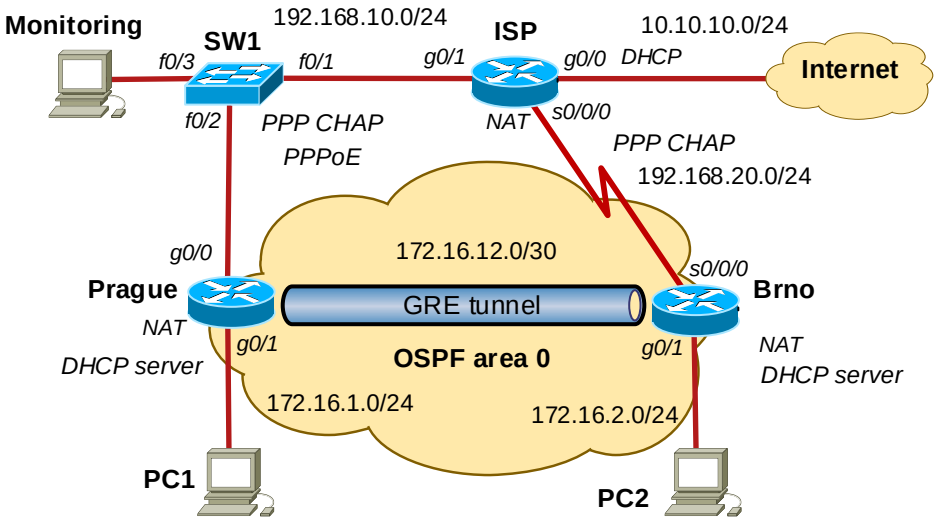
FACULTY OF INFORMATION TECHNOLOGY

CCNA R&S 4

Configuring VPN using GRE tunnel (1/2)



Scenario — Connecting Remote Branch Offices using VPN GRE Tunnel

Industrial company has two offices in Prague and in Brno. Prague's office is connected via DSL connection (emulated by PPPoE), while Brno's branch uses a serial link. In order to secure company communication, a VPN tunnel is created between the edge routers of these branches. Configure ISP connection and VPN tunnel using GRE. Enable OSPF routing over GRE tunnel.

Task 1 — Configure Basic Device Settings.

1. Prepare your network.
Cable network topology.
2. Perform basic router configuration.
Configure the router hostnames to match the topology diagram.
Disable DNS lookup.
Configure IP addressing on ISP router only.
Configure DHCP servers for LANs on Brno and Prague. Exclude the first 10 addresses. DNS server is 10.10.10.1.

Task 2 — Configuring PPP connection over serial link: ISP router.

Configure PPP connection to Brno with one-way authentication using CHAP and IP address assignment. Use username *Brno*, password *Brno1* to authentication the client and IPs from 192.168.20.0.0/24. Exclude the first ten IP addresses.

1. Configure local IP address pool for PPP users over serial connection on ISP router.
router(conf)# ip local pool <serial-link-pool> <starting-IP> <ending-IP>
2. Configure PPP on ISP router.
router(conf)# username <*name*> password <*pwd*>
router(conf-if)# ip address <IP> <mask>
router(conf-if)# encapsulation ppp
router(conf-if)# peer default ip address pool <serial-link-pool>
router(conf-if)# ppp authentication chap callin

Task 3 — Configure PPP connection over serial link: Brno router.

Configure PPP connection on router Brno with CHAP authentication and IP address assignment.
1. Configure PPP on Brno router.
router(conf-if)# encapsulation ppp
router(conf-if)# ppp chap hostname <*name*>
router(conf-if)# ppp chap password <*pwd*>
router(conf-if)# ip address negotiated
2. Verify PPP connection.
router# sh ip interface brief
3. Set up a static default route to the ISP.
router(conf)# ip route 0.0.0.0 0.0.0.0 <ISP-address>

Task 4 — Configure Traffic Monitoring using SPAN Port on the Switch.

1. Configure port mirroring on switch SW1.
switch(conf)# hostname SW1
SW1(conf)# monitor session 1 source interface f0/1
SW1(conf)# monitor session 1 destination interface f0/3
2. Verify monitoring session
SW1# show monitor
3. Open Wireshark network analyzer on Monitoring PC.
Capture and analyze PPP negotiation and PPPoE initialization.

Task 5 — Configure PPPoE connection over Ethernet: ISP router.

1. Create a local pool for PPPoE clients and a local user database for PPPoE customers. Use username cust1 and password cust1pwd. Exclude the first ten IP addresses.
router(conf)# username <username> password <passwd>
router(conf)# ip local pool <pppoe-link-pool> <starting-IP> <ending-IP>

2. Create a virtual template for customers.
router(conf)# interface virtual-template 1
router(conf-if)# ip address <IP-address> <mask> ; specifies the IP address of ISP router
router(conf-if)# mtu 1492
router(conf-if)# peer default ip address pool <name2>
router(conf-if)# ppp authentication chap callin

3. Assign the template to the global broadband aggregation group.
router(conf)# bba-group pppoe global
router(conf-bba-group)# virtual-template 1

