT&T will use global VLANs.

## Cluster

To use the cluster configuration, two UCS 6296 Series Fabric Interconnects must be directly connected with Ethernet cables between the L1 (L1-to-L1) and L2 (L2-to-L2) ports, allowing the two UCS 6296 Series Fabric Interconnects to continuously monitor the status of each other for immediate alert of failure.

If one UCS 6100 Series Fabric Interconnect becomes unavailable, the other UCS 6296 Series Fabric Interconnect automatically takes over.

## Server Management IP Address Pool

One management VLAN should be defined with 11 consecutive IP addresses (1 per fabric interconnect, 1 shared between fabric interconnect, 1 per blade).



The Server Management IP Address Pool is used to assign external IP addresses to each of the blade servers installed. The Cisco UCS Manager uses the IP addresses in a management IP pool for external access to a server through the following:

- KVM console
- Serial over LAN
- IPMI

Note: The IP addresses are assigned to the blades by the system. Currently there is no mechanism available to hard code an IP address to a particular blade.

## UCS Configuration Guidelines

We will create 1 service profile template to handle the ESXi setup. LAN and SAN connectivity will be also provided thus adapter template. The hardware virtualization will require several pools of addresses (UUID, Mac address, WWNN, WWPN).

### UUID

The UUID is a 128bit number (32 hex digits, 16 groups of 2 hex digits) and defines the server itself. This is not the same as the serial number of the server. It is often associated with the “motherboard” of the server. There is a prefix and suffix component to this identifier. There are no rules or restrictions for this string outside of duplication which must be checked by the CMDB database. You can enter text letters limited to ABCDEF and numbers between 0-9 for either the prefix or suffix.

The final UUID string is a combination of the prefix and suffix. A suggested method is to use a company naming convention that possibly reflects geography and roles of the blade.

It is not recommended to use HW UUID's for servers. Use UUID pools. This lends better to stateless compute and service profile migration. You can also use a UUID suffix pool. Cisco UCS Manager automatically generates a unique prefix so that you are guaranteed a unique UUID for each logical server.

### MAC ADDRESS

This is the well-known hardware address of the NIC on the system.

AT&T will create two different pools of MAC addresses one for each fabric interconnect (A and B). These pools can later be used to feed the two vNIC templates that one could create for each fabric.

Cisco pre-populates a critical part of the OUT which is registered to Cisco. It is recommended to use a convention that makes the fabric delineation obvious (A,B).

### WWNN and WWPN

The node name uniquely identifies a communicating object in Fibre channel fabric. This is the parent object for the end ports that send and receive FC frames. UCS assigns a unique to the Converged Network Adapter (CNA) itself. The best practice for both WWNN and WWPN is to keep the first octet as “20” or “21” thus properly identifying the host as an initiator in the FC SAN.

Each port of the CNA gets assigned a WWPN to allow its unique identification on the fabric. UCS CNAs are dual ported so it is recommended to create two pools of WWPNs for each fabric. This allows easy identification which WWPN is engineered to which fabric in steady state operations.

## WWNN

A WWNN (World Wide Node Name) pool is one of two pools used by the Fibre Channel vHBAs in the UCS. You create separate pools for WW node names assigned to the server and WW port names assigned to the vHBA. The purpose of this pool is to assign WWNNs to servers if a pool of WWNNs is included in a service profile; the associated server is assigned a WWNN from that pool.

The use of the Cisco OUI (25:B5) is needed because without it, the MDS switch rejects the WWNN/WWPN. In UCS release 1.0(2d) and above, the Cisco OUI been populated to help alleviate errors.

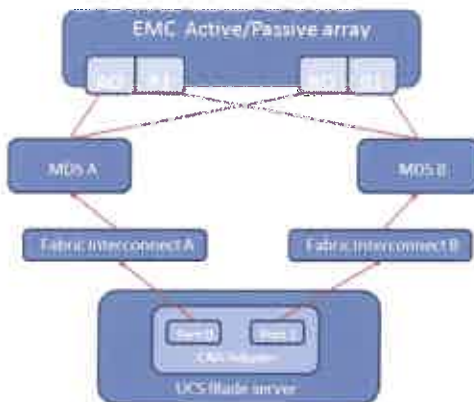
## WWPN

A WWPN (World Wide Port Name) is the second type of pool used by the Fibre Channel vHBAs in the UCS. The purpose of this pool is to assign WWPNs to the vHBAs. If a pool of WWPNs is included in a service profile, the associated server is assigned a WWPN from that pool.

The use of the Cisco OUI (25:B5) is needed because without it, the MDS switch rejects the WWNN/WWPN. In UCS release 1.0(2d), the Cisco OUI been populated to help alleviate errors.

## Boot Policies

The storage array has an active/passive interfaces and also have the concept of trespass which allows failure of paths to be seamless and all the advantages of multi-pathing and failover. The array has one path active for a given time, the other path is passive. This calls for zoning one initiator each from SP-A (port 0 and 1) and one initiator from SP-B (port 0 and 1) as shown in the picture below.



**Figure 22 SAN Boot Policy**

Each service profile will contain 2 HBA interfaces which will have primary and secondary bootable SAN group. We will define two different port groups in each group. This would give the most resilient configuration and guard against any failure on the paths.

## Management Policies

The management policy groups all the mechanisms available for remote access to the blade. It includes IPMI, SOL and KVM console.

For our purposes, we will use only the KVM console and SOL access. A pool of 11 IP addresses will be created to allow those access paths. These addresses must be in the same VLAN as the management interface (mgmt0) of the fabric interconnect.

SOL access will also require a TTY running at the OS level. ESXi hypervisor should have this tty enabled by default.

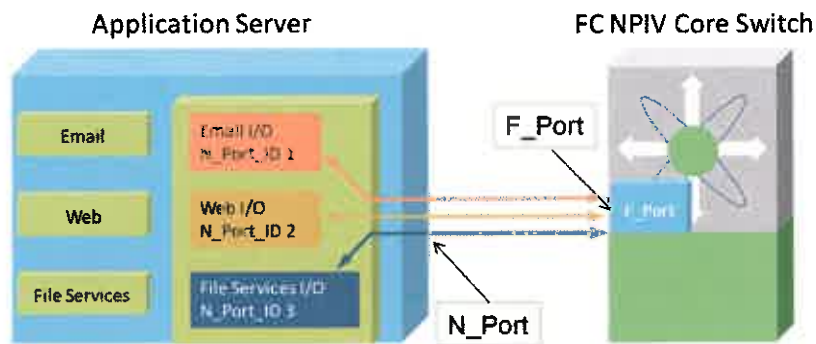
## Network Control Policy

The network control policy will be used to enable Cisco Discovery Protocol (CDP) to exchange information about switch details between platforms and layer 2 switching

## NPIV

N-Port ID Virtualization (NPIV) provides a means to assign multiple FCIDs to a single N\_Port. It allows multiple applications to share the same Fiber Channel adapter port. Different WWPN allow access control, zoning, and port security to be implemented at the application level.

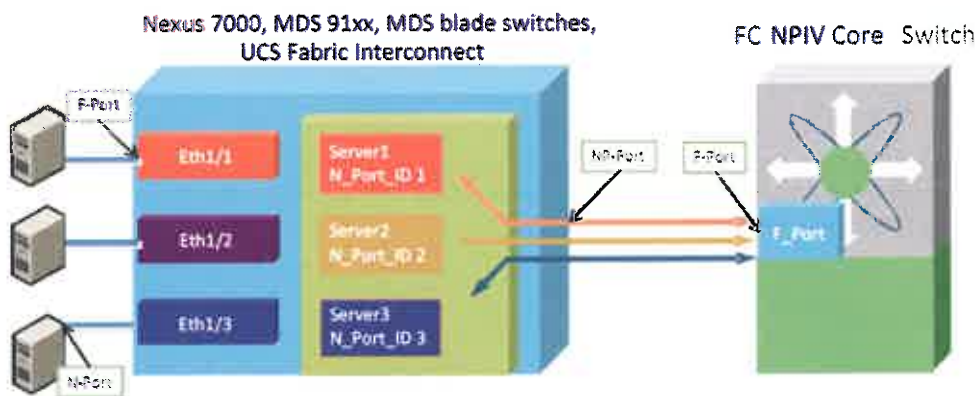
Its usage applies to applications such as VMWare.



**Figure 23 NPIV**

## NPV

N-Port Virtualizer (NPV) utilizes NPIV functionality to allow a “switch” to act like a server performing multiple logins through a single physical link.



**Figure 24 NPV**

# SAN Architecture

## Hardware

SAN storage selection is very important to ensure that each virtual machine gets the required performance needed. The primary measurement used to determine the demands of the SAN system is I/O operations per second (IOPS). Each UC application will have a different maximum IOPS value. The SAN datastore creation should consider these maximum values to ensure the data stores (and LUNs) can support the UC applications.

**Table 3** *SAN Hardware for Watertown, MA and Allen, TX*

Device Name	Description
MDS 9148	Switch SAN
NetApp FAS 3270	Storage
600GB 15K 4GB FC / 180 IOPS	Disks

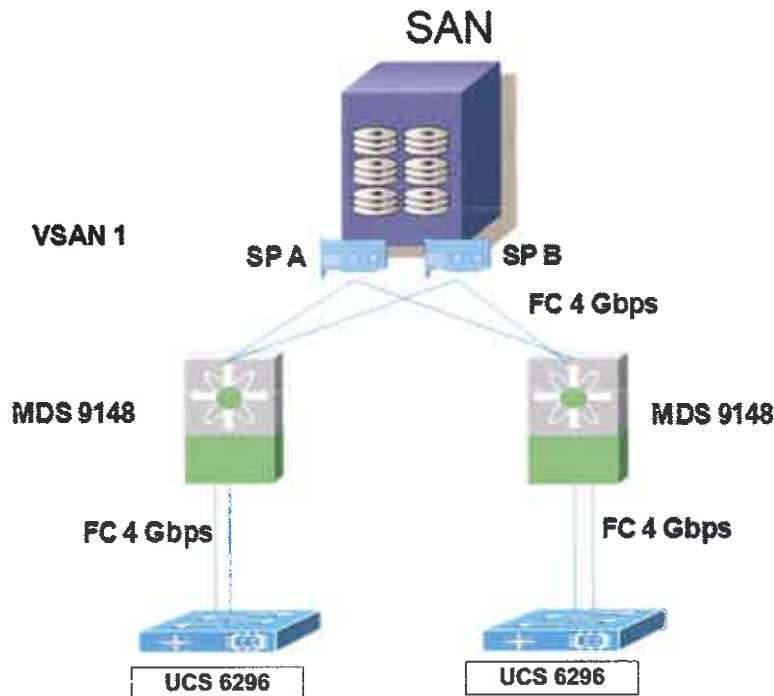
The Cisco® MDS 9148 Multilayer Fabric Switch is a high-performance, flexible, cost-effective platform with the industry's highest port density and lowest power consumption available in a compact one rack-unit (1RU) chassis form factor. It provides 48 line-rate 8-Gbps ports for storage networking deployments in small, medium-sized, and large enterprise environments. The Cisco MDS 9148, based on a purpose-built "switch-on-a-chip" application-specific integrated circuit (ASIC), offers outstanding value by providing high-availability, security, and ease of use at a cost-effective price. With the flexibility to expand from 16 to 48 ports in 8-port increments, the Cisco MDS 9148 offers the densities required to scale from an entry-level departmental switch to top-of-the-rack switch to edge connectivity in enterprise SANs. The Cisco MDS 9148 delivers a nonblocking architecture, with all 48 1/2/4/8-Gbps ports operating at line-rate concurrently.

The Cisco MDS 9148 supports the Cisco Device Manager Quick Configuration Wizard, which allows it to be deployed quickly and easily in networks of any size. Powered by Cisco MDS 9000 NX-OS Software, it includes advanced storage networking features and functions

## Connectivity

Each UCS fabric interconnect will be connected with 2 x 4 Gbps FC links to one SAN switch from the MDS. It is recommended to have at minimum 2 links between a SAN switch and a fabric interconnect.

Each MDS SAN switch will be connected to the two storage controllers from Netapp FAS3270-R5. The storage controllers will function in active/active mode.



**Figure 25** SAN Connectivity

## Storage Requirements

### Latency

Cisco recommends following the specifications for disk latency times defined by VMware:

- disk command latency should be no greater than 15-20 ms

### IOPS

Below are the IOPS numbers for each UC application to allow SAN planning and optimization.

**Table 4** IOPS Requirements Per Application

Cisco Device Name	IOPS Avg per VM	IOPS Max spike per VM
CUCM	50	1000 for midnight maintenance
Unity Connection	100	1500 for 5 min
CUP	20	520 for 7 min
CUOM	4	9

Note: Additional IOPS will be added as needed to support expansion



## Hot Spare

One hot spare will be provided for each drive type.

## Storage Overview

The Netapp SAN FAS 3270-R5 storage consists of the following components and is deployed with self encrypting storage utilizing SafeNet Appliance Secure K460

- Controllers
- Shelves
- Disks (contained in Shelves)
- Power Supplies
- Interfaces (fiber channel ports, Ethernet ports)
- Management

More specifically, on the NetApp FAS 3270R5:

- Up to 2880 TB of storage 24X600GB deployed
- Up to 2 ports per controller configured as front-end (host) connectivity ports
- Up to 4 directly connected servers per active/active configuration

[http://www.sandirect.com/documents/netapp\\_fas3200\\_ds.pdf](http://www.sandirect.com/documents/netapp_fas3200_ds.pdf)



**Figure 26** NetApp FAS 3270-R5

Part Number	Description
FAS3270AEBASR6	FAS3270 HA System with Controller & IOXM
FAS-V32XXCHASSIS-R6-C	ADPT 4-Pt FC 8Gb Target-Init PCIe,-C
X1132A-R6-C	ADPT 4-Pt FC 8Gb Target-Init PCIe,-C
X2065A-R6-C	HBA SAS 4-Port Copper 3/6 Gb QSFP PCIe,-C
X6561-R6-C	Cable,Ethernet,2m RJ45 CAT6,-C
X6560-R6-C	Cable,Ethernet,0.5m RJ45 CAT6,-C
X6558-R6-C	Cable,SAS Cntr-Shelf/Shelf-Shelf/HA,2m,-C
X6553-R6-C	Cable,Cntr-Shelf/Switch,2m,LC/LC,Op,-C

Part Number	Description
X-SFPH10GBCU5M-R6-C	Cisco N50XX 10GBase Copper SFP+cable,5m,-C,R6
X8719A-R6-C	PDU,3-phase,24-Outlet,30A,NEMA,4-Pin,-C,R6
X870D-R6-C	Cab,DS448x,Empty,No PDU,No Rails,-C
X877B-R6-C	Rail Kit II, Cab,-C,R6
X8778-R6-C	Mounting Bracket,Tie-Down,32X0,-C,R6
DOC-32XX-C	Documents,32XX,-C
X800-42U-R6-C	Cabinet Component Power Cable,-C,R6
X1971A-R5-C	Flash Cache 512GB PCIe Module,-C
DS2246-1014-24N-R5-C	DSK SHLF,24x600GB,10K,NSE,-C
SW-3270AONTAP8-C	SW,Data ONTAP Essentials,3270A,-C <b>Message:</b> Includes Http, One Protocol Of Choice, Dedup (Asis), Nearstore, Syncmirror, Dsm/Mpio, Multistore, And Flexcache - System Mgr

Table 5 Netapp Storage Component List

Part Number	Description
X-SFNET-KM-94751-NSER5-C	SafeNet,KeySecurek460 w/NSE10 KeyMgr,-C
X-SFNET-91204-R5-C	Power Cable,SafeNet,110 VAC North America,-C
SW-SFNETKS460-NSEKEY-C	SafeNet,KeySecure Connector License 10 NSE,-C

Table 6 SafeNet Storage Security Appliance

# SafeNet Storage Security Overview

SafeNet KeySecure offers a robust enterprise key lifecycle management solution with the ability to consolidate and centrally manage encryption keys from multiple, disparate encryption platforms. KeySecure simplifies the operational challenges of managing encryption keys—ensuring keys are secure and information is always available to authorized users. As the use of encryption proliferates throughout an organization, security teams must be able to scale their management of encryption keys, including key generation, key import and export, key rotation, and much more. Administrators can simultaneously manage multiple appliances and associated keys, including storage devices such as self-encrypted disks and tape drives, storage encryption platforms, virtual storage, virtual instances, encrypted applications, files, hard disks, databases, and more. With SafeNet Key Secure, security teams gain the critical key management capabilities they need to secure physical, virtual, and cloud-based environments while enforcing security policies surrounding access and use.

## Security:

NIST FIPS 140-2 Level 3 for SafeNet LUNA®  
 PCI-e Cryptographic Module embedded  
 Encryption card (validation in process)

## Cryptography:

- AES, 3DES, DES, RSA (signatures and Encryption), RC4, HMAC SHA-1 – SHA512, SEED encryption
- Asymmetric key sizes
- 1024, 2048, 3072, 4096
- Symmetric key sizes
- 128, 192, 256

## Key Management Protocol

OASIS KMIP (Key Management Interoperability Protocol) 1.0 Specification compliant

- NIST 800-57 Key Lifecycle support
- Symmetric Key, Asymmetric Key, Opaque, Secret Data, Template
- Operations: Create, CreateKeyPair, Register, Get, GetAttribute, GetAttributeList, Locate, Query, Add/Delete/Modify Attributes

## Role-based Management Control

- Multiple restricted roles can be defined for each administrator
- Automated, self-contained key management
- Multi-credential administrative authorization for sensitive security operations

**Key Availability and Capacity**

- Secure key replication to multiple appliances
- Intelligent key sharing via key sharing groups

**High Availability and Redundancy**

- Active-Active mode of clustering
- Multiple geographies
- Hierarchical clustering

**Supported Technologies****API support**

- iCAPI, KMIP, PKCS #11, JCE, MSCAPI, and .NET

**Network management**

- SNMP (v1, v2, and v3), NTP, URL health check, signed secure logs & syslog, automatic log rotation, secured encrypted and integritychecked backups and upgrades, extensive statistics

**System administration**

- Secure Web-based GUI, Secure Shell (SSH), and console
- Supported Directory

**Deployed License Option KeySecure k460**

- Up to 1 million symmetric & asymmetric keys stored per cluster
- Up to 1,000 concurrent clients
- Intel XeonE5620 2.4Ghz, 12M Cache, Turbo, HT, 1066MHz Max Mem processor
- Four (4) 10/100/1000 Mbps Ethernet ports
- Two 500GB 7.2K RPM SATA 2.5" Hot-Plug Hard Drives
- 1U, rack mountable (H: 1.7"; W: 19"; D: 30")
- Two 502W Energy Smart Hot-Plug power supplies
- Embedded SafeNet LUNA PCI card

## Storage Layout

DAE 5	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC
	RAID 5 #13					RAID 5 #14					RAID 5 #15				
DAE 4	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC
	RAID 5 #10					RAID 5 #11					RAID 5 #12				
DAE 3	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC
	RAID 5 #7					RAID 5 #8					RAID 5 #9				
DAE 2	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC
	RAID 5 #4					RAID 5 #5					RAID 5 #6				
DAE 1	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC
	RAID 5 #1					RAID 5 #2					RAID 5 #3				
DAE 0	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC	450GB FC
	VAULT					Hot Spare	Hot Spare	Hot Spare							

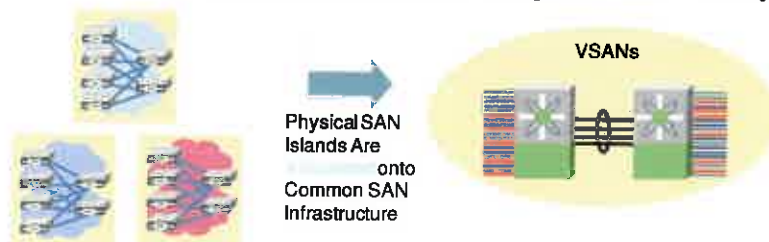
**Figure 27** Example Allocation of Physical Drives in SAN

Vault is where the SAN OS resides. No high-performance usage should be placed on these drives.

AT&T will use a new storage system with DAEs dedicated to HCS. AT&T will use RAID 5 disks on multiple DAEs.

## Virtual SAN

A VSAN provides a method to allocate ports within a physical fabric to create virtual fabrics. Each VSAN in this topology has the same behavior and property of a SAN. A given device can only belong to one VSAN. VSANs allow more efficient SAN fabric utilization by creating hardware based isolated virtual fabrics. Each VSAN is managed as it was a separate physical fabric and can be independently zoned and maintains its own set of fabric devices (PSPF, FLOGI server, Name Server, etc...) for added scalability and resiliency. VSANs allow the cost of the physical SAN infrastructure to be shared among more applications and users while assuring absolute segregation, security of data and management traffic retaining independent control of configuration on a VSAN-by-VSAN basis.



**Figure 28** Virtual SAN

VSAN has the following additional features and benefits:

- Ease of configuration is enhanced since devices can be added or removed from a VSAN without making any physical changes to cabling



- The same Fibre Channel ID (FCID) can be assigned to a host in another VSAN, this increasing VSAN scalability
- Every instance of VSAN runs all required protocols such as FSPF, domain manager and zoning
- Fabric-related configurations in one VSAN do not affect the associated traffic in another VSAN
- Events causing traffic disruptions in one VSAN are contained within that VSAN and are not propagated to others VSANs.

Up to 1024 VSANs can be configured on a physical SAN. Of these, one is the default VSAN (VSAN 1) and another is the isolated VSAN (VSAN 4094). User-specified VSAN IDs range from 2 to 4093.

## Port VSAN Membership

Port VSAN membership is assigned on a port to port basis. By default each port belongs to the default VSAN. You can assign VSAN membership to ports using one of two methods:

- Statically by assigning VSANs to port
- Dynamically by assigning VSANs based on the devices WWN. This method is referred to as dynamic port VSAN membership (DVPM).

The AT&T HCS system will use static port assignment.

## VSAN ID Scheme

VSAN ID and name needs to be unique globally. We do not have any preference or recommendations on the VSAN names, however the following naming convention might be considered by the SAN team: (Name of the VSAN)-(VSAN ID)-Purpose

Purpose might be used if the VSAN name is not clear enough.

Ideally, one VSAN should be used per fabric interconnect at minimum and the VSAN ID should be different than 1 (default VSAN).

An example VSAN name and ID are listed in the table below:

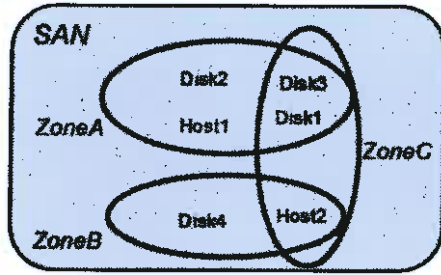
**Table 7** *VSAN Names and IDs*

Data Centre	VSAN Name	VSAN ID	Description
1	Fabric-A	10	VSAN for fabric A DC 1
	Fabric-B	20	VSAN for fabric B DC 1

## Zone and Zone Sets

### Zone

Each member of a fabric (in effect a device attached to an Nx port) can belong to any zone. If a member is not part of any active zone, it is considered to be part of the default zone. Therefore, if no zoneset is active in the fabric all devices are considered to be part of the default zone. Even though a member belongs to multiple zones, a member that is part of the default zone cannot be part of any other zone.



**Figure 29 Zoning Concept Example**

We will keep the default policy which is “deny” for the default zone.

## Zone Sets

While zones provide access control to devices, a zone set is a group of zones to enforce access control across the whole fabric. Multiple zone sets can be created but only a single zone set can be active at once. Zone sets contain the name of member zones.

If one zone set is currently active and another zone set is activated, then the current zone set will deactivate and the new one activated.

## Design

Given that one ESXi host contains 2 HBAs and one storage array (SPE) contains two storage processors, a zone will contain 2 ports, one being an ESXi's HBA and one being a storage processor. All defined zones will be aggregated in one zone set.

Details will be provided in the LLD.

## RAID

A RAID group is a set of physical disks in which you can bind one or more LUNs (covered later). It allows for data protection at the disk level and can increase performance. Note: Clariion supports RAID type 0, 1, 1/0, 3, 5, 6 and hot spare.

For the HCS design RAID 5 will be used.

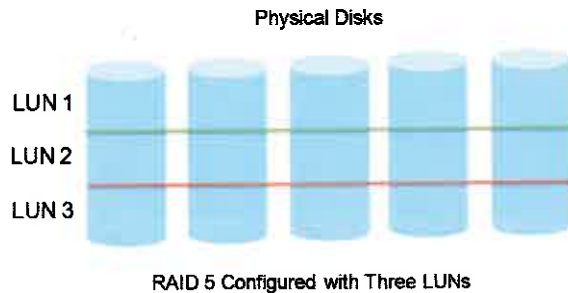
General rules:

- Put the same capacity drives in the same RAID group. The RAID group will be created at the capacity of the lowest capacity drive. Extra space on the bigger drives will be wasted.
- Put same speed drives in the RAID group. This maximizes the service capability of the group.
- Mixing ATA and Fiber Channel drives is not allowed in the same RAID group.

## LUN

### Overview

Logical Unity Numbers are built on top of RAID groups and appear like individual disk to the host's OS. Therefore the disks are bound together so that each LUN uses part of each disk in the array and same sectors on each disk.



**Figure 30 Logical Unity Number Concept**

General guidelines:

- LUN layout will depend partially on the brand of SAN array but guidelines for LUN would be not to put more than 4-8 vm's per LUN.
- (Meta)LUNs should span across multiple RAID group for enhanced performance.
- One host/VM can access multiple LUNs and a LUN can be accessed by multiple host/VM. The access can be enforced by LUN masking rules based on WWNN and WWPN.
- Standard 500 GB LUNs would be used for start, then move to MetaLUN for expansion.
- For VMware VMFS, LUN should not exceed 2 TB.
- As a start, we would propose LUN of 500 GB capacity and MetaLUNs made of 3 LUNs, each on different RAID groups.

## LUN Distribution per DAE

The LUN distribution per DAE should look like this:

	500GB	500GB	500GB	500GB	500GB	500GB	500GB	500GB	500GB
<b>DAE 5</b>	MetaLUN 51 LUN 501 LUN 502 LUN 503			MetaLUN 52 LUN 504 LUN 505 LUN 506			MetaLUN 53 LUN 507 LUN 508 LUN 509		
<b>DAE 4</b>	MetaLUN 41 LUN 401 LUN 402 LUN 403			MetaLUN 42 LUN 404 LUN 405 LUN 406			MetaLUN 43 LUN 407 LUN 408 LUN 409		
<b>DAE 3</b>	MetaLUN 31 LUN 301 LUN 302 LUN 303			MetaLUN 32 LUN 304 LUN 305 LUN 306			MetaLUN 33 LUN 307 LUN 308 LUN 309		
<b>DAE 2</b>	MetaLUN 21 LUN 201 LUN 202 LUN 203			MetaLUN 22 LUN 204 LUN 205 LUN 206			MetaLUN 23 LUN 207 LUN 208 LUN 209		
<b>DAE 1</b>	MetaLUN 11 LUN 101 LUN 102 LUN 103			MetaLUN 12 LUN 104 LUN 105 LUN 106			MetaLUN 13 LUN 107 LUN 108 LUN 109		

**Figure 31 LUN Distribution per DAE**

As explained in the LLD, there are nine LUNs per DAE. Three LUNs are created per RAID 5 group. To distribute the load across all RAID groups of a DAE, we are introducing MetaLUNs. First LUNs of each

RAID group of the same DAE are bundled together to form one MetaLUN. Same applies with second and third LUNs.

## VM Distribution per LUN

This VM distribution per MetaLUN is based on the following rules:

- A VM is always using a colocated MetaLUN (i.e. on same data center).
- Where application level redundancy is involved, primary VMs are using a different MetaLUN than secondary VMs.
- If primary and secondary VMs are spread across two data centers, the MetaLUNs used by primary VMs are also located on a different data center than the ones used by secondary VMs.
- For any given customer, the VMs of a specific UC application are spread across MetaLUNs. This is required to distribute within a MetaLUN the maximum IOPS load generated by the applications' scheduled job. As the schedule job start time is only configurable at the application cluster level, all customer's VMs of a given application needs to be sitting on a different MetaLUN.

This will be covered in more details in the LLD. This VM distribution per LUN approach represents a suggestion for implementation start and could be refined based on further analysis/test learnings.

# VMWare Architecture

## VCenter Setup

### Logical Specifications

This section details the VMware vCenter Server proposed for the vSphere infrastructure design.

**Table 8 vCenter Server Logical Specifications**

Attribute	Specification
vCenter Server version	4.1 (latest version made available by VMWare)
Physical or virtual system	Virtual
Number of CPUs	2
Processor type	VMware vCPU
Processor speed	2.4 GHz
Memory	4GB
Number of vNIC and ports	2
Number of disks and disk size(s)	2 disks: 12GB (C) and 6 GB (D)
Operating system and SP level	Windows Server 2008 Enterprise 64 bits

VMware vCenter Server, the heart of the vSphere infrastructure, will be implemented on a virtual machine as opposed to a standalone physical server. Virtualizing vCenter Server will enable it to benefit from advanced features of vSphere, including VMware HA.

