

Kielce, 03.11.2023 r.

Bezpieczeństwo infrastruktury sieciowej

Projekt: Księgarnia

Autor: Aleksandra Kwiatkowska
Wiktoria Sikora
Grupa: 1ID24B

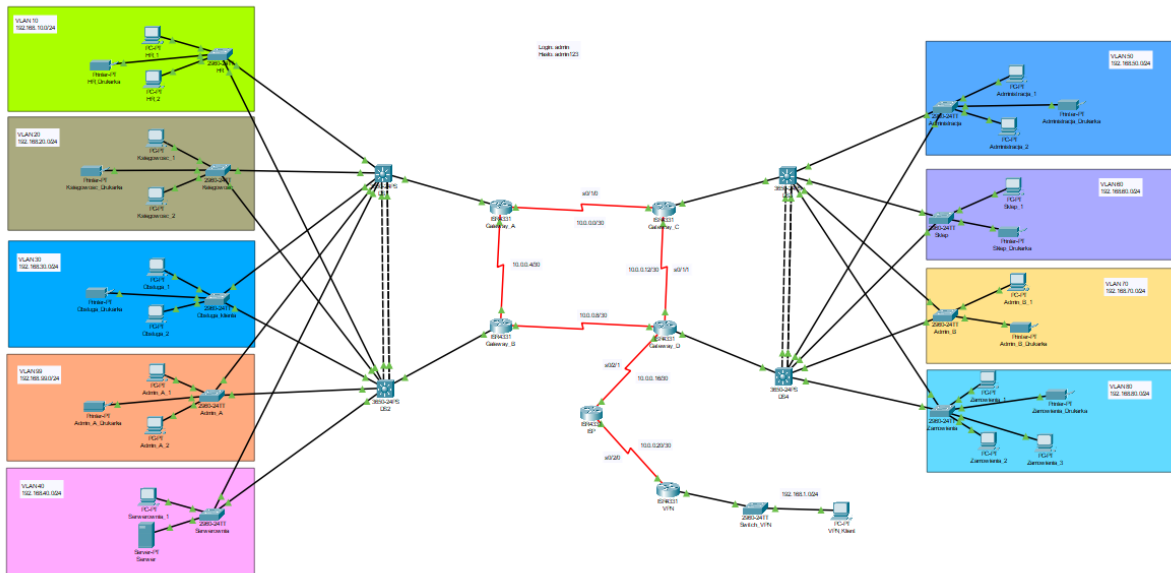
Spis treści

1. Wprowadzenie	3
2. Topologia	3
3. Zagrożenia.....	6
4. Wdrożone technologie	7
4.1. VLAN.....	7
4.2. DHCP.....	9
4.3. STP.....	12
4.4. Etherchannel.....	14
4.5. HSRP	14
4.6. EIGRP	15
4.7. NTP	16
4.8. SSH	17
4.9. Syslog	17
4.10. ACL.....	18
4.11. VPN.....	19
4.12. AAA	21
4.13. SNMP.....	22
4.14. Konfiguracja poziomów dostępowych na urządzeniach sieciowych.....	23
5. Przykłady plików konfiguracyjnych urządzeń	23
5.1. Gateway_A.....	23
5.2. DS1.....	27
5.3. HR.....	31

1. Wprowadzenie

Dokumentacja zawiera szczegółowe informacje dotyczące infrastruktury sieciowej, architektury, konfiguracji i zarządzania siecią w ramach księgarni. Przedstawimy tutaj zasady działania sieci oraz poszczególnych komponentów.

2. Topologia

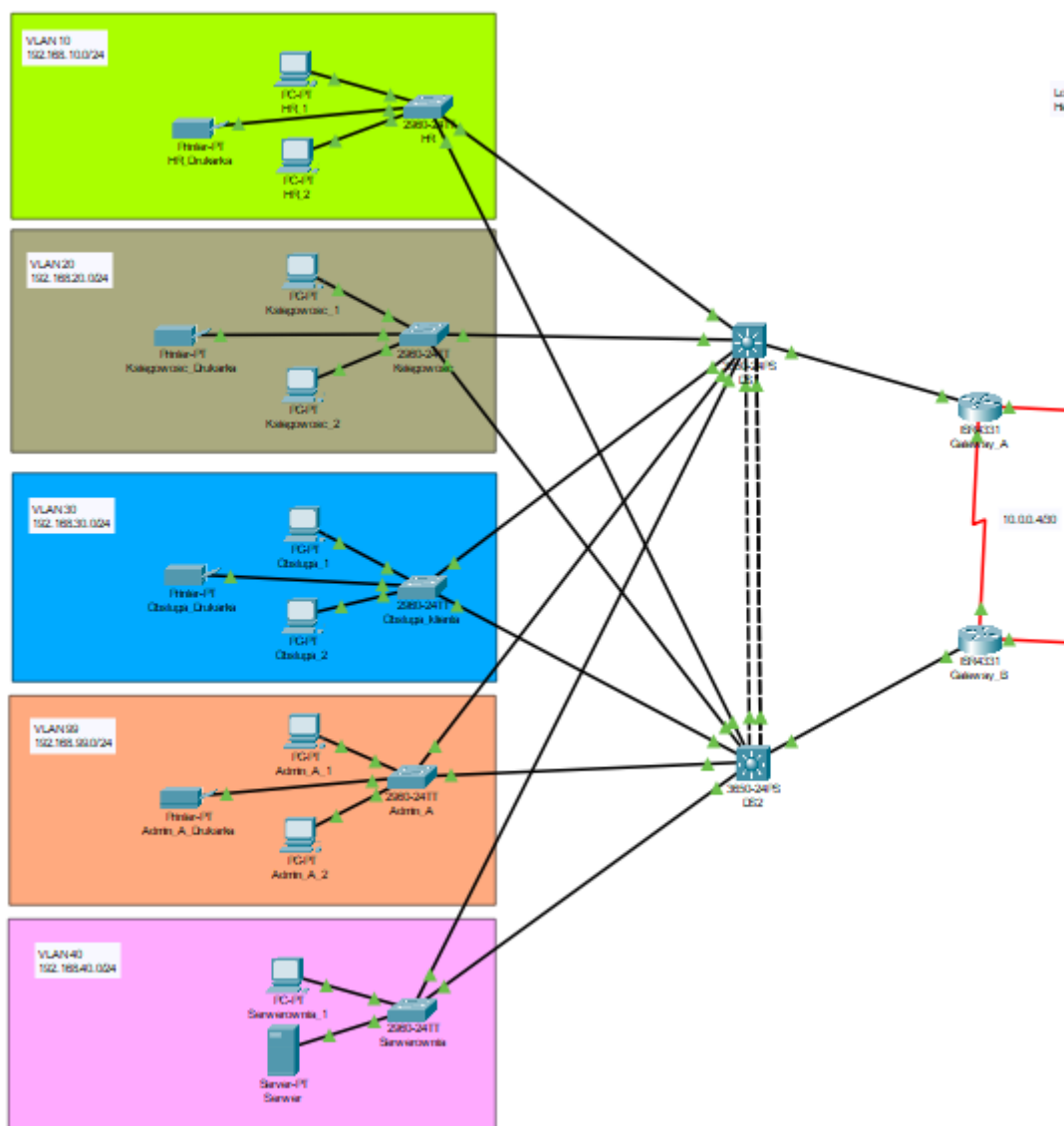


Rysunek 1. Topologia sieci

Sieć można podzielić na Budynek_A oraz Budynek_B. Zarówno w pierwszym budynku jak i drugim występuje sieć hierarchiczna, a dokładniej sieć dwuwarstwowa. Posiadamy warstwę dostępu, która pozwala aby urządzenia końcowe mogły korzystać z sieci. Druga warstwa pełni funkcję warstwy dystrybucji oraz rdzenia, czyli operuje całym ruchem w sieci oraz umożliwia dostęp do i z Internetu. Każdy VLAN posiada PC oraz znajdują się również drukarki. Budynek_A oraz Budynek_B posiadają po dwa routery oraz przełączniki dystrybucji, które mają za zadanie, w razie awarii jakiegoś urządzenia, przejąć ich pracę.

