Deployment Guide

Next Generation Enterprise WAN Regional WAN Deployment Guide

October, 2011

NOTICE: ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R).

Contents

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Screen examples use these conventions:

screen font	Terminal sessions and information in the displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
italic screen font	Nonprinting characters, such as passwords, are in angle brackets.
< >	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

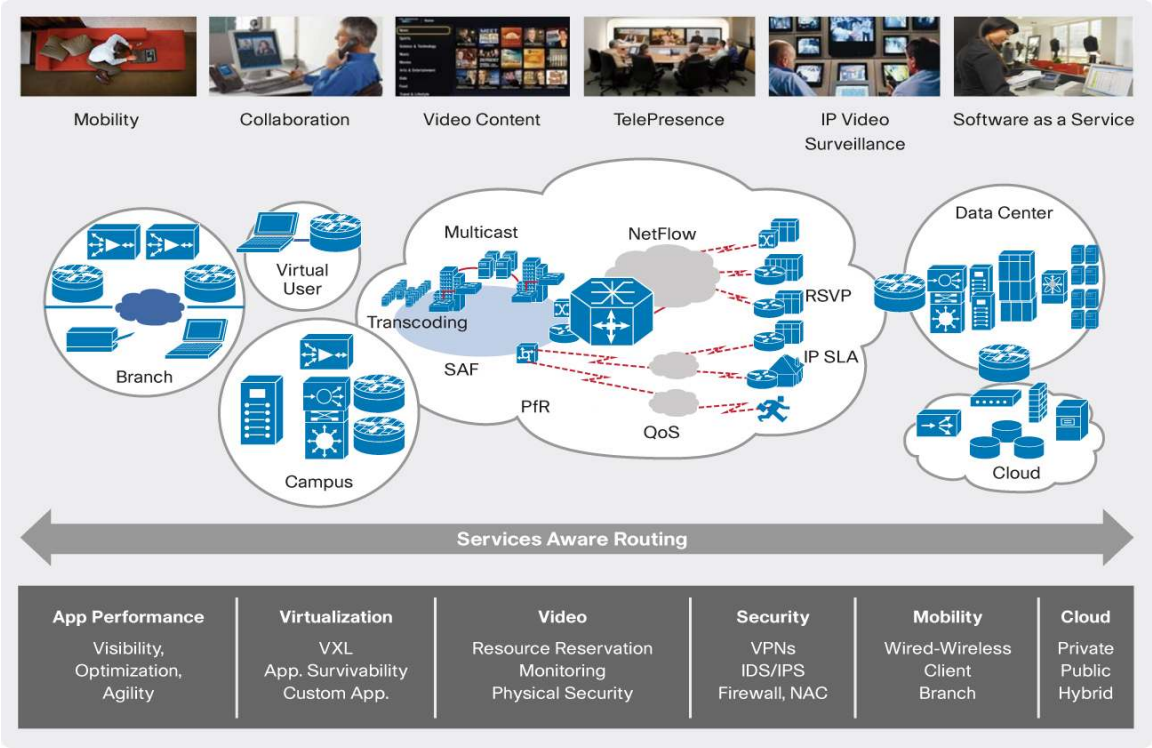
Note: Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Cautions indicate that in this situation, you might do something that could result in equipment damage or loss of data.

Warning: Warnings indicate a potential situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.

NGEW Architecture Overview

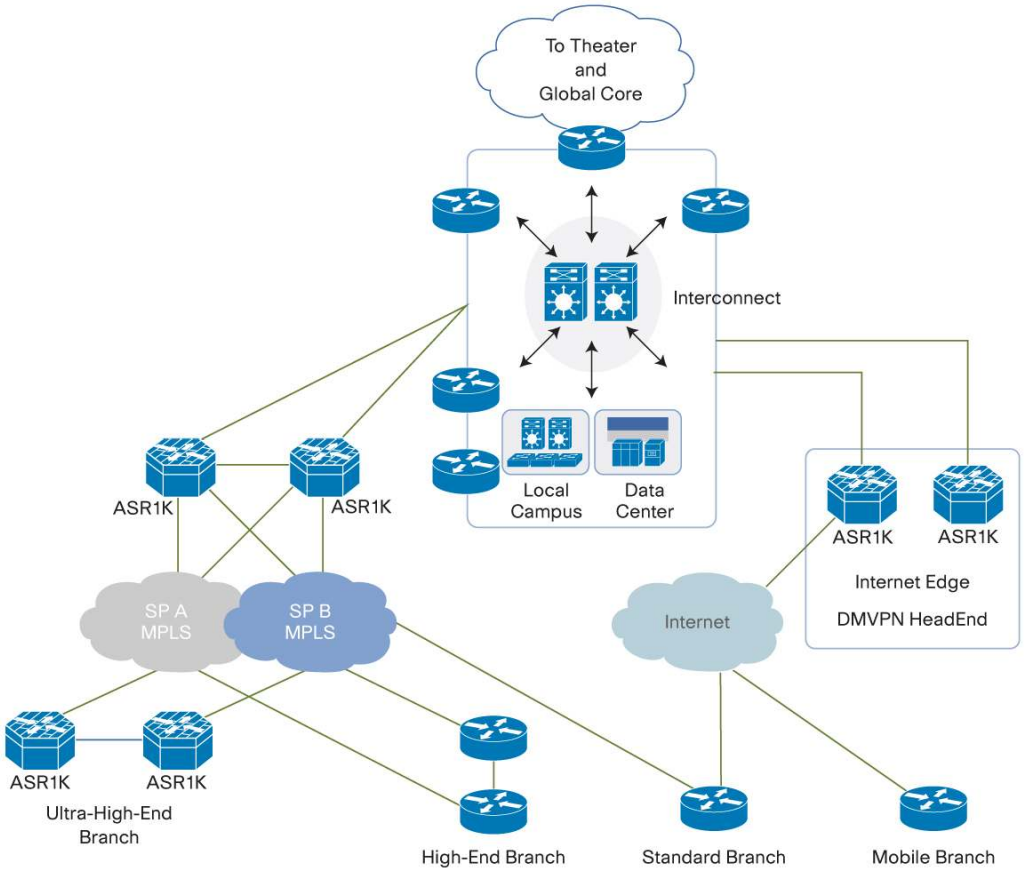
Figure 1. Enterprise Network Architecture



Enterprise networks must adapt to meet new and evolving business requirements. The introduction of cloud services (private, public, or hybrid) brings new challenges to current enterprise network designs. With a more distributed workforce, the proliferation of bandwidth-intensive video-enabled endpoints, and the consolidation of servers into a few centralized locations, require networks to carry more traffic, with increased efficiencies, while offering the same or a high level of performance and availability.

The Cisco® Next Generation Enterprise WAN (NGEW) is an end-to-end architecture that provides foundation building blocks for next-generation enterprise networks. The hierarchical design provides the scalability required by large enterprises, which can be extended and replicated throughout multiple regions and theaters. This consistency leads to ease of deployment, maintenance, and troubleshooting.

Figure 2. NGEW Regional WAN Topology



A logical starting point is the regional WAN (RWAN), where all branch-office locations connect through various access technologies, such as wireless (third- and fourth-generation [3G and 4G, respectively]), DSL, and Multiprotocol Label Switching (MPLS), to the highly scalable aggregation routers at the enterprise interconnect. The enterprise interconnect is the location where traffic from the RWAN is aggregated to the in-theater and global WAN cores. In addition, the enterprise interconnect links all the other components of NGEW, including local data centers and campus, as well as the enterprise edge, which is the demarcation point between enterprise networks and any external network service (for example, Internet, cloud, and voice).

Within the NGEW regional WAN module, NGEW defines four branch-office designs:

- Mobile branch office: Single tier, single WAN link, mobile with minimal redundancy
- Standard branch office: Single tier, dual WAN links providing redundancy for link failures
- High-end branch office: Dual tier, dual WAN links providing maximum redundancy for both device and link failures
- Ultra-high-end branch office: Based on the high-end branch office with increased capacity and higher availability

In addition to providing advanced routing functions, one of the primary design goals of NGEW is to build a network foundation that can reliably support new applications and services, including those in the Cisco Borderless Network - application velocity, medianet, IPv6, and mobility. Customers will benefit from investing in a Cisco network design that has gone through rigorous testing, and scales to support new applications and services to address their continuously evolving business requirements.

RWAN Deployment

Overview

The chosen architecture has all types of RWAN branch offices connecting into the same aggregation at the headend. RWAN aggregation has two types; large-scale or high-end aggregation terminates 5000 branch offices, whereas standard aggregation terminates 1500 branch offices. Tables 1 and 2 show the branch-office mix for both types of aggregation.

Table 1. Standard Aggregation

Branch-Office Type	Branch-Office Mix (%)	Standard-Scale Aggregation (1500 Branch Offices)
Standard	80	1200
Mobile	20	300

Table 2. High-End or Large-Scale Aggregation

Branch-Office Type	Branch-Office Mix (%)	Large-Scale Aggregation (5000 Branch Offices)
High end and ultra high end	5	250
Standard	80	4000
Mobile	15	750

The different types of branch offices can have different types of WAN connectivity to the headend. Branch offices can have 3G or 4G connectivity, service provider MPLS connectivity, or Internet connectivity to reach the headend. In this design mobile branch offices use the Internet as the connectivity for the headend. The standard branch offices have two WAN connections, the primary one being the MPLS Layer 3 VPN (L3VPN) and the Internet as the backup. The high-end branch offices have two MPLS service provider connections for high-bandwidth, highly available connectivity to the headend.

Security is one of the critical features of this design. To secure the branch-office connectivity to the headend over two different types of clouds, two different encryption technologies are used. Group Encrypted Transport VPN (GETVPN) blends well with the L3VPN, whereas Dynamic Multipoint VPN (DMVPN) is the more suitable application over the Internet. GETVPN and DMVPN deployments are described in the following sections.

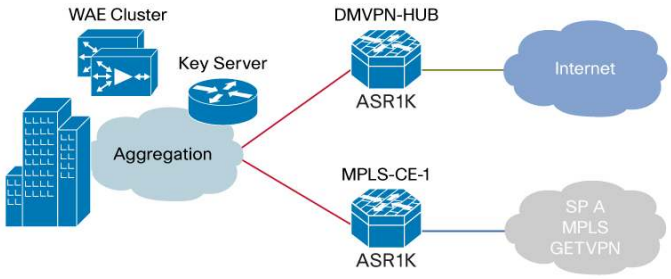
Redundancy and high availability are the main components of this architecture. And with heavy emphasis on voice and video in the branch offices as well as headend, features such as Performance Routing (PfR), quality of service (QoS), and Cisco Wide Area Application Services (WAAS) are deployed to achieve the best user experience.

Standard Aggregation

The standard aggregation design for the RWAN has the primary link to the service provider MPLS cloud for connectivity to the branch offices (Figure 3). The backup link for standard branch offices is through the Internet. The WAN links mentioned are both Ethernet. Ethernet is becoming a dominant carrier handoff in many markets, and it is relevant to include Ethernet as the primary media in the tested architectures. Most of the discussion in this

guide can also be applied to non-Ethernet media (such as T1/E1, DS-3, OC-3, and so on), but they are not explicitly discussed in this design.

Figure 3. RWAN - Standard Aggregation



Deploying Group encrypted Transport VPN for Standard Aggregation

The MPLS cloud interconnects the headend to the branch-office sites. The customer edge (CE) routers on each site act as group members (GMs). The headend customer edge router is also acting as a group member. All these routers are grouped into a Group Domain of Interpretation (GDOI) group. Therefore the keyserver (KS) and group members are part of the same VPN.

In this design the headend customer edge routers that are acting as headend group members are Cisco ASR 1000 Aggregation Services Routers. For standard aggregation the ASR configuration shown in Table 3 is used.

Table 3. Cisco ASR Router Configuration

Component	Type	Redundancy	Performance
Chassis model	Cisco ASR 1002	No	Based on Cisco ASR 1000 Series Route Processor (RP) and Cisco ASR 1000 Series Embedded Services Processor (ESP)
Cisco ASR 1000 Series ESP	Cisco ASR 1000 Series ESP10	No	Upto 4 Gbps encrypted
Cisco ASR 1000 Series Route Processor (RP)	Cisco ASR 1000 Series RP1	No	

The design has Cisco Integrated Services Routers Generation 2 (ISR -G2) routers acting as a keyserverKS. The keyserver is configured with group policies that are pushed to all group members.

Keyserver Configuration

Step 1. Configure IKE phase 1.

Internet Key Exchange (IKE) phase 1 configuration comprises two important parts. Configuring the Internet Security Association and Key Management Protocol (ISAKMP) policy and authentication method. The configuration of IKE phase 1 follows:

```
crypto isakmp policy 10
 encr 3des
 hash md5
 group 2
authentication rsa-sig
```

Step 2. Configure public key infrastructure (PKI) and download certificates.

PKI is the more secure and scalable method of authentication. The following steps must be repeated on all devices in the network.

Note: rsa-sig is the default authentication method for an ISAKMP policy.

Unique Rivest, Shamir, and Adelman (RSA) keys must be generated on all keyservers and group members as follows:

```
crypto key generate rsa general keys label PKI_KS modulus 4096
```

All keyservers and group members must be configured with a trustpoint:

```
crypto pki trustpoint HE-PKI
 ! The URL is the address of the PKI server
 enrollment url http://10.4.226.202:80
 revocation-check none
 ! PKI_KS is the label of the generated keys
 rsakeypair PKI_KS
```

Use the following commands to authenticate to the Certificate Authority (CA) server and download the signed certificate. HE-PKI is the trustpoint.

```
crypto pki authen HE-PKI
crypto pki enroll HE-PKI
```

Step 3. Configure IP Security (IPsec) parameters:

```
crypto ipsec transform-set 3DES esp-aes 256 esp-md5-hmac
!
crypto ipsec profile GN
 set security-association lifetime seconds 3600
 set transform-set 3DES
!
```

Step 4. Install the RSA key used for the rekey:

```
! REKEYRSA" is the name of the key.
crypto key generate rsa modulus 1024 label REKEYRSA
```

Step 5. Configure the GDOI group:

```
crypto gdoi group GN2
 identity number 1102
 server local
  rekey algorithm aes 128
  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa REKEYRSA
  rekey transport unicast
  registration interface Loopback0
```

```
    sa ipsec 1
     profile GN
     match address ipv4 ACL_GN2
     no replay
    ! Source Address of the rekey packet
    address ipv4 10.4.11.210
```

Step 6. Configure an access control list (ACL).

Encryption of the traffic between group members is done based on the access list configured in the GDOI group. Everything that is allowed in the ACL is encrypted. Anything being denied is unencrypted. GDOI and other control traffic such as Network Time Protocol (NTP), Telnet, Simple Network Management Protocol (SNMP), and syslog are denied in the access list, so they are transported without encryption. GDOI uses User Datagram Protocol (UDP) port 848 to communicate with keyserver and group members. In certain cases group members need to go through other group members to reach the keyserver. Therefore, UDP 848 port messages are unencrypted. Control messages for routing or multicast protocols should also be allowed to pass through group members without encryption. Any control packets that need to be traversed between the keyserver and group members before the Transport Encryption Keys (TEKs) are exchanged need to be excluded in the ACL.

```
ip access-list extended ACL_GN2
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   udp any eq 848 any
 deny   udp any any eq 848
 deny   eigrp any any
 deny   udp any any eq ntp
 deny   udp any eq ntp any
 deny   udp any any eq snmp
 deny   udp any eq snmp any
 deny   udp any any eq syslog
 deny   udp any eq syslog any
 deny   tcp any host 10.4.226.202 eq www
 deny   tcp host 10.4.226.202 eq www any
 deny   pim any host 224.0.0.13
 deny   igmp any any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   udp any eq tftp any
 deny   udp any any eq tftp
 permit ip any any

!The configuration is based on the best practices from
GET VPN deployment guide
GET VPN design and Implementation guide
```

Group Member Configuration on the Cisco ASR 1000 (aggregation customer edge)

In addition to ISAKMP and authentication, the group member needs the following configuration to enable GDOI and download the policy:

Step 1. Configure IKE phase 1.

