3G无线远程站点部署指南

智能业务平台

修订版：2012年上半年

前言

本指南是一份思科®智能业务平台（IBA）指南。

本指南的目标受众

本指南主要面向在企业中承担以下职务的人员：

- 需要实施解决方案时的标准规范的系统工程师
- 需要获取参考资料以撰写思科IBA实施项目工作说明书的项目经理
- 需要借助产品指南销售新技术或撰写自己的实施文档的销售合作伙伴
- 需要课堂讲授或在职培训材料的培训人员

一般来说，您也可以将思科IBA指南作为工程师之间技术交流、项目实施经验分享的统一指导文件，或利用它更好地规划项目成本预算和项目工作范围。

版本系列

思科每年对IBA指南进行两次更新和修订。在发布思科IBA指南系列之前，我们将在IBA实验室对其进行整体评测。为确保思科IBA指南中各个设计之间的兼容性，您应使用同一IBA系列中的设计指南文档。

所有思科IBA指南的封面和每页的左下角均标有指南系列的名称。指南系列的命名方式如下：

- 年2月指南系列
- 年8月指南系列

其中的年表示发布该指南系列的公历年度。

您可以在以下网址查看最新的思科IBA指南系列：
客户登录：http://www.cisco.com/go/cn/iba
合作伙伴登录：http://www.cisco.com/go/cn/iba

如何阅读命令

许多思科IBA指南详细说明了思科网络设备的配置步骤，这些设备运行着Cisco IOS、Cisco NX-OS或其他需要通过命令行界面(CLI)进行配置的操作系统。下面描述了系统命令的指定规则，您需要按照这些规则来输入命令。

在CLI中输入的命令如下所示：

```
configure terminal
```

为某个变量指定一个值的命令如下所示：

```
ntp server 10.10.48.17
```

包含您必须定义的变量的命令如下所示：

```
class-map [highest class name]
```

以交互示例形式显示的命令（如脚本和包含提示的命令）如下所示：

```
Router# enable
```

包含自动换行的长命令以下划线表示。应将其作为一个命令进行输入：

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

问题和评论

如需要了解更多有关思科IBA智能业务平台的信息，请访问
http://www.cisco.com/go/cn/iba

如需要注册快速报价工具（QPT），请访问
http://www.cisco.com/go/qpt

如果您希望在出现新评论时获得通知，我们可以发送RSS信息。

目录

本IBA指南的内容

关于IBA

思科IBA能帮助您设计和快速部署一个全服务企业网络。IBA系统是一种规范式设计，即购即用，而且具备出色的可扩展性和灵活性。

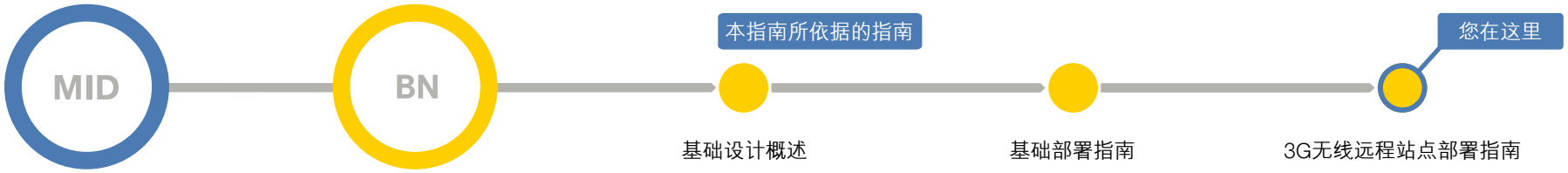
思科IBA在一个综合解决方案中集成了局域网、广域网、无线、安全、数据中心、应用优化和统一通信技术，并对其进行了严格测试，确保能够实现无缝协作。 IBA采用的组件式方法简化了在采用多种技术时通常需要进行的系统集成工作，使您可以随意选择能够满足企业需求的解决方案，而不必担心技术复杂性方面的问题。

关于本指南

本指南是一份附加部署指南。思科IBA部署指南包含以下章节：

- **业务概述** —— 描述了本指南中提出的解决方案的具体功能和应用价值。这一章节的内容对业务决策者尤为重要。
- **技术概述** —— 描述了支持此企业应用情形的技术解决方案，包括对构成此解决方案的思科产品的介绍。 技术决策者可以利用此章节的内容了解解决方案的工作原理。
- **部署详情** —— 详细描述各个部署步骤，指导您部署和配置思科IBA解决方案。系统工程师可以在这些步骤的指导下快速、可靠地配置和启用解决方案。

在成功部署路线图上，附加部署指南总是紧随基础部署指南之后，如下所示。



成功部署路线图

为确保您能够按照本指南中的设计成功完成部署，您应当阅读本指南所依据的所有相关指南——即上面路线图中本指南左侧的所有指南。所有以本指南为依据的指南都在右侧。

如需要了解更多有关思科IBA智能业务平台的信息，请访问：
http://www.cisco.com/go/cn/iba
如需要注册快速报价工具（QPT），请访问：
http://www.cisco.com/go/qpt

业务概述

无线的应用

如今，对于企业数据的访问已不再仅仅局限于某一建筑物的内部。随着世界日益走向移动化，当今的消费者期望能够随时获得产品和服务。例如：

- 移动诊所需要能够与不同的专家进行即时通信，以及交换患者X射线影像、医学检查结果和相关文件。
- 紧急移动部署设备要求即时通信、远程信息反馈和本地站点互通能力。
- 贸易展会和特定活动要求使用交互式信息亭和互联网热点，提供信用卡处理能力，以及基于数字广告开展即时市场营销活动。

图 1. 使用案例

蜂窝连接为您的远程站点提供了一款永续解决方案。永续的解决方案能够为那些用户直接与之交互的应用提供始终可访问的网络，包括从站点间备份与恢复到阅读电子邮件等。用户与网络的交互水平及其获取基本服务的能力影响着企业的整体业绩。

