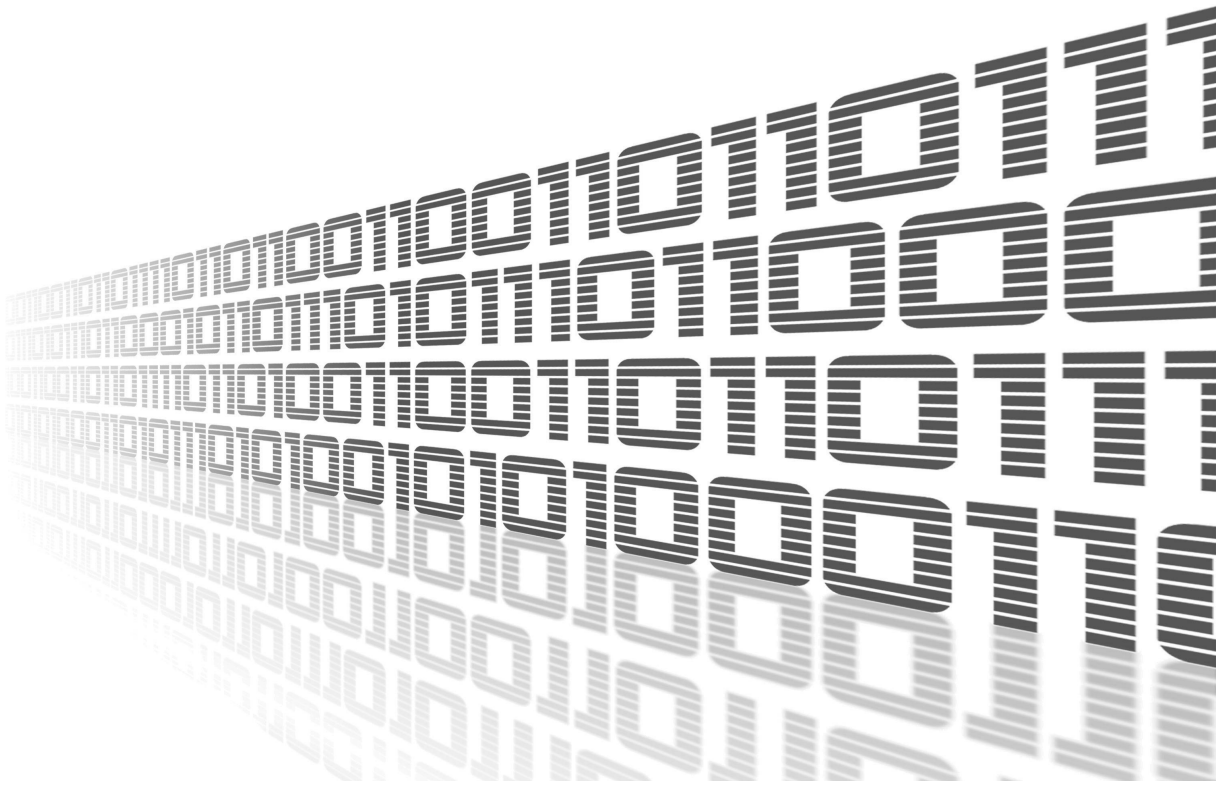
RouterApp

Dynamic Multipoint VPN

APPLICATION NOTE



ADVANTECH

Used symbols

Danger – Information regarding user safety or potential damage to the router.

Attention – Problems that may arise in specific situations.

Information or notice – Useful tips or information of special interest.

Example – Example of function, command or script.

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. APP-0052-EN, revised on October 4, 2022. Released in the Czech Republic.

Contents

1 Basic Information **1**

1.1 Architecture 1
1.2 Necessary Requirements 2

2 Configuration Example **3**

2.1 Headquarter Hub Router Configuration 4
2.2 GRE Tunnel Configuration 6
2.2.1 Configure the other Spoke (Router B) 7
2.3 IPsec Configuration 7
2.4 NHRP Configuration – NHRP Router App 14
2.5 BGP Configuration – FRR Router App 17
2.6 Zebra Configuration – FRR Router App 20
2.7 Check the Function of Dynamic Multipoint VPN 22

3 Related Documents **24**

List of Figures

1 DMVPN architecture . . . 2
2 Configuration example scheme . . . 3
3 Router A – GRE configuration . . . 6
4 Router B – GRE configuration . . . 7
5 IPsec Router A configuration Part 1 . . . 8
6 IPsec Router A configuration Part 2 . . . 9
7 IPsec Router A configuration Part 3 . . . 10
8 IPsec Router B configuration Part 1 . . . 11
9 IPsec Router B configuration Part 2 . . . 12
10 IPsec Router B configuration Part 3 . . . 13
11 NHRP router app configuration . . . 14
12 BGP configuration Router A Part 1 . . . 17
13 BGP configuration Router A Part 2 . . . 18
14 BGP configuration Router B . . . 19
15 Zebra configuration Router A . . . 20
16 Zebra configuration Router B . . . 21
17 Router A – System Log with the NHRP registration success message . . . 22
18 Router C – Route Table . . . 22

List of Tables

1 Router A – GRE configuration . . . 6

1. Basic Information

The described router apps *FRR* and *NHRP* are not contained in the standard router firmware. Uploading of this router app is described in the Configuration manual (see Chapter Related Documents).

A Dynamic Multipoint VPN (DMVPN) is a concept of the secure network that exchanges data between remote routers ("spokes") without needing to pass traffic through a headquarter virtual private network (VPN) router ("hub"). Each spoke is permanently connected to the headquarter (hub) using VPN tunnel. If two spokes need to communicate to each other, temporary VPN tunnel is created between them (headquarter has a role of NHRP server). Tunnels are canceled after finishing of communication. The DMVPN allows establishing VPN tunnels between routers with dynamically assigned port addresses (this is not possible when using "classical" site-to-site VPN). The DMVPN essentially creates a topology that could be called *(full) mesh VPN*. This means that each remote router (spoke) can connect directly to all other remote routers, no matter where they are located.

Spoke-to-spoke capability is not currently supported in our DMVPN solution.

1.1 Architecture

DMVPN concept includes mechanisms such as GRE tunneling and IPsec encryption with Next Hop Resolution Protocol (NHRP) routing that are designed to reduce administrative burden and provide reliable dynamic connectivity between sites.

Key components:

- **Multipoint GRE (mGRE)** – Allows a single GRE interface to support multiple IPsec tunnels (i.e. one mGRE interface supports all spokes), simplifying the size and complexity of the configuration.
- **Dynamic IPsec protocol encryption** – Secures (encrypts) data transmitted through VPN tunnels.
- **Next-Hop Resolution Protocol (NHRP)** – The headquarter router (hub) maintains an NHRP database of the public interface addresses of the each spoke. Each spoke registers its real address on boot. When direct tunnels with other spokes are requested, it queries the NHRP database for real addresses of the spokes' destinations. When the connection is not needed, it is terminated (VPN tunnel is canceled).

The following figure shows the way Dynamic Multipoint VPN concept works. Headquarter router with NHRP database is referred to as *HUB*, remote routers are referred to as *Spoke A* and *Spoke B*.

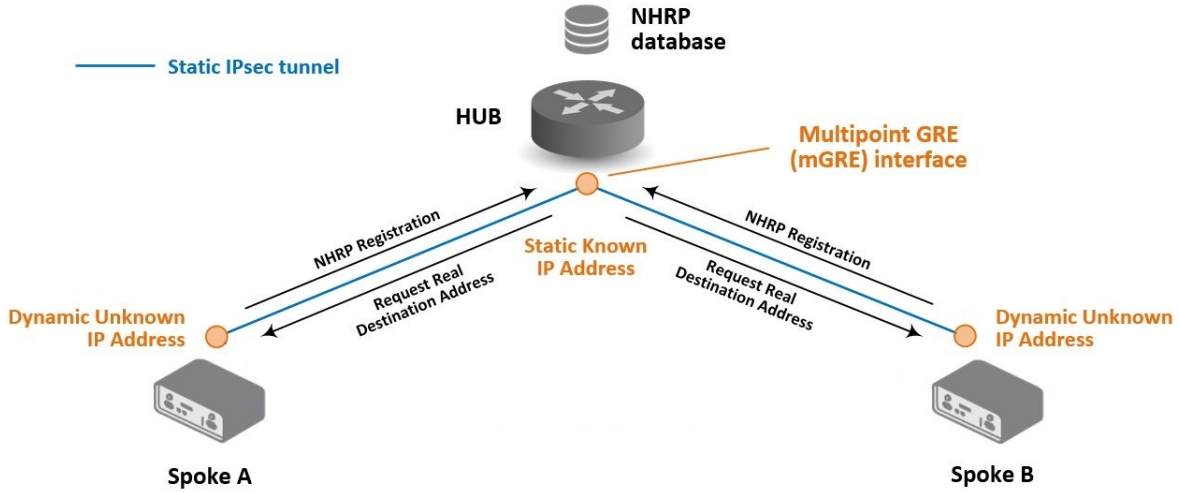


Figure 1: DMVPN architecture

1.2 Necessary Requirements

- Cisco headquarter hub router and connection to the Internet from hub and all spokes. Only Cisco router can be used as headquarter hub router.
- *NHRP* router app in every spoke router.
- *FRR* router app in every spoke router.
- GRE tunnel configuration in every spoke router (with proper IP routes).

