|  |  |
| --- | --- |
| **Politechnika Świętokrzyska w Kielcach**  **Wydział Elektrotechniki, Automatyki i Informatyki** | |
| Kierunek:  **Informatyka** | Projekt:  **Bezpieczeństwo infrastruktury sieciowej** |
| Grupa dziekańska:  **1ID24B** | Wykonał:  **Karol Wykrota Grzegorz Swajda Jakub Sadza** |
| Data wykonania:  **12.12.2023** | Temat :  **Sieć drukarni** |
| Github:  <https://github.com/GrzSwa/BIS_project> | |

**SPIS TREŚCI**

1. TOPOLOGIA 3

2. ADRESACJA SIECI 3

3. ROUTING W SIECI 5

4. ZABEZPIECZENIA SIECI 7

4.1. SERWER AAA 7

4.2. KONFIGURACJA DOSTEPÓD DO URZĄDZEŃ SIECIOWYCH8

4.2.1. SSH8

4.2.2. POZIOMY DOSTĘPU8

4.3. SERWER CZASU ORAZ SYSLOG9

4.4. ACL 9

4.5. HSRP ORAZ ETCHERCHANNEL10

4.6. VTP11

4.7. VPN 12

4.8. POZOSTAŁE ZABEZPIECZENIA SIECI13

4.8.1. ZABEZPIECZENIA PRZED ATAKAMI DHCP13

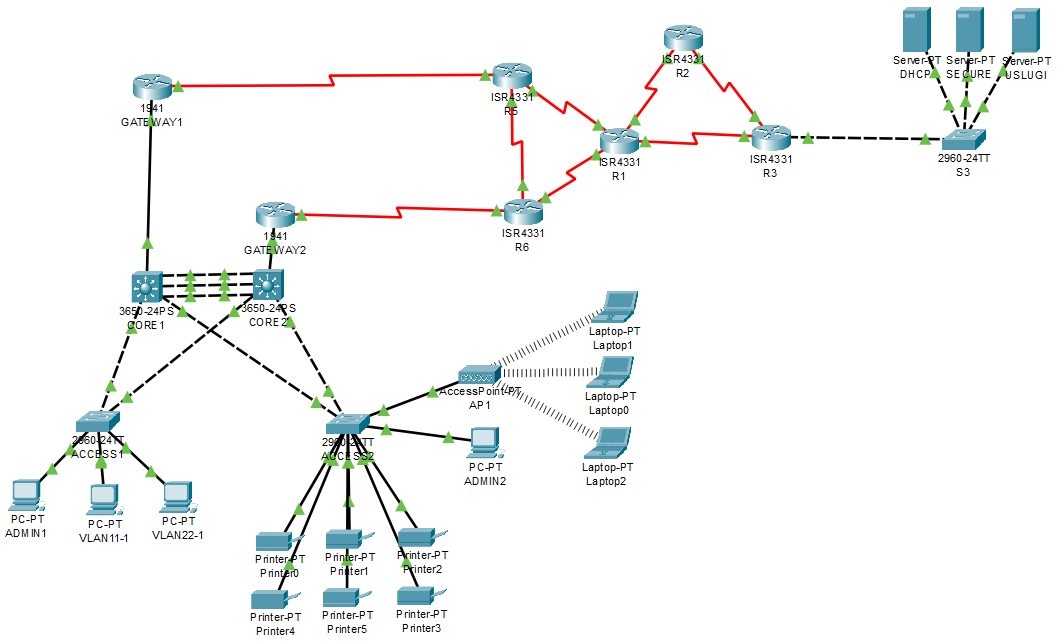
4.8.2. ZABEZPIECZENIA PRZED ATAKAMI VLAN15