思科智能业务平台(IBA)提供了可靠的网络服务，如互联网连接、广域网基础设施和安全性等，能够帮助确保企业依赖诸如Web会议等应用进行关键协作。

远程站点的高可用性是大多数组织实现高生产力和安全保障的基本要求。因此，始终保持连接能力以支持关键业务数据交易成为了思科面向中小企业的IBA设计要实现的首要目标。

面向中小企业的思科IBA智能业务平台是一种规范性架构，致力于通过使用有线连接、无线连接、安全性、广域网优化和统一通信组件，提供一个简单易用、灵活、可扩展的网络。它采用了一种可靠且包含完善支持服务的标准化设计，有效消除了集成不同网络组件的挑战。

读者提示

如需了解更多有关思科IBA智能业务平台的信息，请访问：
http://www.cisco.com/go/cn/iba或
http://www.cisco.com/go/partner/smartarchitecture

技术概述

蜂窝选项

具备蜂窝连接的解决方案提供了灵活性、高速度和高带宽。市场中目前有两种支持蜂窝服务、提供高带宽广域网连接的竞争性技术，分别为：码分多址（CDMA）或全球移动通信系统（GSM）。全球大部分地方只能选择其中之一。

CDMA

码分多址（CDMA）起源于第二次世界大战。它是一项仅涉及空中（over-the-air）传输的技术，使每名用户可以充分利用射频，能够提供比GSM更高的数据速率。CDMA充分利用了时分多址（TDMA）和通用分组无线业务（GPRS）技术，后者是一种分组交换技术。码分多址（CDMA）使用了更强大的信号，当与GSM技术同时用于人口密集的区域时，往往能够以GSM的成本实现更出色的覆盖。

当选择CDMA而不是GSM时，应考虑您是在哪里建立远程站点。CDMA主要用于美国，而很少用于世界其他地方，比如在欧洲根本未得到应用，因为欧盟仅授权使用GSM。

GSM

全球移动通信系统（GSM）于1987年由GSM Association发明。GSM Association是一家国际性组织，专门致力于制定全球范围的GSM标准。GSM的数据速率通常要慢于CDMA，然而，在增强型数据速率GSM演进（EDGE）技术中，性能差距已大幅缩小。GSM同时还具有在全球部署中遥遥领先的优势，在全球所有蜂窝部署中，有超过74%均采用了GSM。而且正如前面所提及的，整个欧洲几乎均采用的是GSM。GSM相比CDMA的另一个显著优势是，它能够在设备间转移用户识别模块（SIM），基本上无需您的电信运营商参与即可在设备间转换服务。

3G和4G

目前广为采用的数据标准是第三代（3G），它理论上可以实现最高14Mbps的数据速率。此外，一些运营商已经开始提供第四代（4G）标准，该标准承诺提供高达每秒千兆位(Gbps) 的数据速率，并且能够提供至少100Mbps的数据速率。这两种标准由国际电信联盟（ITU）定义。

根据ITU的要求，一个4G蜂窝系统必须针对高移动性（如移动访问）实现高达100 Mbps左右的目标峰值数据速率，针对低移动性（如漫游/本地无线访问）提供高达1Gbps左右的数据速率。这些数据速率和带宽的诱人应用前景为远程分支机构带来了极具吸引力的机遇。

部署详情

在您启动部署流程之前，您需要确定在定义物理拓扑时使用哪项技术。

要决定使用哪项技术，需考虑以下问题:

- 在远程站点所在区域，支持哪项技术?

  联系您当地的电信运营商，了解您所在区域支持的技术。例如：欧洲规定所有蜂窝网络仅能使用GSM。

- 您是否需要或要求冗余硬件，以便在出现故障时进行热交换?

  GSM允许您在设备间移动SIM卡，而无需电信运营商的干预。

- 是否要求较高的数据吞吐量?

  虽然各项技术的数据吞吐量差别不大，但CDMA仍具有明显的优势。

- 您的办公室是否要在地区间移动?

  如果您的远程站点需要经常移动，例如健康诊所等，您可能希望在解决方案中同时包含CDMA和GSM技术，以便针对您的所在地点选择最佳技术。

- 如果服务价格或电信运营商服务是考虑因素，那么哪个运营商能够为您的远程站点提供最佳性价比?

  一些电信运营商同时提供了商用和无线服务，以在您远离公共网络（互联网）时提供替代连接，使您能够使用您的专用多协议标签交换(MPLS)网络。

本指南介绍了当您在需要移动的分支机构中进行部署时，诸如灾难恢复车辆、移动诊所、户外活动数据处理中心或其他一些完全移动化的分支机构等，如何充分利用这两种技术。这是针对那些这两种技术共存的极少数地方的独特要求，或许只有在美国该解决方案才有意义。