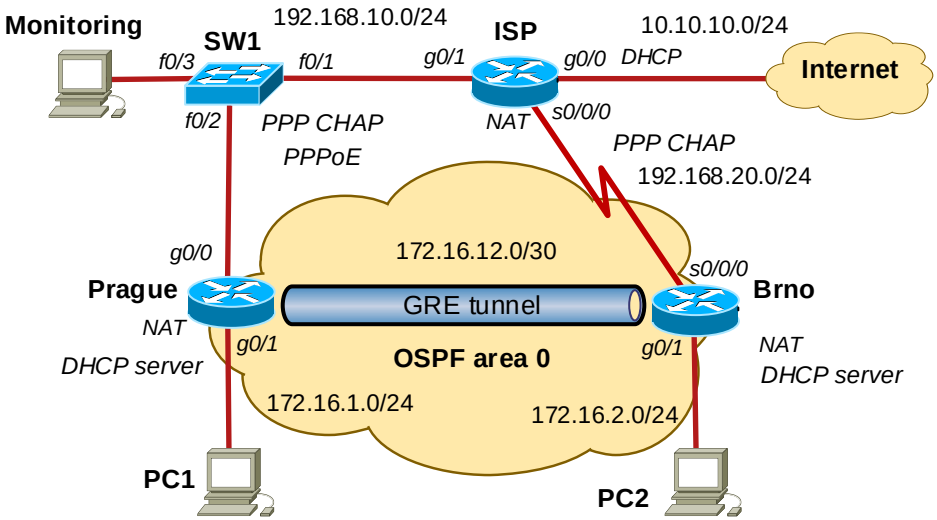
4. Associate the group with the physical interface
router(conf)# interface g0/1
router(conf)# pppoe enable group global
router(conf)# no shutdown

5. Verify the settings
router# show ip interface brief
router# show ip local pool

FACULTY OF INFORMATION TECHNOLOGY

CCNA R&S 4

Configuring VPN using GRE tunnel (2/2)



Task 6 — Configure PPPoE connection over Ethernet: Prague router.

1. Create a virtual dialer interface for PPP.
```
router(conf)# interface dialer 1
router(conf-if)# encapsulation ppp
router(conf-if)# dialer pool 1
router(conf-if)# mtu 1492
router(conf-if)# ip address negotiated
router(conf-if)# ppp authentication chap callin
router(conf-if)# ppp chap hostname <username>
router(conf-if)# ppp chap password <passwd>
```
2. Associate the g0/0 interface with a dialer interface.
```
router(conf)# interface g0/0
router(conf-if)# pppoe enable
router(conf-if)# pppoe-client dial-pool-number 1
```
3. Set up a static default route pointing to the Dialer interface.
```
router(conf)# ip route 0.0.0.0 0.0.0.0 dialer 1
```
4. Set up debugging to display PPP and PPPoE negotiation.
```
router# debug ppp authentication
router# debug pppoe events
```
5. Enable the g0/0 interface.
```
router(conf)# interface g0/0
router(conf-if)# no shutdown
```
6. Verify the setting and test the connection.
```
router# show pppoe session
router# show ip interface brief
router# show ip route
router# ping <IP address>
```
7. Analyze PPPoE encapsulated communication on Monitoring PC.
Look at the format of PPP protocols LCP and NCP and the exchanged messages.
Look at PPPoE header and encapsulation of user traffic, e.g., ICMP, DNS, TCP, etc.

Task 7 — Configure NAT translation on ISP, Prague and Brno.

1. Connect ISP router to the Internet. Configure DHCP client on interface g0/0.
```
router(conf)# interface g0/0
router(conf-if)# ip address dhcp
router(conf-if)# no shutdown
```
2. Configure PAT translation on ISP for all customers
NAT will translate the input traffic from 192.168.10.0/24 and 192.168.20.0/24 networks.
As inside interfaces use the serial interface s0/0/0 and the virtual template interface.
3. Verify NAT translation
```
router# show access-lists
router# show ip nat translation
```
4. Similarly, configure NAT translation on Brno and Prague.
As an outside interface use the dialer interface.

Task 8 — Configure GRE tunnel.

1. Configure the tunnel interface between Prague and Brno routers. Use network 172.16.12.0/30 for inner tunnel addressing.
```
router(conf]# interface tunnel 0
router(conf-if)# ip address <local-tunnel-IP-address> <mask>     ; inner tunneled IP address
router(conf-if)# tunnel source <global-IP-address>               ; outer source IP address
router(conf-if)# tunnel destination <remote-global-IP-address>   ; outer destination IP address
```
2. Verify that the GRE tunnel is functional.
```
router# show ip interface brief
router# show ip interface tunnel 0
```
3. Verify what are the tunnel source, destination and tunneling protocol.
```
router# show interface tunnel 0
```
4. Test connection between PCs in LANs.

Task 9 — Configure OSPF Routing via GRE tunnel.

1. Configure OSPF are 0 between Brno and Prague. Do not distribute OSPF updates to LANs.
```
router(conf)# router ospf <process-id>
router(conf-route)# network <IP> <wildcard> area <area-no>
```
2. Check the routing process and routing tables.
If connection between OSPF neighbors cannot be established, check and update MTU on the tunnel interface.
3. Test connection between PCs in LANs.

Task 10 — Analyzing Encapsulation.

1. Analyze the following connections using network analyzer Wireshark on the Monitoring PC.
(i) Connection from PC1 to PC2 via GRE tunnel.
(ii) Connection from PC1 to ISP.
(iii) Connection from PC1 to the Internet
2. Observe PPPoE and GRE encapsulation (length of the frames, headers).

Task 11 — Finish the Lab.

1. Save your configuration to TFTP server on Monitoring PC.
2. Remove cables.
3. Switch off PCs.