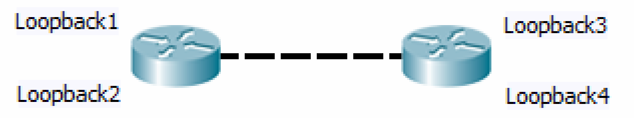
COMPUTER NETWORKS - LABORATORY 071

Subject:

Cisco routers. IGP (Interior) dynamic routing - OSPF.
Redistribution between IGP protocols.
GRE tunneling.

Task A: Dynamic Routing - OSPF

1. Prepare two Cisco routers and connect them as shown below. Connections between routers should be performed using Ethernet or serial interfaces. You should also define some loopback interfaces on routers for testing purposes.

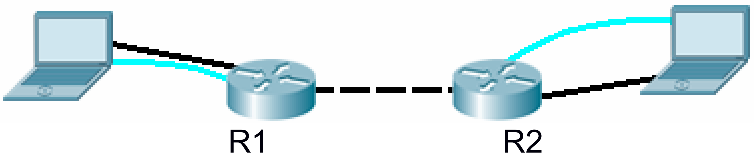


Note: All IP addressing for loopback interfaces defined (in the whole system) must be unique and can not cover addressing of another network.

In the extended version of the system can be connected to additional router interfaces and PC stations - but for the purpose of diagnostics (ping) it will be sufficient to replace them with loopback interfaces. Then it becomes a useful call to ping the Cisco IOS in such a way that the sender of the ICMP Echo Request (IP source address in an ICMP Echo Request) will be a loopback interface, and not the physical interface through which the router sends the ICMP request. The command will be as follows:

Router#ping 200.200.200.1 source 100.100.100.1

where 100.100.100.1 is the loopback interface IP address, and the destination host IP address is 200.200.200.1. Of course, calling this command is meaningful only when you set up dynamic routing processes first, which will be carried out in the following paragraphs.

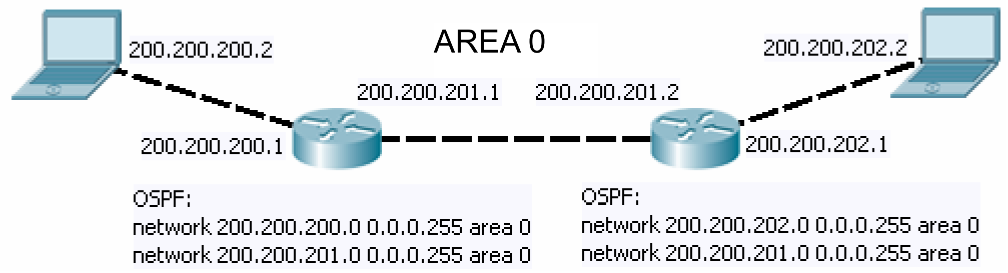


Configure and enable the appropriate interfaces in IP routers - defining different IP networks directly connected to the router (and thus addressing interface IP routers) - in accordance with generally known principles.

2. Starting the OSPF routing in a single area:

Router (config)#router ospf 150

where 150 is OSPF process identifier (1..65536)


AREA 0
200.200.200.2
200.200.202.2
200.200.201.1
200.200.201.2
200.200.200.1
200.200.202.1
OSPF:
network 200.200.200.0 0.0.0.255 area 0
network 200.200.201.0 0.0.0.255 area 0
OSPF:
network 200.200.202.0 0.0.0.255 area 0
network 200.200.201.0 0.0.0.255 area 0

Register directly connected networks, assigned to the OSPF domain:
Router (config-router)#network 200.200.200.0 0.0.0.255 area 0
Router (config-router)#network 200.200.201.0 0.0.0.255 area 0
Note !: The mask is stored in bit inversion.
Check the status of OSPF process:
Router#show ip protocols
Router#show ip interface brief
Router#show ip ospf interface fa 0/0
For NBMA network - Non Broadcast Multiple Access (for example, when emerging cloud frame-relay network) routers also must explicitly register their OSPF neighbors (providing IP addresses to other OSPF routers in the network), np.:
Router(config-router)#neighbor 200.200.100.1
Router(config-router)#neighbor 200.200.200.1
Note! In case of frame-relay network you must configure a set of connections between routers (full-mesh peers). Otherwise some OSPF neighbors will have no communication with each other.

