Application Note

FlexVPN

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. APP-0112-EN, revision from 15th November, 2024.

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

List of Figures

List of Tables

1. Basic Information

Internet Key Exchange Version 2 (IKEv2), a next-generation key management protocol based on RFC 4306, is an enhancement of the IKE Protocol. IKEv2 is used for performing mutual authentication and establishing and maintaining security associations (SAs).

FlexVPN is Cisco's implementation of the IKEv2 standard featuring a unified paradigm and CLI that combines site to site, remote access, hub and spoke topologies and partial meshes (spoke to spoke direct). FlexVPN offers a simple but modular framework that extensively uses the tunnel interface paradigm while remaining compatible with legacy VPN implementations using crypto maps

Large customers deploying IPSec VPN over IP networks are faced with high complexity and high cost of deploying multiple types of VPN to meet different types of connectivity requirements. Customers often have to learn different types of VPNs to manage and operate different types of network. And once a technology is selected for a deployment, migrating or adding functionality to enhance the VPN is often avoided. FlexVPN was created to simplify the deployment of VPNs, to address the complexity of multiple solutions, and as a unified ecosystem to cover all types of VPN: remote access, teleworker, site to site, mobility, managed security services, and others. See Figure 1.

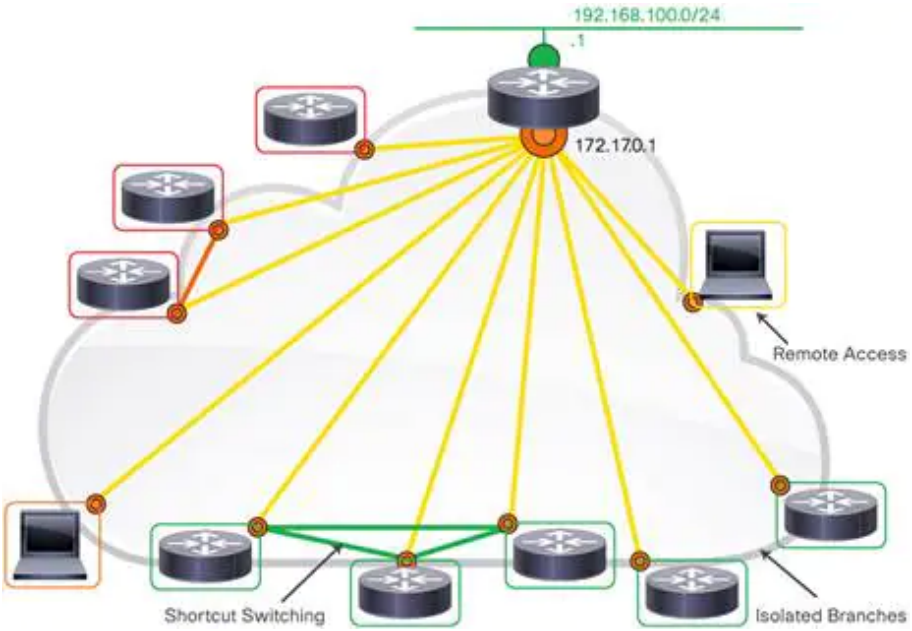


Figure 1: Typical Cisco IOS FlexVPN Deployment

As customer networks increase spans over private, public, and cloud systems, unifying the VPN technology becomes essential, and it became more important to address the need for simplification of design and configuration. Customers can dramatically increase the reach of their network without significantly expanding the complexity of the infrastructure by using Cisco IOS® FlexVPN. FlexVPN is a robust, standards-based encryption technology that helps enable large organizations to securely connect branch offices and remote users and provides significant cost savings compared to supporting multiple separate types of VPN solutions such as GRE, Crypto, and VTI-based solutions. FlexVPN relies on open-standards-based IKEv2 as a security technology and provides on top of it many Cisco® specific enhancements to provide high levels of security, added value, and competitive differentiations.

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.

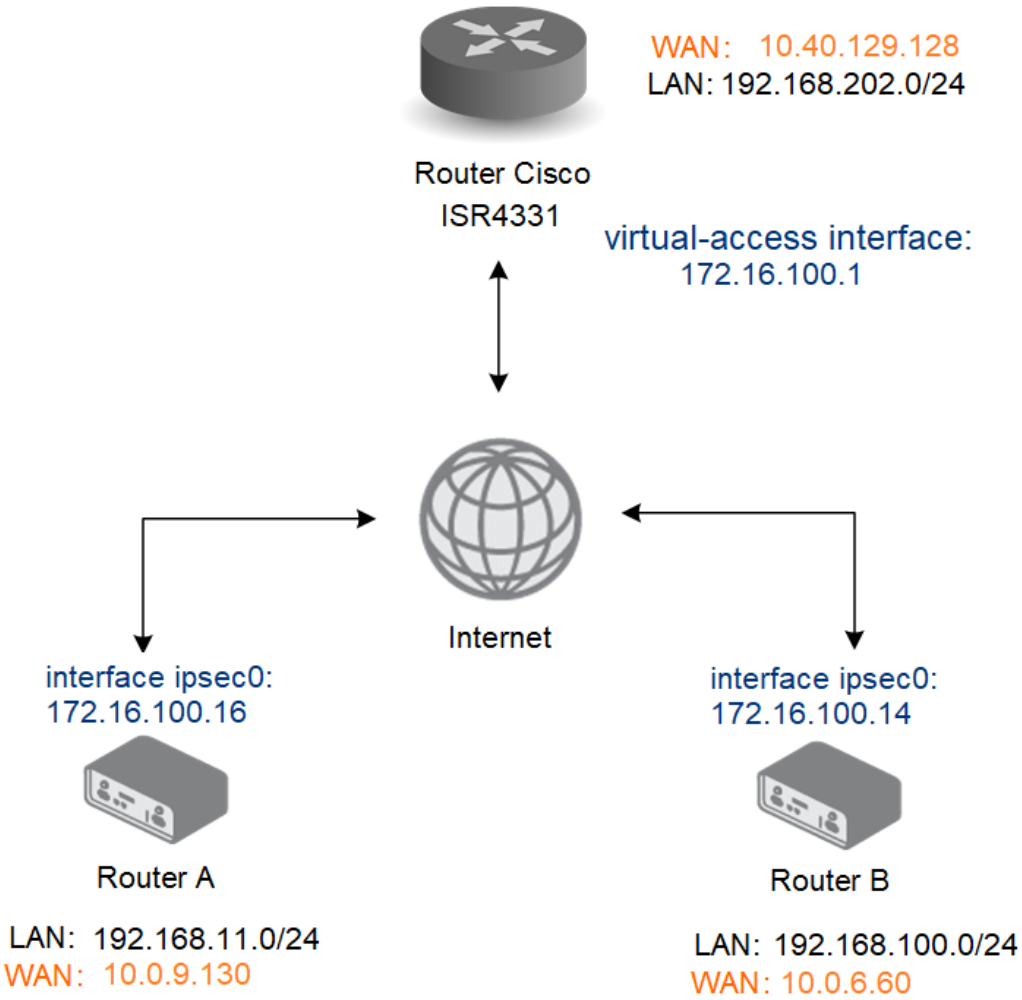


Figure 2: Configuration example scheme

2.1 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.
- *FRR* router app in every spoke router.

See the example configuration below for more details.

> The described router app *FRR* is not included in the standard router firmware. See the Configuration Manual for the description of uploading the router apps to the router.

2.2 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.

