



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

Customer Edge Router (CER) Customer Configuration Guide for AT&T IP Flexible Reach Service and AT&T IP Toll-Free on AT&T VPN Service as the Underlying Transport Service

Cisco 4000 Series Integrated Services Routers

December 8, 2015

Version 1.1

© 2015 AT&T Intellectual Property. All rights reserved.

AT&T, the AT&T logo and all other AT&T 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.

Table of Contents

1	INTRODUCTION	4
1.1	OVERVIEW	4
1.1.1	Access Types	5
1.1.2	Software Information	5
1.2	NETWORK TOPOLOGY	5
1.2.1	AT&T Certified IP-PBX's	6
1.2.2	CER combined with TDM Gateway	8
1.3	SPECIAL CONSIDERATIONS	9
2	NETWORK DESIGN	9
2.1	BANDWIDTH ALLOCATION	9
2.1.1	Simultaneous Voice Calls	9
2.1.2	Per Call Bandwidth	10
2.1.3	Bandwidth Reduction Techniques	12
2.1.4	Putting It Together	12
2.2	SPECIAL ENGINEERING GUIDELINES FOR ETHERNET ACCESS	13
3	TRAFFIC CLASSIFICATION AND QUEUING TECHNIQUES	13
3.1	CLASSIFICATION	14
3.2	QUEUING OPTIONS	14
3.3	TRAFFIC SHAPING	15
4	CUSTOMER EDGE ROUTER (CER) CONFIGURATIONS SPECIFIC TO COS AND WAN INTERFACE	15
4.1	CLASSIFICATION	15
4.1.1	IPv4 Classification	15
4.1.2	IPv6 Classification	17
4.2	LLQ/CBWFQ SET UP AND PACKET MARKING	18
4.2.1	PPP access	19
	PPP access is supported on T1, E1, T3 and E3 speeds	19
4.2.2	Frame Relay Encapsulation	20
4.2.3	Ethernet Access	21
4.2.4	MLPPP Access	22
4.2.5	CoS6 Service Policy Example	22
4.3	FRAME RELAY TRAFFIC SHAPING	23
4.4	INTERFACE CONFIGURATION	23
4.4.1	PPP access	23
4.4.2	Frame Relay Encapsulation	25
4.4.3	Ethernet Access	26
4.4.4	MLPPP	27
APPENDIX A:	SAMPLE CONFIGURATIONS	30
A.1	SAMPLE ETHERNET CONFIGURATION	30
A.2	SAMPLE MLPPP CONFIGURATION	33
A.3	SAMPLE T3 PPP CONFIGURATION	38
APPENDIX B:	INBOUND ALTERNATE ROUTING	43
APPENDIX C:	BRANCH OFFICE EXTENSION (BOE)	43
C.1	INTRODUCTION TO BOE	43
C.2	IMPLEMENTATION CHECKLIST	46
C.3	EMERGENCY SERVICES	47

AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free on AT&T VPN
Cisco 4000 Series ISR Customer Configuration Guide (December 8, 2015, Version 1.0)

C.4 TROUBLESHOOTING	47
APPENDIX D: ACRONYMS	49

1 Introduction

This Customer Configuration Guide (“CCG”) provides recommended guidelines for configuring the Customer-managed Customer Edge Router (CER) for use with AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free on AT&T VPN Service as the Underlying Transport Service. CERs can be utilized for either one of those services or for both services simultaneously. Please ensure your system set-up is consistent with the recommended specifications provided in this document. AT&T reserves the right to modify or update its guidelines at any time without notice so please check the following link to be sure you have the latest version of this document (<http://www.corp.att.com/bvoip/avpn/implementation/> (login: att, password: attvoip)). You may also wish to consult with your AT&T technical sales representative.

1.1 Overview

AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free over AT&T VPN as the underlying transport are AT&T Business Voice over IP (BVoIP) services. AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free on AT&T VPN support network based Class of Service (CoS) which will work in conjunction with edge router configurations to provide the Quality of Service (QoS) that voice traffic requires. Four classes or six classes are available, including a Real Time class that will strictly prioritize voice packets over other data packets. Prioritizing voice packets helps to assure low latency for voice to meet delay budget constraints. This document should be used solely as a general configuration guideline. The Customer is solely responsible for determining the appropriate configuration of their specific environment; AT&T provides resources to assist with that configuration, please contact your AT&T technical support 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 manager 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.

1.1.1 Access Types

Following are the access types that can be ordered on the ISR 4K platforms::

Access Type	Speed (bit/s)
T1/E1 PPP access	1024K to 2M
NXT1/E1 MLPPP access	N = 2 to 8 T1/E1
T3/E3 PPP Access	5M to 45M
T3/E3 Frame Relay Encapsulation	5M to 45M
Ethernet	.5M to 1G

1.1.2 Software Information

Configurations in this guide were tested with IOS XE IOS XE 3.13.2S (Cisco IOS 15.4(3)S2).

CER with combined TDM Gateway or CUBE will require the UC (Unified Communications) Technology Package License.

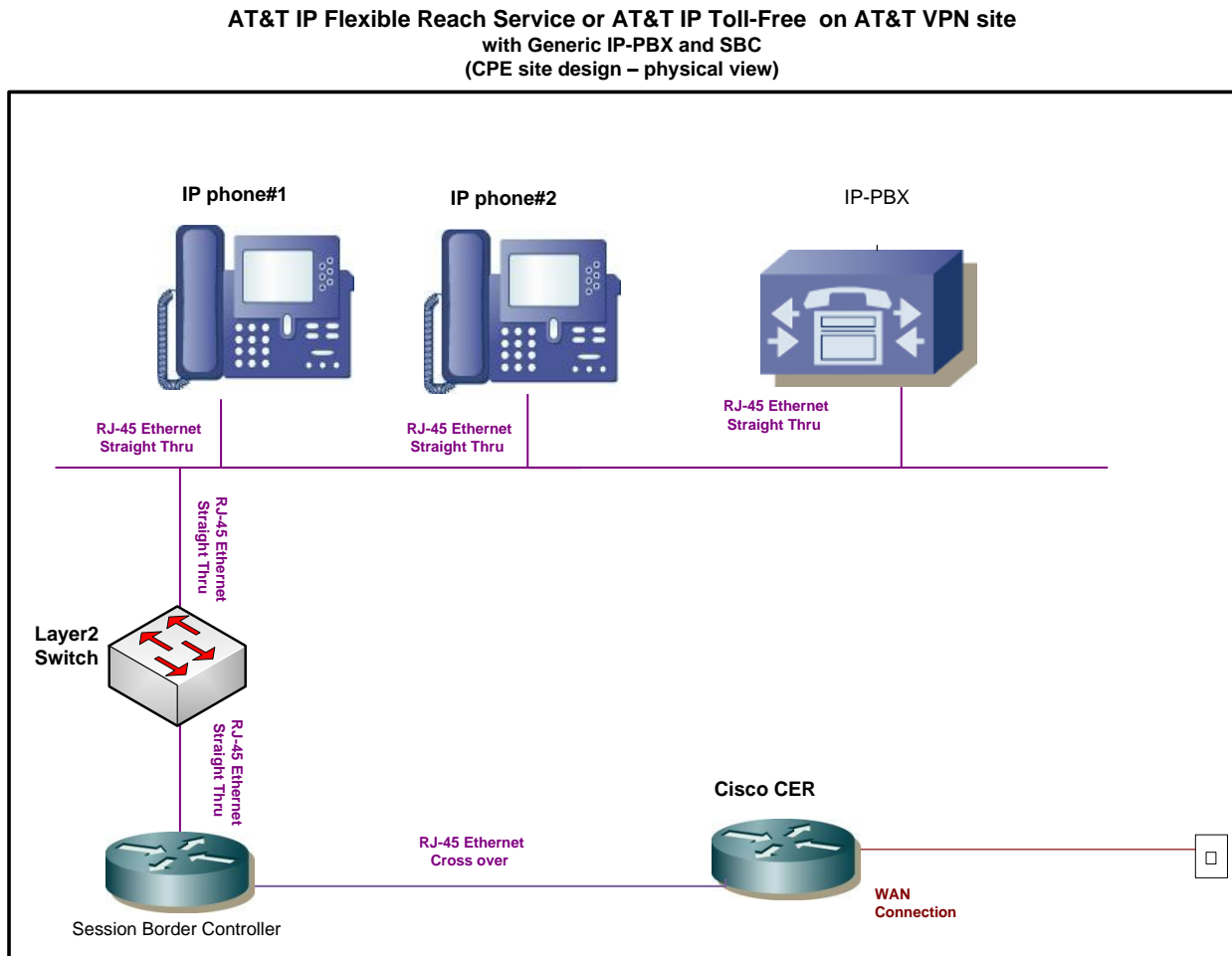
1.2 Network Topology

This section describes the generic AT&T supported topologies for various vendor IP-PBX's.

- Please refer to the following documents for details on configuring vendor specific AT&T supported topologies and related configuration information for IP-PBX's:
 - “*Customer Edge Router Customer Configuration Guide for AT&T Certified IP-PBX Solutions*”. (<http://www.corp.att.com/bvoip/avpn/implementation/> (login: att, password: attvoip)).
 - “*Customer Edge Router Customer Configuration Guide for Integrated CER/CUBE with AT&T Certified IP-PBX Solutions*”. (<http://www.corp.att.com/bvoip/avpn/implementation/> (login: att, password: attvoip)).
- Please refer to the following document for details on configuring a TDM Gateway: “*TDM Gateway Customer Configuration Guide for AT&T IP Flexible Reach Service on AT&T VPN Service and AT&T IP Toll Free on AT&T VPN Service*” (<http://www.corp.att.com/bvoip/avpn/implementation/> (login: att, password: attvoip)). Use the appropriate guide for your router platform.

