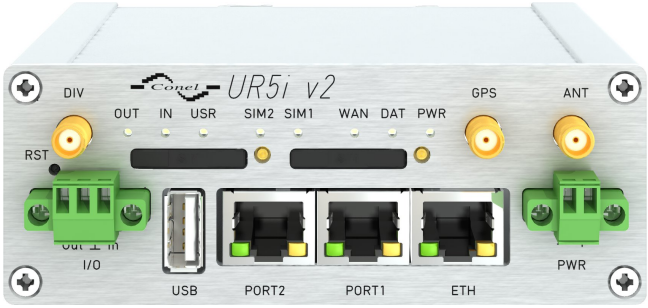
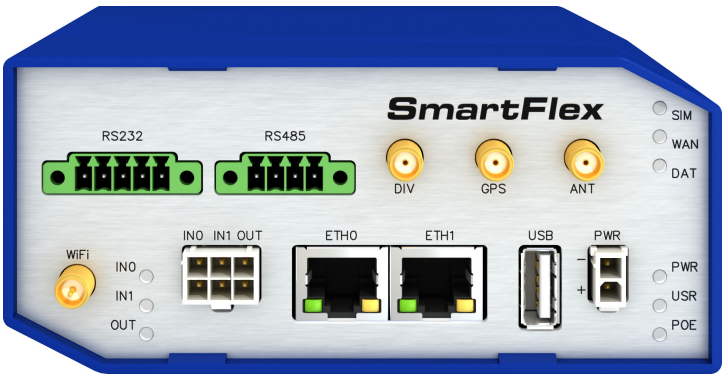
User Module

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 B+B SmartWorx s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. APP-0052-EN, revised on November 29, 2018. Released in the Czech Republic.

Contents

List of Figures

List of Tables

1. Basic Information

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.

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*.

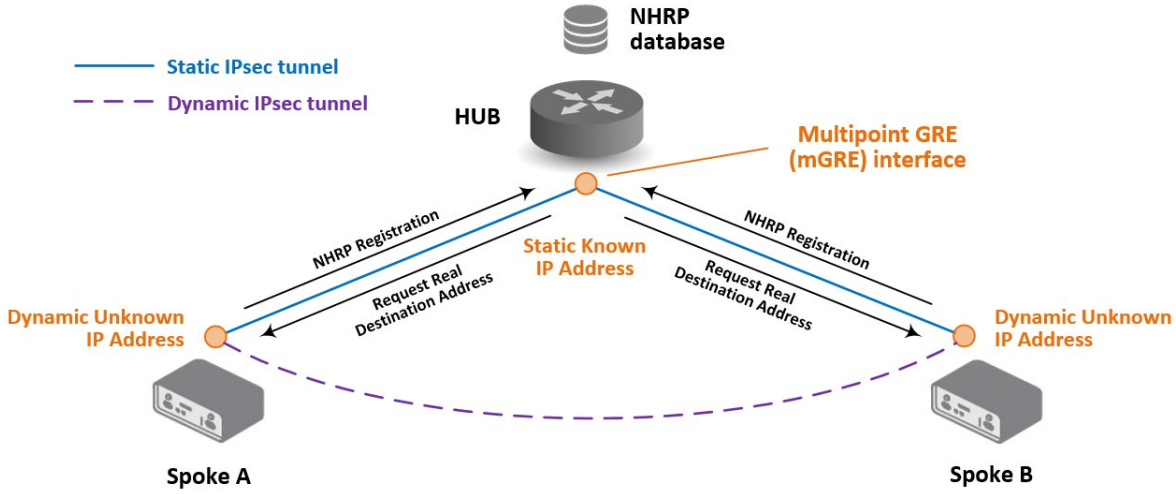


Figure 1: DMVPN architecture

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* user module in every spoke router.
- *IPSec-Tools* user module in every spoke router.
- GRE tunnel configuration in every spoke router (with proper IP routes).

See the example configuration below for more details.

The described user modules *NHRP* and *IPSec-Tools* are not contained in the standard router firmware. See the Configuration Manual ([1, 2]) for the description of uploading the user modules to the router. Please note that NHRP module requires firmware version 3.0.7 or later. Both user modules are v2 and v3 routers compatible.

2. Configuration Example

For a configuration example three Advantech B+B SmartWorx routers were used as spokes (Router A, B and C in scheme below) and one Cisco 871W router as headquarter hub was used.

