CHAPTER 5

高度なネットワーク導入シナリオ

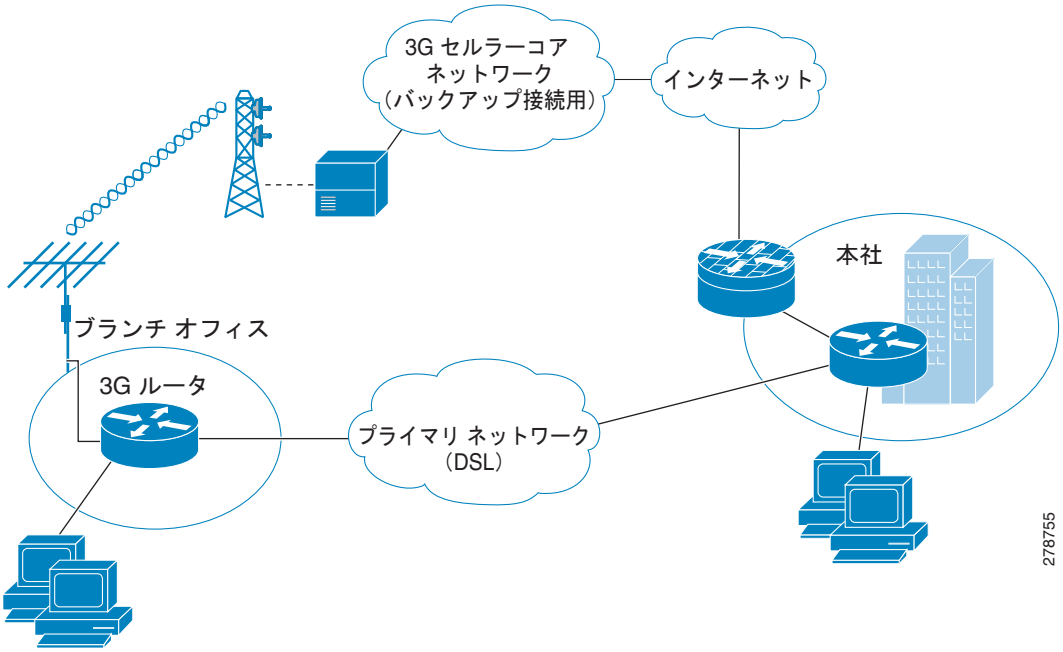
この章では、高度な導入シナリオについて説明します。この章全体で導入シナリオに使用されている設定は、GSM 用です。同じ設定にわずかな変更を加えることで、CDMA 導入シナリオに使用できます。

内容

NAT/PAT および IPSec を使用したプライマリおよびバックアップの導入

図 5-1 には、プライマリ リンクとして DSL インターフェイスを使用し、バックアップ リンクとしてセルラー インターフェイスを使用する導入が示されています。この導入では、ブランチ オフィス ルータのホストとパブリック ネットワーク経由の本社サイトのホスト間のセキュア通信に、ブランチ オフィスで NAT/PAT および IPSec を使用します。この導入により、インターネット上のホストとのノンセキュア（非 IPsec）通信も行えるようになります。

図 5-1　　NAT/PAT および IPSec を使用したプライマリおよびバックアップの導入



ブランチ オフィス ルータの設定

例 5-1　　ブランチ オフィス ルータの設定

この設定内で青色の斜体で記載されたテキストは*コメント*を示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

特に明記されていない限り、太字のテキストは基本セルラー コマンドに関連付けられているコマンドを示します。太字のテキストは暗号化 IPsec 設定、バックアップ設定、IP SLA 設定、およびモバイル IP の設定など、他の設定にも使用されます。これらの各設定に関連付けられているコマンドはサンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
!
!    この設定では、信頼できるオブジェクト トラッキングを使用した IP SLA が使用されます。この設定は
!    任意です。これを使用して、このプライマリ インターフェイスを介した外部ネットワークで、
!    ICMP の ping を使用して、ある既知の IP 宛先アドレスへのプライマリ（DSL）インターフェイスを介した
!    接続性のトラッキングを行えます。ping への応答の受信に失敗すると、プライマリ インターフェイスを介した
```

```
!   デフォルト ルートがルーティング テーブルから削除され、セルラー インターフェイスを介した
!   (より高い管理距離で設定されている) デフォルト ルートが有効なパスになり、
!   バックアップ パスを介して接続できるようになります。
!
!   これが設定されていなくても、PPP/ 物理層でネットワーク接続障害を検出し、
!   バックアップ (セルラー) インターフェイスへのスイッチオーバーを行う
!   'backup interface …' コマンドを使用して、
!   プライマリ / バックアップ接続を実行できます。
!
!
hostname branch-router
!
ip cef
!
ip dhcp excluded-address 10.4.0.254
!
!   基本的に、このコマンドはどのホストに対しても IP アドレス 10.4.0.254 の割り当てを行いません。
!   これは、このアドレスが VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 で
!   接続されているホストのデフォルト ゲートウェイ アドレスとして使用されているからです。
!
ip dhcp pool gsmpool
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.4.0.254
!
!   VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 に接続されている
!   ホストの DHCP プール
!
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 20 "CONNECT"
!
!   セルラー インターフェイスを介したダイヤル アウトへのチャット スクリプト。
!
!
username cisco privilege 15 secret 5 $1$ccw8$TFmKUmI4QVZhOMuxzq/SH/
!
track 234 rtr 1 reachability
!
!   operation 1 を使用して、到達可能性のトラッキングに使用されるトラッキング対象のオブジェクト番号 234
!   を設定します。オブジェクトは、到達可能性条件が満たされる場合は 'UP' です。

!   これは、(プライマリ リンクとして使用される) ATM DSL インターフェイスを介して ping パケットを送信し、
!   応答を監視するために使用されます。また、応答がない場合に (セルラーへの) スイッチオーバーが
!   必要かどうかを判別するために使用されます。
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
!
!   (priority 1 を設定して) IKE ポリシーを定義し、IKE ネゴシエーション中に 3DES を指定します。また、
!   事前定義されたキーを使用して事前共有認証を指定します。ライフタイムの値 (1 日に 86,400 秒に設定)、
!   グループ (768 ビットディフィー・ヘルマン鍵共有に設定)、
!   およびハッシュ (SHA-1 に設定) は、デフォルト値に設定されます。
!
!
crypto isakmp key mykey address 20.20.241.234
!
!   セキュリティ アソシエーションの設定に使用されるキー (mykey)
!   およびゲートウェイの IP アドレス (IPsec peer) を定義します。
!
crypto ipsec transform-set mytransformset ah-sha-hmac esp-3des
!
!   セキュリティ プロトコル、アルゴリズム、および他の設定の許容可能な組み合わせである
!   トランスフォーム セット (mytransformset) を定義して、IPsec で保護されている
```

```
!   トラフィックを適用します。
!
crypto map gsm1 10 ipsec-isakmp
 set peer 20.20.241.234
 set transform-set mytransformset
 match address 103
!
!   クリプト マップ gsm1 を定義します
!
!   クリプト マップは（match address <access-list> コマンドを使用して）保護対象のトラフィック、
!   使用するピア エンド ポイント、および使用するトランスフォーム セット
!   （以前に定義した mytransformset）を指定します。
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 104
!
interface FastEthernet0/1/1
 switchport access vlan 104
!
interface FastEthernet0/1/2
 switchport access vlan 104
!
interface FastEthernet0/1/3
 switchport access vlan 104
!
!   DHCP クライアント ホストによって使用されるファスト イーサネット ポート。
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
!   プライマリ インターフェイスとして使用される ATM（DSL）物理インターフェイス。
!
interface ATM0/0/0.1 point-to-point
 ip nat outside
 ip virtual-reassembly
 no snmp trap link-status
 pvc 0/35
  pppoe-client dial-pool-number 2
!
!
!   プライマリ接続として PVC に使用する ATM サブインターフェイス。このインターフェイスでは
!   NAT（外部）が使用されます。
!
!   pppoe-client dial-pool-number 2 は PPP over Ethernet（PPOE）クライアントを設定し、
!   使用するダイヤラ プール 2 を指定します。このインターフェイスは、以下で定義されている 'interface
!   Dialer 2' に関連付けられます。
!
interface Cellular0/3/0
 ip address negotiated
```

```
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 0
 dialer string gsmscript
 dialer-group 1
 ppp chap hostname isp-provided-hostname
 ppp chap password 0 isp-provided-password
 ppp ipcp dns request
 crypto map gsm1
!
!   上記で定義したクリプト マップ gsm1 を、このバックアップ インターフェイスに適用します。
!
!   dialer-group 1 は group number 1 を定義します。この設定では、これは以下で指定される
!   dialer-list 1... コマンドに関連付けられます。これは、ダイヤル アウトをトリガーし、
!   PPP を確立した後にインターフェイスをオンラインにする「対象のトラフィック」を
!   定義します。通常、このインターフェイスはスタンバイ状態のままになることに注意してください。このため、
!   対象のトラフィックではダイヤル アウトはトリガーされません。トラフィックはすでに
!   プライマリ（ATM DSL）インターフェイスを介してフローしています。
!
!   NAT のインターフェイスを外部で定義します。
!
interface Vlan104
 description ip address used as default gateway address for DHCP    clients
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
!
!   NAT（内部インターフェイス）を使用して、ファスト イーサネット ポート 0/1/0 から 0/1/3
!   に接続されたホストに VLAN 104 を定義します
!
interface Dialer2
 ip address negotiated
 ip mtu 1492
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 load-interval 30
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap hostname isp-provided-hostname
 ppp chap password 0 isp-provided-password
 ppp pap sent-username isp-provided-hostname password 0 isp-provided-password
 ppp ipcp dns request
 crypto map gsm1
!
!   dialer pool 2 コマンドはこのダイヤラ インターフェイスを ATM サブインターフェイス
!   atm0/0/0.1 に関連付けます。'dialer-group 2' は group number 2 を定義します。この設定では、
!   これは以下で指定されている dialer-list 2... コマンドに関連付けられます。これは、PPP を確立した後に、
!   ダイヤル アウトをトリガーし、インターフェイスをオンラインにする「対象のトラフィック」
!   を定義します。
!
!   NAT のインターフェイスを外部で定義します。
!
!   上記で定義したクリプト マップ gsm1 をこのプライマリ インターフェイスに適用します。
!
ip local policy route-map track-primary-if
!
!   ルート マップの track-primary-if で定義されているように、
!   IP ルート ポリシーを指定します。
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
```

```
!
!   上記で定義したトラッキング オブジェクト（234）を指定し、ダイヤラ 2（ATM DSL）
!   を介してデフォルト ルートを定義します。
!
!   ルートはトラッキング対象オブジェクト（234）が 'UP' である場合のみインストールされます。
!
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
!   管理距離を 254（ダイヤラ 2 のインターフェイスより高い）に設定して、
!   セルラー インターフェイスを介してデフォルト ルートを定義します。通常このインターフェイスは
!   バックアップ インターフェイスとして想定されているからです。
!
!
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 5 life 86400 requests 10000
!
ip nat inside source route-map nat2cell interface Cellular0/3/0 overload
!
!   セルラー インターフェイスを介して、外部 NAT トラフィックの条件としてルート マップ nat2cell を
!   定義します（以下で指定）。'overload' オプションを使用すると、PAT が使用されるようになります。
!
!   ルート マップ nat2cell で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
!   上記と同様に、ダイヤラ 2 インターフェイス（ATM DSL）を使用して、外部 NAT トラフィックに対して
!   ルート マップ nat2cell を（以下で定義されているように）定義します。'overload' オプションを
!   使用すると、PAT が使用されるようになります。
!
!   ルート マップ nat2dsl で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip sla 1
 icmp-echo 209.131.36.158 source-interface Dialer2
 timeout 1000
 frequency 2
ip sla schedule 1 life forever start-time now
!
!   2 秒間隔（frequency 2）で、ping への応答に 1000 ミリ秒の待機（タイムアウト 1000）を設定し、
!   ソース インターフェイスとしてダイヤラ 2（ATM DSL）を使用して、
!   IP アドレス 209.131.36.158 に ping を送信するためのサービス レベル契約（SLA）を
!   定義します。
!
!   定義された SLA を開始し、これを継続的に実行します。
!
access-list 1 permit any
!
!   以下の 'dialer-list 1 protocol ip list 1' コマンドに関連付けられています
!
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
!
!   ルート マップ nat2dsl と nat2cell の下に定義されているように、
!   適切な発信インターフェイスを決定するために、トラフィックが一致するように指定します
!   （ネットワーク 10.4.0.0 のソース アドレスと一致）。
!
access-list 102 permit icmp any host 209.131.36.158
!
!   このインターフェイスがアクティブな場合にのみ、ATM DSL インターフェイスを介して送信されるように、
!   ルート マップ 'track-primary-interface' のトラフィックを指定します。
!
!   この特定のアドレスは、ATM DSL インターフェイス（プライマリ リンク）を介して定期的に ping される
!   アドレスであるため、リンク /PPP レベル以外のネットワーク障害も検出される場合があり、
!   セルラー（セカンダリ）インターフェイスへのスイッチオーバーが
```

