AT&T IP Flexible Reach Service on AT&T MIS Service

Encryption Addendum
For
Cisco Unified Border Element (CUBE)
Customer Configuration Guide
with AT&T Certified IP-PBX Solutions

March 21, 2016
Version 1.0

AT&T IP Flexible Reach Service on AT&T MIS Service
Cisco Unified Border Element (CUBE)
Customer Configuration Guide for
Encryption with AT&T Certified IP-PBX Solutions
(March 21, 2016, Version 1.0)

Introduction

This Customer Configuration Guide ("CCG") provides recommended guidelines for configuring the Customer-managed Cisco Unified Border Element (CUBE) for Encryption operation with AT&T IP Flexible Reach Service on AT&T MIS Service ("AT&T MIS") as the Underlying Transport Service, specific to the various AT&T Certified IP-PBX Solutions listed below. The CUBE is cascaded behind the Customer Edge Router (CER). This CCG is to be used in conjunction with the appropriate IP-PBX/SBC CCG which cover the additional configurations required for use with this service including, but not limited to, configuration of the IP PBX and SBC. See the References section below for links to the appropriate documents based on the solution being used.

Encryption enhances the security of telephone communication by scrambling the call setup and audio between Customer end devices such as SBC and IP phones and the AT&T IP Border Element (IPBE) so that only the Customer's equipment and AT&T IPBE can read them. Encryption does not provide blanket security for telephony. Customers must assess their own security requirements and determine if encryption meets their needs. Several prerequisites must be met to enable Encryption. Your account team can help determine if this feature is available in your environment.

The following solutions are currently supported with a cascaded CUBE and are covered in this guide:

- Cisco Unified Communications Manager with cascaded Cisco CER / ASR CUBE 10.0
- Cisco Unified Communications Manager with cascaded ISR G2 CER / CUBE 10.0

Please ensure your system set-up is consistent with the recommended specifications provided in this document. AT&T reserves the right to modify or update its guidelines at any time without notice, so please check the following link to be sure you have the latest version of this

document (**http://www.corp.att.com/bvoip/ipflex/training/** *(login: att, password: attvoip)*). You may also wish to consult with your AT&T technical sales representative to have them verify that you have the latest document.

1 References

The document links below are hosted on either a public Cisco website not requiring authentication or an AT&T website requiring the following authentication; login: att, password: attvoip. Each certified solution is listed below with the required documentation to configure the IP-PBX/CUBE.

1.1 Caveats

Note that the caveats described in the following documents also apply to the Encryption mode of operation. In addition calls to toll free numbers that uses a network prompter (i.e., a valid response from the calling party is required before the toll free number provides connect) fail with no audio and dtmf from the phone to the toll free number. Typically this type of toll free number is used by large scale call handlers such as reservation systems and customer support lines. Fax is supported using the G.711 codec.

1.2 Cisco Unified Communications Manager with cascaded ASR CUBE 10.0 documentation

AT&T IP Flexible Reach Service with Enhanced Features Using MIS / PNT or AT&T Virtual Private Network Transport with Cisco Unified Communications Manager v. 10.5.2 and Cisco UBE v. 10.0.2 on an ASR Router with SIP Interface

http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/interoperability-portal/at-t-ip-flexible-reach-cisco-unified-border-element.pdf

The following documents may be helpful when configuring encryption (typically referred to as security within the documents). Always check with your vendor to verify that your design, environment and configuration are correct.

https://supportforums.cisco.com/document/73611/ip-phone-security-and-ctl-certificate-trust-list
https://supportforums.cisco.com/document/32011/secure-conference-cucm-614
http://www.cisco.com/c/en/us/td/docs/ios/voice/fxs/configuration/guide/15_1/fxs_15_1_cg_book/fxssccptlscm.html
http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/9x/integration/guide/cucm_sip/cucintcucmsip/cucintcucmsip060.pdf

1.3 Cisco Unified Communications Manager with cascaded ISR G2 CUBE documentation

NOTE – CUBE 10.0 requires 15.4(3)M1 IOS or CUBE 11.1 requires 15.5(3)M1 IOS

AT&T IP Flexible Reach Service With Enhanced Features Using MIS / PNT or AT&T Virtual Private Network Transport With Cisco Unified Communications Manager 10.0.1 and Cisco Unified Border Element X.Y
http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/interoperability-portal/application-notes-cucm-att-flexible-Reach.pdf

