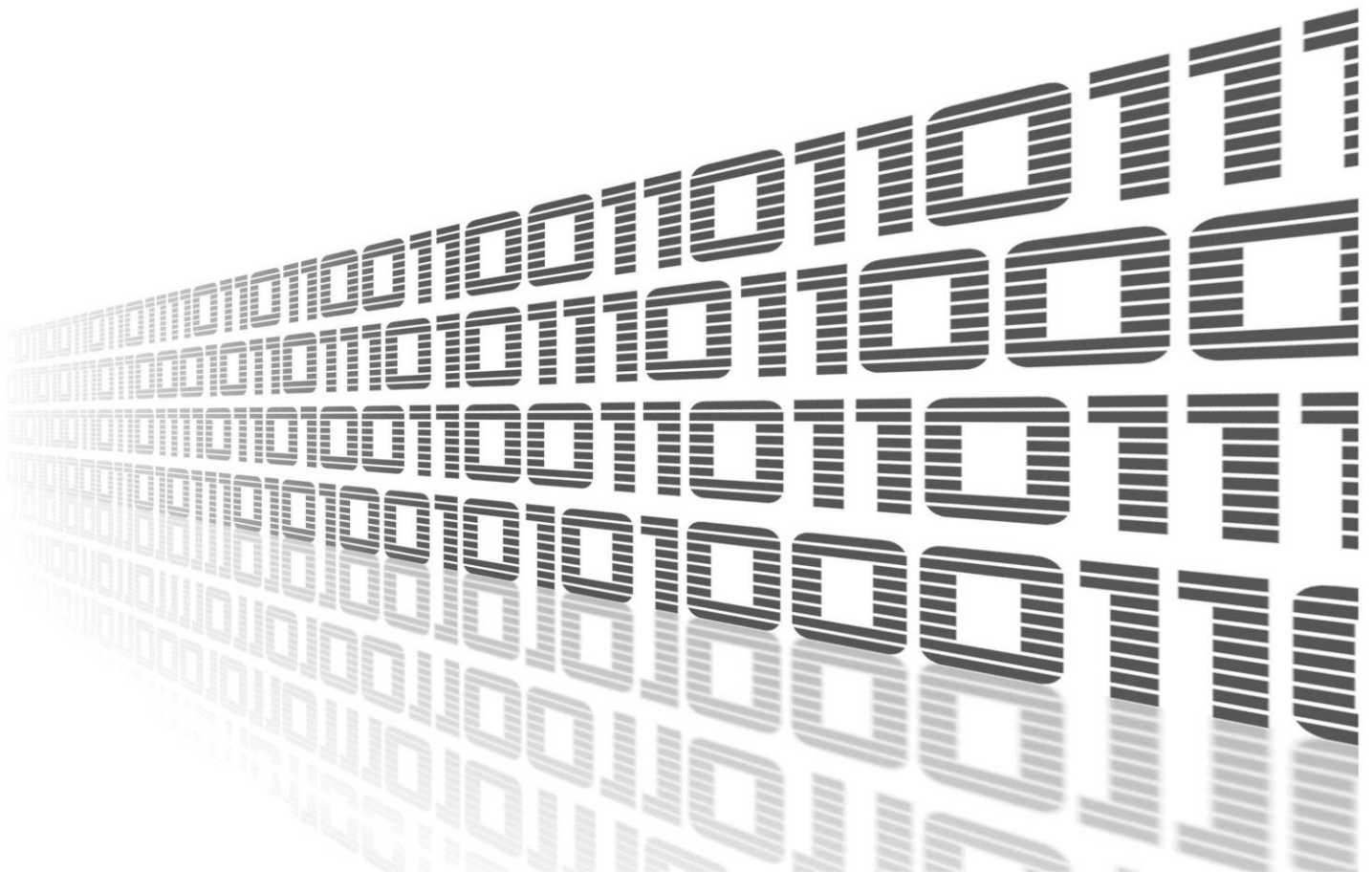




FRR



© 2025 Advantech Czech s.r.o. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photography, recording, or any information storage and retrieval system without written consent. Information in this manual is subject to change without notice, and it does not represent a commitment on the part of Advantech.

Advantech Czech s.r.o. shall not be liable for incidental or consequential damages resulting from the furnishing, performance, or use of this manual.

All brand names used in this manual are the registered trademarks of their respective owners. The use of trademarks or other designations in this publication is for reference purposes only and does not constitute an endorsement by the trademark holder.

Used symbols



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



Attention – Problems that can arise in specific situations.



Information – Useful tips or information of special interest.

Contents

1. Changelog	1
1.1 FRR Changelog	1
2. Router App Description	3
2.1 Introduction	3
2.2 Installation	3
3. Web Interface	4
4. Status	5
5. Configuration	6
5.1 Global	6
5.2 VRF	6
5.3 Static	7
5.4 Zebra	8
5.5 BGP	9
5.5.1 Example of Configuration	9
5.5.2 BGP Basic commands	12
5.6 ISIS	13
5.7 OSPF & OSPF6	13
5.7.1 Example of configuration	14
5.7.2 IPv4 Configuration	15
5.7.3 IPv6 Configuration	17
5.7.4 OSPF Basic commands	19
5.8 RIP & RIPNG	20
5.8.1 Example of configuration	20
5.8.2 IPv4 Configuration	21
5.8.3 IPv6 Configuration	23
5.8.4 RIP Basic commands	24
5.9 NHRP	25
5.9.1 NHRP Configuration Example	27
5.10 MPLS	35
5.11 LDP	36
5.12 PIM-SM	37
5.12.1 BSR - BootStrap Router	37
5.12.2 Interface configuration	38
6. Related Documents	41

List of Figures

1	Menu	4
2	Status Overview Example	5

3	Global Configuration	6
4	VRF Global Configuration	6
5	VRF Interface Configuration	7
6	Static Configuration	7
7	Configuration of zebra daemon	8
8	Model scheme	9
9	Example of configuration	10
10	Configuration of bgpd daemon 1	10
11	Configuration of bgpd daemon 2	11
12	IS-IS Configuration	13
13	OSPF web interface	14
14	Example of configuration	14
15	RIP web interface	20
16	Example of configuration	21
17	NHRP Configuration	25
18	NHRP Example	27
19	Spoke1 GRE Configuration	28
20	Spoke1 IPSEC Configuration Part 1	30
21	Spoke1 IPSEC Configuration Part 2	30
22	Spoke1 Route Table	31
23	Spoke1 GRE Configuration	31
24	Spoke2 IPSEC Configuration Part 1	33
25	Spoke2 IPSEC Configuration Part 2	33
26	Spoke2 Route Table	34
27	Simplified MPLS Domain Example	35
28	MPLS Configuration	35
29	LDP Configuration	36
30	PIM-SM Configuration	37
31	PIM-SM Configuration	37
32	PIM-SM Configuration	38
33	PIM-SM Configuration	39

List of Tables

1	GLOBAL Configuration items description	6
2	BGP Basic commands	12
3	OSPF Basic commands	19
4	RIP Basic commands	24
5	PIM-SM Commands	37

1. Changelog



This Router App has been tested on a router with firmware version 6.3.10. After updating the router's firmware to a higher version, make sure that a newer version of the Router App has not also been released, as it is necessary to update it as well for compatibility reasons.

1.1 FRR Changelog

v1.0.0 (2020-11-20)

- First release

v1.0.1 (2021-01-19)

- Added staticd

v1.1.0 (2021-12-07)

- Upgraded to version 7.5.1
- Added LDP/MPLS support
- Added VRF support
- For proper MPLS function is FW 6.3.3+ needed

v1.1.1 (2022-02-01)

- Fixed FRR routing daemons stopping/restarting
- Fixed MPLS init script

v1.2.0 (2022-06-16)

- Updated FRR to version 8.2.2

v1.3.0 (2022-11-03)

- Reworked license information

v8.4.2 (2023-03-17)

- Updated FRR to version 8.4.2

v8.5.4 (2024-02-01)

- Updated FRR to version 8.5.4
- Recompiled with ModulesSDK 2.1.0
- Added description and summary files

v8.5.4-1 (2024-03-05)

- Fixed description and summary files

v10.2.1 (2025-01-07)

- Updated FRR to version 10.2.1
- Limited settings editing for administrators only
- Added PIM-SM
- Added integrity checks for the -S1 platforms

2. Router App Description

2.1 Introduction

FRRouting (FRR) is a robust and versatile IP routing protocol suite designed for Linux and Unix platforms. It offers a comprehensive range of protocol daemons, empowering users to implement sophisticated routing solutions with ease.