4.8.3. MAC16

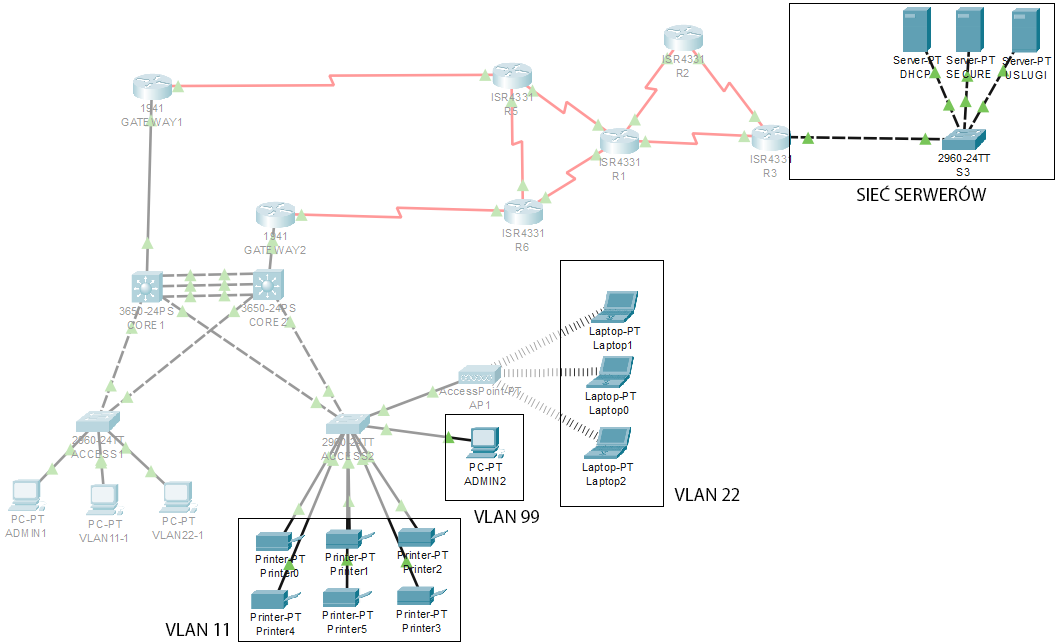
4.8.4. STP17

5. POZOSTAŁE ZABEZPIECZENIA SIECI17

**1. TOPOLOGIA**

****

**2. ADRESACJA SIECI**

****

|  |  |
| --- | --- |
| **SIEĆ PRACOWNIKÓW** | |
| VLAN 11 (SERWER DHCP) | |
| Adres sieci | 172.16.11.0 |
| Adresy hostów | 10-210 |
| Maska sieci | 255.255.255.0 |
| Adres serwera DNS | 172.16.3.5 |
| VLAN 22 (SERWER DHCP) | |
| Adres sieci | 172.16.22.0 |
| Adresy hostów | 10-210 |
| Maska sieci | 255.255.255.0 |
| Adres serwera DNS | 172.16.3.5 |
| VLAN 99 (SERWER DHCP) | |
| Adres sieci | 172.16.99.0 |
| Adresy hostów | 10-210 |
| Maska sieci | 255.255.255.0 |
| Adres serwera DNS | 172.16.3.5 |

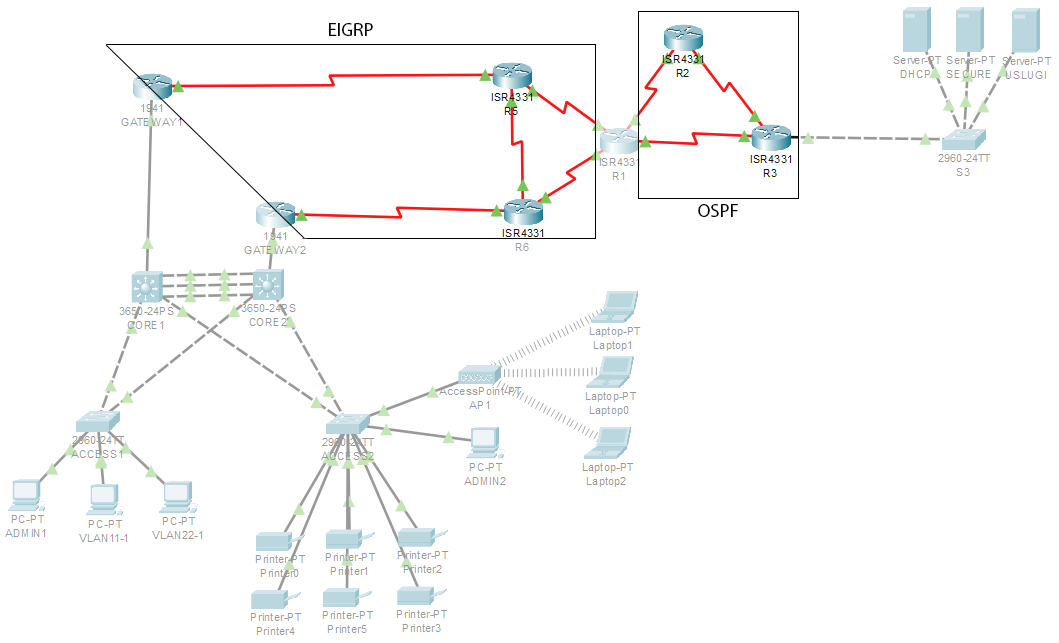
|  |  |
| --- | --- |
| **SIEĆ SERWERÓW** | |
|  | |
| Adres sieci | 172.16.3.0 |
| Adresy hostów | 1-6 |
| Maska sieci | 255.255.255.248 |