```
!   まだ実行される可能性があります。
!
!   ping されるアドレスが信頼でき、ping に応答することを確認します。
!
access-list 103 permit ip host 166.138.186.119 20.20.0.0 0.0.255.255
access-list 103 permit ip host 75.40.113.246 20.20.0.0 0.0.255.255
!
!   クリプト マップ gsm1 の下に定義されたとおりの、
!   IPsec に対して保護されたトラフィックの指定。
!
!   ソース アドレス（166.138.186.119 および 75.40.113.246）は、セルラー インターフェイス（セカンダリ）
!   と ATM DSL インターフェイス（プライマリ）の IP アドレスです。
!
!   20.20.0.0 は宛先ネットワークであり、対応するゲートウェイが接続されています
!
dialer-list 1 protocol ip list 1
!
!   セルラー インターフェイスがダイヤル アウトする原因となる 'interesting traffic' を指定します。
!   それによって、access-list 1 が（上記で定義されたこのコマンドの一部として）さらに指定されます。
!
dialer-list 2 protocol ip permit
!
!   ATM DSL インターフェイスが（ダイヤラ 2 インターフェイスの一部として）ダイヤル アウトするようにする
!   'interesting traffic' を指定します。
!
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2 null0
!
!   ローカル ルーティング用にポリシー条件として使用されるルート マップを指定します
!   （上記の関連するコマンド 'ip local policy route-map track-primary-if'
!   を参照してください）。
!
!   これが宛先 209.131.36.158 の ping パケットで、インターフェイス ダイヤラ 2
!   （ATM DSL）が 'UP' の状態で接続されている場合、ping パケットを送信します。この ping パケットは、
!   ATM DSL インターフェイスを介してのみ送信され、セルラー インターフェイスを介しては送信されません。
!   これは、接続が失敗したときにスイッチオーバーを実行するために、ATM DSL インターフェイスを介して
!   接続（到達可能性）を定期的にモニタリングするためです。
!
route-map nat2dsl permit 10
 match ip address 101
 match interface Dialer2
!
!   上記のアクセス リスト 101 によって定義されている一致条件を満たし、
!   ダイヤラ 2 インターフェイスが 'UP' の状態で接続されている場合、
!   このルート マップが使用されるように指定します。

!   トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
!   インターフェイスのダイヤラ 2 が 'UP' の状態で DSL ネットワークに接続されている場合、
!   このルート マップが 'ip nat inside source nat2dsl ...' コマンドによって使用されます。
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0/3/0
!
!   上記のアクセス リスト 101 によって定義されている一致条件を満たし、
!   ダイヤラ 2 インターフェイスが 'UP' の状態で接続されている場合、
!   このルート マップが使用されるように指定します。
!
!   トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
!   インターフェイス セルラーが 'UP' の状態でセルラー ネットワークに接続されている場合、このルート マップ
!   が 'ip nat inside source nat2cell ...' コマンドによって使用されます。
!
```

```
! スイッチオーバーで、プライマリおよびバックアップ インターフェイスから NAT エントリを削除します。
event manager applet pri_back
 event track 234 state any
 action 2.0 cli command "clear ip nat trans forced"

control-plane
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
 stopbits 1
line aux 0
 stopbits 1
line 0/3/0
 exec-timeout 0 0
 script dialer gsmscript
 login
 modem InOut
 no exec
 transport input all
 transport output all
 rxspeed 236800
 txspeed 118000
line vty 0 4
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000
!
end
```

本社サイトのルータの設定

例 5-2　本社サイトのルータの設定

この設定内で青色の斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
!
hostname gateway-router
!
ip cef
!
ip dhcp excluded-address 20.20.248.254
ip dhcp excluded-address 20.20.248.253
ip dhcp excluded-address 20.20.248.225
ip dhcp excluded-address 10.10.0.254
ip dhcp excluded-address 10.10.0.1
!
```

```
!   DHCP の除外アドレス
!
ip dhcp pool 20
   network 20.20.248.224 255.255.255.224
   dns-server 20.20.248.254
   default-router 20.20.248.254
!
!   20.20 ネットワーク上のホストの DHCP プール
!
ip dhcp pool 10
   network 10.10.0.0 255.255.0.0
   default-router 10.10.0.254
!
!   10.10.0.0 ネットワーク上の VPN のホストの DHCP プール
!
!
username cisco privilege 15 secret 5 $1$QF4K$Z1rE.mwS69FVx1e5l9DCU1
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share

crypto isakmp key mykey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set mytset ah-sha-hmac esp-3des
!
crypto dynamic-map gw_map 10
 description IPsec tunnel to DSL/Cellular at remote branch-router
 set transform-set mytset
 match address 101
!
crypto map mytunnelcrypto 10 ipsec-isakmp dynamic gw_map
!
!   リモート ブランチ ルータで、IPsec トンネルの mytunnelcrypto マップを
!   ATM DSL/ およびセルラー インターフェイスに定義します。
!
!
interface GigabitEthernet0/0
 description connected to cisco network, next hop:20.20.241.233
 ip address 20.20.241.234 255.255.255.252
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
 crypto map mytunnelcrypto
!
!   クリプト マップを適用する物理インターフェイス。上記の IPsec トンネルが
!   確立されるインターフェイス。
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
!
!   VPN のホストが（10.10.0.0 ネットワークで）接続されるファスト イーサネット ポート。
!
interface FastEthernet0/1/8
 switchport stacking-partner interface FastEthernet0/3/8
```

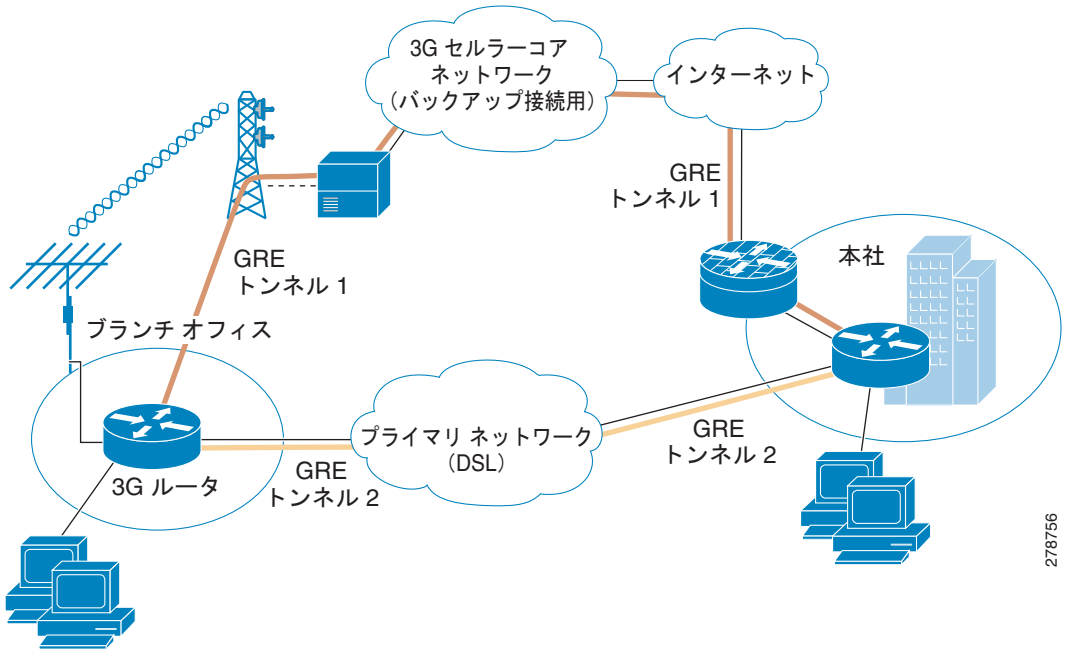
```
!
interface FastEthernet0/3/0
 switchport access vlan 20
 spanning-tree portfast
!
!
!   他のホストが（20.20 ネットワークで）接続されるファスト イーサネット ポート。
!
interface FastEthernet0/3/8
 switchport mode trunk
 switchport stacking-partner interface FastEthernet0/1/8
!
interface Vlan10
 description private networking vlan
 ip address 10.10.0.254 255.255.0.0
 no ip route-cache cef
 vlan-range dot1q 1 4095
 exit-vlan-config
!
!
!   VPN のホストの VLAN（10.10.0.0 ネットワーク内）
!
interface Vlan20
 description network:20.20.248.224/27
 ip address 20.20.248.254 255.255.255.224
 vlan-range dot1q 1 4095
 exit-vlan-config
!
!
!   他のホストの VLAN（20.20 ネットワーク内）
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
!   GigabitEthernet0/0 インターフェイスのネクスト ホップを介するデフォルト ルート。
!
ip dns server
!
access-list 101 permit ip host 20.20.241.234 host 75.40.113.246
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドで DSL インターフェイスに送信されるトラフィックです。
!
access-list 101 permit ip host 20.20.241.234 host 166.138.186.119
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドでセルラー インターフェイスに送信されるトラフィックです。
!
!
control-plane
!
line con 0
 exec-timeout 0 0
 login local
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 privilege level 15
 login local
 transport input telnet
```

```
!
scheduler allocate 20000 1000
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
!
end
```

GRE トンネルおよび IPSec を使用したプライマリおよびバックアップの導入

この導入では、パブリック ネットワークを介したブランチ オフィスのルータのホストと本社サイトのホストの間でセキュアな通信を行うために、GRE トンネルと IPsec をブランチ オフィスで使用して、プライマリ リンクとして DSL インターフェイスを使用し、バックアップ リンクとしてセルラー インターフェイスを使用します。この導入により、インターネット上のホストとのノンセキュア（非 IPsec）通信も行えるようになります。ダイナミック ルーティングを使用した GRE トンネル経由の IPSec 構成の詳細については、「*Configuring a GRE Tunnel over IPsec with OSPF*」を参照してください。

図 5-2　GRE トンネルおよび IPSec を使用したプライマリおよびバックアップの導入



ブランチ オフィス ルータの設定

例 5-3　　ブランチ オフィス ルータの設定

この設定内で青色の斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

特に明記されていない限り、太字のテキストは基本セルラー コマンドに関連付けられているコマンドを示します。太字のテキストは暗号化 IPsec 設定、バックアップ設定、IP SLA 設定、およびモバイル IP の設定など、他の設定にも使用されます。これらの各設定に関連付けられているコマンドはサンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

