Application Note 54

Configuring Dynamic Multipoint VPN (DMVPN) using GRE over IPSec between Cisco routers and Digi TransPort

Tech Support

29 March 2018

Contents

INTRODUCTION

Outline

This document describes how to configure a Dynamic Multipoint VPN (DMVPN) using a GRE tunnel within an IPSec tunnel and Next Hop Resolution Protocol (NHRP). This allows multipoint secure communications between two Cisco routers and a Digi TransPort with dynamic discovery of tunnel endpoints.

Dynamic Multipoint Virtual Private Network (DMVPN) is a dynamic tunnelling form of a virtual private network (VPN) based on the standard protocols, GRE, NHRP and IPsec.

NHRP is a protocol running over a GRE tunnel. It allows the registration and resolution of NBMA (non-broadcast multi access) addresses to a protocol or tunnel address.

This protocol would be used in a multi spoke to hub network in which the network addresses of the spoke routers do not need to be known and so do not need to be configured in the hub router. The advantages of this are a scalable network in which the size of the hub configuration is minimised.

When one spoke of the network needs to send traffic to another spoke a direct transfer is possible without having to add any load onto the hub. This is achieved by the creation of a dynamic GRE tunnel directly to the other spoke. The network address of the target spoke is resolved with the use of the NHRP protocol.

Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi TransPort router and configure it with basic routing functions.

This application note applies only to:

Model: Digi TransPort WR44

Other Compatible Models: Digi TransPort VC7400 VPN Concentrator, WR, SR or DR.

Firmware versions: 5.212 or newer. Cisco 12.4 or newer
revalidated Jan 2018 using 6.1.0.3 and Cisco IOS 15.5

Configuration: This Application Note assumes the devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.

Please note: This application note has been specifically rewritten for firmware release 5.212 and later; earlier versions of firmware will not work. Please contact tech.support@digi.com if you require assistance in upgrading the firmware of the TransPort router.

Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com

Requests for new application notes can be sent to the same address.

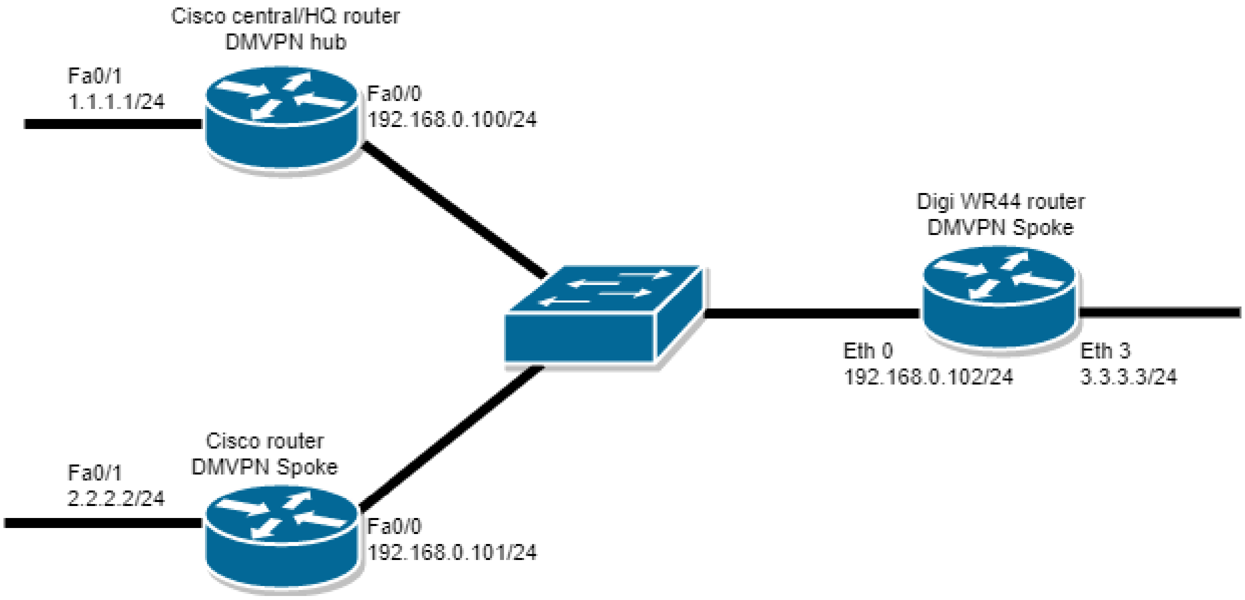
VERSION

Version Number	Status
1.0	Published
1.1	Updates
1.2	Added DMVPN details, configuration updates and BGP.
1.3	Remove BGP. Add EIGRP and OSPF with mutual redistribution. Validate using current firmware versions.

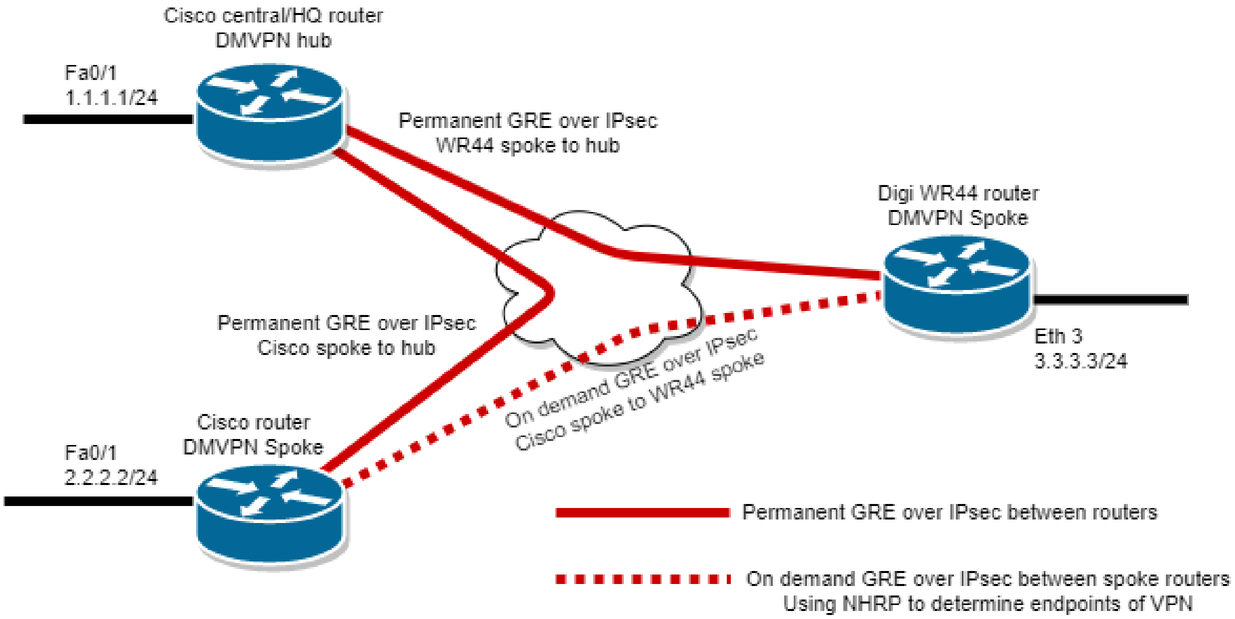
SCENARIO

For the purposes of this application note, the following scenario will be used:

Physical layout of routers



Logical layout of routers with DMVPN configuration



The IP addressing used is as follows:

Digi WR44
WAN = Eth0 = 192.168.0.102/24
LAN = Eth3 = 3.3.3.3/24
GRE = Tunnel 0 = 192.168.1.3/24

Cisco hub
WAN = Fa0/0 = 192.168.0.100/24
LAN = Fa0/1 = 1.1.1.1/24
GRE = Tun0 = 192.168.1.1/24

Cisco spoke1
WAN = Fa0/0 = 192.168.0.101/24
LAN = Fa0/1 = 2.2.2.2/24
GRE = Tun0 = 192.168.1.2/24

IPSec parameters:

IPSec Type: Main mode

Phase 1
Encryption algorithm: DES
Hash algorithm: Message Digest 5 (MD5)
Authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
Lifetime: 86400 seconds, no volume limit
Pre-shared key: cisco123

Phase 2
Encryption algorithm: 3DES
Hash algorithm: Secure Hash Standard (SHA1)
Mode: Tunnel mode
DH group: No PFS

Lifetime: 3600 seconds, no volume limit

CISCO CONFIGURATION HUB

Configure the Ethernet interfaces, Console port and hostname

From the Cisco console port, configure the Ethernet interfaces with the addressing shown in Section 2.
Set the hostname.
Use these commands:

```
hostname hub

interface FastEthernet0/0
 ip address 192.168.0.100 255.255.255.0
 duplex full
 speed 100
 no shut

interface FastEthernet0/1
 ip address 1.1.1.1 255.255.255.0
 ip ospf network point-to-point
 duplex full
 speed 100
 no shut
```

Configure IPSec phase 1 parameters and pre-shared key

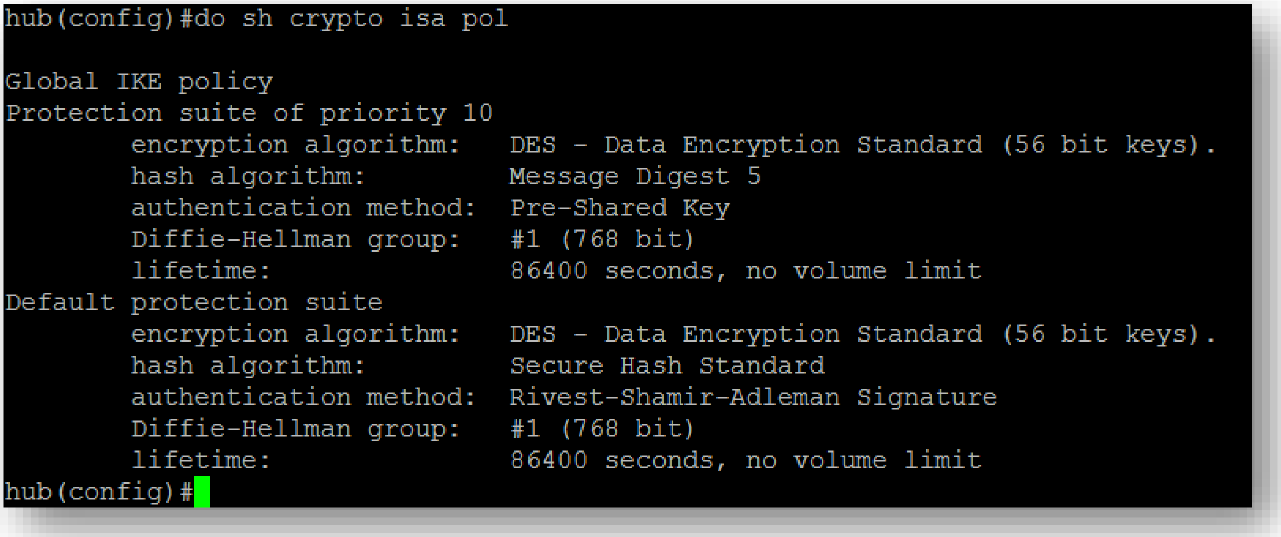
Create an ISAKMP policy and give it is priority 10