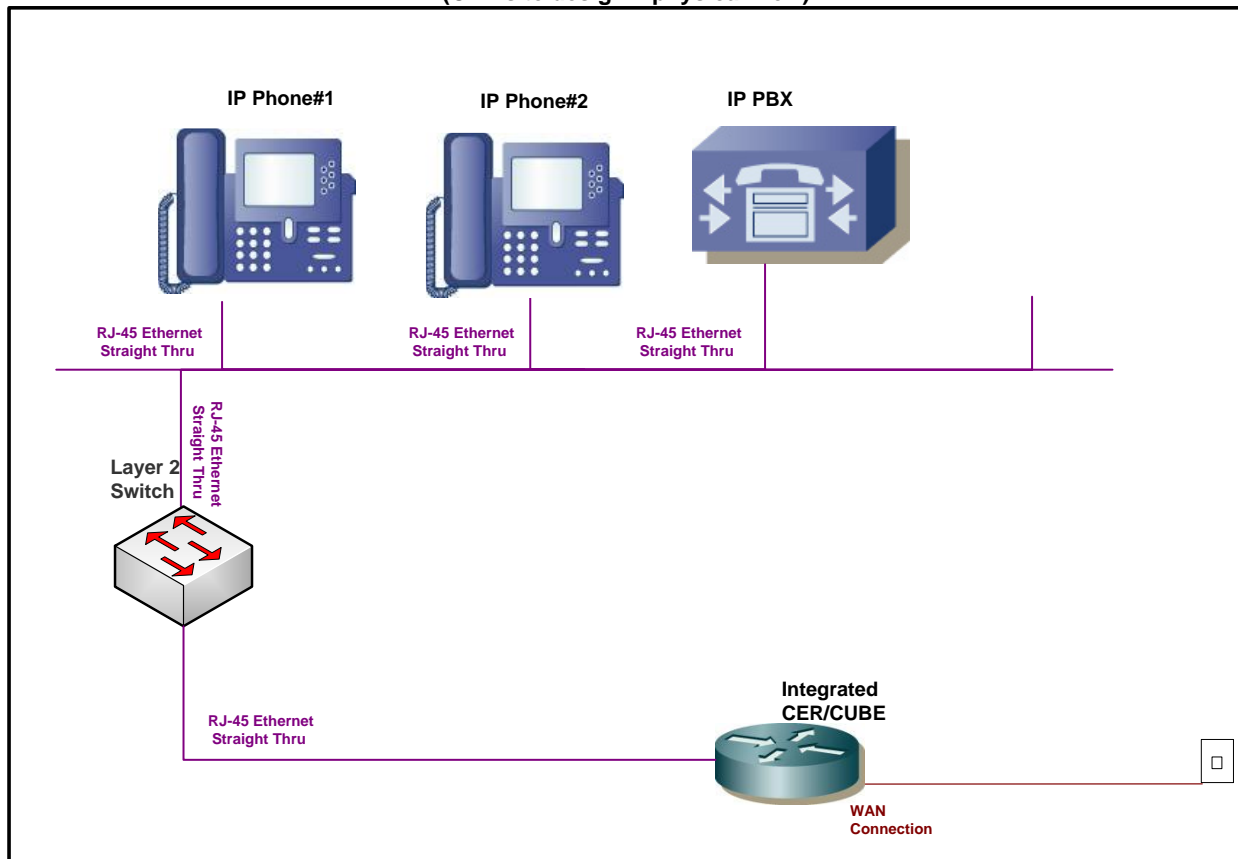
1.2.1 AT&T Certified IP-PBX's

Following is a sample diagram of a network topology for a site with an AT&T Certified IP-PBX. In this design, the Customer Edge Router (CER) and Session Border Controller (SBC) are two separate devices.



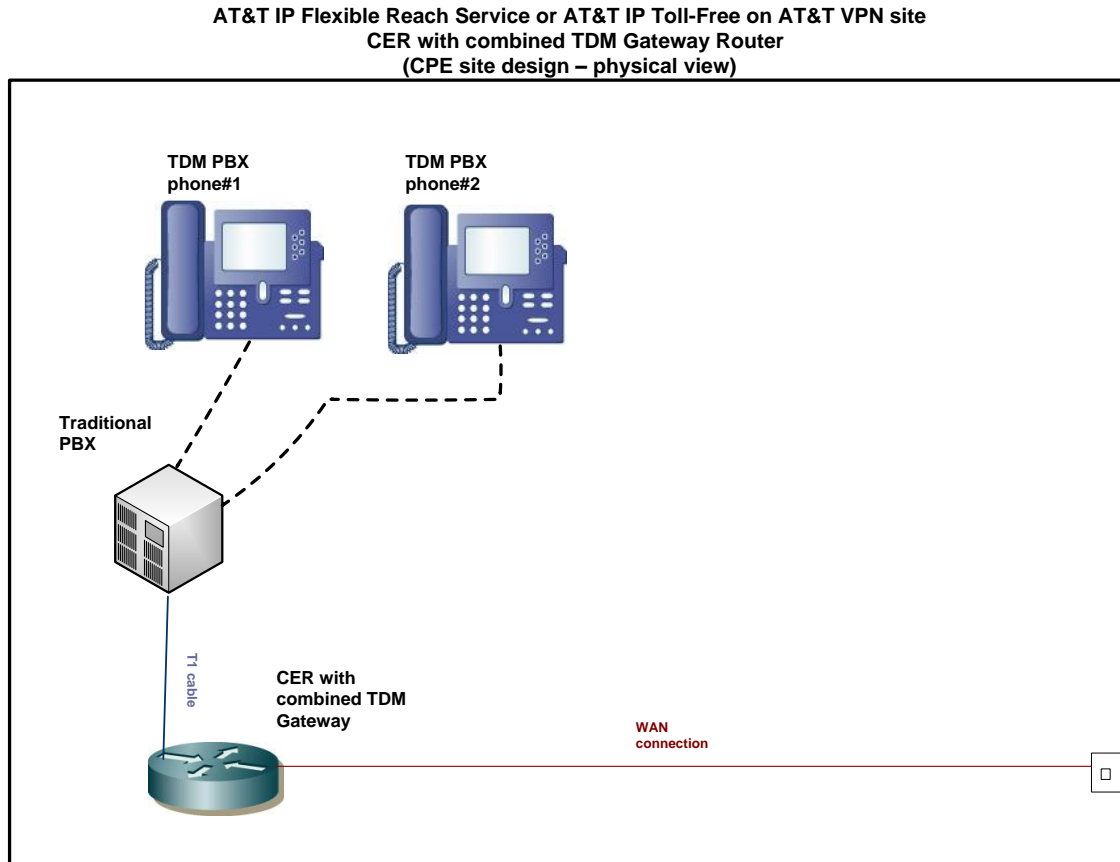
Following is a sample diagram of a network topology for a site with an AT&T Certified IP-PBX. In this design, the Customer Edge Router (CER) and Cisco Unified Border Element (CUBE) Session Border Controller (SBC) are integrated into a single device. NOTE: This solution is only supported for specific scenarios. Please refer to the "[Customer Edge Router Customer Configuration Guide for Integrated CER/CUBE with AT&T Certified IP-PBX Solutions](#)". (<http://www.corp.att.com/bvoip/avpn/implementation/> (login: att, password: attvoip)).

AT&T IP Flexible Reach Service or AT&T IP Toll-Free on AT&T VPN site
with Generic IP-PBX and SBC
(CPE site design – physical view)



1.2.2 CER combined with TDM Gateway

Following is a sample diagram of a network topology for a site with a CER combined with a TDM gateway .



1.3 *Special Considerations*

- The following TCP/IP ports must not be blocked by firewall or access lists:
 - AT&T IP Border Element signaling and media addresses.
 - SIP signaling traffic (UDP port 5060).
 - RTP/RTCP traffic (UDP port range 16384-32767).
- The configuration information in this CCG assumes a single primary CER. Any alternate routing configurations or remote branch connectivity to other sites, within the same or other AT&T VPN, requires proper configuration of the signaling and media paths. Routing configurations in all customer routers need to be set up to assure that the routing in the primary CER is not affected.
- Class of Service (CoS) specific considerations:
 - CoS1 should not be more than 70% for ATM or Ethernet access.

2 Network Design

Before implementing AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free over AT&T VPN as the underlying transport service, it is critical to understand the voice requirements at each location and to plan accordingly. Improper design can ultimately lead to poor voice performance.

The two primary network attributes that must be determined are:

- The allocated bandwidth for voice at each site.
- The delay components and requirements for acceptable voice quality.

2.1 *Bandwidth Allocation*

Primary factors in determining the bandwidth design for AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free over AT&T VPN as the underlying transport service are:

1. The number of simultaneous voice calls.
2. The per call bandwidth (Codec type + overhead).
3. Whether or not bandwidth reduction techniques are required.

Based on the above, the Class of Service (CoS) package can be selected including the calculation of the Committed Information Rate (CIR) and Real Time percentages.

2.1.1 *Simultaneous Voice Calls*

One of the most important aspects in designing a network with AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free over AT&T VPN as the underlying transport service is allocating enough bandwidth for voice calls. The required bandwidth is determined by

calculating the number of concurrent voice calls that must be supported at each location, and multiplying this by the bandwidth required per call. Concurrent call requirements may be simply based on the number of users at a site, or if the busy hour traffic load is known, the number of concurrent calls can be determined using the Erlang B formula. A web-based Erlang calculator, as well as more complex design tools, may be found at <http://www.erlang.com/>. Systems can be configured to accommodate up to the number of concurrent calls contracted for under their AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free contract. If the number of concurrent calls under contract is not sufficient, please contact AT&T to increase the number of concurrent calls under contract.

2.1.2 Per Call Bandwidth

Once the number of concurrent calls has been determined, the per-call bandwidth requirements need to be established. Bandwidth requirements are based on the codec as well as the Layer 2 protocol used to access the network. The most popular codec in use today is G.729; it is the default in Cisco voice equipment and can provide good quality, low bandwidth voice. The following table provides the bandwidth per call over various access types

While the G.729 codec is very popular today, it has limitations that should be investigated while designing the network. Certain call flows (like conference calls, voice mail applications) may require that a G.711 codec be used. Be aware that G.711 requires much higher bandwidth although it does support better call quality. If G.711 needs to be supported on the network, these higher bandwidth requirements should be taken into account in the design phase.

AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free on AT&T VPN
 Cisco 4000 Series ISR Customer Configuration Guide (December 8, 2015, Version 1.0)

Access Type	Codec	Ptime (ms)	IPV4 Bandwith Per call (Kbit/s)
Ethernet	G729 A	20	30.3
	G729 A	30	23.2
	G711	20	86.0
	G711	30	78.8
Ethernet with VLAN	G729 A	20	31.9
	G729 A	30	24.2
	G711	20	87.6
	G711	30	79.9
PPP or FR Encapsulation	G729 A	20	26.3
	G729 A	30	20.5
	G711	20	81.9
	G711	30	76.1
NX T1/E1 MLPPP	G729 A	20	25.5
	G729 A	30	19.9
	G711	20	81.1
	G711	30	75.5

Access Type	Codec	ptime (ms)	IPV6 Bandwith Per call (Kbit/s)
Ethernet with VLAN	G729 A	20	40.0
	G729 A	30	29.6
	G711	20	95.6
	G711	30	85.3
PPP or FR Encapsulation	G729 A	20	34.3
	G729 A	30	25.8
	G711	20	90.0
	G711	30	81.5
NX T1/E1 MLPPP	G729 A	20	33.5
	G729 A	30	25.2
	G711	20	88.9
	G711	30	80.8

Note: T.38 is the recommended protocol for fax as it has reduced bandwidth compared to G.711 fax. Configured properly to a baud rate of 14400 (this speed required for certain PSTN calls).

Note: A bandwidth calculator is available, currently at no charge to Cisco TAC users, that provides the exact layer 2 overhead calculations for voice over IP over Frame Relay and can be found at: http://tools.cisco.com/Support/VBC/jsp/Codec_Calc1.jsp This calculator takes into account overhead and also provides recommendations for potentially changing the default payload size in order to get better per call bandwidth performance.

Note: T.38 is the recommended protocol for fax as it has reduced bandwidth compared to G.711 fax. Configured properly to a baud rate of 14400 (this speed required for certain Public Switched Telephone Network (PSTN) calls), the T.38 fax call will use approximately 25Kbit/s over Frame Relay.

2.1.3 Bandwidth Reduction Techniques

There are several techniques for lowering the per call bandwidth requirements.

VAD or Voice Activity Detection (also known as silence suppression) may be turned on to take advantage of the fact that voice calls are “half duplex”—that is only one speaker in one direction is active at a time. Studies have shown that while theoretically VAD could reduce bandwidth consumption by 50%, a more conservative figure to use in design is 30%. Many users find that VAD can cause call impairment known as clipping — where the first word or words are cut off when a speaker starts and, therefore, they do not use VAD even though it might help with the bandwidth consumption. A “best practice”, conservative design approach would be to size the network without VAD, test calls with VAD once the network is in place and adjust the bandwidth accordingly assuming VAD works effectively.

Most VoIP codecs can be modified from the default parameters to provide more efficient utilization of bandwidth for carrying voice traffic. One popular technique is to increase the number of voice samples in each IP packet. VoIP packets tend to be quite small, with a large percentage of the usable bandwidth consumed by protocol overhead (Layer 2, IP, UDP, RTP). Typically, G.729 encodes two 10mS voice samples in each IP packet. Each voice sample is only 10 bytes. The codec can often be modified to pack 3 or even more voice samples in each IP packet, substantially reducing the overhead:payload ratio. The downside of this approach is that it increases the encoding/decoding delay proportionately and more stringent overall design relative to latency and jitter.

2.1.4 Putting It Together

Once concurrent calls and bandwidth consumption per call have been determined, the network requirements should be chosen. AT&T recommends using the Real Time (RT) Class of Service for voice signaling and media traffic. CoS packages are sold based on percentages of the CIR purchased. Two CoS packages support RT CoS—Multimedia High and Multimedia Low. If the percentage of RT traffic is 50% or lower than the CoS Package is Multi-Media Standard and if the percentage of RT is above 50% the CoS Package is Multi-Media High.

For details on configuring CERs for the basic AVPN transport service, independent of IP Flexible Reach Service and/or AT&T IP Toll-Free, reference:

AT&T VPN Service Customer Router Configuration Guide

This Guide is available on AT&T *BusinessDirect* under *Insight and News, Tech Specs* or from your Sale team.

The bandwidth allocated to the RT class is very important because any traffic presented to RT over the allocation will be strictly policed and dropped in order to prevent queuing and additional delay. For instance, a link is designed for 10 calls and an 11th call comes in. The 11th call will not be denied but will cause packet drops across all calls. Those packet drops can cause voice quality degradation of the existing calls. To avoid this problem, RT sizing is critical.

Note: Sizing of data requirements, possibly including video, is beyond the scope of this document but is covered in: *AT&T Network Services COS Customer Router Configuration Guide*

2.2 Special Engineering Guidelines for Ethernet Access

Three basic types of Ethernet access will be supported: Full Port, single VLAN tag, and stacked dual VLAN tag (Q in Q) ports. Full port is setup the same as single VLAN tag.

Ethernet actually has the most protocol overhead of any supported transport. Ethernet Line Rate requires 112 bytes for each 30 Byte payload. The Line Rate includes the inter-frame gap, preamble, start of frame delimiter, & CRC for each frame which adds to the total. So the protocol difference is about 1.6% more for Ethernet, at approximately 73% protocol overhead of all transported bytes. Ethernet configurations options are unique, as detailed below:

1. CoS1 for Ethernet should not be > than 70% to compensate for overhead.
2. Shaping Rates should be computed to 99% of Port speed – rounded down to the nearest 64K.

3 Traffic Classification and Queuing Techniques

Class of Service features operate in concert with customer router behaviors to provide end-to-end congestion management of application traffic flows. The Customer Edge Router (CER) has several roles in the process. First, it must recognize and categorize the different application types that are to receive differentiated service. Based on this recognition, queuing, fragmentation and interleaving techniques are used as appropriate to provide preferential treatment of priority traffic during congestion. In addition to the treatment within the CER, the network needs to recognize and provide differentiated treatment of customer application traffic. To accommodate this, the CER needs to mark the various application types with appropriate Differentiated Services (DiffServ) codepoints. This allows the network to recognize the different traffic types to provide the desired preferential treatment.

After determining bandwidth requirements and the techniques required to meet the delay budgets, CoS techniques should be applied in the CER to compliment the functionality in the network PER. CoS techniques will help minimize delay, jitter (variation in delay) and drops of voice packets. These techniques include classifying and marking packets by traffic type, using queuing techniques, and traffic shaping.

3.1 **Classification**

The first step in traffic classification is to identify different traffic flows and mark them with the appropriate Differentiated Service Code Point (DSCP) bit. The following table defines the settings expected by the AT&T VPN network.

Class of Service	IP Precedence	DSCP	DSCP Decimal	DSCP Binary (In Contract)
Real Time	5	EF	46	101 110
Bursty High	3	AF31	26	011 010
Bursty Low	2	AF21	18	010 010
Best Effort	0	BE	0	000 000

Additional Classes for CoS6:

Class of Service	IP Precedence	DSCP	DSCP Decimal	DSCP Binary (In Contract)
Video (CoS2V)	4	AF41	34	100 010
Scavenger (CoS5)	1	AF11	10	001 010

3.2 **Queuing Options**

Queuing techniques and implementations have evolved over the past several years and include options that can strictly prioritize voice traffic over data traffic without starving out the data traffic. Strict priority queuing is a mechanism that will always immediately serve any packets in the priority queue before serving any other queue, ensuring the best possible delay characteristics. In the AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free over AT&T VPN as the Underlying Transport Service, AT&T uses Low Latency Queuing with Class Based Weighted Fair Queuing (LLQ/CBWFQ) and recommends that customers use the same techniques in their CERs. LLQ/CBWFQ is configured via a policy map where different classes of traffic are assigned a percentage or specific amount of bandwidth. The LLQ is established with the priority command and given a specific bandwidth in kilobits per second. The LLQ is sized based on the bandwidth allocation recommendations in section 2.1. Other queues are serviced based on the amount of bandwidth allocated to them.

3.3 **Traffic Shaping**

Traffic shaping on high speed circuits is done by setting a “service-policy” on the interface (or sub-interface) as shown in the examples in Appendix A. The shape rate is set by taking a percentage of the available bandwidth for a particular circuit type (or the substrate speed in the case of substrates).

4 **Customer Edge Router (CER) Configurations specific to CoS and WAN interface**

The router configurations in this section are partial configurations for AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free over AT&T VPN as the underlying transport service. Sample configurations, relative to specific environments, have been provided for reference in Appendix A.

The information below will assist you in configuring CoS and the WAN interface on the CER. Please review each of the sections below, Sections 4.1 through 4.5, to identify the configurations applicable to your specific environment.

4.1 **Classification**

Following are the access group list configurations. Data and video classes would be defined by the customer. RTP, SIP, SCCP and BGP access-lists should be configured as they are shown. CoS4 (default class) does not need to be defined. IP

4.1.1 **IPV4 Classification**

The following configurations are for IPV4 classification.

```
ip access-list extended RTP
permit udp any range 16384 32767 any range 16384 32767
ip access-list extended SIP
permit udp any eq 5060 any
permit udp any any eq 5060
permit tcp any eq 5060 any
permit tcp any any eq 5060
ip access-list extended SCCP **Only needed for Cisco UCM solutions**
permit tcp any range 2000 2003 any
permit tcp any any range 2000 2003
```

```
ip access-list extended BGP
permit tcp any eq bgp any
permit tcp any any eq bgp
ip access-list extended COS2-Traffic
permit udp any any eq 2082 <sample only – COS2 customer defined>
permit udp any eq 2082 any <sample only – COS 2 customer defined>
ip access-list extended COS3-Traffic
permit udp any any eq 2083 <sample only – COS3 customer defined>
permit udp any eq 2083 any <sample only – COS3 customer defined>
```

Note: Even if no CoS2 traffic is ordered, a minimum percentage of CoS2 must be configured on the CER if BGP routing is used, because BGP traffic falls into CoS2.