After negotiation delay check routing protocol functioning (ping, traceroute)
Check the diagnostics commands for OSPF:
Router#sh ip ospf interface fa 0 / 0
Router#sh ip ospf neighbor
Verify status of OSPF neighbor each time, identifying selected operating modes (roles) in the OSPF infrastructure - as Designated Router (DR), Backup Designated Router (BDR) or DROTHER (router other than the DR or BDR).
You can try forcing a displacement of DR to another router, increasing the OSPF interface priority (default value is 1, the higher is better, when several OSPF routers have the same priority - the highest value of the OSPF Router ID is used):
Router (conf)#int fa 0/0
Router (config-int)#ip ospf priority 0
Router#show ip ospf interface
Note: In point-to-point or point-to-multipoint network DRs and BDRs are not present (there is no sense in defining it). This situation is indicated by the symbol "-" describing an operation mode of OSPF neighbor in the report.
DRs and BDRs are defined for each IP network (the network segments between routers OSPF) - not for the area (so that one area can have multiple DRs and BDRs).
Hello packets are sent in OSPF all the time. The default interval between hello packets is 10 seconds for the broadcast or point-to-point network and 30 seconds for non-broadcast or point-to-multipoint. Dead-times for these types of networks (time to expire the connection after the neighbor was closed) are respectively 40 and 120 seconds (dead-time is four times longer than the interval for hello)

You can change the hello interval value but it must be consistent for the entire OSPF area, eg .:

```
Router (config-if)#ip ospf hello-interval 15
Router#debug ip ospf adjacency
```

For any link (leading to another router) its cost can be adjusted (the default is 100,000,000 / bandwidth):

```
Router (config)#interface fa 0/0
Router (config-if)#ip ospf cost 35
```

The cost is calculated for the link "entering the router."

General OSPF diagnostics and debugging commands:

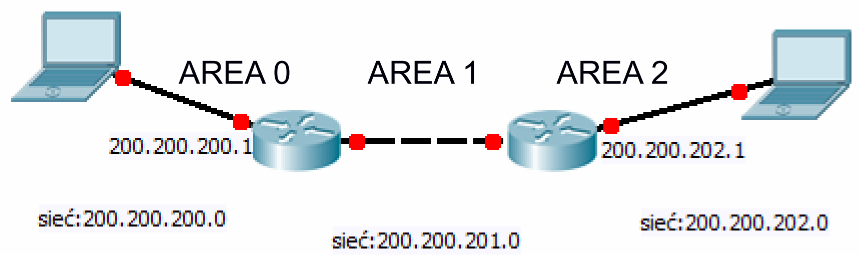
```
Router#debug ip ospf events
Router#show ip route
Router#show ip ospf interface
```

3. The segmentation procedure of OSPF infrastructure works as follows: internal routers are installed within the "area". ABR routers (Area Border Router) are connecting areas, so they have interfaces assigned to different areas in OSPF domain.
   Note: for each domain there must be OSPF area 0 (ie. Backbone area). Other areas can be designated freely. Within the OSPF domain router can have different area identifiers assigned to its various interfaces - this is the ABR. When all area identifiers assigned to OSPF interfaces are in a router are the same – we're dealing with internal router (internal OSPF router).

   The logical OSPF topology requires all areas to have direct contact to the backbone area. However, when the area does not have a direct link to the backbone - it is possible to unblock communication by creating the so-called. Virtual OSPF links. For example, if we have a system: area0 - ABR1 - area1 - ABR2 - area2 you need to create a virtual link between ABR1 and ABR2 routers. Virtual Link will run through area1 to the backbone (area0).

   Rebuild OSPF areas segmentation so it will be compatible with the figure below

Virtual link



Virtual link configuration:

```
RuterABR1 (config)#router ospf 150
RuterABR1 (config-router)#area 1 virtual-link 5.5.5.5
RuterABR2 (config)#router ospf 150
RuterABR2 (config-router)#area 1 virtual-link 6.6.6.6
```

where 5.5.5.5 and 6.6.6.6 are opposite router IDs of the ABR OSPF routers.

Attention! 5.5.5.5 and 6.6.6.6 are not IP addresses, but the so-called – OSPF router IDs. Here, respectively - routers R1 and R2 have IDs generated by the OSPF process (could look the same as IP addresses). The value of the router ID in an OSPF domain must be unique and is usually picked as a copy of the IP address of physical OSPF with the highest numerical value. The value you need to check the router ID command:

```
Router#sh ip ospf interface
```

Naturally, any declaration of virtual-link must point at the opposite end of the connection.

