Deployment Guide

Next-Generation Enterprise WAN:

Cisco ISRs with 4G LTE deployment guide

May 2014

Contents

1. Introduction

The Cisco® Next-Generation Enterprise WAN is an end-to-end architecture that provides foundation building blocks for next-generation enterprise networks. The hierarchical design provides the scalability required by large enterprises that can be extended and replicated throughout multiple regions and topologies. This consistency leads to ease of deployment, maintenance, and troubleshooting.

This guide provides deployment, debugging, and troubleshooting information for the fourth-generation long-term evolution (4G LTE) Cisco Enhanced High-Speed WAN Interface Cards (EHWICs), which provide wireless 4G networking capability on the Cisco Integrated Services Routers Generation 2 (ISR G2) (Cisco 1900, 2900, and 3900 Series Integrated Services Routers). This guide is also applicable to fixed Cisco ISR platforms (Cisco 800 Series ISRs) with 4G LTE as a wireless WAN (WWAN) interface with minor changes pointed out in configurations.

This guide is intended for users of Cisco ISR G2 routers with 4G LTE as a WWAN interface, including system integrators, network architects, and support engineers. This guide provides a brief overview of the cellular networks, their architecture, and their relevance to the enterprise networks. It assumes basic knowledge of Cisco IOS® Software command-line interface (CLI) configuration.

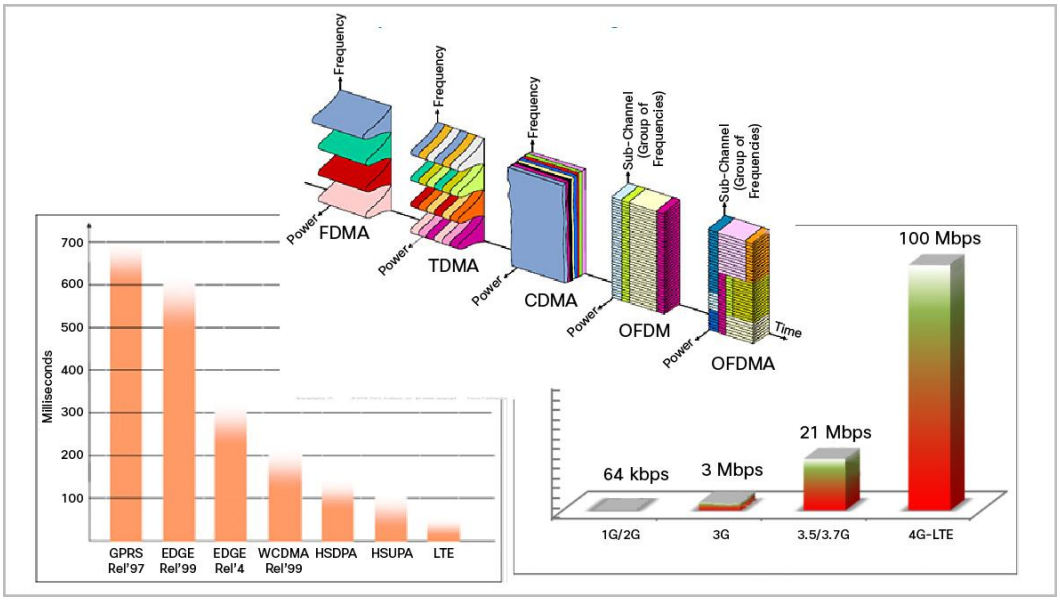
This guide discusses the cellular technology architecture and evolution. It explains how Cisco intends this technology to be used in enterprise networks. Sections provide information about activation, basic configuration, and troubleshooting of the WWAN interface on Cisco ISR G2 routers. This guide builds on that basic information to cover the advanced deployments including VPNs, dynamic routing, and other advanced services that are enabled by Cisco IOS Software.

2. Cellular Technology Evolution to 4G LTE

The basics of the third-generation (3G) and previous-generation cellular networks are covered in the 3G deployment guide at: http://www.cisco.com/en/US/docs/routers/access/1800/1861/software/guide/3Gchapter1.html.

Figure 1 summarizes the evolution of cellular networks in terms of technology, latency, and bandwidth.

Figure 1. Cellular Technology Evolution



This guide builds on the background of the 3G deployment guide and emphasizes the 4G LTE aspects.

With the advent of the 4G LTE, the new architecture was designed as part of two Third-Generation Partnership Project (3GPP) work items:

- System architecture evolution (SAE), which covered the core network
- Long-term evolution (LTE), which covered the radio access network (RAN), air interface, and mobility

Officially, the whole system is known as the evolved packet system (EPS), and LTE refers only to the evolution of the air interface. Despite this official usage, LTE has become a colloquial name for the whole system, and LTE is regularly used in this way by 3GPP Release 8. The Cisco 4G LTE is an all-IP design to carry multimedia services over a packet-switched domain. Currently, data services are offered. Voice and other rich-media services will be available in the future.

2.1 4G LTE Performance Characteristics

The 4G HWIC supports the latest production 3GPP Release 8 cellular standards including Universal Mobile Telecommunications Service (UMTS), high-speed downlink packet access (HSDPA), and the latest production Code Division Multiple Access 2000 (CDMA2000) standards, Evolution-Data Optimized (EVDO) Rev A. Table 1 shows the CDMA2000 technologies and the Global System for Mobile Communications (GSM) and UMTS technologies evolving into 4G LTE.

Table 1. Cellular Technology and Associated Theoretical Bandwidths

GSM TDMA-based worldwide Cellular standard **Speeds: 28 kbps**	**CDMA** IS-95 followed by cdmaOne Adopted in North America, parts of South America, and Asia **Speeds: 28 kbps**
GPRS, EDGE (2.5G) Packet data service over GSM overlay, using multiple time slots **Downlink: 384 kbps** **Uplink: 180 kbps**	**1xRTT (2.5G)** Packet data service using single 1.25-MHz channel **Downlink: 307 kbps** **Uplink: 153 kbps**
UMTS/HSDPA (3G) WCDMA-based data services **Downlink: 3.6 Mbps** **Uplink: 384 kbps**	**EVDO Rev1 (3G)** Dedicated radio channel for data **Downlink: 3.1 Mbps** **Uplink: 1.8 Mbps**
LTE (4G) Packet-switched data services **Downlink: Up to 100 Mbps** **Uplink: Up to 50 Mbps**	**LTE (4G)** Packet-switched data services **Downlink: Up to 50 Mbps** **Uplink: Up to 25 Mbps**

2.2 Throughput

Cellular throughput is stated as a theoretical maximum speed that the given radio technology can provide. Theoretical maximum speed is based on the mathematical calculations of the radio resources and associated bits. In practice, users can achieve 30 percent of the theoretical speeds on average on a normally loaded network. Throughput is shared per cell sector, per carrier frequency. For EVDO Rev A, total theoretical throughput per sector is 3.1-Mbps downlink, 1.8-Mbps uplink. For HSDPA, the theoretical throughput of the EHWIC chipset is 3.6-Mbps downlink, 384-kbps uplink. (Newer versions of HSDPA support 7.2-Mbps downlink) Actual throughput depends on network conditions at the time, Received Signal Strength Indicator (RSSI), and cellular backhaul facilities.

LTE has a theoretical net bit rate capacity of up to 100 Mbps in the downlink and 50 Mbps in the uplink if a 20-MHz channel is used. A higher capacity is possible if multiple-input multiple-output (MIMO) technologies, such as antenna arrays, are used. The physical radio interface uses Orthogonal Frequency Division Multiple Access (OFDMA), now named Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).

2.3 Latency

Latency in the 4G cellular network is designed to be significantly lower than in 3G networks. Latency is dependent on network conditions and the RAN. Table 2 depicts the observed end-to-end throughput and latency during testing on production networks.

Table 2. Cellular Modes and Associated Bandwidth and Latency Characteristics

Technology or Service	Uplink	Downlink	Average Latency (Round-Trip Time [RTT])
EDGE	80 kbps	140 kbps	250-300 ms
UMTS	250 kbps	400 kbps	150-200 ms
HSDPA	**300 kbps**	**700 kbps**	**100 ms**
1xRTT	80 kbps	150 kbps	250 ms
EVDO Rel0	140 kbps	500 kbps	125 ms

Technology or Service	Uplink	Downlink	Average Latency (Round-Trip Time [RTT])
EVDO Rev A	500 kbps	800 kbps	100 ms
LTE (AT&T)	2-5 Mbps	5-12 Mbps	40 ms
LTE (Verizon)	2-5 Mbps	5-12 Mbps	40 ms

Note: AT&T 4G LTE and Verizon 4G LTE provide similar throughput.

2.4 Shared Access

A cellular network is a wireless access network wherein the available radio spectrum is shared between multiple user devices that connect to the same cell tower at any given time. The available theoretical maximum bandwidth is shared among the active users who request access to the network. As a result, it is difficult to predict precisely the available bandwidth to any particular user in a given cell.

2.5 Radio Signal

Receive Signal Strength Indicator (RSSI) is a circuit to measure the strength of an incoming signal. The basic circuit is designed to pick RF signals and generate an output equivalent to the signal strength. The ability of the receiver to pick the weakest of signals is referred to as **receiver sensitivity**. When the receiver sensitivity is high, the performance is better. Circuits measure the signal strength based on the output voltage. If the signal strength is good, the output voltage is higher. If the signal strength is low, the output voltage is poor.

These performance characteristics mean that the sweet spot for the 4G HWIC is basic real-time, 5-10 Mbps applications. As networks evolve, latencies decrease, quality of service (QoS) becomes available, and real-time applications (such as high-definition video calls) become viable.

2.6 QoS over 4G LTE Connection

Cisco IOS QoS mechanisms are applicable on EHWIC 4G LTE interfaces. RAN QoS is not yet available on production cellular networks. Therefore, though the traditional IP QoS is available on the ISRs and on the 4G EHWIC interface, mapping to the airlink is not available. Nonetheless, you can use the Cisco IOS QoS capabilities to improve the application experience. Techniques such as congestion management, congestion avoidance, policing and shaping, and Modular QoS CLI (MQC) are beneficial.

3. Why Cisco 4G LTE?

Cisco introduced the fourth-generation (4G) cellular Cisco Enhanced High-Speed WAN Interface Card (EHWIC) for ISR G2 and fixed platforms with an embedded 4G LTE WAN interface. The 4G LTE WWAN interface on modular and fixed ISRs provides enterprise organizations with the ultimate flexibility in their network deployment. The 4G LTE WWAN interface also enables new mobility-based deployment models and adds a robust way to connect the remote locations with full-feature capabilities. The following examples describe such deployments:

- Remote branch-office backup: The main target service is remote branch-office backup, because many organizations plan to replace T1/T3, 3G, and ISDN links with alternative technologies.
- Rapid employment: Wireless WAN service enabled by the 4G EHWIC is attractive for nomadic connectivity such as workgroups and temporary connectivity from trade shows and construction sites.
- Primary connectivity: Primary connectivity enables high-performance, secure, reliable, and transparent multimedia applications anywhere and anytime. It allows you to deploy and manage the same device for multiple applications, simplifying deployment and management.
- Mobile disaster-recovery solution: Often when wireline facilities suffer major outages, cellular service remains functional because the facilities take alternative paths through different central offices.