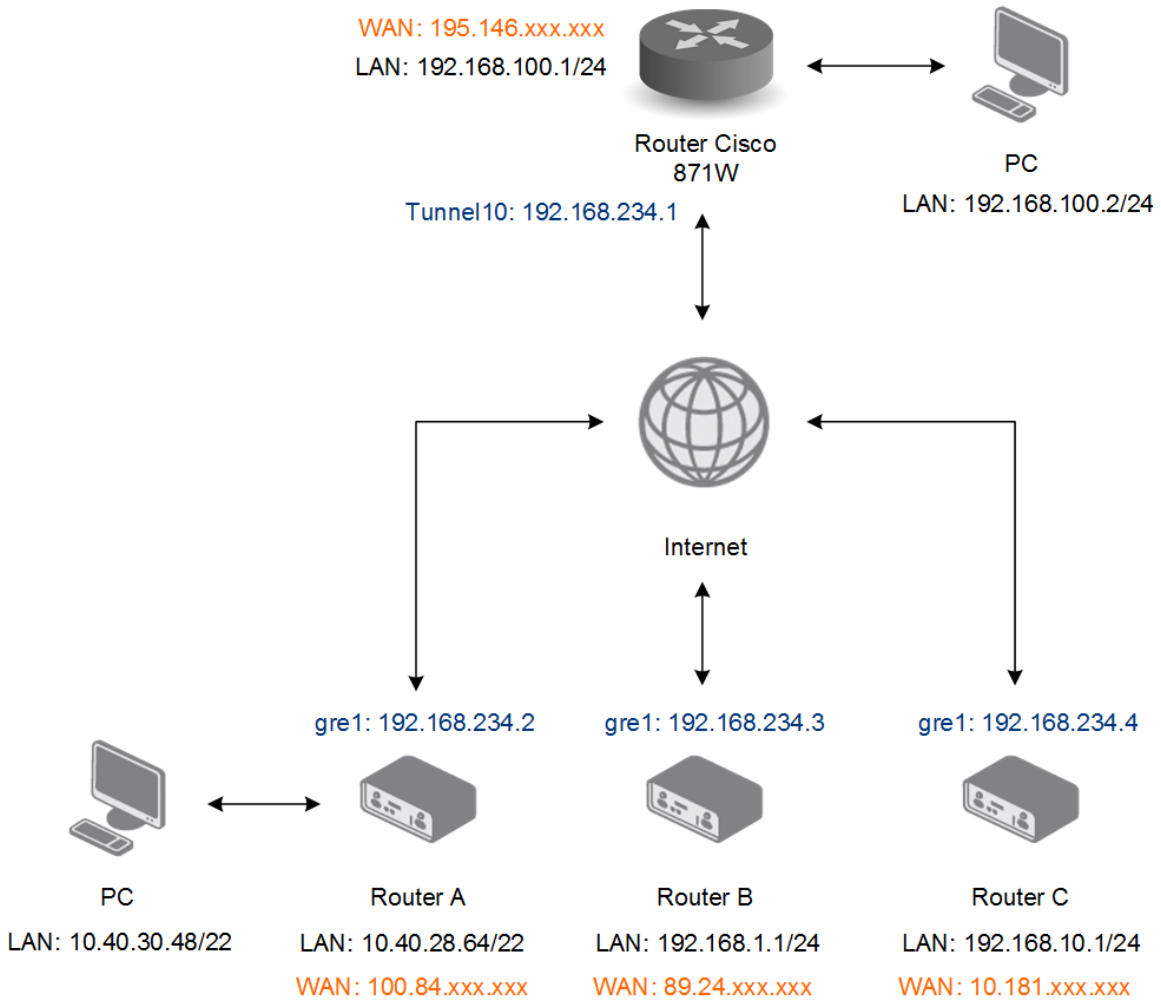


Figure 2: Configuration example scheme

Routes in routers (and PCs) are configured statically in this example, but it is possible to use OSPF Protocol (user module *OSPF* is necessary) or other protocols.

Note: The WAN IP addresses in the example scheme and in the configuration are private and thus end with *xxx.xxx*. Replace them with your own full IP addresses for your configuration.

2.1 Headquarter Hub Router Configuration

In this example configuration, the Cisco 871W 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.)

```
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
lifetime 3600
crypto isakmp key test address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
mode transport
!
crypto ipsec profile DMVPN-P
set transform-set ESP-3DES-MD5
!
!
!
interface Tunnel10
ip address 192.168.234.1 255.255.255.0
no ip redirects
ip nhrp authentication 1234
ip nhrp map multicast dynamic
ip nhrp network-id 1234
no ip nhrp record
no ip nhrp cache non-authoritative
ip ospf 1 area 0
tunnel source FastEthernet4
tunnel mode gre multipoint
tunnel key 1234
tunnel protection ipsec profile DMVPN-P
```

This is to setup the IPsec and Tunnel10 interface as NHRP and GRE multipoint interface.

Add static routes to the spoke's LAN networks According to the network infrastructure in Figure 2:

```
ip route 10.40.28.0 255.255.252.0 192.168.234.2
ip route 192.168.1.0 255.255.255.0 192.168.234.3
ip route 192.168.10.0 255.255.255.0 192.168.234.4
```

2.2 GRE Tunnel Configuration and Startup Script

Create the GRE tunnels between the headquarter (hub router) and remote routers (spokes). The detailed example of the Advantech B+B SmartWorx Router A is described first. Then the varying configuration for routers B and C is explained.

Open the Web interface of the first spoke (*Router A*) and press *GRE* item in the *Configuration* section. Then select one of the rows and press *Edit* button. Fill in the configuration form as indicated in the Figure and Table below.

