Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.
Preface

Who Should Read This Guide
This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series
Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

   month year  Series

For example, the series of guides that we released in August 2011 are the “August 2011 Series”.

You can find the most recent series of SBA guides at the following sites:

   Customer access:  http://www.cisco.com/go/sba
   Partner access:  http://www.cisco.com/go/sbachannel

How to Read Commands
Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

   configure terminal

Commands that specify a value for a variable appear as follows:

   ntp server 10.10.48.17

Commands with variables that you must define appear as follows:

   class-map [highest class name]

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

   Router#  enable

Long commands that line wrap are underlined. Enter them as one command:

   wrq-queue random-detect max-threshold 1 100 100 100 100 100

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

   interface Vlan64
   ip address 10.5.204.5 255.255.255.0

Comments and Questions
If you would like to comment on a guide or ask questions, please use the forum at the bottom of one of the following sites:

   Customer access:  http://www.cisco.com/go/sba
   Partner access:  http://www.cisco.com/go/sbachannel

An RSS feed is available if you would like to be notified when new comments are posted.
# Table of Contents

**What's In This SBA Guide** .................................................. 1
  - About SBA .............................................................. 1
  - About This Guide ..................................................... 1

**Introduction** ..................................................................... 2
  - Business Overview ....................................................... 2
  - Architecture Overview ................................................ 2
  - About This Guide ......................................................... 3
  - Considerations for Deploying the Cellular Remote Site .......... 9
  - Remote Sites—3G/DMVPN Spoke Router Selection ................. 10

**Deployment Details** ....................................................... 12
  - GSM Specific—Remote Site Router Configuration .................. 13
  - CDMA Specific - Remote Site Router Configuration ............... 14
  - Remote-Site 3G/DMVPN Router Configuration ..................... 16
  - Control Usage of 3G Interface ....................................... 27

**Appendix A: 3G Wireless Remote Site Product List** ............... 30
**Appendix B: Configuration** ............................................... 31
  - RS220-1941 .............................................................. 33
  - Remote Site 221: Single-Router, Dual-Link ......................... 38
  - RS221-2921 .............................................................. 38
  - Remote Site 222: Dual-Router, Dual-Link .......................... 43
  - RS222-2921-1 ........................................................... 43
  - RS222-2921-2 ........................................................... 47

---

**ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY 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 THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.
Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization’s problems—without worrying about the technical complexity.

For more information, see the How to Get Started with Cisco SBA document:


**About This Guide**

This additional *deployment guide* includes the following sections:

- **Business Overview**—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations’ operations.

- **Technology Overview**—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.

- **Deployment Details**—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.

**Route to Success**

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: [http://www.cisco.com/go/sba](http://www.cisco.com/go/sba)

For partner access: [http://www.cisco.com/go/sbachannel](http://www.cisco.com/go/sbachannel)
Introduction

Business Overview

Connectivity to an organization's data is no longer confined to the walls of its buildings. The world is more mobile and today's consumers expect products and services to come to them. For example:

- Mobile clinics require up-to-the-minute communication with various specialists and the ability to exchange patient x-rays, medical tests, and files.
- Emergency Mobile Deployment Units require up-to-the-minute communication, remote information feedback, and local site intercommunication.
- Tradeshows and special events require interactive kiosks and Internet hotspots, credit card processing, and up-to-the-minute marketing campaigns through digital advertising.

These are just some situations where cellular is likely the only option for providing high-bandwidth network WAN connectivity.

Cellular connectivity is a resilient solution for your remote site. A resilient remote site provides an always-accessible network for the applications users interact with directly, from site-to-site backup and recovery to email service. How well users interact with the network and their ability to reach essential services impacts the business' overall performance.

Reliable network services provided by Cisco SBA—such as the Internet connection, wide-area network (WAN) infrastructure, and security—help ensure that a business can rely on applications such as web conferencing for critical collaboration.

High availability at the remote sites is an essential requirement for productivity, safety, and security within the majority of organizations. Therefore, the ability to maintain connectivity for critical business data transactions is imperative to the Cisco SBA design.

Cisco SBA for Enterprise Organizations is a prescriptive architecture that delivers an easy-to-use, flexible, and scalable network with wired connectivity, wireless connectivity, security, WAN optimization, and unified communication components. It eliminates the challenges of integrating the various network components by using a standardized design that is reliable and has comprehensive support offerings.

Figure 1 - Use Cases

To learn more about Cisco Smart Business Architecture, visit:
http://www.cisco.com/go/sba or
http://www.cisco.com/go/partner/smartarchitecture

Architecture Overview

This guide provides a design that enables highly available, secure, and optimized connectivity for remote-site LANs by using Cisco 3G technology.

The WAN is the networking infrastructure that provides an Internet protocol (IP)-based connection between remote sites (or branches) that are separated by large geographic distances.

Organizations require the WAN to provide sufficient performance and reliability for the remote-site users to be effective in supporting the business. Although most of the applications and services that the remote-site worker uses are centrally located, the WAN design must provide a common resource access experience to the workforce, regardless of location.

Carrier-based MPLS service is not always available or cost-effective for an organization to use for WAN transport to support remote-site connectivity. Internet-based IP VPNs provide an optional transport that can be used as a resilient backup to a primary MPLS network transport or may be adequate to provide the primary network transport for a remote site. Flexible network
architecture should include Internet VPN as a transport option without significantly increasing the complexity of the overall design.

While Internet IP VPN networks present an attractive option for effective WAN connectivity, anytime an organization sends data across a public network there is risk that the data will be compromised. Loss or corruption of data can result in a regulatory violation and can present a negative public image, either of which can have significant financial impact on an organization. Secure data transport over public networks like the Internet requires adequate encryption to protect business information.

**About This Guide**

This guide is written as an addition to the WAN Deployment Guide and the VPN Remote Site Deployment Guide. This guide provides the basic information you need to deploy a remote site. Additional details are available in the aforementioned guides.

This document shows you how to deploy the network foundation and services to enable the following:

- 3G wireless WAN connectivity for remote sites
- Primary and secondary links to provide redundant topology options for resiliency
- Data privacy via encryption
- Wired and wireless LAN access at all remote sites

**Cellular Options**

Cellular connectivity enables this solution with a flexible, high speed, high bandwidth option. There are two competing technologies that provide high bandwidth network WAN connectivity where cellular is the only option: code division multiple access (CDMA) or Global System for Mobile Communications (GSM). Much of the world can only select one or the other.

**Code Division Multiple Access**

CDMA has its roots in World War II. It only relates to over-the-air transmission, giving each user the full use of the radio spectrum, which can provide higher data rates than can be achieved with GSM. CDMA leverages time-division multiple access (TDMA) and general packet radio service (GPRS), a packetized technology. CDMA uses a much stronger signal and can have a much better coverage model sometimes at the expense of GSM when both technologies exist together in densely populated areas.

When choosing CDMA over GSM, consider where you are deploying your remote site. CDMA is predominately used within the United States but used rarely elsewhere in the world and is nonexistent in Europe because the European Union mandates the sole use of GSM.

**Global System for Mobile Communications**

GSM was invented in 1987 by the GSM Association, an international organization dedicated to developing the GSM standard worldwide. The data rates are typically lower than what can be found with CDMA; however, with enhanced data rates for GSM evolution (EDGE), the performance disparity is getting smaller. GSM also offers the advantage of being the world leader in deployment with over 74% of cellular deployments using GSM, and, as already mentioned, it is used by virtually all of Europe. Another clear advantage of GSM over CDMA is the ability to move the subscriber identity module (SIM) from one device to another, which essentially moves your service from device to device without having to work through your service provider.

**Third Generation and Fourth Generation**

Today’s working data standard is third generation (3G). It provides data rates of 200 kbps for moving users and up to 2Mb/s for stationary users. Some carriers are beginning to market fourth generation (4G) standard products, which promise up to gigabit data rates for stationary users and must be able to achieve at least 100 Mb/s data rates for moving/mobile users. The International Telecommunication Union (ITU) defines both of these standards. The promise of these data rates and bandwidth brings interesting technology opportunities to the remote sites.

Reader Tip

The solution presented in this guide leverages Cisco Integrated Services G2 Routers running Cisco IOS® software. They contain either a CDMA or a GSM high-speed WAN interface card (HWIC).
WAN Design

This document builds upon the reference designs for a WAN aggregation site that are used in the Smart Business Architecture—Borderless Networks for Enterprise Organizations WAN Deployment Guide and VPN Remote Site Deployment Guide as blueprints for deploying a remote site. The primary focus of the design is to use the following commonly deployed WAN transports:

- MPLS Layer 3 VPN
- Internet VPN running over a 3G wireless WAN

The chosen architecture designates a primary WAN aggregation site that is analogous to the hub site in a traditional hub-and-spoke design. This site has direct connections to both WAN transports and high-speed connections to the selected service providers. In addition, the site leverages network equipment scaled for high performance and redundancy. The primary WAN aggregation site is co-resident with the data center and usually the primary campus or LAN as well.

MPLS WAN Transport

Cisco IOS MPLS enables enterprises and service providers to build next-generation intelligent networks that deliver a wide variety of advanced, value-added services over a single infrastructure. This economical solution can be integrated seamlessly over any existing infrastructure such as IP, frame relay, ATM, or Ethernet.

MPLS Layer 3 VPNs use a peer-to-peer VPN model that leverages the border gateway protocol (BGP) to distribute VPN-related information. This peer-to-peer model allows enterprise subscribers to outsource routing information to service providers, which can result in significant cost savings and a reduction in operational complexity for enterprises.

Subscribers who need to transport IP multicast traffic can enable multicast VPNs.

The WAN leverages MPLS VPN as a primary WAN transport.

Internet as WAN Transport

The Internet is essentially a large-scale public WAN composed of multiple interconnected service providers. The Internet can provide reliable high-performance connectivity between various locations, although it lacks any explicit guarantees for these connections. Despite its “best effort” nature, the Internet is a sensible choice for an alternate WAN transport, or for a primary transport when it is not feasible to connect with another transport option.

Internet connections are typically included in discussions relevant to the Internet edge, specifically for the primary site. Remote-site routers also commonly have Internet connections, but do not provide the same breadth of services using the Internet. For security and other reasons, Internet access at remote sites is often routed through the primary site.

The WAN leverages the Internet for VPN site-to-site connections as both a primary WAN transport and as a backup WAN transport (to a primary VPN site-to-site connection).

DMVPN

Cisco Dynamic Multipoint VPN (DMVPN) is a solution for building scalable site-to-site VPNs that support a variety of applications. DMVPN is widely used for encrypted site-to-site connectivity over public or private IP networks and can be implemented on all WAN routers used in this deployment guide.

Cisco DMVPN was selected for the encryption solution for the Internet transport because it supports on-demand full mesh connectivity with a simple hub-and-spoke configuration and a zero-touch hub deployment model for adding remote sites. Cisco DMVPN also supports spoke routers that have 3G WAN HWICs with dynamically assigned IP addresses.

Cisco DMVPN makes use of multipoint generic route encapsulation tunnels (mGRE) to interconnect the hub to all of the spoke routers. These mGRE tunnels are also sometimes referred to as DMVPN clouds in this context. This technology combination supports unicast, multicast, and broadcast IP including the ability to run routing protocols within the tunnels.

WAN Remote-Site Designs

This guide documents multiple remote-site WAN designs, and they are based on various combinations of WAN transports mapped to the site specific requirements for service levels and redundancy.
The remote-site designs include single or dual WAN edge routers. These can be either a CE router or a VPN spoke router. In some cases, a single WAN edge router can perform the role of both a CE router and VPN-spoke router.