Additional Access-Lists for CoS6:

```
ip access-list extended COS2V-Traffic
permit tcp any any range 3230 3231 <sample only – COS2V customer defined>
permit udp any any range 3230 3235 < sample only – COS2V customer defined>

ip access-list extended COS5-Traffic
permit udp any any eq 110 <sample only – COS5 customer defined>
permit udp any eq 110 any <sample only – COS5 customer defined>
```

In order to classify the traffic that will be put into different queues, the class-map statement is used to match access-groups. In this example, the voice traffic is matched from access group lists “RTP”(which includes Real Time Control Protocol (RTCP) traffic) and “SIP” and put into a class called CoS1 for real time traffic. Note that the names used in the class-map are the same names used in the policy map in section 4.2—this is critical to ensure that the right policy will be applied to the right class. Note: These classifications are the same for all access types.

```
class-map match-any COS1
match access-group name RTP
match access-group name SIP
match access-group name SCCP
class-map match-any BGP
match access-group name BGP
class-map match-any COS2
match access-group name COS2-Traffic
match access-group name BGP
class-map match-any COS3
```



```
match access-group name COS3-Traffic
```

Additional Class-maps for CoS6:

```
class-map match-any COS2V
  match access-group name COS2V-Traffic
class-map match-any COS5
  match access-group name COS5-Traffic
```

4.1.2 IPV6 Classification

The following configurations are for IPV6 classification.

```
ipv6 access-list RTP_IPV6
  permit udp any range 16384 32767 any range 16384 32767
!
ipv6 access-list SIP_IPV6
  permit udp any eq 5060 any
  permit udp any any eq 5060
  permit tcp any eq 5060 any
  permit tcp any any eq 5060
!
ipv6 access-list SCCP_IPV6 **Only needed for Cisco UCM solutions**
  permit tcp any range 2000 2003 any
  permit tcp any any range 2000 2003
!
ipv6 access-list BGP_IPV6
  permit tcp any eq bgp any
  permit tcp any any eq bgp
!
ipv6 access-list COS2-Traffic_IPV6
  permit udp any any eq 2082 <sample only – COS2 customer defined>
  permit udp any eq 2082 any <sample only – COS 2 customer defined>
!
ipv6 access-list COS3-Traffic_IPV6
  permit udp any any eq 2083 <sample only – COS3 customer defined>
  permit udp any eq 2083 any <sample only – COS3 customer defined>
```

Note: Even if no CoS2 traffic is ordered, a minimum percentage of CoS2 must be configured on the CER if BGP routing is used, because BGP traffic falls into CoS2.

Additional Access-Lists for CoS6:

```
ipv6 access-list extended COS2V-Traffic_IPV6
permit tcp any any range 3230 3231 <sample only – COS2V customer defined>
permit udp any any range 3230 3235 < sample only – COS2V customer defined>
!
ipv6 access-list extended COS5-Traffic_IPV6
permit udp any any eq 110 <sample only – COS5 customer defined>
permit udp any eq 110 any <sample only – COS5 customer defined>
```

In order to classify the traffic that will be put into different queues, the class-map statement is used to match access-groups. In this example, the voice traffic is matched from access group lists “RTP”(which includes Real Time Control Protocol (RTCP) traffic) and “SIP” and put into a class called CoS1 for real time traffic. Note that the names used in the class-map are the same names used in the policy map in section 4.2—this is critical to ensure that the right policy will be applied to the right class. Note: These classifications are the same for all access types.

```
class-map match-any COS1
match access-group name RTP_IPV6
match access-group name SIP_IPV6
match access-group name SCCP_IPV6
class-map match-any BGP
match access-group name BGP_IPV6
class-map match-any COS2
match access-group name COS2-Traffic_IPV6
match access-group name BGP_IPV6
class-map match-any COS3
match access-group name COS3-Traffic_IPV6
```

Additional Class-maps for CoS6:

```
class-map match-any COS2V
match access-group name COS2V-Traffic
class-map match-any COS5
match access-group name COS5-Traffic
```

4.2 **LLQ/CBWFQ Set up and Packet Marking**

The Low Latency Queue is established through a priority statement. The class “CoS1” is put in the low latency queue. The packets are then marked with IP dscp of ‘ef’ to match the network’s expectation for real time service. The remaining bandwidth is distributed among the other classes—CoS2(bursty high traffic) and CoS3 (bursty low traffic) and marked with the appropriate IP Differentiated Services Code Point (DSCP) marking. Finally, the default class is set for Best Effort traffic. Note that IP Cisco Express Forwarding (CEF) must be enabled on the CER for the service policy to work

In the following section bandwidth is referred to as BW.

Following are examples of how the data queues might be set up:

4.2.1 PPP access

PPP access is supported on T1, E1, T3 and E3 speeds.

PPP access requires a shaping policy map be applied to the Serial Interface. The policy map for the Quality of Service (QoS) is applied to the shaping policy map. The shape rate of the shaping policy map should be set to 95% of the available bandwidth.

Note: Burst interval for CoS1 should always be set to 1 second.

Example for T1/E1/T3/E3 PPP Access:

```
!  
policy-map MARK-BGP  
class BGP  
  set ip dscp cs6  
!  
policy-map COS  
class COS1  
  priority  
  queue-limit 2048 packets  
  police <COS1 BW> <Burst size> conform-action set-dscp-transmit ef exceed-action drop  
class COS2  
  bandwidth remaining percent <COS2 %>  
  set ip dscp af31  
  queue-limit 256 packets  
  service-policy MARK-BGP  
class COS3  
  bandwidth remaining percent <COS3 %>  
  set ip dscp af21  
  queue-limit 256 packets  
class class-default  
  bandwidth remaining percent <COS4 %>  
  set ip dscp default  
  queue-limit 256 packets  
  
policy-map SHAPE_PPP **This policy map applied to serial interface**  
class class-default  
  shape average <Shape Rate> < Shape Rate/250 (rounded up to nearest 128) > 0  
  service-policy COS
```

NOTE: Shape Rate for Full Port Speed = Available Bandwidth * .95 (rounded down to nearest 8K)

Shape Rate for Subrate = Subrate bandwidth

4.2.2 Frame Relay Encapsulation

Frame Relay Encapsulation is supported on E3 and T3 speeds.

Multiple VPN connections over private line access are typically provided using Frame Relay encapsulation on the access link to provide L2 differentiation of the connections.

With Frame Relay encapsulation, a policy-map will be applied to each sub-interface (or one policy-map to each subinterface if there are multiple subinterfaces). The shape rate of the shaping policy map should be set to 95% of the available bandwidth.

Note: Burst interval for CoS1 should always be set to 1 second.

Example for T3/E3 Frame Relay Encapsulation :

```
policy-map MARK-BGP
class BGP
  set ip dscp cs6
!
policy-map COS
class COS1
  priority
  queue-limit 2048 packets
  police <COS1 BW> <Burst Size> conform-action set-dscp-transmit ef exceed-action drop
class COS2
  bandwidth remaining percent <COS2%>
  set ip dscp af31
  queue-limit 256 packets
  service-policy MARK-BGP
class COS3
  bandwidth remaining percent <COS3%>
  set ip dscp af21
  queue-limit 256 packets
class class-default
  bandwidth remaining percent <COS4%>
  set ip dscp default
  queue-limit 256 packets

policy-map SHAPE_FR_ENCAP **This policy map applied to serialsub- interface**
class class-default
  shape average <Shape Rate> <Shape Rate/250 (rounded up to nearest 128)> 0
  service-policy COS
```

NOTE: Shape Rate for Full Port Speed = Available Bandwidth * .95 (rounded down to nearest 8K)
Shape Rate for Subrate = Subrate bandwidth

4.2.3 Ethernet Access

Ethernet access requires a shaping policy map be applied to the Ethernet interface. The policy map for the CoS is applied to the shaping policy map. The shape rate of the shaping policy map should be set to 99% of the available speed (rounded down to the nearest 64K).

For Ethernet access with VLANs, a separate policy-map should be applied to each subinterface.

Note: Burst interval for COS1 should always be set to 1 second.

Example for Ethernet Access:

```
policy-map MARK-BGP
class BGP
set ip dscp cs6
!
policy-map COS
class COS1
priority
queue-limit 2048 packets
police <COS1 BW> <Burst Size> conform-action set-dscp-transmit ef exceed-action drop
class COS2
bandwidth remaining percent <COS2%> account user-defined 28
set ip dscp af31
queue-limit 256 packets
service-policy MARK-BGP
class COS3
bandwidth remaining percent <COS3%> account user-defined 28
set ip dscp af21
queue-limit 256 packets
class class-default
bandwidth remaining percent <COS4%> account user-defined 28
set ip dscp default
queue-limit 256 packets
policy-map Ethernet-SHAPE
class class-default
shape average < Shape Rate > <Shape Rate / 250 (rounded up to nearest 128) > account user-defined
28
service-policy COS
```

NOTE: Shape Rate = Available BW * .99 (rounded down to the nearest 64K)

4.2.4 MLPPP Access

With NXT1/E1 MLPPP Access, the shaping policy-map "SHAPE_MLPPP" is applied to the multilink interface.

Note: Burst interval for COS1 should always be set to 1 second. Burst of 1 second is equal to the COS1 Bandwidth (BW) / 8.

Example for MLPPP access:

```
ip cef
!
policy-map MARK-BGP
class BGP
  set ip dscp cs6
!
policy-map COS_MLPPP
class COS1
  priority
  queue-limit 2048 packets
  police <COS1 BW > <Burst size> conform-action set-dscp-transmit ef exceed-action drop
class COS2
  bandwidth remaining percent <COS2 %> account user-defined 4
  set ip dscp af31
  queue-limit 64 packets
  service-policy MARK-BGP
class COS3
  bandwidth remaining percent <COS3 %> account user-defined 4
  set ip dscp af21
  queue-limit 64 packets
class class-default
  bandwidth remaining percent <COS4 %> account user-defined 4
  set ip dscp default
  queue-limit 64 packets
!
policy-map SHAPE_MLPPP
class class-default
  shape average <Shape Rate> <Shape Rate/250> 0 account user-defined 4
  service-policy COS_MLPPP
```

NOTE: Shape Rate = Available BW * .98 (rounded down to the nearest 64K)

4.2.5 CoS6 Service Policy Example

Following is an example of how to configure a service policy for a CoS6 configuration by adding on the "COS2V" and "COS5" classes.

Note: Burst interval for CoS1 should always be set to 1 second.