接下来，您需要定义物理拓扑。

图2. 总部到远程站点拓扑

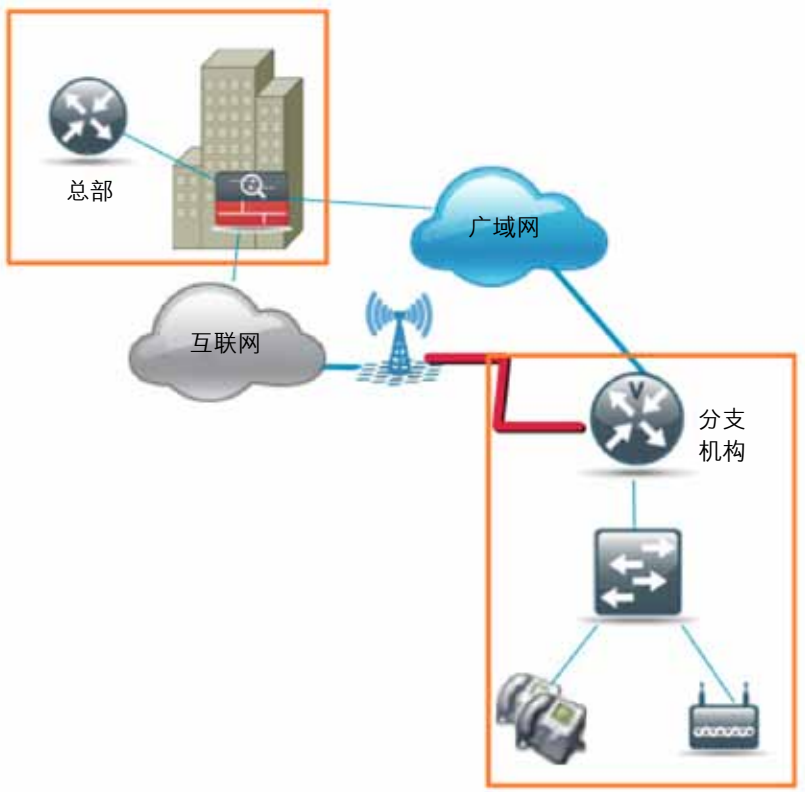
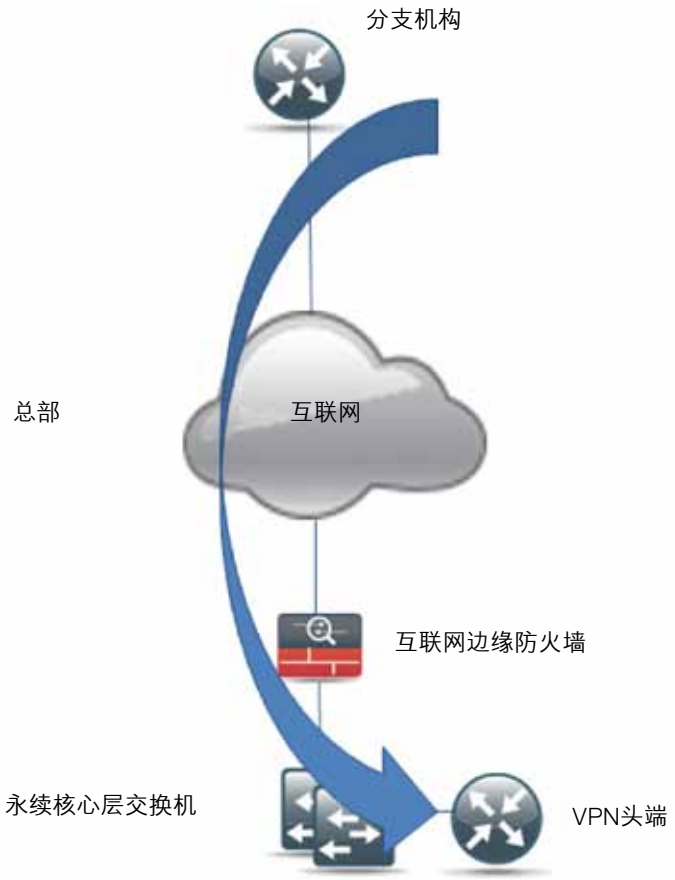


图3中的总部拓扑显示了VPN流量通过互联网边缘防火墙，到达在思科IBA智能业务平台中充当VPN头端路由器的集成多业务路由器(ISR)的情形。

图3. 总部拓扑



流程

采用VTI部署VPN头端路由器

1. 在头端上配置ISAKMP和IPsec
2. 在头端上配置VTI模板
3. 配置总部ASA

按照以下程序配置远程站点IPsec对等体，连接到VPN头端路由器。该设计采用思科IOS IPsec虚拟隧道接口(VTI)加密传输数据和语音信息，只需进行很少的配置便可提供强大功能。VTI 有两种运行模式：

- **静态** —— 静态VTI可以发起到其他静态VTI站点的隧道。
- **动态** —— 多个静态VTI站点可以发起到一个基于模板的动态VTI (DVTI)汇聚点的多条隧道，该汇聚点可提供简单的配置。

选择VTI的原因如下：

- DVTI不要求您了解远程站点的公共地址，从而可简化远程站点的配置。后者可能会被动态地分配一个地址，或使用网络地址转换(NAT)。
- DVTI只要求为头端路由器配置一个隧道，从而最大限度减少了配置和故障排除复杂性。
- 与传统加密映射表(crypto-map) VPN配置相比，VTI为应用服务质量(QoS)策略、NAT、防火墙、入侵探测IPS、访问列表(ACL)和隧道监控提供了一个虚拟接口。
- VTI配置提供了出色的动态路由灵活性，能够有效满足思科IBA设计的需求。
- 远程站点向头端路由器上的DVTI响应程序发起连接，后者为每个远程站点的连接创建一个虚拟隧道接口。DVTI为远程站点连接采用基于模板的配置，以便能使用一个DVTI配置创建多个隧道。您无需进行任何额外的配置来支持多个远程站点。

技术提示

通常，当您向您的远程站点路由器添加WAN永续性时，您应当已经配置了头端或总部路由器，或其他端接点。但是本文档假定这是您第一个利用公共网络的永续远程站点配置。

程序1　在头端上配置ISAKMP和IPsec

步骤1： 配置预共享密钥。

加密密钥环（keyring）定义了一个对IP对等体有效的预共享密钥（或密码）。如果应用于任意IP源，该密钥是一个通配预共享密钥。您可以使用0.0.0.0 0.0.0.0网络/掩码组合配置通配密钥。

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

步骤2： 配置互联网安全关联和密钥管理协议(ISAKMP)策略。

面向VTI的ISAKMP策略采用如下规则：

- 基于128位密钥的高级加密标准（AES）
- 安全哈希标准（SHA）
- 使用预共享密钥进行身份验证
- Diffie-Hellman组2

```
crypto isakmp policy [policy sequence]
 encr aes
 hash sha
 authentication pre-share
 group 2
```