Most remote sites are designed with a single router WAN edge; however, certain remote-site types require a dual router WAN edge. Dual router candidate sites include regional office or remote campus locations with large user populations, as well as sites with business critical needs that justify additional redundancy to remove single points of failure.

The overall WAN design methodology is based on a primary WAN-aggregation site design that can accommodate all of the remote-site types that map to the various link combinations listed in the following table.

---

### Table 1 - WAN Remote-Site Transport Options

<table>
<thead>
<tr>
<th>WAN Remote-Site Router(s)</th>
<th>WAN Transports</th>
<th>Primary Transport</th>
<th>Secondary Transport</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single</td>
<td>Single</td>
<td>Internet (3G)</td>
<td></td>
</tr>
<tr>
<td>Single</td>
<td>Dual</td>
<td>MPLS VPN A</td>
<td>Internet (3G)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MPLS VPN B</td>
<td>Internet (3G)</td>
</tr>
<tr>
<td>Dual</td>
<td>Dual</td>
<td>MPLS VPN A</td>
<td>Internet (3G)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MPLS VPN B</td>
<td>Internet (3G)</td>
</tr>
</tbody>
</table>

Modularity in network design allows you to create design elements that can be replicated throughout the network.

The WAN remote-site designs are standard building blocks in the overall design. Replication of the individual building blocks provides an easy way to scale the network and allows for a consistent deployment method.

### WAN/LAN Interconnect

The primary role of the WAN is to interconnect primary site and remote-site LANs. The LAN discussion within this guide is limited to how the remote-site LANs connect to the remote-site WAN devices. Specific details regarding the LAN components of the design are covered in the Smart Business Architecture—Borderless Networks for Enterprise Organizations LAN Deployment Guide.

At remote sites, the LAN topology depends on the number of connected users and physical geography of the site. Large sites may require the use of a distribution layer to support multiple access layer switches. Other sites may only require an access layer switch directly connected to the WAN remote-site router(s). The variants that are tested and documented in this guide are shown in the following table.

### Table 2 - WAN Remote-Site LAN Options

<table>
<thead>
<tr>
<th>WAN Remote-Site Routers</th>
<th>WAN Transports</th>
<th>LAN Topology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single</td>
<td>Single</td>
<td>Access only</td>
</tr>
<tr>
<td>Single</td>
<td>Dual</td>
<td>Access only</td>
</tr>
<tr>
<td>Dual</td>
<td>Dual</td>
<td>Access only</td>
</tr>
</tbody>
</table>
WAN Remotes Sites—LAN Topology

For consistency and modularity, all WAN remote sites use the same VLAN assignment scheme shown in the following table. This deployment guide uses a convention that is relevant to any location that has a single access switch or access switch stack.

**Tech Tip**

VoIP is not supported over a 3G Wireless WAN. The following VLAN assignments should only be used at remote sites with a MPLS primary connection, and usage of the secondary 3G link should be limited to data only.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Usage (MPLS Primary)</th>
<th>Usage (3G Primary)</th>
<th>L2 Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN 65</td>
<td>Wireless Data</td>
<td>Wireless Data</td>
<td>Yes</td>
</tr>
<tr>
<td>VLAN 70</td>
<td>Wireless Voice</td>
<td>Not supported</td>
<td>Yes</td>
</tr>
<tr>
<td>VLAN 64</td>
<td>Data 1</td>
<td>Data 1</td>
<td>Yes</td>
</tr>
<tr>
<td>VLAN 69</td>
<td>Voice 1</td>
<td>Not supported</td>
<td>Yes</td>
</tr>
<tr>
<td>VLAN99</td>
<td>Transit</td>
<td>Not used</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The benefits of this design are clear: all of the access switches can be configured identically, regardless of the number of sites in this configuration.

Access switches and their configuration are not included in this guide. The Smart Business Architecture—Borderless Networks for Enterprise Organizations LAN Deployment Guide provides configuration details on the various access switching platforms.

**Layer 2 Access**

WAN remote sites that do not require additional distribution layer routing devices are considered to be flat—or from a LAN perspective, they are considered unrouted Layer 2 sites. All Layer 3 services are provided by the attached WAN router(s). The access switch(es), through the use of multiple VLANs, can support services such as data (wired and wireless) and voice (wired and wireless). The design shown in the following figure illustrates the standardized VLAN assignment scheme.

Access switches and their configuration are not included in this guide. The Layer 3 Distribution Layer design is not covered in this guide. Please refer to the WAN Deployment Guide for more detail on configuring a WAN remote site with a distribution layer.

IP subnets are assigned on a per-VLAN basis. This design only allocates subnets with a 255.255.255.0 netmask for the access layer, even if less than 254 IP addresses are required. (This model can be adjusted as necessary to other IP address schemes.) The connection between the router and the access switch must be configured for 802.1Q VLAN trunking with subinterfaces on the router that map to the respective VLANs on the switch. The various router subinterfaces act as the IP default gateways for each of the IP subnet and VLAN combinations.
A similar LAN design can be extended to a dual-router edge, as shown in the following figure. This design change introduces some additional complexity. The first requirement is to run a routing protocol: Enhanced Interior Gateway Protocol (EIGRP) should be configured between the routers. For consistency with the primary site LAN, use EIGRP process 100.

Because there are now two routers per subnet, a First Hop Redundancy Protocol (FHRP) must be implemented. We selected Hot Standby Router Protocol (HSRP) as the FHRP for this design. HSRP is designed to allow for transparent failover of the first-hop IP router. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active router and a standby router. When there are multiple routers on a LAN, the active router is the router of choice for routing packets; the standby router is the router that takes over when the active router fails or when preset conditions are met.

Enhanced Object Tracking (EOT) provides a consistent methodology for various router and switching features to conditionally modify their operation based on information objects available within other processes. The objects that can be tracked include interface line protocol, ip route reachability, and ip sla reachability, as well as several others.

The IP service-level agreement (SLA) feature provides a capability for a router to generate synthetic network traffic that can be sent to a remote responder. The responder can be a generic IP endpoint that can respond to an ICMP echo (ping) request, or it can be a Cisco router running an IP SLA responder process, which can respond to more complex traffic such as jitter probes. The use of IP SLA allows the router to determine end-to-end reachability to a destination and also the roundtrip delay. More complex probe types can also permit the calculation of loss and jitter along the path. IP SLA is used in tandem with EOT within this design.
To improve convergence times after a MPLS WAN failure, HSRP has the capability to monitor the reachability of a next-hop IP neighbor through the use of EOT and IP SLA. This combination allows for a router to give up its HSRP Active role if its upstream neighbor becomes unresponsive, which provides additional network resiliency.

HSRP is configured to be active on the router with the highest priority WAN transport. EOT of IP SLA probes is implemented in conjunction with HSRP so that in the case of WAN transport failure, the standby HSRP router associated with the lower priority (alternate) WAN transport becomes the active HSRP router. The IP SLA probes are sent from the MPLS CE router to the MPLS PE router to ensure reachability of the next hop router. This is more effective than simply monitoring the status of the WAN interface.

The dual router designs also warrant an additional component that is required for proper routing in certain scenarios. In these cases, a traffic flow from a remote-site host might be sent to a destination reachable via the alternate WAN transport (for example: a MPLS + DMVPN remote site communicating with a DMVPN-only remote site). The primary WAN transport router then forwards the traffic out the same data interface to send it to the alternate WAN transport router, which then forwards the traffic to the proper destination. This is referred to as hair-pinning.

The appropriate method to avoid sending the traffic out the same interface is to introduce an additional link between the routers and designate the link as a transit network (Vlan 99). There are no hosts connected to the transit network, and it is only used for router-router communication. The routing protocol runs between router subinterfaces assigned to the transit network. No additional router interfaces are required with this design modification, because the 802.1Q VLAN trunk configuration can easily accommodate an additional subinterface.
Considerations for Deploying the Cellular Remote Site

Before you begin the 3G remote-site deployment process, you need to determine which technology to leverage as you define your physical topology.

In order to decide which technology to use, consider the following questions:

- What technology is supported in the region where this remote site will be located?
  Contact your local service provider to see what technologies are in your area. For example, Europe has mandated GSM for all cellular.
- Do you want or require redundant hardware for hot swap should a failure occur?
  GSM allows you to move your SIM card from device to device without working through your service provider.
- Is high data throughput a requirement?
  Although the difference in data throughput for each technology is closing, CDMA is still the clear leader.
- Will your office move from region to region?
  If your remote site has wheels and moves around, such as a health clinic, you may wish to include both CDMA and GSM within your solution so that you may choose the best operator for your site.
- If price of service or service provider offerings are factors, which provider offers the best features/price for your remote site?
  Some service providers offer both business and wireless services to provide an alternative connection away from the public network (Internet) and drop you on your private MPLS network.
- Where security is a requirement, some service providers can provide a direct connection to customers’ MPLS networks.

GSM allows individuals to move from device to device without working through the service provider.

This guide addresses how you can leverage both technologies if your deployment is in a remote site that is on the move, possibly a disaster recovery vehicle, a mobile clinic, outdoor event data processing center, or some other truly mobile remote site. Leveraging both technologies is possible only in the few places both exist.

Where available, CDMA is currently the clear leader in data throughput.

The 3G remote-site design is based on the designs in the WAN Deployment Guide and VPN Remote Site Deployment Guide. Please refer to those guides for the configuration details for the WAN aggregation devices.

The WAN 100 design:
- Has up to 100 Mbps aggregate bandwidth
- Supports up to 100 remote sites
- Has a single MPLS carrier
- Uses a single Internet link

The WAN 500 design:
- Has up to 1 Gbps aggregate bandwidth
- Supports up to 500 remote sites
- Has multiple MPLS VPN carriers
- Uses a single Internet link

The DMVPN 100 design:
- Has up to 100 Mbps aggregate bandwidth
- Supports up to 100 remote sites
- Uses a single Internet link

The DMVPN 500 design:
- Has up to 1 Gbps aggregate bandwidth
- Supports up to 500 remote sites
- Uses dual Internet links

IP Routing

The 3G remote-site design has the following IP routing goals:

- Provide scheduled or on-demand connectivity based upon business requirements.
- Provide optimal routing connectivity from the primary WAN aggregation site to all remote locations
- Isolate WAN routing topology changes from other portions of the network

At the WAN remote sites, there is no local Internet access for web browsing or cloud services. This model is referred to as a centralized Internet model. It is worth noting that sites with Internet/DMVPN for either primary or backup
transport could potentially provide local Internet capability; however, for this design, only encrypted traffic to other DMVPN sites is permitted to use the Internet link. In the centralized Internet model, Multiple routes are advertised to the WAN remote sites: a default route as well as internal routes from the data center and campus.

**LAN Access**

In the 3G wireless remote-site design, all remote sites support both wired and wireless LAN access.

**Path Selection Preferences**

There are many potential traffic flows based on which WAN transports are in use and whether or not a remote site is using a dual WAN transport.

The single-link 3G/DMVPN connection:
- Connects to a site on the same DMVPN; the optimal route is direct within the DMVPN (only initial traffic is sent to the DMVPN hub), then is cut through via a spoke-spoke tunnel.
- Connects to any other site; the route is through the primary site.

MPLS VPN + 3G/DMVPN dual connected site:
- Connects to a site on the same MPLS VPN; the optimal route is direct within the MPLS VPN (traffic is not sent to the primary site).
- Connects to any DMVPN single-connected site; the optimal route is direct within the DMVPN (only initial traffic is sent to the DMVPN hub, then is cut-through via spoke-spoke tunnel).
- Connects to any other site; the route is through the primary site.