4. Cisco 4G LTE Offerings

Table 3 lists the hardware that Cisco introduced to support 4G LTE WWAN.

Table 3. Cisco 4G LTE Product SKUs

Cisco SKU ID	Modem	Speeds		Cisco IOS Software Version	ISP or Region	Features
		Downlink Mbps	Uplink Mbps			
EHWIC-4G LTE-V	MC7750	50	25	15.3(3)M or later	Verizon	4G speeds, ~25-msec latency, interface MIBs, data callback (voice and Short Message Service [SMS]), subscriber identity module (SIM) lock, diagnostics, remote firmware upgrade, 4G MIBs, SMS, and Global Positioning System (GPS)
C819(H)G-4G-V-K9						
EHWIC-4G LTE-A	MC7700	100	50	15.3(3)M or later	AT&T	
C819(H)G-4G-A-K9						
EHWIC-4G LTE-G	MC7710	100	50	15.3(3)M or later	Europe and regions with same 3G or 4G bands	
C819(H)G-4G-G-K9						
EHWIC-4G LTE-BE	MC700	100	50	15.3(3)M1 or later	Bell (Canada);	
EHWIC-4G LTE-JP	MC7700	100	50	15.3(3)M1 or later	NTTDocomo (Japan)	

- EHWIC-4G-LTE-V: Works on ISR G2 (Cisco 1900, 2900, and 3900) with Verizon 4G LTE network
- C819(H)G-4G-V-K9: Hardened and nonhardened version of Cisco 819 on the Verizon 4G LTE network
- EHWIC-4G-LTE-A: Works on ISR G2 (Cisco 1900, 2900, and 3900) with the AT&T 4G LTE network
- C819(H)G-4G-A-K9: Hardened and nonhardened version of Cisco 819 on AT&T's 4G LTE network
- EHWIC-4G-LTE-G: Works on ISR G2 (Cisco 1900, 2900, and 3900) with global 4G LTE networks (FD-LTE only mode)
- C819(H)G-4G-G-K9: Hardened and nonhardened version of Cisco 819 on global 4G LTE networks (FD LTE only mode)
- EHWIC-BE: Works on ISR G2 (Cisco 1900, 2900, and 3900) with Bell cellular network in Canada
- EHWIC-JP: Works on ISR G2 (Cisco 1900, 2900, and 3900) with NTTDocomo cellular network in Japan

The EHWIC-4G-LTE comes with the Sierra Wireless multimode modem. The multimode modems smoothly hand off between different modes such as 4G LTE to 3G to 2G as per network availability. You do not need to configure it, although you can use the CLI to set a preference for a particular mode. This preference is subject to the ability of the network to honor it - and the network can override it. Multimode capability is as per the 3GPP standards. The EHWIC can operate in the following modes:

- 4G LTE: The 4G LTE mobile specification provides multimegabit bandwidth, a more efficient radio network, latency reduction, and improved mobility. LTE solutions target new cellular networks. These networks initially support up to 100-Mbps peak rates in the downlink and up to 50-Mbps peak rates in the uplink. The throughput of these networks is higher than the existing 3G networks.
- 3G Evolution-Data Optimized (EVDO or DOrA) mode: EVDO is a 3G telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access. DOrA refers to EVDO Rev A. This mode is supported with only the -V version of the LTE products.

- 3G evolution high-speed packet access (HSPA/HSPA+): HSPA is a UMTS-based 3G network. HSPA supports high-speed downlink packet access (HSDPA) and high-speed uplink packet access (HSUPA) data for improved download and upload speeds. This mode is supported on all products except -V version.

Follow the instructions in the Cisco 4G LTE hardware installation guide: http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/EHWIC-4G LTEHW.html.

Connect the antenna properly and make sure that the card is recognized by the ISR on boot-up before you perform the next step.

4.1 Cisco 4G LTE Product-Related Documentation

- Ordering guide: http://www.cisco.com/c/dam/en/us/products/collateral/interfaces-modules/4g-lte-wireless-wan-enhanced-high-speed-wan-interface-card/cisco_4g_lte_for_cisco_og_v1b.pdf
- 4G LTE Q&A: http://www.cisco.com/en/US/prod/collateral/modules/ps5949/ps11540/qa_c67-641302.html
- 4G LTE data sheet: http://www.cisco.com/en/US/prod/collateral/modules/ps5949/ps7272/datasheet_c78-710314.html
- Cisco 4G LTE hardware installation guide: http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/EHWIC-4G LTEHW.html
- Cisco 4G LTE software installation guide: http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/EHWIC-4G LTESW.html

4.2 Service Plans

Access to any cellular service provider network is based on monthly subscription for a fee. You must sign up with the service provider to get the service. When you sign up, you are given a SIM card. Follow the hardware installation guide to install the SIM card.

Cisco does not provide the SIM card. Cisco does not have any special arrangement to get a SIM card from any service providers. Organizations must contact the service provider directly to get appropriate cellular service based on their service needs, such as the amount of monthly data.

5. Configuring the Router for 4G LTE Connectivity

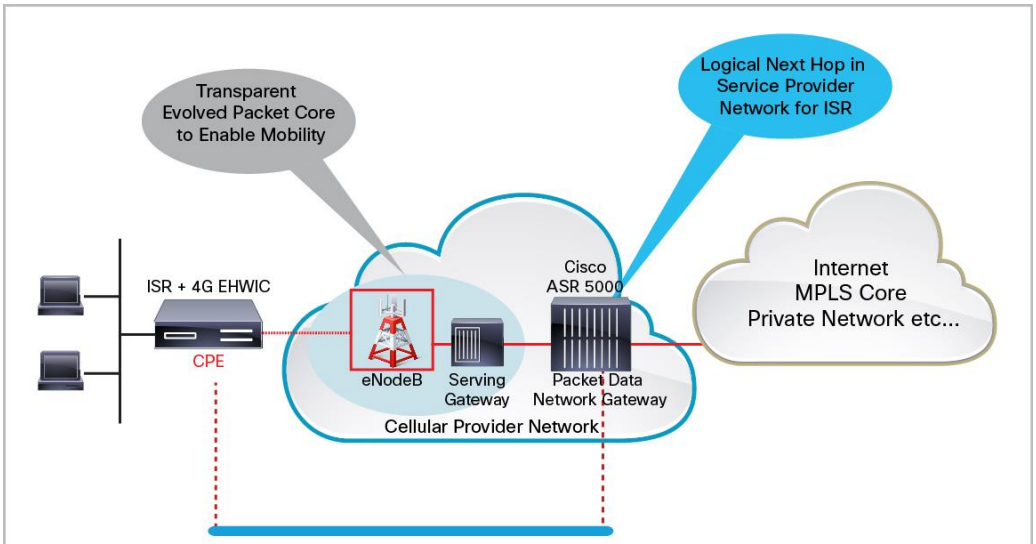
After you decide which hardware is made available with the associated 4G LTE service from an appropriate service provider, follow the instructions in the hardware installation guide to install the hardware properly. For installation instructions, refer to the Cisco 4G LTE hardware installation guide: http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/EHWIC-4G LTEHW.html.

In summary, the minimum hardware that is required includes the Cisco EHWIC-4G LTE-x and a Cisco ISR G2 router.

5.1 4G LTE Basic Configuration

The 4G LTE cellular interface is based on asynchronous serial interface and relies on a dial-on-demand mechanism. This configuration must be similar to any dialer-based interface, such as Serial, ISDN etc.
This configuration involves routing the traffic to the interface and triggering the dialer based on qualified traffic. The traffic can be routed by static or dynamic IP routes, whereas dialing can be accomplished by triggering the dialer (dialer-group/dialer-watch/persistent) and a chat script to pass call-setup parameters to the cellular modem. The rest is typical Layer 3 forwarding after an IP address has been assigned. The Figure 2 provides a very high-level overview depicting the layer-3 connectivity between the cellular core network and the Cisco ISR with 4G-LTE interface. For more information, refer to the Cisco 4G LTE software installation guide: http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/EHWIC-4G LTESW.html.

Figure 2. Basic Network Topology for Internet Access Using Cellular Network



5.2 Preparation to Connect

After the hardware installation is complete, make sure that the cellular card can detect the appropriate network and that the RSSI is within an acceptable range. The **show cellular** commands can be used to check this information:

```
ROUTER#sh cell 0/1/0 all
```

```
<snip>
Network Information
==================
Current Service Status = Normal, Service Error = None
Current Service = Packet switched
<snip>
Radio Information
=================
Radio power mode = ON
Current RSSI = -58 dBm
LTE Technology Preference = AUTO
LTE Technology Selected = LTE

Modem Security Information
==========================
<snip>
SIM Status = OK
<snip>
```

As shown in this output, the RSSI should be better than -90 dBm. The SIM status is “OK” and the current service status is ”Normal”, meaning that the router is ready to make the data call and set up the IP connectivity using the 4G LTE WWAN interface.

5.3 Profile Configuration

Cellular service providers can associate the cellular devices to different pools using the access point names (APNs). These pools can be maintained in different ways, such as per service type or per enterprise type. Cellular service providers typically use the APN for enterprises to provide a specific private IP address or static IP address for the enterprise devices. By default, profile 1 is prepopulated with a default APN that gives a dynamic IP address to the endpoint, such as the EHWIC. Cellular service providers can provide a managed connectivity using an enterprise-specific APN. This profile configuration command can be used to modify the default profile to a specific one:

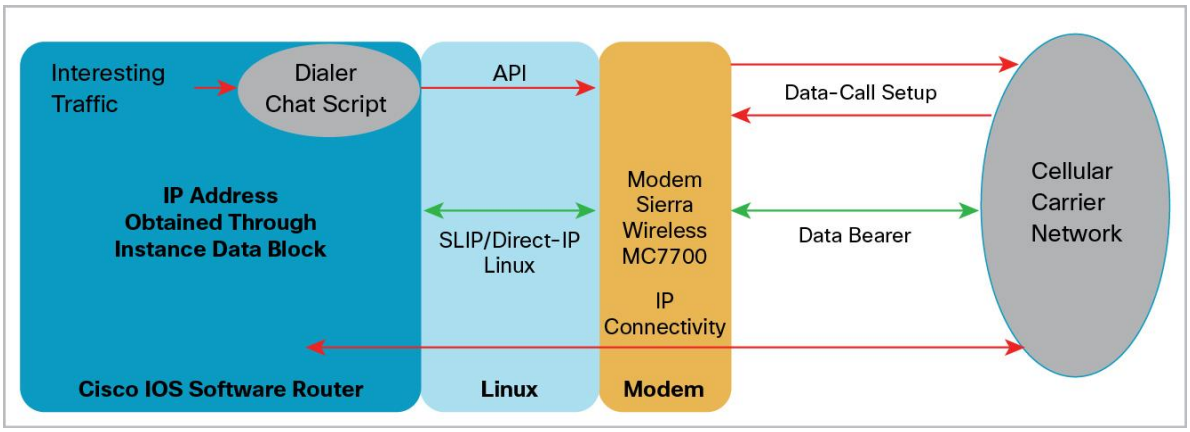
```
ROUTER#cellular <unit> lte profile create <profile#> <APN_name>
```

For more details, refer to the Cisco 4G LTE software installation guide: http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/EHWIC-4GLTESW.html#wp1214437.