步骤3： 创建ISAKMP配置文件。

ISAKMP配置文件在身份地址、VTI虚拟模板和crypto keyring间建立了关联。通配身份地址通过使用0.0.0.0来进行引用。

```
crypto isakmp profile [ISAKMP profile name]
 keyring [keyring name]
 match identity address 0.0.0.0
 virtual-template [VTI template number]
```

步骤4： 定义IPsec转换集。

转换集是一个可接受的安全协议、算法和其他设置的组合，应用于IPsec保护流量。对等体同意在其保护特定的数据流时使用特定的转换集。

IPsec转换集使用以下：

- 采用128位AES加密算法的封装安全有效载荷(ESP)
- 采用SHA（散列消息认证码[HMAC]变体）身份验证算法的ESP

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

步骤5： 创建IPsec配置文件。

IPsec配置文件在一个身份地址和一个IPsec转换集之间创建了一个关联。

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

例如：

```
crypto keyring iba-keys
 pre-shared-key address 0.0.0.0 0.0.0.0 key iba
crypto isakmp policy 1
 encr aes
 hash sha
 authentication pre-share
 group 2
crypto isakmp profile iba-isakmp
  keyring iba-keys
```

```
    match identity address 0.0.0.0
    virtual-template 1
crypto ipsec transform-set iba-xform esp-aes esp-sha-hmac
  crypto ipsec profile iba-ipsec
  set transform-set iba-xform
```

程序2　在头端上配置VTI模板

步骤1： 配置基本接口设置。

```
interface Virtual-Template [VTI template number] type tunnel
  ip unnumbered Loopback0
```

步骤2： 配置隧道模板

隧道源是用于将VTI头端路由器连接到核心交换机的接口。

```
interface Virtual-Template [VTI template number] type tunnel
  tunnel source [source interface]
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile [IPsec profile name]
```

技术提示

在应用虚拟模板配置时，请确保启用了“type tunnel（键入隧道）”选项。如果没有此选项，VTI模板将不会应用于加密配置。

步骤2示例:

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source Port-channel32
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile sba-ipsec
```

步骤3： 配置加强型内部网关路由协议(EIGRP)接口定时器

EIGRP已在VPN头端路由器上进行了配置，但在本步骤中，您将为VTI隧道接口配置一些额外的EIGRP要求。

EIGRP问候间隔(hello interval)增加至20秒，EIGRP保持时间(hold time)增加至60秒，以适应与在3G网络上运行的数据相关的可变延迟和延时。

```
interface Virtual-Template [VTI template number] type tunnel
 ip hello-interval eigrp [as number] [hello-interval (sec)]
 ip hold-time eigrp [as number] [hold-time (sec)]
```

步骤3示例

```
interface Virtual-Template1 type tunnel
 ip hello-interval eigrp 1 20
 ip hold-time eigrp 1 60
```

程序3　配置总部ASA

VPN中枢连接到互联网边缘防火墙后面的网络核心层。互联网边缘自适应安全设备(ASA)必须将所有输入的VPN流量都转发到路由器的专用IP地址，并在ASA的由外到内访问策略中支持VPN流量的传输。

步骤1： 在目前激活的互联网边缘ASA上采用以下配置，将通过把外部地址172.16.20.7转换为VPN头端路由器的专用地址10.10.32.126，支持到VPN头端的连接。此配置允许VPN流量流经ASA，并连接到头端VTI中枢路由器。

```
object network VPN-hub-inside
  host 10.10.32.126
  description Private Address for WAN Router/VPN Hub
object network VPN-hub-outside
  host 172.16.20.7
  description Public IP Address for VPN Hub
!
object-group service isakmp-esp
 service-object udp destination eq 4500
 service-object udp destination eq isakmp
 service-object esp
!
```

```
access-list outside_access_in extended permit object-group
isakmp-esp any object VPN-hub-inside
!
nat (inside,outside) after-auto source static VPN-hub-inside
VPN-hub-outside
!
access-group outside_access_in in interface outside
```

流程

配置GSM专用的远程站点路由器

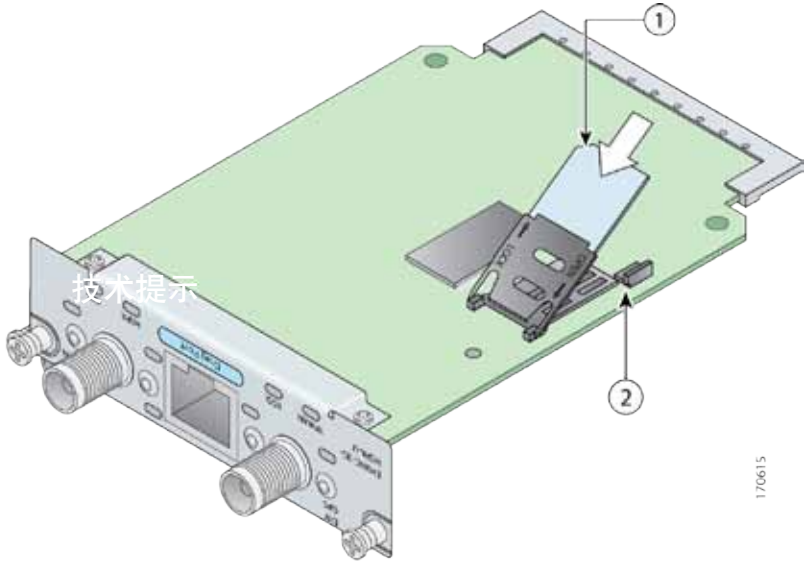
1. 将GSM HWIC安装到ISR中
2. 配置对话脚本和GSM配置文件

技术提示

您必须向电信运营商申请一个数据服务帐户。您将获得一张用于安装在GSM高速广域网接口卡(HWIC)上的SIM卡。此外您也将获得以下信息：PPP质询握手认证协议(CHAP)用户名（主机名），PPP CHAP密码和APN（接入点名称）。

程序1 将GSM HWIC安装到ISR中

图4. GSM HWIC SIM卡安装



步骤1： 将SIM卡插入HWIC。

步骤2： 关闭ISR G2路由器的电源。

步骤3： 将GSM HWIC插入路由器中并固定。

步骤4： 启动路由器并开始配置

程序2 配置对话脚本和GSM配置文件

对话脚本（chat script）是用于发送调制解调器拨号命令的文本字符串，以登录到远程系统，并初始化异步设备（这些设备连接到一个异步线路）。应当像对待任何其它异步接口一样对待3G广域网接口。

以下对话脚本显示了连接到AT&T GSM网络所需的信息。

步骤1：此对话脚本使用运营商特定拨号串和30秒的超时值。注意，您的运营商可能需要不同的对话脚本。

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

步骤1示例：

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

步骤2：将对话脚本应用于异步线路

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

步骤2示例：

对于接口cellular0/0/0，匹配线路编号将为：

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

步骤3：创建GSM配置文件

此步骤应当在启用模式中完成，而不是在配置模式中。