次の設定では、信頼できるオブジェクト トラッキングを使用した IP SLA が使用されます。この設定は任意です。

```
!
hostname branch-router
!
ip cef
!
ip dhcp excluded-address 10.4.0.254
!
!   このアドレスは、VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 上で
!   接続されているホストのデフォルト ゲートウェイ アドレスとして使用されます。
!
ip dhcp pool gsmpool
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.4.0.254
!
!   VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 に
!   接続されているホストの DHCP プール
!
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
!
!   セルラー インターフェイスを介したダイヤル アウトへのチャット スクリプト。
!
!
username cisco privilege 15 secret 5 $1$ccw8$TFmKUmI4QVZhOMuxzq/SH/
!
track 234 rtr 1 reachability
!
!   operation 1 を使用して、到達可能性のトラッキングに使用されるトラッキング対象のオブジェクト番号 234
!   を設定します。オブジェクトは、到達可能性条件が満たされる場合は 'UP' です。
!
!   これは、(プライマリ リンクとして使用される) ATM DSL インターフェイスを介して ping パケットを送信し、
!   応答を監視するために使用されます。また、応答がない場合に (セルラーへの) スイッチオーバーが
!   必要かどうかを判別するために使用されます。
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
!
!   (priority 1 を設定して) IKE ポリシーを定義し、IKE ネゴシエーション中に 3DES を指定します。また、
!   事前定義されたキーを使用して事前共有認証を指定します。ライフタイムの値 (1 日に 86,400 秒に設定)、
!   グループ (768 ビットディフィー・ヘルマン鍵共有に設定)、
!   およびハッシュ (SHA-1 に設定) は、デフォルト値に設定されます。
!
crypto isakmp key mykey address 20.20.241.234
```

```
!
!   セキュリティ アソシエーションの設定に使用されるキー（mykey）
!   およびゲートウェイの IP アドレス（IPsec peer）を定義します。
!
crypto ipsec transform-set mytransformset ah-sha-hmac esp-3des
!
!   セキュリティ プロトコル、アルゴリズム、および他の設定の許容可能な組み合わせである
!   トランスフォーム セット（mytransformset）を定義して、IPsec で保護されている
!   トラフィックを適用します。
!
crypto map mytunnelcrypto 10 ipsec-isakmp
 set peer 20.20.241.234
 set transform-set mytransformset
 match address gre-traffic
!
!   クリプト マップの mytunnelcrypto を定義します
!
!   クリプト マップは（match address <access-list> コマンドを使用して）保護対象のトラフィック、
!   使用するピア エンド ポイント、および使用するトランスフォーム セット
!   （以前に定義した mytransformset）を指定します。
!
!
interface Tunnel1
 ip unnumbered Dialer2
 ip mtu 1400
 tunnel source Dialer2
 tunnel destination 20.20.241.234
!
!   宛先 10.10.0.0 のネットワークへのトラフィックの GRE トンネル。ATM DSL（プライマリ）インター
!   フェイスに関連付けられたトンネル。このトンネルは、通常 'UP' の状態です。リモート トンネルのエンド
!   ポイント（20.20.241.234）は、リモート VPN ゲートウェイにあります。ローカル トンネルのエンドポイント
!   は、ATM DSL リンクによって取得されるアドレスです。
!
interface Tunnel2
 ip unnumbered Cellular0/3/0
 ip mtu 1400
 tunnel source Cellular0/3/0
 tunnel destination 20.20.241.234
!
!   宛先 10.10.0.0 のネットワークへのトラフィックの GRE トンネル。ATM DSL（プライマリ）インターフェイ
!   スに関連付けられたトンネル。セルラー（セカンダリ）インターフェイス。このトンネルは、通常 'Down' の
!   状態です。リモート トンネルのエンドポイント（20.20.241.234）は、リモート VPN ゲートウェイにありま
!   す。ローカル トンネルのエンドポイントは、セルラー リンクによって取得されるアドレスです。このトンネルは、
!   セルラー インターフェイスでスイッチオーバーが行われると 'UP' になります。
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 104
!
interface FastEthernet0/1/1
 switchport access vlan 104
!
interface FastEthernet0/1/2
 switchport access vlan 104
```

```
!
interface FastEthernet0/1/3
 switchport access vlan 104
!
!   DHCP クライアント ホストによって使用されるファスト イーサネット ポート
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
!   プライマリ インターフェイスとして使用される ATM（DSL）物理インターフェイス
!
interface ATM0/0/0.1 point-to-point
 ip nat outside
 ip virtual-reassembly
 no snmp trap link-status
 pvc 0/35
 pppoe-client dial-pool-number 2
!
!
!   プライマリ接続として PVC に使用する ATM サブインターフェイス。このインターフェイスでは
!   NAT（外部）が使用されます。
!
!   pppoe-client dial-pool-number 2 は PPP over Ethernet (PPOE) クライアントを設定し、
!   使用するダイヤラ プール 2 を指定します。このインターフェイスは、
!   'interface Dialer 2' に関連付けられています。
!
interface Cellular0/3/0
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 0
 dialer string gsmscript
 dialer-group 1
 async mode interactive
 ppp chap hostname crlaswlech@wwan.ccs
 ppp chap password 0 frludi3gIa
 ppp ipcp dns request
 crypto map mytunnelcrypto
!
!   上記で定義したクリプト マップ mytunnelcrypto を、このバックアップ インターフェイスに適用します。
!
!   dialer-group 1 は group number 1 を定義します。
!   この設定では、これは以下に定義されている 'dialer-list 1 ...' コマンドに関連付けられます。これは、
!   ダイヤル アウトをトリガーし、PPP を確立した後にインターフェイス をオンラインにする「対象のトラフィッ
!   ク」を定義します。通常、このインターフェイスはスタンバイ状態のままになることに注意してください。
!   このため、対象のトラフィックではダイヤル アウトはトリガーされません。トラフィックはすでに
!   プライマリ（ATM DSL）インターフェイスを介してフローしています。
!
!   NAT のインターフェイスを外部で定義します。
!
!
interface Vlan104
 description used as default gateway address for DHCP clients
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
!
!   NAT（内部インターフェイス）を使用して、ファスト イーサネット ポート 0/1/0 から 0/1/3 に
!   接続されたホストに VLAN 104 を定義します。
!   NAT/PAT は、トンネルを介してピア ゲートウェイの 20.20.0.0 ネットワークに送信されるように
```

```
!   意図されていないトラフィックに使用されます。
!
interface Dialer2
 ip address negotiated
 ip nat outside
 encapsulation ppp
 load-interval 30
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap hostname cisco@cisco.com
 ppp chap password 0 cisco123
 ppp pap sent-username cisco@cisco.com password 0 cisco123
 ppp ipcp dns request
crypto map mytunnelcrypto
!
!   "dialer pool 2 コマンドは、このダイヤラ インターフェイスを ATM サブ インターフェイス
!   atm0/0/0.1 に関連付けます。'dialer-group 2' は group number 2 を定義します。この設定では、
!   これは以下で指定されている 'dialer-list 2 ...' コマンドに関連付けられます。これは、PPP を確立した
!   後に、ダイヤル アウトをトリガーし、インターフェイスをオンラインにする
!   「対象のトラフィック」を定義します。
!
!   NAT のインターフェイスを外部で定義します。
!
!   上記で定義したクリプト マップ mytunnelcrypto をこのプライマリ インターフェイスに適用します。
!
ip local policy route-map track-primary-if
!
!   ルート マップの track-primary-if で定義されているように、
!   IP ルート ポリシーを指定します。
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
!
!   上記で定義したトラッキング オブジェクト（234）を指定し、ダイヤラ 2（ATM DSL）
!   を介してデフォルト ルートを定義します。
!
!   ルートはトラッキング対象オブジェクト（234）が 'UP' である場合のみインストールされます。
!
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
!   管理距離を 254（ダイヤラ 2 のインターフェイスより高い）に設定して、
!   セルラー インターフェイスを介してデフォルト ルートを定義します。通常このインターフェイスは
!   バックアップ インターフェイスとして想定されているからです。
!
ip route 10.10.0.0 255.255.0.0 Tunnel1
!
!   リモート 10.10.0.0 VPN ネットワークへのルートは、ATM DSL（プライマリ）インターフェイスに
!   関連付けられた GRE トンネルを経由します。
!
ip route 10.10.0.0 255.255.0.0 Tunnel2 254
!
!   リモート 10.10.0.0 VPN ネットワークへのルートは、セルラー（セカンダリ）インターフェイスに
!   関連付けられた GRE トンネルを経由します。管理距離は 254（Tunnel1 のものよりも高い）に
!   設定されています。
!
ip nat inside source route-map nat2cell interface Cellular0/3/0 overload
!
!   セルラー インターフェイスを介して、外部 NAT トラフィックの条件としてルート マップ nat2cell を定義し
!   ます（以下で指定）。'overload' オプションを使用すると、PAT が使用されるようになります。
!
!   ルート マップ nat2cell で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
```

```
!   上記と同様に、ダイヤラ 2 インターフェイス（ATM DSL）を使用して、外部 NAT トラフィックに対して
!   route-map nat2cell を（以下で定義されているように）定義します。'overload' オプションを使用すると、
!   PAT が使用されるようになります。
!
!   ルート マップ nat2dsl で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip access-list extended gre-traffic
 permit gre host 75.40.113.246 host 20.20.241.234
 permit gre host 166.138.186.119 host 20.20.241.234
!
!   GRE トンネルを経由して IPSec トラフィックを保護するための gre-traffic アクセス リスト。
!
!   これは DSL/ セルラー インターフェイス（どちらかアクティブな方）と、
!   リモート ゲートウェイ上の IPsec ピア（20.20.241.234）を介した GRE トンネリング
!   されたトラフィックのみを保護します。
!
ip sla 1
 icmp-echo 209.131.36.158 source-interface Dialer2
 timeout 1000
 frequency 2
!
ip sla schedule 1 life forever start-time now
!
!   2 秒間隔（frequency 2）で、ping への応答に 1000 ミリ秒の待機（タイムアウト 1000）を設定し、
!   ソース インターフェイスとしてダイヤラ 2（ATM DSL）を使用して、
!   IP アドレス 209.131.36.158 に ping を送信するための
!   サービス レベル契約（SLA）を定義します。
!
!   定義された SLA を開始し、これを継続的に実行します。
!
access-list 1 permit any
!
!   以下の 'dialer-list 1 protocol ip list 1' コマンドに関連付けられています
!
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
!
!   ルート マップ nat2dsl と nat2cell の下に定義されているように、
!   適切な発信インターフェイスを決定するために、トラフィックが一致するように
!   指定します（ネットワーク 10.4.0.0 のソース アドレスと一致）。
!
access-list 102 permit icmp any host 209.131.36.158
!
!   このインターフェイスがアクティブな場合にのみ、ATM DSL インターフェイスを介して
!   送信されるように、ルート マップ 'track-primary-interface' のトラフィックを指定します。
!
!   この特定のアドレスは、ATM DSL インターフェイス（プライマリ リンク）を介して定期的に ping される
!   アドレスであるため、リンク /PPP レベル以外のネットワーク障害も検出される場合があり、
!   セルラー（セカンダリ）インターフェイスへのスイッチオーバーがまだ実行される
!   可能性があります。
!
!   ping されるアドレスが信頼でき、ping に応答することを確認します。
!
dialer-list 1 protocol ip list 1
!
!   セルラー インターフェイスがダイヤル アウトする原因となる 'interesting traffic' を指定します。
!   それによって、access-list 1 が（上記で定義されたこのコマンドの一部として）さらに指定されます。
!
dialer-list 2 protocol ip permit
!
!   ATM DSL インターフェイスが（ダイヤラ 2 インターフェイスの一部として）ダイヤル アウトするようにする
!   'interesting traffic' を指定します。
!
!
route-map track-primary-if permit 10
```

```
 match ip address 102
 set interface Dialer2 null0
!
!   ローカル ルーティング用にポリシー条件として使用されるルート マップを指定します
!   (上記の関連するコマンド 'ip local policy route-map track-primary-if'
!   を参照してください)。
!
!   これが宛先 209.131.36.158 の ping パケットで、インターフェイス ダイヤラ
!   2（ATM DSL）が 'UP' の状態で接続されている場合、ping パケットを送信します。この ping パケットは、
!   ATM DSL インターフェイスを介してのみ送信され、セルラー インターフェイスを介しては送信されません。
!   これは、接続が失敗したときにスイッチオーバーを実行するために、ATM DSL インターフェイスを介して
!   接続（到達可能性）を定期的にモニタリングするためです。
!
route-map nat2dsl permit 10
 match ip address 101
 match interface Dialer2
!
!   上記のアクセス リスト 101 によって定義されている一致条件を満たし、
!   ダイヤラ 2 インターフェイスが 'UP' の状態で接続されている場合、
!   このルート マップが使用されるように指定します。
!
!   トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
!   インターフェイスのダイヤラ 2 が 'UP' の状態で DSL ネットワークに接続されている場合、
!   このルート マップが 'ip nat inside source nat2dsl ...' コマンドによって使用されます。
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0/3/0
!
!   上記のアクセス リスト 101 によって定義されている一致条件を満たし、
!   ダイヤラ 2 インターフェイスが 'UP' の状態で接続されている場合、
!   このルート マップが使用されるように指定します。
!
!   トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
!   インターフェイス セルラーが 'UP' の状態でセルラー ネットワークに接続されている場合、このルート マップ
!   が 'ip nat inside source nat2cell ...' コマンドによって使用されます。
!
!   スイッチオーバーで、プライマリおよびバックアップ インターフェイスから NAT エントリを削除します。
event manager applet pri_back
 event track 234 state any
 action 2.0 cli command "clear ip nat trans forced"
!
control-plane
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
 stopbits 1
line aux 0
 stopbits 1
line 0/3/0
 exec-timeout 0 0
 script dialer gsmscript
 login
 modem InOut
 no exec
 transport input all
 transport output all
 rxspeed 236800
 txspeed 118000
line vty 0 4
 privilege level 15
 login local
 transport input telnet
```

```
line vty 5 15
 privilege level 15
 login local

transport input telnet
!
scheduler allocate 20000 1000
!
End
```