Building on the power and flexibility of *FRR*, Advantech has developed the innovative *FRR* router app. This application enhances the router's capabilities by supporting an extensive array of routing protocols, including BGP, IS-IS, LDP, MPLS, NHRP, OSPF, OSFP6, PIM-SM, RIP, RIPNG, Static, VRF, and Zebra. With this advanced functionality, the *FRR* router app equips users with the tools to address complex networking demands and ensures seamless, efficient data routing across diverse environments.

2.2 Installation

This router app is not installed on *Advantech* routers by default. However, you can get the *.tgz installation file on the *Engineering Portal*¹.

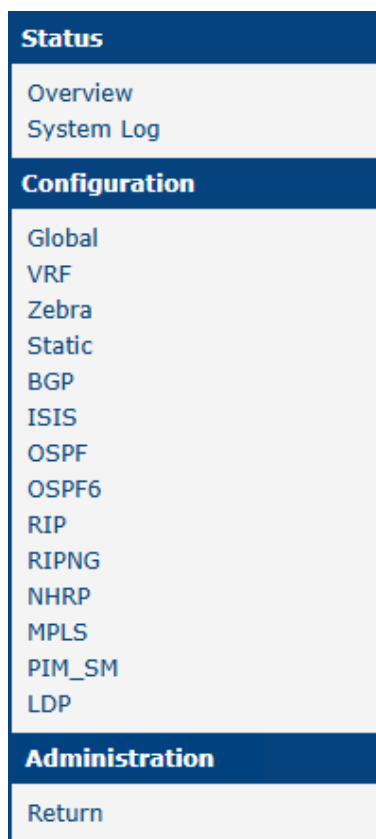
This router app can be installed to the router in the router's GUI by clicking *Customization* → *Router Apps* → *Add or Update* button.

¹<https://icr.advantech.com/products/software/user-modules#frr>

3. Web Interface

Once the installation of the *FRR Router App* is complete, its GUI can be invoked by clicking the module name on the Router apps page of router's web interface.

Left part of this GUI contains menu with *Status* menu section, *Configuration* menu section and *Information* menu section. *Administration* menu section contains only the *Return* item, which switches back from the app's web page to the router's web configuration pages. The main menu of app's GUI is shown on Figure 2.



Status
Overview
System Log
Configuration
Global
VRF
Zebra
Static
BGP
ISIS
OSPF
OSPF6
RIP
RIPNG
NHRP
MPLS
PIM_SM
LDP
Administration
Return

Figure 1: Menu

4. Status

In this section, in the *Overview* part, you can see the status of all protocols which can be configured via the *FRR Router App*. The figure below is an example of the Zebra protocol running.

```
-----  
Status Overview  
-----  
Services  
-----  
Protocol zebra is running  
-----  
FRRouting 7.5 (Router).  
Router# show ip route  
Codes: K - kernel route, C - connected, S - static, R - RIP,  
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,  
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,  
F - PBR, f - OpenFabric,  
> - selected route, * - FIB route, q - queued, r - rejected, b - backup  
  
K>* 0.0.0.0/0 [0/0] via 192.168.253.254, usb0, 00:05:02  
C>* 10.64.0.0/22 is directly connected, eth0, 00:05:02  
C>* 10.65.0.0/22 is directly connected, eth1, 00:05:02  
C>* 10.80.0.85/32 is directly connected, usb0, 00:05:02  
K>* 192.168.253.254/32 [0/0] is directly connected, usb0, 00:05:02  
Router# show ipv6 route  
Codes: K - kernel route, C - connected, S - static, R - RIPng,  
O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,  
v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,  
f - OpenFabric,  
> - selected route, * - FIB route, q - queued, r - rejected, b - backup  
  
C>* 64:ff9b::/96 is directly connected, nat64, 00:05:02  
C>* fd00:a40::/56 is directly connected, eth0, 00:05:02  
C>* fd00:a41::/56 is directly connected, eth1, 00:05:02  
C * fe80::/64 is directly connected, nat64, 00:05:02  
C * fe80::/64 is directly connected, eth1, 00:05:02  
C>* fe80::/64 is directly connected, eth0, 00:05:02  
-----
```

Figure 2: Status Overview Example

In the *System Log* part, you can see a copy of the system log, also available in the router *Status* → *System Log*.

5. Configuration

5.1 Global

All Secure Syslog router app settings can be configured by clicking on the *Global* item in the main menu of module web interface. An overview of configurable items is given below.



Figure 3: Global Configuration

Item	Description
Enable GLOBAL	Enables FRR functionality.
Log Level	Select what level of information will appear in log

Table 1: GLOBAL Configuration items description

5.2 VRF

In IP-based computer networks, virtual routing and forwarding (VRF) is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. More about this protocol and examples can be found in the FRR online documentation¹.

There are more configuration pages for the VRF configuration under *Customization* → *Router Apps* → *FRR* → *Configuration* → *VRF* menu item. The first, see Figure 4, is for the global VRF configuration. You can enable/disable the VRF globally and enable the TCP/UDP I3mdev (the L3 master device) access here as well.

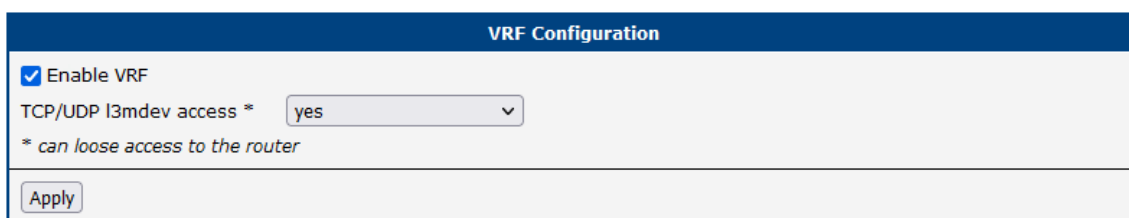


Figure 4: VRF Global Configuration

¹<http://docs.frouting.org/en/latest/zebra.html?highlight=vrf#clcmd-vrf-VRF>

Next are configuration pages for individual VRF interface configurations; see Figure 5.

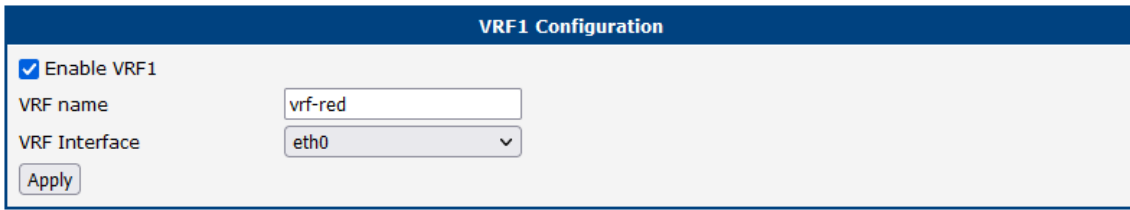


Figure 5: VRF Interface Configuration

5.3 Static

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. More about configuring and examples can be found in the FRR online documentation¹.

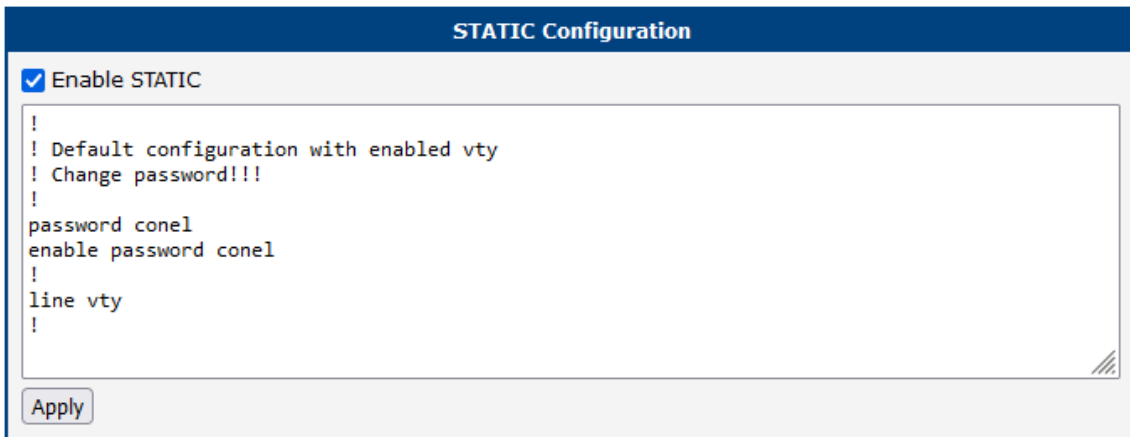


Figure 6: Static Configuration

¹<http://docs.frouting.org/en/latest/static.html>

5.4 Zebra

Zebra is an IP routing manager, It provides kernel routing table updates, interface lookups, and redistribution of routes between different routing protocols. More about configuring and examples can be found in the text below or in the FRR online documentation¹.