W Budynek_A występuje następująca adresacja:

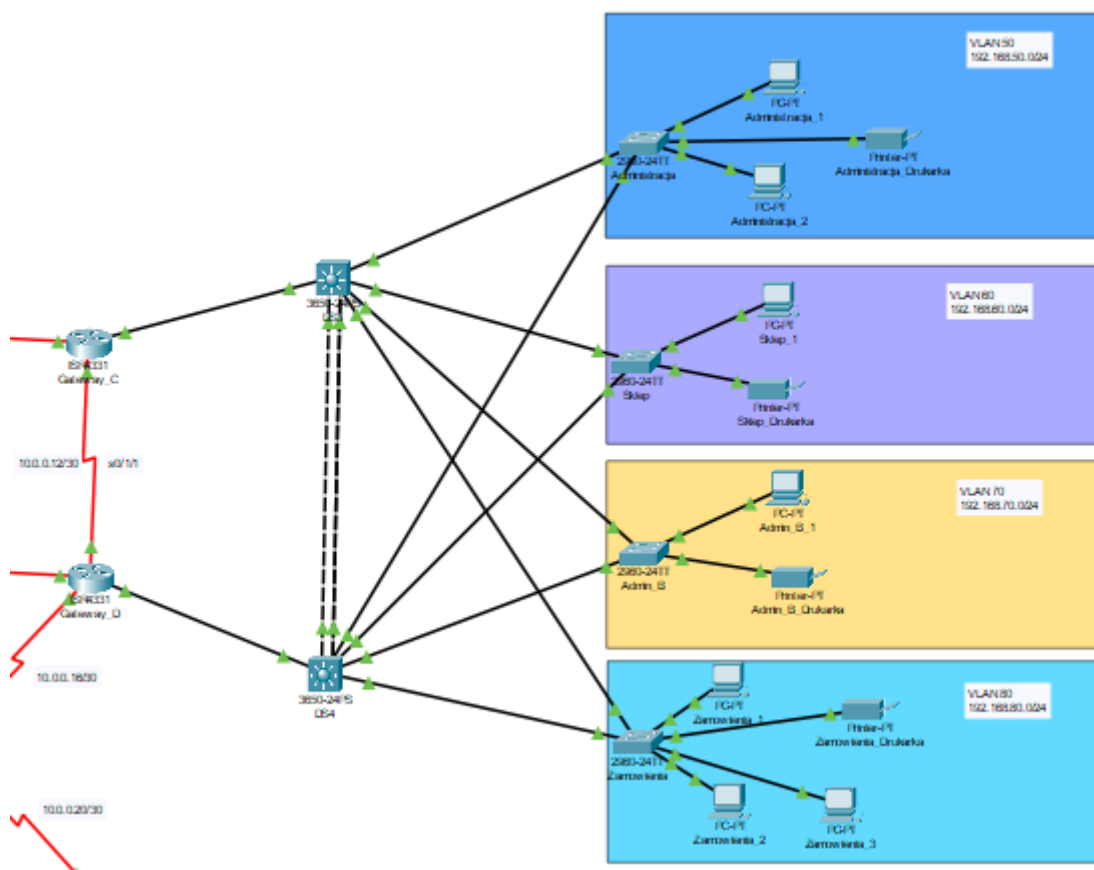
- VLAN 10 (name HR): 192.168.10.0/24
- VLAN 20 (name Księgowosc): 192.168.20.0/24
- VLAN 30 (name Obsługa_klienta): 192.168.30.0/24
- VLAN 99 (name Admin_A): 192.168.99.0/24
- VLAN 40 (name Serwerownia): 192.168.40.0/24



Rysunek 2. Budynek A

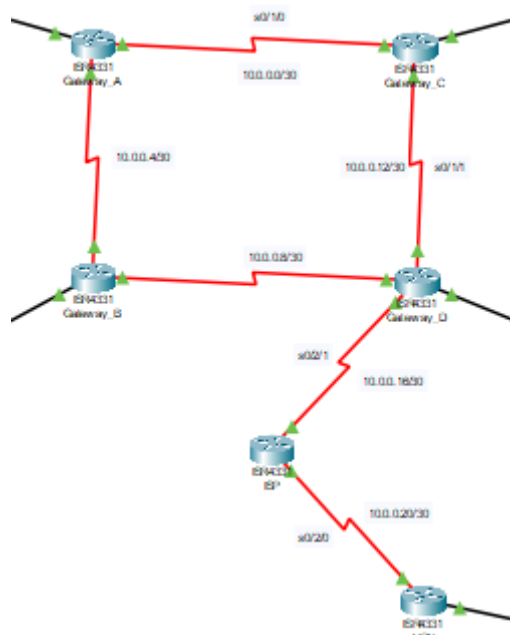
Budynek_B:

- VLAN 50 (name Administracja): 192.168.50.0/24
- VLAN 60 (name Sklep): 192.168.60.0/24
- VLAN 70 (name Admin_B): 192.168.70.0/24
- VLAN 80 (name Zamowienia): 192.168.80.0/24



Rysunek 3. Budynek B

Gateway_A połączony jest z Gateway_B: 10.0.0.4/30
 Gateway_A połączony jest z Gateway_C: 10.0.0.0/30
 Gateway_D połączony jest z Gateway_B: 10.0.0.8/30
 Gateway_D połączony jest z Gateway_C: 10.0.0.12/30
 Gateway_D połączony jest z ISP: 10.0.0.16/30
 ISP połączony jest z VPN: 10.0.0.20/30
 VPN_klient: 192.168.1.0/24



Rysunek 4. Połączenia między ruterami

3. Zagrożenia

Sieć mogą czekać następujące zagrożenia:

- **Ataki zero-day** - to ataki wykorzystujące niedawno odkryte luki w oprogramowaniu. Regularne aktualizacje oprogramowania i monitorowanie ruchu sieciowego mogą pomóc w wykryciu i obronie przed takimi atakami.
- **Ataki DDoS** - to rodzaj cyberataku, w którym grupa atakujących komputerów lub urządzeń sieciowych współpracuje, aby zalać celowaną stronę lub usługę z dużą ilością zapytań lub ruchu internetowego, co ma na celu spowodowanie zakłóceń lub całkowitej niedostępności usługi. Atak DDoS jest nazwany "rozproszonym", ponieważ jest wykonywany z wielu źródeł, co utrudnia zidentyfikowanie i zneutralizowanie atakujących.
- **Ataki wewnętrzne** - to zagrożenia, które wywodzą się od pracowników, dostawców lub innych osób, które mają dostęp do wewnętrznych zasobów organizacji. Ataki wewnętrzne mogą być celowe lub wynikać z nieostrożności lub błędów, ale zawsze stanowią poważne ryzyko dla bezpieczeństwa organizacji.
- **Ataki na warstwę fizyczną sieci** - to próby naruszenia samej infrastruktury sieciowej, czyli komponentów sprzętowych, które stanowią jej fundament. Ataki tego typu mogą mieć poważne konsekwencje, ponieważ wpływają na dostępność sieci i mogą prowadzić do przerw w działaniu.