本社サイトのルータの設定

例 5-4　　本社サイトのルータの設定

この設定内で青色の斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
!
hostname gateway-router
!
ip cef
!
ip dhcp excluded-address 20.20.248.254
ip dhcp excluded-address 20.20.248.253
ip dhcp excluded-address 20.20.248.225
ip dhcp excluded-address 10.10.0.254
ip dhcp excluded-address 10.10.0.1
!
!   DHCP の除外アドレス
!
ip dhcp pool 20
   network 20.20.248.224 255.255.255.224
   dns-server 20.20.248.254
   default-router 20.20.248.254
!
!   20.20 ネットワーク上のホストの DHCP プール
!
ip dhcp pool 10
   network 10.10.0.0 255.255.0.0
   default-router 10.10.0.254
!
!   10.10.0.0 ネットワーク上の VPN のホストの DHCP プール
!
!
username cisco privilege 15 secret 5 $1$QF4K$Z1rE.mwS69FVx1e5l9DCU1
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share

crypto isakmp key mykey address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set mytset ah-sha-hmac esp-3des
!
crypto dynamic-map gre_tunnel2 10
```

```
 description IPsec tunnel to DSL at remote
 set transform-set mytset
 match address gre-tunnel2
!
crypto dynamic-map gre_tunnel21 10
 description IPsec tunnel to Cellular at remote
 set transform-set mytset
 match address gre-tunnel21
!
crypto map mytunnelcrypto 10 ipsec-isakmp dynamic gre_tunnel2

crypto map mytunnelcrypto 20 ipsec-isakmp dynamic gre_tunnel21
!
!
!   リモート ブランチ ルータで、トンネルの mytunnelcrypto マップを ATM DSL インターフェイス
!   (Tunnel2) およびセルラー インターフェイス (Tunnel21) に定義します。
!
!
interface Tunnel2
 description tunnel to remote DSL link 75.40.113.246
 ip unnumbered Vlan20
 tunnel source GigabitEthernet0/0
 tunnel destination 75.40.113.246
!
!   リモート ブランチ ルータの ATM DSL インターフェイスへのトンネル。通常、これは
!   「アクティブなトンネル」です。
!
interface Tunnel21
 description tunnel to remote Cellular link 166.138.186.119
 ip unnumbered Vlan20
 tunnel source GigabitEthernet0/0
 tunnel destination 166.138.186.119
!
!   リモート ブランチ ルータのセルラー インターフェイスへのトンネル。リモート エンドでの DSL インター
!   フェイスを介した接続がダウンしない限り、通常、このトンネルはアクティブではありません。
!
interface GigabitEthernet0/0
 description connected to cisco network, next hop:20.20.241.233
 ip address 20.20.241.234 255.255.255.252
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
 crypto map mytunnelcrypto
!
!   クリプト マップを適用する物理インターフェイス。上記のトンネルが
!   確立されるインターフェイス
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
!
!   VPN のホストが (10.10.0.0 ネットワークで) 接続されるファスト イーサネット ポート。
!
interface FastEthernet0/1/8
 switchport stacking-partner interface FastEthernet0/3/8
!
interface FastEthernet0/3/0
```

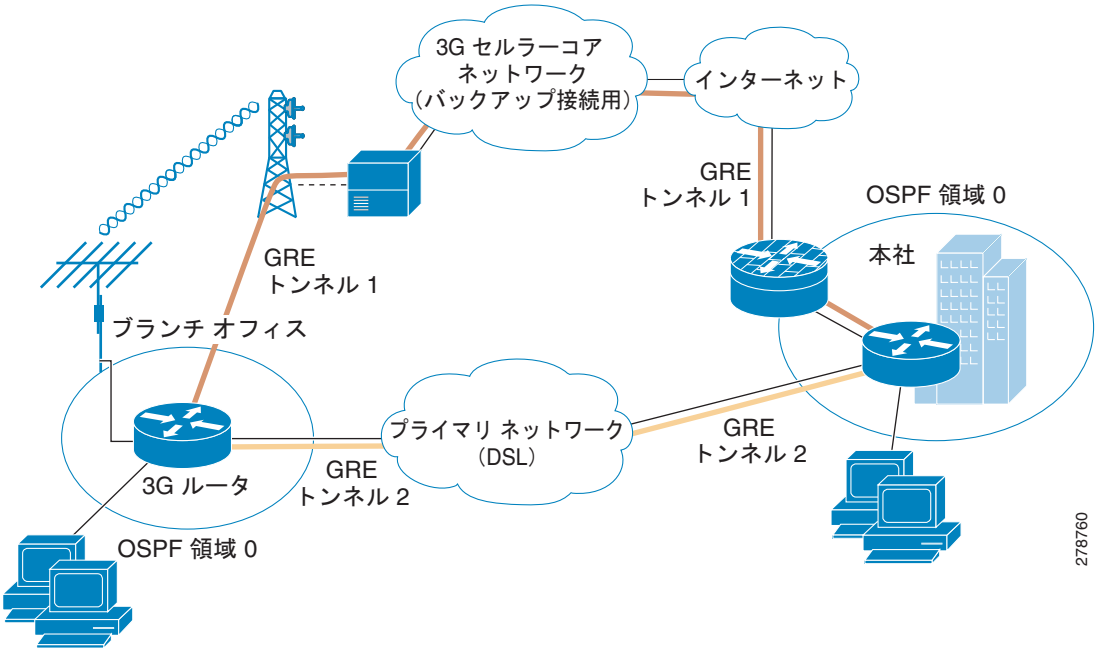
```
 switchport access vlan 20
 spanning-tree portfast
!
!
!   他のホストが（20.20 ネットワークで）接続されるファスト イーサネット ポート。
!
interface FastEthernet0/3/8
 switchport mode trunk
 switchport stacking-partner interface FastEthernet0/1/8
!
interface Vlan10
 description private networking vlan
 ip address 10.10.0.254 255.255.0.0
 vlan-range dot1q 1 4095
 exit-vlan-config
 !
!
!   VPN のホストの VLAN（10.10.0.0 ネットワーク内）
!
interface Vlan20
 description network:20.20.248.224/27
 ip address 20.20.248.254 255.255.255.224
 no ip route-cahe cef
 vlan-range dot1q 1 4095
  exit-vlan-config
 !
!
!   他のホストの VLAN（20.20 ネットワーク内）
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
!   デフォルト ルート
!
ip route 10.4.0.0 255.255.0.0 Tunnel2
!
!   DSL インターフェイスにリモート エンドポイントを持つトンネルを経由する、
!ブランチ ルータ上のリモート VPN（10.4.0.0 ネットワーク）へのルート
!
ip route 10.4.0.0 255.255.0.0 Tunnel21 254
!
!   セルラー インターフェイスにリモート エンドポイントを持つトンネルを経由する、
!   ブランチ ルータ上のリモート VPN（10.4.0.0 ネットワーク）へのルート。このルートの管理距離は
!   高く設定されています。
!
ip access-list extended gre-tunnel2
 permit gre host 20.20.241.234 host 75.40.113.246
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドでセルラー インターフェイスに送信されるトラフィックです。
!
ip access-list extended gre-tunnel21
 permit gre host 20.20.241.234 host 166.138.186.119
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドでセルラー インターフェイスに送信されるトラフィックです。
!
control-plane
!
line con 0
 exec-timeout 0 0
 login local
 stopbits 1
line aux 0
 stopbits 1
```

```
line vty 0 4
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000
!
end
```

GRE トンネル、IPSec、および OSPF ルーティングを使用したプライマリおよびバックアップの導入

この導入では、パブリック ネットワークを介したブランチ オフィスのルータのホストと本社サイトのホストの間でセキュアな通信を行うために、GRE トンネルと IPsec をブランチ オフィスで使用して、プライマリ リンクとして DSL インターフェイスを使用し、バックアップ リンクとしてセルラー インターフェイスを使用します。また、VPN ネットワーク（10.4.0.0 および 10.10.0.0 ネットワーク）で OSPF を使用し、OSPF でサポートされたルーティングを行えるようにもします。この導入により、インターネット上のホストとのノンセキュア（非 IPsec）通信を行えるようになります。詳細については、「*Configuring a GRE Tunnel over IPsec with OSPF*」を参照してください。

図 5-3　GRE トンネル、IPSec、および OSPF ルーティングを使用したプライマリおよびバックアップの導入



ブランチ オフィス ルータの設定

この設定内で青色の斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

次の設定では、信頼できるオブジェクト トラッキングを使用した IP SLA が使用されます。この設定は任意です。

例 5-5　　ブランチ オフィス ルータの設定

```
!
hostname branch-router
!
ip cef
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.4.0.254
!
!   このアドレスは、VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 上の
!   接続済みホスト用デフォルト ゲートウェイ アドレスとして使用されます。
!
ip dhcp pool gsmpool
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.4.0.254
!
!   VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 に接続されている
!   ホストの DHCP プール
!
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
!
!   セルラー インターフェイスを介したダイヤル アウトへのチャット スクリプト
!
!
username cisco privilege 15 secret 5 $1$ccw8$TFmKUmI4QVZhOMuxzq/SH/
!
track 234 rtr 1 reachability
!
!   operation 1 を使用して、到達可能性のトラッキングに使用されるトラッキング対象のオブジェクト番号 234
!   を設定します。オブジェクトは、到達可能性条件が満たされる場合は 'UP' です。
!
!   これは、（プライマリ リンクとして使用される）ATM DSL インターフェイスを介して ping パケットを送信し、
!   応答を監視するために使用されます。また、応答がない場合に（セルラーへの）スイッチオーバーが
!   必要かどうかを判別するために使用されます。
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
!
!   (priority 1 を設定して）IKE ポリシーを定義し、IKE ネゴシエーション中に 3DES を指定します。また、
!   事前定義されたキーを使用して事前共有認証を指定します。ライフタイムの値（1 日に 86,400 秒に設定）、
!   グループ（768 ビット ディフィー・ヘルマン鍵共有に設定）、
!   およびハッシュ（SHA-1 に設定）は、デフォルト値に設定されます。
!
```