|  |  |
| --- | --- |
| **POZOSTAŁE SIECI** | |
| R1 – R2 | |
| Adres sieci | 10.0.3.0 |
| Adresy hostów | 1-2 |
| Maska sieci | 255.255.255.252 |
| R1 – R3 | |
| Adres sieci | 10.0.2.0 |
| Adresy hostów | 1-2 |
| Maska sieci | 255.255.255.252 |
| R2 – R3 | |
| Adres sieci | 10.0.3.0 |
| Adresy hostów | 1-2 |
| Maska sieci | 255.255.255.252 |
| R1 – R5 | |
| Adres sieci | 10.0.1.0 |
| Adresy hostów | 1-2 |
| Maska sieci | 255.255.255.252 |

|  |  |
| --- | --- |
| R1 – R6 | |
| Adres sieci | 10.0.6.0 |
| Adresy hostów | 1-2 |
| Maska sieci | 255.255.255.252 |
| R5 – R6 | |
| Adres sieci | 10.0.5.0 |
| Adresy hostów | 1-2 |
| Maska sieci | 255.255.255.252 |
| R5 – GATEWAY 1 | |
| Adres sieci | 10.0.8.0 |
| Adresy hostów | 1-2 |
| Maska sieci | 255.255.255.252 |
| R6 – GATEWAY 2 | |
| Adres sieci | 10.0.9.0 |
| Adresy hostów | 1-2 |
| Maska sieci | 255.255.255.252 |

**3. ROUTING W SIECI**

W sieci zastosowane zostały dwa typy routingów dynamicznych: EIGRP, OSPF. Router R1 skonfigurowany został w ten sposób aby połączyć je ze sobą.

****

*Fragment konfiguracji routera R1:*

router eigrp 1

**redistribute ospf 1 metric 1544 100 255 1 100**

network 10.0.0.0

!

router ospf 1

log-adjacency-changes

**redistribute eigrp 1 subnets**

*Fragment konfiguracji routera R3:*

router ospf 1

log-adjacency-changes

network 10.0.1.0 0.0.0.3 area 0

network 10.0.2.0 0.0.0.3 area 0

network 172.16.3.0 0.0.0.7 area 1

*Fragment konfiguracji routera R6:*

router eigrp 1

network 10.0.0.0

auto-summary

Na routerach GATEWAY 1 oraz GATEWAY 2 skonfigurowany został routing sieci VLAN (Router on stick), który odpowiada za całą komunikację między sieciami VLAN.

*Fragment konfiguracji routera GATEWAY 1:*

interface GigabitEthernet0/0.11

encapsulation dot1Q 11

ip address 172.16.11.1 255.255.255.0

ip helper-address 172.16.3.3

standby 1 ip 172.16.11.254

standby 1 priority 150

standby 1 preempt

!

interface GigabitEthernet0/0.22

encapsulation dot1Q 22

ip address 172.16.22.1 255.255.255.0

ip helper-address 172.16.3.3

standby 1 ip 172.16.22.254

!

interface GigabitEthernet0/0.99

encapsulation dot1Q 99

ip address 172.16.99.1 255.255.255.0

ip helper-address 172.16.3.3

standby 1 ip 172.16.99.254

standby 1 preempt

DHCP ustawione jest na serwerze w ten sposób, że przydziela konkretną założoną pule adresów dla poszczególnych VLAN’ów. (VLAN 11, VLAN 22, VLAN 99)

**4. ZABEZPIECZENIA SIECI**

**4.1. Serwer AAA (Authentication, Authorization, and Accounting)**

|  |  |
| --- | --- |
| **LOGIN** | **HASŁO** |
| admin | cisco |
| wykrota | wykrota |
| swajda | swajda |
| sadza | sadza |

Usługa AAA została włączona na wszystkich urządzeniach sieciowych. Serwer obsługujący usługę znajduje się na serwerze SECURE.

Konfiguracja określa, że TACACS+ będzie używany do uwierzytelniania użytkownika oraz autoryzacji poziomu uprawnień (enable). Lokalne uwierzytelnianie będzie używane jako kopia zapasowa, jeśli TACACS+ nie jest dostępny.