- **Ataki społeczne** - takie jak phishing, to techniki manipulacji psychologicznej, które atakują naszą ludzką naturę, by uzyskać poufne informacje, hasła, dane osobowe lub dostęp do systemów. Ataki te polegają na oszukiwaniu użytkowników w celu wyłudzenia cennych informacji lub wykonywania niepożądanych działań.

4. Wdrożone technologie

4.1. VLAN

VLAN pozwala w jednej fizycznej sieci lokalnej stworzyć wiele sieci logicznych. Dzięki niej w sieci zostały wprowadzone:

- **Łatwiejsze nadawanie uprawnień** – każda sieć może posiadać swoje ACL
- **Ograniczony ruch rozgłoszeniowy** – każdy VLAN posiada swoją domenę rozgłoszeniową
- **Bezpieczeństwo** – użytkownicy są odseparowani od siebie
- **Logiczny podział sieci** – urządzenia końcowe, które mają znajdować się w logicznych sieciach są podłączone do różnych przełączników.

```
DS1# show vlan brief
```

VLAN	Name	Status
1	default	active
10	HR	active
20	Ksiegowosc	active
30	Obsluga_klienta	active
40	Serwerownia	active
99	Admin_A	active
999	BlackHole	active

Rysunek 5. VLANy na przełączniku DS1

Na każdym z ruterów zostały utworzone podinterfejsy.

```
Device Name: Gateway_A
Device Model: ISR4331
Hostname: Gateway_A
```

Port	Link	VLAN	IP Address
GigabitEthernet0/0/0	Up	--	<not set>
GigabitEthernet0/0/0.10	Up	--	192.168.10.1/24
GigabitEthernet0/0/0.20	Up	--	192.168.20.1/24
GigabitEthernet0/0/0.30	Up	--	192.168.30.1/24
GigabitEthernet0/0/0.40	Up	--	192.168.40.1/24
GigabitEthernet0/0/0.99	Up	--	192.168.99.1/24

Rysunek 6. Podinterfejsy na Gateway_A

W celu poprawy bezpieczeństwa sieci, natywny VLAN został przeniesiony do innej sieci niż domyślna. VLAN natywny, czasem nazywany VLANem pierwotnym, to rodzaj wirtualnej sieci, która obsługuje ruch, który nie jest oznaczony identyfikatorem VLANu. Oznacza to, że przekazuje ramki, które nie posiadają oznaczenia VLANu. Łąca trunkowe mają zdolność obsługi różnych rodzajów ruchu, w tym ruchu z różnych sieci VLAN, oznaczonego tagami, ale także ruchu spoza sieci VLAN. Kiedy ramka nieoznakowana trafia na łącze trunk, jest przekazywana do natywnego VLANu, czyli pierwotnej sieci VLAN. W przypadku przełączników Cisco domyślnym natywnym VLANem jest VLAN 1, do którego są przypisane wszystkie porty przed utworzeniem dodatkowych sieci wirtualnych. Po przeniesieniu VLANu, nieoznakowany ruch trafi do innej sieci, na przykład VLANy o numerze 99 lub 70, w zależności od konfiguracji danego budynku.

```
Sklep#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Gig0/1    on        802.1q         trunking    70
Gig0/2    on        802.1q         trunking    70

Port      Vlans allowed on trunk
Gig0/1    1-1005
Gig0/2    1-1005

Port      Vlans allowed and active in management domain
Gig0/1    1,50,60,70,80,999
Gig0/2    1,50,60,70,80,999

Port      Vlans in spanning tree forwarding state and not pruned
Gig0/1    1,50,60,999
Gig0/2    1,70,80,999
```

Rysunek 7. Przypisanie VLANu 70 w budynku B

VLAN typu „czarna dziura”, znany również jako „Black Hole” VLAN, to specjalny rodzaj VLAN w sieciach komputerowych. W kontekście priorytetu bezpieczeństwa w sieciach, ważne jest skoncentrowanie się na zabezpieczeniu nieużywanych portów. Nieużywane, nieaktywne porty można przypisać do tzw. fałszywego VLANu, w którym żadne maszyny nie działają. Dzięki temu, nawet gdyby intruz uzyskał dostęp do tego fałszywego VLANu, nie będzie w stanie wyrządzić większej szkody, ponieważ w nim nie funkcjonują żadne urządzenia. Idea polega na tym, że nieużywane porty są izolowane w specjalnym "czarnym" VLANie, który działa jako swoista pułapka dla potencjalnych ataków. To podejście pozwala na dodatkową warstwę ochrony, zminimalizowanie ryzyka i utrzymanie bezpieczeństwa sieci, zwłaszcza w sytuacji, gdy nie ma potrzeby korzystania z konkretnych portów. W praktyce, nawet jeśli ktoś uzyska dostęp do tych portów, nie ma tam żadnych aktywnych zasobów, co ogranicza potencjalne zagrożenia.


```
Zamowienia#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
50	Administracja	active	
60	Sklep	active	
70	Admin_B	active	Fa0/24
80	Zamowienia	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
999	BlackHole	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8
			Fa0/9, Fa0/10, Fa0/11, Fa0/12
			Fa0/13, Fa0/14, Fa0/15, Fa0/16
			Fa0/17, Fa0/18, Fa0/19, Fa0/20
			Fa0/21, Fa0/22, Fa0/23
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Rysunek 8. Przypisane interfejsy do VLANów, z uwzględnieniem BlackHole

Cisco używa specjalnego protokołu znanego jako Dynamic Trunking Protocol (DTP) na swoich przełącznikach. Pewne porty automatycznie negocjują między sobą tryb trunk, czyli sposób, w jaki przesyłane są dane pomiędzy przełącznikami. W celu bezpieczeństwa zalecane jest wyłączenie automatycznej negocjacji (auto-negocjacji). W praktyce oznacza to, że zamiast pozostawiać decyzję o trybie trunk w rękach automatycznej negocjacji, administrator sieci ręcznie konfiguruje, czy dany port ma działać jako trunk czy nie.