An example of the zebra configuration file (*zebra.conf*):

```
!  
password conel  
enable password conel  
log syslog  
!  
interface eth0  
!  
interface eth1  
!  
interface tun0  
!  
interface ppp0  
!  
!  
line vty  
!
```

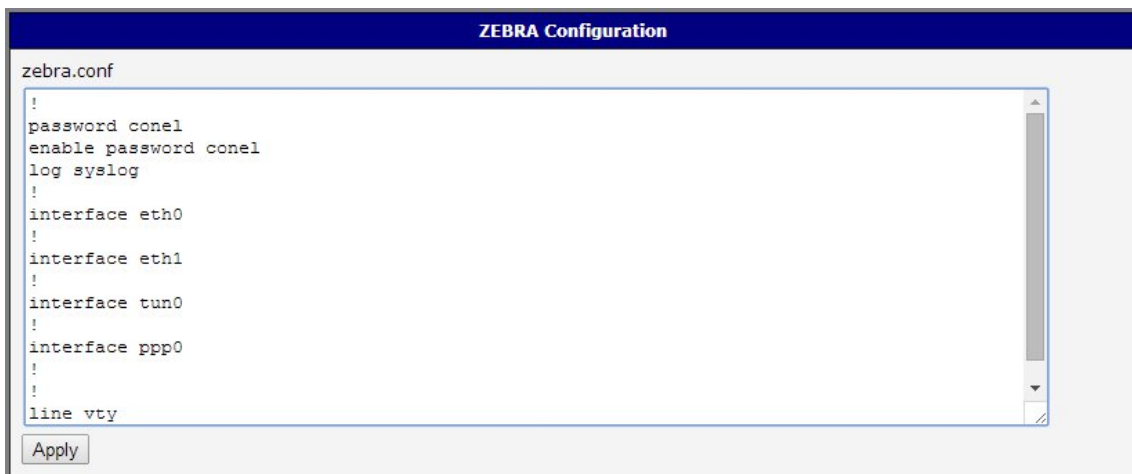


Figure 7: Configuration of zebra daemon

¹<http://docs.frrouting.org/en/latest/zebra.html>

5.5 BGP

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. More about configuring and examples can be found in the text below or in the FRR online documentation¹.

Due to this module it is possible to use the routing between autonomous systems. These systems might be perceived as a group of IP networks and routers under the control of one or more network operators that presents a common clearly defined routing policy (only one of interior gateway protocols). The routing information is exchanged between autonomous systems via border gateway.

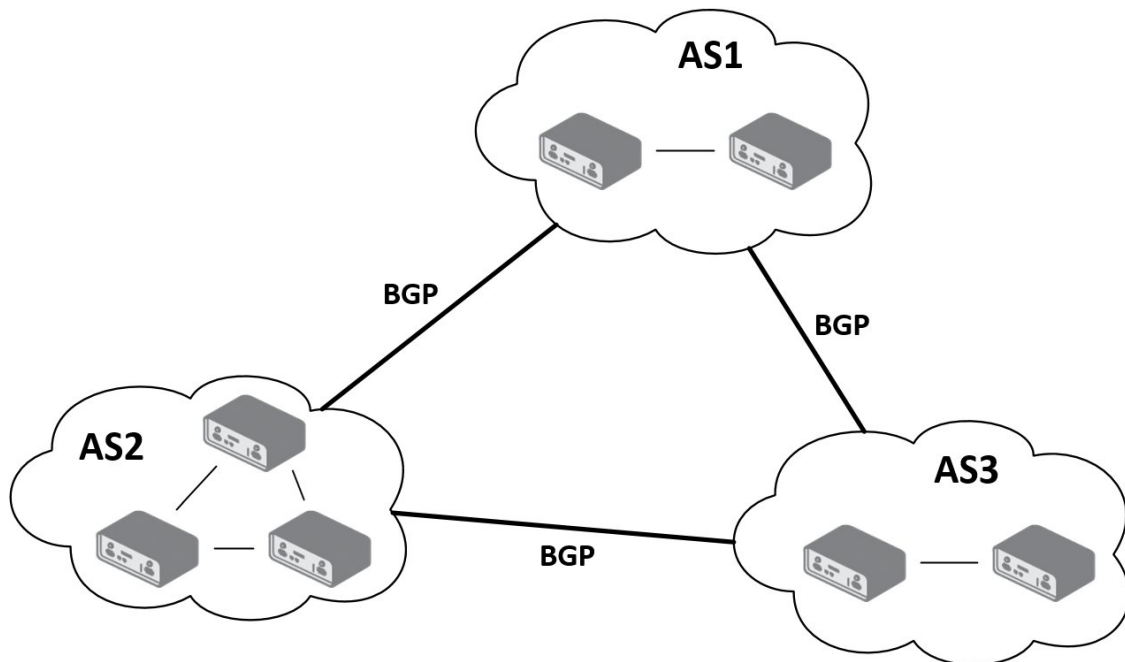


Figure 8: Model scheme

Important notices:

- Using telnet is vty interface of zebra and bgpd daemons available only via the loopback interface 127.0.0.1.
- New configuration files should be created only by an experienced user!

5.5.1 Example of Configuration

The figure below shows a model situation of using the *BGP* router app. Then there are mentioned examples of configuration files of *zebra* and *bgpd* daemons. In this form are entered in the configuration form in the web interface *BGP* or *ZEBRA*.

An example of the *bgpd.conf* configuration file for a device which is referred to as *Advantech router 1* in the figure above:

!

¹<http://docs.frrouting.org/en/latest/bgp.html>

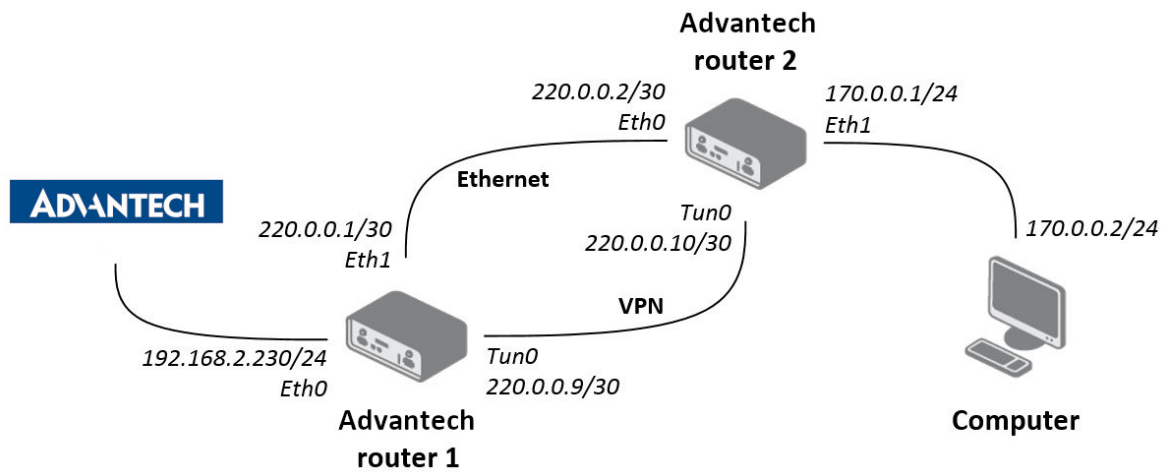


Figure 9: Example of configuration

```

password conel
enable password conel
log syslog
!
router bgp 11111
bgp router-id 220.0.0.1
bgp log-neighbor-changes
network 192.168.2.0/24
!
neighbor 220.0.0.2 remote-as 12345
neighbor 220.0.0.2 next-hop-self