Example for CoS6:

```
policy-map MARK-BGP
class BGP
  set ip dscp cs6
!
policy-map COS
class COS1
  priority
  queue-limit 2048 packets
  police <COS1 BW> <Burst Size> conform-action set-dscp-transmit ef exceed-action drop
class COS2V
  bandwidth remaining percent <COS2V%>
  set ip dscp af41
  queue-limit 256 packets
class COS2
  bandwidth remaining percent <COS2%>
  set ip dscp af31
  queue-limit 256 packets
  service-policy MARK-BGP
class COS3
  bandwidth remaining percent <COS3%>
  set ip dscp af21
  queue-limit 256 packets
class COS5
  bandwidth remaining percent <COS5%>
  set ip dscp af11
  queue-limit 256 packets
class class-default
  bandwidth remaining percent <COS4%>
  set ip dscp default
  queue-limit 256 packets
```

4.3 *Frame Relay traffic shaping*

Frame Relay traffic shaping is not supported on the ISR 4Ks.

4.4 *Interface Configuration*

This section gives examples of how to configure the various interface types.

4.4.1 **PPP access**

4.4.1.1 T1/E1 Speeds

Follow these steps for a T1/E1 PPP configuration with external DSU – NIM-1T.

- Configure the IP address of the interface which should be the CER side of the /30 subnet assigned for the CER/PER link.
- Set encapsulation to “ppp”.
- Apply the CoS policy “SHAPE_PPP”.

Example: T1 or E1 PPP with external DSU - NIM-1T

```
interface Serial10/3/0
 ip address 10.10.20.1 255.255.255.252
 ipv6 address 2001:506:14:6::2/64
 encapsulation ppp
 service-policy output SHAPE_PPP
```

Follow these steps for a T1/E1 PPP configuration with internal CSU/DSU – NIM-1MFT-T1/E1:.

- Configure the card type for T1 or E1
- Configure the controller interface
- Configure the IP address of the interface which should be the CER side of the /30 subnet assigned for the CER/PER link.
- Set encapsulation to “ppp”.
- Apply the CoS policy “SHAPE_PPP”.

Example : T1 PPP with internal CSU/DSU – NIM-1MFT-T1/E1

```
card type t1 0 3
!
controller T1 0/3/0
 framing esf
 linecode b8zs
 cablelength long 0db
 channel-group 0 timeslots 1-24 speed 64
!
interface Serial10/3/0:0
 encapsulation ppp
 ip address 10.10.20.1 255.255.255.252
 ipv6 address 2001:506:14:6::2/64
```


4.4.1.2 T3/E3 Speeds

Follow these steps for a T3/E3 PPP configuration with SM-X-1T3/E3

- Configure the card type for T3 or E3
- Configure the IP address of the interface which should be the CER side of the /30 subnet assigned for the CER/PER link.
- Set encapsulation to “ppp”.
- Configure “scramble” to match transport circuit.
- Apply the CoS policy “SHAPE_PPP”.

Example: T3 PPP with SM-X-1T3/E3

```
card type t3 1 0
!
interface Serial11/0/0
 ip address 195.18.32.9 255.255.255.252
 encapsulation ppp
 ipv6 address 2001:506:15:102::1/64
 scramble
 service-policy output SHAPE_PPP
```

4.4.2 Frame Relay Encapsulation

Follow these steps for a T3/E3 Frame Relay Encapsulation configuration with SM-X-1T3/E3

- Configure the card type for T3 or E3
- On the main interface
 - Set encapsulation to “frame-relay”.
 - Configure “scramble” to match transport circuit.
 - Set the frame-relay lmi-type to ansi
- On the subinterface
 - Configure the IP address on the sub-interface which should be the CER side of the /30 subnet assigned for the CER/PER link.
 - Configure the DLCI number
 - Apply the CoS policy “SHAPE_PPP”.

Example: T3 Frame Encapsulation with SM-X-1T3/E3

```
card type t3 1 0
!
interface Serial11/0/0
 encapsulation frame-relay
 scramble
 frame-relay lmi-type ansi
```

```
!  
interface Serial1/0/0.100 point-to-point  
  ip address 192.168.200.110 255.255.255.252  
  ipv6 address 2001:506:14:6::2/64  
  frame-relay interface-dlci 100 IETF  
  service-policy output SHAPE FR ENCAP
```

4.4.3 Ethernet Access

Follow these steps for Full Port Ethernet:

On the main interface:

- Configure the IP address of the interface which should be the CER side of the /30 subnet assigned for the CER/PER link.
- Configure negotiation for auto.
- Apply the output service policy

Example: Full Port Ethernet

```
interface GigabitEthernet0/0/0  
  negotiation auto  
  ip address 192.168.110.29 255.255.255.252  
  ipv6 address 2001:0506:0014:11a::2/64  
  service-policy output Ethernet-SHAPE
```

Follow these steps for Single Stack VLAN Tag:

On the main interface:

- Configure negotiation for auto.

On the subinterface:

- Configure “encapsulation dot1q” command with the appropriate VLAN tag number.
- Configure the IP address of the interface which should be the CER side of the /30 subnet assigned for the CER/PER link.
- Apply the output service policy

Example: Single Stack VLAN Tag (configured to use SFP):

```
interface GigabitEthernet0/0/0  
  no ip address  
  media-type sfp  
  negotiation auto  
!  
interface GigabitEthernet0/0/0.2202  
  encapsulation dot1Q 2202
```

```
ip address 192.168.110.29 255.255.255.252
ipv6 address 2001:0506:0014:11a::2/64
service-policy output Ether-Shape
```

Follow these steps for Dual Stack VLAN Tag:

On the main interface:

- Configure negotiation for auto.

On the subinterface:

- Configure “encapsulation dot1q <inner VLAN tag #> second-dot1q <outer VLAN tag #>”
- Configure the IP address of the interface which should be the CER side of the /30 subnet assigned for the CER/PER link.
- Apply the output service policy

Example: Dual Stack VLAN Tag

```
interface GigabitEthernet0/0/0
no ip address
negotiation auto
!
interface GigabitEthernet0/0/0.2202
encapsulation dot1Q 2202 second 200
ip address 192.168.110.29 255.255.255.252
ipv6 address 2001:0506:0014:11a::2/64
service-policy output Ether-Shape
```

Inner tag is
2202, outer
tag is 200

4.4.4 MLPPP

Follow these steps for internal CSU/DSU with NIM-1MFT-T1/E1 to NIM-8-1MFT-T1/E1:

1. Configure the card type for T1 or E1.
2. Configure the controller interfaces.
3. Configure the multilink interface. The IP address for the “serial interface” is applied to them multilink interface. The COS service policy is also applied here.
4. Configure the he serial interfaces for “ppp” with additional commands to place the interfaces in a multilink group.

Example – 4 X T1 MLPPP with two NIM-2MFT-T1/E1:

```
card type t1 0 1
card type t1 0 2
```

```
controller T1 0/1/0
  framing esf
  linecode b8zs
  channel-group 0 timeslots 1-24 speed 64
  fdl both

controller T1 0/1/1
  framing esf
  linecode b8zs
  channel-group 0 timeslots 1-24 speed 64
  fdl both

controller T1 0/2/0
  framing esf
  linecode b8zs
  channel-group 0 timeslots 1-24 speed 64
  fdl both

controller T1 0/2/1
  framing esf
  linecode b8zs
  channel-group 0 timeslots 1-24 speed 64
  fdl both
!
interface Multilink1
  ip address 192.168.192.5 255.255.255.252
  ipv6 address 2001:506:14:6::2/64
  ppp multilink
  ppp multilink fragment disable
  ppp multilink group 1
  no peer neighbor-route
  service-policy output COS_MLPPP
!
interface Serial0/1/0:0
  no ip address
  encapsulation ppp
  ppp multilink
  ppp multilink group 1
!
interface Serial0/1/1:0
  no ip address
  encapsulation ppp
  ppp multilink
  ppp multilink group 1
!
interface Serial0/2/0:0
```

```
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 1
!
interface Serial0/2/1:0
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 1
```

Appendix A: Sample Configurations

In these configurations, commands required for proper voice configuration are bolded.

A.1 Sample Ethernet Configuration

```
4321-Geneva#show run
Building configuration...

Current configuration : 11451 bytes
!
! Last configuration change at 14:10:00 EDST Thu Jul 16 2015
! NVRAM config last updated at 14:02:50 EDST Thu Jul 16 2015
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
!
hostname 4321-Geneva
!
boot-start-marker
boot system bootflash:isr4300-universalk9.03.13.02.S.154-3.S2-ext.SPA.bin
boot-end-marker
!
!
!
enable password 7 01100F175804
!
no aaa new-model
clock timezone EST -5 0
clock summer-time EDST recurring
no ip source-route
!
!

no ip domain lookup

!
!
!
subscriber templating
multilink bundle-name authenticated
!
!
!
```

```
license udi pid ISR4321/K9 sn FDO18380LJ0
license accept end user agreement
license boot level uck9
!
username vinny privilege 15 secret 5 $1$vaq0$a65vyjFfeK0bDhqGb5A0d1
username cisco password 7 01100F175804
!
redundancy
mode none
!
!
class-map match-any BGP
match access-group name BGP
class-map match-any COS3
match access-group name COS3-Traffic
class-map match-any COS2
match access-group name COS2-Traffic
match access-group name BGP
class-map match-any COS1
match access-group name RTP
match access-group name SIP
match access-group name SCCP
!
policy-map MARK-BGP
class BGP
set ip dscp cs6
policy-map COS
class COS1
priority
queue-limit 2048 packets
police 50000000 6250000 conform-action set-dscp-transmit ef exceed-action drop
class COS2
bandwidth remaining percent 40
set ip dscp af31
queue-limit 256 packets
service-policy MARK-BGP
class COS3
bandwidth remaining percent 30
set ip dscp af21
queue-limit 256 packets
class class-default
bandwidth remaining percent 30
set ip dscp default
queue-limit 256 packets
policy-map Ethernet-SHAPE
class class-default
shape average 98944000 395776 0 account user-defined 28
service-policy COS
!
!
```

```
!  
!  
!  
!  
interface GigabitEthernet0/0/0  
description WAN interface  
no ip address  
load-interval 30  
negotiation auto  
hold-queue 1024 in  
hold-queue 4096 out  
!  
interface GigabitEthernet0/0/0.2700  
encapsulation dot1Q 2700  
ip address 195.18.34.101 255.255.255.252  
ipv6 address 2001:506:15:270::1/64  
no cdp enable  
service-policy output Ethernet-SHAPE  
ip virtual-reassembly  
!  
interface GigabitEthernet0/0/1  
description LAN interface  
no ip address  
load-interval 30  
negotiation auto  
hold-queue 1024 in  
hold-queue 4096 out  
!  
interface GigabitEthernet0/0/1.88  
encapsulation dot1Q 88  
ip address 10.2.88.1 255.255.255.0  
no cdp enable  
!  
!  
router bgp 65000  
bgp router-id 192.168.0.170  
bgp log-neighbor-changes  
neighbor 2001:506:15:270::2 remote-as 13979  
neighbor 195.18.34.102 remote-as 13979  
!  
address-family ipv4  
network 135.16.206.58 mask 255.255.255.255  
network 172.47.0.0 mask 255.255.192.0  
network 192.168.0.170 mask 255.255.255.255  
no neighbor 2001:506:15:270::2 activate  
neighbor 195.18.34.102 activate  
neighbor 195.18.34.102 allowas-in  
exit-address-family  
!  
!
```



```
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip access-list extended BGP
permit tcp any eq bgp any
permit tcp any any eq bgp
ip access-list extended COS2-Traffic
permit tcp any any eq www
permit tcp any eq www any
ip access-list extended COS3-Traffic
permit tcp any any eq smtp
permit tcp any eq smtp any
ip access-list extended RTP
permit udp any range 16384 32767 any range 16384 32767
ip access-list extended SCCP
permit tcp any range 2000 2003 any
permit tcp any any range 2000 2003
ip access-list extended SIP
permit udp any eq 5060 any
permit udp any any eq 5060
permit tcp any eq 5060 any
permit tcp any any eq 5060
!
!
!
control-plane
!
!
line con 0
exec-timeout 300 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
exec-timeout 600 0
login local
!
end
```