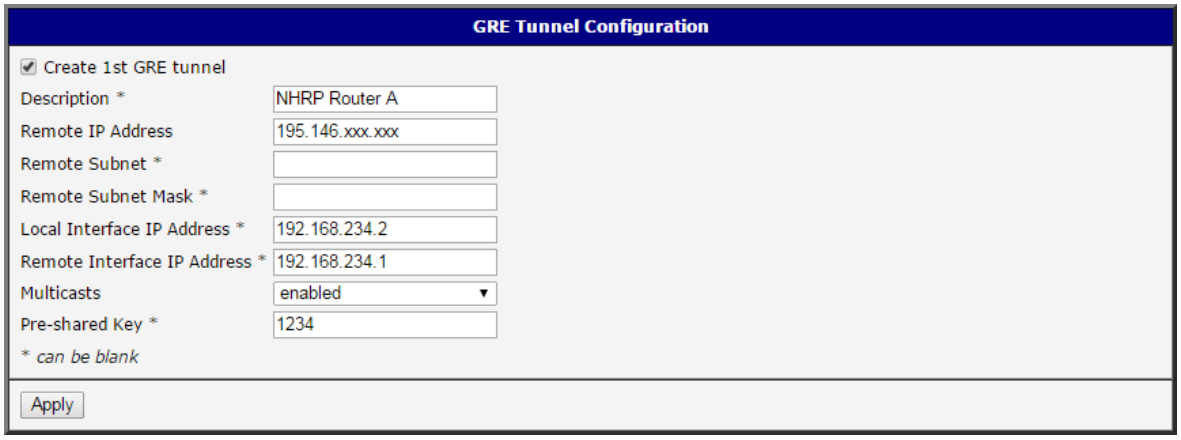


Figure 3: Router A – GRE configuration

Item	Value
Description	NHRP Router A *(optional)*
Remote IP Address	195.146.xxx.xxx *(Cisco headquarter hub)*
Remote Subnet	*do not fill in*
Remote Subnet Mask	*do not fill in*
Local Interface IP Address	192.168.234.2
Remote Interface IP Address	192.168.234.1
Multicasts	enabled
Pre-shared Key	1234

Table 1: Router A – GRE configuration

Ensure you have ticked the *Create 1st GRE tunnel* on the top of the page and press the *Apply* button to save changes.

Now go to the *Startup Script* page in the *Configuration* section of the router and add the proper static routes to other networks. The gateway is Cisco headquarter hub router and the routes are via created *gre1* network interface:

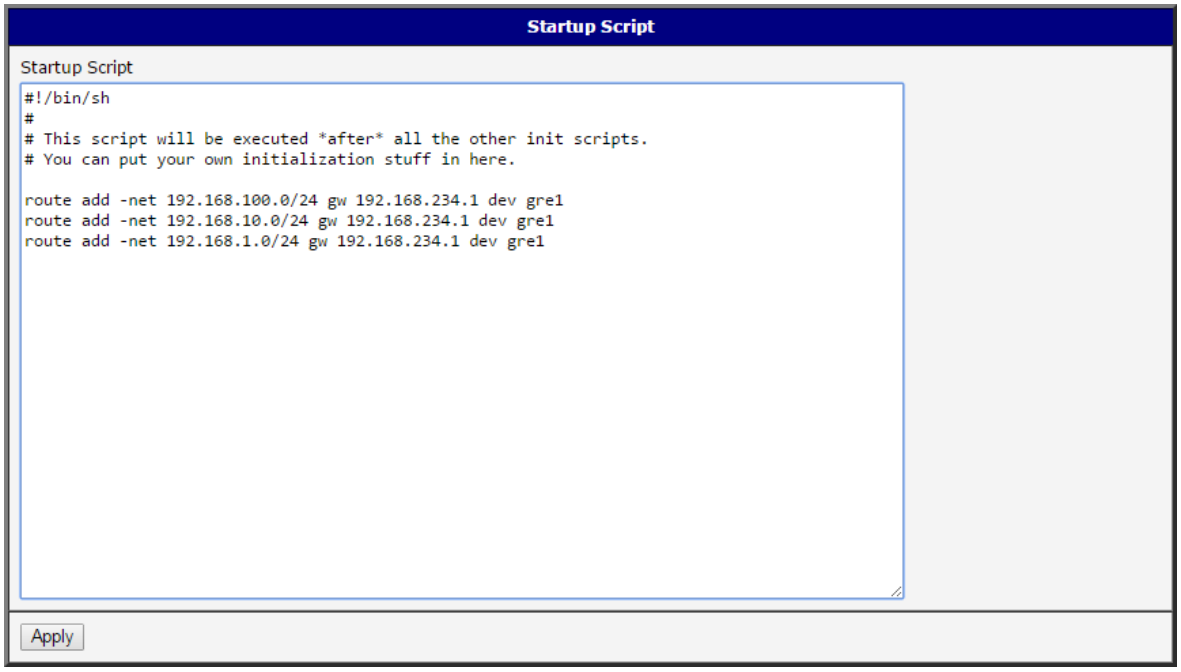


Figure 4: Router A – Static routes in Startup Script

```
route add -net 192.168.100.0/24 gw 192.168.234.1 dev gre1
route add -net 192.168.10.0/24 gw 192.168.234.1 dev gre1
route add -net 192.168.1.0/24 gw 192.168.234.1 dev gre1
```

Press *Apply* to save the changes. You will be prompted to reboot the router. The routes will not be added until you reboot the router, since it is the startup script run when the router starts up.

Note: It is possible to create the whole GRE tunnel in the Startup Script with the static routes instead of the *GRE* page in the Web interface. Just add this another lines to the Startup Script (and disable the GRE tunnel on the *GRE* page).

```
ip tunnel add gre1 mode gre remote 195.146.xxx.xxx key 1234 ttl 255
ip link set gre1 up
ip link set gre1 multicast on
ip addr add 192.168.234.2/24 broadcast 192.168.234.255 dev gre1
```

2.2.1 Configure the Rest of the Spokes (Router B and C)

Make the same configuration for Advantech B+B SmartWorx routers B and C. Change only the items *Description* and *Local Interface IP Address* – local side of the tunnel. Also add the proper static routes to the *Startup Script* of every router. See the Figures and code examples below. Do not forget to reboot the routers because of startup scripts.