See the example configuration below for more details.

2. Configuration Example

For a configuration example two Advantech routers were used as spokes - router A and router B and one Cisco ISR4331 router as headquarter hub.

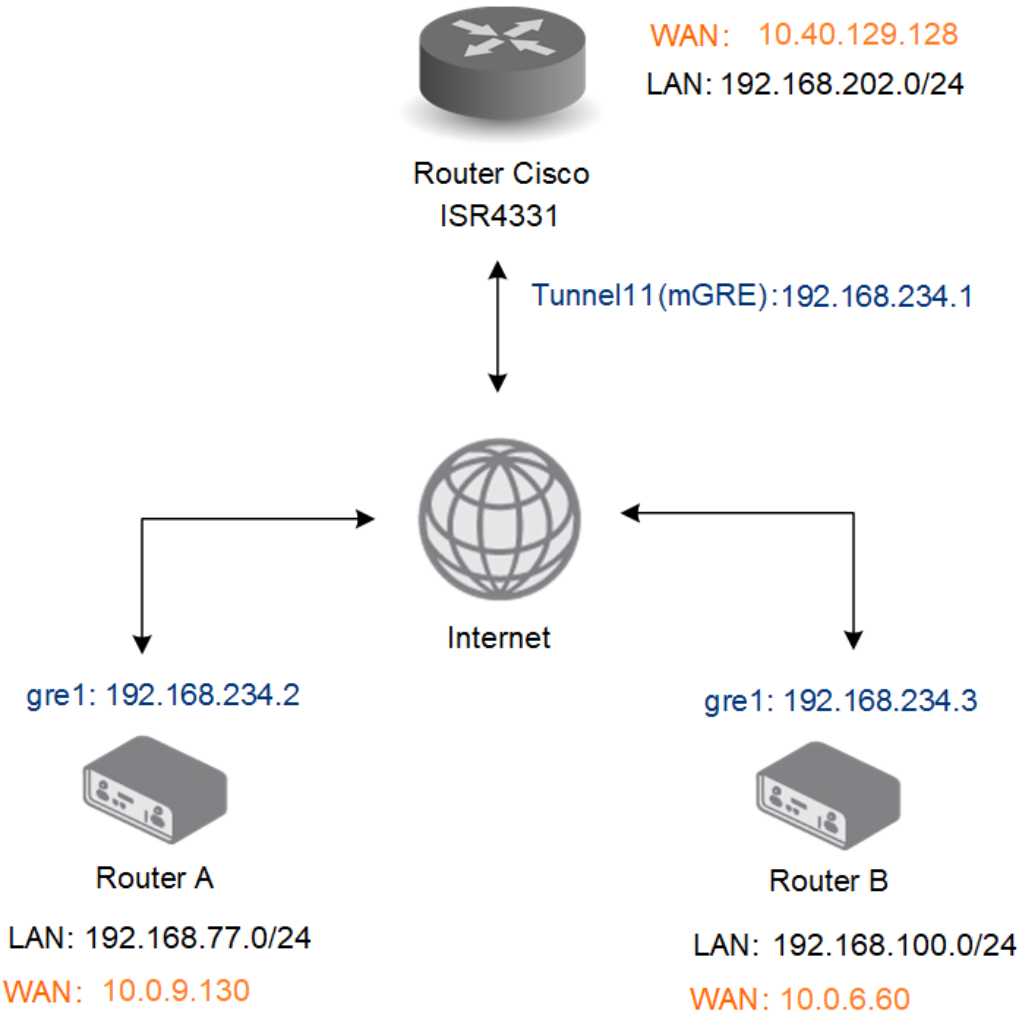


Figure 2: Configuration example scheme

2.1 Headquarter Hub Router Configuration

In this example configuration, the Cisco ISR4331 router was used as the headquarter hub router. The necessary configuration is the following. (Log-in to the Cisco router console and type `config terminal` command. Refer to proper Cisco manual for the instructions how to configure the Cisco router.) More about IPsec Tunnel and certificate generation can be found in IPsec Tunnel Application Note [7]

```
!
crypto pki trustpoint server.cisco
enrollment pkcs12
revocation-check none
rsakeypair server.cisco
!
crypto pki certificate map ike_v2_certmap 10
subject-name co client
!
crypto pki certificate chain server.cisco
certificate 29BEF8C0BE9377F585E4C9E7E569B4B1FEA8544A
308203C2 308202AA A0030201 02021429 BEF8C0BE 9377F585 E4C9E7E5 69B4B1FE
A8544A30 0D06092A 864886F7 0D01010B 05003081 8E310B30 09060355 04061302
...
D1A4308D 19992469 0FB6A78F DCAD252B E83C040E 087BC4E0 F0379F41 02EEC176
56937ECD 03926DF0 3B782620 E1116E19 256426CB D188D214 5DF5A7AC D1E755E5
BDE3837E C26D
quit
certificate ca 29BEF8C0BE9377F585E4C9E7E569B4B1FEA8543C
308203FF 308202E7 A0030201 02021429 BEF8C0BE 9377F585 E4C9E7E5 69B4B1FE
A8543C30 0D06092A 864886F7 0D01010B 05003081 8E310B30 09060355 04061302
...
C319BFFF 3645B107 EA089A1A 9C3BC558 9AA9FF3F EA735430 83E7E464 B5311867
CF1E190B 020AB854 052B06A5 6883BA55 7C604513 82ED6A63 5CF567FD 66F49EE8 899C7B
quit
!
crypto ikev2 proposal ike_v2_proposal
encryption aes-gcm-256
prf sha256
group 21
!
crypto ikev2 policy ike_v2_policy
proposal ike_v2_proposal
!
!
crypto ikev2 profile ike_v2_profile
match certificate ike_v2_certmap
identity local fqdn server.cisco
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint server.cisco
!
crypto ipsec transform-set aes-gcm esp-gcm 256
mode transport
!
crypto ipsec profile FlexVPN
```

```
set security-policy limit 100
set transform-set aes-gcm
set pfs group21
set ikev2-profile ike_v2_profile
responder-only
!
interface Tunnel11
ip address 192.168.234.1 255.255.255.0
no ip redirects
ip nhrp network-id 1234
no ip nhrp record
no ip nhrp cache non-authoritative
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel key 1234
tunnel protection ipsec profile FlexVPN
!
interface GigabitEthernet0/0/0
ip address 10.40.29.128 255.255.252.0
ip nat outside
ip access-group 101 in
negotiation auto
spanning-tree portfast disable
!
interface GigabitEthernet0/0/1
no ip address
negotiation auto
spanning-tree portfast trunk
!
interface GigabitEthernet0/0/1.202
encapsulation dot1Q 202
ip address 192.168.202.254 255.255.255.0
!
router bgp 65001
bgp router-id 192.168.234.1
bgp log-neighbor-changes
bgp listen range 192.168.234.0/24 peer-group DMVPN_SPOKES
network 192.168.202.0
neighbor DMVPN_SPOKES peer-group
neighbor DMVPN_SPOKES remote-as 65001
neighbor DMVPN_SPOKES route-reflector-client
neighbor DMVPN_SPOKES route-map SPOKE_ROUTERS out
!
route-map SPOKE_ROUTERS permit 10
!
```

2.2 GRE Tunnel Configuration

Create the GRE tunnels between the headquarter (hub router) and remote routers (spokes).

Open the Web interface of the first spoke (*Router A*) and press *GRE* item in the *Configuration* section and then select *1st Tunnel*. Fill in the configuration form as indicated in the Figure and Table below.