### Physical Specifications

This section details the physical design specifications of the vCenter Server.

**Table 9 vCenter Server System Hardware Physical Specifications**

Attribute	Specification
Vendor and model	VMware VM virtual hardware 7
Processor type	VMware vCPU
NIC vendor and model	VMware VMXNET3
Number of ports/vNIC x speed	2 x Gigabit Ethernet
Network	Service Console network and Oper/Mgmt
Number of SCSI Disks	2
Storage Adapter for SCSI Disks	PVSCSI
Local disk RAID level	N/A



# ESXi

## Logical Specifications

This section details the VMware vSphere hosts proposed for the vSphere infrastructure design. The logical components specified are required by the vSphere architecture to meet calculated consolidation ratios, protect against failure through component redundancy and support all necessary vSphere features.

**Table 10 VMware ESX/ESXi Logical Specifications**

Attribute	Specification
Host type and version	ESXi 4.1
Number of CPUs	2
Number of cores	4
Total number of cores	8
Processor speed	2.4 GHz (2400 MHz)
Memory	48 GB
Number of NIC ports	2
Number of HBA ports	2
Boot from SAN	Y
Service Console RAM	800 MB

Today vSphere hosts can be deployed using ESX or ESXi versions. ESXi is the only supported version for HCS.

## Physical Specifications

This section details the physical design specifications of the host and attachments corresponding to the previous section that describes the logical design specifications.

**Table 11 VMware ESX/ESXi Host Hardware Physical Specifications**

Attribute	Specification
Vendor and model	Cisco UCS B200 M2
Processor type	Intel Xeon 55xx Dual Quad Core
Total number of cores	8
Onboard NIC ports x speed	2 x 10 Gigabit Ethernet
Number of attached NICs	0
NIC vendor and model	Intel
Total number of NIC ports	2 [8 ?]

Attribute	Specification
Storage HBA vendor and model	Qlogic
Storage HBA type	Converged Network Adapter
Number of HBAs	1
Number of ports/HBA x speed	2/4Gbps
Total number of HBA ports	2
Number and type of local drives	None
System monitoring	IPMI-based

The configuration and assembly process for each system will be standardized, with all components installed the same on each host. Standardizing not only the model but also the physical configuration of the ESXi hosts is critical to providing a manageable and supportable infrastructure: it eliminates variability. Consistent PCI card slot location, especially for network controllers, is essential for accurate alignment of physical to virtual I/O resources.

## Configuration and Optimization

### Database for Host Management

For managing hosts, the pre packaged SQL Express is limited to 5 host instances.

If more than 5 hosts are to be deployed, then a choice must be made between the following where appropriate licenses should be available:

- MS SQL Server 2008
- MS SQL Server 2005
- IBM DB2 9.5
- Oracle 10g
- Oracle 11g
- Leverage from an existing DB

### Real Time Application Support

As ESXi is more secure and is better fitted for running real-time applications, only UC on VMware ESXi 5.0 will be supported. Other VMware platforms will not be supported for production use.

### Boot

VMWare boot from SAN was introduced in VMWare 5.0 The HCS solution at AT&T will use boot from SAN for all blades to minimize failure points and maximize performance.

### NIC Teaming

NIC teaming should be disabled at UCS level. It will be enabled at ESXi level.

## Hyper Threading

ESXi Server supports Intel's Hyper-Threading (HT) technology on servers with Intel processors (not applicable to AMD processors). HT can improve processor performance by taking advantage of additional CPU interrupt controllers and registers, thereby enabling slightly higher utilization levels across the virtual infrastructure. Generally a small improvement in performance can be gained by using HT. This performance gain is achieved by doubling the number of logical processors in an ESXi Server host.

HT should be enabled as a default to offer a potential performance increase.

Notes:

- HT improves performance by supporting concurrent thread processing on the same physical CPU to take advantage of idle thread cycles. Therefore it is important to recognise that any performance increase will not be equivalent to adding more physical processors. In very rare cases enabling HT will actually hinder performance. In order to protect against this, performance should be monitored after changing this setting.
- The applications have also to support multi threading in order to gain the benefits.

## Domain Name Service

Domain Name Service (DNS) must be configured on all of the ESXi Server hosts and must be able to resolve short name and Fully Qualified Domain Names (FQDN) using forward and reverse lookup.

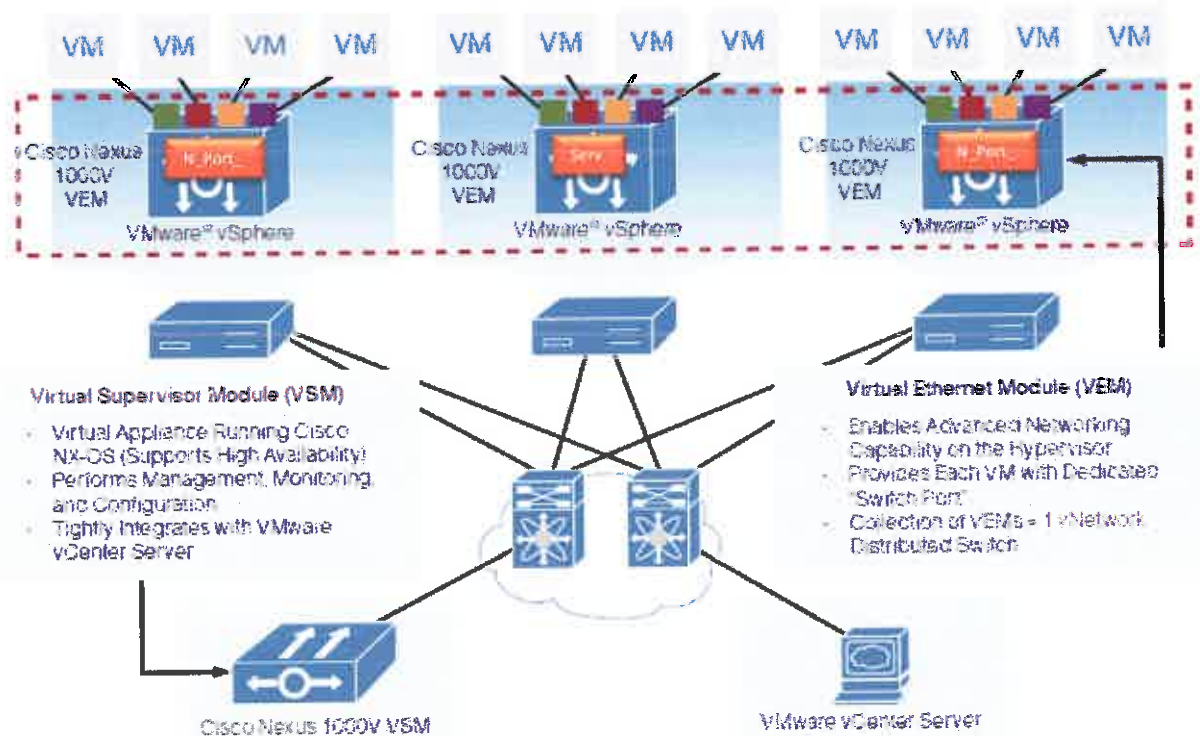
## Network Time Protocol

Network Time Protocol (NTP) must be configured on each ESXi Server host and should be configured to share the same time source as the vCenter Server to ensure consistency of the overall vSphere solution.

## DVS Nexus 1000V

Cisco Nexus 1000V will be used as the Distributed Virtual Switch solution. It is a software switch on a server that delivers Cisco VN-Link services to virtual machines hosted on that server. It takes advantage of the VMware vSphere framework to offer tight integration between server and network environments and help ensure consistent, policy-based network capabilities to all servers in the data center. It allows policy to move with a virtual machine during live migration, ensuring persistent network, security, and storage compliance, resulting in improved business continuance, performance management, and security compliance.

The DVS Nexus 1000V will be used per host. This will provide QoS, VMotion, security and isolation with PVLAN, VLAN management.



**Figure 32 Cisco Nexus 1000V Network Topology**

The VSM (Virtual Supervisor Module) is a virtual machine which can be deployed in variety of ways. In this design guide, it is deployed under UCS blade along with VEM (Virtual Ethernet Module). Nexus 1000V supports redundant VSM (Virtual Supervisor Module). The active and standby are recommended to be configured under separate UCS blade server with the anti-affinity rule under vCenter such that both VSM can never be operating under the same blade server.

Each ESXi host runs a VEM, which is typically configured with two uplinks connected to 10 Gbps interface of the blade server. When installed and provisioned via vCenter, the port-profile designated for uplinks automatically creates port-channel interface for each ESXi host.

## Configuration

The **channel-group auto mode on mac-pinning** will be used to create the port-channel which does **not** run LACP and is not treated as host vPC. This feature creates the source-mac based bonding to one of the uplinks and silently drops packet on other links for any packet with source MAC on that link. As a reminder the Nexus 1000V does not run spanning-tree protocol and thus a technique is needed to make MAC address available via single path.

The **system vlan** command is a critical configuration command that is required to be enabled on set of VLANs. A system VLAN is a VLAN on a port that needs to be brought up before the VEM contacts the VSM. Specifically, this includes the Control/Packet VLANs on the appropriate uplink(s), which is required for the VSM connectivity. It also applies for the ESXi management (service console) VLAN on the uplink and if the management port is on Nexus 1000V: if any reason due the failure, these VLANs should come up on the specified ports first, to establish vCenter connectivity and receive switch configuration data.

## Port Profile

The port-profile capability of Nexus 1000V enables the seamless network connectivity across the UCS domain and ESXi cluster. In this design, each virtual machine is enabled with one virtual interface inheriting a specific profile. The profiles are designed with connectivity requirements and secure separation principles.

## Customer Separation (VLAN/PVLAN)

Secured separation is one of the basic requirements for the multi-tenant environment as each customer requires some level of isolation from each other. VLANs are the primary means of separation in multi-tenant design meaning that each customer will sit in a dedicated VLAN. PVLAN will be used to isolate if customer VMs are sitting on a shared VLAN.

## VMotion

The VMotion feature is not yet supported for a UC application environment; however, this design will enable this capability day one. The VMotion interface will rely on a Nexus 1000V port profile.

## Virtual Machine Setup

Most of applications used in this system will be virtualized on UCS platform. Specifically the following applications will be virtualized: CUCM, CUCM-SME, CUCxn, CUPS, CUOM, CUPM, HCM-Mediation, VSX, HCM, and VOSS USM. However, AT&T may not use the complete list of virtualized applications.

## VM Specifications per Application

Each UC application has different hardware needs. The table below shows the Virtual CPU (vCPU) and memory requirements for Unified Communications applications running on the B-series blade servers under VMware ESXi 5.0

**As mentioned before, there can be no oversubscription of either vCPU<sup>1</sup> or memory on a Blade server;** i.e. the number of vCPUs and amount of memory required by a combination of applications on a blade cannot exceed that blade's resources. Each application also requires a single virtual NIC.

At this time if a Cisco Unity Connection virtual machine is loaded and powered on a B-series blade server the application does require an idle/unused vCPU to remain available for the ESXi scheduler to properly schedule and allow for predictable real-time audio streaming which Cisco Unity Connection voice messaging depends on.



**Table 12 VM Specifications per Application (per VM)**

Product	Users	vCPU	vRAM	vDisk	VNIC
<b>Infrastructure</b>					
N1KV VSM	N/A	1 vCPU	2 GB	1 x 10 GB	3 vNIC
Vcenter	N/A	2 vCPU	4 GB	2 x 12 GB	2 vNIC
<b>Service Assurance</b>					
HCM	N/A	2 vCPU	16 GB	1 x 400 GB	1 vNIC
FMS	N/A	2 vCPU	4 GB	1 x 20 GB	1 vNIC
DCNM	N/A	2 vCPU	6 GB	1 x 80 GB	1 vNIC
<b>Service Fulfillment</b>					
<b>UC Management</b>					
CUOM/CUSM	Up to 10,000 phones	2 vCPU	4 GB	1 x 80 GB	1 vNIC
CUOM/CUSM	Up to 30,000 phones	6 vCPU	8 GB	1 x 80 GB	1 vNIC
<b>UC Applications</b>					
CUCM	7,500	2 vCPU	6 GB	2 x 80 GB	1 vNIC
UCxn <sup>2</sup>	10,000	4 vCPU	4 GB	2 x 144 GB	1 vNIC
CUP <sup>3</sup>	5000	4 vCPU	4 GB	2 x 80 GB	1 vNIC

]

Virtual machine templates are recommended and available for most Unified Communications application. These templates have pre-partitioned disks that are aligned on 64k boundaries.

A VMware OVA file will be created for each UC application that defines exactly the needs for that given application, based on the target size (#phones, devices, users, etc). Regarding disk, we recommend VM alignment for optimal performance. The provided OVA files will contain hard drives with partitions that are already aligned.

<sup>2</sup> Limits:

- 150 ports G.711 or G.729a (combined TUI, VUI, or TTS)
- 25 ports iLBC or G.722
- 10,000 users

<sup>3</sup> Adding 1 GB memory can help the virtual machines performance if experiencing performance issues. Resource reservation is highly recommended if maximum number of users is configured. Set kernel timer frequency divider to 10 if performance is critical, or seeing performance issues.

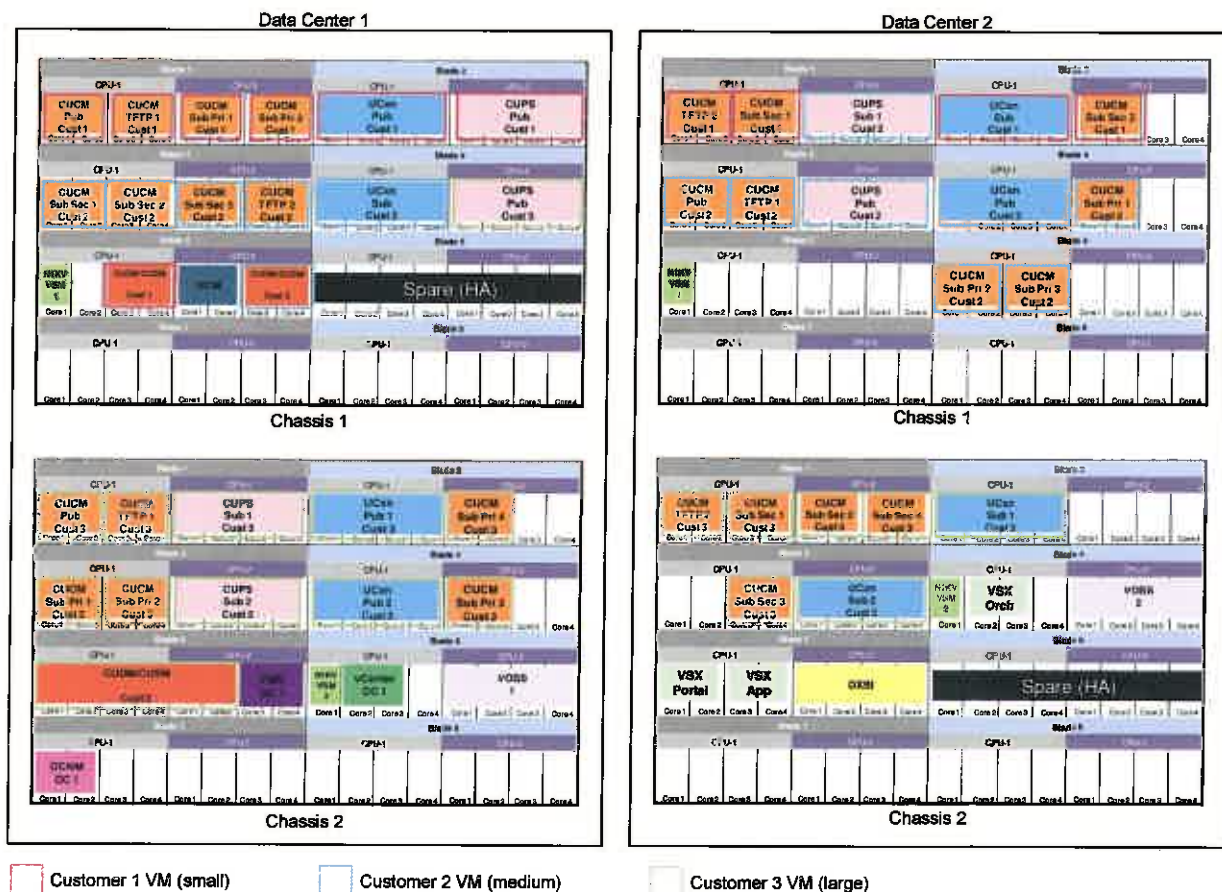
## VM Distribution per Blade per Chassis

There are many ways to layout applications to optimize UCS blade utilization. Here are some items to consider when defining the layout of UC applications on a blade:

- **Availability:** If the UC applications are being used in a high availability mode (clustered), then each node in a cluster should be placed apart from the other nodes. That spacing could be on a separate blade, a separate chassis, or even a separate data center depending on the availability requirements.
- **Sharing of memory:** When running a group of UC applications that are all running the same software load/version it is more likely VMware will be able to share some of the common memory between those applications. This memory sharing is built into VMware and the amount of memory shared will vary depending on each application and how each application is used.
- **Resource requirements:** Each application will have unique demands for resources (CPUs and memory). For example, one application may need a dedicated CPU while others can share CPU resources. In that case it might make sense to spread out the applications that require dedicated CPUs so that the other applications can share the remaining CPUs and take advantage of the additional memory that would normally be taken in a completely CPU oversubscription layout.

An example layout is as follows:

**Figure 33 Example Layout of Applications per Chassis/Blade**



## Notes:

- The above diagram does not suggest CPU affinity.
- VM HA will require one free blade. Alternatively, one powered off blade can be used to restart the service profile running an impaired blade. This backup blade can be reserved for many blades/chassis. This approach can only work if boot from SAN is used (not supported by VMware yet).
- All non UC applications should be deployed on a specific blade. HCS UC application VMs should not be mixed on the same blade with 3<sup>rd</sup> party application VMs. If 3<sup>rd</sup> party applications are present, there must be one dedicated spare blade for this purpose.

## VMWare Features Support

**Table 13** VMWare Features Support in HCS

VMWare Feature	Status	Comment
VMware Consolidated Backup		
VMware Dynamic ResourceScheduler (DRS)		Requires VMotion
VMware High Availability (HA)		
VMware Site Recovery Manager		
VMware Snapshots		
VMware Snapshots with Memory		
VMware Storage VMotion		
VMware VMotion		
VMware vCenter Update Manager		With limitations

## Status Key

Status	Comment
	Supported
	Not supported

## Notes:

- vCenter Update Manager is not supported for UC applications.
- VMotion: VMotion and features that leverage it are not supported because VMotion presents significant challenges for the Cisco Unified Communications applications (service interruption, degraded voice quality after the migration for voice calls that were in progress, etc.).

## VMware High Availability (HA)

The VMware HA feature allows a VM to be automatically restarted in case of a physical host failure when there are available resources on another host. The result is equivalent to a reboot.

## VMotion

The VMware VMotion feature has several variations: live VMotion, storage VMotion, etc.

There are many different scenarios that could affect the behavior of the UC applications while performing a VMotion, i.e. features in use, the state of the application, the network bandwidth, etc.

Therefore, the recommendation stands to do VMotion during maintenance hours only.

## SRM

VMware Site Recovery Manager allows SAN storage to be synchronized between datastores.

## Snapshots

Snapshots should not be used as they can decrease the performance of the virtual machine.

## VDR

VMware Data Recovery is a way to backup and restore virtual machines.

## FT

VMware Fault Tolerance currently only supports virtual machines with one vCPU. Some of our UC applications are 1 vCPU systems and in theory could use FT. However, this feature has not been tested for inclusion in HCS.

# UC Architecture

## UC Feature Requirements

This section lists the UC features as required by the customer against what is in the scope of the HCS program:

**Table 14 UC Feature Customer Requirement Against HCS Support**

UC Feature	End Customer Requirement	HCS Support
Onnet Intra Enterprise VOIP Calls	Y	Y
Onnet Inter Enterprise VOIP Calls	Y	Y
Offnet calls to PSTN	Y	Y
Offnet calls to SIP Network	Y	Y
Offnet calls to AT&T BTIP H.323	Y	Y
Delayed Offer to Early Offer	Y	Y
DTMF Inband (RFC 2833)	Y	Y
Emergency calls – offnet to PSTN	Y	Y
Number dialing: local, national, international	Y	Y
Supplementary Voice Service	Y	Y
CFNA	Y	Y
CFU	Y	Y
Call park	Y	Y
Call Transfer (Blind, Consultative)	Y	Y
3 Way Conference Call	Y	Y
Call Waiting	Y	Y
Call Hold/Resume	Y	Y
CLIP/CLIR	Y	Y
Extension Mobility	Y	Y
Intra Enterprise (ptp video) using SIP video Phone	Y	Y

## Overview

The proposed solution is to provide managed Unified Communications to AT&T end customers using Cisco Systems Unified Communications technology running on virtual machines.



The call routing and control functions will be provided by Cisco Unified Communication Manager clusters located in the AT&T data centers in Watertown, MA; Dallas, TX; Amsterdam, Netherlands; and the Singapore data center.

The access to PSTN for an end customer can be provided by a local media gateway or via the AT&T centralized PSTN breakout via a SIP trunk.

Cisco IP phones will connect to LAN switches being rolled out to the AT&T end customer locations as part of a separate project/design.

The central Cisco Unified Communication Manager clusters and different end customer remote sites are linked by the AT&T MPLS network.

End customer's remote location within scope of the project may have a local PSTN gateway deployed at the site.

It is recommended that the local gateway also provide Ad hoc conferencing resources and SRST fallback. Streaming of multicast Music-on-Hold for the site is also a good option.

IP telephone calls within a site will use the G.711 u-law codec. Calls that traverse the AT&T MPLS network will also use G.711 u-law codec.

There will be no direct inter-cluster call routing. Calls between end customers will be routed out and back via the local or central breakout. In case of central breakout, this will mean that the call will stay VoIP all the way with the CUBE-SP SBC as the anchor for media and signalling.

## Technical Description of Components

### Clustering Across UCS Chassis/Data Centers

The Intra-Cluster Communication Signaling (ICCS) between Cisco Unified Communication Manager servers consists of many traffic types. The ICCS traffic types are classified as either priority or best-effort. Priority ICCS traffic is marked with IP Precedence 3 (DSCP 24 or PHB CS3 for release 4.0 and later). Best-effort ICCS traffic is marked with IP Precedence 0 (DSCP 0 or PHB BE).

The following design guidelines apply to the indicated WAN characteristics:

- **Delay:** The maximum one-way delay between any Cisco Unified Communication Manager servers for all priority ICCS traffic should not exceed 20 ms, or 40 ms round-trip time (RTT). Delay for other ICCS traffic should be kept reasonable to provide timely database and directory access. Propagation delay between two sites introduces 6 microseconds per kilometer without any other network delays being considered.
- **Jitter:** Jitter is the varying delay that packets incur through the network due to processing, queue, buffer, congestion, or path variation delay. Jitter for the IP Precedence 3 ICCS traffic must be minimized using Quality of Service (QoS) features.
- **Packet loss and errors:** The network should be engineered for zero percent packet loss and errors for all ICCS, especially the priority ICCS traffic, because packet loss and errors will have adverse effects on the real-time call processing within the cluster.
- **Bandwidth:** Provision the correct amount of bandwidth between each server for the expected call volume, type of devices, and number of devices. This bandwidth is in addition to any other bandwidth for other applications sharing the network, including voice and video traffic between the sites. The bandwidth provisioned must have QoS enabled to provide the prioritization and scheduling for the different classes of traffic. The general rule of thumb for bandwidth is to over-provision and under-subscribe.
- **Quality of Service:** The network infrastructure relies on QoS engineering to provide consistent and predictable end-to-end levels of service for traffic. Neither QoS nor bandwidth alone is the solution; rather, QoS-enabled bandwidth must be engineered into the network infrastructure.

## Planning Guidelines

Every 10,000 busy hour call attempts (BHCA) requires 900 kbps of bandwidth for Intra-Cluster Communication Signaling (ICCS). This is a minimum bandwidth requirement, and bandwidth is allocated in multiples of 900 kbps.

The minimum recommended bandwidth between clustered servers is 1.544 Mbps. This amount allows for the minimum of 900 kbps for ICCS and 644 kbps for SQL, LDAP, and other inter-server traffic.

A maximum Round Trip Time (RTT) of 40 ms is allowed between any two servers in the Cisco Unified Communication Manager cluster. This time equates to a 20 ms maximum one-way delay, or a transmission distance of approximately 1860 miles (3000 km) under ideal conditions.

A minimum of 644KB per cluster is required in the bronze queue for other low priority intra-cluster signaling traffic. This traffic is marked by the CCM as Best effort. It may be required to re-classify this traffic as best effort from the CCM servers to CS3 in the local LAN switch.

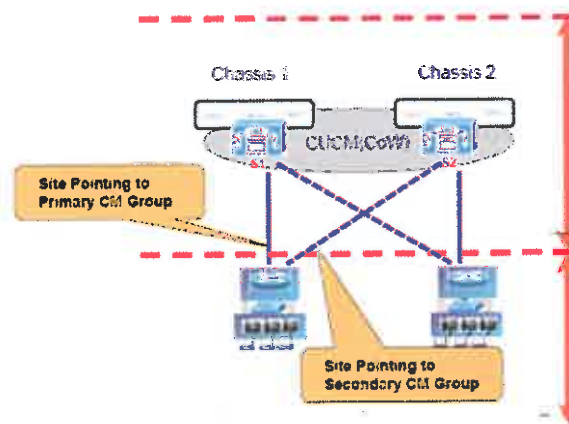
Note: Cisco has begun to change the marking of voice control protocols from DSCP 26 (PHB AF31) to DSCP 24 (PHB CS3). However many products still mark signaling traffic as DSCP 26 (PHB AF31); therefore, in the interim, Cisco recommends that you reserve both AF31 and CS3 for call signaling. Cisco Unified Communication Manager 4.x and later uses the new CS3 marking.

## Call Processing Redundancy

Cisco Unified CallManager clustering technology provides for Cisco CallManager redundancy. CallManager redundancy is the ability to provide a “hot standby” call processing server to all IPT endpoint capable of re-homing its connection from a designated primary CallManager subscriber to a backup or secondary CallManager subscriber automatically without any service interruption.

Hardware 1:1 redundancy gives the ability to equally balance all IPT endpoints in the cluster over the primary and backup CallManager server pairs. CallManager server clustering over different location provides the added benefit of server redundancy and diversity built in to CallManager redundancy.

Using CallManager Redundancy Group and Device Pools, you can home half of the devices in a remote site to one CM server while the other CM server across the other UCS chassis/datacenter acts as the backup CM server and vice versa to the rest of the sites endpoints.



**Figure 34 Call Processing Redundancy**

Distributing the endpoints this way reduces the impact of any server becoming unavailable. Care must be taken when distributing load making sure device count does not exceed number of devices allowed per CM server. In other words, the total load on the primary and secondary subscribers should not exceed that of a single subscriber.

However, this hardware oriented redundancy mechanism may not be totally suitable for a virtualized environment as it increases the number of virtual machines and therefore consuming resources out of

CPU/RAM pools (i.e impacting the overall total number of managed customers for a given set of resources).

## TFTP Redundancy

The TFTP server performs an important role in IPT endpoints registration with CallManager. It is the source of files for services such as MoH, configuration files for devices such as phones and gateways, binary files for the upgrade of phones as well as some gateways, and various security files.

The TFTP server is required by phones and gateways to obtain its configuration information during registration otherwise it will fail to register to the CallManager.

Generally the recommendation is to deploy at least two TFTP servers to provide for load balancing and redundancy. TFTP redundancy is done by defining two IP address array in the devices DHCP scope configuration. Load balance TFTP by carefully assigning for example DHCP scope "A" with TFTP1 server as the primary TFTP server and TFTP2 server as the backup TFTP server. Similarly, assign the rest of the devices with DHCP scope "B" with TFTP2 server as the primary and TFTP1 server as the backup TFTP server. Depending on the size of the cluster, CallManager Administrator can modify the default number of TFTP sessions allowed to improve performance on dedicated TFTP servers.



Figure 35 TFTP Redundancy

## Media Resources

Media resources such as conferencing, annunciator, transcoding, media termination point (MTP) and music on hold services may be provided in a couple of ways depending on the size of the cluster.

The following brief description describes these services:

- **Music on Hold (MoH)** — Provides multicast or unicast music to devices that are placed on hold or temporary hold, transferred, or added to a conference. The advantage of doing a multicast considerably reduces the amount of MoH sessions required to a group of people and for remote sites this means bandwidth savings. Only supported for SCCP endpoints.
- **Annunciator service** — Provides announcements in place of tones to indicate incorrectly dialed numbers or call routing unavailability.
- **Conference bridges** — Provide software-based or hardware based conferencing for ad-hoc and meet-me conferences.
- **Media termination point (MTP) services** — provide features for H.323 clients, H.323 trunks, and Session Initiation Protocol (SIP) trunks.

Cisco best practice is to allocate hardware conferencing resources for at least 5% of the user base at the site. If the user attempts an ad-hoc conference and there are not enough DSP resources provisioned, then the ad conference will fail and the user will see an error message displayed on their IP phone.

