

Politechnika Świętokrzyska	
Wydział Elektrotechniki, Automatyki i Informatyki	
Bezpieczeństwo Infrastruktury Sieciowej	
Projekt	
Skład zespołu: Dawid Jaszczuk, Diana Nowak, Dawid Bujak	
Grupa 1ID24A	Data: 10.10.2023
Temat: Projekt infrastruktury sieciowej prywatnej przychodni lekarskiej (parter i piętro)	

Repozytorium: <https://github.com/Dawol1/PrzychodniaBIS>

Spis treści

1. Cel projektu	4
2. Harmonogram prac	4
3. Założenia sieci.....	4
4. Opis zagrożeń	6
5. Podział na podsieci	6
6. Konfiguracja urządzeń	8
7. Bezpieczeństwo sieci	16
Radius	16
DNS	17
Firewall	18
ACL.....	19
Logowanie do R1	22
SSH.....	22
NTP	23
AAA	24
Port Monitor.....	24
RIP.....	25
OSPF.....	25
STP	26
Etherchannel	26

Spis ilustracji

Rysunek 3.1 Schemat sieci.....	5
Rysunek 6.1 DHCP R1	15
Rysunek 6.2 DHCP R2	15
Rysunek 6.3 DHCP R3	15
Rysunek 7.1 Radius.....	16
Rysunek 7.2 Syslog	16
Rysunek 7.3 DNS - konfiguracja.....	17
Rysunek 7.4 Uruchomiona strona	18
Rysunek 7.5 Sprawdzenie działania firewall.....	19
Rysunek 7.6 Efekt działania firewall	19
Rysunek 7.7 ACL - ta sama podsieć	20
Rysunek 7.8 ACL - inna podsieć	20
Rysunek 7.9 ACL - drukarka w tej samej podsieci	21
Rysunek 7.10 ACL - drukarka w innej podsieci	21
Rysunek 7.11 Zabezpieczenie dostępu.....	22
Rysunek 7.12 SSH	22

Rysunek 7.13 NTP - konfiguracja	23
Rysunek 7.14 NTP - sprawdzenie	23
Rysunek 7.15 AAA.....	24
Rysunek 7.16 Port monitor - konfiguracja.....	24
Rysunek 7.17 Port monitor - sprawdzenie działania	25
Rysunek 7.18 Konfiguracja RIP	25
Rysunek 7.19 Konfiguracja OSPF	25
Rysunek 7.20 STP.....	26
Rysunek 7.21 EtherChannel.....	26

1. Cel projektu

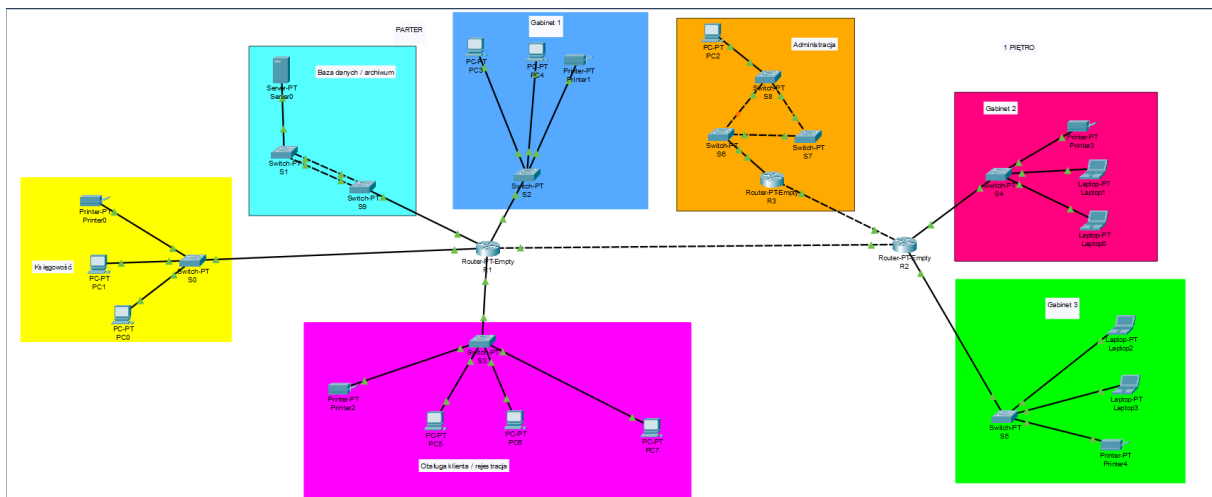
W ramach projektu z zajęć „Bezpieczeństwo infrastruktury sieciowej” należy przygotować projekt sieci organizacji w programie Cisco Packet Tracer. Sieć ta musi odzwierciedlać prawdziwą topologię organizacji, czyli fizyczne odzwierciedlenie sprzętu komputerowego, połączeń oraz konfiguracji. Sieć musi zawierać także kilka protokołów zabezpieczających ją.

2. Harmonogram prac

Data	Planowane wykonane czynności
10.10.2023	Ustalenie tematu projektu oraz jego zakresu, a także harmonogramu.
14.11.2023	Określenie wymagań, jakie mogą czekać wykreowaną sieć. Gotowy schemat infrastruktury sieciowej w programie Cisco Packet Tracer. Przydzielenie sieci, podsieci, zaadresowanie urządzeń, konfiguracja serwera DHCP, konfiguracja poziomów dostępowych na urządzeniach sieciowych, dynamiczne protokoły routingu. Weryfikacja z wymagania projektu oraz z harmonogramem.
19.12.2023	Dalszy rozwój projektu. Konfiguracja różnych usług, m.in. Syslog, NTP, AAAA, listy ACL, VLANY, RIP, OSPF. Weryfikacja z wymagania projektu oraz z harmonogramem.
16.01.2023	Weryfikacja działania skonfigurowanego projektu sieci, a także weryfikacja z wymaganiami i harmonogramem. Prezentacja oraz obrona gotowego projektu.

3. Założenia sieci

Naszym tematem projektowanej topologii sieci jest przychodnia medyczna. W tej organizacji zakładamy, że sprzęt komputerowy czy sieciowy będzie rozmieszczony na parterze oraz 1 piętrze. Topologia przedstawia się następująco:



Rysunek 3.1 Schemat sieci

Mamy tutaj podział na 2 piętra.