```

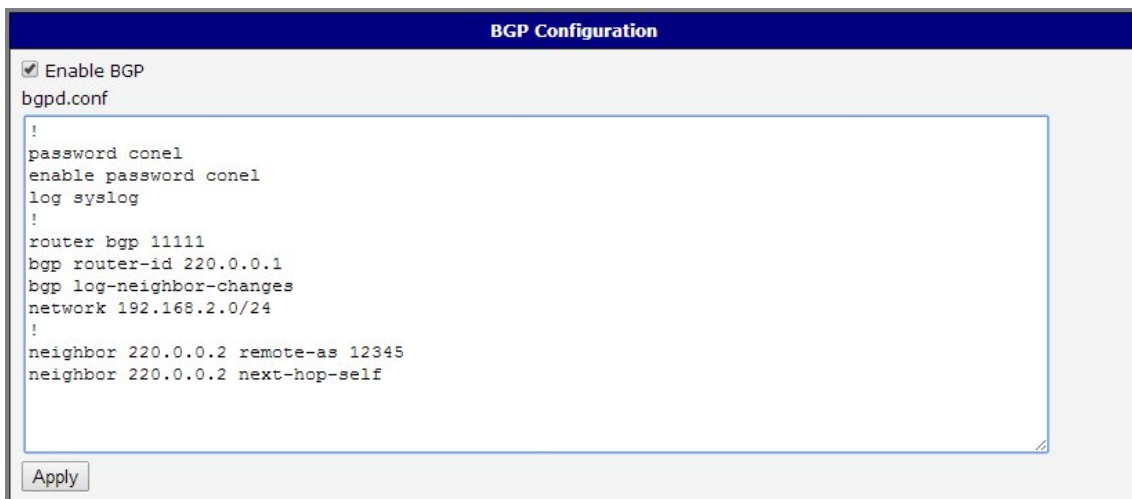


Figure 10: Configuration of bgpd daemon 1

An example of the *bgpd.conf* configuration file for a device which is referred to as *Advantech router 2* in the figure above:

```

!
password conel
enable password conel

```

```
log syslog
!  
router bgp 12345  
  bgp router-id 220.0.0.2  
  bgp log-neighbor-changes  
  network 170.0.0.0/24  
!  
neighbor 220.0.0.1 remote-as 11111  
neighbor 220.0.0.1 next-hop-self
```



Figure 11: Configuration of bgpd daemon 2

5.5.2 BGP Basic commands

The following table lists basic commands which can be used when editing *bgpd.conf* file and description of these commands:

Item	Description
router bgp <ASN>	Configures the BGP routing process for ASN (autonomous system number)
no router bgp <ASN>	Removes a routing process from ASN
bgp router-id <ip-address>	Configures a fixed router ID for a BGP-speaking router
no bgp router-id <ip-address>	Removes the <i>bgp router-id</i> command from the configuration file and restore the default value of the router ID
distance bgp <1-255><1-255> <1-255>	Allows the use of external, internal, and local distances that could be a better route to a node
no distance bgp	Returns distances to the default values (20, 200, 200)
network <network-number>	Specifies the list of networks for the BGP routing process
no network <network-number>	Removes network from the list
aggregate-address <address>	Creates an aggregate entry in a BGP routing table
no aggregate-address <address>	Disables this function
bgp log-neighbor-changes	Enables logging of BGP neighbor resets
no bgp log-neighbor-changes	Disables logging of changes
neighbor <ip-address/peer> remote-as <number>	Adds an entry to the BGP neighbor table
no neighbor <ip-address/peer> remote-as <number>	Removes an entry from the BGP neighbor table
neighbor <ip-address/peer> next-hop-self	Disables next-hop processing of BGP updates on the router
no neighbor <ip-address/peer> next-hop-self	Disables this feature
neighbor <ip-address/peer> version <version>	Sets up the neighbor's BGP version (4, 4+, 4-)
neighbor <name> peer-group	Defines a new BGP peer group
no neighbor <name> peer-group	Removes the peer group and all of its members
show ip bgp	Displays entries in the BGP routing table

Table 2: BGP Basic commands

5.6 ISIS

IS-IS (Intermediate System – Intermediate System) is routing protocol, which is designed for the exchange of routing information between routers. More about this protocol and examples can be found in *IS-IS Application Note* [1] or in the FRR online documentation¹.

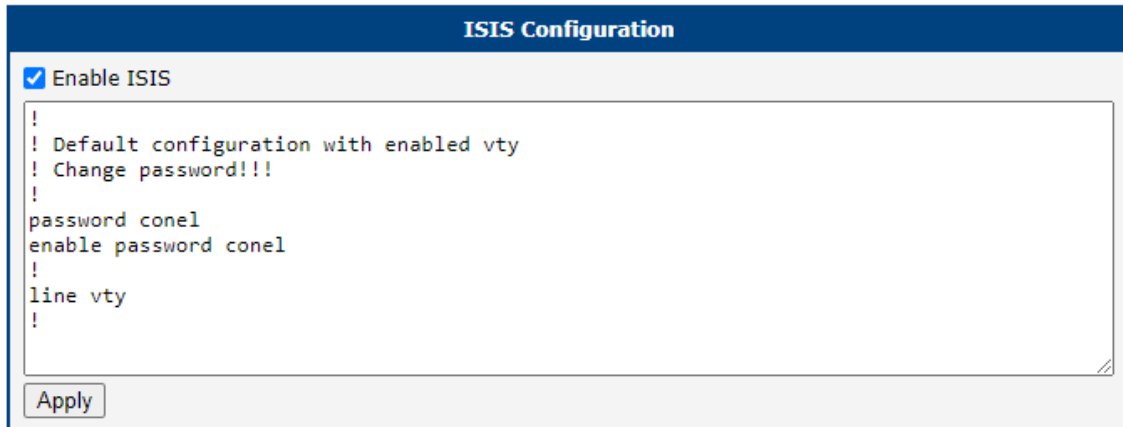


Figure 12: IS-IS Configuration

5.7 OSPF & OSPF6

OSPF and OSPF6 which is IPv6 version of this protocol, are designed for exchanging routing information within an autonomous system. The OSPF is a link state protocol, which means that routers maintain a map of the network (link state database) that is updated after any change to the network topology. To compute the shortest (least cost) path between the router and all the networks is used Dijkstra's algorithm. Then these data are filled in the routing table. More about this protocol and examples can be found in the text below or in the FRR online documentation¹².

Due to this module the OSPF routing protocol is available. This protocol is designed for exchanging routing information within an autonomous system. The OSPF is a link state protocol, which means that routers maintain a map of the network (link state database) that is updated after any change to the network topology. To compute the shortest (least cost) path between the router and all the networks is used Dijkstra's algorithm. Then these data are filled in the routing table.

¹<http://docs.frrouting.org/en/latest/isisd.html>

¹<http://docs.frrouting.org/en/latest/ospfd.html>

²<http://docs.frrouting.org/en/latest/ospf6d.html>

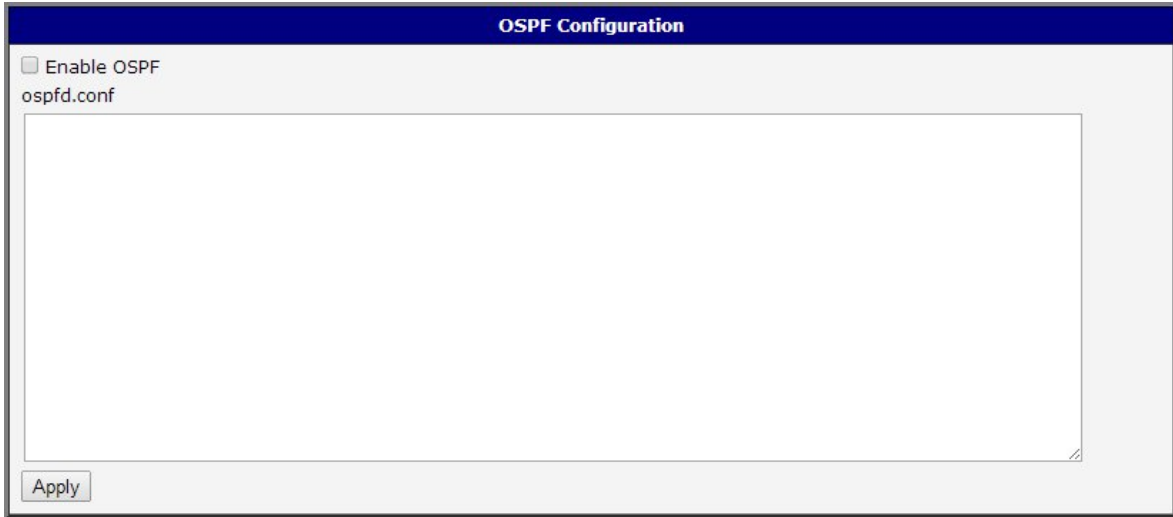


Figure 13: OSPF web interface

Important notices:

- Using telnet is vty interface of zebra and ospfd daemons available only via the loopback interface 127.0.0.1.
- New configuration files should be created only by an experienced user!

5.7.1 Example of configuration

The figure below shows a model situation of using the *OSPF* router app. Then there are mentioned examples of configuration files of *zebra* and *ospfd* daemons. In this form are entered in the configuration form in the web interface *OSPF* or *ZEBRA*.