Create an OSPF virtual link between the selected ABRs. And check the configuration of virtual links:

```
RuterABR1#show ip ospf virtual-links
```

To create a new OSPF area it is enough to add define any interface with a new unique area ID - even a loopback interface:

```
Router (config)#int loopback 5
Router (config-if)#ip addr 200.200.101.1 255.255.255.0
Router (config-if)#exit
Router (config)#router ospf 150
Router (config-router)#network 200.200.101.0 0.0.0.255 area 6
```

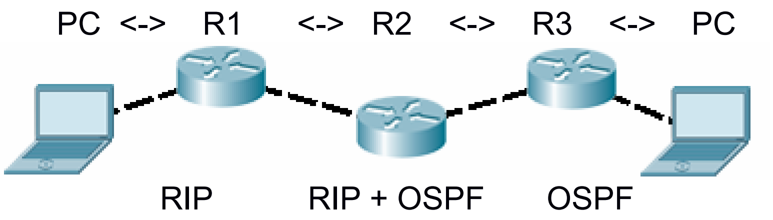
Final checks:

```
Router (config)#show ip ospf border routers
Router (config)#show ospf virtual-IP links
```

Task C: Redistribution of routes between IGP protocols

1. In case of several routing protocols working at the same time it is possible to use the mechanism of redistribution of routes between them. Redistribution allows to migrate an information about routes into another routing system. The current task will be to redistribute between IGP protocols. It is also possible to redistribute outside, with (EGP).

2. Built a system consisting of three routers (R1, R2, R3) and two PC computers (or loopback interfaces in router):



3. All interfaces should also be configured with proper IP in addressing, in accordance with general rules.
4. Router R2 will support two routing protocols at the same time (in the exercise RIP + OSPF). Router R1 - only RIP. Router R3 - only OSPF. The aim will be to force

router R2 to redistribute between these two protocols.

5. Turn on the appropriate dynamic routing protocol on routers.

6. After completing the installation check the contents of all routing tables - routers R1 and R3 should have information only on routes that are within the range of routing protocols (OSPF and RIP respectively). To extend that knowledge, router R2 will be involved in the redistribution process between RIP and OSPF routing protocols.

7. Configuring the redistribution from OSPF into RIP:
R2 (config)#router ospf 150
R2 (config-router)#redistribute rip metric 170 subnets
After entering the command, check whether the router R3 gain the routes from RIP (will be indicated with O E1 - External OSPF marking)
R1#show ip route
These routes will also get a new metrics value of 170.

8. Configuring the redistribution from RIP into OSPF:
R2 (config)#router rip
R2 (config-router)#redistribute ospf 4 metric 11
where 4 is the ID of the OSPF process.
After entering the command, verify if the router R1 reached route information from OSPF. It should be marked with the symbol 'R':
R1#show ip route
Metric value for the RIP must be reduced (as it's just a hops count to destination with max of 15).

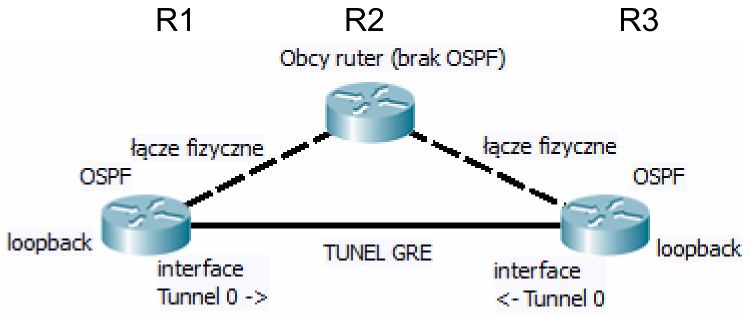
   Comments:
   - Redistribution of RIP to OSPF requires keyword of 'subnets' in command. Otherwise, router will propagate only classfull networks
   - RIP option 1 does not support VLSM routing protocol (it is classfull only)
   - In case of redistribution from another protocol to RIP a metric conversion is required - RIP routes are hop counts, not cost points.

