Newer Cisco SBA for Government Guides Available

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

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.

Wireless Remote Site Deployment Guide

SBA FOR GOVERNMENT

Revision: H2CY10

The Purpose of this Document

This guide demonstrates a secondary or alternate means of connecting a remote site using an available cellular network.

It explains the requirements that were considered when building the Cisco Smart Business Architecture (SBA) for Government design and introduces each of the products that were selected.

Who Should Read This Guide

This guide is intended for the reader who is looking for any or all of the following:

- More advanced features than are available in the SBA foundation branch module
- Cellular backup or the ability to leverage cellular connectivity in the branch
- Alternative integrated connectivity
- Truly mobile connectivity, where physical connectivity is impossible
- The ability to reduce cost by optimizing connectivity solutions and improve employee productivity
- The assurance of a tested solution

- The reader should have:
- An agency with 100–1000 connected employees
- IT workers with a CCNA® certification or equivalent experience

Related Documents

BN — Design Overview

BN — Foundation Deployment Guide

DC — Data Center Deployment Guide

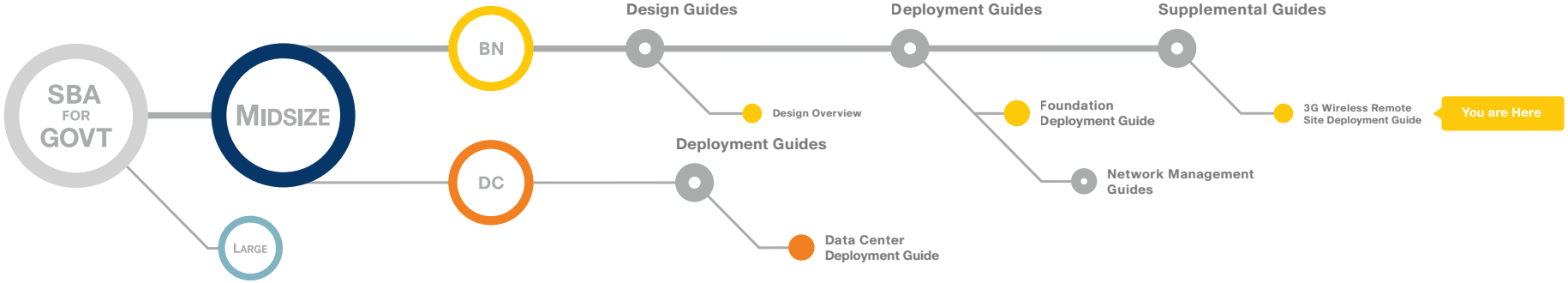


Table of Contents

Introduction

The Cisco® SBA is a comprehensive design for networks with up to 1000 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible.

The Cisco SBA for Midsize incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your agency's problems rather than worrying about the technical details.

We have designed the Cisco SBA to be easy to configure, deploy, and manage. This architecture:

- Provides a solid network foundation
- Makes deployment fast and easy
- Accelerates your ability to easily deploy additional services
- Avoids the need for re-engineering of the core network

By deploying the Cisco SBA, your agency can gain:

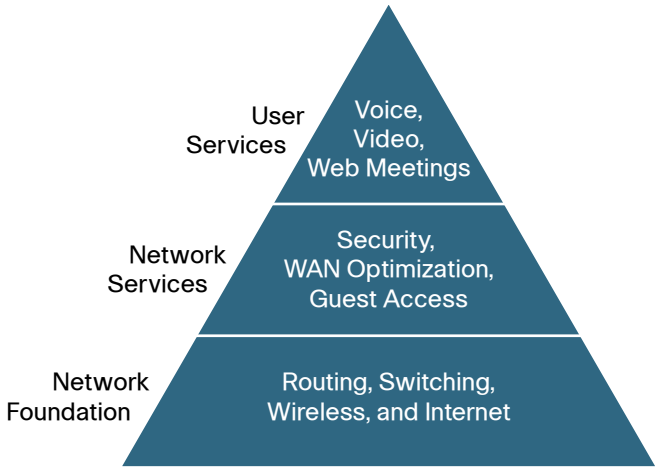
- A standardized design, tested and supported by Cisco
- Optimized architecture for midsize agencies with up to 1000 users and up to 20 remote sites
- Flexible architecture to help ensure easy migration as the agency grows
- Seamless support for quick deployment of wired and wireless network access for data, voice, teleworker, and wireless guest
- Security and high availability for agency information resources, servers, and Internet-facing applications
- Improved WAN performance and cost reduction through the use of WAN optimization
- Simplified deployment and operation by IT workers with a CCNA® certification or equivalent experience
- Cisco enterprise-class reliability in products designed for midsize agencies

Guiding Principles

The deployment process was divided into modules according to the following principles:

- **Ease of use:** A top requirement of Cisco SBA was to develop a design that could be deployed with the minimal amount of configuration and day-two management.
- **Cost-effective:** Another critical requirement in the selection of products was to meet the budget guidelines for an agency of this size.
- **Flexibility and scalability:** As the agency grows, so too must its infrastructure. Products selected needed to have the ability to grow or be repurposed within the architecture.
- **Reuse:** The goal, when possible, was to reuse the same products throughout the various modules to minimize the number of products required for spares.

Figure 1. SBA Model



The Cisco SBA can be broken down into three primary modular, yet interdependent, components for the midsize agency. They are the Network Foundation, Network Services, and User Services.

- A network that provides the foundation
- Network services that operate in the background to improve and enable the experience without direct user awareness
- User services that are the applications with which a user interacts directly

Agency Overview

The Case for Wireless

Connectivity to the agency's data is no longer confined to the walls of the building. 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 2. 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 branch office provides an always-accessible network for the applications users interact with directly, from site-to-site backup and recovery to using the email service to read email. How well users interact with the network and their ability to reach essential services impacts the agency's overall performance.

Reliable Network Services provided by Cisco SBA, such as the Internet connection, wide-area network (WAN) infrastructure, and security, help ensure an agency can rely on applications such as Web conferencing for critical collaboration.

High availability at the Branch is an essential requirement for productivity, safety, and security within the majority of agencies. Therefore the ability to maintain connectivity for critical data transactions is imperative to the Cisco SBA for Midsize Agencies design.

SBA for Midsize Agencies is a prescriptive architecture that delivers an easy-to-use, flexible, and scalable network with wired, wireless, 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 SBA, visit: http://www.cisco.com/go/sba or http://www.cisco.com/go/partner/smartarchitecture

Technology Overview

Cellular Options

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

Code Division Multiple Access

CDMA has its roots in World War II. It only relates to over-the-air transmission, giving each user the full use of the radio spectrum, which can provide higher data rates than can be achieved with GSM, which 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 branch office, given that CDMA is predominately used within the United States, but used rarely elsewhere in the world, and is nonexistent in Europe because the European Union mandates the sole use of GSM.