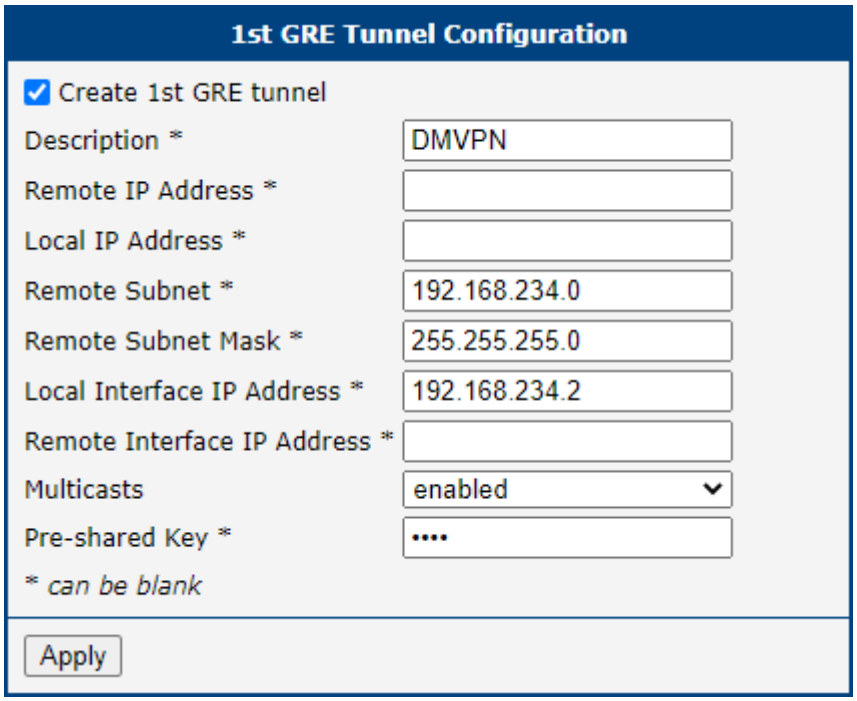


Figure 3: Router A – GRE configuration

Item	Value
Remote Subnet	192.168.234.0 *(Cisco headquarter hub)*
Local Interface IP Address	192.168.234.2
Pre-shared Key	1234

Table 1: Router A – GRE configuration

2.2.1 Configure the other Spoke (Router B)

Make the same configuration for Advantech routers B. Change only the local side of the tunnel IP address.

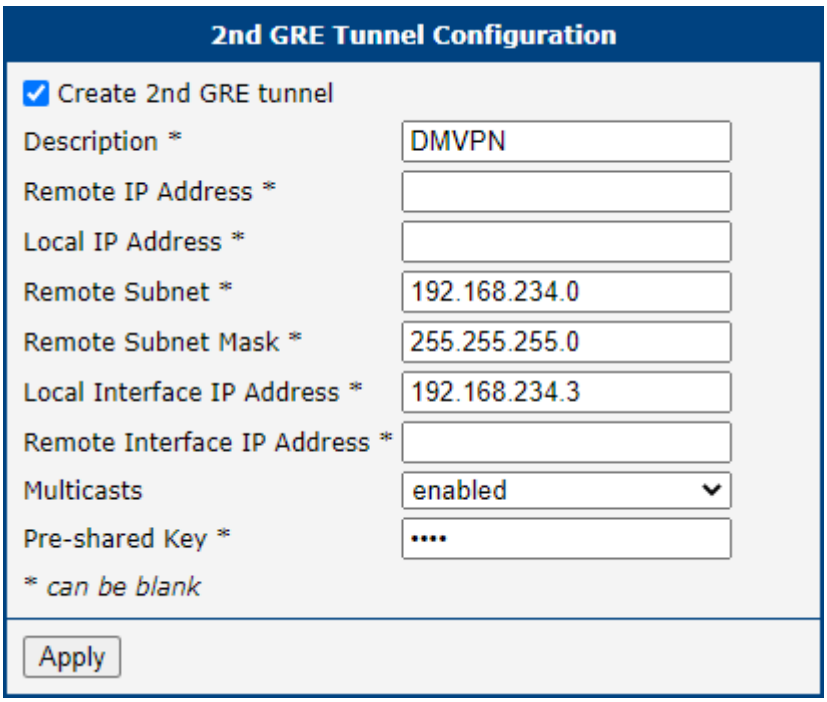


Figure 4: Router B – GRE configuration

2.3 IPsec Configuration

It is necessary to configure IPsec for remote Advantech routers A and B (spokes) to ensure the security (encryption) of tunnel connections.

Open the Web interface of the first spoke (*Router A*) and press *IPsec* item in the *Configuration* section and then select *1st Tunnel*. Fill in the configuration form as indicated in the Figure and Table below.

