



# 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.





BORDERLESS  
NETWORKS

DEPLOYMENT  
GUIDE

# VPN Remote Site over 3G/4G Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

August 2012 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 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.

The Release Notes for a series provides a summary of additions and changes made in the 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 2012 are the “August 2012 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:

```
wrr-queue random-detect max-threshold 1 100 100 100 100  
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 [SBA feedback form](#).

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

# Table of Contents

<b>What's In This SBA Guide</b> .....	<b>1</b>	<b>Appendix A: Product List</b> .....	<b>45</b>
Cisco SBA Borderless Networks .....	1	<b>Appendix B: Configuration</b> .....	<b>47</b>
Route to Success .....	1	Remote-Site 220: Single-Router, Single-Link .....	48
About This Guide .....	1	RS220-1941 (with GSM 3G HSPA+) .....	48
<b>Introduction</b> .....	<b>2</b>	RS220-1941 (with 4G/LTE) .....	52
Business Overview .....	2	Remote-Site 221: Single-Router, Dual-Link.....	57
Technical Overview .....	2	RS221-2921.....	57
Considerations for Deploying the Cellular Remote Site .....	8	Remote-Site 222: Dual-Router, Dual-Link .....	62
Remote Sites—DMVPN Spoke Router Selection.....	10	RS222-2921-1.....	62
<b>Deployment Details</b> .....	<b>13</b>	RS222-2921-2 .....	66
Configuring a Remote-Site Router—GSM-Specific .....	14	<b>Appendix C: Changes</b> .....	<b>71</b>
Configuring a Remote-Site Router—CDMA-Specific .....	15		
Configuring a Remote-Site Router—4G/LTE-Specific .....	17		
Configuring a Remote-Site 3G or 4G DMVPN Router .....	18		
Modifying Router 1 for Dual-Router Design .....	31		
Configuring 3G/4G Router for Dual-Router Design .....	35		
Controlling Usage of 3G or 4G Interface .....	37		
Implementing Automated Recovery for 4G/LTE Interface .....	40		
Configuring WAN Quality of Service .....	41		

# What's In This SBA Guide

## Cisco SBA Borderless Networks

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.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

## Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

## About This Guide

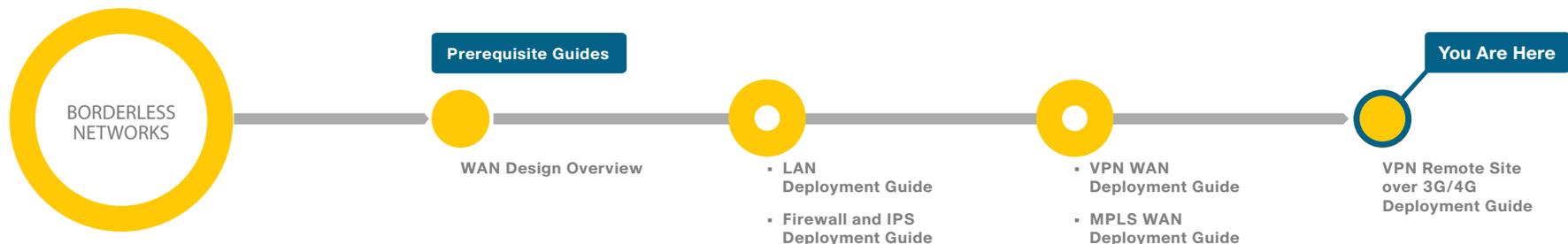
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

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

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>



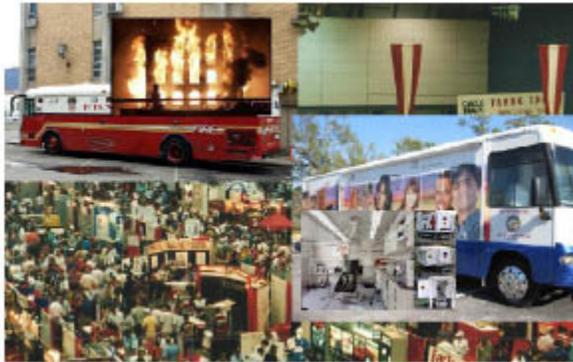
# Introduction

## 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.

Figure 1 - Use cases



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.



### Reader Tip

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

## Technical Overview

This guide provides a design that uses Cisco 3G and 4G technology in order to enable highly available, secure, and optimized connectivity for remote-site LANs .

This guide is written as an addition to the *MPLS WAN Deployment Guide* and the *VPN WAN Deployment Guide*. It 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 or 4G wireless WAN connectivity for remotes sites
- Primary and secondary links to provide redundant topology options for resiliency
- Data privacy via encryption
- Wired LAN access at all remote sites

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 Multiprotocol Label Switching (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.

## Cellular Options

Cellular connectivity enables this solution with a flexible, high speed, high bandwidth option. There are two competing 3G technologies that provide high bandwidth network WAN connectivity where cellular is the only option: Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM). Much of the world can only select one or the other of the CDMA and GSM options. There are now higher-speed 4G technology options based on Long Term Evolution (LTE) and WiMAX.

### 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 predominantly 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 2 Mbps for stationary users. Carriers now support fourth generation (4G) standard products, which promise up to gigabit data rates for stationary users and must be able to achieve at least 100 Mbps 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.

### Long-Term Evolution

LTE uses an IP transport and an Orthogonal Frequency Division Multiple Access (OFDMA) air interface as its core technologies. There are many similarities between LTE and WiMAX; however, LTE currently has a more dominant global market share. LTE data rates are asymmetric like most wireless WAN technologies. You can expect downloads at speeds ranging from 5-12 Mbps and uploads at speeds ranging from 2-5 Mbps.



#### Reader Tip

The solutions presented in this guide leverage Cisco Integrated Services G2 Routers running Cisco IOS software. They contain CDMA, GSM, or 4G/LTE high-speed WAN interfaces.

## WAN Design

This document builds upon the reference designs for a WAN aggregation site that are used in the *MPLS WAN Deployment Guide* and the *VPN WAN 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 or 4G 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) in order 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 both as 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.

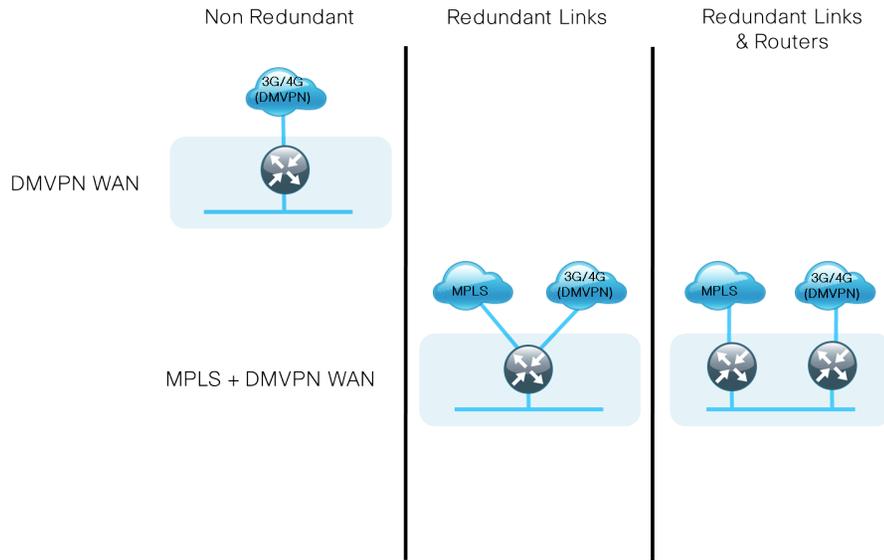
Cisco DMVPN was selected for the encryption solution for the Internet transport because it supports on-demand full mesh connectivity with a simple hub-and-spoke configuration and a zero-touch hub deployment model for adding remote sites. Cisco DMVPN also supports spoke routers that have 3G/4G WAN high-speed WAN interface cards (HWIC) with dynamically assigned IP addresses.

Cisco DMVPN makes use of multipoint generic routing encapsulation (mGRE) tunnels 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.

Figure 2 - WAN remote-site designs



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

WAN remote-site router(s)	WAN transports	Primary transport	Secondary transport
Single	Single	Internet (3G/4G)	
Single	Dual	MPLS VPN A	Internet (3G/4G)
		MPLS VPN B	Internet (3G/4G)
Dual	Dual	MPLS VPN A	Internet (3G/4G)
		MPLS VPN B	Internet (3G/4G)

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.



**Reader Tip**

Specific details regarding the LAN components of the design are covered in the *LAN Deployment Guide*.

At remote sites, the LAN topology depends on the number of connected users and the 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

WAN remote-site routers	WAN transports	LAN topology
Single	Single	Access only
Single	Dual	Access only
Dual	Dual	Access only

### WAN Remote 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**

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

Table 3 - WAN remote sites—VLAN assignment

VLAN	Usage (MPLS primary)	Usage (3G/4G primary)	Layer 2 access
VLAN 64	Data 1	Data 1	Yes
VLAN 69	Voice 1	Not supported	Yes
VLAN 99	Transit	Not used	Yes (dual router only)

### 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. 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.

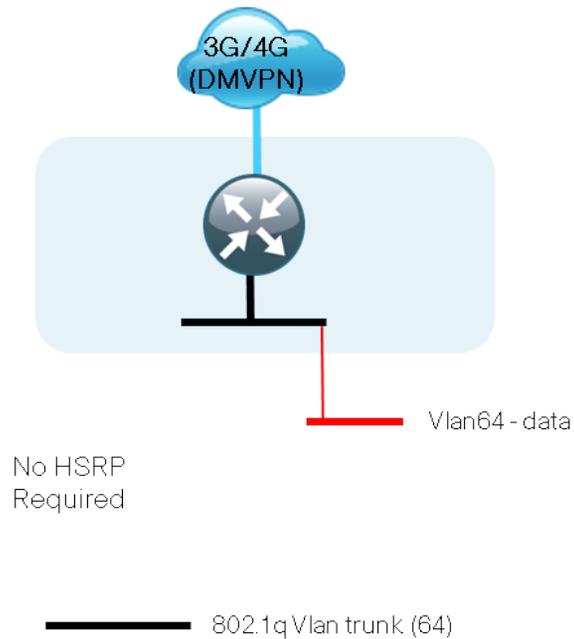
**Reader Tip**

Access switches and their configuration are not included in this guide. The *LAN Deployment Guide* provides configuration details on the various access switching platforms.