Parter:

- Księgowość
 - S0
 - PC0
 - PC1
 - Printer0
- Baza danych/archiwum
 - Server0
 - S1
 - S9
- Gabinet1
 - S2
 - PC3
 - PC4
 - Printer1
- Obsługa klienta / rejestracja
 - S3
 - PC5
 - PC6
 - PC7
 - Printer2
- R0

Pierwsze piętro:

- Administracja
 - R3
 - S6
 - S7
 - S8
 - PC2

- Gabinet 2
 - S4
 - Laptop0
 - Laptop1
 - Printer3
- Gabinet 3
 - S5
 - Laptop2
 - Laptop3
 - Printer4
- R1
- R3

Pomiędzy parterem a pierwszym piętrzem występuje łączenie poprzez routery.

4. Opis zagrożeń

Jak każda infrastruktura, tworzony projekt też będzie podatny na przeróżne zagrożenia.

Pierwszym potencjalnym zagrożeniem jest dostęp osób z zewnątrz do serwera a tym samym do danych medycznych.

Drugim potencjalnym zagrożeniem są ataki DDoS, którą mogą obciążyć całą sieć, spowolnić ją lub nawet doprowadzić do awarii.

Kolejnym potencjalnym zagrożeniem jest nieautoryzowany dostęp pracowników. Nie każdy pracownik musi mieć dostęp do wszystkiego, a jedynie do niezbędnych zasobów. Należy więc zadbać o to, aby uprawnienia były odpowiednio nadane. W sieci przewidywane są także komputery dla pacjentów, które szczególnie trzeba zabezpieczyć przed ewentualną niechcianą ingerencją.

Innym potencjalnym zagrożeniem jest ryzyko przechwycenia danych pacjentów, ze względu na brak szyfrowania komunikacji.

Jeszcze innym zagrożeniem jest nieautoryzowany dostęp. Brak odpowiednich mechanizmów uwierzytelniania i autoryzacji może prowadzić do nieautoryzowanego dostępu do danych pacjentów.

Wszystkie zagrożenia są dosyć niebezpieczne i mogą być fatalne w skutkach. Należy więc zadbać o prawidłowe zabezpieczenie, co pozwoli na ich wyeliminowanie lub zminimalizowanie.

5. Podział na podsieci

W projektowanej sieci zastosowaliśmy następujący podział:

- **Parter**
 - Adres sieci: 192.168.1.0
 - Maska: 255.255.255.0

Podział na podsieci:

- **Obsługa klienta / rejestracja**
 - Adres sieci: 192.168.1.0
 - Maska: 255.255.255.248
- **Księgowość**
 - Adres sieci: 192.168.1.8
 - Maska: 255.255.255.248
- **Baza danych / archiwum**
 - Adres sieci: 192.168.1.24
 - Maska: 255.255.255.248
- **Gabinet 1**
 - Adres sieci: 192.168.1.16
 - Maska: 255.255.255.248
- **Połączenie pomiędzy routerami**
 - Adres sieci: 192.168.1.32
 - Maska: 255.255.255.252
- **Połączenie pomiędzy routerami**
 - Adres sieci: 192.168.1.36
 - Maska: 255.255.255.248
- **Pierwsze piętro**
 - Adres sieci: 192.168.2.0
 - Maska: 255.255.255.0

Podział na podsieci:

- **Gabinet 1**
 - Adres sieci: 192.168.2.0
 - Maska: 255.255.255.248
- **Księgowość**
 - Adres sieci: 192.168.2.8
 - Maska: 255.255.255.248
- **Połączenie pomiędzy routerami**
 - Adres sieci: 192.168.2.16
 - Maska: 255.255.255.248
- **Administracja**

- Adres sieci: 192.168.2.24
- Maska: 255.255.255.248

6. Konfiguracja urządzeń

Server0

- Brama: 192.168.1.25
- Serwer DNS: 0.0.0.0
- FastEthernet0
 - Adres: 192.168.1.26
 - Maska: 255.255.255.252
- Uruchomiony serwer DNS: strona.pl na adresie 192.168.1.26
- Uruchomiony firewall – możliwość dostępu do strony ale brak możliwości pingowania serwera
- Uruchomione AAA, serwer Radius
 - Nazwa hosta: R1
 - Adres: 192.168.1.25
 - Typ: Radius
 - Hasło/klucz: cisco
 - Użytkownicy
 - Nazwa: user
 - Hasło: cisco
- Uruchomiony serwer Syslog
- Uruchomiony serwer NTP
 - Klucz: 1
 - Hasło: cisco

PC0

- Brama: 192.168.1.9
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres: 192.168.1.10
 - Maska: 255.255.255.248

PC2

- Brama: 192.168.1.9
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres: 192.168.1.11
 - Maska: 255.255.255.248

Printer0

- Brama: 192.168.1.9
- Serwer DNS: 192.168.1.26
- FastEthernet0

- Adres:192.168.1.10
- Maska: 255.255.255.248

S0

- VLAN1
 - Adres:192.168.1.13
 - Maska: 255.255.255.248
- Konfiguracja ssh
 - Nazwa : user
 - Hasło: hasło
- Konfiguracja Port Monitor – z portów FastEthernet3/1 i FastEthernet1/1 na port FastEthernet2/1.
- Hasło: hasło

Printer0

- Brama: 192.168.1.25
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.1.16
 - Maska: 255.255.255.248

S1

- VLAN1
 - Adres:192.168.1.27
 - Maska: 255.255.255.248
- Konfiguracja ssh
 - Nazwa : user
 - Hasło: hasło
- Hasło: hasło

S2

- VLAN1
 - Adres:192.168.1.22
 - Maska: 255.255.255.248
- Konfiguracja ssh
 - Nazwa : user
 - Hasło: hasło
- Hasło: hasło

PC3

- Brama: 192.168.1.17
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.1.18
 - Maska: 255.255.255.248

PC4

- Brama: 192.168.1.17
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.1.19
 - Maska: 255.255.255.248

Printer1

- Brama: 192.168.1.17
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.1.20
 - Maska: 255.255.255.248

S3

- VLAN1
 - Adres:192.168.1.6
 - Maska: 255.255.255.248
- Konfiguracja ssh
 - Nazwa : user
 - Hasło: haslo
- Hasło: haslo

Printer1

- Brama: 192.168.1.1
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.1.5
 - Maska: 255.255.255.248

PC5

- Brama: 192.168.1.1
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.1.2
 - Maska: 255.255.255.248

PC6

- Brama: 192.168.1.1
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.1.3
 - Maska: 255.255.255.248

PC7

- Brama: 192.168.1.1
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.1.4
 - Maska: 255.255.255.248
- Zabroniony dostęp przez ACL (brak możliwości komunikacji z siecią, komputer dla pacjentów)