Set DES encryption, the authentication mode as pre-shared keys, DH group is left as default (1)

Use these commands:

```
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
```

The phase 1 policy can be confirmed:



```
hub(config)#do sh crypto isa pol

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
hub(config)#
```

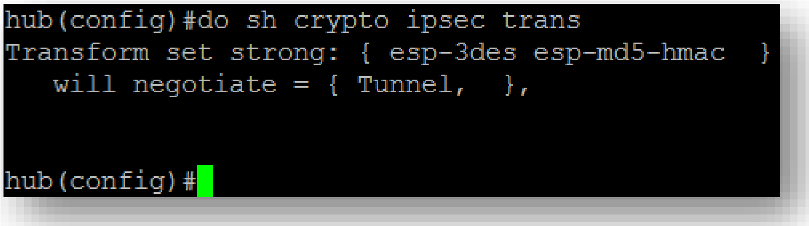
Configure IPSec phase 2 parameters

Create a transform set and enable 3DES & SHA1
Create an IPSec profile named cisco
Link the transform set T1 to the IPSec profile cisco

Use these commands:

```
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
crypto ipsec profile cisco
 set security-association lifetime seconds 1200
 set transform-set strong
```

The phase 2 transform set can be confirmed:



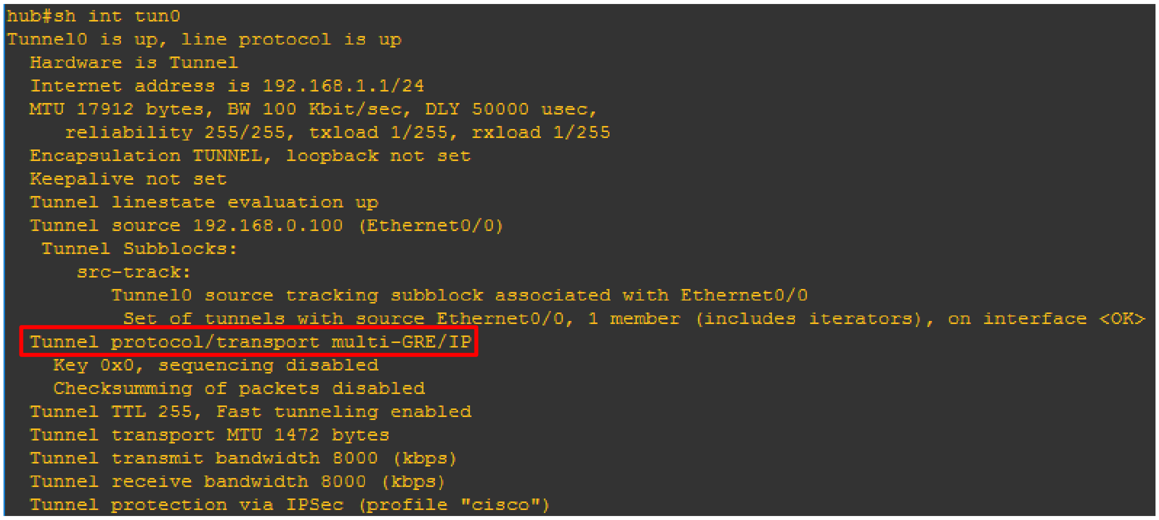
```
hub(config)#do sh crypto ipsec trans
Transform set strong: { esp-3des esp-md5-hmac  }
   will negotiate = { Tunnel,  },


hub(config)#
```

Configure the Tunnel 0 interface

Create tunnel0
Set the IP address
Set nhrp authentication key to cisco123
Set nhrp multicast route discovery to dynamic
Set nhrp network id to 1
Set nhrp holdtime to 600
Tunnel0 source interface will be Fa0/0 (WAN)
Tunnel0 mode is GRE multipoint
Tunnel0 will use the IPSec profile cisco
EIGRP protocol will be used between Cisco's for automatic route discovery. As EIGRP is not supported in the Digi TransPort, this example will use OSPF on the TransPort router. The Cisco hub router will be configured to redistribute dynamic routes from EIGRP into OSPF also from OSPF into EIGRP.
Use these commands:

```
interface Tunnel0
 ip address 192.168.1.1 255.255.255.0
 no ip redirects
 ip mtu 1440
 no ip next-hop-self eigrp 90
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 600
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile cisco shared
```

Confirm the mode of the tunnel is GRE/IP multipoint



```
hub#sh int tun0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.1.1/24
  MTU 17912 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 192.168.0.100 (Ethernet0/0)
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with Ethernet0/0
          Set of tunnels with source Ethernet0/0, 1 member (includes iterators), on interface <OK>
  Tunnel protocol/transport multi-GRE/IP
    Key 0x0, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1472 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "cisco")
```

If the tunnel is showing anything other than multi-GRE/IP, use the following command to set the tunnel mode correctly:

```
interface Tunnel0
 tunnel mode gre multipoint
```

Configure EIGRP - for Cisco dynamic routing

```
router eigrp 90
 network 1.1.1.0 0.0.0.255
 network 192.168.1.0
 no auto-summary
int tun0
no ip next-hop-self eigrp 90
no ip split-horizon eigrp 90
```

Configure OSPF – for TransPort dynamic routing

The TransPort router will run OSPF, this Cisco hub will also need to run OSPF, then be configured to redistribute dynamic routes between the 2 routing protocols.

Add OSPF to the Cisco hub router:

```
router ospf 1
 router-id 1.1.1.1
 priority 100
 passive-interface default
 no passive-interface Tunnel0
 network 1.1.1.1 0.0.0.0 area 0
 network 192.168.1.1 0.0.0.0 area 0
```

Configure mutual redistribution of OSPF and EIGRP

Add redistribution from EIGRP into OSPF:

```
router ospf 1
redistribute eigrp 90 metric 100 subnets
```

Add redistribution from OSPF into EIGRP:

```
router eigrp 90
redistribute ospf 1 metric 10000 100 255 1 1500
```

Exit the global configuration mode and save the config

```
end
copy run start
```

CISCO CONFIGURATION SPOKE1

Configure the Ethernet interfaces, Console port and hostname

From the Cisco console port, configure the Ethernet interfaces with the addressing shown in Section 2.
Set the hostname

```
hostname spoke1

interface FastEthernet0/0
 ip address 192.168.0.101 255.255.255.0
 duplex full
 speed 100
 no shut

interface FastEthernet0/1
 ip address 2.2.2.2 255.255.255.0
 ip ospf network point-to-point
 duplex full
 speed 100
 no shut
```

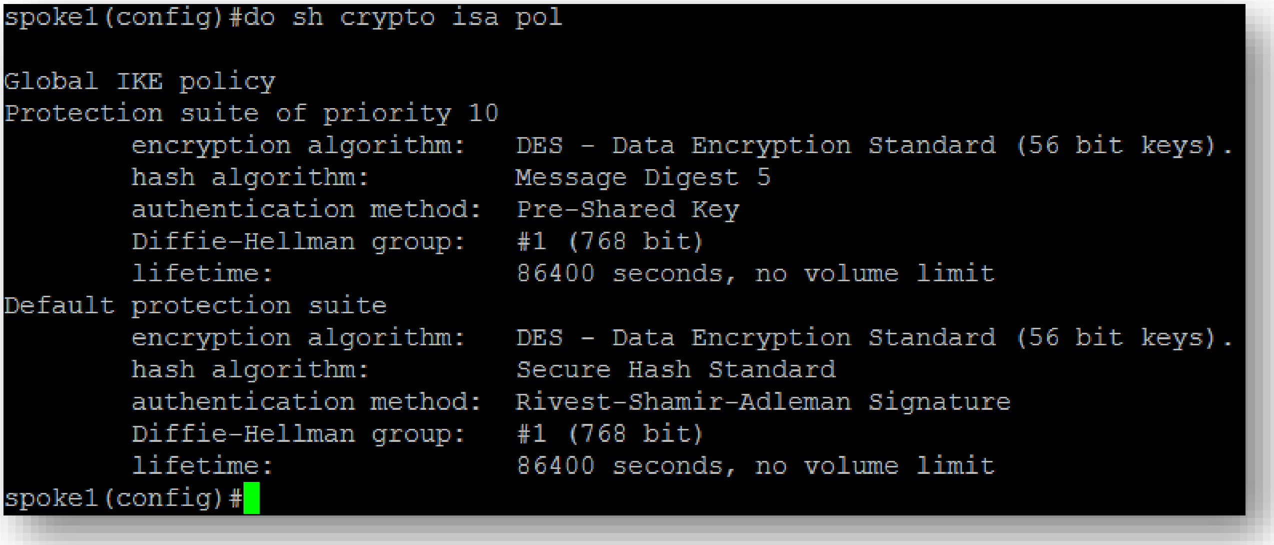
Configure IPSec phase 1 parameters and pre-shared key

Create an ISAKMP policy and give it is priority 10

Set DES encryption, the authentication mode as pre-shared keys, DH group is left as default (1)

```
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
```

The phase 1 policy can be confirmed:



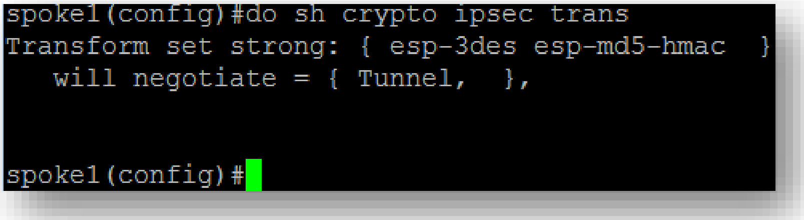
```
spoke1(config)#do sh crypto isa pol

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
spoke1(config)#
```

Configure IPSec phase 2 parameters

Create a transform set and enable 3DES & SHA1
Create an IPSec profile named cisco
Link the transform set T1 to the IPSec profile cisco

```
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
crypto ipsec profile cisco
 set security-association lifetime seconds 1200
 set transform-set strong
```

The phase 2 transform set can be confirmed:



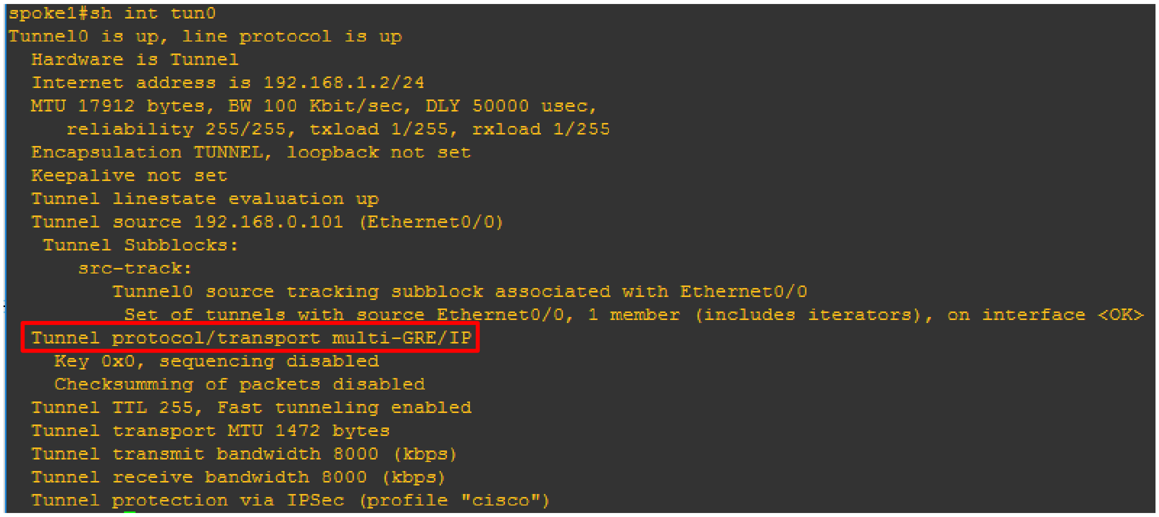
```
spoke1(config)#do sh crypto ipsec trans
Transform set strong: { esp-3des esp-md5-hmac  }
   will negotiate = { Tunnel,  },


spoke1(config)#
```

Configure the Tunnel 0 interface

Create tunnel0
Set the IP address
Set nhrp authentication key to cisco123
Set nhrp multicast route discovery to dynamic
Set nhrp network id to 1
Set nhrp holdtime to 600
Tunnel0 source interface will be Fa0/0 (WAN)
Tunnel0 mode is GRE multipoint
Tunnel0 will use the IPSec profile cisco
EIGRP protocol will be used between Cisco's for automatic route discovery.

```
interface Tunnel0
 ip address 192.168.1.2 255.255.255.0
 no ip redirects
 ip mtu 1440
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp map 192.168.1.1 192.168.0.100
 ip nhrp map multicast 192.168.0.100
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip nhrp nhs 192.168.1.1
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile cisco
```

Confirm the mode of the tunnel is GRE/IP multipoint



```
spoke1#sh int tun0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.1.2/24
  MTU 17912 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 192.168.0.101 (Ethernet0/0)
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with Ethernet0/0
          Set of tunnels with source Ethernet0/0, 1 member (includes iterators), on interface <OK>
  Tunnel protocol/transport multi-GRE/IP
    Key 0x0, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1472 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "cisco")
```

If the tunnel is showing anything other than multi-GRE/IP, use the following command to set the tunnel mode correctly:

```
interface Tunnel0
 tunnel mode gre multipoint
```

Configure EIGRP - for Cisco dynamic routing

```
router eigrp 90
 network 2.2.2.0 0.0.0.255
 network 192.168.1.0
 no auto-summary
```

Exit global config mode and save the configuration

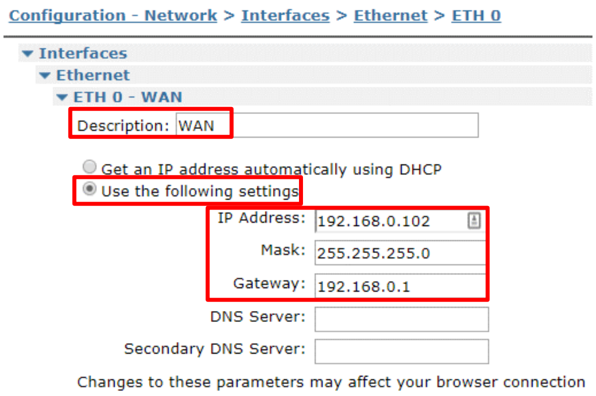
This is done by using CTRL+Z. Save the configuration with:

```
end
copy run start
```

Configure the Ethernet interfaces

Ethernet 0 – The WAN interface

Browse to **Configuration – Network > Interfaces > Ethernet > ETH0**
Set the Description, IP address & Mask.



Configuration - Network > Interfaces > Ethernet > ETH 0

▾ Interfaces
▾ Ethernet
▾ ETH 0 - WAN

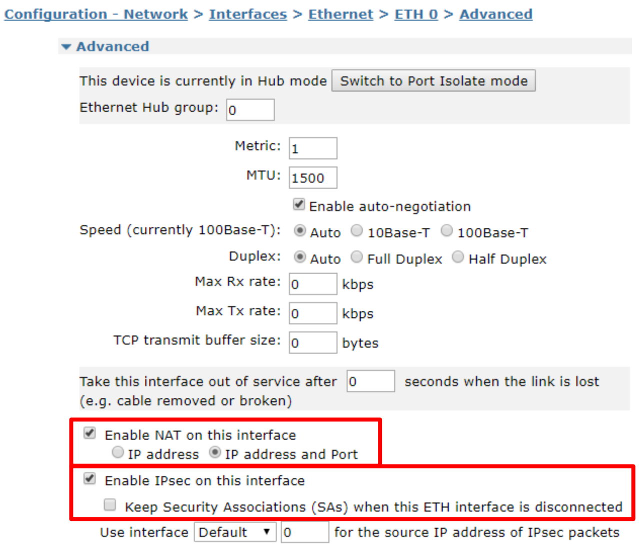
Description: WAN

○ Get an IP address automatically using DHCP
● Use the following settings

IP Address: 192.168.0.102
Mask: 255.255.255.0
Gateway: 192.168.0.1
DNS Server:
Secondary DNS Server:

Changes to these parameters may affect your browser connection

Click Advanced and enable NAT & IPSec.
Configuration – Network > Interfaces > Ethernet > ETH0 > Advanced



Configuration - Network > Interfaces > Ethernet > ETH 0 > Advanced

▾ Advanced

This device is currently in Hub mode [Switch to Port Isolate mode]
Ethernet Hub group: 0

Metric: 1
MTU: 1500
☑ Enable auto-negotiation
Speed (currently 100Base-T): ● Auto ○ 10Base-T ○ 100Base-T
Duplex: ● Auto ○ Full Duplex ○ Half Duplex
Max Rx rate: 0 kbps
Max Tx rate: 0 kbps
TCP transmit buffer size: 0 bytes

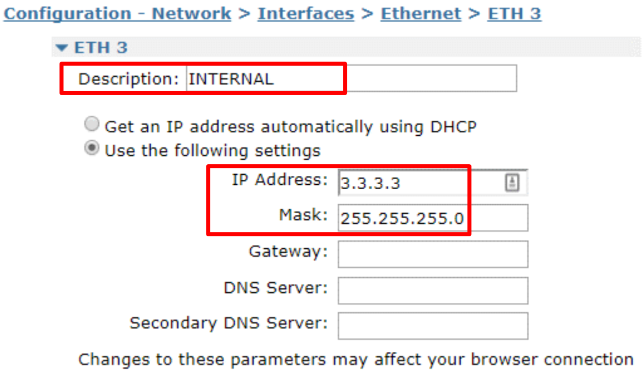
Take this interface out of service after 0 seconds when the link is lost
(e.g. cable removed or broken)

☑ Enable NAT on this interface
○ IP address ● IP address and Port
☑ Enable IPsec on this interface
☐ Keep Security Associations (SAs) when this ETH interface is disconnected
Use interface Default ▾ 0 for the source IP address of IPsec packets

Parameter	Setting	Description
Description	WAN	Friendly name for this interface
IP address	192.168.0.102	IP address
Mask	255.255.255.0	Subnet mask
Enable NAT on this interface	Enabled with IP address and Port	Enables NAT on this interface
Enable IPSec on this interface	Enabled	Enables IPSec on this interface

Ethernet 1 – The LAN interface

Browse to **Configuration – Network > Interfaces > Ethernet > ETH3**
Set the Description, IP address. NAT and IPSec should remain disabled.



Configuration - Network > Interfaces > Ethernet > ETH 3

▼ ETH 3

Description: INTERNAL

○ Get an IP address automatically using DHCP
● Use the following settings

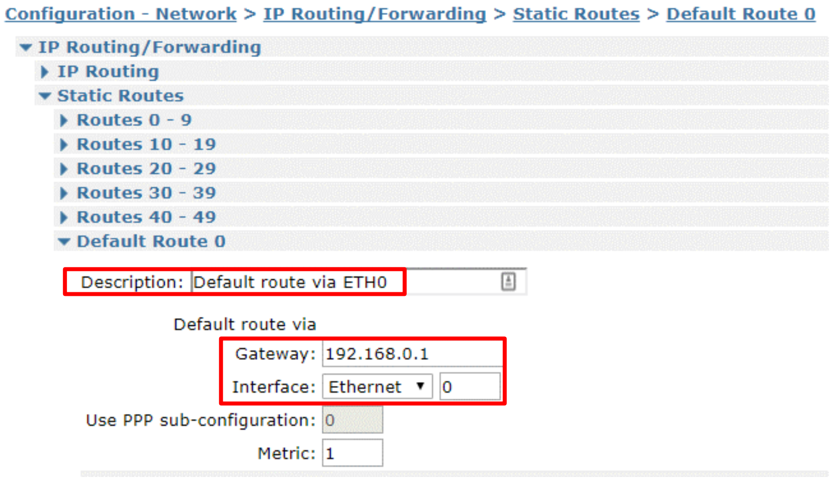
IP Address: 3.3.3.3
Mask: 255.255.255.0
Gateway:
DNS Server:
Secondary DNS Server:

Changes to these parameters may affect your browser connection

Parameter	Setting	Description
Description	INTERNAL	Friendly name for this interface
IP address	3.3.3.3	IP address
Mask	255.255.255.0	Subnet mask

Configure the default route

Browse to **Configuration – Network > IP Routing/Forwarding > Static Routes > Routes 0-9 > Route 0**
Set the Description, Destination Network, IP address, Mask, Interface, Metric and exit interface.



