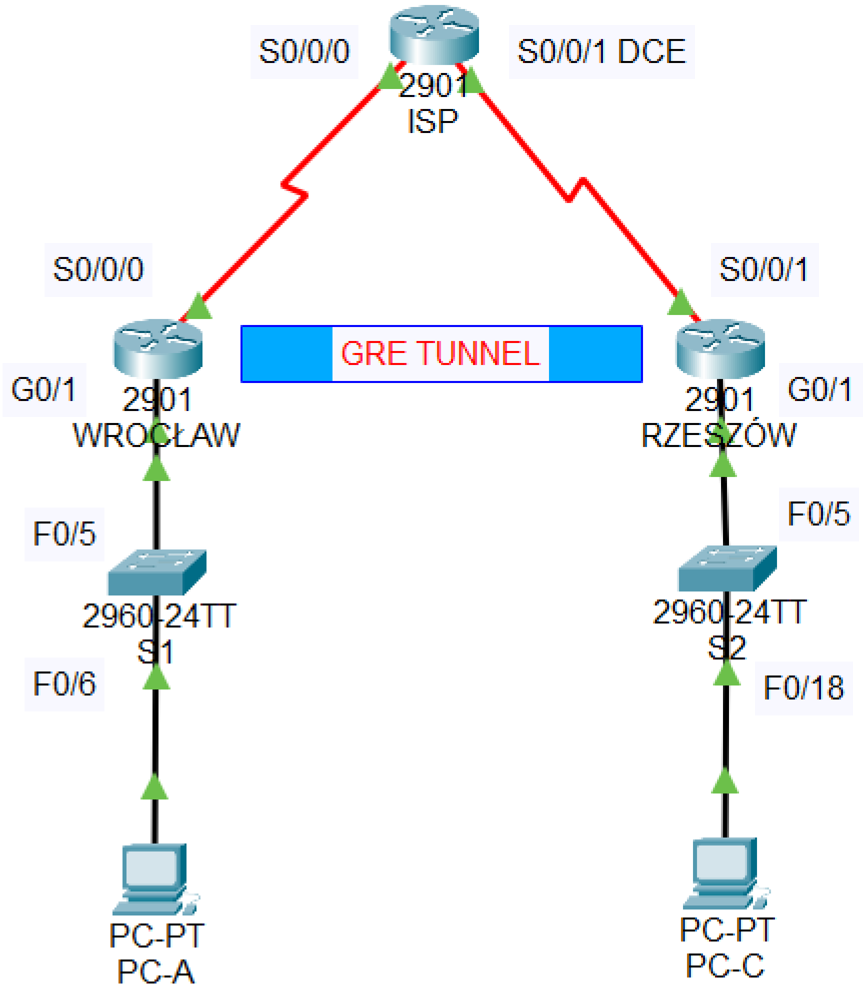
Network Security - Laboratory Exercise Report

GRE Tunnel Configuration with OSPF Implementation

Exercise Objectives

The primary objective was to implement and verify a secure GRE tunnel with OSPF routing between remote network locations, demonstrating proficiency in enterprise network protocols and security measures.



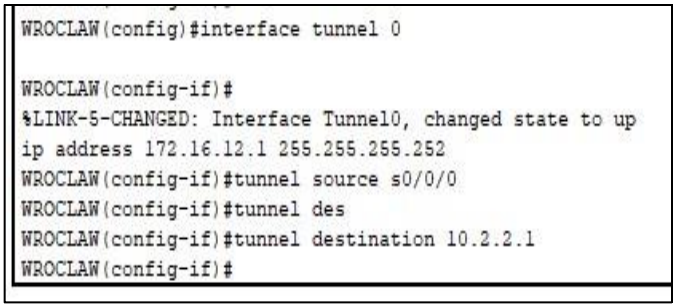
Network Architecture

Implementation Environment:

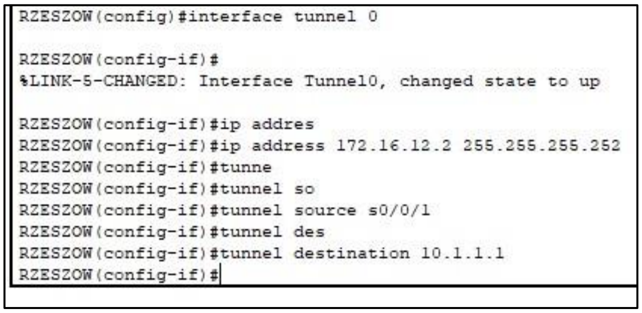
- 3x Cisco 2911 Routers (WROCLAW, RZESZOW, ISP)
- 2x End Devices (PC-A, PC-C)
- Network Segments: 172.16.1.0/24, 172.16.2.0/24
- Tunnel Network: 172.16.12.0/30
- ISP Links: 10.1.1.0/30, 10.2.2.0/30

