# Application

This task is for beginners in cisco packet tracer. The task is to set up a simple network consisting of 3 branches. The task already describes a work plan for configuring the network. You will find the working network in the work\_network directory, and the configuration of all network equipment will also be there. The task in English is called readme\_eng, and the tasks in Russian are called readme\_ru. All network configuration is in the conf\_net.

## !!! Attention!!!

The network is fully configured. In addition to point 1 (Basic Configuration), the network equipment is also named. The base settings will be Basic\_settings. You need to copy the contents of the file and in configuration mode paste and press Enter. After that, the network will be finally configured.

The task consists of three independent modules, which participants complete sequentially on competition days C1, C2 and C3. Each module is evaluated on the day of its implementation. Verification using automated verification tools is allowed.

The contest task is classified. The task for each module will be issued to participants on the day of its completion.

## **Task modules and required time**

Table 1.

| **Module name** | | **Competition Day (C1, C2, C3)** | **Time for task** |
| --- | --- | --- | --- |
| **A** | **Module A: "Information infrastructure commissioning"** | **C1** | **4 hours** |
| **B** | **Module B: "Troubleshooting"** | **C2** | **4 h** |
| **C** | **Module C: "Network infrastructure deployment and maintenance"** | **C3** | **4 hours** |

*Module C: Deployment and maintenance of network infrastructure.*

## **Task**

**1) Basic setup**

1.1 Specify the name of all devices according to the topology.

1.2 Assign the domain name junior14. wsr to all devices

1.3 Configure the mode where all passwords in the configuration are stored in encrypted form.

1.4 Create jun14 users on all devices with the password P@ssw0rd

a) The user's password must be stored in the configuration as the result of a hash function.

b) The user must have the maximum privilege level

On all devices, set the wsr password to enter privileged mode.

c) The password must NOT be stored in the configuration as the result of a hash function.

1.5 On devices that are allowed access, in accordance with Table 1, assign IP addresses to interfaces, subinterfaces, and VTI interfaces. Where necessary, assign a default gateway and route.

1.6 All devices must be accessible for management only via SSH version 2.

1.7 When connecting via the console, the device must request a user account.

**2) Configuring services**

2.1 Configure the dynamic host configuration protocol with the following characteristics:

2.1.1 On the R1 router:

a) Pool name-CLIENTS

b) Network address-from the corresponding subnet

c) The DNS server address is 8.8.8.8.

d) Prohibit issuing addresses from .1 to .100 from the corresponding subnet.

e) Clients must receive IP addresses via DHCP.

2.1.2 On the R3 router:

a) The pool name is LAN10, LAN20, LAN30, and LAN40, respectively.

b) Network address-from the corresponding subnet

c) The DNS server address is 8.8.8.8.

d) Prohibit issuing addresses from .1 to .100 from the corresponding subnet.

e) Clients must receive IP addresses via DHCP.

2.1.3 On the R4 router:

a) a DHCP relay for the appropriate subnet

b) Clients must receive IP addresses via DHCP.

2.1.4 On the SW1 switch:

a) The pool name is LAN110 and LAN120, respectively.

b) Network address-from the corresponding subnet

c) The DNS server address is 8.8.8.8.

d) Prohibit issuing addresses from .1 to .100 from the corresponding subnet.

e) Clients must receive IP addresses via DHCP.

2.1.5 On router R1, R2, R3, configure PAT for all your local networks.

a) vlan30 and vlan40 clients must use PAT configured on R3

b) There should be no PAT setting on the R4 router.

c) Use a named standard access list named NAT.

**3) Configure routing.**

3.1 Configure OSPF between R3 and R4 routers.

a) Use process number 1 and area 0.

b) Include all necessary networks in the routing updates.

c) All interfaces must be in passive mode by default. Disable passive mode for the interface only in the direction of R3 and R4, respectively.

d) The default route from the R3 router must be distributed over OSPF.

3.2 Configure EIGRP between Router R2 and Switch SW1.

a) Use the autonomous system number 2021.

b) Include all necessary networks in the routing updates.

c) All interfaces must be in passive mode by default. Disable passive mode for the interface only towards R2 and SW1, respectively.

d) Disable route summation

e) The default route from the R2 router must be propagated via EIGRP.