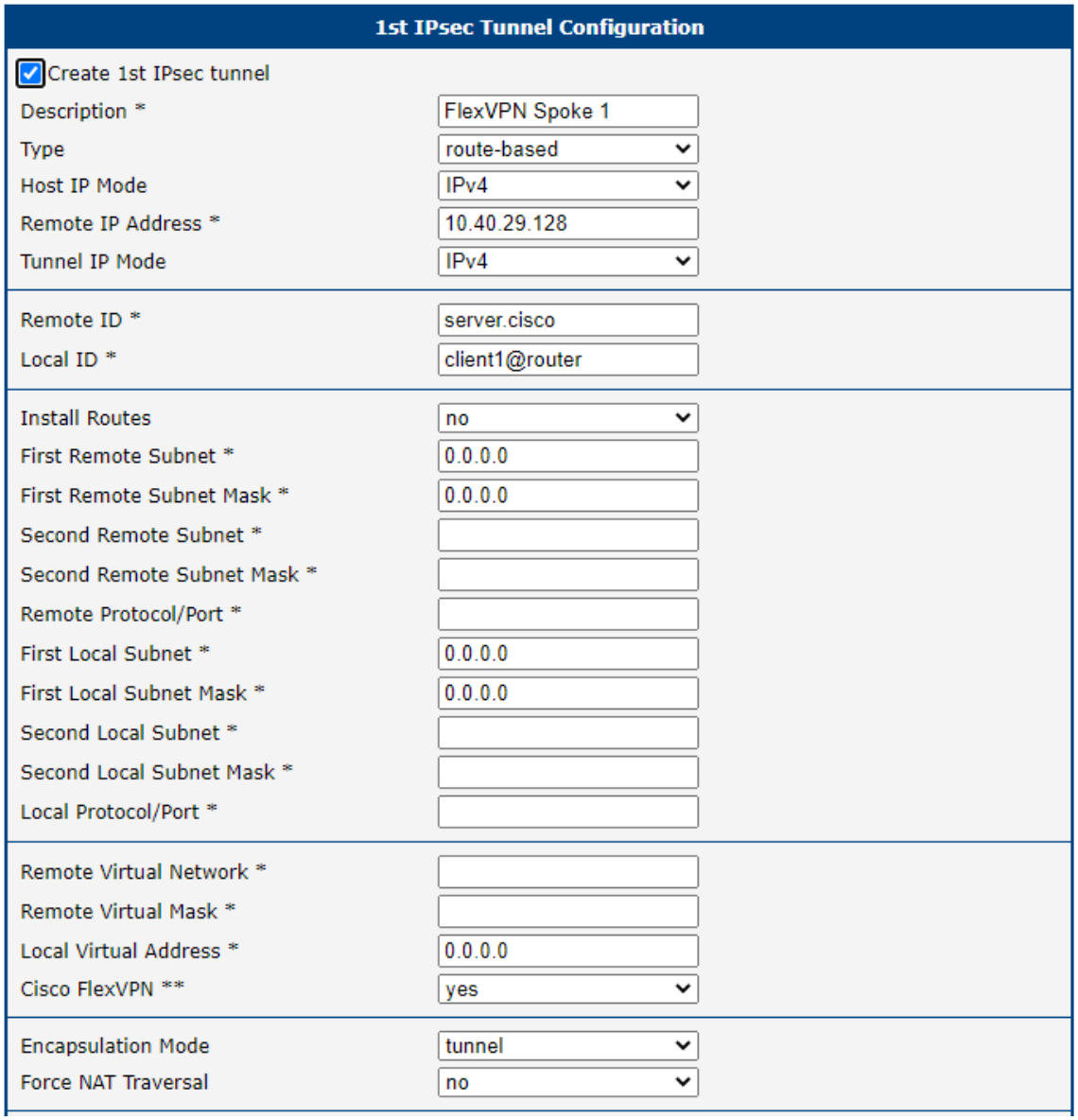
```
aaa authorization network FLEXVPN-AAA-AUTHORIZATION local
!
crypto pki trustpoint server.cisco
enrollment pkcs12
revocation-check none
rsakeypair server.cisco
!
crypto pki certificate map ike_v2_certmap 10
subject-name co client
!
crypto pki certificate chain server.cisco
 certificate 29BEF8C0BE9377F585E4C9E7E569B4B1FEA8544A
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 authorization policy ike_v2_policy
!
crypto ikev2 authorization policy IKE-AUTH-POLICY
pool VPN-SPLIT-TUNNEL-ADDRESSES
route set interface
!
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
aaa authorization group cert list FLEXVPN-AAA-AUTHORIZATION IKE-AUTH-POLICY
virtual-template 20
!
crypto ipsec transform-set aes-gcm esp-gcm 256
mode tunnel
!
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 Loopback2
ip address 172.16.100.1 255.255.255.255
!
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 GigabitEthernet0/0/1.202
encapsulation dot1Q 202
ip address 192.168.202.254 255.255.255.0
!
interface Virtual-Template20 type tunnel
ip unnumbered Loopback2
no ip redirects
tunnel source 10.40.29.128
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN
!
router bgp 65001
bgp router-id 172.16.100.1
bgp log-neighbor-changes
bgp listen range 172.16.100.0/24 peer-group FLEXVPN_SPOKES
neighbor FLEXVPN_SPOKES peer-group
neighbor FLEXVPN_SPOKES remote-as 65001
neighbor FLEXVPN_SPOKES transport connection-mode passive
neighbor FLEXVPN_SPOKES update-source Loopback2
!
address-family ipv4
network 172.16.100.0 mask 255.255.255.0
network 192.168.202.0
neighbor FLEXVPN_SPOKES activate
neighbor FLEXVPN_SPOKES route-reflector-client
neighbor FLEXVPN_SPOKES next-hop-self
neighbor FLEXVPN_SPOKES route-map rr-out out
exit-address-family
!
ip local pool VPN-SPLIT-TUNNEL-ADDRESSES 172.16.100.2 172.16.100.200
```

```
ip route 172.16.100.0 255.255.255.0 Null0
!
route-map rr-out permit 10
set ip next-hop 172.16.100.1
!
```

2.3 IPsec Configuration

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.



1st IPsec Tunnel Configuration	
☑ Create 1st IPsec tunnel	
Description *	FlexVPN Spoke 1
Type	route-based
Host IP Mode	IPv4
Remote IP Address *	10.40.29.128
Tunnel IP Mode	IPv4
Remote ID *	server.cisco
Local ID *	client1@router
Install Routes	no
First Remote Subnet *	0.0.0.0
First Remote Subnet Mask *	0.0.0.0
Second Remote Subnet *	
Second Remote Subnet Mask *	
Remote Protocol/Port *	
First Local Subnet *	0.0.0.0
First Local Subnet Mask *	0.0.0.0
Second Local Subnet *	
Second Local Subnet Mask *	
Local Protocol/Port *	
Remote Virtual Network *	
Remote Virtual Mask *	
Local Virtual Address *	0.0.0.0
Cisco FlexVPN **	yes
Encapsulation Mode	tunnel
Force NAT Traversal	no

Figure 3: IPsec Router A configuration Part 1

IKE Protocol	IKEv2	
IKE Mode	main	
IKE Algorithm	manual	
IKE Encryption	AES256GCM128	
IKE Hash	SHA256	
IKE DH Group	21	
IKE Reauthentication	no	
XAUTH Enabled	no	
XAUTH Mode	client	
XAUTH Username		
XAUTH Password		
ESP Algorithm	manual	
ESP Encryption	AES256GCM128	
ESP Hash	MD5	
PFS	enabled	
PFS DH Group	21	
Key Lifetime	3600	sec
IKE Lifetime	3600	sec
Rekey Margin	540	sec
Rekey Fuzz	100	%
DPD Delay *	60	sec
DPD Timeout *		sec