The following documents may be helpful when configuring encryption (typically referred to as security within the documents). Always check with your vendor to verify that your design, environment and configuration are correct.

https://supportforums.cisco.com/document/73611/ip-phone-security-and-ctl-certificate-trust-list
https://supportforums.cisco.com/document/32011/secure-conference-cucm-614
http://www.cisco.com/c/en/us/td/docs/ios/voice/fxs/configuration/guide/15_1/fxs_15_1_cg_book/fxssccptlscm.html

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/9x/integration/guide/cucm_sip/cucintcucmsip/cucintcucmsip060.pdf

2 Overview

AT&T IP Flexible Reach Service over AT&T MIS as the Underlying Transport Service is an AT&T Business Voice over IP (BVoIP) Service.

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

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

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

3 Special Considerations

- The following TCP/IP ports must not be blocked by firewall or access lists:
  - AT&T IP Border Element signaling and media addresses.
  - SIP signaling traffic (TCP port 5061).
  - SRTP/SRTCP traffic (UDP port range 16384-32767).
- The configuration information in this CCG assumes a single primary CER. Any alternate routing configurations or remote branch connectivity to other sites, within the same or other AT&T MIS, requires proper configuration of the signaling and media paths. Routing configurations in all Customer routers need to be set up to assure that the routing in the primary CER is not affected.
- All Customer managed components that will communicate with the AT&T IP Flexible Reach Service must be configured for secure operation. This includes configuring the CUBE to use Transport Layer Security (TLS) and Secure Real-Time Protocol (SRTP). Configuration may also include configuring CUCM, IP Phones, Cisco Unity Connection, Conference bridges, Voice Gateways and other components for TLS and/or SRTP operation.
- This solution does not use a secure transport between the CUCM and the CUBE. The customer is solely responsible for securing the connection between the CUCM and CUBE.

4 Cisco Unified Border Element Configurations for various IP-PBX Solutions

This section will assist in properly configuring Encryption on the Cisco Unified Border Element (CUBE) to insure interoperability with AT&T Certified IP-PBX solutions for use on AT&T IP Flexible Reach Service on AT&T MIS transport. Please review the section below that is applicable to your environment.

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

4.1 Cisco Unified Communications Manager with cascaded ISR G2 CUBE 10.0 or cascaded ASR CUBE 10.0 – Encryption with Media Flow Around (MFA)

This Cisco Unified Communications Manager (CUCM) solution works in conjunction with a CUBE that is separate from a Cisco CER (referred to as cascaded CUBE). This section covers the CUBE and CUCM specific commands. Please see the appropriate CCGs for CUCM specific configuration.

Note:

- The cascaded CUBE with Encryption only supports Customer Managed Sites running IOS **15.4(3)M1 (CUBE 10.0) on the ISR G2** or IOS **15.4(3)S1 (CUBE 10.0) on the ASR 1001 or ASR 1002.**
- **Please see the appropriate CCG for Media Flow Around configuration.**
- **Network Address Translation (NAT) of the Signaling Address is not an option for the cascaded CUBE solution with Encryption.**
- This section contains the additional steps and configuration required to support encryption.

4.1.1 High Level Requirements

- To support IP Phones at Internet connected remote sites the customer must provide a VPN tunnel for all communication between the CUCM and IP phones.
- The customer must obtain a certificate from a supported Certificate Authority (CA) for installation on CUBE. The only supported CA at this time is Symantec.
- The CUCM must be a restricted installation. There is a restricted and unrestricted product available from Cisco. Only the restricted product allows encryption of media and signaling.
- Cisco Unity Connection must be a restricted installation.
- Any other elements that exchange media with the AT&T IP Flexible Reach Service **MUST** support SRTP.
- CUCM must be put into mixed mode operation.

- The approach provided here employs encryption of: signaling between the CUBE and the AT&T IP Flexible Reach Service and media between Customer Premise Equipment (CPE) and the AT&T IP Flexible Reach Service.
- The customer is solely responsible for securing signaling between CPE components e.g., IP phones and CUCM or CUCM and CUBE.