A.2 Sample MLPPP Configuration

```
4321-Zurich#sh run
Building configuration...

Current configuration : 11714 bytes
!
```

AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free on AT&T VPN
Cisco 4000 Series ISR Customer Configuration Guide (December 8, 2015, Version 1.0)

```
! Last configuration change at 11:29:15 EDST Tue Aug 4 2015
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no platform punt-keepalive disable-kernel-core
platform hardware throughput level 50000
!
hostname 4321-Zurich
!
boot-start-marker
boot system bootflash:isr4300-universalk9.03.13.02.S.154-3.S2-ext.SPA.bin
boot-end-marker
!
!
card type t1 0 1
enable password 7 045802150C2E
!
no aaa new-model
clock timezone EST -5 0
clock summer-time EDST recurring
no ip source-route
!
no ip domain lookup
!
!
subscriber templating
multilink bundle-name authenticated
!
!
license udi pid ISR4321/K9 sn FDO18380LLU
license boot level uck9
!
username vinny privilege 15 secret 5 $1$vaq0$a65vyjFfeK0bDhqGb5A0d1
username cisco password 7 01100F175804
!
redundancy
mode none
!
controller T1 0/1/0
framing esf
linecode b8zs
cablelength long 0db
channel-group 0 timeslots 1-24
!
controller T1 0/1/1
framing esf
linecode b8zs
cablelength long 0db
```

```
channel-group 0 timeslots 1-24
!  
controller T1 0/1/2  
framing esf  
linecode b8zs  
cablelength long 0db  
channel-group 0 timeslots 1-24  
!  
controller T1 0/1/3  
framing esf  
linecode b8zs  
cablelength long 0db  
channel-group 0 timeslots 1-24  
!  
!  
!  
class-map match-any BGP  
match access-group name BGP  
class-map match-any COS3  
match access-group name COS3-Traffic  
class-map match-any COS2  
match access-group name COS2-Traffic  
match access-group name BGP  
class-map match-any COS1  
match access-group name RTP  
match access-group name SIP  
match access-group name SCCP  
!  
policy-map MARK-BGP  
class BGP  
set ip dscp cs6  
policy-map COS_MLPPP  
class COS1  
priority  
queue-limit 2048 packets  
police 3968000 496000 conform-action set-dscp-transmit ef exceed-action drop  
class COS2  
bandwidth remaining percent 40 account user-defined 4  
set ip dscp af31  
queue-limit 64 packets  
service-policy MARK-BGP  
class COS3  
bandwidth remaining percent 30 account user-defined 4  
set ip dscp af21  
queue-limit 64 packets  
class class-default  
bandwidth remaining percent 30 account user-defined 4  
set ip dscp default  
queue-limit 64 packets  
policy-map SHAPE_MLPPP
```

```
class class-default
  shape average 7744000 30976 0 account user-defined 4
  service-policy COS_MLPPP
!
!
!
!
!
interface Multilink101
  ip address 195.18.32.89 255.255.255.252
  load-interval 30
  ipv6 address 2001:506:15:121::1/64
  ppp chap hostname 195.18.32.90
  ppp multilink
  ppp multilink group 101
  ppp multilink fragment disable
  service-policy output SHAPE_MLPPP
!
interface GigabitEthernet0/0/1
  description LAN interface
  no ip address
  load-interval 30
  negotiation auto
!
interface GigabitEthernet0/0/1.271
  encapsulation dot1Q 271
  ip address 172.47.64.1 255.255.192.0
  ipv6 address 2001:506:16:171::1/64
  no cdp enable
!
!
interface Serial0/1/0:0
  no ip address
  encapsulation ppp
  load-interval 30
  ppp chap hostname 195.18.32.90
  ppp multilink
  ppp multilink group 101
!
interface Serial0/1/1:0
  no ip address
  encapsulation ppp
  load-interval 30
  ppp chap hostname 195.18.32.90
  ppp multilink
  ppp multilink group 101
!
interface Serial0/1/2:0
  no ip address
  encapsulation ppp
```

```
load-interval 30
ppp chap hostname 195.18.32.90
ppp multilink
ppp multilink group 101
!
interface Serial0/1/3:0
no ip address
encapsulation ppp
load-interval 30
ppp chap hostname 195.18.32.90
ppp multilink
ppp multilink group 101
!
!
router bgp 65000
bgp router-id 192.168.0.171
bgp log-neighbor-changes
neighbor 2001:506:15:271::2 remote-as 13979
neighbor 195.18.32.90 remote-as 13979
!
address-family ipv4
network 172.47.64.0 mask 255.255.192.0
network 178.10.10.5 mask 255.255.255.255
network 192.168.0.171 mask 255.255.255.255
no neighbor 2001:506:15:271::2 activate
neighbor 195.18.32.90 activate
exit-address-family
!
!
!
!
ip access-list extended BGP
permit tcp any eq bgp any
permit tcp any any eq bgp
ip access-list extended COS2-Traffic
permit tcp any any eq www
permit tcp any eq www any
ip access-list extended COS3-Traffic
permit tcp any any eq smtp
permit tcp any eq smtp any
ip access-list extended RTP
permit udp any range 16384 32767 any range 16384 32767
ip access-list extended SCCP
permit tcp any range 2000 2003 any
permit tcp any any range 2000 2003
ip access-list extended SIP
permit udp any eq 5060 any
permit udp any any eq 5060
permit tcp any eq 5060 any
permit tcp any any eq 5060
```

```
!  
!  
snmp-server community liartff RO  
!  
!  
control-plane  
!  
!  
!  
line con 0  
  exec-timeout 300 0  
  length 0  
  stopbits 1  
line aux 0  
  stopbits 1  
line vty 0 4  
  exec-timeout 600 0  
  login local  
!  
end
```

A.3 Sample T3 PPP Configuration

```
Building configuration...  
  
Current configuration : 20882 bytes  
!  
! Last configuration change at 16:17:16 EDST Mon Aug 17 2015  
! NVRAM config last updated at 09:26:48 EDST Mon Aug 3 2015 by vinny  
!  
version 15.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
no platform punt-keepalive disable-kernel-core  
platform hardware throughput level 1000000  
!  
hostname 4451-St-Anton  
!  
boot-start-marker  
boot system bootflash:isr4400-universalk9.03.13.02.S.154-3.S2-ext.SPA.bin  
boot-end-marker  
!  
!  
!  
card type t3 1 0  
enable password 7 094F471A1A0A  
!  
no aaa new-model  
clock timezone EST -5 0
```

```
clock summer-time EDST recurring
no ip source-route
!
no ip domain lookup
!
no ipv6 source-route
ipv6 unicast-routing
!
!
subscriber templating
!
multilink bundle-name authenticated
!
!
license udi pid ISR4451-X/K9 sn FOC172771H1
license boot level appxk9
license boot level uck9
license boot level securityk9
spanning-tree extend system-id
!
username vinny privilege 15 secret 5 $1$vaq0$a65vyjFfeK0bDhqGb5A0d1
username cisco password 7 01100F175804
!
redundancy
mode none
!
!
class-map match-any BGP
  match access-group name BGP_IPV6
class-map match-any COS3
  match access-group name COS3-Traffic_IPV6
class-map match-any COS2
  match access-group name COS2-Traffic_IPV6
  match access-group name BGP_IPV6
class-map match-any COS1
  match access-group name RTP_IPV6
  match access-group name SIP_IPV6
  match access-group name SCCP_IPV6
!
policy-map MARK-BGP
  class BGP
    set ip dscp cs6
policy-map COS
  class COS1
    priority
    queue-limit 2048 packets
    police 26528000 3316000 conform-action set-dscp-transmit ef exceed-action drop
  class COS2
    bandwidth remaining percent 60
    set ip dscp af31
```

```
queue-limit 256 packets
service-policy MARK-BGP
class COS3
bandwidth remaining percent 30
set ip dscp af21
queue-limit 256 packets
class class-default
bandwidth remaining percent 10
set ip dscp default
queue-limit 256 packets
policy-map SHAPE_PPP
class class-default
shape average 41992000 168064 0
service-policy COS
!
!
!
!
!
interface GigabitEthernet0/0/1
description Lan Interface
no ip address
load-interval 30
negotiation auto
hold-queue 1024 in
hold-queue 1024 out
!
interface GigabitEthernet0/0/1.278
encapsulation dot1Q 278
ip address 172.50.128.1 255.255.128.0
ipv6 address 2001:506:16:178::1/64
no cdp enable
arp timeout 720
!
!
interface Service-Engine0/4/0
!
interface Serial1/0/0
description WAN Link
bandwidth 41992
ip address 195.18.32.9 255.255.255.252
encapsulation ppp
ipv6 address 2001:506:15:102::1/64
dsu bandwidth 44210
scramble
framing c-bit
cablelength 10
service-policy output SHAPE_PPP
!
!
```



```
router bgp 65000
  bgp router-id 192.168.0.178
  bgp log-neighbor-changes
  timers bgp 3 9
  neighbor 2001:506:15:102::2 remote-as 13979
  neighbor 195.18.32.10 remote-as 13979
  !
  address-family ipv4
    network 172.50.128.0 mask 255.255.128.0
    network 192.160.102.2 mask 255.255.255.255
    network 192.168.0.178 mask 255.255.255.255
    network 195.18.32.8 mask 255.255.255.252
    neighbor 195.18.32.10 activate
    neighbor 195.18.32.10 allowas-in
  exit-address-family
  !
  address-family ipv6
    network 2001:506:15:102::/64
    network 2001:506:16:100::178/128
    network 2001:506:16:178::/64
    network 2001:506:16:200::/64
    network 2001:506:16:300::/64
    network 2002::500:100/126
    neighbor 2001:506:15:102::2 activate
    neighbor 2001:506:15:102::2 allowas-in
  exit-address-family
  !
  ip forward-protocol nd
  no ip http server
  no ip http secure-server
  !
  !
  ipv6 access-list BGP_IPV6
  permit tcp any eq bgp any
  permit tcp any any eq bgp
  !
  ipv6 access-list COS2-Traffic_IPV6
  permit tcp any any eq www
  permit tcp any eq www any
  !
  ipv6 access-list COS3-Traffic_IPV6
  permit tcp any any eq smtp
  permit tcp any eq smtp any
  !
  ipv6 access-list RTP_IPV6
  permit udp any range 16384 32767 any range 16384 32767
  !
  ipv6 access-list SCCP_IPV6
  permit tcp any range 2000 2003 any
  permit tcp any any range 2000 2003
```

```
!  
ipv6 access-list SIP_IPV6  
permit udp any eq 5060 any  
permit udp any any eq 5060  
permit tcp any eq 5060 any  
!  
control-plane  
!  
!  
!  
!  
!  
!  
line con 0  
exec-timeout 300 0  
stopbits 1  
line aux 0  
stopbits 1  
line vty 0 4  
exec-timeout 600 0  
login local  
!  
ntp server 135.16.205.66  
!  
end
```