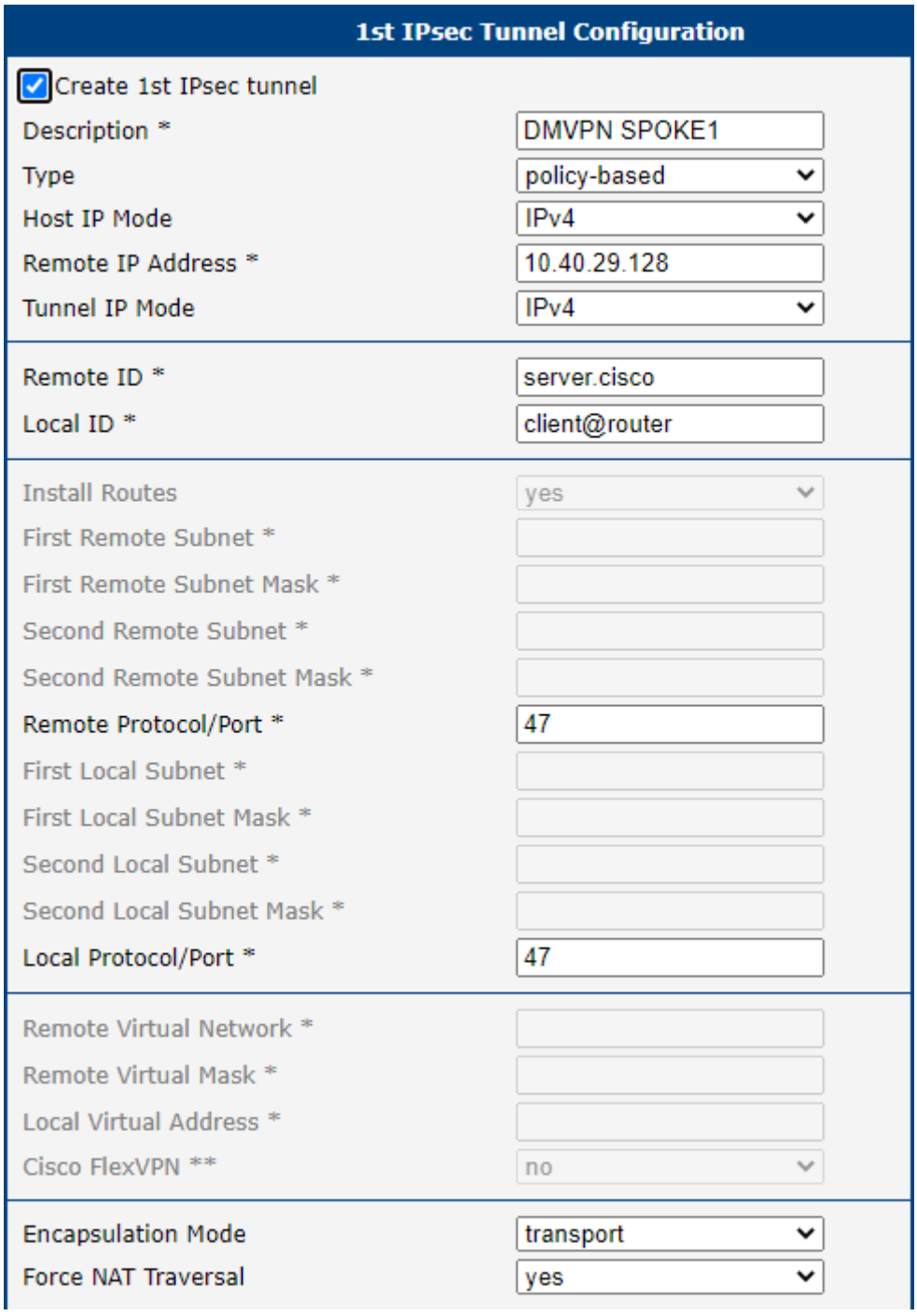


Figure 5: IPsec Router A configuration Part 1

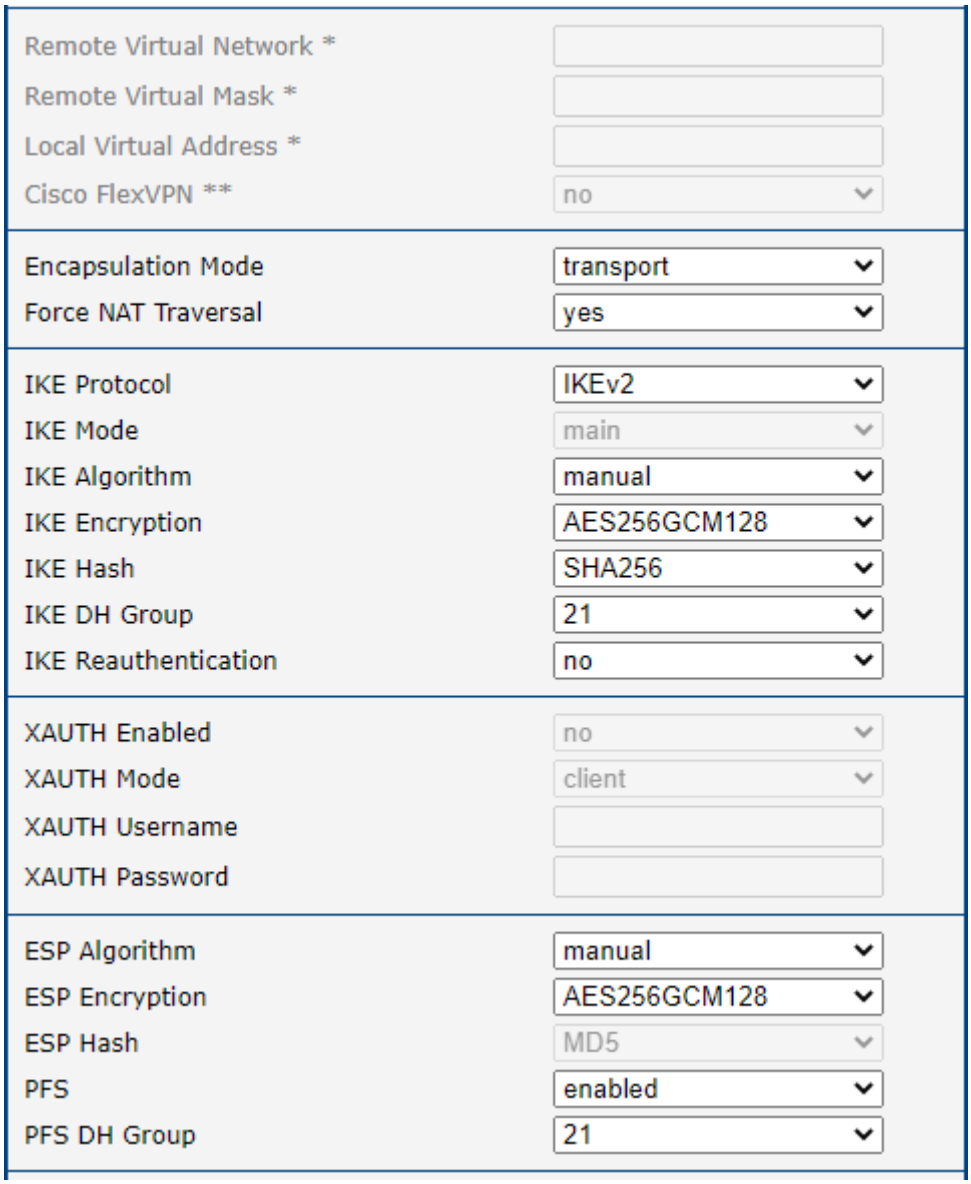


Figure 6: IPsec Router A configuration Part 2

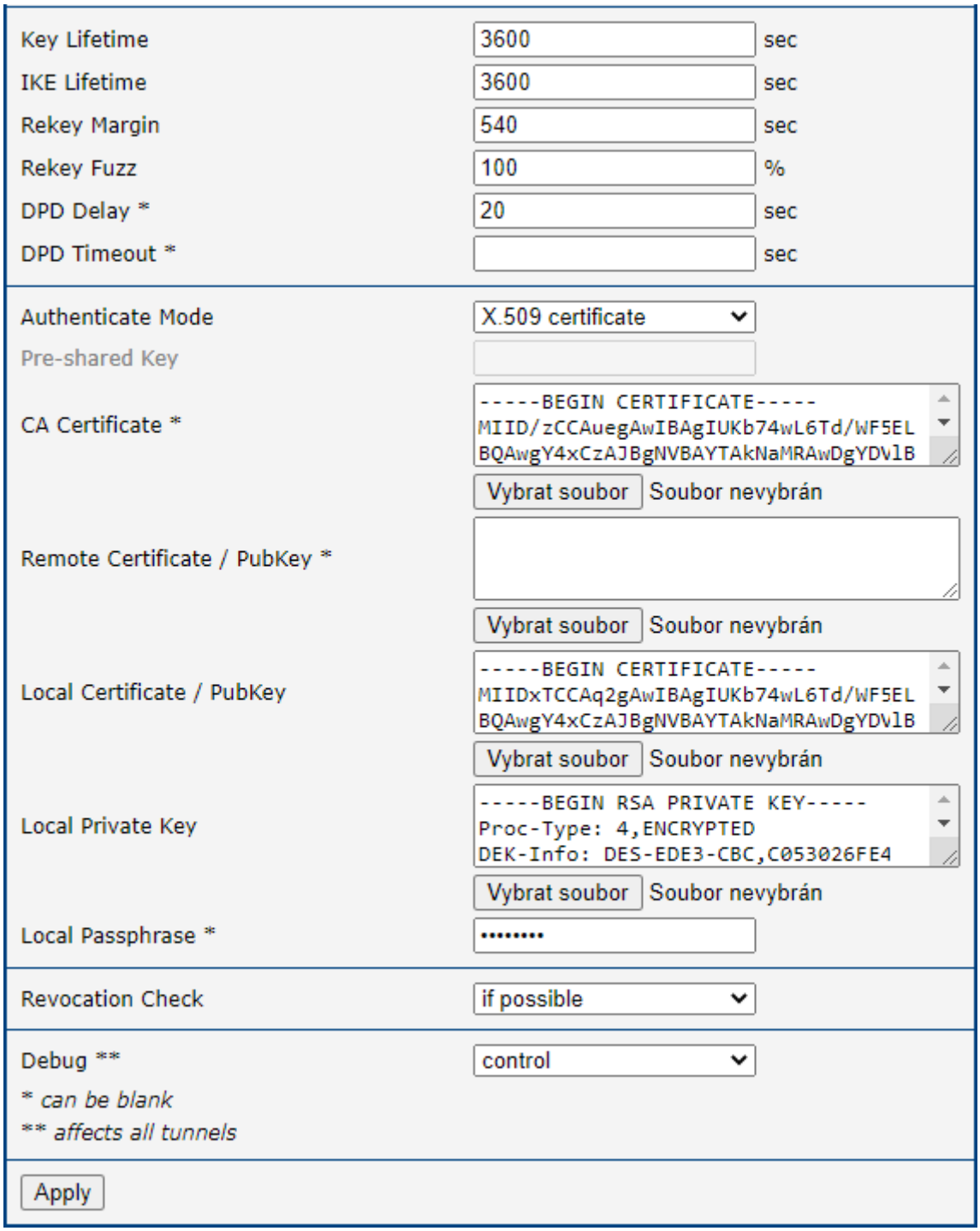


Figure 7: IPsec Router A configuration Part 3

Save the changes using the *Apply* button. Use the same procedure for all spokes – the *IPsec* For Router B the configuration should look like this:

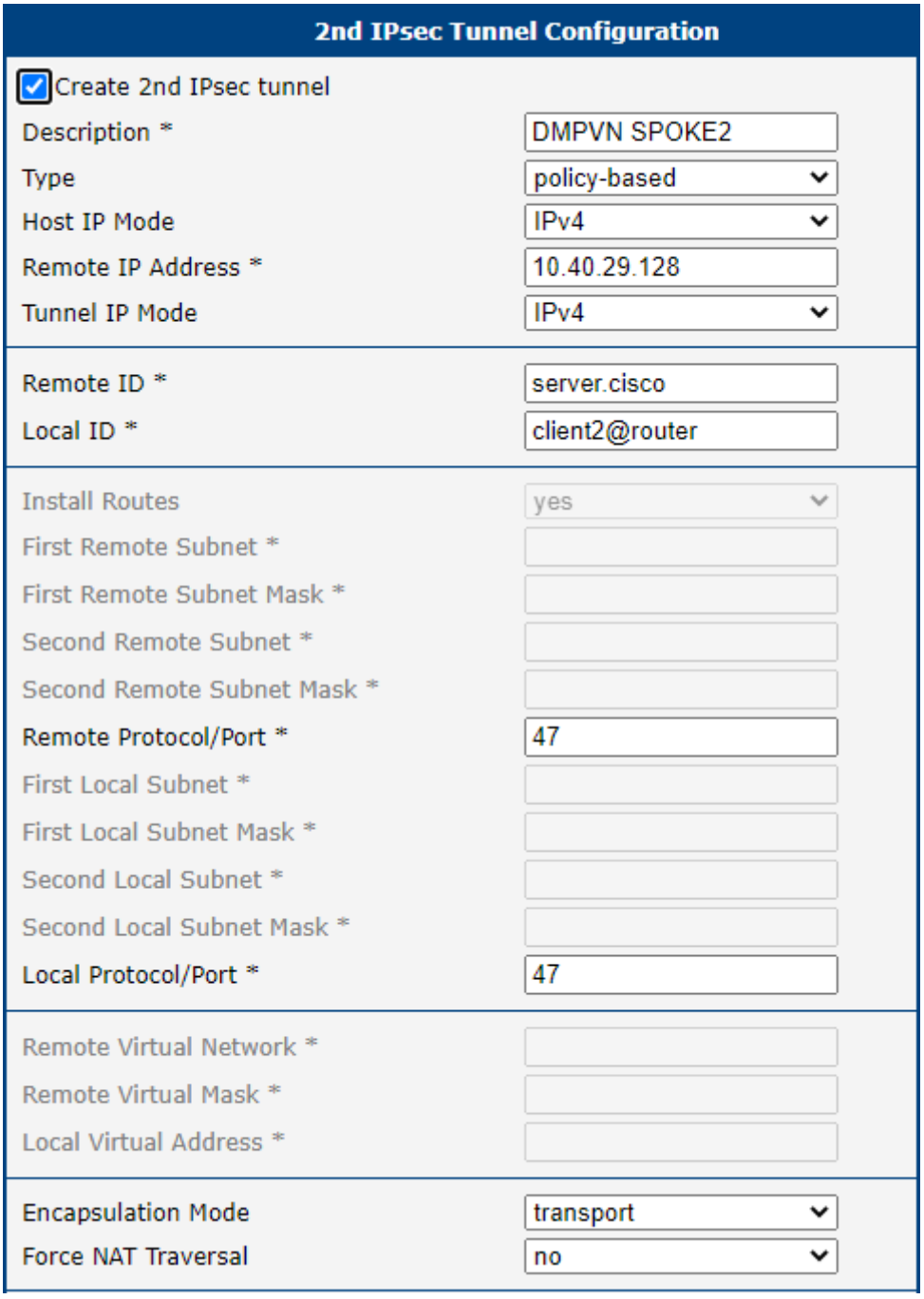


Figure 8: IPsec Router B configuration Part 1

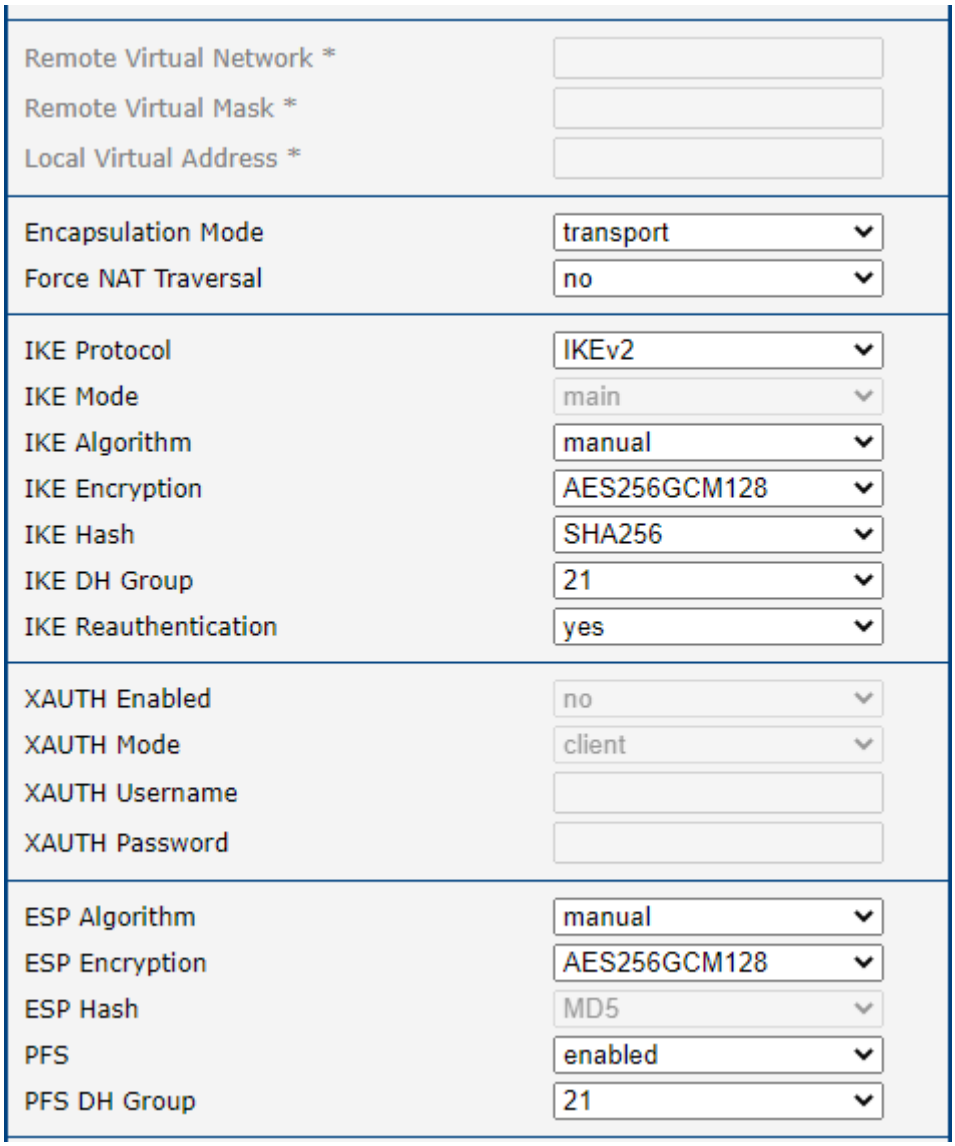


Figure 9: IPsec Router B configuration Part 2

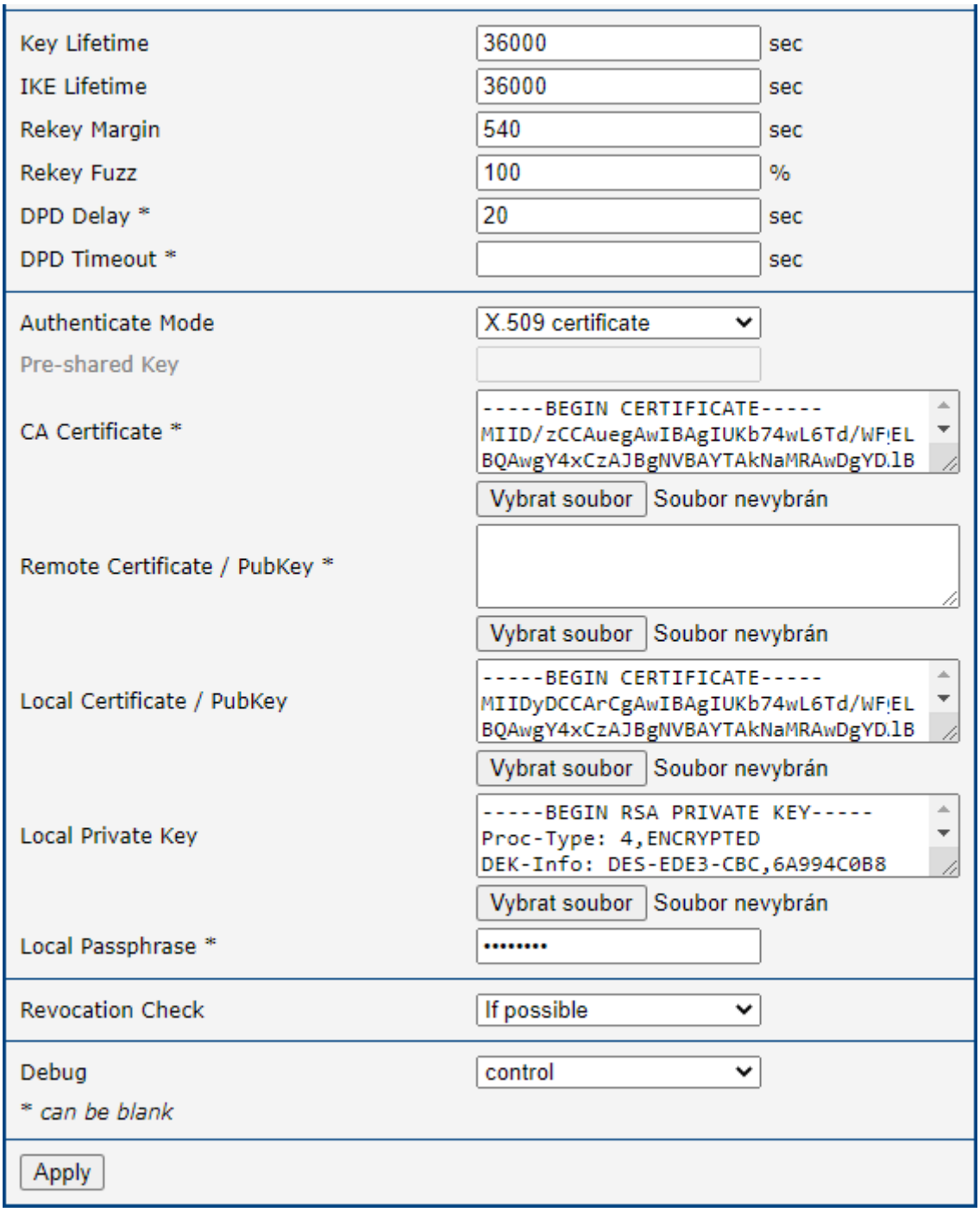


Figure 10: IPsec Router B configuration Part 3

2.4 NHRP Configuration – NHRP Router App

NHRP configuration can be done via the *NHRP* router app. The *OpenNHRP* Linux implementation of NHRP – Next-Hop Resolution Protocol – is used in the router app. It is Cisco DMVPN compatible.

The router app *NHRP* is not part of the standard router firmware. See the Configuration Manual ([1, 2]) for the description of uploading the router app to the router.

Go to the *Router Apps* page and then *NHRP* to configure the *NHRP* router app. Tick the *Enable NHRP* box and insert the configuration commands in the fields.

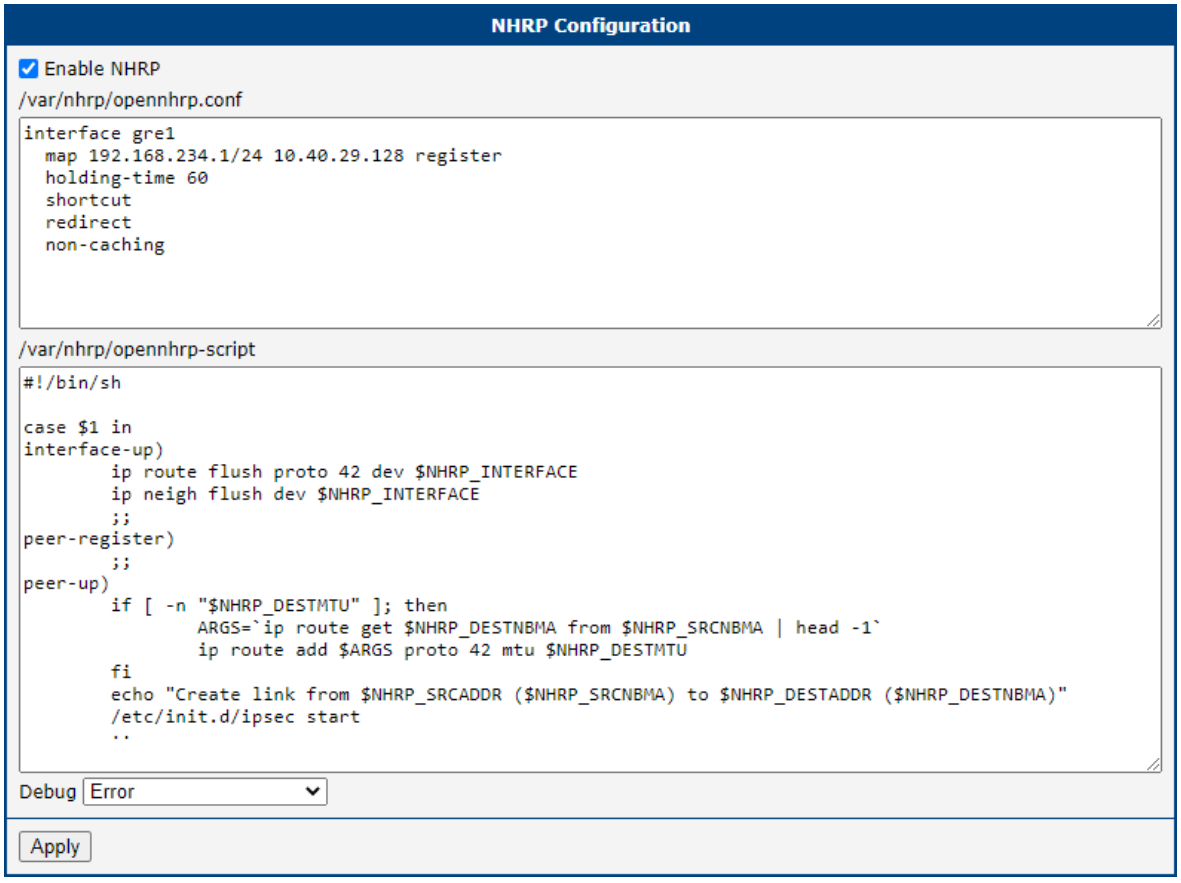


Figure 11: NHRP router app configuration

Field */var/nhrp/opennhrp.conf* – insert the following configuration. It is to register the proper interface to the NHRP headquarter hub router and other needed parameters (edit to your own needs).

```
1   interface gre1
2   map 192.168.234.1/24 10.40.29.128 register
3   holding-time 60
4   shortcut
5   redirect
6   non-caching
```

Field */var/nhrp/opennhrp-script* – this is the *OpenNHRP* script to define the behavior in various situations. You can left it unchanged. If you accidentally edit it, you can copy it from the next page.