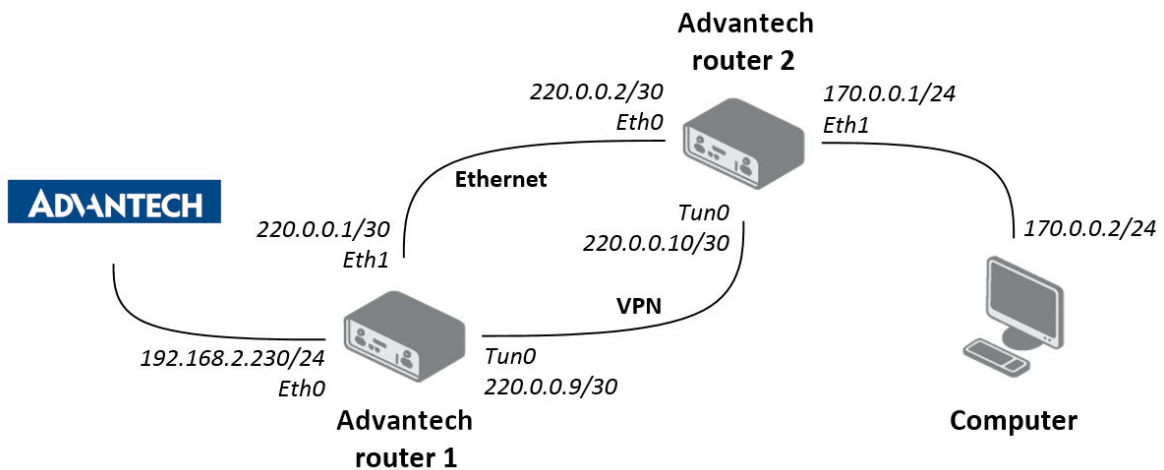


Figure 14: Example of configuration

5.7.2 IPv4 Configuration

An example of the *ospfd.conf* configuration file for a device which is referred to as *Advantech router 1* in the figure above:

```
!  
password conel  
enable password conel  
!  
log syslog  
!  
! interface ven  
! interface eth0  
! interface ppp0  
! po eth  
interface eth1  
ip ospf cost 1  
ip ospf dead-interval 40  
ip ospf hello-interval 10  
!  
! tunelem  
interface tun0  
ip ospf cost 100  
ip ospf dead-interval 40  
ip ospf hello-interval 30  
!  
!  
router ospf  
ospf router-id 220.0.0.1  
redistribute connected metric-type 1  
redistribute static metric-type 1  
!  
network 220.0.0.0/24 area 0  
!  
line vty  
!
```

An example of the *ospfd.conf* configuration file for a device which is referred to as *Advantech router 2* in the figure above:

```
!  
password conel  
enable password conel  
!  
log syslog  
!  
! interface ven  
! interface eth0  
! interface ppp0  
! po eth  
interface eth0  
ip ospf cost 1  
ip ospf dead-interval 40  
ip ospf hello-interval 10  
!  
! tunelem  
interface tun0  
ip ospf cost 100  
ip ospf dead-interval 40  
ip ospf hello-interval 30  
!  
!  
router ospf  
ospf router-id 220.0.0.2  
redistribute connected metric-type 1  
redistribute static metric-type 1  
!  
network 220.0.0.0/24 area 0  
!  
line vty  
!
```

5.7.3 IPv6 Configuration

An example of the *ospf6d.conf* configuration file for a device which is referred to as *Advantech router 1* in the figure above:

```
!  
password conel  
enable password conel  
!  
log syslog  
!  
interface eth1  
ipv6 ospf6 instance-id 1  
ipv6 ospf6 cost 1  
ipv6 ospf6 dead-interval 40  
ipv6 ospf6 hello-interval 10  
ipv6 ospf6 retransmit-interval 5  
!  
interface tun0  
ipv6 ospf6 instance-id 2  
ipv6 ospf6 cost 1  
ipv6 ospf6 dead-interval 40  
ipv6 ospf6 hello-interval 10  
ipv6 ospf6 retransmit-interval 5  
!  
!  
router ospf6  
router-id 220.0.0.1  
redistribute connected  
redistribute static  
interface eth0 area 0.0.0.0  
interface eth1 area 0.0.0.0
```

An example of the *ospf6d.conf* configuration file for a device which is referred to as *Advantech router 2* in the figure above:

```
!  
password conel  
enable password conel  
!  
log syslog  
!  
interface eth0  
ipv6 ospf6 instance-id 1  
ipv6 ospf6 cost 1  
ipv6 ospf6 dead-interval 40  
ipv6 ospf6 hello-interval 10  
ipv6 ospf6 retransmit-interval 5  
!  
interface tun0  
ipv6 ospf6 instance-id 2  
ipv6 ospf6 cost 1  
ipv6 ospf6 dead-interval 40  
ipv6 ospf6 hello-interval 10  
ipv6 ospf6 retransmit-interval 5  
!  
!  
router ospf6  
router-id 220.0.0.2  
redistribute connected  
redistribute static  
interface eth0 area 0.0.0.0  
interface eth1 area 0.0.0.0
```

5.7.4 OSPF Basic commands

The following table lists basic commands which can be used when editing *ospfd.conf* and *ospf6d.conf* files and description of these commands:

Item	Description
router ospf	Enables the OSPF process
no router ospf	Disables the OSPF process
ospf router-id <i><ip-address></i>	Sets the router-ID of the OSPF process
no ospf router-id	Forces OSPF to use the previous OSPF router-id behavior
log-adjacency-changes	Configures the router to send a syslog message when an OSPF neighbor goes up or down
no log-adjacency-changes	Turns off <i>log-adjacency-changes</i> function
network <i><address></i> area <i><areaid></i>	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces
no network <i><address></i> area <i><area-id></i>	Disables OSPF routing for interfaces defined with <i>address</i>
area <i><area-id></i> range <i><address mask></i>	Consolidates and summarizes routes at an area boundary
no area <i><area-id></i> range <i><address mask></i>	Disables this function
area <i><area-id></i> authentication	Enables authentication for an OSPF area
no area <i><area-id></i> authentication	Removes an area's authentication
ip ospf authentication-key <i><password></i>	Assigns a password to be used by neighboring routers that are using OSPF's simple password authentication
no ip ospf authentication-key <i><password></i>	Removes a previously assigned OSPF password
ip ospf cost <i><cost></i>	Specifies the cost of sending packet on an interface
no ip ospf cost	Resets the path cost to the default value
ip ospf dead-interval <i><seconds></i>	Sets how long hello packets must not have been seen before its neighbors declare the router down
no ip ospf dead-interval	Returns to the default time
ip ospf hello-interval <i><seconds></i>	Specifies the interval between hello packets that are sending on the interface
no ip ospf hello-interval	Returns to the default time
ip ospf priority <i><number></i>	Sets the router priority (0-255)
redistribute <i><protocol></i>	Redistributes routes from one routing domain into another domain
no redistribute <i><protocol></i>	Disables redistribution
default-metric	Sets default metric values for the OSPF routing protocol
no default-metric	Returns to the default state
show ip ospf	Displays general information about OSPF routing processes
show ip ospf interface	Displays OSPF-related interface information
show ip ospf neighbor	Displays OSPF-neighbor information

Table 3: OSPF Basic commands

5.8 RIP & RIPNG

RIP and RIPNG which is an IPv6 version of RIP, allows the routers to communicate with each other and react to changes in network topology. The RIP is a distance-vector protocol, which means that routers send each other updated routing tables (don't know the entire network topology). More about this protocol and examples can be found in the text below or in the FRR online documentation¹².

Due to this module the RIP routing protocol is available. Allows the routers to communicate with each other and react to changes in network topology. The RIP is a distance-vector protocol, which means that routers send each other updated routing tables (don't know the entire network topology). Searching the shortest paths in the network is based on the Bellman-Ford's algorithm. The decisive factor is the number of routers leading to the destination network. In terms of safety (protection against routing loops), this number is limited to 15. However, this maximum also limits the size of a network.



Figure 15: RIP web interface

Important notices:

- Using telnet is vty interface of zebra and ripd daemons available only via the loopback interface 127.0.0.1.
- New configuration files should be created only by an experienced user!

5.8.1 Example of configuration

The figure below shows a model situation of using the *RIP* router app. Then there are mentioned examples of configuration files of *zebra* and *ripd* daemons. In this form are entered in the configuration form in the web interface *RIP* or *ZEBRA*.