9. Remove an OSPF from routers and place EIGRP instead. Try to redistribute with EIGRP involved.

Task D: GRE tunnels - remote connections over multi segment IP networks

When it's necessary to create a coherent system of distributed dynamic IP routing (for example, deployed in a number of buildings connected by the Internet) it is possible to use IP tunneling. GRE (General Routing Encapsulation) tunnels are implemented using special virtual interfaces (called the Tunnel) to provide the functionality of the ISO OSI layer 3 communication between remote IP networks. That tunnel can be established between two or more Cisco routers.

1. Build a system involving three routers connected as shown below. Routers R1 and R3 will be involved in the tunneling system. Router R2 will not (it simulates an area of the Internet). Routers R1 and R3 will contain logical interfaces of Tunnel (GRE tunnel endpoints).

   Note: The link marked in the drawing as a GRE tunnel is not a physical link (the cable will not be set between routers)

2. Configure addressable physical interfaces in routers R1, R2, R3, in accordance with the general principles e.g.:

   ```
   R1 (config)#interface FastEthernet0 / 0
   R1 (config-if)#ip address 200.200.200.1 255.255.255.0
   R2 (config)#interface FastEthernet0 / 0
   R2 (config-if)#ip address 200.200.200.2 255.255.255.0
   R2 (config)#interface FastEthernet0 / 1
   R2 (config-if)#ip address 200.200.201.2 255.255.255.0
   R3 (config)#interface FastEthernet0 / 0
   R3 (config-if)#ip address 200.200.201.1 255.255.255.0
   ```

3. In routers R1 and R3 enter the routing mechanism that enables communication between 200.200.200.1 and 200.200.201.1 (simulated Internet over which a GRE tunnel will be established):

   ```
   R1(config)#ip route 200.200.201.0  255.255.255.0 200.200.200.2
   R3(config)#ip route 200.200.200.0 255.255.255.0 200.200.201.2
   ```

4. In routers R1 and R3 define a GRE tunnel (paying attention to the correct addresses defined on opposite endpoints of the tunnel):

   ```
   R1 (config)#interface Tunnel 0
   R1 (config-if)#tunnel source FastEthernet0/0
   R1 (config-if)#ip address 192.168.5.1 255.255.255.0
   R1 (config-if)#tunnel destination 200.200.201.1
   R3 (config)#interface Tunnel 0
   R3 (config-if#tunnel source FastEthernet0 / 0
   R3 (config-if)#ip address 192.168.5.2 255.255.255.0
   R3 (config-if)#tunnel destination 200.200.200.1
   ```

   Check the GRE tunnel operation:

   ```
   R1#ping 192.168.5.2
   R1#show interfaces tunnel 0
   ```

   Received report will identify IP addresses of local and remote endpoints of the tunnel and datagram counts sent through the tunnel.

5. The routers R1 and R3 define the loopback interface (simulating an existence of a local networks connected thru a tunnel), e.g.:

   ```
   R1 (config)#interface Loopback 0
   R1 (config-if)#ip address 192.168.0.1 255.255.255.0
   R3 (config)#interface Loopback 0
   R3 (config-if)#ip address 192.168.1.1 255.255.255.0
   ```

6. Start a dynamic routing system in routers R1 and R3 on loopback and tunnel networks (for example: OSPF):

   ```
   R1 (config)#router ospf 1
   R1 (config-router)#network 192.168.0.0 0.0.0.255 area 0
   R1 (config-router)#network 192.168.5.0 0.0.0.255 area 0

   R3 (config)#router ospf 1
   R3 (config-router)#network 192.168.1.0 0.0.0.255 area 0
   R3 (config-router)#network 192.168.5.0 0.0.0.255 area 0
   ```

   You can also start OSPF diagnostics with:

   ```
   R1 (config-router)#log-adjacency-changes
   ```

7. Check (ping, traceroute, ospf show ip route, show ip ospf neighbors) routing operation in the system.

8. In order to maintain the transmission tunnel fragmentation properly it is necessary to change parameters of MTU (Maximum Transmition Unit) for TCP protocol transmissions used in the tunnel (tunneling generates an extra header in packets, so maximum payload length is lower), e.g.:

   ```
   R1 (config)#interface Tunnel 0
   R1 (config-if)#ip MTU 1460
   R1 (config-if)#ip adjust tcp-mss 1430
   R3 (config)#interface Tunnel 0
   R3 (config-if)#ip MTU 1460
   R3 (config-if)#ip adjust tcp-mss 1430
   ```

   where mss is the maximum segment size.

   Warning: The above values must be set identically on both sides of the tunnel.