R1

- Ethernet0/0
 - Adres:192.168.1.1
 - Maska: 255.255.255.248
- Ethernet0/1
 - Adres:192.168.1.9
 - Maska: 255.255.255.248
- Ethernet0/2
 - Adres:192.168.1.25
 - Maska: 255.255.255.252
- Ethernet0/3
 - Adres:192.168.1.17
 - Maska: 255.255.255.248
- Ethernet0/4
 - Adres:192.168.1.33
 - Maska: 255.255.255.252
- Routing statyczny
 - 192.168.2.0/24 przez port 192.168.1.34
- RIP
 - 192.168.1.0
- OSPF
 - 192.168.1.0
- ACL
 - Numer listy: 1
 - Zabroniona komunikacja dla PC7 (komputer dla pacjentów)
 - Standard IP access list 1
 - 10 deny host 192.168.1.4 (16 match(es))
 - 20 permit any (16 match(es))
 - Numer listy : 2
 - Zabroniona komunikacja z drukarkami poza tymi, które znajdują się w danej podsieci
 - Standard IP access list 2
 - 10 deny host 192.168.1.12 (3 match(es))
 - 20 deny host 192.168.1.20 (7 match(es))
 - 30 deny host 192.168.1.5
 - 40 deny host 192.168.2.4
 - 50 deny host 192.168.2.12

- 60 permit any (23 match(es))
- Synchronizacja z serwerem NTP
- Username: user
- Hasło: cisco
- Hasło do trybu enable: cisco

R2

- Ethernet0/0
 - Adres: 192.168.1.34
 - Maska: 255.255.255.252
- Ethernet0/1
 - Adres: 192.168.2.1
 - Maska: 255.255.255.248
- Ethernet0/2
 - Adres: 192.168.2.9
 - Maska: 255.255.255.248
- Ethernet0/3
 - Adres: 192.168.2.17
 - Maska: 255.255.255.248
- Routing statyczny
 - 192.168.1.0/24 przez port 192.168.1.33
 - 192.168.2.24/29 przez port 192.168.2.18
- RIP
 - 192.168.1.0
 - 192.168.2.0
- OSPF
 - 192.168.1.0
 - 192.168.2.0
- ACL
 - Numer listy: 1
 - Zabroniona komunikacja dla PC7 (komputer dla pacjentów)
 - Standard IP access list 1
 - 10 deny host 192.168.1.4 (32 match(es))
 - 20 permit any (39 match(es))
 - Numer listy : 2
 - Zabroniona komunikacja z drukarkami poza tymi, które znajdują się w danej podsięci
 - Standard IP access list 2
 - 10 deny host 192.168.1.12
 - 20 deny host 192.168.1.20
 - 30 deny host 192.168.1.5
 - 40 deny host 192.168.2.4 (4 match(es))
 - 50 deny host 192.168.2.12 (4 match(es))
 - 60 permit any (16 match(es))
- Synchronizacja z serwerem NTP
- Username: user
- Hasło: cisco

- Hasło do trybu enable: cisco

R3

- Ethernet0/0
 - Adres:192.168.2.18
 - Maska: 255.255.255.252
- Ethernet1/0
 - Adres:192.168.2.25
 - Maska: 255.255.255.248
- Routing statyczny
 - 192.168.1.0/24 przez port 192.168.2.17
- RIP
 - 192.168.2.0
- OSPF
 - 192.168.2.0
- Synchronizacja z serwerem NTP
- Username: user
- Hasło: cisco
- Hasło do trybu enable: cisco

S6

- VLAN1
 - Adres:192.168.2.27
 - Maska: 255.255.255.248
- Hasło: haslo

PC2

- Brama: 192.168.2.17
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.2.26
 - Maska: 255.255.255.248

S4

- VLAN1
 - Adres:192.168.2.5
 - Maska: 255.255.255.248
- Hasło: haslo

Printer3

- Brama: 192.168.2.1
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.2.4
 - Maska: 255.255.255.248

Laptop1

- Brama: 192.168.2.1
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.2.3
 - Maska: 255.255.255.248

Laptop0

- Brama: 192.168.2.1
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.2.2
 - Maska: 255.255.255.248

S5

- VLAN1
 - Adres:192.168.2.13
 - Maska: 255.255.255.248
- Hasło: hasło

Printer4

- Brama: 192.168.2.9
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.2.12
 - Maska: 255.255.255.248

Laptop2

- Brama: 192.168.2.9
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.2.10
 - Maska: 255.255.255.248

Laptop3

- Brama: 192.168.2.9
- Serwer DNS: 192.168.1.26
- FastEthernet0
 - Adres:192.168.2.11
 - Maska: 255.255.255.248

S7

- Hasło: hasło
- STP

S8

- Hasło: hasło
- STP

S9

- Hasło: hasło
- Etherchannel

DHCP

R1

```
ip dhcp pool rejestracja
 network 192.168.1.0 255.255.255.248
 default-router 192.168.1.1
 dns-server 192.168.1.26
ip dhcp pool ksiegowosc
 network 192.168.1.8 255.255.255.248
 default-router 192.168.1.9
 dns-server 192.168.1.26
ip dhcp pool gabinet1
 network 192.168.1.16 255.255.255.248
 default-router 192.168.1.17
 dns-server 192.168.1.26
!
```

Rysunek 6.1 DHCP R1

R2

```
ip dhcp pool gabinet2
 network 192.168.2.0 255.255.255.248
 default-router 192.168.2.1
 dns-server 192.168.1.26
ip dhcp pool gabinet3
 network 192.168.2.8 255.255.255.248
 default-router 192.168.2.9
 dns-server 192.168.1.26
clock timezone CST -6
!
```

Rysunek 6.2 DHCP R2

R3

```
ip dhcp pool administracja
 network 192.168.2.24 255.255.255.248
 default-router 192.168.2.25
 dns-server 192.168.1.26
clock timezone CST -6
!
```