```
HR# show interface g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Admin_A)
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
```

Rysunek 9. Wyłączona automatyczna negocjacja na przełączniku HR, interfejsie Gig0/1

4.2. DHCP

DHCP – pozwala urządzeniom końcowym podłączonym do sieci na automatyczne pobranie adresu IP, maski podsieci, adresu bramy oraz innych ustawień jakie zostały skonfigurowane

w puli adresów. W przedstawionej sieci DHCP zostało skonfigurowane na ruterach Gateway_A, Gateway_B, Gateway_C i Gateway_D.

```
Gateway_D#show ip dhcp pool

Pool vlan50 :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 0
  Excluded addresses                : 22
  Pending event                    : none

  1 subnet is currently in the pool
  Current index      IP address range      Leased/Excluded/Total
  192.168.50.1       192.168.50.1 - 192.168.50.254    0 / 22 / 254

Pool vlan60 :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 0
  Excluded addresses                : 22
  Pending event                    : none

  1 subnet is currently in the pool
  Current index      IP address range      Leased/Excluded/Total
  192.168.60.1       192.168.60.1 - 192.168.60.254    0 / 22 / 254

Pool vlan70 :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 2
  Excluded addresses                : 22
  Pending event                    : none

  1 subnet is currently in the pool
  Current index      IP address range      Leased/Excluded/Total
  192.168.70.1       192.168.70.1 - 192.168.70.254    2 / 22 / 254

Pool vlan80 :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 4
  Excluded addresses                : 22
  Pending event                    : none

  1 subnet is currently in the pool
  Current index      IP address range      Leased/Excluded/Total
  192.168.80.1       192.168.80.1 - 192.168.80.254    4 / 22 / 254
```

Rysunek 10. Konfiguracja puli adresów IP na Gateway_D

Usługa DHCP opiera się na wysyłaniu komunikatów broadcast, co oznacza, że przesyła informacje do wszystkich urządzeń w sieci. Niestety, taka otwarta natura może stanowić ryzyko, gdyż ktoś z zewnątrz może skutecznie zasypać serwer DHCP ciągłymi żądaniem o przydzielenie adresu IP, co może sparaliżować jego działanie. W takim przypadku, podejście niezaufanej jednostki mogłoby również polegać na wprowadzeniu do sieci fałszywego serwera

DHCP, który zacznie przydzielanie adresów IP według własnego uznania. Rozwiązaniem tego problemu jest funkcjonalność DHCP Snooping, która polega na przypisywaniu konkretnego, zaufanego portu dla serwera DHCP. Dzięki temu zabiegowi uniemożliwia się podłączenie nieautoryzowanego serwera do sieci, który próbowałby obsługiwać komunikaty DHCP. Dodatkowo, funkcja ta pozwala na ograniczenie ilości komunikatów DHCP Discover wysyłanych z innych portów. W ten sposób DHCP Snooping pomaga zabezpieczyć funkcjonowanie usługi DHCP przed niepożądanymi ingerencjami i zapewnia stabilność działania sieci.

```
Zamowienia#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
70,80
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)
FastEthernet0/3	no	10
FastEthernet0/1	no	10
FastEthernet0/2	no	10
FastEthernet0/9	no	10
FastEthernet0/7	no	10
FastEthernet0/6	no	10
FastEthernet0/10	no	10
FastEthernet0/4	no	10
FastEthernet0/5	no	10
FastEthernet0/8	no	10
FastEthernet0/19	no	10
FastEthernet0/12	no	10
FastEthernet0/17	no	10
FastEthernet0/23	no	10
FastEthernet0/14	no	10
FastEthernet0/11	no	10
FastEthernet0/13	no	10
FastEthernet0/15	no	10
FastEthernet0/16	no	10
FastEthernet0/18	no	10
FastEthernet0/20	no	10
FastEthernet0/21	no	10
FastEthernet0/22	no	10
FastEthernet0/24	no	10
GigabitEthernet0/1	yes	unlimited
GigabitEthernet0/2	yes	unlimited

```
Zamowienia#
```

Rysunek 11. Konfiguracja DHCP Snooping na przełączniku Zamowienia

W celu wdrożenia mechanizmu DHCP Snooping na urządzeniu sieciowym, wykonano następujące kroki:

- Włączono funkcję DHCP Snooping (*ip dhcp snooping*)
- Zdefiniowano zaufane porty, na których ruch DHCP nie będzie podlegał kontroli DHCP Snooping (*int range g0/1-2, ip dhcp snooping trust*)

- Ograniczono liczbę komunikatów DHCP Discover na portach FastEthernet 0/1 do 0/24 do maksymalnie 10 na sekundę (*int range f0/1-24, ip dhcp snooping limit rate 10*)
- Określono, które VLAN-y (VLAN 70 i 80) będą objęte kontrolą DHCP Snooping (*ip dhcp snooping vlan 70,80*)

4.3. STP

STP ma za zadanie utrzymywać tylko jednej aktywnej ścieżki od nadawcy do odbiorcy w sieci kiedy są nadmiarowe połączenia. Połączenia nadmiarowe są dezaktywowane, dzięki czemu nie występuje pętla ramek. Jeśli jedno z połączeń będzie miało awarię wtedy zostanie uruchomione inne, aby zachować ciągłość pracy. Poniżej pokazano przykład skonfigurowanego STP na DS3 dla VLAN-ów 50, 60, 70, 80, 90. Możemy zauważyć, że VLAN 50, 60 STP mają skonfigurowany jako główny na przełączniku DS3, a jako zastępczy dla VLAN 70, 80.

```
VLAN0050
Spanning tree enabled protocol rstp
Root ID    Priority    24626
           Address    00D0.D3D0.18B4
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    24626 (priority 24576 sys-id-ext 50)
           Address    00D0.D3D0.18B4
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 20

VLAN0060
Spanning tree enabled protocol rstp
Root ID    Priority    24636
           Address    00D0.D3D0.18B4
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    24636 (priority 24576 sys-id-ext 60)
           Address    00D0.D3D0.18B4
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 20

VLAN0070
Spanning tree enabled protocol rstp
Root ID    Priority    24646
           Address    000A.41DB.558E
           Cost        3
           Port        29(Port-channell)
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    28742 (priority 28672 sys-id-ext 70)
           Address    00D0.D3D0.18B4
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 20

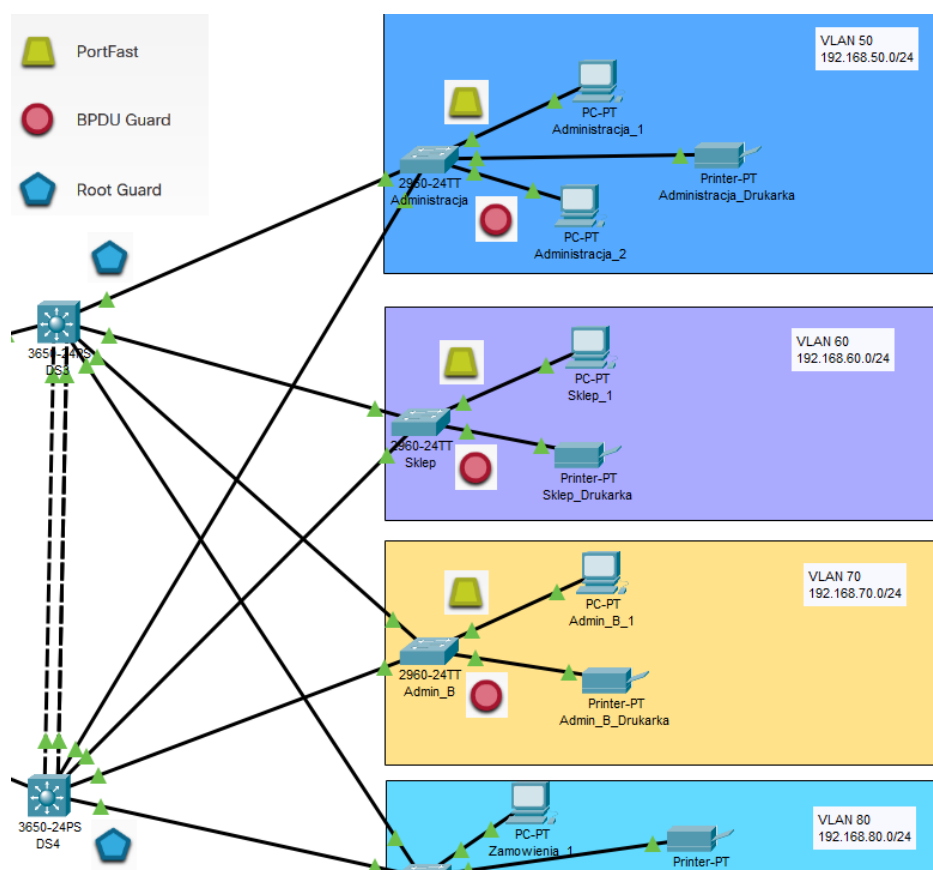
VLAN0080
Spanning tree enabled protocol rstp
Root ID    Priority    24656
           Address    000A.41DB.558E
           Cost        3
           Port        29(Port-channell)
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    28752 (priority 28672 sys-id-ext 80)
           Address    00D0.D3D0.18B4
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 20
```