Description: Default route via ETH0

Default route via

Gateway: 192.168.0.1

Interface: Ethernet 0

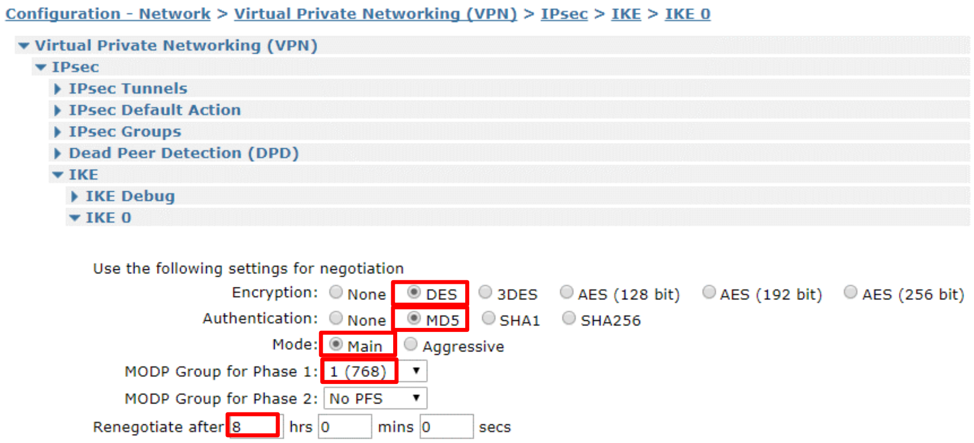
Use PPP sub-configuration: 0

Metric: 1

Parameter	Setting	Description
Description	Default route via ETH0	Friendly name for this interface
Gateway	192.168.0.1	Specify the IP address of the gateway router (ethernet routes only)
Interface	ETH 0	Interface to use for this route

Configure IPSec phase 1 parameters

Browse to **Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0**
These parameters must match the Cisco phase 1 parameters.



Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0

▾ Virtual Private Networking (VPN)
  ▾ IPsec
    ▸ IPsec Tunnels
    ▸ IPsec Default Action
    ▸ IPsec Groups
    ▸ Dead Peer Detection (DPD)
    ▾ IKE
      ▸ IKE Debug
      ▾ IKE 0

Use the following settings for negotiation

Encryption: ○ None ● DES ○ 3DES ○ AES (128 bit) ○ AES (192 bit) ○ AES (256 bit)

Authentication: ○ None ● MD5 ○ SHA1 ○ SHA256

Mode: ● Main ○ Aggressive

MODP Group for Phase 1: 1 (768)

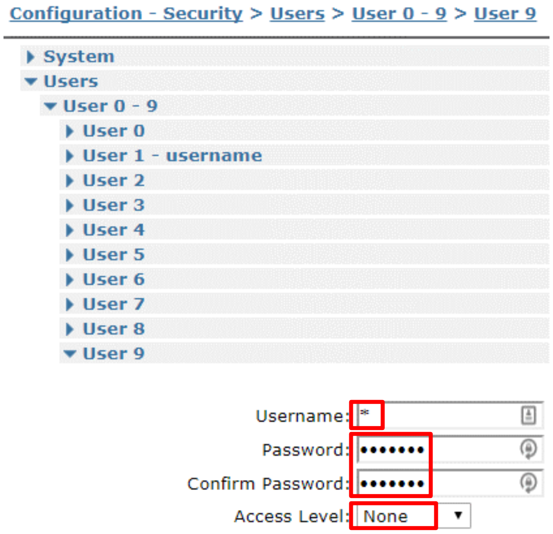
MODP Group for Phase 2: No PFS

Renegotiate after 8 hrs 0 mins 0 secs

Parameter	Setting	Description
Encryption	DES	Use DES encryption
Authentication	MD5	Use MD5 authentication
MODP Group for Phase 1	1 (768)	Use DH group 1
MODP Group for Phase 2	No PFS	No DH group for phase 2
Renegotiate after	8	Phase 1 lifetime in hours

Configure the Pre-shared key

Browse to the highest number unused User in the user table. In this example, this is User 9.
The name is set to an asterisk symbol which is a catch all wildcard for the IP addresses of the IPSec peers.
The Password is the Pre-shared key. Access level should be set to **None**, so if anyone knows these credentials, they cannot access the router for configuration or management.
Browse to **Configuration - Security > Users > User 0 - 9 > User 9**



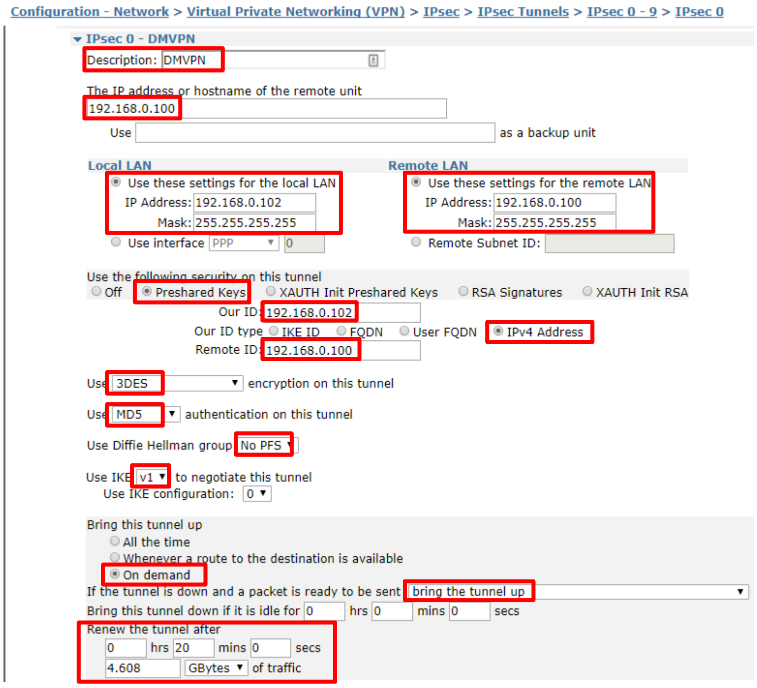
Username: *
Password: •••••••
Confirm Password: •••••••
Access Level: None

Parameter	Setting	Description
Username	*	Wildcard to catch all usernames not otherwise defined
Password	cisco123	Pre-shared key
Confirm Password	cisco123	Pre-shared key
Access Level	None	No access to router management for this user

Configure IPSec 0 phase 2 parameters

Browse to **Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0**

These parameters must match the Cisco phase 2 parameters



Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 0

IPsec 0 - DMVPN

Description: DMVPN

The IP address or hostname of the remote unit
192.168.0.100
Use as a backup unit

Local LAN
● Use these settings for the local LAN
IP Address: 192.168.0.102
Mask: 255.255.255.255
○ Use interface PPP 0

Remote LAN
● Use these settings for the remote LAN
IP Address: 192.168.0.100
Mask: 255.255.255.255
○ Remote Subnet ID:

Use the following security on this tunnel
○ Off ● Preshared Keys ○ XAUTH Init Preshared Keys ○ RSA Signatures ○ XAUTH Init RSA
Our ID: 192.168.0.102
Our ID type ○ IKE ID ○ FQDN ○ User FQDN ● IPv4 Address
Remote ID: 192.168.0.100

Use 3DES encryption on this tunnel

Use MD5 authentication on this tunnel

Use Diffie Hellman group No PFS

Use IKE v1 to negotiate this tunnel
Use IKE configuration: 0

Bring this tunnel up
○ All the time
○ Whenever a route to the destination is available
● On demand
If the tunnel is down and a packet is ready to be sent bring the tunnel up
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs
Renew the tunnel after
0 hrs 20 mins 0 secs
4.608 GBytes of traffic

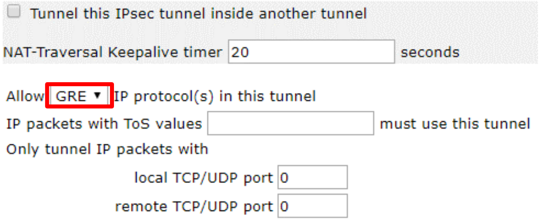
Parameter	Setting	Description
Description	DMVPN	Friendly name for this tunnel
Remote unit IP/hostname	192.168.0.100	The IP address or hostname of the remote unit
Local LAN	Use these setting for the local LAN	Use the specified settings below
IP Address	192.168.0.102	Local IPSec endpoint (WR44 WAN address)
Mask	255.255.255.255	Local IPSec endpoint mask (Must be/32)
Remote LAN	Use these setting for the remote LAN	Use the specified settings below

Parameter	Setting	**Description**
IP Address	192.168.0.100	Remote IPSec endpoint (Cisco hub WAN address)
Mask	255.255.255.255	Remote IPSec endpoint mask (Must be /32)
Use the following security on this tunnel	Preshared Keys	Use Preshared keys for authentication between routers
Our ID	192.168.0.102	Local router IPSec ID (WR44 WAN address)
Our ID type	IPv4 Address	Type of Ids used. IPv4 addresses
Remote ID	192.168.0.100	IPSec peer ID (Cisco hub WAN address)
Use X encryption on this tunnel	3DES	Use 3DES encryption
Use X authentication on this tunnel	MD5	Use MD5 authentication
Bring this tunnel up	On demand	Create SAs, but only if there is a valid route and interface to create the IPSec tunnel on.
If the tunnel is down and a packet is ready to be sent	Bring the tunnel up	If there is no IPSec SA, use IKE to create one.
Renew the tunnel after	1hrs/4608000 Kbytes	Lifetime of phase 2 SA in seconds / Lifetime of phase 2 SA in kilobytes

Configure IP Protocols to be used in the tunnel

Browse to **Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 > Advanced**

Select **GRE** under “Allow IP protocol(s) in this tunnel



☐ Tunnel this IPsec tunnel inside another tunnel

NAT-Traversal Keepalive timer 20 seconds

Allow GRE ▾ IP protocol(s) in this tunnel

IP packets with ToS values must use this tunnel

Only tunnel IP packets with

local TCP/UDP port 0

remote TCP/UDP port 0

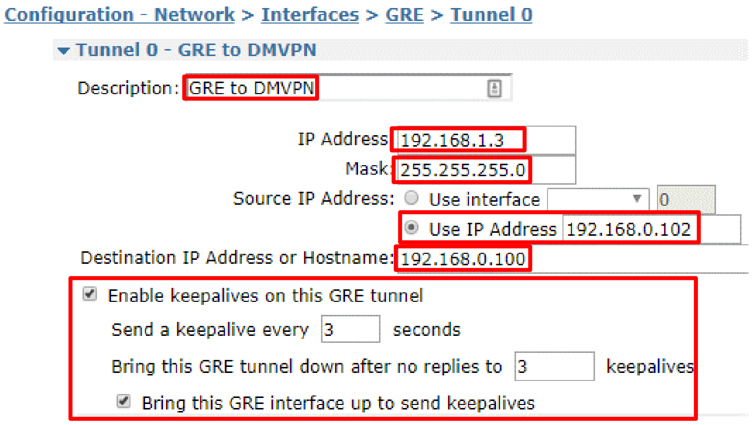
click **Apply**

Configure the GRE tunnel

This is the Digi TransPort end of the point to multipoint GRE tunnel.

Configure the tunnel IP address, and source and destination. Note that the source and destination addresses are the WAN interface addresses of the primary Cisco router (**hub**).