```
cellular [Cellular-Interface] gsm profile create [sequence-Number] [AP-Name] ipv4 chap [username] [password]
```

步骤3示例：

从启用模式，使用此配置文件来识别电信运营商提供给您的用户名和密码。使用蜂窝接口标识符和关键字gsm。

```
cellular 0/0/0 gsm profile create 1 isp.cingular ipv4 chap ISP@CINGULARGPRS.COM CINGULAR1
```

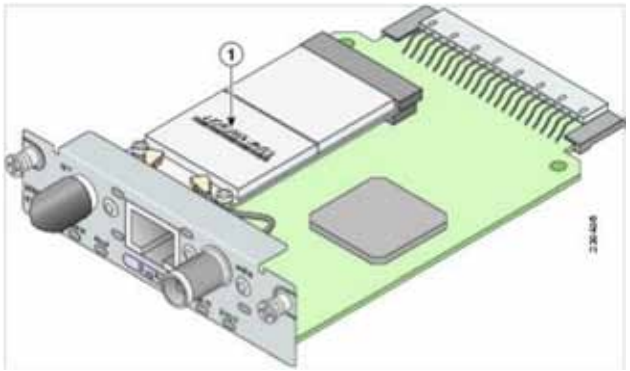
流程

配置CDMA专用的远程站点路由器

1. 将CDMA HWIC安装到ISR中
2. 激活CDMA调制解调器
3. 配置对话脚本

CDMA部署与GSM部署不同。您无需使用配置文件。

图5. CDMA HWIC ESN位置



技术提示

您必须获得无线数据服务并确保HWIC已在无线电信运营商的网络中进行了注册。电信运营商将提供激活号码，通过呼叫此号码来激活调制解调器。

程序1　将CDMA HWIC安装到ISR中

步骤1：使用在HWIC上发现的电子序列号(ESN)，向电信运营商注册CDMA HWIC。

步骤2：关闭ISR G2路由器的电源。

步骤3：将CDMA HWIC插入路由器中并固定。

步骤4：启动路由器并开始配置。

程序2　激活CDMA调制解调器

步骤1：在使用CDMA HWIC之前，您必须先激活它。请使用CDMA运营商提供的激活号码进行激活。

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

示例（Verizon CDMA网络）：

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

程序3　配置对话脚本

对话脚本是用于发送调制解调器拨号命令的文本字符串，以登录到远程系统，并初始化异步设备（这些设备连接到一个异步线路）。应当像对待任何其它异步接口一样对待3G广域网接口。

以下对话脚本显示了连接到Verizon CDMA网络所需的信息。

步骤1：此对话脚本使用了运营商特定拨号串和30秒的超时值。注意，您的运营商可能需要不同的对话脚本。

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

步骤1示例:

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

步骤2：将对话脚本应用于异步线路

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

步骤2示例:

对于接口cellular0/0/0，匹配线路号码将为：

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

流程

配置远程站点3G路由器

1. 配置蜂窝接口
2. 配置拨号接口
3. 为备用链路配置路由
4. 应用访问列表
5. 配置ISAKMP和IPsec
6. 配置VTI隧道
7. 配置EIGRP

在此流程中，您将为使用GSM或CDMA技术的远程站点配置3G/VTI分支路由器。

程序1　配置蜂窝接口

在本程序中，您向拨号池(dialer pool)添加蜂窝接口，并在程序2中将所有其它配置参数分配给拨号接口。同时带宽值被设置为与远程站点所采用的技术的上行链路速度相匹配。

表1 GSM 3G和CDMA 3G的上行链路和下行链路速度

技术	最大下行链路速度（Kbps）	最大上行链路速度（Kbps）
GSM 3G	3600	384
CDMA 3G	3100	1800

步骤1：向拨号池指定物理接口：

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

示例（显示给GSM 3G的带宽）：

```
interface Cellular0/0/0
 bandwidth 384
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 no peer default ip address
 async mode interactive
 no shutdown
```

程序2 配置拨号接口

拨号接口(dialer interface)是一个逻辑接口，可让您控制由一个或多个物理接口组成的接口池。拨号接口提供了一致的配置，避免受到底层物理接口的类型和相关接口编号的影响。

步骤1：指定拨号参数

```
interface Dialer [Dialer Interface Number]
 bandwidth [bandwidth (Kbps)]
 dialer pool [Dialer Pool Number]
 dialer idle-timeout 0
 dialer string [Chat Script Name]
 dialer persistent
 no shutdown
```

技术提示

对于拨号串，请使用您之前创建的对话脚本。
对于GSM网络，请使用GSM
对于CDMA网络，请使用CDMA

步骤2：指定基本点到点协议(PPP)参数

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

步骤3：指定PPP身份验证参数。此步骤仅适用于使用GSM技术的路由器。

技术提示

PPP身份验证信息由您的GSM电信运营商提供。不必为使用CDMA技术的路由器配置PPP CHAP主机名称和密码。

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

示例：