The Layer 3 distribution layer design is not covered in this guide. Please refer to the *MPLS 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 fewer 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.

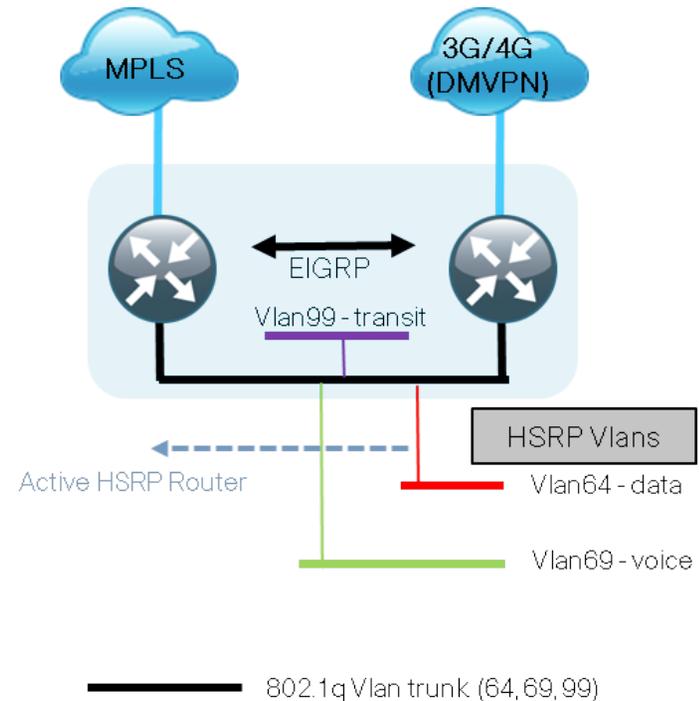
Figure 3 - WAN remote site—flat Layer 2 LAN (single router)



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 Routing 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.

Figure 4 - WAN remote site—flat Layer 2 LAN (dual router)

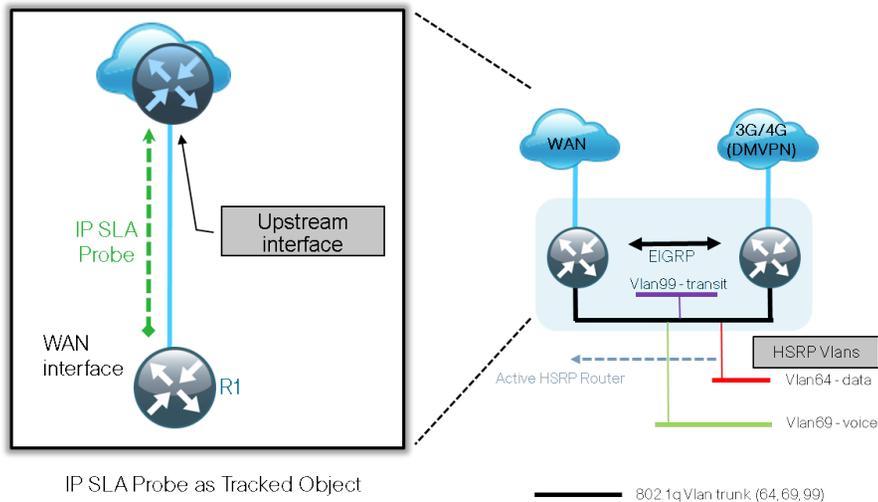


Enhanced Object Tracking (EOT) provides a consistent methodology for various router and switching features to conditionally modify their operation, based on information objects available within other processes. The objects that can be tracked include interface line protocol, IP route reachability, and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

The IP 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 Internet Control Message Protocol (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 an 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.

Figure 5 - WAN remote-site IP SLA probe to verify upstream device reachability



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: an 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 *hairpinning*.

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/4G 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?
- Do you want or require redundant hardware for hot swap should a failure occur?

Contact your local service provider to see what technologies are in your area. For example, Europe has mandated GSM for all cellular.

GSM allows you to move your SIM card from device to device without working through your service provider.

- Is high data throughput a requirement?
- 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 all of the 3G and 4G options 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, can the service provider provide a direct connection to customers' MPLS networks?

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.



### Reader Tip

The 3G/4G remote-site design is based on the designs in the *MPLS WAN Deployment Guide* and the *VPN WAN Deployment Guide*. Please refer to those guides for the configuration details for the WAN aggregation devices.

The design for a 3G/4G-only transport is similar to the design models in the following table, and either the DMVPN Only or Dual DMVPN WAN aggregation designs can be used.

*Table 4 - VPN-only WAN-aggregation design models from VPN WAN Deployment Guide*

Model	Remote sites	WAN links	DMVPN hubs	Transport 1	Transport 2
DMVPN Only	Up to 100	Single	Single	Internet VPN	
Dual DMVPN	Up to 500	Dual	Dual	Internet VPN	Internet VPN

The remote-site designs using 3G/4G for a backup transport assume that the primary MPLS links are already configured using one of the design models in the following table.

*Table 5 - MPLS WAN-aggregation design models from MPLS WAN Deployment Guide*

Model	Remote sites	WAN links	Edge routers	WAN routing protocol	Transport 1	Transport 2
MPLS Static	Up to 50	Single	Single	None (static)	MPLS VPN A	
MPLS Dynamic	Up to 100	Single	Single	BGP (dynamic)	MPLS VPN A	
Dual MPLS	Up to 500	Dual	Dual	BGP (dynamic)	MPLS VPN A	MPLS VPN B

The remote-site designs using 3G/4G for a backup transport assume that the DMVPN hub router is already configured and otherwise align to the backup variants in the following table.

*Table 6 - VPN-backup WAN-aggregation design models from VPN WAN Deployment Guide*

Model	Remote sites	WAN links	DMVPN hubs	Transport 1 (existing)	Transport 2 (existing)	Backup transport
DMVPN Backup Shared	Up to 50	Dual	Single (shared with MPLS CE)	MPLS VPN A		Internet VPN
DMVPN Backup Dedicated	Up to 500	Multiple	Single	MPLS VPN A	MPLS VPN B	Internet VPN

## IP Routing

The 3G/4G 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/4G wireless remote-site designs, all remote sites support wired 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 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 + 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/4G 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 7 - Universal design parameters*

Network service	IP address
Domain Name	cisco.local
Active Directory, DNS Server, DHCP	10.4.48.10
Authentication Control System	10.4.48.15
Network Time Protocol (NTP) Server	10.4.48.17

## Remote Sites—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 DMVPN spoke routers, and the expected performance is shown in the following table.

Table 8 - WAN remote-site 3G or 4G router options

Option	1941 <sup>1</sup>	2911	2921	2951	3925	3945
Ethernet WAN with Services <sup>2</sup>	25 Mbps	35 Mbps	50 Mbps	75	100 Mbps	150 Mbps
On-board GE ports	2	3	3	3	3	3
Service Module Slots <sup>3</sup>	0	1	1	2	2	4
Redundant Power Supply Option	No	No	No	No	Yes	Yes

Notes:

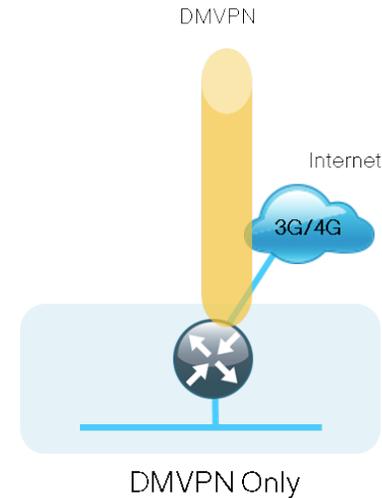
1. The 1941 is recommended for use at single-router, single-link remote sites.
2. The performance numbers are conservative numbers obtained when the router is passing Internet mix (IMIX) traffic with heavy services configured and the CPU utilization is under 75 percent.
3. Some service modules are double-wide.

The compact 819 router, which is available in both hardened (819HG) and nonhardened (819G) variants, 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 or 4G 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 6 - DMVPN remote site (single link—single router)



The DMVPN connection can be the primary WAN transport or can also be the alternate to an MPLS WAN transport. The 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 7 - MPLS WAN + DMVPN remote site (single router - dual link options)

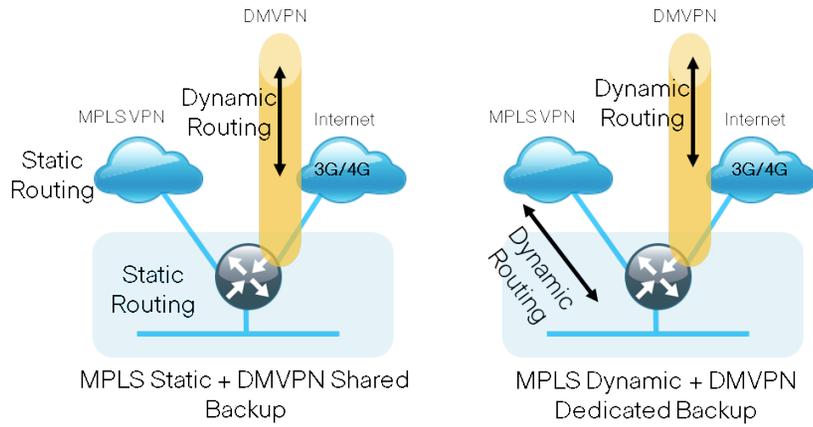
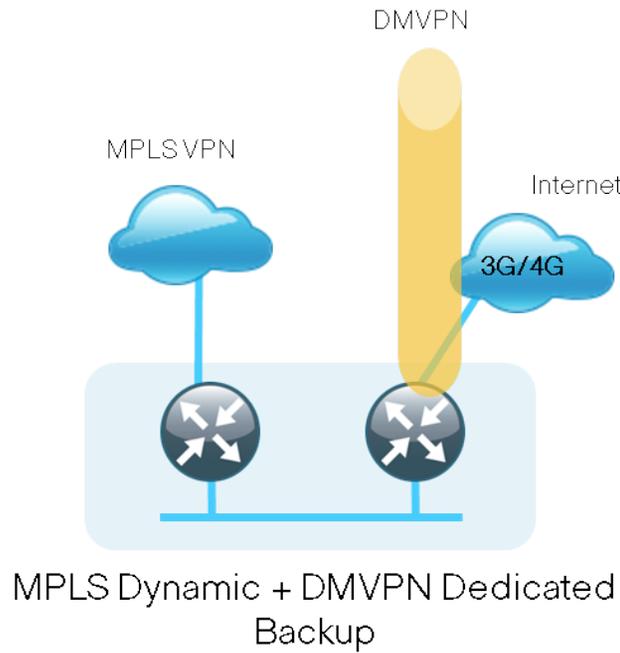


Figure 8 - MPLS WAN + DMVPN remote site (dual router - dual link options)



## Notes

# Deployment Details

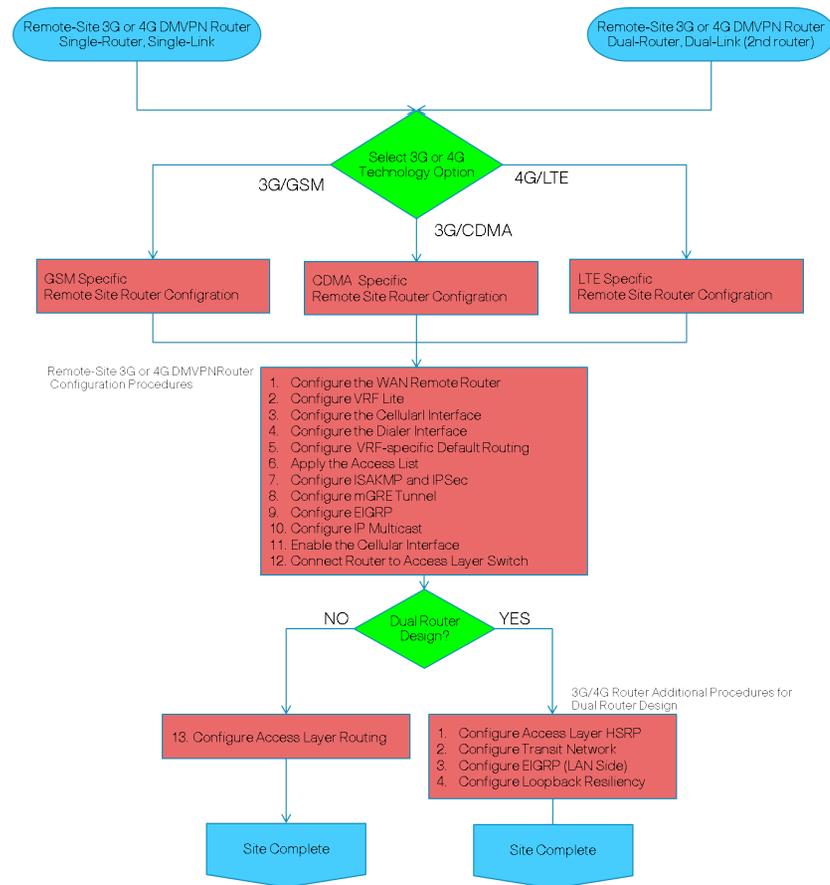
This section provides the processes for deploying the remote-site devices for a 3G/4G DMVPN remote site or an MPLS + 3G/4G DMVPN remote site.

There are two variants of 3G HWIC cards available for the routers. One supports GSM, and the other supports CDMA. There is one 4G HWIC available for the routers; it supports LTE. These cards all use similar configurations but with minor differences. Similarly, deployment guidance for a fixed-configuration 3G router is also included. 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 DMVPN spoke router. This flowchart applies for a single-router, for a single-link design (DMVPN only), and for a dual-router, dual-link design (MPLS + DMVPN backup).

Figure 9 - Flowchart for remote-site 3G or 4G DMVPN spoke router configuration



The following flowchart provides details on how to add 3G or 4G DMVPN backup on an existing remote-site MPLS CE router. This specifically applies for a single-router, dual-link design (MPLS + DMVPN backup). It is assumed that the MPLS CE router has already been configured using the guidance provided in the *MPLS WAN Deployment Guide*.



The following chat script shows the required information to connect to the AT&T GSM network. It uses a carrier-specific dial string and a timeout value of 30 seconds. Note that your carrier may require a different chat script.

**Step 1:** Create a chat script.

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

**Example**