Figure 4: IPsec Router A configuration Part 2

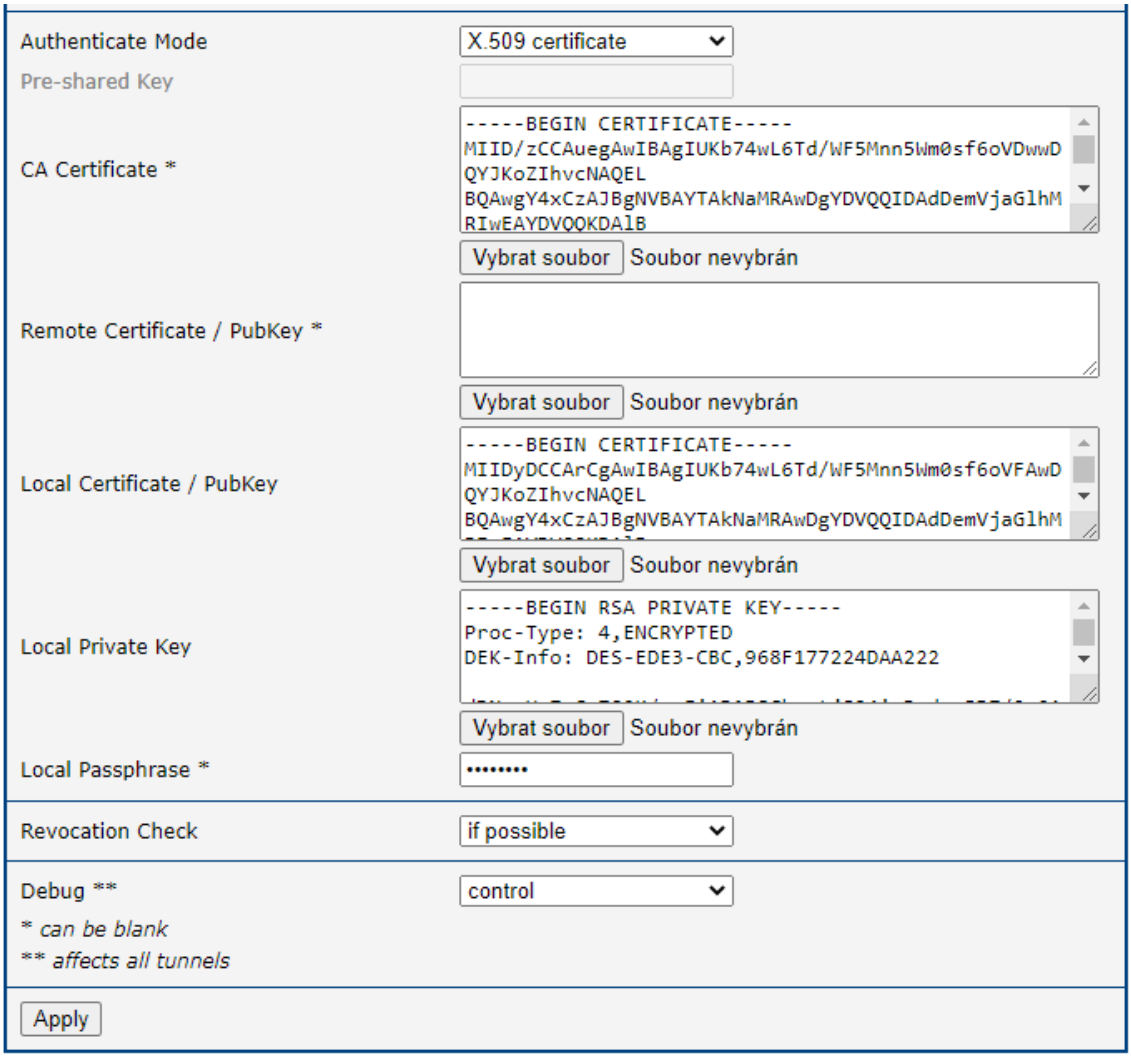


Figure 5: IPsec Router A configuration Part 3

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:

1st IPsec Tunnel Configuration

☑ Create 1st IPsec tunnel	
Description *	FlexVPN Spoke 2
Type	route-based
Host IP Mode	IPv4
Remote IP Address *	10.40.29.128
Tunnel IP Mode	IPv4
Remote ID *	server.cisco
Local ID *	client2@router
Install Routes	no
First Remote Subnet *	0.0.0.0
First Remote Subnet Mask *	0.0.0.0
Second Remote Subnet *	
Second Remote Subnet Mask *	
Remote Protocol/Port *	
First Local Subnet *	0.0.0.0
First Local Subnet Mask *	0.0.0.0
Second Local Subnet *	
Second Local Subnet Mask *	
Local Protocol/Port *	
Remote Virtual Network *	
Remote Virtual Mask *	
Local Virtual Address *	0.0.0.0
Cisco FlexVPN **	yes
Encapsulation Mode	tunnel
Force NAT Traversal	no

Figure 6: IPsec Router B configuration Part 1

IKE Protocol	IKEv2	
IKE Mode	main	
IKE Algorithm	manual	
IKE Encryption	AES256GCM128	
IKE Hash	SHA256	
IKE DH Group	21	
IKE Reauthentication	no	
XAUTH Enabled	no	
XAUTH Mode	client	
XAUTH Username		
XAUTH Password		
ESP Algorithm	manual	
ESP Encryption	AES256GCM128	
ESP Hash	MD5	
PFS	enabled	
PFS DH Group	21	
Key Lifetime	3600	sec
IKE Lifetime	3600	sec
Rekey Margin	540	sec
Rekey Fuzz	100	%
DPD Delay *	60	sec
DPD Timeout *		sec

