

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ  
ІНСТИТУТ КОМП'ЮТЕРНИХ СИСТЕМ  
КАФЕДРА КОМП'ЮТЕРНИХ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ І МЕРЕЖ

Протокол  
Лабораторна робота №4  
На тему “Захист мережевої інфраструктури”  
По предмету: «Захист інформації у комп'ютерних системах»

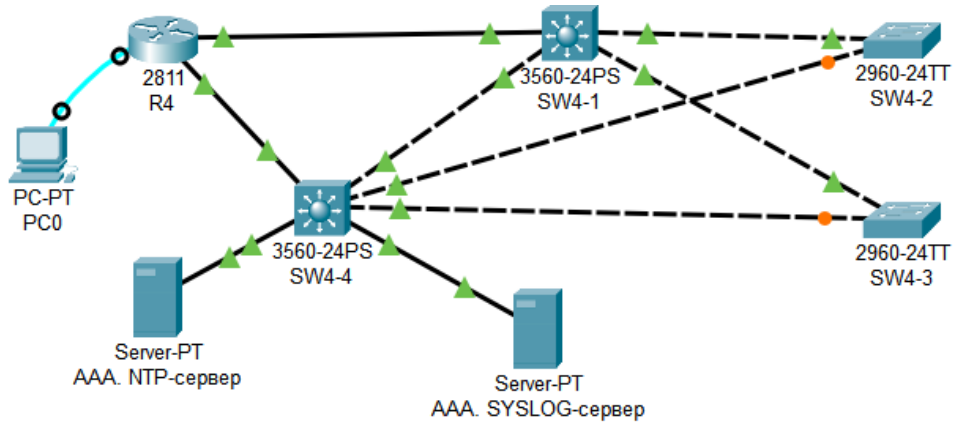
Виконав:  
студент групи АМ-182  
Борщов М.І.  
Перевірив:  
Шапорін В. О.

Одеса 2022

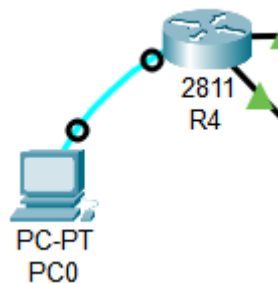
## **Перелік завдань до лабораторної роботи**

1. Підключитися до маршрутизатора R4 через консольний порт з робочої станції адміністратора мережі.
2. Поставити ім'я маршрутизатора і домен. Згенерувати криптографічні ключі, використовувані в криптографічному протоколі SSH, для чого задати ім'я вузла мережі та домен.
3. Включити доступ до маршрутизатора за протоколом SSHv2, задати кількість спроб аутентифікації.
4. Налаштувати видачу попереджувального повідомлення про підключення до мережного обладнання.
5. Створити локального користувача та встановити пароль на доступ до конфігураційного режиму.
6. Відключити служби DNS і CDP, включити шифрування паролів у файлі конфігурації.
7. Виконати налаштування доступу до маршрутизатора за технологією AAA на основі протоколу TACACS +.
8. Налаштувати віддалений доступ до маршрутизатора з дозволених IP-адрес робочих станцій мережі управління філії.
9. Виконати налаштування служби реєстрації подій та їх відправки на сервер реєстрації подій філії (IP-адреса 192.168.4.2) по протоколу SYSLOG.
10. Виконати налаштування протоколу SNMP для доступу до маршрутизатора з сервера моніторингу.
11. Виконати налаштування протоколу NTP для синхронізації часу з сервером точного часу (IP-адреса 192.168.4.1).
12. Виконати налаштування комутаторів ЛВС філії для підключення до мережі внеполосного управління відповідно до схеми, представленої на рис. 1. На комутаторах налаштувати віртуальний інтерфейс типу SVI.
13. На маршрутизаторі R4 виконати налаштування щодо обмеження доступу до мережі управління з ЛВС передачі даних.

## Хід роботи



## З'єднання обладнання



Підключення до маршрутизатора R4 через консольний порт з робочої станції адміністратора мережі

```
enable secret 5 $1$mERr$DadO.ZoS.MDbWMQdR.LSo0  
hostname R4  
| ip domain-name router_R4
```

Використання у криптографічному протоколі SSH задання ім'я вузла мережі та домен

```
| ip ssh version 2  
| ip ssh authentication-retries 2  
| ip ssh time-out 60
```

Включити доступ до маршрутизатора за протоколом SSHv2, задати кількість спроб аутентифікації

```

banner login ^C
*****
* Bank Router
* UNAUTHORIZED ACCESS IS PROHIBITED *
* You have accessed network equipment. *
* You must have authorized permission to access *
* Or configure this device. All activities *
* Performed on this device are monitored and *
* Logged. *
***** ^C

```

Налаштувати видачу попереджувального повідомлення про підключення до мережного обладнання

```

username admin secret 5 $l$mERr$3HhIgMGBA/9qNmgezccuxv0

```

Створити локального користувача та встановити пароль на доступ до конфігураційного режиму

```

no ip domain-lookup

no cdp run

service password-encryption

