



UNI tasks

MagicWorks Inc. is the market leading recycling company in Hungary. The headquarters of the company is located in **Budapest** and the data center in **Pecs**. Currently, there is an expansion going on that will result in a new site in **Debrecen**. The network infrastructure has already been planned, designed and the equipment deployed, your job is to configure all the devices in order to make them work properly and interoperate with the existing network.

Below you will find a summary of the network requirements of the new site.

Note: Only the interfaces explicitly marked in the topology are to be used (e.g. executing commands on) or referred to, all the other interfaces should remain unused. Each serial interface should use **PPP** encapsulation and **/30** subnets. Pay attention to setting the clockrate on the DCE sides!

Basic router tasks

1. Each router is to be named according to the topology and has to be secured with the password **cisco**. The passwords stored in the startup configuration file must be encrypted with **MD5**.
2. Ensure that username **student** with password **cisco** will be used for login to the console and all VTY lines of the routers. The passwords stored in the startup configuration file must be encrypted with **MD5**.
3. Enable protocol **PPP** and set the clock rate to **128kbps** on each serial link connecting the routers.
4. **Disable DNS lookup** on each network device in the case of mistyped commands.
5. Set the IP addresses according to the diagram. Verify link connectivity by executing pings. Set the loopback addresses (use **Loopback 1**) as following: 192.168.1.Y/32 , where Y=1 in case of Budapest, Y=2 in case of Pecs, Y=3 in case of Debrecen). (e.g. the Budapest router's loopback address will be 192.168.1.1/32)
6. **Enable CLI synchronization** (to separate CLI commands from router messages) on VTY lines and on the console port.

Basic LAN tasks

1. Each switch is to be named according to the topology and has to be secured with the password **cisco**. The passwords stored in the startup configuration file must be encrypted with **MD5**.
2. **Disable DNS lookup** on each network device in the case of mistyped commands.



3. **Enable CLI synchronization** (to separate CLI commands from switch messages) on VTY lines and on the console port.

VTP

Each switch should be set to belong to the VTP domain **Hungary**. Switch S1 should be the server, the others are the clients.

VLAN

1. Create the following VLANs and name them accordingly.

VLAN number	VLAN name
2	2ndVLAN
3	3rdVLAN
10	Management
20	Dumb

2. The **Fa 0/1** interfaces on both switches – **S2 and S3** – should be set to the corresponding VLAN memberships (VLAN 2 – S2's Fa 0/1 and VLAN3 – S3's Fa 0/1).
3. Create **subinterfaces** of the **Fa0/0** interface on router **Debrecen**. For subinterface ID use the VLAN's number. The form of the addresses should be **10.10.x.0 /24**, where **x=VLAN number** (No need to create subinterface for VLAN 20!). The router should always have the **10.10.x.1** address (which will be the default gateway for that subnet).
4. Switches should get their IP addresses from **VLAN 10** (which is the **Management** VLAN). The IP addresses should end in the following way: **S1 – 10, S2 – 20, S3 – 30**.

Security

1. **Disable the trunking** autonegotiation protocol on every switch and interface.
2. Each **unused port** on the switches (except Fa 0/1 – 0/3) should be assigned to **VLAN 20** and be **disabled** after that.
3. Switches should be reachable from anywhere by using protocol Telnet. Ensure that username **student** with password **cisco** will be used for login to all VTY lines of the switches. The passwords stored in the startup configuration file **should not be** encrypted with **MD5**, but the real passwords must be **hidden** in the running-config.

Internet

On router **Budapest** set the link towards the Internet. Use the **195.228.1.2/30** IP address and the **appropriate encapsulation**. Set the default route using the **next-hop IP address**.



OSPF

1. Activate and configure the routing protocol **OSPF** to use **two different areas** for the entire topology. The backbone area starts with the interface **S0/0/0** of router **Budapest** towards router **Pecs** including the internal subnet of router **Pecs**, while **any other subnet** should be in **Area 1**. Each internal subnet (therefore excluding the Internet links) should be reachable from anywhere with their proper mask information. When the OSPF networks are defined, **the IP addresses of the interfaces should be used as "networks"**.
2. Secure the OSPF updates! The updates **should not use a plain-text authentication!** The key should be **md5pass**, the **key ID should be "1"**, and set up link by link!
3. Set Set router **Budapest to advertise the default route**.
4. The routing protocol OSPF should be set to **use the actual transmission speed** of the serial interfaces (metric calculation).

Other

Set up the **dynamic management** of the IP address allocation on router **Debrecen**. The **10.10.2.0 /24** subnet should be used, but the last octet of the **IP addresses should be limited to the interval 100-200**. Default gateway: **10.10.2.1**. The pool name should be **NAG2010!**

NAT

Hide all your inside IP addresses from the rest of the world, use Network Address Translation on router **Budapest!** **One public IP address should be used** by all the inside local addresses to communicate with the Internet. Use **access-list 1** to permit all the **10.0.0.0 /8** subnets to be translated. Verify the proper operation of the address translation by pinging the router **ISP** from inside.

IPV6

1. Set the **2002:1:2:3:4:5:6:2 /64** IPv6 address on the **S 0/1/0** interface of **Budapest**.
2. On router **Budapest** set a **host IPv6 address** for the **loopback 1** interface. The IPv6 address should start with the starting date of NAG 2010: **year-month-day-10-00** and the **end should be 1**. **Do not use any hexadecimal numbers** for the missing parts of the address.

SECURITY

Apply a security policy on router **Pecs** to **deny telnet** connections originating from the LAN subnets of router **Debrecen** (except VLAN 10) to router **Pecs itself**. However, telnet traffic with any other (behind router Pecs) should be allowed. Any other kind of traffic is permitted. **Use a named rule** for this policy, where the name should be **TELNET**.