Rysunek 6.3 DHCP R3

7. Bezpieczeństwo sieci

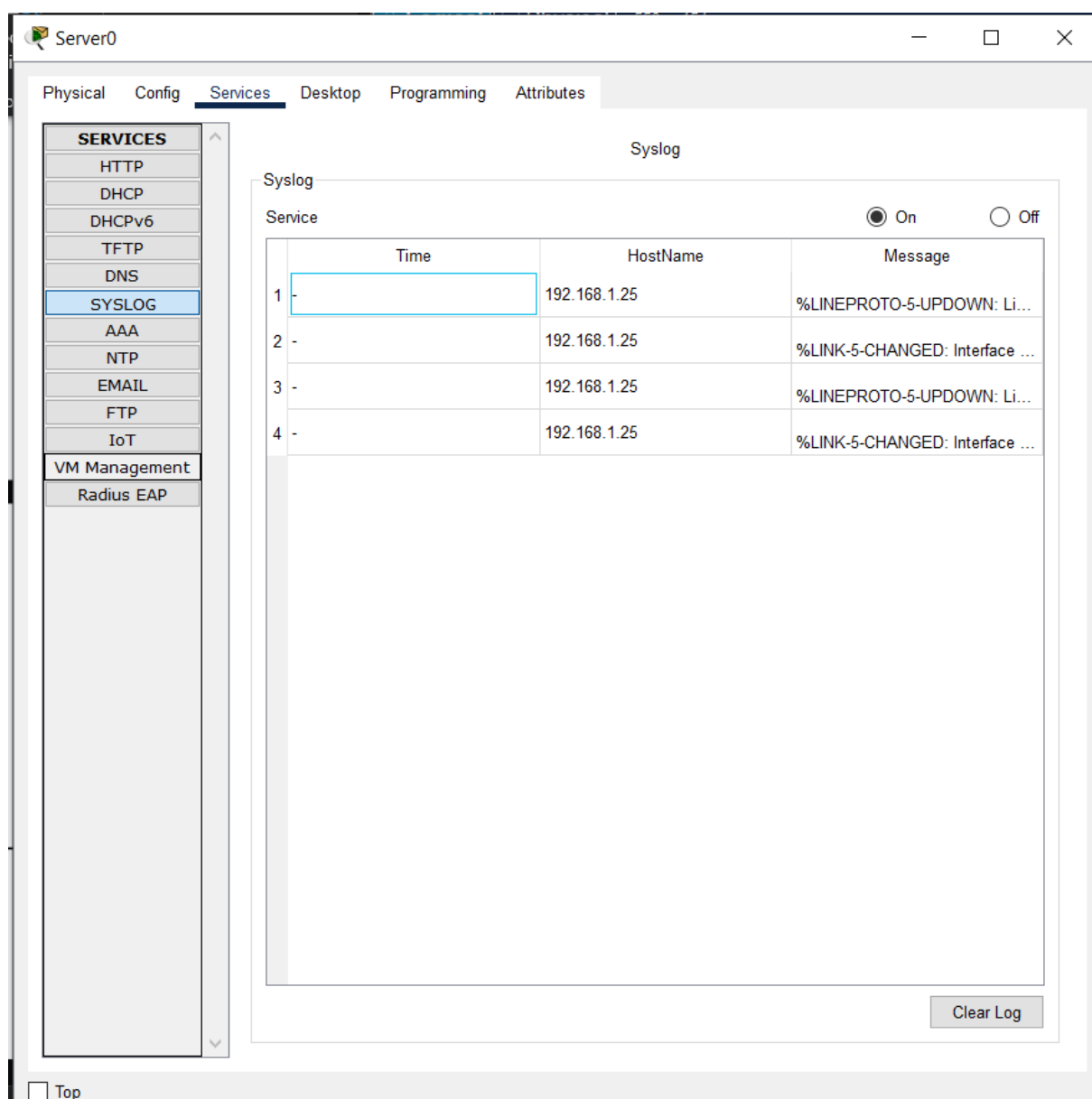
Radius

Próbujemy z R2 połączyć się z serwerem



Rysunek 7.1 Radius

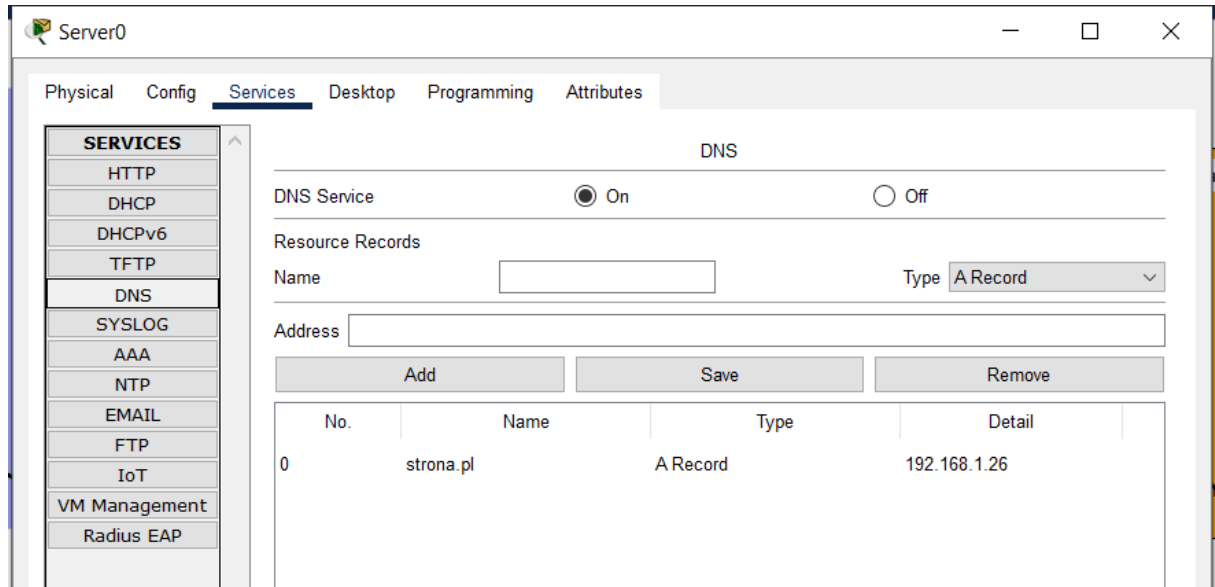
Sprawdzanie działania serwera Syslog



Rysunek 7.2 Syslog

DNS

Na serwerze pod adresem strona.pl uruchomiona jest usługa DNS. Widnieje strona przychodni pod adresem 192.168.1.26 lub nazwą DNS, czyli strona.pl.