```
crypto isakmp key mykey address 20.20.241.234
!
!   セキュリティ アソシエーションの設定に使用されるキー（mykey）およびゲートウェイの
!   IP アドレス（IPsec peer）を定義します。
!
!
crypto ipsec transform-set mytransformset ah-sha-hmac esp-3des
!
!   セキュリティ プロトコル、アルゴリズム、および他の設定の許容可能な組み合わせである
!   トランスフォーム セット（mytransformset）を定義して、IPsec で保護されている
!   トラフィックを適用します。
!
crypto map mytunnelcrypto 10 ipsec-isakmp
 set peer 20.20.241.234
 set transform-set mytransformset
 match address gre-traffic
!
!   クリプト マップの mytunnelcrypto を定義します
!
!   クリプト マップは（match address <access-list> コマンドを使用して）保護対象のトラフィック、
!   使用するピア エンド ポイント、および使用するトランスフォーム セット（以前に定義した
!   mytransformset）を指定します。
!
!
interface Tunnel1
ip unnumbered Vlan104
 ip mtu 1400
 tunnel source Dialer2
 tunnel destination 20.20.241.234
!
!   宛先 10.10.0.0 のネットワークへのトラフィックの GRE トンネル。ATM DSL（プライマリ）
!   インターフェイスに関連付けられたトンネル。このトンネルは、通常 'UP' の状態です。リモート トンネルの
!   エンドポイント（20.20.241.234）は、リモート VPN ゲートウェイにあります。ローカル トンネルのエンド
!   ポイントは、ATM DSL リンクによって取得されるアドレスです。
!
interface Tunnel2
 ip ospf demand-circuit
 ip unnumbered Vlan104
 ip mtu 1400
 tunnel source Cellular0/3/0
 tunnel destination 20.20.241.234
!
!   'ip ospf demand-circuit' オプション コマンドは、OSPF Hello パケットを抑止します。これは、
!   定期的に、セルラー無線レベルの接続が不必要に（「休止」状態から）「アクティブ」状態
!   にならないように保つのに役立ちます。
!
!   宛先 10.10.0.0 のネットワークへのトラフィックの GRE トンネル。セルラー（セカンダリ）インターフェイス
!   に関連付けられたトンネル。このトンネルは、通常 'Down' の状態です。リモート トンネルの
!   エンドポイント（20.20.241.234）は、リモート VPN ゲートウェイにあります。ローカル トンネルのエンド
!   ポイントは、セルラー リンクによって取得されるアドレスです。このトンネルは、
!   セルラー インターフェイスでスイッチオーバーが行われると 'UP' になります。
!
interface Loopback1
ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
```

```
 switchport access vlan 104
!
interface FastEthernet0/1/1
 switchport access vlan 104
!
interface FastEthernet0/1/2
 switchport access vlan 104
!
interface FastEthernet0/1/3
 switchport access vlan 104
!
!   DHCP クライアント ホストによって使用されるファスト イーサネット ポート
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
!   プライマリ インターフェイスとして使用される ATM（DSL）物理インターフェイス
!
interface ATM0/0/0.1 point-to-point
 ip nat outside
 ip virtual-reassembly
 no snmp trap link-status
 pvc 0/35
 pppoe-client dial-pool-number 2
!
!
!   プライマリ接続として PVC に使用する ATM サブ インターフェイス。このインターフェイスでは
!   NAT（外部）が使用されます。
!
!   'pppoe-client dial-pool-number 2' は PPP over Ethernet（PPOE）クライアントを設定し、
!   使用するダイヤラ プール 2 を指定します。このインターフェイスは、以下で定義されている 'interface
!   Dialer 2' に関連付けられます。
!
interface Cellular0/3/0
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 ip ospf demand-circuit
 dialer in-band
 dialer idle-timeout 0
 dialer string gsmscript
 dialer-group 1
 async mode interactive
 ppp chap hostname crlaswlech@wwan.ccs
 ppp chap password 0 frludi3gIa
 ppp ipcp dns request
 crypto map mytunnelcrypto
!
!   'ip ospf demand-circuit' オプション コマンドは、OSPF Hello パケットを抑止します。これは、定期的
!   に、セルラー無線レベルの接続が不必要に（「休止」状態から）「アクティブ」状態に
!   ならないように保つのに役立ちます。
!
!   上記で定義したクリプト マップ mytunnelcrypto を、このバックアップ インターフェイスに適用します。
!
!   'dialer-group 1' は group number 1 を定義します。
!   この設定では、これは以下に定義されている 'dialer-list 1 ...' コマンドに関連付けられます。これは、
!   ダイヤル アウトをトリガーし、PPP を確立した後にインターフェイス をオンラインにする
!   「対象のトラフィック」を定義します。通常、このインターフェイスはスタンバイ状態のままになることに注意して
!   ください。このため、対象のトラフィックではダイヤル アウトはトリガーされません。トラフィックはすでに
```

```
!   プライマリ（ATM DSL）インターフェイスを介してフローしています。
!
!   NAT のインターフェイスを外部で定義します。
!
!
interface Vlan104
 description used as default gateway address for DHCP clients
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
!
!   NAT（内部インターフェイス）を使用して、ファスト イーサネット ポート 0/1/0 から 0/1/3 に
!   接続されたホストに VLAN 104 を定義します。
!
!   NAT/PAT は、トンネルを介してピア ゲートウェイの 20.20.0.0 ネットワークに送信されるように
!   意図されていないトラフィックに使用されます。
!
interface Dialer2
 ip address negotiated
 ip nat outside
 encapsulation ppp
 load-interval 30
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap hostname cisco@cisco.com
 ppp chap password 0 cisco123
 ppp pap sent-username cisco@cisco.com password 0 cisco123
 ppp ipcp dns request
 crypto map mytunnelcrypto
!
!   'dialer pool 2' コマンドはこのダイヤラ インターフェイスを ATM サブインターフェイス
!   atm0/0/0.1 に関連付けます。'dialer-group 2' は group number 2 を定義します。この設定では、
!   これは以下で指定されている 'dialer-list 2 ...' コマンドに関連付けられます。これは、
!   PPP を確立した後に、ダイヤル アウトをトリガーし、インターフェイスをオンラインにする
!   「対象のトラフィック」を定義します。
!
!   NAT のインターフェイスを外部で定義します。
!
!   上記で定義したクリプト マップ mytunnelcrypto をこのプライマリ インターフェイスに適用します。
!
router ospf 11
 log-adjacency-changes
 network 10.4.0.0 0.0.0.255 area 0
!
!   VPN ネットワーク 10.4.0.0（Tunnel1/Tunnel2 が含まれます）は、OSPF エリア 0 に含まれています
!
!   OSP Hello は、これらのトンネルを介してブランチ ルータに送信されます
!
ip local policy route-map track-primary-if
!
!   ルート マップの 'track-primary-if' で定義されているように、IP ルート ポリシーを指定します
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
!
!   上記で定義したトラッキング オブジェクト（234）を指定し、ダイヤラ 2（ATM DSL）
!   を介してデフォルト ルートを定義します。
!
!   ルートはトラッキング対象オブジェクト（234）が 'UP' である場合のみインストールされます。
!
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
!   管理距離を 254（ダイヤラ 2 のインターフェイスより高い）に設定して、
!   セルラー インターフェイスを介してデフォルト ルートを定義します。通常このインターフェイスは
```

```
!   バックアップ インターフェイスとして想定されているからです。
!
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 5 life 86400 requests 10000

ip nat inside source route-map nat2cell interface Cellular0/3/0 overload
!
!   セルラー インターフェイスを介して、外部 NAT トラフィックの条件としてルート マップ nat2cell を定義し
!   ます（以下で指定）。'overload' オプションを使用すると、PAT が使用されるようになります。
!
!   ルート マップ nat2cell で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
!   上記と同様に、ダイヤラ 2 インターフェイス（ATM DSL）を使用して、
!   ルート マップ nat2cell を定義します（以下で指定）。'overload' オプションを使用すると、
!   PAT が使用されるようになります。
!
!   ルート マップ nat2dsl で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip access-list extended gre-traffic
 permit gre host 75.40.113.246 host 20.20.241.234
 permit gre host 166.138.186.119 host 20.20.241.234
!
!   GRE トンネルを経由して IPSec トラフィックを保護するための 'gre-traffic' アクセス リスト
!
!   これは DSL/ セルラー インターフェイス（どちらかアクティブな方）と、リモート ゲートウェイ上の
!   IPsec ピア（20.20.241.234）を介した GRE トンネリングされた
!   トラフィックのみを保護します。
!
ip sla 1
 icmp-echo 209.131.36.158 source-interface Dialer2
 timeout 1000
 frequency 2

ip sla schedule 1 life forever start-time now
!
!   2 秒間隔（frequency 2）で、ping への応答に 1000 ミリ秒の待機（タイムアウト 1000）を設定し、
!   ソース インターフェイスとしてダイヤラ 2（ATM DSL）を使用して、
!   IP アドレス 209.131.36.158 に ping を送信するための
!   サービス レベル契約（SLA）を定義します。
!
!   定義された SLA を開始し、これを継続的に実行します。
!
access-list 1 permit any
!
!   以下の 'dialer-list 1 protocol ip list 1' コマンドに関連付けられています
!
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
!
!   ルート マップ nat2dsl と nat2cell の下に定義されているように、適切な発信インターフェイスを
!   決定するために、トラフィックが一致するように指定します
!   （ネットワーク 10.4.0.0 のソース アドレスと一致）。
!
access-list 102 permit icmp any host 209.131.36.158
!
!   このインターフェイスがアクティブな場合にのみ、ICMP の ping が ATM DSL インターフェイスを介して
!   送信されるように、ルート マップ 'track-primary-interface' のトラフィックを指定します。
!
!   この特定のアドレスは、ATM DSL インターフェイス（プライマリ リンク）を介して定期的に ping される
!   アドレスであるため、リンク /PPP レベル以外のネットワーク障害も検出される場合があり、
!   セルラー（セカンダリ）インターフェイスへのスイッチオーバーが
```

```
!   まだ実行される可能性があります。
!
!   ping されるアドレスが信頼でき、ping に応答することを確認します。
!
dialer-list 1 protocol ip list 1
!
!   セルラー インターフェイスがダイヤル アウトする原因となる 'interesting traffic' を指定します。
!   それによって、access-list 1 が（上記で定義されたこのコマンドの一部として）さらに指定されます。
!
dialer-list 2 protocol ip permit
!
!   ATM DSL インターフェイスが（ダイヤラ 2 インターフェイスの一部として）
!   ダイヤル アウトするようにする 'interesting traffic' を指定します。
!
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2 null0
!
!   ローカル ルーティング用にポリシー条件として使用されるルート マップを指定します
!   （上記の関連するコマンド 'ip local policy route-map track-primary-if'
!   を参照してください）。
!
!   これが宛先 209.131.36.158 の ping パケットで、インターフェイス ダイヤラ
!   2（ATM DSL）が 'UP' の状態で接続されている場合、ping パケットを送信します。この ping パケットは、
!   ATM DSL インターフェイスを介してのみ送信され、セルラー インターフェイスを介しては送信されません。
!   これは、接続が失敗したときにスイッチオーバーを実行するために、ATM DSL インターフェイスを介して
!   接続（到達可能性）を定期的にモニタリングするためです。
!
route-map nat2dsl permit 10
 match ip address 101
 match interface Dialer2
!
!   上記のアクセス リスト 101 によって定義されている一致条件を満たし、
!   ダイヤラ 2 インターフェイスが 'UP' の状態で接続されている場合、
!   このルート マップが使用されるように指定します。
!
!   トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
!   インターフェイスのダイヤラ 2 が 'UP' の状態で DSL ネットワークに接続されている場合、
!   このルート マップが 'ip nat inside source nat2dsl ...' コマンドによって使用されます。
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0/3/0
!
!   上記のアクセス リスト 101 によって定義されている一致条件を満たし、
!   ダイヤラ 2 インターフェイスが 'UP' の状態で接続されている場合、
!   このルート マップが使用されるように指定します。
!
!   トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
!   インターフェイス セルラーが 'UP' の状態でセルラー ネットワークに接続されている場合、このルート マップ
!   が 'ip nat inside source nat2cell ...' コマンドによって使用されます。
!
!   スイッチオーバーで、プライマリおよびバックアップ インターフェイスから NAT エントリを削除します。
event manager applet pri_back
 event track 234 state any
 action 2.0 cli command "clear ip nat trans forced"
!
control-plane
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
 stopbits 1
```