5.4 LTE Data-Call Setup

As shown in Figure 3, Cisco IOS Software acts as the host operating system, which operates the cellular modem to set up the data call on the radio side with the cellular network. After the call is set up, the modem passes the IP address to the Cisco IOS Software. All subsequent data traffic is passed to Cisco IOS Software by the modem in a data-packet format.

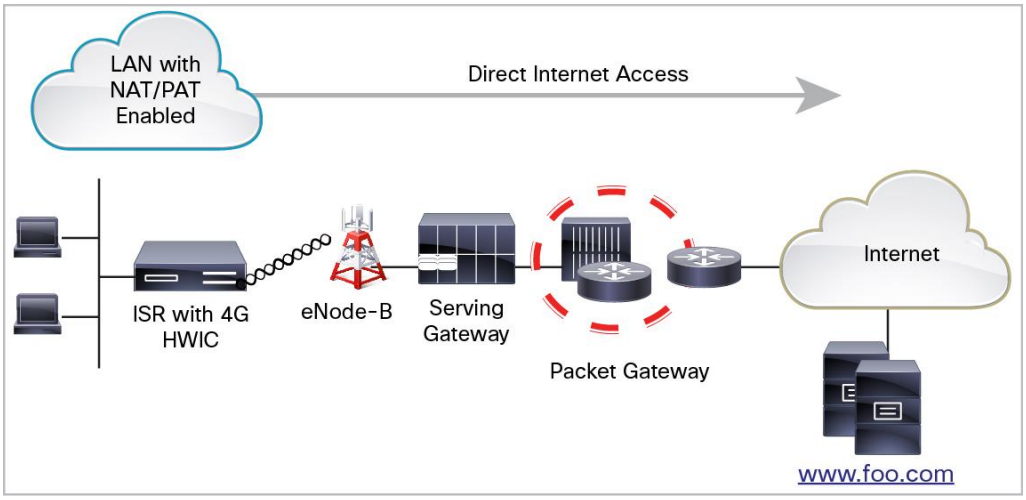
Figure 3. 4G LTE Data-Call Setup from Cisco IOS Software to Cellular Network



5.5 Basic Internet Connectivity

To make a data call to the service provider network, the router must have a basic configuration in place. This configuration includes the cellular interface configuration with **encapsulation, dialer string**, and **dialer group** commands. This configuration also includes the global configuration for commands that are related to chat script, dialer list, IP routing, and the associated line commands. Figure 4 shows a working configuration.

Figure 4. Basic Internet Connectivity Using 4G-LTE as WAN Using NAT/PAT for LAN Hosts



Configuring the router for the Basic internet Connectivity over cellular interface using NT/PATThe following configuration shows the basic configuration that must be in place to make sure the router can use the cellular interface that is acting as a WAN Internet interface. This deployment uses the Port Address Translation (PAT) technique to map local private IP hosts on the LAN to a single Internet IP address on the cellular interface.

```
chat-script lte "" "AT!CALL1" TIMEOUT 20 "OK"
!The chat script used to make a call!
interface GigabitEthernet0/1/0
 switchport access vlan 18  !>> switch port part of LAN to connect local user
```

```
!
interface GigabitEthernet0/1/1
 no ip address
!
interface GigabitEthernet0/1/2
 no ip address
!
interface Cellular0/0/0
 ip address negotiated
 ip nat outside   !>> NAT enabled
no ip virtual-reassembly in
 encapsulation slip !>>default encap changed from PPP in 3G to slip for 4G
 dialer in-band
 dialer string lte  !>> must match to the chat-script name
 dialer-group 1  !>>dialer group number must match the dialer list number
!
interface Vlan18
 ip address 192.168.18.1 255.255.255.0
 ip nat inside
!Vlan 18 is used as LAN interface and traffic from entering via this interface is
NAT'ed
!
ip nat inside source list 2 interface Cellular0/0/0 overload
!NAT statement to match the NAT traffic as per access-list 2
ip route 0.0.0.0 0.0.0.0 Cellular0/0/0
!Default route pointing to the cellular interface
!
access-list 1 permit any   !>> define what traffic can trigger the dialer
access-list 2 permit 192.168.18.0 0.0.0.255
dialer-list 1 protocol ip list 1  !>>associate acl 1 to dialer-list 1
!
line 0/0/0  !>> line associated with cellular 0/0/0
 script dialer lte  !>>> "lte" matches to dialer string and the chat-script name
 modem InOut
```

Validating Basic Internet Connectivity

To determine if the basic configuration is working, enter the following **show** commands:

```
ROUTER#sh ip route
<snip>
S*    0.0.0.0/0 is directly connected, Cellular0/0/0
```

```
!The default route is configured as the cellular interface where it serves as the
primary WAN link
!
C        10.165.149.83 is directly connected, Cellular0/0/0

ROUTER#sh cell 0/0/0 all
<snip>
Profile Information
==========
Profile 1 = ACTIVE*    !>>>>if things are configured correct, profile is active
when the call is up
--------
PDP Type = IPv4
PDP address = 10.176.219.57 !>> IP address is assigned
Data Connection Information
==========
Data Transmitted = 1967 bytes, Received = 1835 bytes
```

```
Profile 1, Packet Session Status = ACTIVE
        IP address = 10.176.219.57
        Primary DNS address = 198.224.174.135
        Secondary DNS address = 198.224.173.135
!Currently, only one active profile is supported and is seen to be functional as
listed above.
!<snip>

Network Information
==================
Current Service Status = Normal
Current Service = Packet switched
<SNIP>
Radio Information
=================
Radio power mode = ON
Current RSSI = -73 dBm
!
ROUTER#sh ip nat st
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 1, occurred 01:23:43 ago
Outside interfaces:
  Cellular0/0/0     !>>> outgoing interface after NAT
Inside interfaces:
  Vlan18         !>>> incoming LAN interface for traffic to be NAT'ed
Hits: 5  Misses: 0
<snip>
```

Troubleshooting the Basic Connectivity

When basic connectivity does not work properly, use the debugging capability of Cisco IOS Software. Various **debug** commands can be used to determine the root cause of the problem and how to fix it. **The most common causes are typos in the configuration.**

- The dialer string, chat-script name, and dialer script name must match in all three places.
- Make sure that the IP route is configured.
- Make sure that the NAT access list and NAT statement are properly configured.
- Make sure that the basic configuration is in place, please refer to section 5.1.

The **show cellular x/x/x all** command is used to make sure that basic parameters such as RSSI, service, and SIM are showing correctly.

The **debug chat** command can be used to enable debugs that will show if the cellular interface is able to set up a connection. This log shows a successful connection:

```
ROUTER#debug chat
ROUTER#ping cisco.com
Translating "cisco.com"...domain server (72.163.4.161)
*Jan 31 00:03:41.514: CHAT0/0/0: Attempting async line dialer script
<snip>
*Jan 31 00:03:41.514: CHAT0/0/0: Chat script lte started
*Jan 31 00:03:41.514: CHAT0/0/0: Sending string: AT!CALL1
<snip>
*Jan 31 00:03:42.378: CHAT0/0/0: Chat script lte finished, status = Success
!Expected string, and received string has a match based on chat script parameters
<snip>
*Jan 31 00:03:45.378: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cellular0/0/0, changed state to up (198.224.174.135) [OK]
<snip>
```

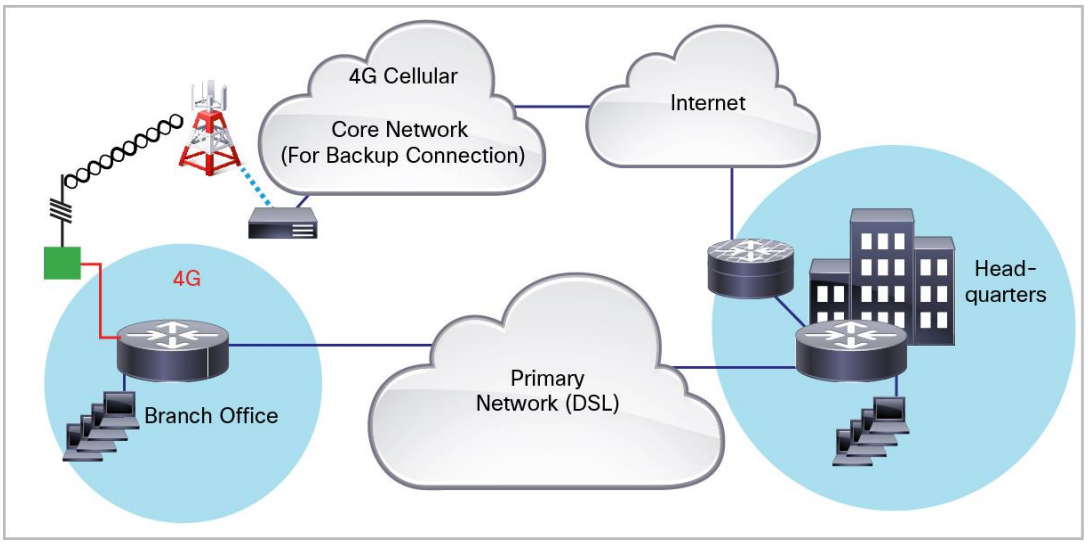
Other debugs that can be enabled are **debug dialer** and **debug cellular x/x/x messages callcontrol.**

For detailed troubleshooting and debug outputs, refer to the “Troubleshooting” section in the Cisco 4G LTE Software installation guide: http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/EHWIC-4GLTESW.html#wp1176080.

5.6 4G as a Backup to Wired Primary WAN Connection

The most popular deployment in the enterprise world for a cellular WAN interface is backup. Enterprises have adopted the 3G/4G cellular WAN connections as a backup to their primary connection such as Multiprotocol Label Switching (MPLS) over T1s or DSL. Figure 5 depicts this network topology. The 4G network, being the most resilient network in disastrous conditions, is an excellent backup WAN connectivity solution. Unlike wired WAN, it has its own transport infrastructure from the router to the Internet, which provides excellent path diversity. When all access is down because of natural disasters, cellular is often the only mode of communication for emergency response and early disaster recovery. Cellular WWAN connection is integrated in the ISR, so it automatically takes over when the primary WAN connection failure is detected. The most recommended method is based on Cisco IOS Software object tracking. In this method, the primary WAN connection is tracked by sending end-to-end pings to the far-end server/host. When the pings to the far end fail, the system concludes that the primary connection is not working and the backup starts routing the packets appropriately.