GRE Configuration for the Router B:

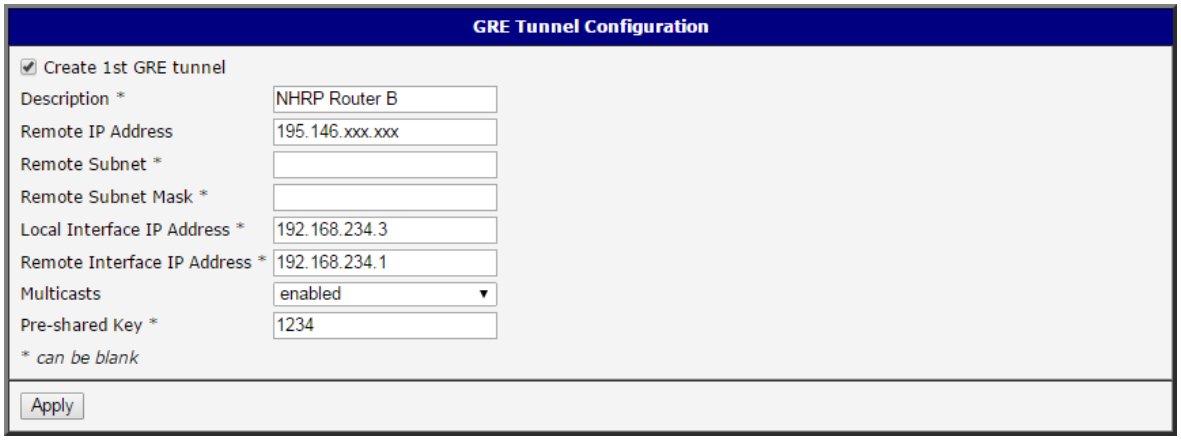


Figure 5: Router B – GRE configuration

Startup Script for the Router B – static routes:

```
route add -net 192.168.100.0/24 gw 192.168.234.1 dev gre1
route add -net 192.168.10.0/24 gw 192.168.234.1 dev gre1
route add -net 10.40.28.0/22 gw 192.168.234.1 dev gre1
```

GRE Configuration for the Router C:

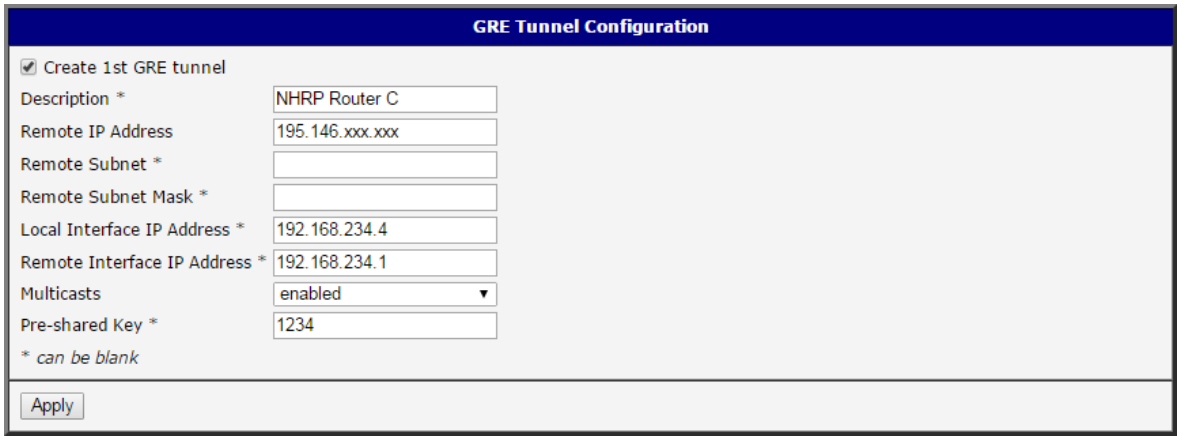


Figure 6: Router C – GRE configuration

Startup Script for the Router C – static routes:

```
route add -net 192.168.100.0/24 gw 192.168.234.1 dev gre1
route add -net 192.168.1.0/24 gw 192.168.234.1 dev gre1
route add -net 10.40.28.0/22 gw 192.168.234.1 dev gre1
```

2.3 IPsec Configuration – IPSec-Tools User Module

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

Do not use *IPsec Tunnels Configuration* page in the router's Web interface. Use the *IPSec-Tools* user module instead in version 1.0.1 or later to configure the IPsec tunnel for Dynamic Multipoint VPN. The user module *IPSec-Tools* is not part of the standard router firmware. See the Configuration Manual ([1, 2]) for the description of uploading the user module to the router. *IPSec-Tools* user module is v2 and v3 routers compatible.

The *IPSec-Tools* user module uses *racoon* instead of router's standard *OpenSwan* as IPsec implementation. It works better with the Cisco Dynamic Multipoint VPN.

Go to the *IPSec-Tools* user module on the *User Modules* page (Figure 7).

