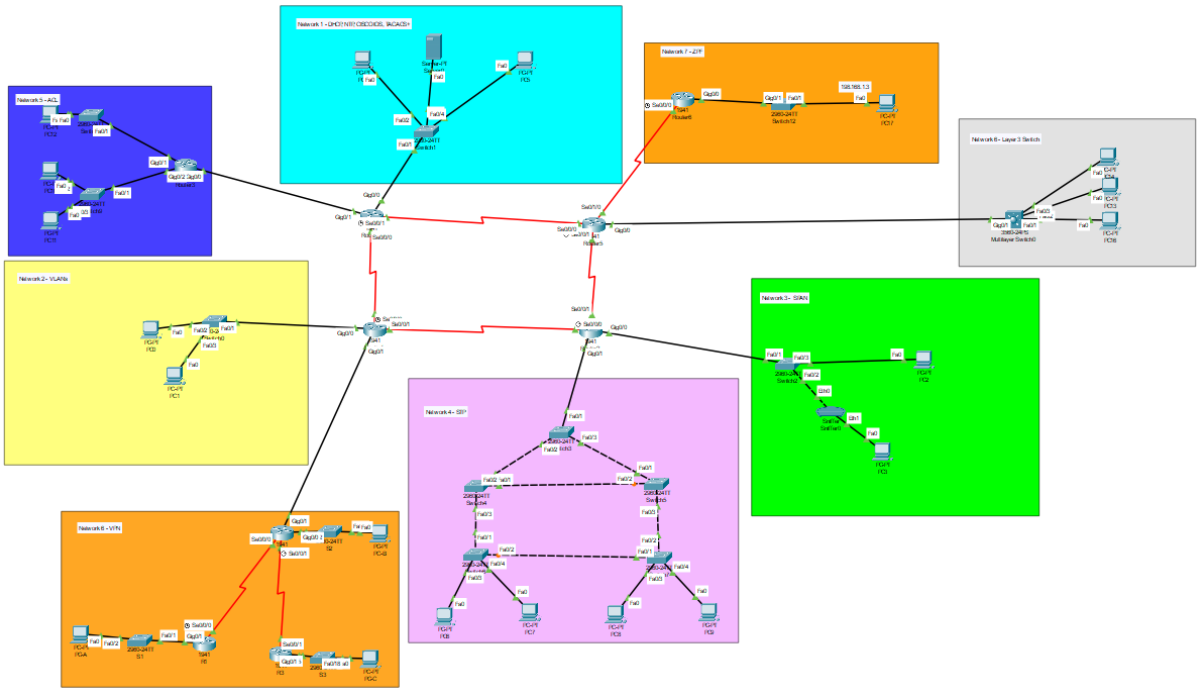
Politechnika Świętokrzyska w Kielcach

Wydział Elektrotechniki, Automatyki i Informatyki
Katedra Informatyki, Elektroniki i Elektrotechniki

Kierunek	Projekt	
Informatyka	**Wstęp do cyberbezpieczeństwa**	
Grupa dziekańska **1ID25A**	Wykonał: • **Arkadiusz Wolski** • **Bartosz Kasprzycki**	Temat: **Osiedle**

1. Struktura sieci



2. Tabele adresacji

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
PC0	Fa0	192.168.1.10	255.255.255.0	192.168.1.1
PC1	Fa0	192.168.2.10	255.255.255.0	192.168.2.2
Switch0	FastEthernet0/1	--	--	--
Switch0	FastEthernet0/2	--	--	--
Switch0	FastEthernet0/3	--	--	--
Router1	Gig0/0.10	192.168.1.1	255.255.255.0	--
Router1	Gig0/0.20	192.168.2.2	255.255.255.0	--

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
PC2	Fa0	194.168.1.3	255.255.255.0	194.168.1.1
PC3	Fa0	194.168.1.4	255.255.255.0	194.168.1.1
Switch2	VLAN 1	194.168.1.2	255.255.255.0	194.168.1.1
Router2	Gig0/0	194.168.1.1	255.255.255.0	--

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
PC4	Fa0	DHCP	255.255.255.0	DHCP
PC5	Fa0	DHCP	255.255.255.0	DHCP
Server0	Fa0	193.168.1.3	255.255.255.0	193.168.1.1
Switch1	VLAN 1	193.168.1.2	255.255.255.0	193.168.1.1
Router0	Gig0/0	193.168.1.1	255.255.255.0	--

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
Router1	Serial0/0/0	1.0.0.1	255.0.0.0	--
Router0	Serial0/0/0	1.0.0.2	255.0.0.0	--

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
Router5	Serial0/0/1	3.0.0.2	255.0.0.0	--
Router2	Serial0/0/1	3.0.0.1	255.0.0.0	--

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
Router2	Serial0/0/0	2.0.0.2	255.0.0.0	--
Router1	Serial0/0/1	2.0.0.1	255.0.0.0	--

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
Router5	Serial0/0/1	3.0.0.2	255.0.0.0	--
Router0	Serial0/0/1	3.0.0.1	255.0.0.0	--

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
PC6	Fa0	195.168.1.10	255.255.255.0	195.168.1.1
PC7	Fa0	195.168.1.11	255.255.255.0	195.168.1.1
PC8	Fa0	195.168.1.12	255.255.255.0	195.168.1.1
PC9	Fa0	195.168.1.13	255.255.255.0	195.168.1.1
Switch3	--	--	--	--
Switch4	--	--	--	--
Switch5	--	--	--	--
Switch6	--	--	--	--
Switch7	--	--	--	--
Router2	Gig0/1	195.168.1.1	255.255.255.0	--

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
PC10	Fa0	196.168.20.3	255.255.255.0	196.168.20.1
PC11	Fa0	196.168.20.4	255.255.255.0	196.168.20.1
PC12	Fa0	196.168.10.3	255.255.255.0	196.168.10.1
Switch8	--	--	--	--
Switch9	--	--	--	--
Router3	Gig0/1	196.168.10.1	255.255.255.0	--
Router3	Gig0/2	196.168.20.1	255.255.255.0	--

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
Router3	Se0/3/0	4.0.0.2	255.0.0.0	--
Router0	Se0/1/0	4.0.0.1	255.0.0.0	--

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
PC13	Fa0	172.16.31.3	255.255.255.0	172.16.31.1
PC14	Fa0	172.16.31.4	255.255.255.0	172.16.31.1
PC16	Fa0	172.16.31.2	255.255.255.0	172.16.31.1
Multilayer Switch0	GigabitEthernet0/1	197.168.1.2	255.255.255.0	--
Multilayer Switch0	Vlan1	172.16.31.1	255.255.255.0	--
Router5	Gig0/0	197.168.1.1	255.255.255.0	--