```
interface Dialer1
 bandwidth 384
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 0
 dialer string GSM          ! This example shows GSM (vs CDMA)
 dialer persistent
 ppp chap hostname ISP@CINGULARGPRS.COM ! Required for GSM only
 ppp chap password CINGULAR1           ! Required for GSM only
 ppp ipcp address accept
 ppp timeout retry 120
 ppp timeout ncp 30
```

程序3　为备用链路配置路由

使用3G/VTI的远程站点为拨号接口采用PPP协商IP地址。与DHCP不同，PPP协商不会自动设置静态路由。这一步骤必须手动完成。

步骤1：配置一个主机路由，通过拨号接口实现VPN头端路由器的IP可达性：

```
ip route [IP Address of VPN Headend] 255.255.255.255
[interface type] [number]
```

例如：

```
ip route 172.16.20.7 255.255.255.255 Dialer1
```

程序4　应用访问列表

3G路由器直接连接至互联网，无需单独的防火墙。这一连接采用IP访问列表来进行保护。访问列表仅允许传输加密隧道所需的流量，以及进行故障排除所需要的各种互联网控制消息协议(ICMP)协议。

步骤1：应用访问列表。

IP访问列表必须许可下表中指定的协议。访问列表应用于广域网接口的入站方向，因此将对前往路由器的流量进行过滤。

表2. 必需的IPsec VTI协议

名称	协议	用途
non500-isakmp	UDP 4500	基于NAT-T的IPsec
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec

必需协议示例：

```
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
```

下表中所列的其他协议可以协助进行故障排除，但并非IPsec VTI正常运行所必需的协议。

表3. 可选的访问列表协议

名称	协议	用途
ICMP echo	ICMP type 0, code 0	允许远程ping
ICMP echo-reply	ICMP type8, code 0	允许ping回复
ICMP ttl-exceeded	ICMP type 11, Code0	Windows跟踪路由(traceroute)
ICMP port-unreachable	ICMP type 3, code 3	服务无法到达

其他可添加到访问列表中以支持ping的可选条目如下所示：

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

其他可添加到访问列表中以支持Windows路由跟踪的可选条目如下所示：

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

必需协议和用于ping的可选协议示例

```
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
```

程序5　配置ISAKMP和IPsec

步骤1： 配置预共享密钥。

加密ISAKMP密钥定义了一个与IPsec对等体上的密钥相匹配的预共享密钥（或密码）。远程站点仅连接到用于连接VPN头端路由器的互联网地址，因此对等体的地址在ISAKMP配置中进行定义：

```
crypto isakmp key [pre-shared key] address [IP Address VPN Hub Router]
```

步骤2： 配置ISAKMP策略

面向VTI的ISAKMP策略采用如下规则：

- 基于128位密钥的AES
- SHA
- 使用预共享密钥进行身份验证
- Diffie-Hellman组2

```
crypto isakmp policy [policy sequence]
 encr aes
 hash sha
 authentication pre-share
 group 2
```

步骤3： 定义IPsec转换集。

转换集是一个可接受的安全协议、算法和其他设置的组合，应用于IPsec保护流量。对等体同意在保护特定的数据流时使用特定的转换集。

IPsec转换集采用如下规则：

- 采用128位AES加密算法的ESP
- 采用SHA（HMAC变体）身份验证算法的ESP

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

步骤4：创建IPsec配置文件。

IPsec配置文件在一个身份地址和一个IPsec转换集创建了一个关联。

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

示例

```
crypto isakmp policy 1
 encr aes
 hash sha
 authentication pre-share
 group 2
crypto isakmp key iba address 172.16.20.7
!
!
crypto ipsec transform-set iba-xform esp-aes esp-sha-hmac
!
crypto ipsec profile iba-ipsec
 set transform-set iba-xform
```

程序6　配置VTI隧道

步骤1：配置基本接口设置。

隧道接口在配置的过程中创建。隧道编号可随意设定，但最好从10或更大的数字开始编号，这是因为这一设计中部署的其他特性也可能需要使用隧道，它们可能在缺省情况下选择了较小的数字。您需要向隧道分配明确的IP地址。它与回环(loopback)使用相同的地址。

```
interface Tunnel [number]
  ip unnumbered Loopback0
```

步骤2：配置隧道。

VTI使用IPSec IPv4隧道。这一隧道类型仅需要一个源接口。源接口应与用于连接互联网的接口相同。隧道目的地是VPN头端路由器。

在这一接口上启用加密要求采用在程序5中配置的IPsec配置文件。

```
interface Tunnel [number]
 tunnel source [source interface]
 tunnel mode ipsec ipv4
 tunnel destination [IP Address VPN Hub Router]
 tunnel protection ipsec profile [IPSec profile name]
```

步骤3：配置EIGRP。

EIGRP在程序7中进行配置，但在本步骤中您将为VTI隧道接口配置一些额外的EIGRP要求。

EIGRP问候间隔(hello interval)增加至20秒，EIGRP保持时间(hold time)增加至60秒，以适应与在3G网络上运行的数据相关的可变延迟和延时。

```
interface Tunnel [number]
 ip hello-interval eigrp [as number] [hello-interval (sec)]
 ip hold-time eigrp [as number] [hold-time (sec)]
```

远程站点局域网必须进行通告。远程站点的IP分配经过专门设计，旨在确保正在使用的所有网络均能够在单个汇聚路由中进行汇总。如下配置的汇总地址可以禁止更多特定的路由。如果该汇总结果中的任何网络出现在路由表中，汇总结果将被通告给VPN中枢，从而提供了一种永续性措施。如果各个局域网不能进行汇总，那么EIGRP将继续通告特定的路由。

```
interface Tunnel [number]
  ip summary-address eigrp [as number] [summary network]
[summary mask]
```

示例:

```
interface Tunnel10
 ip unnumbered Loopback0
 ip hello-interval eigrp 1 20
 ip hold-time eigrp 1 60
 ip summary-address eigrp 1 10.11.216.0 255.255.248.0
 tunnel source Dialer1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.20.7
 tunnel protection ipsec profile iba-ipsec
```

程序7　配置EIGRP

单个EIGRP进程运行在3G路由器上。VPN隧道接口是一个非被动EIGRP接口，该路由器上的所有局域网接口均为被动EIGRP接口。网络范围必须在单个网络声明或多个网络声明中包含所有接口IP地址。所有VPN 分支路由器应运行EIGRP存根路由(stub routing)，以提高网络稳定性和降低资源消耗。

步骤1：向回环地址指定路由器ID。

```
router eigrp [as number]
  network [WAN remote range] [inverse mask]
  passive-interface default
  no passive-interface [tunnel interface]
  eigrp stub connected summary
  no auto-summary
```

示例

```
router eigrp 1
  network 10.11.0.0 0.0.255.255
  passive-interface default
  no passive-interface Tunnel10
  eigrp stub connected summary
  no auto-summary
```

流程

控制3G接口的使用

1. 监视MPLS邻居的可达性

许多3G电信运营商未提供无使用限制的移动数据套餐。通常，您需要选择基于使用情况的套餐，并采用符合对远程站点业务要求的带宽。为了最大限度降低3G解决方案的经常性成本，建议仅在必要时才使用3G无线广域网。

使用3G/VTI作为备用传输方式的远程站点能够跟踪主用MPLS链路的状态，并在必要时激活3G WAN作为备用链路。

程序1　监视MPLS邻居的可达性

这一程序应用于控制双链路设计中3G接口的使用。MPLS VPN为主用广域网传输，只要它运行，3G接口就保持关闭。

远程站点3G路由器能够使用IP SLA特性来将回声探测发送至该站点的MPLS PE路由器，如果PE路由器不可达，则该路由器可使用嵌入式事件管理器（EEM）来动态启用3G接口。

步骤1：启用IP SLA探测

此设计使用了标准ICMP echo (ping)探测，每隔15秒发送一次。响应必须在1000毫秒时间内收到。如果您使用MPLS Provider Edge (PE)路由器作为探测目的地，则目的地地址与之前在该路由器上配置的IP缺省路由next-hop（下一跳）地址相同。使用MPLS广域网接口作为探测源接口。

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

步骤2：配置增强的对象跟踪

将IP SLA探测状态链接至EEM脚本所监视的一个对象。

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

步骤3：配置EEM脚本，以启用或禁用3G接口

一个事件跟踪EEM脚本可监视对象的状态，并针对特定状态运行思科IOS路由器命令。它也是生成syslog（系统日志）消息的最佳实践，syslog消息可提供有关EEM的状态信息。

```
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]"
```

示例

```
track 60 ip sla 100 reachability
ip sla 100
 icmp-echo 192.168.5.134 source-interface GigabitEthernet0/0
 threshold 1000
 frequency 15
ip sla schedule 100 life forever start-time now
```

用于在MPLS链路发生故障时启用3G接口的EEM脚本:

```
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"
```

用于在MPLS链路恢复后禁用3G接口的EEM脚本:

```
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"
```

备注

附录A：产品部件编号

以下产品和软件版本已经过验证，可用于思科IBA智能业务平台：

功能区域	产品	产品编号	软件版本
总部	Cisco 3925集成多业务路由器G2	C3925	15.1(4)M2
分支机构	Cisco 2911集成多业务路由器G2	C2911-VSEC/K9 EHWIC-3G-EVDO-V HWIC-3G-CDMA HWIC-3G-GSM	15.1(4)M2

附录B：针对GSM的分支机构ISR配置

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname Br4-1941
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$BFVP$A2lWGXIS0HtzpB0y7oy9B0
!
no aaa new-model
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
chat-script GSM "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
crypto pki token default removal timeout 0
!
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
!
track 60 ip sla 100 reachability
!
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
crypto isakmp key sba address 172.16.20.7
!
!
crypto ipsec transform-set sba-xform esp-aes esp-sha-hmac
!
crypto ipsec profile sba-ipsec
 set transform-set sba-xform
!
!
```

```
!
!
!
!
interface Loopback0
 ip address 10.11.216.254 255.255.255.255
!
interface Tunnel10
 ip unnumbered Loopback0
 ip hello-interval eigrp 1 20
 ip hold-time eigrp 1 60
 ip summary-address eigrp 1 10.11.216.0 255.255.248.0
 tunnel source Dialer1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.20.7
 tunnel protection ipsec profile sba-ipsec
!
interface GigabitEthernet0/0
 ip address 192.168.5.133 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.64
 description Data
 encapsulation dot1Q 64
 ip address 10.11.220.1 255.255.255.0
!
interface GigabitEthernet0/1.65
 description WirelessData
 encapsulation dot1Q 65
 ip address 10.11.218.1 255.255.255.0
!
interface Cellular0/0/0
 bandwidth 384
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 no peer default ip address
 async mode interactive
!
interface Vlan1
 no ip address
!
interface Dialer1
 bandwidth 384
 ip address negotiated
 ip access-group ACL-INET-PUBLIC in
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 0
 dialer string GSM
 dialer persistent
 ppp chap hostname ISP@CINGULARGPRS.COM
 ppp chap password 7 <password omitted>
 ppp ipcp address accept
 ppp timeout retry 120
 ppp timeout ncp 30
!
!
router eigrp 1
 network 10.11.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp stub connected summary
!
ip forward-protocol nd
!
no ip http server
ip http secure-server
!
```

```
ip route 0.0.0.0 0.0.0.0 192.168.5.134
ip route 172.16.20.7 255.255.255.255 Dialer1
!
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 sla 100
 icmp-echo 192.168.5.134 source-interface GigabitEthernet0/0
 threshold 1000
 frequency 15
ip sla schedule 100 life forever start-time now
access-list 10 permit 239.1.0.0 0.0.255.255
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
!
control-plane
!
!
!
line con 0
 logging synchronous
line aux 0
line 0/0/0
 script dialer GSM
 no exec
 rxspeed 3600000
 txspeed 384000
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
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.10.48.17
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"
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"
!
end
```