*Fragment konfiguracji routera R3:*

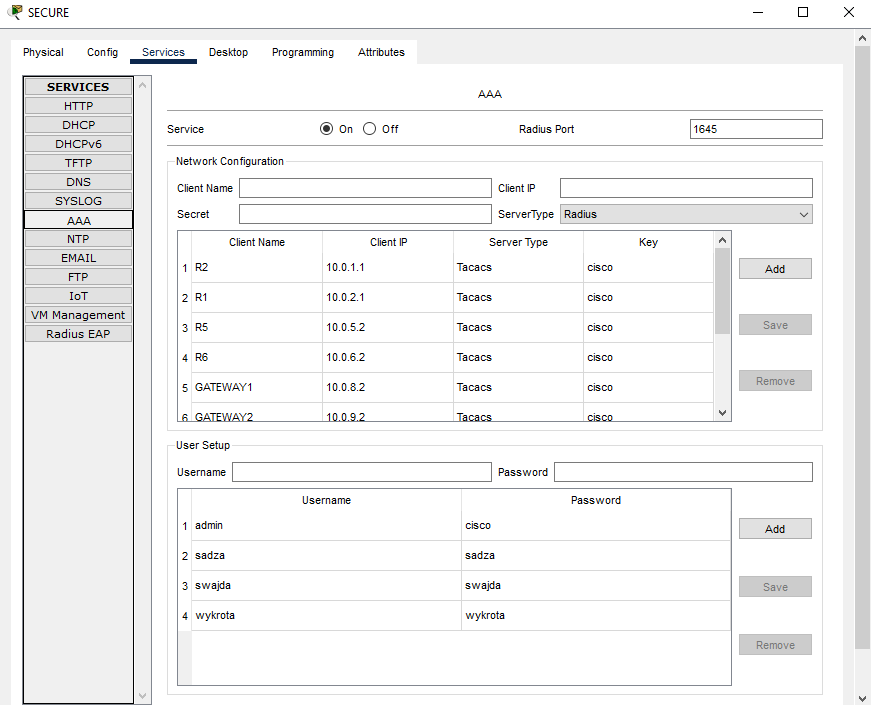
aaa new-model

!

aaa authentication login default group tacacs+ local

aaa authentication enable default group tacacs+ enable

Ta konfiguracja zapewnia większe bezpieczeństwo niż korzystanie z lokalnego uwierzytelniania i autoryzacji. TACACS+ to protokół uwierzytelniania i autoryzacji sieciowej, który zapewnia centralne przechowywanie informacji o użytkownikach i uprawnieniach.



**4.2. Konfiguracja dostępów do urządzeń sieciowych**

**4.2.1 SSH**

Usługa SSH (Secure Shell) umożliwia bezpośrednie zarządzanie serwerem, z wykorzystaniem połączenia terminalowego.

*Fragment konfiguracji routera GATEWAY 2:*

line vty 0 4

exec-timeout 5 0

login authentication default

transport input ssh

line vty 5 15

transport input ssh

**4.2.2 Poziomy dostępu**

*Fragment konfiguracji przełącznika CORE1:*

username admin privilege 15

username sadza

username swajda privilege 15

username wykrota  
!  
privilege exec level 15 configure

privilege exec level 15 configure terminal

privilege exec level 15 copy

privilege exec level 15 copy running-config

privilege exec level 15 copy running-config startup-config

privilege exec level 1 disable

privilege exec level 15 enable

privilege exec level 1 exit

privilege exec level 1 logout

privilege exec level 1 ping

privilege exec level 1 reload

privilege exec level 1 show

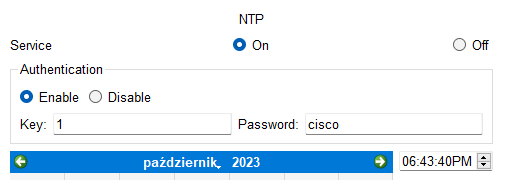
privilege exec level 1 show interfaces

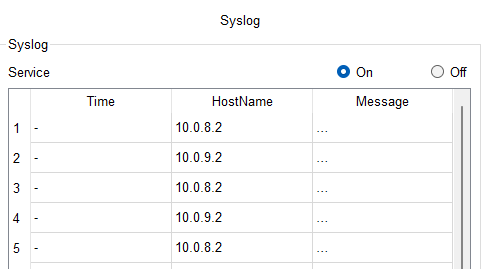
privilege exec level 15 show running-config

privilege exec level 1 show version

**4.3. Serwer czasu oraz SysLog**

Na serwerze SECURE uruchomiona została usługa Syslog zapisująca zdarzenia ze wszystich urządzeń w topologii.





**4.4. ACL**

W sieci zrobiono 2 rozszerzone wersje list ACL:

* Pierwsza, która blokuje ruch wychodzący WWW dla vlan’u 11,
* Druga, która pozwala na dostęp zdalny do SSH dla vlan’u 99 (admin), zaś dla pozostałych blokuje.

*Fragment konfiguracji routera GATEWAY 2:*

ip access-list extended www\_accesss

deny tcp 172.16.11.0 0.0.0.255 any eq www

deny tcp 172.16.11.0 0.0.0.255 any eq 443

deny udp 172.16.11.0 0.0.0.255 any eq domain

permit ip any any

ip access-list extended ssh\_access

deny tcp 172.16.11.0 0.0.0.255 any eq 22

deny tcp 172.16.22.0 0.0.0.255 any eq 22

permit ip any any

!