```
chat-script HSPA "" "AT!SCACT=1,1" TIMEOUT 60 "OK"
```

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

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

**Example**

For the interface cellular0/0/0, the matching line would be as follows.

```
line 0/0/0
  script dialer HSPA
```

**Step 3:** Create the GSM profile. From enable mode, use the profile to identify the APN provided to you by your service provider. Use the cellular interface identifier and the keyword **GSM**.

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



### Tech Tip

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

**Example**

```
cellular 0/0/0 gsm profile create 1 isp.cingular
```

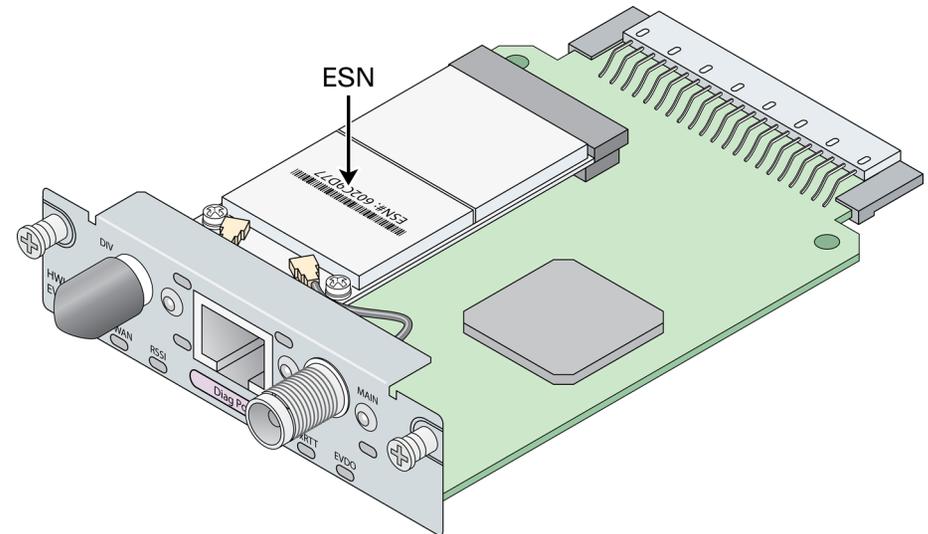
## Process

Configuring a Remote-Site Router—CDMA-Specific

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 12 - CDMA HWIC ESN location





## Tech Tip

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.

### Procedure 1

#### Install CDMA HWIC into ISR

**Step 1:** Using the ESN number found on the HWIC, register CDMA HWIC with a service provider. The ESN is located on the modem that is attached to the back of the HWIC. The ESN is just below the barcode, as shown in Figure 12.

After you complete this procedure, you can also determine the ESN number by using the following command.

```
CDMA-Router# show cellular 0/0/0 hardware
Modem Firmware Version = p2813301
Modem Firmware built = 06-24-10
Hardware Version = MC5728V Rev 1.0
Electronic Serial Number (ESN) = 0x60E4A2C5 [09614983877]
Preferred Roaming List (PRL) Version = 61086
PRI SKU ID = 535491
Current Modem Temperature = 35 degrees Celsius
Endpoint Port Map = 75
```

**Step 2:** Power down the Integrated Services G2 Router.

**Step 3:** Insert and fasten CDMA HWIC into the router.

**Step 4:** Power up the router and begin activation.

### Procedure 2

#### Activate the CDMA modem

Before using your CDMA HWIC, it must be activated.

##### Option 1. Verizon CDMA

**Step 1:** Activate the Verizon CDMA modem by using the activation number provided by the CDMA carrier.

```
cellular [interface number] cdma activate otasp [activation
number]
```

Example

```
cellular 0/0/0 cdma activate otasp *22899
```

##### Option 2. Sprint CDMA

**Step 1:** Activate the Sprint CDMA modem by providing the following information.

```
cellular [interface number] cdma activate oma-dm device-config
cellular [interface number] cdma activate oma-dm prl-update
```

Example

```
cellular 0/0/0 cdma activate oma-dm device-config
cellular 0/0/0 cdma activate oma-dm prl-update
```

### 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. It uses a carrier-specific dial string and a timeout value of 30 seconds. Note that your carrier may require a different chat script.

**Step 1:** Create the chat script.

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

**Example**

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

```
line 0/0/0  
script dialer CDMA
```

## Process

Configuring a Remote-Site Router—4G/LTE-Specific

1. Install LTE EHWIC into ISR
2. Configure chat script

You must get a data service account from your service provider. You should receive a SIM card that you should install on the 4G/LTE EHWIC.



### Caution

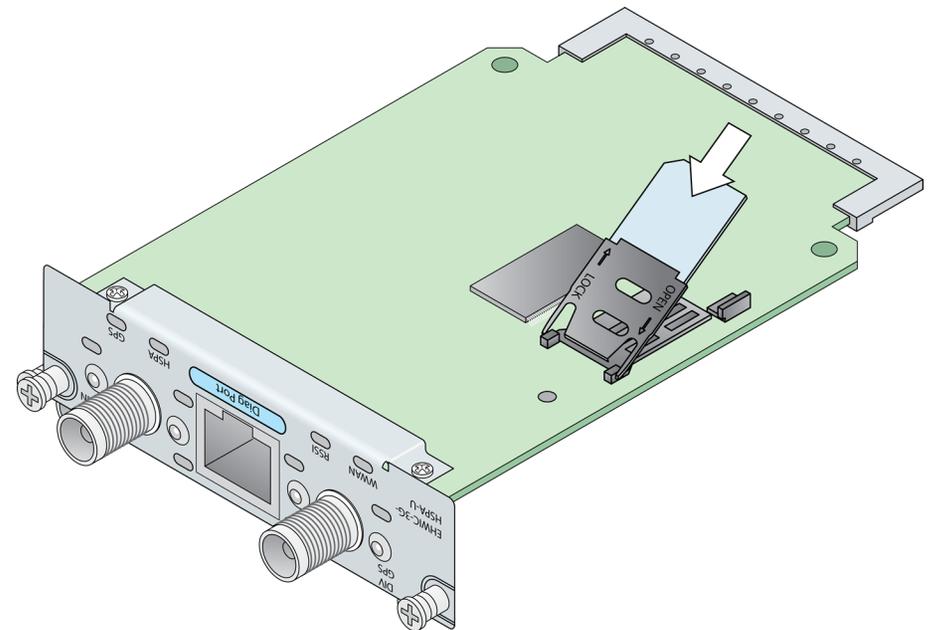
It is recommended that you implement the automated recovery scripts as detailed in the process "Implementing Automated Recovery for 4G/LTE Interface" in this guide.

Complete this process after all other router configuration is complete.

## Procedure 1

## Install LTE EHWIC into ISR

Figure 13 - LTE EHWIC SIM card installation



**Step 1:** Insert SIM card into EHWIC.

**Step 2:** Power down the Integrated Services Router G2.

**Step 3:** Insert and fasten LTE EHWIC into the router.

**Step 4:** Power up the router and begin configuration.

## Procedure 2

### 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 4G WAN interface should be treated just like any other asynchronous interface.

The following chat script shows the required information to connect to the Verizon LTE network. It uses a carrier specific dial string and a timeout value of 30 seconds. Note that your carrier may require a different chat script.

**Step 1:** Create the chat script.

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

**Example**

```
chat-script LTE "" "AT!CALL1" TIMEOUT 30 "OK"
```

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

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

**Example**

For the interface cellular0/0/0, the matching line would be as follows.

