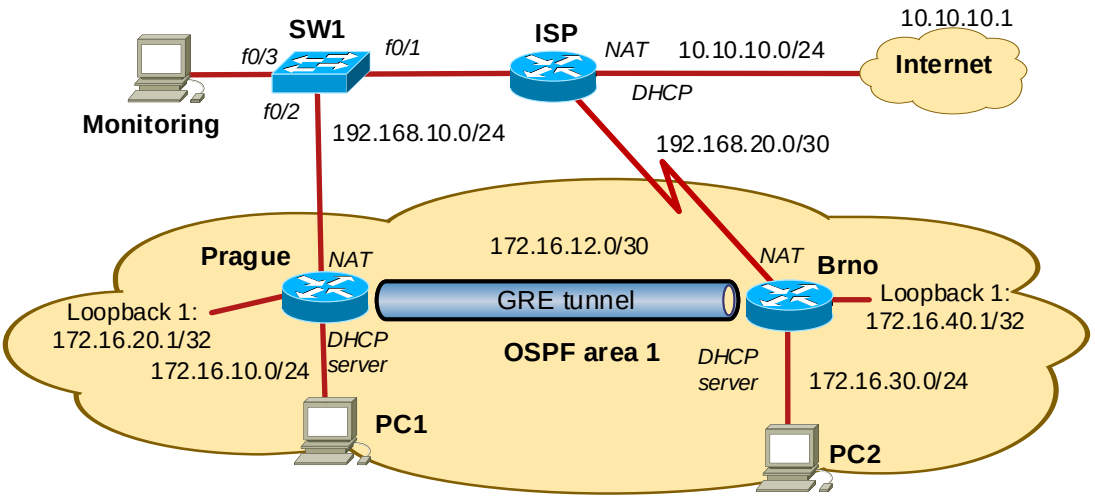
FACULTY OF INFORMATION TECHNOLOGY

ENSA Configuring VPN using GRE tunnel



Scenario — Connecting Remote Sites Using GRE VPN

Brno Tech, Ltd. with headquarter in Brno has a branch in Prague. Both site are connected to the ISP using a serial line. Configure a VPN connection between both side using the GRE tunnel. Enable OSPF routing using the VPN tunnel.

Task 1 — Basic configuration.

Configure routers Prague, ISP, and Brno and switch SW1.

1. Set router names, disable DNS lookup on the routers. Configure links on routers Brno and Prague towards ISP. ISP is connected to the Internet using a DHCP.
2. Connect Monitoring station to the SW1. Do not set IP address on the Monitoring station.

Configuring local DHCP server.

1. On router Prague, resp. Brno, configure a DHCP server for LAN 172.16.10.0/24, resp. 172.16.30.0/24. Reserve the first for 10 addresses for future usage. Set DNS server to 10.10.10.1.
2. Configure loopback interfaces on Prague and Brno.

Task 2 — Edge router configuration.

Configure edge routers Prague and Brno. All local traffic will be translated towards ISP using PAT.

1. Configure PAT for all local LANs on Prague/Brno.
2. Set a default static routes on Prague and Brno towards ISP.
2. Verify connection:

ping PC1 -> Prague:	YES - NO	ping PC2 -> Brno:	YES – NO
ping PC1 -> ISP:	YES - NO	ping PC2 -> ISP:	YES – NO
ping PC1 -> PC2:	YES - NO	ping Brno -> PC2:	YES – NO
ping PC1 -> www.fit.vut.cz:	YES - NO	ping Brno -> www.fit.vut.cz:	YES – NO

Task 3 — Configure NAT translation to the Internet

Configure PAT translation on the ISP router.

1. Only traffic from 192.168.10.0/24 and 192.168.20.0/30 is allowed to be NAT translated.
2. Verify connection from PC1 and PC2 to www.fit.vutbr.cz.

Task 4 — Configure GRE tunnel and verify connection.

1. Configure GRE tunnel between Prague and Brno. Use network 172.16.12.0/30 for the tunnel.
2. Verify the state of the tunnel.
3. Verify connection:
ping Prague -> Brno: YES – NO ping PC1 -> PC2: YES – NO

Task 5 — Configure routing between local sites over VPN.