**With regards to MoH, the proposal is to use hardware based MoH based on multicast from CPE. In the event that this is not available, the following alternatives are proposed.**

1. Create separate dedicated MoH VM. This will consume additional resources on the Blades and will reduce the amount of available blade space for provisioning new end customers and users. As

long as the end-customer count and license mix remains inline with the projections, there should be space available on the blades for a small number of end customers to choose this option.

2. Turn on MoH on the publisher and/or subscriber. As this has not been tested yet, AT&T should be willing to find out a sustainable combination of service activations (call processing and MoH) among publisher and subscriber. This option might be viable for a very small end-customer but should not be considered for large customers.

**Table 15 Media Resources Support in HCS**

Media Resource	HCS Support
Audio Conferencing (ad-hoc conferencing)	HW based (Switch/Router based platform with DSP modules)
Media Termination Point	HW based as above (Switch/Router based platform with DSP modules)
MoH	HW based (Router based platform with IP multicast)
Annunciator	SW based
Transcoder	HW based (Switch/Router based platform with DSP modules)

## Dial Plan Overview

The goal here is to define a generic dial plan that can be used as a foundation for AT&T HCS across the network.

The resulting CUCM dial plans must be simple, consistent and scalable across AT&T HCS network.

## Dial Plan Requirements

The dial plan requirements must be divided into 2 categories:

1. Dial plan requirements for the leaf CUCM cluster
2. Dial plan requirements for the SIP aggregation device

### Leaf Cluster

The dial plan requirements for the leaf CUCM cluster should be supporting:

- It should be applicable to a single cluster hosting a single customer.
- Multiple locations can exist on the Cluster.
- Intra Site Calling & Inter Site Calling within the customer is supported.

- Intra Site & Inter Site (aka location) are routed within the Cluster.
- PSTN calls are sent out to an aggregation layer over a SIP trunk (centralized breakout) or to a local gateway (local breakout).
- The leaf cluster should automatically choose the WAN or the PSTN as the path for the call, and this should be transparent to the user.
- Conversion to & from E.164 numbers are handled by the leaf cluster CUCM.
- There will be no overlapping of extensions in any sites within a single cluster.
- SRST may be utilized for remote sites connected through WAN circuits. While in this mode the users do not need to alter their dialing habits.
- This dial plan must be implemented in a way that effectively utilizes Wide Area Network (WAN) circuits in the AT&T network as the first route choice at all times.
- Remote gateways will be configured to provide SRST in case of a WAN failure.

The following outlines the generic dial plan:

- Intra Site Calling – 5 digits dialing
- Inter Site Calling – access code “8” + 7 digits;
- The voicemail is reached by dialing 5 digits from user extension, or by calling the full e.164 number from the PSTN; or by calling an toll number access from the PSTN
- LD and Local Calling – access code “9” + 10 digits; 9+11 digits; 9+7 digits
- International Calling – access code “9” + 00+ Country Code + City Code + Number
- Each line appearance in the CallManager system is a unique 7 digit directory number (DN).

The following requirements may also apply based on the end customer service policy:

- At least four (4) Classes of Service restriction are necessary (internal, local, long distance, international)
- SRST should provide the same COR (Class of Restriction)
- Extension mobility (optional)
- Call Forward All (CFA) to local, long distance, and international numbers are not allowed.

## Aggregation Device (i.e. CUBE-SP)

The dial plan requirements for the aggregation device should be supporting:

- Suitable dial plans will be created on the aggregation device to route the calls to the PSTN as appropriate.
- Suitable dial plans will be created on the aggregation device to route the calls to the respective leaf CUCM clusters as desirable.
- Inter Enterprise calls are routed by the aggregation layer.
- Access voice mail from PSTN
- Route emergency calls from leaf clusters to the proper emergency services



## Inbound and Outbound Call Flows

### On-net

- **Intra cluster intra site:**  
Customer A user 1 calls customer A user 2 located on the same site and leaf cluster. This should be possible by only dialing the extension end digits.
- **Intra cluster inter site:**  
Customer A user 1 calls customer A user 2 located on a different site but on the same leaf cluster. This should be possible by dialing the full extension digits.
- **Inter cluster:**  
Customer A user 1 calls customer B user 2 located on a different leaf cluster. Customer A leaf cluster decides to route this call in SIP to the aggregation layer which routes the call to AT&T (for CALEA compliance), then back thru the aggregation layer in SIP to the Customer B leaf cluster. This should be possible by dialing the full E.164 digits.

### Off-net

- **To PSTN via local breakout:**  
Customer A user 1 calls PSTN number. The leaf cluster routes this call to the PSTN via the local gateway. This is transparent to the end user.
- **To PSTN via central breakout:**  
Customer A user 1 calls PSTN number. The leaf cluster routes this call to the PSTN via the central aggregation device in SIP. This is transparent to the end user.
- **From PSTN via local breakout:**  
PSTN user 1 calls Customer A user 2 by dialing user 2 E.164 number. The PSTN routes this call to the local gateway driven by the Customer A leaf cluster which routes this call to user 2.
- **From PSTN via central breakout:**  
PSTN user 1 calls Customer A user 2 by dialing user 2 E.164 number. The PSTN routes this call to the aggregation layer which in turn routes the call in SIP to Customer A leaf cluster delivering this call to user 2.
- **Inter cluster:**  
Customer A user 1 calls customer B user 2 located on a different leaf cluster. Customer A leaf cluster decides to route this call to PSTN via its local gateway. This should be possible by dialing the full E.164 digits.

## Class of Service

A set of classes of service are defined for provisioning each time a customer's location is added to the platform. The calling categories are platform wide and defined in USM. These categories will be defined as part of the network design phase. They include such categories as internal, local, national, mobile, international, premium rate, call forward local, call forward international etc. Once the categories are defined, the dialed patterns associated with the categories are defined on a per country basis.

When adding a phone or extension mobility user to the system, the appropriate COS is chosen. The COS may be changed after the phone or user has been added. It is possible to have different COS's on different lines on the same device.

# Network Quality of Service and Bandwidth Requirements for Voice

## Bearer Traffic

A summary of the key QoS requirements and recommendations for Voice (bearer traffic) are:

- Voice traffic should be marked to DSCP EF per the QoS Baseline and RFC 3246.
- Loss should be no more than 0.5 percent.
- One-way Latency (mouth-to-ear) should be no more than 150 ms.
- Average one-way Jitter should be targeted under 30 ms.
- 21–320 kbps of guaranteed priority bandwidth is required per call (depending on the sampling rate, VoIP codec and Layer 2 media overhead).

Voice quality is directly affected by all three QoS quality factors: loss, latency and jitter.

## Signaling Traffic

The following are the key QoS requirements and recommendations for Call Signaling traffic:

- Call-Signaling traffic should be marked as DSCP CS3 per the QoS Baseline (during migration, it may also be marked the legacy value of DSCP AF31).
- 265 bps per (phone+gateway) of guaranteed bandwidth is required for voice control traffic; more may be required, depending on whether call signaling encryption is in use.

It is expected that some MPLS sites will have ISDN backup for business continuity. It is recommended that AT&T should ensure that Unified Communications voice signaling and media traffic is blocked from traversing these ISDN links (unless the ISDN links are sized and QoS enabled to cater for this traffic). This will ensure Unified Communications devices will fallback to SRST when the WAN is running in ISDN backup mode.

## Voice Gateways and SRST

### Cisco Voice Gateway Types

AT&T supports Cisco ISR routers to support local PSTN access on customer premise

### Gateway Protocols

SIP is the preferred gateway protocol.

### Site Remote Survivability Telephony (SRST)

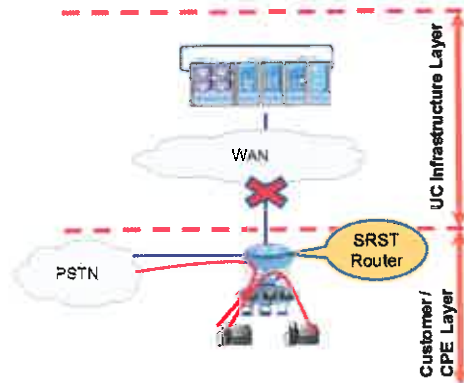
In a centralized Cisco Unified Communication Manager environment, IP phones can lose connectivity to Cisco Unified Communication Manager when the WAN is down or a Cisco Unified Communication Manager server becomes unreachable.

SRST provides a temporary call processing service for IP phones in remote branch offices to continue operation. The Survivable Remote Site Telephony (SRST) feature provides basic IP telephony backup

services so that IP phones can fall back using the router in local branch offices when losing keepalives to the Cisco Communication Manager.

The SRS Telephony feature leverages existing IOS gateway features to provide basic telephony service such as basic dialing, conferencing, MoH, caller ID, calling name, etc.

AT&T will offer SRST to its different end customers.



**Figure 36 SRST**

## Fax and Modem

Analog fax/modem ports will be supported on CPE devices for end customers

## Call Admission Control

Already supported CAC features (i.e. on CUCM, router and SBC) should continue to work over HCS.

## Locations Based CAC

This can be used to manage the access link bandwidth for remote locations that are bandwidth constrained. This is the most likely scenario and the easiest option to deploy on the leaf clusters.

## SBC Based CAC

For the extra cluster calls, where the inter cluster call is a sub category, the CAC could be implemented at the SBC level based on the adjacency mechanism (assumes the use of Cisco SBC).

## Features and Functions

### Emergency Call

To be transparent for extension mobility users, the device CSS will contain the correct translation rule to format the calling number as the main site number. This call will be routed via central breakout accordingly.

# Unity Connection Architecture

---

## Overview

Cisco Unity Connection (CUCxn) is a feature-rich voice messaging platform that runs on the same Linux-based Cisco Unified Communications Operating System that is used by Cisco Unified Communications Manager. Connection scales to support enterprise organizations with up to 50,000 users. It includes an intuitive telephone interface, voice-enabled navigation of messages, and desktop access to messages directly from a PC.

Key features of Cisco Unity Connection include:

- Voicemail system integrated with CUCM for internal and external callers
- Voicemail access from IP-Phone or from a PSTN public number
- Desktop messaging with the Unity Inbox web client
- Desktop messaging with IMAP-based e-mail clients
- Personal call transfer rules, which allow call routing based on caller, time of day, Outlook calendar status, and other parameters
- Message notifications to pagers, SMS phones, and other devices
- Automated attendant capabilities
- (optional) - Text-to-speech (TTS), which allows access to Exchange e-mails from a telephone
- (optional) - Voice-enabled message navigation (such as play, delete, reply, forward)

Telephony User Interface (TUI) and end-user Graphical User Interface (GUI) is available in multiple languages since version 7.0. This is also true for the VoiceMail for Outlook client (VMO) and the optional Text-to-Speech Engine. The Optional Voice Recognition engine supports English only.

Full list of supported languages in different CUCxn components is referenced at the following URL:

[http://www.cisco.com/en/US/partner/docs/voice\\_ip\\_comm/connection/8x/requirements/8xcucsysreqs.html#wp190847](http://www.cisco.com/en/US/partner/docs/voice_ip_comm/connection/8x/requirements/8xcucsysreqs.html#wp190847)

CUCxn offers voicemail and integrated messaging. Integrated messaging offers the ability to Play, delete and save messages within email client, and to compose, reply to and forward messages as a voice message or as an email. This offers a user experience close to Unified Messaging, except that emails and voicemails are stored in different Message Stores on the server side, and in different Inboxes on the client side.

CUCxn avoids integration and dependency on Microsoft Exchange and Active Directory, which brings significant benefits for IT in terms of installation time and operations effort.

## Requirements for Installing Cisco Unity Connection on a Virtual Machine

- A physical host that meets Connection specifications and that is supported for use in a virtualized environment. See the Cisco Unity Connection 8.x Supported Platforms List at [http://www.cisco.com/en/US/partner/docs/voice\\_ip\\_comm/connection/8x/supported\\_platforms/8xcucspl.html](http://www.cisco.com/en/US/partner/docs/voice_ip_comm/connection/8x/supported_platforms/8xcucspl.html)
- The physical host must have a Fibre Channel or Fibre Channel over Ethernet (FCoE) connection to a storage area network (SAN).
- VMware ESXi Version 5 or later installed on the host server on which the Connection virtual machine will run.

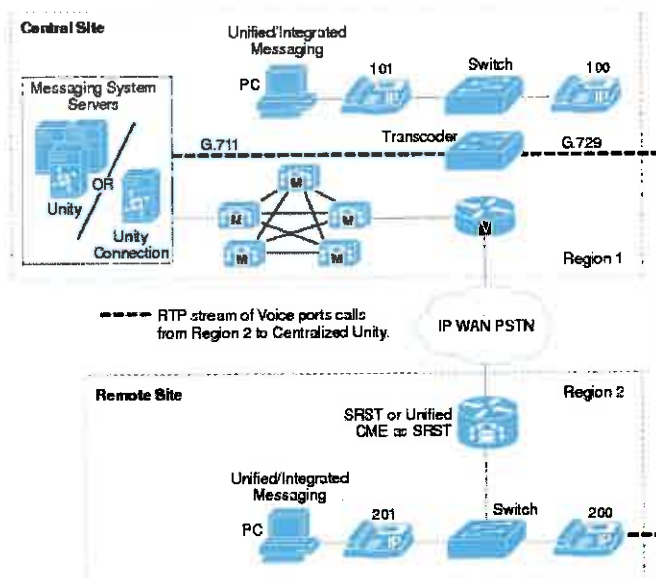
- Minimum VMware configuration as defined in Table 12 page 74.
- Connection version 8.0(2) or later.
- VMware High Availability (HA) is supported. Other VMware features, including Consolidated Backup, Dynamic Resource Scheduler, Fault Tolerance, Hot Add, Site Recovery Manager, Snapshots, Snapshots (with memory), Storage vMotion, vMotion, VMSafe, and vStorage Thin Provisioning are not supported.
- Accessing a USB key is not supported.
- At least one processor core must be available for the VMware hypervisor.
- All virtual disks assigned to the Connection virtual machine must be configured in independent-persistent mode, which provides the best storage performance.
- Installing applications other than Cisco Unified Communications applications on a physical host is not supported.
- A network time protocol (NTP) server must be accessible to the Connection server.

Notes:

- When configuring a Connection cluster, you can install Connection on one physical server and one virtual machine, or on two virtual machines, but the two virtual machines must be on separate physical hosts. When using blades as hosts, we recommend that the blades be on separate chassis.
- Connection 7.1(3) is required to migrate from a physical server running Connection 7.1(2) or earlier to a virtual server when the physical Connection server is not supported for use with Connection 8.x. However, after you complete the migration, you must upgrade the Connection virtual machine to version 8.0(2) or later. Running an earlier version in a production virtual environment is not supported.

## Centralized Messaging and Centralized Call Processing

In centralized messaging, the voice messaging server is located in the same site as the Unified CM cluster. With centralized call processing, subscribers may be located either remotely and/or locally to the cluster and messaging server(s).

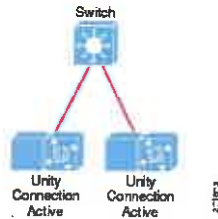


**Figure 37 Centralized Messaging with Centralized Call Processing**



## Redundancy

Cisco Unity Connection supports messaging redundancy and load balancing in an active-active redundancy model consisting of two servers, a primary and a secondary, configured as an active/active redundant pair of servers, where both the primary and secondary servers actively accept calls as well as HTTP and IMAP requests.



**Figure 38 Redundancy of Cisco Unity Connection Messaging**

Cisco Unity Connection SIP trunk implementation requires call forking for messaging redundancy functionality. Currently, Unified CM does not support call forking on SIP trunks. When using SIP trunks with a Cisco Unity Connection server pair in active/active redundancy, Cisco recommends that you configure two separate SIP trunks, one to each server in the server pair, and add them to the same route group associated to the same route list. This configuration allows Unified CM to load-balance calls to the two servers.

## Deploying Cisco Unity Connection with Unified CM

### Managing Bandwidth

Cisco Unity Connection relies on Unified CM to manage bandwidth and to route calls. Unified CM provides regions and locations for call admission control.

### Cisco Unity Connection Operation

Cisco Unity Connection handles transcoding operations differently than Cisco Unity. In Cisco Unity Connection, a call in any codec format supported by Cisco Unity Connection SCCP or SIP signaling (G.711 mu-law, G.711 a-law, G.729, iLBC, and G.722) will always be transcoded to Linear PCM. From Linear PCM, the recording is encoded in the system-level recording format (Linear PCM, G.711 mu-law/a-law, G.729a, or G.726), which is set system-wide in the general configuration settings (G.711 mu-law is the default). As such the overall impact of transcoding in Cisco Unity Connection is quite different from Cisco Unity. We refer to the codec negotiated between the calling device and Unity Connection as the "line codec," and we refer to the codec set in the system-level recording format as the "recording codec."

Because transcoding is inherent in every connection, there is little difference in system impact when the line codec differs from the recording codec. The exception to this is when using iLBC or G.722. G.722 and iLBC require more computation to transcode, therefore they have a higher system impact. G.722 and iLBC use approximately twice the amount of resources as G.711 mu-law. The subsequent impact this has is that a system can support only half as many G.722 or iLBC connections as it can G.711 mu-law connections.

As a general rule, Cisco recommends leaving the default codec as G.711.

**Table 16 Codec Characteristics**

Recording Format (Codec)	Audio Quality	Supportability	Disk Space (Bandwidth)
Linear PCM	Highest	Widely supported	16 kbps
G.711 mu-law and a-law	Moderate	Widely supported	8 kbps

Recording Format (Codec)	Audio Quality	Supportability	Disk Space (Bandwidth)
G.729a	Lowest	Poorly supported	1 kbps
G.726	Moderate	Moderately supported	3 kbps
GSM 6.10	Moderate	Moderately supported	1.6 kbps

## Version

For integrations through a SIP trunk, versions of Connection 8.x and Cisco Unified CM are supported only in the combinations listed in the table below.

**Table 17 Supported Versions for CUCXN 11.x and CUCM**

CUCM	CUCM
11.X	10.6

## CUCM SIP Trunk Integration Guide for CUCxn Release 10.6

The Cisco Unified Communications Manager SIP trunk integration makes connections through a LAN or WAN. A gateway provides connections to the PSTN.

## Requirements

The Cisco Unified CM SIP integration supports configurations of the following components:

### CUCM

- CUCM 10.x
- For the CUCM extensions, one of the following configurations:
  - Only SIP phones that support DTMF relay as described in RFC-2833 (Best practice).
  - Both SCCP phones and SIP phones (older SCCP phone models may require a MTP to function correctly).
- For multiple CUCM clusters, the capability for users to dial an extension on another CUCM cluster without having to dial a trunk access code or prefix.

### CUCxn

- The applicable version of CUCxn (for HCS, this is provided in the Software Versions documentation).
- CUCxn installed and ready for the integration, as described in the Installation Guide for CUCxn at [http://www.cisco.com/en/US/products/ps6509/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html)
- A license that enables the applicable number of voice messaging ports.

## Call Information

The phone system sends the following information with forwarded calls:

- The extension of the called party
- The extension of the calling party (for internal calls) or the phone number of the calling party (if it is an external call and the system uses caller ID)
- The reason for the forward (the extension is busy, does not answer, or is set to forward all calls)

CUCxn uses this information to answer the call appropriately. For example, a call forwarded to CUCxn is answered with the personal greeting of the user. If the phone system routes the call without this information, CUCxn answers with the opening greeting.

## Integration Functionality

The Cisco Unified CM SIP trunk integration with Cisco Unity Connection provides the following features:

- Call forward to personal greeting
- Call forward to busy greeting
- Caller ID
- Easy message access (a user can retrieve messages without entering an ID; Cisco Unity Connection identifies a user based on the extension from which the call originated; a password may be required)
- Identified user messaging (Cisco Unity Connection automatically identifies a user who leaves a message during a forwarded internal call, based on the extension from which the call originated)
- Message waiting indication (MWI)

## End-User Features

- Flexible User Interface
- Automated Attendant Functionality
- Dial Plan Flexibility: Partitions and Search Spaces
- Languages
- Access to Calendar, Meeting, and Contact Information
- Access to Emails in an External Message Store
- Desktop Message Access
- Mobile Clients
- Fax Messages

## Flexible User Interface

There are two ways in which users can interact with Cisco Unity Connection by phone:

1. Phone keypad keys
2. Voice commands

The Connection conversations can be customized both by administrators and by end users to maximize company and individual productivity.

To maximize the productivity of mobile workers, consider enabling the speech-activated voice command interface. This interface allows users to browse and manage voice messages and to call other Connection users or personal contacts by using simple, natural speech commands.

The phone interface also allows for access to Microsoft Exchange calendars, contacts, and emails, and to Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express meetings.

## Automated Attendant Functionality

Cisco Unity Connection includes a full-featured automated attendant that is customizable to suit the needs of your organization. Connection provides a number of different call management elements that you can combine to customize how your system handles calls and collects input from callers.

## Dial Plan Flexibility: Partitions and Search Spaces

Dial plan flexibility is supported through the use of partitions and search spaces, with which you can segment the Cisco Unity Connection directory for both dialing and addressing. For example, partitions and search spaces can be configured to allow for overlapping extensions, abbreviated dialing, or multi-tenant configurations.

## Languages

When multiple languages are installed, you can configure the language for system prompts that are played to users and callers. Separate greetings can be recorded for users and call handlers in each language that is installed on the system. Routing rules can be configured to set the language for a call based on how the call reached the system.

## Access to Calendar, Meeting, and Contact Information

When Cisco Unity Connection is configured for calendar integration, users can access calendar and meeting information from Cisco Unified MeetingPlace, Cisco Unified MeetingPlace Express, and Microsoft Exchange, and can import Exchange contacts for use by rules created in the Personal Call Transfer Rules web tool and for use by voice commands when placing outgoing calls.

## Desktop Message Access

Cisco Unity Connection supports access to voice messages through a wide range of desktop clients, including:

- **IMAP clients**—Third-party IMAP clients such as email clients are supported for accessing voice messages from Connection. Users can read, reply to, and forward messages from these types of clients.
- **Cisco Unity Connection ViewMail for Microsoft Outlook plug-in**—In addition to basic IMAP access to Cisco Unity Connection voice messages, the Cisco Unity Connection ViewMail for Microsoft Outlook form allows playing and recording messages by using either the phone or workstation speakers and microphones. Users can compose, read, reply to, and forward messages when using ViewMail.
- **Cisco Unity Inbox**—The Cisco Unity Inbox is a web tool available on the Cisco Personal Communications Assistant (PCA) website. Users can compose, read, reply to, and forward messages from the Cisco Unity Inbox.

- **Cisco Unified Personal Communicator**—Cisco Unified Personal Communicator is a desktop client that allows users to play voice messages. Users can read and delete messages from Cisco Unified Personal Communicator.
- **Cisco Unified Messaging with IBM Lotus Sametime**—Cisco Unified Messaging with IBM Lotus Sametime integrates Connection voicemail into the IBM Lotus Sametime instant messaging application, allowing users to play their voice messages within Lotus Sametime. A list of all voice messages, including the caller name or number and the date and time, are displayed in a panel on the client window. Users simply click to play their voice messages. They can also sort and delete messages directly from the Lotus Sametime application.
- **Cisco Phone View**—Cisco Unity Connection Phone View allows users to display voice messages on the LCD screen of a Cisco IP phone and to play the voice messages. This feature uses either touchtone keys or voice commands. The criteria that you use to search for messages depends on the conversation version that you are using.
- **RSS Feeds**—Another alternative to checking messages by phone or by using the Cisco Unity Inbox or an IMAP client, users can retrieve voice messages by using an RSS (Really Simple Syndication) reader. When a user marks a message as read, the message is no longer displayed in the RSS reader, but a saved copy is available in the Connection mailbox of the user.

## Mobile Clients

Available mobile clients include Jabber 9.0 for iPhone, iPad, Android, MAC and PC

## Fax Messages

Cisco Unity Connection can integrate with Cisco Fax Server 9.0 or later to support fax messages. Users can send a fax to a fax machine for printing (users can specify the fax number by phone), download a fax from a supported IMAP client, and forward fax messages to other Connection users.



# Cisco Presence Architecture

---

## Overview

The Cisco Unified Presence server (CUP) uses standards-based SIP, SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE), and Extensible Messaging and Presence Protocol (XMPP) to provide a common demarcation point for integrating clients and applications into the Cisco Unified Communications System.

CUP also provides an HTTP interface that has a configuration interface through Simple Object Access Protocol (SOAP), a presence interface through Representational State Transfer (REST), and a presence, instant messaging, and roster interface through JabberWerx AJAX. The JabberWerx AJAX interface communicates to the Bidirectional-streams Over Synchronous HTTP (BOSH) interface on the Extensible Communications Platform within Cisco Unified Presence.

The CUP server collects, aggregates, and distributes user capabilities and attributes using these standards-based SIP, SIMPLE, XMPP, and HTTP interfaces.

The core components of the CUP server consist of:

- the Jabber Extensible Communications Platform (XCP), which handles presence, instant messaging, roster, routing, policy, and federation management;
- the Rich Presence Service, which handles presence state gathering, network-based rich presence composition, and presence-enabled routing functionality;
- the support for ad-hoc group chat storage with persistent chat and message archiving handled to an external database. If persistent chat is enabled, ad-hoc rooms are stored to the external PostgreSQL database for the duration of the ad-hoc chat. This allows a room owner to escalate an ad-hoc chat to a persistent chat; otherwise, these ad-hoc chats are purged from PostgreSQL at the end of the chat. If persistent chat is disabled, ad-hoc chats are stored in volatile memory for the duration of the chat.

Applications (either Cisco or third-party) can integrate presence and provide services that improve the end user experience and efficiency.

By default, the CUP server contains the IP Phone Messenger application to allow for instant messaging and presence status using Cisco Unified IP Phones. In addition, Cisco Unified Personal Communicator is a supported client of the CUP server that also integrates instant messaging and presence status.

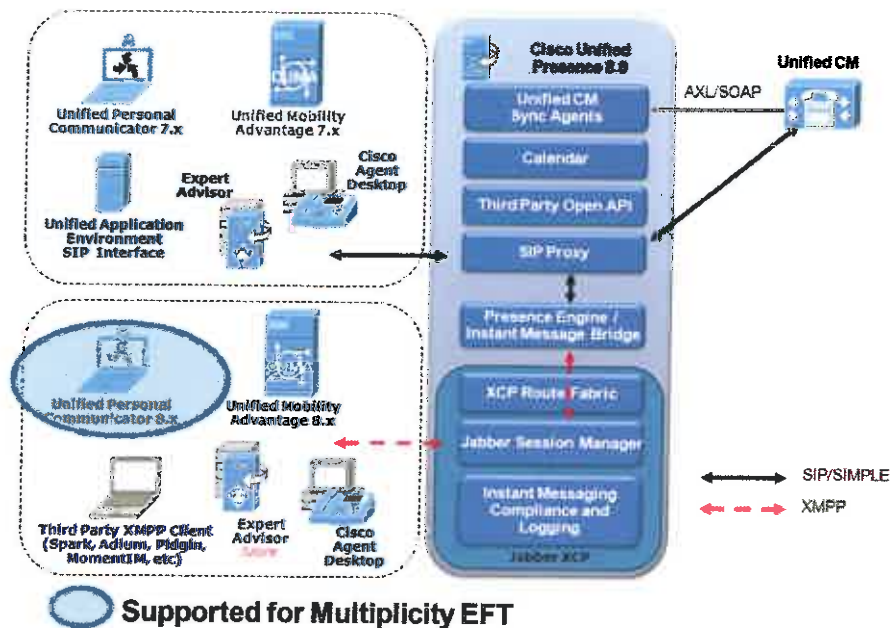


Figure 39 CUP 8.0 Architecture

## Cisco Unified Presence Components

CUP consists of many components that enhance the value of a Cisco Unified Communications system. The main presence component of the solution is the CUP server, which incorporates the Jabber Extensible Communications Platform and supports SIP/SIMPLE and Extensible Messaging and Presence Protocol (XMPP) for collecting information regarding a user's availability status and communications capabilities.

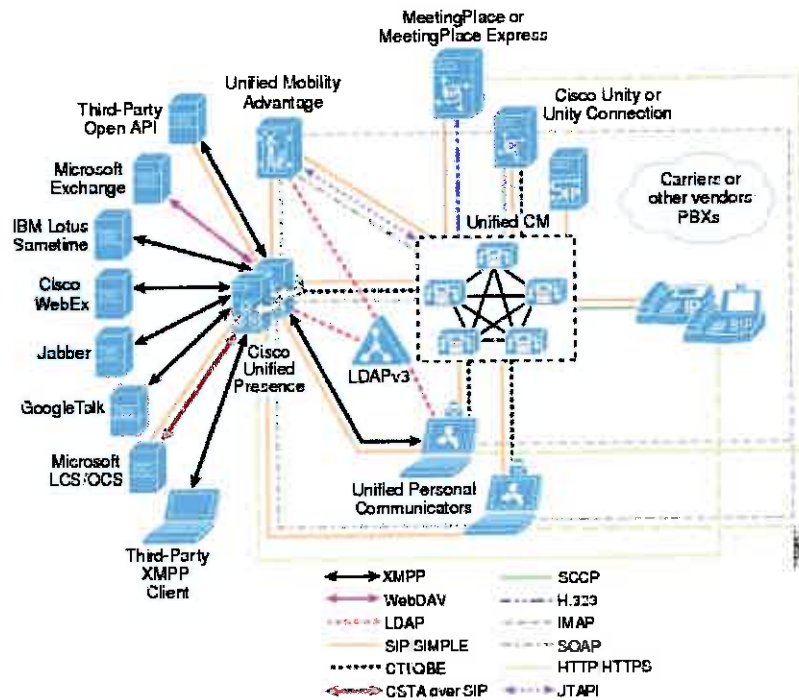
The user's availability status indicates whether or not the user is actively using a particular communications device such as a phone. The user's communications capabilities indicate the types of communications that user is capable of using, such as video conferencing, web collaboration, instant messaging, or basic audio.