```
line 0/0/0
  script dialer LTE
```

## Process

Configuring a Remote-Site 3G or 4G DMVPN Router

1. Configure the WAN remote router
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
11. Enable the cellular interface
12. Connect router to access layer switch
13. Configure access layer routing

This set of procedures is for the configuration of a 3G or 4G DMVPN spoke router for a remote site that uses GSM, CDMA, or LTE technology. Procedure 1, Procedure 12, and Procedure 13 are not required when adding a 3G or 4G DMVPN backup on an existing MPLS CE router. Otherwise, complete Procedure 1 through Procedure 13 for all cases, and additionally the process "Configuring 3G/4G Additional Procedures for Dual Router Design" when this is the second router of a dual-router design.

**(Optional)**

If you are adding a 3G or 4G DMVPN backup on an existing MPLS CE router, skip this procedure.

Within this design, there are features and services that are common across all WAN remote-site routers. These are system settings that simplify and secure the management of the solution.

**Step 1:** Configure the device host name to make it easy to identify the device.

```
hostname [hostname]
```

**Step 2:** Configure local login and password.

The local login account and password provide basic access authentication to a router that provides only limited operational privileges. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the disclosure of plain text passwords when viewing configuration files.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

By default, HTTPS access to the router uses the enable password for authentication.

**Step 3:** If you want to centralize the authentication, authorization and accounting (AAA) service, reduce operational tasks per device, and provide an audit log of user access for security compliance and root cause analysis, configure centralized user authentication.

When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

**Reader Tip**

The authentication, authorization, and accounting (AAA) server used in this architecture is Cisco Secure Access Control System (ACS). For details about ACS configuration, see the *Device Management Using ACS Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

**Step 4:** Configure device management protocols, specifying the **transport preferred none** command on vty lines to prevent errant connection attempts from the CLI prompt. Without this command, if the server defined with the **ip name-server** command is unreachable, long timeout delays may occur for mistyped commands.

In this example, secure management of the network device is enabled through the use of the Secure Shell (SSH) and Secure HTTP (HTTPS) protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15      ! for 819G and 819HG use "line vty 0 4"
  transport input ssh
  transport preferred none
```

**Step 5:** Allow typing at the device console when debugging is enabled.

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

```
line con 0
  logging synchronous
```

**Step 6:** Enable Simple Network Management Protocol (SNMP).

This allows the network infrastructure devices to be managed by a Network Management System (NMS). Ensure that SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

**Step 7:** If you have a network where operational support is centralized, you can configure an access list.

This limits the networks that can access your device, which helps to increase network security. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15      ! for 819G and 819HG use "line vty 0 4"
  access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```



### Tech Tip

If you configure an access list on the vty interface you may lose the ability to use SSH to log in from one router to the next for hop-by-hop troubleshooting.

**Step 8:** Configure a synchronized clock by programming network devices to synchronize to a local NTP server in the network. This typically references a more accurate clock feed from an outside source. Also, configure console messages, logs, and debug output to provide time stamps on output so that you can cross-reference events in a network.

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

**Step 9:** Configure a loopback interface for in-band management. The loopback address is commonly a host address with a 32-bit address mask. Allocate the loopback address from a unique network range that is not part of any other internal network summary range.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 processes and features are also bound to the loopback interface to ensure process resiliency.

```
interface Loopback 0
  ip address [ip address] 255.255.255.255
  ip pim sparse-mode
```

The **ip pim sparse-mode** command will be explained in Step 13.

**Step 10:** Bind the device processes for SNMP, SSH, PIM, TACACS+, and NTP to the loopback interface address for optimal resiliency.

```
snmp-server trap-source Loopback0
ip ssh source-interface Loopback0
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

Next, configure IP Multicast routing.

IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP Telephony MOH and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an Internet Group Management Protocol (IGMP) message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as a rendezvous point (RP) to map the receivers to active sources so they can join their streams.

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

**Step 11:** Enable IP Multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

**Step 12:** Configure every Layer 3 switch and router to discover the IP Multicast RP with Auto-RP. 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.

```
ip pim autorp listener
```

**Step 13:** Enable all Layer 3 interfaces in the network for sparse mode multicast operation.

```
ip pim sparse-mode
```

## Procedure 2

## Configure VRF Lite

An Internet-facing Virtual Route Forwarding (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 route distinguisher (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 autonomous system number (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

```
ip vrf INET-PUBLIC1
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 minimum uplink speed of the chosen technology as shown in this table. Configure the interface administratively down until the configuration is complete.

Table 9 - 3G and 4G encapsulation and bandwidth parameters

Technology	Encapsulation	Downlink speed (Kbps)	Uplink speed (Kbps)
GSM 3G HSPA+	Direct IP (SLIP)	21600	5760
CDMA 3G	PPP	3100	1800
LTE 4G	Direct IP (SLIP)	8000 to 12000 (range)	2000 to 5000 (range)



### Tech Tip

3G CDMA cellular interfaces and associated dialer interfaces must be configured with Point-to-Point Protocol (PPP) encapsulation.

4G and 3G GSM HSPA+ cellular interfaces and associated dialer interfaces use Direct IP encapsulation. Use the Serial Line Internet Protocol (SLIP) keyword when configuring Direct IP encapsulation.

## Step 1: Assign physical interface to dialer pool.

```
interface Cellular [Interface-Number]
bandwidth [bandwidth (Kbps)]
no ip address
encapsulation [encapsulation type]
dialer in-band
dialer pool-member [Dialer Pool Number]
no peer default ip address
async mode interactive
shutdown
```

### Example (bandwidth and encapsulation are shown for CDMA 3G)

```
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
shutdown
```

### Example (bandwidth and encapsulation are shown for LTE 4G)

```
interface Cellular0/0/0
bandwidth 2000
no ip address
encapsulation slip
dialer in-band
dialer pool-member 1
no peer default ip address
async mode interactive
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 interface 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 HSPA+ networks use: HSPA  
For CDMA networks use: CDMA  
For LTE networks use: LTE

**Step 2:** Assign interface encapsulation parameters.

```
interface Dialer [Dialer Interface Number]
  ip address negotiated
  encapsulation [encapsulation type]
```

**Step 3:** If you are using CDMA technology, assign basic PPP parameters.

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

## Example (CDMA)

```
interface Dialer1
  bandwidth 1800
  ip vrf forwarding INET-PUBLIC1
  ip address negotiated
  encapsulation ppp
  dialer pool 1
  dialer idle-timeout 0
  dialer string GSM
  dialer persistent
  ppp ipcp address accept
  ppp timeout retry 120
  ppp timeout ncp 30
```

## Example (LTE)

```
interface Dialer1
  bandwidth 2000
  ip vrf forwarding INET-PUBLIC1
  ip address negotiated
  encapsulation slip
  dialer pool 1
  dialer idle-timeout 0
  dialer string LTE
  dialer persistent
```

## Procedure 5 Configure VRF-specific default routing

The remote sites using 3G or 4G DMVPN use negotiated IP addresses for the dialer interfaces. Unlike DHCP, the 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 INET-PUBLIC1 0.0.0.0 0.0.0.0 Dialer1
```

## Procedure 6 Apply the access list

The 3G or 4G 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:** Configure and 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 10 - Required DMVPN protocols

Name	Protocol	Usage
non500-isakmp	UDP 4500	IPsec via NAT-T
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec

### Example

```
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 troubleshooting but are not explicitly required to allow DMVPN to function properly.

Table 11 - Optional access-list parameters

Name	Protocol	Usage
icmp echo	ICMP type 0, code 0	Allow remote pings
icmp echo-reply	ICMP type 8, code 0	Allow ping replies
icmp ttl-exceeded	ICMP type 11, Code0	Windows traceroute
icmp port-unreachable	ICMP type 3, code 3	Service unreachable

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

```
interface Dialer1
  ip access-group ACL-INET-PUBLIC in
  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
```

## 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 DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

**Step 2:** Configure the Internet Security Association and Key Management Protocol (ISAKMP) policy and dead peer detection (DPD).

The ISAKMP policy for DMVPN uses the following:

- Advanced Encryption Standard (AES) with a 256-bit key
- Secure Hash Algorithm (SHA)
- Authentication by pre-shared key
- Diffie-Hellman group: 2

In this example, 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 FVRF-ISAKMP-INET-PUBLIC1
  keyring DMVPN-KEYRING1
  match identity address 0.0.0.0 INET-PUBLIC1
```

**Step 4:** Define the IP Security (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:

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

Since the DMVPN hub router is behind a Network Address Translation (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 it is included here for completeness.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT 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 DMVPN-PROFILE1
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
```

## 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 provided by the 3G or 4G technology as specified in Table 9. 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 Tunnel10
  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 the front door VRF.

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

```
interface Tunnel10
  tunnel source Dialer1
  tunnel mode gre multipoint
  tunnel vrf INET-PUBLIC1
  tunnel protection ipsec profile DMVPN-PROFILE1
```

## Step 3: Configure Next Hop Resolution Protocol (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 ASA 5500 Series Adaptive Security Appliances. This design uses the values shown in the following table.

Table 12 - DMVPN configuration parameters

DMVPN cloud	VRF	DMVPN hub public address (actual)	DMVPN hub public address (externally routable after NAT)	Tunnel IP address (NHS)	Tunnel number	NHRP network IP
Primary	INET-PUBLIC1	192.168.18.10	172.16.130.1	10.4.34.1	10	101

## Notes

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

This design supports DMVPN spoke routers that receive their external IP addresses through Dynamic Host Configuration Protocol (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 allows existing cache entries to be overwritten. This feature is only required on NHRP clients (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.

```
interface Tunnel10
  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 nhrp redirect
```

**Step 4:** Configure EIGRP by increasing the EIGRP hello interval to 20 seconds and increasing the EIGRP hold time to 60 seconds. This accommodates up to 500 remote sites on a single DMVPN cloud.

You configure EIGRP in Procedure 9, but it has some specific requirements for the mGRE tunnel interface. Do this and the following step during the tunnel configuration.