IKE phase 1 configuration comprises two important parts: configuring the ISAKMP policy and the authentication method. The configuration of IKE phase 1 follows:

```
crypto isakmp policy 10
 encr 3des
 hash md5
 group 2
 lifetime 300
authentication rsa-sig
```

Step 2. Configure PKI and download certificates.

PKI is the more secure and scalable method of authentication. The following steps must be repeated on all devices in the network.

Note: rsa-sig is the default authentication method for an ISAKMP policy.

Unique RSA keys must be generated on the keyserver and group members as follows:

```
crypto key generate rsa general keys label PKI_KS modulus 4096
```

All keyservers and group members must be configured with a trustpoint:

```
crypto pki trustpoint HE-PKI
 ! The URL is the address of the PKI server
 enrollment url http://10.4.226.202:80
 revocation-check none
 rsakeypair PKI_KS
```

Authenticate to the CA server and download the signed certificate:

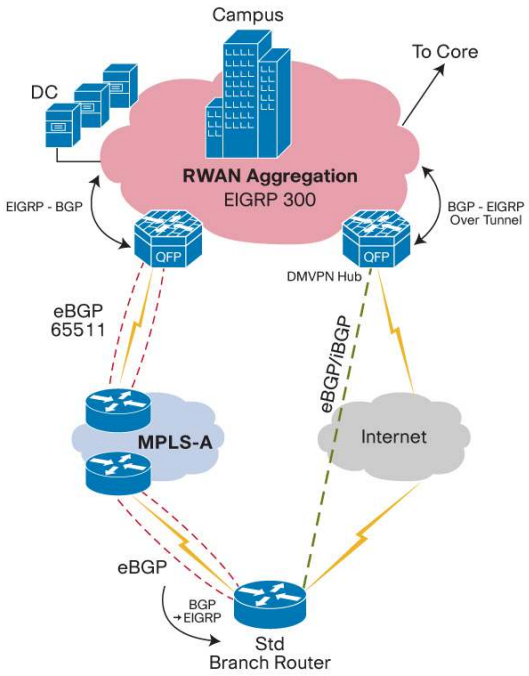
```
crypto pki authen HE-PKI
crypto pki enroll HE-PKI
```

Step 3. Configure the GDOI group to download the policies from the keyserver:

```
crypto gdoi group GN2
 identity number 1102
 ! Key server address
 server address ipv4 10.4.11.210
crypto map GN2 local-address Loopback0
crypto map GN2 10 gdoi
 set group GN2
```

Step 4. Configure routing on the group member (Figure 4).

Figure 4. Routing design for Standard Aggregation



The group member runs external Border Gateway Protocol (eBGP) to connect to the service provider. The internal network of the enterprise runs Enhanced IGRP (EIGRP). Route redistribution is configured between EIGRP and BGP. Here is the routing configuration:

```
router eigrp 300
 distribute-list Block-CE in
 default-metric 100000 100 255 1 1500
 network 10.4.0.0 0.0.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface Port-channel1
 no passive-interface GigabitEthernet0/0/1
 eigrp router-id 10.4.11.204
!
router bgp 65511
 bgp router-id 10.4.11.204
 bgp log-neighbor-changes
 neighbor 10.4.81.1 remote-as 65000
 !
 address-family ipv4
  network 10.4.81.0 mask 255.255.255.252
  redistribute eigrp 300
  neighbor 10.4.81.1 activate
 exit-address-family
```

```
!
```

Deploying DMVPN for Standard Aggregation

Mobile branch offices connect to the headend using Internet connectivity. This link is the primary and the only link to connect to the headend. Standard branch offices use the Internet connection as the backup link to connect to the headend. In both cases this design has DMVPN to secure the links.

The authentication method on the hub is both certificate and preshared. Although certificate is the preferred method, it might not be feasible for some of the mobile client routers to download the certificate. In that case there are two options: either have the certificate loaded on the box before installing it on the mobile site or use the preshared key to authenticate the peer.

The routing protocol used over DMVPN is BGP. The hub router also acts as the route reflectors. All spokes are defined as route-reflector clients. Route redistribution is configured between EIGRP used internally in the RWAN aggregation and BGP or EIGRP with the spokes over the DMVPN tunnel.

DMVPN Hub on Cisco ASR 1000 Configuration

Step 1. Configure IKE phase 1:

```
crypto isakmp policy 20
 encr aes 256
 group 2
crypto isakmp identity hostname
crypto isakmp profile inet-public
   keyring DMVPN
   match identity address 0.0.0.0 Inet-public
!
!
```

Step 2. Configure IKE phase 2:

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-profile
 set transform-set AES256/SHA/TRANSPORT
```

Step 3. Configure the DMVPN tunnel:

```
interface Tunnel10
 bandwidth 100000
 ip address 10.3.0.1 255.255.224.0
 no ip redirects
 ip mtu 1400
 ip wccp 62 redirect in
 no ip next-hop-self eigrp 200
 no ip split-horizon eigrp 200
 ip pim nbma-mode
 ip pim sparse-mode
```

```
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp redirect
 ip tcp adjust-mss 1360
 load-interval 30
 qos pre-classify
 cdp enable
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 101
 tunnel vrf Inet-public
 tunnel protection ipsec profile DMVPN-profile
!
```

Step 4. Configure BGP as the routing protocol:

The routing protocols in this design are either BGP or EIGRP. For deployments with more than 1000 spokes, BGP is recommended. For fewer than 1000 spokes, EIGRP can be used. Following is the BGP configuration on the hub. If the BGP autonomous system (AS) is unique for each of the standard branch-office routers, you must use eBGP instead of iBGP. Here is the configuration:

```
router bgp 1000
 bgp router-id 99.2.1.1
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 timers bgp 120 480
 redistribute connected
 neighbor spoke1 peer-group
 neighbor spoke1 remote-as 1000
 neighbor spoke1 update-source Tunnel1
 neighbor spoke1 route-reflector-client
 neighbor spoke1 next-hop-self
 neighbor spoke2 peer-group
 neighbor spoke2 remote-as 1000
 neighbor spoke2 update-source Tunnel1
 neighbor spoke2 route-reflector-client
 neighbor spoke2 next-hop-self
 neighbor spoke3 peer-group
 neighbor spoke3 remote-as 1000
 neighbor spoke3 update-source Tunnel1
 neighbor switch peer-group
 neighbor switch remote-as 1000
 neighbor switch update-source GigabitEthernet0/0/1
```

```
 neighbor switch route-reflector-client
 neighbor switch next-hop-self
 neighbor 21.1.10.1 peer-group spoke2
 neighbor 21.1.10.2 peer-group spoke2
```

If you use EIGRP as the routing protocol over the tunnels, it is recommended that you have all the spokes defined as EIGRP stub routers. On the headend the configuration follows:

```
router eigrp 10
 network 192.168.0.0 0.0.255.255
 network 200.0.0.0 0.255.255.255
 no auto-summary
interface Tunnel1
 bandwidth 1000000
 ip hello-interval eigrp 10 500
 ip hold-time eigrp 10 5000
 ip summary-address eigrp 10 200.0.0.0 255.0.0.0 5                    !
```

Deploying WAAS for Standard Aggregation

Cisco Wide Area Applications Services (WAAS) is centrally managed and requires one or more Cisco WAAS Central Manager devices that are physically located within the data center and accessible through a web interface.

Multiple Cisco Wide Area Application Engine (WAE) devices at one location can operate as a cluster. The routers performing the Web Cache Control Protocol (WCCP) redirection are responsible for load sharing across the various WAE devices within a cluster. WAAS high availability uses what is referred to as an N + 1 model. This name means that if N equivalent devices are required to support the required performance, then one additional device is required to provide redundancy.

In standard aggregation the Cisco WAE-674 appliance is used as the Cisco WAAS Central Manager deployed in the data center. The Cisco WAE-674 can manage up to 2000 devices. Cisco WAE Clustering with N + 1 redundancy is used for the WAE appliance devices deployed in the RWAN aggregation. The Cisco WAE-7371 appliance is used based on the hardware capacity. The sizing details are provided in Table 4. A more comprehensive, interactive WAAS sizing tool is available at cisco.com: http://tools.cisco.com/WAAS/sizing.

Table 4. Sizing Details for Cisco WAE Devices

Device	Maximum Optimized TCP Connections	Maximum Recommended WAN Link (Mbps)	Maximum Optimized Throughput (Mbps)	Maximum Peers Devices
Cisco WAE-7341	12000	300	1000	1400
Cisco WAE-7371	50000	1000	2500	2800

The number of WAE appliances is determined based on the total number of users online during an hour window and the number of TCP connections per user. A minimum of two Cisco WAE-7371 appliances are required for the standard aggregation. Both devices are connected to the RWAN distribution switch.

Deploying Cisco WAAS Central Manager

In standard aggregation, Cisco WAAS Central Manager is deployed in the data center:

```
!Session into the WAE console with the default user/password is admin/default and
```

```
run the setup.

!Select the device mode as Central manager

Step 2: Configure as central manager.
1. Application Accelerator
2. Central Manager
Select device mode [1]: 2

!Configure Default Gateway, NTP and DNS server Ip address

!Enable the Enterprise license after completing the setup save the configuration
and reload the appliance.

!After reload enable the SSH. Enabling SSH requires the generation of the RSA key
and enabling of the sshd service:

ssh-key-generate key-length 2048
sshd version 2
sshd enable
```

Deploying Cisco WAE in the Aggregation

Cisco EtherChannel technology is used in the Cisco WAE appliances to connect to the distribution switches. If the WCCP routers are Cisco ASR 1000 Series routers, then change the default setting of hash-source-ip to mask-assign. Make this change on the WAE devices, not on the routers.

This design uses a negotiated return generic routing encapsulation (GRE) tunnel from the WAE to the router. Traffic to be reinjected into the network uses a negotiated return WCCP GRE tunnel egress method back to the originating router. This method is preferred because it allows the WAE appliances to be located one or more routed hops away from the WCCP router. A default mask is used in the WAE in the configuration that follows.

Configuring Cisco WAE Appliance

Step 1. Configure the Cisco WAE-1:

```
!Session into the WAE console with the default user/password is admin/default and
run the setup.

!Select the device mode as Application accelerator

Step 2: Configure as Application accelerator.
1. Application Accelerator
2. Central Manager
Select device mode [1]: 1

!Configure Default Gateway, NTP and DNS server Ip address

!Enable the Enterprise license after completing the setup save the configuration
and reload the appliance.

!Configure the port channel interface required for etherchannel
!
interface PortChannel 1
 ip address 10.4.226.131 255.255.255.224
 exit
!
!Both Gig1/0 & Gig2/0 are members of portchannel 1
!
interface GigabitEthernet 1/0
 channel-group 1
 exit
interface GigabitEthernet 2/0
 channel-group1
 exit

!Configure portchannel as the primary interface

primary-interface PortChannel 1

!Configure the default gateway


ip default-gateway 10.4.226.129


!Configure the wccp router list and mask assign is used in the router list
(10.4.11.204 is ip address of GETVPN CE, 10.4.11.205 & 10.4.11.206 is the ip
```

```
address of DMVPN Hubs)

wccp router-list 1 10.4.11.204 10.4.11.205 10.4.11.206
! default wccp mask is src-ip-mask 0xf00 dst-ip-mask 0x0

wccp tcp-promiscuous router-list-num 1 mask-assign

! Configure GRE negotiated return  WAE devices

egress-method negotiated-return intercept-method wccp
```

Step 2. Configure the WAE-2; repeat the previous steps. The IP address is configured as follows:

```
!Configure the port channel interface required for etherchannel
!
interface PortChannel 1
 ip address 10.4.226.132 255.255.255.224
 exit
!
!Both Gig1/0 & Gig2/0 are members of portchannel 1
!
interface GigabitEthernet 1/0
 channel-group 1
 exit
interface GigabitEthernet 2/0
 channel-group1
 exit

!Confgiure portchannel as the primary interface

primary-interface PortChannel 1

!Configure the default gateway


ip default-gateway 10.4.226.129
```

Step 3. Configure the WAN distribution switch ports connecting to the WAE:

```
! Create a VLAN in the WAN Distribution switch and configure the Etherchannel.
WAE-1 is connected to Gig-E ports 1/0/3 & 1/0/4 and part of Port-channel 5.

interface GigabitEthernet1/0/3
 switchport access vlan 350
 channel-group 5 mode on
end

interface GigabitEthernet1/0/4
 switchport access vlan 350
 channel-group 5 mode on
end

!
interface Port-channel5
 switchport access vlan 350
end


! Gig-E ports 1/0/5 & 1/0/6 are connected to WAE-2 are part of Port-channel6.


interface GigabitEthernet1/0/3
 switchport access vlan 350
 channel-group 6 mode on
end

interface GigabitEthernet1/0/4
 switchport access vlan 350
 channel-group 6 mode on
end


interface Port-channel6
 switchport access vlan 350
end


interface Vlan350
 ip address 10.4.226.129 255.255.255.224
end
```

Step 4. Register the WAE with WAAS Central Manager

```
! Configure the CMS IP

central-manager address 10.4.200.20

!Register the WAE device with Waas Central Manager for centralized management

  cms enable
```

Enabling WAAS on the MPLS-CE (Cisco ASR 1000)

This design uses WCCP 61 inbound on LAN-facing interfaces to match unoptimized data sourced from the data center that is destined for clients at the WAN remote sites. WCCP 62 is used inbound on WAN-facing interfaces, matching optimized data sourced from the WAN remote sites.

Step 1. Confgure WCCP on the MPLS customer edge router:

```
! Create an extended access-list for the traffic which needs to be optimized

ip access-list extended WAAS-REDIRECT-LIST
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any



!Create a standard access-list with WAE-1 & 2 ip address

 ip access-list standard WAE
  permit 10.4.226.132
  permit 10.4.226.131


!Enable wccp 61,62 with redirect list and WAE access-list

 ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAE
 ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAE
```

Step 2. Enable WCCP redirection on the interface:

```
! Enable wccp 62 redirect on the WAN interface
```

```
interface GigabitEthernet0/0/0
 ip address 10.4.81.2 255.255.255.252
 ip wccp 62 redirect in
 ip flow ingress
 ip flow egress
 ip pim sparse-mode
 load-interval 30
 negotiation auto
 cdp enable
 crypto map GN2
 service-policy output WAN

! Enable wccp 61 redirect on the LAN interface

interface Port-channel1
 ip address 10.4.226.2 255.255.255.252
 ip wccp 61 redirect in
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 load-interval 30
 no negotiation auto
```

Enabling WAAS on the DMVPN Hub (Cisco ASR 1000)

This design uses WCCP 61 inbound on LAN-facing interfaces to match unoptimized data sourced from the data center that is destined for clients at the WAN remote sites. WCCP 62 is used inbound on the tunnel interface, matching optimized data sourced from the WAN remote sites.

Step 1. Confgure WCCP on the DMVPN hub router. Do step 1 of “Enabling WAAS on the MPLS-CE”

Step 2. Enable WCCP redirection on the interface:

```
! Enable wccp 62 redirect on the tunnel interface for the DMVPN hub

interface Tunnel10
 bandwidth 100000
 ip address 10.3.0.1 255.255.224.0
 no ip redirects
 ip mtu 1400
 ip wccp 62 redirect in
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
```

```
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp redirect
 ip tcp adjust-mss 1360
 load-interval 30
 qos pre-classify
 cdp enable
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 101
 tunnel vrf Inet-public
 tunnel protection ipsec profile DMVPN-profile

! Enable “wccp 61 redirect in” and “wccp 62 redirect out” on the LAN interface.
WCCP 62 out is required on the LAN interface to support dynamic creation of
spoke-to-spoke tunnels. In such case traffic from the WAN is intercepted with
service 62 out configured on the lan interface

interface Port-channel1
 ip address 10.4.226.18 255.255.255.252
 ip wccp 61 redirect in
 ip wccp 62 redirect out
 no negotiation auto
 end
```

Deploying QoS on Standard Aggregation

In standard aggregation the headend and the standard branch offices have six classes of service The QoS classes listed in Table 5 are used in this design. Further details about end-to-end QoS and remarking from 6 to 4 class are discussed in the NGEW QoS deployment guide.

Table 5. QoS Classes

Layer 3				Layer 2
Service Class	Per-Hop Behavior (PHB)	Differentiated Services Code Point (DSCP)	IP Precedence (IPP)	CoS
Network Control	CS6	48	6	6
Telephony	EF	46	5	5
Signaling	CS3	24	3	3
Multimedia conferencing	AF41, 42, and 43	34, 36, and 38	4	4
Real-time interactive	CS4	32	4	4
Multimedia streaming	AF31, 32, and 34	26, 28, and 30	3	3
Low-latency data	AF21, 22, and 23	18, 20, and 22	2	2
Operations, administration, and maintenance (OAM)	CS2	16	2	2
Bulk data	AF11, 12, and 13	10, 12, and 14	1	1
Scavenger	CS1	8	1	1

Layer 3				Layer 2
Default “best effort”	DF	0	0	0

Deploying QoS for Cisco ASR 1000 (MPLS-CE)

Step 1. Configure class maps:

```
! Configure the class maps, routing protocol used also should be included in the
network control. BGP is not marked with dscp value by default, so NBAR is used to
identify BGP traffic and dscp value is set to cs6.

class-map match-any VOICE
 match ip dscp ef
class-map match-any VIDEO-RT-INTERACTIVE
 match ip dscp cs4 af41
class-map match-any NETWORK-MGMT-OAM
 match ip dscp cs2 cs6
class-map match-any STREAMING-SIGNALLING
 match ip dscp cs3 af31
class-map match-any CRITICAL-DATA
 match ip dscp af21 af22 af23
class-map match-any BULK-SCAVENGER
 match ip dscp cs1 af11
class-map match-any BGP-Routing
 match protocol bgp
!

! Policy map is configured to set the dscp value to cs6.
policy-map MARK-BGP
 class BGP-Routing
  set dscp cs6

! NBAR is enabled on the WAN interface connecting to the MPLS
interface GigabitEthernet0/1
 ip address 10.4.81.2 255.255.255.252
 ip nbar protocol-discovery
 duplex auto
 speed auto
 media-type rj45
```

Step 2. Configure the QoS policy map:

```
! Policy map with queuing and sample bandwidth reservation (bandwidth percentage
can be changed based on the traffic profile). Policy-map used for BGP marking is
added in the class NETWOK-MGMT-OAM.

policy-map WAN-SP-CLASS-OUTPUT
 class VOICE
```

```
    priority percent 18
   class VIDEO-RT-INTERACTIVE
    priority percent 15
   class NETWORK-MGMT-OAM
    bandwidth percent 5
    service-policy MARK-BGP
  class STREAMING-SIGNALLING
    bandwidth percent 17
   class CRITICAL-DATA
    bandwidth percent 15
   class BULK-SCAVENGER
    bandwidth percent 5
    random-detect
   class class-default
    bandwidth percent 25
    random-detect
```

Step 3. Configure shaping and apply the QoS:

```
! Shaping is done to make sure the load does not exceed the bandwidth subscribed
from the provider. For MPLS aggregation 1000Mbps is recommended bandwidth,
shaping is done for the same. The policy with queuing is applied as child policy.

policy-map Int-Gig-Aggr
 class class-default
  shape average 1000000000
  service-policy WAN



interface GigabitEthernet0/1
 ip address 10.4.81.2 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 service-policy output Int-Gig-Aggr
```

Deploying QoS for DMVPN Hub

For DMVPN, traffic shaping is configured in QoS for the backup link of the standard branch offices to the aggregation and primary link of the mobile branch offices. With limitations that exist today, the best approach is to group similar branch offices into one policy and shape on that group. Because both traffic policing and queuing are required, a two-level hierarchy is used: policing on the child level and shaping on the parent level.

Step 1. Configure class maps.

Class maps for the two types of branch offices are configured with different traffic types. In this design six traffic classes are used:

```
ip access-list extended MOBILE
```

```
 permit ip any 50.1.0.0 0.0.255.255

ip access-list extended STANDARD
 permit ip any 50.2.0.0 0.0.255.255

class-map match-any MOBILE
 match access-group name MOBILE

class-map match-any STANDARD
 match access-group name STANDARD

class-map match-any DATA
 match ip dscp af21
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4  af41
 match ip dscp cs4  af41
class-map match-any CRITICAL-DATA
 match dscp cs3  af31
class-map match-any VOICE
 match dscp ef
 match ip dscp ef
class-map match-any NETWORK-CRITICAL
 match ip dscp cs2  cs6
class-map match-any SCAVENGER
 match ip dscp cs1  af11
 match ip dscp cs3  af31
```

Step 2. Policy based on different traffic types:

```
policy-map STAND-BR
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
 class class-default
  bandwidth percent 25
  random-detect
```

```
!


policy-map MOBILE-BR
 class DATA
  bandwidth percent 33
 class CRITICAL-DATA
  bandwidth percent 35
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 2
 class class-default
  bandwidth percent 25
  random-detect
!
```

Step 3. Configure parent policy to shape on the two different types of branch offices:

```
policy-map PARENT
 class MOBILE
  service-policy MOBILE-BR
  shape average 150000000
 class STANDARD
  service-policy STAND-BR
  shape average 200000000
 class class-default
  shape average 1000000
```

Step 4. Apply the policy on the physical interface:

```
interface GigabitEthernet0/0/1
 description OUTGOING Interface
 service-policy output PARENT
```

Deploying Remote Sites for Standard Aggregation

Two types of remote sites are supported with RWAN standard aggregation: standard branch office and mobile branch office (Table 6).

Table 6. Types of remote sites with Standard Aggregation

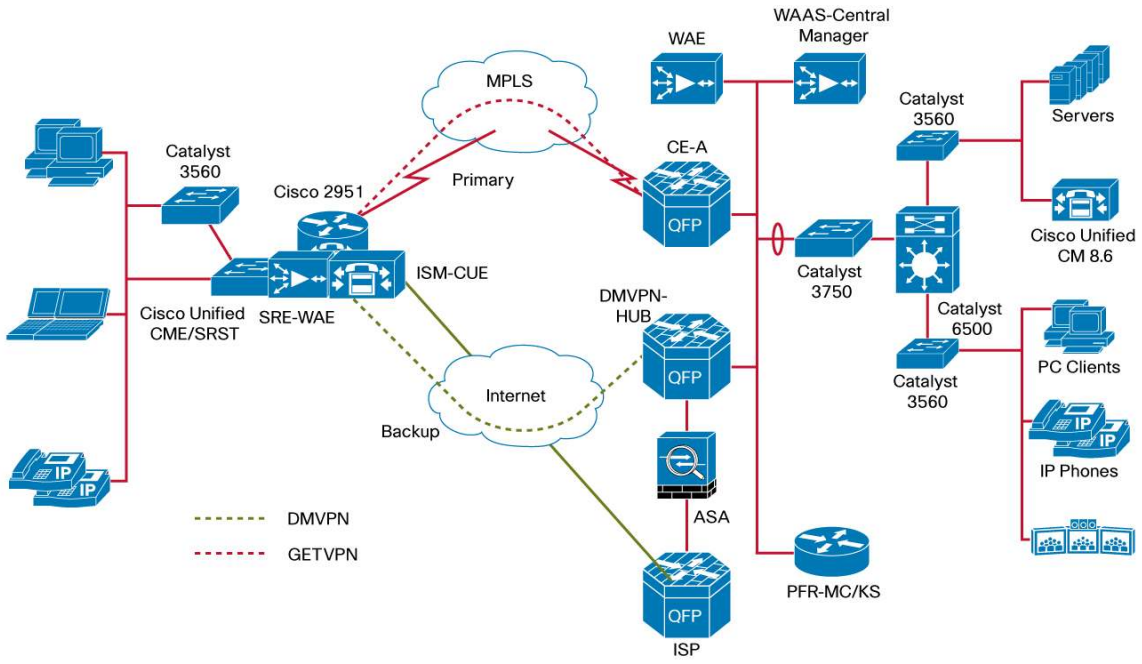
Branch-Office Type	Platform	WAN Link	Wan Optimization	Secure Connectivity
Mobile	Cisco 1941	Single - 3G	WAAS Express	DMVPN
Standard	Cisco 2951	Dual - MPLS and Internet	SRE-WAE	GETVPN Group Encrypted Transport VPN and DMVPN

Mobile Branch Office

The mobile branch office has a Cisco 1941 Integrated Services Router, part of the Cisco ISR G2 router portfolio, with 3G wireless connection to the Internet as the WAN link and DMVPN for secure connectivity to the RWAN

aggregation. Cisco WAAS Express (WAASX) embedded with Cisco IOS® Software is used for WAN optimization, which is suitable for low-bandwidth (<2 Mbps) WAN links (Figure 5).

Figure 5. Mobile Branch Topology



Deploying Branch-Office CDMA

Step 1. Install the Code Division Multiple Access (CDMA) high-speed WAN interface card (HWIC) and register with the service provider using the Electronic Serial Number (ESN) found on the HWIC.

Step 2. Create a chat script for CDMA connection. Chat scripts are strings of text used to send commands for modem dialing:

```
chat-script cdma "" "atdt#777" TIMEOUT 30 "CONNECT”
```

Step 3. Apply the chat script to the line interface of cellular interface 0/1/0:

```
line 0/1/0
 script dialer cdma
```

Step 4. Create the dialer list from the global configuration mode:

```
dialer-list 1 protocol ip permit
```

Step 5. Configure the cellular interface:

```
interface Cellular0/1/0
 encapsulation ppp
 load-interval 30
 dialer in-band
 dialer-group 1
 dialer-pool member 1
```

```
 async mode interactive
 fair-queue 64 16 256
 no ppp lcp fast-start
```

Step 6. Configure the dialer interface:

```
interface Dialer1
 ip vrf forwarding INET-PUBLIC
ip address negotiated
encapsulation ppp
dialer pool 1
dialer idle-timeout 0
dialer string cdma
dialer persistent
dialer-group 1
no ppp lcp fast-start ppp
ipcp address accept
ppp timeout retry 120
ppp timeout ncp 30
```

DMVPN for the Mobile Branch Office

Step 1. Configure Virtual Route Forwarding Lite (VRF-Lite) for DMVPN. The DMVPN design uses VRF for the interface connecting to the Internet:

```
ip vrf Inet-public
 rd 65512:1

! Configure default route with vrf Inet-public to the Internet using dialer
interface
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 Dialer1
```

Step 2. Configure the ISAKMP and IPsec. For the mobile branch office, preshared authentication is used in this design. If the PKI server is present in the demilitarized zone of the RWAN aggregation, you can also use PKI authentication:

```
!crypto keyring defines a pre-shared key to be used with specific vrf.

crypto keyring DMVPN vrf Inet-public
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123

! Configure ISAKMP policy with AES 256 bit encryption and authentication pre-
share

crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2

!ISAKMP profile associated the key ring with address source and vrf. Here wild
card address 0.0.0.0 is used
crypto isakmp profile inet-public

   keyring DMVPN
   match identity address 0.0.0.0 Inet-public

!ISAKMP transform set is defined here. ESP with 256 bit AES algorithm is used for
encryption and ESP with SHA HMAC for authentication

crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport

!IPSEC profile creates the association with transform set and isakmp profile

crypto ipsec profile DMVPN-profile
 set transform-set AES256/SHA/TRANSPORT
 set isakmp profile inet-public
```

Step 3. Configure the mGRE tunnel:

```
! Configure the tunnel interface with dialer as source interface and tunnel mode
as gre multipoint

interface Tunnel10
 ip address 10.3.0.5 255.255.224.0
 tunnel source dialer0
 tunnel mode gre multipoint

! Here 10.3.0.1 is the private IP address of the DMVPN HUB mGRE Tunnel interface.
76.227.67.123 is the routable public address of the DMVPN Hub

 ip nhrp map 10.3.0.1 76.227.67.123
 ip nhrp map multicast 76.227.67.123

! Configure the vrf Inet-public used for Internet routing

tunnel vrf Inet-public

! Apply the ipsec profile

tunnel protection ipsec profile DMVPN-profile
```

Step 4. Configure routing:

```
!10.6.24.0 to 10.6.31.0 is used for the LAN interfaces

router eigrp 200
 network 10.3.0.0 0.0.31.255
 network 10.6.24.0 0.0.7.255
```

Enabling Cisco WAAS Express for the Mobile Branch Office

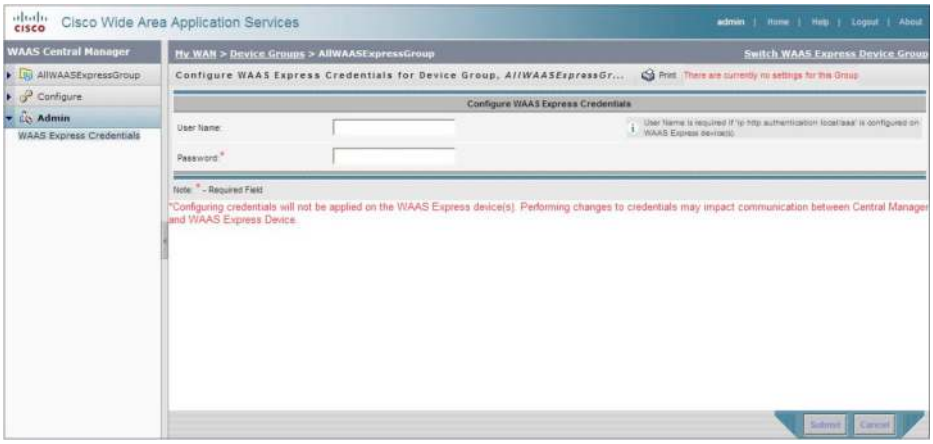
Step 1. Configure Cisco WAAS Express on the DMVPN tunnel interface:

```
interface Tunnel10
 waas enable
```

Configuring the Central Manager for the Cisco WAAS Express

Step 1. Configure the username and password for the Cisco WAAS Express router in Cisco WAAS Central Manager (WCM). (Refer to Figure 6.)

Figure 6. WAAS Express user configuration in WCM



Step 2. Export the digital certificate from the Cisco WCM:

```
telnet 10.4.200.20

Trying 10.4.200.20 ... Open

Cisco Wide Area Application Services Central Manager



NGEW-WCM login: admin

Password:********

System Initialization Finished.

