

# Verizon Wireless Dynamic Mobile Network Routing LTE - Cisco Integrated Services Router (ISR G2) and Connected Grid Router

Mobile Router Configuration Guide - Group Encrypted  
Transport VPN – Primary Access 3G/4G

Revision 3.5

---

## Introduction

Group Encrypted Transport VPN (GETVPN) is a tunnel-less technology that provides end-to-end security for voice, video, and data in a native mode for a full meshed network. Group Encrypted Transport VPN expands the standard IP Security (IPsec) with the concept of trusted group members to provide secure any-to-any communication over a variety of network infrastructures. The main benefits over existing VPN solutions include:

- Large-scale any-to-any encrypted communications
- Native routing without tunnel overlay
- Transport agnostic:
  - Private WAN and LAN
  - Frame Relay
  - Multiprotocol Label Switching (MPLS)
  - Third and Fourth-generation (3G and 4G) with Verizon Wireless Dynamic Mobile Network Routing (DMNR)
- Centralized management of policies and keys in the key server

The immediate and long-term benefits of implementing Group Encrypted Transport VPN include:

- Minimal configuration of crypto endpoints
  - All devices, with the exception of key servers, share the same configuration; thus there is less chance of making mistakes. There is no peer configuration or crypto access control lists (ACLs).
- Native routing
  - No modifications are required to the existing routing protocol configuration.
- No tunnel overlay
  - No additional complexity of generic-routing-encapsulation (GRE) tunnels and Next Hop Resolution Protocol (NHRP) as in the case of Dynamic Multipoint VPN (DMVPN). There are no secondary routing protocols over the tunnels.
- Group encryption
  - Group Encrypted Transport VPN minimizes latency because encryption is not performed on a per-link basis, but is encrypted only at the source (ATM or branch office) and decrypted at the destination (headquarters or data center).
- RF usage conservation
  - With only VPN there are no frequent periodic keep-alives. For example, Dead Peer Detection (DPD) and Internet Key Exchange (IKE).
  - Group member (GM) re-registrations are at 3600 seconds and ISAKMP (Internet Security Association and Key Management Protocol) SA lifetime is 24 hours, resulting in a very low RF usage because encryption is used.
- High availability

## Notes

1. The lifetime of the ISAKMP sessions on the key server should be no less than 24 hours.
2. Advanced Encryption Standard (AES) mode is recommended for the Traffic Encryption Key and Key Encryption Key.
3. Use multiple key servers with the co-operative protocol. There should be persistent multiple paths between co-op key servers.
4. If there are multiple key servers, RSA keys should be generated on one of the co-op key servers as exportable and should be imported on all other key servers.
5. The encryption policy should have explicit denies for traffic not requiring encryption followed by global permit statements that are symmetric.
6. On the group member, specify the loopback address that is routed by NEMO as the source of rekey messages with the command **crypto map *crypto-name* local-address Loopback XYZ**.
7. For a key system, it is recommended to always use a loopback interface as the key system IP address for the Group Domain of Interpretation (GDOI) protocol.
8. Fail/open and fail/closed modes are both supported with DMNR.
9. Unicast rekey process is the only rekey method supported.
10. The GDOI crypto map must be applied to the NEMO Tunnel interface using the template method as shown in Figure 1.

## Assumptions and Guidelines

This document assumes the reader has followed the “Verizon Wireless Dynamic Mobile Network Routing - Mobile Router Configuration Guide for Primary Wireless Access” document and DMNR is operating and verified before attempting the tasks outlined herein.

For implementation please consult Cisco for proper customer-premises-equipment (CPE) hardware selection and scalability.

## Hardware Platforms and Software Images

This document is written based on the following software versions and hardware. The following list is not the complete list of platforms supported. Consult Cisco for the required software image.