Rysunek 12. Konfiguracja STP na DS3

Aby załagodzić ataki manipulacyjne STP, zostały zastosowane mechanizmy stabilności STP:

- **PortFast** to funkcja na przełącznikach Cisco, która eliminuje opóźnienia w ustanawianiu łączności na porcie przełącznika, przyspieszając proces przechodzenia portu z trybu blocking (blokowania) do trybu forwarding (przekazywania). Jest zazwyczaj używana na portach podłączonych do urządzeń końcowych, takich jak komputery lub drukarki.
- **BPDU Guard** to funkcja, która wyłącza port, jeśli ten port otrzymuje jakiekolwiek BPDUs (Bridge Protocol Data Units). Jest to zabezpieczenie przed sytuacjami, w których nieuprawnione urządzenie próbuje zostać mostem w sieci, co może prowadzić do pętli broadcastowych.
- **Root Guard** to mechanizm, który uniemożliwia portowi przełącznika przejęcie roli korzenia (root bridge) w drzewie rozpinającym (spanning tree). Chroni przed przypadkowym lub złośliwym przejęciem kontroli nad siecią przez nieuprawniony port.



Rysunek 13. Fragment topologii, w jaki sposób zostały skonfigurowane mechanizmy stabilności

4.4. Etherchannel

Jak można zauważyć przełączniki DS1 i DS2 oraz DS3 i DS4 są ze sobą połączone w razie awarii jednego z ruterów. Jednocześnie między przełącznikami występuje połączenie trzema kablami, w razie awarii jednego z nich nadal sieć będzie działać. Stosując takie połączenie należało zastosować Etherchannel a dokładniej LaCP. LaCP to protokół umożliwiający dynamiczną konfigurację EtherChannel. Pozwala na automatyczną agregację łączy, negocjowanie i monitorowanie połączeń EtherChannel między urządzeniami. LaCP pomaga w unikaniu konfliktów konfiguracyjnych poprzez dynamiczną synchronizację ustawień między połączonymi urządzeniami.

```
DS4#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)        LACP        Gig1/0/22(P) Gig1/0/23(P) Gig1/0/24(P)
```

Rysunek 14. Konfiguracja Etherchannel na DS4

4.5. HSRP

Projektując sieć zostało zastosowane HSRP, dzięki czemu sieć jest bardziej odporna na fizyczne uszkodzenia. Celem protokołu jest nieprzerwane działanie sieci w przypadku awarii jednej z bram. Jeden z ruterów działa w stanie aktywnym, a drugi w trybie czuwania. Jeśli ruter będący aktywnym zostanie uszkodzony, wtedy drugi ruter przejmie jego wszystkie obowiązki. Konfiguracja w sieci:

- Budynek A:
 - Gateway_A jest w stanie aktywnym dla VLANów 10, 20, 30
 - Gateway_B jest w stanie aktywnym dla VLANów 40, 99
- Budynek B:
 - Gateway_C jest w stanie aktywnym dla VLANów 50, 60
 - Gateway_D jest w stanie aktywnym dla VLANów 70, 80


```

Gateway_D#show standby
GigabitEthernet0/0/0.50 - Group 6
  State is Standby
    12 state changes, last state change 00:00:01
  Virtual IP address is 192.168.50.254
  Active virtual MAC address is 0000.0C07.AC06
    Local virtual MAC address is 0000.0C07.AC06 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.35 secs
  Preemption disabled
  Active router is 192.168.50.1
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Gig-6 (default)
GigabitEthernet0/0/0.60 - Group 7
  State is Standby
    9 state changes, last state change 00:00:01
  Virtual IP address is 192.168.60.254
  Active virtual MAC address is 0000.0C07.AC07
    Local virtual MAC address is 0000.0C07.AC07 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.411 secs
  Preemption disabled
  Active router is 192.168.60.1, priority 150 (expires in 6 sec)
    MAC address is 0000.0C07.AC07
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Gig-7 (default)
GigabitEthernet0/0/0.70 - Group 8
  State is Active
    4 state changes, last state change 00:00:18
  Virtual IP address is 192.168.70.254
  Active virtual MAC address is 0000.0C07.AC08
    Local virtual MAC address is 0000.0C07.AC08 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.539 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.70.1, priority 100 (expires in 7 sec)
  Priority 150 (configured 150)
  Group name is hsrp-Gig-8 (default)
GigabitEthernet0/0/0.80 - Group 9
  State is Active
    4 state changes, last state change 00:00:18
  Virtual IP address is 192.168.80.254
  Active virtual MAC address is 0000.0C07.AC09
    Local virtual MAC address is 0000.0C07.AC09 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.919 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.80.1, priority 100 (expires in 9 sec)
  Priority 150 (configured 150)
  Group name is hsrp-Gig-9 (default)

```

Rysunek 15. Konfiguracja HSRP na Gateway_D

4.6. EIGRP

W sieci zastosowano routing dynamiczny EIGRP, który pozwala na komunikację między wszystkimi VLAN-ami w sieci.

```

Gateway_A#show ip eigrp neighbors
IP-EIGRP neighbors for process 100