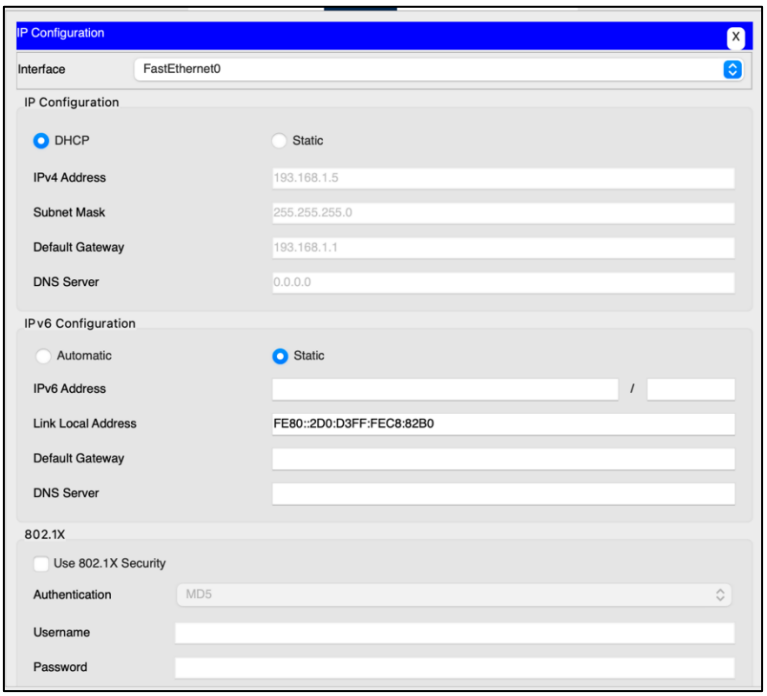
Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
PC17	Fa0	198.168.1.3	255.255.255.0	198.168.1.1
Switch12	--	--	--	--
Router6	Gig0/0	198.168.1.1	255.255.255.0	--
Router6	Se0/0/0	7.0.0.2	255.0.0.0	--
Router5	Se0/1/0	7.0.0.1	255.0.0.0	--

Sprzęt	Interfejs	Adres IP	Maska	Brama wyjściowa
PC-A	Fa0	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	Fa0	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	Fa0	192.168.3.3	255.255.255.0	192.168.3.1
S1	--	--	--	--
S2	--	--	--	--
S3	--	--	--	--
R1	Gig0/1	192.168.1.1	255.255.255.0	--
R1	Se0/0/0	10.1.1.2	255.255.255.252	--
R2	Gig0/0	192.168.2.1	255.255.255.0	--
R2	Se0/1/0	6.0.0.2	255.0.0.0	--
R2	Serial0/0/0	10.1.1.1	255.255.255.252	--
R2	Serial0/0/1	10.2.2.1	255.255.255.252	--
R3	Gig0/1	192.168.3.1	255.255.255.0	--
R3	Se0/0/1	10.2.2.2	255.255.255.252	--
Router1	Se0/1/0	6.0.0.1	255.0.0.0	--

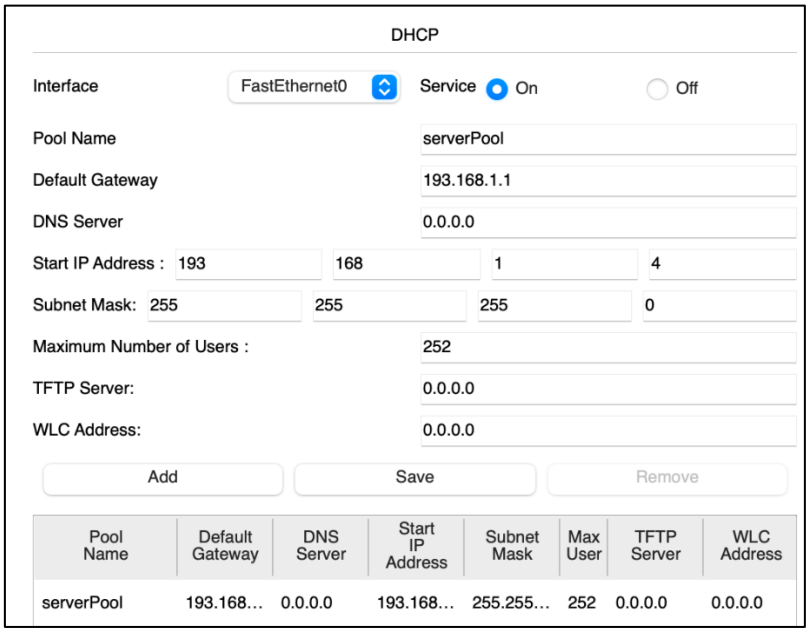
3. Konfiguracja urządzeń

3.1. DHCP

Serwer w podsieci *Network 1* został skonfigurowany tak, by przydzielać komputerom adresy z puli adresów przy pomocy protokołu DHCP. Poniżej przedstawiono przykładowy adres IP hosta uzyskany z wykorzystaniem protokołu DHCP.



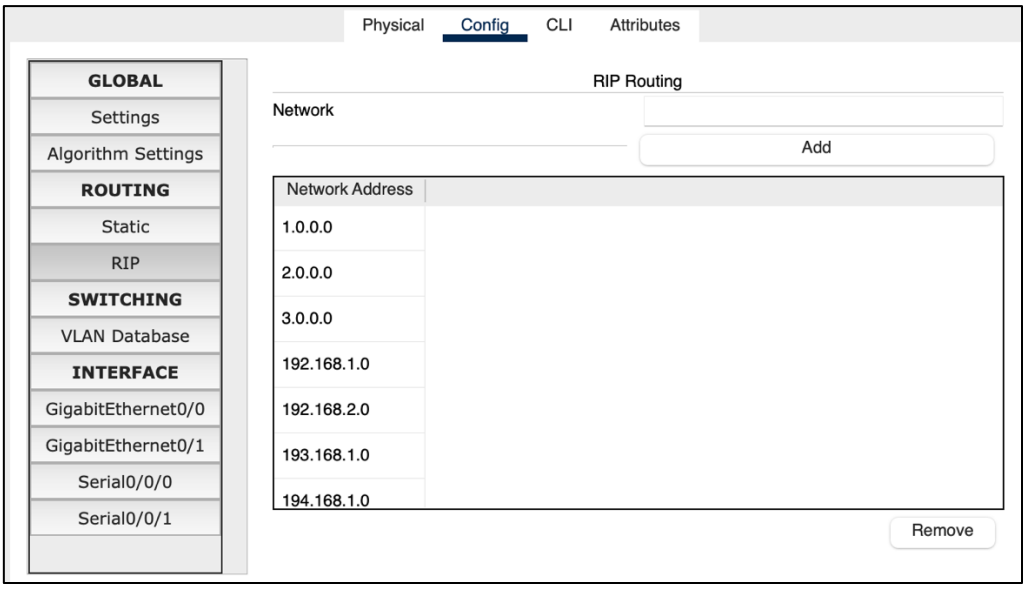
Rys. 3.1. Przykład działania protokołu DHCP dla hosta