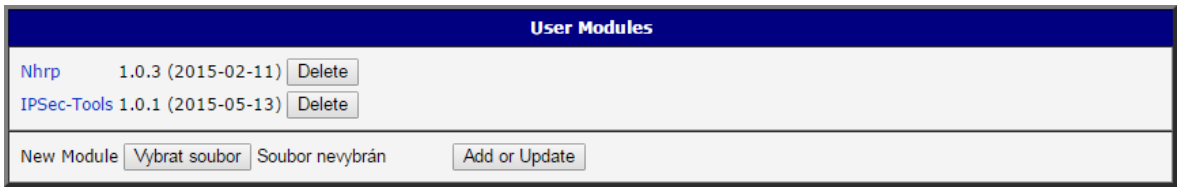


Figure 7: Necessary user modules

Tick the *Enable IPSec-Tools* box at the top and insert the following configuration commands to the proper configuration input fields – see Figure 8:

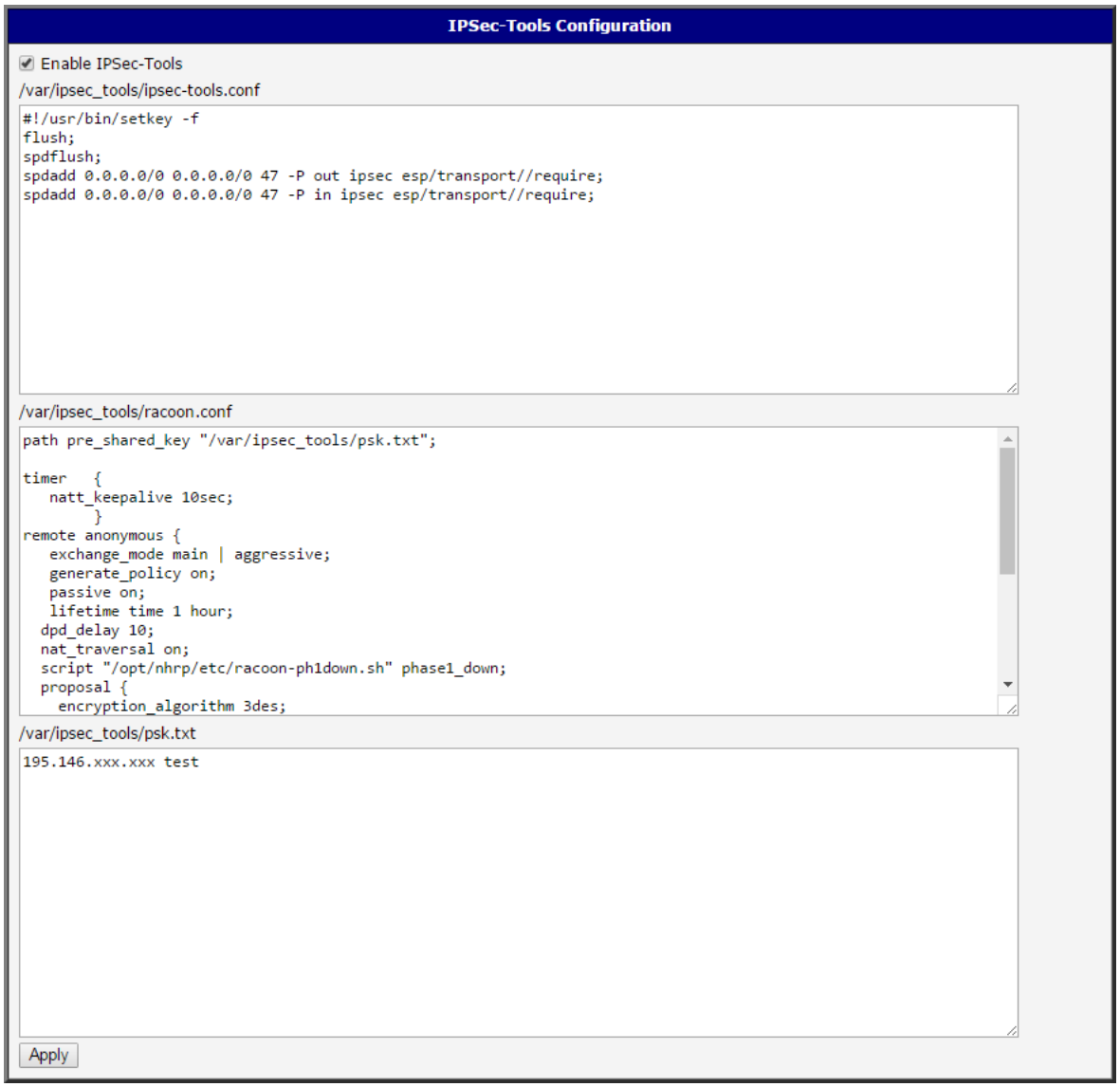


Figure 8: User module IPSec-Tools configuration

Field */var/ipsec_tools/ipsec-tools.conf* – set the security policy, transport mode:

```
#!/usr/bin/setkey -f
flush;
spdflush;
spdadd 0.0.0.0/0 0.0.0.0/0 47 -P out ipsec esp/transport//require;
spdadd 0.0.0.0/0 0.0.0.0/0 47 -P in ipsec esp/transport//require;
```

Field */var/ipsec_tools/racoon.conf* – set the path to pre-shared key file, used algorithms, encryption and other parameters:

```
path pre_shared_key "/var/ipsec_tools/psk.txt";

timer   {
   natt_keepalive 10sec;
}
remote anonymous {
   exchange_mode main | aggressive;
   generate_policy on;
   passive on;
   lifetime time 1 hour;
   dpd_delay 10;
   nat_traversal on;
   script "/opt/nhrp/etc/racoon-ph1down.sh" phase1_down;
   proposal {
      encryption_algorithm 3des;
      hash_algorithm md5;
      authentication_method pre_shared_key;
      dh_group 2;
   }
}
sainfo anonymous {
   lifetime time 3600 seconds;
   encryption_algorithm 3des;
   authentication_algorithm hmac_md5;
   compression_algorithm deflate;
}
```

Field */var/ipsec_tools/psk.txt* – set the pre-shared key for the Cisco headquarter hub router – same as you have set at the Cisco router:

```
195.146.xxx.xxx test
```

Save the changes using the *Apply* button. Use the same procedure for all spokes – the *IPSec-Tools Configuration* remains the same for all the spoke routers.

