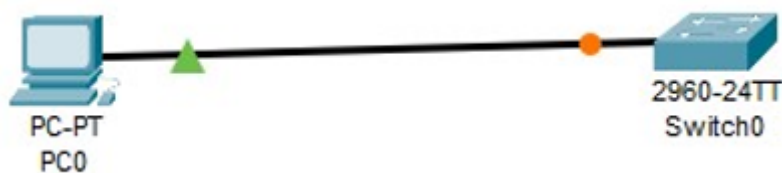


Практическая работа 15 – Настройка Telnet.

Создана сеть с одним ПК (PC0) и коммутатором (Switch0).



На интерфейс VLAN1 коммутатора назначен IP-адрес (192.168.0.2/24).

Интерфейс VLAN1 был активирован командой no shutdown.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#int vlan 1
Switch(config-if)#no sh

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#ip address 192.168.0.2 255.255.255.0
Switch(config-if)#exit
```

Пропингован коммутатор с ПК (с помощью команды ping 192.168.0.2) для проверки доступности.

Переход в режим конфигурации терминала (conf t). Настройка линий виртуального терминала (vty): line vty 0 5 (разрешает до 6 одновременных подключений). Установка пароля для доступа по Telnet: password 111. Активация Telnet: login.



2960

Sw

Device Name: Switch0

Custom Device Model: 2960 IOS15

Hostname: Switch

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	1	--	0030.F23E
FastEthernet0/2	Down	1	--	0030.F23E
FastEthernet0/3	Down	1	--	0030.F23E
FastEthernet0/4	Down	1	--	0030.F23E
FastEthernet0/5	Down	1	--	0030.F23E
FastEthernet0/6	Down	1	--	0030.F23E
FastEthernet0/7	Down	1	--	0030.F23E
FastEthernet0/8	Down	1	--	0030.F23E
FastEthernet0/9	Down	1	--	0030.F23E
FastEthernet0/10	Down	1	--	0030.F23E
FastEthernet0/11	Down	1	--	0030.F23E
FastEthernet0/12	Down	1	--	0030.F23E
FastEthernet0/13	Down	1	--	0030.F23E
FastEthernet0/14	Down	1	--	0030.F23E
FastEthernet0/15	Down	1	--	0030.F23E
FastEthernet0/16	Down	1	--	0030.F23E
FastEthernet0/17	Down	1	--	0030.F23E
FastEthernet0/18	Down	1	--	0030.F23E
FastEthernet0/19	Down	1	--	0030.F23E
FastEthernet0/20	Down	1	--	0030.F23E
FastEthernet0/21	Down	1	--	0030.F23E
FastEthernet0/22	Down	1	--	0030.F23E
FastEthernet0/23	Down	1	--	0030.F23E
FastEthernet0/24	Down	1	--	0030.F23E
GigabitEthernet0/1	Down	1	--	0030.F23E
GigabitEthernet0/2	Down	1	--	0030.F23E
Vlan1	Up	1	192.168.0.2/24	00D0.FF0C

Las

С ПК запущена утилита telnet 192.168.0.2. Введен пароль (111). После успешной авторизации протестированы команды для просмотра конфигурации коммутатора (например, show vlan).

```
C:\>telnet 192.168.0.2
Trying 192.168.0.2 ...Open

[Connection to 192.168.0.2 closed by foreign host]
C:\>
```

```
Switch(config)#line vty 0 5
Switch(config-line)#pass 111
```

```

password:
Switch>show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gig0/1, Gig0/2
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default          active

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp   BrdgMode Trans1 Trans2
-----
1    enet    100001    1500  -       -       -       -   -       0       0
1002 fddi    101002    1500  -       -       -       -   -       0       0
1003 tr      101003    1500  -       -       -       -   -       0       0
1004 fdnet   101004    1500  -       -       -       ieee -       0       0
1005 trnet   101005    1500  -       -       -       ibm  -       0       0
--More--

Switch(config)#enable secret 123
Switch(config)#

Switch>
Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#

```

Настройка пароля привилегированного режима (enable secret).

Вывод:

Telnet позволяет удаленно управлять сетевым оборудованием. Настройка Telnet включает в себя настройку IP-адреса на коммутаторе, настройку линий VTY и установку пароля для доступа. Важно помнить, что Telnet передает данные в незашифрованном виде, поэтому для более безопасного удаленного доступа следует использовать SSH.