The aggregated user information captured by the CUP server enables Cisco Unified Personal Communicator, Cisco Unified Communications Manager applications, and third-party applications to increase user productivity. These applications help connect colleagues more efficiently by determining the most effective form of communication.

The CUP basic architecture for this project encompasses the following components:

- Cisco Unified Presence server (CUPS)
- Cisco Unified Communications Manager (CUCM)
- Cisco Unified Personal Communicator (CUPC) – PC based software client
- Cisco Unity Connection (optional)
- Lightweight Directory Access Protocol (LDAP) Server v3.0
- Cisco Unified IP Phones

The following figure illustrated CUP components.



**Figure 40 CUP Components**

Note: In HCS version 8.0.2 there is no support for MeetingPlace, WebEx, Googletalk, IBM, CUMA, etc.

## Unified CM Presence Guidelines

Unified CM enables the system administrator to configure and control user phone state presence capabilities from within Unified CM Administration. Observe the following guidelines when configuring presence within Unified CM:

- Select the appropriate model of Cisco Unified IP Phones that have the ability to display user phone state presence status.
- Define a presence policy for presence users.
  - Use SUBSCRIBE calling search spaces to control the routing of a watcher presence-based SIP SUBSCRIBE message to the correct destinations.
  - Use presence groups to define sets of similar users and to define whether presence status updates of other user groups are allowed or disallowed.
- Call history list presence capabilities are enabled on a global basis; however, user status can be secured by using a presence policy.
- BLF speed dials are administratively controlled and are not impacted by the presence policy configuration.

## Unified CM Presence Performance

CUP server clusters support single-server as well as multi-server configurations. However, if multiple servers are used, each server must be on the same type of server platform as the publisher server.

The table below lists the hardware platform requirements for the CUP server as well as the maximum number of users supported per platform. The maximum number supported for a CUP cluster is 15,000 users.

**Table 18 CUP Server Platforms and Number of Users Supported**

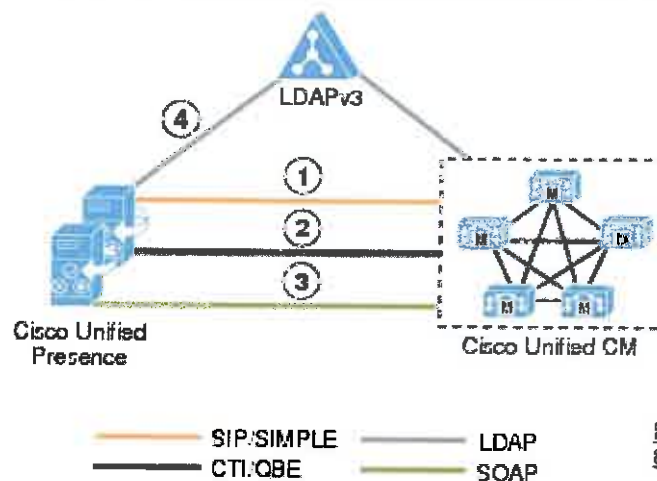
Server Platform	Users Supported per Platform
Cisco UCS B-Series Blade Server (2 vCPU, 4 GB RAM, 80 GB drive, 1 vNIC)	2500
Cisco UCS B-Series Blade Server (4 vCPU, 4 GB RAM, two 80 GB drives, 1 vNIC)	5000

**Notes:**

- Application level redundancy for CUPS is not intended to be implemented for the AT&T HCS system

## CUP Single-Cluster Deployment

The figure below represents the communication protocols between Cisco Unified Presence, the LDAP server, and Cisco Unified Communications Manager for basic functionality.

**Figure 41 Interactions Between CUP Components**

1. The SIP connection between the CUP server and Unified CM handles all the phone state presence information exchange.

Unified CM configuration requires the CUP servers to be added as application servers on Unified CM and also requires a SIP trunk pointing to the CUP server. The address configured on the SIP trunk could be a Domain Name System (DNS) server (SRV) fully qualified domain name (FQDN) that resolves to the CUP servers, or it could simply be an IP address of an individual CUP server. CUP 7.0(3) and later releases handle the configuration of the CUCM application server entry automatically through AXL/SOAP once the administrator adds a node in the system topology page through CUP administration.

**Notes:**

- a. If DNS is highly available within your network and DNS SRV is an option, configure the SIP trunk on Unified CM with a DNS SRV FQDN of the CUP publisher and subscriber. Also configure the Presence Gateway on the CUP server with a DNS SRV FQDN of the Unified CM subscribers, equally weighted. This configuration will allow for presence messaging to be shared equally among all the servers used for presence information exchange.

- b. If DNS is not highly available or not a viable option within your network, use IP addressing. When using an IP address, presence messaging traffic cannot be equally shared across multiple Unified CM subscribers because it points to a single subscriber.
  - c. Unified CM provides the ability to further streamline communications and reduce bandwidth utilization by means of the service parameter CUP PUBLISH Trunk, which allows for the PUBLISH method (rather than SUBSCRIBE/NOTIFY) to be configured and used on the SIP trunk interface to Cisco Unified Presence. Once the CUP PUBLISH Trunk service parameter has been enabled, the users must be associated with a line appearance and not just a primary extension.
2. The Computer Telephony Integration Quick Buffer Encoding (CTI-QBE) connection between CUP and Unified CM is the protocol used by presence-enabled users in CUP to control their associated phones registered to Unified CM. This CTI communication occurs when Cisco Unified Personal Communicator is using Desk Phone mode to do Click to Call or when Microsoft Office Communicator is doing Click to Call through Microsoft Live Communications Server 2005 or Office Communications Server 2007.

Unified CM configuration requires the user to be associated with a CTI Enabled Group, and the primary extension assigned to that user must be enabled for CTI control (checkbox on the Directory Number page). The CTI Manager Service must also be activated on each of the Unified CM subscribers used for communication with the CUP publisher and subscriber. Integration with Microsoft Live Communications Server 2005 or Office Communications Server 2007 requires that you configure an Application User, with CTI Enabled Group and Role, on Unified CM.

CUP CTI configuration (CTI Server and Profile) for use with Cisco Unified Personal Communicator is automatically created during the database synchronization with Unified CM. All Cisco Unified Personal Communicator CTI communication occurs directly with Unified CM and not through the CUP server.

Note:

CUP CTI configuration (CTI Gateway) for use with Microsoft Live Communications Server 2005 or Office Communications Server 2007 requires you to set the CTI Gateway address (Cisco Unified Communications Manager Address) and a provider, which is the application user configured previously in Unified CM. Up to eight Cisco Unified Communications Manager Addresses can be provisioned for increased scalability. Only IP addresses can be used for CTI gateway configuration in the CUP server.

3. The AXL/SOAP interface handles the database synchronization from Unified CM to populate the CUP database. No additional configuration is required on Unified CM. CUP security configuration requires you to set a user and password for the Unified CM AXL account in the AXL configuration.

Note:

The Sync Agent Service Parameter, User Assignment, set to balanced by default, will load-balance all users equally across all servers within the CUP cluster. The administrator can also manually assign users to a particular server in the CUP cluster by changing the User Assignment service parameter to None.

4. The LDAP interface is used for LDAP authentication of Cisco Unified Personal Communicator users during login.
5. Unified CM is responsible for all user entries via manual configuration or synchronization directly from LDAP, and CUP then synchronizes all the user information from Unified CM. If a Cisco Unified Personal Communicator user logs into the CUP server and LDAP authentication is enabled on Unified CM, CUP will go directly to LDAP for the Cisco Unified Personal Communicator user authentication using the Bind operation. Once Cisco Unified Personal Communicator is authenticated, CUP forwards the information to Cisco Unified Personal Communicator to continue login.

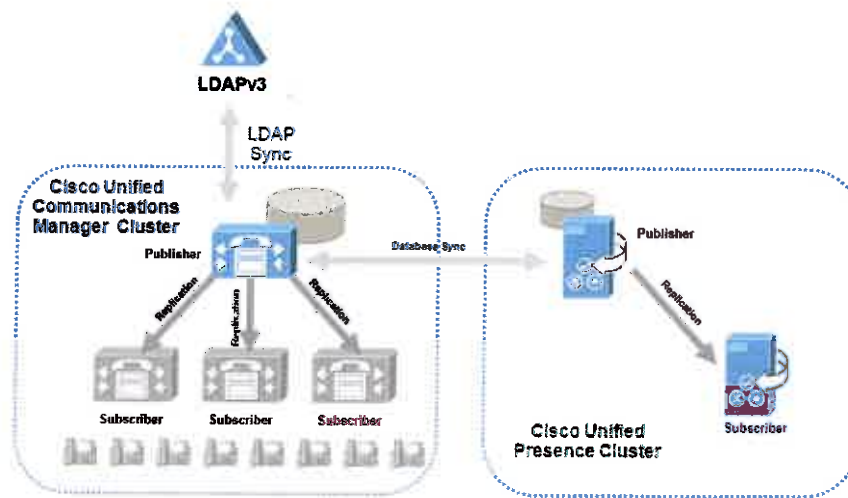
When using Microsoft Active Directory, consider the choice of parameters carefully. Performance of CUP might be unacceptable when a large Active Directory implementation exists and the

configuration uses a Domain Controller. To improve the response time of Active Directory, it might be necessary to promote the Domain Controller to a Global Catalog and configure the LDAP port as 3268.

## Cisco Unified Presence Cluster

The CUP server uses the same underlying appliance model and hardware used by Unified CM as well as Unified CM on the Cisco Unified Computing System (UCS) platform, including a similar administration interface.

CUP consists of up to six servers, including one designated as a publisher, which utilize the same architectural concepts as the Unified CM publisher and subscriber. Within a CUP cluster, individual servers can be grouped to form a subcluster, and the subcluster can have at most two servers associated with it. The figure below shows the basic topology for a CUP cluster.



**Figure 42 Basic CUP Deployment**

For the AT&T HCS network, we will deploy only CUP publishers.

## Design Considerations for Cisco Unified Presence

- If LDAP integration is possible, LDAP synchronization with Unified CM should be used to pull all user information (number, ID, and so forth) from a single source. **However, if the deployment includes both an LDAP server and Unified CM that does not have LDAP synchronization enabled, then the administrator should ensure consistent configuration across Unified CM and LDAP when configuring user directory number associations.**
- CUP marks Layer 3 IP packets via Differentiated Services Code Point (DSCP). CUP marks all call signaling traffic based on the Differential Service Value service parameter under SIP Proxy, which defaults to a value of DSCP 24 (PHB CS3).
- Presence Policy for CUP is controlled strictly by a defined set of rules created by the user.
- The CUP publisher and subscriber must be co-located with the Unified CM publisher.
- Use the service parameter CUP PUBLISH Trunk to streamline SIP communication traffic with the CUP server.
- Associate presence users in Unified CM with a line appearance, rather than just a primary extension, to allow for increased granularity of device and user presence status. When using the service parameter CUP PUBLISH Trunk, you must associate presence users in Unified CM with a line appearance.



- A Presence User Profile (the user activity and contact list contacts and size) must be taken into consideration for determining the server hardware and cluster topology characteristics.
- Use the User Assignment Mode sync agent parameter default of balanced for best overall cluster performance.
- CUP requires an external database instance for each server within in the cluster for persistent chat, and one database instance per cluster for message archiving and native compliance. The database instances can share the same hardware; however, the only external database supported is PostgreSQL.
- CUP supports a total of 15,000 users per cluster. The sizing for users must take into account the number of SIP/SIMPLE users and the number of XMPP users. XMPP users have slightly better performance because SIP/SIMPLE users employ the IM Gateway functionality into the Jabber XCP architecture.
- When migrating a CUP deployment from version 7.x to 8.0, you must deactivate the presence engine service prior to the upgrade and re-enable it after all servers have been upgraded to 8.0.
- All eXtensible Communications Platform (XCP) communications and logging are stored in GMT and not localized to the installed location.
- CUP 8.0 is compatible with Unified CM 6.x, 7.x, and 8.x.
- Cisco Unified Communications Manager Business Edition (Unified CMBE) 7.x supports LDAP synchronization, which should be enabled when integrating Unified CMBE with Cisco Unified Presence.

For a complete listing of ports used by Cisco Unified Presence, refer to Port Usage Information for Cisco Unified Presence, available at

[http://www.cisco.com/en/US/products/ps6837/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html)

# Mobility Architecture

---

## Overview

Cisco mobility applications provide the enterprise features to mobile worker. Mobility users can handle calls to their enterprise directory number, not only on their desk phone, but also on one or more remote phones. Mobility users can also make calls from a remote phone as if they are dialing inside the enterprise. In addition, mobility users can take advantage of enterprise features such as hold, transfer, and conference as well as enterprise applications such as voicemail, conferencing, and presence on their mobile phones. This ensures continued productivity for users even when they are traveling outside the organization.

**For the purposes of the HCS 8.0.2, the following categories of applications will be offered:**

- **Mobile Connect (SNR)**
- **Mobile Connect Mid-Call Features**
- **Dual-Mode Phones and Clients**

## Features

### Mobile Connect (SNR)

The Mobile Connect feature allows an incoming call to an enterprise user to be offered to the user's IP desk phone as well as up to 10 configurable remote destinations. Typically a user's remote destination is their mobile or cellular telephone. Once the call is offered to both the desktop and remote destination phone(s), the user can answer at any of those phones. Upon answering the call on one of the remote destination phones or on the IP desk phone, the user has the option to hand off or pick up the call on the other phone.

Mobile Connect supports these use case scenarios:

- **Desk Phone Pickup** (i.e. receiving an outside call on desktop or cellular phone): An outside caller dials the user's desktop extension. The desktop phone and cellular phone ring simultaneously. When the user answers one of the phones, the other phone stops from a desktop telephone to a cellular phone. The user can switch from the desktop phone to cellular phone during a call without losing the connection. Switching is supported for incoming and outgoing calls.
- **Remote Destination Phone Pickup** (i.e. moving back from a cellular phone to a desktop phone): If a call was initiated to or from the desktop phone and then shifted to the cellular phone, the call can be shifted back to the desktop phone.

Access lists can be configured within Cisco Unified CM and associated to a remote destination. Access lists are used to allow or block inbound calls (based on incoming caller ID) from being extended to a mobility-enabled user's remote destinations. Furthermore, these access lists are invoked based on the time of day.

### Mobile Connect Mid Call Features

Once a user answers a Mobile Connect call at the remote destination device, the user can invoke mid-call features such as hold, resume, transfer, conference, and directed call park by sending DTMF digits from the remote destination phone to CUCM via the PSTN. When the mid-call feature hold, transfer, conference, or directed call park is invoked, MoH is forwarded from CUCM to the held party. In-progress calls can be transferred to another phone or directed call park number, or additional phones can be conferenced using enterprise conference resources.

Mid-call features are invoked at the remote destination phone by a series of DTMF digits forwarded to CUCM. Once received by CUCM, these digit sequences are matched to the configured Enterprise Feature Access Codes for Hold, Exclusive Hold, Resume, Transfer, and Conference CUCM, and the appropriate function is performed.

Mid Call Features can be invoked on Smartphones and manually. The table below shows the invocation. If smart client applications do not provide programmed softkeys for automating mid-call features, the manual key sequences should be used.

## Dual-Mode Phones and Clients

Dual-mode phones and the clients that run on them afford an enterprise the ability to provide customized voice and data services to users while inside the enterprise and to leverage the mobile carrier network as a backup provider of general voice and data services, all by using a single mobile phone.

For example, voice over IP (VoIP) calls made on the enterprise network will typically incur less cost than those same calls made over the mobile voice network.

For HCS 8.0.2, we will cover two specific dual-mode clients:

1. Cisco Mobile: A dual-mode client for the iPhone mobile device, providing the ability to make VoIP calls on the enterprise WLAN network. Note: access corporate directory and voicemail services are not covered in HCS 8.0.2.
2. Nokia Call Connect: A dual-mode client for Nokia mobile devices, providing the ability to make VoIP calls on the enterprise WLAN network. Note: access corporate directory and other applications and services are not covered in HCS 8.0.2.

## Design Considerations

### Mobile Connect (SNR)

#### Design Requirements

Observe the following design recommendations when deploying Mobile Connect:

- End-to-end DTMF interworking must be carefully planned.
- Caller ID must be provided by the service provider for all inbound calls to the enterprise if Enterprise Feature Access Two-Stage Dialing or mid-call transfer, conference, and directed call park features are needed.
- Outbound caller ID must not be restricted by the service provider if there is an expectation that mobility-enabled users will receive the caller ID of the original caller at their remote destination rather than a general enterprise system number or other non-meaningful caller ID. However, some providers restrict outbound caller ID on a trunk to only those DID's handled by that trunk. For this reason, a second PRI trunk that does not restrict caller ID might have to be acquired from the provider. To obtain an unrestricted PRI trunk, some providers might require a signed agreement from the customer indicating they will not send or make calls to emergency numbers over this trunk.
- Some providers allow unrestricted outbound caller ID on a trunk as long as the Redirected Dialed Number Identification Service (RDNIS) field or SIP Diversion Header contains a DID handled by the trunk. Beginning with Cisco Unified CM 7.1(3), the RDNIS or SIP Diversion Header for forked calls to remote destinations can be populated with the enterprise number of the user by checking the Redirecting Number IE Delivery - Outbound check box on the gateway or trunk configuration page.

- If a PSTN incoming call is answered at the remote destination, the voice media path will be hairpinned within the PSTN gateway utilizing two gateway ports. This utilization must be considered when deploying the Mobile Connect feature.
- Mobility users on a CUCMBE system can have a maximum of four remote destinations.

## Caveats

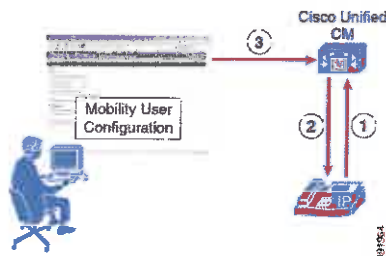
- Mobile Connect can support up to two simultaneous calls per user. Any additional calls that come in are automatically transferred to the user's voicemail.
- Mobile Connect does not work with Multilevel Precedence and Preemption (MLPP). If a call is preempted with MLPP, Mobile Connect features are disabled for that call.
- Mobile Connect services do not extend to video calls. A video call received at the desktop phone cannot be picked up on the cellular phone.
- The Unified CM Forced Authorization Code and Client Matter Code (FAC/CMC) feature does not work with Mobile Voice Access.
- Remote destinations must be Time Division Multiplex (TDM) devices or off-system IP phones on other clusters or systems. You cannot configure IP phones within the same Unified CM cluster as remote destinations.

## Architecture

The figure below depicts the message flows and architecture required for Mobile Connect.

The following sequence of interactions and events can occur between CUCM, the Mobile Connect user, and the Mobile Connect user's desk phone:

1. The Mobile Connect phone user who wishes to either enable or disable the Mobile Connect feature or to pick up an in-progress call on their remote destination phone pushes the Mobility softkey on their desk phone (step 1).
2. Unified CM returns the Mobile Connect status (On or Off) and offers the user the ability to select the Send Call to Mobile Phone option when the phone is in the Connected state, or it offers the user the ability to enable or disable the Mobile Connect status when the phone is in the On Hook state (step 2).
3. Mobile Connect users can use the Unified CM User Options interface to configure their own mobility settings via the web-based configuration pages located at the IP address of the Unified CM publisher server (step 3).



**Figure 43 Mobile Connect Architecture**

## High Availability

The Mobile Connect feature relies on the following components:

- CUCM servers
- PSTN gateway

Each component must be redundant or resilient in order for Mobile Connect to continue functioning fully during various failure scenarios.

## CUCM Server Redundancy

The CUCM server is required for the Mobile Connect feature. Unified CM server failures are non-disruptive to Mobile Connect functionality, assuming phone and gateway registrations are made redundant using Unified CM Groups.

In order for Mobile Connect users to use the Unified CM User Options web interface to configure their mobility settings (remote destinations and access lists), the Unified CM publisher server must be available. If the publisher is down, users will not be able to change mobility settings. Likewise, administrators will be unable to make mobility configuration changes to Unified CM. However, existing mobility configurations and functionality will continue.

Finally, changes to Mobile Connect status must be written by the system on the Unified CM publisher server. If the Unified CM publisher is unavailable, then enabling or disabling Mobile Connect will not be possible.

Note: In a virtualized environment where HA is enabled, publisher unavailability should be minimal.

## PSTN Gateway Redundancy

Because the Mobile Connect feature relies on the ability to extend additional call legs to the PSTN to reach the Mobile Connect users' remote destination phones, PSTN access redundancy is important.

Redundancy of PSTN access will be maintained up to the point of hand-off to the AT&T network. Beyond that redundancy is outside the scope of the HCS solution.

Regarding CUCM, the dial plan should provide redundancy for PSTN access by providing PSTN gateway redundancy (local and central breakout) and call re-routing capabilities as well as enough capacity to handle expected call activity.

## Mobile Connect Mid Call Features

In order to perform the transfer, conference, and directed call park mid-call features, a second call leg is generated by the remote destination phone to a system-configured Enterprise Feature Access DID that answers the call, takes user input (including PIN number, mid-call feature access code, and target number), and then creates the required call leg to complete the transfer, conference, or directed call park operation.

## Dual-Mode Phones and Clients

### Design Requirements

Observe the following design recommendations when deploying dual-mode phones and clients:

- Dual-mode phones must be capable of dual transfer mode (DTM) in order to be connected simultaneously to both the mobile voice and data network and the WLAN network. This allows the device to be reachable and able to make and receive calls on both the cellular radio and WLAN interface of the device. In some cases proper dual-mode client operation might not be possible if mobile voice and data networks do not support dual-connected devices.
- APs should be deployed with cell overlap of 20% for 2.4 GHz (802.11b/g) deployments. Channel overlap for 5 GHz (802.11a) deployments should overlap between 15% and 20%. This overlap

ensures that a dual-mode device can successfully roam from one AP to the next as the device moves around within a location, while still maintaining voice and data network connectivity.

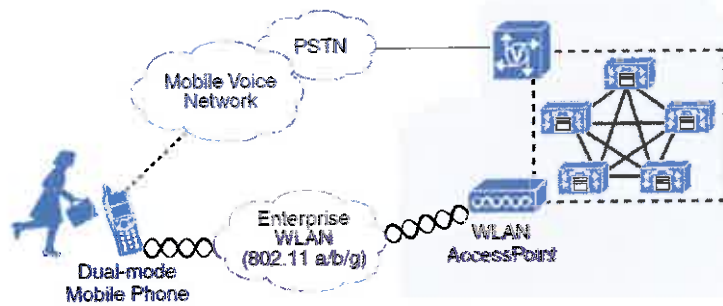
- APs should be deployed with cell power level boundaries (or channel cell radius) of -67 dBm in order to minimize packet loss. Furthermore, the same-channel cell boundary separation should be approximately 19 dBm. A same-channel cell separation of 19 dBm is critical for ensuring that APs or clients do not cause co-channel interference to other devices associated to the same channel, which would likely result in poor voice quality.
- Cisco recommends using only an enterprise class voice-optimized WLAN network for connecting dual-mode phones and clients. While most dual-mode phones and clients are capable of attaching to public or private WLAN access points or hotspots for connecting back to the enterprise through the Internet for call control and other Unified Communications services, Cisco cannot guarantee voice quality for these types of connections.
- The Unified Mobility Mobile Connect feature will not extend incoming calls to the dual-mode device's configured mobility identity if the dual-mode device is inside the enterprise and registered to Unified CM. This is by design in order to reduce utilization of enterprise PSTN resources. Only when the dual-mode device is unregistered will Mobile Connect extend incoming calls to the user's enterprise number out to the mobility identity number on the PSTN.
- When deploying dual-mode phones, Cisco recommends normalizing required dialing strings so that users reach a particular called destination by calling a single number, whether inside or outside the enterprise. Because dialing on the mobile network is typically done using full E.164 (with or without a preceding '+') and mobile phone contacts are typically stored with full E.164 numbers, Cisco recommends configuring the enterprise dial plan to accommodate full E.164 or full E.164 with preceding '+' for dual-mode phones.
- Cisco recommends that dual-mode phone users rely on the mobile voice network for making emergency calls and determining device and user location. This is because mobile provider networks typically provide much more reliable location indication than enterprise WLAN networks. To ensure that dual-mode phones rely exclusively on the mobile voice network for emergency and location services, configure dual-mode devices within Unified CM so that they do not have access to route patterns that allow calls to emergency numbers. Dual-mode phone users should be advised to make all emergency calls over the mobile voice network rather than the enterprise network.
- Nokia Call Connect 2.0 and later clients are capable of performing automatic hand-out and hand-in.
- Cisco recommends to increase the default 1500 byte MTU on MPLS VPN core network to 1508 bytes and above to avoid mobile client registration fragmentation issue. Cisco Mobile 8.0 on iPhone sends register message with DF bit set to 1 so no fragmentation is allowed which could prevent client to register to the CUCM if the MTU size in MPLS VPN core network is less than the register package size.

## Architecture

Dual-mode phones provide two physical interfaces or radios that enable the device to connect to both mobile voice and data carrier networks by means of traditional cellular or mobile network technologies and wireless local area networks (WLANs) using IEEE 802.11 standards.

**Note:** The use of the term dual-mode phone in this section refers specifically to devices with 802.11 radios in addition to the cellular radio for carrier voice and data network connectivity. Dual-mode devices that provide Digital Enhanced Cordless Telecommunications (DECT) or other wireless radios and/or multiple cellular radios are outside the scope.





**Figure 44 Dual-Mode Phone Architecture**

Figure above depicts the basic dual-mode solution architecture for incorporating dual-mode devices into a Cisco Unified Communications System. The dual-mode phone associates to the enterprise WLAN, and then the dual-mode client registers to Cisco Unified CM as an enterprise phone. Once registered, the dual-mode device relies on the underlying enterprise Cisco IP telephony network for making and receiving calls. Only when enterprise WLAN connectivity is unavailable, will the dual-mode phone fall back to the mobile voice network for making and receiving calls.

When the dual-mode phone is associated to the enterprise WLAN and the client is registered to CUCM, the phone will be reachable through the user's enterprise number. Any inbound calls to the user's enterprise number will ring the dual-mode phone. If the user has a Cisco IP desk phone, then the dual-mode client registration enables a shared line instance for the user's enterprise number so that an incoming call rings both the user's desk phone and the dual-mode phone.

When unregistered, the dual-mode client will not receive incoming enterprise calls at the dual-mode phone unless the user has been enabled for Cisco Unified Mobility and Mobile Connect (or single number reach) has been turned on for the user's mobile number.

## High Availability

Although dual-mode phones by their nature are highly available with regard to network connectivity, enterprise WLAN and IP telephony infrastructure high availability must still consider the following aspects:

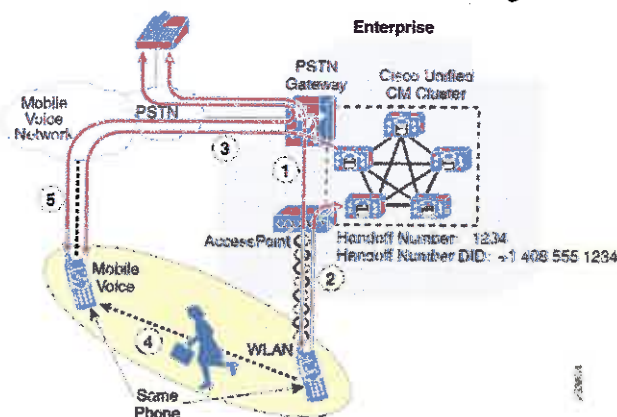
1. The enterprise WLAN must be deployed in a manner that provides redundant WLAN access. For example, APs and other WLAN infrastructure components should be deployed so that the failure of a wireless AP does not impact network connectivity for the dual-mode device. Likewise, WLAN management and security infrastructure must be deployed in a highly redundant fashion so that dual-mode devices are always able to connect securely to the network.
2. CUCM call processing and registration service high availability must be considered. Provided a redundant nature of the customer CUCM cluster in a virtualized environment, dual-mode device registration and call routing should be highly available even in scenarios of a CUCM server, UCS blade or UCS chassis failure.
3. Multiple PSTN gateways and call routing paths should be deployed to ensure highly available access to the PSTN.