Global System for Mobile Communications

GSM was invented in 1987 by the GSM Association, an international organization dedicated to developing the GSM standard worldwide. The data rates are typically lower than what can be found from 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 the 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), that theoretically can achieve data rates up to 14 Mb/s. Some carriers are beginning to offer the latest Fourth Generation (4G) standard, which promises up to Gigabit data rates, and must be able to at least achieve 100 Mb/s data rates. Both of these standards are defined by the International Telecommunication Union (ITU).

According to the ITU requirements, a 4G cellular system must have target peak data rates of up to approximately 100 Mbit/s for high mobility such as mobile access and up to approximately 1 Gbit/s for low mobility such as nomadic/local wireless access. The promise of these data rates and bandwidth brings interesting opportunities with technology to the remote branch offices.

Tech Tip

The solution presented in this guide leverages the Cisco Integrated Services Router running Cisco IOS® Software. It contained both a CDMA and GSM HWIC running in the same chassis. As you follow this deployment guide, you will find that each of these interfaces are referenced in different locations that illustrate this point.

Deploying Branch Cellular Backup

Before you begin the deployment process, you need to determine which technology to leverage and 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 branch office will be located?

Contact your local service provider to see what is in your area. As an example: Europe has mandated GSM for all cellular.

Do you want or require redundant hardware for hot swap should a failure occur?

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

Is high data throughput a requirement?

Although the difference in data throughput for each technology is closing, CDMA is still the clear leader.

Will your office move from region to region?

If your branch has wheels and moves around, such as a health clinic, you may wish to include both CDMA and GSM within your solution, so that you may choose the best operator for your site.

If price of service or service provider offerings are factors, which will provide the best feature/price for your branch?

Some service providers offer both a business and wireless service to provide an alternative connection away from the public network (Internet) and drop you on your private Multiprotocol Label Switching (MPLS) network.

Where security is a requirement, some service providers can provide a direct connection to customers' MPLS networks.

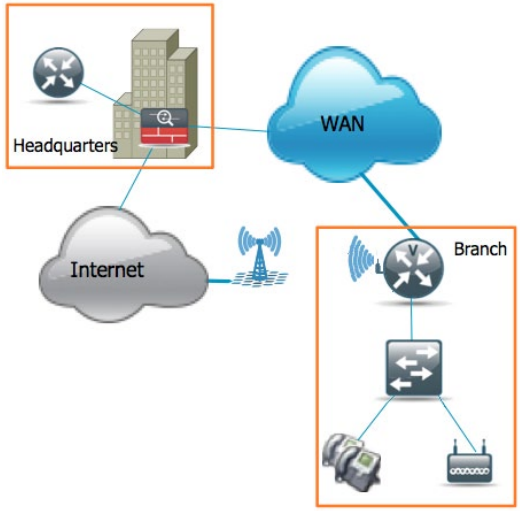
GSM allows individuals to move from device to device without working through the service provider.

This guide addresses how you can leverage both technologies if your deployment is with a branch office that is on the move, possibly a disaster recovery vehicle, a mobile clinic, outdoor event data processing center, or some other truly "mobile branch." This is a unique requirement for the few places both technologies exist; making perhaps the United States the only region this would or could make sense.

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

Next you need to define the physical topology as shown below in Figure 3

Figure 3. Headquarters to Branch Topology



The Cisco 2911 Integrated Services Router (ISR) shown on Figure 4 has 4 interfaces

- 2 GigabitEthernet interfaces labeled G0/0 and G1/0
- 1 GSM HWIC interface labeled cellular 0/1/0
- 1 CDMA HWIC interface labeled cellular 0/2/0.

Figure 4. ISR with GSM HWIC installed

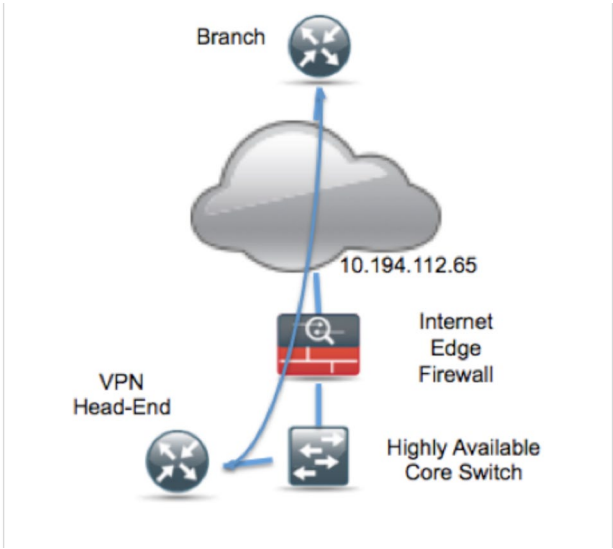
Process

Configuring Headquarters

1. Connect Peers to Headend DR Routers
2. Configure the Headquarters ASA

The Headquarters topology (see Figure 5) shows the Internet edge firewall passing VPN traffic through to the Integrated Services Router that plays the VPN headend within the SBA.

Figure 5. Headquarters Topology



Procedure 1 Connect Peers to Headend DR Routers

The following example shows the configuration needed to connect branch IPsec peers to the headend DR router. The design applies Cisco IOS IPsec Virtual Tunnel Interface (VTI) to provide encrypted transport of data and voice information with minimal configuration burden and maximum functionality. VTI offers two modes of operation:

- Static VTI can initiate tunnels to other static VTI sites.
- Multiple static VTI sites can initiate tunnels to a template-based dynamic VTI (DVTI) aggregation point that offers simple configuration.

VTI is recommended because:

- Dynamic VTI does not require that you know the remote sites' public address, which simplifies configuration for remote sites that may be assigned a dynamic address or translated by a (Network Address Translation) NAT.
- Dynamic VTI requires just one tunnel configuration for the headend, offering the least complex configuration and troubleshooting.
- VTI offers a virtual interface for applications of QoS policies, NAT, firewall, IPS, ACLs, and tunnel monitoring, as compared to traditional crypto-map VPN configuration.

- VTI configuration provides superior dynamic routing flexibility to enable the requirements of the SBA design.
- Remote sites initiate their connection to the DVTI responder on the headend router, which will create a virtual tunnel interface for every remote site's connection. DVTI applies a template-based configuration for remote sites' connectivity so that multiple tunnels may be created with one DVTI configuration; additional configuration is not needed to support multiple branches.