NGEW-WCM#sh crypto certificate-detail admin | begin BEGIN



...skipping

-----BEGIN CERTIFICATE-----

MIIDiTCCAvKgAwIBAgIBIDANBgkqhkiG9w0BAQUFADCBkDELMAkGA1UEBhMCVVMx

EzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMQ0wCwYDVQQL

EwRBREJVMRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtOTy1IT1NU

TkFNRTEcMBoGCSqGSIb3DQEJARYNdGFjQGNpc2NvLmNvbTAeFw0xMDEyMTQxNTIz
```

```
MzFaFw0xNTEyMTMxNTIzMzFaMIGQMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs

aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxDTALBgNVBAsTBEFEQlUxFjAUBgNV

BAoTDUNpc2NvIFN5c3RlbXMxFDASBgNVBAMTC05PLUhPU1ROQU1FMRwwGgYJKoZI

hvcNAQkBFg10YWNAY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB

gQDGhWerw662QhU/h8hnYDdjZZjUxxpVXgWRgM/o6xqfegGwVRszny4+nkZ+Vhs9

cVyCCDEsCNCfo49mq7cwXP50O+YB3wMQbDMtaxfy0CK+RuEECbUMz/FdIHqegOCz

IjO1ex5Q9Bawp2jFPWrvMgZEYe2hZLqvDnHxRGkTdb+DewIDAQABo4HwMIHtMB0G

A1UdDgQWBBQU5oxwKxYCyFZWfAWQ/5/U/WP96DCBvQYDVR0jBIG1MIGygBQU5oxw

KxYCyFZWfAWQ/5/U/WP96KGBlqSBkzCBkDELMAkGA1UEBhMCVVMxEzARBgNVBAgT

CkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMQ0wCwYDVQQLEwRBREJVMRYw

FAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtOTy1IT1NUTkFNRTEcMBoG

CSqGSIb3DQEJARYNdGFjQGNpc2NvLmNvbYIBIDAMBgNVHRMEBTADAQH/MA0GCSqG

SIb3DQEBBQUAA4GBAD3RUJzL3XoKbn4kVCT8CoKdrB2BdDrnFjVN/BZz3s+6TF3E

AmbLlCtmZKZ8x+ALDf+g3ZhUwI04hpN4hr4WI14QYeVGd4zbKuXKACk9uE34u8PJ

RnTlEzzDECRHYj9MpIqx8rKIZE/lbIk2DAC+IbSsBnKi6CrHUEDXys+17TJ2

-----END CERTIFICATE-----
```

Step 3. Configure a self-signed certificate and enable the Secure HTTP (HTTPS) server in the router:

```
crypto pki trustpoint SELF-SIGNED-TRUSTPOINT
enrollment selfsigned
subject-alt-name Bri-3GBrnch-1941.cisco.com
revocation-check none
rsakeypair SELF-SIGNED-RSAKEYPAIR 2048









crypto pki enroll SELF-SIGNED-TRUSTPOINT
```

```
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no

Generate Self Signed Router Certificate? [yes/no]: yes
Generate Self Signed Router Certificate? [yes/no]: yes



!Router Self Signed Certificate successfully created

ip http client source-interface Loopback 0
ip http secure-serve
ip http authentication local
ip http secure-trustpoint SELF-SIGNED-TRUSTPOINT
ip http client source-interface Loopback
ip http client secure-trustpoint SELF-SIGNED-TRUSTPOINT
```

Step 4. Create another trustpoint and install the certificate copied from the Cisco WCM:

```
crypto pki trustpoint NGEW-WAAS-WCM
revocation-check none
enrollment terminal pem
exit

crypto pki authenticate  NGEW-WAAS-WCM


Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself


MIIDiTCCAvKgAwIBAgIBIDANBgkqhkiG9w0BAQUFADCBkDELMAkGA1UEBhMCVVMx

EzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMQ0wCwYDVQQL

EwRBREJVMRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtOTy1IT1NU

TkFNRTEcMBoGCSqGSIb3DQEJARYNdGFjQGNpc2NvLmNvbTAeFw0xMDEyMTQxNTIz

MzFaFw0xNTEyMTMxNTIzMzFaMIGQMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs

aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxDTALBgNVBAsTBEFEQlUxFjAUBgNV

BAoTDUNpc2NvIFN5c3RlbXMxFDASBgNVBAMTC05PLUhPU1ROQU1FMRwwGgYJKoZI

hvcNAQkBFg10YWNAY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
```

```
gQDGhWerw662QhU/h8hnYDdjZZjUxxpVXgWRgM/o6xqfegGwVRszny4+nkZ+Vhs9

cVyCCDEsCNCfo49mq7cwXP50O+YB3wMQbDMtaxfy0CK+RuEECbUMz/FdIHqegOCz

IjO1ex5Q9Bawp2jFPWrvMgZEYe2hZLqvDnHxRGkTdb+DewIDAQABo4HwMIHtMB0G

A1UdDgQWBBQU5oxwKxYCyFZWfAWQ/5/U/WP96DCBvQYDVR0jBIG1MIGygBQU5oxw

KxYCyFZWfAWQ/5/U/WP96KGBlqSBkzCBkDELMAkGA1UEBhMCVVMxEzARBgNVBAgT

CkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMQ0wCwYDVQQLEwRBREJVMRYw

FAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtOTy1IT1NUTkFNRTEcMBoG

CSqGSIb3DQEJARYNdGFjQGNpc2NvLmNvbYIBIDAMBgNVHRMEBTADAQH/MA0GCSqG

SIb3DQEBBQUAA4GBAD3RUJzL3XoKbn4kVCT8CoKdrB2BdDrnFjVN/BZz3s+6TF3E

AmbLlCtmZKZ8x+ALDf+g3ZhUwI04hpN4hr4WI14QYeVGd4zbKuXKACk9uE34u8PJ

RnTlEzzDECRHYj9MpIqx8rKIZE/lbIk2DAC+IbSsBnKi6CrHUEDXys+17TJ2

quit

Certificate has the following attributes:

       Fingerprint MD5: E05B6B41 E3706CA1 81FB799F 60941E32

      Fingerprint SHA1: 79FDE4F7 979AEF79 C2B815DE 38DD65D4 937064A3



% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully import
```

Step 5. Register the Cisco WAAS Express with the Cisco WCM:

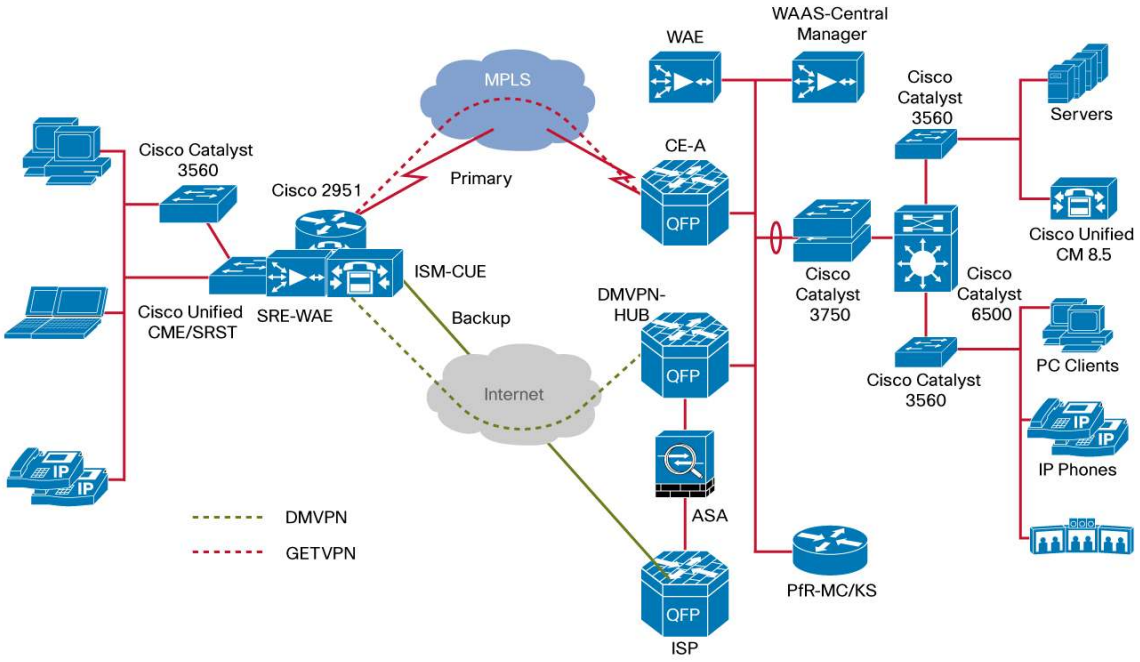
```
3GBrnch#waas cm-register https://10.4.200.20:8443/wcm/register

%WAAS-6-WAAS_CM_REGISTER_SUCCESS: IOS-WAAS registered with Central Manager
successfully
```

Standard Branch Office

A standard branch office has a Cisco 2951 Integrated Services Router, part of the Cisco ISR G2 router portfolio, with a MPLS connection to the provider as the primary WAN link and DSL (asymmetric DSL [ADSL] or symmetric high-speed DSL [SHDSL]) as the backup connection to the Internet (Figure 7). Cisco Unified Communications Manager Express is used for providing IP telephony services to the branch office. Cisco Unified Communications endpoints, including the Cisco Unified IP Phone 9971 videophones, are included in this branch-office design. Voicemail service is provided to the branch office using the Cisco Unity® Express Integrated Services Module (ISM-CUE) installed in the router. The Cisco WAE on Cisco Services-Ready Engine (SRE-WAE) module is used for enabling WAN optimization. A packet voice digital signal processor 3 module (PVDM3) provides videoconferencing services to the videophones registered to the Cisco Unified Communications Manager Express. Video deployment details with medianet features are provided in the Video Implementation guide. PfR deployment details are covered in the NGEW PfR Implementation guide.

Figure 7. Standard Branch-Office Topology



Standard Branch Office - Migration from Services-Ready Branch-Office Architecture

WAN link migration from 2T1 multilink to Ethernet.

Existing WAN links based on a Mutiple-T1 or serial interface can be migrated to Ethernet-based MPLS or Metro Ethernet services with a Cisco 2951 Integrated Services Router. The Cisco 2951 has three onboard Gigabit Ethernet interfaces that provide an easy migration option to an Ethernet-based WAN link. The Ethernet-based WAN link provides flexibility to add bandwidth. In the standard branch-office design, a 10-Mbps WAN link is used; it can be upgraded to 100 Mbps cost-effectively without new customer-premises-equipment (CPE) hardware. Traffic shaping needs to be configured in the QoS to ensure the load does not exceed the subscribed bandwidth from the service provider.

An example configuration for migrating from a 2T1 multilink to an Ethernet-based WAN link follows:

```
! Current configuration on the branch router

 controller T1 0/0/0
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/0/1
 cablelength long 0db
 channel-group 0 timeslots 1-24



interface Multilink1
 ip address 10.4.81.114 255.255.255.252
 ip virtual-reassembly in
 ppp multilink
 ppp multilink group 1

interface Serial0/0/0:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
 max-reserved-bandwidth 100

interface Serial0/0/1:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
 no cdp enable


! Ethernet WAN link configuration. In this example bandwidth offered by provider
is 10Mbps. 10 Mbps will be used for the QoS bandwidth calculation.

interface GigabitEthernet0/1
 bandwidth 10000
 ip address 10.4.81.114 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
```

Routing Deployment for Standard Branch Office

Step 1. Configure BGP as the routing protocol with the MPLS provider edge as the neighbor:

```
! Configure the BGP with the AS number given by the MPLS service provider.
!10.4.82.25 is the IP address of the MPLS-PE router.
!10.4.82.26 is the IP address of the GIG-E interface connected to the MPLS

router bgp 65534
 bgp router-id 10.5.16.253
 bgp log-neighbor-changes
 network 10.4.82.24 mask 255.255.255.252
 network 10.5.16.253 mask 255.255.255.255
 network 10.5.17.0 mask 255.255.255.0
 network 10.5.18.0 mask 255.255.255.0
 network 10.5.19.0 mask 255.255.255.0
 network 10.5.20.0 mask 255.255.255.0
 neighbor 10.4.82.25 remote-as 65400
 no auto-summary
```

Deploying GETVPNGroup Encrypted Transport VPN for Standard Branch Office

Step 1. Configure the PKI trustpoint and enroll the certificate. PKI authentication is used for GETVPN:

```
! Create a trustpoint with PKI server 10.4.226.202

crypto pki trustpoint HE-PKI
 enrollment url http://10.4.226.202:80
 revocation-check none
 rsakeypair MCP

!Generate the key with the label MCP
 crypto key generate rsa modulus 4096 label MCP

!Authenticate and enroll the certificate with the CA server

crypto pki authenticate HE-PKI

crypto pki enroll HE-PKI
```

Step 2. Configure the ISAKMP policy with PKI authentication:

```
! Configure ISAKMP policy with 3DES encryption and authentication using PKI (RSA-
SIG)
```

```
crypto isakmp policy 10
 encr 3des
 hash md5
 group 2
crypto isakmp identity hostname
```

Step 3. Configure the GDOI group and associate it with the crypto map:

```
! Create GDOI group and configure the Key server IP address.10.4.11.210 and
10.4.11.211 are the IP address of the primary and secondary Key server. The
identity number is same in all the Group Members and Key server.



crypto gdoi group GN2
 identity number 1102
 server address ipv4 10.4.11.210
 server address ipv4 10.4.11.211
!
!Create a crypto map and associate the source interface and GDOI group
!
crypto map GN2 local-address Loopback0
crypto map GN2 10 gdoi
 set group GN2
```

Step 4. Apply the crypto map in the MPLS WAN interface:

```
interface GigabitEthernet0/1
 bandwidth 100000
 ip address 10.4.82.26 255.255.255.252
 crypto map GN2
```

Deploying DMVPN for Standard Branch Office

PKI-based authentication can be used for DMVPN with a standard branch office because the certificate can be enrolled with the PKI server using the MPLS WAN link. The procedure is the same as that for the mobile branch office except PKI authentication is used in the standard branch office.

Step 1. Configure the ISAKMP and IPsec:

```
! Configure ISAKMP policy with AES 256 bit encryption and authentication PKI. The
cli “authentication rsa-sig” is not shown below since that is the default
authentication method.

crypto isakmp policy 10
 encr aes 256
  group 2
```

```
!ISAKMP transform set is defined here. ESP with 256 bit AES algorithm is used for
encryption and ESP with SHA HMAC for authentication

crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport

!IPSEC profile creates the association with transform set and isakmp profile

crypto ipsec profile DMVPN-profile
 set transform-set AES256/SHA/TRANSPORT
```

Step 2. Configure the backup SHDSL link to the Internet:

```
! HWIC-4SHDSL card is used for backup Internet link. The controller is configured
for 4 pairs with ATM IMA.

controller SHDSL 0/2/0
 termination cpe
 dsl-group 0 pairs  0, 1, 2, 3 ima
  shdsl annex A-B
  shdsl rate auto