**Data Privacy (Encryption)**

The 3G wireless remote-site design encrypts all remote-site traffic transported over public IP networks such as the Internet.

The use of encryption should not limit the performance or availability of a remote-site application and should be transparent to end users.

**Design Parameters**

This deployment guide uses certain standard design parameters, and it references various network infrastructure services that are not located within the WAN. These parameters are listed in the following table.

**Table 4 - Universal Design Parameters**

<table>
<thead>
<tr>
<th>Network Service</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Cisco.local</td>
</tr>
<tr>
<td>Active Directory, DNS Server, DHCP</td>
<td>10.4.48.10</td>
</tr>
<tr>
<td>Authentication Control System</td>
<td>10.4.48.15</td>
</tr>
<tr>
<td>Network Time Protocol (NTP) Server</td>
<td>10.4.48.17</td>
</tr>
</tbody>
</table>

**Remote Sites—3G/DMVPN Spoke Router Selection**

The actual WAN remote-site routing platforms remain unspecified because the specification is tied closely to the bandwidth required for a location and the potential requirement for the use of service module slots. The ability to implement this solution with a variety of potential router choices is one of the benefits of a modular design approach.

There are many factors to consider in the selection of the WAN remote-site routers. Among those, and key to the initial deployment, is the ability to process the expected amount and type of traffic. Also we need to be concerned with having enough interfaces, enough module slots, and a properly licensed Cisco IOS image that supports the set of features that is required by the topology. We tested five integrated service router models as 3G/DMVPN spoke routers and the expected performance is shown in the following table.

**Table 5 - WAN Remote-Site 3G Router Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>1941¹</th>
<th>2911</th>
<th>2921</th>
<th>3925</th>
<th>3945</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet WAN with Services²</td>
<td>25 Mbps</td>
<td>35 Mbps</td>
<td>50 Mbps</td>
<td>100 Mbps</td>
<td>150 Mbps</td>
</tr>
<tr>
<td>On-board GE ports</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Service Module Slots³</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Redundant Power Supply Option</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Notes:
1. The 1941 is recommended for use at single-router, single-link remote sites.
2. The performance numbers are conservative numbers obtained when the router is passing IMIX traffic with heavy services configured and the CPU utilization is under 75 percent.
3. Some service modules are double-wide.
The compact 819 router, which is available in both hardened (819HG) and nonhardened variants (819G), is also recommended for use in 3G/DMVPN only remote sites. This router is developed specifically to support machine-to-machine applications for financial, telemetry, utility, retail, industrial automation, and transportation.

The DMVPN spoke routers at the WAN remote sites connect to the Internet directly through a 3G HWIC router interface. More details about the security configuration of the remote-site routers connected to the Internet are discussed later in this guide. The single link DMVPN remote site is the most basic of building blocks for any remote location.

The IP routing is straightforward and can be handled entirely by static routing; using static routes at the WAN-aggregation site and static default routes at the remote site. However, there is significant value to configuring this type of site with dynamic routing. It is easy to add or modify IP networks at the remote site when using dynamic routing because any changes are immediately propagated to the rest of the network.

*Figure 5 - 3G/DMVPN Remote Site (Single Link—Single Router)*

The 3G/DMVPN connection can be the primary WAN transport, or can also be the alternate to an MPLS WAN transport. The 3G/DMVPN single-link design can be added to an existing MPLS WAN design to provide additional resiliency either connecting on the same router or on an additional router. Adding an additional link provides the first level of high availability for the remote site. A failure in the primary link can be automatically detected by the router and traffic can be rerouted to the secondary path. It is mandatory to run dynamic routing when there are multiple paths. The routing protocols are tuned to ensure the desired traffic flows.

The dual-router, dual-link design continues to improve upon the level of high availability for the site. This design can tolerate the loss of the primary router and traffic can be rerouted via the secondary router (through the alternate path).

*Figure 6 - MPLS WAN + 3G/DMVPN Remote Site (Dual Link Options)*
Deployment Details

This section provides the processes for deploying the remote-site devices for a 3G/DMVPN remote site or a MPLS + DMVPN/3G remote site.

There are two variants of 3G HWIC cards available for the routers. One supports GSM and the other supports CDMA. They both use similar configurations but with minor differences. The processes that are unique to each technology type are covered first. Follow the process that matches the technology you have chosen.

After completing the technology specific tasks, proceed with the common processes that are independent of the chosen technology.

The following flowchart provides details on how to complete the configuration of a remote-site 3G/DMVPN spoke router. This flowchart applies for a single-router, single-link design (3G/DVMPN only) and for a dual-router, dual-link design (MPLS + 3G/DMVPN backup).

Figure 7 - Remote-Site 3G/DMVPN Spoke Router Configuration Flowchart

Remote-Site 3G/DMVPN Router
Single-Router, Single-Link

Remote-Site 3G/DMVPN Router
Dual-Router, Dual-Link (2nd router)

Remote-Site MPLS CE Router
Configuration Procedures

GSM

3G Technology

CDMA

1. GSM Specific
   Remote Site Router Configuration

1. CDMA Specific
   Remote Site Router Configuration

1. Finish the WAN Router Universal Configuration
2. Configure VRF Lite
3. Configure the Cellular Interface
4. Configure the Dialer Interface
5. Configure VRF-Specific Default Routing
6. Apply the Access List
7. Configure SA/MP and IPSec
8. Configure mGRE Tunnel
9. Configure OSPF
10. Configure IP Multicast

NO

Dual Router Design?

YES

11. Configure Access Layer Routing
12. Configure Access Layer HSRP
13. Configure Transit Network
14. Configure ESRP (LAN Side)

Site Complete

Site Complete
The following flowchart provides details on how to add 3G/DMVPN backup on an existing remote-site MPLS CE router. This specifically applies for a single-router, dual-link design (MPLS + 3G/DMVPN backup). It is assumed that the MPLS CE router has already been configured using the guidance provided in the *Smart Business Architecture—Borderless Networks for Enterprise Organizations WAN Deployment Guide*.

**Figure 8 - Adding 3G/DMVPN Backup to an Existing Remote-Site Router Configuration Flowchart**

1. **Process**
   - GSM Specific—Remote Site Router Configuration
     1. Install GSM HWIC into ISR
     2. Configure Chat Script and GSM Profile

You must get a data service account from your service provider. You should receive a SIM card that you should install on the 3G-HWIC. You will also receive the following information: PPP CHAP User-Name (hostname), PPP CHAP Password, APN (access point name).

**Procedure 1** Install GSM HWIC into ISR

**Figure 9 - GSM HWIC SIM card installation**

Step 1: Insert SIM card into HWIC.

Step 2: Power off the Integrated Services Router G2.
Step 3: Insert and fasten GSM HWIC into the router.

Step 4: Power on the router and begin configuration.

**Procedure 2  Configure Chat Script and GSM Profile**

Chat scripts are strings of text used to send commands for modem dialing, to log in to remote systems, and to initialize asynchronous devices connected to an asynchronous line. The 3G WAN interface should be treated just like any other asynchronous interface.

The following chat script shows the required information to connect to the AT&T GSM network.

**Step 1:** This chat script uses a carrier specific dial string and a timeout value of 30 seconds. Note that your carrier may require a different chat script.

```
chat-script [Script-Name] [Script]
```

Example for Step 1:

```
chat-script GSM "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
```

**Step 2:** Apply chat-script to the async line.

```
line [Cellular-Interface-Number]
script dialer [Script-Name]
```

Example for Step 2:

For the interface cellular0/0/0, the matching line would be:

```
line 0/0/0
script dialer GSM
```

**Step 3:** Create the GSM Profile

```
cellular [Cellular-Interface] gsm profile create [sequence-Number] [AP-Name] chap [username] [password]
```

Example for Step 3:

From enable mode, use the profile to identify the username and password provided to you by your service provider. Use the cellular interface identifier and the keyword GSM.

---

**Tech Tip**

This step should be completed from enable mode and not from configuration mode.

```
cellular 0/0/0 gsm profile create 1 isp.cingular chap ISP@CINGULARGPRS.COM CINGULAR1
```

**Process**

**CDMA Specific - Remote Site Router Configuration**

1. Install CDMA HWIC into ISR
2. Activate the CDMA Modem
3. Configure Chat Script

The CDMA deployment is different from the GSM deployment. The use of a profile is not required.

*Figure 10 - CDMA HWIC ESN Location*
Deployment Details

You must obtain wireless data services and ensure the HWIC has been registered with the wireless service provider’s network. The service provider will provide an activation number to call to activate the modem.

**Tech Tip**

**Procedure 1** Install CDMA HWIC into ISR

- **Step 1:** Register CDMA HWIC with SP using the ESN number found on the HWIC.
- **Step 2:** Power off the Integrated Services G2 Router.
- **Step 3:** Insert and fasten CDMA HWIC into the router. Power on the router and begin configuration.

**Procedure 2** Activate the CDMA Modem

- **Step 1:** Before using your CDMA HWIC, it must be activated. Using the activation number provided by the CDMA carrier, proceed with the following step.
  
  ```
  cellular [interface number] cdma activate otasp [activation number]
  ```

  Example (for Verizon CDMA network):
  ```
  Router# cellular 0/0/0 cdma activate otasp *22899
  ```

- **Step 2:** Apply chat-script to the async line
  ```
  line [Cellular-Interface-Number] script dialer [Script-Name]
  ```

  Example for Step 2:
  ```
  For the interface cellular0/0/0, the matching line would be:
  line 0/0/0
  script dialer CDMA
  ```

**Procedure 3** Configure Chat Script

Chat scripts are strings of text used to send commands for modem dialing, to log in to remote systems, and to initialize asynchronous devices connected to an asynchronous line. The 3G WAN interface should be treated just like any other asynchronous interface.

The following chat script shows the required information to connect to the Verizon CDMA network.

**Step 1:** This chat script uses a carrier specific dial string and a timeout value of 30 seconds. Note that your carrier may require a different chat script.

```
chat-script [Script-Name] [Script]
```

**Example for Step 1:**

```
chat-script CDMA "\"atdt#777\" TIMEOUT 30 \"CONNECT\"
```

**Step 2:**

Apply chat-script to the async line

```
line [Cellular-Interface-Number] script dialer [Script-Name]
```

**Example for Step 2:**

For the interface cellular0/0/0, the matching line would be:

```
line 0/0/0
script dialer CDMA
```
Remote-Site 3G/DMVPN Router Configuration

1. Finish WAN Router Universal Configuration
2. Configure VRF-lite
3. Configure the Cellular Interface
4. Configure the Dialer Interface
5. Configure VRF-Specific Default Routing
6. Apply the Access List
7. Configure ISAKMP and IPsec
8. Configure the mGRE Tunnel
9. Configure EIGRP
10. Configure IP Multicast Routing
11. Configure Access Layer Routing
12. Configure Access Layer HSRP
13. Configure Transit Network
14. Configure EIGRP (LAN Side)

This set of procedures is for the configuration of a 3G/DMVPN spoke router for a remote site that uses either GSM or CDMA technology. Procedure 1 and Procedure 11 are not required when adding a 3G/DMVPN backup on an existing MPLS CE router. Otherwise, complete Procedure 1 through Procedure 11 for all cases, and additionally Procedure 12 through Procedure 14 when configuring the dual-router option.

**Process**

**Procedure 1**  Finish WAN Router Universal Configuration

**Reader Tip**

Skip this procedure when adding a 3G/DMVPN backup on an existing MPLS CE router.