Browse to **Configuration - Network > Interfaces > GRE > Tunnel 0**



Configuration - Network > Interfaces > GRE > Tunnel 0

▾ Tunnel 0 - GRE to DMVPN

Description: GRE to DMVPN

IP Address 192.168.1.3

Mask 255.255.255.0

Source IP Address: ○ Use interface ▾ 0

● Use IP Address 192.168.0.102

Destination IP Address or Hostname: 192.168.0.100

☑ Enable keepalives on this GRE tunnel

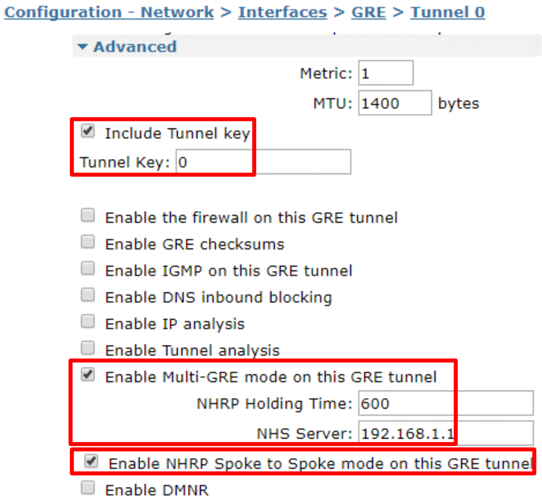
Send a keepalive every 3 seconds

Bring this GRE tunnel down after no replies to 3 keepalives

☑ Bring this GRE interface up to send keepalives

Parameter	Setting	Description
Description	GRE to DMVPN	Friendly name for this interface
IP address	192.168.1.3	GRE local endpoint IP address
Mask	255.255.255.0	GRE local endpoint subnet mask
Source IP Address	Use IP Address / 192.168.0.102	Source IP address of this tunnel (WR44 WAN interface)
Destination IP Address of Hostname	192.168.0.100	Destination IP address of this tunnel (Cisco hub WAN interface)
Enable keepalives on this GRE tunnel	Ticked	Sends 1 keepalive every 3 seconds
Bring this GRE tunnel down after no replies to x keepalives	3	If 3 keepalives packets fail, the tunnel is marked as down
Bring this GRE tunnel up to send keepalives	Ticked	Tunnel will be brought up to send keepalives packets

Browse to **Configuration - Network > Interfaces > GRE > Tunnel 0 > Advanced**



Configuration - Network > Interfaces > GRE > Tunnel 0

▾ Advanced

Metric: 1

MTU: 1400 bytes

☑ Include Tunnel key

Tunnel Key: 0

□ Enable the firewall on this GRE tunnel

□ Enable GRE checksums

□ Enable IGMP on this GRE tunnel

□ Enable DNS inbound blocking

□ Enable IP analysis

□ Enable Tunnel analysis

☑ Enable Multi-GRE mode on this GRE tunnel

NHRP Holding Time: 600

NHS Server: 192.168.1.1

☑ Enable NHRP Spoke to Spoke mode on this GRE tunnel

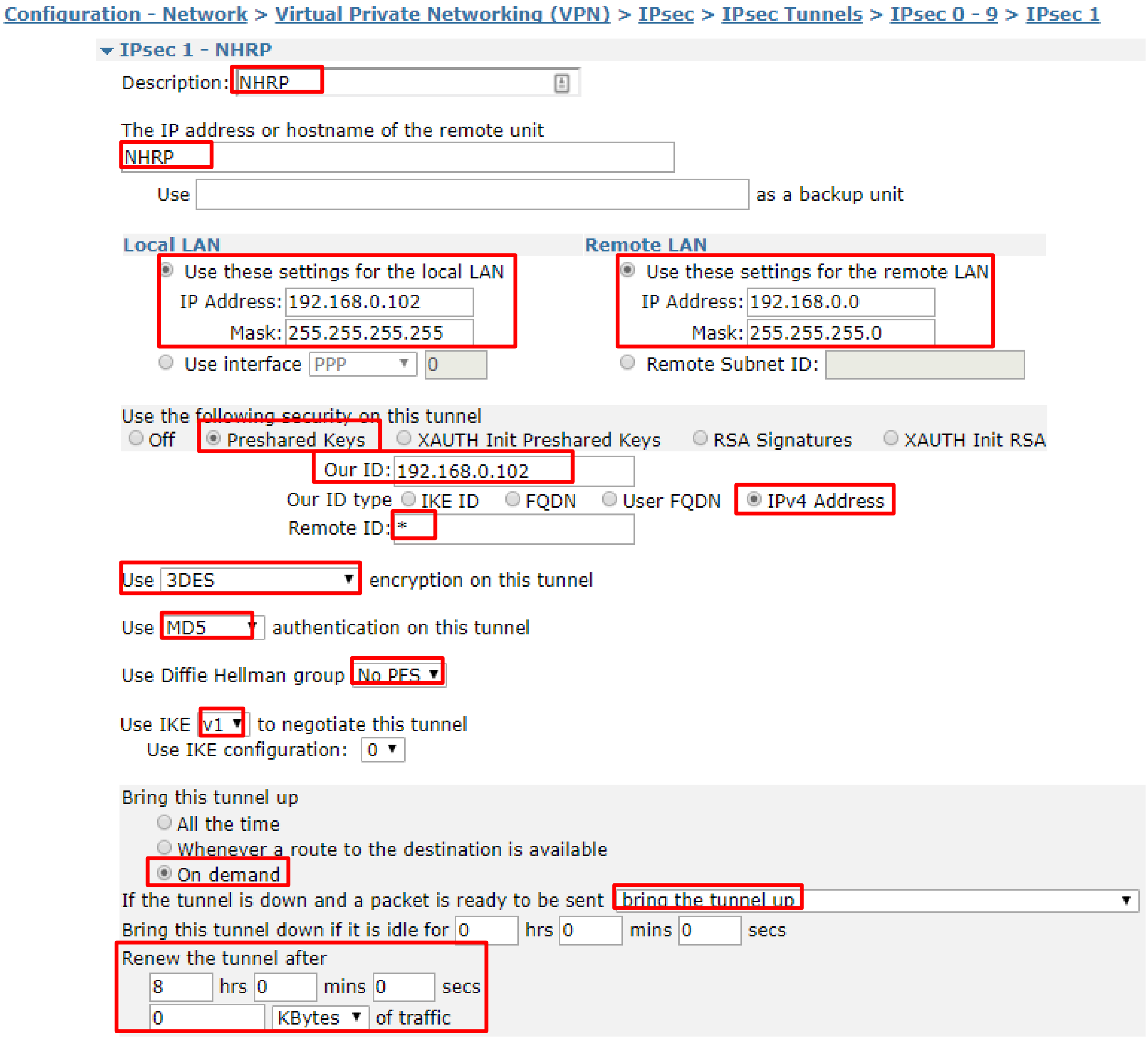
□ Enable DMNR

Click **Apply**

Parameter	Setting	Description
Include Tunnel key	Ticked	Set tunnel key
Tunnel Key	0	Tunnel key (0 = not used)
Enable Multi-GRE mode on this GRE tunnel	Ticked	Enable Multi-GRE mode
NHRP Holding time	600	Set NHRP holding time
NHS Server	192.168.1.1	IP address of Cisco GRE interface for NHS
Enable NHRP Spoke to Spoke mode on this GRE tunnel	Ticked	Enable spoke to spoke mode

Configure IPsec 1 for NHRP

IPsec 1 is used as a dynamic VPN that is created when a VPN needs to be created to another spoke router. This allows direct communication between spoke routers. NHRP is used to determine the WAN IP address of the spoke router that this TransPort router will create IPsec SAs with.



Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 1

▾ IPsec 1 - NHRP

Description: NHRP

The IP address or hostname of the remote unit
NHRP

Use as a backup unit

Local LAN
● Use these settings for the local LAN
IP Address: 192.168.0.102
Mask: 255.255.255.255
○ Use interface PPP ▾ 0

Remote LAN
● Use these settings for the remote LAN
IP Address: 192.168.0.0
Mask: 255.255.255.0
○ Remote Subnet ID:

Use the following security on this tunnel
○ Off ● Preshared Keys ○ XAUTH Init Preshared Keys ○ RSA Signatures ○ XAUTH Init RSA
Our ID: 192.168.0.102
Our ID type ○ IKE ID ○ FQDN ○ User FQDN ● IPv4 Address
Remote ID: *

Use 3DES ▾ encryption on this tunnel

Use MD5 ▾ authentication on this tunnel

Use Diffie Hellman group No PFS ▾

Use IKE v1 ▾ to negotiate this tunnel
Use IKE configuration: 0 ▾

Bring this tunnel up
○ All the time
○ Whenever a route to the destination is available
● On demand
If the tunnel is down and a packet is ready to be sent bring the tunnel up ▾
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs
Renew the tunnel after
8 hrs 0 mins 0 secs
0 KBytes ▾ of traffic

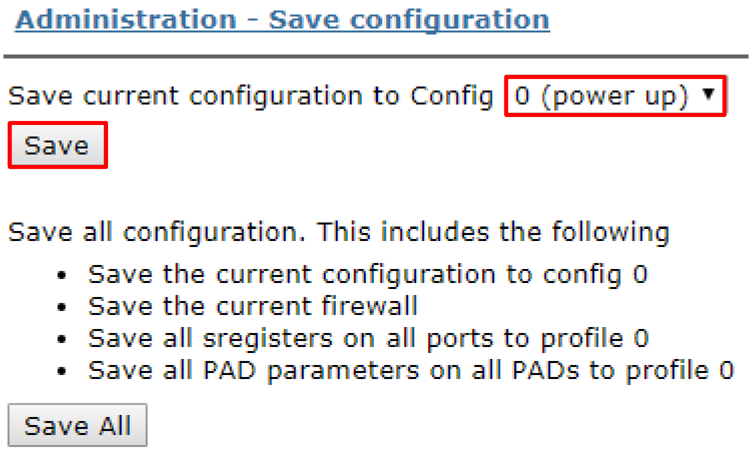
Parameter	Setting	Description
Description	NHRP	Friendly name for this tunnel
Remote unit IP/hostname	NHRP	Sets NHRP protocol as method to obtain other spoke router IP addresses

Parameter	Setting	Description
Local LAN	Use these setting for the local LAN	Use the specified settings below
IP Address	192.168.0.102	Local IPSec endpoint (WR44 WAN address)
Mask	255.255.255.255	Local IPSec endpoint mask (Must be/32)
Remote LAN	Use these setting for the remote LAN	Use the specified settings below
IP Address	192.168.0.0	192.168.0.0 encompasses all WAN addresses
Mask	255.255.255.0	/24 used with IP address above
Use the following security on this tunnel	Preshared Keys	Use Preshared keys for authentication between routers
Our ID	192.168.0.102	Local router IPSec ID (WR44 WAN address)
Our ID type	IPv4 Address	Type of Ids used. IPv4 addresses
Remote ID	*	* means any remote ID
Use X encryption on this tunnel	3DES	Use 3DES encryption
Use X authentication on this tunnel	MD5	Use MD5 authentication
Bring this tunnel up	On demand	Create SAs, but only if there is a valid route and interface to create the IPSec tunnel on.
If the tunnel is down and a packet is ready to be sent	Bring the tunnel up	If there is no IPSec SA, use IKE to create one.
Renew the tunnel after	1hrs/4608000 Kbytes	Lifetime of phase 2 SA in seconds / Lifetime of phase 2 SA in kilobytes

Save the configuration

Browse to **Administration - Save configuration**

Save the configuration to profile 0, the default power up config.