4.1.2 Certificate Overview

The customer must obtain a certificate from an AT&T supported certificate authority. The request for a certificate requires information from the CUBE know as a Certificate Signing Request (CSR). To generate a CSR the customer must use the valid fully qualified domain name (FQDN) they will use to obtain the certificate as well as the customer's subject information. With this information the customer will generate the CSR and use it to obtain a certificate. The customer must then load on the CUBE, both their own certificate (here after referred to as customer certificate) and the Certificate Authority (CA) intermediate certificate.

4.1.3 Certificate Signing Request (CSR) to Support Encryption

Step 1: Generate an Exportable Key

In configuration mode issue the following command to generate an exportable key.

```
crypto key generate  rsa label <example_name>.key modulus 2048 exportable general-keys
```

Step 2: Create a Trustpoint

Create a trust point with the following commands.

```
crypto pki trustpoint <example_name>.trustpoint
!The prompt is now ca-trustpoint.
enrollment terminal
revocation-check none
rsakeypair <example_name>.key
fqdn <customer.supplied.fully.qualified.domain.name>
```

subject-name CN=<customer_supplied>,OU=<customer_supplied>,0=<customer_supplied>,C=<customer_supplied>,St=<customer supplied>,L=<customer_supplied>
!All of the subject-name information is provided by the customer and must agree exactly with the !information the customer will use to obtain the certificate. Note that if any subject-name value contains a !special character (space, comma, period, etc.) it should be enclosed in double quotes.

Step 3: Request the CSR

Request the CSR with this command. Note the prompts and answers.

crypto pki enroll <example_name_from_above>.trustpoint
!lines beginning with % are prompts from the CUBE
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=xxx.yyy.gtld,OU=aaa,O="asdf, inc.",C=zx,St=yyyyy,L=uuuuuuuuu
% The subject name in the certificate will include: <customer.supplied.fully.qualified.domain.name>
% Include the router serial number in the subject name? [yes/no]: ***no***
% Include an IP address in the subject name? [no]: ***no***
Display Certificate Request to terminal? [yes/no]: ***yes***
Certificate Request follows:
-----BEGIN NEW CERTIFICATE REQUEST-----
….removed for brevity….
-----END NEW CERTIFICATE REQUEST-----
Redisplay enrollment request? [yes/no]: ***no***
! NOTE – ASR does not include the BEGIN and END lines. They must be added manually when requesting a certificate.

Router configuration output:

crypto pki trustpoint <example_name>.trustpoint
enrollment terminal
fqdn <customer.supplied.fully.qualified.domain.name>
subject-name *CN=<customer.supplied.fully.qualified.domain.name>,OU=aaa,O="asdf, inc.",C=zx,St=yyyyy,L=uuuuuuuuu*

```
revocation-check none
rsakeypair <example_name>.key
```

Step 4: Using the CSR Obtain a Certificate

Copy the entire certificate and use it to obtain a certificate from a supported Certificate Authority. No formatting, line breaks, carriage returns, or other changes can be introduced.

4.1.4 Load the Certificates on the CUBE

Step 1: Load the Intermediate Certificate

Load the intermediate CA certificate. This certificate is provided by the CA to any users of this CA. Note the prompts and responses. Paste the certificate including the begin and end markers. Note that no formatting carriage return, line feed, etc. characters can be introduced to the certificate.

```
crypto pki authenticate <same trustpoint name as above>.trustpoint
!Enter the base 64 encoded CA certificate.
!End with a blank line or the word "quit" on a line by itself

        -----BEGIN CERTIFICATE-----
        ….removed for brevity….
        -----END CERTIFICATE-----
        quit
        Trustpoint '<example_name>.trustpoint' is a subordinate CA and holds a non self signed cert
        Certificate has the following attributes:
             Fingerprint MD5: XXXXXXXXXXXXXXXXXXXXXXXXXXXX
            Fingerprint SHA1: YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY

        % Do you accept this certificate? [yes/no]: yes
        Trustpoint CA certificate accepted.
        % Certificate successfully imported
```

