

Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет инфокоммуникаций
Кафедра защиты информации

Практическая работа №4
«УЯЗВИМОСТИ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ»
Шифр 672

Проверила:
Белоусова Е.С.

Выполнила:
ст. гр. 961401
Акулова П.Г.

Минск 2022

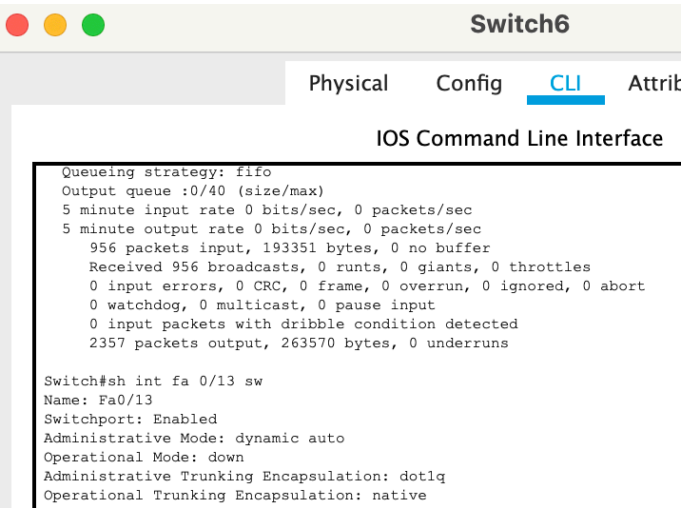
Цель: проанализировать уязвимости VLAN и принципы реализации атак, эксплуатирующие данные уязвимости. Научиться реализовывать защиту от атак на виртуальные локальные сети.

Таблица 1.1 – Исходные данные для смоделированной сети

Вторая цифра шифра	IP-адрес сети	Router-id	Номер VLAN	Третья цифра шифра	Номера VLAN для видеокamer, системы контроля доступа, пожаротушения, контроля дыма, освещения, температуры
7	172.10.0.0/24	45.45.45.45	33, 32, 30	2	201–206

1.Атака VLAN-hopping на уязвимость DTP протокола

-Результат команды *show interfaces fastEthernet 0/13 switchport*



-Отправка DTP-пакета устройству злоумышленника

DTP		
0	1	2
VERSION:1	TYPE: 1	LENGTH:5
	DOMAIN NAME:	TYPE: 2
LENGTH: 5		STATUS:Dynamic Auto
TYPE: 3		LENGTH: 5
TRUNK:1		TYPE: 4
LENGTH: 10		
SENDER ID:0040.0B22.780D		

-Отправка DTP-пакета устройству от злоумышленника

DTP			
0	1	2	3
VERSION:1	TYPE: 1		LENGTH:5
	DOMAIN NAME:	TYPE: 2	
LENGTH: 5		STATUS:Trunk	
TYPE: 3		LENGTH: 5	
TRUNK:1		TYPE: 4	
LENGTH: 10			
SENDER ID:0009.7C11.4801			

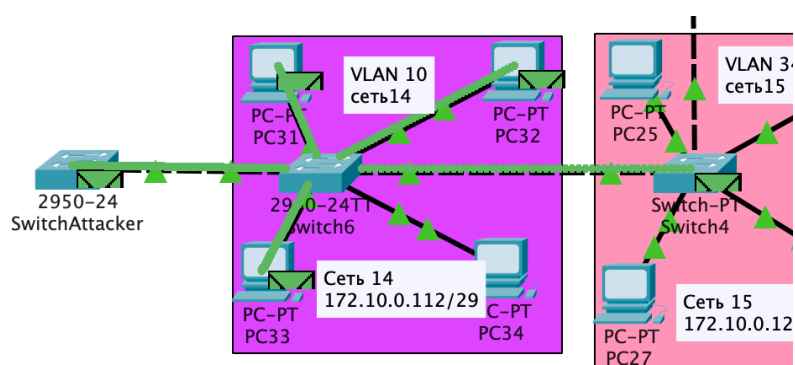
-Результат автоматического согласования портов в режиме trunk
Switch6

```
Switch#sh int fa 0/13 sw
Name: Fa0/13
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
```