Rys. 3.2. Przykładowa konfiguracja protokołu DHCP

3.2. RIP

Routery wykorzystują protokół RIP do obliczania najlepszej trasy do celu dla pakietów danych. Przykładowa konfiguracja protokołu RIP została zaprezentowana poniżej.



Rys. 3.3. Przykładowa konfiguracja protokołu RIP

3.3. Zabezpieczenia

Na Routerach i Switch-ach w podsieciach: *Network 1, Network 2, Network 6* zabezpieczony został dostęp do trybu uprzywilejowanego oraz do portów konsolowych i wirtualnych terminali. Dodatkowo, hasła zostały zaszyfrowane, by uniknąć ich przechowywania w formie jawnej. Dla celów tego projektu, hasła w *Network 1* i *Network 2* to: **cisco**. Poniżej przedstawiono przykładową konfigurację zabezpieczeń. *W Network 6* do *console line* hasło to ciscoconpa55, dla linii vty ciscovtypa55, dla trybu uprzywilejowanego enable ciscoenpa55.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#service password-encryption
Switch(config)#enable password cisco
Switch(config)#line console 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Rys. 3.4. Przykładowa konfiguracja zabezpieczeń

3.4. VLAN-y

W podsieci *Network 2* zostały stworzone dwa VLAN-y: VLAN 10 i VLAN 20. Jeden komputer o adresie IP 192.168.1.10 jest w VLAN-ie 10, natomiast drugi komputer o adresie IP 192.168.2.10 jest w VLAN-ie 20. Pierwszy komputer ma bramę 192.168.1.1, natomiast drugi 192.168.2.2. Kabel, który łączy switch z routerem jest trunkingowy, co oznacza, że należy do wszystkich VLAN-ów. Na routerze interfejs podłączony do switcha skonfigurowano tak, że dla VLAN-u 10 ma adres IP 192.168.1.1, a dla VLAN-u 20 192.168.2.2. Przedstawiono konfigurację adresów na routerze na rysunku poniżej. Na drugim rysunku przedstawiono utworzone VLAN-y na switchu.

```
Device Name: Router1
Device Model: 1941
Hostname: Router

Port                  Link   VLAN   IP Address        IPv6 Address                            MAC Address
GigabitEthernet0/0    Up     --     <not set>         <not set>                               0001.4277.A101
GigabitEthernet0/0.10 Up     --     192.168.1.1/24    <not set>                               0001.4277.A101
GigabitEthernet0/0.20 Up     --     192.168.2.2/24    <not set>                               0001.4277.A101
GigabitEthernet0/1    Down   --     <not set>         <not set>                               0001.4277.A102
Serial0/0/0           Up     --     1.0.0.1/8         <not set>                               <not set>
Serial0/0/1           Up     --     2.0.0.1/8         <not set>                               <not set>
Vlan1                 Down   1      <not set>         <not set>                               0040.0B18.80B7

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router1
```

Rys. 3.5. Konfiguracja adresów na routerze

VLAN No	VLAN Name
1	default
10	HR
20	IT
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

Rys. 3.6. VLAN-y na switchu

3.5. Konfiguracja urządzeń pod kątem dostępu SSH

Do wykonania konfiguracji urządzeń pod kątem dostępu do SSH wybraliśmy urządzenia: *Router2* oraz *Swtich1*.

W przypadku routera jak i switcha konfiguracja wyglądała bardzo podobnie. Na początku określona została nazwa domeny, po czym utworzony został użytkownik z loginem ***cisco*** i zaszyfrowanym hasłem ***cisco.*** Następnie utworzony został 1024-bitowy klucz RSA. W kolejnym kroku wykonana została konfiguracja linii VTY w celu umożliwienia dostępu do urządzeń z wykorzystaniem SSH z wykorzystaniem danych utworzonego wcześniej użytkownika. Poniżej przedstawiona została szczegółowa konfiguracja routera oraz switcha.

```
Router2(config)#ip domain-name router2
Router2(config)#username cisco secret cisco
Router2(config)#crypto key generate rsa g
Router2(config)#crypto key generate rsa general-keys mo
Router2(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Router2.router2

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:2:21.590: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router2(config)#line vty 0 4
Router2(config-line)#transport input ssh
Router2(config-line)#login local
Router2(config-line)#
```

Rys. 3.5. Konfiguracja routera pod kątem dostepu SSH

```
Switch1(config)#ip domain-name switch1
Switch1(config)#crypto key generate rsa ge
Switch1(config)#crypto key generate rsa general-keys mo
Switch1(config)#crypto key generate rsa general-keys modulus 1024
% You already have RSA keys defined named Switch1.switch1
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Apr 12 22:10:59.780: %SSH-5-ENABLED: SSH 1.99 has been enabled
Switch1(config)#username cisco secret cisco
Switch1(config)#line vty 0 15
Switch1(config-line)#transport input ssh
Switch1(config-line)#login local
Switch1(config-line)#
```

Rys. 3.6. Konfiguracja switcha pod kątem dostępu SSH

```
Command Prompt                                                    X

Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l cisco 193.168.1.2

Password:



Switch1>
```