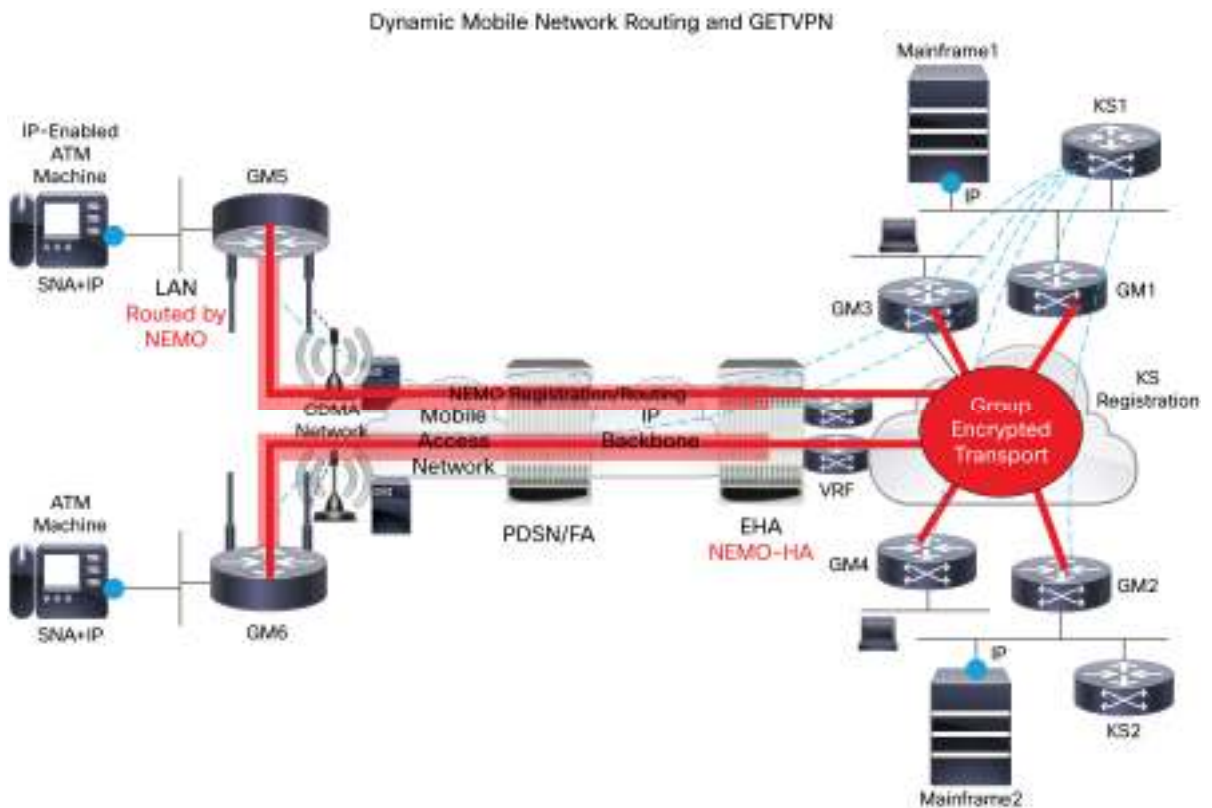
- Key sever: **7206VXR**: 12.4 (22)T ADVIPSERVICESK9-M, **3945**: 15.1(3)T1 Universal K9, **3845**: 15.1(3)T1 ADVIPSERVICESK9-MZ
- MPLS/CE GM:
  - 1900/2900/3900 with LTE eHWIC**: IOS 15.3(3)M2 with security license
  - C819G-4G-V**: IOS 15.3(3)M2 (security license included)
  - CGR2010 with LTE GRWIC**: 15.3(1)T1 with security license
  - 881G with EVDO**: 15.1(1)T universalk9-MZ
  - ASR 1002**: 15.1(1)S2 ADVENTERPRISEk9, **2911**:15.1(2)T3 Universal K9

The Cisco 1941 Integrated Services Router is shown as the LTE/group member example. Many Cisco Integrated Services Routers (ISRs) that can run NEMO and Group Encrypted Transport VPN can be used, but a Cisco IOS®

Software Release 12.4(15)T and later Advanced IP or Cisco IOS Software Release 15.1(3)T (exact) Data and Security license are the minimum required with 3G.