Step 2: Load the CA Customer Certificate

Load the customer certificate. Note the prompts and responses. Paste the certificate including the begin and end markers. Note that no formatting carriage return, line feed, etc. characters can be introduced to the certificate.

```
crypto pki import <example_name>.trustpoint certificate
!Enter the base 64 encoded CA certificate.
!End with a blank line or the word "quit" on a line by itself

        -----BEGIN CERTIFICATE-----
        ….removed for brevity….
        -----END CERTIFICATE-----
        quit
        % Router Certificate successfully imported
```

4.1.5 Additional CUBE Configuration

Step 1: Add the Trustpoint to the SIP-UA Configuration

Add the trustpoint to the sip-ua section of the configuration.

```
sip-ua
 crypto signaling default trustpoint <example_name>.trustpoint
```

Step 2: Add Transport Layer Security (TLS) support to AT&T IP Flexible Reach Service Facing Dial-peers

Add support for TLS to each dial-peer that communicates with the AT&T IP Flexible Reach service. These changes are NOT made to dial-peers that communicate with the CUCM.

```
dial-peer voice <wxyz> voip
 session transport tcp tls
```

Step 3: Add Secure Real-Time Protocol (SRTP) support to ALL dial-peers

Add support for SRTP to each dial-peer involved in calls to or from the AT&T IP Flexible Reach service. These changes include dial-peers that communicate with the CUCM.

```
dial-peer voice <wxyz> voip
 srtp fallback
```

4.2 Cisco Unified Communications Manager with cascaded ISR G2 CUBE 11.1 or cascaded ASR CUBE 11.1 – Encryption with Media Flow Through

This Cisco Unified Communications Manager (CUCM) solution works in conjunction with a CUBE that is separate from a Cisco CER (referred to as cascaded CUBE). This section covers the CUBE and CUCM specific commands. Please see the appropriate CCGs for CUCM specific configuration.

Note:

- The cascaded CUBE with Encryption only supports Customer Managed Sites running IOS **15.5(3)M1 (CUBE 11.1) on the ISR G2** or IOS **15.5(3)S1a (CUBE 10.0) on the ASR 1001 or ASR 1002.**
- **Note the later IOS version required for CUBE when operating in media flow through mode.**
- **Network Address Translation (NAT) of the Signaling Address is not an option for the cascaded CUBE solution with Encryption.**
- This section contains the additional steps and configuration required to support encryption.

4.2.1 High Level Requirements

- To support IP Phones at Internet connected remote sites the customer must provide a VPN tunnel for all communication between the CUCM and IP phones.
- The customer must obtain a certificate from a supported Certificate Authority (CA) for installation on CUBE. The only supported CA at this time is Symantec.
- The CUCM must be a restricted installation. There is a restricted and unrestricted product available from Cisco. Only the restricted product allows encryption of media and signaling.
- Cisco Unity Connection must be a restricted installation.
- Any other elements that exchange media with the AT&T IP Flexible Reach Service **MUST** support SRTP.

- CUCM must be put into mixed mode operation.
- The approach provided here employs encryption of: signaling between the CUBE and the AT&T IP Flexible Reach Service and media between Customer Premise Equipment (CPE) and the AT&T IP Flexible Reach Service.
- The customer is solely responsible for securing signaling between CPE components e.g., IP phones and CUCM or CUCM and CUBE.

4.2.2 Certificate Overview

The customer must obtain a certificate from an AT&T supported certificate authority. The request for a certificate requires information from the CUBE know as a Certificate Signing Request (CSR). To generate a CSR the customer must use the valid fully qualified domain name (FQDN) they will use to obtain the certificate as well as the customer's subject information. With this information the customer will generate the CSR and use it to obtain a certificate. The customer must then load on the CUBE, both their own certificate (here after referred to as customer certificate) and the Certificate Authority (CA) intermediate certificate.

4.2.3 Certificate Signing Request (CSR) to Support Encryption

Step 1: Generate an Exportable Key

In configuration mode issue the following command to generate an exportable key.

```
crypto key generate  rsa label <example_name>.key modulus 2048 exportable general-keys
```

Step 2: Create a Trustpoint

Create a trust point with the following commands.

```
crypto pki trustpoint <example_name>.trustpoint
!The prompt is now ca-trustpoint.
enrollment terminal
revocation-check none
rsakeypair <example_name>.key
```

fqdn <customer.supplied.fully.qualified.domain.name>
subject-name
CN=<customer_supplied>,OU=<customer_supplied>,0=<customer_supplied>,C=<customer_supplied>,St=<customer supplied>,L=<customer_supplied>
!All of the subject-name information is provided by the customer and must agree exactly with the !information the customer will use to obtain the certificate. Note that if any subject-name value contains a !special character (space, comma, period, etc.) it should be enclosed in double quotes.