Rys. 3.7. Logowanie poprzez SSH do switcha

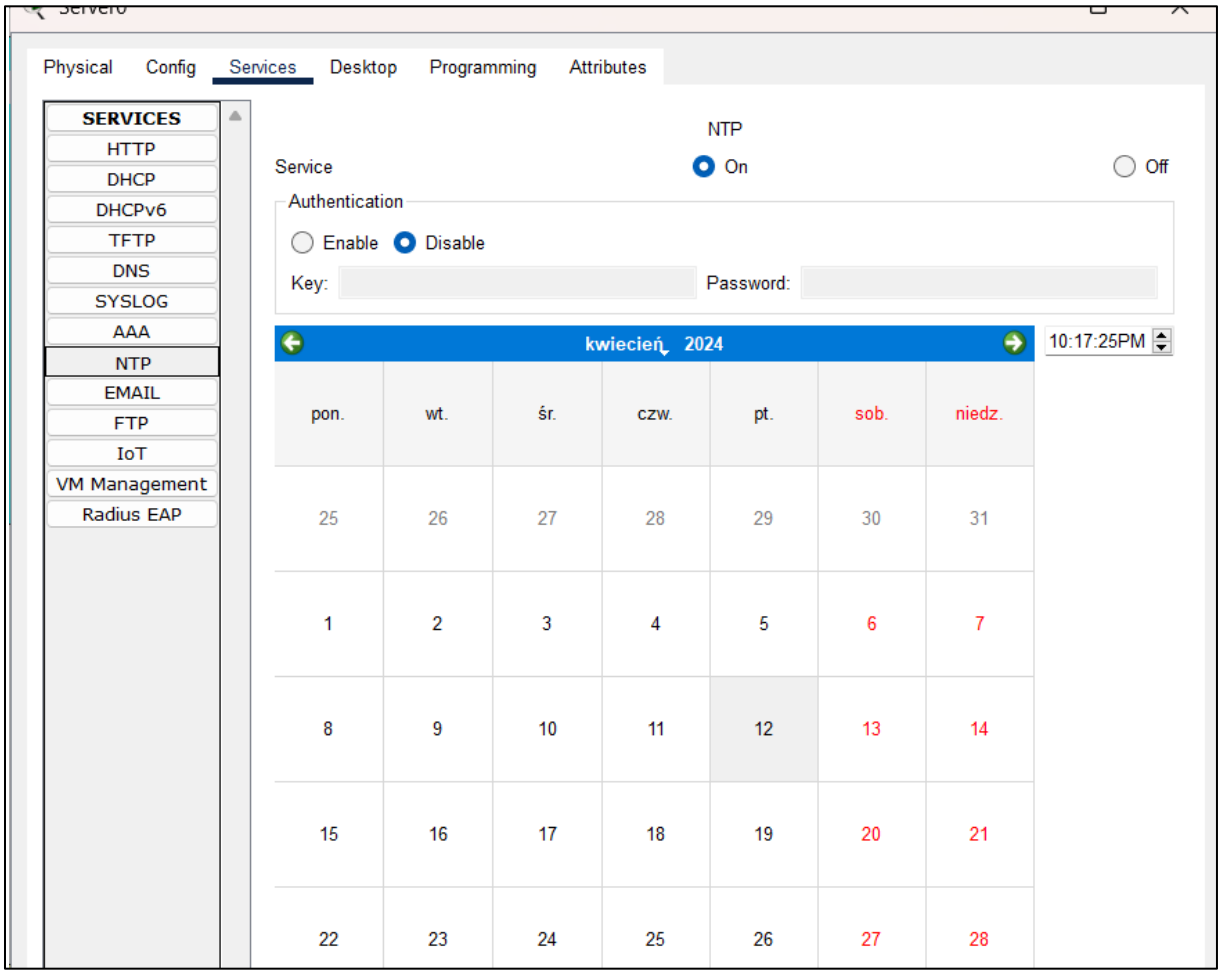
Rys. 3.8. Logowanie poprzez SSH do routera

3.6. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS

Konfiguracja NTP oraz CISCO IOS również wykonana została na urządzeniach *Router0* oraz *Switch1* znajdujących się w sieci *Network1*.

3.6.1. Konfiguracja NTP

Na początku na serwerze włączona została usługa NTP oraz ustawiony został aktualny czas.



Rys. 3.9. Włączenie usługi NTP

Następnie na routerze jak i na switchu określony został adres ip serwera ntp wraz z konfiguracją logowania pod kątem dołączania znaczników czasu zawierających datę, godzinę

oraz milisekundy.

```
Router0(config)#ntp server 193.168.1.3
Router0(config)#service time
Router0(config)#service timestamps log d
Router0(config)#service timestamps log datetime m
Router0(config)#service timestamps log datetime msec
Router0(config)#interface loopback 0

Router0(config-if)#
*Mar 01, 00:21:39.2121: %LINK-5-CHANGED: Interface Loopback0, changed state to up
*Mar 01, 00:21:39.2121: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to
up
Router0(config-if)#no shutdown
Router0(config-if)#shutdown

Router0(config-if)#
*Mar 01, 00:22:06.2222: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively
down
*Mar 01, 00:22:06.2222: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to
down
Router0(config-if)#
```

Rys. 3.10. Konfiguracja NTP na routerze

```
Router0#show clock
22:29:42.70 UTC Fri Apr 12 2024
Router0#
```

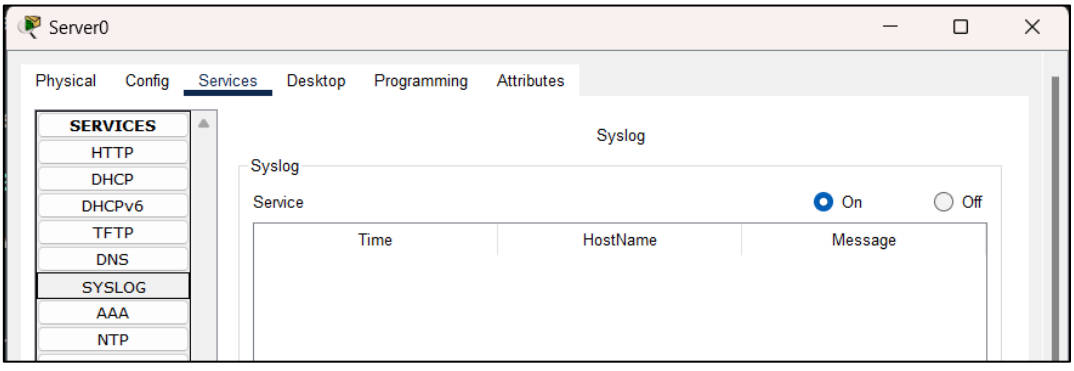
Rys. 3.11. Konfiguracja NTP na routerze (czas)

```
Switch1(config)#ntp server 193.168.1.3
Switch1(config)#service timestamps log
Switch1(config)#service timestamps log da
Switch1(config)#service timestamps log datetime m
Switch1(config)#service timestamps log datetime msec
Switch1(config)#exit
Switch1#
*Apr 12, 22:24:48.2424: SYS-5-CONFIG_I: Configured from console by console
Switch1#show clock
22:24:52.135 UTC Fri Apr 12 2024
Switch1#
```

Rys. 3.12. Konfiguracja NTP na switchu

3.6.2. Konfiguracja CISCO IOS

Podobnie, jak w przypadku konfiguracji NTP, pierwszym krokiem było włączenie usługi CISCO IOS na serwerze.