```
line aux 0
 stopbits 1
line 0/3/0
 exec-timeout 0 0
 script dialer gsmscript
 login
 modem InOut
 no exec
 transport input all
 transport output all
 rxspeed 236800
 txspeed 118000
line vty 0 4
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000
!
End
```

本社サイトのルータの設定

例 5-6　　本社サイトのルータの設定

この設定内で青色の斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
!
hostname gateway-router
!
ip cef
!
ip dhcp excluded-address 20.20.248.254
ip dhcp excluded-address 10.10.0.254
ip dhcp excluded-address 10.10.0.1
!
!   DHCP の除外アドレス
!
ip dhcp pool 20
   network 20.20.248.224 255.255.255.224
   dns-server 20.20.248.254
   default-router 20.20.248.254
!
!   20.20 ネットワーク上のホストの DHCP プール
!
ip dhcp pool 10
   network 10.10.0.0 255.255.0.0
   default-router 10.10.0.254
!
!   10.10.0.0 ネットワーク上の VPN のホストの DHCP プール
```

```
!
!
username cisco privilege 15 secret 5 $1$QF4K$Z1rE.mwS69FVx1e5l9DCU1
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share

crypto isakmp key mykey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set mytset ah-sha-hmac esp-3des
!
crypto dynamic-map gre_tunnel2 10
 description IPsec tunnel to DSL at remote
 set transform-set mytset
 match address gre-tunnel2
!
crypto dynamic-map gre_tunnel21 10
 description IPsec tunnel to Cellular at remote
 set transform-set mytset
 match address gre-tunnel21
!
crypto map mytunnelcrypto 10 ipsec-isakmp dynamic gre_tunnel2

crypto map mytunnelcrypto 20 ipsec-isakmp dynamic gre_tunnel21
!
!   リモート ブランチ ルータで、トンネルの mytunnelcrypto マップを ATM DSL インターフェイス
!   (Tunnel2) およびセルラー インターフェイス (Tunnel21) に定義します。
!
!
interface Tunnel2
 description tunnel to remote DSL link 75.40.113.246
 ip unnumbered Vlan10
 ip mtu 1400
 tunnel source GigabitEthernet0/0
 tunnel destination 75.40.113.246
!
!   リモート ブランチ ルータの ATM DSL インターフェイスへのトンネル。通常、これは
!   「アクティブなトンネル」です。
!
interface Tunnel21
 description tunnel to remote Cellular link 166.138.186.119
 ip unnumbered Vlan10
 ip mtu 1400
 tunnel source GigabitEthernet0/0
 tunnel destination 166.138.186.119
!
!   リモート ブランチ ルータのセルラー インターフェイスへのトンネル。リモート エンドでの DSL インター
!   フェイスを介した接続がダウンしない限り、通常、このトンネルはアクティブではありません。
!
interface GigabitEthernet0/0
 description connected to cisco network, next hop:20.20.241.233
 ip address 20.20.241.234 255.255.255.252
 load-interval 30
 crypto map mytunnelcrypto
!
!   クリプト マップを適用する物理インターフェイス。上記のトンネルが
!   確立されるインターフェイス。
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
```

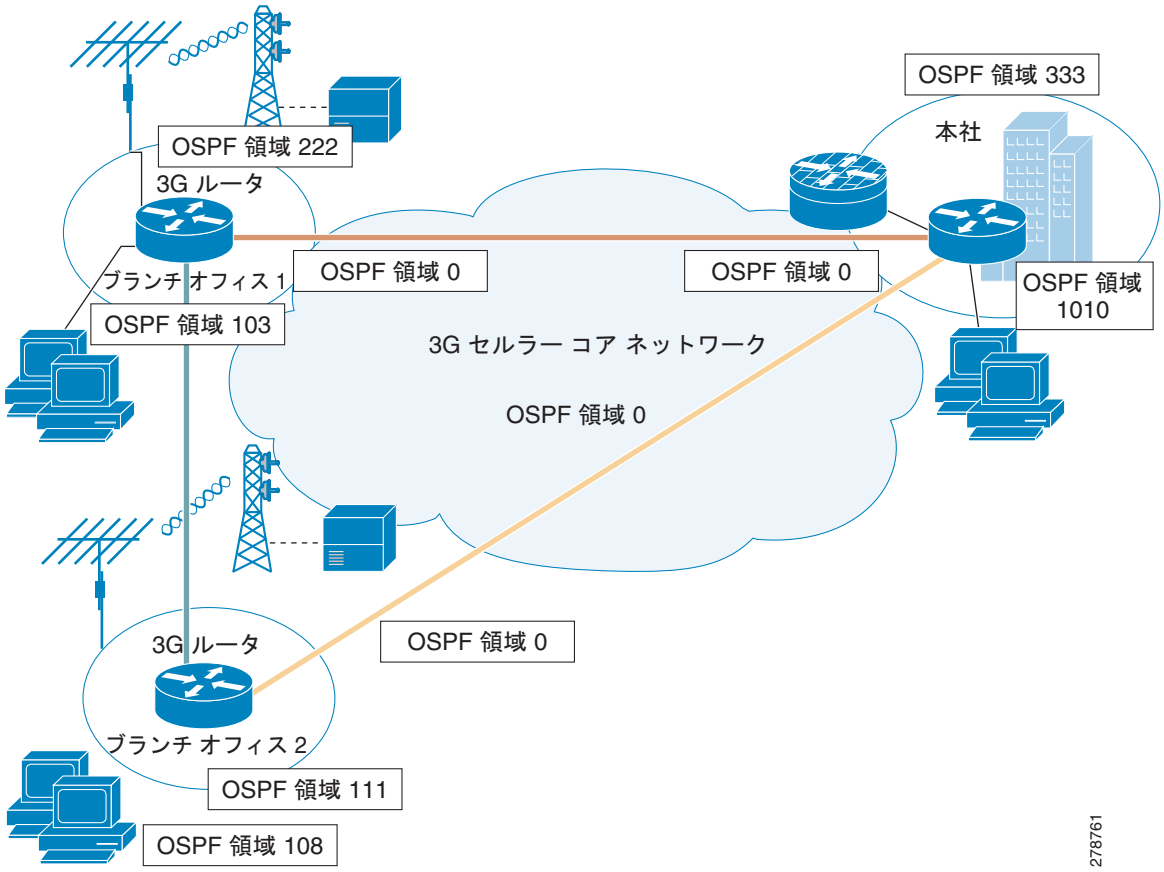
```
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
!   VPN のホストが（10.10.0.0 ネットワークで）接続されるファスト イーサネット ポート。
!
interface FastEthernet0/1/8
 switchport stacking-partner interface FastEthernet0/3/8
!
interface FastEthernet0/3/0
 switchport access vlan 20
 spanning-tree portfast
!
!   他のホストが（20.20 ネットワークで）接続されるファスト イーサネット ポート。
!
interface FastEthernet0/3/8
 switchport mode trunk
 switchport stacking-partner interface FastEthernet0/1/8
!
interface Vlan10
 description private networking vlan
 ip address 10.10.0.254 255.255.0.0
 no ip route-cache cef
 vlan-range dot1q 1 4095
 exit-vlan-config
 !
!
!   VPN のホストの VLAN（10.10.0.0 ネットワーク内）。
!
interface Vlan20
 description network:20.20.248.224/27
 ip address 20.20.248.254 255.255.255.224
 no ip route-cahe cef
 vlan-range dot1q 1 4095
 exit-vlan-config
 !
!
!   他のホストの VLAN（20.20 ネットワーク内）
!
router ospf 10
 log-adjacency-changes
 network 10.10.0.0 0.0.0.255 area 0
!
!   VPN ネットワーク 10.10.0.0（Tunnel2/Tunnel21 が含まれています）は、OSPF エリア 0 に含まれています
!
!   OSP Hello は、これらのトンネルを介してブランチ ルータに送信されます
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
!   GigabitEthernet0/0 インターフェイスのネクスト ホップを介するデフォルト ルート。
!
ip dns server
!
ip access-list extended gre-tunnel2
 permit gre host 20.20.241.234 host 75.40.113.246
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドで DSL インターフェイスに送信されるトラフィックです。
!
ip access-list extended gre-tunnel21
 permit gre host 20.20.241.234 host 166.138.186.119
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドでセルラー インターフェイスに送信されるトラフィックです。
```

```
!
control-plane
!
line con 0
 exec-timeout 0 0
 login local
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000
!
End
```

IPSec および OSPF を使用した DMVPN の導入

この導入では、ルーティング プロトコルの OSPF とパブリック ネットワークを使用して、ブランチ オフィスのルータのホストと、本社サイトのホストの間でセキュアな通信を行うために、DMVPN（GRE トンネル）と IPsec を使用し、プライマリ リンクとしてセルラー インターフェイスを使用します。DMVPN の詳細については、「*Dynamic Multipoint VPN (DMVPN)*」を参照してください。

図 5-4　IPSec および OSPF 使用する DMVPN を使用した初期導入



ブランチ 1 のオフィス ルータの設定

例 5-7　　ブランチ 1 のオフィス ルータの設定

この設定内で青色の斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
!
hostname DMVPN_Spoke_1
!
Ip cef
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
!
!
!   フェーズ 1 ネゴシエーションの ISAKMP ポリシー
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!   ハブの事前共有キー、およびリモート DMVPN スポーク
!
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
!   実際のデータ暗号化 / 整合性のための IPsec（フェーズ 2）ポリシー
!
!
crypto ipsec profile cisco
 set security-association lifetime seconds 86400
 set transform-set strong
!
!   IPsec を介した GRE トンネルに動的に適用される IPsec プロファイル
!
!
ip dhcp excluded-address 10.3.0.254
!
ip dhcp pool cdmapool
   network 10.3.0.0 255.255.0.0
   dns-server 68.28.58.11
   default-router 10.3.0.254
!
chat-script cdma1 "" "atdt#777" TIMEOUT 180 "CONNECT"
!
username cisco privilege 15 secret 5 $1$c/5O$W4sr3BFW3AhIB9BRXjy84/
!
interface Loopback0
 ip address 2.2.2.1 255.255.255.0
!
interface Tunnel0
 ip address 192.168.10.3 255.255.255.0
 no ip redirects
 ip mtu 1440
 ip nhrp map multicast dynamic
 ip nhrp map multicast 20.20.241.234
```

```
 ip nhrp map 192.168.10.1 20.20.241.234
 ip nhrp network-id 1
 ip nhrp nhs 192.168.10.1
 ip nhrp registration no-unique
 ip nhrp cache non-authoritative
 ip ospf network broadcast
 tunnel source dialer 1
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile Cisco
!
!    動的に作成されたすべての GRE トンネルに割り当てられた GRE トンネル テンプレート。
!
!
interface GigabitEthernet0/0
 no ip address
 shut down
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/2/0
 switchport access vlan 103
!
interface FastEthernet0/2/1
 switchport access vlan 103
!
interface FastEthernet0/2/2
 switchport access vlan 103
!
interface FastEthernet0/2/3
 switchport access vlan 103
!
!
!    次のセルラー設定は永続的ダイヤラ用です。これは、常にセルラー インターフェイスを
!    起動状態に保ち、IP アドレスを取得します。ダイヤラ プールおよび dialer pool-member コマンドは、
!    ダイヤラ インターフェイスとセルラー インターフェイスを関連付けます。
!