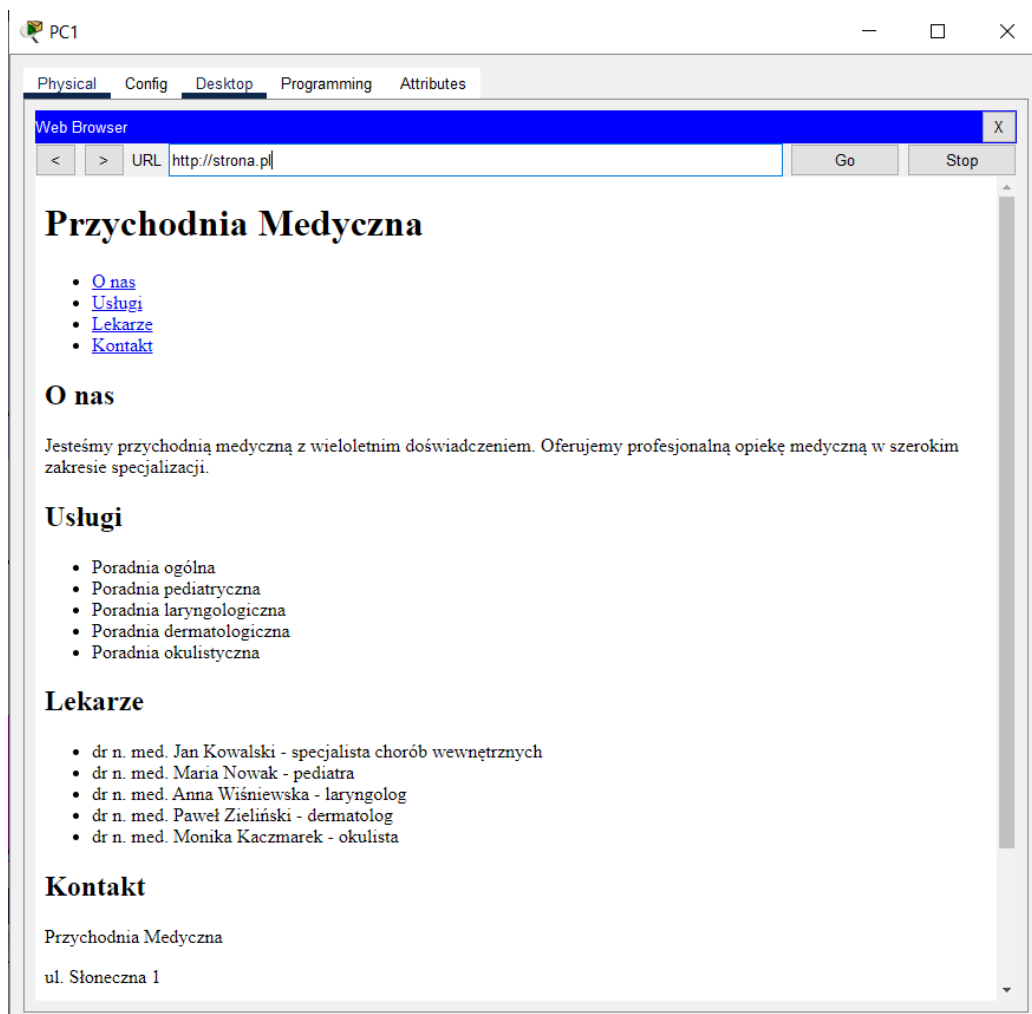


The screenshot shows the WinBox configuration window for 'Server0'. The 'Services' tab is selected, and the 'DNS' service is enabled. The 'Resource Records' section shows a single record for 'strona.pl' of type 'A Record' pointing to '192.168.1.26'.

No.	Name	Type	Detail
0	strona.pl	A Record	192.168.1.26

Rysunek 7.3 DNS - konfiguracja

Po wejściu na adres strona.pl widnieje taka strona.

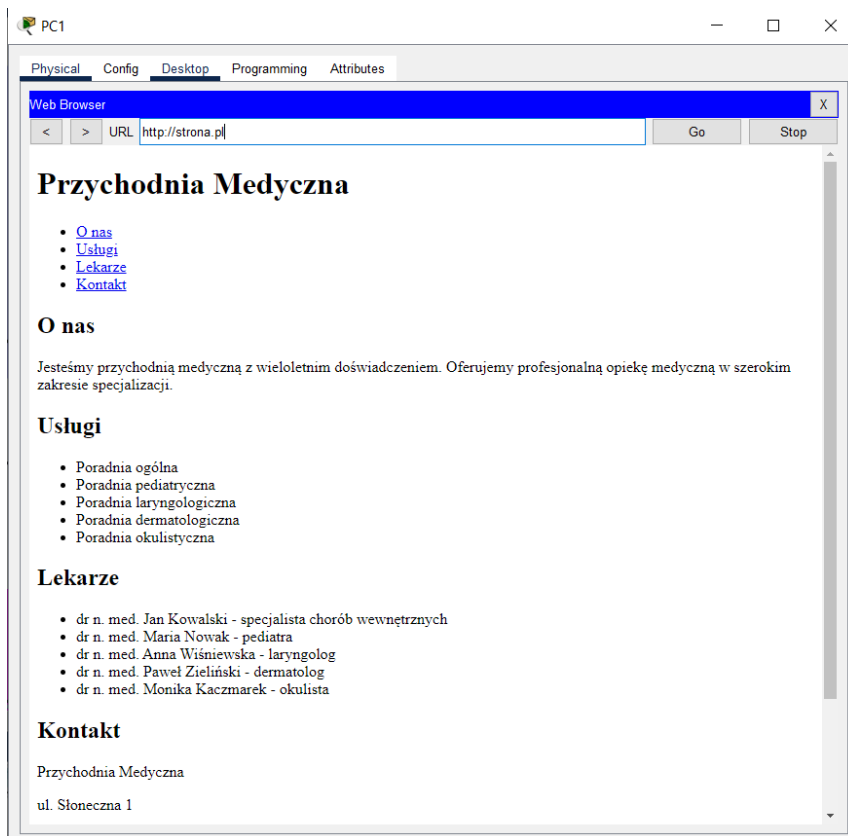


Rysunek 7.4 Uruchomiona strona

Firewall

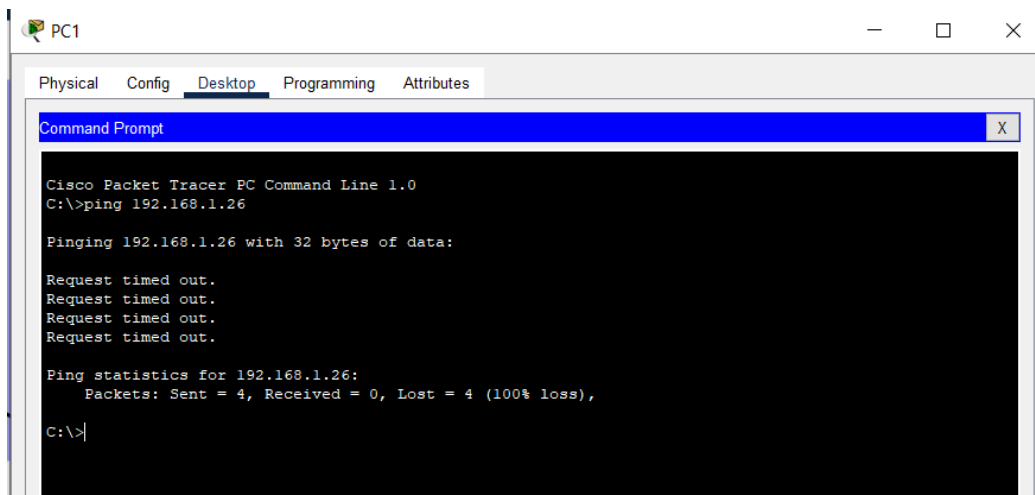
Na serwerze Server0 skonfigurowana jest usługa firewall. Oznacza to, że nikt nie może pingować serwera, jednak może korzystać z usług na nim uruchomionych, np. DNS.