2.4 NHRP Configuration – NHRP User Module

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

> The user module *NHRP* is not part of the standard router firmware. See the Configuration Manual ([1, 2]) for the description of uploading the user module to the router. Please note that *NHRP* module requires router's firmware version 3.0.7 or later. Use the 1.0.3 version of the *NHRP* user module or later! It is v2 and v3 routers compatible.

Go to the *User Modules* page (Figure 7) and then *NHRP* to configure the *NHRP* user module. Tick the *Enable NHRP* box and insert the configuration commands in the fields.

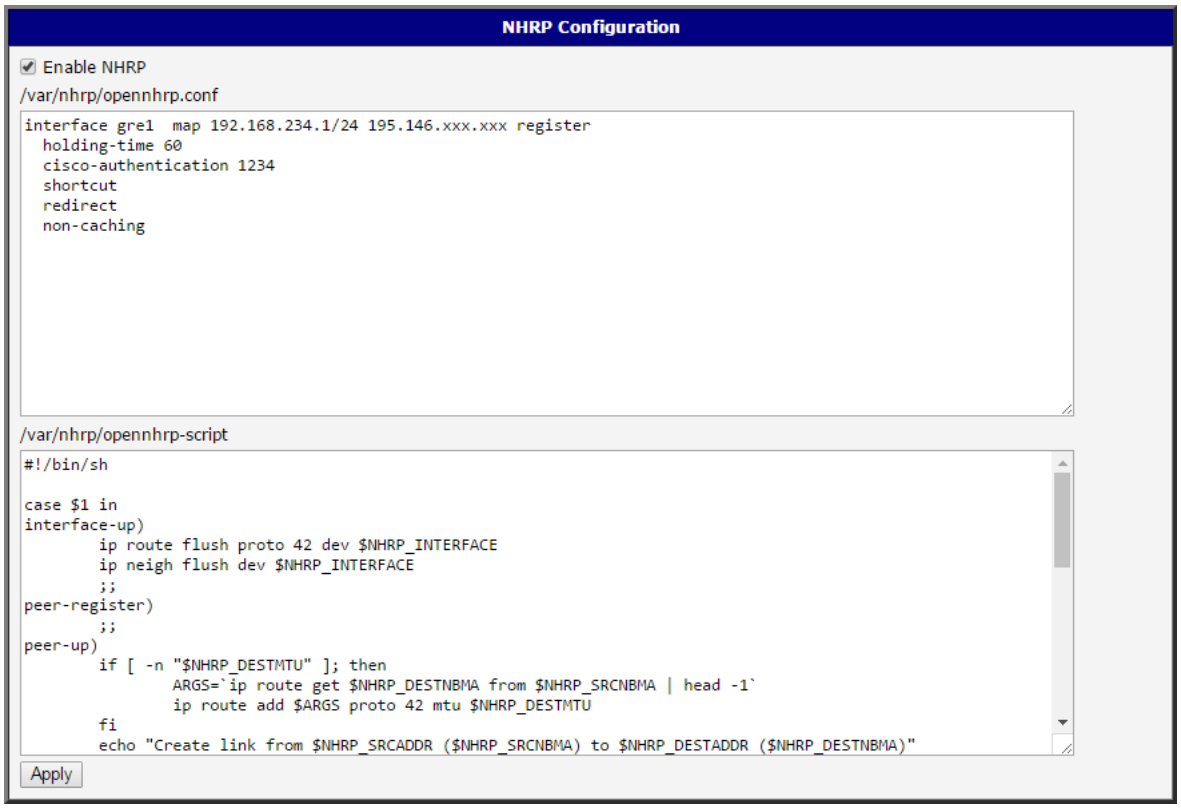


Figure 9: NHRP user module configuration

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).

```
interface gre1  map 192.168.234.1/24 195.146.xxx.xxx register
  holding-time 60
  cisco-authentication 1234
  shortcut
  redirect
  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.

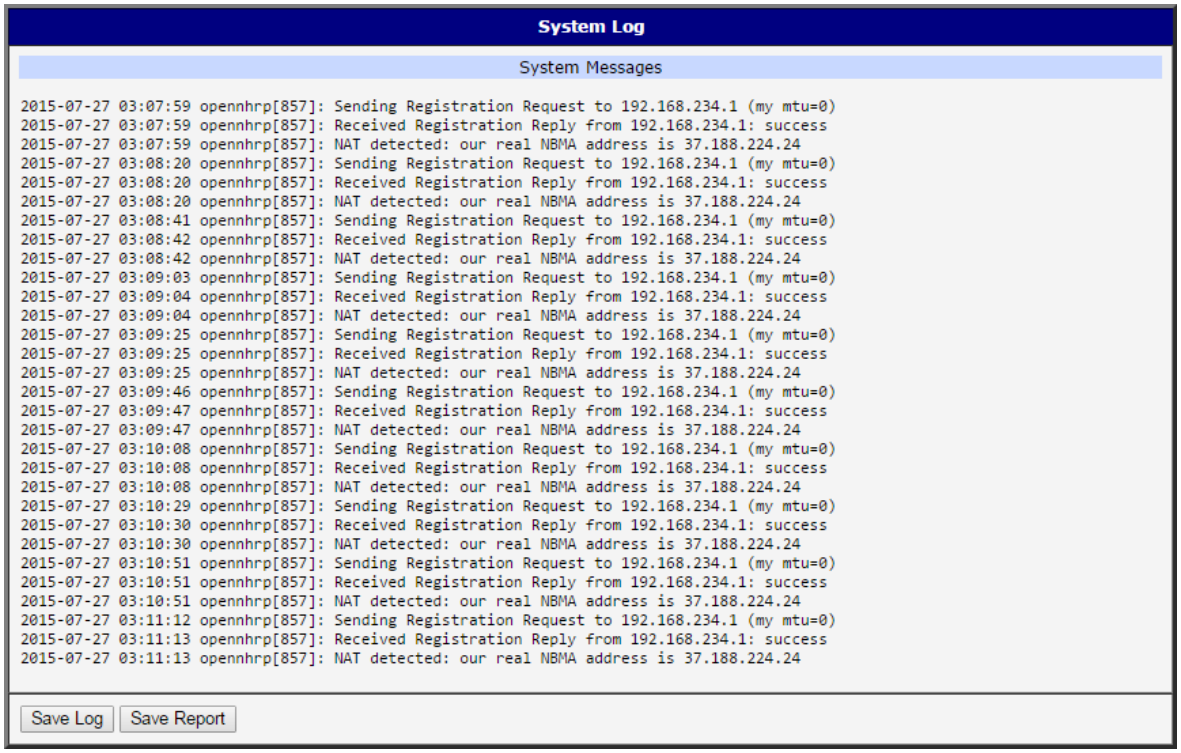
Field */var/nhrp/opennhrp-script*

```
#!/bin/sh

case $1 in
interface-up)
ip route flush proto 42 dev $NHRP_INTERFACE
ip neigh flush dev $NHRP_INTERFACE
;;
peer-register)
;;
peer-up)
if [ -n "$NHRP_DESTMTU" ]; then
ARGS=`ip route get $NHRP_DESTNBMA from $NHRP_SRCNBMA | head -1`