Figure 5. Network Topology for Primary/Backup Scenario



Branch-Office Router Configuration

This router configuration configures the router to use cellular as a backup Internet connection. The primary WAN connection in this case is an integrated DSL connection.

```
!
ip dhcp pool LAN
 network 192.168.18.0 255.255.255.0
 default-router 192.168.18.1
 dns-server 192.168.100.11
!DHCP pool to give out IP address to local hosts
!
chat-script lte "" "AT!CALL1" TIMEOUT 20 "OK"
!chat script to use to dial out for setting up cellular connection
!
track 234 ip sla 1 rechability
!Enable the object tracking

!
interface GigabitEthernet0/1/0
 switchport access vlan 18
 no ip address
!Switch-port to connect local client to router
!
interface ATM0/0/0
 no ip address
```

```
 no atm ilmi-keepalive
 dsl operating-mode auto
!
!       ATM (DSL) physical interface used as primary interface
!
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 Cellular0/0/0
 ip address negotiated
 ip nat outside
 encapsulation slip
 !Starting with HSPA+7 and LTE, encapsulation is changed from PPP to SLIP
 dialer in-band
 dialer string lte
 dialer-group 1
 async mode interactive
!
interface Vlan18
 ip address 192.168.18.1 255.255.255.0
 ip nat inside
!VLAN 18 to connect the local LAN clients and associated with DHCP pool LAN
!
interface Dialer2
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 2
 dialer-group 2
!Assigned the dialer to ATM0/0/0.1 using dialer pool configuration
 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
!
```

```
ip local policy route-map track-primary-if
!local policy to swtich NAT when the primary to backup switch-over happens
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!NAT entry for primary internface
ip nat inside source route-map nat2cell interface Cellular0/0/0 overload
!NAT entry for the backup interface
!
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
!primary route being tracked by 234 track defined earlier
!
ip route 0.0.0.0 0.0.0.0 Cellular0/0/0 254
!
!Backup router with higher admin distance (254), this will become primary when
track fails
!
ip sla 1
 icmp-echo 128.107.248.252 source-interface Dialer2
 frequency 2000
ip sla schedule 1 life forever start-time now
!IP SLA defines the IP address to ping to and how often, when ping fails, the
!
dialer-list 1 protocol ip permit
!
!dialer list 1 allows the dialer group 1 to dial out for any IP packet
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2 Null0
!to make sure we are sending tracking pings only via primary
route-map nat2dsl permit 10
 match ip address 101
 match interface Dialer2
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0/0/0
!above route maps (nat2cell and nat2dsl) to choose correct interface in use to
NAT
```

```
!
access-list 101 permit ip 192.168.0.0 0.0.255.255 any
!Identify local traffic to Nat, used in route-map statements above
!
access-list 102 permit icmp any host 128.107.248.252
!
!ping traffic to far end systems, referred in track_primary_if route-map
!
event manager applet pri_back
 event track 234 state any
 action 2.0 cli command "clear ip nat trans forced"
!
! Clears the NAT entries from the primary/backup interface upon switchover.

line 0/0/0
 script dialer lte
!the script dialer must match to chat-script string
 modem inout
```

Validating Primary and Backup Connectivity

You can use the following **show** commands to check if the router is functioning as per requirements of the primary and backup scenario:

- **Show cellular 0/0/0 all:** Provides the details related to cellular service such as signal strength, type of service connected, data transmitted, and hardware type and version
- **Show ip route track:** Shows if the monitoring is on and whether or not the primary is working

5.7 Enterprise Deployments Using 4G LTE as a WAN Interface

The recommended enterprise deployments for the 4G LTE WAN in an enterprise is Dynamic Multipoint VPN (DMVPN). DMVPN provides a scalable secure solution for enterprise deployments. It provides dynamic routing across the enterprise's main and branch offices, headquarters, and data center for the private IP subnet on both ends. DMVPN also allows branch offices to communicate directly and does not need to traverse through the central hub securely.

Other popular deployments are preferred because of the ease of deployments or other specific reasons. The next sections describe these popular enterprise deployments to cover a wide range:

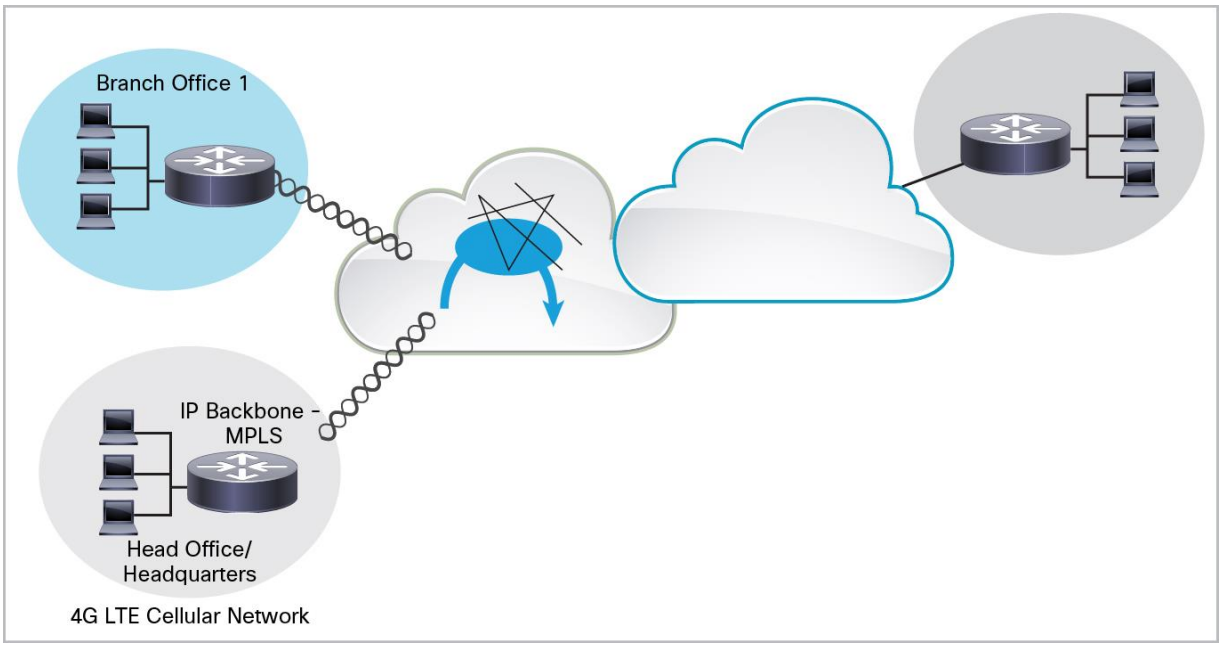
- DMVPN over 4G LTE
- Site-to-site IP Security (IPsec) VPN
- Generic routing encapsulation (GRE) and IPsec with dynamic routing
- Easy VPN
- Mobile IP (network mobility)

6. DMVPN over 4G LTE as a Primary WAN

For enterprise deployments with a large number of remote sites or branch offices, DMVPN is used. DMVPN provides the scalability and manageability required by such large-scale deployments. This hub-to-spoke topology also supports spoke-to-spoke traffic patterns. At startup, a branch-office (spoke) site establishes a DMVPN connection to the hub site and establishes a routing protocol adjacency. Traffic between the spoke and hub traverses this DMVPN connection. When traffic needs to flow between branch offices, DMVPN establishes a spoke-to-spoke tunnel dynamically for more direct and efficient traffic forwarding.

Figure 6 shows a sample configuration, which uses Enhanced IGRP (EIGRP) as an Interior Gateway Protocol (IGP) for dynamic routing updates between the DMVPN hub and spokes.

Figure 6. DMVPN over 4G LTE as Primary WAN



Configuration of Branch Office 1 as a DMVPN Spoke

```
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
!
!ISAKMP policy for phase 1 negotiation
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!Preshared key for Hub, and remote DMVPN spokes
```

```
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
!IPsec (Phase 2) policy for actual data encryption/integrity
!
crypto ipsec profile cisco
 set security-association lifetime seconds 86400
 set transform-set strong
!
!IPsec Profile to be applied dynamically to the GRE over IPsec tunnels
!
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 lte "" "AT!CALL1" TIMEOUT 20 "OK"
!
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
tunnel source cellular 0/1/0
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile Cisco
!
!GRE tunnel template which will be applied to all dynamically created
!GRE tunnels
!
interface FastEthernet0/2/0
```

```
 switchport access vlan 103
!
!
interface Cellular0/1/0
 ip address negotiated
 encapsulation slip
 dialer in-band
 dialer string LTE
 dialer watch-group 1
 async mode interactive
!
interface Vlan103
 ip address 10.3.0.254 255.255.0.0
 ip nat inside
!
router eigrp 90
 default-metric 100000 100 255 1 1500
 network 2.2.2.0 0.0.0.255
 network 10.3.0.0 0.0.255.255
 network 192.168.10.0 0.0.0.255
!
dialer watch-list 1 ip 5.6.7.8 0.0.0.0
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
!
!dialer watch-list configuration to keep the cellular connection up with ip
address
!
ip route 20.20.241.234 255.255.255.255 cellular 0/1/0
!
line 0/1/0
 script dialer lte
 modem InOut
!
```

Configuration of Branch Office 2 as a DMVPN Spoke

```
!
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
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
!
!ISAKMP policy for phase 1 negotiation
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!Preshared key for all the remote DMVPN spokes
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
!IPsec (Phase 2) policy for actual data encryption/integrity    !
!
crypto ipsec profile cisco
 set security-association lifetime seconds 86400
 set transform-set strong
!
!IPsec Profile to be applied dynamically to the GRE over IPsec tunnels
!
chat-script lte "" "AT!CALL1" TIMEOUT 20 "OK"
!
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
 tunnel source cellular 0/1/0
 tunnel mode gre multipoint
```

```
 tunnel key 0
 tunnel protection ipsec profile Cisco
!
!GRE tunnel template which will be applied to all dynamically created GRE tunnels
!
interface FastEthernet0/3/0
 switchport access vlan 108
!
interface Cellular0/1/0
 ip address negotiated
 encapsulation slip
 dialer in-band
 dialer string LTE
 dialer watch-group 1
 async mode interactive
!
interface Vlan108
 ip address 10.8.0.254 255.255.0.0
!
router eigrp 90
 default-metric 100000 100 255 1 1500
 network 1.1.1.0 0.0.0.255
 network 10.8.0.0 0.0.0.255
 network 192.168.10.0 0.0.0.255
!
dialer watch-list 1 ip 5.6.7.8 0.0.0.0
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
!
!dialer watch-list configuration to keep the cellular connection up with ip
address
!
ip route 20.20.241.234 255.255.255.255 cellular 0/1/0
!
line 0/1/0
 script dialer lte
 modem InOut
```

Configuration of Central-Office Router as a DMVPN Hub

```
!
hostname DMVPN_Hub
!
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
!
!ISAKMP policy for phase 1 negotiation
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!Preshared key for all the remote DMVPN spokes
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
!IPsec (Phase 2) policy for actual data encryption/integrity
!
crypto ipsec profile cisco
 set security-association lifetime seconds 86400
 set transform-set strong
!
!IPsec Profile to be applied dynamically to the GRE over IPsec tunnels
!
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
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile cisco
!
!GRE tunnel template for dynamically created GRE tunnels
!
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 FastEthernet0/1/0
 switchport access vlan 10
!
interface Vlan10
 ip address 10.10.0.254 255.255.0.0
!
router eigrp 90
 default-metric 100000 100 255 1 1500
 network 3.3.3.0 0.0.0.255
 network 10.10.0.0 0.0.255.255
 network 192.168.10.0 0.0.0.255
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
```

Troubleshooting and Debugging

For detailed troubleshooting for the DMVPN, refer to the following guide:
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a008014bcd7.shtml.