附录C：针对CDMA的分支机构ISR配置

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname Br5-1941
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$BFVP$A2lWGXIS0HtzpB0y7oy9B0
!
no aaa new-model
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
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 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
!
track 60 ip sla 100 reachability
!
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
crypto isakmp key sba address 172.16.20.7
!
!
crypto ipsec transform-set sba-xform esp-aes esp-sha-hmac
!
crypto ipsec profile sba-ipsec
 set transform-set sba-xform
!
!
```

```
!
!
!
!
interface Loopback0
 ip address 10.11.216.254 255.255.255.255
!
interface Tunnel10
 ip unnumbered Loopback0
 ip hello-interval eigrp 1 20
 ip hold-time eigrp 1 60
 ip summary-address eigrp 1 10.11.216.0 255.255.248.0
 tunnel source Dialer1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.20.7
 tunnel protection ipsec profile sba-ipsec
!
interface GigabitEthernet0/0
 ip address 192.168.5.133 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.64
 description Data
 encapsulation dot1Q 64
 ip address 10.11.220.1 255.255.255.0
!
interface GigabitEthernet0/1.65
 description WirelessData
 encapsulation dot1Q 65
 ip address 10.11.218.1 255.255.255.0
!
interface Cellular0/0/0
 bandwidth 384
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 no peer default ip address
 async mode interactive
!
interface Vlan1
 no ip address
!
interface Dialer1
 bandwidth 384
 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
 ppp timeout retry 120
 ppp timeout ncp 30
!
!
router eigrp 1
 network 10.11.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp stub connected summary
!
ip forward-protocol nd
!
no ip http server
ip http secure-server
!
```

```
ip route 0.0.0.0 0.0.0.0 192.168.5.134
ip route 172.16.20.7 255.255.255.255 Dialer1
!
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 sla 100
 icmp-echo 192.168.5.134 source-interface GigabitEthernet0/0
 threshold 1000
 frequency 15
ip sla schedule 100 life forever start-time now
access-list 10 permit 239.1.0.0 0.0.255.255
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
!
control-plane
!
!
!
line con 0
 logging synchronous
line aux 0
line 0/0/0
 script dialer CDMA
 no exec
 rxspeed 3600000
 txspeed 384000
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
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.10.48.17
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"
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"
!
end
```

附录D:
头端或总部ISR配置

```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname hq-isr3925
!
boot-start-marker
boot system flash flash:/c3900-universalk9-mz.SPA.151-4.M2.bin
boot-end-marker
!
card type t1 0 1
enable secret 5 $1$I8CP$uHwNRwZcdZng6MojLVDva.
!
no aaa new-model
!
!
!
clock timezone PST -8
clock summer-time PDT recurring
no network-clock-participate wic 1
!
!
!crypto pki trustpoint TP-self-signed-4285596865
! enrollment selfsigned
! subject-name cn=IOS-Self-Signed-Certificate-4285596865
! revocation-check none
! rsakeypair TP-self-signed-4285596865
!
!
!crypto pki certificate chain TP-self-signed-4285596865
! certificate self-signed 02
!
! <certificate information intentionally removed>
!
no ipv6 cef
ip source-route
ip cef
!
!
ip multicast-routing
!
!
ip domain name cisco.local
ip name-server 10.10.48.10
ip wccp 61 redirect-list WAAS-REDIRECT-LIST password 7
070C705F4D06485744
ip wccp 62 redirect-list WAAS-REDIRECT-LIST password 7
130646010803557878
!
multilink bundle-name authenticated
!
!
license udi pid C3900-SPE100/K9 sn FOC13102BQZ
license boot module c3900 technology-package securityk9
license boot module c3900 technology-package datak9
!
!
username admin privilege 15 secret 5 $1$G/
Dq$SJnlAbOOz10zUSeHeVZxu1
!
redundancy
!
!
controller T1 0/1/0
```

```
 cablelength long 0db
!
!
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 esp-sha-hmac
!
crypto ipsec profile sba
 set transform-set xform
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.32.255 255.255.255.255
 !
!
interface Port-channel32
 description uplink to 4507 Core
 ip address 10.10.32.126 255.255.255.128
 ip wccp 62 redirect in
 ip pim sparse-mode
 ip flow ingress
 !
 hold-queue 150 in
!
interface GigabitEthernet0/0
 description uplink to MPLS WAN
 ip address 192.168.5.65 255.255.255.252
 ip wccp 61 redirect in
 ip flow ingress
 duplex auto
 speed auto
 !
!
interface GigabitEthernet0/1
 no ip address
 ip flow ingress
 duplex auto
 speed auto
 media-type rj45
 channel-group 32
 !
!
interface GigabitEthernet0/2
 no ip address
 ip flow ingress
 duplex auto
 speed auto
 channel-group 32
 !
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip hello-interval eigrp 1 20
 ip hold-time eigrp 1 60
 tunnel source Port-channel32
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile sba
 !
!
```

```
!
!
router eigrp 1
 network 10.10.0.0 0.0.255.255
 redistribute static
!
ip forward-protocol nd
!
no ip http server
ip http secure-server
ip flow-cache timeout active 1
ip flow-export version 5
!
ip route 10.11.0.0 255.255.0.0 192.168.5.66
ip route 192.168.5.64 255.255.255.224 192.168.5.66
!
ip access-list extended WAAS-REDIRECT-LIST
 permit tcp any any
!
!
!
!
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
!
control-plane
 !
!
!
line con 0
line aux 0
line vty 0 4
 login local
line vty 5 15
 login local
!
scheduler allocate 20000 1000
ntp master
ntp server 10.10.48.17
end
```

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.**

B-0000501-2 2/12