

|  |
| --- |
| The Project of Network Fundamentals |
|  |
| December 22  Nazlıcan Aydın 200444008  Tolga ÜNLÜ 200444409 |

# About Project

|  |
| --- |
| After fulfilling all the necessary requirements for this project, which has 8 Routers, 11 Switches, 1 Access Point, 1 DHCP Server, 1 DNS Server and 3 Web Servers, we also made Port Security TACACS+ and SNMP Configurations as a bonus. If we look at the overall structure of the project, we performed the operations as if it were the topology of an institution with 1 DNS and 1 DHCP Server inside, and the institution rented 3 servers from a cloud provider as if for web servers, and as the main site of these servers “main.com ” and who are our sites “nazlican.com and tolga.com ” we assumed that it implements these address. In addition, we did not forget to add HTML and CSS codes to the index.html of these sites so that it can be a nice presentation. We started the project by assigning IP addresses between routers and decided that the IP addresses between routers should be 10.0.0.0/24. We have ensured that the endpoint devices in the topology have IP addresses numbered 192.168.0.0. We chose R2 as the last router to go to the Internet and assigned the IP address 78.1.1.0 with a subnet mask of 255.255.255.240 to the branch between the ISP router and R2. We have also defined the 8.8.8.0/24 IP address to the part where the web servers are located. We have defined a separate DHCP pool for all endpoint devices and tested that all devices automatically receive IP from DHCP. In addition, we also registered the domain of 3 different web servers in the project to our internal DNS server and controlled access from all endpoint devices. We have added SSH to most routers and switches in the project and set their passwords as “admin”. In addition, we have provided telnet access to all routers in the project with the username “admin”, password “admin”. We provided access to the access point with a wifi called NazTolAp and set the password for this Wi-Fi as “E4F4C3BD2E”. With the PortSecurity configuration, we assigned and tested the ability for endpoint branches connected to Switch8 to use more than five ports and to close the port if more than five user logins are made. We also implemented TACACS on Switch3 and opened the AAA service of the DHCP server at the same time and tested whether the switch was accessed by typing the telnet 192.168.122.5 code with any endpoint device connected to Switch3 and entering the username “nazli” password “tolga”. We have blocked the VLAN named Guest from accessing the Internet. We implemented the SNMP feature in R31 and tested changing the name of R31 from PC8, which is connected to R31. We also made the Dynamic NAT and Dynamic Routing (OSPF) configurations and provided their controls, and also checked the communication between all computers in the organization. We encountered a problem that we thought was caused by Cisco Packet tracer. Even though we consulted all our friends, we had a problem writing the ACL of the Guest device. Even though all the syntax is correct, the guest device can access the internet with the codes I wrote.  Ip access-list extended newinternet  Deny tcp 192.168.33.0 0.0.0.127 8.8.8.0 0.0.0.0  Interface gi0/0  Ip access-group newinternet in |