ip route add $ARGS proto 42 mtu $NHRP_DESTMTU
fi
echo "Create link from $NHRP_SRCADDR ($NHRP_SRCNBMA) \
to $NHRP_DESTADDR ($NHRP_DESTNBMA)"
racoonctl establish-sa -w isakmp inet $NHRP_SRCNBMA $NHRP_DESTNBMA || exit 1
racoonctl establish-sa -w esp inet $NHRP_SRCNBMA $NHRP_DESTNBMA gre || exit 1
;;
peer-down)
echo "Delete link from $NHRP_SRCADDR ($NHRP_SRCNBMA) \
to $NHRP_DESTADDR ($NHRP_DESTNBMA)"
if [ "$NHRP_PEER_DOWN_REASON" != "lower-down" ]; then
racoonctl delete-sa isakmp inet $NHRP_SRCNBMA $NHRP_DESTNBMA
fi
ip route del $NHRP_DESTNBMA src $NHRP_SRCNBMA proto 42
;;
route-up)
echo "Route $NHRP_DESTADDR/$NHRP_DESTPREFIX is up"
ip route replace $NHRP_DESTADDR/$NHRP_DESTPREFIX proto 42 \
via $NHRP_NEXTHOP dev $NHRP_INTERFACE
ip route flush cache
;;
route-down)
echo "Route $NHRP_DESTADDR/$NHRP_DESTPREFIX is down"
ip route del $NHRP_DESTADDR/$NHRP_DESTPREFIX proto 42
ip route flush cache
;;
esac

exit 0
```

2.5 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, B and C. The router is sending NHRP Registration Request and is receiving the success message (same on router A, B and C):

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



System Log

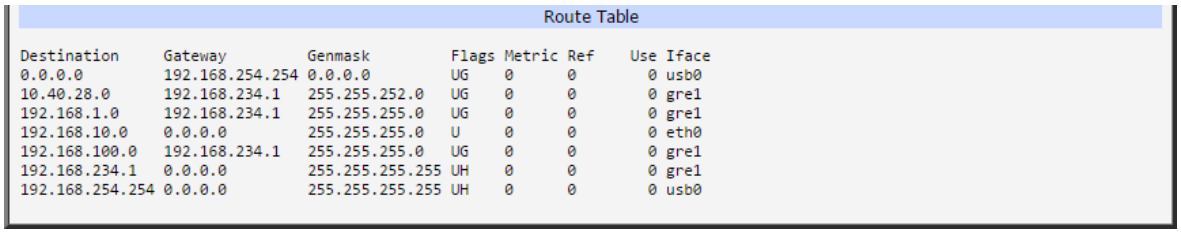
System Messages