Appendix B: Inbound Alternate Routing

The Inbound Alternate Routing [IAR] feature enhances AT&T IP Flexible Reach service by providing customers the capability to have an alternate way to complete calls for the purpose of adding a backup path.

With the IAR feature, we define a primary site as a site that is an AT&T IP Flexible Reach location with an active dial plan and is defined with the appropriate calling plan. We define a secondary site (alternate route site) where calls will be routed to in the case where the primary site is unavailable. The secondary site would mirror the dial plan of the primary site.

IAR will be triggered based on the following conditions -

1. No response from the primary site, triggering a time-out (SIP error 408)
2. Error conditions that result in call failure
3. Concurrent call limit has been reached (IPBE signals a SIP error 503).
4. Network Busy (also a SIP 503).
5. Busy out of the trunks at TDM/IP PBX signaling a SIP error 503.

Appendix C: Branch Office Extension (BOE)

C.1 Introduction to BOE

The configuration information in this CCG assumes a single primary CER. Any use by customers of alternate routing configurations or remote branch connectivity to other sites within the same or other AT&T VPN requires proper configuration of the signaling and media paths of the primary CER per this CCG so the AT&T IP Flexible Reach Service on AT&T VPN service works properly. The routing configurations in other customer routers needs to be set up to assure that the routing in their primary CER is not affected. Contact your AT&T technical sales team for further advice in these cases.

While AT&T BVoIP service offers multiple calling plans, the Branch Office IP PBX Extensions capability is supported with two calling plans: Local and Long Distance (plan B) and Local and Long Distance Package (plan C).

AT&T IP Flexible Reach Service on AT&T VPN with Branch Office IP PBX Extensions option provides the capability to deliver telephone numbers for all the Branch Office sites supported by customer's single centralized IP PBX. This configuration uses the IP PBX to support IP phones in a "plug-and-play" manner and does not require any additional premises-based hardware. The customer is able to use the

AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free on AT&T VPN
Cisco 4000 Series ISR Customer Configuration Guide (December 8, 2015, Version 1.0)

AT&T VPN network or their existing data network to distribute calls to their branch office sites and normal local calling capability can be assigned. Only Branch Office sites with fixed locations are supported by the option.

AT&T collects the address data on the Branch Office site so the appropriate directory listing, taxing, regulatory fees, E911 and telephone number (TN) assignments can be associated with the Branch Office site. Branch office sites must be within the footprint of AT&T's BVoIP local service area for AT&T BVoIP with Calling Plans B or C. The customer must provide correct information to AT&T regarding the address and telephone numbers of its Branch Offices and customer's IP PBX must transmit the necessary address information to permit AT&T to route Branch Office E911 calls to the proper PSAP.

Customers choose the calling capacity they require in units of **Concurrent Calls** which are similar to simultaneous calls and can be engineered using standard voice traffic tools (including Class of Service considerations or by using the customer's existing voice channel capacity).

The components required for the service include:

- An existing AT&T VoIP router at the hub site connected via AT&T VPN as the underlying transport service
- An IP PBX at the hub site.
- A branch office site that may be connected via either 1) AT&T VPN as the underlying transport service or 2) private customer data network.

Outbound voice and fax calling is supported between:

- US VoIP-enabled locations (On-net)
- PSTN connected locations (Off-net)

Inbound service from the PSTN is supported with Calling Plans B or C.

Note that the management and maintenance of the Branch Office site and router is the responsibility of the customer. AT&T support for data transmission for AT&T Flexible Reach ends at the customer's IP PBX.

Branch Office site

The branch office site is defined as a site on the customer data network with IP phones. If the IP phones at the Branch Office site need access to AT&T IP Flexible Reach Service on AT&T VPN, then the Branch Office will be defined as having as having Branch Office IP PBX Extensions service. A Branch Office site with Internet access is not supported unless end-end IP VPN tunneling is used. A branch office site may be connected via either 1) AT&T VPN as the underlying transport service or 2) private customer data network.

Note: The branch office must have an IP route to the hub site in order for signaling and media to be exchanged.

Hub site

The hub site is the client's centralized IP PBX Flexible Reach site. The hub site will have a customer managed CER connected to the AT&T VPN as the underlying transport service. The customer may reach the remote branch office sites via this CER (over the AT&T VPN as the underlying transport

AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free on AT&T VPN
 Cisco 4000 Series ISR Customer Configuration Guide (December 8, 2015, Version 1.0)

service) or they can deploy a second customer managed router that provides their own connectivity to the customer's data network.

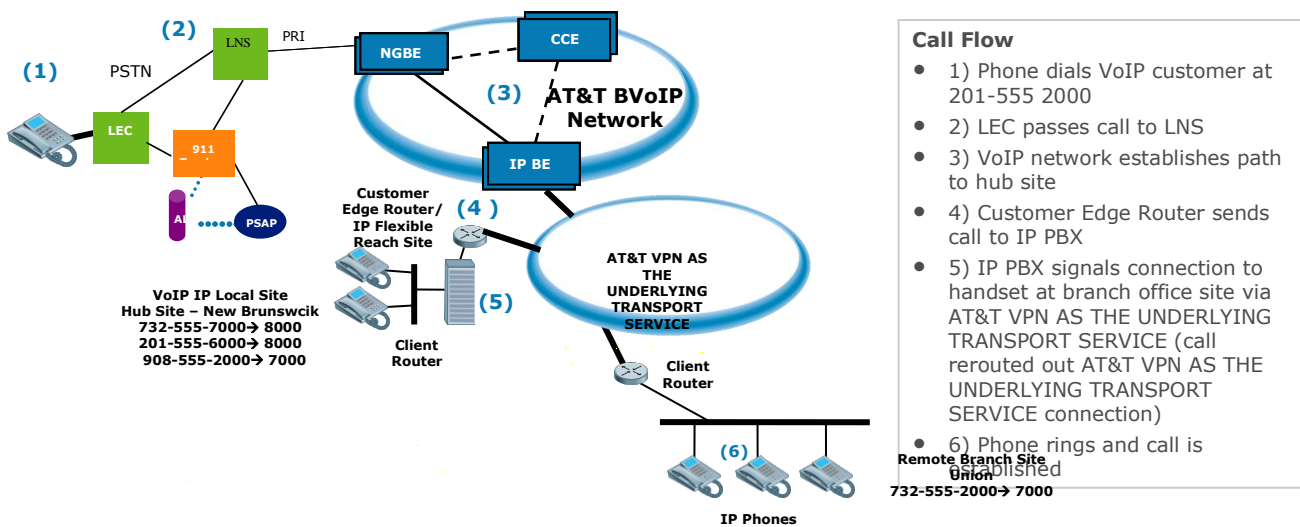
Important Note: The number of concurrent calls at the Hub site must be engineered for all voice traffic originating and terminating at the Hub and Branch Office sites. Concurrent calls are the number of VoIP calls expected to occur at the same time at the Hub site. Be aware if BOE calls are hairpinned through the existing hub site router over the AT&T VPN as the underlying transport service, then the bandwidth required at the hub site for the BOE calls must be doubled (as the RTP for a BOE call traverses the WAN at the hub site twice). Also it is important to take growth at the BOE sites in mind when determining bandwidth requirements.

If the number of concurrent calls needs to be increased, a separate order must be placed and completed prior to initiating the Branch Office order.