Sprawdzamy więc poprawność. Z PC1 uruchamiamy stronę strona.pl.



Rysunek 7.5 Sprawdzenie działania firewall

A teraz spróbujmy użyć polecenia ping z PC1 do serwera.



Rysunek 7.6 Efekt działania firewall

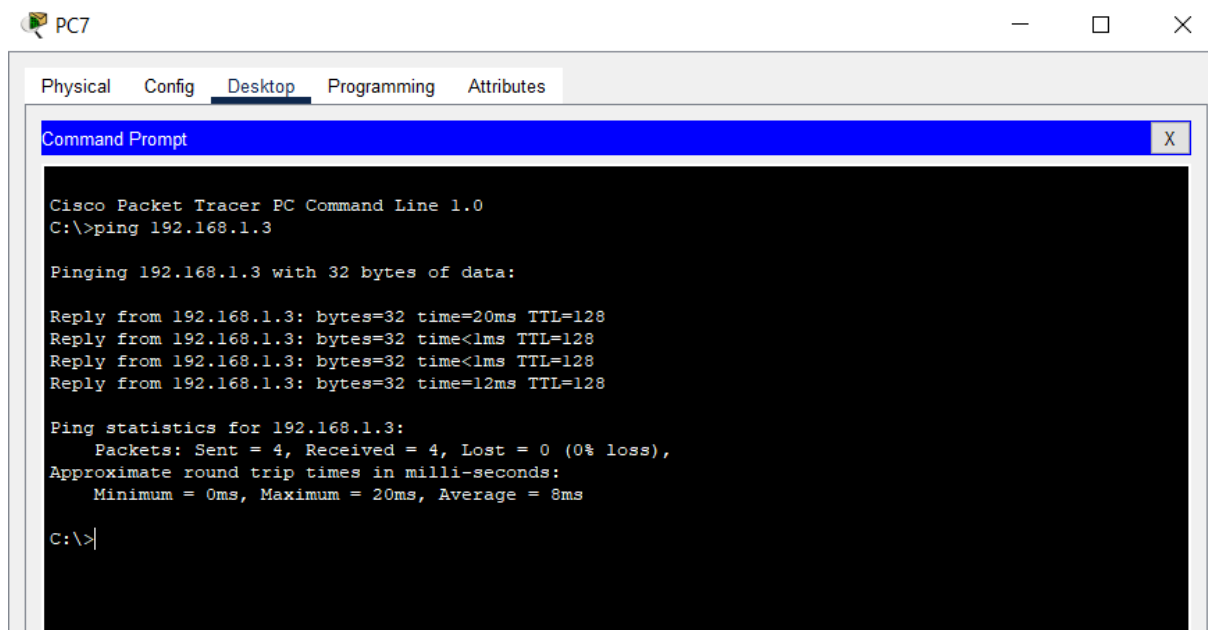
Jak widać konfiguracja działa poprawnie.

ACL

Na routerach zostały skonfigurowane listy ACL.

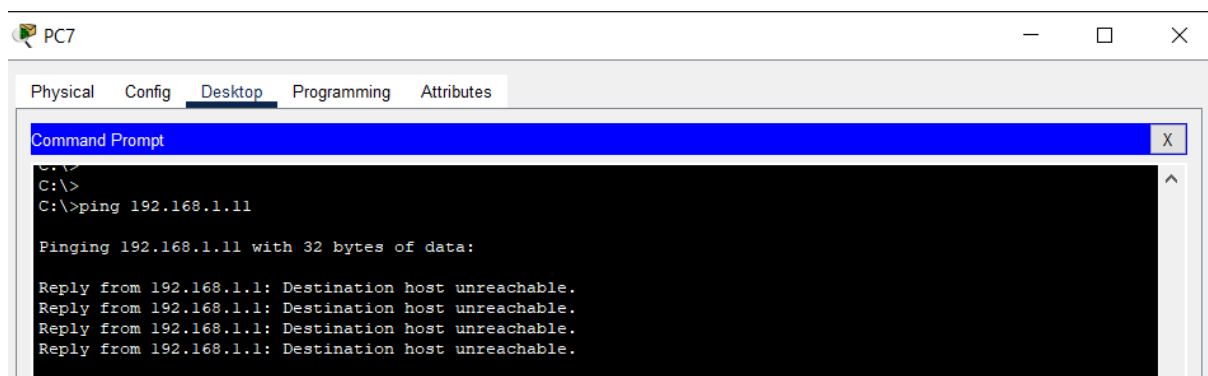
Ograniczenie dotyczy PC7, który nie może pingować się poza podsiecią, w której się znajduje.

Ping do PC6 znajdującego się w tej samej podsieci.



Rysunek 7.7 ACL - ta sama podsieć

Ping do PC1 znajdującego się poza podsiecią.



Rysunek 7.8 ACL - inna podsieć

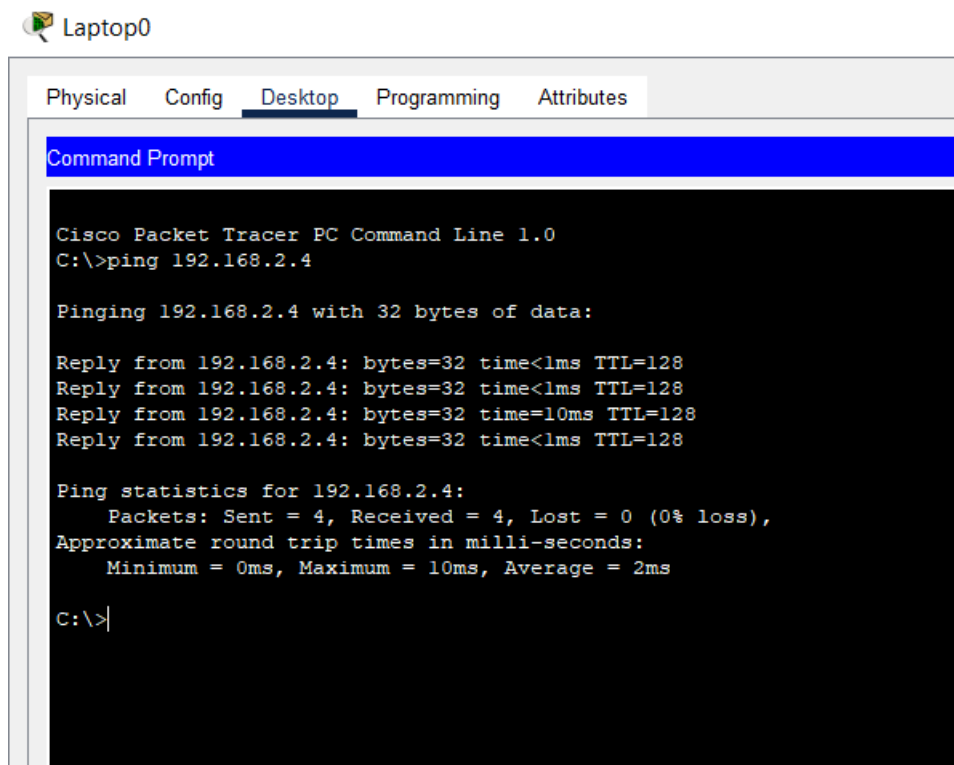
Jak widać lista ACL działa poprawnie.