Technical Implementation

1. GRE Tunnel Configuration

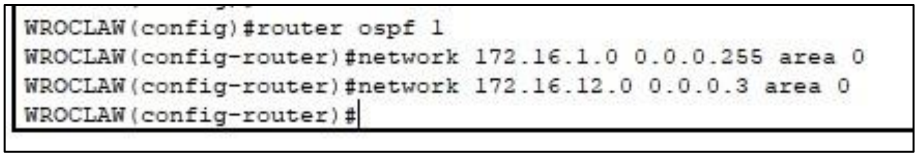


```
WROCLAW(config)#interface tunnel 0

WROCLAW(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up
ip address 172.16.12.1 255.255.255.252
WROCLAW(config-if)#tunnel source s0/0/0
WROCLAW(config-if)#tunnel des
WROCLAW(config-if)#tunnel destination 10.2.2.1
WROCLAW(config-if)#
```

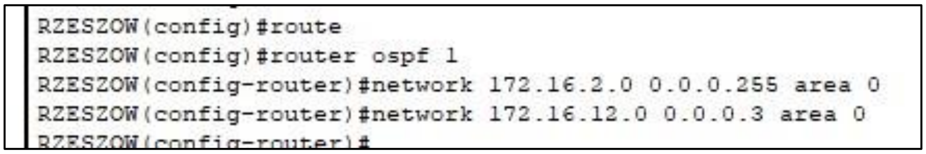


```
RZESZOW(config)#interface tunnel 0

RZESZOW(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

RZESZOW(config-if)#ip addres
RZESZOW(config-if)#ip address 172.16.12.2 255.255.255.252
RZESZOW(config-if)#tunne
RZESZOW(config-if)#tunnel so
RZESZOW(config-if)#tunnel source s0/0/1
RZESZOW(config-if)#tunnel des
RZESZOW(config-if)#tunnel destination 10.1.1.1
RZESZOW(config-if)#
```

2. OSPF Integration



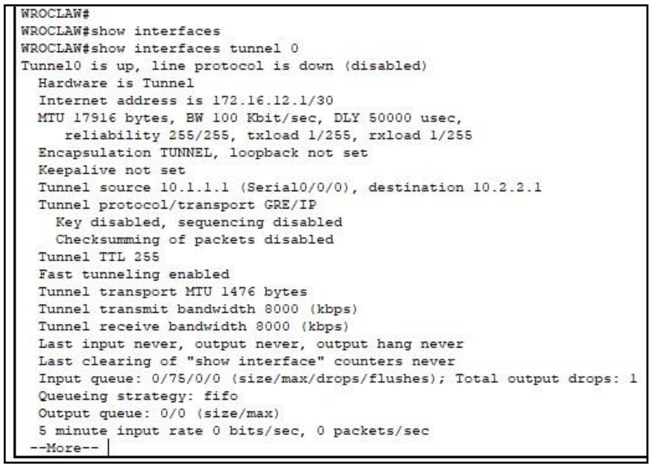
```
WROCLAW(config)#router ospf 1
WROCLAW(config-router)#network 172.16.1.0 0.0.0.255 area 0
WROCLAW(config-router)#network 172.16.12.0 0.0.0.3 area 0
WROCLAW(config-router)#
```



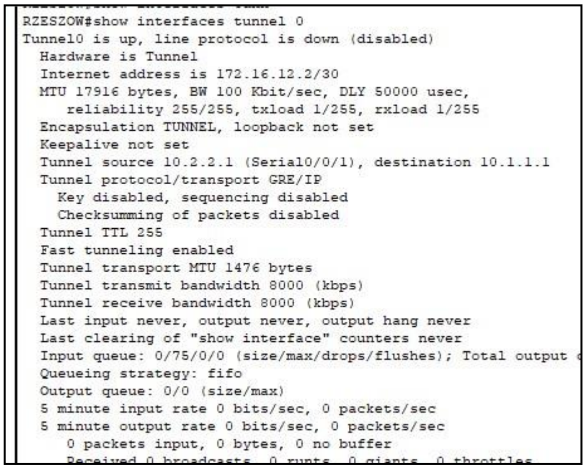
```
RZESZOW(config)#route
RZESZOW(config)#router ospf 1
RZESZOW(config-router)#network 172.16.2.0 0.0.0.255 area 0
RZESZOW(config-router)#network 172.16.12.0 0.0.0.3 area 0
RZESZOW(config-router)#
```