**Step 1:** Configure the device hostname.

   hostname [hostname]

**Step 2:** Configure in-band management interface.

All devices leverage a loopback address. A loopback is a virtual interface that is consistently reachable when multiple paths exist to the device. Various other features may use the loopback.

   interface Loopback0
   ip address [IP address] 255.255.255.255

**Step 3:** Configure device-management protocols.

SSH is an application and a protocol that provides a secure replacement to RSH and Telnet. Secure management access is enabled through the use of the SSH and/or HTTPS protocols. HTTPS provides the capability to connect a HTTP server securely. It uses SSL and TLS to provide device authentication and data encryption. Both protocols are encrypted for privacy and the non-secure protocols, Telnet and HTTP, have been disabled.

   ip domain-name cisco.local
   no ip http server

Enabling SSH requires that a public/private keypair be generated for the device:

   crypto key generate rsa modulus 2048
   ip ssh version 2
   ip ssh source-interface Loopback0
Various levels of device management may be available through a web interface. For secure access to this interface you must enable the secure server (the following command also generates a public/private keypair as shown previously):

```
ip http secure-server
```

Allow only SSH access to the device:

```
line vty 0 15
transport input ssh
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. This command is also useful for allowing you to continue typing at the device console when debugging is enabled.

```
line con 0
logging synchronous
```

SNMP is enabled to allow the network infrastructure devices to be managed by a NMS. SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
```

**Step 4:** Configure secure user authentication.

AAA is enabled for access control. All management access to the network infrastructure devices (SSH, Telnet, HTTP, and HTTPS) is controlled with AAA. A local AAA user database is defined on the network infrastructure devices to provide the ability to manage them in case the centralized RADIUS server is unavailable or you do not have a RADIUS server in your organization. We highly recommend the use of a centralized authentication database.

```
enable secret cisco123
service password-encryption
!
username admin password cisco123
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
ip tacacs source-interface Loopback0
tacacs-server host 10.4.48.15 key SecretKey
```

**Step 5:** Configure a synchronized clock.

NTP is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

Network devices should be programmed to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. Configuring console messages, logs, and debug output on switches, routers, and other devices in the network to provide timestamps on output allows cross-referencing of events in a network.

```
ntp server 10.4.48.17
ntp source Loopback0
ntp update-calendar
!
clock timezone PST -8

clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

**Procedure 2** Configure VRF-lite

An Internet-facing VRF is created to support the front door VRF for DMVPN. The VRF name is arbitrary, but it is useful to select a name that describes the VRF. To make the VRF functional, you must also configure an associated RD. The RD configuration also creates the routing and forwarding tables and associates the RD with the VRF instance.

This design uses VRF-lite so you can arbitrarily choose the RD value. It is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

An RD is one of two types:

- **ASN-related**—Composed of an ASN and an arbitrary number.
- **IP-address-related**—Composed of an IP address and an arbitrary number.
Step 1: Enter an RD in either of these formats:
- 16-bit autonomous-system-number: your 32-bit number
  For example, 65512:1
- 32-bit IP address: your 16-bit number
  For example, 192.168.122.15:1.

```
ip vrf [vrf-name]
  rd [ASN:number]
```

Example for Procedure 2:
```
ip vrf INET-PUBLIC
  rd 65512:1
```

**Procedure 3  Configure the Cellular Interface**

The cellular interface is added to a dialer pool and all additional configuration parameters are assigned to the dialer interface in a subsequent procedure. The bandwidth value is set to match the uplink speed of the chosen technology.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Maximum Downlink speed (Kbps)</th>
<th>Maximum Uplink speed (Kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM 3G</td>
<td>3600</td>
<td>384</td>
</tr>
<tr>
<td>CDMA 3G</td>
<td>3100</td>
<td>1800</td>
</tr>
</tbody>
</table>

Step 1: Assign physical interface to dialer pool:
```
interface Cellular [Interface-Number]
  bandwidth [bandwidth (Kbps)]
  no ip address
  encapsulation ppp
  dialer in-band
  dialer pool-member [Dialer Pool Number]
  no peer default ip address
  async mode interactive
  no shutdown
```

Example for Procedure 3 (bandwidth shown for GSM 3G):
```
interface Cellular0/0/0
  bandwidth 384
  no ip address
  encapsulation ppp
  dialer in-band
  dialer pool-member 1
  no peer default ip address
  async mode interactive
  no shutdown
```

**Procedure 4  Configure the Dialer Interface**

The Dialer interface is a logical interface that allows control over a pool of one or more physical interfaces. The usage of a Dialer interfaces provides consistency of configuration that is independent of the type of underlying physical interface and the associated interface numbering.

Step 1: Assign VRF and dialer parameters
```
interface Dialer [Dialer Interface Number]
  bandwidth [bandwidth (Kbps)]
  ip vrf forwarding [vrf name]
  dialer pool [Dialer Pool Number]
  dialer idle-timeout 0
  dialer string [Chat Script Name]
  dialer persistent
  no shutdown
```

**Tech Tip**

The CHAT script used as the dialer string has already been created in a previous process.
- For GSM networks use: GSM
- For CDMA networks use: CDMA
Step 2: Assign basic PPP parameters

```
interface Dialer [Dialer Interface Number]
  ip address negotiated
  encapsulation ppp
  ppp ipcp address accept
  ppp timeout retry 120
  ppp timeout ncp 30
```

Step 3: Assign PPP authentication parameters. This step is only required for routers using GSM technology.

**Tech Tip**

PPP authentication information is provided by your GSM service provider. It is not necessary to configure PPP CHAP hostname and password for routers using CDMA technology.

```
interface Dialer [Dialer Interface Number]
  ppp chap hostname [PPP CHAP username for GSM]
  ppp chap password [PPP CHAP password for GSM]
```

Procedure 4 Example:

```
interface Dialer1
  bandwidth 384
  ip vrf forwarding INET-PUBLIC
  ip address negotiated
  encapsulation ppp
  dialer pool 1
  dialer idle-timeout 0
  dialer string GSM ! This example shows GSM (vs CDMA)
  dialer persistent
  ppp chap hostname ISP@CINGULARGPRS.COM ! Required for GSM only
  ppp chap password CINGULAR1 ! Required for GSM only
  ppp ipcp address accept
```

Procedure 5 Configure VRF-Specific Default Routing

The remote sites using 3G/DMVPN use PPP negotiated IP addresses for the dialer interfaces. Unlike DHCP, the PPP negotiation does not automatically set a default route. This step must be completed manually.

**Step 1:** Configure a VRF specific default route for the dialer interface.

```
ip route vrf [vrf name] 0.0.0.0 0.0.0.0 [interface type] [number]
```

**Example:**

```
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 Dialer1
```

Procedure 6 Apply the Access List

The 3G/DMVPN spoke router connects directly to the Internet without a separate firewall. This connection is secured in two ways. Because the Internet interface is in a separate VRF, no traffic can access the global VRF except traffic sourced through the DMVPN tunnel. This design provides implicit security. Additionally, an IP access list permits only the traffic required for an encrypted tunnel, as well as various ICMP protocols for troubleshooting.

**Step 1:** Apply the access list.

The IP access list must permit the protocols specified in the following table. The access list is applied inbound on the WAN interface, so filtering is done on traffic destined to the router.

**Table 6 - Required DMVPN Protocols**

<table>
<thead>
<tr>
<th>Name</th>
<th>Protocol</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>non500-isakmp</td>
<td>UDP 4500</td>
<td>IPsec via NAT-T</td>
</tr>
<tr>
<td>isakmp</td>
<td>UDP 500</td>
<td>ISAKMP</td>
</tr>
<tr>
<td>esp</td>
<td>IP 50</td>
<td>IPsec</td>
</tr>
</tbody>
</table>
Example access list:

```
interface [interface type] [number]
ip access-group [ACL name] in
ip access-list extended [ACL name]
  permit udp any any eq non500-isakmp
  permit udp any any eq isakmp
  permit esp any any
```

The additional protocols listed in the following table may assist in trouble-shooting, but are not explicitly required to allow DMVPN to function properly.

**Table 7 - Optional Access-List Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Protocol</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp echo</td>
<td>ICMP type 0, code 0</td>
<td>Allow remote pings</td>
</tr>
<tr>
<td>icmp echo-reply</td>
<td>ICMP type 8, code 0</td>
<td>Allow ping replies</td>
</tr>
<tr>
<td>icmp ttl-exceeded</td>
<td>ICMP type 11, Code0</td>
<td>Windows traceroute</td>
</tr>
<tr>
<td>icmp port-unreachable</td>
<td>ICMP type 3, code 3</td>
<td>Service unreachable</td>
</tr>
</tbody>
</table>

The additional optional entries for an access list to support ping are as follows:

```
    permit icmp any any echo
    permit icmp any any echo-reply
```

The additional optional entries for an access list to support a Windows traceroute are as follows:

```
    permit icmp any any ttl-exceeded ! traceroute (sourced)
    permit icmp any any port-unreachable ! traceroute (sourced)
```

Example for Procedure 6:

```
interface Dialer1
  ip access-group [ACL name] in
  ip access-list extended [ACL name]
  permit udp any any eq non500-isakmp
  permit udp any any eq isakmp
  permit esp any any
  permit icmp any any echo
  permit icmp any any echo-reply
```

---

**Procedure 7** Configure ISAKMP and IPsec

**Step 1:** Configure the crypto keyring.

The crypto keyring defines a pre-shared key (or password) valid for IP sources reachable within a particular VRF. If it applies to any IP source, this key is a wildcard pre-shared key. You configure a wildcard key by using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring [keyring name] vrf [vrf name]
  pre-shared-key address 0.0.0.0 0.0.0.0 key [pre-shared key]
```

**Step 2:** Configure the ISAKMP Policy and Dead Peer Detection.

- The ISAKMP policy for DMVPN uses the following:
  - AES with a 256-bit key
  - SHA
  - Authentication by pre-shared key
  - Diffie-Hellman group: 2

DPD is enabled with keepalives sent at 30-second intervals with a 5-second retry interval, which is considered to be a reasonable setting to detect a failed hub.

```
crypto isakmp policy 10
  encr aes 256
  hash sha
  authentication pre-share
  group 2
  !
  crypto isakmp keepalive 30 5
```

**Step 3:** Create the ISAKMP profile.

The ISAKMP profile creates an association between an identity address, a VRF and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0.

```
crypto isakmp profile [ISAKMP profile name]
  keyring [keyring name]
  match identity address 0.0.0.0 [vrf name]
```
Step 4: Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Since the DMVPN hub router is behind a NAT device, the IPsec transform set must be configured for transport mode. This transform set has already been created for use in the single-router, single-link configuration, but is included here for completeness.

```
crypto ipsec transform-set [IPSec transform-set name] esp-aes
256 esp-sha-hmac
mode transport
```

Step 5: Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile [IPSec profile name]
  set transform-set [IPSec transform-set name]
  set isakmp-profile [ISAKMP profile name]
```

Example for Procedure 7:

```
crypto keyring DMVPN-KEYRING vrf INET-PUBLIC
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto isakmp policy 10
  encr aes 256
  hash sha
  authentication pre-share
  group 2
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
  keyring DMVPN-KEYRING
  match identity address 0.0.0.0 INET-PUBLIC
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
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
```

Procedure 8 Configure the mGRE Tunnel

Step 1: Configure basic interface settings.

Tunnel interfaces are created as they are configured. The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

Set the bandwidth setting to match the Internet bandwidth.

The IP MTU should be configured to 1400 and the ip tcp adjust-mss should be configured to 1360. There is a 40 byte difference, which corresponds to the combined IP and TCP header length.

