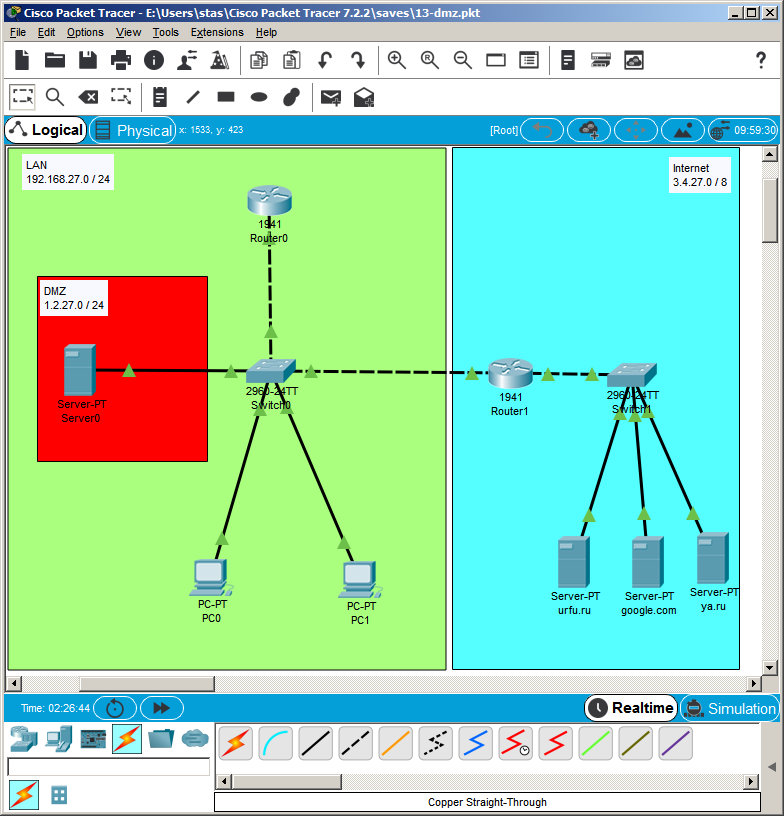
Лабораторная работа № 13. DMZ

В данной лабораторной работе мы познакомимся с:

1. понятием демилитаризованной зоны (DMZ: Demilitarized Zone)
2. Архитектурой «Маршрутизатор на палочке» (Router on a Stick)

Демилитаризованная зона – сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных. При практической реализации много внимания уделяется разграничению прав доступа к разным сегментам подсети, но в нашей лабораторной этот круг вопросов опущен для краткости. ДМЗ – это часть локальной сети, которая не безопасна, как остальная локальная сеть, но и не так опасна, как внешний мир. Как правило, доступ из ДМЗ к локальной сети серьёзно (или полностью) ограничен.

Архитектура «Маршрутизатор на палочке» чаще всего применяется при нехватке физических портов на маршрутизаторе, позволяя организовать дополнительные виртуальные порты при помощи механизма VLAN.



1. Определимся с нумерацией

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Сеть** | **LAN** | **DMZ** | **ISP** | **Internet** |
| **IP** | 192.168.27.0 | 1.2.27.0 | 3.4.27.0 | 5.6.27.0 |
| **Маска** | 255.255.255.0 | 255.255.255.0 | 255.255.255.252 | 255.0.0.0 |
| **/Маска** | /24 | /24 | /30 | /8 |
| **VLAN** | 10 | 20 | 30 | - |
| **Шлюз** | 192.168.27.1 | 1.2.27.1 | 3.4.27.1 | 5.6.27.1 |
| **Коммутатор** | 192.168.27.2 | - | - | - |
| **Сервера** |  | 1.2.27.2 |  | 5.6.27.2  5.6.27.42  5.6.27.108 |
| **WS** | DHCP | - | - | - |
| **Router** | 192.168.27.1 | 1.2.27.1 | 3.4.27.2 |  |
| **ISP Router** |  |  | 3.4.27.1 | 5.6.27.1 |

1. Нарисуем схему сети
2. Расставим оборудование
   * Маршрутизатор Cisco 1941
   * Коммутатор Cisco 2960
   * Сервер DMS (DNS + Web)
   * Пару рабочих станций
   * Маршрутизатор провайдера Cisco 1941
   * Коммутатор Интернет Cisco 2960
   * Сервера Интернет (Web)
3. Настроим сеть провайдера
   * см. Приложение
   * Провайдер настраивает маршрут до общедоступных сервисов клиента (DMZ)
   * ip route 1.2.27.0 255.255.255.0 3.4.27.2
   * Web-сервера
     + Статические адреса
     + Службы HTTP
4. Настроим локальную сеть
   * Маршрутизатор – см. Приложение
   * Коммутатор – см. Приложение
   * Сервер
     + Статический IP: 1.2.27.2
     + DNS
       - www: 1.2.27.2
       - urfu.ru: 5.6.27.2
       - google.com: 5.6.27.42
       - ya.ru: 5.6.27.108
     + HTTP
5. Проверка работоспособности
   * С рабочих станций (по имени и по IP)
     + DMZ
     + Интернет
   * Из Интернет (по IP)
     + DMZ
     + Интернет
     + ~~Рабочие станции~~

Приложение

## Примерная конфигурация активного сетевого оборудования

hostname ro-13-me

interface GigabitEthernet0/0

no shutdown

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.27.1 255.255.255.0

ip nat inside

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 1.2.27.1 255.255.255.0

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 3.4.27.2 255.255.255.252

ip nat outside

ip nat inside source list NAT interface GigabitEthernet0/0.30 overload

ip route 0.0.0.0 0.0.0.0 3.4.27.1

ip access-list standard NAT

permit 192.168.27.0 0.0.0.255

hostname sw-13

ip dhcp excluded-address 192.168.27.0 192.168.27.9

ip dhcp pool LAN

network 192.168.27.0 255.255.255.0

default-router 192.168.27.1

dns-server 1.2.27.2

spanning-tree mode rapid-pvst

interface range FastEthernet0/1-9

switchport access vlan 10

interface FastEthernet0/10

switchport access vlan 20

interface GigabitEthernet0/1

switchport mode trunk

interface GigabitEthernet0/2

switchport access vlan 30

interface Vlan10

ip address 192.168.27.2 255.255.255.0

hostname ro-13-inet

interface GigabitEthernet0/0

ip address 3.4.27.1 255.255.255.252

interface GigabitEthernet0/1

ip address 5.6.27.1 255.0.0.0

ip route 1.2.27.0 255.255.255.0 3.4.27.2