Figure 7: IPsec Router B configuration Part 2

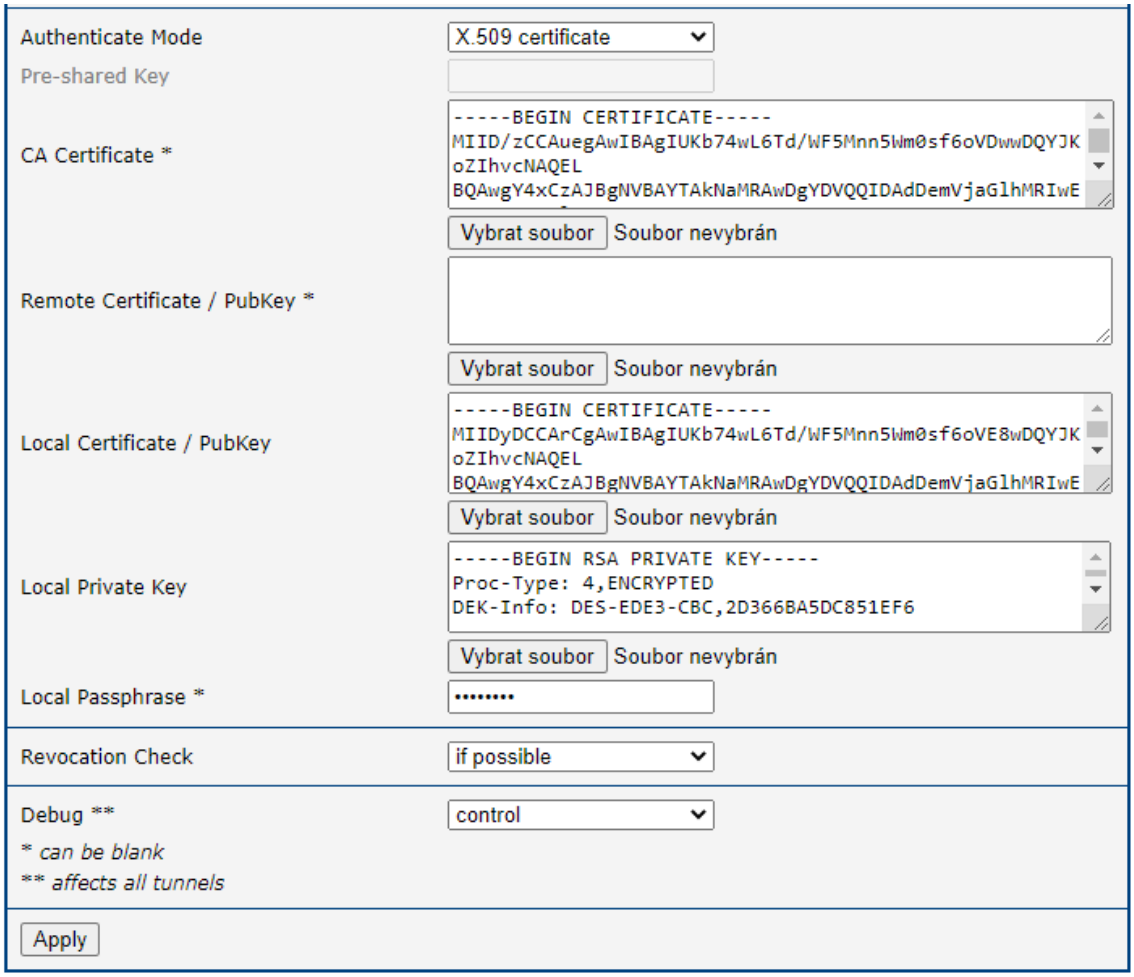


Figure 8: IPsec Router B configuration Part 3

IPsec status of the first router should look something like this

IPsec Status

IPsec Tunnels Information

```
Daemon Information:

strongSwan swanctl 5.9.4
uptime: 19 minutes, since Jan 10 13:17:47 2022
worker threads: 16 total, 11 idle, working: 4/0/1/0
job queues: 0/0/0/0
jobs scheduled: 3
IKE_SAs: 1 total, 0 half-open
mallinfo: sbrk 2588672, mmap 0, used 1291520, free 1297152
loaded plugins: charon tpm nonce revocation pubkey pkcs1 pem openssl curl kernel-netlink socket-default vici updown xauth-generic

Connections:

ipsec1: IKEv2, no reauthentication, rekeying every 3060s, dpd delay 60s
  local:  0.0.0.0
  remote: 10.40.29.128
  local public key authentication:
    id: client1@router
    certs: C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=client1@router
  remote public key authentication:
    id: server.cisco
    cacerts: C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=www.advantech.com, E=advantech@advantech.com
  ipsec1: TUNNEL, rekeying every 3060s, dpd action is restart
    local:  0.0.0.0/0
    remote: 0.0.0.0/0

Security Associations:

ipsec1: #1, ESTABLISHED, IKEv2, e73f2996cf9e9373_i* 50dbd32498e87942_r
  local  'client1@router' @ 10.0.6.60[4500] [172.16.100.14]
  remote 'server.cisco' @ 10.40.29.128[4500]
  AES_GCM_16-256/PRF_HMAC_SHA2_256/ECP_521
  established 1180s ago, rekeying in 1685s
  ipsec1: #1, reqid 1, INSTALLED, TUNNEL, ESP:AES_GCM_16-256
    installed 1180s ago, rekeying in 1490s, expires in 2420s
    in  c657eacc (-|0x00000001),  31586 bytes,   646 packets,   524s ago
    out f1f90200 (-|0x00000001),  35714 bytes,   677 packets,     0s ago
    local  0.0.0.0/0
    remote 0.0.0.0/0
```

Figure 9: IPsec status of router 1 part 1

```
List of X.509 End Entity Certificates

  subject:  "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=client1@router"
  issuer:   "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=www.advantech.com, E=advantech@advantech.com"
  validity:  not before Dec 16 11:38:27 2020, ok
             not after  Jan 01 00:59:59 2031, ok (expires in 3277 days)
  serial:    29:be:f8:c0:be:93:77:f5:85:e4:c9:e7:e5:69:b4:b1:fe:a8:54:50
  altNames:  62.141.23.118, client1.router, client1@router
  flags:     serverAuth
  subjkeyId: ae:56:71:5c:8d:9b:39:e8:f5:af:16:48:ec:3e:e8:56:4b:20:7f:b0
  pubkey:    RSA 2048 bits, has private key
  keyid:     76:8e:b0:fc:32:00:04:03:84:74:8a:a2:2f:48:34:62:f1:fb:3f:66
  subjkey:   ae:56:71:5c:8d:9b:39:e8:f5:af:16:48:ec:3e:e8:56:4b:20:7f:b0

  subject:  "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=server@cisco"
  issuer:   "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=www.advantech.com, E=advantech@advantech.com"
  validity:  not before Nov 27 10:23:30 2019, ok
             not after  Jan 01 00:59:59 2031, ok (expires in 3277 days)
  serial:    29:be:f8:c0:be:93:77:f5:85:e4:c9:e7:e5:69:b4:b1:fe:a8:54:4a
  altNames:  85.207.4.118, server.cisco, server@cisco
  flags:     serverAuth
  subjkeyId: f4:b8:24:c4:69:ca:38:4a:e4:db:bd:c1:33:6b:31:60:d7:5d:1c:62
  pubkey:    RSA 2048 bits
  keyid:     30:42:39:b4:a5:b3:0a:86:9b:f4:82:f6:56:c5:7f:95:14:4e:2c:ad
  subjkey:   f4:b8:24:c4:69:ca:38:4a:e4:db:bd:c1:33:6b:31:60:d7:5d:1c:62

List of X.509 CA Certificates

  subject:  "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=www.advantech.com, E=advantech@advantech.com"
  issuer:   "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=www.advantech.com, E=advantech@advantech.com"
  validity:  not before Nov 25 14:14:59 2019, ok
             not after  Jan 01 00:59:59 2031, ok (expires in 3277 days)
  serial:    29:be:f8:c0:be:93:77:f5:85:e4:c9:e7:e5:69:b4:b1:fe:a8:54:3c
  flags:     CA self-signed
  authkeyId: 3a:04:72:c0:fb:1d:90:25:ee:23:e4:15:1e:92:78:a0:1f:10:3f:36
  subjkeyId: 3a:04:72:c0:fb:1d:90:25:ee:23:e4:15:1e:92:78:a0:1f:10:3f:36
  pubkey:    RSA 2048 bits
  keyid:     43:aa:cc:37:40:80:21:61:c7:9d:9d:52:b3:ba:02:d5:94:e4:47:aa
  subjkey:   3a:04:72:c0:fb:1d:90:25:ee:23:e4:15:1e:92:78:a0:1f:10:3f:36
```

Figure 10: IPsec status of router 1 part 2

and of the second router

IPsec Status

IPsec Tunnels Information

```
Daemon Information:

strongSwan swanctl 5.9.4
uptime: 25 minutes, since Jan 10 13:29:51 2022
worker threads: 16 total, 11 idle, working: 4/0/1/0
job queues: 0/0/0/0
jobs scheduled: 3
IKE_SAs: 1 total, 0 half-open
mallinfo: sbrk 684032, mmap 0, used 510128, free 173904
loaded plugins: charon nonce revocation pubkey pem openssl curl kernel-netlink socket-default vici updown xauth-generic

Connections:

ipsec1: IKEv2, no reauthentication, rekeying every 3060s, dpd delay 60s
  local:  0.0.0.0
  remote: 10.40.29.128
  local public key authentication:
    id: client2@router
    certs: C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=client2@router
  remote public key authentication:
    id: server.cisco
    cacerts: C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=www.advantech.com, E=advantech@advantech.com
  ipsec1: TUNNEL, rekeying every 3060s, dpd action is restart
    local:  0.0.0.0/0
    remote: 0.0.0.0/0

Security Associations:

ipsec1: #1, ESTABLISHED, IKEv2, d778e23c4899e2e5_i* 1da72387e58a1801_r
  local  'client2@router' @ 10.0.9.130[4500] [172.16.100.16]
  remote 'server.cisco' @ 10.40.29.128[4500]
  AES_GCM_16-256/PRF_HMAC_SHA2_256/ECP_521
  established 1506s ago, rekeying in 1320s
  ipsec1: #1, reqid 1, INSTALLED, TUNNEL, ESP:AES_GCM_16-256
    installed 1508s ago, rekeying in 1110s, expires in 2094s
    in  ccd135ad (-|0x00000001),  40550 bytes,   828 packets
    out 2b095580 (-|0x00000001),  44605 bytes,   851 packets,     0s ago
    local  0.0.0.0/0
    remote 0.0.0.0/0
```