```
interface Tunnel [number]
  bandwidth [bandwidth (kbps)]
  ip address [IP address] [netmask]
  no ip redirects
  ip mtu 1400
  ip tcp adjust-mss 1360
```

Step 2: Configure the tunnel.

DMVPN uses multipoint GRE (mGRE) tunnels. This type of tunnel requires a source interface only. The source interface should be the same interface used to connect to the Internet. The tunnel vrf command should be set to the VRF defined previously for Front Door VRF.

Enabling encryption on this interface requires the application of the IPsec profile configured in the previous procedure.

```
interface Tunnel [number]
  tunnel source [source interface]
  tunnel mode gre multipoint
  tunnel vrf [vrf name]
  tunnel protection ipsec profile [IPSec profile name]
```

Step 3: Configure NHRP.

The DMVPN hub router is the NHRP server for all of the spokes. NHRP is used by remote routers to determine the tunnel destinations for peers attached to the mGRE tunnel.
The spoke router requires several additional configuration statements to define the NHRP server (NHS) and NHRP map statements for the DMVPN hub router mGRE tunnel IP address. EIGRP (configured in Procedure 9) relies on a multicast transport. Spoke routers require the NHRP static multicast mapping.

The value used for the NHS is the mGRE tunnel address for the DMVPN hub router. The map entries must be set to the outside NAT value of the DMVPN hub, as configured on the Cisco ASA5500. This design uses the values shown in the following table.

### Table 8 - DMVPN Hub IP Address Information

<table>
<thead>
<tr>
<th>DMVPN Cloud</th>
<th>DMVPN Hub Public Address (Actual)</th>
<th>DMVPN Hub Public Address (Externally routable after NAT)</th>
<th>NHS (DMVPN Hub mGRE Tunnel Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.4.32.133</td>
<td>172.16.130.1</td>
<td>10.4.34.1</td>
</tr>
</tbody>
</table>

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. The NHRP cache holdtime should be configured to 600 seconds.

This design supports DMVPN spoke routers that receive their external IP addresses through DHCP. It is possible for these routers to acquire different IP addresses after a reload. When the router attempts to register with the NHRP server, it may appear as a duplicate to an entry already in the cache and be rejected. The registration no-unique option allow existing cache entries to be overwritten. This feature is only required on NHRP clients (3G/DMVPN spoke routers).

The `ip nhrp redirect` command allows the DMVPN hub to notify spoke routers that a more optimal path may exist to a destination network, which may be required for DMVPN spoke-to-spoke direct communications. DMVPN spoke routers also use shortcut switching when building spoke-to-spoke tunnels.

### Example for Procedure 8:

```conf
interface Tunnel10
  bandwidth 384
  ip address 10.4.34.220 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip hello-interval eigrp 200 20
  ip hold-time eigrp 200 60
  ip nhrp authentication cisco123
  ip nhrp map 10.4.34.1 172.16.130.1
  ip nhrp map multicast 172.16.130.1
  ip nhrp network-id 101
  ip nhrp holdtime 600
  ip nhrp nhs 10.4.34.1
  ip nhrp registration no-unique
```
Deployment Details

Procedure 9 Configure EIGRP

An single EIGRP process runs on the DMVPN spoke router. All interfaces on the router are EIGRP interfaces, but only the DMVPN tunnel interface is non-passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. All DMVPN spoke routers should run EIGRP stub routing to improve network stability and reduce resource utilization.

Step 1: Assign the router ID to a loopback address.

```
router eigrp [as number (dmvpn)]
  network [mGRE tunnel network] [inverse mask]
  network [WAN remote range] [inverse mask]
  passive-interface default
  no passive-interface [mGRE tunnel interface]
  eigrp router-id [IP address of Loopback0]
  eigrp stub connected summary
  no auto-summary
```

Example for Procedure 9:

```
router eigrp 200
  network 10.4.34.0 0.0.1.255
  network 10.5.0.0 0.0.255.255
  passive-interface default
  no passive-interface Tunnel10
  eigrp router-id 10.5.216.254
  eigrp stub connected summary
  no auto-summary
```

Procedure 10 Configure IP Multicast Routing

In this design, which is based on sparse mode multicast operation, Auto-RP is used to provide a simple yet scalable way to provide a highly resilient multicast environment.

This procedure applies to all DMVPN spoke routers.

Step 1: Enable IP multicast routing on the platforms in the global configuration mode.

```
   ip multicast-routing
```

Step 2: Every router must be configured to discover the IP multicast RP with autorp. Use the `ip pim autorp listener` command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP multicast environment and can change based on network needs and design. The PIM source is configured to be the device loopback for resiliency at sites with multiple WAN transports.

```
   ip pim autorp listener
   ip pim register-source Loopback0
```

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.

Do not enable PIM on the Internet (dialer) interface, as no multicast traffic should be requested from this interface.

```
   interface [interface type] [number]
     ip pim sparse-mode
```

Step 3: Enable PIM non-broadcast multiple access mode for the DMVPN tunnel.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This inability to directly exchange information can also cause problems when running IP multicast.

Resolving the NBMA issue requires a method where each remote PIM neighbor has its join messages tracked separately. A router in PIM NBMA mode treats each remote PIM neighbor as if it were connected to the router through a point-to-point link.

```
   interface Tunnel [number]
     ip pim nbma-mode
```
Step 4: Configure the Designated Router (DR) priority for the DMVPN spoke router.

Proper multicast operation across a DMVPN cloud requires that the hub router assumes the role of PIM Designated Router (DR). Spoke routers should never become the DR. This can be prevented by setting the DR priority to 0 for the spokes.

```
interface Tunnel [number]
ip pim dr-priority 0
```

Example for Procedure 10:

```
ip multicast-routing
!
interface Loopback0
  ip pim sparse-mode
!
interface GigabitEthernet0/2.64
  ip pim sparse-mode
!
interface GigabitEthernet0/2.65
  ip pim sparse-mode
!
interface Tunnel10
  ip pim dr-priority 0
  ip pim nbma-mode
  ip pim sparse-mode
!
ip pim autorp listener
ip pim register-source Loopback0
```

Procedure 11: Configure Access Layer Routing

Skip this procedure when adding a 3G/DMVPN backup on an existing MPLS CE router.

In the access layer design, the remote-sites use collapsed routing, with 802.1Q trunk interfaces to the LAN access layer. The VLAN numbering is locally significant only. The access switches are Layer 2 only.

Step 1: Enable the physical interface.

```
interface [interface type] [number]
  no ip address
  no shutdown
```

Step 2: Create subinterfaces and assign VLAN tags.

After the physical interface has been enabled, then the appropriate data or voice subinterfaces can be mapped to the VLANs on the LAN switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration. The subinterface portion of the configuration should be repeated for all data or voice VLANs.

```
interface [interface type] [number].[sub-interface number]
  encapsulation dot1Q [dot1q VLAN tag]
```

Step 3: Configure IP settings for each subinterface.

This design uses an IP addressing convention with the default gateway router assigned an IP address and IP mask combination of N.N.N.1 255.255.255.0 where N.N.N is the IP network and 1 is the IP host.

All router LAN interfaces that use DHCP for end-station IP assignment must use an IP helper to reach a centralized DHCP server in this design.

If the remote-site 3G/DMVPN spoke router is the second router of a dual-router design then HSRP is configured at the access layer. This requires a modified IP configuration on each subinterface.
For the modified procedure, you should skip to Procedure 12 after completing Steps 1 and 2.

interface [interface type] [number].[sub-interface number]
capsulation dot1Q [dot1q VLAN tag]
ip address [LAN network 1] [LAN network 1 netmask]
ip helper-address [IP address of DHCP server]

Example for Procedure 11:

interface GigabitEthernet0/2
no ip address
no shutdown
!

interface GigabitEthernet0/2.64
description Data
capsulation dot1Q 64
ip address 10.5.220.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!

interface GigabitEthernet0/2.65
description WirelessData
capsulation dot1Q 65
ip address 10.5.218.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!

The following procedures (Procedure 12 through Procedure 14) are only relevant for the dual-router design.

### Procedure 12 - Configure Access Layer HSRP

**Tech Tip**

In the dual-router design, the primary MPLS-CE router configuration details are documented in the *Smart Business Architecture—Borderless Networks for Enterprise Organizations WAN Deployment Guide*. The following procedures include examples for the secondary 3G/DMVPN router only.

**Tech Tip**

In the dual-router design, the primary MPLS-CE router configuration details are documented in the *Smart Business Architecture—Borderless Networks for Enterprise Organizations WAN Deployment Guide*. The following procedures include examples for the secondary 3G/DMVPN router only.

**Tech Tip**

In the dual-router design, the primary MPLS-CE router configuration details are documented in the *Smart Business Architecture—Borderless Networks for Enterprise Organizations WAN Deployment Guide*. The following procedures include examples for the secondary 3G/DMVPN router only.

The dual-router access-layer design requires a modification for resilient multicast. The PIM DR should be on the HSRP active router. The DR is normally elected based on the highest IP address and has no awareness of the HSRP configuration. In this design, the HSRP active router has a lower real IP address than the HSRP standby router, which requires a modification to the PIM configuration. The PIM DR election can be influenced by explicitly setting the DR priority on the LAN-facing subinterfaces for the routers.

**Procedure 12 - Configure Access Layer HSRP**

(Dual-Router Design Only)

HSRP is configured to enable a VIP to be used as a default gateway that is shared between two routers. The HSRP active router is the MPLS CE router connected to the primary MPLS carrier and the HSRP standby router is the 3G/DMVPN spoke router. Configure the HSRP standby router with a standby priority that is lower than the HSRP active router.

The router with the higher standby priority value is elected as the HSRP active router. The preempt option allows a router with a higher priority to become the HSRP active, without waiting for a scenario where there is no router in the HSRP active state. The relevant HSRP parameters for the router configuration are shown in the following table.

<table>
<thead>
<tr>
<th>Router</th>
<th>HSRP Role</th>
<th>Virtual IP Address (VIP)</th>
<th>Real IP Address</th>
<th>HSRP Priority</th>
<th>PIM DR Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS CE</td>
<td>Active</td>
<td>.1</td>
<td>.2</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>(primary)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3G/DMVPN Spoke</td>
<td>Standby</td>
<td>.1</td>
<td>.3</td>
<td>105</td>
<td>105</td>
</tr>
</tbody>
</table>

Table 9 - WAN Remote-Site HSRP Parameters (Dual Router)
Deployment Details

The HSRP priority and PIM DR priority are shown in the previous table to be the same value; however there is no requirement that these values must be identical.

Tech Tip

This procedure should be repeated for all data or voice subinterfaces.

```
interface [interface type] [number].[sub-interface number]
encapsulation dot1Q [dot1q VLAN tag]
ip address [LAN network 1 address] [LAN network 1 netmask]
ip helper-address [IP address of DHCP server]
ip pim sparse-mode
ip pim dr-priority [PIM DR priority]
standby [number] ip [LAN network 1 gateway address]
standby [number] priority [priority]
standby [number] preempt
```

Example—3G/DMVPN Spoke Router:

```
interface GigabitEthernet0/2.64
description Data
encapsulation dot1Q 64
ip address 10.5.28.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby 1 ip 10.5.28.1
standby 1 priority 105
standby 1 preempt
```

Procedure 13 Configure Transit Network

(Dual-Router Design Only)
The transit network is configured between the two routers. This network is used for router-router communication and to avoid hair-pinning. The transit network should use an additional subinterface on the router interface that is already being used for data or voice.

There are no end stations connected to this network, so HSRP and DHCP are not required.