Administration - Save configuration

Save current configuration to Config 0 (power up)

Save all configuration. This includes the following

- Save the current configuration to config 0
- Save the current firewall
- Save all sregisters on all ports to profile 0
- Save all PAD parameters on all PADs to profile 0

Configure OSPF

TransPort routers use a text file for the majority of the OSPF configuration.

There are 2 main methods of creating this configuration file, pick one method:

Option 1: Web GUI

Use the GUI interface, navigate to: Configuration - Network > IP Routing/Forwarding > OSPF

Check 'Enable OSPF' to reveal the configuration options.

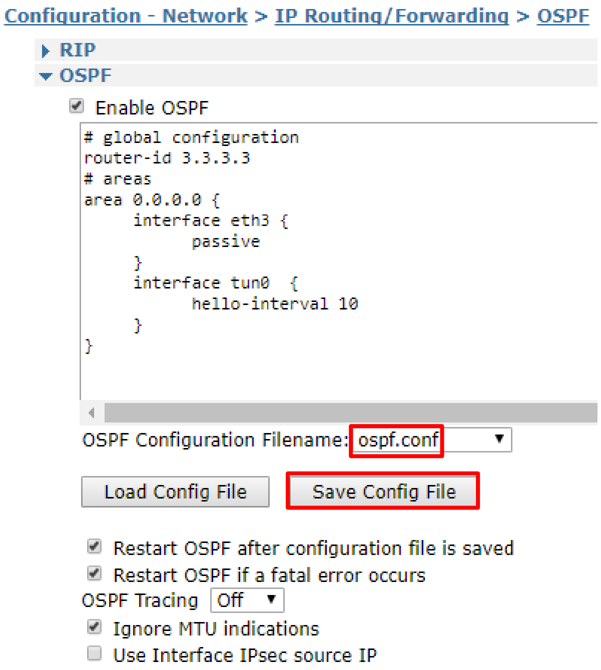
Paste the text into the text box:

```
# global configuration
router-id 3.3.3.3
# areas
area 0.0.0.0 {
     interface eth3 {
            passive
     }
     interface tun0 {
            hello-interval 10
     }
}

```

Note that there is a **blank line** after the final } and this **IS required**, **otherwise OSPF will fail to initialise**.

Ensure --edit-- is shown in the Filename dropdown box, then expand and close the list, this will allow you to overtype the filename from --edit-- to a filename of your choice.

Use the filename ospf.conf, click 'Save Config File'.



☑ Enable OSPF

```
# global configuration
router-id 3.3.3.3
# areas
area 0.0.0.0 {
     interface eth3 {
           passive
     }
     interface tun0  {
           hello-interval 10
     }
}
```

OSPF Configuration Filename: ospf.conf

☑ Restart OSPF after configuration file is saved
☑ Restart OSPF if a fatal error occurs
OSPF Tracing: Off
☑ Ignore MTU indications
☐ Use Interface IPsec source IP

Option 2: Plain text editor (eg: Notepad) + FTP + CLI

The file is created in notepad (or other plain text editor) then transferred to the TransPort router using FTP. The file should be named ospf.conf

The OSPF file should contain these lines:

```
# global configuration
router-id 3.3.3.3
# areas
area 0.0.0.0 {
     interface eth3 {
           passive
     }
     interface tun0 {
           hello-interval 10
     }
}

```

Note that there is a **blank line** after the final } and this **IS required**, **otherwise OSPF will fail to initialise**.

Transfer this ‘ospf.conf’ file to the TransPort router using an FTP client.

The router should be configured via the CLI to run this OSPF file by using these commands:

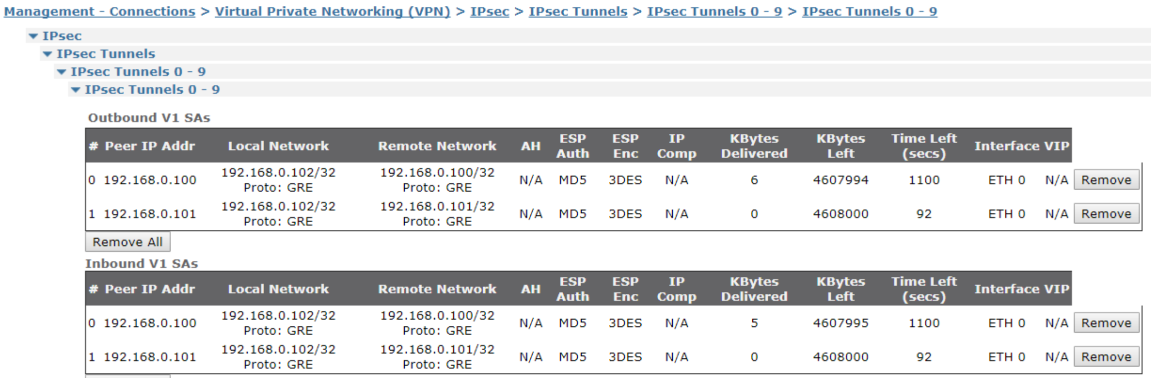
```
# You only need the following line if you named the OSPF config file
# something other than the default name of ospf.conf
ospf 0 conffile <OSPF file name>

# Enable OSPF
ospf 0 enable on
```

CONFIRM IPSEC & GRE IS UP AND PING TEST THE CONNECTION

Using the Digi WR44

Check the IPSec SA status

Browse to **Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels**



Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec Tunnels 0 - 9 > IPsec Tunnels 0 - 9

Outbound V1 SAs

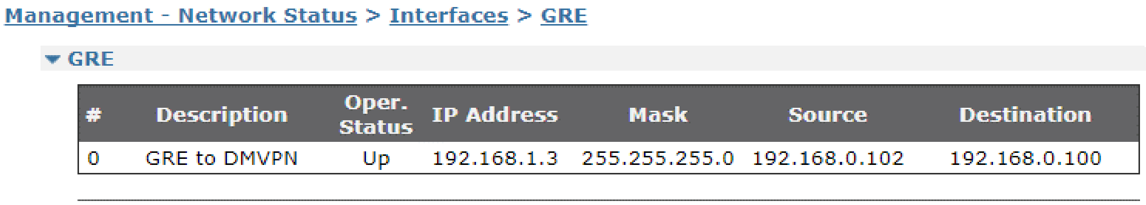
#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	VIP	
0	192.168.0.100	192.168.0.102/32 Proto: GRE	192.168.0.100/32 Proto: GRE	N/A	MD5	3DES	N/A	6	4607994	1100	ETH 0	N/A	Remove
1	192.168.0.101	192.168.0.102/32 Proto: GRE	192.168.0.101/32 Proto: GRE	N/A	MD5	3DES	N/A	0	4608000	92	ETH 0	N/A	Remove

Inbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	VIP	
0	192.168.0.100	192.168.0.102/32 Proto: GRE	192.168.0.100/32 Proto: GRE	N/A	MD5	3DES	N/A	5	4607995	1100	ETH 0	N/A	Remove
1	192.168.0.101	192.168.0.102/32 Proto: GRE	192.168.0.101/32 Proto: GRE	N/A	MD5	3DES	N/A	0	4608000	92	ETH 0	N/A	Remove

Check the GRE tunnel status

Browse to **Management - Network Status > Interfaces > GRE**

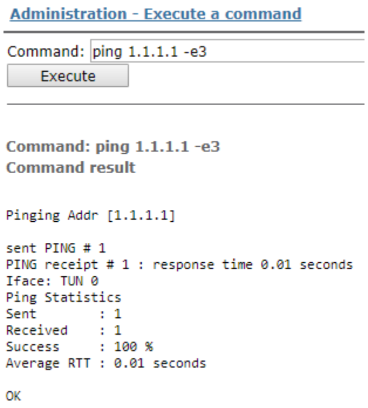


Management - Network Status > Interfaces > GRE

#	Description	Oper. Status	IP Address	Mask	Source	Destination
0	GRE to DMVPN	Up	192.168.1.3	255.255.255.0	192.168.0.102	192.168.0.100

Ping the LAN interface of the Primary Cisco hub and the Cisco spoke

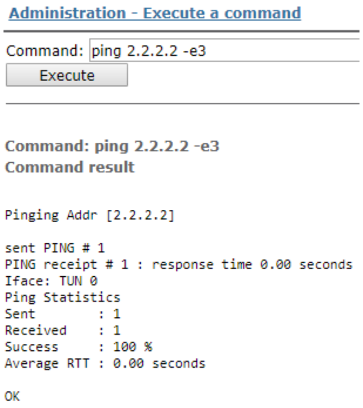
Make sure you specify the source interface with -e3, to use Eth 3 IP address as the source IP address.



Administration - Execute a command

Command: ping 1.1.1.1 -e3

```
Command: ping 1.1.1.1 -e3
Command result

Pinging Addr [1.1.1.1]

sent PING # 1
PING receipt # 1 : response time 0.01 seconds
Iface: TUN 0
Ping Statistics
Sent        : 1
Received    : 1
Success     : 100 %
Average RTT : 0.01 seconds

OK
```



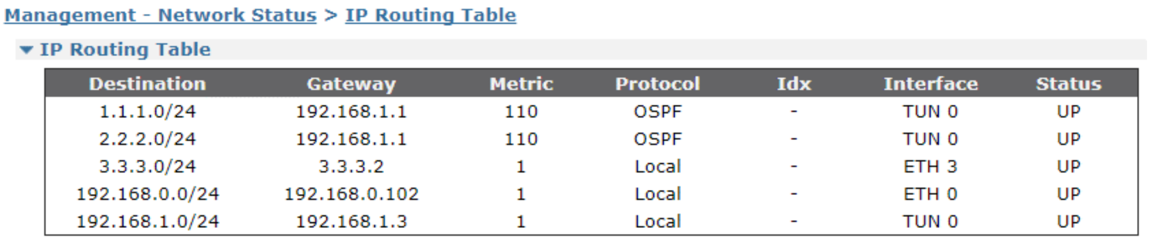
Administration - Execute a command

Command: ping 2.2.2.2 -e3

```
Command: ping 2.2.2.2 -e3
Command result

Pinging Addr [2.2.2.2]

sent PING # 1
PING receipt # 1 : response time 0.00 seconds
Iface: TUN 0
Ping Statistics
Sent        : 1
Received    : 1
Success     : 100 %
Average RTT : 0.00 seconds

OK
```