Rys. 3.13. Włączenie usługi CISCO IOS

Następnie, z wykorzystaniem komendy *logging* na routerze oraz switchu określony został adres serwera z włączoną usługą logowania.

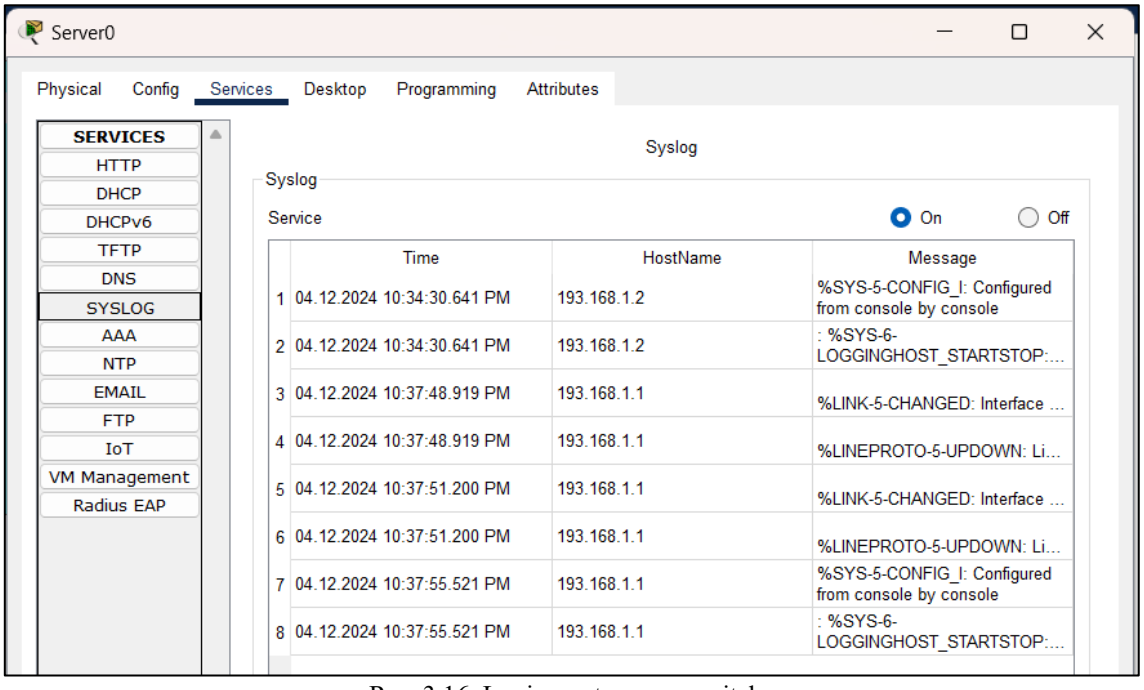
```
Switch1(config)#logging 193.168.1.3
Switch1(config)#exit
Switch1#
*Apr 12, 22:34:30.3434: SYS-5-CONFIG_I: Configured from console by console
*Apr 12, 22:34:30.3434:  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 193.168.1.3 port 514 started
- CLI initiatede
```

Rys. 3.14. Konfiguracja CISCO IOS na switchu

```
Router0(config)#logging 193.168.1.3
Router0(config)#interface loop
Router0(config)#interface loopback 0
Router0(config-if)#no shutdown

Router0(config-if)#
*Apr 12, 22:37:48.3737: %LINK-5-CHANGED: Interface Loopback0, changed state to up
*Apr 12, 22:37:48.3737: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to
up
Router0(config-if)#shutdown

Router0(config-if)#
*Apr 12, 22:37:51.3737: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively
down
*Apr 12, 22:37:51.3737: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to
down
Router0(config-if)#exit
Router0(config)#exit
Router0#
*Apr 12, 22:37:55.3737: SYS-5-CONFIG_I: Configured from console by console
*Apr 12, 22:37:55.3737:  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 193.168.1.3 port 514 started
- CLI initiated
Router0#
```

Rys. 3.15. Konfiguracja CISCO IOS na routerze

Poniżej przedstawione zostały logi pochodzące z routera oraz switcha.