```
interface [interface type] [number].[sub-interface number]
encapsulation dot1Q [dot1q VLAN tag]
ip address [transit net address] [transit net netmask]
```

Example—3G/DMVPN Spoke Router:

```
interface GigabitEthernet0/2.99
description Transit Net
encapsulation dot1Q 99
ip address 10.5.24.2 255.255.255.252
```
(Dual-Router Design Only)

A routing protocol must be configured between the two routers. This ensures that the HSRP active router has full reachability information for all WAN remote sites.

**Step 1:** Enable EIGRP-100.

EIGRP-100 is configured facing the access layer. In this design, all LAN-facing interfaces and the loopback must be EIGRP interfaces. All interfaces except the transit-network subinterface should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. Do not include the WAN interface (MPLS PE-CE link interface) as an EIGRP interface.

```
router eigrp [as number]
  network [network] [inverse mask]
  passive-interface default
  no passive-interface [interface]
eigrp router-id [IP address of Loopback0]
  no auto-summary
```

**Step 2:** Redistribute EIGRP-200 (DMVPN) into EIGRP-100.

This step should only be completed on the 3G/DMVPN spoke router. EIGRP-200 is already configured for the DMVPN mGRE interface. Routes from this EIGRP process are redistributed. Since the routing protocol is the same, no default metric is required.

```
router eigrp [as number]
  redistribute eigrp [as number (DMVPN)]
```

**Example—3G/DMVPN Spoke Router:**

`router eigrp 100`
`  network 10.5.0.0 0.0.255.255`
`  redistribute eigrp 200`
`  passive-interface default`
`  no passive-interface GigabitEthernet0/1.99`
`  eigrp router-id 10.5.24.253`
`  no auto-summary`

---

**Process**

Control Usage of 3G Interface

1. Schedule Auto-Control of 3G Interface
2. Monitor Reachability of Upstream Router

Many 3G service providers do not offer a mobile data plan with unlimited usage. More typically, you will need to select a usage based plan with a bandwidth tier that aligns with the business requirements for the remote site. To minimize recurring costs of the 3G solution, it is a best practice to limit the use of the 3G wireless WAN specifically to the periods where it must active.

A 3G/DMVPN only site can be manually controlled, but if operation on a regular schedule is required, the router can be configured to activate the 3G as a primary link according to repeating weekly schedule. This method is detailed in Procedure 1.

The remote-sites, which use 3G/DMVPN as a secondary transport, can track the status of the primary MPLS link and activate the 3G as a secondary link when necessary. This method is detailed in Procedure 2.

**Procedure 1** Schedule Auto-Control of 3G Interface

**Step 1:** This procedure should be used to control the 3G interface usage for the single-link design. The 3G interface is controlled using the Embedded Event Manager time-based scheduling using cron.
Step 2: Configure EEM Scripting to Enable or Disable 3G Interface.

A cron EEM script is activated based on a schedule and runs specified router IOS commands at period intervals. It is also a best practice to generate syslog messages that provide status information regarding EEM. The syntax of the cron entry is consistent with other commonly used applications such as UNIX.

```
event manager applet [EEM script name]
  event timer cron cron-entry "[min] [hr] [day of month]
  [month] [day of week]"
  action [sequence 1] cli command "[command 1]"
  action [sequence 2] cli command "[command 2]"
  action [sequence 3] cli command "[command 3]"
  action [sequence ...] cli command "[command ...]"
  action [sequence N] syslog msg "[syslog message test]"
```

Example for Procedure 1:

EEM script to enable 3G interface at the beginning of a work day (Monday-Friday at 4:45AM):

```
event manager applet TIME-OF-DAY-ACTIVATE-3G
  event timer cron cron-entry "45 4 * * 1-5"
  action 1 cli command "enable"
  action 2 cli command "configure terminal"
  action 3 cli command "interface cellular0/0/0"
  action 4 cli command "no shutdown"
  action 5 cli command "end"
  action 99 syslog msg "M-F @ 4:45AM Activating 3G interface"
```

EEM script to disable 3G at the end of a work day (Monday-Friday at 6:15PM):

```
event manager applet TIME-OF-DAY-DEACTIVATE-3G
  event timer cron cron-entry "15 18 * * 1-5"
  action 1 cli command "enable"
  action 2 cli command "configure terminal"
  action 3 cli command "interface cellular0/0/0"
  action 4 cli command "shutdown"
  action 5 cli command "end"
  action 99 syslog msg "M-F @ 6:15PM Deactivating 3G interface"
```

Procedure 2

Monitor Reachability of Upstream Router

This procedure should be used to control the 3G interface usage for the dual-link designs (single-router, dual-link and dual-router, dual-link). The MPLS VPN is the primary WAN transport, and as long as it is operational, the 3G interface remains shut down.

The remote-site 3G/DMVPN router can use the IP SLA feature to send echo probes to the site’s MPLS PE router, and if the PE router becomes unreachable, then the router can use the Embedded Event Manager (EEM) to dynamically enable the 3G interface.

Step 1: Enable the IP SLA probe.

Standard ICMP echo (ping) probes are used, and are sent at 15 second intervals. Responses must be received before the timeout of 1000 ms expires. If using the MPLS PE router as the probe destination, the destination address is the same as the BGP neighbor address already configured. If using the single-router, dual-link design, then use the MPLS WAN interface as the probe source-interface. If using the dual-router, dual-link design then use the transit-net subinterface as the probe source-interface.

```
  ip sla [probe number]
    icmp-echo [probe destination IP address] source-interface
    [interface]
    timeout 1000
    threshold 1000
    frequency 15
  ip sla schedule [probe number] life forever start-time now
```

Step 2: Configure Enhanced Object Tracking.

This step links the status of the IP SLA probe to an object which is monitored by EEM scripts.

```
  track [object number] ip sla [probe number] reachability
```
Step 3: Configure EEM Scripting to Enable or Disable 3G Interface

An event tracking EEM script monitors the state of an object and runs router IOS commands for that particular state. It is also a best practice to generate syslog messages that provide status information regarding EEM.

```
event manager applet [EEM script name]
    event track [object number] state [tracked object state]
    action [sequence 1] cli command "[command 1]"
    action [sequence 2] cli command "[command 2]"
    action [sequence 3] cli command "[command 3]"
    action [sequence …] cli command "[command …]"
    action [sequence N] syslog msg "[syslog message test]"
```

Example for Procedure 2:

```
track 60 ip sla 100 reachability
ip sla 100
    icmp-echo 192.168.4.18 source-interface GigabitEthernet0/0
    threshold 1000
    frequency 15
ip sla schedule 100 life forever start-time now
```

EEM script to enable 3G interface upon MPLS link failure:

```
event manager applet ACTIVATE-3G
    event track 60 state down
    action 1 cli command "enable"
    action 2 cli command "configure terminal"
    action 3 cli command "interface cellular0/0/0"
    action 4 cli command "no shutdown"
    action 5 cli command "end"
    action 99 syslog msg "Primary Link Down - Activating 3G interface"
```

EEM script to disable 3G interface upon MPLS link restoration:

```
event manager applet DEACTIVATE-3G
    event track 60 state up
    action 1 cli command "enable"
    action 2 cli command "configure terminal"
    action 3 cli command "interface cellular0/0/0"
    action 4 cli command "shutdown"
    action 5 cli command "end"
    action 99 syslog msg "Primary Link Restored - Deactivating 3G interface"
```
## Appendix A: 3G Wireless Remote Site Product List

<table>
<thead>
<tr>
<th>WAN Remote Site Routers</th>
<th>15.1(4)M4</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1941-WAASX-SEC/K9</td>
<td>c1900-universalk9-mz.SPA.151-4.M4.bin</td>
</tr>
<tr>
<td>FL-C1941-WAASX</td>
<td></td>
</tr>
<tr>
<td>MEM-1900-512U2.5GB</td>
<td></td>
</tr>
<tr>
<td>EHWIC-3G-EVDO-V</td>
<td></td>
</tr>
<tr>
<td>HWIC-3G-CDMA</td>
<td></td>
</tr>
<tr>
<td>HWIC-3G-GSM</td>
<td></td>
</tr>
<tr>
<td>CISCO2911-VSEC/K9</td>
<td>c2900-universalk9-mz.SPA.151-4.M4.bin</td>
</tr>
<tr>
<td>EHWIC-3G-EVDO-V or</td>
<td></td>
</tr>
<tr>
<td>HWIC-3G-CDMA or</td>
<td></td>
</tr>
<tr>
<td>HWIC-3G-GSM</td>
<td></td>
</tr>
<tr>
<td>CISCO2921-VSEC/K9</td>
<td>c2900-universalk9-mz.SPA.151-4.M4.bin</td>
</tr>
<tr>
<td>EHWIC-3G-EVDO-V or</td>
<td></td>
</tr>
<tr>
<td>HWIC-3G-CDMA or</td>
<td></td>
</tr>
<tr>
<td>HWIC-3G-GSM</td>
<td></td>
</tr>
<tr>
<td>CISCO819G-S-K9 or</td>
<td>15.1(4)M1</td>
</tr>
<tr>
<td>CISCO819HG-S-K9</td>
<td>c800-universalk9-mz.SPA.151-4.M1.bin</td>
</tr>
<tr>
<td>(Other variants available - select the model required by your carrier and geographic location)</td>
<td></td>
</tr>
<tr>
<td>CISCO819G-x-K9 or</td>
<td></td>
</tr>
<tr>
<td>CISCO819HG-x-K9</td>
<td></td>
</tr>
</tbody>
</table>
Appendix B: Configuration

This section includes configuration files corresponding to the WAN remote-site design topologies as referenced in the following figure. Each remote-site type has its respective devices grouped together along with any other relevant configuration information.

Figure 11 - WAN Remote-Site Designs
### Table 10 - Remote-Site WAN Connection Details

<table>
<thead>
<tr>
<th>Remote-Site Information</th>
<th>MPLS (Our AS = 65511)</th>
<th>DMVPN</th>
<th>LAN Interfaces</th>
<th>Loopbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Location</td>
<td>Net Block</td>
<td>MPLS CE</td>
<td>MPLS PE</td>
</tr>
<tr>
<td>Remote Site 220 [GSM]</td>
<td></td>
<td>10.5.216.0/21</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Site 221 [CDMA]</td>
<td></td>
<td>10.5.24.0/21</td>
<td>(gi0/0)</td>
<td>192.168.3.33</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Site 222 (dual router) [CDMA]</td>
<td></td>
<td>10.5.24.0/21</td>
<td>(gi0/0)</td>
<td>192.168.3.33</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Remote Site 220: Single-Router, Single-Link

The following table shows the IP address information for Remote Site 220.

### Table 11 - Remote Site 221—IP Address Information

<table>
<thead>
<tr>
<th>Remote-Site Information</th>
<th>Wired Subnets</th>
<th>Wireless Subnets</th>
<th>Operational IP Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Location</td>
<td>Net Block</td>
<td>Voice (Vlan 69)</td>
</tr>
<tr>
<td>Remote Site 220</td>
<td>10.5.216.0/21</td>
<td>10.5.220.0/24</td>
<td>n/a</td>
</tr>
</tbody>
</table>
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service internal
!
hostname RS220-1941
!
!
enable secret 5 $1$yUWN$6eDcL43qiYsgeZtF4VxWT.
!
!  
!  
!  
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
    server 10.4.48.15
!
!  
!  
!  
!  
!  
!  
!  
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
class-map match-any INTERACTIVE-VIDEO
    match dscp cs4 af41
class-map match-any CRITICAL-DATA
    match dscp cs3 af31
class-map match-any VOICE
    match dscp ef
class-map match-any SCAVENGER
    match ip dscp cs1 af11
class-map match-any NETWORK-CRITICAL
    match ip dscp cs2 cs6
    match access-group name ISAKMP
!

policy-map WAN
    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 WAN-INTERFACE-Dialer1
    class class-default
        shape average 384000
        service-policy WAN
!
crypto keyring DMVPN-KEYRING vrf INET-PUBLIC
    pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
    encr aes 256
    authentication pre-share
    group 2
    crypto isakmp keepalive 30 5
    crypto isakmp profile FVRP-ISAKMP-INET-PUBLIC
        keyring DMVPN-KEYRING
        match identity address 0.0.0.0 INET-PUBLIC
!

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
    set isakmp-profile FVRP-ISAKMP-INET-PUBLIC
!
!
interface Loopback0
    ip address 10.5.216.254 255.255.255.255
!
interface Tunnel110
    bandwidth 384
    ip address 10.4.34.220 255.255.255.0
    no ip redirects
    ip mtu 1400
    ip pim dr-priority 0
    ip pim nbma-mode
    ip pim sparse-mode
ip hello-interval eigrp 200 20
ip hold-time eigrp 200 60
ip nhrp authentication cisco123
ip nhrp map multicast 172.16.130.1
ip nhrp map 10.4.34.1 172.16.130.1
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp nhs 10.4.34.1
ip nhrp registration no-unique
ip nhrp shortcut
ip virtual-reassembly in
ip virtual-reassembly out
ip tcp adjust-mss 1360
ip summary-address eigrp 200 10.5.216.0 255.255.248.0
tunnel source Dialer1
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC
tunnel protection ipsec profile DMVPN-PROFILE

! interface GigabitEthernet0/0
  no ip address
  shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
  no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.64
  description Data1
  encapsulation dot1Q 64
  ip address 10.5.220.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode

! interface GigabitEthernet0/1.65
  description wireless data
  encapsulation dot1Q 65
  ip address 10.5.218.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode

! interface Cellular0/0/0
  bandwidth 384
  no ip address
  encapsulation ppp
dialer in-band
dialer pool-member 1
  no peer default ip address
  async mode interactive
  no ppp lcp fast-start
  service-policy output WAN-INTERFACE-Dialer1
!
interface Vlan1
  no ip address
!
interface Dialer1
  bandwidth 384
  ip vrf forwarding INET-PUBLIC
  ip address negotiated
  ip access-group ACL-INET-PUBLIC in
  encapsulation ppp
dialer pool 1
dialer idle-timeout 0
dialer string GSM
dialer persistent
  no ppp lcp fast-start
  ppp chap hostname ISP@CINGULARGPRS.COM
  ppp chap password 7 02252D752C3323007E1F
  ppp ipcp address accept
  ppp timeout retry 120
  ppp timeout ncp 30
service-policy output WAN-INTERFACE-Dialer1
!
!
router eigrp 200
  network 10.4.34.0 0.0.1.255
  network 10.5.0.0 0.0.255.255
  passive-interface default
  no passive-interface Tunnel110
  eigrp router-id 10.5.216.254
  eigrp stub connected summary
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
!
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 Dialer1
ip tacacs source-interface Loopback0
!
ip access-list extended ACL-INET-PUBLIC
  permit udp any any eq non500-isakmp
  permit udp any any eq isakmp
  permit esp any any
  permit icmp any any echo
  permit icmp any any echo-reply
ip access-list extended ISAKMP
  permit udp any eq isakmp any eq isakmp
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
action 1 cli command “enable”
action 2 cli command “configure terminal”
action 3 cli command “interface cellular0/0/0”
action 4 cli command “no shutdown”
action 5 cli command “end”
action 99 syslog msg “M-F @ 4:45AM Activating 3G interface”
event manager applet TIME-OF-DAY-DEACTIVATE-3G
  event timer cron cron-entry “15 18 * * 1-5”
action 1 cli command “enable”
action 2 cli command “configure terminal”
action 3 cli command “interface cellular0/0/0”
action 4 cli command “shutdown”
action 5 cli command “end”
action 99 syslog msg “M-F @ 6:15PM Deactivating 3G interface”
!
end
Remote Site 221: Single-Router, Dual-Link

The following table shows the IP address information for Remote Site 221.

Table 12 - Remote Site 221—IP Address Information

<table>
<thead>
<tr>
<th>Remote-Site Information</th>
<th>Wired Subnets</th>
<th>Wireless Subnets</th>
<th>Operational IP Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Location</td>
<td>Wired Subnets</td>
<td>Wireless Subnets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data (Vlan 64)</td>
<td>Voice (Vlan 69)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.5.28.0/24</td>
<td>10.5.29.0/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.5.26.0/24</td>
<td>10.5.27.0/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.5.24.254 (r)</td>
<td>10.5.28.5 (sw)</td>
</tr>
</tbody>
</table>

RS221-2921

version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service internal

! hostname RS221-2921

! enable secret 5 $1$yUWN$6eDcL43qiYsge2tF4VxWT.

! aaa new-model

! aaa group server tacacs+ TACACS-SERVERS

  server 10.4.48.15

! aaa authentication login default group TACACS-SERVERS local

! aaa authorization console

! aaa authorization exec default group TACACS-SERVERS local

! no ipv6 cef

! ip source-route

! ip cef

! ip vrf INET-PUBLIC

  rd 65512:1

! ip multicast-routing

! no ip domain lookup

! ip domain name cisco.local

! multilink bundle-name authenticated

! chat-script CDMA """"ATDT#777"""" TIMEOUT 30 """"CONNECT"

crypto pki token default removal timeout 0
license udi pid CISCO2921/K9 sn FTX1444AKQA
license boot module c2900 technology-package securityk9
!
username admin password 7 141443180F0B7B7977
!
redundancy
!
controller Cellular 0/0
!
ip tftp source-interface Loopback0
ip ssh source-interface Loopback0
ip ssh version 2
!
track 60 ip sla 100 reachability
!
class-map match-any DATA
  match ip dscp af21
class-map match-any BGP-ROUTING
  match protocol bgp
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4  af41
class-map match-any CRITICAL-DATA
  match dscp cs3  af31
class-map match-any VOICE
  match dscp ef
class-map match-any SCAVENGER
  match ip dscp cs1  af11
class-map match-any NETWORK-CRITICAL
  match ip dscp cs2  cs6
  match access-group name ISAKMP
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
policy-map MARK-BGP
  class BGP-ROUTING
    set dscp cs6
policy-map WAN
  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
  service-policy MARK-BGP
  class class-default
    bandwidth percent 25
    random-detect
policy-map WAN-INTERFACE-Dialer1
  class class-default
    shape average 1800000
  service-policy WAN
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 10000000
  service-policy WAN
!
!
crypto keyring DMVPN-KEYRING vrf INET-PUBLIC
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 2
lifetime 1200
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
  keyring DMVPN-KEYRING
  match identity address 0.0.0.0 INET-PUBLIC!
!
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
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC!
!
interface Loopback0
  ip address 10.5.24.254 255.255.255.255
  ip pim sparse-mode!
interface Tunnel10
  bandwidth 1800
  ip address 10.4.34.221 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip pim dr-priority 0
  ip pim nbma-mode
  ip pim sparse-mode
  ip nhrp authentication cisco123
  ip nhrp map multicast 172.16.130.1
  ip nhrp map 10.4.34.1 172.16.130.1
  ip nhrp network-id 101
  ip nhrp holdtime 600
  ip nhrp nhs 10.4.34.1
  ip nhrp registration no-unique
  ip nhrp shortcut
  ip tcp adjust-mss 1360
  ip summary-address eigrp 200 10.5.24.0 255.255.248.0
tunnel source Dialer1
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC
tunnel protection ipsec profile DMVPN-PROFILE
!
interface GigabitEthernet0/0
  ip address 192.168.3.33 255.255.255.252
  duplex auto
  speed auto
  no cdp enable
  service-policy output WAN-INTERFACE-G0/0!
interface GigabitEthernet0/1
  no ip address
  shutdown
duplex auto
  speed auto
!
interface GigabitEthernet0/2
  no ip address
duplex auto
  speed auto
!
interface GigabitEthernet0/2.64
  description Data1
derivatization dot1Q 64
  ip address 10.5.28.1 255.255.255.0
  ip helper-address 10.4.48.10
interface GigabitEthernet0/2.65
  description wireless data
  encapsulation dot1Q 65
  ip address 10.5.26.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface GigabitEthernet0/2.69
  description voice 1
  encapsulation dot1Q 69
  ip address 10.5.29.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface GigabitEthernet0/2.70
  description wireless voice
  encapsulation dot1Q 70
  ip address 10.5.27.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface Cellular0/0/0
  bandwidth 1800
  no ip address
  encapsulation ppp
dialer in-band
dialer pool-member 1
  no peer default ip address
  async mode interactive
  no ppp lcp fast-start
!
interface Dialer1
  bandwidth 1800
  ip vrf forwarding INET-PUBLIC
  ip address negotiated
  ip access-group ACL-INET-PUBLIC in
  encapsulation ppp
dialer pool 1
dialer idle-timeout 0
dialer string CDMA
dialer persistent
  ppp ipcp address accept
  service-policy output WAN-INTERFACE-Dialer1
!
!
router eigrp 200
  network 10.4.34.0 0.0.1.255
  network 10.5.0.0 0.0.255.255
  passive-interface default
  no passive-interface Tunnel10
eigrp router-id 10.5.24.254