Tech Tip

Usually, when adding WAN redundancy to your Branch router, your headend or headquarters router or other termination point is already configured. However, with this document we will assume this is your first resilient branch office configuration leveraging the public network. If you are using a different policy with your headend encryption, you must follow the criteria set forth with your security policy and VPN configuration when you move to the final step of configuring your branch office router.

Step 1: Configure Internet Security-Association Key Management Protocol (ISAKMP) to define cryptographic shared-secret key and negotiation policy shared between remote sites and the headend:

```
crypto keyring sba-keys pre-shared-key address 0.0.0.0 0.0.0.0 key
sba crypto isakmp policy 1
encr aes authentication pre-share group 2
crypto isakmp profile sba-isakmp keyring sba-keys
match identity address 0.0.0.0 virtual-template 1
```

Step 2: Apply IPsec policy to define the cryptographic cipher that the router will apply to data transiting the tunnel. Cisco IOS Software supports a wide range of cryptographic transforms, from older Digital Encryption Standard (DES) and 3DES to various strengths of Advanced Encryption Standard (AES).

This example applies 128-bit AES, which is the current recommendation that offers the best combination of performance and cryptographic security. Note that the sba-xform label is used to apply the esp-aes IPsec policy to the IPsec profile.

```
crypto ipsec transform-set sba-xform esp-aes crypto ipsec
profile sba-ipsec
set transform-set sba-xform
```

Step 3: Configure the tunnel interface to define the IP address on the tunnel interface, as well as local and remote tunnel endpoints, and associates IPsec protection with the virtual interface.

```
interface Virtual-Template1 type tunnel ip unnumbered
Port-channel1.159 tunnel source FastEthernet0/2/0 tunnel mode
ipsec ipv4
tunnel protection ipsec profile sba-ipsec
```

Tech Tip

Use unique, intuitive labels for configuration of keyring, ISAKMP profile, and IPsec profile rather than general or random labels. This will make troubleshooting much easier.

Tech Tip

When applying the virtual-template configuration, be sure that you apply the type tunnel option. Without the option, Interface Virtual-Template will not apply to the cryptographic configuration.

Procedure 2 Configure the Headquarters ASA

The VPN hub is connected to the network core, behind the Internet edge firewall. The Internet Edge ASA must forward all incoming VPN traffic to the router's private IP address, and accommodate the VPN traffic in the ASA's outside-to-inside access policy.

Step 1: Apply the following configuration on the active Internet Edge ASA, to enable connectivity to the VPN headend by translating the outside address of 10.194.112.101 to the VPN headend's private address, 192.168.159.2. This configuration will allow VPN traffic to traverse the ASA and connect to the headend DR router.

```
name 192.168.159.2 vpn-hub
!object-group service isakmp-esp service-object esp service-
object udp eq 4500
!service-object udp eq isakmp
access-list outside_access_in extended permit object-group
isakmp-esp any host 10.194.112.101
!static (inside,outside) 10.194.112.101 vpn-hub netmask
255.255.255.255 ! access-group outside_access_in in interface
outside
```

Process

Configuring the ISR

1. Configure the Branch Office Router
2. Create an Access List

Once you have decided which technology you will leverage, it is time to configure the WSA.

Procedure 1 Configure the Branch Office Router

Step 1: With your service activated, work through the configuration process with each service provider to get your branch up and fully operational. Two separate deployment models are used:

- The first leveraging GSM with American Telephone & Telegraph (AT&T).
- The second using CDMA with Verizon Wireless.

Both of these technologies leverage a Cisco Third-Generation (3G) High-Performance WAN Interface Card (HWIC).

Tech Tip

Your carrier, the interface identifiers of the router, and IP addressing may differ; however, the approach and concepts illustrated in this guide will help you resolve these differences quickly.

Procedure 2 Create an Access List

Third-generation interfaces vary by technology, region, and sometimes simple physical placement of the received antenna.

In Europe, HSPA+ with its greater bandwidth, lower delay, and jitter can handle the rigors of voice and video applications. Elsewhere, delay and jitter can create challenges to voice and video. In those cases, an access-list should be applied preventing this kind of traffic from using this backup interface.

As there are so many different applications, the following example addresses only RTP traffic, but the same logic can be used for the applications where this may apply in your environment.

Step 1: Enter the following from the global configuration command:

```
access-list 101 deny tcp any any eq 2000
access-list 101 permit ip any any
```

Step 2: Enter the following from the Interface sub-command:

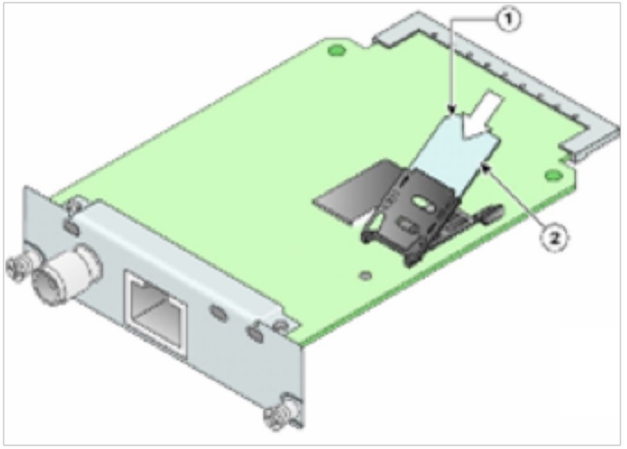
```
ip access-group 101 out
```

Process

Deploying Branch GSM

1. Install HWIC into ISR
2. Configure the Dialer Interface
3. Create Chat Script and AUX Line
4. Configure the Cellular Interface
5. Configure Routing

Figure 6. GSM HWIC SIM card installation



Tech Tip

You must get a data service account from your service provider. You should receive a SIM card that you should install on the 3G-HWIC.You will also receive the following information:

- PPP CHAP User-Name (hostname)
- PPP CHAP Password
- APN (Access Point Name)

Procedure 1 Install GSM HWIC into ISR

Step 1: Insert SIM card into HWIC as show in Figure 6

Step 2: Power off the Integrated Services Router

Step 3: Insert and fasten GSM HWIC into ISR

Step 4: Power on ISR and log in

Procedure 2 Configure the Dialer Interface

The Dialer interface brings capabilities to the 3G GSM interface that cannot be handled with the cellular interface alone.