## Capacity Planning

Capacity planning considerations for dual-mode phones are the same as for other IP telephony endpoints or devices that rely on the IP telephony infrastructure and applications for registration, call processing, and PSTN access services.

## Cisco Mobile Hand-Out (WLAN to Cellular)

- Step 1: There is an existing call between the iPhone dual-mode device associated to the enterprise WLAN and registered to Unified CM, and a phone on the PSTN network.
- Step 2: Because this is a manual process, the user must select the Use Mobile Network button from the in-call menu within the Cisco Mobile client, which signals to Unified CM the need to hand-out the call
- Step 3: Unified CM generates a call to the configured mobility identity number corresponding to this Cisco Mobile device through the enterprise PSTN gateway.
- Step 4: This call to the mobility identity is made to the mobile voice network or cellular interface of the iPhone. The user can now move out of the enterprise and away from WLAN network coverage.
- Step 5: In the meantime, the inbound call from Unified CM is received at the mobile voice network interface, and the user must answer the call manually to complete the hand-out. Once the inbound call on the cellular interface is answered, the RTP stream that was traversing the WLAN is redirected to the PSTN gateway, and the call continues uninterrupted between the Cisco Mobile dual-mode client and the original PSTN phone with the call anchored in the enterprise gateway.



**Figure 45 Cisco Mobile Dual-Mode Hand-Out (WLAN-to-Mobile Voice Network)**

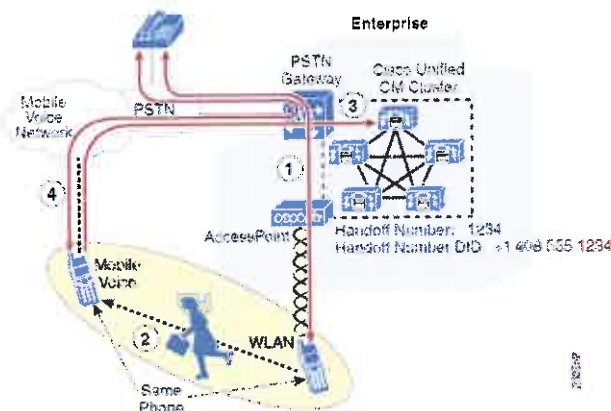
## Cisco Mobile Hand-In (Cellular to WLAN)

Cisco Mobile does not support hand-in. In scenarios where an in-progress call is active between the iPhone mobile voice network or cellular interface and an enterprise phone (or a PSTN phone with the call anchored in the enterprise gateway), the only way to move the call to the WLAN interface of the iPhone is to hang up the call and redial once the Cisco Mobile client has associated to the enterprise WLAN and registered to Unified CM.

## Nokia Call Connect Hand-Out (WLAN to Cellular)

- Step 1: there is an existing call between the Nokia dual-mode device associated to the enterprise WLAN and registered to CUCM, and a phone on the PSTN network.
- Step 2: The Nokia dual-mode user begins to leave the enterprise.
- Step 3: As the WLAN signal strength drops below -78 dBm (default value for the WLAN HO threshold setting in VCC) for a period of 1,000,000 microseconds (1 second, default value for the WLAN HO hysteresis setting in VCC), a silent background call is opened to the configured Cellular Handover Number in VCC and corresponding to the Handoff Number configured in CUCM over the mobile voice network and PSTN into the enterprise PSTN gateway and is delivered to CUCM.

- Step 4: Once received, the calling number is checked against all configured mobility identities on the system, and assuming a match is found, the RTP stream that was traversing the WLAN is now redirected to the PSTN gateway and the call is continued uninterrupted between the dual-mode device and the original PSTN phone with the call anchored in the enterprise gateway.

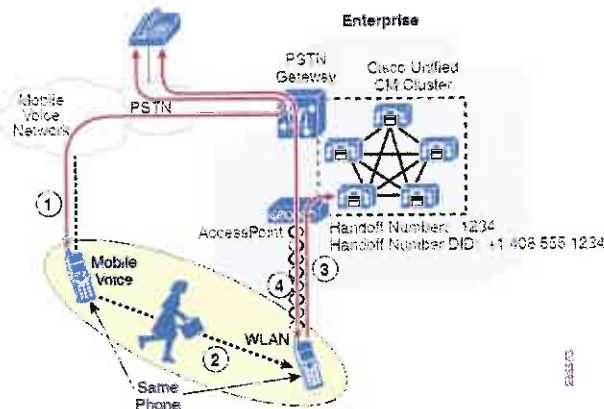


**Figure 46 Nokia Call Connect Dual-Mode Hand-Out (WLAN-to-Mobile Voice Network)**

The Nokia Call Connect dual-mode client also supports manual hand-out using the Switch to Cellular or Handover to GSM in-call menu options depending on the device type and firmware version.

## Nokia Call Connect Hand-In (Cellular to WLAN)

- Step 1: There is an existing call between the Nokia dual-mode device on the mobile voice network and a phone on the PSTN network.
- Step 2: The Nokia dual-mode user moves into the enterprise
- Step 3: The device associates in the background to the WLAN infrastructure and registers to Unified CM. After registration, the device will wait for the amount of time specified by the WLAN HO hysteresis high setting in VCC (60 seconds by default), and then a silent background call is opened to the configured VoIP Handover Number in VCC, which corresponds to the Unified CM Handoff Number configured in Unified CM, and delivered to Unified CM.
- Step 4: Once received, the enterprise calling number is checked against configured Nokia S60 dual-mode phones on the system, and assuming a match is found, the call that was traversing the mobile voice network/PSTN and the enterprise PSTN gateway is now redirected to the WLAN network, and the call is continued uninterrupted between the dual-mode device and the original PSTN phone.



**Figure 47 Nokia Call Connect Dual-Mode Hand-In (Mobile Voice Network-to-WLAN)**

# Provisioning

## Mobile Connect (SNR)

In order to configure and provision the call routing behavior and dial plan implications of the Remote Destination Profile (RDP) configuration must be taken into account the following parameters:

- CSS
- Rerouting Calling Search Space
- Caller ID Matching and Enterprise Call Anchoring
- Caller ID Transformations

### CSS

This setting combines with the directory number or line-level CSS to determine which partitions can be accessed for mobility dialed calls.

### Rerouting Calling Search Space

This setting determines which partitions are accessed when calls are sent to a user's remote destination phone.

### Caller ID Matching and Enterprise Call Anchoring

Whenever an inbound call comes into the system, the presented caller ID for that call is compared against all configured remote destination phones. If a match is found, the call will automatically be anchored in the enterprise, thus allowing the user to invoke mid-call features and to pick up in-progress calls at their desk phone. This behavior occurs for all inbound calls from any mobility user's remote destination phone, even if the inbound call is not originated as a mobility call using Mobile Voice Access or Enterprise Feature Access. Automatic inbound caller ID matching for configured remote destination numbers is affected by whether the Matching Caller ID with Remote Destination service parameter is set to Partial or Complete Match.

### Caller ID Transformations

Any calls made into the cluster by configured remote destination numbers will automatically have their caller ID or calling number changed from the calling remote destination phone number to the enterprise directory number of the associated desk phone. This ensures that the active call caller ID display and call history log caller ID reflect a mobility user's enterprise desk phone number rather than their mobile phone number, and it ensures that any return calls are made to the user's enterprise number, thus anchoring those calls within the enterprise.

Likewise, calls from a remote destination phone to external PSTN destinations and anchored in the enterprise via Mobile Voice Access or Enterprise Feature Access two-stage dialing, or those calls forked to the PSTN as a result of Mobile Connect, will also have caller ID changed from the calling remote destination phone number to the associated enterprise directory number.

Finally, in order to deliver the calling party number as an enterprise DID number rather than an enterprise directory number to external PSTN phones, calling party transformation patterns can be used. By using calling party transformation patterns to transform caller IDs from enterprise directory numbers to enterprise DIDs, return calls from external destinations will be anchored within the enterprise because they will be dialed using the full enterprise DID number.

## Mobile Connect Mid Call Features

Media resource allocation for mid-call features such as hold and conference is determined by the Remote Destination Profile (RDP) configuration. The media resource group list (MRGL) of the device pool configured for the RDP is used to allocate a conference bridge for the conferencing mid-call feature. The User Hold Audio Source and Network Hold MoH Audio Source settings of the RDP, in combination with the media resource group list (MRGL) of the device pool, are used to determine the appropriate MoH stream to be sent to a held device.

## Dual-Mode Phones and Clients

### Cisco Mobile

Cisco Mobile is a dual-mode client for the Apple iPhone.

### Installation Steps

1. Once the client application is downloaded from the Apple Application Store and installed on the iPhone using iTunes, the iPhone can associate to the enterprise WLAN network and register to Unified CM as a SIP enterprise phone.
2. To provide registration and call control services to the Cisco Mobile dual-mode iPhone client, the device must be configured within Unified CM as a Cisco Dual-Mode for iPhone device type.
3. Next the iPhone must be configured to access the enterprise WLAN for connectivity based on the enterprise WLAN infrastructure and security policies.
4. Once the iPhone has been configured to access the WLAN, when the Cisco Mobile client is launched, it will register the device to Unified CM.
5. To integrate to Unified Mobility and to leverage hand-off functionality, the mobile number of the iPhone must be configured as a mobility identity associated to the Cisco Dual-Mode for iPhone device within Unified CM.

The Cisco Mobile client is supported on iPhone models 3G and 3GS running firmware version 3.0.1 or later. The iPhone WLAN interface supports 802.11b and g network connectivity.

### Interactions Between Cisco Mobile and Cisco Unified Mobility

The Cisco Mobile dual-mode client for the iPhone can be integrated with Cisco Unified Mobility to leverage Cisco Mobile Connect, mid-call DTMF features, two-stage dialing, single enterprise voicemail box, and desk phone pickup.

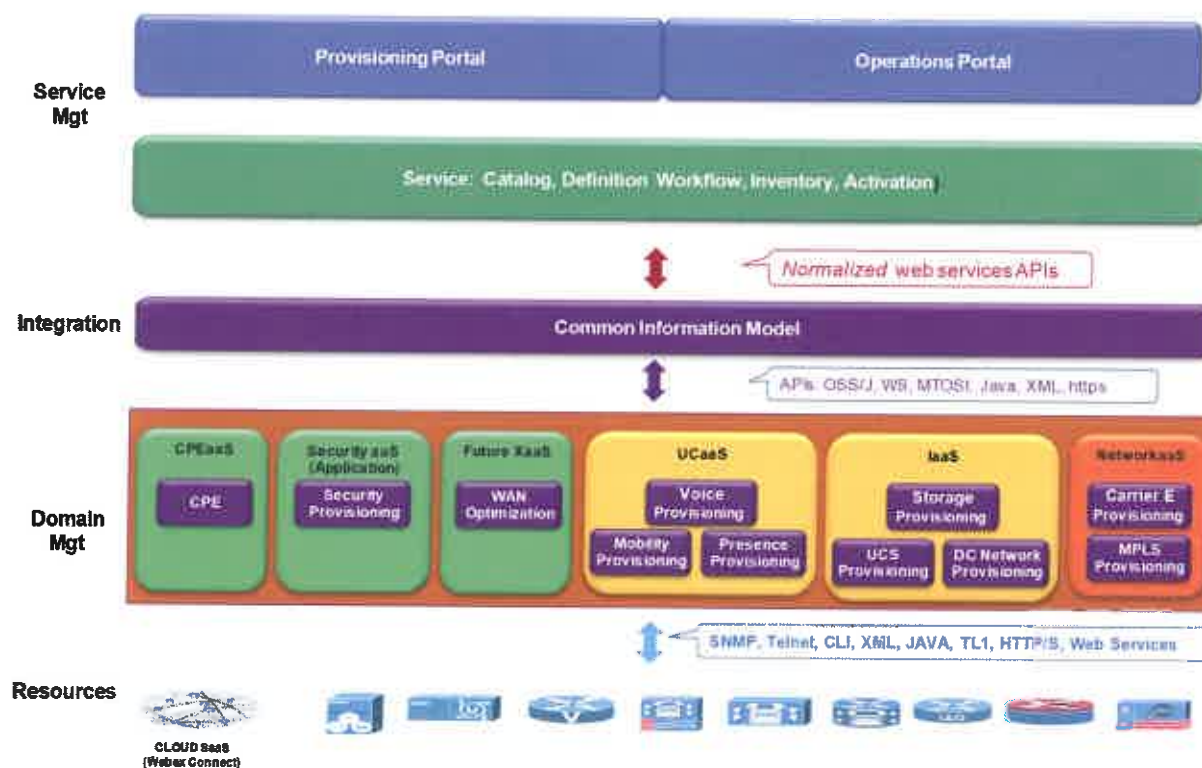
# Management Architecture

## AT&T UC Node HCS Platform Management Overview

Managing various managed services with Cisco and other vendors' products for multiple businesses over a variety of architectures is crucial for the managed SP. The speed of service innovation is rapidly increasing, especially among Web 2.0 and software as a service (SaaS) vendors.

The model of introducing new services only after integrating them with existing provisioning applications hinders time to market. To address rapid service creation, multiple domain managers (or element managers) must be quickly enabled to provision and monitor services and to coordinate these services centrally, regardless of whether they are delivered with equipment on the customer's premises, in the service provider's network or data center, or in the facilities of a partner service provider or SaaS vendor.

A modular management framework, i.e. Cisco Managed Services Service Management Framework (Cisco HCS Management), is illustrated in Figure below. It enables the accelerated deployment of services for managed service providers. Cisco managed services and other solutions can be remotely provisioned and monitored with the solutions in this framework and coordinated through the OSS and BSS via an integration layer.



**Figure 48 Cisco HCS Management Service Enablement**

With this flexible, plug and play management framework from Cisco that supports an ecosystem of partners, managed service providers can deploy new services faster and more easily.



## Service Management Layer

Firstly, the service management layer consists of a self care portal and a status portal. This will be provided by USM from VOSS and by Cisco's VSX software.

The self-care portal enables a privileged user, e.g. SP admin or enterprise admin, to perform the Create, Retrieve, Update, Delete (CRUD) or Moves, Adds, Changes, Deletions (MACD) operations.

The status portal can range in capability. It provides summary status of the underlying services, and equipment. It may also allow the user to drill down on to get details on the status of a particular incident. The status portal will periodically get updates from the underlying infrastructure. It can either poll or receive autonomous indications as and when events occur.

Secondly, the service management layer provides the following functions:

- Product catalog
- Service catalog
- Customer Relationship Management (CRM) system. Service definition
- Service lifecycle management
- Service inventory
- Resource Management
- Localization (local language support)
- Subscriber management

## Integration Layer

The integration layer provides an abstraction of the underlying domain managers and helps the SP avoid a point-to-point integration of domain managers.

In the context of the Cisco HCS Management the Integration layer consists of the Common Information Model (CIM). It receives order-to-activation service requests from the OSS/BSS through the normalized APIs. It decomposes the requests to the appropriate services (e.g., voice and security), and maps the service parameters to the respective domain manager supporting the service. The CIM may federate and enrich the data and may do conditional processing, if required. The DMs, in turn, provision the respective devices based on the data received from the CIM. Finally, the CIM returns a success or failure to the OSS/BSS layer. The object model (Shared Information Data) of the Integration Layer is based on Forum's SID (GB922).

## Domain Management Layer

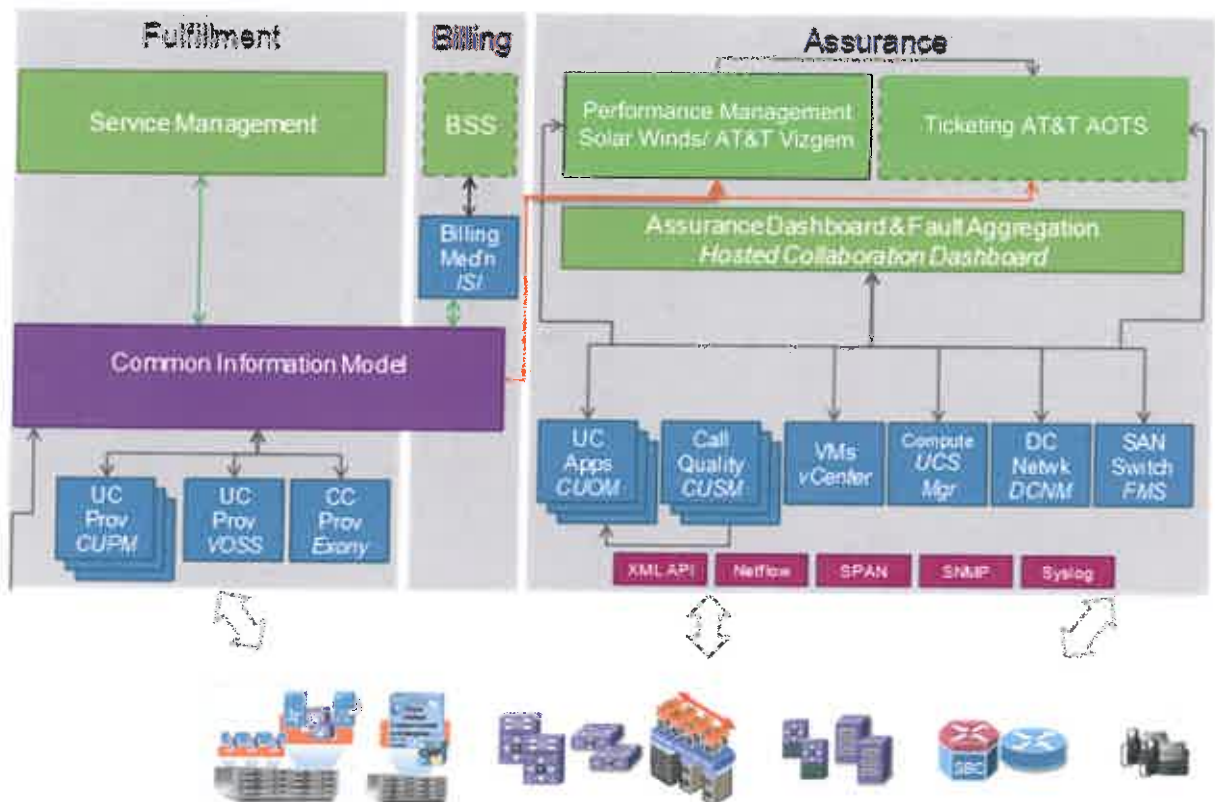
The domain layer consists of domain managers that manage the services and the devices. Examples of different services are security, voice, email, and storage. Each domain manager manages a specific service. The domain managers are required to expose a NB API to enable integration with the Integration Layer. Some examples of domain managers for Service Assurance are, Cisco Unified Operations Manager (CUOM), Cisco Unified Service Manager (CUSM), VMware Venter, Data Center Network Manager (DCNM), etc. For the AT&T network, VOSS USM will be used as a domain manager for Service Fulfilment for UC. This layered model supports an ecosystem of domain managers whereby a subset of the domain managers can make up a service management solution for a service provider.

## Devices

The device layer (e.g. CUCM, Presence etc.) communicates with the domain managers using standards based protocols. The protocols supported by these devices include XML, SNMP, AXL/SOAP, TR-069, CLI, and WSMA.

## HCS Platform Management Services

The HCS Management will be deployed as follows:



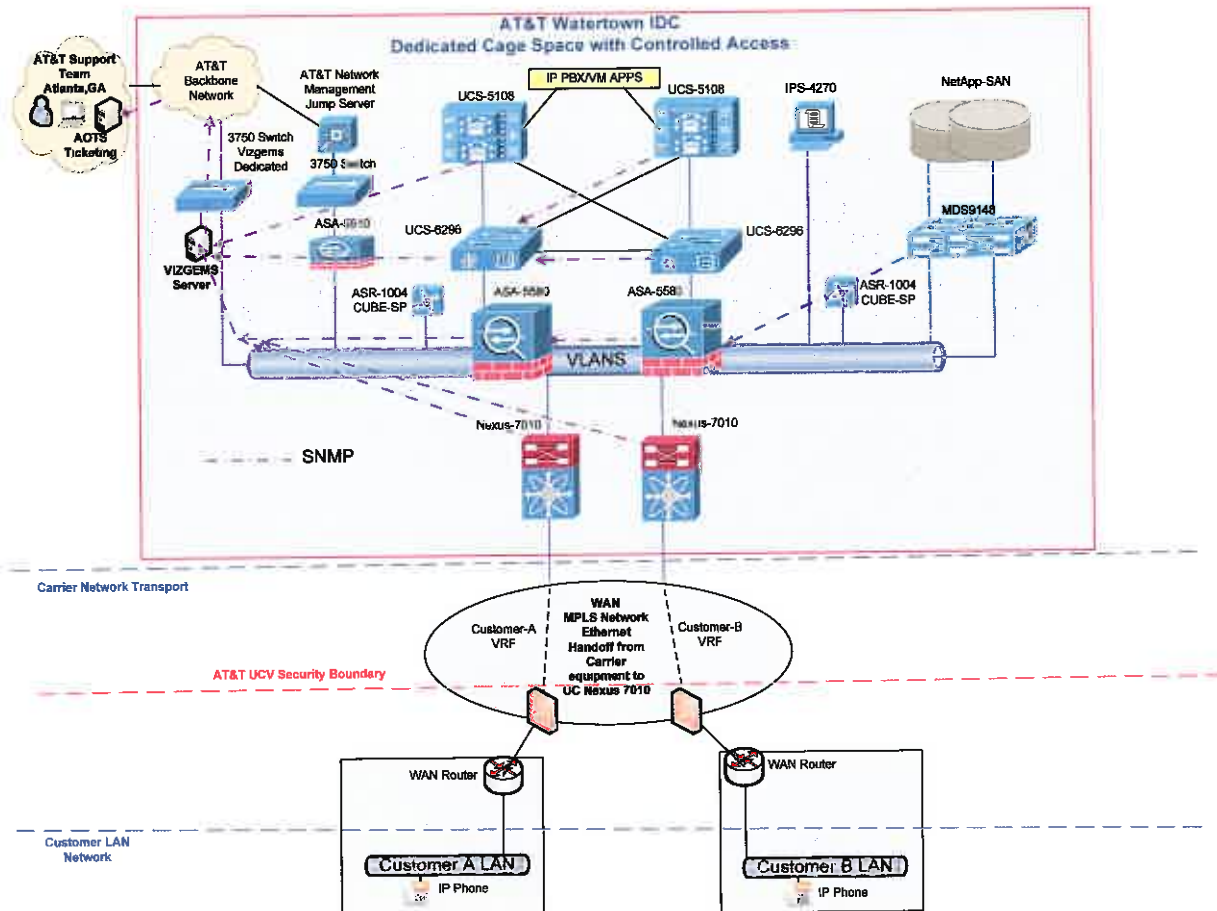
**Figure 49 HCS Management Solution for AT&T**

All Cisco applications supporting the service delivery and service management run on the same UCS 5108 chassis as customer applications. AT&T also utilizes two non Cisco applications to support monitoring and ticket generation for the AT&T support team to utilize in fault isolation as well as tracking the status of all applications.

## Vizgems Monitoring Application

AT&T has developed and in house monitoring applications that is utilized to detect basic up and down status for HCS hardware deployed as part of the FISMA platform. The Vizgem dashboard serves as the status portal for HCS and the UC Support team based in Atlanta, GA. It is a web based application that aggregates information from multiple virtualized instances of the HCS infrastructure. The Vizgems platform collects information via SNMP via a direct connection from a Cisco 3750 switch that has connectivity into the core Nexus 7010 switches. The SNMP traps are sent to the core collection application via dedicated AT&T backbone circuit deliver directly into the Watertown, MA FISMA cage. Monitoring functionalities provided by the Vizgems monitoring dashboard include:

- Basic up and down status of core HCS hardware
- Ticket Generation based on fault severity to AT&T ticketing system (AOTS)
- Statistics on up time and Mean Time Between Failure analysis



**Figure 50 AT&T Vizgems Monitoring Topology**

## Solar Winds Monitoring and Management

SolarWinds Network Configuration Manager (NCM) keeps you ahead of network issues with immediate visibility into the cause and effect relationship between configuration errors and network performance. NCM Provides support for nightly config backups, bulk config changes, user tracking, and inventory and compliance reporting. The NCM application is deployed on the UCS-5108 Chassis utilizing VMware and a B200 blade within the Watertown, MA cage 21560 and provided the following services:

- Enables bulk configuration, community string, ACL, & MAC address changes
- Automates network configuration backups & compliance reporting
- Detects & reports on configuration policy violations & delivers real-time alerts
- Protect against unauthorized, unscheduled, or erroneous config changes
- Automatically discovers SNMP-enabled network devices within the core HCS platform

### Supported Protocols:

SolarWinds Network Configuration Manager supports multiple protocols, including SNMP v1/v2/v3, Telnet, SSH v1/v2, and TFTP

## Domain Management Layer

HCS management for AT&T will use VOSS USM and Cisco Unified Operations Manager (CUOM).

### CUCDM USM

HCS supported Unified Services Manager (USM) will provide an API to be accessed via the DXSI layer which will accept service requests. These service requests will provide sufficient data for USM to provision the UC components in accordance with the pre-loaded provisioning rules.

In the event that a required function is not accessible via VSX and DSXI, a cross launch facility will allow access via VSX to the USM.

Currently VOSS USM does not support overlapping IP subnets used for phones. This requires management of customer address space to prohibit the case where multiple customers use the same address space for phones. Software development is required on VOSS USM to relax this requirement

USM will be deployed in two clusters of 2 instances. USM version 7.3 will be deployed.

This configuration is an Active / Standby cluster. Within a cluster, it is of utmost importance that connectivity between the servers is maintained to ensure consistent databases. To this end, each server has two interfaces dedicated to intra cluster connectivity.

Each cluster of VOSS servers consists of a VOSSDIR1 and VOSSDIR2 function.

### DHCP

The DHCP service for the IP Telephony network will be provided as an optional part of the HCS solution.

The VisionOSS USM platform manages the allocation of IP Subnets and the allocation of IP Addresses to IP Phones. USM then configures the appropriate DHCP server, so that it offers a specific address to a specific phone. For this reason traditional subnet sharing strategies typically used in resilient DHCP architectures are inappropriate and not required in a clustered server environment.

Where a central DHCP server is not required, it is possible to use local DHCP servers such as the DHCP server available in the CPE routers. Where this method is used, the CUCM will pass the IP address and phone details during registration to USM via syslog messages. For initial phone deployment, this allows dynamic addition of phones to the network.

It is expected that the platform will use local DHCP servers only

### USM redundancy

USM will offer redundancy in two ways. Firstly, dual UCM clusters are configured in the Watertown data center. Secondly, a disaster recovery (DR) cluster is provided. The proposed USM servers are arranged as follows:

**Table 19** *USM server layout*

Server number	Function	Location
---------------	----------	----------

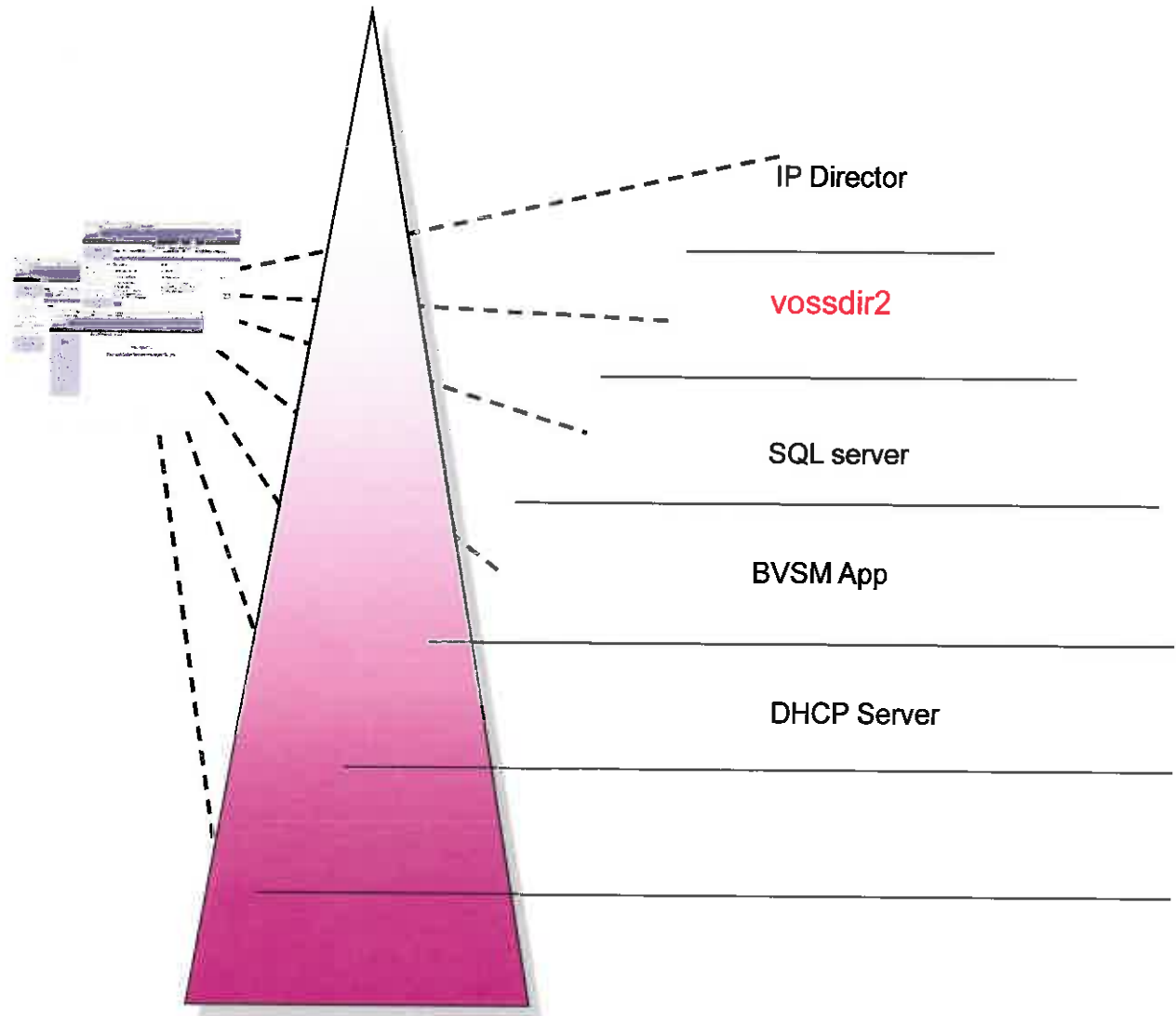
1	VoSSDir1	Chassis 1
2	VoSSDir2	Chassis 1
3	VoSSDir1	Chassis 2
4	VoSSDir2	Chassis 2

Note that automated failover between the primary cluster and the DR cluster is not supported. To activate the DR cluster, a manual procedure must be followed. Automated failover is supported within a cluster for server failure cases. This allows, for example, that failure of the active VoSSDir server will result in automated failover to the remaining VoSSDir server.