Figure 11: IPsec status of router 2 part 1

```
List of X.509 End Entity Certificates

  subject:  "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=client2@router"
  issuer:   "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=www.advantech.com, E=advantech@advantech.com"
  validity:  not before Dec 16 11:36:14 2020, ok
             not after  Jan 01 00:59:59 2031, ok (expires in 3277 days)
  serial:    29:be:f8:c0:be:93:77:f5:85:e4:c9:e7:e5:69:b4:b1:fe:a8:54:4f
  altNames:  62.141.23.118, client2.router, client2@router
  flags:     serverAuth
  subjkeyId: 7f:0b:9c:9d:2c:ae:2c:59:13:f4:6d:5d:be:a6:bc:f7:6d:65:b6:ee
  pubkey:    RSA 2048 bits, has private key
  keyid:     99:e8:e4:94:61:72:d7:1a:8c:b5:53:a3:27:44:b6:1f:7f:89:8b:d4
  subjkey:   7f:0b:9c:9d:2c:ae:2c:59:13:f4:6d:5d:be:a6:bc:f7:6d:65:b6:ee

  subject:  "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=server@cisco"
  issuer:   "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=www.advantech.com, E=advantech@advantech.com"
  validity:  not before Nov 27 10:23:30 2019, ok
             not after  Jan 01 00:59:59 2031, ok (expires in 3277 days)
  serial:    29:be:f8:c0:be:93:77:f5:85:e4:c9:e7:e5:69:b4:b1:fe:a8:54:4a
  altNames:  85.207.4.118, server.cisco, server@cisco
  flags:     serverAuth
  subjkeyId: f4:b8:24:c4:69:ca:38:4a:e4:db:bd:c1:33:6b:31:60:d7:5d:1c:62
  pubkey:    RSA 2048 bits
  keyid:     30:42:39:b4:a5:b3:0a:86:9b:f4:82:f6:56:c5:7f:95:14:4e:2c:ad
  subjkey:   f4:b8:24:c4:69:ca:38:4a:e4:db:bd:c1:33:6b:31:60:d7:5d:1c:62

List of X.509 CA Certificates

  subject:  "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=www.advantech.com, E=advantech@advantech.com"
  issuer:   "C=CZ, ST=Czechia, O=Advantech, OU=Advantech CZ, CN=www.advantech.com, E=advantech@advantech.com"
  validity:  not before Nov 25 14:14:59 2019, ok
             not after  Jan 01 00:59:59 2031, ok (expires in 3277 days)
  serial:    29:be:f8:c0:be:93:77:f5:85:e4:c9:e7:e5:69:b4:b1:fe:a8:54:3c
  flags:     CA self-signed
  authkeyId: 3a:04:72:c0:fb:1d:90:25:ee:23:e4:15:1e:92:78:a0:1f:10:3f:36
  subjkeyId: 3a:04:72:c0:fb:1d:90:25:ee:23:e4:15:1e:92:78:a0:1f:10:3f:36
  pubkey:    RSA 2048 bits
  keyid:     43:aa:cc:37:40:80:21:61:c7:9d:9d:52:b3:ba:02:d5:94:e4:47:aa
  subjkey:   3a:04:72:c0:fb:1d:90:25:ee:23:e4:15:1e:92:78:a0:1f:10:3f:36
```

Figure 12: IPsec status of router 2 part 2

2.4 Zebra Configuration – FRR Router App

Zebra 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 of your router 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 *ZEBRA* protocol of this router. In the *ZEBRA* tick the *Enable ZEBRA* box and insert the configuration commands in the field.

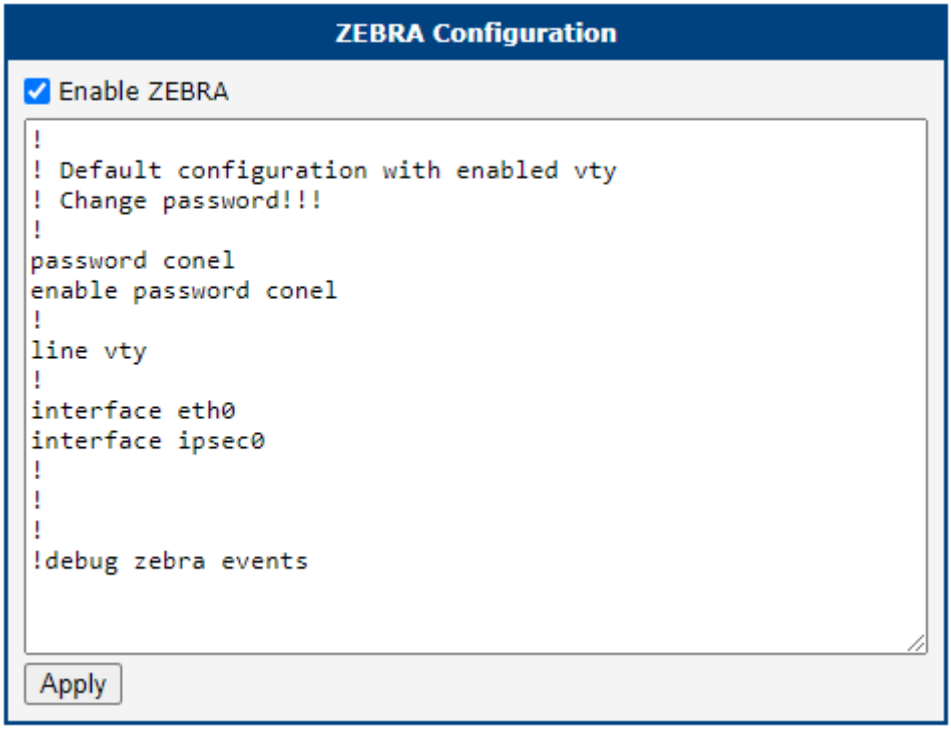


Figure 13: Zebra configuration Router A

and for router B the ZEBRA configuration should be:

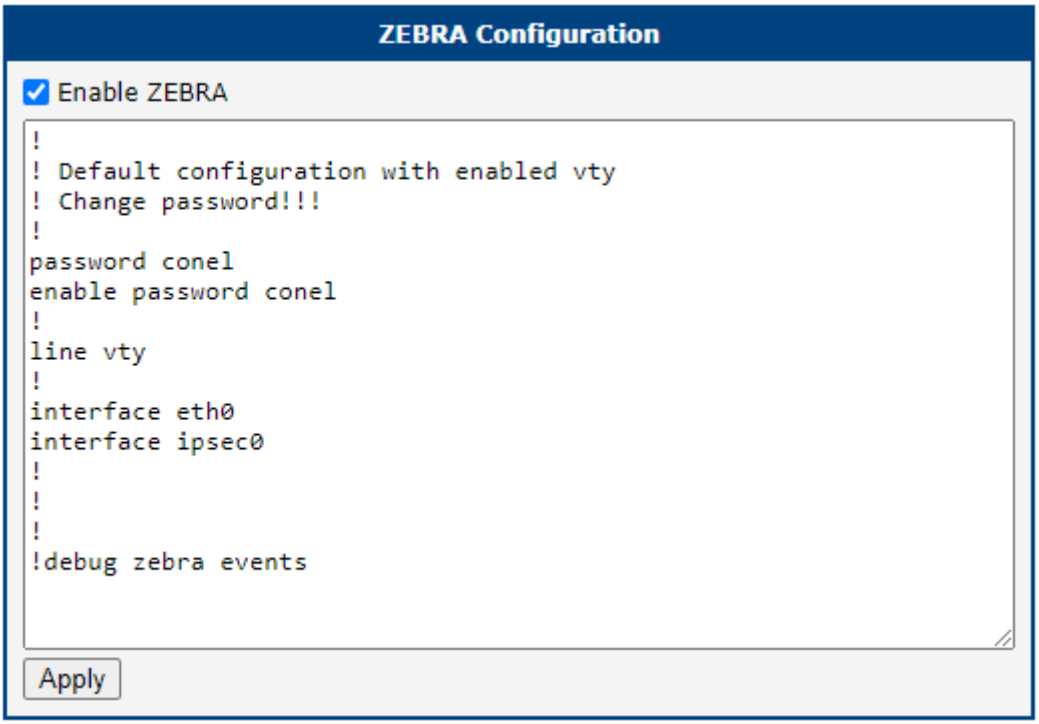


Figure 14: Zebra configuration Router B

2.5 Static Configuration – FRR Router App

Like in Zebra section before, the Static 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 *STATIC* protocol of this router. In the *STATIC* tick the *Enable STATIC* box and insert the configuration commands in the field.

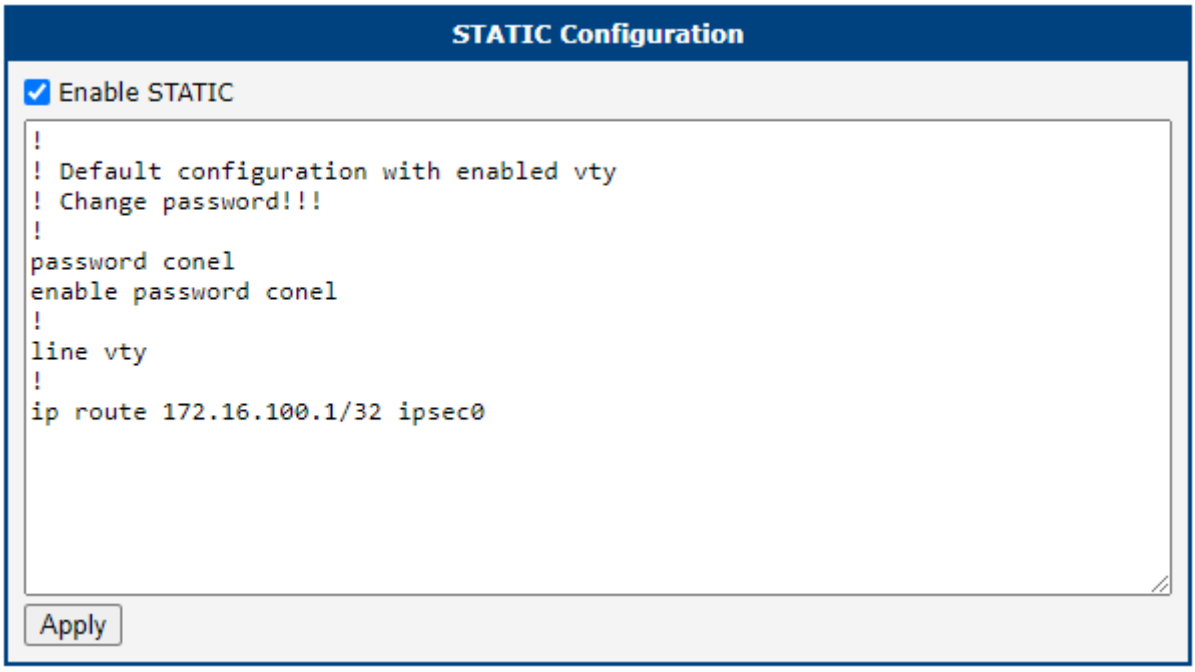


Figure 15: Static configuration Router A

and for router B the Static configuration should be:

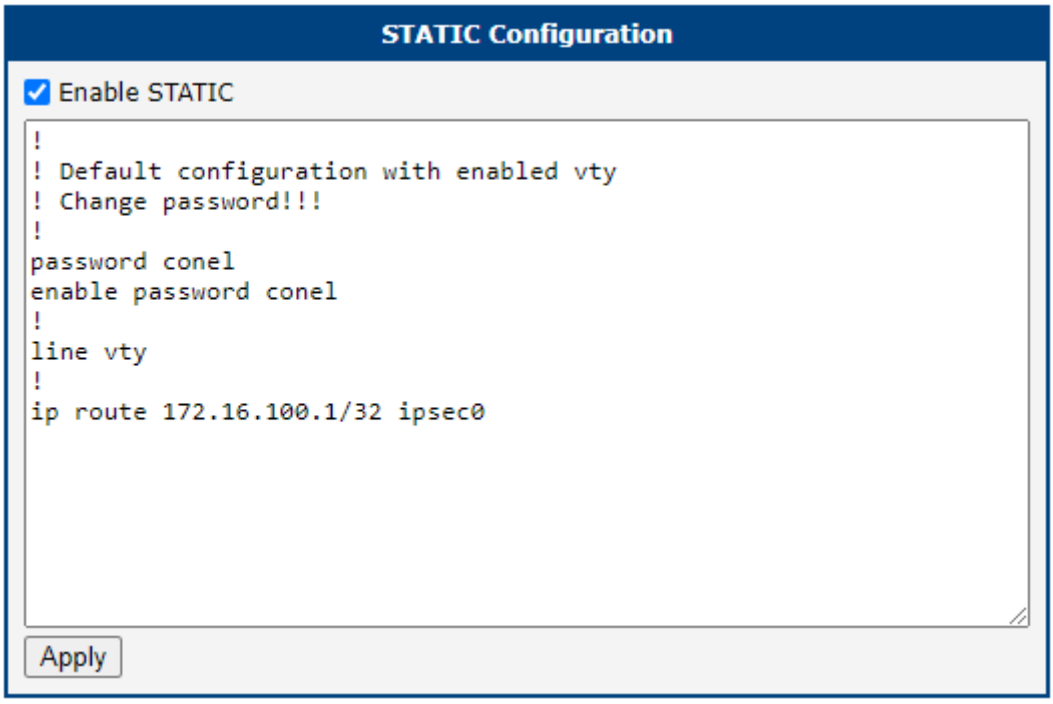


Figure 16: Static configuration Router B

2.6 BGP Configuration – FRR Router App

Like Static and Zebra sections above, the BGP 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 *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:

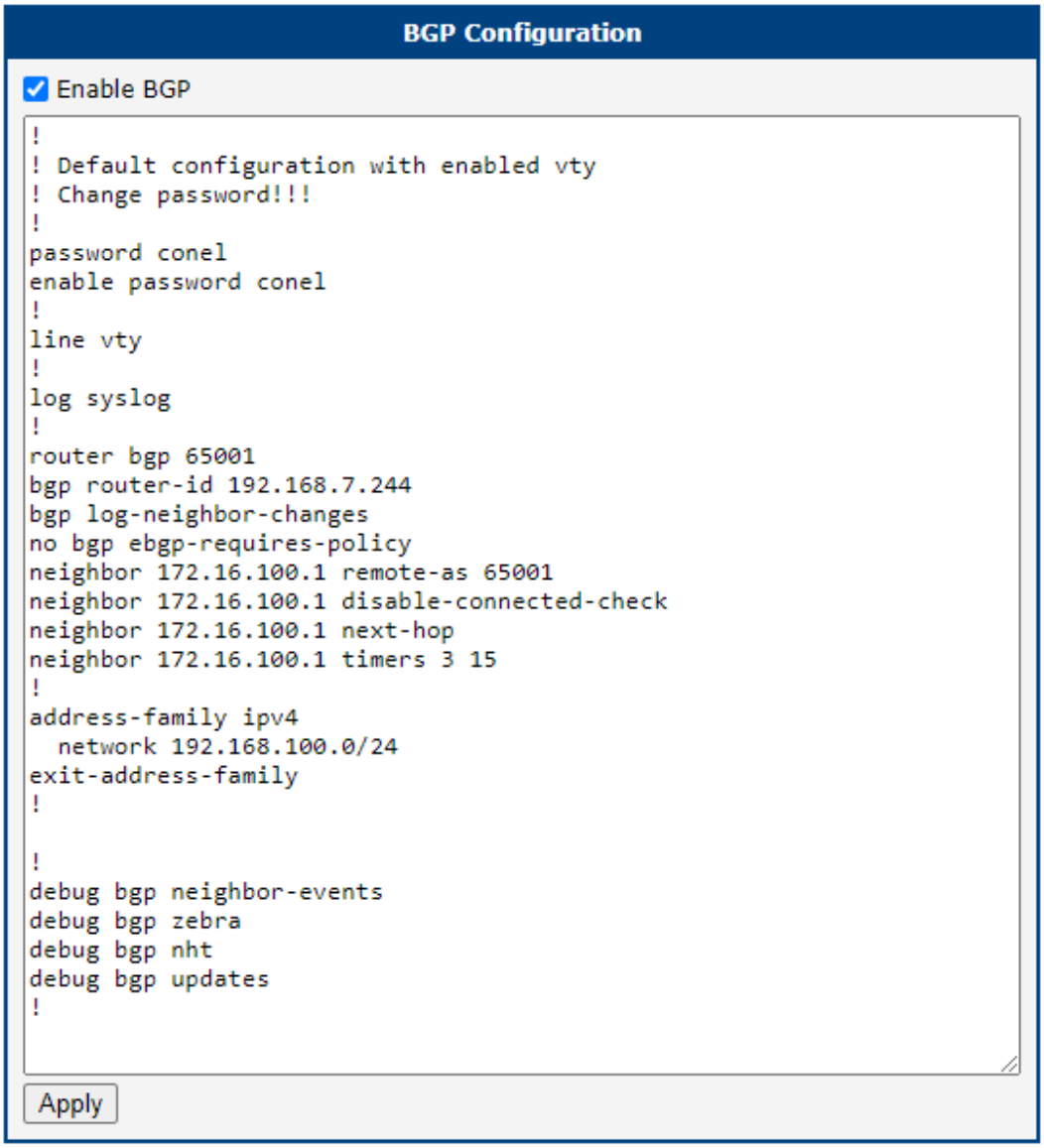


Figure 17: BGP configuration Router A

and BGP configuration for router B can be 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 192.168.7.231
bgp log-neighbor-changes
no bgp ebgp-requires-policy
neighbor 172.16.100.1 remote-as 65001
neighbor 172.16.100.1 disable-connected-check
neighbor 172.16.100.1 next-hop
neighbor 172.16.100.1 timers 3 15
!
address-family ipv4
  network 192.168.11.0/24
exit-address-family
timers bgp 3 15
!
debug bgp neighbor-events
debug bgp zebra
debug bgp nht
debug bgp updates
!
```

Apply

Figure 18: BGP configuration Router B

2.7 Check the Function of FlexVPN

If the configuration is done correctly, you should see changes in the Route Tables of the routers. Here the *Route Table* of the Router B – page *Network* in the *Status* section of the router.

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
172.16.100.0	172.16.100.1	255.255.255.0	UG	20	0	0	ipsec0
172.16.100.1	0.0.0.0	255.255.255.255	UH	20	0	0	ipsec0
192.168.7.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
192.168.11.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.100.0	172.16.100.1	255.255.255.0	UG	20	0	0	ipsec0
192.168.202.0	172.16.100.1	255.255.255.0	UG	20	0	0	ipsec0
192.168.253.254	0.0.0.0	255.255.255.255	UH	0	0	0	usb0

Figure 19: Router B – 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 crypto ikev2 sa detailed
IPv4 Crypto IKEv2  SA

Tunnel-id Local                  Remote                 fvrf/ivrf              Status
3         10.40.29.128/4500      10.0.9.130/4500        none/none              READY
Encr: AES-GCM, keysize: 256, PRF: SHA256, Hash: None, DH Grp:21, Auth sign: RSA, Auth verify: RSA
Life/Active Time: 86400/298 sec
CE id: 1066, Session-id: 39
Status Description: Negotiation done
Local spi: 1DA72387E58A1801       Remote spi: D778E23C4899E2E5
Local id: server.cisco
Remote id: client2@router
Local req msg id:  0              Remote req msg id:  6
Local next msg id: 0              Remote next msg id: 6
Local req queued:  0              Remote req queued:  6
Local window:      5              Remote window:      1
DPD configured for 0 seconds, retry 0
Fragmentation not  configured.
Dynamic Route Update: disabled
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Assigned host addr: 172.16.100.16
Initiator of SA : No

Tunnel-id Local                  Remote                 fvrf/ivrf              Status
1         10.40.29.128/4500      10.0.6.60/4500         none/none              READY
Encr: AES-GCM, keysize: 256, PRF: SHA256, Hash: None, DH Grp:21, Auth sign: RSA, Auth verify: RSA
Life/Active Time: 86400/1023 sec
CE id: 1064, Session-id: 37
Status Description: Negotiation done
Local spi: 50DBD32498E87942       Remote spi: E73F2996CF9E9373
Local id: server.cisco
Remote id: client1@router
Local req msg id:  0              Remote req msg id:  18
Local next msg id: 0              Remote next msg id: 18
Local req queued:  0              Remote req queued:  18
Local window:      5              Remote window:      1
DPD configured for 0 seconds, retry 0
Fragmentation not  configured.
Dynamic Route Update: disabled
Extended Authentication not configured.
```

```
NAT-T is not detected
Cisco Trust Security SGT is disabled
Assigned host addr: 172.16.100.14
Initiator of SA : No

IPv6 Crypto IKEv2  SA

Router#show ip bgp
BGP table version is 11, local router ID is 172.16.100.1
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
*>   172.16.100.0/24  0.0.0.0                  0         32768 i
*>i  192.168.11.0     172.16.100.16            0    100      0 i
*>i  192.168.100.0    172.16.100.14            0    100      0 i
*>   192.168.202.0    0.0.0.0                  0         32768 i

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

Gateway of last resort is 10.40.30.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.40.30.1
is directly connected, GigabitEthernet0/0/0
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.40.28.0/22 is directly connected, GigabitEthernet0/0/0
L        10.40.29.128/32 is directly connected, GigabitEthernet0/0/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
S        172.16.100.0/24 is directly connected, Null0
C        172.16.100.1/32 is directly connected, Loopback2
S        172.16.100.14/32 is directly connected, Virtual-Access1
S        172.16.100.16/32 is directly connected, Virtual-Access3
B     192.168.11.0/24 [200/0] via 172.16.100.16, 00:07:49
B     192.168.100.0/24 [200/0] via 172.16.100.14, 00:10:16
192.168.202.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.202.0/24 is directly connected, GigabitEthernet0/0/1.202
L        192.168.202.254/32 is directly connected, GigabitEthernet0/0/1.202

Router#ping 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 59/61/67 ms
Router#ping 192.168.11.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 217/245/298 ms
Router#ping 172.16.100.14
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.100.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/76/128 ms
Router#ping 172.16.100.16
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.100.16, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 136/228/285 ms
Router#
```