SwitchAttacker

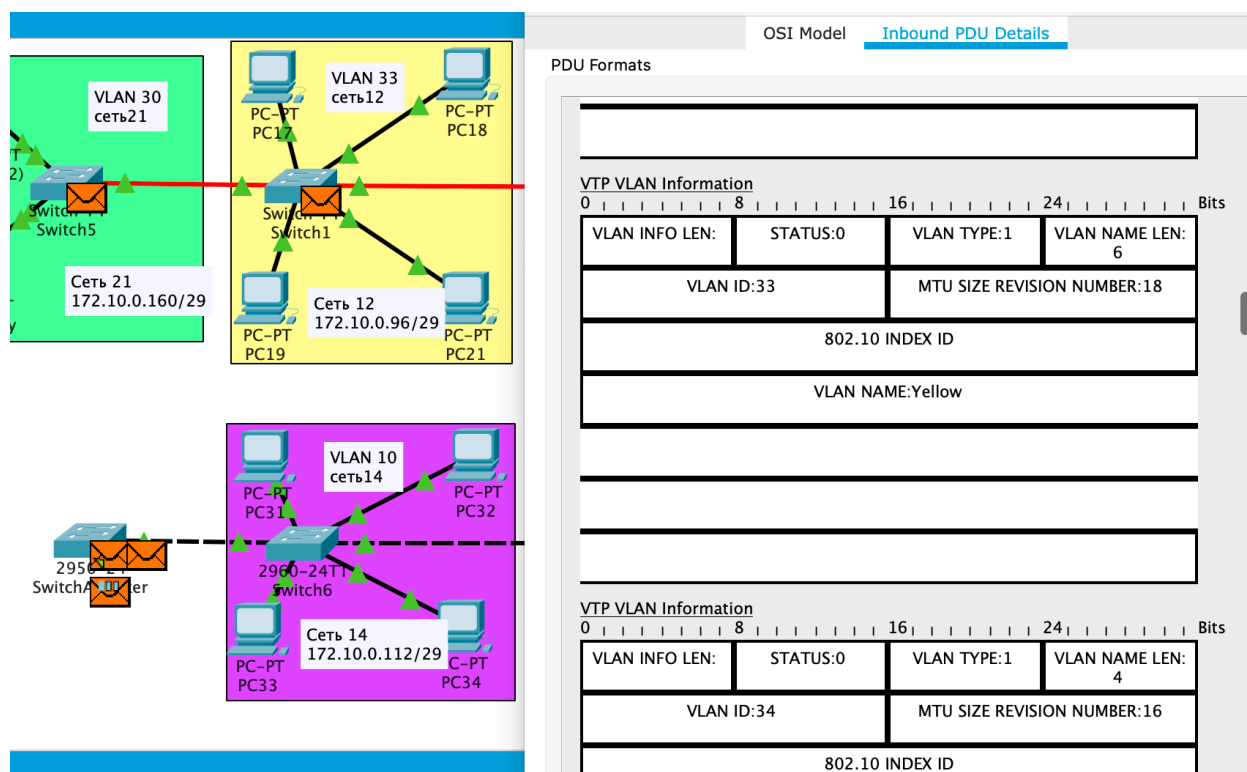
```
Switch#sh int fa 0/1 sw
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
```

-Результат получения ARP-пакета устройством злоумышленника



2. Атака VLAN-hopping на уязвимость VTP протокола

-Получение устройством злоумышленника пакета VTP



4. Реализация защиты от DHCP-spoofing, MitM, DNS-spoofing

-Против DVT уязвимости: *switchport nonegotiate*

```
Switch6
Physical Config CLI
IOS Command Line Interface

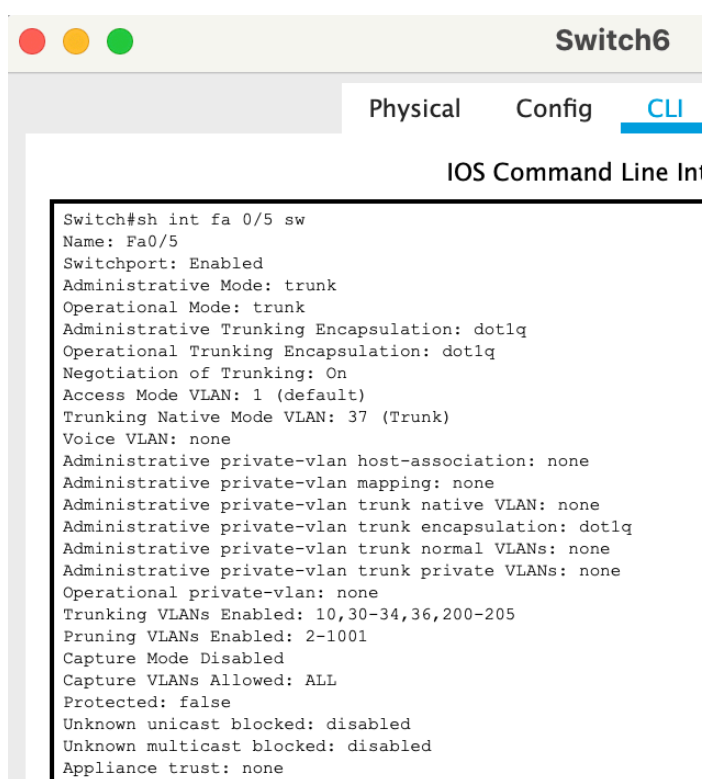
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 39 (Useless)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Name: Fa0/8
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 39 (Useless)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
```

-Против VTP уязвимости: *vtp mode transparent*

```
Switch#sh vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 18
VTP Operating Mode         : Transparent
VTP Domain Name            : cisco
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0x75 0x3C 0x20 0x78 0xB7 0x90 0xCB 0xE4
Configuration last modified by 0.0.0.0 at 3-1-93 00:06:20
Switch#
```

- Native VLAN не default (VLAN 1) и передача данных только определенных VLAN, используемых в сети



The screenshot shows a network switch interface with a title bar 'Switch6' and three window control buttons (red, yellow, green). Below the title bar are three tabs: 'Physical', 'Config', and 'CLI', with 'CLI' being the active tab. The main content area is titled 'IOS Command Line Interface'. It displays the output of the command 'Switch#sh int fa 0/5 sw', showing detailed configuration for interface Fa0/5, including administrative and operational modes, trunking settings, and VLAN configurations.

```
Switch#sh int fa 0/5 sw
Name: Fa0/5
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 37 (Trunk)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,30-34,36,200-205
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Вывод: по результатам выполнения работы выяснила, что самой эффективной защитой от несанкционированного подключения к сети является вручную переводить. Неиспользуемые порты коммутатора в режим shutdown. Также поняла логику настройки защиты от уязвимостей протоколов VTP и DTP.