```
2015-07-27 03:07:59 opennhrp[857]: Sending Registration Request to 192.168.234.1 (my mtu=0)
2015-07-27 03:07:59 opennhrp[857]: Received Registration Reply from 192.168.234.1: success
2015-07-27 03:07:59 opennhrp[857]: NAT detected: our real NBMA address is 37.188.224.24
2015-07-27 03:08:20 opennhrp[857]: Sending Registration Request to 192.168.234.1 (my mtu=0)
2015-07-27 03:08:20 opennhrp[857]: Received Registration Reply from 192.168.234.1: success
2015-07-27 03:08:20 opennhrp[857]: NAT detected: our real NBMA address is 37.188.224.24
2015-07-27 03:08:41 opennhrp[857]: Sending Registration Request to 192.168.234.1 (my mtu=0)
2015-07-27 03:08:42 opennhrp[857]: Received Registration Reply from 192.168.234.1: success
2015-07-27 03:08:42 opennhrp[857]: NAT detected: our real NBMA address is 37.188.224.24
2015-07-27 03:09:03 opennhrp[857]: Sending Registration Request to 192.168.234.1 (my mtu=0)
2015-07-27 03:09:04 opennhrp[857]: Received Registration Reply from 192.168.234.1: success
2015-07-27 03:09:04 opennhrp[857]: NAT detected: our real NBMA address is 37.188.224.24
2015-07-27 03:09:25 opennhrp[857]: Sending Registration Request to 192.168.234.1 (my mtu=0)
2015-07-27 03:09:25 opennhrp[857]: Received Registration Reply from 192.168.234.1: success
2015-07-27 03:09:25 opennhrp[857]: NAT detected: our real NBMA address is 37.188.224.24
2015-07-27 03:09:46 opennhrp[857]: Sending Registration Request to 192.168.234.1 (my mtu=0)
2015-07-27 03:09:47 opennhrp[857]: Received Registration Reply from 192.168.234.1: success
2015-07-27 03:09:47 opennhrp[857]: NAT detected: our real NBMA address is 37.188.224.24
2015-07-27 03:10:08 opennhrp[857]: Sending Registration Request to 192.168.234.1 (my mtu=0)
2015-07-27 03:10:08 opennhrp[857]: Received Registration Reply from 192.168.234.1: success
2015-07-27 03:10:08 opennhrp[857]: NAT detected: our real NBMA address is 37.188.224.24
2015-07-27 03:10:29 opennhrp[857]: Sending Registration Request to 192.168.234.1 (my mtu=0)
2015-07-27 03:10:30 opennhrp[857]: Received Registration Reply from 192.168.234.1: success
2015-07-27 03:10:30 opennhrp[857]: NAT detected: our real NBMA address is 37.188.224.24
2015-07-27 03:10:51 opennhrp[857]: Sending Registration Request to 192.168.234.1 (my mtu=0)
2015-07-27 03:10:51 opennhrp[857]: Received Registration Reply from 192.168.234.1: success
2015-07-27 03:10:51 opennhrp[857]: NAT detected: our real NBMA address is 37.188.224.24
2015-07-27 03:11:12 opennhrp[857]: Sending Registration Request to 192.168.234.1 (my mtu=0)
2015-07-27 03:11:13 opennhrp[857]: Received Registration Reply from 192.168.234.1: success
2015-07-27 03:11:13 opennhrp[857]: NAT detected: our real NBMA address is 37.188.224.24
```

Save Log | Save Report

Figure 10: 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.



Route Table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.254.254	0.0.0.0	UG	0	0	0	usb0
10.40.28.0	192.168.234.1	255.255.252.0	UG	0	0	0	gre1
192.168.1.0	192.168.234.1	255.255.255.0	UG	0	0	0	gre1
192.168.10.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.100.0	192.168.234.1	255.255.255.0	UG	0	0	0	gre1
192.168.234.1	0.0.0.0	255.255.255.255	UH	0	0	0	gre1
192.168.254.254	0.0.0.0	255.255.255.255	UH	0	0	0	usb0

Figure 11: 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:

```
conel#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel10, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1   37.188.224.24   192.168.234.2    UP 02:17:42    DN
     1     89.24.3.182   192.168.234.3    UP 00:34:32     D
     1    37.48.51.222   192.168.234.4    UP 01:21:17    DN
```

Figure 12: Cisco router – show dmvpn command

You can also try to ping from the routers (SSH or Telnet login) to each other's LAN IP addresses (E.g. from Router A to Cisco router at 192.168.100.1 IP address, etc.). If you add the proper static routes in the PCs connected, you can ping from the PCs to the rest LAN IP addresses in the network, too.

Add static IP routes to the PCs in Figure 2 if you want to access the network via the tunnels. In Windows OS it can be done using the command:

`route ADD ‘‘network’’ MASK ‘‘subnet mask’’ ‘‘gateway ip’’`

E.g. use command

`route ADD 192.168.10.0 MASK 255.255.255.0 10.40.28.64`

for the Windows PC down left in Figure 2 to reach the network of Router C, etc.

3. Recommended literature

[1] Advantech B+B SmartWorx: **v2 Routers Configuration Manual** (MAN-0021-EN)
[2] Advantech B+B SmartWorx: **SmartFlex Configuration Manual** (MAN-0023-EN)
[3] Advantech B+B SmartWorx: **SmartMotion Configuration Manual** (MAN-0024-EN)
[4] Advantech B+B SmartWorx: **SmartStart Configuration Manual** (MAN-0022-EN)
[5] Advantech B+B SmartWorx: **ICR-3200 Configuration Manual** (MAN-0042-EN)

Product related documents can be obtained on *Engineering Portal* at `https://ep.advantech-bb.cz/` address.