And the FRR status of the first router could look like this

Status Overview

Services

```
-----------------------------------------------------------------------
Protocol mpls is stopped
-----------------------------------------------------------------------
-----------------------------------------------------------------------
Protocol zebra is running
-----------------------------------------------------------------------
FRRouting 7.5.1 (Router).
Router# show ip route vrf all
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

VRF default:
K>* 0.0.0.0/0 [0/0] via 192.168.253.254, usb0, 00:19:11
C>* 10.0.6.60/32 is directly connected, usb0, 00:19:11
B>  172.16.100.0/24 [200/0] via 172.16.100.1 (recursive), weight 1, 00:19:08
  *                           via 172.16.100.1, ipsec0 onlink, weight 1, 00:19:08
S>* 172.16.100.1/32 [1/0] is directly connected, ipsec0, weight 1, 00:19:10
C * 172.16.100.14/32 is directly connected, ipsec0, 00:19:11
C>* 172.16.100.14/32 is directly connected, usb0, 00:19:11
C>* 192.168.7.0/24 is directly connected, eth1, 00:19:11
B>  192.168.11.0/24 [200/0] via 172.16.100.1 (recursive), weight 1, 00:15:04
  *                           via 172.16.100.1, ipsec0 onlink, weight 1, 00:15:04
C>* 192.168.100.0/24 is directly connected, eth0, 00:17:31
B>  192.168.202.0/24 [200/0] via 172.16.100.1 (recursive), weight 1, 00:19:08
  *                            via 172.16.100.1, ipsec0 onlink, weight 1, 00:19:08
K>* 192.168.253.254/32 [0/0] is directly connected, usb0, 00:19:11
Router# show ipv6 route vrf all
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

VRF default:
C>* 64:ff9b::/96 is directly connected, nat64, 00:19:11
C * fe80::/64 is directly connected, lan1, 00:17:31
C * fe80::/64 is directly connected, ipsec0, 00:19:11
C * fe80::/64 is directly connected, nat64, 00:19:11
C>* fe80::/64 is directly connected, switch0, 00:19:11
Router# show mpls table
```

Figure 20: FRR status of router 1 part 1

```
-----------------------------------------------------------------------------
Protocol nhrp is stopped
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
Protocol bgp is running
-----------------------------------------------------------------------------
Router# show bgp summary

IPv4 Unicast Summary:
BGP router identifier 192.168.7.244, local AS number 65001 vrf-id 0
BGP table version 6
RIB entries 7, using 1344 bytes of memory
Peers 1, using 21 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt
172.16.100.1    4      65001       230       386        0    0    0 00:19:09            3        1

Total number of neighbors 1
Router# show ip bgp vrf all

Instance default:
BGP table version is 6, local router ID is 192.168.7.244, vrf id 0
Default local pref 100, local AS 65001
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i172.16.100.0/24  172.16.100.1             0    100      0 i
*>i192.168.11.0/24  172.16.100.1             0    100      0 i
*> 192.168.100.0/24 0.0.0.0                  0         32768 i
*>i192.168.202.0/24 172.16.100.1             0    100      0 i

Displayed  4 routes and 4 total paths
Router# show ip bgp ipv4 vpn
No BGP prefixes displayed, 0 exist


-----------------------------------------------------------------------------
Protocol isis is stopped
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
Protocol ldpd is stopped
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
Protocol ospf is stopped
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
Protocol ospf6 is stopped
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
Protocol rip is stopped
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
Protocol ripng is stopped
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
Protocol staticd is running
-----------------------------------------------------------------------------
```

Figure 21: FRR status of router 1 part 2

And for the second router

Status Overview

Services

```
-----------------------------------------------------------------------
Protocol mpls is stopped
-----------------------------------------------------------------------
-----------------------------------------------------------------------
Protocol zebra is running
-----------------------------------------------------------------------
FRRouting 7.5.1 (Router).
Router# show ip route vrf all
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

VRF default:
K>* 0.0.0.0/0 [0/0] via 192.168.253.254, usb0, 00:30:50
C>* 10.0.9.130/32 is directly connected, usb0, 00:34:51
B>  172.16.100.0/24 [200/0] via 172.16.100.1 (recursive), weight 1, 00:30:40
  *                           via 172.16.100.1, ipsec0 onlink, weight 1, 00:30:40
S>* 172.16.100.1/32 [1/0] is directly connected, ipsec0, weight 1, 00:30:44
C * 172.16.100.16/32 is directly connected, ipsec0, 00:30:43
C>* 172.16.100.16/32 is directly connected, usb0, 00:30:44
C>* 192.168.7.0/24 is directly connected, eth1, 00:34:51
C>* 192.168.11.0/24 is directly connected, eth0, 00:31:24
B>  192.168.100.0/24 [200/0] via 172.16.100.1 (recursive), weight 1, 00:30:40
  *                            via 172.16.100.1, ipsec0 onlink, weight 1, 00:30:40
B>  192.168.202.0/24 [200/0] via 172.16.100.1 (recursive), weight 1, 00:30:40
  *                            via 172.16.100.1, ipsec0 onlink, weight 1, 00:30:40
K>* 192.168.253.254/32 [0/0] is directly connected, usb0, 00:30:50
Router# show ipv6 route vrf all
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

VRF default:
C>* 64:ff9b::/96 is directly connected, nat64, 00:30:50
C>* fd00::/64 is directly connected, eth1, 00:31:02
C * fe80::/64 is directly connected, ipsec0, 00:30:44
C * fe80::/64 is directly connected, nat64, 00:30:50
C>* fe80::/64 is directly connected, eth1, 00:34:51
Router# show mpls table
```

Figure 22: FRR status of router 2 part 1

```
------------------------------------------------------------------------------
Protocol nhrp is stopped
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Protocol bgp is running
------------------------------------------------------------------------------
Router# show bgp summary

IPv4 Unicast Summary:
BGP router identifier 192.168.7.231, local AS number 65001 vrf-id 0
BGP table version 16
RIB entries 7, using 896 bytes of memory
Peers 1, using 18 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt
172.16.100.1    4      65001       422       703        0    0    0 00:30:43            3        1

Total number of neighbors 1
Router# show ip bgp vrf all

Instance default:
BGP table version is 16, local router ID is 192.168.7.231, vrf id 0
Default local pref 100, local AS 65001
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i172.16.100.0/24  172.16.100.1             0    100      0 i
*> 192.168.11.0/24  0.0.0.0                  0         32768 i
*>i192.168.100.0/24 172.16.100.1             0    100      0 i
*>i192.168.202.0/24 172.16.100.1             0    100      0 i

Displayed  4 routes and 4 total paths
Router# show ip bgp ipv4 vpn
No BGP prefixes displayed, 0 exist


------------------------------------------------------------------------------
Protocol isis is stopped
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Protocol ldpd is stopped
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Protocol ospf is stopped
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Protocol ospf6 is stopped
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Protocol rip is stopped
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Protocol ripng is stopped
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Protocol staticd is running
------------------------------------------------------------------------------
```

Figure 23: FRR status of router 2 part 2

3. Related Documents

You can obtain product-related documents on the **Engineering Portal** at *icr.advantech.com*.

To access your router's documents or firmware, go to the *Router Models* page, locate the required model, and select the appropriate tab below.

Documents that are common to all models and describe specific functionality areas are available on the *Application Notes* page.

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

If you are interested in further options for extending router functionality, either through scripts or custom Router Apps, please see the information available on the *Development* page.