! ATM interface is configured with point-to-point link, IP address will be given
by the Internet service provider. VRF Inet-public is configured in the interface.


interface ATM0/2/IMA0.1 point-to-point
 ip vrf forwarding Inet-public
 ip address 172.38.10.2 255.255.255.252
 pvc 5/5
  protocol ip 172.38.10.1 broadcast
  vbr-rt 8912 8912
  oam-pvc manage
  encapsulation aal5mux ppp Virtual-Template12

! Virtual template is configured with VRF Inet-public

interface Virtual-Template12
 bandwidth 8192
 ip vrf forwarding Inet-public
 ip unnumbered ATM0/2/IMA0.1
```

```
end

! Static route with vrf Inet-public is added to the IP address of the ISP.

ip route vrf Inet-public 0.0.0.0 0.0.0.0 172.38.10.1
```

Step 3. Configure the tunnel interface:

```
! Tunnel source interface is configured with ATM0/2/IMA0.1. VRF Inet-public used
with the ATM interface is configured as tunnel vrf.



interface Tunnel10
 bandwidth 8192
 ip address 10.3.0.2 255.255.224.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco123
 ip nhrp map 10.3.0.1 172.36.10.10
 ip nhrp map multicast 172.36.10.10
 ip nhrp network-id 101
 ip nhrp holdtime 600
ip nhrp nhs 10.3.0.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
 ip summary-address eigrp 200 10.6.0.0 255.255.248.0
 load-interval 30
 tunnel source ATM0/2/IMA0.1
 tunnel mode gre multipoint
 tunnel key 101
 tunnel vrf Inet-public
 tunnel protection ipsec profile DMVPN-profile
```

Step 4. Enable routing for the DMVPN:

```
!EIGRP is used for the routing over DMVPN. All the interfaces except Tunnel 10 is
configured as passive. 10.6.0.0 is the branch LAN network.


router eigrp 200
 network 10.3.0.0 0.0.31.255
 network 10.6.0.0 0.0.7.255
 passive-interface default
 no passive-interface Tunnel10
```

Deploying WAAS for Standard Branch Office

In the standard branch office the Cisco WAE on Cisco Services-Ready Engine (SRE-WAE) is used for application optimization. In this design the external Gigabit Ethernet interface in the Cisco WAE on Cisco Services-Ready Engine module is used for all traffic forwarding to the branch-office router. In the standard branch office the Cisco WAE on the Cisco Services-Ready Engine is installed in slot 2.

Step 1. Configure the IP address and the default gateway for the Cisco WAE on Cisco Services-Ready Engine module:

```
! Configure the IP address on the service module. This is required to session
into the module

interface SM2/0
 ip address 2.2.2.2 255.255.255.252

!IP address of the service module used for router communication and the default

 service-module external ip address 10.6.1.10 255.255.255.0
 service-module ip default-gateway 10.6.1.1
```

Step 2. Configure Cisco WAE:

```
!Session into the WAE console from the router command prompt, the default
user/password is admin/default

Br-MPLSA-StdCE1#service-module sm2/0 session

!Run the setup on the WAE

NOHOSTNAME#setup

!Configure interception method and time zone

Configure Interception method:WCCP

Enter time zone:PDT -8 0

!Configure the interface and disable DHCP. The IP address and the default gateway
are configured from router SM2/0 interface on the router

Select management interface:Gig2/0

Disable DHCP

!Configure the Central Manager IP address
```

```
Enter CMS IP address:10.4.200.20

!Configure the DNS server, domain name and NTP server


Enter DNS server IP: 10.4.11.212

Enter domain name: bri.cisco.com

Enter host name:Br1-ST-WAE1

Enter NTP server IP address: 10.4.11.212

!Configure the WCCP router list with loopback address and select “Enterprise”
License

Enter the WCCP router list: 10.6.0.254
Enter the license(s) you purchased :2

!Apply the configuration on the WAE
```

Step 3. Configure the GRE negotiated return:

```
! GRE negotiated return is used in all WAE devices

egress-method negotiated-return intercept-method wccp
```

Step 4. Configure the WCCP router list:

```
! Remove the default list created by the setup and create a ne w router list

 Br1-ST-WAE1#sh run | include wccp router-list
wccp router-list 7 10.6.1.1

 no wccp router-list 7 10.6.1.1
 wccp router-list 1 10.6.0.254

 wccp tcp-promiscuous router-list-num 1
```

Step 5. Register with WAAS Central Manager:

```
! Register the WAE device with Waas Central Manager for centralized management
   cms enable
```

Step 6. Confgure WCCP on the router:

```
! Create an extended access-list for the traffic which needs to be optimized

ip access-list extended WAAS-REDIRECT-LIST
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any

!Create a standard access-list with WAE ip address

 ip access-list standard WAE
   permit 10.6.1.10
!Enable wccp 61,62 with redirect list and WAE access-list

 ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAE
 ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAE
```

Step 7. Enable WCCP redirection on the interface:

```
! Enable wccp 62 redirect on the WAN interface

  interface GigabitEthernet0/1
   bandwidth 10000
   ip address 10.4.81.114 255.255.255.252
   ip wccp 62 redirect in


! Enable wccp 61 redirect on the LAN interface
   interface GigabitEthernet0/0.1
    description wired DATA-VLAN
    encapsulation dot1Q 15
    ip address 10.6.1.1 255.255.255.0
    ip wccp 61 redirect in
```

Deploying Rich-Media Services

Step 1. Configure Cisco Unified Communications Manager Express:

```
! The IP address of the voice vlan interface is configured as IP source address.
Max phones is configured as 100 and max dns as 200.

 telephony-service
 sdspfarm conference mute-on 1 mute-off 1
 sdspfarm conference lecture-mode on #11 release #22
```

```
 sdspfarm units 5
 conference hardware
 video
  maximum bit-rate 2000
 max-ephones 100
 max-dn 200
 ip source-address 10.6.10.1 port 2000
 max-redirect 5
 dialplan-pattern 4 972400.... extension-length 4
 max-conferences 3 gain -6
 call-park system application
 call-forward pattern .T
 transfer-system full-consult

! DN configuration

ephone-dn  1
 number 1001

ephone-dn  1
 number 1002


! sample configuration for 7970 voice phone with dn number 1001

ephone  1
 device-security-mode none
 mac-address 0021.A02D.0E67
 max-calls-per-button 2
 type 7970
 button  1:1

! sample configuration for 7985 video phone with dn number 1002

ephone  2
 device-security-mode none
 video
 mac-address 0050.6003.8720
 ephone-template 1
 type 7985
 keep-conference endcall
 button  1:2
```

Step 2. Configure a Session Initiation Protocol (SIP) trunk to Cisco Unified Communications Manager:

```
! The IP address of the CUCM is 10.4.200.15. The dn for the phones in campus
starts with 408 prefix. The trunk is configured with video codec h264 to support
```

```
calls to video phones registered with CUCM.


dial-peer voice 2 voip
 destination-pattern 408.......
 video codec h264
 rtp payload-type cisco-codec-fax-ack 111
 rtp payload-type cisco-codec-video-h264 97
 session protocol sipv2
 session target ipv4:10.4.200.15
 incoming called-number 972.......
 dtmf-relay rtp-nte
 codec g711ulaw
```

Deploying QoS for Standard Branch Office

Further details about end-to-end QoS and remarking from 6 to 4 class are discussed in the NGEW QoS deployment guide.

Deploying QoS for MPLS WAN Link

Step 1. Configure class maps:

```
! class-maps are configured to similar to the MPLS-CE in the aggregation
```

Step 2. Configure the QoS policy map:

```
! Policy map with queuing and sample bandwidth reservation (bandwidth percentage
can be changed based on the traffic profile). Policy-map used for BGP marking is
added in the class NETWOK-MGMT-OAM.


policy-map WAN-SP-CLASS-OUTPUT
 class VOICE
  priority percent 10
 class VIDEO-RT-INTERACTIVE
  priority percent 23
 class NETWORK-MGMT-OAM
  bandwidth percent 5
  service-policy MARK-BGP
class STREAMING-SIGNALLING
  bandwidth percent 17
 class CRITICAL-DATA
  bandwidth percent 15
 class BULK-SCAVENGER
  bandwidth percent 5
  random-detect
 class class-default
```

```
  bandwidth percent 25
  random-detect
```

Step 3. Configure shaping and apply the QoS:

```
! Shaping is done to make sure the load does not exceed the bandwidth subscribed
from the provider. For Standard branch 10Mbps is recommended bandwidth, shaping
is done for the same. The policy with queuing is applied as child policy.

policy-map Int-Gig-SBr
 class class-default
  shape average 10000000
  service-policy WAN



interface GigabitEthernet0/1
 ip address 10.4.81.114 255.255.255.252
 ip nbar protocol-discovery
 duplex auto
 speed auto
 media-type rj45
 service-policy output Int-Gig-SBr
```

Deploying QoS for DMVPN Tunnel

Step 1. Configure shaping and apply QoS:

```
! Shaping is done to make sure the load does not exceed the bandwidth subscribed
from the provider. SHDSL 4 pair has a maximum bandwidth of 9216 Mbps, the
subscribed bandwidth in this example is 8912. The policy with queuing is applied
as child policy.

policy-map Int-ATM
 class class-default
  shape average 8900000
  service-policy WAN

!QoS is applied on the ATM0/2/IMA0.1 interface
interface ATM0/2/IMA0.1 point-to-point
 ip vrf forwarding Inet-public
 ip address 172.38.10.2 255.255.255.252
 pvc 5/5
  protocol ip 172.38.10.1 broadcast
  vbr-rt 8912 8912
  oam-pvc manage
  encapsulation aal5mux ppp Virtual-Template12
```

```
    service-policy output Int-ATM
```

High-End Aggregation

High-end Aggregation can terminate up to 5000 branches which consist of all 4 types of branch profiles. High-end Aggregation requires the highest availability and performance, and will contain redundant components and multiple connections to both MPLS and Internet.

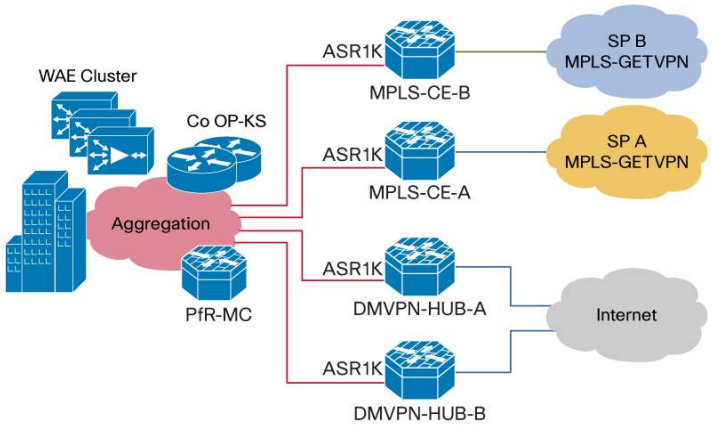
In this design the headend customer edge routers, which are acting as headend group members, are Cisco ASR 1000 Series routers. For High-end aggregation the configuration of Cisco ASR 1000 Series routers shown in Table 7 is used.

Table 7. Configuration of Cisco ASR 1000 Series Routers

Component	Type	Redundancy	Performance
Chassis model	Cisco ASR 1006	No	Based on RP and ESP
ESP	ESP40	Yes	Up to 10 Gbps encrypted
RP	RP2	Yes	

The design has Cisco ISR G2 routers acting as keyserver. The keyserver is configured with group policies that are pushed to all group members.

Figure 8. RWAN High-End Aggregation



Deploying Group Encrpted Transport VPN for High-End Aggregation

One of the main differences in high-end vs. standard aggregation is the high availability of six 9s. To have six 9s availability, a redundant keyserver is used in this design. PKI is the mandatory requirement for high-end and standard branch offices.

The MPLS cloud interconnects the headend to the branch-office sites. The customer edge routers on each site act as group members. The headend customer edge router is also acting as a group member. All these routers are grouped into a GDOI group. Therefore all keyservers and group members are part of the same VPN. For redundancy and high availability, there are two keyservers.

Keyserver Configuration

For redundancy, two keyservers are used in this design.

Primary Keyserver Configuration

The keyserver configuration procedure is similar to that for standard aggregation. Please follow the step-by-step procedure defined for standard aggregation except for the following:

Step 1. Generate an RSA key for rekey on co-op keyservers

The cryptography key used for rekey must be generated with the export option; the same key is imported into the secondary keyserver:

```
! REKEYRSA" is the name of the key.
crypto key generate rsa modulus 1024 label REKEYRSA exportable
```

Note: It is a good practice not to save the exported keys anywhere; instead import them to the other routers directly by copying and pasting from the console of the first keyserver. It should be done through a secure computer. If the keys are compromised, the security of the network will be undermined.

Step 2. Configure the GDOI group with a secondary keyserver address:

```
! 10.4.11.210 is the loopback ip address of the local (primary) KS. 10.4.11.211
is the ip address of the secondary KS server. The KS with higher priority number
is elected as primary.

crypto gdoi group GN2
 identity number 1102
 server local
  rekey algorithm aes 128
  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa REKEYRSA
  registration interface Loopback0
  registration interface GigabitEthernet0/1
  sa ipsec 1
   profile GN
   match address ipv4 ACL_GN2
   no replay
  address ipv4 10.4.11.210
  redundancy
   local priority 250
   peer address ipv4 10.4.11.211
```

Co-op Keyserver Configuration

Step 1. Configure IKE phase 1.

IKE phase 1 configuration comprises two important parts: configuring ISAKMP policy and authentication method:

```
crypto isakmp policy 10
```

```
 encr 3des
 hash md5
 group 2
authentication rsa-sig
```

Step 2. Configure PKI and download certificates.

PKI is the more secure and scalable method of authentication. The following steps must be repeated on all devices in the network.

Note: rsa-sig is the default authentication method for an ISAKMP policy.

Unique RSA keys must be generated on all keyservers and group members as follows:

```
crypto key generate rsa general keys label pki_KS modulus 4096
```

All keyserver and group members must be configured with a trustpoint:

```
crypto pki trustpoint HE-PKI
 ! The URL is the address of the PKI server
 enrollment url http://10.4.226.202:80
 revocation-check none
 ! PKI_KS is the label of the generated keys
 rsakeypair PKI_KS
```

Authenticate to the CA server and download the signed certificate:

```
crypto pki authen HE-PKI
crypto pki enroll HE-PKI
```

Step 3. Configure IPsec parameters:

```
crypto ipsec transform-set 3DES esp-aes 256 esp-md5-hmac
!
crypto ipsec profile GN
 set security-association lifetime seconds 3600
 set transform-set 3DES
!
```

Step 4. Import the RSA key that is used for rekey from the primary keyserver:

```
! The key is exported first from the primary KS.Execute the below command at the
configuration prompt of the primary KS. “cisco123” is the passcode
crypto key export rsa REKEYRSA pem terminal 3des cisco123
% Key name: REKEYRSA
Usage: General Purpose Key
Key data:
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCuKbSROW7eSqxC+IjB0ipplVkT
...
...
...
```

```
NtSRSR51ooWQW5CXRwIDAQAB
-----END PUBLIC KEY-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,B2CE8D823EE52FDC
Zi82W/lX3u0WiHN0ezi6qH5Jeo1baptdqzLlVk2jioAyZabWJqc7+svFY+DJ8rT+
...
...
...
p3dHnQSBaLu1pH3YI9gebQhMgqH6Ie00ucEYVl4/jArzUjifjdCvkQ==
-----END RSA PRIVATE KEY-----