```
interface Tunnel10
  ip hello-interval eigrp 200 20
  ip hold-time eigrp 200 60
```

**Step 5:** Advertise the remote-site LAN networks.

The IP assignment for the remote sites was designed so that all of the networks in use can be summarized within a single aggregate route. The summary address as configured below suppresses the more specific routes. If any network within the summary is present in the route table, the summary is advertised to the DMVPN hub, which offers a measure of resiliency. If the various LAN networks cannot be summarized, then EIGRP continues to advertise the specific routes.

```
interface Tunnel10
  ip summary-address eigrp 200 10.5.216.0 255.255.248.0
```

## Procedure 9

## Configure EIGRP

**Step 1:** Configure EIGRP on the DMVPN spoke router.

A 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.

```
router eigrp 200
  network 10.4.34.0 0.0.1.255
  network 10.5.0.0 0.0.255.255
  network 10.255.0.0 0.0.255.255
  passive-interface default
  no passive-interface Tunnel10
  eigrp router-id [IP address of Loopback0]
  eigrp stub connected summary
  no auto-summary
```

## Procedure 10 Configure IP Multicast

This procedure includes additional steps for configuring IP Multicast for a DMVPN tunnel on a router with IP Multicast already enabled.

**Step 1:** Configure Protocol Independent Multicast (PIM) on the DMVPN tunnel interface.

Enable IP PIM sparse mode on the DMVPN tunnel interface.

```
interface Tunnel10
 ip pim sparse-mode
```

**Step 2:** Enable PIM non-broadcast multiple access (NBMA) 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.

To resolve the NBMA issue, you need to implement 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 Tunnel10
 ip pim nbma-mode
```

**Step 3:** Configure the 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. You can prevent that by setting the DR priority to 0 for the spokes.

```
interface Tunnel10
 ip pim dr-priority 0
```

## Procedure 11 Enable the cellular interface

The 3G/4G portion of the router configuration is essentially complete.

**Step 1:** Enable the cellular interface to bring up the DMVPN tunnel.

```
interface Cellular0/0/0
 no shutdown
```

## Procedure 12 Connect router to access layer switch

### (Optional)

Skip this procedure when adding a 3G or 4G DMVPN backup on an existing MPLS CE router.



### Reader Tip

Please refer to the *LAN Deployment Guide* for complete access layer configuration details. This guide only includes the additional steps to complete the access layer configuration.

Layer 2 EtherChannels are used to interconnect the CE router to the access layer in the most resilient method possible. If your access layer device is a single fixed configuration switch, use a simple Layer 2 trunk between the router and switch.

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.

## Option 1. Layer 2 EtherChannel from router to access layer switch

**Step 1:** Configure port-channel interface on the router.

```
interface Port-channel1
  description EtherChannel link to RS221-A2960S
  no shutdown
```

**Step 2:** Configure EtherChannel member interfaces on the router. Configure the physical interfaces to tie to the logical port-channel by using the **channel-group** command. The number for the port-channel and channel-group must match. Not all router platforms can support Link Aggregation Control Protocol (LACP) to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet0/1
  description RS221-A2960S Gig1/0/24
  !
interface GigabitEthernet0/2
  description RS221-A2960S Gig2/0/24
  !
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 1
  no shutdown
```

**Step 3:** Configure EtherChannel member interfaces on the access layer switch.

Connect the router EtherChannel uplinks to separate switches in the access layer switch stack, or in the case of the Cisco Catalyst 4507R+E distribution layer, to separate redundant modules for additional resiliency.

You should configure the physical interfaces that are members of a Layer 2 EtherChannel prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration and reduces errors because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication.

Configure two physical interfaces to be members of the EtherChannel. Also, apply the egress QoS macro that was defined in the LAN switch platform configuration procedure to ensure traffic is prioritized appropriately.

Not all connected router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet1/0/24
  description Link to RS221-2911-1 Gig0/1
interface GigabitEthernet2/0/24
  description Link to RS221-2911-1 Gig0/2
  !
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
  switchport
  macro apply EgressQoS
  channel-group 1 mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

**Step 4:** Configure EtherChannel trunk on the access layer switch.

Use an 802.1Q trunk, which allows the router to provide the Layer 3 services to all the VLANs defined on the access layer switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the access layer switch. When using EtherChannel, ensure the interface type is port-channel and match the number the channel group configured in the previous step. Set DHCP Snooping and Address Resolution Protocol (ARP) inspection to trust.

```
interface Port-channel1
  description EtherChannel link to RS221-2911-1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,69
  switchport mode trunk
  ip arp inspection trust
  spanning-tree portfast trunk
  ip dhcp snooping trust
  no shutdown
```

The Catalyst 2960-S and 4500 do not require the **switchport trunk encapsulation dot1q** command.

## Option 2. Layer 2 trunk from router to access layer switch

### Tech Tip

If you are using an 819G/819HG router, use the Gigabit Ethernet port labeled “GE WAN 0” to connect to the access layer switch.

**Step 1:** Enable the physical interface on the router.

```
interface GigabitEthernet0/2
  description RS220-A2960S Gig1/0/24
  no ip address
  no shutdown
```

**Step 2:** Configure the trunk on the access layer switch.

Use an 802.1Q trunk for the connection, which allows the router to provide the Layer 3 services to all the VLANs defined on the access layer switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the access switch. Set DHCP Snooping and Address Resolution Protocol (ARP) inspection to trust.

```
interface GigabitEthernet1/0/24
  description Link to RS220-1941 Gig0/2
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64
  switchport mode trunk
  ip arp inspection trust
  spanning-tree portfast trunk
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  ip dhcp snooping trust
  no shutdown
```

The Catalyst 2960-S and 4500 do not require the **switchport trunk encapsulation dot1q** command.

## Procedure 13 Configure access layer routing

### (Optional)

Skip this procedure when adding a 3G or 4G DMVPN backup on an existing MPLS CE router.

**Step 1:** Create subinterfaces and assign VLAN tags.

After you enable the physical interface or port-channel, then you can map the appropriate data or voice subinterfaces 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. You should repeat the subinterface portion of the configuration for all data or voice VLANs.

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

**Step 2:** 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.

If you are using a centralized DHCP server, you must use an IP helper for routers with LAN interfaces connected to a LAN using DHCP for end-station IP addressing.

If the remote-site router is the first router of a dual-router design, then configure HSRP at the access layer. This requires a modified IP configuration on each subinterface.

```
interface [type] [number] . [sub-interface number]
  ip address [LAN network 1] [LAN network 1 netmask]
  ip helper-address 10.4.48.10
  ip pim sparse-mode
```

## Example: Layer 2 EtherChannel

```
interface Port-channel1
no ip address
no shutdown
!
interface Port-channel1.64
description Data
encapsulation dot1Q 64
ip address 10.5.220.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
```

## Example: Layer 2 Trunk

```
interface GigabitEthernet0/2
no ip address
no shutdown
!
interface GigabitEthernet0/2.64
description Data
encapsulation dot1Q 64
ip address 10.5.220.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
```

## Process

Modifying Router 1 for Dual-Router Design

1. Configure access layer HSRP
2. Configure transit network
3. Configure EIGRP (LAN side)
4. Enable Enhanced Object Tracking
5. Configure loopback resiliency

This process is required when the first router has already been configured using the “Remote-Site MPLS CE Router Configuration” process in the *MPLS WAN Deployment Guide*.



### Tech Tip

Complete this process before continuing with the “Configuring 3G/4G Router Additional Procedures for Dual Router Design” process.

## Procedure 1

### Configure access layer HSRP

You need to configure HSRP to enable the use of a Virtual IP (VIP) as a default gateway that is shared between two routers. The HSRP active router is the router connected to the primary carrier and the HSRP standby router is the router connected to the secondary carrier or backup link. Configure the HSRP active router with a standby priority that is higher than the HSRP standby 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 13 - WAN remote-site HSRP parameters (dual router)

Router	HSRP role	Virtual IP address (VIP)	Real IP address	HSRP priority	PIM DR priority
Primary	Active	.1	.2	110	110
Secondary	Standby	.1	.3	105	105

The assigned IP addresses override those configured in the previous procedure, so the default gateway IP address remains consistent across locations with single or dual routers.

The dual-router access-layer design requires a modification for resilient multicast. The PIM designated router (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.

i
Tech Tip

The HSRP priority and PIM DR priority are shown in the previous table to be the same value; however you are not required to use identical values.

**Step 1:** Configure access layer HSRP.

```
interface [type][number].[sub-interface number]
 ip address [LAN network 1 address] [LAN network 1 netmask]
 ip pim dr-priority 110
 standby version 2
 standby 1 ip [LAN network 1 gateway address]
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

Repeat this procedure for all data or voice subinterfaces.

**Example: Layer 2 EtherChannel**

```
interface PortChannel2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.116.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.116.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

**Example: Layer 2 link**

```
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.116.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.116.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

Procedure 2

Configure transit network

The transit network is configured between the two routers. This network is used for router-router communication and to avoid hairpinning. 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.

**Step 1:** Configure the transit network subinterface.

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

#### Example

```
interface GigabitEthernet0/2.99
  description Transit Net
  encapsulation dot1q 99
  ip address 10.5.112.1 255.255.255.252
  ip pim sparse-mode
```

**Step 2:** Add transit network VLAN to the access layer switch. If the VLAN does not already exist on the access layer switch, configure it now.

```
vlan 99
  name Transit-net
```

**Step 3:** Add transit network VLAN to existing access layer switch trunk.

```
interface GigabitEthernet1/0/24
  switchport trunk allowed vlan add 99
```

### Procedure 3 Configure EIGRP (LAN side)

You must configure a routing protocol between the two routers. This ensures that the HSRP active router has full reachability information for all WAN remote sites.

**Step 1:** Enable and configure EIGRP-100 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 100
  network [network] [inverse mask]
  network [remote site loopback range] [inverse mask]
  passive-interface default
  no passive-interface [Transit interface]
  eigrp router-id [IP address of Loopback0]
  no auto-summary
```

**Step 2:** Redistribute BGP into EIGRP-100.

The BGP routes are redistributed into EIGRP with a default metric. By default, only the bandwidth and delay values are used for metric calculation.

