МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ   
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

Security and WAN Access Between the MedGroup Clinics

Отчет по лабораторной работе № 10

по дисциплине «Компьютерные сети»

студента 2 курса группы ПИ-б-о-233(1)  
Иващенко Дениса Олеговича

Направления подготовки 09.03.04«Программная инженерия»

Симферополь, 2025

MedGroup Packet Tracer Skills Integration Challenge:  
Part 4—Add Security and WAN Access Between the MedGroup Clinics



**Objectives**

·         Configure basic switch security.

·         Configure access control lists to filter internal traffic.

·         Configure dynamic and static routing.

·         Configure Frame Relay.

**Background and Preparation**

After adding wireless access points to MedGroup’s new topology, you had a meeting with the project manager to review your work. She is ready to assign you the next task to add security and WAN access between the MedGroup clinics. She provides you with the security policies, routing policies, and WAN connectivity requirements. In addition, she has already configured a NAT firewall on UC-GATE using the following commands:

interface FastEthernet0/0

 ip nat outside

interface FastEthernet0/1.7

 ip nat inside

interface FastEthernet0/1.10

 ip nat inside

interface FastEthernet0/1.50

 ip nat inside

interface FastEthernet0/1.100

 ip nat inside

interface FastEthernet0/1.200

 ip nat inside

interface Serial0/0/0

 ip nat inside

ip nat inside source list 1 interface FastEthernet0/0 overload

access-list 1 permit 10.0.0.0 0.0.0.3

access-list 1 permit 192.168.0.0 0.0.255.255

Your task is to configure and verify the security and routing policies and implement the WAN requirements. This task completes the MedGroup prototype.

To complete the activity, you must use the Packet Tracer file MedGroup\_CaseStudy\_Part4.pka.

**Step 1: Review the specifications provided by the project manager.**

a.       For switch security, implement the following on the two urban clinic switches:

·         Enable port security on all access ports configured with an active VLAN. You do not need to configure port security on the interfaces assigned to VLAN 3.

·         Limit the number of MAC addresses to two.

·         Learned MAC addresses should “stick” to the switch configuration.

·         Any violation of the port security policy should cause the port to shut down.

·         Shut down all ports not assigned an access VLAN.

b.       For the ACL security policy, implement the following on Urban Clinic:

·         Allow traffic from the Guest VLAN access to the Internet.

·         Deny traffic with the internal network as the destination.

c.       For WAN connectivity, configure Frame Relay between Urban Clinic and Rural Clinic.

d.       For the routing policies, implement the following on Urban Clinic and Rural Clinic:

·         Use EIGRP between Urban Clinic and Rural Clinic.

·         Use a default route to the Internet through the DSL connection.

**Step 2: Configure basic switch security in Urban Clinic.**

a.       All Cisco IOS devices are configured with the user password **cisco** and the enable password **class**.

b.       Configure the switch security policy as specified in Step 1a.









c.       Verify that security is implemented using the appropriate **show** commands.

**Step 3: Configure access control lists to filter internal traffic.**

* Verify that the Guest laptop can ping internal wired hosts, such as Billing or any of the servers.



b.       Configure the security policy for the Guest VLAN. Although there are multiple correct ways of implementing the policy, use the following guidelines to ensure accurate grading:

·         Use number 100.

·         Block traffic coming into UC-GATE from the entire Guest VLAN network (192.168.200.0/24) bound for any destination in the 192.168.0.0/16 address space.

·         Allow all other traffic.





* Verify that the Guest laptop can no longer ping internal wired hosts.



**Step 4: Configure Frame Relay access between Urban Clinic and Rural Clinic.**

a.       Configure UC-GATE and RC-GATE with the following IP addresses:

|  |  |
| --- | --- |
| **Device** | **Interface Addressing** |
| UC-GATE | Fa0/0 209.165.201.2/30  S0/0/0 10.0.0.1/30 |
| RC-GATE | S0/0/0 10.0.0.2/30 |







* Configure UC-GATE and RC-GATE with Frame Relay.





c.       Verify that Frame Relay is operational.

**Step 5: Configure dynamic and static routing.**

* Configure a default route on UC-GATE pointing to the Internet. Use the outbound interface argument.



b.       Configure EIGRP routing between UC-GATE and RC-GATE using the following criteria:

·         Use AS 100.

·         Advertise all directly connected networks, except the 209.165.201.0/30 network used to connect to the Internet.

·         Redistribute the default route to RC-GATE using the **redistribute static** command.





c.       Verify that both UC-GATE and RC-GATE have full routing tables and a gateway of last resort.

d.       All internal hosts from the urban clinic and rural clinic should now be able to ping the Cisco web server.

**Step 6: Check your results.**

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed. You might need to ping devices to get the MAC address to stick to the configuration before you can achieve a 100%.

*All contents are Copyright © 1992 - 2010 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.*