!Execute the below command on the configuration prompt of the Secondary KS and
paste the key copied from the export.


crypto key import rsa REKEYRSA pem terminal cisco123
% Enter PEM-formatted public General Purpose key or certificate.
% End with a blank line or "quit" on a line by itself.
<Paste the public key from the output of the key export. Paste
the hexadecimel information the linesmarkedBEGIN and END.>
quit
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
<Paste the private key from the output of the key export. Paste
the hexadecimel information the linesmarkedBEGIN and END.>
quit
!
Repeat the process for all other Key Servers.
```

Step 5. Configure GDOI group:

```
! 10.4.11.211 is the loopback ip address of the local (secondary) KS. 10.4.11.210
is the ip address of the secondary KS server. The priority number of this KS is
configured with a lower number.


crypto gdoi group GN2
 identity number 1102
 server local
  rekey algorithm aes 128
  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa REKEYRSA
  registration interface Loopback0
  registration interface GigabitEthernet0/1
  sa ipsec 1
   profile GN
```

```
     match address ipv4 ACL_GN2
     no replay
    address ipv4 10.4.11.211
    redundancy
     local priority 1
     peer address ipv4 10.4.11.210
```

Step 6. Configure ACL:

Everything that is allowed in the ACL is traffic to be encrypted. Anything denied will go unencrypted:

```
  ip access-list extended ACL_GN2
   deny   tcp any eq bgp any
   deny   tcp any any eq bgp
   deny   udp any eq 848 any
   deny   udp any any eq 848
   deny   eigrp any any
   deny   udp any any eq ntp
   deny   udp any eq ntp any
   deny   udp any any eq snmp
   deny   udp any eq snmp any
   deny   udp any any eq syslog
   deny   udp any eq syslog any
   deny   tcp any host 10.4.226.202 eq www
   deny   tcp host 10.4.226.202 eq www any
   deny   pim any host 224.0.0.13
   deny   igmp any any
   deny   tcp any eq telnet any
   deny   tcp any any eq telnet
   deny   udp any eq tftp any
   deny   udp any any eq tftp
   permit ip any any
```

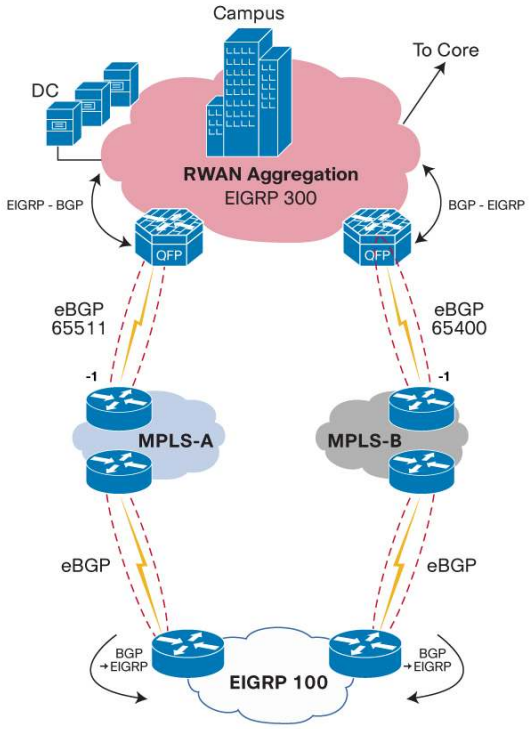
Group Member Configuration on the Aggregation Customer Edge (Cisco ASR 1000)

Group member configuration is similar to the group member configuration in the standard design section. However, routing is slightly different, as described in the following section.

Routing on Group Member

The group member is running eBGP to connect to the service provider edge. The internal network of the RWAN aggregation is running EIGRP. Route redistribution is configured between EIGRP and BGP for high-end aggregation because there are two headend routers for redundancy. Because it is possible to get the same route from two different providers into the LAN, it is necessary to apply an ACL to avoid looping (Figure 9). The configuration follows.

Figure 9. Routing Desing for High-End Aggregation




```
router eigrp 300
 distribute-list Block-CE in
 default-metric 100000 100 255 1 1500
 network 10.4.0.0 0.0.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface Port-channel1
 no passive-interface GigabitEthernet0/0/1
 eigrp router-id 10.4.11.204
!
router bgp 65511
 bgp router-id 10.4.11.204
 bgp log-neighbor-changes
 neighbor 10.4.81.1 remote-as 65000
!
 address-family ipv4
  network 10.4.81.0 mask 255.255.255.252
  redistribute eigrp 300
  neighbor 10.4.81.1 activate
exit-address-family
 !
!
```

```
ip access-list standard Block-CE
 deny   10.5.0.0 0.0.255.255
 deny   10.4.81.0 0.0.0.255
 deny   10.4.82.0 0.0.0.255
 permit any!
```

Deploying DMVPN for High-End Aggregation

In this design dual hubs are used for redundancy and high availability. The spokes terminate on both hubs and have routing preference to connect to the primary hub.

The authentication method on the hub is both certificate and preshared. Although certificate is the preferred method, it might not be feasible for some of the mobile client routers to download the certificate. In that case there are two options: either have the certificate loaded on the box before installing it on the mobile site or use the preshared key to authenticate the peer.

The routing protocol used over DMVPN is BGP. The hub routers also act as the route reflectors. All spokes are defined as route-reflector clients. Route redistribution is configured between EIGRP used internally in the RWAN aggregation and BGP with the spokes over the DMVPN tunnel.

DMVPN Hub-A Configuration

Step 1. Configure IKE phase 1:

```
crypto isakmp policy 20
 encr aes 256
 group 2
crypto isakmp identity hostname
crypto isakmp profile inet-public
   keyring DMVPN
   match identity address 0.0.0.0 Inet-public
!
!
```

Step 2. Configure IKE phase 2:

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-profile
 set transform-set AES256/SHA/TRANSPORT
```

Step 3. Configure the DMVPN tunnel:

```
interface Tunnel10
 bandwidth 100000
 ip address 10.3.0.1 255.255.224.0
 no ip redirects
 ip mtu 1400
 ip wccp 62 redirect in
 no ip next-hop-self eigrp 200
```

```
 no ip split-horizon eigrp 200
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp redirect
 ip tcp adjust-mss 1360
 load-interval 30
 qos pre-classify
 cdp enable
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 101
 tunnel vrf Inet-public
 tunnel protection ipsec profile DMVPN-profile
!
```

Step 4. Configure BGP as the routing protocol.

Following is the BGP configuration on the hub. If the BGP autonomous system is unique for each of the standard branch-office routers, you should use eBGP instead of iBGP:

```
router bgp 1000
 bgp router-id 99.2.1.1
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 timers bgp 120 480
 redistribute connected
 neighbor spoke1 peer-group
 neighbor spoke1 remote-as 1000
 neighbor spoke1 update-source Tunnel1
 neighbor spoke1 route-reflector-client
 neighbor spoke1 next-hop-self
 neighbor spoke2 peer-group
 neighbor spoke2 remote-as 1000
 neighbor spoke2 update-source Tunnel1
 neighbor spoke2 route-reflector-client
 neighbor spoke2 next-hop-self
 neighbor spoke3 peer-group
 neighbor spoke3 remote-as 1000
 neighbor spoke3 update-source Tunnel1
 neighbor switch peer-group
 neighbor switch remote-as 1000
 neighbor switch update-source GigabitEthernet0/0/1
```

```
    neighbor switch route-reflector-client
    neighbor switch next-hop-self
    neighbor 21.1.10.1 peer-group spoke2
    neighbor 21.1.10.2 peer-group spoke2
```

DMVPN Hub-B Configuration

The configuration procedure is same as the previous steps 1-3.

Deploying WAAS for High-End Aggregation

In high-end aggregation the Cisco WAE-7371 appliance is used as a Cisco WAAS Central Manager deployed in the data center. The Cisco WAE-7371 can manage up to 2000 devices. WAE clustering with the N + 1 redundancy model is used for the WAE appliance devices deployed in the RWAN aggregation. The Cisco WAE-7371 appliance is used based on the hardware capacity. The sizing details are provided in Table 8. A more comprehensive, interactive WAAS sizing tool is available at cisco.com: http://tools.cisco.com/WAAS/sizing.

Table 8. Sizing Details for Cisco WAE-7371

Device	Maximum Optimized TCP Connections	Maximum Recommended WAN Link (Mbps)	Maximum Optimized Throughput (Mbps)	Maximum Peers Devices
Cisco WAE-7341	12000	300	1000	1400
Cisco WAE-7371	50000	1000	2500	2800

The number of Cisco WAE appliances is based on the total number of users online during an hour window and the number of TCP connections per user. A minimum of four Cisco WAE-7371 appliances are required for the high-end aggregation. All the devices are connected to the RWAN distribution switch. Please refer to the section “Deploying WAAS for Standard Aggregation” for the step-by-step configuration procedure.

Deploying QoS for High-End Aggregation

In high-end aggregation the QoS classes mentioned in Table 9 are used. Most of the service providers support only six classes. The broadcast video class is re-marked in the WAN interface before traffic is sent to the provider. In this design, because Group Encrpted Transport VPN is used in the WAN interface, the DSCP value re-marking is done on the encrypted packet header. When the packet is decrypted in the remote site, the original DSCP value - in this case CS5 for broadcast video - will be preserved. No re-marking is required in the remote site. The same is applicable for the DMVPN link also. Further details about end-to-end QoS and remarking are discussed in the NGEW QoS deployment guide.

Table 9. QoS Classes

Layer 3				Layer 2
Service Class	**PHB**	**DSCP**	**IPP**	**CoS**
Network control	CS6	48	6	6
Telephony	EF	46	5	5
Signaling	CS3	24	3	3
Multimedia conferencing	AF41, 42, and 43	34, 36, and 38	4	4
Real-time interactive	CS4	32	4	4
Multimedia streaming	AF31, 32, and 34	26, 28, 30	3	3
Broadcast video	CS5	40	5	5
Low-latency data	AF21, 22, and 23	18, 20, 22	2	2

Layer 3				Layer 2
OAM	CS2	16	2	2
Bulk data	AF11, 12, and 13	10, 12, 14	1	1
Scavenger	CS1	8	1	1
Default “best effort”	DF	0	0	0

Deploying QoS for MPLS Customer Edge

Step 1. Configure class maps:

```
! Configure the class maps, routing protocol used also should be included in the
network control. NBAR is used to identify BGP traffic and dscp value is set to
cs6.



class-map match-any VOICE
 match ip dscp ef
class-map match-any VIDEO-RT-INTERACTIVE
 match ip dscp cs4 af41
class-map match-any NETWORK-MGMT-OAM
 match ip dscp cs2 cs6
class-map match-any STREAMING-SIGNALLING
 match ip dscp cs3 af31
class-map match-any CRITICAL-DATA
 match ip dscp af21 af22 af23
class-map match-any BULK-SCAVENGER
 match ip dscp cs1 af11
class-map match-any BROADCAST-VIDEO
 match ip dscp cs5
class-map match-any BEST-EFFORT
 match ip dscp default
class-map match-any BGP-Routing
 match protocol bgp
!

! Policy map is configured to set the dscp value to cs6.
policy-map MARK-BGP
 class BGP-Routing
  set dscp cs6

! NBAR is enabled on the WAN interface connecting to the MPLS
interface GigabitEthernet0/1
 ip address 10.4.81.10 255.255.255.252
 ip nbar protocol-discovery
 duplex auto
 speed auto
 media-type rj45
```

Step 2. Configure the QoS policy map:

```
! Policy map with class cs5 (Broadcast video) remarked to af41 to match with
Service Provider 6 class offering.


policy-map WAN-SP-CLASS-OUTPUT
 class VOICE
  priority percent 10
 class VIDEO-RT-INTERACTIVE
  priority percent 23
 class NETWORK-MGMT-OAM
  bandwidth percent 5
  service-policy MARK-BGP
class BROADCAST-VIDEO
 set ip dscp af41
 bandwidth percent 7
 class STREAMING-SIGNALLING
  bandwidth percent 10
 class CRITICAL-DATA
  bandwidth percent 15
 class BULK-SCAVENGER
  bandwidth percent 5
  random-detect
 class class-default
  bandwidth percent 25
  random-detect
```

Step 3. Configure shaping and apply the QoS:

```
! Shaping is done to make sure the load does not exceed the bandwidth subscribed
from the provider. For high end aggregation 1000Mbps is recommended bandwidth,
shaping is done for the same. The policy with queuing is applied as child policy.


policy-map Int-Gig-Agg-HE
 class class-default
  shape average 1000000000
  service-policy WAN



interface GigabitEthernet0/1
 ip address 10.4.81.2 255.255.255.252
 duplex auto
 speed auto
```

```
    media-type rj45
    service-policy output Int-Gig-Agg-HE
```

Deploying QoS for DMVPN Hub

For DMVPN, traffic shaping is configured in QoS for the backup link of the standard branch offices to the aggregation and primary link of the mobile branch offices. With limitations that exist today, the best approach is to group similar branch offices into one policy and shape on that group. Because both traffic policing and queuing are required, a two-level hierarchy is used: policing on the child level and shaping on the parent level.

For the step-by-step configuration procedure, refer to the section “Deploying QoS in DMVPN hub for Standard Aggregation”.

Deploying Remote Sites for High-End Aggregation

Three different types of remote sites are supported in the RWAN high-end or large-scale aggregation (Table 10).

Table 10. Types of Remote Sites with High-End Aggregation

Branch-Office Type	Platform	WAN Link	Wan Optimization	Secure Connectivity
Mobile	Cisco 1941 ISR	Single: 3G	WAAS-Express	DMVPN
Standard	Cisco 2951 ISR	Dual: MPLS and Internet	SRE-WAE	Group Encrypted Transport VPN/DMVPN
High end	Two Cisco 3945 ISRs	One MPLS link on each router	SRE-WAE	Group Encrypted Transport VPN
Ultra high end	Two Cisco ASR 1001 Routers	One MPLS link on each router	WAE appliance	Group Encrypted Transport VPN

Mobile Branch Office

The mobile branch office has a Cisco 1941 ISR with a 3G wireless connection to the Internet as the WAN link and DMVPN for secure connectivity to the RWAN aggregation. Cisco WAAS Express embedded with Cisco IOS Software is used for WAN optimization, which is suitable for low-bandwidth (< 2 Mbps) WAN links. Deployment details are provided in the section for mobile branch-office standard aggregation.