```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	10.0.0.2	Se0/1/0	12	00:00:00	40	1000	0	37
1	10.0.0.6	Se0/1/1	11	353141:45:1940		1000	0	25
2	192.168.99.2	Gig	12	353141:44:1940		1000	0	37
3	192.168.10.2	Gig	14	353141:44:1840		1000	0	38
4	192.168.40.2	Gig	13	353141:44:1640		1000	0	39
5	192.168.30.2	Gig	13	353141:42:5340		1000	0	40
6	192.168.20.2	Gig	14	353141:42:5340		1000	0	41

Rysunek 16. Informacje o sąsiadach dla Gateway_A

```

Gateway_A# show ip route eigrp
10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
D    10.0.0.0/8 is a summary, 00:59:27, Null0
D    10.0.0.8/30 [90/2681856] via 10.0.0.6, 00:59:20, Serial0/1/1
D    10.0.0.12/30 [90/2681856] via 10.0.0.2, 00:59:20, Serial0/1/0
D    10.0.0.16/30 [90/3193856] via 10.0.0.2, 00:59:20, Serial0/1/0
    [90/3193856] via 10.0.0.6, 00:59:20, Serial0/1/1
D    10.0.0.20/30 [90/3705856] via 10.0.0.2, 00:59:19, Serial0/1/0
    [90/3705856] via 10.0.0.6, 00:59:19, Serial0/1/1
D    192.168.1.0/24 [90/3196672] via 10.0.0.2, 00:59:17, Serial0/1/0
    [90/3196672] via 192.168.99.2, 00:58:19, GigabitEthernet0/0/0.99
    [90/3196672] via 192.168.10.2, 00:58:18, GigabitEthernet0/0/0.10
    [90/3196672] via 192.168.40.2, 00:58:16, GigabitEthernet0/0/0.40
    [90/3196672] via 192.168.30.2, 00:56:54, GigabitEthernet0/0/0.30
    [90/3196672] via 192.168.20.2, 00:56:54, GigabitEthernet0/0/0.20
192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
D    192.168.50.0/24 [90/2172416] via 10.0.0.2, 00:59:20, Serial0/1/0
D    192.168.60.0/24 [90/2172416] via 10.0.0.2, 00:59:20, Serial0/1/0
D    192.168.70.0/24 [90/2172416] via 10.0.0.2, 00:59:20, Serial0/1/0
D    192.168.80.0/24 [90/2172416] via 10.0.0.2, 00:59:20, Serial0/1/0

```

Rysunek 17. Tablica routingu

4.7. NTP

NTP służy do synchronizacji zegarów na urządzeniach sieciowych w całej sieci. Ustawiony serwer z NTP:

NTP

Service ☒ On ☐ Off

Authentication

☒ Enable ☐ Disable

Key: Password:

listopad, 2023 09:21:42PM

pon.	wt.	śr.	czw.	pt.	sob.	niedz.
30	31	1	2	3	4	5
6	7	8	9	10	11	12
..

Rysunek 18. Serwer NTP

```

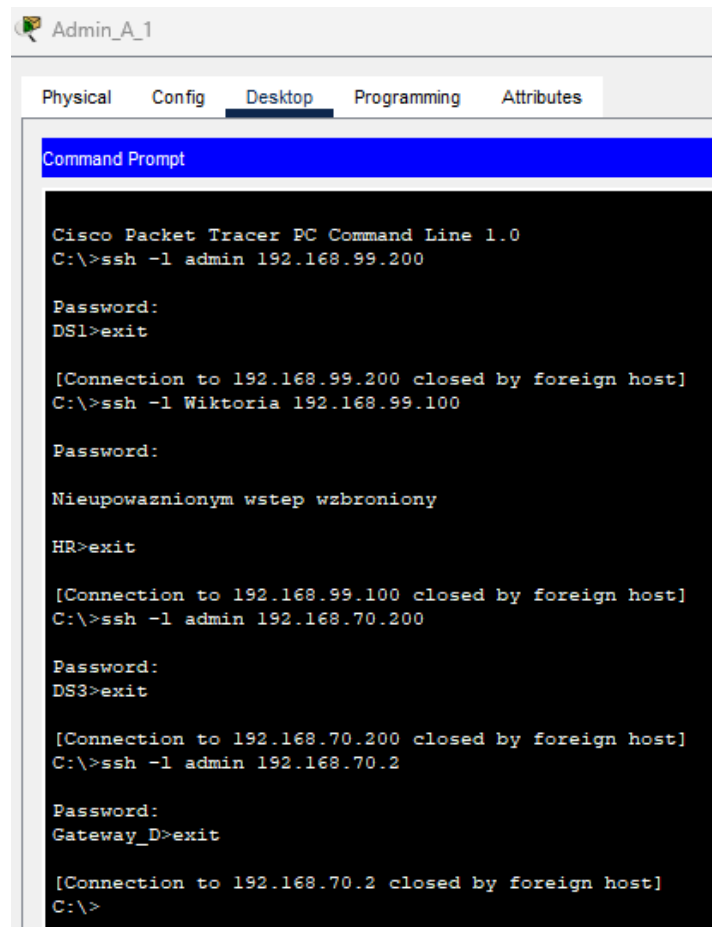
Gateway_B#show ntp sta
Clock is synchronized, stratum 2, reference is 192.168.40.3
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E8CD9B9E.0000015E (21:20:30.350 UTC Sat Nov 11 2023)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 122.56 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 15 sec ago.

```

Rysunek 19. Status NTP na Gateway_B

4.8. SSH

SSH jest to protokół zdalnego dostępu, który umożliwia zdalne łączenie się z przełącznikami, serwerami czy ruterami, stosując szyfrowaną komunikację.



```
Admin_A_1
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.99.200

Password:
DSL>exit

[Connection to 192.168.99.200 closed by foreign host]
C:\>ssh -l Wiktoria 192.168.99.100

Password:
Nieupowaznionym wstep wzbroniony
HR>exit

[Connection to 192.168.99.100 closed by foreign host]
C:\>ssh -l admin 192.168.70.200

Password:
DS3>exit

[Connection to 192.168.70.200 closed by foreign host]
C:\>ssh -l admin 192.168.70.2

Password:
Gateway_D>exit

[Connection to 192.168.70.2 closed by foreign host]
C:\>
```

Rysunek 20. Dostęp SSH z PC admina

4.9. Syslog

Syslog to protokół komunikacyjny używany w sieciach komputerowych do zbierania, przesyłania i zarządzania logami z różnych urządzeń i aplikacji. Jest szeroko stosowany w systemach operacyjnych, serwerach, routerach, przełącznikach i innych urządzeniach sieciowych. Głównym celem sysloga jest dostarczenie centralnego mechanizmu zbierania i przechowywania logów z wielu źródeł w sieci. Dzięki temu administratorzy mogą monitorować i analizować zdarzenia systemowe, ostrzeżenia bezpieczeństwa, błędy aplikacji oraz inne ważne informacje, które pomagają w diagnozowaniu problemów, audycji bezpieczeństwa i śledzeniu aktywności w sieci. Aby pobierał on logi od urządzeń należy wykonać tylko dwie komendy:

- service timestamps log datetime msec

- logging 192.168.40.20

Syslog

Syslog

Service ☒ On ☐ Off

	Time	HostName	Message
1	11.11.2023 08:22:57.007 PM	192.168.99.201	%LINK-5-CHANGED: Interface Port-...
2	11.11.2023 08:22:57.007 PM	192.168.99.201	%LINEPROTO-5-UPDOWN: Line ...
3	11.11.2023 08:22:58.066 PM	192.168.40.2	%DUAL-5-NBRCHANGE: IP-EIGRP ...
4	11.11.2023 08:23:16.235 PM	10.0.0.10	%HSRP-6-STATECHANGE: ...
5	11.11.2023 08:23:16.248 PM	10.0.0.10	%HSRP-6-STATECHANGE: ...
6	11.11.2023 08:23:01.618 PM	192.168.40.2	%HSRP-6-STATECHANGE: ...
7	11.11.2023 08:23:16.771 PM	10.0.0.10	%DUAL-5-NBRCHANGE: IP-EIGRP ...
8	11.11.2023 08:23:03.185 PM	192.168.40.2	%HSRP-6-STATECHANGE: ...
9	11.11.2023 08:23:05.230 PM	192.168.40.2	%HSRP-6-STATECHANGE: ...
10	11.11.2023 08:23:21.416 PM	10.0.0.10	%DUAL-5-NBRCHANGE: IP-EIGRP ...
11	11.11.2023 08:23:07.959 PM	192.168.40.2	%DUAL-5-NBRCHANGE: IP-EIGRP ...
12	11.11.2023 08:23:23.259 PM	10.0.0.10	%DUAL-5-NBRCHANGE: IP-EIGRP ...
13	11.11.2023 08:23:25.176 PM	10.0.0.10	%HSRP-6-STATECHANGE: ...
14	11.11.2023 08:23:28.046 PM	10.0.0.10	%HSRP-6-STATECHANGE: ...

Rysunek 21. Fragment logów z serwera

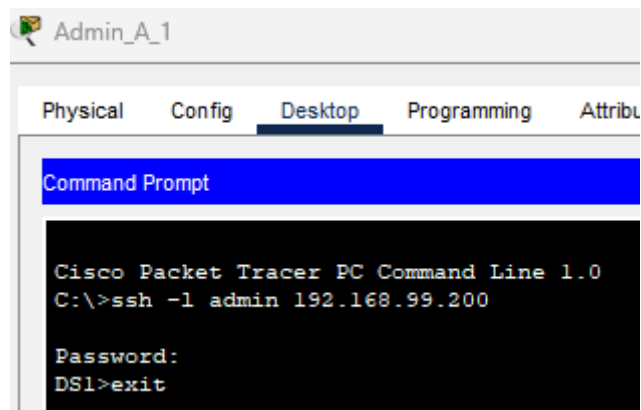
4.10. ACL

ACL (Access Control List) to lista kontroli dostępu, która służy do zarządzania uprawnieniami i kontrolowania dostępu do zasobów w sieci komputerowej lub systemie operacyjnym. ACL definiuje, które użytkownicy, grupy użytkowników lub hosty mają prawo do korzystania z określonych zasobów lub wykonania określonych operacji. W topologii zostały wykorzystane do blokowania VLAN-om dostępu do SSH, z wyjątkiem Adminów.

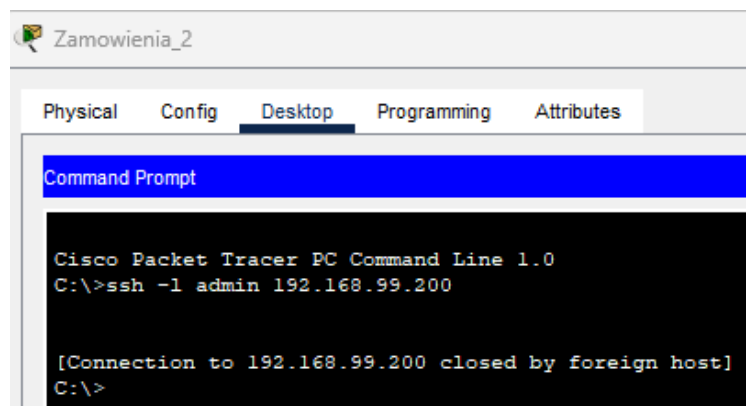
```
Gateway_C#show ip access-lists
Extended IP access list sl_def_acl
 0 deny tcp any any eq telnet
 0 deny tcp any any eq www
 0 deny tcp any any eq 22
 0 permit tcp any any eq 22
Extended IP access list ADMIN_SSH
10 permit tcp 192.168.99.0 0.0.0.255 any eq 22
20 permit tcp 192.168.70.0 0.0.0.255 any eq 22
30 deny tcp any any eq 22
```

Rysunek 22. Konfiguracja ACL dostępu do SSH

Testy połączenia:



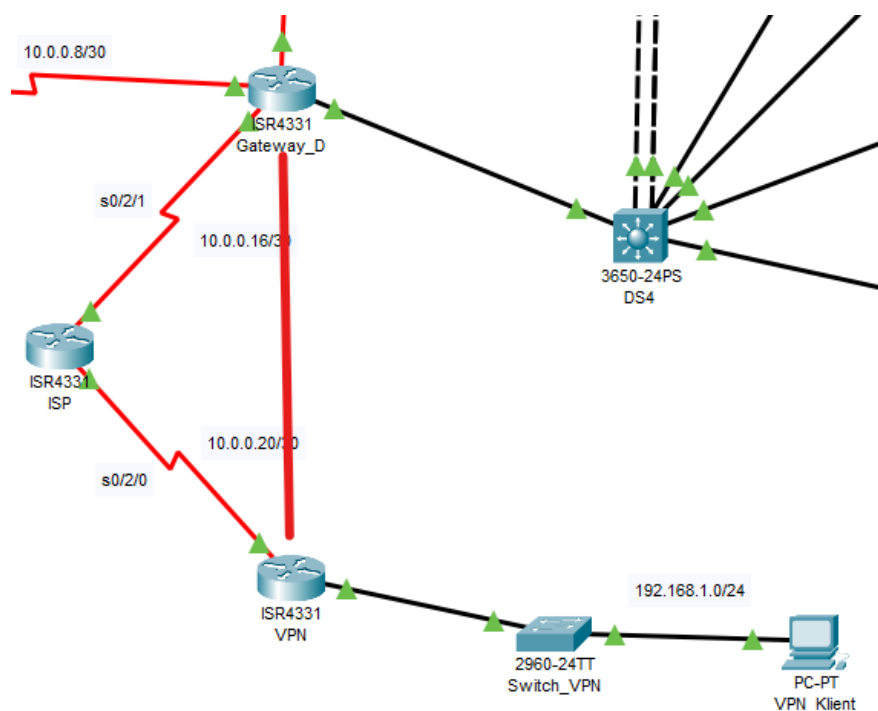
Rysunek 23. Dostęp do SSH z konta admina



Rysunek 24. Brak dostępu do SSH z działu zamówienia

4.11. VPN

VPN IPsec Site-to-Site jest technologią, która umożliwia bezpieczne połączenie dwóch oddzielnych sieci lokalnych (site) poprzez publiczną infrastrukturę, taką jak Internet. W przypadku VPN IPsec Site-to-Site tworzone jest bezpieczne, zaszyfrowane połączenie pomiędzy bramkami VPN znajdującymi się na granicach obu sieci. Zastosowany VPN (na czerwono):