Rys. 3.16. Logi z routera oraz switcha

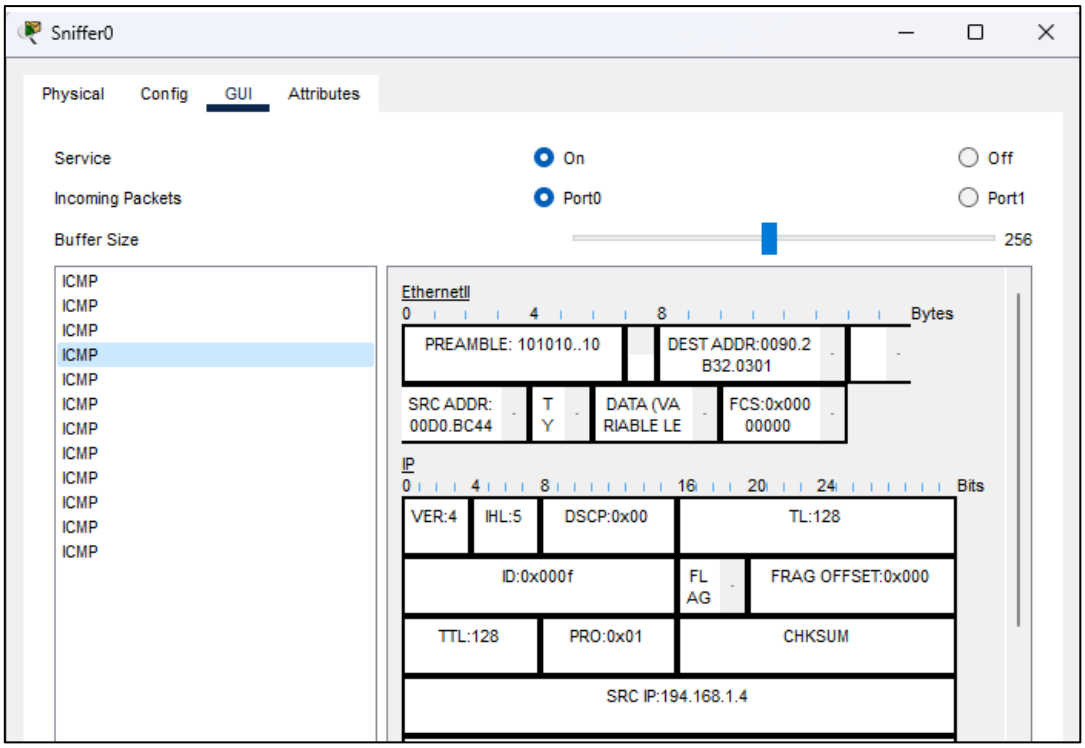
3.7. Implementacja lokalnego SPAN

Konfiguracja lokalnego SPAN wykonana została w sieci *Network 3*. Switch2 został skonfigurowany tak, by ruch z portu FastEthernet 0/1 był kopiowany i przesyłany na port FastEthernet 0/2.

```
Switch2(config)#monitor session 1 source interface f
Switch2(config)#monitor session 1 source interface fastEthernet 0/1
Switch2(config)#monitor session 1 destination inter
Switch2(config)#monitor session 1 destination interface f
Switch2(config)#monitor session 1 destination interface fastEthernet 0/2
Switch2(config)#exit
Switch2#
%SYS-5-CONFIG_I: Configured from console by console

Switch2#show monitor session 1
Session 1
---------
Type                   : Local Session
Description            : -
Source Ports           :
    Both               : Fa0/1
Destination Ports      : Fa0/2
    Encapsulation      : Native
          Ingress      : Disabled


Switch2#
```

Rys. 3.17. Konfiguracja lokalnego SPAN

Poniżej zaprezentowano pakiety przechwycone przez Sniffera prezentujące działanie STP.



Rys. 3.18. Pakiety przechwycone przez Sniffera

3.8. Implementacja listy kontroli ACL wewnątrz zabezpieczonej sieci

Najpierw tworzona jest lista kontroli ACL. „Permit icmp any any", która zezwala na cały ruch ICMP w sieci. „Deny ip any 196.168.10.0 0.0.0.255" blokuje cały ruch IP do tej sieci. „Deny ip 196.168.10.0 0.0.0.255 any" blokuje cały ruch z tej sieci do dowolnego celu. „Permit ip any any" zezwala na cały pozostały ruch. Następnie do interfejsów są przypisywane listy ACL, aby kontrolować na nich ruch.

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit icmp any any
Router(config)#access-list 100 deny ip any 196.168.10.0 0.0.0.255
Router(config)#access-list 100 deny ip 196.168.10.0 0.0.0.255 any
Router(config)#access-list 100 permit ip any any
Router(config)#
Router(config)#interface GigabitEthernet0/2
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/2
Router(config-if)#ip access-group 100 in
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/2
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#
```

Rys. 3.7 Ustawianie list kontrolnych

3.9. Implementacja zabezpieczeń STP

Na początku konfiguracji zabezpieczenia STP jako główny węzeł drzewa(*root*) wybrano urządzenie *Switch3*, natomiast jako root-primary wybrano *Switch4*.

```
Switch3(config)#spanning-tree vlan 1 root primary
Switch3(config)#
```

Rys. 3.19. Konfiguracja urządzenia Switch3 jako głównego węzła drzewa

```
Switch4(config)#spanning-tree vlan 1 root secondary
Switch4(config)#
```

Rys. 3.20. Konfiguracja urządzenia Switch4 jako root-secondary

Następnie wykonano konfiguracje zabezpieczającą przed atakami manipulacyjnymi STP, polegające na ustawieniu funkcji *PortFast* oraz *BPDU Guard* na urządzeniach *Switch6* oraz *Switch7*. Dodatkowo, na głównych węzłach drzewa ustawiony został *Root Guard*.

```
Switch6(config)#int range f0/3-4
Switch6(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/3 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
Switch6(config-if-range)#spanning-tree bpduguard enable
Switch6(config-if-range)#
```

Rys. 3.21. Konfiguracja PortFast oraz BPDU Guard na urządzeniu Switch6

```
Switch7(config)#int range f0/3-4
Switch7(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/3 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
Switch7(config-if-range)#spanning-tree bpduguard enable
Switch7(config-if-range)#
```

Rys. 3.22. Konfiguracja PortFast oraz BPDU Guard na urządzeni Switch7

```
Switch4(config)#int range f0/2-3
Switch4(config-if-range)#spanning-tree guard root
Switch4(config-if-range)#
```

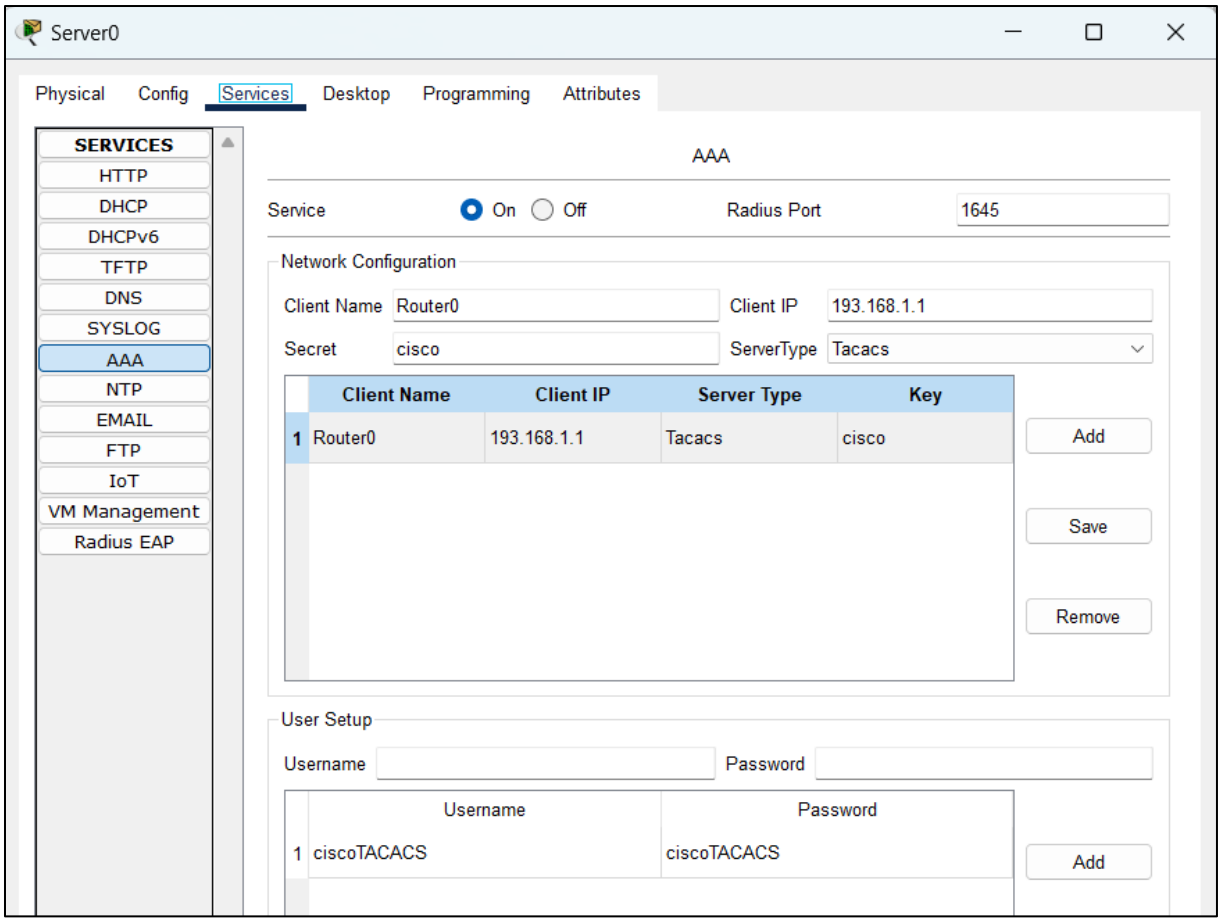
Rys. 3.23. Konfiguracja Root Guard na urządzeniu Switch4