Inną konfiguracją listy jest ograniczenie możliwości pingowania drukarki to tej samej podsieci.

Oznacza to, że komputery mogą pingować drukarkę w tej samej podsieci, jednak drukarkę znajdującą się w innej podsieci już nie.

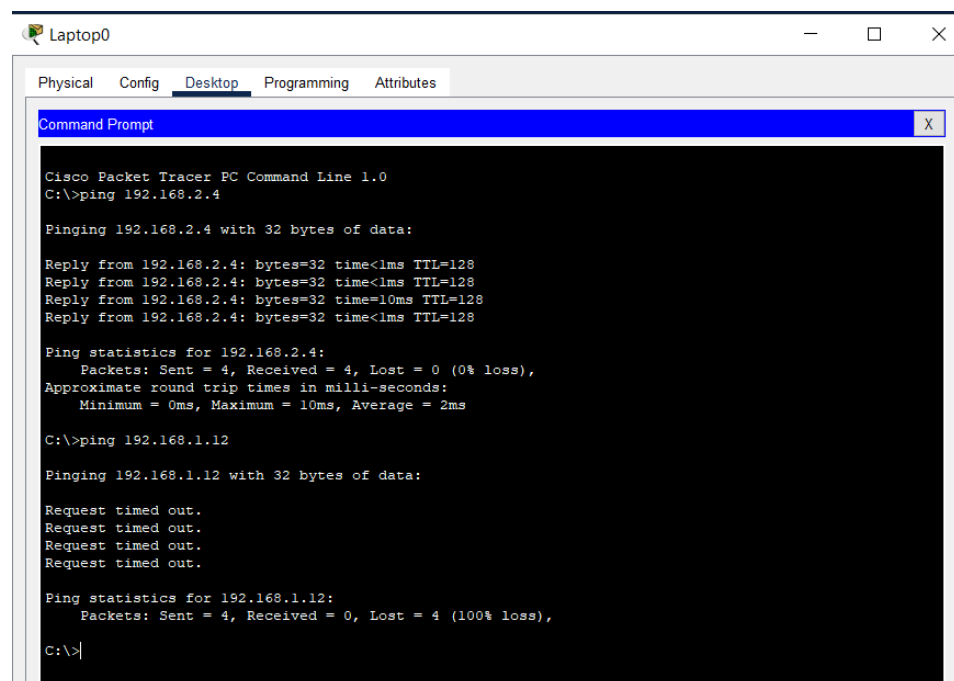
Wyberzmy dla przykładu Gabinet 2.

Pingujemy z Laptopa0 do Printer3.



Rysunek 7.9 ACL - drukarka w tej samej podsieci

Jak widać ping działa poprawnie. A teraz założmy, że z laptopa0 chcemy spingować Printer0 znajdującą się w Księgowości.



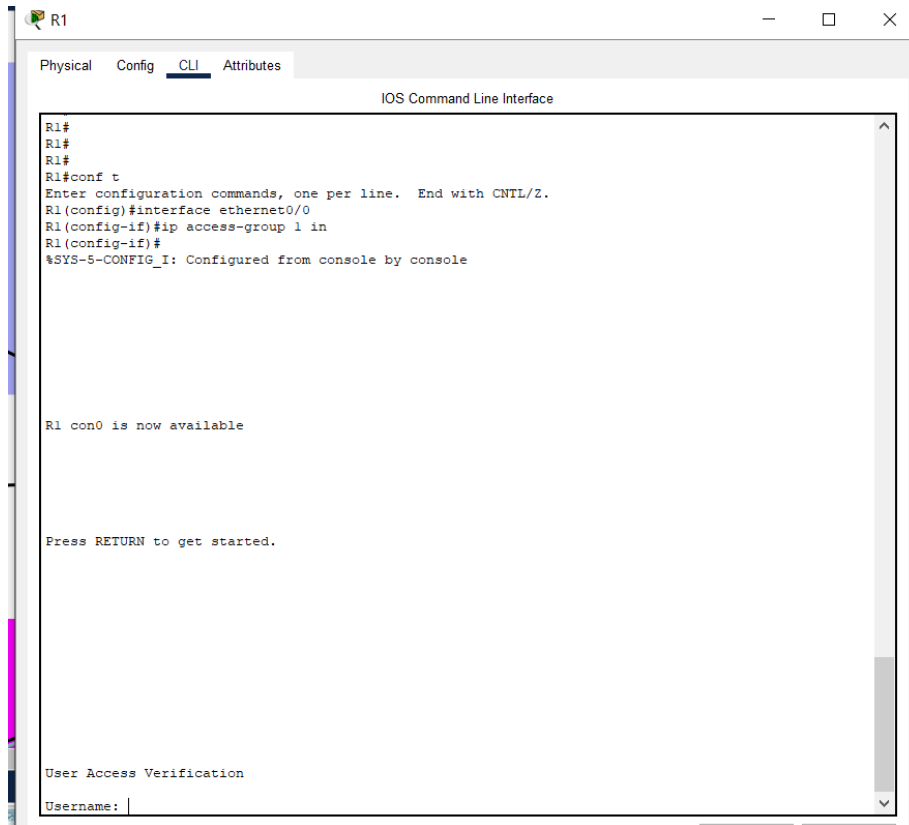
Rysunek 7.10 ACL - drukarka w innej podsieci

Jak widać ping jest nieosiągalny.

Tak samo ograniczenie analogicznie wygląda dla pozostałych drukarek.

Lista ACL 2 jak widać działa.