Standard Branch Office

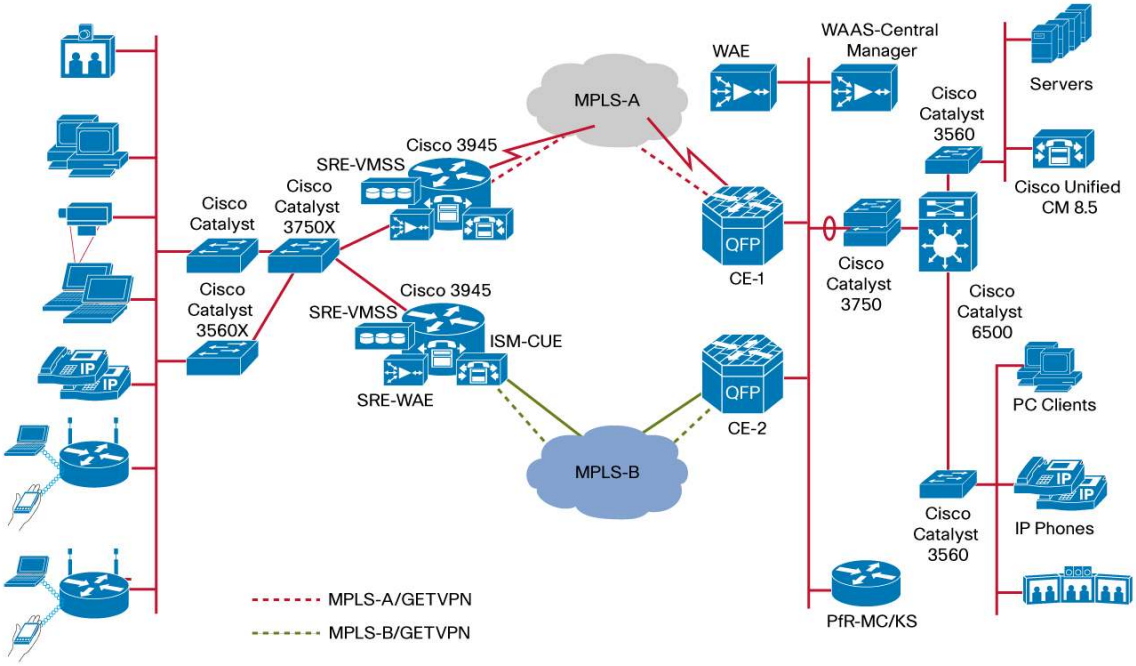
The standard branch office has a Cisco 2951 ISR with a MPLS connection to the provider as the primary WAN link and DSL (ADSL/SHDSL) as the backup connection to the Internet. Cisco Unified Communications Manager Express is used for providing IP telephony services to the branch office. Cisco Unified Communications endpoints, including Cisco Unified IP Phones 9971 videophones, are included in this branch-office design. Voicemail service is provided to the branch office using the Cisco Unity Express ISM (ISM-CUE) installed in the router. The Cisco WAE on the Cisco Services-Ready Engine (SRE-WAE) module is used for enabling WAN optimization. A PVDM3 DSP installed in the Cisco 2951 is used for providing videoconferencing services to the videophones registered to the Cisco Unified Communications Manager Express. Deployment details are provided in the section for standard aggregation for the standard branch office .

High-End Branch Office

The high-end branch office has redundant Cisco 3945 ISRs with Hot Standby Router Protocol (HSRP) enabled on the LAN interface. Both the routers have a single MPLS connection to different providers using a Gigabit Ethernet interface as the WAN link with bandwidth provisioned to 100 Mbps. Rich-media services such as video surveillance, Survivable Remote Site Telephony (SRST), video streaming, and different types of endpoints are included in this design. The centralized Cisco Unified Communications Manager deployed in the data center

provides IP telephony services to the branch office. A PVDM3 installed in Cisco 3945 is used for providing local videoconferencing services to the Cisco videophones such as the Cisco Unified IP Phone 9971 registered to Cisco Unified Communications Manager and Cisco TelePresence® System EX90 (EX90), E20, and Cisco TelePresence Movi registered to the Cisco TelePresence Video Communication Server Expressway (VCS Expressway). Cisco WAE on Cisco Services-Ready Engine (SRE-WAE) module installed in both of the branch-office routers enables the WAN optimization service in cluster mode. PfR is used to provide application-level intelligent routing and load distribution between the two MPLS links. PfR deployment details are provided in the NGEW PfR Implementation guide. Video deployments with medianet features are provided in the NGEW Video Implementation guide.

Figure 10. High-End Branch-Office Topology



Migration from Services-Ready Branch-Office Architecture

WAN Link Migration from DS-3 to Gigabit Ethernet

Existing WAN links based on DS-3 can be migrated to Ethernet-based MPLS or Metro Ethernet services with the Cisco 3945 ISR. The Cisco 3945 has three onboard Gigabit Ethernet interfaces that provide an easy migration option to an Ethernet-based WAN link. An Ethernet-based WAN link provides flexibility to add bandwidth. In the high-end branch-office design, a 100-Mbps WAN link is used; it can be upgraded to higher bandwidth later cost-effectively without new CPE hardware. Traffic shaping needs to be configured in the QoS to ensure the load does not exceed the subscribed bandwidth from the service provider.

An example configuration for migrating from a DS-3 to an Ethernet-based WAN link follows:

```
! Current configuration on the branch router

 controller T3 1/0 (DS3 controller)
```

```
interface Serial1/0
 ip address 10.4.81.10 255.255.255.252
 ip flow ingress
 ip flow egress
 encapsulation ppp
 load-interval 30
 dsu bandwidth 44210
 end


!Gigabit Ethernet WAN link configuration. The bandwidth offered by provider is
100Mbps.

interface GigabitEthernet0/1
 bandwidth 100000
 ip address 10.4.81.10 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
```

Deploying HSRP

In a high-end branch-office, HSRP is configured on the LAN interfaces of the branch-office routers to provide first-hop redundancy for all the branch-office IP endpoints. An HSRP virtual IP that is shared between two branch-office routers is configured as the default gateway for all the endpoints. HSRP operates in active/standby mode; based on the HSRP priority configured, one of the branch-office routers is active and the other router is standby. In this design the HSRP priority is configured in such a way that router A is configured with higher priority for the data VLAN interface and router B is configured for the voice VLAN. So, router A would be the active router for all the hosts configured in the data VLAN and router B for voice and video endpoints:

```
! HSRP configuration in Router A. Router A is configured with higher standby
priority for data vlan.

!Virtual IP address 10.5.17.100 is configured as default gateway for all the
hosts

 interface GigabitEthernet0/2.1
 description Vlan-Data
 encapsulation dot1Q 31
 ip address 10.5.17.1 255.255.255.0
 standby 1 ip 10.5.17.100
 standby 1 priority 110
 standby 1 preempt
```

```
 standby 1 track 1 decrement 10

interface GigabitEthernet0/2.2
 description Vlan-Voice
 encapsulation dot1Q 32
 ip address 10.5.18.1 255.255.255.0
 ip pim sparse-mode
 standby 1 ip 10.5.18.100
 standby 1 priority 110
 standby 1 preempt
 standby 1 track 1 decrement 10
 ip tcp adjust-mss 1360

!HSRP configuration in Router B. Router B is configured with higher priority for
Voice vlan.

!Virtual IP address 10.5.18.100 is configured as default gateway for all the
voice/video endpoints



interface GigabitEthernet0/2.1
 description Vlan-Data
 encapsulation dot1Q 31
 ip address 10.5.17.2 255.255.255.0
 standby 1 ip 10.5.17.100
 standby 1 priority 100
 standby 1 preempt
 standby 1 track 1 decrement 10

interface GigabitEthernet0/2.2
 description Vlan-Voice
 encapsulation dot1Q 32
 ip address 10.5.18.2 255.255.255.0
 ip pim sparse-mode
 standby 1 ip 10.5.18.100
 standby 1 priority 120
 standby 1 preempt
 standby 1 track 1 decrement 10
 ip tcp adjust-mss 1360
```

Transit Network

The transit network is configured between the two routers. This network is used for router-router communication and to avoid hair-pinning. This network is used for PfR also; for more information, refer to the NGEW PfR Deployment guide. The transit network should use an additional subinterface on the router interface that is already being used for data, voice, or the physical interface, if available. The configuration follows:

```
! Transit network configuration in Router A.
```

```
interface GigabitEthernet0/2.10
 description Transit network
 ip address 10.5.16.1 255.255.255.252

Transit network configuration in Router B.

interface GigabitEthernet0/2.10
 description Transit network
 ip address 10.5.16.2 255.255.255.252
```

Routing Deployment for High-End Branch Office

BGP is used as the routing protocol for MPLS with the provider edge devices. The MPLS carrier gives the autonomous system number (ASN) for the BGP. The MPLS provider edge router uses a different BGP ASN, so eBGP is used between them. EIGRP is used between the two branch-office routers so that full reachability to all the remote sites can be achieved. BGP routes from the MPLS are redistributed to the EIGRP. The configuration follows:

```
! BGP ASN 65534 is used and PE's ASN is 65400. The local router MPLS WAN link IP
is 10.4.82.26 and PE is 10.4.82.25. All the LAN networks 10.5.17.0- 10.5.20.0 is
configure in the BGP.


router bgp 65534
 bgp router-id 10.5.16.253
 bgp log-neighbor-changes
 network 10.4.82.24 mask 255.255.255.252
 network 10.5.16.253 mask 255.255.255.255
 network 10.5.17.0 mask 255.255.255.0
 network 10.5.18.0 mask 255.255.255.0
 network 10.5.19.0 mask 255.255.255.0
 network 10.5.20.0 mask 255.255.255.0
 neighbor 10.4.82.25 remote-as 65400
 no auto-summary

! EIGRP 200 is used between the two routers. A network statement matching the
local interface IP address is used. BGP 65534 is redistributed in EIGRP. All the
interface is configured as passive except the transit network.


router eigrp 300
 default-metric 100000 100 255 1 1500
 network 10.5.16.0 0.0.7.255
 passive-interface default
```

```
 redistribute bgp 65534
 no passive-interface GigabitEthernet0/2.10
 eigrp router-id 10.5.16.253
!
```

Deploying Group Encrpted Transport VPN in the High-End Branch Office

Step 1. Configure the ISAKMP and IPsec. PKI authentication is used for Group Encrpted Transport VPN in this design:

```
! Same as the GETVPN deployment for Standard branch in Standard aggregation
```

Step 2. Configure the ISAKMP and IPsec. PKI authentication is used for Group Encrpted Transport VPN in this design:

```
!Same as the GETVPN deployment for Standard branch in Standard aggregation
```

Step 3. Configure the GDOI group and associate it with the crypto map:

```
! Same as the GETVPN deployment for Standard branch in Standard aggregation
```

Step 4. Apply the crypto map in the MPLS WAN interface:

```
interface GigabitEthernet0/1
 bandwidth 100000
 ip address 10.4.82.26 255.255.255.252
 crypto map GN2
```

Deploying WAAS in the High-End Branch Office

In the high-end branch office, the Cisco WAE on Cisco Services-Ready Engine (SRE-WAE) is used for application optimization. In this design the external Gigabit Ethernet interface in the Cisco WAE on the Cisco Services-Ready Engine module is used for all traffic forwarding to the branch-office router.

Deploying Cisco WAAS on Router A

Step 1. Configure the IP address and the default gateway for the Cisco WAE on Cisco Services-Ready Engine module in router A WAE1:

```
! Configure the IP address on the service module. This is required to session
into the module

interface SM2/0
 ip address 1.1.1.2 255.255.255.252
```

```
!IP address of the service module used for router communication and the default
gateway. The default gateway configured here is the HSRP IP address of the data
vlan

 service-module external ip address 10.5.17.10 255.255.255.0
 service-module ip default-gateway 10.5.17.100
```

Step 2. Configure Cisco WAE:

```
This is similar to the standard branch only the IP address will be 10.5.17.10
```

Step 3. Configure the GRE negotiated return:

```
! GRE negotiated return is used in all WAE devices

egress-method negotiated-return intercept-method wccp
```

Step 4. Configure the WCCP router list:

```
!WCCP router list is configured with loopback address of both the routers

 wccp router-list 1 10.5.16.254 10.5.16.253

 wccp tcp-promiscuous router-list-num 1
```

Step 5. Register with WAAS Central Manager:

```
! Register the WAE device with Waas Central Manager for centralized management
   cms enable
```

Step 6. Confgure WCCP on the router:

```
! Create an extended access-list for the traffic which needs to be optimized

ip access-list extended WAAS-REDIRECT-LIST
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any

!Create a standard access-list with IP address of WAE-1 & WAE-2 for HA and load
```

```
balancing

ip access-list standard WAE
 permit 10.5.17.10
 permit 10.5.17.11

!Enable wccp 61,62 with redirect list and WAE access-list

 ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAE
 ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAE
```

Step 7. Enable WCCP redirection on the interface:

```
! Enable wccp 62 redirect on the WAN interface

 interface GigabitEthernet0/1
 bandwidth 100000
 ip address 10.4.81.10 255.255.255.252
 ip wccp 62 redirect in
 duplex auto
 speed auto
 media-type rj45
 service-policy output WAN

! Enable wccp 61 redirect on the LAN interface, this is enabled only on the Data
Vlan Interface

interface GigabitEthernet0/2.1
 description Vlan-Data
 encapsulation dot1Q 31
 ip address 10.5.17.2 255.255.255.0
 ip wccp 61 redirect in
 standby 1 ip 10.5.17.100
 standby 1 priority 110
 standby 1 preempt
 standby 1 track 1 decrement 10
```

Deploying WAAS on Router B

Step 1. Configure the IP address and the default gateway for the Cisco WAE on the Cisco Services-Ready Engine module in router B WAE2:

```
! Configure the IP address on the service module. This is required to session
into the module


interface SM2/0
```

```
 ip address 1.1.1.5 255.255.255.252

!IP address of the service module used for router communication and the default
gateway. The default gateway configured here is the HSRP IP address of the data
vlan

 service-module external ip address 10.5.17.11 255.255.255.0
 service-module ip default-gateway 10.5.17.100
```

Step 2. Configure Cisoc WAE:

```
!This is similar to the standard branch only the IP address will be 10.5.17.11
```

Step 3. Configure the GRE negotiated return:

```
!This is similar to WAE-1 configuration
```

Step 4. Configure the WCCP router list:

```
!WCCP router list is same as WAE-1
```

Step 5. Register with WAAS Central Manager:

```
! Register the WAE device with Waas Central Manager for centralized management
   cms enable
```

Step 6. Confgure WCCP on the router:

```
! Same as router 1
```

Step 7. Enable WCCP redirection on the interface:

```
! Same as router1
```

Deploying Rich-Media Services for High-End Branch Office

Please refer to the Cisco Unified Communications Systems Solution reference guide for deployment details of Cisco Unified Communications Manager.

Step 1. Configure SRST:

```
! The IP address of the voice vlan interface is configured as IP source address.
```

```
Max phones is configured as 200 and max dns as 400.

 call-manager-fallback
 video
 max-conferences 8 gain -6
 transfer-system full-consult
 ip source-address 10.5.10.100 port 2000
 max-ephones 200
 max-dn 400
 system message primary VIDEO-SCCP-SRST
```

Deploying QoS for High-End Branch Office

Further details about end-to-end QoS and remarking are discussed in the NGEW QoS deployment guide.