Press the *Apply* button to save the changes. Use the same procedure for all spokes – the *NHRP Configuration* remains the same for all the spoke routers.

Field */var/nhrp/opennhrp-script*

```
1  #!/bin/sh
2
3  case $1 in
4  interface-up)
5  ip route flush proto 42 dev $NHRP_INTERFACE
6  ip neigh flush dev $NHRP_INTERFACE
7  ;;
8  peer-register)
9  ;;
10 peer-up)
11 if [ -n "$NHRP_DESTMTU" ]; then
12 ARGS=‘ip route get $NHRP_DESTNBMA from $NHRP_SRCNBMA | head -1‘
13 ip route add $ARGS proto 42 mtu $NHRP_DESTMTU
14 fi
15 echo "Create link from $NHRP_SRCADDR ($NHRP_SRCNBMA) to $NHRP_DESTADDR (
       $NHRP_DESTNBMA)"
16 /etc/init.d/ipsec start
17 ;;
18 peer-down)
19 echo "Delete link from $NHRP_SRCADDR ($NHRP_SRCNBMA) to $NHRP_DESTADDR (
       $NHRP_DESTNBMA)"
20 if [ "$NHRP_PEER_DOWN_REASON" != "lower-down" ]; then
21 /etc/init.d/ipsec stop
22 fi
23 ip route del $NHRP_DESTNBMA src $NHRP_SRCNBMA proto 42
24 ;;
25 route-up)
26 echo "Route $NHRP_DESTADDR/$NHRP_DESTPREFIX is up"
27 ip route replace $NHRP_DESTADDR/$NHRP_DESTPREFIX proto 42 via $NHRP_NEXTHOP dev
       $NHRP_INTERFACE
28 ip route flush cache
```

```
29 ;;
30 route-down)
31 echo "Route $NHRP_DESTADDR/$NHRP_DESTPREFIX is down"
32 ip route del $NHRP_DESTADDR/$NHRP_DESTPREFIX proto 42
33 ip route flush cache
34 ;;
35 esac
36
37 exit 0
```

2.5 BGP Configuration – FRR Router App

BGP configuration can be done via the *FRR* router app.