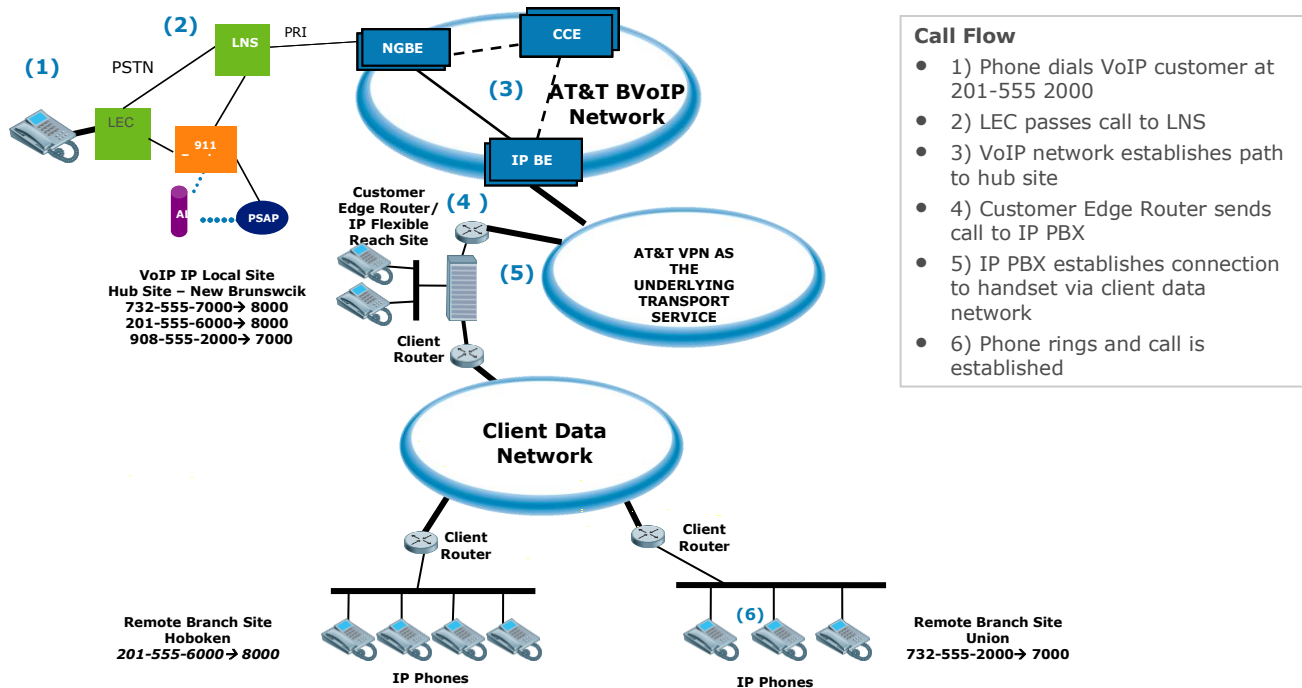
See section 2.1.2 for Bandwidth Per Call Requirements.

Note: The hub office must have an IP route to the branch office site in order for signaling and media to be exchanged.

AT&T BVoIP Branch Office Extension (BOE) using AT&T VPN AS THE UNDERLYING TRANSPORT SERVICE network to connect to BOE site:



AT&T BVoIP Branch Office Extension (BOE) using Client Data Network to connect to BOE site:



- Call Flow**
- 1) Phone dials VoIP customer at 201-555-2000
 - 2) LEC passes call to LNS
 - 3) VoIP network establishes path to hub site
 - 4) Customer Edge Router sends call to IP PBX
 - 5) IP PBX establishes connection to handset via client data network
 - 6) Phone rings and call is established

C.2 Implementation Checklist

- 1) If porting in telephone numbers from another carrier, please ensure that site(s) will be ready on the date of the scheduled service activation:
 - a. Failure to ensure that the site is ready on the activation date will result in an out-of-service condition for the ported telephone numbers.
 - b. If a delay in activation is required for any reason, contact AT&T at least five business days prior to the service activation.
- 2) The Customer Administrator should verify that the Branch Office site can communicate to the hub site by placing test telephone and fax calls.
 - a. Ensure that the Branch Office is able to make a call to the hub site. (Note: If this does not work, the customer needs to contact their local or third-party data and voice network administrator)
 - b. Ensure that the hub site is able to make a call to the Branch Office. (Note: If this does not work, the customer needs to contact their local or third-party data and voice network administrator.)
 - c. Ensure that the hub site is able to make a Long Distance call.

- 3) Make sure the proper bandwidth is in place for the amount of concurrent calls required.
- 4) The customer is responsible for testing all the Branch Office locations after the service activation is done. Customer Administrator is responsible for performing self testing that will include placing test telephone and fax calls to on-net VoIP sites and to off-net numbers.

Special Note for site with Avaya Communications Manager if IP phones are PATed at the CER: The private IP address space of the additional BOE IP phones must be added to the access list referenced to in the PAT statement to ensure the phones are translated to a public IP address.

C.3 Emergency Services

AT&T Flexible Reach service plans B and C, including Branch Office IP PBX Extensions, are limited to locations where AT&T can provide 911/E911 service. The 911 service provided is based on the site registered location information provided to AT&T by the customer. The customer must provide AT&T with the correct business name and address information for each AT&T IP Flexible Reach Service on AT&T VPN location including all Branch Offices. The customer must also ensure that AT&T BVoIP telephone numbers are assigned to the appropriate service location (identified during service ordering) and not assigned or used from another service location.

The customer premises equipment should be configured to use the telephone number of the phone device making the 911 call as the calling party number. This ensures both, AT&T will route the call to the appropriate public emergency service agency and that the correct address information will be displayed to emergency service agent handling the call. In addition, should the call be terminated inadvertently the agent will have a call back number to re-establish communication with the person seeking emergency services.

Should the customer choose to configure premises equipment to send a single telephone number as the calling party number on all 911 calls originating from a particular site, the customer must ensure the calling party number used is an AT&T BVoIP telephone number assigned to the site and the telephone is manned to handle potential call back from the emergency service agent.

C.4 Troubleshooting

If the customer is not able to make calls, then perform the following steps:

- Ensure that the Branch Office is able to make a call to the hub site.
 - If the above step is not successful, the customer needs to contact their local or third-party data and voice network administrator.
- Ensure that the hub site is able to make a call to the Branch Office.
 - If the above step is not successful, the customer needs to contact their local or third-party data and voice network administrator.
- Ensure that the hub site is able to make a Long Distance call.
 - If the above step is not successful, the customer needs to contact AT&T Professional Services by contacting your sales representative.
- Ensure that the Branch Office is able to make an offnet call.

AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free on AT&T VPN
Cisco 4000 Series ISR Customer Configuration Guide (December 8, 2015, Version 1.0)

- If the above step is not successful, then ping and trace from the Branch Office to the router at the Hub site. Check to see where the trace stops and contact the local Administrator to check ACL on corresponding routers and/or firewalls.
- If the above test calls work, the customer will be able to make off-net calls from the Branch Office. The number of simultaneous calls from Branch Office and hub site are subject to the purchased Concurrent Call limit.

Appendix D: Acronyms

Acronym	Translation
ADSL	Asymmetric Digital Subscriber Line
AIM	Advanced Integration Module A
AS	Autonomous System
ASR	Aggregation Services Router
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
BVoIP	Business Voice over Internet Protocol
CAS	Channel Associated Signaling
CBWFQ	Class Based Weighted Fair Queuing
CCG	Customer Configuration Guide
CCS	Common Channel Signaling
CDR	Committed Data Rate
CEF	Cisco Express Forwarding
CER	Customer Edge Router
CHAP	Challenge Handshake Authentication Protocol
CIR	Committed Information Rate
CLI	Command Line Interface
CM	Communications Manager
COS	Class of Service
CPE	Customer Premise Equipment
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRTP	Compress Real Time Protocol
CSU/DSU	Channel Service Unit / Data Service Unit
CUBE	Cisco Unified Border Element
CUCM	Cisco Unified Communications Manager
DID	Direct Inward Dial
DS	Down Stream
DSCP	Differentiated Service Code Point
DSL	Digital Subscriber Line
DSP	Digital Signal Processors
DTMF	Dual Tone Multi Frequency
E&M	Ear & Mouth

AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free on AT&T VPN
Cisco 4000 Series ISR Customer Configuration Guide (December 8, 2015, Version 1.0)

Acronym	Translation
EF	Expedient Forwarding
ePVC	Enhanced Permanent Virtual Circuit
FR	Frame Relay
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station
GSM FR	Global System for Mobile communications Full Rate
HDV	High Density Voice
HWIC	High-speed WAN Interface Card
IAR	Inbound Alternate Routing
IETF	Internet Engineering Task Force
IMA	Inverse Multiplexing over ATM
IOS	Internetwork Operation System
IP	Internet Protocol
IPBE	Internet Protocol Border Element
IPSEC	Internet Protocol Security
ISR	Integrated Services Router
ITU-T	International Telecommunication Union - Telecommunications
GW	Gateway
LAN	Local Area Network
LFI	Link Fragmentation and Interleaving
LLQ	Low Latency Queuing
LD	Long Distance
MLPPP	Multi-Link Point-to-Point Protocol
MM	Multi Media
MOW	Most Of World
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NET	Network Equipment Technologies
NM	Network Module
NPE	Network Processing Engine
OAM	Operation Administration & Maintenance
OCS	Office Communication Server
PA	Port Adapter
PAT	Port Address Translation
PBX	Private Branch Exchange
PC	Personal Computer
PCR	Peak Cell Rate
PER	Provider Edge Router
POS	Packet over SONET
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PQ	Priority Queue

AT&T IP Flexible Reach Service and/or AT&T IP Toll-Free on AT&T VPN
Cisco 4000 Series ISR Customer Configuration Guide (December 8, 2015, Version 1.0)

Acronym	Translation
PRI	Primary Rate Interface
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
PVDM	Packet Voice DSP Module
QOS	Quality of Service
QSIG	Q Signaling
RC	Receive
RFC	Request for Comment
RT	Real Time
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SBC	Session Border Controller
SCCP	Skinny Call Control Protocol
SCR	Sustainable Cell Rate
SHDSL	Single-Pair High-Speed Digital Subscriber Line
SIP	Session Initiation Protocol
SM	Session Manager
SPE	Synchronous Payload Envelope
TAC	Technical Assistance Center
TC	Time Interval
TDM	Time Division Multiplexing
TN	Telephone Number
TX	Transmit
UDP	User Datagram Protocol
US	Up Stream or United States
VAD	Voice Activity Detection
VCI	Virtual Circuit Identifier
VLAN	Virtual Local Area Network
VNI	Voice Network Infrastructure
VoIP	Voice over Internet Protocol
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VT	Virtual Template
WAN	Wide Area Network
WFQ	Weighted Fair Queuing
WIC	WAN Interface Card

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

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