```

Відключити служби DNS і CDP, включити шифрування паролів у файлі конфігурації

```

tacacs-server host 192.168.4.1 key cisco
tacacs-server host 192.168.4.2 key cisco

aaa new-model
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
!
!
aaa authorization exec default group tacacs+ local

```

Виконати налаштування доступу до маршрутизатора за технологією AAA на основі протоколу TACACS +

```

ip access-list extended iacl-vty
permit tcp 192.168.4.0 0.0.0.63 any eq 22
deny ip any any

!
line con 0
exec-timeout 5 0
login authentication default
!
line aux 0
!
line vty 0 4
access-class iacl-vty in
transport input ssh
line vty 5 15
access-class iacl-vty in
transport input ssh

```

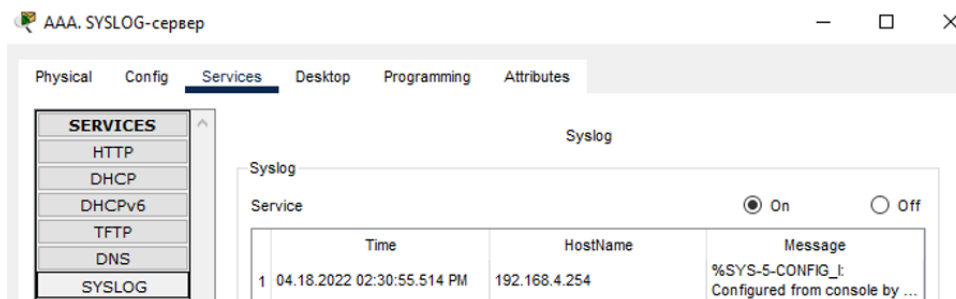
Налаштувати віддалений доступ до маршрутизатора з дозволених IP-адрес робочих станцій мережі управління філії

```

service timestamps log datetime msec
service timestamps debug datetime msec

logging trap debugging
logging 192.168.4.2

```



Виконати налаштування служби реєстрації подій та їх відправки на сервер реєстрації подій філії (IP-адреса 192.168.4.2) по протоколу SYSLOG

```
snmp-server community cisco_snmp RW
```

Виконати налаштування протоколу SNMP для доступу до маршрутизатора з сервера моніторингу

```
ntp authentication-key 1 md5 0822455D0A16 7
ntp authenticate
ntp trusted-key 1
ntp server 192.168.4.1 key 1
```

AAA, NTP-сервер

Physical Config **Services** Desktop Programming Attributes

**SERVICES**

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP**
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

NTP Service ☒ On ☐ Off

Authentication ☒ Enable ☐ Disable

Key: 1 Password: cisco

← Апрель, 2022 → 02:34:41

Пн	Вт	Ср	Чт	Пт	Сб	Вс
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1
2	3	4	5	6	7	8

```
R4#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.4.1
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E5E068C8.00000155 (14:35:52.341 UTC Mon Apr 18 2022)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 41.22 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 13 sec ago.
```

Виконати налаштування протоколу NTP для синхронізації часу з сервером точного часу (IP-адреса 192.168.4.1)

```
interface Vlan100
 mac-address 0001.64d1.1d01
 ip address 192.168.4.253 255.255.255.0
 !
 ip default-gateway 192.168.4.254
```

Налаштування L3-комутатора SW4-1

```
interface Vlan100
 ip address 192.168.4.252 255.255.255.0
 !
 ip default-gateway 192.168.4.254
```

## Налаштування L2-комутатора SW4-2

```
interface Vlan100
 ip address 192.168.4.251 255.255.255.0
 !
 ip default-gateway 192.168.4.254
```

## Налаштування L2-комутатора SW4-3

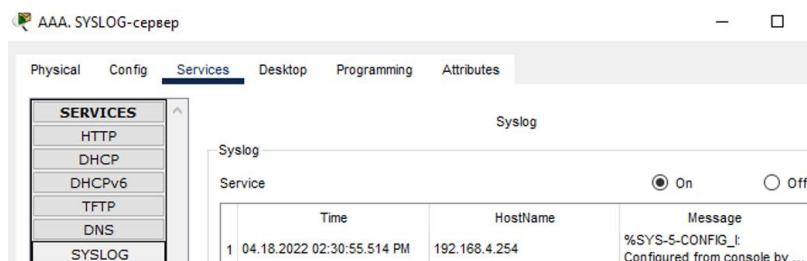
```
interface Vlan100
 mac-address 0002.178c.6801
 ip address 192.168.4.250 255.255.255.0
 !
 ip default-gateway 192.168.4.254
```

## Налаштування L3-комутатора SW4-4

```
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 192.168.4.254 255.255.255.0
 ip access-group iacl-in-management in
 ip access-group iacl-out-management out

ip access-list extended iacl-in-management
 permit ip 192.168.4.0 0.0.0.255 192.168.4.0 0.0.0.255
ip access-list extended iacl-out-management
 permit ip 192.168.4.0 0.0.0.255 192.168.4.0 0.0.0.255
 deny ip any any
```

На маршрутизаторі R4 виконати налаштування щодо обмеження доступу до мережі управління з ЛВС передачі даних



Успішна реєстрація подій на сервері SYSLOG