interface GigabitEthernet0/0.99

encapsulation dot1Q 99

ip address 172.16.99.2 255.255.255.0

ip helper-address 172.16.3.3

**ip access-group ssh\_access in**

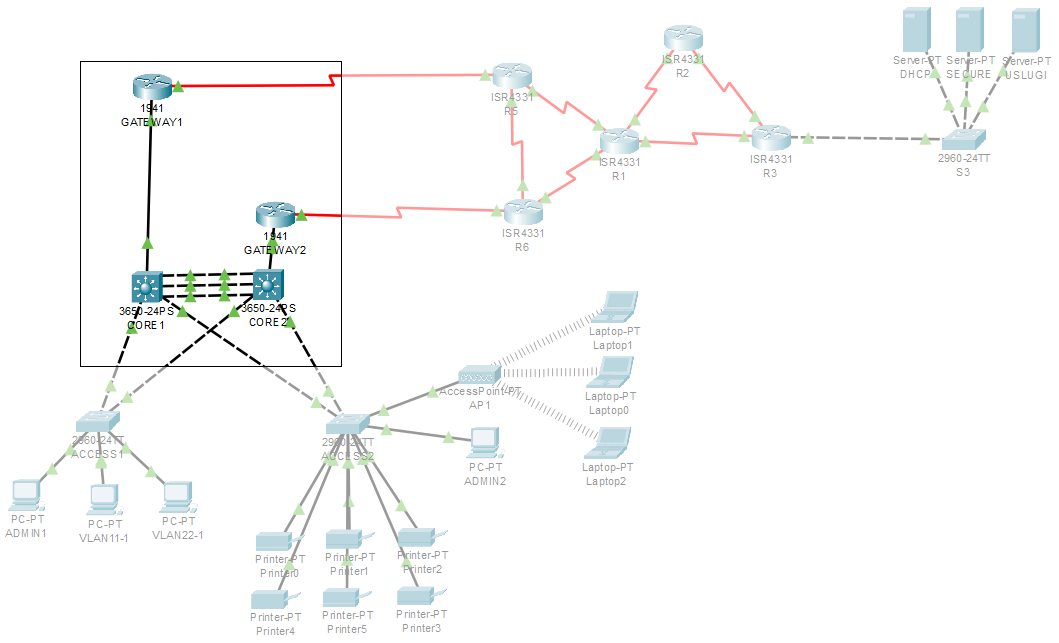
standby 1 ip 172.16.99.254

standby 1 priority 110

**4.5. HSRP oraz EtcherChannel**

HSRP zapewnia redundancje w sieci. Zostało to zaimplementowane w miejscu, gdzie zastosowanie jednego routera mogłoby całkowicie sparaliżować dostęp użytkowników do pozostałej części sieci.

EtherChannel został skonfigurowany pomiędzy urządzeniami CORE1 oraz CORE2, co ma na celu zwiększenie przepustowości, niezawodności oraz równoważy obciążenie.

****

*Fragment konfiguracji przełącznika CORE 1:*

interface Port-channel1

switchport mode trunk

switchport nonegotiate

!

interface GigabitEthernet1/0/1

switchport mode trunk

switchport nonegotiate

channel-group 1 mode auto

!

interface GigabitEthernet1/0/2

switchport mode trunk

switchport nonegotiate

channel-group 1 mode auto

!

interface GigabitEthernet1/0/3

switchport mode trunk

switchport nonegotiate

channel-group 1 mode auto

*Fragment konfiguracji routera GATWEAY 1:*

GigabitEthernet0/0.11 - Group 1

State is Active

6 state changes, last state change 00:00:28

Virtual IP address is 172.16.11.254

Active virtual MAC address is 0000.0C07.AC01

Local virtual MAC address is 0000.0C07.AC01 (v1 default)

Hello time 3 sec, hold time 10 sec

Next hello sent in 0.399 secs

Preemption enabled

Active router is local

Standby router is 172.16.11.2

Priority 150 (configured 150)

Group name is hsrp-Gig-1 (default)

P indicates configured to preempt.

|

Interface Grp Pri P State Active Standby Virtual IP

Gig 1 150 P Active local 172.16.11.2 172.16.11.254

Gig 1 100 Active local unknown 172.16.22.254

Gig 1 100 P Active local unknown 172.16.99.254

**4.6. VTP**

Protokół VTP (VLAN Trunking Protocol) został zastosowany dla przełączników warstwy 3 – CORE1 oraz CORE2. Działa on w ten sposób, że to, co zostanie zastosowane na przełącznikach ustawionych w trybie Server (CORE1, CORE2), zostanie odwzorowane na podłączonych do nich przełącznikach ustawionych w trybie Client (ACCESS1, ACCESS2). VTP skraca użytkownikowi czas, który musiałby poświęcić na konfigurowanie wszystkich urządzeń, a dzięki zastosowaniu VTP w teorii musi skonfigurować tylko 1 urządzenie ustawione w trybie serwera.