```
router eigrp 100
  default-metric [bandwidth] [delay] 255 1 1500
  redistribute bgp 65511
```



#### Tech Tip

Command Reference:

**default-metric**—bandwidth delay reliability loading mtu

**bandwidth**—Minimum bandwidth of the route in kilobits per second

**delay**—Route delay in tens of microseconds

#### Example

```
router eigrp 100
  default-metric 100000 100 255 1 1500
  network 10.5.0.0 0.0.255.255
  network 10.255.0.0 0.0.255.255
  redistribute bgp 65511
  passive-interface default
  no passive-interface GigabitEthernet0/2.99
  eigrp router-id 10.255.252.222
  no auto-summary
```

## Procedure 4 Enable Enhanced Object Tracking

The HSRP active router remains the active router unless the router is reloaded or fails. Having the HSRP router remain as the active router can lead to undesired behavior. If the primary WAN transport were to fail, the HSRP active router would learn an alternate path through the transit network to the HSRP standby router and begin to forward traffic across the alternate path. This is sub-optimal routing, and you can address it by using EOT.

The HSRP active router (primary MPLS CE) can use the IP SLA feature to send echo probes to its MPLS PE router, and if the PE router becomes unreachable, then the router can lower its HSRP priority, so that the HSRP standby router can preempt and become the HSRP active router.

This procedure is valid only on the router connected to the primary transport.

### Step 1: Enable the IP SLA probe.

Use standard ICMP echo (ping) probes, and send them at 15-second intervals. Responses must be received before the timeout of 1000 ms expires. If you are using the MPLS PE router as the probe destination, ensure the destination address is the same as the BGP neighbor address.

```
ip sla 100
 icmp-echo [probe destination IP address] source-interface
 [WAN interface]
 threshold 1000
 timeout 1000
 frequency 15
 ip sla schedule 100 life forever start-time now
```

### Step 2: Configure EOT.

A tracked object is created based on the IP SLA probe. The object being tracked is the reachability success or failure of the probe. If the probe is successful, the tracked object status is up; if it fails, the tracked object status is down.

```
track 50 ip sla 100 reachability
```

**Step 3:** Link HSRP with the tracked object. You should enable HSRP tracking for all data or voice subinterfaces.

HSRP can monitor the tracked object status. If the status is down, the HSRP priority is decremented by the configured priority. If the decrease is large enough, the HSRP standby router preempts.

```
interface [interface type] [number].[sub-interface number]
 standby 1 track 50 decrement 10
```

### Example

```
interface GigabitEthernet0/2.64
 standby 1 track 50 decrement 10
!
interface GigabitEthernet0/2.69
 standby 1 track 50 decrement 10
!
track 50 ip sla 100 reachability
!
ip sla 100
 icmp-echo 192.168.4.22 source-interface GigabitEthernet0/0
 threshold 1000
 timeout 1000
 frequency 15
 ip sla schedule 100 life forever start-time now
```

## Procedure 5 Configure loopback resiliency

The remote-site routers have in-band management configured via the loopback interface. To ensure reachability of the loopback interface in a dual-router design, you must advertise the loopback of the secondary router into the WAN routing protocol on the primary router.

**Step 1:** Configure BGP on the primary router to advertise the secondary router's loopback IP address.

```
router bgp 65511
 network 10.255.253.203 mask 255.255.255.255
```

## Process

### Configuring 3G/4G Router for Dual-Router Design

1. Configure access layer HSRP
2. Configure transit network
3. Configure EIGRP (LAN side)
4. Configure loopback resiliency

This process is required for the dual-router design. The following procedures include examples for the secondary 3G or 4G DMVPN router only.

## Procedure 1 **Configure access layer HSRP**

You need to configure HSRP to enable the use of 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 or 4G 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 14 - WAN remote-site HSRP parameters (dual router)

Router	HSRP role	Virtual IP address (VIP)	Real IP address	HSRP priority	PIM DR priority
MPLS CE (primary)	Active	.1	.2	110	110
DMVPN Spoke	Standby	.1	.3	105	105

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.



## Tech Tip

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.

### Step 1: Configure access layer HSRP.

```
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 10.4.48.10
 ip pim sparse-mode
 ip pim dr-priority 105
 standby version 2
 standby 1 ip [LAN network 1 gateway address]
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

Repeat this procedure for all data or voice subinterfaces.

## Example: Layer 2 EtherChannel

```
interface PortChannel2.64
description Data
encapsulation dot1Q 64
ip address 10.5.116.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.116.1
standby 1 priority 105
standby 1 preempt
standby 1 authentication md5 key-string cisco123
```

## Example: Layer 2 Link

```
interface GigabitEthernet0/2.64
description Data
encapsulation dot1Q 64
ip address 10.5.116.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.116.1
standby 1 priority 105
standby 1 preempt
standby 1 authentication md5 key-string cisco123
```

## Procedure 2

### Configure transit network

The transit network is configured between the two routers. This network is used for router-to-router communication and to avoid hairpinning. 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.

**Step 1:** Configure the transit network subinterface.

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

### Example

```
interface GigabitEthernet0/2.99
description Transit Net
encapsulation dot1Q 99
ip address 10.5.112.2 255.255.255.252
ip pim sparse-mode
```

**Step 2:** Add transit network VLAN to existing access layer switch trunk.

```
interface GigabitEthernet1/0/23
switchport trunk allowed vlan add 99
```

## Procedure 3

### Configure EIGRP (LAN side)

You must configure a routing protocol 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.

Configure EIGRP-100 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 DMVPN mGRE interface as an EIGRP interface.

```
router eigrp 100
 network [network] [inverse mask]
 network [remote site loopback range] [inverse mask]
 passive-interface default
 no passive-interface [Transit interface]
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

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

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 100
 redistribute eigrp 200
```

### Example

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 200
 passive-interface default
 no passive-interface GigabitEthernet0/2.99
 eigrp router-id 10.255.253.222
 no auto-summary
```

## Procedure 4 Configure loopback resiliency

The remote-site routers have in-band management configured via the loopback interface. To ensure reachability of the loopback interface in a dual-router design, redistribute the loopback of the adjacent primary router into the WAN routing protocol EIGRP-200 (DMVPN).

**Step 1:** Configure an access list to limit the redistribution to only the adjacent router's loopback IP address.

```
ip access-list standard R[number]-LOOPBACK
 permit [IP Address of Adjacent Router Loopback]
 route-map LOOPBACK-ONLY permit 10
 match ip address R[number]-LOOPBACK
```

### Example

```
ip access-list standard R1-LOOPBACK
 permit 10.255.252.222
 !
 route-map LOOPBACK-ONLY permit 10
 match ip address R1-LOOPBACK
```

**Step 2:** Configure EIGRP to redistribute the adjacent router's loopback IP address learned from EIGRP-100 into EIGRP-200 (DMVPN). The route-map limits the redistribution to a single route. The EIGRP stub routing must be adjusted to permit redistributed routes.

```
router eigrp 200
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 eigrp stub connected summary redistributed
```

## Process

Controlling Usage of 3G or 4G Interface

1. Schedule auto-control of interface
2. Monitor reachability of upstream router

Many 3G or 4G 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 or 4G solution, it is a best practice to limit the use of the wireless WAN specifically to the periods where it must active.

A 3G or 4G 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 or 4G as a primary link according to a 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 interface

This procedure should be used to control the 3G or 4G interface usage for the single-link design. The 3G or 4G interface is controlled using the Embedded Event Manager (EEM) time-based scheduling using cron.

**Step 1:** Configure EEM scripting to enable or disable the 3G or 4G interface.

A cron EEM script is activated based on a schedule and runs specified router Cisco 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]"
```

## Examples

The following is an EEM script to enable 3G or 4G 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"
```

The following is an 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 or 4G interface usage for the dual-link designs (single-router, dual-link and dual-router, dual-link). The MPLS VPN link is the primary WAN transport, and as long as it is operational, the cellular interface remains shut down.



## Tech Tip

If using the WAN25 or WAN75 designs with static routing, if the cellular interface is brought up when the MPLS VPN link is still operational, all traffic to and from the remote site will use the 3G/4G link.

The remote-site 3G or 4G 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 or 4G 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]
 threshold 1000
 timeout 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 that is monitored by EEM scripts.

```
track [object number] ip sla [probe number] reachability
```

### Step 3: Configure EEM scripting to enable or disable the 3G or 4G interface.

An event-tracking EEM script monitors the state of an object and runs router Cisco 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]"
```

### Examples

```
track 60 ip sla 100 reachability
ip sla 100
 icmp-echo 192.168.3.34 source-interface GigabitEthernet0/0
 threshold 1000
 timeout 1000
 frequency 15
 ip sla schedule 100 life forever start-time now
```

The following is an 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"
```

The following is an 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"
```

## Process

### Implementing Automated Recovery for 4G/LTE Interface

1. Download recovery scripts
2. Install and configure the scripts

There are instances where the 4G/LTE EHWIC experiences an out-of-sync condition with its on-board LTE modem. These include: losing then regaining signal, fallback to 3G data rates and recovery to LTE, and other network-related events. When this occurs, the modem may become inoperative; the cellular interface appears up to the ISR but no data can be transmitted or received.

Cisco has developed Tool Command Language (TCL) scripts for automated recovery when these error conditions are present.

This process provides the necessary details for downloading and installing the TCL scripts and configuring the router for automated recovery with these scripts. This process should be completed after all other router configuration is complete.

## Procedure 1

### Download recovery scripts

**Step 1:** Download the automated recovery script from cisco.com.

The scripts are posted here:

<http://www.cisco.com/cisco/pub/software/portal/select.html?&i=!m&mdfid=283733571>

The screenshot shows the Cisco Download Software interface. The breadcrumb trail is: Downloads Home > Products > Cisco Interfaces and Modules > Cisco High-Speed WAN Interface Cards > Cisco 4G LTE Wireless WAN Enhanced High-speed WAN Interface Card > Cellular Recovery Script-LTE\_RECOVERY\_1.0. The main heading is "Cisco 4G LTE Wireless WAN Enhanced High-speed WAN Interface Card". Below this, there is a search bar and a "Release LTE\_RECOVERY\_1.0" section. A table lists the files for this release:

File Information	Release Date	Size	
Cellular LTE link recovery and profile configuration scripts lte_recovery_v1.0.tar	03-MAY-2012	0.80 MB	<a href="#">Download</a> <a href="#">Add to cart</a>

**Step 2:** Extract files from the downloaded archive file by using a file archiver program (such as 7-Zip) to open the archive. The following two scripts are required:

```
cell_cli_v1.tcl  
cell_recovery_v1.tcl
```

**Step 3:** Make the files available for download on a Trivial File Transfer Protocol (TFTP) server.



### Tech Tip

Other methods for file transfer include HTTP(S), FTP, and SCP.