!
interface Cellular0/1/0
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
!
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer string cdma1
 dialer persistent
 ppp chap hostname isp-provided-hostname
 ppp chap password 0 isp-provided-password
 ppp ipcp dns request
!
interface Vlan1
 no ip address
!
interface Vlan103
 ip address 10.3.0.254 255.255.0.0
 ip nat inside
```

```
 ip virtual-reassembly
!
router ospf 90
 log-adjacency-changes
 network 2.2.2.0 0.0.0.255 area 222
 network 10.3.0.0 0.0.255.255 area 103
 network 192.168.10.0 0.0.0.255 area 0
!
ip route 20.20.241.234 255.255.255.255 dialer 1
!
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
line 0/1/0
 exec-timeout 0 0
 script dialer cdma1
 login
 modem InOut
 no exec
 transport input all
 transport output all
 rxspeed 3100000
 txspeed 1800000
line vty 0 4
 privilege level 15
 no login
 transport input telnet
line vty 5 15
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000

!
webvpn cef
!
end
```

ブランチ 2 のオフィス ルータの設定

例 5-8　　ブランチ 2 のオフィス ルータの設定

この設定内で青色の斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
!
hostname DMVPN_Spoke_2
!
!
crypto isakmp policy 10
```

```
 hash md5
 authentication pre-share
!
!   フェーズ 1 ネゴシエーションの ISAKMP ポリシー
!
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!   すべてのリモート DMVPN スポークの事前共有キー
!
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
!   実際のデータ暗号化 / 整合性のための IPsec（フェーズ 2）ポリシー
!
!
crypto ipsec profile cisco
 set security-association lifetime seconds 86400
 set transform-set strong
!
!   IPsec を介した GRE トンネルに動的に適用される IPsec プロファイル
!
!
ip cef
!
ip dhcp excluded-address 10.8.0.1
ip dhcp excluded-address 10.8.0.254
!
ip dhcp pool cdmapool
   network 10.8.0.0 255.255.0.0
   default-router 10.8.0.254
!
!
chat-script cdma2 "" "atdt#777" TIMEOUT 180 "CONNECT"
!
username cisco privilege 15 secret 5 $1$YNWp$1OLVYb0qkTnZFmkgcCK1L0
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.0
!
interface Tunnel0
 ip address 192.168.10.2 255.255.255.0
 no ip redirects
 ip mtu 1440
 ip nhrp map multicast dynamic
 ip nhrp map multicast 20.20.241.234
 ip nhrp map 192.168.10.1 20.20.241.234
 ip nhrp network-id 1
 ip nhrp nhs 192.168.10.1
 ip nhrp registration no-unique
 ip nhrp cache non-authoritative
 ip ospf network broadcast
 tunnel source dialer 1
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile Cisco
!
!   動的に作成されたすべての GRE トンネルに割り当てられた GRE トンネル テンプレート。
!
!
interface FastEthernet0/0
 no ip address
 shutdown
!
```

```
interface FastEthernet0/1
 ip address dhcp
 shutdown
!
interface FastEthernet0/3/0
 switchport access vlan 108
!
interface FastEthernet0/3/1
!
interface FastEthernet0/3/2
 switchport access vlan 108
!
interface FastEthernet0/3/3
 switchport access vlan 108
!
!
!   次のセルラー設定は永続的ダイヤラ用です。これは、常にセルラー インターフェイスを起動状態に保ち、
!   IP アドレスを取得します。ダイヤラ プールおよび dialer pool-member コマンドは、
!   ダイヤラ インターフェイスとセルラー インターフェイスを関連付けます。
!

!
interface Cellular0/1/0
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
!
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer string cdma2
 dialer persistent
 ppp chap hostname isp-provided-hostname
 ppp chap password 0 isp-provided-password
 ppp ipcp dns request
!
interface Vlan108
 description used as default gateway address for DHCP clients
 ip address 10.8.0.254 255.255.0.0
 ip virtual-reassembly
!
router ospf 90
 log-adjacency-changes
 network 1.1.1.0 0.0.0.255 area 111
 network 10.8.0.0 0.0.0.255 area 108
 network 192.168.10.0 0.0.0.255 area 0
!
ip route 20.20.241.234 255.255.255.255 dialer 1
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
line 0/1/0
 exec-timeout 0 0
 script dialer cdma2
 login
 modem InOut
 no exec
 transport input all
```

```
 transport output all
 autoselect during-login
 autoselect ppp
 rxspeed 3100000
 txspeed 1800000
line vty 0 4
 access-class 23 in
 privilege level 15
 login local
 transport input telnet ssh
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

本社サイトのルータの設定

例 5-9　　本社サイトのルータの設定

この設定内で青色の斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
!
hostname DMVPN_Hub
!
ip cef
!
ip dhcp pool 20
   network 20.20.248.224 255.255.255.224
   dns-server 20.20.248.254
   default-router 20.20.248.254
!
ip dhcp pool 10
   network 10.10.0.0 255.255.0.0
   default-router 10.10.0.254
!
ip dhcp pool 192
   network 192.168.1.0 255.255.255.0
   dns-server 192.168.1.254
   default-router 192.168.1.254
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
!
!   フェーズ 1 ネゴシエーションの ISAKMP ポリシー
!
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
```

```
!
!   すべてのリモート DMVPN スポークの事前共有キー
!
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
!   実際のデータ暗号化 / 整合性のための IPsec（フェーズ 2）ポリシー
!
!
crypto ipsec profile cisco
 set security-association lifetime seconds 86400
 set transform-set strong
!
!   IPsec を介した GRE トンネルに動的に適用される IPsec プロファイル
!
!
username cisco privilege 15 secret 5 $1$QF4K$Z1rE.mwS69FVx1e5l9DCU1
!
interface Loopback33
 ip address 3.3.3.3 255.255.255.0
!
interface Tunnel0
 ip address 192.168.10.1 255.255.255.0
 no ip redirects
 ip mtu 1440
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp cache non-authoritative
 ip ospf network broadcast
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile cisco
!
!
!   動的に作成されたすべての GRE トンネルに割り当てられた
!   GRE トンネル テンプレート
!
interface GigabitEthernet0/0
 description connected to cisco network, next hop:20.20.241.233
 ip address 20.20.241.234 255.255.255.252
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 10
 no cdp enable
 spanning-tree portfast
!
!
interface FastEthernet0/1/8
 switchport stacking-partner interface FastEthernet0/3/8
 no cdp enable
!
interface FastEthernet0/3/0
 switchport access vlan 20
 no cdp enable
 spanning-tree portfast
!
interface FastEthernet0/3/8
 switchport mode trunk
 switchport stacking-partner interface FastEthernet0/1/8
```

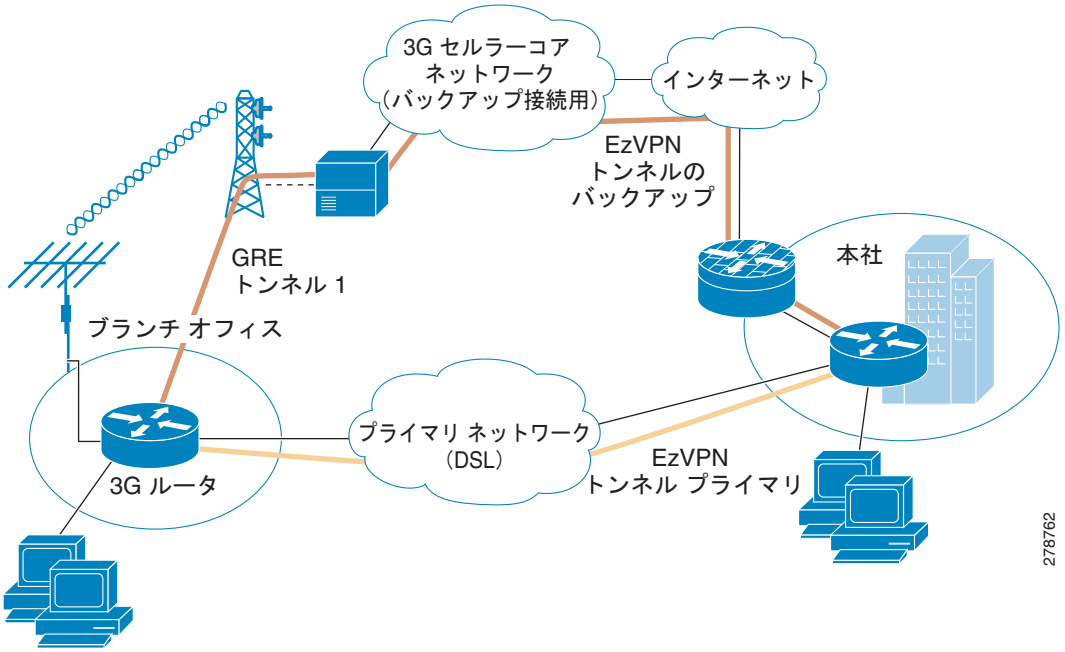
```
 no cdp enable
!
interface Vlan10
 description private networking vlan
 ip address 10.10.0.254 255.255.0.0
 no ip route-cache cef
!
interface Vlan20
 description network:20.20.248.224,mask:/27,last host:20.20.248.254
 ip address 20.20.248.254 255.255.255.224
 no ip route-cache cef
!
router ospf 90
 log-adjacency-changes
 network 3.3.3.0 0.0.0.255 area 333
 network 10.10.0.0 0.0.255.255 area 1010
 network 192.168.10.0 0.0.0.255 area 0
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 privilege level 15
 transport input telnet
line vty 5 15
 privilege level 15
 transport input telnet
!
scheduler allocate 20000 1000

!
webvpn cef
!
end
```

プライマリ リンクおよびバックアップ リンクを使用した EzVPN 導入

EzVPN は、特に、多数のブランチを持つ本社ブランチでの導入に対して導入と拡張を簡単に行えるように設計されています。この導入では、プライマリ リンクとして DSL インターフェイスを使用し、バックアップ リンクとしてセルラー リンクを使用します。EzVPN の詳細については、「*Cisco Easy VPN*」を参照してください。

図 5-5　プライマリおよびバックアップを使用した EzVPN の導入



EzVPN クライアント（ブランチ ルータ）の設定

例 5-10　　EzVPN クライアント（ブランチ ルータ）の設定

この設定内で青色の斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
!
hostname branch-router
!
ip cef
!
ip dhcp excluded-address 10.13.0.254
!
ip dhcp pool gsmpool
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.13.0.254
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 20 "CONNECT"
!
!   セルラー インターフェイスを介したダイヤル アウトへのチャット スクリプト
!
username cisco123@cisco.com password 0 lab
username cisco password 0 lab
username sachin@cisco.com password 0 lab
!
!   EzVPN クライアント認証用のローカル ユーザ名およびパスワード。
!
!
track 234 rtr 1 reachability
!
crypto ipsec client ezvpn hw-client-pri
 connect auto
 group hw-client-group key cisco123
 backup hw-client track 234
 mode network-extension
 peer 128.107.248.243
 username cisco123@cisco.com password lab
 xauth userid mode local
!
!   プライマリ WAN インターフェイスの EzVPN クライアントの設定。バックアップ WAN の使用中に、
!   ファイルオーバーにトラック 234 を使用してバックアップします。
!
!
crypto ipsec client ezvpn hw-client
 connect auto
 group hw-client-group key cisco123
 mode network-extension
 peer 128.107.248.243
 username sachin@cisco.com password lab
 xauth userid mode local
!
!   バックアップ WAN インターフェイスの EzVPN クライアントの設定
!
!
```

```
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 104
!
interface FastEthernet0/1/1
 switchport access vlan 104
!
interface FastEthernet0/1/2
 switchport access vlan 104
!
interface FastEthernet0/1/3
 switchport access vlan 104
!
!   DHCP クライアント ホストによって使用されるファスト イーサネット ポート。
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
!   プライマリ インターフェイスとして使用される ATM（DSL）物理インターフェイス
!
interface ATM0/0/0.1 point-to-point
 ip nat outside
 ip virtual-reassembly
 no snmp trap link-status
 pvc 0/35
  pppoe-client dial-pool-number 2
!
interface Cellular0/1/0
 no ip address
 ip nat outside
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 dialer-group 1
 async mode interactive
 ppp ipcp dns request
!
interface Vlan104
 description ip address used as default gateway address for DHCP    clients
 ip address 10.13.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
 crypto ipsec client ezvpn hw-client-pri inside
 crypto ipsec client ezvpn hw-client inside
!
!   EzVPN 暗号化のための内部インターフェイスの一部となるように、ファスト イーサネット ポート
!   0/1/0 から 0/1/3 に接続されたホストに VLAN 104 を定義します。
!
interface Dialer1
 ip address negotiated
```

```
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer string gsmscript
 dialer persistent
 dialer-group 1
 ppp chap hostname cisco@cisco.com
 ppp chap password 0 cisco123
 ppp ipcp dns request
 crypto ipsec client ezvpn hw-client
!
!    セルラー インターフェイスと関連付ける外部ダイヤラ インターフェイス
!
!    このバックアップ インターフェイスにおいて、上記で定義した暗号化 IPsec クライアント ezvpn hw-client。
!    これにより、これが EzVPN 暗号化の外部インターフェイスであることが確認されます
!
interface Dialer2
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 2
 dialer-group 2
 ppp chap hostname Cisco@cisco.com
 ppp chap password 0 cisco
 ppp ipcp dns request
 crypto ipsec client ezvpn hw-client-pri inside
!
!
!    プライマリ WAN の外部 EzVPN インターフェイスを定義します。
!
ip local policy route-map track-primary-if
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
ip route 0.0.0.0 0.0.0.0 Dialer 1 253
!
access-list 1 permit any
!
access-list 102 permit icmp any host 209.131.36.158
!
dialer-list 1 protocol ip list 1
!
dialer-list 2 protocol ip permit
no cdp run
!
!
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2 null0
!
control-plane
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
 stopbits 1
line aux 0
 stopbits 1
line 0/1/0
 exec-timeout 0 0
 script dialer gsmscript
 login
 modem InOut
 no exec
```