```
Switch5(config)#int f0/3
Switch5(config-if)#spanning-tree guard root
Switch5(config-if)#
```

Rys. 3.24. Konfiguracja Root Guard na urządzeniu Switch5

3.10. Konfiguracja uwierzytelniania AAA na serwerze przy użyciu TACACS+

Pierwszym krokiem podczas konfigurowania uwierzytelniania AAA przy użyciu TACACS+ było włączenie tej usługi na serwerze w podcięci *Network 1* oraz utworzenie wpisu dotyczącego routera, który ma być zabezpieczony, oraz danych do logowania: **ciscoTacacs**.



Rys. 3.25. Konfiguracja uwierzytelniania AAA przy użyciu TACACS+ na serwerze.

Następne kroki konfiguracyjne dotyczyły *Routera0*, i polegały na włączeniu uwierzytelniania AAA, określeniu serwera TACACS+ oraz włączenia logowania z wykorzystaniem TACACS+.

```
Router0(config)#tacacs-se
Router0(config)#tacacs-server ho
Router0(config)#tacacs-server host 192.168.3.1
Router0(config)#tacacs-server key ci
Router0(config)#tacacs-server key cisco
Router0(config)#aaa ne
Router0(config)#aaa new-model
Router0(config)#aaa au
Router0(config)#aaa authentica
Router0(config)#aaa authentication login de
Router0(config)#aaa authentication login default gr
Router0(config)#aaa authentication login default group taca
Router0(config)#aaa authentication login default group tacacs+ lo
Router0(config)#aaa authentication login default group tacacs+ local
Router0(config)#line console 0
Router0(config-line)#login authen
Router0(config-line)#login authentication def
Router0(config-line)#login authentication default
Router0(config-line)#
```

Rys. 3.26. Konfiguracja TACACS+ na routerze

Po wykonaniu tych kroków dostęp do routera wymaga podania danych uwierzytelniających określonych podczas konfiguracji.

```
User Access Verification

Username: ciscoTACACS
Password:
Router0>
```

Rys. 3.27. Zabezpieczony dostęp wykorzystujący TACACS+

3.11. Zaprojektowanie zapory sieciowej typu ZPF

Pierwszym krokiem podczas tworzenia zapory sieciowej typu ZPF było utworzenie dwóch stref: wewnętrznej i zewnętrznej.

```
Router6(config)#zone security IN-ZONE
Router6(config-sec-zone)#exit
Router6(config)#zone security OUT-ZONE
Router6(config-sec-zone)#exit
```

Rys. 3.28. Tworzenie stref

Następnie utworzona została lista kontroli pozwalająca na ruch wychodzący z sieci wewnętrznej do sieci zewnętrznych.

```
Router6(config)#access-list 101 permit ip 198.168.1.0 0.0.0.255 any
```

Rys. 3.29. Lista kontroli określająca zasady ruchu sieci wewnętrznej

W kolejnym kroku tworzony jest klasyfikator ruchu typu class-map definiujący cały ruch związany z ruchem bazującym na wcześniej zdefiniowanej liście kontroli ACL. Na tej podstawie tworzona jest mapa zasad policy-map, określającą kontrolę dostępu opartą na kontekście dla określonego ruchu sieciowego.

```
Router6(config)#class-map type inspect match-all IN-NET-CLASS-MAP
Router6(config-cmap)#match access-group 101
Router6(config-cmap)#exit
```

Rys. 3.30. Utworzenie klasyfikatora ruchu typu class-map

```
Router6(config)#policy-map type inspect IN-2-OUT-PMAP
Router6(config-pmap)#class type inspect IN-NET-CLASS-MAP
Router6(config-pmap-c)#inspect
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols will be
inspected
Router6(config-pmap-c)#exit
Router6(config-pmap)#exit
```

Rys. 3.31. Tworzenie mapy zasad policy-map

Ostatnim krokiem jest zastosowanie zapory poprzez określenie pary stref, przypisanie mapy zasad zajmującej się ruchem pomiędzy strefami oraz przypisanie interfejsów do poszczególnych stref.

```
Router6(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
Router6(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
Router6(config-sec-zone-pair)#exit
```

Rys. 3.32. Utworzenie pary stref i przypisanie zasad obsługi ruchu

```
Router6(config-if)#zone-member security IN-ZONE
Router6(config-if)#exit
Router6(config)#
Router6(config)#int s0/0/0
Router6(config-if)#zone-member security OUT-ZONE
Router6(config-if)#exit
```

Rys. 3.33. Przypisanie interfejsów do poszczególnych stref

3.12. Konfiguracja i weryfikacja sieci VPN IPsec

Na routerze R1 najpierw utworzono listę ACL 110, która zezwala na ruch z sieci 192.168.1.0 do 192.168.3.0. Utworzono politykę ISAKMP z numerem 10 i ustawiono szyfrowanie AES 256-bitowe. Następnie ustawiono uwierzytelnianie przy użyciu pre-shared key i ustawiono grupę Diffie-Hellman 5 dla wymiany kluczy. Ustawiono pre-shared key „vpnpa55" dla peer o adresie 10.2.2.2. Utworzono zestaw transformacji IPsec nazwany „VPN-SET", który używa szyfrowanie AES i uwierzytelnianie HMAC-SHA. Utworzono mapę kryptograficzną „VPN-MAP" z numerem sekwencji 10 używającą IPsec z ISAKMP. Ustawiono adres drugiej strony połączenia na 10.2.2.2. Przypisano zestaw transformacji „VPN-SET: do mapy kryptograficznej. Ustawiono dopasowanie ruchu IP zgodnie z ACL 110. Przypisano mapę kryptogradiczną do interfejsu S0/0/0.

Na routerze R3 podjęto podobne kroki, jednak z pewnymi różnicami takimi jak: ACL zezwala na ruch z sieci 192.168.3.0 do sieci 192.168.1.0, użyto adresu peer 10.1.1.2 zamiast 10.2.2.2 i przypisano mapę kryptograficzną do interfejsu S0/0/1 zamiast S0/0/0.