Step 3: Request the CSR

Request the CSR with this command. Note the prompts and answers.

crypto pki enroll <example_name_from_above>.trustpoint
!lines beginning with % are prompts from the CUBE
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=xxx.yyy.gtld,OU=aaa,O="asdf, inc.",C=zx,St=yyyyy,L=uuuuuuuuu
% The subject name in the certificate will include: <customer.supplied.fully.qualified.domain.name>
% Include the router serial number in the subject name? [yes/no]: ***no***
% Include an IP address in the subject name? [no]: ***no***
Display Certificate Request to terminal? [yes/no]: ***yes***
Certificate Request follows:
-----BEGIN CERTIFICATE-----
….removed for brevity….
-----END CERTIFICATE-----

Router configuration output:

crypto pki trustpoint <example_name>.trustpoint
enrollment terminal
fqdn <customer.supplied.fully.qualified.domain.name>
subject-name *CN=<customer.supplied.fully.qualified.domain.name>,OU=aaa,O="asdf, inc.",C=zx,St=yyyyy,L=uuuuuuuuu*
revocation-check none
rsakeypair <example_name>.key

Step 4: Using the CSR Obtain a Certificate

Copy the entire certificate and use it to obtain a certificate from a supported Certificate Authority. No formatting, line breaks, carriage returns, or other changes can be introduced.

4.2.4 Load the Certificates on the CUBE

Step 1: Load the Customer Certificate

Load the customer certificate. Note the prompts and responses. Paste the certificate including the begin and end markers. Note that no formatting carriage return, line feed, etc. characters can be introduced to the certificate.

crypto pki authenticate <same trustpoint name as above>.trustpoint
!Enter the base 64 encoded CA certificate.
!End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
….removed for brevity….
-----END CERTIFICATE-----
quit
Trustpoint '<example_name>.trustpoint' is a subordinate CA and holds a non self signed cert
Certificate has the following attributes:
Fingerprint MD5: XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Fingerprint SHA1: YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY

% Do you accept this certificate? [yes/no]: ***yes***
Trustpoint CA certificate accepted.
% Certificate successfully imported

Step 2: Load the CA Intermediate Certificate

Load the CA intermediate certificate provided by the customer. Note the prompts and responses. Paste the certificate including the begin and end markers. Note that no formatting carriage return, line feed, etc. characters can be introduced to the certificate.

```
crypto pki import <example_name>.trustpoint certificate
!Enter the base 64 encoded CA certificate.
!End with a blank line or the word "quit" on a line by itself

        -----BEGIN CERTIFICATE-----
        ….removed for brevity….
        -----END CERTIFICATE-----
        quit
        % Router Certificate successfully imported
```

4.2.5 Additional CUBE Configuration

Step 1: Add the Trustpoint to the SIP-UA Configuration

Add the trustpoint to the sip-ua section of the configuration.

```
sip-ua
 crypto signaling default <example_name>.trustpoint
```

Step 2: Add Transport Layer Security (TLS) support to AT&T IP Flexible Reach Service Facing Dial-peers

Add support for TLS to each dial-peer that communicates with the AT&T IP Flexible Reach service. These changes are NOT made to dial-peers that communicate with the CUCM.

```
dial-peer voice <wxyz> voip
 session transport tcp tls
```

Step 3: Add Secure Real-Time Protocol (SRTP) support to ALL dial-peers

Add support for SRTP to each dial-peer involved in calls to or from the AT&T IP Flexible Reach service. These changes include dial-peers that communicate with the CUCM.

```
dial-peer voice <wxyz> voip
 srtp fallback
```