For ISR 1900, 2900, 3900 with LTE eHWIC or C819G-4G-V, the minimum IOS Software release is 15.3(3)M2. For CGR-2010, the minimum IOS release is 15.3(1)T1.

**Figure 1.** Architecture



1. Mobile IP is enabled on the group member.
2. The high-speed WAN interface card (HWIC) or modem registers to The Verizon Enterprise Home Agent (EHA) and obtains a /32 address.
3. Mobile IP registration to EHA is followed by dynamic NEMO GRE Tunnel creation.
4. After registration and authentication to EHA, a dynamic mobile default route (M) is installed with AD 3.

## Implementation:

### Group Member

```
C1941-NEMO-LTE#wr t
Building configuration...
!
! Last configuration change at 15:18:27 UTC Thu Aug 2 2012
version 15.2
service internal
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C1941-NEMO-LTE
!
boot-start-marker
boot system flash:c1900-universalk9-mz.SPA.153-3.M2.bin
boot-end-marker
!
enable password cisco
!
ip dhcp excluded-address 10.21.65.129 10.21.65.136
!
ip dhcp pool mobile
    network 10.21.65.128 255.255.255.128
    default-router 10.21.65.129
    option 150 ip 11.11.11.11
    dns-server 4.2.2.2
!
ip cef
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
chat-script LTE "" "AT!CALL1" TIMEOUT 20 "OK"
!
license udi pid CISCO1941W-A/K9 sn FTX153901PZ
license boot module c1900 technology-package securityk9
license boot module c1900 technology-package datak9
hw-module ism 0
!
controller Cellular 0/0
!
no ip ftp passive
ip ftp source-interface Vlan2
!
!### Define ISAKMP Policy and PSK ###
crypto isakmp policy 10
  encr aes
  authentication pre-share
crypto isakmp key nemo address 0.0.0.0 0.0.0.0 no-xauth
!
!
```

```

##### Define GDOI Group and KS Address ###
crypto gdoi group nemo
  identity number 434
  server address ipv4 10.0.67.1
!
!
##### Define source IP for GETVPN crypto-map. The source MUST be routed by
NEMO ###
crypto map NEMO-GETVPN local-address Loopback100
crypto map NEMO-GETVPN 10 gdoi
  set group nemo
!
!
interface Loopback0
  description ### NEMO Router Home Address . Dummy non-Routable IP ###
  ip address 1.2.3.4 255.255.255.255
!
interface Loopback100
  description ### Loopback Routed by NEMO ###
  ip address 10.0.66.1 255.255.255.255
!
interface Loopback101
  ip address 10.0.66.2 255.255.255.255
!
interface Loopback102
  ip address 10.0.66.3 255.255.255.255
!
##### Define the tunnel template to be able to apply the GETVPN crypto-map to
the dynamic NEMO tunnel ###
interface Tunnel434
  no ip address
  crypto map NEMO-GETVPN
!
interface GigabitEthernet0/0
  no ip address
!
interface GigabitEthernet0/1
  no ip address
!
interface GigabitEthernet0/1/0
  description ### LAN Segment and Subnet Routed by NEMO ###
  switchport access vlan 2
  no keepalive
!
interface GigabitEthernet0/1/1
  switchport access vlan 2
!
interface GigabitEthernet0/1/2
  switchport access vlan 2
!
interface GigabitEthernet0/1/3
  switchport access vlan 2
!
##### Setup cellular interface for NEMO, disable idle timer, assign dialer-
watch group for compulsive dial" ###
interface Cellular0/0/0