```
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2
R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#interface s0/0/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

Rys. 3.34. Konfiguracja routera R1

```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#interface s0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#
```

Rys. 3.35. Konfiguracja routera R3

3.13. Przełącznik warstwy trzeciej

Pierwszym krokiem podczas konfigurowania przełącznika warstwy trzeciej było włączenie routingu. Następnie zmieniono tryb interfejsu *GigabitEthernet 0/1* na tryb warstwy trzeciej, po czym skonfigurowano adresy poszczególnych interfejsów.

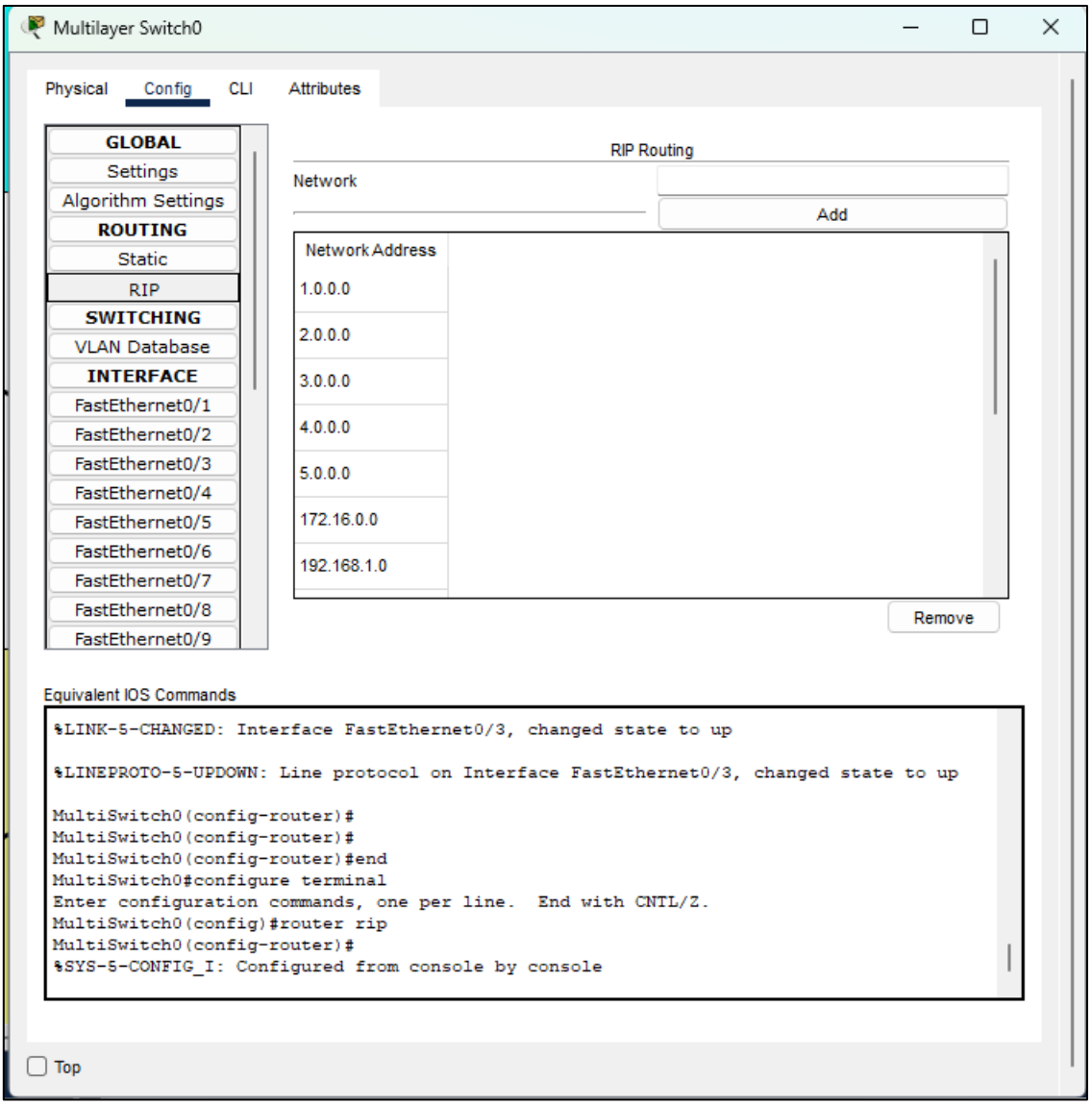
```
Switch(config)#hostname MultiSwitch0
MultiSwitch0(config)#ip rou
MultiSwitch0(config)#ip routin
MultiSwitch0(config)#ip routing
MultiSwitch0(config)#int gig0/1
MultiSwitch0(config-if)#no switch
MultiSwitch0(config-if)#no switchport
MultiSwitch0(config-if)#ip address 197.168.1.2 255.255.255.0
MultiSwitch0(config-if)#no shutdown
MultiSwitch0(config-if)#exit
MultiSwitch0(config)#int vlan1
MultiSwitch0(config-if)#ip address 172.16.31.1 255.255.255.0
MultiSwitch0(config-if)#no shutdown

MultiSwitch0(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

MultiSwitch0(config-if)#
```

Rys. 3.36. Konfiguracja przełącznika warstwy trzeciej

Ostatnim krokiem konfiguracji było określenie trasy domyślnej oraz konfiguracja protokołu RIP na switchu.

```
Router5(config)#ip route 0.0.0.0 0.0.0.0 197.168.1.2
Router5(config)#
```

Rys. 3.37. Określenie trasy domyślnej



Rys. 3.38. Konfiguracja protokołu RIP