*Fragment konfiguracji przełącznika CORE 1:*

VTP Version capable : 1 to 2

VTP version running : 2

VTP Domain Name : NET00

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : 0001.4217.DC00

Configuration last modified by 172.16.99.2 at 10-10-23 18:24:11

Local updater ID is 172.16.99.2 on interface Vl99 (lowest numbered VLAN interface found)

Feature VLAN :

--------------

VTP Operating Mode : Server

Maximum VLANs supported locally : 1005

Number of existing VLANs : 9

Configuration Revision : 103

MD5 digest : 0x90 0x8B 0x3E 0xE2 0xB6 0x61 0x53 0xC7

0xE2 0x6D 0x11 0xFC 0x3C 0x0E 0x17 0x86

*Fragment konfiguracji przełącznika ACCESS 1:*

VTP Version capable : 1 to 2

VTP version running : 2

VTP Domain Name : NET00

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : 0000.0CE4.7450

Configuration last modified by 172.16.99.2 at 10-10-23 18:24:11

Feature VLAN :

--------------

VTP Operating Mode : Client

Maximum VLANs supported locally : 255

Number of existing VLANs : 9

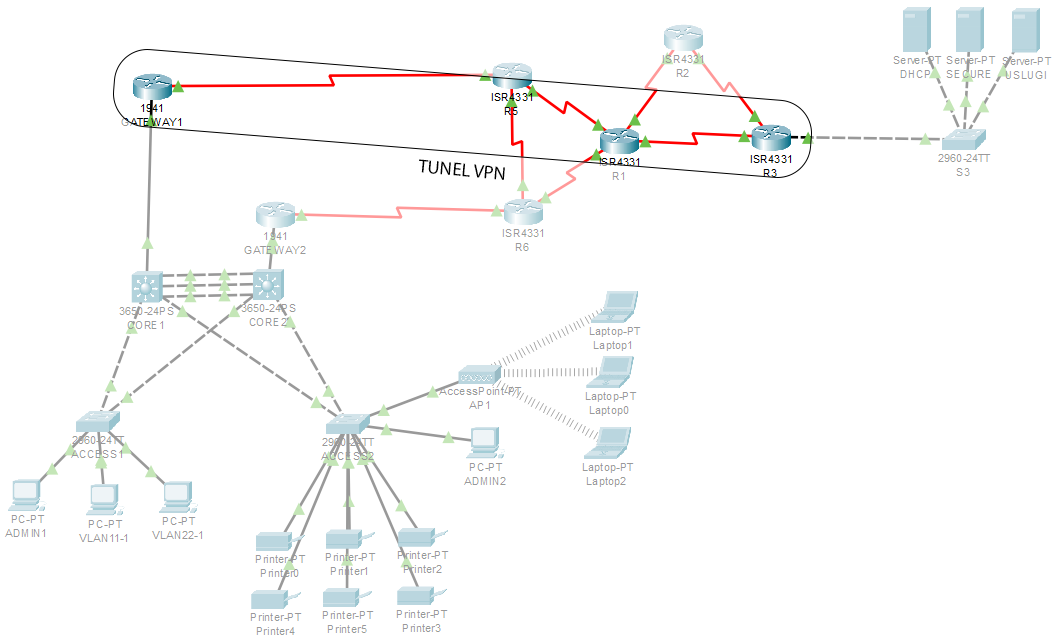
Configuration Revision : 103

MD5 digest : 0x90 0x8B 0x3E 0xE2 0xB6 0x61 0x53 0xC7

0xE2 0x6D 0x11 0xFC 0x3C 0x0E 0x17 0x86

**4.7. VPN**

Tunelowanie zostało włączone między routerem R3 a GATEWAY1.