The router app *FRR* is not part of the standard router firmware. See the Configuration Manual ([1, 2]) for the description of uploading the router app to the router.

Go to the *Router apps* page and then find the *FRR* item in the Configuration section to configure the *BGP* protocol of this router. In the *BGP* tick the *Enable BGP* box and insert the configuration commands in the field.

Configuration for Router A should look like this:

BGP Configuration

Enable BGP

```
!
! Default configuration with enabled vty
! Change password!!!
!
password conel
enable password conel
!
line vty
!
log syslog
!
router bgp 65001
 bgp router-id 192.168.234.2
 bgp log-neighbor-changes
 no bgp ebgp-requires-policy
!
 neighbor 192.168.234.1 remote-as 65001
 neighbor 192.168.234.1 disable-connected-check
!
 address-family ipv4 unicast
   network 192.168.100.0/24
 exit-address-family
 timers bgp 3 15
!
debug bgp neighbor-events
debug bgp zebra
debug bgp nht
debug bgp updates
!
!
```

Figure 12: BGP configuration Router A Part 1

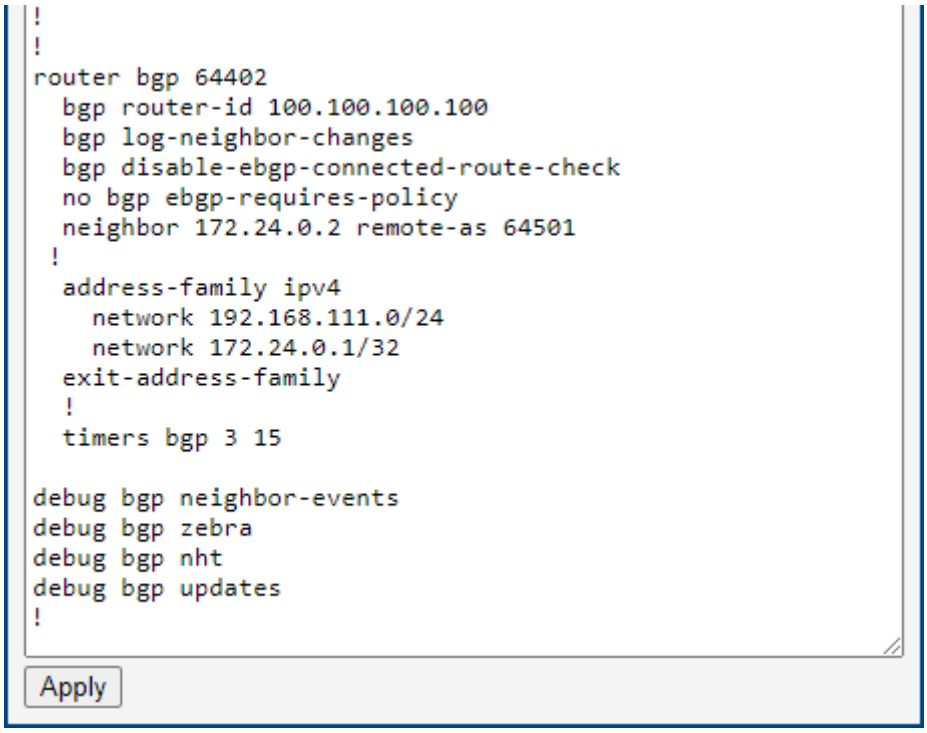


Figure 13: BGP configuration Router A Part 2

and BGP configuration for router B can be like this:

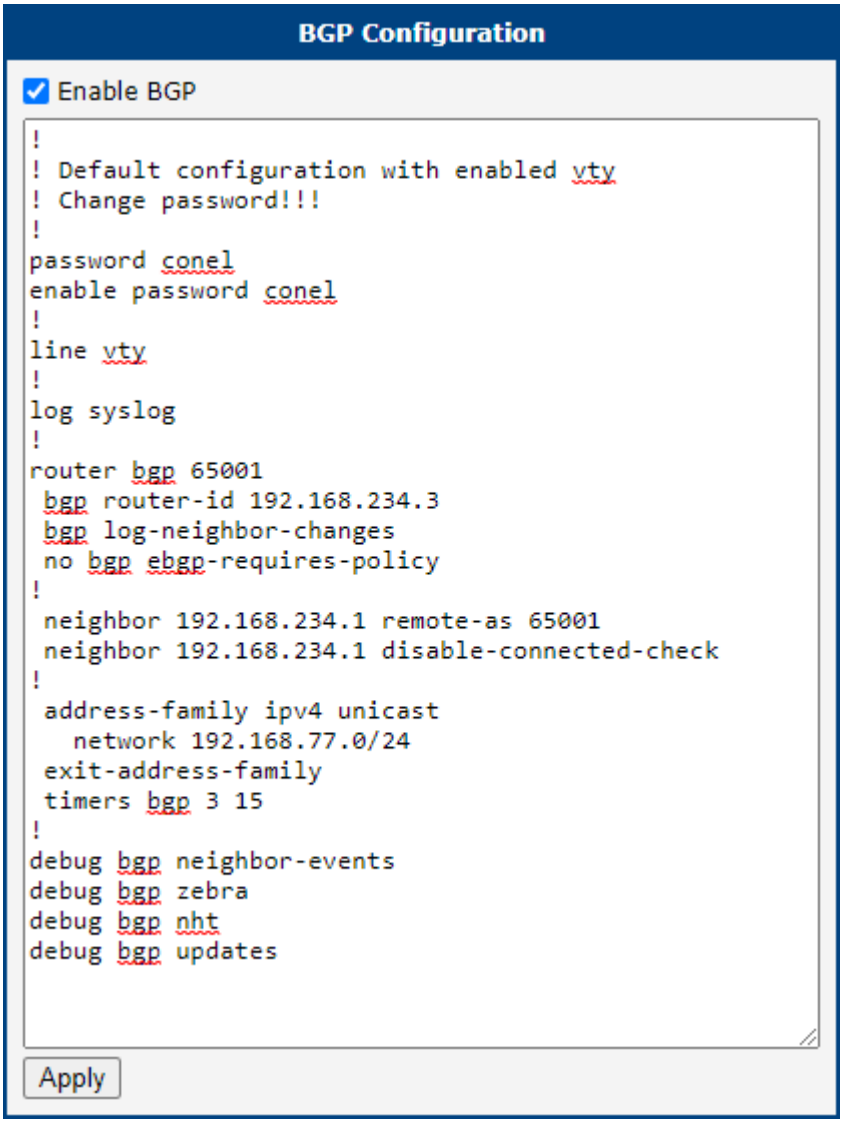


Figure 14: BGP configuration Router B

2.6 Zebra Configuration – FRR Router App

Like in BGP section before, the Zeebra configuration can be done via the *FRR* router app.

Go to the *Router Apps* page and then find the *FRR* item in the Configuration section to configure the *ZEBRA* protocol of this router. In the *ZEBRA* tick the *Enable ZEBRA* box and insert the configuration commands in the field.