```
 transport input all
 transport output all
 rxspeed 236800
 txspeed 118000
line vty 0 4
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000
!
end
```

EzVPN サーバ ルータの設定

例 5-11　　EzVPN サーバ ルータの設定

この設定内で青色の斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

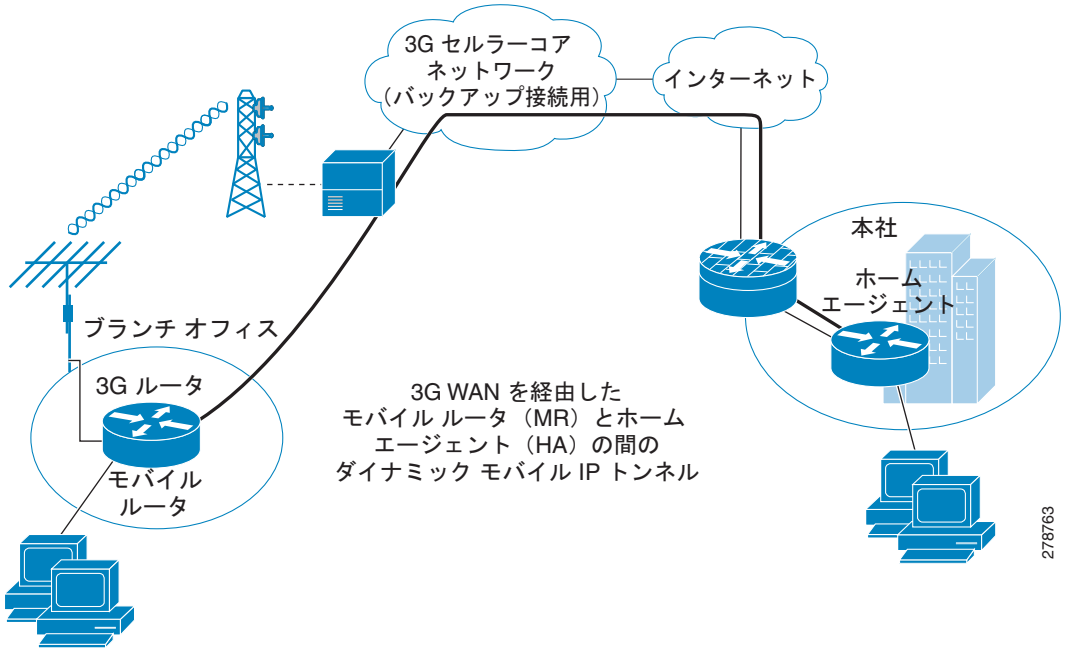
```
hostname ezvpn_gw
!
ip cef
!
username cisco123@cisco.com password 0 lab
username sachin@cisco.com password 0 lab
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 1800
crypto isakmp client configuration address-pool local dynpool
!
crypto isakmp client configuration group hw-client-group
 key cisco123
 dns 10.11.0.1
 domain cisco.com
 pool dynpool
 acl 111
!
!
crypto ipsec transform-set set1 esp-3des esp-md5-hmac
!
crypto dynamic-map dynmap 1
 set transform-set set1
!
!
crypto map dynmap isakmp authorization list hw-client-groupname
```

```
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!   EzVPN サーバ側設定。ACL 111 は、EzVPN クライアントから暗号化される許可されたトラフィックを定義し、
!   IPSec トンネルのセットアップ中にネゴシエーションされます
!
!
interface GigabitEthernet0/0
 ip address 128.107.248.243 255.255.255.224
 ip nat outside
 duplex auto
 speed auto
 crypto map dynmap
!
!
!   クリプト マップはサーバの WAN インターフェイスに適用されます。
!
!
interface GigabitEthernet0/1
 ip address 10.11.0.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
!
ip local pool dynpool 10.11.0.50 10.11.0.100
!
!   ローカル プールを定義して、IP アドレスをリモート EzVPN クライアントに指定します。
!
!
ip nat inside source list 101 interface GigabitEthernet0/0 overload
ip route 0.0.0.0 0.0.0.0 128.107.248.254
!
access-list 111 permit ip 10.11.0.0 0.0.0.255 10.13.0.0 0.0.0.255
!
!   EzVPN リモート クライアント用の暗号化が許可される必要のある対象トラフィックを
!   定義します。このような ACL 版は、暗号化および NAT 用に EzVPN の
!   リモート クライアントに伝達されます。
!
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
line aux 0
line vty 0 4
 login
!
end
```

CCOA-Only モードでの NEMO Over 3G

Network Mobility（NEMO）は、広範囲にわたる地理的領域にわたって、スタブ ネットワークとして複数のブランチを導入するために使用できる、スケーラブルなオプションです。すべてのブランチはブランチ ルータの背後に接続されたモバイル ネットワークとして機能し、WAN リンクを介したダイナミック モバイル IP トンネルによって、すべての接続を確立します。次の設定例は、Foreign Agent（FA）が存在しない、コロケーション気付アドレスのみ（CCOA-only）のモードでのモバイル IP を示しています。ブランチでの NEMO 導入の詳細については、「*Introduction to Mobile IP*」を参照してください。

図 5-6　　3G WAN 経由での NEMO の配置



ブランチ オフィスのモバイル ルータ（MR）の設定

例 5-12　　ブランチ オフィスのモバイル ルータ（MR）の設定

```
!
hostname mobile-router
!
ip cef
!
ip dhcp excluded-address 10.13.0.254
!
ip dhcp pool gsmpool
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.13.0.254
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 20 "CONNECT"
!
!    セルラー インターフェイスを介したダイヤル アウトへのチャット スクリプト
!
```

```
track 234 rtr 1 reachability
!
!   バックアップ方法のオブジェクト トラッキング。
!
interface Loopback100
 ip address 10.100.0.3 255.255.255.0
!
!   モバイル ルータに割り当てられた静的 IP アドレス。このアドレスは
!   HA-MR サブネットの一部です
!
interface GigabitEthernet0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 104
!
interface FastEthernet0/1/1
 switchport access vlan 104
!
interface FastEthernet0/1/2
 switchport access vlan 104
!
interface FastEthernet0/1/3
 switchport access vlan 104
!
!   DHCP クライアント ホストによって使用されるファスト イーサネット ポート
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
!   プライマリ インターフェイスとして使用される ATM（DSL）物理インターフェイス。
!
interface ATM0/0/0.1 point-to-point
 ip nat outside
 ip virtual-reassembly
 no snmp trap link-status
 pvc 0/35
  pppoe-client dial-pool-number 2
!
interface Cellular0/1/0
 no ip address
 ip nat outside
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 dialer-group 1
 async mode interactive
 ppp ipcp dns request
!
!   モバイル IP の導入に外部ダイヤラ（ダイヤラ 1）を使用し、ダイヤラ pool-member 1 は、
!   ダイヤラ プール 1 が設定されているダイヤラ 1 にセルラー インターフェイスを関連付けます
!
!
interface Vlan104
 description ip address used as default gateway address for DHCP    clients
```

```
 ip address 10.13.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
!
!   ファスト イーサネット ポート 0/1/0 から 0/1/3 に接続されたホストに VLAN 104 を定義します。
!   このサブネットは、モバイル ルータの背後にあるモバイル ネットワークになります。
!
interface Dialer1
 ip address negotiated
 ip nat outside
 ip mobile router-service roam
 ip mobile router-service collocated ccoa-only
 encapsulation ppp
 dialer pool 1
 dialer string gsmscript
 dialer persistent
 dialer-group 1
 ppp chap hostname cisco@cisco.com
 ppp chap password 0 cisco123
 ppp ipcp dns request
!
!   ccoa-only モバイル IP モードのモバイル IP 設定のセルラーと関連付けられた
!   外部のダイヤラ インターフェイス。
!

interface Dialer2
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 2
 dialer-group 2
 ppp chap hostname Cisco@cisco.com
 ppp chap password 0 cisco
 ppp ipcp dns request
!
router mobile
!
!   このコマンドはルータでモバイル IP 機能をオンにします
!

!
ip local policy route-map track-primary-if
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
ip route 0.0.0.0 0.0.0.0 dialer 0/0/0 253
!
ip mobile secure home-agent 128.107.248.243 spi decimal 1003 key ascii 1234567891234563
algorithm md5 mode prefix-suffix
!
!   このステートメントは ASCII 値を使用して暗号化の詳細と認証を定義します。
!   ASCII 値は HQ 側のルータの HA 設定の値と一致している必要があります
!
ip mobile registration-lifetime 1800
ip mobile router
 address 10.100.0.3 255.255.255.0
 collocated single-tunnel
 home-agent 128.107.248.243
 mobile-network GigabitEthernet0/1
 register retransmit initial 5000 maximum 10000 retry 5
 reverse-tunnel
!
!   アドレスは、ループバック 100 に定義されたモバイル ルータの静的 IP アドレスを定義します
!
!   モバイル IP リクエストを開始するユーザをルータが認識できるように、
```

```
!    ホーム エージェント アドレスが定義されます。
!

ip sla 1
 icmp-echo 209.131.36.158 source-interface Dialer2
 timeout 1000
 frequency 2

ip sla schedule 1 life forever start-time now

access-list 1 permit any
!
access-list 102 permit icmp any host 209.131.36.158
!
dialer-list 1 protocol ip list 1
!
dialer-list 2 protocol ip permit
no cdp run
!
!
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2 null0
!
control-plane
!
bridge 1 protocol ieee
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
 stopbits 1
line aux 0
 stopbits 1
line 0/1/0
 exec-timeout 0 0
 script dialer gsmscript
 login
 modem InOut
 no exec
 transport input all
 transport output all
 rxspeed 236800
 txspeed 118000
line vty 0 4
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000
!
end
```

本社のホーム エージェント（HA）のルータの設定

例 5-13　　本社のホーム エージェント（HA）のルータの設定

この設定内で青色の斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
hostname HQ-HomeAgent
!
ip cef
!
interface Loopback100
 ip address 10.100.0.1 255.255.255.0
!
!   ホーム エージェント（HA）とモバイル ルータ（MR）間のモバイル IP サブネット
!
interface GigabitEthernet0/0
 ip address 128.107.248.243 255.255.255.224
 ip nat outside
 duplex auto
 speed auto
!
!   これは、インターネットを介してモバイル ルータに接続する WAN インターフェイスです
!
interface GigabitEthernet0/1
 ip address 10.11.0.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
!
router mobile
!
!   HA のルータ上のモバイル IP を有効にします
!
!
ip nat inside source list 101 interface GigabitEthernet0/0 overload
!
ip route 0.0.0.0 0.0.0.0 128.107.248.254
!
ip mobile home-agent reverse-tunnel private-address
ip mobile home-agent QoS policer
ip mobile home-agent address 128.107.248.243 lifetime 1800 replay 255 unknown-ha accept
reply
!
!   ホーム エージェントの設定
!
ip mobile host 10.100.0.3 virtual-network 10.100.0.0 255.255.255.0
ip mobile mobile-networks 10.100.0.3
 register
!
!   登録用のモバイル ルータ エントリ
!
```

```
ip mobile secure host 10.100.0.3 spi decimal 1003 key ascii 1234567891234563 algorithm md5
mode prefix-suffix
ip mobile registration-lifetime 1800
!
!    セキュアな通信のためのモバイル ルータ認証（MR に設定されているものと同じ ASCII）
!    および暗号化詳細
!
access-list 101 permit ip 13.1.1.0 0.0.0.255 any
!
control-plane
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
line aux 0
line vty 0 4
 login
!
end
```