Step 1: Apply the following configuration.

```
interface Dialer1
  ip address negotiated
!Specifies that the IP address with be negotiated with PPP
encapsulation ppp
  load-interval 30
  dialer pool 1
  dialer idle-timeout 0
  dialer string gsm
dialer persistent
  dialer-group 1
  no peer default ip address
  no ppp lcp fast-start
  ppp ipcp dns request
  ppp timeout retry 120
  ppp timeout ncp 30
```

Tech Tip

Dialer persistent, which is highlighted in Step 1, allows the cellular interface to come up and establish a PPP connection, but not pass any traffic until required. This will greatly reduce the failover times should it become required.

Procedure 3 Create Chat Script and AUX Line

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. Your 3G WAN interface should be treated just like any other asynchronous interface.

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

Step 1: Define a timeout value. This chat script is called "gsm" with a timeout value of 30 seconds. Note that your carrier may require a different chat script.

```
chat-script gsm "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
For the interface cellular0/1/0, the matching line would be:
line 0/1/0
  script dialer gsm
```

Step 2: From enable mode, use the profile to identify the username and password provided to you by your service provider. Use the cellular interface identifier and the keyword "gsm".

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

Procedure 4 Configure the Cellular Interface

Step 1: Before configuring the interface, identify traffic of interest for this interface, which is the traffic that triggers the interface to become active. From global configuration mode, enter the dialer-list configuration command:

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

Step 2: Apply the following configuration:

```
interface Cellular0/1/0
ip address negotiated
encapsulation ppp
load-interval 30
dialer in-band
dialer idle-timeout 300
dialer string gsm
dialer-group 1
no peer default ip address
async mode interactive
no ppp lcp fast-start
ppp chap hostname ISP@CINGULARGPRS.COM
ppp chap password 0 CINGULAR1
ppp ipcp dns request
ppp timeout retry 120
ppp timeout ncp 30
fair-queue 64 16 256
routing dynamic
```

Procedure 5 Configure Routing

The decision to use floating statics was based upon the SBA design requirements to keep the design straightforward, easy to understand, and at the same time, highly avaliable.

Step 1: There is not a default route, but a route to the directly connected gateway IP address and since the IP address is typically dynamic with the cellular interface, the physical interface is specified and weighted as 200. If the physical route to 10.0.2.5 is down, traffic will then forward to the encrypted gateway through the cellular interface.

```
ip route 10.194.112.101 255.255.255.255 Cellular0/1/0 200
ip route 10.194.112.101 255.255.255.255 10.0.2.5
```

Step 2: Never forget that the cellular interface is an asynchronous interface leveraging the dialer commands and you must specify traffic.

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

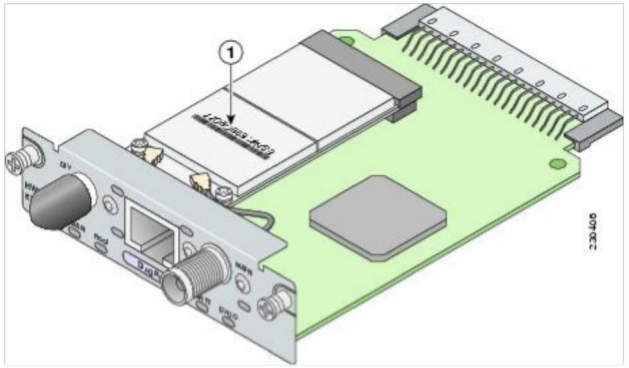
Process

Deploying Branch CDMA

1. Create Chat Script and AUX Line
2. Configure the Cellular Interface
3. Configure Routing

The CDMA deployment is different from the GSM deployment, as it has two fewer steps. You no longer require a profile and the interface does not need to use the dialer interface to maintain a persistent state.

Figure 7. 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.

Procedure 1 Install CDMA HWIC into ISR

Step 1: Register CDMA HWIC with SP using the ESN number found on the HWIC as illustrated above in Figure 7

Step 2: Power off the Integrated Services Router

Step 3: Insert and fasten CDMA HWIC into ISR

Step 4: Power on ISR and log in

Procedure 2 Create Chat Script and AUX Line

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. Your 3G WAN interface should be treated just like any other asynchronous interface.

Step 1: Apply the chat script described below, which shows the required information to connect to the Verizon CDMA network.

The CDMA chat script is similar to the GSM with the name "cdma" but with a timeout of 60 seconds. It is worth stating again that your specific CDMA service provider may have small variations to this script.

```
chat-script cdma "" "atdt#777" TIMEOUT 60 "CONNECT"
```

For the interface cellular0/2/0 from the sub-line, the configuration is:

```
line 0/2/0
script dialr cdma
```

Procedure 3 Configure the Cellular Interface

Step 1: Before configuring the interface, identify traffic of interest for this interface, which is the traffic that triggers the interface to become active. From global configuration mode, enter the dialer-list command:

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

Step 2: Apply the following configuration:

```
interface Cellular0/2/0
ip address negotiated
encapsulation ppp
dialer in-band
dialer idle-timeout 0
dialer string cdma
dialer-group 2
no peer default ip address
async mode interactive
no ppp lcp fast-start
ppp ipcp dns request
routing dynamic
```

Procedure 4 Configure Routing

The decision to use floating statics was based upon the SBA design requirements to keep the design straightforward, make it easy to understand, and achieve the best possible results.

Step 1: There is not a default route, but a route to the directly connected gateway IP address and since the IP address is typically dynamic with the cellular interface, the physical interface is specified and weighted as 200. If the physical route to 10.0.2.5 is down, traffic will then forward to the encrypted gateway through the cellular interface.

```
ip route 10.194.112.101 255.255.255.255 Cellular0/2/0 200
ip route 10.194.112.101 255.255.255.255 10.0.2.5
```

Step 2: Never forget that the cellular interface is an asynchronous interface leveraging the dialer commands and you must specify traffic.

```
dialer-list 2 protocol ip permit
```

Process

Configuring Branch DVPN

1. Configure IPsec VTI
2. Apply Interface Tracking
3. Verify and Test the Setup

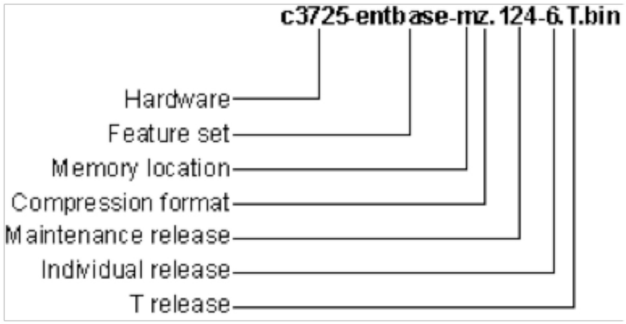
Configuring this feature requires a specific Cisco Internet Operating System (IOS) feature set unlike any other feature previously recommended. Figure 8 illustrates how to understand the IOS image name to verify you can complete the steps outlined in this section.