Check the TransPort routing table

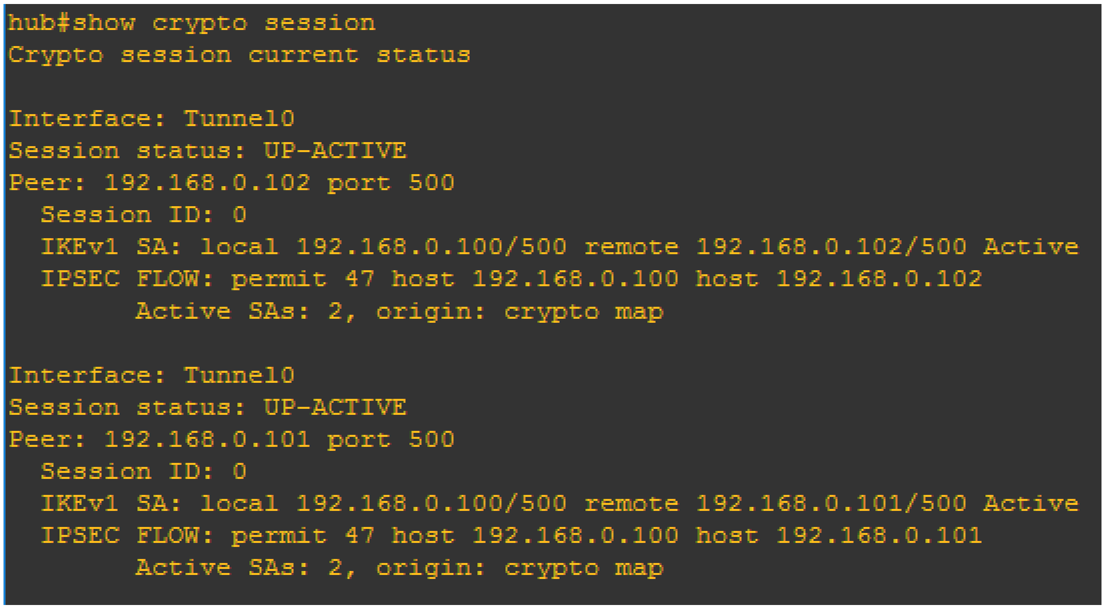
When you have sent pings to the hub and spoke 1, check the routing table on the TransPort router. You should see OSPF routes to 2 networks, 1.1.1.0/24 & 2.2.2.0/24:



Destination	Gateway	Metric	Protocol	Idx	Interface	Status
1.1.1.0/24	192.168.1.1	110	OSPF	-	TUN 0	UP
2.2.2.0/24	192.168.1.1	110	OSPF	-	TUN 0	UP
3.3.3.0/24	3.3.3.2	1	Local	-	ETH 3	UP
192.168.0.0/24	192.168.0.102	1	Local	-	ETH 0	UP
192.168.1.0/24	192.168.1.3	1	Local	-	TUN 0	UP

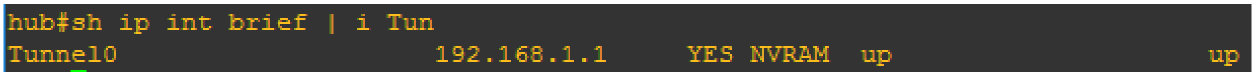
Using the Primary Cisco (hub)

Check the IPSec SA status



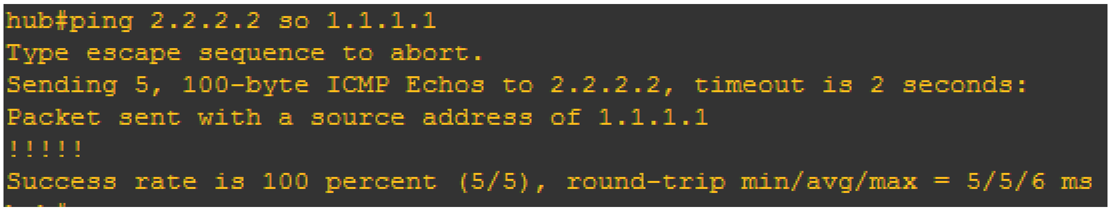
```
hub#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 192.168.0.102 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.0.100/500 remote 192.168.0.102/500 Active
  IPSEC FLOW: permit 47 host 192.168.0.100 host 192.168.0.102
        Active SAs: 2, origin: crypto map

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 192.168.0.101 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.0.100/500 remote 192.168.0.101/500 Active
  IPSEC FLOW: permit 47 host 192.168.0.100 host 192.168.0.101
        Active SAs: 2, origin: crypto map
```

Check the GRE tunnel status



```
hub#sh ip int brief | i Tun
Tunnel0                    192.168.1.1     YES NVRAM  up                    up
```

Ping the Cisco Spoke



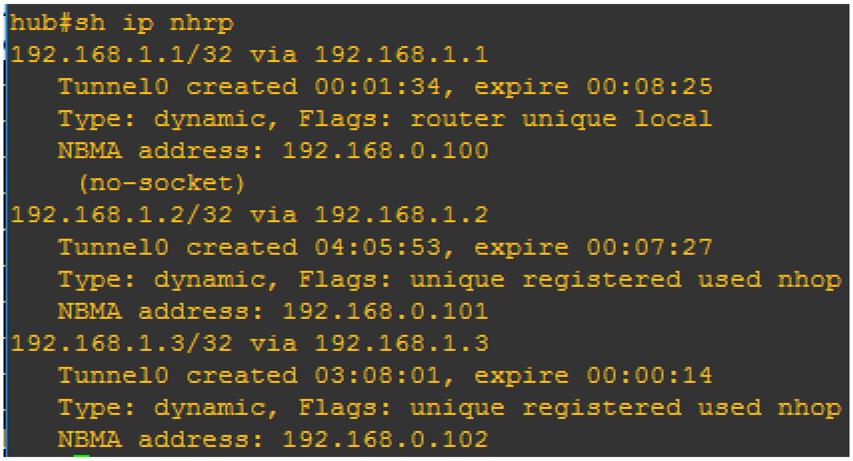
```
hub#ping 2.2.2.2 so 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

Check the routing table on the Cisco hub router

You are expecting to see a route to the TransPort router 4.4.4.4 from OSPF and a route to the other Cisco Spoke(s) from EIGRP.

```
hub#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [254/0] via 192.168.0.1
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, Ethernet0/1
L        1.1.1.1/32 is directly connected, Ethernet0/1
      2.0.0.0/24 is subnetted, 1 subnets
D        2.2.2.0 [90/26905600] via 192.168.1.2, 00:22:28, Tunnel0
      3.0.0.0/24 is subnetted, 1 subnets
O        3.3.3.0 [110/1010] via 192.168.1.3, 00:05:50, Tunnel0
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, Ethernet0/0
L        192.168.0.100/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Tunnel0
L        192.168.1.1/32 is directly connected, Tunnel0
hub#
```

Check NHRP registrations on the Cisco hub router



```
hub#sh ip nhrp
192.168.1.1/32 via 192.168.1.1
   Tunnel0 created 00:01:34, expire 00:08:25
   Type: dynamic, Flags: router unique local
   NBMA address: 192.168.0.100
    (no-socket)
192.168.1.2/32 via 192.168.1.2
   Tunnel0 created 04:05:53, expire 00:07:27
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 192.168.0.101
192.168.1.3/32 via 192.168.1.3
   Tunnel0 created 03:08:01, expire 00:00:14
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 192.168.0.102
```

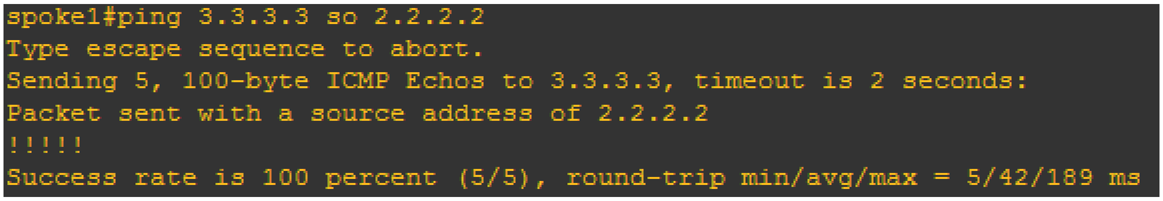
Check the routing table on a Cisco spoke router

Connect to one of the Cisco Spoke routers and check the routing table, you are expecting to see an EIGRP route to the Cisco hub router and an External EIGRP route to the TransPort router as this was via redistribution from OSPF.

```
Spoke1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [254/0] via 192.168.0.1
      1.0.0.0/24 is subnetted, 1 subnets
D        1.1.1.0 [90/26905600] via 192.168.1.1, 00:28:41, Tunnel0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, Ethernet0/1
L        2.2.2.2/32 is directly connected, Ethernet0/1
      3.0.0.0/24 is subnetted, 1 subnets
D EX     3.3.3.0 [170/26905600] via 192.168.1.3, 00:12:03, Tunnel0
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, Ethernet0/0
L        192.168.0.101/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Tunnel0
L        192.168.1.2/32 is directly connected, Tunnel0
Spoke1#
```

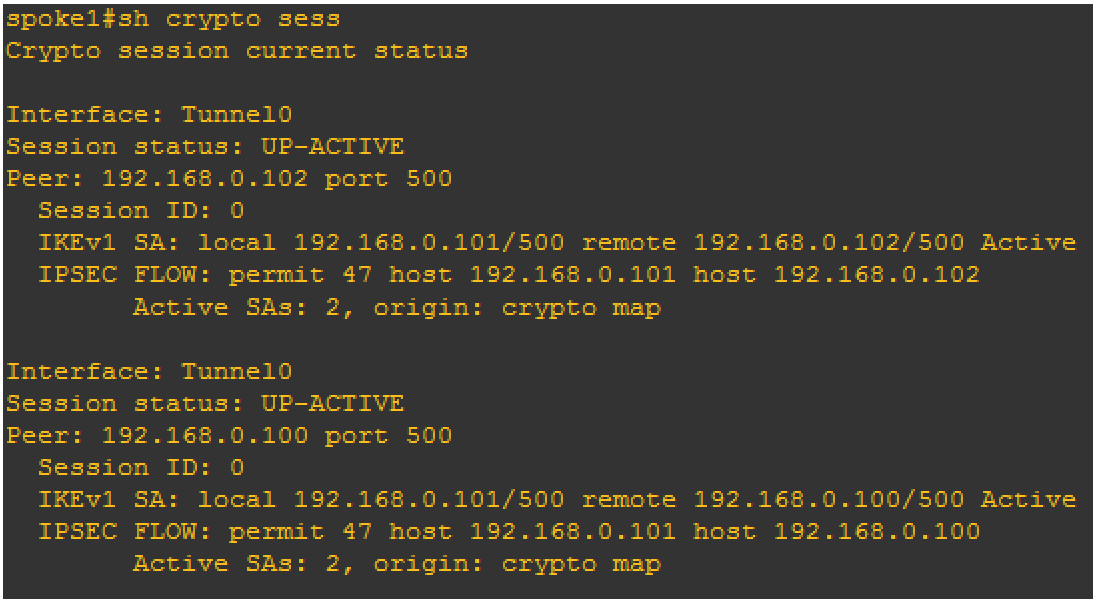
Send pings to the WR44 spoke router

Be sure to specify the correct source IP address, the IP address of 2.2.2.2