## Multi-level administration

USM offers 7 levels of administration. These levels allow administration by an individual end user up to the system administrator. At all levels, there is enforcement of scope of administration capability which covers both the available administrative activities, and the components on which those activities are permitted. For example, a location administrator only has access to his own location, and may only perform the actions which he has been authorized for within that location.

- Ability to add new customers to HCM and established connectivity with their domain manager instance.
- Single Sign-on capability for domain managers for a customer
- Ability to add new Portal users with different usage/view privileges
- Customer aware and context sensitive launching of domain manager UI's
- Customer specific views



## Self Care

The self-care portal is available at a different URL than the remainder of the administrative functions. The self-care function may be customized to deliver the appropriate level of administration. Different users may have different functions available to them. Also, the web pages may be “branded” such that an individual user may see his own company logo etc. when using self-care.



## Cisco Unified Operations Manager

CUOM is an element/network management system that performs monitoring, performance management and service assurance for the Cisco Unified Communications suite of devices and applications.

CUOM has the following high level functionalities:

- Network auto discovery for devices
- Device inventory collection
- Monitoring of devices through polling (SNMP and AXL), SNMP traps and syslogs
- Performance data collection and thresholding
- Diagnostic tests for verifying the status of phones, IPSLA devices, etc.

## Devices/Applications

CUOM supports various UC solutions categorized as follows:

- Call processing services
- Contact center services
- Voice messaging services
- Conferencing services
- Mobility services
- Video/TelePresence services
- End-points (IP Phones/soft clients)
- Other voice application services
- Infrastructure services.

## Interfaces

CUOM exposes the above functionalities through User Interfaces (Web UI), north bound programming interface and notifications through Trap, Syslog and E-mail.

## User Interfaces

CUOM offers web based user interfaces for management. The key applications are:

- Portal for monitoring of CUCM devices
- Event Monitor for fault management
- Logical connectivity topology view reflecting real time updates to the devices.
- Administration views for configuring OM and device configuration.

## North Bound Programming Interface

CUOM exposes a north bound programming interface as a SOAP service. The interface is published in WSDL format.

CUOM uses method call, enumeration and notification features of SOAP to expose its interfaces.

## Virtualization

CUOM is supported on virtual machine running in VMWare. The tested configuration includes a Virtual Machine with the storage in a SAN Disk.

CUOM on a virtual machine requires configuration as defined in Table 12 page 74.

## Virtualization (vSphere)

In HCS, initialization of Customer UC infrastructure (i.e. creation and initialization of UC applications and Domain manager) will be virtualized. For example, virtual instances of domain managers would be created for every customer. VMware vSphere will provide the Domain Manager function for the VMware applications. Control of vSphere will be accomplished from within VSX utilizing DXSI and the API of vSphere. Preprovisioned scripts will be able to create new virtual machines of the appropriate size and capacity when new end customers are added to HCS.

# Management Network

A management network is required, with no access to the signaling network. This Out-of-band management network will protect the integrity of the end customers applications and data while allowing for full remote access to the system by Cisco in order to conduct release management, capacity management, platform architecture and engineering, and troubleshooting

The management network will consist of:

- Management interface on Nexus 6296 which controls UCS
- ESXi management of host server in management VLAN
- USM Management interface
- Nexus 7K Management interface
- VSphere management server

## Network Management System: Best Practices White Paper

[http://www.cisco.com/en/US/tech/tk869/tk769/technologies\\_white\\_paper09186a00800aca9c.shtml](http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800aca9c.shtml)

# Security Architecture

## Overview

The goal of this section of the document is to provide a high-level description of the security architecture used to protect the AT&T UC Voice platform. AT&T utilizes a layered approach to security. Each layer builds upon the next to ensure safeguards for our customers. We adhere to security standards that match or exceed the best practices outlined by AT&T chief Security Offices Information Security Standard and Center for Internet Security. We also follow best practices defined by equipment vendors and standards developed by AT&T Labs, AT&T Security Policy Requirements (ASPR) for data center security defining a layered security approach:

- **Secure the core switches:** Layer 2/Layer 3 switches build the data center core and aggregate links from other data centers. These switches are secured using the practices described in the Secure Network Foundation section of the SAFE Security Architecture design guide, Center for Internet Security best practices. Both are based on best practices for securing Cisco LAN switching environments
- **Segmentation of distribution switches:** Redundant distribution switches are responsible for aggregating the Layer 2/Layer 3 links connecting the access switches. Where a multilayer design is required, each layer is implemented as a separate VLAN that may span from distribution all the way to the access switches.
- **Stateful firewall deployment:** AT&T Security Architecture for Data Centers design uses stateful firewalls configured in failover mode to protect servers and help ensure segregation between application layers. The firewalls deep packet inspection mitigates DoS attacks and enforces protocol compliance. Web and UC applications are protected with a web applications firewall.
- **Traffic inspection and protection:** An IDS device is used to identify well-known attacks and suspicious activity. Complementary to the IDS, an anomaly detection system is also deployed at the web tier.
- **Server protection:** Servers residing at the different layers are protected with endpoint security software. Alerts and alarms generated by the IDS and endpoint security software are processed by a monitoring and analysis system.

**Switch hardening:** All switches are hardened using the procedures in the Cisco SAFE Security Architectures Secure Network Foundations section. This section is the bases for the Center for Internet Security best practices In addition, the access switches are configured with port security and other Layer 2 protection features.

## Network Functional Areas

AT&T UC Node network has been segmented into separate functional areas. Segmentation of the network allows control over the interactions between different sets of devices and users, and facilitates the deployment of control and monitoring technologies, which are essential components of a secure network. Segmentation also allows containment of network attacks, for example should an attacker gain access to one of the network areas, or a worm outbreak occurs, the security filters between the areas can stop the attacker or worm reaching other parts of the network.

The following functional areas exist in relation to the UC Node network:

- The core AT&T IP network.
- Customer IP networks, which connect to the core AT&T UC Node IP network.
- Per-customer VRFs that carry customer traffic across the core IP network.
- Per-customer virtualised voice servers.

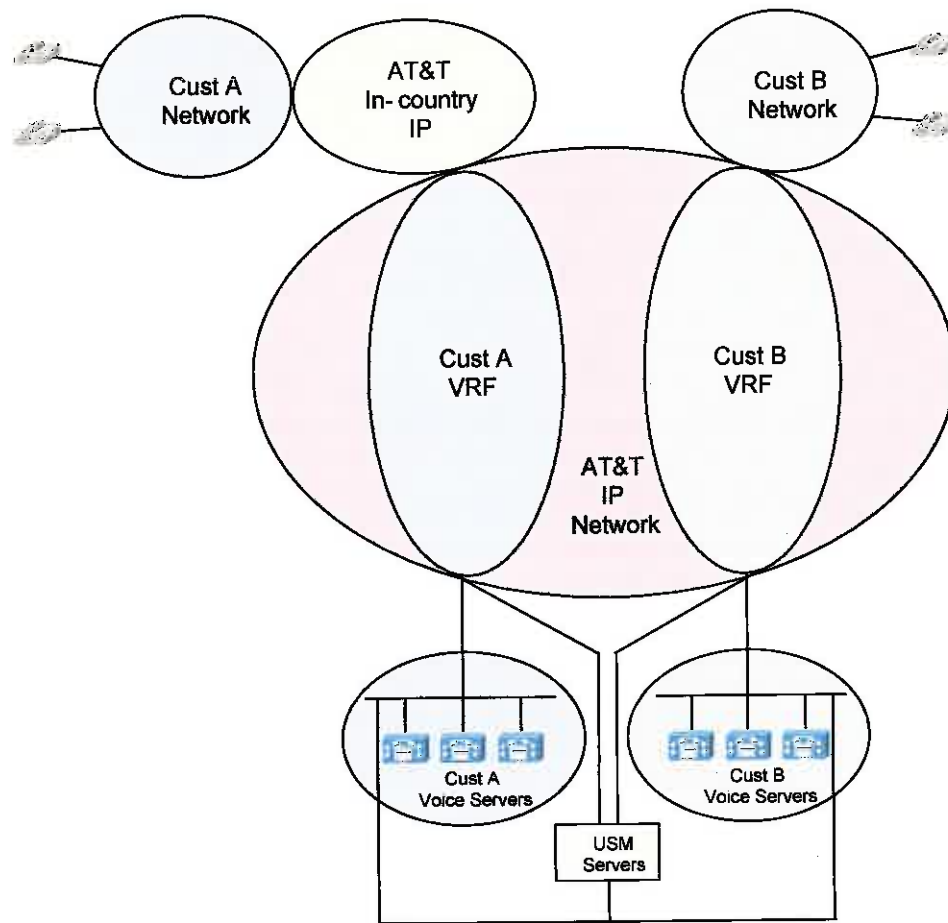
- USM voice management systems.
- UC Node management network that is logically separate from the user plane of the production service network.

**Note**

The functional network areas listed above are those which are related to the security scope of this document.

An overview of these network functional areas is shown in the figure below.

**Figure 51 AT&T HCS Network Functional Areas**

**Note**

The figure above represents the interactions between the various elements of the HCS network functional areas. It does not show the actual connectivity and traffic flows between the elements.

**Note**

The HCS management network which is logically separate from the user plane of the production service network is not shown in the figure above.

Customer's phones are connected to their own networks, which in turn connect directly to the core IP network, or to the AT&T in-country networks and then on to the core IP network. Each customer has their

own VRF on the IP network which isolates them from the other customers, and connects their phones to their own set of virtualised voice servers, which will be located at the HCS data centres.

Customers can also connect to the USM servers, which provide user configuration of phone features. Connectivity will only be allowed via the customer's internal network and VRF.

The HCS network will be supported by four data centres. The centralized management applications will be located in the HCS management network in Watertown, MA data center. Other than the HCS management network all other security configurations will be identical between the data centers.

## Security Architecture

### Firewalling

#### Key Aspects

The following describes the key aspects of firewall functionality on the AT&T HCS network:

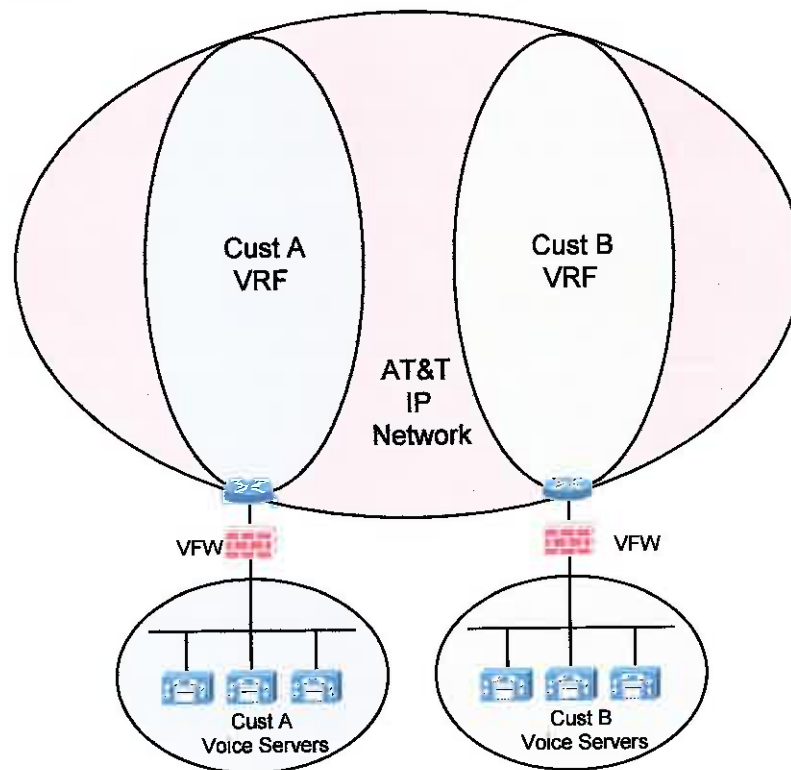
- Cisco ASA5580 security appliances will be used to provide redundant, stateful firewall functionality on the HCS network.
- A total of eight ASA5580s will be deployed in four resilient pairs:
  - One 'pair' at the Watertown data center
- The ASA5580s will be resilient within each data centre; they will not be resilient between the data centres.
- The ASA5580s will operate in routed mode.
- The ASA5580s will be logically split into a number of virtual firewalls (known as contexts), which will be used to control the interactions between network functional areas:
  - Customer phone to customer voice servers.
  - Customer to USM servers via internal network.
  - USM servers to customer voice servers.
- The ASA5580s will use a dedicated physical connection from the logically separate management network for out-of-band management.
- Management of the ASAs will be from the Admin context only.

#### Firewall: Customer Phone to Customer Voice Servers

Each customer will have a dedicated virtual firewall to control the interaction between their phones and their virtualized voice servers.

The figure below shows a high-level view of the customer phone to customer voice servers firewalling on the HCS network:



**Figure 52 Customer Phone to Customer Voice Servers Firewalling****Note**

For clarity in the above figure, separate routers are shown between the customer VRFs on the IP network and the customer virtual firewalls. In reality, these routers will be a single router (or two routers for redundancy).

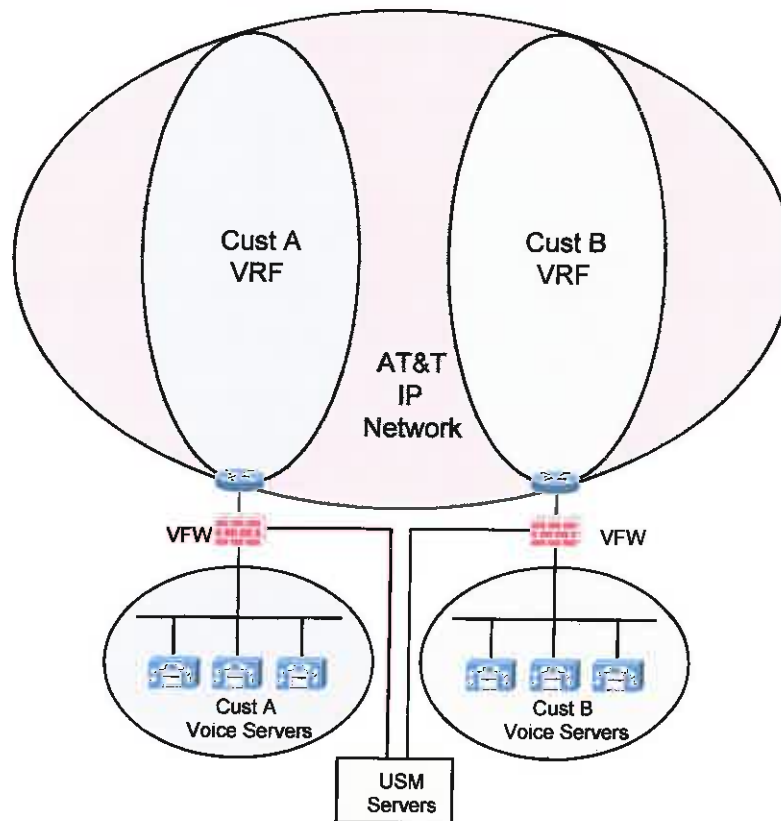
**Firewall: Customer to USM Servers via Internal Network**

When accessing the USM servers from the customer's internal network, each customer will connect to the USM servers via a DMZ on their dedicated virtual firewall, which will control the interaction between the customer and the USM servers.

**Note**

The USM servers have a flat structure with a single VIP (Virtual IP Address) to represent all of the servers in the cluster.

The figure below shows a high-level view of the customer to USM servers firewalling on the HCS network for connections coming from the customer's internal network:

**Figure 53 Customer to USM Servers Firewalling via Internal Network****Note**

For clarity in the above figure, separate routers are shown between the customer VRFs on the IP network and the customer virtual firewalls. In reality, these routers will be a single router (or two routers for redundancy).

**Note**

In the above figure a connection from each virtual firewall is shown to the USM servers. In reality, the USM servers can only have one IP address, so the connections from the virtual firewalls to the USM servers will have to go through an intermediate layer 3 device.

## Firewall: USM Servers to Customer Voice Servers

After a customer has changed the configuration of their phone on the USM servers, the USM servers communicate with the customer's virtualised voice servers to enact the change.

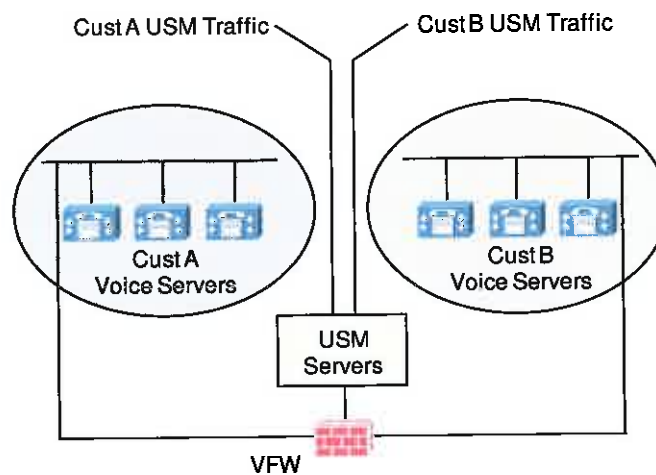
A virtual firewall will control the interaction between the USM servers and each customer's virtualised voice servers.

**Note**

The USM servers have a flat structure with a single VIP (Virtual IP Address) to represent all of the servers in the cluster.

The figure below shows a high-level view of the USM servers to customer voice servers firewalling on the HCS network:

**Figure 54 USM Servers to Customer Voice Servers**



**Note**

In the above figure a connection from each customer virtual firewall is shown to the USM servers and from the USM servers to the 'USM Servers to Customer Voice Servers' firewall. In reality, the USM servers can only have one IP address, so the connections from the virtual firewalls to the USM servers will have to go through an intermediate layer 3 devices.

## Monitoring

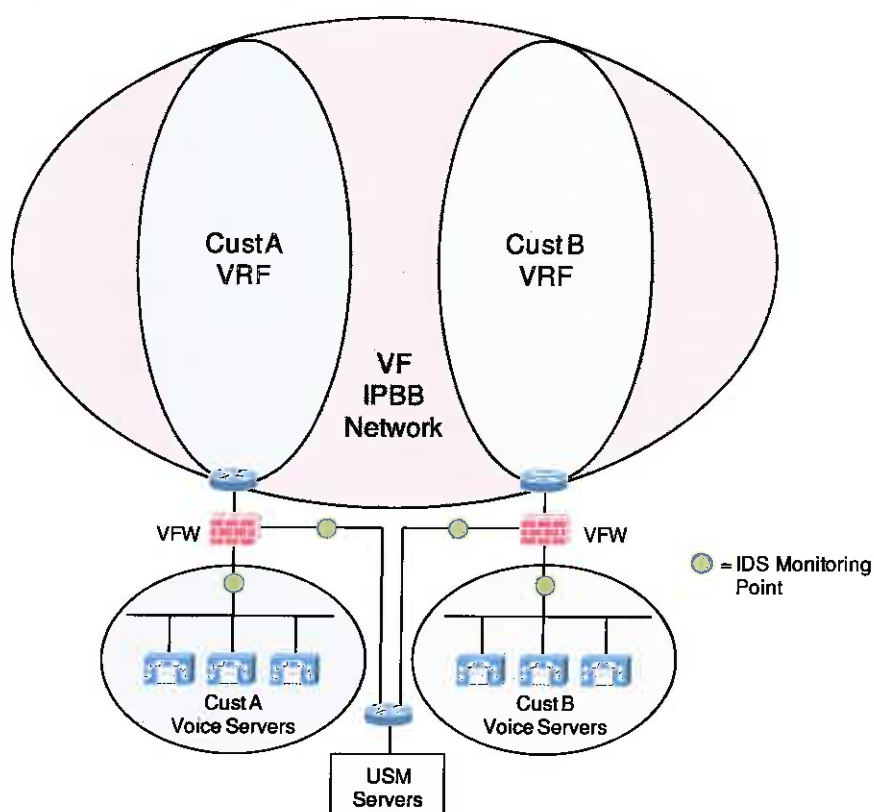
### Intrusion Detection

The following describes the key aspects of intrusion detection on the HCS network at the four data centres:

- The Cisco IPS-4270 will be used as an Intrusion Detection System (IDS) will be used to monitor traffic for attack patterns at the following points on the HCS network:
  - Each customer's voice signalling traffic destined for their voice servers, on the 'inside' of their virtual firewall.
  - Each customer's 'command' traffic destined for the USM servers, on the 'USM' interface of their virtual firewall.
  - 'Command' traffic from the USM servers destined for the customer's voice servers, on the 'USM' interface of their virtual firewall.
- The Cisco Security Manager monitoring system located at the Watertown data center will be used to collect and analyse the alerts from the IDS.
- The traffic flows will be accessed through the use of ERSPAN within the Nexus switching architecture.

The figure below shows a high-level view of the monitoring points on the HCS network:

Figure 55 HCS Data Centre IDS Monitoring Points



## Logging

The following describes the key aspects of logging on the HCS network:

- Syslog events from the following 'in scope' devices on the HCS network will be sent to an AT&T controlled Syslog server:
  - ASA5580s and all associated virtual firewalls.
  - Routers.
  - Switches.
  - UCM.
  - Unity.
- SNMP traps from the following 'in scope' devices on the HCS network will be sent to an AT&T controlled SNMP server:
  - ASA5580s and all associated virtual firewalls.
  - Routers.
  - Switches.
  - UCM.
  - Unity.
- Syslog events and SNMP traps will be stored for a suitable length of time.
- Traps and events be transferred to the central servers over the management network

## Access Control

AT&T utilizes and established dedicated backbone network to support remote access from the Network Operations Center (NOC) and Security Operations Center (SOC) located in Atlanta, GA. UC Support Team (UCST) staff adhere to the following security process for access:

All UCST staff members that will be accessing the UC Voice Federal platform will have the appropriate security clearances for access

All UCST staff members will access the UC Voice Federal platform utilizing computers that have been approved for use by AT&T Chief Security Office (CSO).

Remote access from the support staff requires the use of Two Factor RSA SecureID® Token Authentication

VPN access for support from vendors and or remote work staff shall be provide through dedicated ASA 5510 firewalls defined with specific user access . The ASA 5510 shall be separate from ASA-5580 firewalls providing customer security and segmentation.

Secure Access is provide via AT&T Jump Server

- Access to the network devices that the ACS servers are providing AAA service for will be via a dedicated management network.
- The following design details apply to AAA services for network device access:
  - ACS will also be used to authenticate user access to network devices for management and administration purposes.
  - A backup username and password will be configured on each device's local database, which will be used to authenticate a login if there is no response or an error is returned from the AAA Server.
  - AAA will be used as the access method for all devices on the network, and apart from the backup account, no user accounts will be configured locally on any device.
  - Each network administrator will have their own username and password for accessing network devices.
  - Different levels of access (authorization levels) will be granted to different groups of network administrators. For example, junior support engineers will not be allowed to reload devices, which is a feature that should only be granted to more experienced support personnel.
  - Accounting will be enabled on network devices, so that user login/logout times are recorded, along with each command that is entered, on the AAA server. This will provide valuable forensic information as all changes on the network will be logged in a central repository, along with the user who made the change.

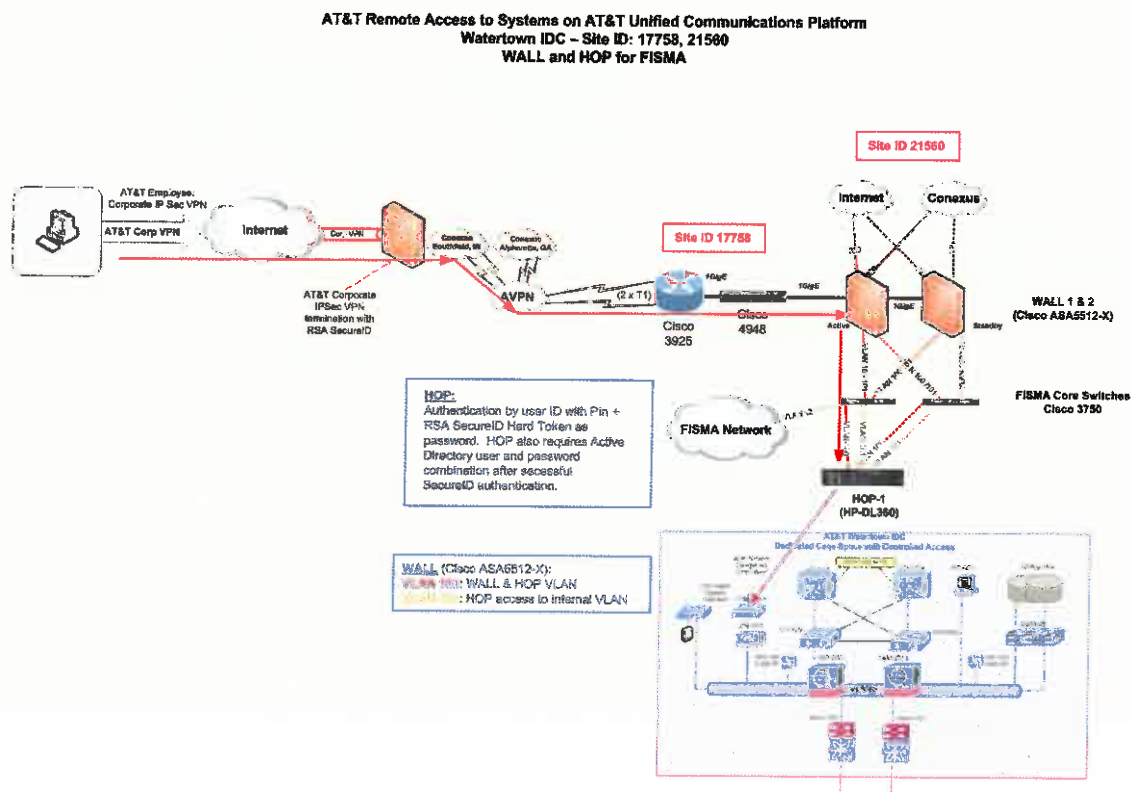


Figure 56 Access Control Pat

## Management Plane Level

### Management Plane Level 1-2

Description: Services, settings and data streams related to setting up and examining the static configuration of the router, and the authentication and authorization of router administrators. Examples of management plane services include: administrative telnet and ssh, SNMP, TFTP for image file upload, and security protocols like RADIUS and TACACS+.

1. **AT&T provides AAA Service:** AT&T supports Authentication, authorization and accounting (AAA) systems for Local Console, Login, VTY, enable mode specific to Cisco IOS devices. AAA accounting supported
2. **AT&T provides local user encrypted password support:** All Cisco devices admin, user devices have encrypted passwords
3. **AT&T provides SSH for Remote Device Access/ VTY Transport SSH :** (SSH) access is configured on all management connections. Support for Automatic disconnect after 10 minutes.
4. **Auxiliary Port Disabled for core equipment:** Core LAN and routers are defined with “transport input none” to ensure prevention of un authorized connection
5. **Access Control Lists (ACL) for VTY:** IP address specific access for AT&T NOC users with configuration level access
6. **EXEC Banner Support:** Banner display security access restricted statement per AT&T standard for MOTD and login



7. **Password Rules:** AT&T Enable secrets use a strong, one-way cryptographic hash (MD5).
8. **Encrypted Line and User Passwords:** AT&T requires a password to be set on each line. Local usernames (level 1) or TACACS+ (level 2) line passwords are not used for authentication.
9. **SNMP Rules:** AT&T deploys SNMPv3 which utilizes authentication, authorization and data privatization encryption. No default SNMP community strings are utilized. SNMP control restricted by ACL to specific AT&T NOC administrators with configuration access level capabilities

## Control Plane Level

### Control Plane Level 1-2

The control plane covers monitoring, route table updates, and generally the dynamic operation of the router. Services, settings, and data streams that support and document the operation, traffic handling, and dynamic status of the router. Examples of control plane services include: logging (e.g. Syslog), routing protocols, status protocols like CDP and HSRP, network topology protocols like STP, and traffic security control protocols like IKE. Network control protocols like ICMP, NTP, ARP, and IGMP directed to or sent by the router itself also fall into this area.

