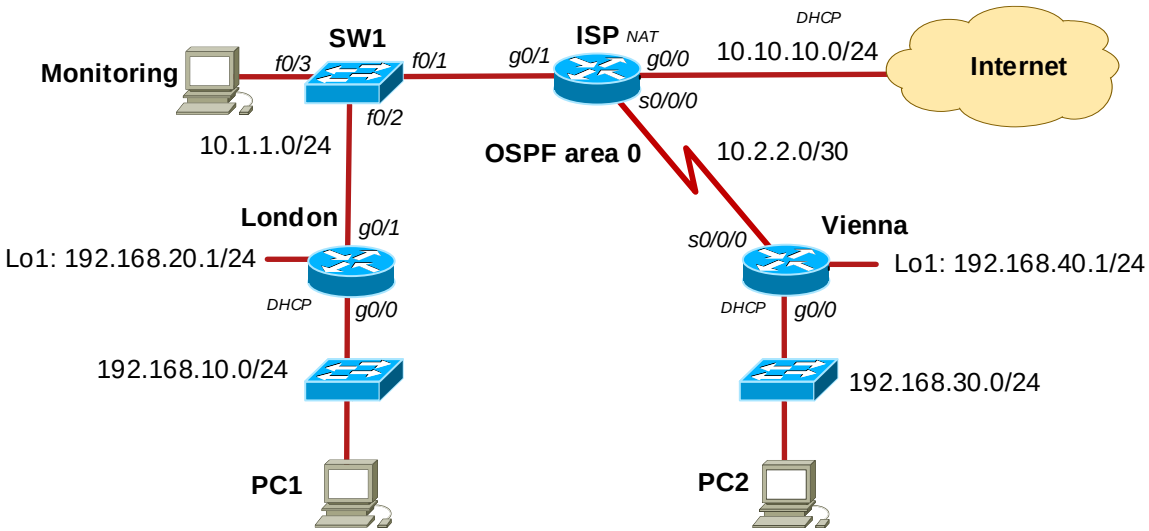
FACULTY OF INFORMATION TECHNOLOGY

CCNA R&S 4

Filtering Network Traffic 1/2



Scenario — Configure WAN Connection with ACL filtering.

Company ZeroX has two branches in London and Vienna. Management has established access policies which you must implement. You would not be allowed any administrative access to an ISP router as you can only control and manage London and Vienna routers.

Task 1 — Configuring Basic Device Settings.

1. Cable network topology..

2. Perform basic router configuration.

Configure the router hostnames to match the topology diagram. Disable DNS lookup.
Assign *cisco* as the privileged EXEC mode password.
Configure IP addresses on the routers. Ethernet link on ISP receives the address from the DHCP server.
Configure DHCP server on London and Vienna. Exclude the first 10 addresses. Use DNS address 10.10.10.1.
Configure NAT translation towards the Internet on ISP for all local networks (incl. loopbacks).

3. Enable web access on London and Vienna to simulate a web server with local authentication user *admin* with password *class.*

```
router(conf)# ip http server
router(conf)# ip http authentication local
router(conf)# username <user> privilege 15 secret <passwd>
```

4. Enable SSH on London and Vienna. Assign *cisco* as the console password.

```
router(conf)# ip domain-name [london.com/vienna.com]
router(conf)# crypto key generate rsa modulus 1024
router(conf-if)# line vty 0 4
router(conf-line)# login local
router(conf-line)# transport input ssh
```

5. Configure OSPF routing to exchange routing information about all networks. Do not send routing updates towards the Internet and the LANs.

6. Verify connectivity between devices and Internet. Test SSH connection. Test access to web servers.

Task 2 — Configure Traffic Filtering

Implement the following security policy for the network:

1. Allow web traffic originating from the 192.168.10.0/24 network to go to any network.
2. Allow an SSH connection to the Vienna serial interface from PC1.
3. Allow users on 192.168.10.0/24 network access to 192.168.20.0/24 network (any traffic). Other traffic from 192.168.10.0/24 will be blocked.
4. Network 192.168.30.0/24 is allowed to communicate with network 192.168.40.0/24 (all traffic) and with London via web communication only. No other traffic is allowed to originate from this network.