****

*Fragment konfiguracji routera GATEWAY1:*

interface Tunnel1

ip address 209.169.90.1 255.255.255.0

mtu 1476

tunnel source Serial0/1/0

tunnel destination 10.0.2.2

*Fragment konfiguracji routera R3:*

interface Tunnel1

ip address 209.168.90.2 255.255.255.0

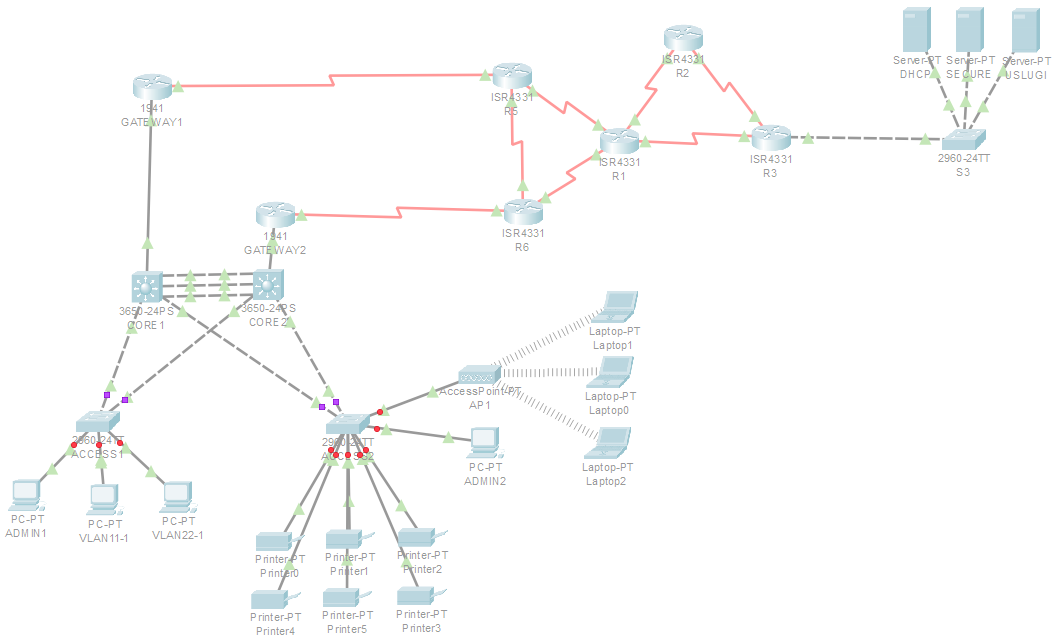
mtu 1476

tunnel source Serial0/1/1

tunnel destination 10.0.8.2

**4.8. Pozostałe zabezpieczenia sieci**

**4.8.1. Zabezpieczenia przed atakami DHCP**



⚫- niezaufany port

⬛- port zaufany

Na przełączniku ACCESS 2 na wszystkich interfejsach, które mają tryb access zastosowano DHCP Snooping. Pozwoli to na wysyłanie maksymalnie 5 zapytań do serwera DHCP na sekundę. Razem z zabezpieczeniem DHCP, zostało skonfigurowane zabezpieczenie ARP Snooping.

*Fragment konfiguracji przełącznika ACCESS 2:*

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:

11,22,99

Insertion of option 82 is enabled

Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Interface Trusted Rate limit (pps)

----------------------- ------- ----------------

FastEthernet0/10 yes 5

FastEthernet0/6 yes 5

FastEthernet0/2 no 5

FastEthernet0/7 yes 5

FastEthernet0/1 yes 5

FastEthernet0/4 yes 5

FastEthernet0/5 yes 5

FastEthernet0/8 yes 5

FastEthernet0/9 yes 5

FastEthernet0/3 yes 5

FastEthernet0/16 yes 5

FastEthernet0/18 yes 5

FastEthernet0/13 yes 5

FastEthernet0/11 yes 5

FastEthernet0/19 yes 5

FastEthernet0/20 yes 5

FastEthernet0/21 yes 5

FastEthernet0/14 yes 5

FastEthernet0/15 yes 5

FastEthernet0/12 yes 5

FastEthernet0/17 yes 5

FastEthernet0/23 yes 5

FastEthernet0/22 yes 5

FastEthernet0/24 yes 5

ACCESS2#show ip arp inspection

Source Mac Validation : Disabled

Destination Mac Validation : Disabled

IP Address Validation : Enabled

Vlan Configuration Operation ACL Match Static ACL

---- ------------- --------- --------- ----------

11 Enabled Active

22 Enabled Active

99 Enabled Active

Vlan ACL Logging DHCP Logging Probe Logging

---- ----------- ------------ -------------

11 Deny Deny Off

22 Deny Deny Off

99 Deny Deny Off

Vlan Forwarded Dropped DHCP Drops ACL Drops

---- --------- ------- ---------- ---------

11 12 0 0 0

22 0 0 0 0

99 2 0 0 0

Vlan DHCP Permits ACL Permits Probe Permits Source MAC Failures

---- ------------ ----------- ------------- -------------------

11 12 0 0 0

22 0 0 0 0

99 2 0 0 0

Vlan Dest MAC Failures IP Validation Failures Invalid Protocol Data

---- ----------------- ---------------------- ---------------------

11 0 0 0

22 0 0 0

99 0 0 0

**4.8.2. Zabezpieczenia przed atakami VLAN**

VLANy stworzone dla tej sieci, oddzielają użytkowników użytkowych (pracowników drukarni – VLAN 11 oraz VLAN 22) od użytkowników administracyjnych (VLAN 99). Również w celach zabezpieczenia sieci, nieużywane porty przełącznika zostały przypisane do vlanu 1000, który nie jest rutowany z innymi vlanami.