¹<http://docs.frrouting.org/en/latest/ripd.html>

²<http://docs.frrouting.org/en/latest/ripngd.html>

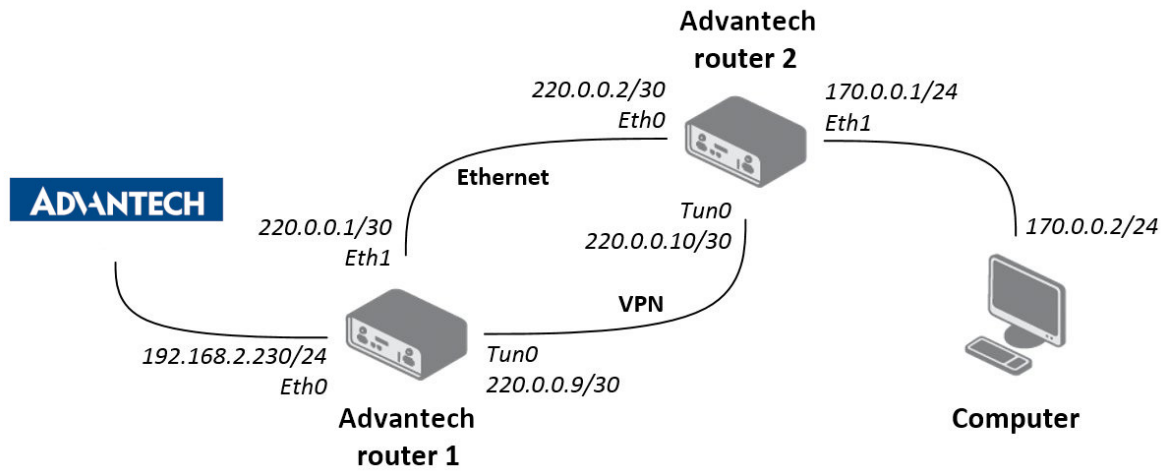


Figure 16: Example of configuration

5.8.2 IPv4 Configuration

An example of the `ripd.conf` configuration file for a device which is referred to as *Advantech router 1* in the figure above:

```
!
password conel
enable password conel
log syslog
!
interface eth0
!
interface eth1
!
interface ppp0
!
interface tun0
!
router rip
version 2
network eth0
network eth1
network tun0
passive-interface eth0
!
line vty
!
```

An example of the *ripd.conf* configuration file for a device which is referred to as *Advantech router 2* in the figure above:

```
!  
password conel  
enable password conel  
log syslog  
!  
interface eth0  
!  
interface eth1  
!  
interface ppp0  
!  
interface tun0  
!  
router rip  
version 2  
network eth0  
network eth1  
network tun0  
! passive-interface eth1  
!  
line vty  
!
```

5.8.3 IPv6 Configuration

An example of the *ripngd.conf* configuration file for a device which is referred to as *Advantech router 1* in the figure above:

```
!  
password conel  
enable password conel  
log syslog  
!  
router ripng  
!  
network eth0  
network eth1  
!  
passive-interface eth0  
!
```

An example of the *ripngd.conf* configuration file for a device which is referred to as *Advantech router 2* in the figure above:

```
!  
password conel  
enable password conel  
log syslog  
!  
router ripng  
!  
network eth0  
network eth1  
!  
! passive-interface eth1  
!
```

5.8.4 RIP Basic commands

The following table lists basic commands which can be used when editing *ripd.conf* and *ripngd.conf* files and description of these commands:

Item	Description
router rip	necessary command to enable RIP
no router rip	disables RIP
network <network>	sets the RIP enable interface by specified network
no network <network>	disables RIP for the specified network
network <ifname>	both the sending and receiving of RIP packets will be enabled on the port specified in this command
no network <ifname>	disables RIP on the specified interface
neighbor <ip-address>	defines a neighboring router with which to exchange routing information
no neighbor <ip-address>	disables the RIP neighbor
passive-interface <ifname>	sets the specified interface to passive mode, i.e. disables sending routing updates on an interface
passive-interface default	sets all interfaces to passive mode
no passive-interface <ifname>	sets the specified interface to normal mode
ip split-horizon	enables the split horizon mechanism (information about the routing is never sent back on the same interface)
no ip split-horizon	disables the split horizon mechanism (enabled on each interface by default)
version <version>	specifies a RIP version used globally by the router (it can be either 1 or 2)
no version	resets the global version setting back to the default
ip rip send version <version>	specifies a RIP version to send on an interface basis
ip rip receive version <version>	specifies a RIP version to receive on an interface basis
show ip rip	shows RIP routes
show ip protocols	displays the parameters and current state of the active routing protocol process

Table 4: RIP Basic commands

5.9 NHRP

The NHRP implementation in this Router App does not support some proprietary Cisco extensions. If you want to use NHRP in conjunction with Cisco devices, consider the following options:

- Use FlexVPN by configuring it on the *IPsec* configuration page. See the *FlexVPN* application note for details.
- Install the dedicated NHRP Router App, which is called *Protocol NHRP (DMVPN)*.

The Next Hop Resolution Protocol (NHRP) is an extension of the ATM ARP routing mechanism that is sometimes used to improve the efficiency of routing computer network traffic over Non-Broadcast, Multiple Access (NBMA) Networks. It can be used by a sender to determine a route with the fewest hops to a receiver. More about this protocol and configuration can be found in the text below or in the FRR online documentation¹.

NHRP Configuration

Enable NHRP

`/var/nhrp/opennhrp.conf`

```
interface gre1
  map 192.168.234.1/24 10.40.29.128 register
  holding-time 60
  shortcut
  redirect
  non-caching
```

`/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)"
  /etc/init.d/ipsec start
  ..
```

Debug Error

Figure 17: NHRP Configuration

¹<http://docs.frrouting.org/en/latest/nhrpd.html>

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 10.40.29.128 register
holding-time 60
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)"
/etc/init.d/ipsec start
;;
peer-down)
echo "Delete link from $NHRP_SRCADDR ($NHRP_SRCNBMA) to $NHRP_DESTADDR ($NHRP_DESTNBMA)"
if [ "$NHRP_PEER_DOWN_REASON" != "lower-down" ]; then
/etc/init.d/ipsec stop
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
```

5.9.1 NHRP Configuration Example

In this example we'll show how to configure situation showed on the diagram below using FRR + IPsec + NHRP + BGP protocols.

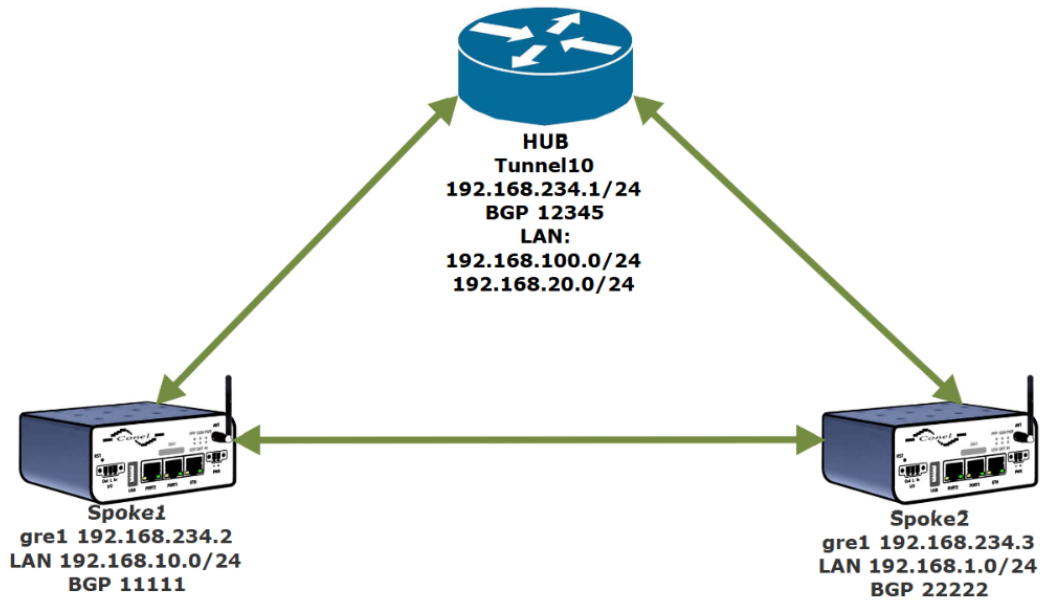


Figure 18: NHRP Example

HUB - Cisco 819

```

!
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 network-id 1234
no ip nhrp record
no ip nhrp cache non-authoritative
ip nhrp redirect
ip ospf 1 area 0
tunnel source FastEthernet4
tunnel mode gre multipoint
tunnel key 1234
tunnel protection ipsec profile DMVPN-P
!