Implementation notes:

Configure one numbered extended ACL on London and one named extended ACL on Vienna only.
Place the ACLs as close to the source as possible.
Add a comment to each of the ACL to explain its function.

Hints:

```
router(conf)# access-list <num> remark <description>
router(conf)# access-list <num> permit/deny <proto> <source> <dest> [eq <port>]
router(conf-if)# ip access-group <num> in/out
router# show access-lists
router(conf)# ip access-list standard/extended <name>
router(conf-ext-nacl)# permit/deny <proto> <source> <dest> [eq <port>]
```

Task 3 — Verify ACLs.

1. Testing policies 1 – 2:

(i) Open up a web browser on PC1 and access any Internet web site.
(ii) Establish SSH connection from PC1 to Vienna.
(iii) From PC1 command prompt, issue a ping to Vienna.
(iv) Check the result on London
router(conf]# show access-lists

2. Testing policy 3:

(i) From PC1 command prompt, issue a ping to Lo0 on London.

3. Testing policy 4:

(i) Open up a web browser on PC2 and access any web site on the Internet.
(ii) From PC2, open a web session to London.
(iii) From PC2, open a web connection to 192.168.40.1.
(iv) From PC2, ping PC1.

Task 4 — Modify ACLs.

Management has decided to allow DNS resolution and ICMP communication for all local networks. Modify the existing ACLs so that ICMP and DNS communication can be transferred.

Verify the settings.

(i) From PC1, ping to PC2.
(ii) From PC1, ping to Vienna.
(iii) From PC2, ping to PC1.
(iv) From PC2, ping to London.

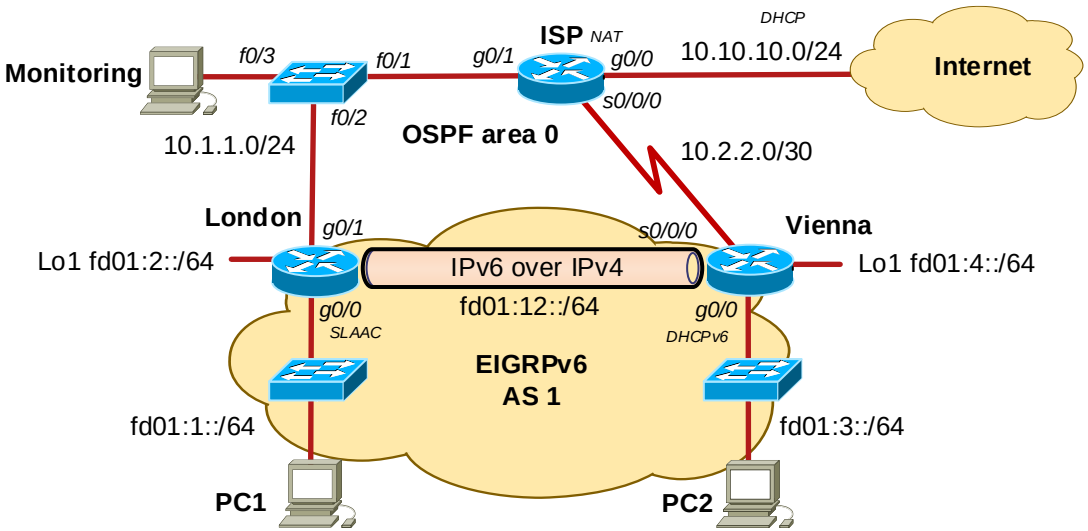
Task 5 — Configure SPAN port on SW1

Configure port mirroring on SW1 using SPAN port. Data from f0/1 will be sent to f0/3.

```
SW1(conf)# monitoring session 1 source interface f0/1 both
SW1(conf)# monitoring session 1 destination interface f0/3
```

FACULTY OF INFORMATION TECHNOLOGY

CCNA R&S 4 — Filtering Network Traffic 2/2



Scenario — Establishing IPv6 Between Remote Branches.

Local networks at London and Vienna needs to communicate via IPv6. Configure dual-stack IPv6 addressing on London and Vienna. Create an IPv6 over IPv4 tunnel to connect both sides via ISP IPv4 network. Implement network security using IPv6 ACL lists.