The feature set must be the Advanced Feature Set, the Advanced Security Feature Set, or above (for example: Enterprise Feature Set).

Tech Tip

The encryption policy set forth in this document is not a requirement to allow for 3G cellular connectivity, but a policy that provides security and functionality as outlined in the Headquarters configuration section. If your security policy differs from this model, the interface configuration guide will allow you to bring up the interface and talk to your headquarters router.

Figure 8. Cisco IOS Naming Convention



Procedure 1 Configure IPsec VTI

Follow the IPsec VTI configuration as applied on the Branch site router to connect to the DR site. The branch IPsec tunnel is activated when the router sends traffic on the tunnel interface, which is most likely EIGRP running on the interface that is attempting to establish a neighbor relationship with a peer at the other end of the tunnel. After the IPsec tunnel is up, the branch and headend routers become EIGRP neighbors and routing information is exchanged over the tunnel. These routes should only take precedence when the primary leased-line connectivity is unavailable, and the higher-cost routes over the tunnel take precedence.

To make troubleshooting much easier, use unique, intuitive labels for configuration of the keyring, ISAKMP profile, and IPsec profile rather than general or random labels.

Step 1: Apply the following configuration:

```
crypto isakmp policy 1
encr aes
authentication pre-share
group 2
crypto isakmp key sba address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set sba-xform esp-aes
!
crypto ipsec profile sba-ipsec
set transform-set sba-xform
!
interface Tunnel0
ip unnumbered FastEthernet0/0.72
```

```
tunnel source Serial0/0/1:0
tunnel destination 10.0.1.250
tunnel mode ipsec ipv4
tunnel protection ipsec profile sba-ipsec
```

This configuration will establish and maintain a permanent tunnel over the backup WAN connection when backup WAN connectivity is available.

Procedure 2 Apply Interface Tracking

If the tunnel should only be established when the primary link is down, interface tracking enables and disables the tunnel as needed.

Step 1: Apply the following interface-tracking configuration to monitor the primary WAN interface's ability to route IP traffic:

```
track 123 interface Serial0/0/0:0 ip routing
```

Embedded Event Manager (EEM) is a Cisco IOS feature that provides the capability for the router to execute scripts that are a portion of the router's configuration. This ability to execute scripts provides an integrated capability for the router to react and adjust to changes in network connectivity and behavior. EEM scripts are part of the router's CLI configuration, and are entered, as any other configuration, from the router's configuration prompt.

Step 2: Enter the first EEM script, which enables the IPsec VPN connection when the primary WAN loses its ability to route:

```
event manager applet start-tunnel
event track 123 state down
action 1 cli command "enable"
action 2 cli command "configure terminal"
action 3 cli command "interface tunnel0"
action 4 cli command "no shut"
action 5 cli command "end"
```

Step 3: Enter the second EEM script, which disables the IPsec VPN connection when the primary WAN's ability to carry traffic is restored:

```
event manager applet stop-tunnel
event track 123 state up
action 1 cli command "enable"
action 2 cli command "configure terminal"
action 3 cli command "interface tunnel0"
action 4 cli command "shut"
action 5 cli command "end"
```

This configuration will offer the benefit of reducing connectivity fees over the secondary connection and should only be used if the second link is subject to bandwidth or time-based usage charges. Failover to the IPsec connection will take longer with this method as the router must bring up the IPsec tunnel and routing must converge before the connection will pass user data.

Procedure 3 Verify and Test the Setup

With the branch office up and configured to the headquarters, it is time to verify the operation of this backup. The primary link is being tracked and monitored by the Embedded Event Manager; if routing fails, the event manager will trigger the 3G connection to come up and encrypt traffic to your headquarters through the public Internet.

Step 1: Disable this primary interface by either unplugging or in some other way disabling the primary interface while on the console of the branch router.

Step 2: Enter the show ip route command to verify that the routes are lost and again return via the tunnel interface that traverses the public internet through the 3G interface.

Reader Tip

Complete and current information on the Cisco SBA can be found at:

http://www.cisco.com/en/US/solutions/ns340/ ns414/ns742/ns982/landing_sBus_archit.html

Appendix A: Product Part Numbers

The following products and software versions have been validated for the Cisco SBA:

Functional Area	Product	Part Numbers	Software Version
Headquarters	Cisco 3925 or 3845 Integrated Services Router	C3925 C3845	15.0.1r.M1
Branch	Cisco 2911 or 2811 Integrated Services Router	C2911-VSEC/K9 C2811-VSEC-SRST/K HWIC-3G-CDMA HWIC-3G-GSM	15.0.1M