Verification Results

1. Tunnel Status Analysis



```
WROCLAW#
WROCLAW#show interfaces
WROCLAW#show interfaces tunnel 0
Tunnel0 is up, line protocol is down (disabled)
  Hardware is Tunnel
  Internet address is 172.16.12.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.1.1.1 (Serial0/0/0), destination 10.2.2.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
 --More--
```



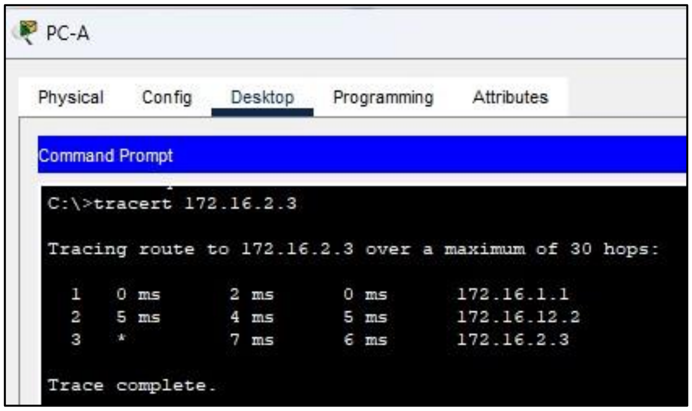
```
RZESZOW#show interfaces tunnel 0
Tunnel0 is up, line protocol is down (disabled)
  Hardware is Tunnel
  Internet address is 172.16.12.2/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.2.2.1 (Serial0/0/1), destination 10.1.1.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Execution of 'show interfaces tunnel 0' revealed:

- Protocol: GRE/IP
- MTU: 1476 bytes
- Bandwidth: 100 Kbit/sec
- Tunnel source (WROCLAW): 10.1.1.1
- Tunnel destination (WROCLAW): 10.2.2.1
- Tunnel source (RZESZOW): 10.2.2.1
- Tunnel destination (RZESZOW): 10.1.1.1
-

2. Route Verification

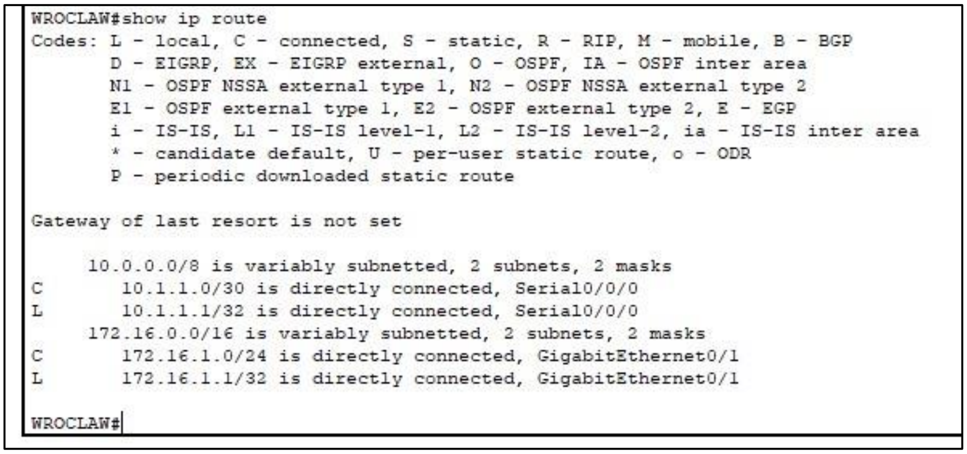
Traceroute results from PC-A to PC-C showed successful path:



```
C:\>tracert 172.16.2.3

Tracing route to 172.16.2.3 over a maximum of 30 hops:

  1   0 ms      2 ms      0 ms      172.16.1.1
  2   5 ms      4 ms      5 ms      172.16.12.2
  3   *         7 ms      6 ms      172.16.2.3

Trace complete.
```

- Path: PC-A → WROCLAW → GRE Tunnel → RZESZOW → PC-C
- All hops successfully traced
- Connectivity confirmed

3. OSPF Neighbor Verification



```
WROCLAW#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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/1
L       172.16.1.1/32 is directly connected, GigabitEthernet0/1

WROCLAW#
```

Router WROCLAW routing table showed:

- Direct connection: 172.16.1.0/24
- OSPF learned route: 172.16.2.0/24 via Tunnel0
- Next-hop address: 172.16.12.2

Conclusion

Successfully demonstrated:

1. GRE tunnel implementation
2. OSPF routing integration
3. End-to-end connectivity
4. Basic security configuration

Future Recommendations:

1. Implement IPSec for tunnel security
2. Add authentication mechanisms
3. Establish monitoring protocols
4. Develop backup tunnel configuration

This laboratory exercise effectively demonstrated practical implementation of enterprise networking concepts and security protocols, while identifying areas for security enhancement.