1. Configure OSPF routing between both local sites over VPN tunnel.
Do not distribute routing information towards ISP or to the local networks.
2. Clean NAT translation tables on all routers.
router# clear ip nat translation *
3. Verify connection:
ping PC1 -> PC2: YES – NO ping PC1 -> 172.16.40.1: YES – NO
ping PC2 -> 172.16.20.1: YES – NO
4. Verify NAT translation tables on Prague/Brno and ISP. Why there are no ICMP entries in the NAT table? Explain.

5. Write the OSPF entries in the routing table on Prague or Brno, respectively:
router# show ip route ospf

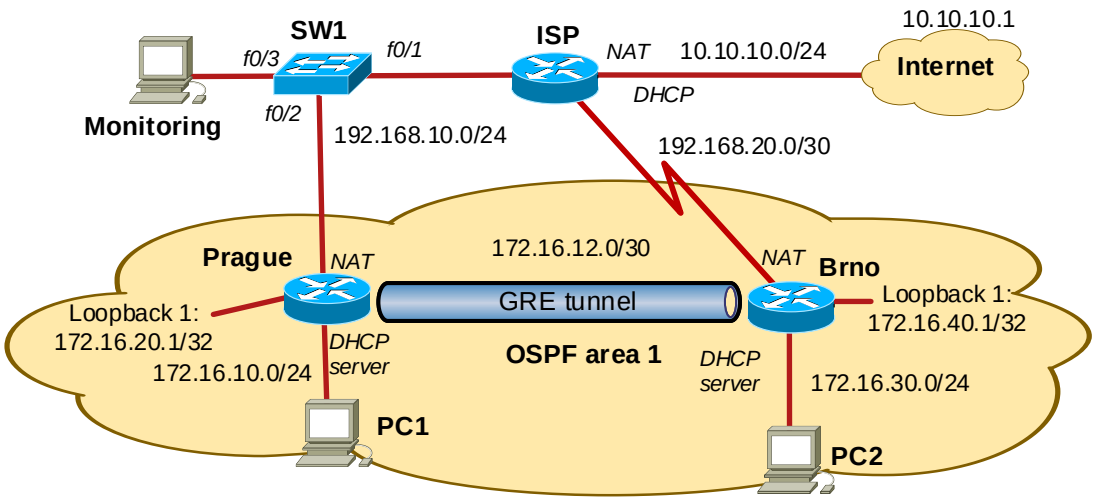
Hints:

 # GRE tunnel configuration
router(conf]# interface tunnel 1
router(conf-if)# ip address *<tunnel-source-IP-address> <mask>* ; internal tunnel address
router(conf-if)# tunnel source *<source-IP-address>* ; external source address
router(conf-if)# tunnel destination *<remote-IP-address>* ; external destination address
router(conf-if)# tunnel mode gre ip ; tunnel type

 # Verify GRE tunnel
router# show ip interface brief
router# show interface tunnel 1

FACULTY OF INFORMATION TECHNOLOGY

ENSA Configuring VPN using GRE tunnel



Encapsulated OSPF packets:

Transport Src IP address:	Transport Dst IP address:
IP protocol type:	GRE type:
Encapsulated Src IP address:	
Encapsulated Dst IP address:	

Ping PC1 -> www.fit.vut.cz:

Source IP address:

Dst IP address:

IP protocol type:

ICMP type and code:

Task 6 Configure Traffic Monitoring using SPAN Port on the Switch

1. **Basic switch configuration.**
   Configure switch name. Disable DNS lookup on the switch.
2. **Configure port mirroring on switch SW1.**
   SW1(conf)# monitor session 1 source interface f0/1
   SW1(conf)# monitor session 1 destination interface f0/3
3. **Verify monitoring session**
   SW1# show monitor
4. **Open Wireshark network analyzer on Monitoring PC.**
   Start ping from PC1 to PC2.
   Start ping from PC1 to www.fit.vut.cz.
   Capture and analyze GRE Communication and other communication of interest. Fill the following table:

Ping PC1-> PC2:

Transport Src IP address:	Transport IP address:
IP protocol type:	GRE type:
Encapsulated Src IP address:	Encapsulated Dst IP address:
IP protocol type:	ICMP type and code:

Task 7 Finish the Lab

1. **Remove cables.**
2. **Switch off the PCs.**

Hints:

 # Configuring switch SPAN port
; define the port name where packets will be captured
sw(conf)# monitor session <number> source interface <if-name>

; define the port name where captured packets will be sent
sw(conf)# monitor session <number> destination interface <if-name>

; verify the monitor:
sw# show monitor