```

```

ip address negotiated
no ip unreachable
ip mobile router-service roam
ip mobile router-service collocated ccoa-only
encapsulation slip
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer enable-timeout 6
dialer string LTE
dialer watch-group 1
!
interface Vlan1
  no ip address
!
##### Configure LAN interface: TCP MSS to avoid fragmentation, clear-df for
non-TCP traffic ###
interface Vlan2
  ip address 10.21.65.129 255.255.255.128
  ip tcp adjust-mss 1300
  ip policy route-map clear-df
!
##### Turn on Mobile Routing ###
router mobile
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
##### Define NEMO-HA Security Parameters. Use the appropriate EXGW IP address
based on the geographic location ###
!
ip mobile secure home-agent 66.174.X.Y spi decimal 256 key ascii VzWNeMo
algorithm hmac-md5
!
##### Configure Mobile Router ###
ip mobile router address 1.2.3.4 255.255.255.0
  collocated single-tunnel
  home-agent 66.174.X.Y
  mobile-network Loopback100
  mobile-network Loopback101
  mobile-network Loopback102
  mobile-network Vlan2
  template Tunnel434
  register extend expire 10 retry 3 interval 5
  reverse-tunnel
  tunnel mode gre
!
##### Define dialer watch parameters ###
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
!
route-map clear-df permit 10
  set ip df 0
!

```

---

```
control-plane
!
!
line con 0
  no modem enable
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line 0/0/0
  script dialer LTE
  modem InOut
  no exec
  rxspeed 100000000
  txspeed 50000000
line vty 0 4
  password cisco
  login
  transport input all
!
exception data-corruption buffer truncate
scheduler max-task-time 5000
!
End
```

CGR-2010 with LTE GRWIC is configured similarly to the ISR with LTE eHWIC.

C819G-4G-V is configured similarly to the ISR with LTE eHWIC with these caveats:

- The cell interface is “cellular 0”
- The line interface representing LTE is “line 3”



---

## KEY SERVER

---

Identify the location of the key servers. Provide the key server name and whether the server has a primary or secondary role.

IPSec has two sets of policies to be configured, the ISAKMP policy and the IPSec Policy, also referred to as the transform set.

Configuration for Primary key server is shown below.

### **Key Server Configuration – ISAKMP Policy**

---

```
Hostname keyserver-name
!### Define the ISAKMP Policy ###
crypto isakmp policy 10
authentication pre-share
encryption aes
hash sha
group 5
lifetime 86400
!### Define pre-shared keys for each GM and other KS if any ###
crypto isakmp key NEMO address 0.0.0.0 0.0.0.0 no-xauth
```

### **Key Server Configuration – IPsec Policy**

---

```
!### Define the IPsec Policy ###
crypto ipsec transform-set NEMO esp-aes esp-sha-hmac
!
crypto ipsec profile NEMO
set security-association lifetime seconds 28800
set transform-set NEMO
```

### **Key Server Configuration – GDOI**

---

```
!### GDOI Configuration ###
crypto gdoi group NEMO
  identity number 1
  server local
rekey retransmit 10 number 2
rekey authentication mypubkey rsa NEMO
rekey transport unicast
sa ipsec 1
  profile NEMO
  match address ipv4 NEMO-GETVPN
  replay counter window-size 64
address ipv4 <KS1 address> or <KS2 address>
```

---

### ***Server Crypto ACL (This configuration is a sample & needs to be customized for deployment)***

---

```
##### Crypto ACL #####
ip access-list extended NEMO-GETVPN
deny tcp any any eq ssh
deny tcp any eq ssh any
deny udp any any eq 848
deny udp eq 848 any
deny tcp any any eq bgp          !when GM uses BGP for PE-CE
deny tcp any eq bgp any         !when GM uses BGP for PE-CE
!deny udp any any eq ntp        !optional
!deny udp any any eq dns        !optional
!deny udp any any eq snmp       !optional
!deny udp any any eq syslog     !optional
!deny udp any any eq 1645       !optional
!deny udp any any eq 1646       !optional
!deny udp any any eq 1812       !optional
!deny udp any any eq 1813       !optional
!deny tcp any eq 443 any        !optional
!deny tcp any any eq 443        !optional
permit ip any any
```

---

**Note:** Crypto access control list (ACL) must be designed per customer traffic requirements. The ACL provided is an example only.