3.3 On routers R1, R2, and R3, configure static routing to all internal networks via the appropriate tunnel interfaces.

a) Configure the reallocation of static routes to the appropriate dynamic routing protocol.

**4) Setting up a wireless network**

4.1 Configure a wireless network on the R1 router:

a) Wireless Network Name – SSID) - WIFI

b) We allow you to broadcast our network

c) Use WPA authentication

d) Use WPA-PSK with the passphrase ciscocisco

e) Use the dot11Radio 0 interface

f) Use AES-ccm encryption

**5) Switching setup**

5.1 On SW1, SW2, and SW3 switches, the VLAN table must contain:

a) VLAN100 named LAN100

b) VLAN110 named LAN110

c) VLAN120 named LAN120

5.2 On the SW4 switch and R3 router, the VLAN table should contain:

a) VLAN10 named LAN10

b) VLAN20 named LAN20

5.3 On the SW5 switch, the VLAN table should contain:

a) VLAN30 named LAN30

b) VLAN40 named LAN40

5.4 Configure the Trunks:

a) Between SW1, SW2 and SW3. Only VLANs 100, 110, and 120 should be allowed.

b) Between R3 and SW4. Only VLANs 10, 20 should be allowed.

c) Between R4 and SW5. Only VLANs 30, 40 should be allowed.

d) Use the non-dynamic matching mode for all trunks. Disable DTP explicitly.

5.5 On all R1 and R3 switches and routers, enable Rapid-PVST+

5.6 The SW1 switch must be the root of the spanning tree in VLANs 100, 110, and 120. If SW1 fails, the SW2 switch must be the root.

5.7 Switch ports to which computers are connected must be configured in access mode.

a) Switch SW2: fa0 / 1 – VLAN110; fa0 / 2-vlan120

b) Switch SW3: fa0 / 1 – vlan120; fa0 / 2-vlan110

c) Switch SW4: fa0 / 1 – VLAN10; fa0 / 2 and FA0 / 3 – vlan20

d) Switch SW5: fa0 / 1 – VLAN30; fa0 / 2-vlan40

6) Configuration of private virtual networks

6.1 Set up a GRE tunnel between R1 and R2:

a) Use the Tunnel1 interface as the VTI

b) Use addressing according to the addressing table

6.2 Set up a GRE tunnel between R2 and R3:

a) Use the Tunnel2 interface as the VTI

b) Use addressing according to the addressing table

6.3 Set up a GRE tunnel between R1 and R3:

a) Use the Tunnel3 interface as the VTI

b) Use addressing according to the addressing table

### Addressing table

| Device | Interface | Адрес IPv4/ Маска |
| --- | --- | --- |
| ISP | gig0/0 | 1.1.1.1/30 |
| gig0/0/0 | 2.2.2.1/30 |
| gig0/1/0 | 3.3.3.1/30 |
| R1 | gig0 | 1.1.1.2/30 |
| vlan1 | 192.168.1.1/24 |
| wlan-ap0 | 192.168.1.1/24 |
| tun1 | 10.0.1.1/30 |
| tun3 | 10.0.3.2/30 |
| R2 | gig0/0/0 | 2.2.2.2/30 |
| gig0/0 | 10.10.10.5/30 |
| tun1 | 10.0.1.2/30 |
| tun2 | 10.0.2.1/30 |
| R3 | gig0/1/0 | 3.3.3.2/30 |
| gig0/0 | 10.10.10.1/30 |
| vlan10 | 192.168.10.1/24 |
| vlan20 | 192.168.20.1/24 |
| tun2 | 10.0.2.2/30 |
| tun3 | 10.0.3.1/30 |
| R4 | gig0/0 | 10.10.10.2/30 |
| gig0/1.30 | 192.168.30.1/24 |
| gig0/1.40 | 192.168.40.1/24 |
| SW1 | gig1/0/1 | 10.10.10.6/30 |
| vlan100 | 192.168.100.1/24 |
| vlan110 | 192.168.110.1/24 |
| vlan120 | 192.168.120.1/24 |
| SW2 | vlan100 | 192.168.100.2/24 |
| SW3 | vlan100 | 192.168.100.3/24 |
| SW4 | vlan10 | 192.168.10.2/24 |
| SW5 | vlan30 | 192.168.30.2/24 |
| PC0 | Fa0 | DHCP |
| PC1 | Fa0 | DHCP |
| PC2 | Fa0 | DHCP |
| PC3 | Fa0 | DHCP |
| PC4 | Fa0 | DHCP |
| PC5 | Fa0 | DHCP |
| PC6 | Fa0 | DHCP |
| PC7 | Fa0 | DHCP |
| PC8 | Fa0 | DHCP |
| PC9 | Fa0 | DHCP |
| PC10 | Fa0 | DHCP |
| PC11 | Fa0 | DHCP |
| PC12 | Fa0 | DHCP |
| PC13 | Fa0 | DHCP |