These **show** commands check the status of the cryptography tunnels:

- **show crypto engine connection active:** Displays the total encrypts and decrypts per security association
- **show crypto ipsec sa:** Displays the statistics on the active tunnels
- **show crypto isakmp sa:** Displays the state for the Internet Security Association and Key Management Protocol (ISAKMP) security association

These **debug** commands debug cryptography setup:

- **debug crypto ipsec:** Displays IPsec events
- **debug crypto isakmp:** Displays messages about Internet Key Exchange (IKE) events
- **debug crypto engine:** Displays information from the cryptography engine

For the Next Hop Resolution Protocol (NHRP), these **show** commands check the status:

- **show ip nhrp dynamic:** Shows dynamic spoke-to-spoke tunnels
- **show ip nhrp static:** Shows the static tunnels between the hub and spokes
- **show ip nhrp detail:** Shows the details around the NHRP protocol status
- **show ip nhrp summary:** Shows the brief details about the NHRP protocol current state

To debug the NHRP, use these **debug** commands:

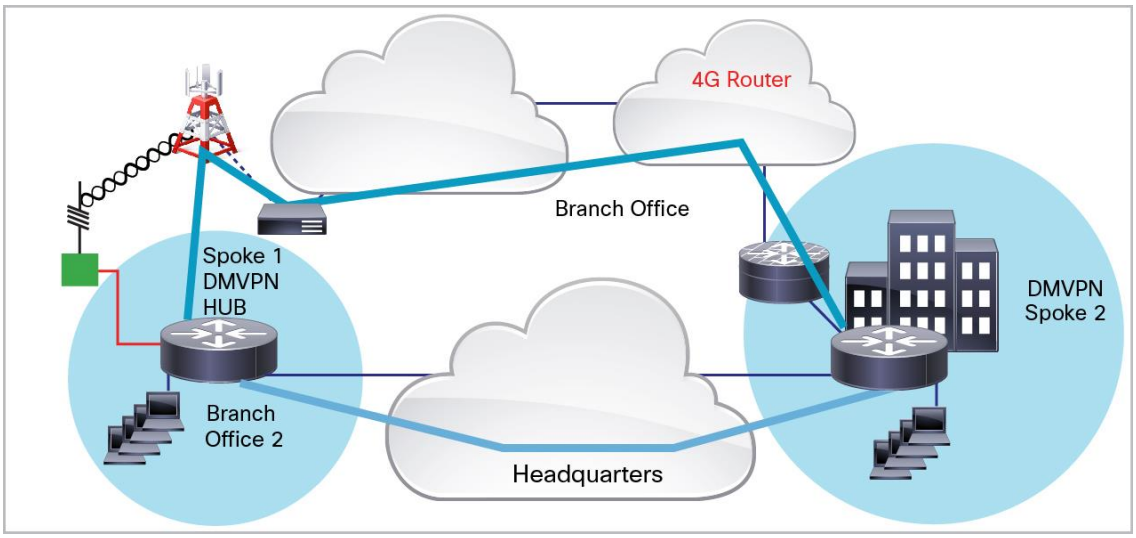
- **debug nhrp?**
  - attribute NHRP attribute
  - cache NHRP cache operations
  - condition NHRP conditional debugging
  - error NHRP errors
  - extension NHRP extension processing
  - group NHRP groups
  - packet NHRP activity
  - rate NHRP rate limiting
  - routing NHRP routing

7. Site-to-Site IPsec VPN

The enterprise world is a mix of different industries with their unique requirements. The goal of the enterprise network is to transfer information reliably and securely between two or more endpoints. This section discusses commonly deployed methods in enterprise networks to achieve this goal. Most enterprise networks use common features such as encryption, tunneling, dynamic routing, and policy-based routing. Depending on the scale and manageability of an enterprise network, different techniques and methods are used to design the enterprise networks.

Most enterprises use some type of encryption when they pass information across the WAN between sites. The simplest deployment is site-to-site IPsec to encrypt information between two routers. Figure 7 shows the site-to-site IPsec connectivity between the branch office and the central office. The branch-office router has DSL as a wired primary connection and 4G LTE as a backup WAN. The site-to-site IPsec is configured over both WAN transports. Object tracking is used to achieve primary-to-backup failover.

Figure 7. Network Topology for Site to IPsec over 4G as Backup



Configuration of Branch-Office Router

```
!
ip dhcp excluded-address 10.4.0.254
!
ip dhcp pool lte
   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
!
chat-script lte "" "AT!CALL1" TIMEOUT 20 "OK"
!
track 234 ip sla 1 rechability
```

```
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
!
!defines the IKE policy (with priority 1), specifies 3DES during IKE negotiation,
and
!authentication as pre-shared, using pre-defined keys. The values for lifetime
(set to
!86,400 sec – one day), group (set to 768 bit Diffie-Hellman), and Hash (set to
SHA-1)
!are set to their default values.
!
!
crypto isakmp key mykey address 20.20.241.234
!
!defines the key (mykey) and the IP address of the gateway
! (IPsec peer) with which the Security Association will be set
!
crypto ipsec transform-set mytransformset ah-sha-hmac esp-3des
!
!defines the transform set (mytransformset), which is an acceptable combination
of
!security protocols, algorithms, and other settings to apply to IPsec-protected
!traffic.
!
crypto map lte 10 ipsec-isakmp
 set peer 20.20.241.234
 set transform-set mytransformset
 match address 101

!defines the crypto map lte
!crypto map specifies the traffic to be protected (using match address !<access-
list> !command); the peer end-point to be used, and the !transform set to use
!(mytransformset, defined earlier).
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/1/0
 switchport access vlan 104
```

```
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
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 Cellular0/3/0
 ip address negotiated
 ip nat outside
 encapsulation slip
 !Starting with HSPA+7 and LTE, encapsulation is changed from PPP to SLIP
 dialer in-band
 dialer string lte
 dialer-group 1
 async mode interactive
 crypto map lte
!
interface Vlan104
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
!
interface Dialer2
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap hostname <hostname>
 ppp chap password 0 <password>
 ppp pap sent-username <username> password 0 <password>
```

```
 ppp ipcp dns request
 crypto map lte
!
!applies crypto map lte, defined above, on this primary interface
!
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 Cellular0/3/0 254
!
ip nat inside source route-map nat2cell interface Cellular0/3/0 overload
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
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 101 permit ip 10.4.0.0 0.0.255.255 10.10.0.0 0.0.255.255
!
!ACL to identify the traffic for IPsec tunnel, as defined under crypto map lte.
!10.4.x.x is local subnet and 10.10.x.x is far-end subnet
!
access-list 102 permit icmp any host 209.131.36.158
!
access-list 103 permit ip 10.4.0.0 0.0.255 any
!
dialer-list 1 protocol ip permit
!
dialer-list 2 protocol ip permit
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2 null0
!
route-map nat2dsl permit 10
 match ip address 103
```

```
 match interface Dialer2
!
route-map nat2cell permit 10
 match ip address 103
 match interface Cellular0/3/0
!
event manager applet pri_back
 event track 234 state any
 action 2.0 cli command "clear ip nat trans forced"
!
control-plane
!
line 0/3/0
 exec-timeout 0 0
 script dialer lte
 login
 modem InOut
```

Configuration of Headquarters Router

```
hostname gateway-router
!
ip dhcp excluded-address 10.10.0.254
ip dhcp excluded-address 10.10.0.1
!
ip dhcp pool 10
   network 10.10.0.0 255.255.0.0
   default-router 10.10.0.254
!
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 myset ah-sha-hmac esp-3des
!
crypto dynamic-map gw_map 10
 description IPsec tunnel to DSL/Cellular at remote branch-router
```

```
 set transform-set myset
 match address 101
!
crypto map gateway 10 ipsec-isakmp dynamic gw_map
!
!defines the gateway map for IPsec tunnels to the ATM DSL/ and Cellular
!interface at the remote branch-router.
!
!
interface GigabitEthernet0/0
 ip address 20.20.241.234 255.255.255.252
 crypto map gateway
!
!Physical interface on which the crypto map is applied. The interface through
which
!the above IPsec tunnels are established
!
!
interface FastEthernet0/1/0
 switchport access vlan 10
!
!Fast Ethernet ports on which the VPN hosts (10.10.0.0 subnet) are connected.
!
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
!
!VLAN for the VPN hosts (on the 10.10.0.0 network)
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
access-list 101 permit ip 10.10.0.0 0.0.255.255 10.4.0.0 0.0.255.255
!
!access list defining the traffic for IPsec tunnel
!
```

Troubleshooting and Debugging

For details about the IPsec technology, refer to the IPsec guide at: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/16439-IPSECpart8.html.