Port Name Status Vlan Duplex Speed Type

Fa0/1 disabled 1000 auto auto 10/100BaseTX

Fa0/2 disabled 1000 auto auto 10/100BaseTX

Fa0/3 connected 11 auto auto 10/100BaseTX

Fa0/4 connected 11 auto auto 10/100BaseTX

Fa0/5 connected 11 auto auto 10/100BaseTX

Fa0/6 connected 11 auto auto 10/100BaseTX

Fa0/7 connected 11 auto auto 10/100BaseTX

Fa0/8 connected 11 auto auto 10/100BaseTX

Fa0/9 disabled 1000 auto auto 10/100BaseTX

Fa0/10 connected 22 auto auto 10/100BaseTX

Fa0/11 disabled 1000 auto auto 10/100BaseTX

Fa0/12 disabled 1000 auto auto 10/100BaseTX

Fa0/13 disabled 1000 auto auto 10/100BaseTX

Fa0/14 disabled 1000 auto auto 10/100BaseTX

Fa0/15 disabled 1000 auto auto 10/100BaseTX

Fa0/16 disabled 1000 auto auto 10/100BaseTX

Fa0/17 disabled 1000 auto auto 10/100BaseTX

Fa0/18 disabled 1000 auto auto 10/100BaseTX

Fa0/19 disabled 1000 auto auto 10/100BaseTX

Fa0/20 disabled 1000 auto auto 10/100BaseTX

Fa0/21 disabled 1000 auto auto 10/100BaseTX

Fa0/22 disabled 1000 auto auto 10/100BaseTX

Fa0/23 disabled 1000 auto auto 10/100BaseTX

Fa0/24 connected 99 auto auto 10/100BaseTX

Gig0/1 connected trunk auto auto 10/100BaseTX

Gig0/2 connected trunk auto auto 10/100BaseTX

**4.8.3. Zabezpieczenia przed atakami MAC**

Zabezpieczenia MAC zostały zastosowane dla wszystkich dostępnych portów urządzeń ACCESS1 oraz ACCESS2. Został wymuszony na nich tryb obsługi bezpieczeństwa - restrict. Co oznacza, że odrzuca wszystkie pakiety z niezabezpieczonych hostów, ale pozostaje włączone i zostawi ślad w dzienniku.

*Fragment konfiguracji przełącznika CORE 1:*

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

--------------------------------------------------------------------

Fa0/2 1 0 0 Restrict

Fa0/3 1 1 0 Restrict

Fa0/4 1 1 0 Restrict

Fa0/5 1 1 0 Restrict

Fa0/6 1 1 0 Restrict

Fa0/7 1 1 0 Restrict

Fa0/8 1 1 0 Restrict

Fa0/9 1 0 0 Restrict

----------------------------------------------------------------------

**4.8.4. Zabezpieczenia przed atakami STP**

*Fragment konfiguracji przełącznika CORE 1:*

interface FastEthernet0/2

switchport access vlan 1000

ip arp inspection trust

ip dhcp snooping limit rate 5

switchport mode access

switchport voice vlan 11

switchport port-security

switchport port-security mac-address sticky

switchport port-security violation restrict

switchport port-security aging time 5

spanning-tree portfast

spanning-tree bpduguard enable

shutdown

**5. ZAGROŻENIA**

Sieć została starannie zabezpieczona przed różnorodnymi zagrożeniami, zarówno zewnętrznymi, jak i wewnętrznymi. Jednym z potencjalnych ryzyk było wystawienie na ataki takie jak ARP spoofing czy DHCP spoofing. W celu skutecznego przeciwdziałania tym zagrożeniom zastosowano szereg środków bezpieczeństwa, w tym mechanizmy DHCP oraz ARP snooping. Dzięki nim atakujący nie ma możliwości podszywania się pod adresy hostów w sieci, co podnosi ogólny poziom bezpieczeństwa. Dodatkowo sieć została wzmocniona przed potencjalnymi atakami wewnętrznymi poprzez właściwe zabezpieczenie portów, vlanów oraz adresów MAC. Nieaktywne porty zostały wyłączone i przypisane do vlanu, który znajduje się poza obszarem routingu między vlanami, co ogranicza potencjalne punkty ataku. Aby uniknąć przepełnienia tablicy adresów MAC, skonfigurowano odpowiednie zabezpieczenia, a dynamiczna, lepka nauka portów umożliwia podłączenie maksymalnie dwóch urządzeń do konkretnego portu przełącznika. W celu zabezpieczenia dostępu do urządzeń każde z nich zostało skonfigurowane z odpowiednimi poziomami uprawnień dla autoryzowanych użytkowników. To ogranicza możliwość wykonania potencjalnie niebezpiecznych komend przez nieupoważnione osoby. W szczególności, dostęp do urządzeń poprzez port SSH został ograniczony tylko dla hostów, które powinny mieć wyłączny dostęp do konfiguracji urządzeń sieciowych. Zastosowane zostały rozszerzone listy dostępu (ACL), które skutecznie chronią przed nieautoryzowanym dostępem. Dodatkowo dostęp do protokołu WWW został zablokowany dla hostów, które nie powinny mieć do tego rodzaju dostępu, co stanowi dodatkową warstwę zabezpieczeń przeciwko potencjalnym atakom z wewnątrz sieci.