Step 1. Configure class maps:

```
Configure the class map, routing protocol used also should be included in the
network control. BGP is not marked with dscp value by default, so NBAR is used to
identify BGP traffic and dscp value is set to cs6.



class-map match-any VOICE
 match ip dscp ef
class-map match-any VIDEO-RT-INTERACTIVE
 match ip dscp cs4 af41
class-map match-any NETWORK-MGMT-OAM
 match ip dscp cs2 cs6
class-map match-any STREAMING-SIGNALLING
 match ip dscp cs3 af31
class-map match-any CRITICAL-DATA
 match ip dscp af21 af22 af23
class-map match-any BULK-SCAVENGER
 match ip dscp cs1 af11
class-map match-any BROADCAST-VIDEO
 match ip dscp cs5
class-map match-any BEST-EFFORT
 match ip dscp default
class-map match-any BGP-Routing
 match protocol bgp
!

! Policy map is configured to set the dscp value to cs6.
policy-map MARK-BGP
 class BGP-Routing
  set dscp cs6

! NBAR is enabled on the WAN interface connecting to the MPLS
```

```
interface GigabitEthernet0/1
 ip address 10.4.81.10 255.255.255.252
 ip nbar protocol-discovery
 duplex auto
 speed auto
 media-type rj45
```

Step 2. Configure the QoS policy map:

```
! Policy map with class cs5 (Broadcast video) remarked to af41 to match with
Service Provider 6 class offering. Policy map with queuing and sample bandwidth
reservation. Policy-map used for BGP marking is added in the class NETWOK-MGMT-
OAM.



policy-map WAN-SP-CLASS-OUTPUT
 class VOICE
  priority percent 10
 class VIDEO-RT-INTERACTIVE
  priority percent 23
 class NETWORK-MGMT-OAM
  bandwidth percent 5
  service-policy MARK-BGP
class BROADCAST-VIDEO
 set ip dscp af41
 bandwidth percent 7
 class STREAMING-SIGNALLING
  bandwidth percent 10
 class CRITICAL-DATA
  bandwidth percent 15
 class BULK-SCAVENGER
  bandwidth percent 5
  random-detect
 class class-default
  bandwidth percent 25
  random-detect
```

Step 3. Configure shaping and apply the QoS:

```
! Shaping is done to make sure the load does not exceed the bandwidth subscribed
from the provider. For high end 100Mbps is recommended bandwidth, shaping is done
for the same. The policy with queuing is applied as child policy.


policy-map Int-Gig-HE
```

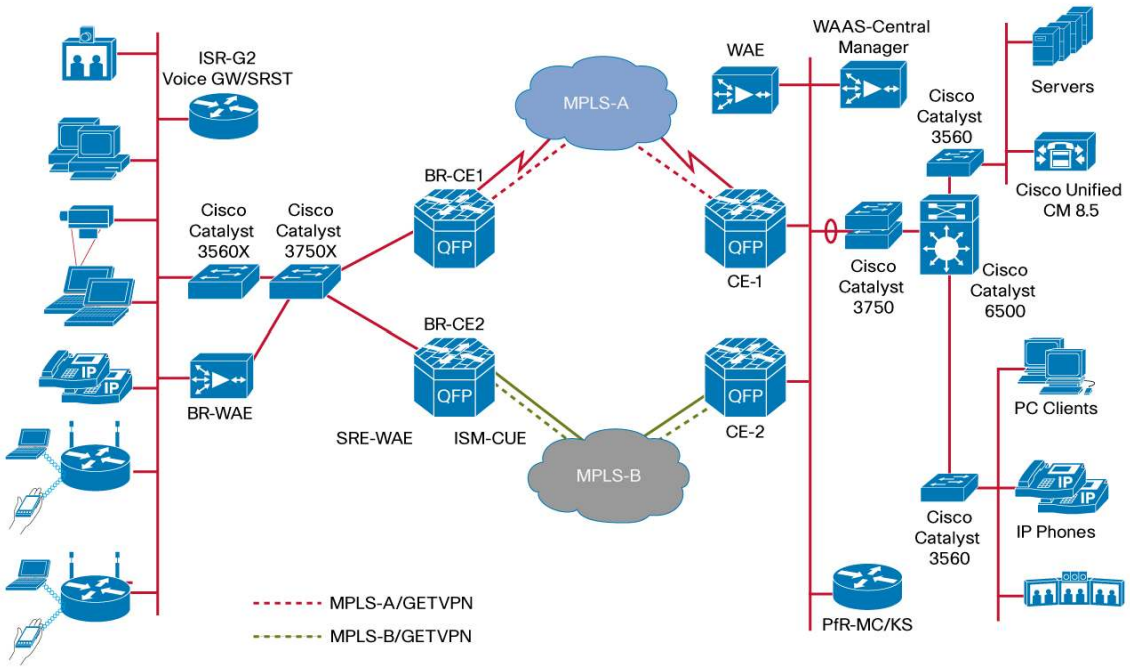
```
 class class-default
  shape average 100000000
  service-policy WAN


interface GigabitEthernet0/1
 bandwidth 100000
 ip address 10.4.81.10 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 service-policy output Int-Gig-HE
```

Ultra-High-End Branch Office

The ultra-high-end branch office has redundant Cisco ASR 1001 routers with HSRP enabled on the LAN interface (Figure 11). Both the routers have a single MPLS connection to different providers using a Gigabit Ethernet interface as the WAN link with bandwidth provisioned to 1 Gbps. The centralized Cisco Unified Communications Manager deployed in the data center provides IP telephony services to the branch office. The Cisco 3945 is used for providing rich-media services such as SRST and videoconferencing. Different types of IP telephony endpoints are included in this design. A PVDM3 installed in the Cisco 3945 provides local videoconferencing services to the Cisco videophones such as the Cisco Unified IP Phone 9971 registered to Cisco Unified Communications Manager and EX90, E20, and Cisco TelePresence Movi registered to the Cisco VCS Expressway. Two Cisco WAE-674-K9 appliances installed in the branch office enable the WAN optimization service in cluster mode. PfR provides application-level intelligent routing and load distribution between the two MPLS links. PfR deployment details are provided in the NGEW PfR Implementation guide.

Figure 11. Ultra-High-End Branch-Office Topology



Deploying HSRP

In the ultra-high-end branch office, HSRP is configured on the LAN interfaces of the branch-office routers to provide first-hop redundancy for all the branch-office IP endpoints. The HSRP virtual IP that is shared between two branch-office routers is configured as the default gateway for all the endpoints. HSRP operates in active/standby mode; based on the HSRP priority configured, one of the branch-office routers is active and the other router is standby. In this design the HSRP priority is configured in such a way that router A is configured with higher priority for the data VLAN interface and router B is configured for the voice VLAN. So, router A is the active router for all the hosts configured in the data VLAN and router B is the active router for voice and video endpoints:

```
! HSRP configuration in BR-CE1. BR-CE1 is configured with higher standby priority
for data vlan.


!Virtual IP address 10.5.25.100 is configured as default gateway for all the
hosts
interface GigabitEthernet0/0/1.1
 description Vlan-Data
 encapsulation dot1Q 61
 ip address 10.5.25.1 255.255.255.0
 ip wccp 61 redirect in
 ip pim sparse-mode
 standby 1 ip 10.5.25.100
 standby 1 priority 110
 standby 1 preempt
 standby 1 track 1 decrement 10
!
interface GigabitEthernet0/0/1.2
 description Vlan-Voice
 encapsulation dot1Q 62
 ip address 10.5.26.1 255.255.255.0
 standby 1 ip 10.5.26.100
 standby 1 priority 110
 standby 1 preempt
 standby 1 track 1 decrement 10
 ip tcp adjust-mss 1360


!HSRP configuration in BR-CE2. BR-CE2 is configured with higher priority for
Voice vlan.


!Virtual IP address 10.5.26.100 is configured as default gateway for all the
voice/video endpoints



interface GigabitEthernet0/0/1.1
 description Vlan-Data
 encapsulation dot1Q 61
 ip address 10.5.25.2 255.255.255.0
 ip wccp 61 redirect in
```

```
 ip flow ingress
 ip flow egress
 ip pim sparse-mode
 standby 1 ip 10.5.25.100
 standby 1 priority 100
 standby 1 preempt
 standby 1 track 1 decrement 10
!
interface GigabitEthernet0/0/1.2
 description Vlan-Voice
 encapsulation dot1Q 62
 ip address 10.5.26.2 255.255.255.0
 ip flow ingress
 ip flow egress
 ip pim sparse-mode
 standby 1 ip 10.5.26.100
 standby 1 priority 120
 standby 1 preempt
 standby 1 track 1 decrement 10
 ip tcp adjust-mss 1360
```

Transit Network

The transit network is configured between the two routers. This network is used for router-router communication and to avoid hair-pinning. This network is used for PfR also; for more information, please refer to the PFR Deployment guide.The transit network should use an additional subinterface on the router interface that is already being used for data, voice, or physical interface, if available. The configuration follows:

```
! Transit network configuration in BR-CE1.
 interface GigabitEthernet0/0/1.5
 encapsulation dot1Q 60
 ip address 10.5.24.1 255.255.255.252

!Transit network configuration in BR-CE2.
 interface GigabitEthernet0/0/1.5
 encapsulation dot1Q 60
 ip address 10.5.24.2 255.255.255.252
```

Routing Deployment for Ultra-High-End Branch Office

BGP is used as the routing protocol for MPLS with the provider edge. The MPLS carrier gives the ASN for the BGP. The MPLS provider edge router uses a different BGP ASN, so eBGP is used between them. EIGRP is used between the two branch-office routers so that full reachability to all the remote sites can be achieved. BGP routes from the MPLS are redistributed to the EIGRP. The configuration follows:

```
! BGP ASN 65402 is used and PE's ASN is 65000. The local router MPLS WAN link IP
is 10.4.81.138 and PE is 10.4.81.137. All the LAN networks 10.5.25.0- 10.5.28.0
is configured in the BGP.

router bgp 65402
 bgp router-id 10.5.24.253
 bgp log-neighbor-changes
 network 10.4.81.136 mask 255.255.255.252
 network 10.5.24.253 mask 255.255.255.255
 network 10.5.25.0 mask 255.255.255.0
 network 10.5.26.0 mask 255.255.255.0
 network 10.5.27.0 mask 255.255.255.0
 network 10.5.28.0 mask 255.255.255.0
 neighbor 10.4.81.137 remote-as 65000

! EIGRP 200 is used between the two routers. A network statement matching the
local interface IP address is used. BGP 65402 is redistributed in EIGRP. All the
interfaces are configured as passive except the transit network.

router eigrp 200
 default-metric 100000 100 255 1 1500
 network 10.5.24.0 0.0.7.255
 redistribute bgp 65402
 passive-interface default
 no passive-interface GigabitEthernet0/0/1.5
 eigrp router-id 10.5.24.253
!
```

Deploying Group Encrpted Transport VPN on the Ultra-High-End Branch Office

The Group Encrpted Transport VPN deployment steps are similar to those for the high-end branch office. Please refer to the procedure for deploying Group Encrpted Transport VPN for the high-end branch office for step-by-step instructions.

Deploying WAAS in the Ultra-High-End Branch Office

In the ultra-high-end branch office, the Cisco WAE appliance is used for application optimization. In this design two Cisco WAE-674 appliances are used for high availability and load sharing. The appliances are connected to the data VLAN of the branch office.

Deploying WAE

This design is similar to the WAE deployment in the standard aggregation; a negotiated return GRE tunnel is used from the Cisco WAE to the router. Traffic to be reinjected into the network uses a negotiated return WCCP GRE tunnel egress method back to the originating router. This method is preferred because it allows the Cisco WAE appliances to be located one or more routed hops away from the WCCP router. A default mask is used in the WAE in the configuration that follows.

For step-by-step instructions, please refer to “Configuring WAE on the Standard Aggregation”.

Enabling WAAS on the BR-CE1

This design uses WCCP 61 inbound on LAN-facing interfaces to match unoptimized data from the clients. WCCP 62 is used inbound on WAN-facing interfaces, matching optimized data sourced from the data center.

Step 1. Confgure WCCP on the router:

```
! Create an extended access-list for the traffic which needs to be optimized

ip access-list extended WAAS-REDIRECT-LIST
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any

!Create a standard access-list with IP address of WAE-1 & WAE-2 for HA and load
balancing

ip access-list standard WAE
 permit 10.5.25.10
 permit 10.5.25.11

!Enable wccp 61,62 with redirect list and WAE access-list

 ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAE
 ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAE
```

Step 2. Enable WCCP redirection on the interface:

```
! Enable wccp 62 redirect on the WAN interface
interface GigabitEthernet0/0/0
 bandwidth 10000
 ip address 10.4.81.138 255.255.255.252
 ip mtu 1400
 ip wccp 62 redirect in
 ip pim sparse-mode
 load-interval 30
 negotiation auto
 crypto map GN2

! Enable wccp 61 redirect on the LAN interface, this is enabled only on the Data
```

```
Vlan Interface

interface GigabitEthernet0/0/1.1
 description Vlan-Data
 encapsulation dot1Q 61
 ip address 10.5.25.1 255.255.255.0
 ip wccp 61 redirect in
 ip flow ingress
 ip flow egress
 ip pim sparse-mode
 standby 1 ip 10.5.25.100
 standby 1 priority 110
 standby 1 preempt
 standby 1 track 1 decrement 10
```

Deploying WAAS on BR-CE2

Please follow the previous steps 1 and 2 for the BR-CE1.

Deploying Rich-Media Services for Ultra-High-End Branch Office

The Cisco 3945 is used in the ultra-high-end branch office for providing SRST service for the branch-office users. A PVDM3 DSP module is also installed in this router to provide videoconferencing services for the branch office. Please refer to the NGEW Video Implementation guide for the configuration procedure for the videoconferencing service.

Please refer to the Cisco Unified Communications Systems Solution reference guide for deployment details of Cisco Unified Communications Manager.

Step 1. Configure SRST:

```
! The IP address of the ISR-G2 voice vlan interface is configured as IP source
address. Max phones is configured as 200 and max dns as 400.

 call-manager-fallback
 video
 max-conferences 8 gain -6
 transfer-system full-consult
 ip source-address 10.5.25.10 port 2000
 max-ephones 200
 max-dn 400
 system message primary VIDEO-SCCP-SRST
```

Deploying QoS for Ultra-High-End Branch Office

The QoS deployment procedure is the same as that for the high-end branch office. QoS shaping is done on the bandwidth provisioned in the WAN interface. Further details about end-to-end QoS and remarking are discussed in the NGEW QoS deployment guide.

Step 2. Configure shaping and apply the QoS:

```
! Shaping is done to make sure the load does not exceed the bandwidth subscribed
from the provider. For high end 100Mbps is recommended bandwidth, shaping is done
for the same. The policy with queuing is applied as child policy.

policy-map Int-Gig-HE
 class class-default
  shape average 100000000
  service-policy WAN


interface GigabitEthernet0/1
 bandwidth 100000
 ip address 10.4.81.10 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 service-policy output Int-Gig-HE
```

Product List

Table 11. Products list for NGEW WAN

Role	Hardware or Software	Software Version
Standard aggregation - MPLS customer edge	Cisco ASR 1002	RLS 3.3
Standard aggregation -DMVPN hub	Cisco ASR 1002	RLS 3.3
Mobile branch office	Cisco 1941W	15.1(4)M
Standard branch office	Cisco 2951	15.1(4)M
	Cisco PVDM3-256	
High-end branch office	Cisco 3945	15.1(4)M
	Cisco PVDM3-256	
Ultra-high-end branch office	Cisco ASR 1001	RLS 3.3
	Cisco 3945	15.1(4)M
Cisco WAAS Central Manager	Cisco WAE-674 and WAE-7371	4.4
High-end aggregation -MPLS customer edge	Cisco ASR 1006	RLS 3.3
High-end aggregation -DMVPN hub	Cisco ASR 1006	RLS 3.3
Cisco WAE appliance	Cisco WAE-7371	4.4
Call control	Cisco Unified Communications Manager	8.6
	Cisco Unified Communications Manager Express (embedded in Cisco IOS Software)	8.6

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C07-680894-00 10/11