```



```

router bgp 12345
no synchronization
bgp router-id 192.168.234.1
bgp log-neighbor-changes
network 192.168.20.0
network 192.168.100.0
neighbor 192.168.234.2 remote-as 11111
neighbor 192.168.234.3 remote-as 22222
neighbor 192.168.234.4 remote-as 33333
no auto-summary

```

Spoke1 GRE:

1st GRE Tunnel Configuration

Create 1st GRE tunnel

Description *

Remote IP Address *

Local IP Address *

Remote Subnet *

Remote Subnet Mask *

Local Interface IP Address *

Remote Interface IP Address *

Multicasts ▼

Pre-shared Key *

** can be blank*

Figure 19: Spoke1 GRE Configuration

Spoke1 ZEBRA:

```

!
! Default configuration with enabled vty
! Change password!!!
!
password conel
enable password conel
!
line vty
!
log syslog
!
interface eth0
!
interface eth1
!
interface gre1
!
interface usb0
!

```

Spoke1 BGP:

```
!!
Default configuration with enabled vty
! Change password!!!
!
password conel
enable password conel
!!
ine vty
!!
!
router bgp 1111
bgp router-id 192.168.234.2
no bgp ebgp-requires-policy
neighbor 192.168.234.1 remote-as 12345
neighbor 192.168.234.1 disable-connected-check
!
address-family ipv4 unicast
network 192.168.10.0/24
!neighbor 192.168.234.1 soft-reconfiguration inbound
redistribute nhrp
exit-address-family
```

Spoke1 NHRP:

```
! Default configuration with enabled vty
! Change password!!!
!
password conel
enable password conel
!!
ine vty
!!
nhrp nflog-group 1
interface gre1
description DMVPN Tunnel Interface
ip nhrp network-id 1234
tunnel key 1234
ip nhrp redirect
ip nhrp registration no-unique
ip nhrp shortcut
no link-detect
tunnel mode gre multipoint
tunnel source usb0
!i
p nhrp nhs dynamic nbma cisco-ip-address
ip nhrp authentication 1234
```

Spoke1 IPSEC:

1st IPsec Tunnel Configuration	
<input checked="" type="checkbox"/> Create 1st IPsec tunnel	
Description *	NHRP-test
Type	policy-based ▼
Host IP Mode	IPv4 ▼
1st Remote IP Address *	cisco-ip-address
2nd Remote IP Address *	
Tunnel IP Mode	IPv4 ▼
Remote ID *	
Local ID *	

Figure 20: Spoke1 IPSEC Configuration Part 1

First Remote Subnet *	
First Remote Subnet Mask *	
Second Remote Subnet *	
Second Remote Subnet Mask *	
Remote Protocol/Port *	47
First Local Subnet *	
First Local Subnet Mask *	
Second Local Subnet *	
Second Local Subnet Mask *	
Local Protocol/Port *	47
MTU	1426
Remote Virtual Network *	
Remote Virtual Mask *	
Local Virtual Address *	
Cisco FlexVPN **	no ▼
Encapsulation Mode	transport ▼
Force NAT Traversal	yes ▼

Figure 21: Spoke1 IPSEC Configuration Part 2

Route Table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.253.254	0.0.0.0	UG	0	0	0	usb0
192.168.1.0	192.168.234.3	255.255.255.0	UG	20	0	0	gre1
192.168.10.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.20.0	192.168.234.1	255.255.255.0	UG	20	0	0	gre1
192.168.100.0	192.168.234.1	255.255.255.0	UG	20	0	0	gre1
192.168.234.0	0.0.0.0	255.255.255.0	U	0	0	0	gre1
192.168.253.254	0.0.0.0	255.255.255.255	UH	0	0	0	usb0

Figure 22: Spoke1 Route Table

Spoke2 GRE:

1st GRE Tunnel Configuration

Create 1st GRE tunnel

Description *

Remote IP Address *

Local IP Address *

Remote Subnet *

Remote Subnet Mask *

Local Interface IP Address *

Remote Interface IP Address *

Multicasts ▼

Pre-shared Key *

Figure 23: Spoke1 GRE Configuration

Spoke2 ZEBRA:

```
!!
Default configuration with enabled vty
! Change password!!!
!
password conel
enable password conel
!!
ine vty
!!
og syslog
!i
nterface eth0
!i
nterface eth1
!i
nterface gre1
!i
nterface usb0
!
```

Spoke2 BGP:

```
!  
!!  
Default configuration with enabled vty  
! Change password!!!  
!  
password conel  
enable password conel  
!!  
ine vty  
!!  
router bgp 22222  
bgp router-id 192.168.234.3  
no bgp ebgp-requires-policy  
neighbor 192.168.234.1 remote-as 12345  
neighbor 192.168.234.1 disable-connected-check  
!  
address-family ipv4 unicast  
network 192.168.1.0/24  
!neighbor 192.168.234.1 soft-reconfiguration inbound  
redistribute nhrp  
exit-address-family
```

Spoke2 NHRP:

```
! Default configuration with enabled vty  
! Change password!!!  
!  
password conel  
enable password conel  
!!  
ine vty  
!!  
nhrp nflog-group 1  
interface gre1  
description DMVPN Tunnel Interface  
ip nhrp network-id 1234  
tunnel key 1234  
ip nhrp redirect  
ip nhrp registration no-unique  
ip nhrp shortcut  
no link-detect  
tunnel mode gre multipoint  
tunnel source usb0  
!  
!i  
p nhrp nhs dynamic nbma cisco-ip-address  
ip nhrp authentication 1234
```

1st IPsec Tunnel Configuration	
<input checked="" type="checkbox"/> Create 1st IPsec tunnel	
Description *	NHRP-test
Type	policy-based
Host IP Mode	IPv4
1st Remote IP Address *	cisco-ip-address
2nd Remote IP Address *	
Tunnel IP Mode	IPv4
Remote ID *	
Local ID *	

Figure 24: Spoke2 IPSEC Configuration Part 1

First Remote Subnet *	
First Remote Subnet Mask *	
Second Remote Subnet *	
Second Remote Subnet Mask *	
Remote Protocol/Port *	47
First Local Subnet *	
First Local Subnet Mask *	
Second Local Subnet *	
Second Local Subnet Mask *	
Local Protocol/Port *	47
MTU	1426
Remote Virtual Network *	
Remote Virtual Mask *	
Local Virtual Address *	
Cisco FlexVPN **	no
Encapsulation Mode	transport
Force NAT Traversal	yes

Figure 25: Spoke2 IPSEC Configuration Part 2

Route Table						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
0.0.0.0	192.168.253.254	0.0.0.0	UG	0	0	0 usb0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0 eth0
192.168.10.0	192.168.234.2	255.255.255.0	UG	20	0	0 gre1
192.168.20.0	192.168.234.1	255.255.255.0	UG	20	0	0 gre1
192.168.100.0	192.168.234.1	255.255.255.0	UG	20	0	0 gre1
192.168.234.0	0.0.0.0	255.255.255.0	U	0	0	0 gre1
192.168.253.254	0.0.0.0	255.255.255.255	UH	0	0	0 usb0

Figure 26: Spoke2 Route Table

5.10 MPLS

Multiprotocol Label Switching (MPLS) is a routing technique in telecommunications networks that directs data from one node to the next based on labels rather than network addresses. Whereas network addresses identify endpoints, the labels identify established paths between endpoints. MPLS can encapsulate packets of various network protocols, hence the multiprotocol component of the name. MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL.

Figure 27 shows a simplified version of an MPLS domain. There are routers that exist within the MPLS network or domain, and they communicate with each other via a specific label distribution protocol to set up the LSPs. There are other routers that are outside of the MPLS domain that simply forwards IP traffic like a normal router.

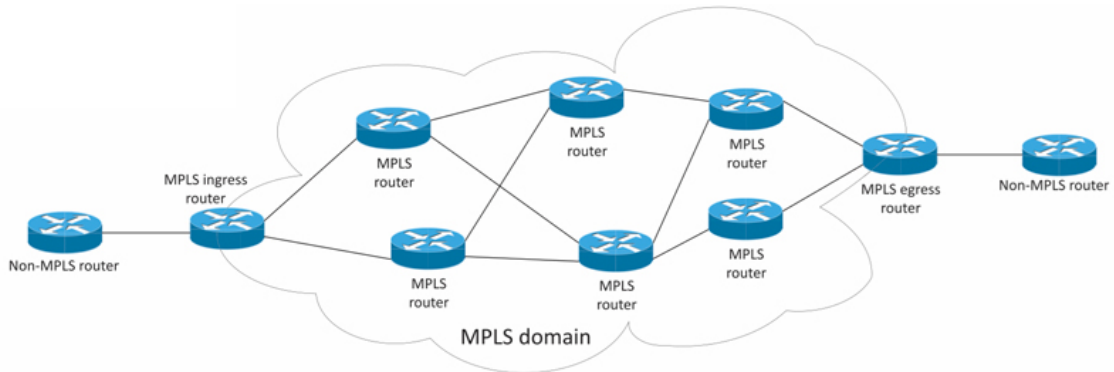


Figure 27: Simplified MPLS Domain Example

To enable the MPLS routing on an Advantech router, install the *FRR* router app first (see Chapter 2.2). Go to the router app’s configuration GUI, select the *Customization* → *Router Apps* → *FRR* → *Configuration* → *MPLS* configuration page. Here, enable the MPLS service and choose which interfaces to enable for the MPLS, as shown in Figure 28. You can set the *Platform Labels* value here as well.