## Important Group Member Show and PING Commands

### SHOW CRYPTO GDOI

---

```
C1941-NEMO-LTE#sh crypto gdoi
```

#### GROUP INFORMATION

```
Group Name           : nemo
Group Identity       : 434
Rekeys received      : 348
IPSec SA Direction   : Both

Group Server list    : 10.0.67.1

Group member         : 10.0.66.1          vrf: None
  Registration status : Registered
  Registered with     : 10.0.67.1
  Re-registers in    : 413 sec
  Succeeded registration: 26
  Attempted registration: 29
  Last rekey from    : 10.0.67.1
  Last rekey seq num : 33
  Unicast rekey received: 348
  Rekey ACKs sent    : 348
  Rekey Rcvd(hh:mm:ss) : 00:50:06
  allowable rekey cipher: any
  allowable rekey hash : any
  allowable transformtag: any ESP

Rekeys cumulative
  Total received      : 348
  After latest register : 3
  Rekey Acks sents    : 348
```

```
ACL Downloaded From KS 10.0.67.1:
access-list permit ip any 10.245.1.0 0.0.0.255
access-list permit ip 10.245.1.0 0.0.0.255 any
```

#### KEK POLICY:

```
Rekey Transport Type : Unicast
Lifetime (secs)      : 6810
Encrypt Algorithm     : 3DES
Key Size              : 192
Sig Hash Algorithm    : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024
```

#### TEK POLICY for the current KS-Policy ACEs Downloaded:

```
Tunnel0:
IPsec SA:
  spi: 0xA5A7BF26(2779234086)
  transform: esp-aes esp-sha-hmac
  sa timing:remaining key lifetime (sec): (593)
  Anti-Replay : Disabled
```

## SHOW CRYPTO ISAKMP SA

---

```
C1941-NEMO-LTE#sh cry isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
10.0.67.1    10.0.66.1    GDOI_IDLE     2047 ACTIVE
10.0.66.1    10.0.67.1    GDOI_REKEY    2049 ACTIVE
```