Acronyms

Acronym	Translation
ADSL	Asymmetric Digital Subscriber Line
AIM	Advanced Integration Module A
AS	Autonomous System
ATM	Asynchronous Transfer Mode
AT&T VPN	AT&T Virtual Private Network
BC	Committed Burst
BE	Excess Burst or Best Effort
BGP	Border Gateway Protocol
BH	Bursty High
BL	Bursty Low
BOE	Branch Office Extension
CA	Certificate Authority
CAS	Channel Associated Signaling
CBWFQ	Class Based Weighted Fair Queuing
CCG	Customer Configuration Guide
CCS	Common Channel Signaling
CDR	Committed Data Rate
CEF	Cisco Express Forwarding
CER	Customer Edge Router
CHAP	Challenge Handshake Authentication Protocol
CIR	Committed Information Rate
CLI	Command Line Interface
CM	Communications Manager
COS	Class of Service
CPE	Customer Premise Equipment

Acronym	Translation
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRTP	Compress Real Time Protocol
CSR	Certificate Signing Request
CSU/DSU	Channel Service Unit / Data Service Unit
CUBE	Cisco Unified Border Element
CUCM	Cisco Unified Communications Manager
DID	Direct Inward Dial
DS	Down Stream
DSCP	Differentiated Service Code Point
DSL	Digital Subscriber Line
DSP	Digital Signal Processors
DTMF	Dual Tone Multi Frequency
E&M	Ear & Mouth
EF	Expedient Forwarding
ePVC	Enhanced Permanent Virtual Circuit
FR	Frame Relay
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station
FQDN	Fully Qualified Domain Name
GSM FR	Global System for Mobile communications Full Rate
HDV	High Density Voice
HWIC	High-speed WAN Interface Card
IAR	Inbound Alternate Routing
IETF	Internet Engineering Task Force
IMA	Inverse Multiplexing over ATM
IOS	Internetwork Operation System
IP	Internet Protocol
IPBE	Internet Protocol Border Element

Acronym	Translation
IPSEC	Internet Protocol Security
ISR	Integrated Services Router
ITU-T	International Telecommunication Union - Telecommunications
GW	Gateway
LAN	Local Area Network
LFI	Link Fragmentation and Interleaving
LLQ	Low Latency Queuing
LD	Long Distance
MFA	Media Flow Around
MGCP	Media Gateway Control Protocol
MLPPP	Multi-Link Point-to-Point Protocol
MM	Multi Media
MOW	Most Of World
MRG	Media Resource Group
MRGL	Media Resource Group List
MTP	Media Termination Point
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NET	Network Equipment Technologies
NM	Network Module
NPE	Network Processing Engine
NTE	Named Telephone Event
OAM	Operation Administration & Maintenance
OCS	Office Communication Server
PA	Port Adapter
PAT	Port Address Translation
PBX	Private Branch Exchange
PC	Personal Computer
PCR	Peak Cell Rate

Acronym	Translation
PER	Provider Edge Router
POS	Packet over SONET
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PQ	Priority Queue
PRI	Primary Rate Interface
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
PVDM	Packet Voice DSP Module
QOS	Quality of Service
QSIG	Q Signaling
RC	Receive
RFC	Request for Comment
RT	Real Time
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SBC	Session Border Controller
SCCP	Skinny Call Control Protocol
SCR	Sustainable Cell Rate
SHDSL	Single-Pair High-Speed Digital Subscriber Line
SIP	Session Initiation Protocol
SM	Session Manager
SPE	Synchronous Payload Envelope
SRTP	Secure Real-Time Protocol
TAC	Technical Assistance Center
TC	Time Interval
TCP	Transport Control Protocol
TDM	Time Division Multiplexing

Acronym	Translation
TLS	Transport Layer Security
TN	Telephone Number
TX	Transmit
UDP	User Datagram Protocol
US	Up Stream or United States
VAD	Voice Activity Detection
VCI	Virtual Circuit Identifier
VLAN	Virtual Local Area Network
VNI	Voice Network Infrastructure
VoIP	Voice over Internet Protocol
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VT	Virtual Template
WAN	Wide Area Network
WFQ	Weighted Fair Queuing
WIC	WAN Interface Card

This Customer Configuration Guide ("CCG") is offered as a convenience to AT&T's customers. The specifications and information regarding the product in this CCG are subject to change without notice. All statements, information, and recommendations in this CCG are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided “AS IS”. Users must take full responsibility for the application of the specifications and information in this CCG.

In no event shall AT&T or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage arising out of the use or inability to use this CCG, even if AT&T or its suppliers have been advised of the possibility of such damage.