Logowanie do R1

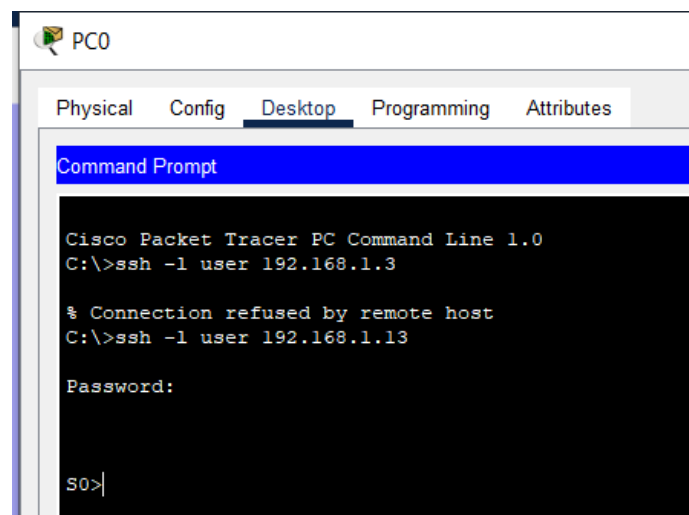


Rysunek 7.11 Zabezpieczenie dostępu

Logowanie do R1 zabezpieczone jest nazwą user i hasłem cisco.

SSH

Na switchach zostały skonfigurowane SSH.



Rysunek 7.12 SSH

Danymi do logowania jest user oraz hasło cisco.

NTP

Skonfigurowany został również serwer NTP.

Server0

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

marzec 2023 05:31:45PM

pon.	wt.	śr.	czw.	pt.	sob.	niedz.
27	28	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	31	1	2
3	4	5	6	7	8	9

☐ Top

Rysunek 7.13 NTP - konfiguracja

Sprawdzenie konfiguracji

```
---
R1#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.26
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E7A8B931.000003D5 (17:32:33.981 UTC Wed Mar 29 2023)
clock offset is 0.00 msec, root delay is 1.00 msec
root dispersion is 57.06 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 2 sec ago.
R1#
```

Rysunek 7.14 NTP - sprawdzenie

AAA

Skonfigurowano również AAA.

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

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

AAA

Service ☒ On ☐ Off Radius Port

Network Configuration

Client Name Client IP

Secret ServerType

	Client Name	Client IP	Server Type	Key	
1	R1	192.168.1.25	Radius	cisco	<input type="button" value="Add"/>

User Setup

Username Password

	Username	Password	
1	user	cisco	<input type="button" value="Add"/>

☐ Top

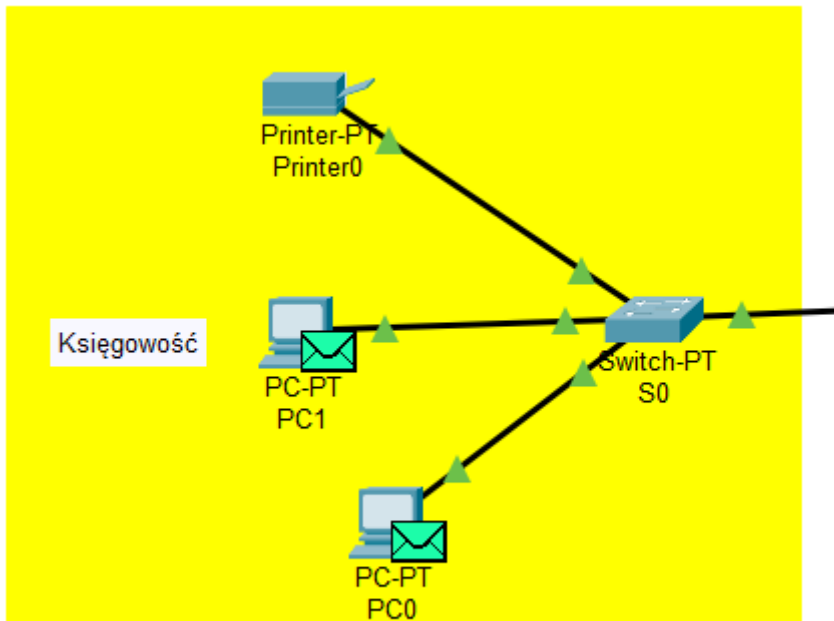
Rysunek 7.15 AAA

Port Monitor

```
S0(config)#monitor session 1 source interface FastEthernet3/1
S0(config)#monitor session 1 source interface FastEthernet1/1
S0(config)#monitor session 1 destination interface FastEthernet2/1
S0(config)#
```

Rysunek 7.16 Port monitor - konfiguracja

Wszystkie dane przychodzące do księgowości kopiowane są więc port FastEthernet2/1.



Rysunek 7.17 Port monitor - sprawdzenie działania

Jak widać konfiguracja działa poprawnie.

RIP

```
R2#show ip rip database
192.168.1.24/30    auto-summary
192.168.1.24/30
    [1] via 192.168.1.33, 00:00:01, Ethernet0/0
192.168.1.32/30    auto-summary
192.168.1.32/30    directly connected, Ethernet0/0
192.168.2.0/29     auto-summary
192.168.2.0/29     directly connected, Ethernet1/0
192.168.2.8/29     auto-summary
192.168.2.8/29     directly connected, Ethernet2/0
192.168.2.16/29    auto-summary
192.168.2.16/29    directly connected, Ethernet3/0
192.168.2.24/29    auto-summary
192.168.2.24/29
    [1] via 192.168.2.18, 00:00:24, Ethernet3/0
R2#
```

Rysunek 7.18 Konfiguracja RIP

OSPF

```
R2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.2.25	1	FULL/DR	00:00:39	192.168.2.18	Ethernet3/0
192.168.1.33	1	FULL/BDR	00:00:39	192.168.1.33	Ethernet0/0

Rysunek 7.19 Konfiguracja OSPF

STP

Zostały także uruchomione usługi portfast oraz BPDUGuard.

```
S7#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
    Root ID      Priority      32769
                Address        0002.1679.E298
                This bridge is the root
                Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID     Priority      32769 (priority 32768 sys-id-ext 1)
                Address        0002.1679.E298
                Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
                Aging Time 20

Interface        Role Sts Cost        Prio.Nbr Type
-----
Fa1/1            Desg FWD 19          128.2    P2p
Fa2/1            Desg FWD 19          128.3    P2p
```

Rysunek 7.20 STP

Etherchannel

```
S9#show etherchannel
Channel-group listing:
-----

Group: 1
-----
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol: -
S9#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Pol(SU)          -           Fa2/1(P) Fa3/1(P)
S9#
```

Rysunek 7.21 EtherChannel