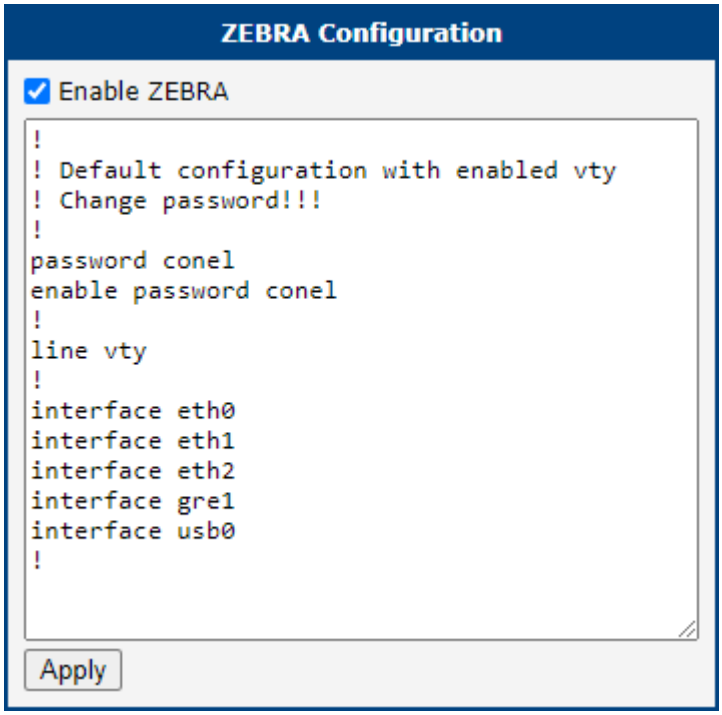


Figure 15: Zebra configuration Router A

and for router B the ZEBRA configuration should be:

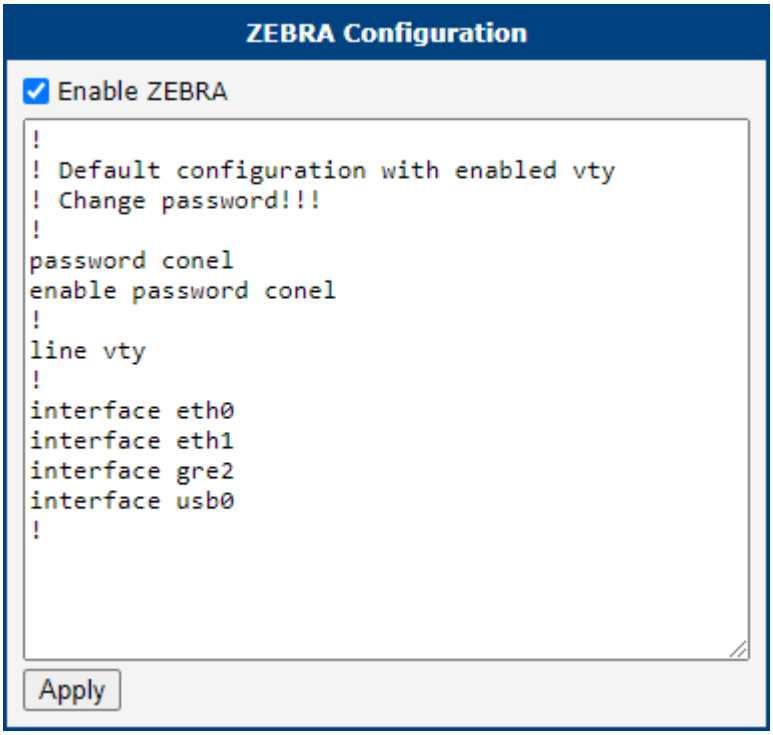


Figure 16: Zebra configuration Router B

2.7 Check the Function of Dynamic Multipoint VPN

If the configuration is done correctly, the following information will be displayed on *System Log* page of router A and B. The router is sending NHRP Registration Request and is receiving the success message (same on router A and B):

```
Received Registration Reply from 192.168.234.1:  success
```

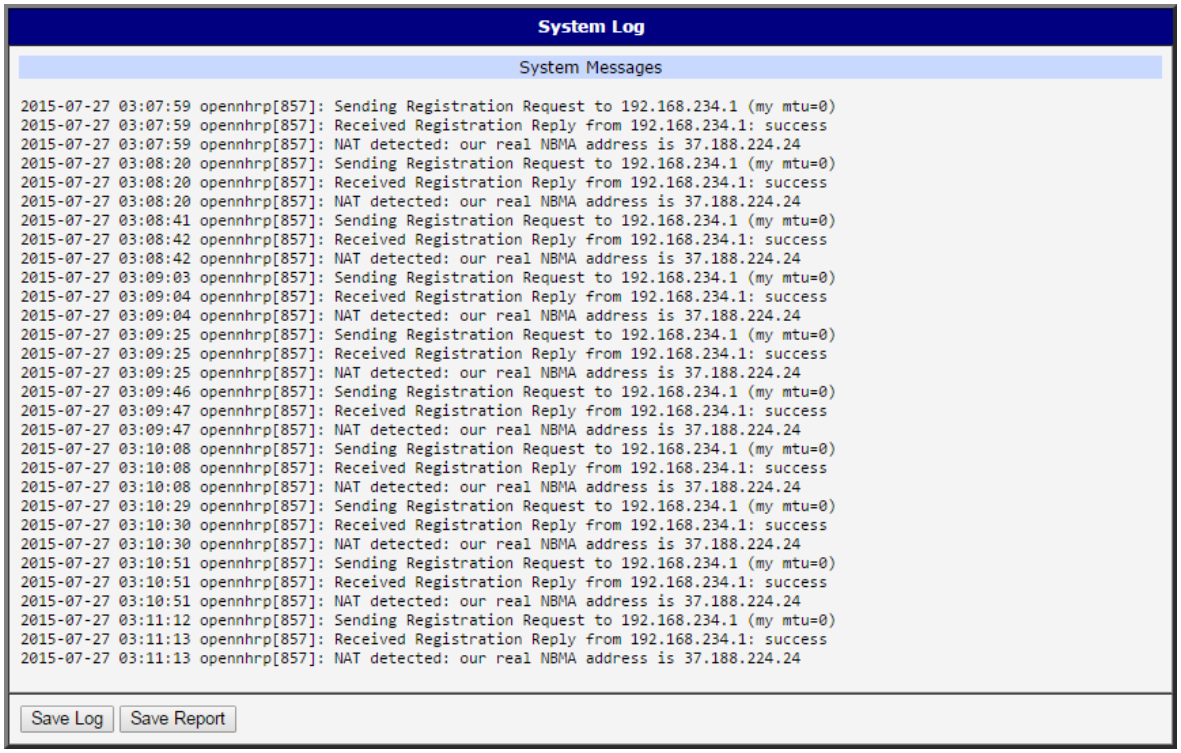


Figure 17: Router A – System Log with the NHRP registration success message

You should see changes in the Route Tables of the routers. Here the *Route Table* of the Router C – page *Network* in the *Status* section of the router. See the routes to the networks according to the scheme in Figure 2 via gre1 tunnel network interface.

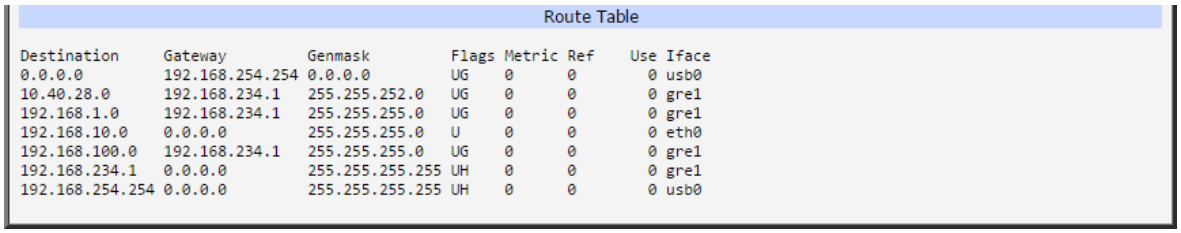


Figure 18: Router C – Route Table

If you login to the Cisco headquarter hub router and run the `show dmvpn` command, you should see the spokes (peers) connected with the proper tunnel addresses and other information:

```
Router#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
T1 - Route Installed, T2 - Nexthop-override
C - CTS Capable, I2 - Temporary
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface: Tunnel11, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,

# Ent  Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 10.0.9.130      192.168.234.2  UP 00:34:01    D
1 10.0.6.60       192.168.234.3  UP 00:30:03    D

Router#show ip bgp
BGP table version is 42, local router ID is 192.168.234.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network          Next Hop            Metric LocPrf Weight Path
*>i  192.168.77.0    192.168.234.3            0    100      0 i
*>i  192.168.100.0   192.168.234.2            0    100      0 i
*>   192.168.202.0   0.0.0.0                  0         32768 i
Router#ping 192.168.77.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.77.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 38/39/41 ms
Router#ping 192.168.100.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 38/47/55 ms
Router#
```

3. Related Documents

[1] Advantech Czech: **IPsec Tunnel Application Note** (APP-0006-EN)

You can obtain product-related documents on *Engineering Portal* at *icr.advantech.cz* address.

To get your router's *Quick Start Guide*, *User Manual*, *Configuration Manual*, or *Firmware* go to the *Router Models* page, find the required model, and switch to the *Manuals* or *Firmware* tab, respectively.

The *Router Apps* installation packages and manuals are available on the *Router Apps* page.

For the *Development Documents*, go to the *DevZone* page.