Task 6 — Configure IPv6 Addressing on the Routers.

1. Enable IPv6 routing.
router(conf)# ipv6 unicast-routing
2. Configure static IPv6 addresses on loopbacks. Use unique local addresses from fd00::/8.
router(conf)# interface *lo1*
router(conf-if)# ipv6 address <*IPv6-address*> / <*prefix*> ; configure unique local address
router(conf-if)# no shutdown
3. Configure IPv6 address and SLAAC on London.
router(conf)# interface *g0/0*
router(conf-if)# ipv6 address <*IPv6-address*> / <*prefix*> ; configure unique local address
router(conf-if)# ipv6 address *fe80::1 link-local* ; configure link local address
router(conf-if)# no shutdown
4. Configure IPv6 address and stateless DHCPv6 server on Vienna.
router(conf)# ipv6 dhcp pool <*name*> ; define DHCPv6 pool
router(conf-dhcpv6)# domain-name *vienna.com*
router(conf)# interface *g0/0*
router(conf-if)# ipv6 address <*IPv6-address*> / <*prefix*> ; configure unique local address
router(conf-if)# ipv6 address *fe80::1 link-local* ; configure link local address
router(conf-if)# ipv6 nd other-config-flag ; define stateless DHCPv6 server
router(conf-if)# ipv6 dhcp server <*name*> ; assign the DHCPv6 pool to the interface
router(conf-if)# no shutdown
5. Verify settings.
router# show ipv6 interface brief
Ping from PC to fe80::1 and between PC1 and PC2.

Task 7 — Configure IPv6 over IPv4 Tunnel.

1. Configure the tunnel interface on the London and the Vienna routers.
router(conf)# interface tunnel 1
router(conf-if)# ipv6 address <*tunnel-IPv6-address*> / <prefix>
router(conf-if)# tunnel source <*interface*>
router(conf-if)# tunnel destination <*remote-IPv4-address*>
router(conf-if)# tunnel mode ipv6ip
2. Verify the connection.
router# show ipv6 interface brief
router# show interface tunnel 1
router# ping <*IPv6-address*>

Task 8 — Configure EIGRPv6 Routing with AS 1.

1. Configure EIGRPv6 process. Do not set routing updates on LAN and loopback interfaces.
router(conf)# ipv6 router eigrp <*AS-number*>
router(conf-rtr)# eigrp router-id <*IPv4-loopback-address*>
router(conf-rtr)# passive-interface <*interface*>
router(conf-rtr)# no shutdown
2. Enable EIGRPv6 on the interfaces.
router(conf-if)# ipv6 eigrp <*AS-number*>
3. Verify routing.
router# show ipv6 route
router# show ipv6 eigrp neighbors
router# show ipv6 protocols
4. Test IPv6 end-to-end connection between PC1 and PC2.

Task 9 — Configure IPv6 Traffic Filtering.

On London, restrict access to VTY. Create an ACL to allow only hosts from fd01:1::/64 to telnet to London via IPv6. Other hosts should access London using SSH only.
1. Create an ACL
router(conf)# ipv6 access-list <*name*>
router(conf-ipv6-acl)# permit <proto> <ipv6-source> <ipv6-dest> [eq <port>]
... ; format: host <ipv6-address> or <ipv6-address>/<prefix>
2. Apply the rule on VTY.
router(conf)# line vty 0 4
router(conf-line)# ipv6 access-class <*name*> in
3. Verify ACL using telnet and ssh access from different hosts. Allow Telnet on VTY.
router# show ipv6 access-list <name>

On Vienna, configure an ACL that will drop all the traffic originating from fd01:3::/64 except web traffic and ICMPv6.
1. Create an ACL
router(conf)# ipv6 access-list <*name*>
router(conf-ipv6-acl)# permit <proto> <ipv6-source> <ipv6-dest> [eq <port>]
...
2. Apply the rule on the interface
router(conf)# interface <*interface*>
router(conf-if)# ipv6 traffic-filter <*name*> <*in/out*>
3. Verify the ACL using web connection and ping. Why ping to www.seznam.cz does not work?

Task 10 — Finish the lab, remove cables, switch off PCs.