Appendix B: Branch ISR Configuration for GSM

```
Current configuration : 8351 bytes
!
! Last configuration change at 00:02:02 UTC Sat Jan 30 2010
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname BRISR-GSM
!
boot-start-marker
boot-end-marker
!
card type t1 0 0
enable password 7 141443180F0B7B7977
!
no aaa new-model
!
!
!
network-clock-participate wic 0
network-clock-select 1 T1 0/0/0
network-clock-select 2 T1 0/0/1
!
no ipv6 cef
ip source-route
ip cef
!
!
ip multicast-routing
ip dhcp excluded-address 192.168.72.1 192.168.72.10
ip dhcp excluded-address 192.168.73.1 192.168.73.10
ip dhcp excluded-address 192.168.76.1 192.168.76.10
ip dhcp excluded-address 192.168.77.1 192.168.77.10
!
ip dhcp pool wired_data
network 192.168.72.0 255.255.255.0
dns-server 192.168.28.10 192.168.152.10
domain-name cisco.local
default-router 192.168.72.1
!
ip dhcp pool wired_voice
network 192.168.73.0 255.255.255.0
dns-server 192.168.28.10 192.168.152.10
default-router 192.168.73.1
domain-name cisco.local
option 150 ip 192.168.28.20 192.168.29.20
!
ip dhcp pool wireless_data
network 192.168.76.0 255.255.255.0
default-router 192.168.76.1
domain-name cisco.local
dns-server 192.168.28.10 192.168.152.10
!
ip dhcp pool wireless_voice
network 192.168.77.0 255.255.255.0
default-router 192.168.77.1
domain-name cisco.local
dns-server 192.168.28.10 192.168.152.10
option 150 ip 192.168.28.20 192.168.29.20
!
!
ip domain name cisco.local
ip name-server 192.168.28.10
ip name-server 192.168.152.10
!
!
multilink bundle-name authenticated
!
!
!
!
!
chat-script gsm "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
!
crypto pki trustpoint TP-self-signed-1428771843
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1428771843
```

```
revocation-check none
rsakeypair TP-self-signed-1428771843
!
!
crypto pki certificate chain TP-self-signed-1428771843
  certificate self-signed 01
3082024A 308201B3 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
69666963 6174652D 31343238 37373138 3433301E 170D3039 31303239
32313330
34305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31
34323837
37313834 3330819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
8100A1B8 7A1A2759 7A934340 1E6A6B63 F1778708 265C3AD3 AE745D9A
0CE44B53
7F553A8C 10B16095 AF5A1D05 F4D4E60E 21D2E78C DC6B6E94 9949A3F0
8FEF5629
E695263A 08F41555 CBC4A4BE A5D4DD75 97B2DEAD 21AF97E1 B9CB0734
3EAF1AE1
52634F51 AA459719 19D18B14 11A7C8D7 4C026B58 9310ACEB 91852A9F
F1B531B7
312D0203 010001A3 72307030 0F060355 1D130101 FF040530 030101FF
301D0603
551D1104 16301482 12425232 4953522E 63697363 6F2E6C6F 63616C30
1F060355
1D230418 30168014 34EFB0EF 8BC219F2 C6CE69D2 F7C31BAF EA7B1A9D
301D0603
551D0E04 16041434 EFB0EF8B C219F2C6 CE69D2F7 C31BAFEA 7B1A9D30
0D06092A
864886F7 0D010104 05000381 81001F20 2904AFD6 B6D8258B DA941189
459546B3
E0928B52 676BAC46 D182ED89 E69506CF 56E98F73 DBC065BC 58B73D54
78F99AF5
74A30461 1F4C4953 4B10F5F3 FAC5DCDE D82B7B3D 7229569F 5B8FE53F
D2B95F84
E329F4CB 21B5CC29 BF91EF97 5C66C9DB C9D47784 C98A9594 7768855E
21427A80
86128A10 591D4CB3 4FC4C84E 8B13
                  quit
voice-card 0
!
!
!
!
!
!
!
!
license udi pid CISCO2911/K9 sn FHK1332F1N9
!
!
archive
  log config
    hidekeys
username admin privilege 15 password 7 0508571C22431F5B4A
!
redundancy
!
!
controller T1 0/0/0
cablelength long 0db
channel-group 0 timeslots 1-24
!
controller T1 0/0/1
cablelength long 0db
channel-group 0 timeslots 1-4
!
!
track 123 interface Serial0/0/0:0 ip routing
!
!
crypto isakmp policy 1
encr aes
authentication pre-share
group 2
crypto isakmp key sba address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set xform esp-aes
!
crypto ipsec profile sba
  set transform-set xform
!
!
!
!
!
!
interface Tunnel0
description ###### Encrypted tunnel to DC2 ISR ########
ip unnumbered GigabitEthernet1/0.72
```

```
tunnel source Cellular0/1/0
tunnel mode ipsec ipv4
tunnel destination 10.194.112.101
tunnel protection ipsec profile sba
!
!
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
shutdown
duplex auto
speed auto
!
!
interface Serial0/0/0:0
description Primary Wide Area network
ip address 10.0.1.6 255.255.255.252
ip wccp 62 redirect in
ip pim sparse-mode
load-interval 30
!
!
!
interface Cellular0/1/0
ip address negotiated
encapsulation ppp
load-interval 30
dialer in-band
dialer idle-timeout 300
dialer string gsm
dialer-group 1
no peer default ip address
async mode interactive
no ppp lcp fast-start
ppp chap hostname ISP@CINGULARGPRS.COM
ppp chap password 0 CINGULAR
ppp ipcp dns request
ppp timeout retry 120
ppp timeout ncp 30
fair-queue 64 16 256
!
routing dynamic
!
!
interface GigabitEthernet1/0
description Uplink to Switch
ip unnumbered GigabitEthernet1/0.72
!
hold-queue 60 out
!
interface GigabitEthernet1/0.72
description Wired Data Access
encapsulation dot1Q 72
ip address 192.168.72.1 255.255.255.0
!
interface GigabitEthernet1/0.73
description Wired Voice Access
encapsulation dot1Q 73
ip address 192.168.73.1 255.255.255.0
!
interface GigabitEthernet1/0.76
description Wireless Data Access
encapsulation dot1Q 76
ip address 192.168.76.1 255.255.255.0
!
interface GigabitEthernet1/0.77
description Wireless Voice Access
encapsulation dot1Q 77
ip address 192.168.77.1 255.255.255.0
!
interface Dialer1
ip address negotiated
ip virtual-reassembly
encapsulation ppp
load-interval 30
dialer pool 1
dialer idle-timeout 0
dialer string gsm
dialer persistent
dialer-group 1
no peer default ip address
```

```
no ppp lcp fast-start
ppp ipcp dns request
ppp timeout retry 120
ppp timeout ncp 30
!
!
!
!
router eigrp 1
network 10.0.1.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Serial0/0/0:0
no passive-interface Tunnel0
!
ip forward-protocol nd
!
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 10.194.112.101 255.255.255.255 10.0.2.5
ip route 10.194.112.101 255.255.255.255 Cellular0/1/0 234
!
access-list 1 permit any
dialer-list 1 protocol ip permit
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
!
control-plane
  !
!
!
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
  exec-timeout 0 0
line aux 0
line 0/1/0
script dialer gsm
modem InOut
no exec
rxspeed 3600000
txspeed 384000
line vty 0 3
exec-timeout 0 0
login local
transport input all
line vty 4
  login
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
event manager applet start-tunnel
event track 123 state down
action 1 cli command "enable"
action 2 cli command "configure terminal"
action 3 cli command "interface tunnel0"
action 4 cli command "no shut"
action 5 cli command "end"
event manager applet stop-tunnel
event track 123 state up
action 1 cli command "enable"
action 2 cli command "configure terminal"
action 3 cli command "interface tunnel0"
action 4 cli command "shut"
action 5 cli command "end"
!
End
```