MPLS Configuration	
<input checked="" type="checkbox"/> Enable MPLS	
Enable MPLS on eth0	yes
Enable MPLS on eth1	yes
Enable MPLS on eth2	no
Enable MPLS on gre1	no
Enable MPLS on gre2	no
Platform Labels	10000
<input type="button" value="Apply"/>	

Figure 28: MPLS Configuration

5.11 LDP

Label Distribution Protocol (LDP) is a protocol in which routers capable of Multiprotocol Label Switching (MPLS) exchange label mapping information. Two routers with an established session are called LDP peers and the exchange of information is bi-directional. LDP is used to build and maintain LSP databases that are used to forward traffic through MPLS networks. More about this protocol and examples can be found in the FRR online documentation¹.

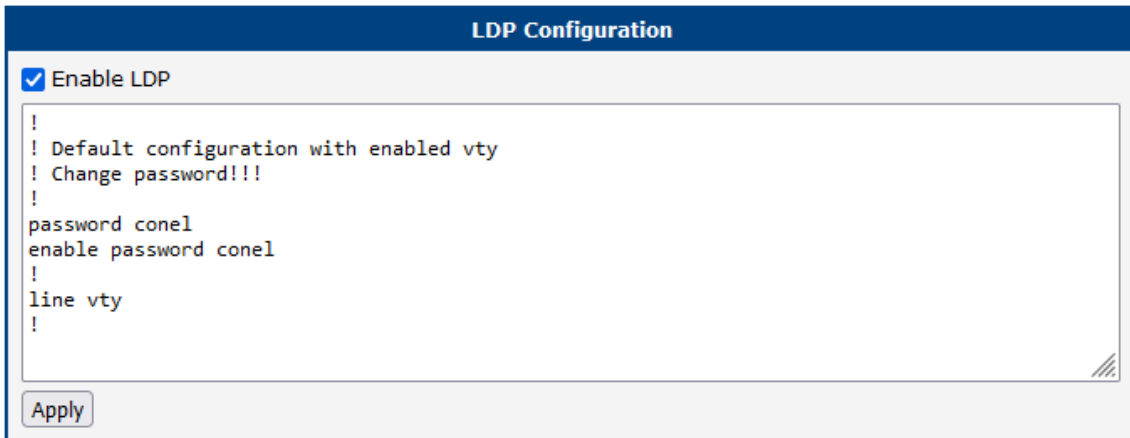


Figure 29: LDP Configuration

¹<http://docs.frrouting.org/en/latest/ldpd.html?highlight=ldp>

5.12 PIM-SM

PIM-SM (Protocol Independent Multicast – Sparse Mode) protocol is the most commonly used multicast routing protocol that is designed on the assumption that recipients for any particular multicast group will be sparsely distributed throughout the network. In order to receive multicast data, routers must explicitly tell their upstream neighbors about their interest in particular groups. PIM-SM by default uses shared trees, which are multicast distribution trees rooted at some selected node (this router is called the Rendezvous Point, RP) and used by all routers sending to the multicast group.

Config of PIM-SM is bit longer and will be split into 3 parts.

The screenshot shows a configuration window titled "PIM_SM Configuration". It contains a checkbox labeled "Enable PIM_SM" which is currently unchecked. Below it is a text input field labeled "RP address*" which is empty.

Figure 30: PIM-SM Configuration

Item	Description
RP Address	IP address of Rendezvous Point. This address needs to be the same on all routers in a routing domain. This field may remain empty if RP is selected using BSR (described later).

Table 5: PIM-SM Commands

When device starts sending multicast traffic, router closest to the source (First Hop Router or FHR) will register itself with RP and starts sending the multicast traffic to the RP router. When a client requests multicast traffic, router closest to the client (Last Hop Router or LHR) will request this traffic from RP. RP will then forward all traffic received from FHR to all LHRs that requested it.

There is also a optimization which takes place, where after LHR starts receiving multicast from RP, it may request the traffic directly from FHR, which should help with latency and load on RP.

5.12.1 BSR - BootStrap Router

The screenshot shows a configuration window titled "BSR configuration". It contains several fields: "Enable BSR" (unchecked checkbox), "Candidate BSR" (unchecked checkbox), "BSR priority" (input field with value 64), "Candidate RP" (unchecked checkbox), "RP priority" (input field with value 192), and "Advertised group" (input field with value 224.0.0.0/4).

Figure 31: PIM-SM Configuration

BSR is a mechanism using which routers automatically decide which router(s) will become RP. All routers that are candidate BSRs (aka C-BSRs) advertise themselves to other routers. C-BSR with **highest** priority will be elected as a BSR.

When BSR is elected, all candidate RPs (or C-RPs) will advertise themselves to the BSR. BSR will choose a C-RP with **lowest** priority and announce to the rest of the network that this router will be the RP. BSR may choose multiple C-RPs if they advertise different groups. A router can be C-BSR, C-RP or both.

When C-RP advertises itself, it includes for range of multicast groups (specified in Advertised group field) for which the router is willing to act as RP.

BSR then chooses subset of C-RPs based on priority and group they advertise.

5.12.2 Interface configuration

Interface configuration		
Interface	DR Priority	Passive
<input type="checkbox"/> eth0	1	<input type="checkbox"/>
<input type="checkbox"/> eth1	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>
<input type="checkbox"/>	1	<input type="checkbox"/>

Use raw config instead

```
!
! Default configuration with enabled vty
! Change password!!!
!
```

* can be blank

Apply

Figure 32: PIM-SM Configuration

First checkbox decides whether interface is included in PIM-SM topology, second field is interface name.

If there are multiple routers connected to the same network segment, like this:

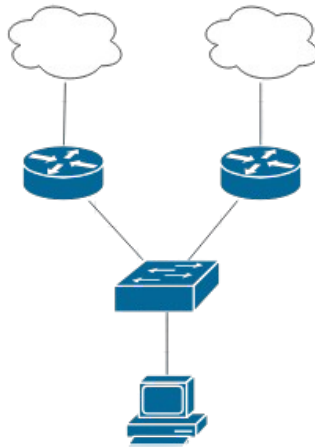


Figure 33: PIM-SM Configuration

All routers will send PIM Hello messages (which routers use to announce themselves and find other routers). Router with highest DR priority will become the Designated Router (DR). Only DR registers multicast source with RP and only DR requests multicast from RP.

However because hello messages are not authenticated, it is sometimes considered a security issue. Mainly because bad actor can send a spoofed PIM hello message causing his computer to be elected as DR. For these situations interface configuration includes “Passive” checkbox.

If interface is configured as passive, it will not send hello or BSR messages to that interface, nor will it process any received hello/BSR messages received on that interface.

- If interface is not enabled and client requests multicast, router will NOT request the multicast from RP, nor will it send hello messages from that interface.
- If interface is enabled and is not passive, router will send hello messages from that interface and if client requests multicast, router will request it from RP.
- If interface is enabled, but it’s also passive, router will NOT send hello messages, but if client requests multicast, router will request it from RP.

If “Use raw config instead” is checked, the above configuration will be ignored and configuration from the field below it will be used instead.

Example below shows a setup where the RP is manually configured, but the BSR is also enabled. On eth0, PIM is enabled in passive mode, while on eth1, PIM is enabled with a modified DR priority. FRR offers more options, which are described on [FRR documentation page](#).

```
!  
router pim  
rp 192.0.2.0 224.0.0.0/4  
bsr candidate-bsr source any priority 64  
bsr candidate-rp source any priority 192  
bsr candidate-rp group 224.0.0.0/4  
!  
interface eth0  
ip pim  
ip igmp  
ip pim passive  
!  
interface eth1  
ip pim  
ip igmp  
ip pim drpriority 20  
!
```

6. Related Documents

[1] [Protocol IS-IS Application Note](#)

[2] [DMVPN Application Note](#)

You can obtain product-related documents on *Engineering Portal* at icr.advantech.com 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 [Development](#) page.