These commands check the status of the IPsec connection:

- **show crypto ipsec sa:** Shows the phase 2 security associations
- **show crypto isakmp sa:** Shows the phase 1 security associations

These commands debug the IPsec connection:

- **debug crypto ipsec:** Shows the IPsec negotiations of phase 2
- **debug crypto isakmp:** Shows the ISAKMP negotiations of phase 1
- **debug crypto engine:** Shows the traffic that is encrypted
- **clear crypto isakmp:** Clears the security associations related to phase 1
- **clear crypto sa:** Clears the security associations related to phase 2

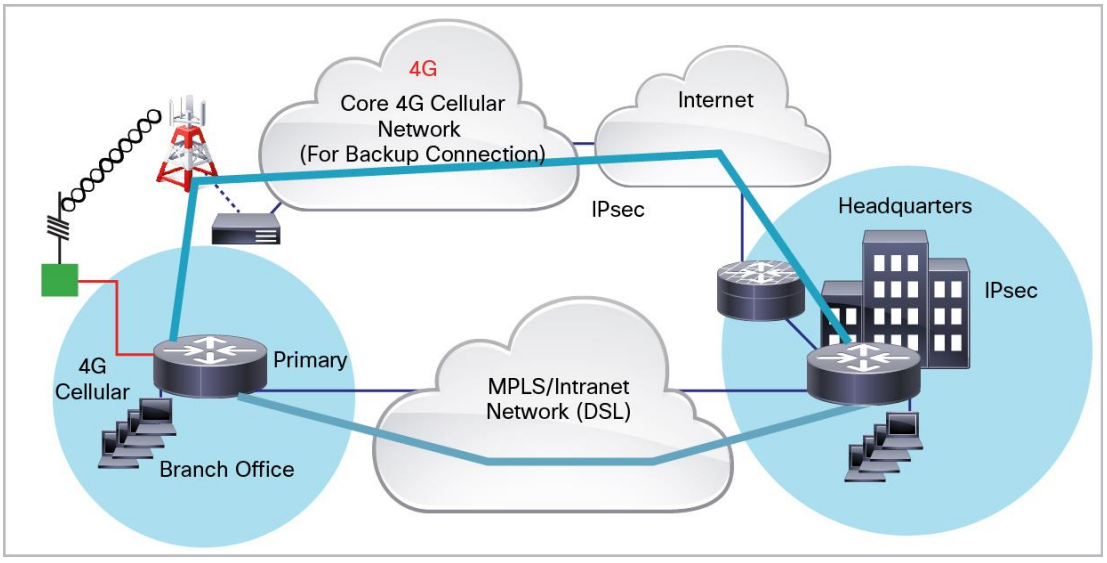
8. Site-to-Site IPsec with GRE for Dynamic Routing

Most enterprise deployments need end-to-end rechability using their private IP addresses that are given to end devices in the branch and central offices. The IP reachability of such a network is managed with the dynamic routing protocols such as OSPF and EIGRP. These branch and central offices are connected using the Internet backbone through the service provider network, so tunnels are used to carry the private IP address packets across the public network. In smaller deployments with fewer branch offices and one central office, it is easier to deploy GRE tunnels and site-to-site IPsec encryption. GRE tunnels allow use of dynamic routing protocols, and IPsec helps ensure that the data is encrypted and securely delivered to intended endpoints.

This section provides the details for deployment of 4G as a backup to the primary WAN connection over a DSL link. Object tracking is used to manage primary backup failover. Figure 8 shows the network topology of the GRE based IPSec solution with dynamic routing. The GRE tunnel is configured over the primary DSL and backup 4G connection. Site-to-site IPsec is used to encrypt the enterprise traffic through GRE tunnels. OSPF is used as a dynamic routing protocol to maintain Layer 3 convergence among the private IP subnets behind the branch and central offices. The configuration is followed by commands to verify if the deployment is working as expected. Troubleshooting tips are provided to debug if the connectivity is not working as expected.

Note: For the point-to-point static GRE tunnel to work, you must subscribe to a service with a publicly routable static IP address on the cellular interface. Normal 4G LTE connections are provided with a dynamic private IP address, which cannot be used for the point-to-point static GRE tunnels. Cellular service providers provide static IP addresses on 4G LTE interfaces as a separate service.

Figure 8. Network Topology for Dynamic Tunneling Using GRE with IPsec Over 4G as Backup



Configuration of Branch-Office Router

```
hostname branch-router
!
ip dhcp excluded-address 10.4.0.254
!
ip dhcp pool lte
   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
!
chat-script lte "" "AT!CALL1" TIMEOUT 20 "OK"
!
track 234 ip sla 1 rechability
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
!
crypto isakmp key mykey address 20.20.241.234
!
crypto ipsec transform-set mytransformset ah-sha-hmac esp-3des
mode transport
!transport mode encrypts only the payload and avoids IPinIP tunnel over GRE
tunnel
crypto map lte 10 ipsec-isakmp
 set peer 20.20.241.234
 set transform-set mytransformset
 match address gre-traffic
!
interface Tunnel1
 ip unnumbered vlan104
 ip mtu 1400
 tunnel source Dialer2
 tunnel destination 20.20.241.234
!
!GRE over primary (DSL)
!
interface Tunnel2
 ip ospf demand-circuit
```

```
 ip unnumbered vlan104
 ip mtu 1400
 tunnel source Cellular0/3/0
 tunnel destination 20.20.241.234
!
!GRE over backup (cellular)
!
interface FastEthernet0/1/0
 switchport access vlan 104
!
interface ATM0/0/0
 no ip address
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0/0/0.1 point-to-point
 ip nat outside
 ip virtual-reassembly
 pvc 0/35
 pppoe-client dial-pool-number 2
!
!
interface Cellular0/3/0
 ip address negotiated
 ip nat outside
 encapsulation slip
 !Starting with HSPA+7 and LTE, encapsulation is changed from PPP to SLIP
 dialer in-band
 dialer string lte
 dialer-group 1
 async mode interactive
 crypto map lte
!
!applies crypto map lte, defined above, on this backup interface.
!
interface Vlan104
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
!
interface Dialer2
```

```
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap hostname <hostname>
 ppp chap password 0 <password>
 ppp pap sent-username <username> password 0 <password>
 ppp ipcp dns request
 crypto map lte
!
!Applies crypto map on the primary interface
!
router ospf 11
log-adjacency-changes
network 10.4.0.0 0.0.0.255 area 0
!
!VPN network 10.4.0.0 (of which Tunnel1/Tunnel2 are part) is part of OSPF area 0
!OSPF Hello will be sent across to branch-router via these tunnels
!
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 Cellular0/3/0 254
!
ip nat inside source route-map nat2cell interface Cellular0/3/0 overload
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
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-traffic' access-list to identify traffic to encapsulate in IPSEC
!
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 101 permit ip 10.4.0.0 0.0.255.255 any
!
access-list 102 permit icmp any host 209.131.36.158
!
dialer-list 1 protocol ip permit
!
dialer-list 2 protocol ip permit
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2 null0
!
route-map nat2dsl permit 10
 match ip address 101
 match interface Dialer2
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0/3/0
!
event manager applet pri_back
 event track 234 state any
 action 2.0 cli command "clear ip nat trans forced"
!
control-plane
!
line 0/3/0
 exec-timeout 0 0
 script dialer lte
 modem InOut
```

Configuration of Central-Office Router

```
!
hostname gateway-router
!
ip dhcp excluded-address 10.10.0.254
ip dhcp excluded-address 10.10.0.1
!
!
ip dhcp pool 10
   network 10.10.0.0 255.255.0.0
   default-router 10.10.0.254
!
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 gateway 10 ipsec-isakmp dynamic gre_tunnel2

crypto map gateway 20 ipsec-isakmp dynamic gre_tunnel21
!
!defines the gateway map for tunnels to the ATM DSL interface (Tunnel2) and
!Cellular interface (Tunnel21) at the remote branch-router.
!
!
```

```
interface Tunnel2
 ip unnumbered Vlan10
 ip mtu 1400
 tunnel source GigabitEthernet0/0
 tunnel destination 75.40.113.246
!
!Tunnel to the ATM DSL interface on the remote branch-router.
!
interface Tunnel21
 ip unnumbered Vlan10
 ip mtu 1400
 tunnel source GigabitEthernet0/0
 tunnel destination 166.138.186.119
!
!Tunnel to the Cellular interface on the remote branch-router.
!
interface GigabitEthernet0/0
 ip address 20.20.241.234 255.255.255.252
 load-interval 30
 crypto map gateway
!
!Physical interface on which the crypto map is applied.
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
!Fast Ethernet ports on which the VPN hosts (on the 10.10.0.0 network) are
connected.
!
interface Vlan10
 ip address 10.10.0.254 255.255.0.0
!
!VLAN for the VPN hosts (on the 10.10.0.0 network)
!
```

```
router ospf 10
 log-adjacency-changes
 network 10.10.0.0 0.0.0.255 area 0
!
!VPN network 10.10.0.0 (of which Tunnel2/Tunnel21 are part) is part of OSPF
area 0
!OSPF Hello will be sent across to branch-router via these tunnels
!
ip access-list extended gre-tunnel2
 permit gre host 20.20.241.234 host 75.40.113.246
!
!access list defining the traffic that will be protected via IPsec. This is the
!traffic sent to the DSL interface at the remote end.
!
ip access-list extended gre-tunnel21
 permit gre host 20.20.241.234 host 166.138.186.119
!
!access list defining the traffic that will be protected via IPsec. This is the
!traffic sent to the Cellular interface at the remote end.
!
```

Troubleshooting and Debugging

For details about the GRE tunnels and dynamic IP routing, refer to the following guide: http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/9221-quicktip.html.

For IPsec troubleshooting, refer to Section 7, Site-to-Site IPsec VPN.

For dynamic routing using OSPF, refer to the Cisco technology page for OSPF: http://www.cisco.com/c/en/us/tech/ip/open-shortest-path-first-ospf/index.html.

These commands check the current status:

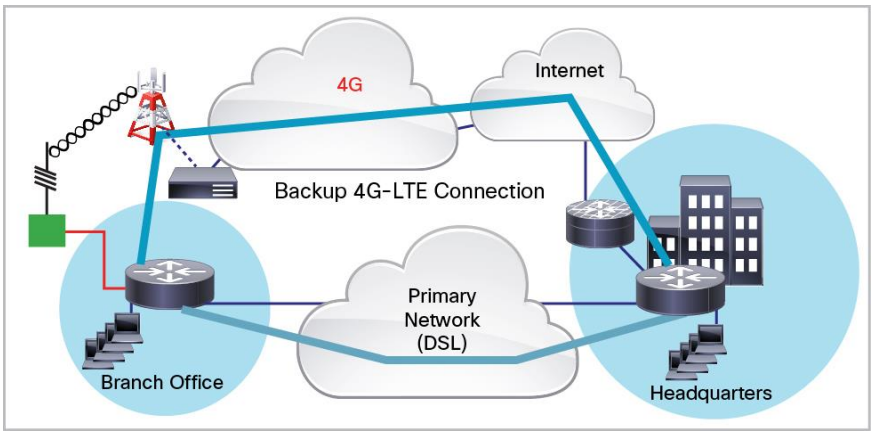
- **show interface tunnel <number>**
- **debug tunnel:** Enables the debugging for tunnel-related events
- **show ip interface brief:** Checks to make sure that all the relevant interfaces such as cellular and tunnel are operational and have appropriate IP address
- **show ip route:** Checks to make sure that the dynamic routing protocol (OSPF) has populated routing entries learned through the routing process; the OSPF entries start with “o” in the routing table
- **Show ip ospf database:** To check the status of OSPF protocol related information
- **debug ip ospf commands:** To troubleshoot if OSPF is converging the routing topology on the branch or HQ side

9. Cisco Easy VPN over 4G LTE

In a small setup with very few branch offices and one central office, a dynamic routing protocol is not needed. The IPsec tunnels can carry private traffic with policies based on an access control list (ACL) and reverse route injection. Cisco Easy VPN makes such deployment very simple to deploy and manage with minimal configuration on the branch-office side. Figure 9 below shows the network topology of such deployment. Cisco Easy VPN makes it very simple for the network administrator to manage the network deployment.