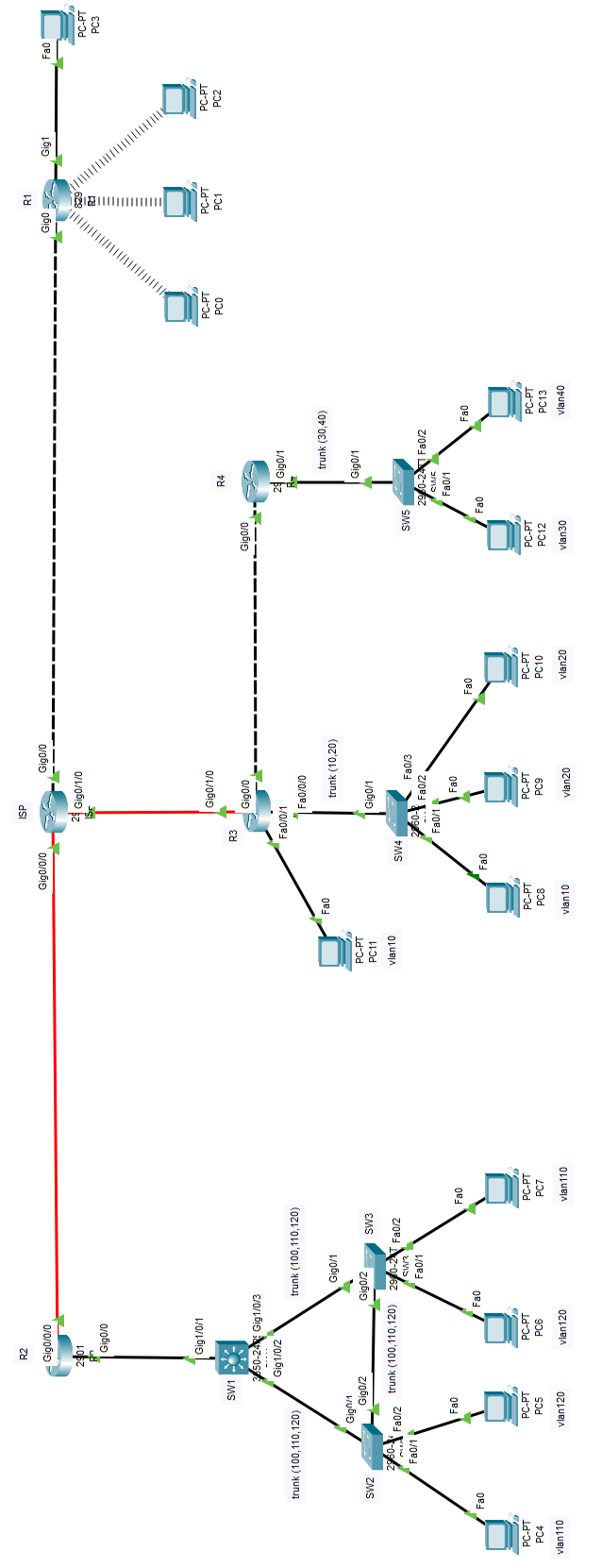


Figure – Network diagram

## **Evaluation criteria.**

Table 2.

| **Criterion** | | **Points** | | |
| --- | --- | --- | --- | --- |
| **Judicial aspects** | **Objective assessment** | **Overall rating** |
| **A** | **Module A: "Information infrastructure commissioning"** | **0** | **15** | **15** |
| **B** | **Module B: "Troubleshooting"** | **0** | **15** | **15** |
| **C** | **Module C: "Network infrastructure deployment and maintenance"** | **0** | **15** | **15** |
| **Total** | | **0** | **45** | **45** |