```
spoke1#ping 3.3.3.3 so 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/42/189 ms
```

Check IPsec sessions to confirm an IPsec SA direct with the WR44



```
spoke1#sh crypto sess
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 192.168.0.102 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.0.101/500 remote 192.168.0.102/500 Active
  IPSEC FLOW: permit 47 host 192.168.0.101 host 192.168.0.102
        Active SAs: 2, origin: crypto map

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 192.168.0.100 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.0.101/500 remote 192.168.0.100/500 Active
  IPSEC FLOW: permit 47 host 192.168.0.101 host 192.168.0.100
        Active SAs: 2, origin: crypto map
```

FIRMWARE VERSIONS

Digi TransPort WR44

```
Digi TransPort WR44v2-UX00-DE2-XX Ser#:239628
Software Build Ver6.1.0.3.  Jan 25 2018 17:13:23  LW
ARM Bios Ver 7.62u v45 800MHz B995-M1003-F80-O801,0 MAC:00042d03a80c
Async Driver              Revision: 1.19  Int clk
Wi-Fi                     Revision: 2.0
Ethernet Hub Driver       Revision: 1.11
Firewall                  Revision: 1.0
EventEdit                 Revision: 1.0
Timer Module              Revision: 1.1
AAL                       Revision: 1.0
DSL                       Revision: 1.0
(B)USBHOST                Revision: 1.0
SDMMC                     Revision: 1.0
L2TP                      Revision: 1.10
PPTP                      Revision: 1.00
TACPLUS                   Revision: 1.00
MODBUS                    Revision: 0.00
MySQL                     Revision: 0.01
RealPort                  Revision: 0.00
MultiTX                   Revision: 1.00
LAPB                      Revision: 1.12
X25 Layer                 Revision: 1.19
MACRO                     Revision: 1.0
PAD                       Revision: 1.4
X25 Switch                Revision: 1.7
V120                      Revision: 1.16
TPAD Interface            Revision: 1.12
GPS                       Revision: 1.0
TELITUPD                  Revision: 1.0
SCRIBATSK                 Revision: 1.0
BASTSK                    Revision: 1.0
PYTHON                    Revision: 1.0
CLOUDSMS                  Revision: 1.0
ARM Sync Driver           Revision: 1.18
TCP (HASH mode)           Revision: 1.14
TCP Utils                 Revision: 1.13
PPP                       Revision: 5.2
WEB                       Revision: 1.5
SMTP                      Revision: 1.1
FTP Client                Revision: 1.5
FTP                       Revision: 1.5
IKE                       Revision: 1.0
PollANS                   Revision: 1.2
PPPOE                     Revision: 1.0
BRIDGE                    Revision: 1.1
MODEM CC (Telit 3G)       Revision: 5.2
FLASH Write               Revision: 1.3
```

```
Command Interpreter       Revision: 1.38
SSLCLI                    Revision: 1.0
OSPF                      Revision: 1.0
BGP                       Revision: 1.0
QOS                       Revision: 1.0
PWRCTRL                   Revision: 1.0
RADIUS Client             Revision: 1.0
SSH Server                Revision: 1.0
SCP                       Revision: 1.0
SSH Client                Revision: 1.0
CERT                      Revision: 1.0
LowPrio                   Revision: 1.0
Tunnel                    Revision: 1.2
OVPN                      Revision: 1.2
TEMPLOG                   Revision: 1.0
QDL                       Revision: 1.0
OK
```

Cisco (Primary and Spoke)

```
sv9-2#sh ver
Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version
15.5(2)T, DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Thu 26-Mar-15 07:36 by prod_rel_team

ROM: Bootstrap program is Linux

sv9-3 uptime is 33 minutes
System returned to ROM by reload at 0
System image file is "unix:/opt/gns3/images/IOU/i86bi-linux-l3-
adventerprisek9-ms.155-2.T."
Last reload reason: Unknown reason



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found
at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Linux Unix (Intel-x86) processor with 349732K bytes of memory.
```

```
Processor board ID 2048002
8 Ethernet interfaces
8 Serial interfaces
256K bytes of NVRAM.



Configuration register is 0x0
```

CONFIGURATION FILES

Digi TransPort WR44

```
WR44>config c show
eth 0 descr "WAN"
eth 0 IPaddr "192.168.0.102"
eth 0 gateway "192.168.0.1"
eth 0 do_nat 1
eth 0 ipsec 1
eth 3 descr "INTERNAL"
eth 3 group 3
eth 3 IPaddr "3.3.3.3"
eth 3 group 3
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cidr ON
def_route 0 gateway "192.168.0.1"
def_route 0 ll_ent "ETH"
eroute 0 descr "DMVPN"
eroute 0 peerip "192.168.0.100"
eroute 0 peerid "192.168.0.100"
eroute 0 ourid "192.168.0.102"
eroute 0 ouridtype 3
eroute 0 locip "192.168.0.102"
eroute 0 locmsk "255.255.255.255"
eroute 0 remip "192.168.0.100"
eroute 0 remmsk "255.255.255.255"
eroute 0 ESPauth "MD5"
eroute 0 ESPenc "3DES"
eroute 0 proto "GRE"
eroute 0 ltime 1200
eroute 0 lkbytes 4608000
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 debug ON
eroute 1 descr "NHRP"
eroute 1 peerip "NHRP"
eroute 1 peerid "*"
eroute 1 ourid "192.168.0.102"
eroute 1 ouridtype 3
eroute 1 locip "192.168.0.102"
eroute 1 locmsk "255.255.255.255"
eroute 1 remip "192.168.0.0"
eroute 1 remmsk "255.255.255.0"
eroute 1 ESPauth "md5"
eroute 1 ESPenc "3des"
eroute 1 proto "gre"
eroute 1 authmeth "preshared"
eroute 1 nosa "try"
eroute 1 debug ON
dhcp 0 respdelms 4000
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
dhcp 3 IPmin "3.3.3.3"
dhcp 3 IPrange 1
dhcp 3 lease 30
dhcp 3 mask "255.255.255.0"
dhcp 3 gateway "3.3.3.2"
sntp 0 server "time.etherios.com"
sockopt 0 sock_inact 9000
ppp 0 timeout 300
ppp 1 name "W-WAN (HSPA 3G)"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 r_chap OFF
ppp 3 name "DSL"
ppp 3 l1iface "AAL"
ppp 3 username "Enter ADSL Username"
ppp 3 r_addr OFF
ppp 3 IPaddr "0.0.0.0"
ppp 3 l_addr ON
ppp 3 timeout 0
ppp 3 do_nat 2
ppp 3 immoos ON
ppp 3 echo 10
ppp 3 echodropcnt 5
ppp 3 l_pap OFF
ppp 3 l_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
modemcc 0 info_asy_add 6
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Your.APN.goes.here"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 anon ON
ana 0 l1on ON
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 ipaddfilt "~192.168.0.101,2.2.2.2"
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "WR44>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 1
cmd 0 tremto 1200
cmd 0 rcihttp ON
cmd 4 cmd_processor OFF
user 0 access 0
user 1 name "username"
user 1 epassword "KD5lSVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 name "*"
user 9 epassword "OzZlWUodFQ8="
user 9 access 0
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ospf 0 enable ON
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
tun 0 descr "GRE to DMVPN"
tun 0 IPaddr "192.168.1.3"
tun 0 source "192.168.0.102"
tun 0 dest "192.168.0.100"
tun 0 kadelay 3
tun 0 usekey ON
tun 0 mgre ON
tun 0 nhs "192.168.1.1"
tun 0 nhrp_auth "cisco123"
cloud 0 ssl ON
OK
```

Cisco Primary (hub)

```
hub#sh run
Building configuration...

Current configuration : 3252 bytes
!
! Last configuration change at 15:05:26 UTC Tue Feb 27 2018
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname hub
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$62FK$OsITedYtDxU6GlrAX0EPN/
!
no aaa new-model
!
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
!
!
!
!
!
!
!
no ip domain lookup
ip domain name lab.local
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
cts logging verbose
!
!
```

```
archive
 log config
  hidekeys
!
redundancy
!
!
ip tcp synwait-time 5
!
!
!
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
!
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
 mode tunnel
!
crypto ipsec profile cisco
 set security-association lifetime seconds 1200
 set transform-set strong
!
!
!
!
!
!
!
interface Tunnel0
 ip address 192.168.1.1 255.255.255.0
 no ip redirects
 ip mtu 1440
 no ip next-hop-self eigrp 90
 no ip split-horizon eigrp 90
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 600
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
 ip address 192.168.0.100 255.255.255.0
!
interface FastEthernet0/1
 ip address 1.1.1.1 255.255.255.0
 ip ospf network point-to-point
!
!
!
```

```
router eigrp 90
 network 1.1.1.0 0.0.0.255
 network 192.168.1.0
 redistribute ospf 1 metric 10000 100 255 1 1500
!
router ospf 1
 router-id 1.1.1.1
 priority 100
 redistribute eigrp 90 metric 100 subnets
 passive-interface default
 no passive-interface Tunnel0
 network 1.1.1.1 0.0.0.0 area 0
 network 192.168.1.1 0.0.0.0 area 0
!
ip forward-protocol nd
!
!
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.0.1 254
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 transport preferred ssh
 transport output all
 escape-character 27
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 transport preferred ssh
 transport output all
line vty 0 4
 password cisco
 login
 transport preferred ssh
 transport input all
 transport output all
!
!
end
```

Cisco Spoke

```
spoke1#sh run
Building configuration...

Current configuration : 2995 bytes
!
! Last configuration change at 11:51:41 UTC Tue Feb 27 2018
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname spoke1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$RaUY$W5uw7ZNp7mMfIm2CK4dOT/
!
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip domain name lab.local
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
cts logging verbose
!
!
archive
 log config
  hidekeys
!
redundancy
```

```
!
!
ip tcp synwait-time 5
!
!
!
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
!
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
 mode tunnel
!
crypto ipsec profile cisco
 set security-association lifetime seconds 120
 set transform-set strong
!
!
!
!
!
!
!
interface Tunnel0
 ip address 192.168.1.2 255.255.255.0
 no ip redirects
 ip mtu 1440
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp map 192.168.1.1 192.168.0.100
 ip nhrp map multicast 192.168.0.100
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip nhrp nhs 192.168.1.1
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
 ip address 192.168.0.101 255.255.255.0
!
interface FastEthernet0/1
 ip address 2.2.2.2 255.255.255.0
!
!
!
router eigrp 90
 network 2.2.2.0 0.0.0.255
 network 192.168.1.0
!
ip forward-protocol nd
```

```
!
!
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.0.1 254
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 transport preferred ssh
 transport output all
 escape-character 27
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 transport preferred ssh
 transport output all
line vty 0 4
 password cisco
 login
 transport preferred ssh
 transport input all
 transport output all
!
!
end
```