This section discusses how to set up the Cisco Easy VPN server at the central office and how to set up a branch office with a primary wired connection over a DSL and 4G LTE backup connection. The branch-office router initiates the Easy VPN tunnel on the current working WAN interface.

Figure 9. Cisco Easy VPN Topology with DSL as Primary and 4G LTE as Backup WAN



Configuration of Branch-Office Router

```
!
ip dhcp excluded-address 10.13.0.254
!
ip dhcp pool lte
   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 lte "" "AT!CALL1" TIMEOUT 20 "OK"
!
username sachin@cisco.com password 0 lab
!
!Local username and password for authentication for EzVPN client.
!
track 234 ip sla 1 rechability
```

```
!
crypto ipsec client ezvpn hw-client-pri
 connect auto
 group hw-client-group key cisco123
 backup hw-client track 234
 mode network-extension
 peer 20.20.248.243
 username cisco123@cisco.com password lab
 xauth userid mode local
!
!Ezvpn client configuration for Primary WAN interface. Uses track 234 to failover
to !backup when backup wan is being used
!
!
crypto ipsec client ezvpn hw-client
 connect auto
 group hw-client-group key cisco123
 mode network-extension
 peer 20.20.248.243
 username sachin@cisco.com password lab
 xauth userid mode local
!
!Ezvpn client configuration for Backup WAN interface
!
interface FastEthernet0/1/0
 switchport access vlan 104
!
!Fast Ethernet ports used by DHCP Client hosts
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
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
 ip address negotiated
 ip nat outside
 encapsulation slip
 !Starting with HSPA+7 and LTE, encapsulation is changed from PPP to SLIP
 dialer in-band
 dialer string lte
 dialer-group 1
 async mode interactive
 crypto ipsec client ezvpn hw-client
!
!defines the outside EzVPN interface for primary WAN
!
interface Vlan104
 ip address 10.13.0.254 255.255.0.0
 ip nat inside
 crypto ipsec client ezvpn hw-client-pri inside
 crypto ipsec client ezvpn hw-client inside
!
!defines VLAN 104 for the hosts connected on the Fast Ethernet switched ports
!hosts connecting to switched ports are local vpn clients
!
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
!
!defines the outside EzVPN interface for primary WAN
!External dialer interface to associate with the cellular interface
!crypto ipsec client ezvpn hw-client defined above, on this backup interface.
This
```

```
!ensures that this is external interface for ezvpn for encryption
!
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 cellular 0/1/0 253
!
access-list 102 permit icmp any host 209.131.36.158
!
dialer-list 1 protocol ip permit
!
dialer-list 2 protocol ip permit
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2 null0
!
line 0/1/0
 script dialer lte
 modem InOut
```

Configuration on a Cisco Easy VPN Hub Gateway

```
hostname ezvpn_gw
!
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
!
!Easy VPN server side configuration. ACL 111 defines the allowed traffic to be
encrypted
!from the ezvpn client and is negotiated during IPsec tunnel setup
!
interface GigabitEthernet0/0
 ip address 128.107.248.243 255.255.255.224
 ip nat outside
 crypto map dynmap
!
!Crypto map is applied on the WAN interface of the server.
!
interface GigabitEthernet0/1
 ip address 10.11.0.1 255.255.255.0
 ip nat inside
!
ip local pool dynpool 10.11.0.50 10.11.0.100
!
!Define the local pool to give IP address to the remote ezvpn clients
!
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 101 permit ip 13.1.1.0 0.0.0.255 any
access-list 111 permit ip 10.11.0.0 0.0.0.255 10.13.0.0 0.0.0.255
!
```

```
!Defines interesting traffic that should be allowed to be encrypted for the ezvpn
!remote clients. The counterpart of such acl is communicated to the ezvpn remote
!client for encryption and NAT
!
```

Troubleshooting the Cisco Easy VPN Setup

For details about the Cisco Easy VPN technology and deployment details, refer to the configuration guide: http://www.cisco.com/en/US/partner/tech/tk583/tk372/technologies_configuration_example09186a0080808395.shtml.

These commands check the status of the Easy VPN setup:

- **show crypto ipsec sa**
- **show crypto isakmp sa**
- **show crypto ipsec client ezvpn**

In addition to common cryptography debugs in section 7, this **debug** command can be used:

- **debug crypto ipsec client ezvpn**

10. Mobile IP Enterprise-Managed Deployments

4G LTE brings mobility to enterprise deployments. It provides rapid deployment of the network to serve enterprise-class data needs in areas where no wired infrastructure exists. Such areas are construction sites and temporary deployments such as kiosks at events. All such requirements need a mechanism that quickly reacts to changes in topology as well as having the lowest overhead possible. Mobile IP is designed to serve such situations, and it is much more resilient to change in WAN access such as make/break of connection and change in connection point while mobile. Mobile IP is also designed to use the bandwidth optimally while providing the dynamic routing capabilities without the use of dynamic routing protocols. Mobile IP makes the end deployment simple to deploy and manage.

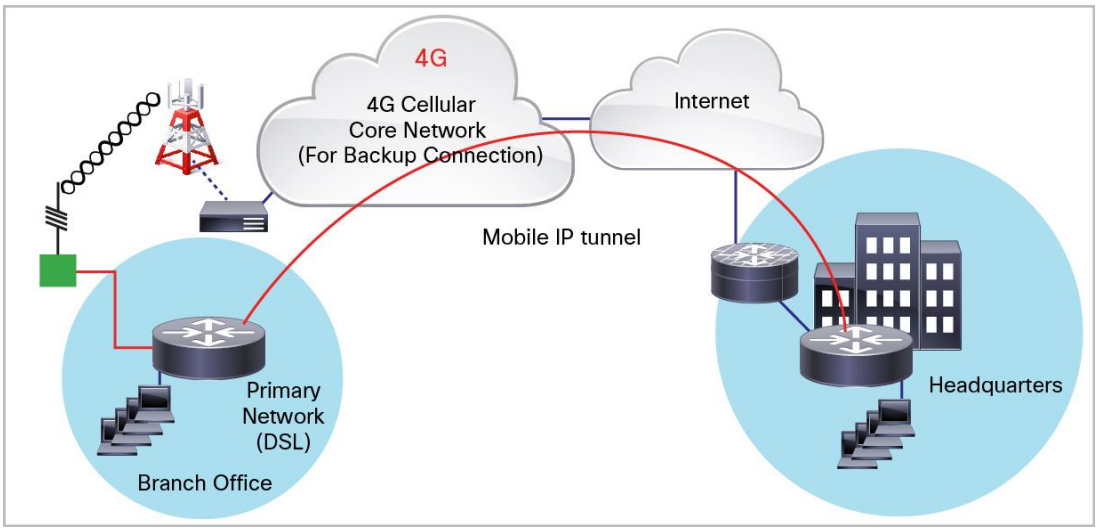
Figure 10 shows the Mobile IP baed topology for enterprise deployments. Mobile IP involves the home agent and mobile router. The home agent is an anchor point for all branch-office routers. All the branch-office routers act as mobile routers and set up their Mobile IP tunnel to the home agent. The mobile router uses the Mobile IP tunnel as a default route and informs the home agent about the private subnets connected to it on the LAN side as part of the Mobile IP registration and Mobile IP tunnel setup. The home agent internally distributes this information in the central-office network. This central-office network is called the home network, and it performs routing between the endpoints that are connected to the mobile router and the central-office endpoints without the need for any additional routing protocols over the 4G LTE WAN.

Mobile IP can have two types of deployments: service provider-managed and enterprise-managed. In a service provider-managed connection, the service provider hosts the home agent in its core networks. This deployment has an advantage in that the service provider can bridge the MPLS network and the 4G LTE connection by making the home agent a service provider edge router on the MPLS side. In the enterprise-managed scenario, the home agent is hosted by the enterprise. The advantage of this solution is that the enterprise has full control over the Mobile IP tunnel and can use multiple service provider connections across different branch offices to connect back to the enterprise network.

This section provides the configurations on the branch-office router as the mobile router and central-office router as the home agent.

Note: For enterprise-managed Mobile IP to work, you must subscribe to a service with a static IP address on the cellular interface. Normal 4G LTE connections are provided with a dynamic private IP address, which cannot be used for the mobile node association on the home agent side in enterprise headquarters. Cellular service providers provide static IP addresses on 4G LTE interfaces as a separate service.

Figure 10. Mobile IP Topology with 4G LTE as Primary WAN



Configuration of Branch-Office Router as Mobile Router

```
!
hostname mobile-router
!
ip dhcp excluded-address 10.13.0.254
!
ip dhcp pool lte
   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 lte "" "AT!CALL1" TIMEOUT 20 "OK"
!
track 234 ip sla 1 rechability
!
interface Loopback100
 ip address 10.100.0.3 255.255.255.0
!
!Static ip address assigned to the mobile router. This address is part of
!the HA-MR subnet
!
interface FastEthernet0/1/0
 switchport access vlan 104
!
!Fast Ethernet ports used by DHCP Client hosts
```

```
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
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 Vlan104
 ip address 10.13.0.254 255.255.0.0
 ip nat inside
!
interface Cellular0/0/0
 ip address negotiated
 ip mobile router-service roam
 ip mobile router-service collocated registration nat traversal
 ip mobile router-service collocated ccoa-only
 encapsulation slip
 !Starting with HSPA+7 and LTE, encapsulation is changed from PPP to SLIP
 dialer in-band
 dialer string lte
 dialer-group 1
 async mode interactive
!
!external dialer interface associated with the cellular with the mobile ip
!ipconfiguration for ccoa-only mobile ip mode
!
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
!
!this commands turns on the mobile ip functionality on the router
!

!
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
!
!This statement defines the encryption details and authentication using !ascii
value. The ascii value must match to that of the HA configuration on !the HQ side
router
!
ip mobile registration-lifetime 1800
ip mobile router
 address 10.100.0.3 255.255.255.0
 collocated single-tunnel
 home-agent 20.20.248.243
 mobile-network GigabitEthernet0/1
 register retransmit initial 5000 maximum 10000 retry 5
 reverse-tunnel
!
!Address defines the Mobile router static ip address defined on the loopback !100
!Home agent address is defined so the router knows who to initiate the
!mobile ip request to.
!
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 102 permit icmp any host 209.131.36.158
!
dialer-list 1 protocol ip permit
!
dialer-list 2 protocol ip permit
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2 null0
!
line 0/1/0
 script dialer lte
 modem InOut
!
```

Configuration of Headquarters Router as Home Agent

```
hostname HQ-HomeAgent
!
interface Loopback100
 ip address 10.100.0.1 255.255.255.0
!
!Mobile IP Subnet between the Home-agent (HA) and Mobile router (MR)
!
interface GigabitEthernet0/0
 ip address 20.20.248.243 255.255.255.224
 ip nat outside
!
!This is the WAN interface connecting to Mobile routers over internet
!
interface GigabitEthernet0/1
 ip address 10.11.0.1 255.255.255.0
 ip nat inside
!
router mobile
!
!Enable mobile ip on HA router
```

```
!
ip nat inside source list 101 interface GigabitEthernet0/0 overload
!
ip route 0.0.0.0 0.0.0.0 20.20.248.254
!
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
!
!Home agent configuration
!
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
!
!Mobile router entry for registration
!
ip mobile secure host 10.100.0.3 spi decimal 1003 key ascii 1234567891234563
algorithm md5 mode prefix-suffix
ip mobile registration-lifetime 1800
!
!Mobile router authentication (same ascii configured as that on the MR) and
encryption !details for secure communication
!
access-list 101 permit ip 13.1.1.0 0.0.0.255 any
!
```

Troubleshooting the Mobile IP Setup

For details about Mobile IP technology and configuration, refer to the following white paper: http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfmobip.html.