## Procedure 2

### Install and configure the scripts

**Step 1:** Create a scripts subdirectory on the router's flash memory.

```
mkdir flash:/scripts
```

**Step 2:** Copy scripts from file server to the router.

```
copy tftp://[file server IP]/cell_cli_v1.tcl flash:/scripts/  
copy tftp://[file server IP]/cell_recovery_v1.tcl flash0:/  
scripts/
```

**Step 3:** Configure EEM scripting to enable the recovery scripts.

The scripts require that you set environment variables for proper operation.

```
event manager environment cell_int [cellular interface number]  
event manager environment sysboot_time [delay after bootup  
(sec)]  
event manager environment ip2ping [DMVPN NHS address]  
event manager directory user policy "[script directory]"
```

#### Example

```
event manager environment cell_int Cellular0/0/0  
event manager environment sysboot_time 300  
event manager environment ip2ping 10.4.34.1  
event manager directory user policy "flash:/scripts/"
```

**Step 4:** Activate the automated recovery scripts.

```
event manager scheduler script thread class N number 1  
event manager policy cell_recovery_v1.tcl class N  
authorization bypass  
event manager policy cell_cli_v1.tcl class N
```

## Process

### Configuring WAN Quality of Service

1. Create the QoS maps to classify traffic
2. Add ISAKMP traffic to network-critical
3. Define policy map to use queuing policy
4. Configure physical interface S&Q policy
5. Apply WAN QoS policy to physical interface

When configuring the WAN-edge QoS, you are defining how traffic egresses your network. It is critical that the classification, marking, and bandwidth allocations align to the service provider offering to ensure consistent QoS treatment end to end.

The QoS policies referenced in this process are consistent with those used in other SBA WAN deployment guides and include traffic types, such as voice and interactive video, which are not typically recommended for use on 3G and 4G links. It is useful to include all traffic classes in the QoS policy so that the network operator can verify that the actual traffic transmitted per class matches the expected values.

## Procedure 1

### Create the QoS maps to classify traffic

This procedure applies to all WAN routers.

Use the **class-map** command to define a traffic class and identify traffic to associate with the class name. These class names are used when configuring policy maps that define actions you want to take against the traffic type. The **class-map** command sets the match logic. In this case, the match-any keyword indicates that the maps match any of the specified criteria. This keyword is followed by the name you want to assign to the class of service. After you have configured the **class-map** command, you define specific values, such as DSCP and protocols to match with the match command. You use the following two forms of the **match** command: **match dscp** and **match protocol**.

Use the following steps to configure the required WAN class-maps and matching criteria.

**Step 1:** Create the class maps for DSCP matching. Repeat this step to create a class-map for each of the six WAN classes of service listed in the following table.

You do not need to explicitly configure the default class.

```
class-map match-any [class-map name]
  match dscp [dscp value] [optional additional dscp value(s)]
```

Table 15 - QoS classes of service

Class of service	Traffic type	DSCP values	Bandwidth %	Congestion avoidance
VOICE	Voice traffic	ef	10 (PQ)	-
INTERACTIVE-VIDEO	Interactive video (video conferencing)	cs4, af41	23 (PQ)	-
CRITICAL-DATA	Highly interactive (such as Telnet, Citrix, and Oracle thin clients)	af31, cs3	15	DSCP based
DATA	Data	af21	19	DSCP based
SCAVENGER	Scavenger	af11, cs1	5	-
NETWORK-CRITICAL	Routing protocols, Operations, administration and maintenance (OAM) traffic.	cs6, cs2	3	-
default	Best effort	Other	25	random

## Example

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



### Tech Tip

You do not need to configure a Best-Effort Class. This is implicitly included within class-default as shown in Procedure 4 in this process.

## Procedure 2

### Add ISAKMP traffic to network-critical

For a WAN connection using DMVPN, you need to ensure proper treatment of ISAKMP traffic in the WAN. To classify this traffic requires the creation of an access-list and the addition of the access-list name to the NETWORK-CRITICAL class-map created in Procedure 1.

This procedure is only required for a WAN-aggregation DMVPN hub router or a WAN remote-site DMVPN spoke router.

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

```
ip access-list extended ISAKMP
 permit udp any eq isakmp any eq isakmp
```

**Step 2:** Add the match criteria to the existing NETWORK-CRITICAL class-map.

```
class-map match-any NETWORK-CRITICAL
 match access-group name ISAKMP
```

### Procedure 3 Define policy map to use queuing policy

This procedure applies to all WAN routers.

The WAN policy map references the class names you created in the previous procedures and defines the queuing behavior along with the maximum guaranteed bandwidth allocated to each class. This specification is accomplished with the use of a policy-map. Then, each class within the policy map invokes an egress queue, assigns a percentage of bandwidth, and associates a specific traffic class to that queue. One additional default class defines the minimum allowed bandwidth available for best effort traffic.



#### Tech Tip

The local router policy maps define seven classes while most service providers offer only six classes of service. The NETWORK-CRITICAL policy map is defined to ensure the correct classification, marking, and queuing of network-critical traffic on egress to the WAN. After the traffic has been transmitted to the service provider, the network-critical traffic is typically remapped by the service provider into the critical data class. Most providers perform this remapping by matching on DSCP values cs6 and cs2.

**Step 1:** Create the parent policy map.

```
policy-map [policy-map-name]
```

**Step 2:** Repeat Step 3 through Step 6 for each class in Table 15, including class-default.

**Step 3:** Apply the previously created class-map.

```
class [class-name]
```

**Step 4:** If you want, you can assign the maximum guaranteed bandwidth for the class.

```
bandwidth percent [percentage]
```

**Step 5:** If you want, you can define the priority queue for the class.

```
priority percent [percentage]
```

**Step 6:** If you want, you can define the congestion mechanism.

```
random-detect [type]
```

#### Example

```
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
```



## Tech Tip

Although these bandwidth assignments represent a good baseline, it is important to consider your actual traffic requirements per class and adjust the bandwidth settings accordingly.

### Procedure 4 Configure physical interface S&Q policy

With WAN interfaces using 3G/4G as an access technology, the demarcation point between the enterprise and service provider may no longer have a physical-interface bandwidth constraint. Instead, each 3G/4G technology provides a variable uplink speed depending on signal strength and other conditions.

To ensure the offered load to the service provider does not exceed the capabilities of the link that results in oversubscription, you need to configure shaping on the physical interface. This shaping is accomplished with a QoS service policy. You configure a QoS service policy on the outside Ethernet interface, and this parent policy includes a shaper that then references a second or subordinate (child) policy that enables queuing within the shaped rate. This is called a hierarchical Class-Based Weighted Fair Queuing (HCBWFQ) configuration. When you configure the **shape average** command, ensure that the value matches the contracted bandwidth rate from your service provider.

This procedure applies to all 3G/4G WAN routers. Suggested bandwidth parameters are included in the following table.

Table 16 - 3G and 4G bandwidth parameters

Technology	Downlink speed (Kbps)	Uplink speed (Kbps)
GSM 3G HSPA+	21600	5760
CDMA 3G	3100	1800
LTE 4G	8000 to 12000 (range)	2000 to 5000 (range)

**Step 1:** Create the parent policy map.

As a best practice, embed the interface name within the name of the parent policy map.

```
policy-map [policy-map-name]
```

**Step 2:** Configure the shaper.

```
class [class-name]
  shape [average | peak] [bandwidth (kbps)]
```

**Step 3:** Apply the child service policy.

```
service-policy [policy-map-name]
```

### Example

This example shows a router with a 1.8-Mbps link on interface Dialer1.

```
policy-map WAN-INTERFACE-Dialer1
  class class-default
    shape average 1800000
  service-policy WAN
```

### Procedure 5 Apply WAN QoS policy to physical interface

To invoke shaping and queuing on a physical interface, you must apply the parent policy that you configured in the previous procedure.

This procedure applies to all WAN routers. You can repeat this procedure multiple times to support devices that have multiple WAN connections attached to different interfaces.

**Step 1:** Select the WAN interface.

```
interface [interface type] [number]
```

**Step 2:** Apply the WAN QoS policy.

The service policy needs to be applied in the outbound direction.

```
service-policy output [policy-map-name]
```

### Example

```
interface Dialer1
  service-policy output WAN-INTERFACE-Dialer1
```

# Appendix A: Product List

## WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.2(4)M1 securityk9, datak9
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
	3G EV-DO Wireless WAN EHWIC supporting 1xRTT, EV-DO Rev A/Rev 0 (Verizon SKU)	EHWIC-3G-EVDO-V	
	3.7G HSPA Wireless WAN EHWIC supporting GPRS/EDGE/UMTS/HSDPA/HSUPA/HSPA (North America SKU)	EHWIC-3G-HSPA+7-A	
	4G LTE EHWIC for Verizon, 700 MHz Band 13 / CDMA Rev A	EHWIC-4G-LTE-V	
Modular WAN Remote-site Router	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	15.2(4)M1 securityk9, datak9
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	
	3G EV-DO Wireless WAN EHWIC supporting 1xRTT, EV-DO Rev A/Rev 0 (Verizon SKU)	EHWIC-3G-EVDO-V	
	3.7G HSPA Wireless WAN EHWIC supporting GPRS/EDGE/UMTS/HSDPA/HSUPA/HSPA (North America SKU)	EHWIC-3G-HSPA+7-A	
	4G LTE EHWIC for Verizon, 700 MHz Band 13 / CDMA Rev A	EHWIC-4G-LTE-V	
Modular WAN Remote-site Router	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	15.2(4)M1 securityk9, datak9
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	
	3G EV-DO Wireless WAN EHWIC supporting 1xRTT, EV-DO Rev A/Rev 0 (Verizon SKU)	EHWIC-3G-EVDO-V	
	3.7G HSPA Wireless WAN EHWIC supporting GPRS/EDGE/UMTS/HSDPA/HSUPA/HSPA (North America SKU)	EHWIC-3G-HSPA+7-A	
	4G LTE EHWIC for Verizon, 700 MHz Band 13 / CDMA Rev A	EHWIC-4G-LTE-V	
Fixed WAN Remote-site Router	Cisco 819 Integrated Services Router	CISCO819G-x-K9 or CISCO819HG-x-K9	15.2(4)M1 securityk9, datak9
	Cisco 819 Integrated Services Router	CISCO819G-S-K9 or CISCO819HG-S-K9	