1. **Clock Time zone - UTC:** AT&T configures the devices clock time zone to coordinated universal time (UTC) explicitly.
2. **Cisco CDP:** AT&T disables Cisco Discovery Protocol (CDP) service at device level in the UC core. Specific management VLANs are defined where CDP is required.
3. **AT&T Default Disabled Services:** Finger Services, IP BOOTP server, Identification Service, IP HTTP Server, Remote Startup Configuration
4. **AT&T TCP Enabled Services:** TCP keepalives-in Service, TCP keepalives-out Service, TCP-small-servers
5. **Logging Rules:** AT&T supports logging buffers, logging to AT&T administered syslog server, Trap severity levels with time stamp in log messages
6. **Multilevel NTP:** AT&T provides Primary, Secondary and Tertiary Network Timing support from secure stratum level clocking sources.
7. **Loopback Rules:** AT&T supports Binding AAA, NTP, TFTP Services to Loopback Interface

## Data Plane Level

### Data Plane Level 1-2

Services and settings related to the data passing through the router (as opposed to direct to it). The data plane is for everything not in control or management planes. Settings on a router concerned with the data plane include interface access lists, firewall functionality (e.g. CBAC), NAT, and IPSec. Settings for traffic-affecting services like unicast RPF verification and CAR/QoS also fall into this area.

1. **Routing Rules :** AT&T default disabled routing components include; Directed Broadcast, IP source-route
2. **Border Router Filtering AT&T access restrictions:** Restrict Private Source Addresses from External Networks and External Source Addresses on Outbound Traffic
3. **Routing Protocol Neighbor Authentication Requirements:** Require Authentication for BGP, EIGRP, OSPF, and RIPV2 as required.
4. **Routing Rules Requirements:** Enable Unicast Reverse-Path Forwarding. Disable IP Proxy ARP and Tunnel Interfaces

## Virtual Platform Security

### Virtual Platform Security

AT&T Utilizes Cisco UCS 5108 platform with *VMware ESX 5.x* and has defined the following supported process for security.

1. **VMware Management:** AT&T creates separate Management Network and data segments
2. **VMware Patches:** AT&T has three categories for patches: Security, Critical, and General. The patch # refers to KB (knowledge base) article number that goes into more detail. VMware will (usually) issue a KB article when they become aware of security vulnerabilities AT&T tests patches in its staging lab prior to implementing on production environments.
3. **BIOS Configuration:** AT&T disables the server's ability to boot off all non-hard disk devices, including floppy, CD-ROM, and USB.
4. **NTP Support:** AT&T enables system clock synchronization with Network Time Protocol (NTP) server(s). The Network Time servers are provided via AT&T network backbone that extends to the NTP platforms housed with the Watertown IDC in separate cage.
5. **System Access, Authentication, Authorization, and User Accounts:** Specific NOC administrators are allowed access using secure shell (SSH). AT&T does not enable Direct Root SSH. Do not enable direct su to root, only allow sudo .
6. **Password History:** AT&T retains a history of previous passwords used and configure the authentication controls to validate new passwords against greater than or equal to 10 recently used credentials

**Password Complexity:** Password strength requirements:

- Ignored when 1 character class is used.
- Ignored when 2 character classes are used.
- Ignore passphrases.
- Greater than or equal to 12 characters in length when 3 character classes are used.
- Greater than or equal to 8 characters in length when 4 character classes are used.

- Ignore reuse of any number of characters from the old password unless the new password is exactly the same as the old password.

#### (Virtual Platform Security)

AT&T Utilizes Cisco UCS 5108 platform with VMware ESX 4.X and has defined the following supported process for security.

1. **Failed Login Attempts :** AT&T sets the number of login attempts allowed before the account is locked / disabled to 3
2. **Maximum Days Before Password Change:** Set the maximum number of days before a password is required to be changed to 90 days
3. **Minimum Days before Password Change:** Set the minimum number of days a password must exist before it can be changed to: Greater than or equal to 7 days.
4. **Minimum Password Length:** Greater than or equal to 8 Characters
5. **Log Compression and Rotation:** Increase the file size 2096K and enable compression for the log files vmkernel and vmksummary
6. **Review Logs:** *Configure syslogd to Send Logs to a Remote LogHost are reviewed once a day by AT&T security team or when specific event dictate and are sent to an off box location to reduce being compromised*
7. **MAC Spoofing:** *AT&T protects Against MAC Address Spoofing, Forged Transmits, and Promiscuous mode by changing the flags to reject for the settings MAC Address*
8. **VMware Internal Firewall:** *AT&T configures the Firewall to Allow Only Authorized Traffic*
9. **Storage :** AT&T configures connections to iSCSI storage devices to use the CHAP protocol for authentication
10. **Warning Banners:** AT&T creates warning banners for console and remote access.
11. **Guest Interaction with the Host:** AT&T does not allow guests to control hardware devices outside of ESX or vCenter.
12. **AT&T Default Disables:** *Disable Group and Other Write File Permissions for .vmx Files, Disable Group and Other Read, Write and Execute File Permissions for .vmdk Files*

## IPSec VPN Termination

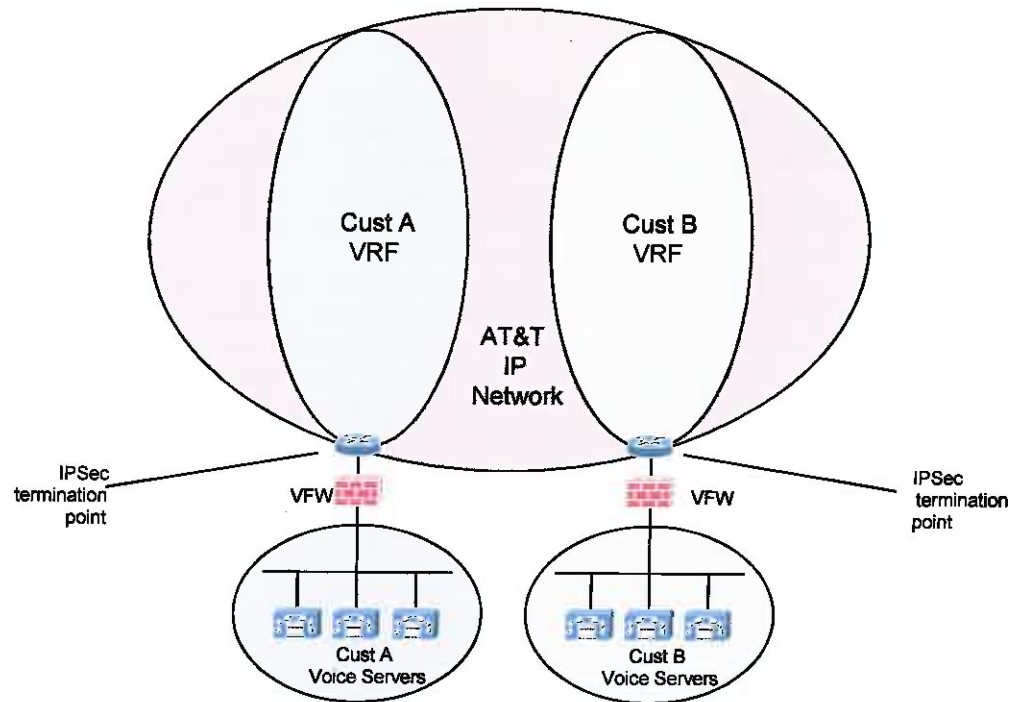
The following describes the key aspects of IPSec VPN termination on the HCS network:

- Customer traffic may be encrypted across the AT&T network, in which case it will be terminated at the AT&T router that connects to the Cisco ASA5580.
- Remote access to the environment will be through Cisco provided ASA5510 devices, enforcing strong authentication.
- The ASA5510 device will be configured for AAA using the ACS system. Cisco will be responsible for managing access to the HCS platform through the ASA5510 devices.
- AT&T will provide backup access to the HCS platform for Cisco through their IPSec VPN infrastructure.

- AT&T will be responsible for the IPSec termination on their network.

The figure below shows a high-level view of the IPSec termination on the HCS network:

**Figure 57 IPSec Termination Points on the HCS Network**



**Note**

For clarity in the above figure, separate routers are shown between the customer VRFs on the IP network and the customer virtual firewalls. In reality, these routers will be a single router (or two routers for redundancy).

## Security Device Management

Cisco ASDM (Adaptive Security Device Manager) will be used to manage the ASA5580s on the HCS network.

ASDM is a 'one-to-one' GUI based management system that allows configuration, monitoring and troubleshooting of the ASA with the following features:

- Setup wizards for configuration and management.
- Powerful real-time log viewer and monitoring dashboards that provide an at-a-glance view of device status and health.
- Handy troubleshooting features and powerful debugging tools such as packet trace and packet capture.

Further details on ASDM can be found at the following URL:

<http://www.cisco.com/en/US/products/ps6121/index.html>

## Security Equipment

This section provides an overview of the Cisco security equipment that will be used on the HCS network, along with URLs, which provide full details.

### ASA5500

The Cisco ASA 5500 Series Adaptive Security Appliance is a modular platform that provides next generation security and VPN services for small and medium-sized business and enterprise applications. The comprehensive portfolio of services within the Cisco ASA 5500 Series enables customization for location-specific needs through its tailored package product editions: enterprise-firewall, IPS, anti-X, and VPN. Each edition combines a focused set of services within the Cisco ASA family to meet the needs of specific environments within the enterprise network.

At the same time, the Cisco ASA 5500 Series enables standardization on a single platform to reduce the overall operational cost of security. A common environment for configuration simplifies management and reduces training costs for staff, while the common hardware platform of the series reduces sparing costs.

Each edition addresses specific enterprise environment needs:

- **Firewall Edition** - Enables businesses to securely deploy mission-critical applications and networks in a reliable manner, while providing significant investment protection and lower operational costs through its unique, modular design.
- **IPS Edition** - Protects business-critical servers and infrastructure from worms, hackers, and other threats through the combination of firewall, application security, and intrusion prevention services.
- **Anti-X Edition** - Protects users at small or remote sites with a comprehensive package of security services. Enterprise-grade firewall and VPN services provide secure connectivity back to the corporate head-end. Industry-leading anti-X services from Trend Micro protect the client system from malicious websites and content-based threats such as viruses, spyware, and phishing.
- **VPN Edition** - Enables secure remote user access to internal network systems and services, and supports VPN clustering for larger enterprise deployments. This solution combines Secure Sockets Layer (SSL) and IP Security (IPSec) VPN remote-access technologies with threat mitigation technologies such as Cisco Secure Desktop (CSD), and firewall and intrusion prevention services to ensure VPN traffic does not introduce threats to the enterprise.

Additional information on the ASA 5500 series can be found at the following URL:

<http://www.cisco.com/en/US/products/ps6120/index.html>

The data sheets for the ASA 5500 series can be found at the following URL:

[http://www.cisco.com/en/US/products/ps6120/products\\_data\\_sheets\\_list.html](http://www.cisco.com/en/US/products/ps6120/products_data_sheets_list.html)

### ASA5580

The Cisco ASA 5580-40 Adaptive Security Appliances deliver multi-gigabit security services for large enterprise, data centre, and service-provider networks in a robust, 4-rack-unit form factor. The ASA5580 series is offered at two performance levels: the ASA5580-20 with 5 Gbps of real-world firewall performance, and the high-end ASA5580-40 with 10 Gbps of real-world firewall performance.

The following table lists the features of the ASA5580 series:

**Table 20 ASA5580 Capabilities and Capacities**

Feature	ASA5580
Maximum Firewall Throughput	5 Gbps (real-world HTTP), 10 Gbps (jumbo frames)

Maximum VPN Throughput	1 Gbps	
Concurrent Sessions	1,000,000	
IPSec VPN Peers	10000	
SSL VPN Peer License Levels*	2,10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, and 10,000	2,10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, and 10000
Security Contexts	Up to 50*	Up to 50*
Interfaces	2 Gigabit Ethernet management	2 Gigabit Ethernet management
Interface Card Slots	6	6
Interface Card Options	- 4 Port 10/100/1000, RJ45 - 4 Port Gigabit Ethernet fiber, SR, LC - 2 Port 10Gigabit Ethernet fiber, SR, LC	- 4 Port 10/100/1000, RJ45 - 4 Port Gigabit Ethernet fiber, SR, LC - 2 Port 10Gigabit Ethernet fiber, SR, LC
Virtual Interfaces (VLANs)	100	100
Redundant Power	Supported (second power supply optional)	Supported (second power supply optional)

\* Separately licensed feature.

The data sheet for the ASA5580 can be found at the following URL:

[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product\\_data\\_sheet0900aecd802930c5.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html)

## ASA 5510

The Cisco ASA 5510 Adaptive Security Appliance delivers advanced security and networking services for small and medium-sized businesses and enterprise remote/branch offices in an easy-to-deploy, cost-effective appliance. The Cisco ASA 5510 Adaptive Security Appliance provides high-performance firewall and VPN services and five integrated 10/100 Fast Ethernet interfaces.

Up to 250 AnyConnect and/or clientless VPN peers can be supported on each Cisco ASA 5510 by installing an Essential or a Premium AnyConnect VPN license; up to 250 IPsec VPN peers are supported on the base platform.

**Table 21 ASA5510 Capabilities and Capacities**

Feature	Description
VPN Throughput	Up to 170 Mbps
Concurrent Sessions	50,000; 130,000*



IPsec VPN Peers	250
Premium AnyConnect VPN Peer License Levels**	2, 10, 25, 50, 100, or 250
Security Contexts	Up to 5***
Interfaces*	5 Fast Ethernet ports; 2 Gigabit Ethernet + 3 Fast Ethernet*
Virtual Interfaces (VLANs)	50; 100*

## IPS 4270

Cisco IPS 4200 Series Sensors deliver high-performance intelligent detection with precision response, extending the diverse Cisco IPS solution from the network edge to the data center for both IPv4 and IPv6 networks.

Cisco IPS 4200 Series Sensors accurately identify, classify, and stop malicious traffic before it affects your business.

- Cisco IPS technology is engineered to prevent malicious activity, including worms, directed attacks, distributed denial of service attacks, reconnaissance, and application abuse.
- Built on advanced Cisco security and network intelligence, modular inspection capabilities can detect and prevent threats to the entire network stack, from applications to Address Resolution Protocol (ARP). Cisco IPS technology extends this expertise by providing industry-leading protection from evasion.
- Cisco IPS provides adaptive vulnerability and anomaly detection. Signatures are focused on vulnerabilities, so your ability to detect threats remains intact, even as exploits change. For emerging "zero-day" threats, a Cisco IPS sensor learns about your network, detects behavioral anomalies, and mitigates attacks without a signature update.
- Cisco IPS is the only intrusion prevention system that uses Global Correlation. Global Correlation harnesses the power of Cisco Security Intelligence Operations, the world's largest threat monitoring network, to achieve unprecedented threat management efficacy. Global threat information is turned into actionable intelligence, such as reputation scores, and pushed out to all enabled technologies. Using Global Correlation, Cisco IPS can stop twice the amount of malicious activity that traditional signature-only IPS technologies can, and with fewer false positives. With Global Correlation updates every five minutes, the Cisco IPS can also adjust to changing threat conditions 100 times faster than signature updates alone.
- Cisco IPS technology and signature services are developed by an extensive global team of Cisco security experts. These experts conduct ongoing research into emerging threats, inspection methods, and prevention strategies, in order to continue to deliver up-to-date vulnerability-based signatures and advanced intrusion prevention capabilities.

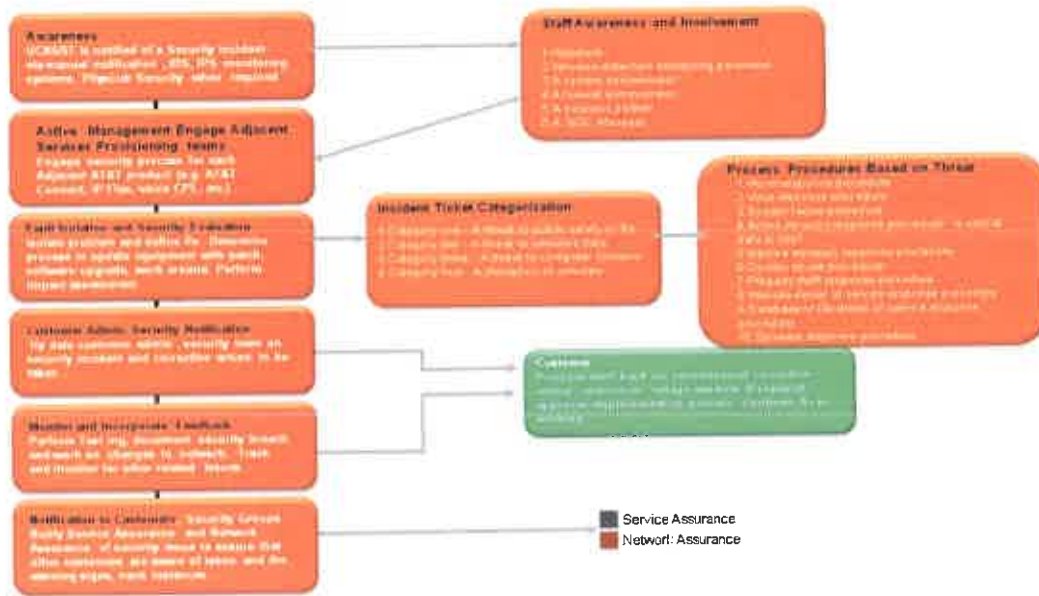
**Table 22** *IPS4270 Capabilities and Capacities*

	Cisco IPS 4270
	
Performance: Media-rich	4 Gbps

Performance: Transactional	2 Gbps
Standard monitoring interface	Four 10/100/1000BASE-TX or four 1000BASE-SX
Standard command and control interface	10/100/1000BASE-TX
Optional monitoring interfaces	<ul style="list-style-type: none"> <li>• Four 10/100/1000BASE-TX</li> <li>• Two 1000BASE-SX (fiber) (up to 16 total monitoring interfaces)</li> </ul>
Redundant power supply	Yes
Form factor	Four rack units
Height	6.94 in. (17.6 cm)
Width	19 in. (48.3 cm)
Depth	26.5 in. (67.3 cm)
Weight	80 lb (36.3 kg)
Rack-mountable	Yes
Auto-switching	100 to 240 VAC
Frequency	50 to 60 Hz, single-phase
Operating current	12.0A (100 VAC), 4.9A (200 VAC)
Operating temperature	10 to 35°C (50 to 95°F)
Nonoperating temperature	-40 to 70°C (-104 to 158°F)
Operating relative humidity	10 to 90% (noncondensing)
Nonoperating relative humidity	5 to 95% (noncondensing)
Heat dissipation @ full power	1893 Btu/hr

## Security Incident Management

AT&T utilizes IPS 4270 to capture details on inbound packets, IP address source and destination information. When traffic is determined to not match MAC, IP addresses defined in IPS for valid customers it is tagged and alert generated by the IPS to the security incident management team for handling and quarantine. The following process flows demonstrates the security approach.



Page 2

**Figure 58 Security Incident Management**

## Two Factor RSA Security ID Token Authentication

AT&T uses an RSA SecureID® token based scheme for two factor authentication. Two factor authentication uses “something you have” and “something you know” to establish authenticity. For the UC Voice service, two factor authentications require possession of a token fob as well as knowledge of your Personal Identification Number (PIN).

AT&T has a separate pool of tokens used for administering security devices for all customers. Use of a common token pool simplifies overall token administration. A multiple (two) realm arrangement provides for separation of UC Voice users, servers and device data from Commercial customers' data. Employing cross realm authentication an administrator can support multiple services with one token fob.

Each realm contains an independent database of the valid userids, PIN + token codes, servers and devices that are available for two factor authentications. (Some devices in UC Voices do not support two factor authentications.) UserIDs are designated as local (authentication performed completely in local realm) or remote (authentication performed in conjunction with remote home realm). When a remote realm is engaged, this process is called cross realm authentication.

AT&T's commercial service administrators are provisioned in the NBFW realm. AT&T's UC Voice service administrators are provisioned in the UC VOICE realm. The respective realms are further divided into roles to further segregate administrators by specific function.

AT&T has deployed primary and replica servers for both realms. Either the primary or replica of a given realm is capable of authenticating a user.

Two factor authentications are processed as follows:

1. A potential administrator attempts to log in to a given server or device.

2. The administrator is prompted for a Passcode, which is a combination of their PIN + Token Code.
3. Upon submission of these credentials, the userID (login) is checked against the UC Voice realm.
4. If the userID is not found in the UC Voice realm, the login request is rejected. If the userID is provisioned in the UC Voice realm, the PIN and token code values are evaluated by that user's home realm for confirmation.
5. If the home realm produces a negative response for the PIN and token code, the login is rejected. If denied, the administrator must wait until the token's display has changed (thirty (30) seconds maximum) before making another attempt to authenticate. After a positive confirmation, the UC Voice authentication servers will permit access to the user's desired server or device.

An administrator must allow the token code to update prior to attempting to log in to another system. Note that a given token code can only be used once.

Authentication requests are logged. Local realm logging includes userID, server or device name, status (successful or failed) as well as a cross realm indication, if cross realm was attempted. Remote realms log userID, status (successful or failed) as well as the fact that a cross realm authentication was attempted. The server or device name from the local realm is not available to the remote realm to prevent sharing of local information.

# Ports and Protocols

## Media and Signalling Protocols

Some customer requirements for security include utilizing firewalls on premise to further segment the UC environment. The following signaling and media ports must be opened to ensure proper operation of the UC Voice services. Other ports may apply for future applications support. Updates will be posted in this document as new requirements for ports are known.

Feature	From / To	Protocol	Transport	Ports Enabled
Client Download	Browser / Portal	HTTP	TCP	80
Applications, Authentication, Directories, Services, etc.	Browser / Portal Phone / CUCM	XML / HTTP	TCP	8080
Self-Provisioning	Browser / Portal	Secure HTTPS	TCP	443
Instant Messaging	UC Client / Server	Secure MSRP	TCP	2855 and 2856
Domain Name Service	UC Client / Network	DNS	TCP UDP	53
Call Control	Phone / CUCM	SIP over TLS	UDP TCP and UDP	5060 5060 and 5061
Voice / Media	IP VMS / Phone	Secure RTP	UDP	16384 to 32767 Cisco limits to: 24576 to 32767
Voice - Alternative	IP VMS / Phone	RTP	UDP	1584
Cisco Signaling	Phone / CUCM	SCCP Skinny Client Control Protocol	TCP	2000
Cisco Signaling	Phone / CUCM	SCCPS	TCP	2443
Cisco Trust Verification	Phone / CUCM	SCCPS	TCP	2445

Feature	From / To	Protocol	Transport	Ports Enabled
Locally Significant Certificates	Phone / CUCM	CAPF Certificate Authority Proxy Function	TCP	3804
Phone Firmware and Configuration	Phone / CUCM	TFTP	UDP	69, then Ephemeral
Remote Access	Admin/ Voice Gateways	SSH	TCP	22

#### UC Ports CUCI-LYNC/MOC and Mobile 8.0

Ports Used for Outbound Traffic by Cisco Unified Client Services Framework		
Port	Protocol	Description
69	UDP	Connects to the Trivial File Transfer Protocol (TFTP) server to download the TFTP file.
80	TCP HTTP	Connects to services such as Cisco Unified Meeting Place for meetings, Cisco Unity or Cisco Unity Connection for voicemail features.
143	IMAP (TCP/TLS)	Connects to Cisco Unity or Cisco Unity Connection to retrieve and manage the list of voice messages for the user, and the voice messages themselves.
389	TCP	Connects to the LDAP server for contact searches.
443	TCP HTTPS	Connects to services such as Cisco Unified Meeting Place for meetings, Cisco Unity or Cisco Unity Connection for voicemail features.
636	LDAPS	Connects to the secure LDAP server for contact searches.
993	IMAP (SSL)	Connects to Cisco Unity or Cisco Unity Connection to retrieve and manage the list of voice messages for the user, and the voice messages themselves.
2748	TCP	Connects to the CTI gateway, which is the CT Manager component of Cisco Unified Communications Manager.
5060	UDP/TCP	Provides Session Initiation Protocol (SIP) call signaling.
5061	TCP	Provides secure SIP call signaling.
7993	IMAP (TLS)	Connects to Cisco Unity Connection to retrieve and manage the list of secure voice messages for the user, and the secure voice messages themselves.



8191	TCP	Connects to the local port to provide Simple Object Access Protocol (SOAP) web services.
8443	TCP, HTTPS	Connects to the Cisco Unified Communications Manager IP Phone (CCMCIP) server to get a list of currently-assigned devices. In a single sign on (SSO) deployment, this connects to the Cisco Unified Communications Manager User Data Service (UDS) instead of CCMCIP.  In an SSO deployment, an outbound HTTPS connection is made to the Open AM server. Typically, port 8443 is configured on the Open AM server for this connection. However, the administrator of the Open AM server might configure the server to use a different port for HTTPS traffic, for example, 443.
16384-32766	UDP	Sends RTP media streams for audio and video.

## Monitoring and Management Ports (Vizgems and Solar Winds)

Feature	From / To	Protocol	Transport	Ports Enabled
Client Download	Browser / Portal	HTTP	TCP	80
Applications, Authentication, Directories, Services, etc.	Browser / Portal	XML / HTTP	TCP	8080
Network Monitoring	SolarWinds/HCS	SNMP General Messages	UDP	161
Network Monitoring	SolarWinds/HCS	SNMP Traps	UDP	162
Phone Firmware and Configuration	Phone / CUCM	TFTP	UDP	69, then Ephemeral
Remote Access	Admin/Voice Gateways	SSH	TCP	22

# Data center requirements

## CUCM requirements

### WAN Considerations

For clustering over the WAN to be successful, you must carefully plan, design, and implement various characteristics of the WAN itself. The Intra-Cluster Communication Signaling (ICCS) between Unified CM servers consists of many traffic types. The ICCS traffic types are classified as either priority or best-effort. Priority ICCS traffic is marked with IP Precedence 3 (DSCP 24 or PHB CS3). Best-effort ICCS traffic is marked with IP Precedence 0 (DSCP 0 or PHB BE). The various types of ICCS traffic are described in [Intra-Cluster Communications](#), which also provides further guidelines for provisioning. The following design guidelines apply to the indicated WAN characteristics:

- Delay

The maximum one-way delay between any two Unified CM servers should not exceed 40 msec, or 80 msec round-trip time. Measuring the delay is covered in [Delay Testing](#). Propagation delay between two sites introduces 6 microseconds per kilometer without any other network delays being considered. This equates to a theoretical maximum distance of approximately 3000 km for 20 ms delay or approximately 1860 miles. These distances are provided only as relative guidelines and in reality will be shorter due to other delay incurred within the network.

- Jitter

Jitter is the varying delay that packets incur through the network due to processing, queue, buffer, congestion, or path variation delay. Jitter for the IP Precedence 3 ICCS traffic must be minimized using Quality of Service (QoS) features.

- Packet loss and errors

The network should be engineered to provide sufficient prioritized bandwidth for all ICCS traffic, especially the priority ICCS traffic. Standard QoS mechanisms must be implemented to avoid congestion and packet loss. If packets are lost due to line errors or other "real world" conditions, the ICCS packet will be retransmitted because it uses the TCP protocol for reliable transmission. The retransmission might result in a call being delayed during setup, disconnect (teardown), or other supplementary services during the call. Some packet loss conditions could result in a lost call, but this scenario should be no more likely than errors occurring on a T1 or E1, which affect calls via a trunk to the PSTN/ISDN.

- Bandwidth

Provision the correct amount of bandwidth between each server for the expected call volume, type of devices, and number of devices. This bandwidth is in addition to any other bandwidth for other applications sharing the network, including voice and video traffic between the sites. The bandwidth provisioned must have QoS enabled to provide the prioritization and scheduling for the different classes of traffic. The general rule of thumb for bandwidth is to over-provision and under-subscribe.

- Quality of Service

The network infrastructure relies on QoS engineering to provide consistent and predictable end-to-end levels of service for traffic. Neither QoS nor bandwidth alone is the solution; rather, QoS-enabled bandwidth must be engineered into the network infrastructure.

## Intra-Cluster Communications

In general, intra-cluster communications means all traffic between servers. There is also a real-time protocol called Intra-Cluster Communication Signaling (ICCS), which provides the communications with the Cisco CallManager Service process that is at the heart of the call processing in each server or node within the cluster.