eigrp stub connected summary
!
router bgp 65511
  bgp log-neighbor-changes
  network 10.5.28.0 mask 255.255.255.0
  network 10.5.29.0 mask 255.255.255.0
  network 192.168.3.32 mask 255.255.255.252
  aggregate-address 10.5.24.0 255.255.248.0 summary-only
  neighbor 192.168.3.34 remote-as 65401
  no auto-summary
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
  no ip http server
ip http secure-server
!
ip dns view vrf INET-PUBLIC default
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 Dialer1
ip tacacs source-interface Loopback0
ip access-list extended ACL-INET-PUBLIC
  permit udp any any eq non500-isakmp
  permit udp any any eq isakmp
  permit esp any any
  permit icmp any any echo
  permit icmp any any echo-reply
ip access-list extended ISAKMP
  permit udp any eq isakmp any eq isakmp
!
ip sla 100
  icmp-echo 192.168.3.34 source-interface GigabitEthernet0/0
  threshold 1000
  frequency 15
ip sla schedule 100 life forever start-time now
!
!
tacacs-server host 10.4.48.15 key 7 00371605165E1F2D0A38
!
control-plane
!
line con 0
line aux 0
line 0/0/0
  script dialer CDMA
  no exec
  rxspeed 3100000
  txspeed 1800000
line vty 0 4
  transport input all
!
scheduler allocate 20000 1000

ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
event manager applet ACTIVATE-3G
  event track 60 state down
    action 1 cli command "enable"
    action 2 cli command "configure terminal"
    action 3 cli command "interface cellular0/0/0"
    action 4 cli command "no shutdown"
    action 5 cli command "end"
    action 99 syslog msg "Primary Link Down - Activating 3G interface"
  event manager applet DEACTIVATE-3G
    event track 60 state up
    action 1 cli command "enable"
    action 2 cli command "configure terminal"
    action 3 cli command "interface cellular0/0/0"
    action 4 cli command "shutdown"
    action 5 cli command "end"
    action 99 syslog msg "Primary Link Restored - Deactivating 3G interface"
!
end
Remote Site 222: Dual-Router, Dual-Link

The following table shows the IP address information for Remote Site 222.

**Table 13 - Remote Site 222—IP Address Information**

<table>
<thead>
<tr>
<th>Remote-Site Information</th>
<th>Wired Subnets</th>
<th>Wireless Subnets</th>
<th>Operational IP Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Location</td>
<td>Net Block</td>
<td>Data (Vlan 64)</td>
</tr>
<tr>
<td></td>
<td>Remote Site</td>
<td>10.5.24.0/21</td>
<td>10.5.28.0/24</td>
</tr>
<tr>
<td></td>
<td>222</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

RS222-2921-1

version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS222-2921-1
!
boot-start-marker
boot system flash flash0:c2900-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
enable secret 5 $1$yUWN$6eDcL43qiYsgeZtF4VxWT.
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
  server 10.4.48.15
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
crypto pki token default removal timeout 0
!
!
voice-card 0
!
!
!
license udi pid CISCO2921/K9 sn FTX1446AKD2
license boot module c2900 technology-package securityk9
hw-module pvdm 0/0
!
!
!
username admin password 7 141443180F0B7B7977
!
!
!
username admin password 7 141443180F0B7B7977
!
!
!
ip ftp source-interface Loopback0
ip ftp username bn
ip ftp password 7 141443180F0B7B7977
ip tftp source-interface Loopback0
ip ssh source-interface Loopback0
ip ssh version 2
!
track 50 ip sla 100 reachability
!
class-map match-any DATA
  match ip dscp af21
class-map match-any BGP-ROUTING
  match protocol bgp
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
class-map match-any CRITICAL-DATA
  match dscp cs3 af31
class-map match-any VOICE
  match dscp ef
class-map match-any SCAVENGER
  match ip dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match ip dscp cs2 cs6
!
!
!
policy-map MARK-BGP
  class BGP-ROUTING
    set dscp cs6
policy-map WAN
  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
  service-policy MARK-BGP
policy-map WAN-INTERFACE-G0/0
  class class-default
    bandwidth percent 25
    random-detect

shape average 10000000
service-policy WAN
!
!
!
!
interface Loopback0
  ip address 10.5.24.254 255.255.255.255
  ip pim sparse-mode
!
interface GigabitEthernet0/0
  ip address 192.168.3.33 255.255.255.252
  ip pim sparse-mode
duplex auto
speed auto
no cdp enable
service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
  no ip address
  shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/2
  no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2.64
description Data1
  encapsulation dot1Q 64
  ip address 10.5.28.2 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim dr-priority 110
  ip pim sparse-mode
  standby 1 ip 10.5.28.1
  standby 1 priority 110
  standby 1 preempt
  standby 1 track 50 decrement 10
!
interface GigabitEthernet0/2.65
description wireless data
  encapsulation dot1Q 65
  ip address 10.5.26.2 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim dr-priority 110
  ip pim sparse-mode
  standby 1 ip 10.5.26.1
  standby 1 priority 110
  standby 1 preempt
  standby 1 track 50 decrement 10
!
interface GigabitEthernet0/2.69
description voice 1
  encapsulation dot1Q 69
  ip address 10.5.29.2 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim dr-priority 110
  ip pim sparse-mode
  standby 1 ip 10.5.29.1
  standby 1 priority 110
  standby 1 preempt
  standby 1 track 50 decrement 10
!
interface GigabitEthernet0/2.70
description wireless voice
  encapsulation dot1Q 70
  ip address 10.5.27.2 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim dr-priority 110
  ip pim sparse-mode
  standby 1 ip 10.5.27.1
standby 1 priority 110
standby 1 preempt
standby 1 track 50 decrement 10
!
interface GigabitEthernet0/2.99
  encapsulation dot1Q 99
  ip address 10.5.24.1 255.255.255.252
!
!
routing eigrp 100
  default-metric 100000 100 255 1 1500
  network 10.5.0.0 0.0.255.255
  redistribute bgp 65511
  passive-interface default
  no passive-interface GigabitEthernet0/2.99
  eigrp router-id 10.5.24.254
!
routing bgp 65511
  bgp log-neighbor-changes
  network 10.5.28.0 mask 255.255.255.0
  network 10.5.29.0 mask 255.255.255.0
  network 192.168.3.32 mask 255.255.255.252
  aggregate-address 10.5.24.0 255.255.248.0 summary-only
  neighbor 192.168.3.34 remote-as 65401
  no auto-summary
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http secure-server
!
ip tacacs source-interface Loopback0
!
ip sla 100
  icmp-echo 192.168.3.34 source-interface GigabitEthernet0/0
  threshold 1000
  frequency 15
  ip sla schedule 100 life forever start-time now
  !
  !
  !
  !
tacacs-server host 10.4.48.15 key 7 00371605165E1F2D0A38
  !
  !
  !
  !
mgcp profile default
!
!
!
!
!

gatekeeper
  shutdown
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
  transport input all
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
end
RS222-2921-2

version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service internal

hostname RS222-2921-2

boot-start-marker
boot system flash flash0:c2900-universalk9-mz.SPA.151-3.T.bin
boot-end-marker

logging buffered 1024000
enable secret 5 $1$yUWN$6eDcL43qiYsge2tF4VxWT.

aaa new-model

aaa group server tacacs+ TACACS-SERVERS
  server 10.4.48.15

aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local

aaa session-id common

clock timezone PST -8 0
clock summer-time PDT recurring

no ipv6 cef

ip source-route
ip cef

ip vrf INET-PUBLIC
  rd 65512:1

ip multicast-routing

no ip domain lookup
ip domain name cisco.local

multilink bundle-name authenticated

chat-script CDMA "" ""ATDT#777" TIMEOUT 30 "CONNECT"
crypto pki token default removal timeout 0

license udi pid CISCO2921/K9 sn FTX1444AKQA
license boot module c2900 technology-package securityk9

username admin password 7 141443180F0B7B7977

redundancy

controller Cellular 0/0

ip ftp source-interface Loopback0
ip ftp username bn
ip ftp password 7 0205554808095E731F
ip tftp source-interface Loopback0
ip ssh source-interface Loopback0
ip ssh version 2
!
track 60 ip sla 100 reachability
!
 class-map match-any DATA
  match ip dscp af21
 class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
 class-map match-any CRITICAL-DATA
  match dscp cs3 af31
 class-map match-any VOICE
  match dscp ef
 class-map match-any SCAVENGER
  match ip dscp cs1 af11
 class-map match-any NETWORK-CRITICAL
  match ip dscp cs2 cs6
  match access-group name ISAKMP
!
 policy-map WAN
  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 WAN-INTERFACE-Dialer1
  class class-default
    shape average 1800000
    service-policy WAN
!
crypto keyring DMVPN-KEYRING vrf INET-PUBLIC
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
  lifetime 1200
  crypto isakmp keepalive 30 5
  crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
    keyring DMVPN-KEYRING
    match identity address 0.0.0.0 INET-PUBLIC
!
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
    set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
!
!
interface Loopback0
  ip address 10.5.24.253 255.255.255.255
  ip pim sparse-mode
interface Tunnel10
bandwidth 1800
ip address 10.4.34.222 255.255.254.0
no ip redirects
ip mtu 1400
ip pim dr-priority 0
ip pim nbma-mode
ip pim sparse-mode
ip hello-interval eigrp 200 20
ip hold-time eigrp 200 60
ip nhrp authentication cisco123
ip nhrp map 10.4.34.1 172.16.130.1
ip nhrp map multicast 172.16.130.1
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp nhs 10.4.34.1
ip nhrp registration no-unique
ip nhrp shortcut
ip tcp adjust-mss 1360
ip summary-address eigrp 200 10.5.24.0 255.255.248.0
tunnel source Dialer1
tunnel mode gre multipoint
tunnel vrf INET-PUBLIC
tunnel protection ipsec profile DMVPN-PROFILE
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2.64
description Datal	encapsulation dot1Q 64
ip address 10.5.28.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
standby 1 ip 10.5.28.1
standby 1 priority 105
standby 1 preempt
!
interface GigabitEthernet0/2.65
description wireless data
ten encapsulation dot1Q 65
ip address 10.5.26.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
standby 1 ip 10.5.26.1
standby 1 priority 105
standby 1 preempt
!
interface GigabitEthernet0/2.69
description voice 1
ten encapsulation dot1Q 69
ip address 10.5.29.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
standby 1 ip 10.5.29.1
standby 1 priority 105
standby 1 preempt
!
interface GigabitEthernet0/2.70
description wireless voice
encapsulation dot1q 70
ip address 10.5.27.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
standby 1 ip 10.5.27.1
standby 1 priority 105
standby 1 preempt
!
interface GigabitEthernet0/2.99
  encapsulation dot1q 99
  ip address 10.5.24.2 255.255.255.252
!
interface Cellular0/0/0
  bandwidth 1800
  no ip address
  encapsulation ppp
  shutdown
dialer in-band
dialer pool-member 1
  no peer default ip address
  async mode interactive
  no ppp lcp fast-start
  service-policy output WAN-INTERFACE-Dialer1
!
interface Dialer1
  bandwidth 1800
  ip vrf forwarding INET-PUBLIC
  ip address negotiated
  ip access-group ACL-INET-PUBLIC in
  encapsulation ppp
dialer pool 1
dialer idle-timeout 0
dialer string CDMA
dialer persistent
  ppp ipcp address accept
  service-policy output WAN-INTERFACE-Dialer1
!
router eigrp 200
  network 10.4.34.0 0.0.1.255
  network 10.5.0.0 0.0.255.255
  passive-interface default
  no passive-interface Tunnel10
eigrp router-id 10.5.24.253
eigrp stub connected summary
!
router eigrp 100
  network 10.5.0.0 0.0.255.255
  redistribute eigrp 200
  passive-interface default
  no passive-interface GigabitEthernet0/2.99
eigrp router-id 10.5.24.253
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http secure-server
!
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 Dialer1
ip tacacs source-interface Loopback0
!
ip access-list extended ACL-INET-PUBLIC
  permit udp any any eq non500-isakmp
  permit udp any any eq isakmp
  permit esp any any
  permit icmp any any echo
  permit icmp any any echo-reply
ip access-list extended ISAKMP
  permit udp any eq isakmp any eq isakmp
!
ip sla 100
icmp-echo 192.168.3.34 source-interface GigabitEthernet0/2.99
threshold 1000
frequency 15
ip sla schedule 100 life forever start-time now
!
!
!
tacacs-server host 10.4.48.15 key 7 00371605165E1F2D0A38
!
control-plane
!
!
line con 0
line aux 0
line 0/0/0
  script dialer CDMA
  no exec
  rxspeed 3100000
  txspeed 1800000
line vty 0 4
  transport input all
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
event manager applet ACTIVATE-3G
  event track 60 state up
  action 1 cli command “enable”
  action 2 cli command “configure terminal”
  action 3 cli command “interface cellular0/0/0”
  action 4 cli command “shutdown”
  action 5 cli command “end”
  action 99 syslog msg “Activating 3G interface”
!
event manager applet DEACTIVATE-3G
  event track 60 state down
  action 1 cli command “enable”
  action 2 cli command “configure terminal”
  action 3 cli command “interface cellular0/0/0”
  action 4 cli command “shutdown”
  action 5 cli command “end”
  action 99 syslog msg “Deactivating 3G interface”
!
end