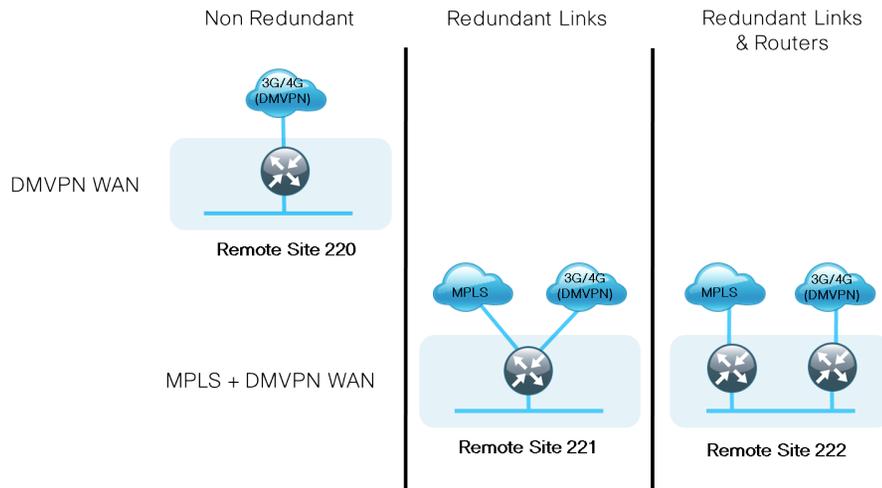
## LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) IP Base
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(1)SE2 LAN Base
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

# 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 14 - WAN remote-site designs



## Notes

Table 17 - Remote-site WAN connection details

Remote-Site Information		MPLS (Our AS = 65511)			DMVPN	LAN interfaces	Loopbacks
Location	Net block	MPLS CE	MPLS PE	Carrier AS			
RS220 [HSPA+]	10.5.216.0/21				(dialer1) SLIP	(gi0/1)	10.5.216.254 (r)
RS220 [LTE]	10.5.216.0/21				(dialer1) SLIP	(gi0/1)	
RS221 [CDMA]	10.5.24.0/21	(gi0/0) 192.168.3.33	192.168.3.34	65401 (A)	(dialer1) PPP	(gi0/2)	10.5.24.254 (r)
RS222 (dual router) [CDMA]	10.5.24.0/21	(gi0/0) 192.168.3.33	192.168.3.34	65401 (A)	(dialer1) PPP	(gi0/2) (gi0/2)	10.5.24.254 (r1) 10.5.24.253 (r2)

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

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

Table 18 - Remote-site 220— IP address information

Remote-site information		Wired subnets		Wireless subnets		Operational IP assignments	
Location	Net block	Data (Vlan 64)	Voice (Vlan 69)	Data (Vlan 65)	Voice (Vlan 70)	Loopbacks and switches	WAE
RS220	10.5.216.0/21	10.5.220.0/24	n/a	10.5.218.0/24	n/a	10.255.253.220 (r) 10.5.220.5 (sw)	WAASx

### RS220-1941 (with GSM 3G HSPA+)

```
version 15.2
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 name TACACS-SERVER-1
!
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
service-module wlan-ap 0 bootimage autonomous
!
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 HSPA "" "AT!SCACT=1,1" TIMEOUT 60 "OK"
!
crypto pki token default removal timeout 0
!
```

```

license udi pid CISCO1941W-A/K9 sn FTX1447003H
license boot module c1900 technology-package securityk9
hw-module ism 0
!
!
!
username admin password 7 141443180F0B7B7977
!
redundancy
!
!
!
!
controller Cellular 0/0
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
  match 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 dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match 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 5760000
    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 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 10.255.253.220 255.255.255.255
!
interface Tunnel10
  bandwidth 384
  ip address 10.4.34.220 255.255.254.0
  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 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 5760
  no ip address
  encapsulation slip
  dialer in-band
  dialer pool-member 1
  no peer default ip address
  async mode interactive
  service-policy output WAN-INTERFACE-Dialer1
!

```

```

interface Vlan1
  no ip address
!
interface Dialer1
  bandwidth 5760
  ip vrf forwarding INET-PUBLIC
  ip address negotiated
  ip access-group ACL-INET-PUBLIC in
  encapsulation slip
  dialer pool 1
  dialer idle-timeout 0
  dialer string HSPA
  dialer persistent
  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
  network 10.255.0.0 0.0.255.255
  passive-interface default
  no passive-interface Tunnel10
  eigrp router-id 10.255.253.220
  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
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key 7 113A1C0605171F270133
!
!
control-plane
!
!
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line 0/0/0
  script dialer HSPA
  modem InOut
  no exec
  rxspeed 21600000
  txspeed 5760000
line 67
  no activation-character

```

```

no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
transport input ssh
line vty 5 15
transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
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"
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

```

## RS220-1941 (with 4G/LTE)

```

version 15.2
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 name TACACS-SERVER-1
!
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
service-module wlan-ap 0 bootimage autonomous
!
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 LTE "" "AT!CALL1" TIMEOUT 20 "OK"
crypto pki token default removal timeout 0
!
license udi pid CISCO1941W-A/K9 sn FTX1447003H
license boot module c1900 technology-package securityk9
hw-module ism 0
!
!
!
username admin password 7 141443180F0B7B7977
!
redundancy
!
!
!
!
controller Cellular 0/0
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
  match 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 dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match 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 2000000
    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 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 10.255.253.220 255.255.255.255
!
interface Tunnel10
  bandwidth 2000
  ip address 10.4.34.220 255.255.254.0
  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 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 2000
no ip address
encapsulation slip
dialer in-band
dialer pool-member 1
no peer default ip address
async mode interactive
service-policy output WAN-INTERFACE-Dialer1
!
interface Vlan1
no ip address
!
interface Dialer1
bandwidth 2000
ip vrf forwarding INET-PUBLIC
ip address negotiated
ip access-group ACL-INET-PUBLIC in
encapsulation slip
dialer pool 1
dialer idle-timeout 0
dialer string LTE
dialer persistent
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
network 10.255.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel10

```

```

eigrp router-id 10.255.253.220
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
!
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key 7 113A1C0605171F270133
!
!
control-plane

```

```

!
!
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line 0/0/0
  script dialer LTE
  modem InOut
  no exec
line 67
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
  transport input ssh
line vty 5 15
  transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
event manager applet TIME-OF-DAY-ACTIVATE-4G
  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 4G interface"
event manager applet TIME-OF-DAY-DEACTIVATE-4G
  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 4G interface"
!
end

```

## Remote-Site 221: Single-Router, Dual-Link

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

Table 19 - Remote-site 221— IP address information

Remote-site information		Wired subnets		Wireless subnets		Operational IP assignments
Location	Net block	Data (Vlan 64)	Voice (Vlan 69)	Data (Vlan 65)	Voice (Vlan 70)	Loopbacks and switches
RS221	10.5.24.0/21	10.5.28.0/24	10.5.29.0/24	10.5.26.0/24	10.5.27.0/24	10.255.253.221 (r) 10.5.28.5 (sw)

### RS221-2921

```
version 15.2
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$6eDcL43qiYsgeZtF4VxWT.
!
aaaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
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 ssh source-interface Loopback0
ip ssh version 2
!
track 60 ip sla 100 reachability
!
class-map match-any DATA
  match 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 dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match 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 10.255.253.221 255.255.255.255
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
encapsulation dot1Q 64
ip address 10.5.28.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
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
network 10.255.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel10
eigrp router-id 10.255.253.221
eigrp stub connected summary
!
router bgp 65511
bgp router-id 10.255.251.221
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 10.255.253.221 mask 255.255.255.255
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 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 TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 113A1C0605171F270133!
!
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 20 - Remote-site 222— IP address information

Remote-site information		Wired subnets		Wireless subnets		Operational IP assignments
Location	Net block	Data (Vlan 64)	Voice (Vlan 69)	Data (Vlan 65)	Voice (Vlan 70)	Loopbacks and switches
RS222	10.5.24.0/21	10.5.28.0/24	10.5.29.0/24	10.5.26.0/24	10.5.27.0/24	10.255.251.222 (r1) 10.255.253.222 (r2) 10.5.28.5 (sw)

### 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
!
!
enable secret 5 $1$yUWN$6eDcL43qiYsgeZtF4VxWT.
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
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 multicast-routing
!
!
no ip domain lookup
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
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
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
track 50 ip sla 100 reachability
!
class-map match-any DATA
  match 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 dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match 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
  class class-default
    bandwidth percent 25
    random-detect
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 10000000
    service-policy WAN
!
!
!
!
interface Loopback0

```

```

ip address 10.255.251.222 255.255.255.255
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
!

```

```

!
router eigrp 100
 default-metric 100000 100 255 1 1500
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface GigabitEthernet0/2.99
 eigrp router-id 10.255.251.222
!
router bgp 65511
 bgp router-id 10.255.251.222
 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 10.255.251.222 mask 255.255.255.255
 network 10.255.253.222 mask 255.255.255.255
 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 TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 113A1C0605171F270133
!
!
control-plane
!
!
!
!
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 15.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service internal
!
hostname RS222-2921-2
!
!
logging buffered 1024000
enable secret 5 $1$yUWN$6eDcL43qiYsgeZtF4VxWT.
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
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 ssh source-interface Loopback0
ip ssh version 2
!
track 60 ip sla 100 reachability
!
class-map match-any DATA
  match 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 dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match 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 Data1

```

```

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
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
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
  description Transit Net
  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
  network 10.255.0.0 0.0.255.255
  redistribute eigrp 100 route-map LOOPBACK-ONLY

```

```

  passive-interface default
  no passive-interface Tunnel10
  eigrp router-id 10.255.253.222
  eigrp stub connected summary redistributed
!
!
router eigrp 100
  network 10.5.0.0 0.0.255.255
  network 10.255.0.0 0.0.255.255
  redistribute eigrp 200
  passive-interface default
  no passive-interface GigabitEthernet0/2.99
  eigrp router-id 10.255.253.222
!
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 standard R1-LOOPBACK
  permit 10.255.251.222
!
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
!
!
!
!
!
route-map LOOPBACK-ONLY permit 10
 match ip address R1-LOOPBACK
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 113A1C0605171F270133
!
!
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 "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 "Deactivating 3G interface"
!
end

```

# Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- To enable 4G/LTE interface support, the EHWIC-4G-LTE-V is now included and relevant procedures to support its usage were added.
- The “Implementing Automated Recovery for 4G/LTE Interface” section was added.

## Notes

## Feedback

Click [here](#) to provide feedback to Cisco SBA.



SMART BUSINESS ARCHITECTURE

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 NON-INFRINGEMENT 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.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

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

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)