Appendix C: Branch ISR Configuration for CDMA

```
Current configuration : 8351 bytes
!
! Last configuration change at 00:02:02 UTC Sat Jan 30 2010
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname BRISR-CDMA
!
boot-start-marker
boot-end-marker
!
card type t1 0 0
enable password 7 141443180F0B7B7977
!
no aaa new-model
!
!
!
network-clock-participate wic 0
network-clock-select 1 T1 0/0/0
network-clock-select 2 T1 0/0/1
!
no ipv6 cef
ip source-route
ip cef
!
!
ip multicast-routing
ip dhcp excluded-address 192.168.72.1 192.168.72.10
ip dhcp excluded-address 192.168.73.1 192.168.73.10
ip dhcp excluded-address 192.168.76.1 192.168.76.10
ip dhcp excluded-address 192.168.77.1 192.168.77.10
!
ip dhcp pool wired_data
network 192.168.72.0 255.255.255.0
dns-server 192.168.28.10 192.168.152.10
domain-name cisco.local
default-router 192.168.72.1
!
ip dhcp pool wired_voice
network 192.168.73.0 255.255.255.0
dns-server 192.168.28.10 192.168.152.10
default-router 192.168.73.1
domain-name cisco.local
option 150 ip 192.168.28.20 192.168.29.20
!
ip dhcp pool wireless_data
network 192.168.76.0 255.255.255.0
default-router 192.168.76.1
domain-name cisco.local
dns-server 192.168.28.10 192.168.152.10
!
ip dhcp pool wireless_voice
network 192.168.77.0 255.255.255.0
default-router 192.168.77.1
domain-name cisco.local
dns-server 192.168.28.10 192.168.152.10
option 150 ip 192.168.28.20 192.168.29.20
!
!
ip domain name cisco.local
ip name-server 192.168.28.10
ip name-server 192.168.152.10
!
!
multilink bundle-name authenticated
!
!
!
!
!
chat-script cdma "" "atdt#777" TIMEOUT 60 "CONNECT"
!
crypto pki trustpoint TP-self-signed-1428771843
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1428771843
```

```
revocation-check none
rsakeypair TP-self-signed-1428771843
!
!
crypto pki certificate chain TP-self-signed-1428771843
  certificate self-signed 01
3082024A 308201B3 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
69666963 6174652D 31343238 37373138 3433301E 170D3039 31303239
32313330
34305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31
34323837
37313834 3330819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
8100A1B8 7A1A2759 7A934340 1E6A6B63 F1778708 265C3AD3 AE745D9A
0CE44B53
7F553A8C 10B16095 AF5A1D05 F4D4E60E 21D2E78C DC6B6E94 9949A3F0
8FEF5629
E695263A 08F41555 CBC4A4BE A5D4DD75 97B2DEAD 21AF97E1 B9CB0734
3EAF1AE1
52634F51 AA459719 19D18B14 11A7C8D7 4C026B58 9310ACEB 91852A9F
F1B531B7
312D0203 010001A3 72307030 0F060355 1D130101 FF040530 030101FF
301D0603
551D1104 16301482 12425232 4953522E 63697363 6F2E6C6F 63616C30
1F060355
1D230418 30168014 34EFB0EF 8BC219F2 C6CE69D2 F7C31BAF EA7B1A9D
301D0603
551D0E04 16041434 EFB0EF8B C219F2C6 CE69D2F7 C31BAFEA 7B1A9D30
0D06092A
864886F7 0D010104 05000381 81001F20 2904AFD6 B6D8258B DA941189
459546B3
E0928B52 676BAC46 D182ED89 E69506CF 56E98F73 DBC065BC 58B73D54
78F99AF5
74A30461 1F4C4953 4B10F5F3 FAC5DCDE D82B7B3D 7229569F 5B8FE53F
D2B95F84
E329F4CB 21B5CC29 BF91EF97 5C66C9DB C9D47784 C98A9594 7768855E
21427A80
86128A10 591D4CB3 4FC4C84E 8B13
                  quit
voice-card 0
!
!
!
!
!
!
!
!
license udi pid CISCO2911/K9 sn FHK1332F1N9
!
!
archive
  log config
    hidekeys
username admin privilege 15 password 7 0508571C22431F5B4A
!
redundancy
!
!
controller T1 0/0/0
cablelength long 0db
channel-group 0 timeslots 1-24
!
controller T1 0/0/1
cablelength long 0db
channel-group 0 timeslots 1-4
!
!
track 123 interface Serial0/0/0:0 ip routing
!
!
crypto isakmp policy 1
encr aes
authentication pre-share
group 2
crypto isakmp key sba address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set xform esp-aes
!
crypto ipsec profile sba
  set transform-set xform
!
!
!
!
!
!
interface Tunnel0
description ###### Encrypted tunnel to DC2 ISR ########
ip unnumbered GigabitEthernet1/0.72
```

```
tunnel source Cellular0/2/0
tunnel mode ipsec ipv4
tunnel destination 10.194.112.101
tunnel protection ipsec profile sba
!
!
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
shutdown
duplex auto
speed auto
!
!
interface Serial0/0/0:0
description Primary Wide Area network
ip address 10.0.1.6 255.255.255.252
ip wccp 62 redirect in
ip pim sparse-mode
load-interval 30
!
!
interface Serial0/0/1:0
description Backup Link (Internet)
ip address 10.0.2.6 255.255.255.252
ip wccp 62 redirect in
ip pim sparse-mode
load-interval 30
!
!
!
interface Cellular0/2/0
ip address negotiated
encapsulation ppp
dialer in-band
dialer idle-timeout 0
dialer string cdma
dialer-group 2
no peer default ip address
async mode interactive
no ppp lcp fast-start
ppp ipcp dns request
!
routing dynamic
!
interface GigabitEthernet1/0
description Uplink to Switch
ip unnumbered GigabitEthernet1/0.72
!
hold-queue 60 out
!
interface GigabitEthernet1/0.72
description Wired Data Access
encapsulation dot1Q 72
ip address 192.168.72.1 255.255.255.0
!
interface GigabitEthernet1/0.73
description Wired Voice Access
encapsulation dot1Q 73
ip address 192.168.73.1 255.255.255.0
!
interface GigabitEthernet1/0.76
description Wireless Data Access
encapsulation dot1Q 76
ip address 192.168.76.1 255.255.255.0
!
interface GigabitEthernet1/0.77
description Wireless Voice Access
encapsulation dot1Q 77
ip address 192.168.77.1 255.255.255.0
!
!
!
!
!
router eigrp 1
network 10.0.1.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Serial0/0/0:0
no passive-interface Tunnel0
```

```
!
ip forward-protocol nd
!
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 10.194.112.101 255.255.255.255 10.0.2.5
ip route 10.194.112.101 255.255.255.255 Cellular0/2/0 235
!
access-list 2 permit any
dialer-list 2 protocol ip permit
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
!
control-plane
  !
!
!
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
!
!
!
!
gatekeeper
  shutdown
!
!
line con 0
  exec-timeout 0 0
line aux 0
line 0/2/0
script dialer cdma
modem InOut
no exec
transport input all
transport output all
rxspeed 3100000
txspeed 1800000
line 67
no activation-character
no exec
transport preferred none
transport input all
transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
flowcontrol software
line vty 0 3
exec-timeout 0 0
login local
transport input all
line vty 4
  login
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
event manager applet start-tunnel
event track 123 state down
action 1 cli command "enable"
action 2 cli command "configure terminal"
action 3 cli command "interface tunnel0"
action 4 cli command "no shut"
action 5 cli command "end"
event manager applet stop-tunnel
event track 123 state up
action 1 cli command "enable"
action 2 cli command "configure terminal"
action 3 cli command "interface tunnel0"
action 4 cli command "shut"
action 5 cli command "end"
!
End
```