The intra-cluster traffic between the servers consists of the following:

- Database traffic from the IBM Informix Dynamic Server (IDS) database that provides the main configuration information. The IDS traffic may be re-prioritized in line with Cisco QoS recommendations to a higher priority data service (for example, IP Precedence 1 if required by the particular business needs). An example of this is extensive use of Extension Mobility, which relies on IDS database configuration.
- Firewall management traffic, which is used to authenticate the subscribers to the publisher to access the publisher's database. The management traffic flows between all servers in a cluster. The management traffic may be prioritized in line with Cisco QoS recommendations to a higher priority data service (for example, IP Precedence 1 if required by the particular business needs).
- ICCS real-time traffic, which consists of signaling, call admission control, and other information regarding calls as they are initiated and completed. ICCS uses a Transmission Control Protocol (TCP) connection between all servers that have the Cisco CallManager Service enabled. The connections are a full mesh between these servers. Because only eight servers may have the Cisco CallManager Service enabled in a cluster, there may be up to seven connections on each server. This traffic is priority ICCS traffic and is marked dependant on release and service parameter configuration.
- CTI Manager real-time traffic is used for CTI devices involved in calls or for controlling or monitoring other third-party devices on the Unified CM servers. This traffic is marked as priority ICCS traffic and exists between the Unified CM server with the CTI Manager and the Unified CM server with the CTI device.

For Unified CM 6.1 and later releases, a minimum of 1.544 Mbps (T1) bandwidth is required for Intra-Cluster Communication Signaling (ICCS) for 10,000 busy hour call attempts (BHCA) between sites that are clustered over the WAN. This is a minimum bandwidth requirement for call control traffic, and it applies to deployments where directory numbers are not shared between sites that are clustered over the WAN.

This call control traffic is classified as priority traffic. Priority ICCS traffic is marked with IP Precedence 3 (DSCP 24 or PHB CS3).

In addition to the bandwidth required for Intra-Cluster Communication Signaling (ICCS) traffic, a minimum of 1.544 Mbps (T1) bandwidth is required for database and other inter-server traffic for every subscriber server remote to the publisher in Unified CM 6.1 and later releases.

## Unity connection requirements

Cisco Unity Connection supports active/active clustering for redundancy and can be deployed over the WAN. The active/active or "high availability" configuration provides both high availability and

redundancy. Both servers in the active/active pair run the Cisco Unity Connection application to accept calls as well as HTTP and IMAP requests from clients. Each of the servers from the cluster can be deployed over the WAN at different sites following required design consideration.

The following requirements apply to deployments of Cisco Unity Connection servers over different sites:

- Maximum of 150 ms RTT between an active/active pair at different sites.
- Minimum of 7 Mbps bandwidth is required for every 50 ports. (For example, 250 ports require 35 Mbps.)

## USM requirements

During normal operation, the USM DR cluster database is synchronised with the primary cluster, and only rows which change are copied between the clusters. Therefore real time provisioning bandwidth requirements are low. However, there may be instances where the whole database is copied between the primary and DR cluster. This is commonly encountered during system maintenance or upgrade.

The database size for a 50k user deployment is likely to reach the size of 10Gbytes. It must be possible to transfer this between the datacentres in an acceptable time. To achieve this copy in one hour will require a bandwidth of approximately 23Mbps. To achieve this copy in three hours will require a bandwidth of approximately 7.5Mbps.

Provisioning bandwidth between USM and the network components must be considered. The primary component that USM configures is the CUCM. It is common practice to locate the CUCM publisher in a primary data center which also houses the USM. Therefore no WAN bandwidth is normally needed between USM and CUCM. In the case of AT&T, the CUCM publisher may be located in any of the four data centers while the USM will be centrally located in the Watertown data center. Bandwidth between the data centers must be adequate to allow USM to configure a CUCM publisher located in a remote data center.

## Network VLAN and Subnets

# **Appendix I Rack Elevation Diagrams**

---

## Glossary

Please refer to the CCO Internetworking Terms and Acronyms Guide at [http://docwiki.cisco.com/wiki/Category:Internetworking Terms and Acronyms %28ITA%29](http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_%28ITA%29) for additional terms.

Acronym	Description
AAA	Authorization, Authentication, Accounting
ACL	Access Control List
ACE	Application Control Engine (Cisco)
AMS	AT&T Mobile Security
AS	Autonomous System
ASN	Autonomous System Number
ATM	Asynchronous Transfer Mode
AOTS	AT&T One Ticketing System
AVMS	Anti-Virus Management System
AVPN	AT&T Virtual Private Network
BD	AT&T BusinessDirect®
BGP	Border Gateway Protocol
C&A	Certification and Accreditation
C&C	Command and Control
CBB	AT&T Common Backbone
CCB	Configuration Control Board
CM	Configuration Management
CMP	Configuration Management Plan
CO	Central Office
COBC	Code of Business Conduct
CP	Contingency Plan
CPE	Customer Premises Equipment
CSP-IdM	Common Security Platform – Identity Management
DA	Data Acquisition
DB	Database
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNI	Director, National Intelligence
DNS	Domain Name System
DOP	Drop Off Point



Acronym	Description
EPVC	Enterprise Permanent Virtual Circuit
ESM	Enterprise Security Manager
EVM	Enterprise Vulnerability Management
EVPN	Enhanced Virtual Private Network
FSE	Field Service Equipment
FTP	File Transfer Protocol
GAB	Group Atomic Broadcast
GFE	Government Furnished Equipment
GigE	Gigabit Ethernet
GRL	Global Response Loop
HBA	Host Bus Adapter
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IA	Information Assurance
IAW	In Accordance With
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IGP	Interior Gateway Protocol
iNG	Intrepid-Next Generation
IP	Internet Protocol
IPeATM	AT&T IP Enabled ATM
IPeFR	AT&T IP Enabled Frame Relay
IPS	Intrusion Prevention System
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISP	Internet Service Provider
JBOD	Just a Bunch Of Disks
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LBMP	LinMin Bare Metal Provisioning
LLT	Low Latency Transport
LUN	Logical Unit Number
MIS	Managed Internet Services
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MSS-OPS	Managed Security Services - Operations
UC VOICE	Unified Connection Voice over IP Service
NAT	Network Address Translation

Acronym	Description
NBFW	Network Based Firewall
NOC	Network Operations Center
OAM	zone that supports OA&M functions
OA&M	Operations, Administration and Management
OSPF	Open Shortest Path First
PAG	Parser Aggregator
PAT	Port Address Translation
PE	Provider Edge
PIN	Personal Identification Number
PNT	AT&T Private Network Transport
PVC	Permanent Virtual Circuit
QM	Quarantine Manager
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
RIP	Routing Information Protocol
ROB	Rules of Behavior
RPC	Remote Procedure Call
RRL	Rapid Response Loop
SAN	Storage Array Network
SCI	Watertown sitive Compartmented Information
SCN	Shared Component Node
SATP	Security Awareness and Training Plan
SCP	Secure Copy
SDD	System Design Document
SED	Service Enabling Device
WATERTOWN	Security Enforcement Nodes
SMTP	Simple Mail Transfer Protocol
SNRC	Service Node Routing Complex
SOC	Security Operations Analysis Center
SOC	Security Operations Center
SOC	Security Operations Management Center
SSL	Secure Socket Layer
SSP	System Security Plan
TB	Terabyte
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TIC	Trusted Internet Connection
TICAP	Trusted Internet Connection Access Provider

Acronym	Description
TMS	Threat Management Solution
UDP	User Datagram Protocol
UGN	AT&T Corporate Network
US-CERT	United States Computer Emergency Readiness Team
URL	Uniform Resource Locator
VCS	VERITAS Clustering System
VIP	Virtual Internet Protocol address
VLAN	Virtual Local Area Network
VPG	Virtual Private Gateway
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
VRRP	Virtual Router Redundancy Protocol
USDA	United States Department of Agriculture
VxFS	VERITAS File System
WAN	Wide Area Network
WDC	Windows Domain Controller

# About This Document

---

Author(s): Mark Beranek

Change Authority: Mark Beranek

## History

Version No.	Issue Date	Status	Reason for Change
1.0	Dec 30, 2012	Draft	Initial Draft SDD
1.1	Jan 20, 2013	Draft	First Release to CSO
2.0	Feb7, 2013	Draft	Updated for HCS 10.6 release version
2.1	Feb 7, 2013	Draft	Updated based on feedback
2.2	Feb 20, 2013	Final Draft	Added new hardware information
2.3	May 10, 2013	Updates	Alternate site description
2.4	May 20	Updates	Contingency planning (UC Support Team Add
2.5	July 12	Updates	Interim Backup
2.6	August 4	Updates	Diagrams, Vigems, Jump server, ports and solar winds updates
2.7	Dec 5 2015	Updates	Removed IP address details for changes

**ADDENDUM ACKNOWLEDGEMENT FORM**  
**SOLICITATION NO.: CRFP 0212 SWC1900000001**

**Instructions:** Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

**Acknowledgment:** I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

**Addendum Numbers Received:**

(Check the box next to each addendum received)

<input checked="" type="checkbox"/> Addendum No. 1	<input type="checkbox"/> Addendum No. 6
<input checked="" type="checkbox"/> Addendum No. 2	<input type="checkbox"/> Addendum No. 7
<input checked="" type="checkbox"/> Addendum No. 3	<input type="checkbox"/> Addendum No. 8
<input checked="" type="checkbox"/> Addendum No. 4	<input type="checkbox"/> Addendum No. 9
<input checked="" type="checkbox"/> Addendum No. 5	<input type="checkbox"/> Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

\_\_\_\_\_  
ATT Corp.  
Company

\_\_\_\_\_  
*Elizabeth Spradlin*  
Authorized Signature

\_\_\_\_\_  
11/27/18  
Date

**NOTE:** This addendum acknowledgement should be submitted with the bid to expedite document processing.

STATE OF WEST VIRGINIA  
Purchasing Division

## PURCHASING AFFIDAVIT

**CONSTRUCTION CONTRACTS:** Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

**ALL CONTRACTS:** Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

**EXCEPTION:** The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

**DEFINITIONS:**

**"Debt"** means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

**"Employer default"** means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

**"Related party"** means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceeds five percent of the total contract amount.

**AFFIRMATION:** By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (W. Va. Code §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

**WITNESS THE FOLLOWING SIGNATURE:**

Vendor's Name: Brian Troup, VP - SLED East

Authorized Signature: [Signature] Date: 11/26/2018

State of Texas

County of Dallas, to-wit:

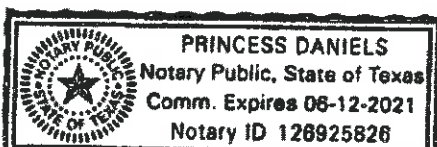
Taken, subscribed, and sworn to before me this 26 day of November, 2018.

My Commission expires 6-12, 2021.

**AFFIX SEAL HERE**

**NOTARY PUBLIC**

Princess Daniels



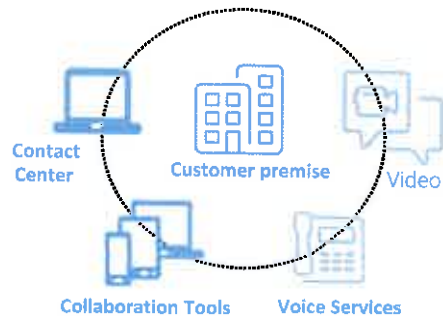
*Purchasing Affidavit (Revised 01/19/2018)*



# Multiple Unified Communications Delivery Options

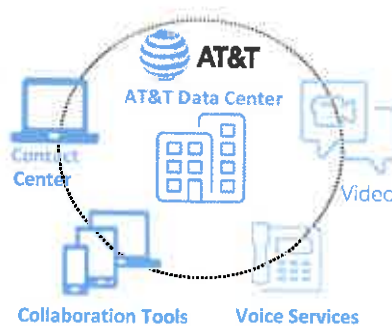
## Customer Premise

- AT&T Consulting Systems Integration, Strategy, Program Management, Transformation and Technical Design Services
- AT&T SIP Trunk Service
- Deployment & Support from AT&T Field Services
- Built Specific for Customer
- Customer Data Center



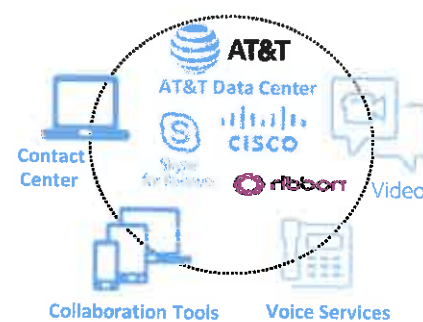
## Dedicated Hosted

- AT&T provides core servers
- AT&T provides UC applications
- Single Tenant in AT&T provided data centers with AT&T providing servers and core LAN, Firewall
- Full Voice Capabilities Including Integration
- Day 2 support services
- AT&T Consulting



## UC as a Service

- UC as a Service (Opex Model)
- Monthly Recurring UC Profiles
- Day 2 Support
- SBA/SBC Support
- Design and Implementation support
- Cloud Contact Center (AI)
- Integrated SDWAN Option

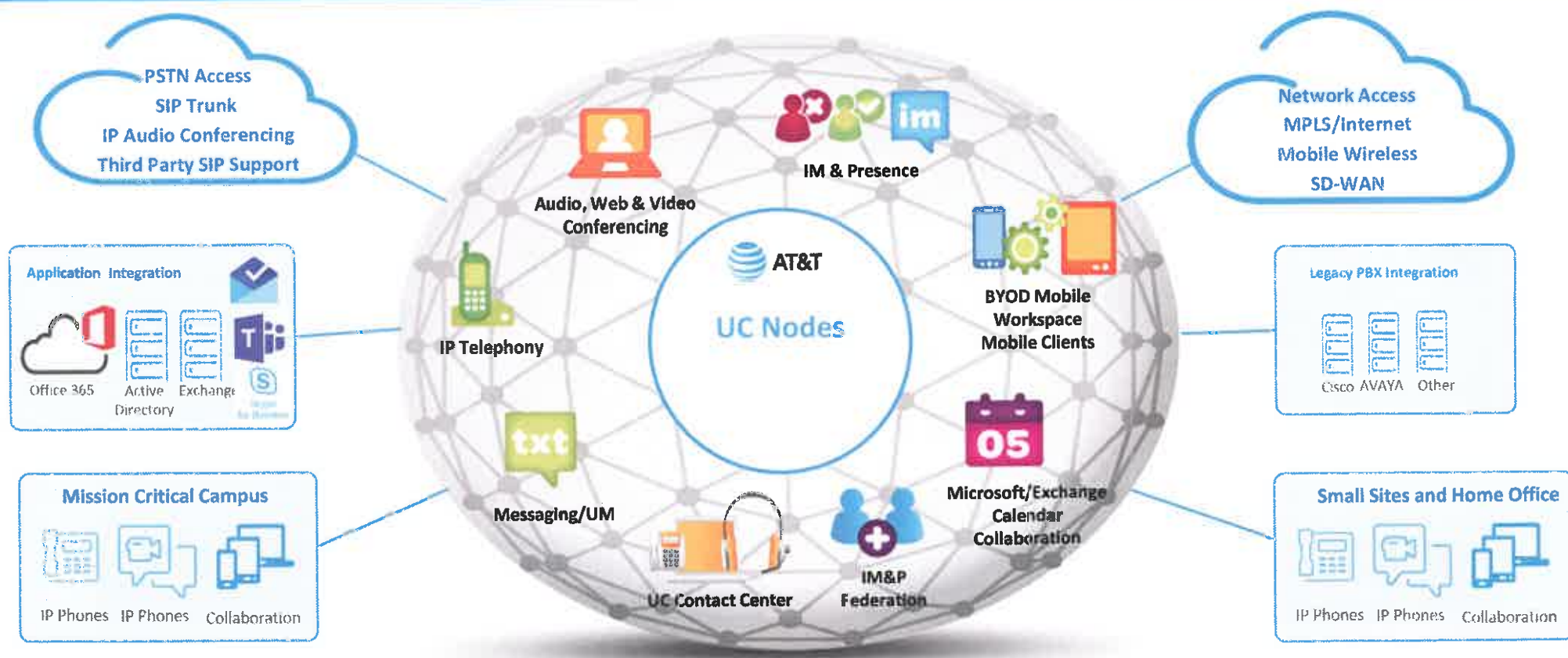


## Skype/Teams as a Service

- Microsoft Direct Route
- AT&T provides CCE and SBC from AT&T data center
- Utilize existing TDM or SIP trunk with via CCE and gateway
- Integrate and extend existing telephone numbers to Microsoft cloud or O365



# AT&T Integrated Communications Approach



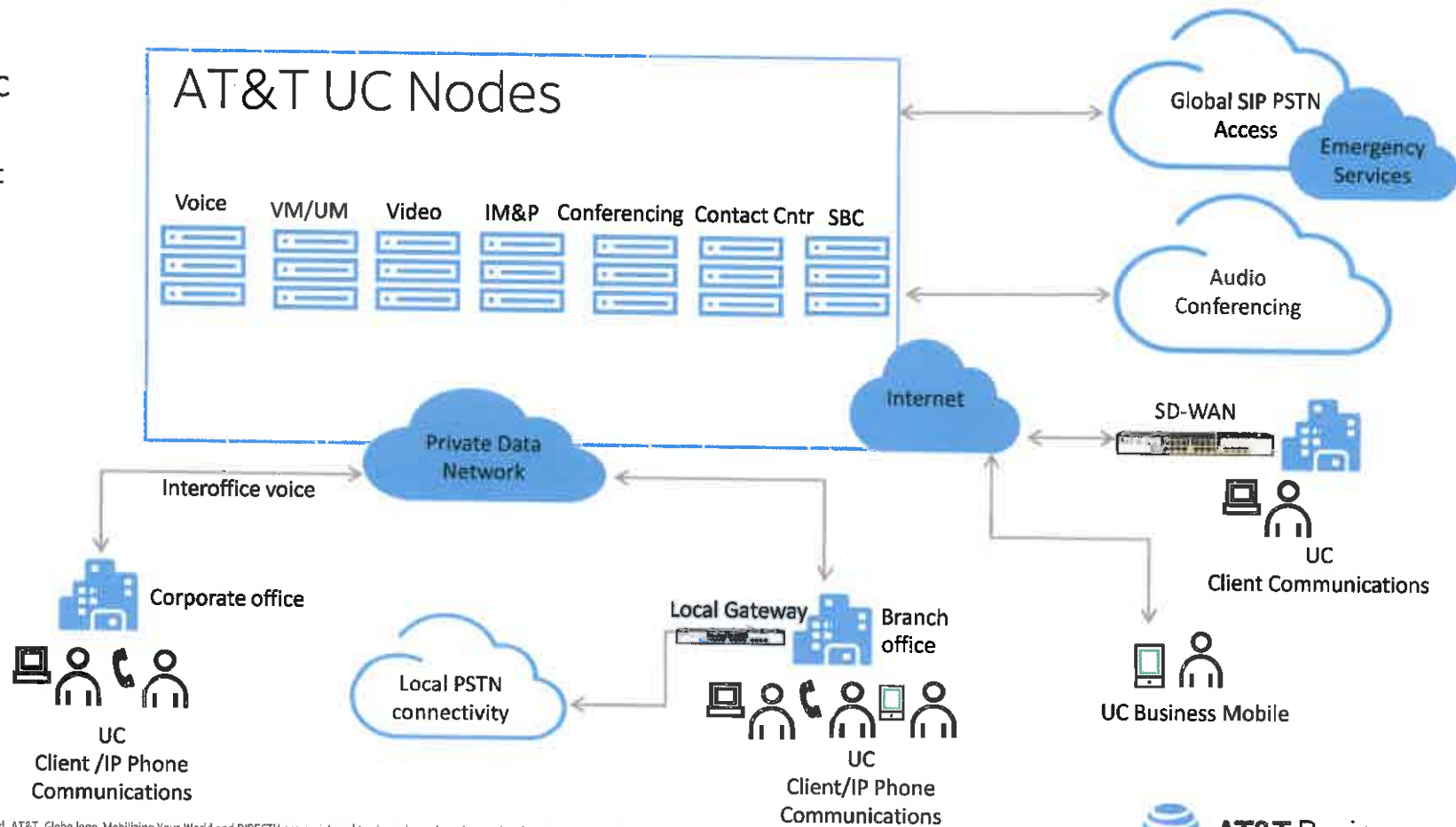
© 2018 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.



# AT&T UC as a Service Topology

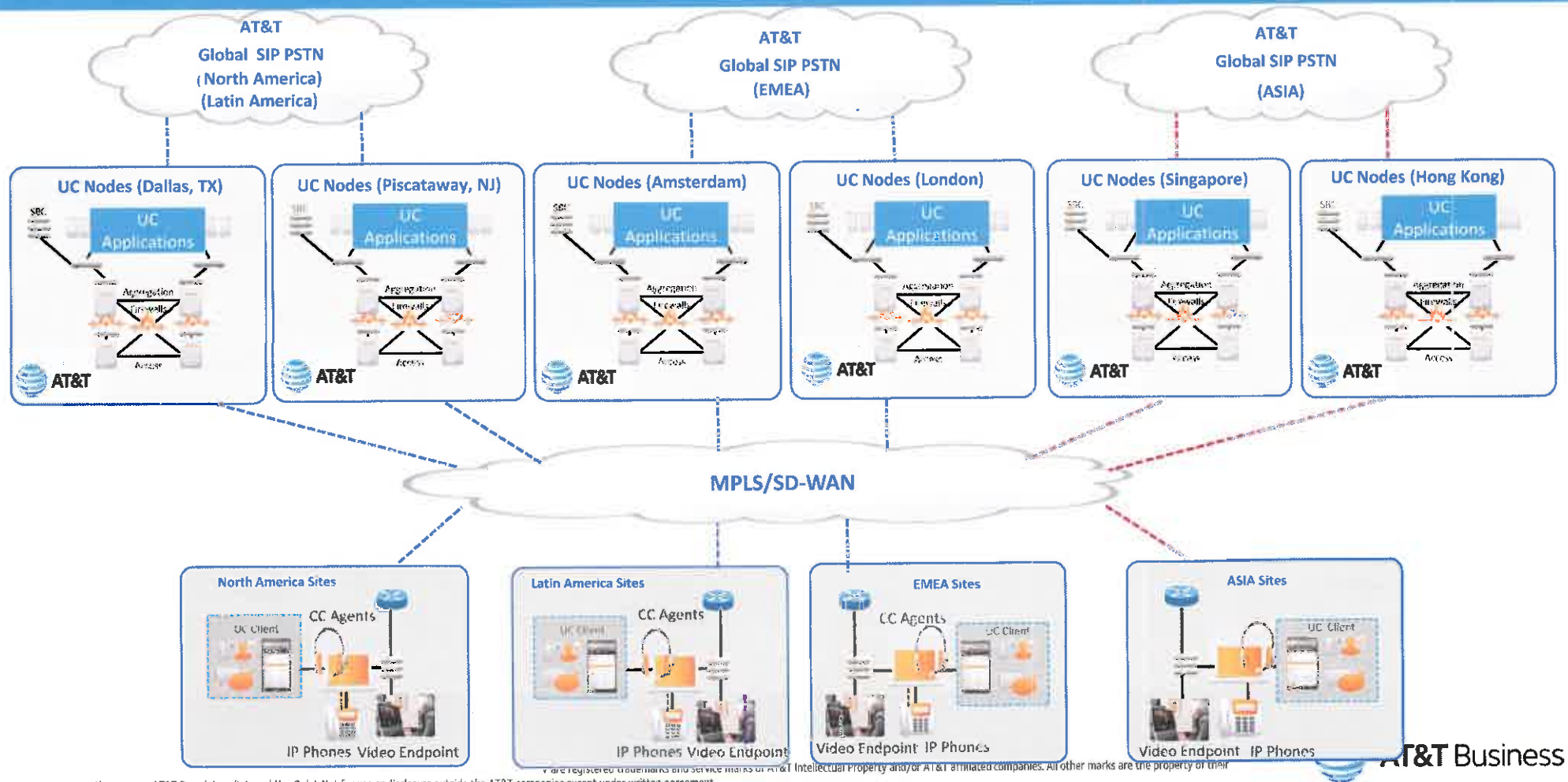
## Key benefits

- Price per user profile MRC
- Voice, Video, Web Conferencing and content sharing support
- Centralized SBC for SIP trunk Support
- PBX Integration (Avaya, Cisco)
- 7X24X365 Support
- Geo-Redundant Options
- Managed Gateways
- IP Phone management
- Multiple network access options
- Cloud Contact Center Options and AI



© 2018 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.

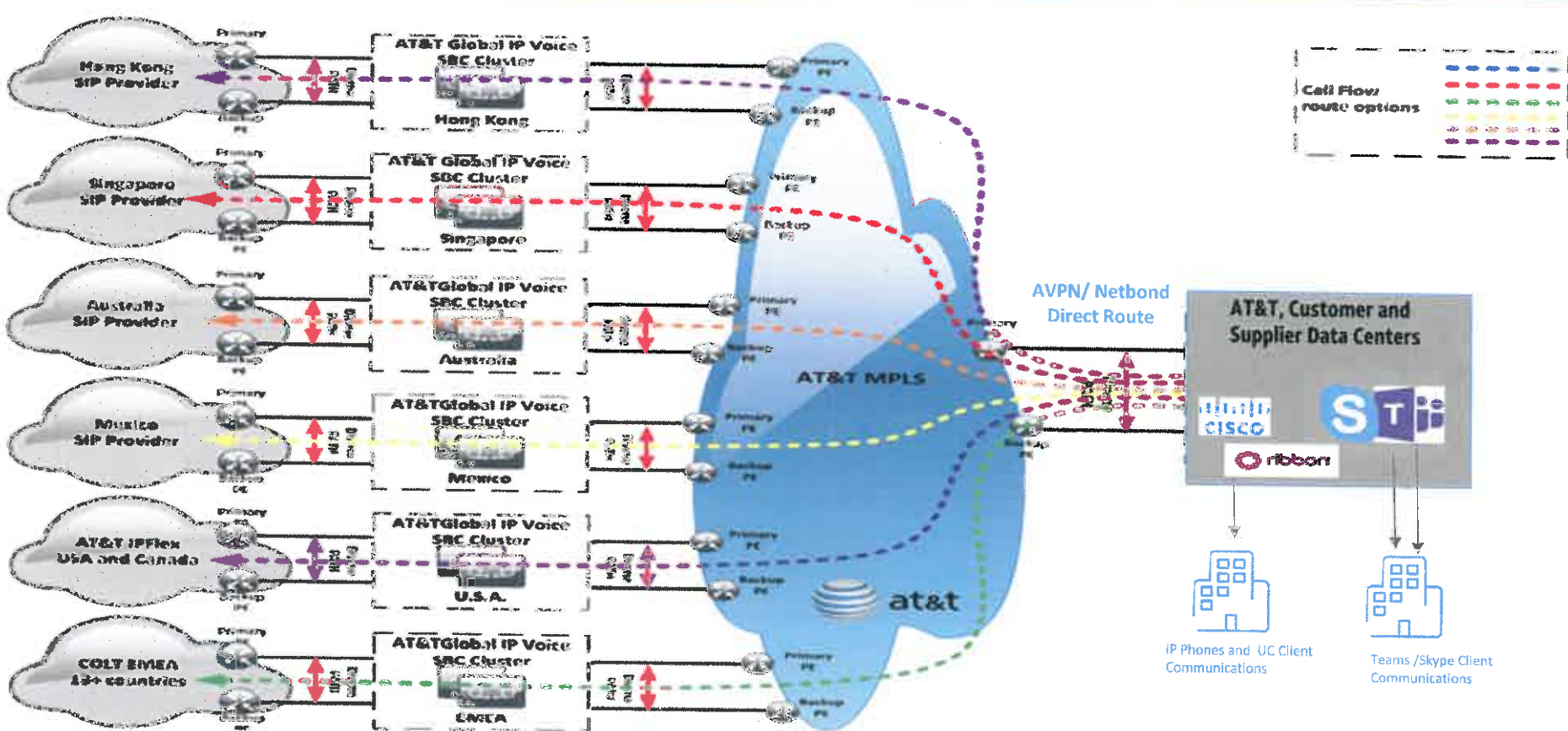
# AT&T Global Reach Approach



are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.



# Global SIP and core SBC for PSTN Access



© 2018 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.

# AT&T UC Profile Options

Monthly UC Port Charge Includes ( End User License, MACD Support, Core Hardware, Software upgrades, Monitoring and management support)

## UC Profiles

### UC Enhanced Profile



### UC Standard Profile



### UC Basic Profile



### UC Essential Profile



## Capabilities

#### UC Enhanced High level Feature Overview

- Presence/IM Client for mobile, PC and Tablet
- IP Phone Support
- Client for PC, MAC, iPad
- Single Number Reach
- Fixed Mobile Convergence (Call Grabber)
- Voicemail
- Provides audio, web, multi-party video conferencing + content sharing

#### UC Standard High Level Feature Overview

- Presence/IM Client for mobile, PC and Tablet
- IP Phone Support
- Single Number Reach
- Fixed Mobile Convergence
- Voice Mail
- Video Point to Point Call

#### UC Basic High Level Feature Overview

- IP Phone Support
- Single Number Reach
- Fixed Mobile Convergence
- Voice Mail

#### UC Essential High Level Feature Overview

- IP Phone and analog device support
- Common area phone features basic internal calling