## SHOW CRYPTO IPSEC SA

---

```
C1941-NEMO-LTE#sh crypto ipsec sa

interface: Tunnel434
  Crypto map tag: NEMO-GETVPN, local addr 10.0.66.1

  protected vrf: (none)
  local ident (addr/mask/prot/port): (10.245.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 0.0.0.0 port 848
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

  local crypto endpt.: 10.0.66.1, remote crypto endpt.: 0.0.0.0
  path mtu 1476, ip mtu 1476, ip mtu idb Tunnel434
  current outbound spi: 0xA5A7BF26(2779234086)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
    spi: 0xA5A7BF26(2779234086)
      transform: esp-aes esp-sha-hmac ,
      in use settings = {Tunnel, }
      conn id: 89, flow_id: Onboard VPN:89, sibling_flags 80000040, crypto
map: NEMO-GETVPN
      sa timing: remaining key lifetime (sec): (520)
      Kilobyte Volume Rekey has been disabled
      IV size: 16 bytes
      replay detection support: N
      Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
    spi: 0xA5A7BF26(2779234086)
      transform: esp-aes esp-sha-hmac ,
      in use settings = {Tunnel, }
      conn id: 90, flow_id: Onboard VPN:90, sibling_flags 80000040, crypto
map: NEMO-GETVPN
```

```
sa timing: remaining key lifetime (sec): (520)
Kilobyte Volume Rekey has been disabled
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.245.1.0/255.255.255.0/0/0)
current_peer 0.0.0.0 port 848
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 12131, #pkts encrypt: 12131, #pkts digest: 12131
#pkts decaps: 11870, #pkts decrypt: 11870, #pkts verify: 11870
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.0.66.1, remote crypto endpt.: 0.0.0.0
path mtu 1476, ip mtu 1476, ip mtu idb Tunnel434
current outbound spi: 0xA5A7BF26(2779234086)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xA5A7BF26(2779234086)
  transform: esp-aes esp-sha-hmac ,
  in use settings = {Tunnel, }
  conn id: 87, flow_id: Onboard VPN:87, sibling_flags 80000040, crypto
map: NEMO-GETVPN
  sa timing: remaining key lifetime (sec): (520)
  Kilobyte Volume Rekey has been disabled
  IV size: 16 bytes
  replay detection support: N
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xA5A7BF26(2779234086)
  transform: esp-aes esp-sha-hmac ,
  in use settings = {Tunnel, }
  conn id: 88, flow_id: Onboard VPN:88, sibling_flags 80000040, crypto
map: NEMO-GETVPN
  sa timing: remaining key lifetime (sec): (520)
  Kilobyte Volume Rekey has been disabled
  IV size: 16 bytes
  replay detection support: N
  Status: ACTIVE

outbound ah sas:
```

```
outbound pcp sas:

interface: Tunnel0
  Crypto map tag: NEMO-GETVPN, local addr 10.0.66.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.245.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 0.0.0.0 port 848
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.0.66.1, remote crypto endpt.: 0.0.0.0
path mtu 1476, ip mtu 1476, ip mtu idb Tunnel434
current outbound spi: 0xA5A7BF26(2779234086)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xA5A7BF26(2779234086)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 89, flow_id: Onboard VPN:89, sibling_flags 80000040, crypto
map: NEMO-GETVPN
  sa timing: remaining key lifetime (sec): (520)
  Kilobyte Volume Rekey has been disabled
  IV size: 16 bytes
  replay detection support: N
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xA5A7BF26(2779234086)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 90, flow_id: Onboard VPN:90, sibling_flags 80000040, crypto
map: NEMO-GETVPN
  sa timing: remaining key lifetime (sec): (520)
  Kilobyte Volume Rekey has been disabled
  IV size: 16 bytes
  replay detection support: N
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.245.1.0/255.255.255.0/0/0)
current_peer 0.0.0.0 port 848
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 12131, #pkts encrypt: 12131, #pkts digest: 12131
#pkts decaps: 11870, #pkts decrypt: 11870, #pkts verify: 11870
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.0.66.1, remote crypto endpt.: 0.0.0.0
path mtu 1476, ip mtu 1476, ip mtu idb Tunnel434
current outbound spi: 0xA5A7BF26(2779234086)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xA5A7BF26(2779234086)
  transform: esp-aes esp-sha-hmac ,
  in use settings = {Tunnel, }
  conn id: 87, flow_id: Onboard VPN:87, sibling_flags 80000040, crypto
map: NEMO-GETVPN
  sa timing: remaining key lifetime (sec): (520)
  Kilobyte Volume Rekey has been disabled
  IV size: 16 bytes
  replay detection support: N
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xA5A7BF26(2779234086)
  transform: esp-aes esp-sha-hmac ,
  in use settings = {Tunnel, }
  conn id: 88, flow_id: Onboard VPN:88, sibling_flags 80000040, crypto
map: NEMO-GETVPN
  sa timing: remaining key lifetime (sec): (520)
  Kilobyte Volume Rekey has been disabled
  IV size: 16 bytes
  replay detection support: N
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:
C1941-NEMO-LTE#
```

## **PING FROM INSIDE SOURCE**

---

```
C1941-NEMO-LTE#ping 10.245.1.1 source 10.21.65.129 repeat 100
```

---

```
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.245.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.21.65.129
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 44/72/524 ms
```




---

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

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

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

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

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