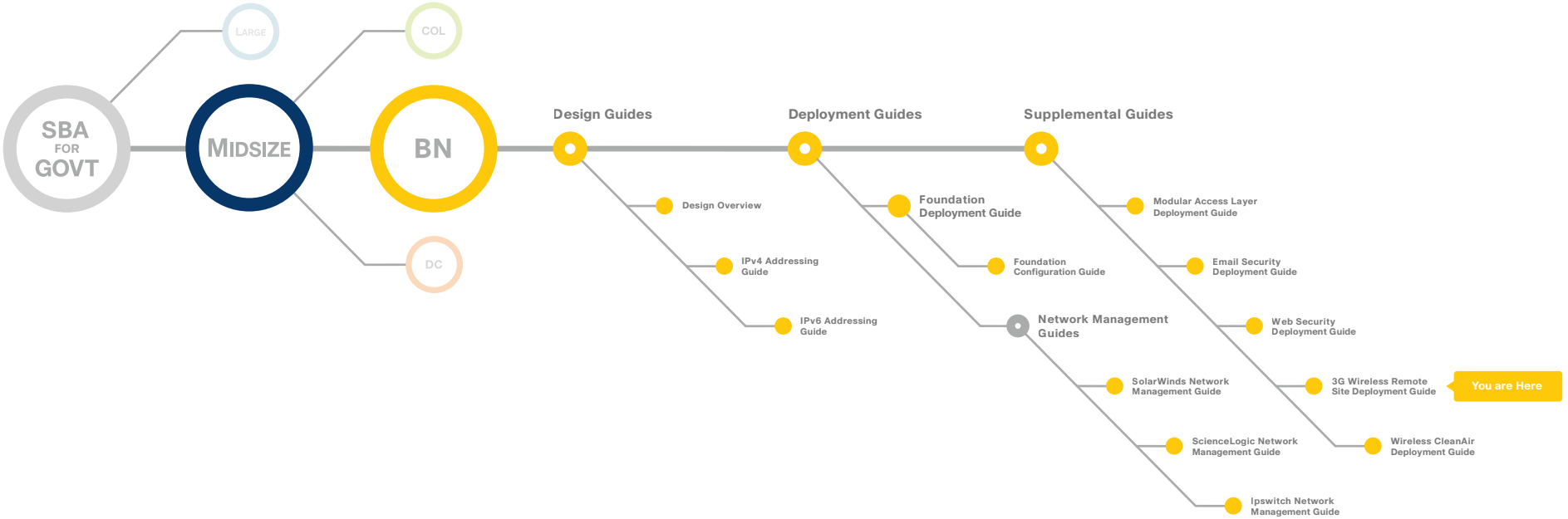
Appendix D: Headend or Headquarters ISR Configuration

```
Current configuration : 3324 bytes
!
! Last configuration change at 22:39:57 UTC Wed Jan 13 2010
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname DC2ISR
!
boot-start-marker
boot-end-marker
!
enable password c1sco123
!
no aaa new-model
!
!
!
!
!
!
no ipv6 cef
ip source-route
ip cef
!
!
!
!
ip host wwwin 171.71.181.19
ip wccp 61
ip wccp 62
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
license udi pid C3900-SPE150/K9 sn FOC133037KH
license boot module c3900 technology-package securityk9
license boot module c3900 technology-package uck9
license boot module c3900 technology-package datak9
!
!
archive
  log config
     hidekeys
username cisco password 0 cisco123
username admin privilege 15 password 0 c1sco123
!
redundancy
!
!
!
crypto keyring sba-keys
  pre-shared-key address 0.0.0.0 0.0.0.0 key sba
!
crypto isakmp policy 1
encr aes
authentication pre-share
group 2
crypto isakmp profile sba-profile
keyring sba-keys
match identity address 0.0.0.0
virtual-template 1
!
!
crypto ipsec transform-set xform esp-aes
!
crypto ipsec profile sba
  set transform-set xform
```

```
!
!
!
!
!
!
interface Port-channel1
no ip address
!
hold-queue 150 in
!
interface Port-channel1.159
encapsulation dot1Q 159
ip address 192.168.159.2 255.255.255.0
ip wccp 62 redirect in
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
channel-group 1
!
!
interface GigabitEthernet0/0.159
  channel-group 1
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
media-type rj45
channel-group 1
!
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
!
interface FastEthernet0/2/0
ip address 10.0.1.250 255.255.255.252
ip wccp 61 redirect in
duplex auto
speed auto
!
!
interface FastEthernet0/2/1
ip address 10.194.112.79 255.255.255.192
ip access-group 143 in
ip access-group 143 out
ip policy route-map VPN-ROUTE
shutdown
duplex auto
speed auto
!
!
interface Virtual-Template1 type tunnel
ip unnumbered Port-channel1.159
tunnel source Port-channel1.159
tunnel mode ipsec ipv4
tunnel protection ipsec profile sba
!
!
!
!
router eigrp 1
network 10.0.1.0 0.0.0.255
network 192.168.0.0 0.0.255.255
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 192.168.0.0 255.255.255.0 10.194.112.80
!
access-list 122 remark *** Default gateway for remote sites ***
access-list 122 permit ip 192.168.80.0 0.0.1.255 any
access-list 122 permit ip 192.168.84.0 0.0.1.255 any
access-list 143 remark *** ACL to select VPN Traffic ***
access-list 143 permit esp any any
access-list 143 permit udp any any eq non500-isakmp
access-list 143 permit udp any any eq isakmp
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
route-map VPN-ROUTE permit 10
match ip address 143
set ip next-hop 10.194.112.80
!
```

```
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Port-channel1.159
snmp-server source-interface informs Port-channel1.159
!
control-plane
  !
!
!
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
!
!
!
!
gatekeeper
  shutdown
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
password c1sco123
login
line vty 5 16
password c1sco123
login
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

Appendix E:
SBA for Midsize Agencies Document System



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.**

C07-593072-01 10/10