For detailed troubleshooting of Mobile IP, refer to the guide at: http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfmobip.html#wp1001065.

These **show** commands verify that the Mobile IP is working on the ISR:

- **show ip mobile router:** Displays the parameters and status that are related to Mobile IP
- **show ip mobile router agent:** Displays the Mobile IP binding with local IP address and other Layer 3 details of the interface being used to set up the Mobile IP tunnel
- **show ip mobile interface:** Shows the Layer 2 interface-level details of the interface being used to set up Mobile IP tunnel

- **show ip mobile binding:** A command on the home-agent side that shows the connected mobile routers and other binding-level details for each mobile router

These **debug** commands help to troubleshoot if the Mobile IP tunnel is not establishing or not working as expected:

- **debug ip mobile advertise**
- **debug ip mobile router**
- **debug ip mobile router registration**
- **debug ip mobile host** - on the home-agent side

For more details about troubleshooting, refer to this guide:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfmobip.html#wp1001065.

11. WAN Optimization over 4G LTE

Cellular WAN connections such as 4G LTE or 3G are shared medium. Many users contend for the same maximum bandwidth that is offered by the service cell tower. The ability to efficiently transmit data depends heavily on the radio conditions. These radio conditions are affected by the signal strength, surrounding objects that block the signal, and other nearby radio sources that cause interference. The packet loss is quite normal over a radio link. The recovery mechanism for such bits and bytes puts further strain on useful data throughput for end users. These conditions significantly affect the end-user experience for the cellular as a WAN connection.

As a result, enterprise deployments face these challenges:

- Varying latency: Latency for a packet varies by the packet size as well as signal conditions.
- Varying bandwidth: The shared medium, unpredictable interference, and radio-link retransmissions cause significant fluctuation in meaningful bandwidth.
- Cost: Unlike wired WAN such as DSL/Cable/T1s, cellular WAN have higher per-usage charges beyond a included monthly data-caps. This could prove costly depending on the service contract with the SP.

To overcome these challenges, Cisco has designed Cisco Wide Area Application Services (WAAS). These services improve the application experience by optimizing the existing WAN link. The Cisco WAAS techniques follow:

- TCP flow optimization: This technique improves the overall TCP transactions by eliminating the inherent efficiencies around TCP window, back-off mechanism, etc.
- Data redundancy elimination (DRE): DRE allows the routers to avoid repeating certain traffic by using caching and forwarding the pointers to cached data instead of the data itself. It reduces the sheer number of bits sent over the WAN while achieving the same goal of information exchanged.

- Compression: By nature, the data being exchanged is highly compressible using the advanced compression algorithm. The router takes the burden and latency of the compression from the end-user applications and applies that just before it sends the packet, thereby reducing the payload that must be sent. Compression results in fewer bytes exchanged and faster response to applications that are waiting for data.
- Application optimization: The application-optimization technique takes advantage of how certain applications behave. The algorithm uses several factors to improve the application performance, such as perfecting, anticipation, caches, and many more. Application optimization benefits popular applications such as email messaging, web browsing, and data transfer (FTP).

The combination of Cisco WAAS and 4G LTE yields these benefits:

- Lower WAN expenses: When the amount of data that is transferred over the radio is reduced, the associated bill from the service provider is reduced significantly.
- Improved application performance: The end-user applications run much faster and overall user experience is better, resulting in improved productivity and better return on investment (ROI).
- Enable more services: Do more with less. Cisco WAAS allows the enterprise to deploy more services for a given WAN than it could without it. The WAN bandwidth and latency are managed efficiently to support more applications and services per router.

For more details about Cisco WAAS, refer to the technology homepage: http://www.cisco.com/en/US/products/ps5680/Products_Sub_Category_Home.html.

12. Quality of Service

3GPP standards have created an end-to-end QoS architecture for the 4G LTE network. This architecture allows the cellular service provider to enforce QoS over the radio interface and in the cellular core. You can use this mechanism to guarantee certain bandwidth to an end user even if the radio is a shared medium. This architecture also enables the service provider to prioritize certain types of user traffic over the rest. Such a mechanism requires support from a mobile node such as the Cisco 4G LTE interface as well as the core elements of the service provider network, such as packet gateway and Policy and Charging Rules Function (PCRF).

The Cisco hardware is designed to take advantage of such service whenever service providers offer it. Cisco works closely with the service provider to put this end-to-end architecture in place so that customers can use it for their enterprise-class services without compromising the VPNs and encryption mechanisms. Cisco provides the packet gateway in the core and the ISR in the branch office; Cisco provides equipment on both sides to achieve such a complicated solution.

Cisco IOS Software has a rich set of hierarchical QoS (HQoS) services. You can use HQoS in conjunction with the end-to-end LTE QoS. You can use the Cisco IOS Software-based classic HQoS to maintain queues and prioritized traffic before passing it on to the LTE interface. The LTE interface then uses the network-enforced QoS after the traffic leaves the router. In this way, the Cisco HQoS augments the LTE end-to-end QoS designed by the 3GPP standards.

For Cisco HQoS configuration, refer to the technology homepage for Cisco QoS: http://www.cisco.com/en/US/products/ps6558/products_ios_technology_home.html.

Use Case

Cisco IOS QoS provides a solution for taking charge of the available bandwidth and managing it efficiently to meet application demands. Mechanisms such as Class-Based Weighted Fair Queuing (CBWFQ) and Low Latency Queuing allow the most efficient distribution of the available bandwidth among the applications. A mechanism such as Weighted Random Early Detection (WRED) puts control in the user's hand to decide what to drop when congestion occurs. A shaping mechanism allows the user to adapt to the available bandwidth of a given WAN interface and avoid unnecessary congestion.

A classic example is prioritizing voice over data using Low Latency Queuing. Typical enterprises use three to four queues: Low Latency Queuing, high priority, low priority, and default. The Low Latency Queuing Protocol is for real-time traffic with voice or other critical traffic, such as financial updates. The high-priority traffic consists of the business-critical applications, and low-priority traffic consists of other business applications. The default traffic is the catch-all for best-effort traffic.

13. Using Multiple 4G LTE Interfaces for Load-Sharing and Balancing

4G LTE is a Layer 3 wireless WAN connection. Every 4G LTE connection is considered as a Layer 3 point-to-point connection from the mobile node (ISR) to the packet gateway in the service provider core. Because of the mobile architecture, the two cellular interfaces from the same service provider cannot be bonded at the radio level in a similar way as the Multilink PPP.

Cisco IOS Software has a rich feature set that allows it to use two simultaneous Layer 3 WAN connections to do the load balancing of the existing traffic load in a branch office. The Cisco ISR can use the Cisco IOS Policy-Based Routing (PBR) mechanism to send traffic across two different WAN interfaces. Cisco IOS Software has the Cisco Performance Routing (Cisco PfR) feature, which allows the enterprise to deploy a network where the routers can dynamically decide the most efficient way to use multiple WAN interfaces on a branch office to send traffic across to the headquarters.

For more details about Cisco PfR, refer to the Cisco PfR technology page: http://www.cisco.com/c/en/us/products/ios-nx-os-software/performance-routing-pfr/index.html.

14. Glossary

3G	Third-generation technology in the context of q mobile phone. The services associated with 3G include wide-area wireless voice telephony and broadband wireless data, all in a mobile environment
3GPP	Third-Generation Partnership Project
3GPP2	Third-Generation Partnership Project 2
4G	Fourth-generation technology in the context of a mobile phone or cellular network; typically, the LTE is considered a 4G technology
4G LTE	Fourth-generation long-term evolution
ACL	Access control list
APN	Access-point name
CBWFQ	Class-Based Weighted Fair Queuing
CDMA	Code Division Multiple Access
CDMA2000	A hybrid 2.5G/3G protocol of mobile telecommunications standards that uses CDMA, a multiple access scheme for digital radio, to send voice, data, and signaling data (such as a dialed telephone number) between mobile phones and cell sites; CDMA2000 is considered a 2.5G protocol in 1xRTT and a 3G protocol in EVDO
Cisco PfR	Cisco Performance Routing
DMVPN	Dynamic Multipoint Virtual Private Network
DRE	Data redundancy elimination
EDGE	Enhanced Data Rates for GSM Evolution or Enhanced GPRS (EGPRS)
EHWIC	Enhanced high-speed WAN interface card
EPS	Evolved packet system
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
EVDO	Evolution-Data Optimized or Evolution-Data Only
GSM	Global System for Mobile Communications
HQoS	Hierarchical quality of service
HSDPA	High-speed downlink packet access (sometimes known as high-speed downlink protocol access)
HSPA	High-speed packet access
HSUPA	High-speed uplink packet access
HWIC	High-speed WAN interface card
IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISR G2	Integrated Services Routers Generation 2
LTE	Long-term evolution
MIMO	multiple-input multiple-output
MQC	Modular QoS CLI
NHRP	Next Hop Resolution Protocol
OFDMA	Orthogonal Frequency Division Multiple Access
OSPF	Open Shortest Path First
PAT	Port Address Translation
PBR	Policy-Based Routing
QoS	Quality of service
RAN	Radio access network
RSSI	Received Signal Strength Indicator
SAE	System architecture evolution
SIM	Subscriber identity module

UMTS	Universal Mobile Telecommunications Service, one of the 3G mobile phone technologies
WAAS	Wide Area Application Services
WRED	Weighted Random Early Detection
WWAN	Wireless WAN

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.

Printed in USA C07-731484-00 05/14