Rysunek 25. Fragment topologii – VPN

```
Gateway_D#show crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
Peer = 10.0.0.22
Extended IP access list 110
  access-list 110 permit ip 192.168.50.0 0.0.0.255 192.168.1.0 0.0.0.255
  access-list 110 permit ip 192.168.60.0 0.0.0.255 192.168.1.0 0.0.0.255
  access-list 110 permit ip 192.168.70.0 0.0.0.255 192.168.1.0 0.0.0.255
  access-list 110 permit ip 192.168.80.0 0.0.0.255 192.168.1.0 0.0.0.255
  access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.1.0 0.0.0.255
  access-list 110 permit ip 192.168.20.0 0.0.0.255 192.168.1.0 0.0.0.255
  access-list 110 permit ip 192.168.30.0 0.0.0.255 192.168.1.0 0.0.0.255
  access-list 110 permit ip 192.168.40.0 0.0.0.255 192.168.1.0 0.0.0.255
  access-list 110 permit ip 192.168.99.0 0.0.0.255 192.168.1.0 0.0.0.255
Current peer: 10.0.0.22
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={
  VPN-SET,
}
Interfaces using crypto map VPN-MAP:
  Serial0/2/1
```

Rysunek 26. Konfiguracja VPN i ACL

Została skonfigurowana lista kontrolna dostępu (ACL) o numerze 110 zawiera kilka reguł, które pozwalają na ruch między podsieciami 192.168.1.0/24 a innymi podsieciami. Utworzono politykę isakmp o numerze 10, używając szyfrowania AES-256, autentykacji pre-share, i grupy Diffie-Hellman 5. Skonfigurowano klucz isakmp. Skonfigurowano zestaw transformacji IPsec o nazwie VPN-SET, używając szyfrowania AES i autentykacji SHA-HMAC. Utworzono mapę kryptograficzną o nazwie VPN-MAP i numerze 10, która łączy politykę isakmp, zestaw

transformacji IPsec oraz listę ACL. Przypisano mapę kryptograficzną VPN-MAP do odpowiednich interfejsów.

Testy VPN:

```
C:\>tracert 192.168.10.4

Tracing route to 192.168.10.4 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.1.1
  2  6 ms    0 ms    0 ms    10.0.0.21
  3  1 ms    18 ms   15 ms   10.0.0.17
  4  23 ms   1 ms    18 ms   10.0.0.9
  5  *        8 ms    11 ms   192.168.10.4

Trace complete.
```

Rysunek 27. Połączenie bez VPN

```
C:\>tracert 192.168.10.4

Tracing route to 192.168.10.4 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.1.1
  2  *        8 ms    2 ms    10.0.0.17
  3  27 ms    8 ms    3 ms    10.0.0.9
  4  4 ms     9 ms    8 ms    192.168.10.4

Trace complete.
```

Rysunek 28. Połączenie z VPN

4.12. AAA

AAA oznacza Authentication, Authorization oraz Accounting.

- Uwierzytelnienie – sprawdzenie czy dany użytkownik jest faktycznie tym za kogo się podaje,
- Autoryzacja – weryfikowanie do jakich zasobów konkretny użytkownik ma dostęp,
- Accounting – zbieranie informacji – logów o czynnościach jakie wykonał użytkownik.

AAA może wykorzystywać lokalną bazę użytkowników lub bazę na serwerach logowania, które mogą wykorzystywać protokół uwierzytelniania RADIUS lub TACACS+. W topologii użyto drugiego protokołu. Poniżej znajduje się konfiguracja na urządzeniu oraz na serwerze:

```
aaa new-model
!
aaa authentication login default group tacacs+ local
tacacs-server host 192.168.40.3
tacacs-server key GD_haslo
,
```

Rysunek 29. Konfiguracja AAA na routerze

AAA

Service ☒ On ☐ Off Radius Port

Network Configuration

Client Name Client IP

Secret ServerType

	Client Name	Client IP	Server Type	Key
1	GD	10.0.0.10	Tacacs	GD_haslo
2	GC	10.0.0.2	Tacacs	GC_haslo
3	GA	192.168.40.1	Tacacs	GA_haslo
4	GB	192.168.40.2	Tacacs	GB_haslo
5	DS3	192.168.70.200	Tacacs	DS3_haslo
6	DS4	192.168.70.201	Tacacs	DS4_haslo

Add
Save
Remove

User Setup

Username Password

	Username	Password
1	admin	admin123

Add

Rysunek 30. Konfiguracja AAA na serwerze

4.13. SNMP

SNMP (Simple Network Management Protocol) jest protokołem używanym do monitorowania i zarządzania urządzeniami sieciowymi. SNMPv1 jest jedną z wersji tego protokołu. SNMPv1 wprowadza pewne aspekty bezpieczeństwa, ale jego zabezpieczenia są ograniczone. Używa jedynie prostego mechanizmu uwierzytelniania opartego na "community strings". Działa to w sposób podobny do hasła, gdzie urządzenie i system zarządzający muszą używać tego samego "community string" do komunikacji. Istnieją dwa rodzaje "community strings" w SNMPv1: "read-only" (do odczytu) i "read-write" (do odczytu i zapisu). Obejmuje to publiczne "community string" (domyślnie "public") do odczytu oraz prywatne "community string" (domyślnie "private") do odczytu i zapisu.

```
Gateway_A#show running-config | include snmp
snmp-server community admin RW
Gateway_A#
```

Rysunek 31. Gateway_A z SNMP

4.14. Konfiguracja poziomów dostępowych na urządzeniach sieciowych

Konfiguracja poziomów dostępowych na urządzeniach sieciowych odnosi się zazwyczaj do zarządzania dostępem do tych urządzeń poprzez role użytkowników i przyznawanie im odpowiednich uprawnień. Zostały utworzone konta użytkowników, którzy będą korzystać z urządzeń. Każdy użytkownik ma nadaną unikalną nazwę użytkownika i hasło. Został skonfigurowany protokół dostępowy SSH, w celu umożliwienia dostępu do urządzeń. Również zastosowano mechanizmy AAA. Hasła zostały zaszyfrowane za pomocą algorytmów szyfrujących.

5. Przykłady plików konfiguracyjnych urządzeń

5.1. Gateway_A

```
Current configuration : 4366 bytes
!
version 15.4
service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 8
!
hostname Gateway_A
!
login block-for 120 attempts 3 within 60
!
!
enable secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
!
ip dhcp relay information trust-all
!
!
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.10.2
ip dhcp excluded-address 192.168.10.254
ip dhcp excluded-address 192.168.10.255
ip dhcp excluded-address 192.168.20.1
ip dhcp excluded-address 192.168.20.2
ip dhcp excluded-address 192.168.20.254
ip dhcp excluded-address 192.168.20.255
ip dhcp excluded-address 192.168.30.1
ip dhcp excluded-address 192.168.30.2
ip dhcp excluded-address 192.168.30.254
ip dhcp excluded-address 192.168.30.255
ip dhcp excluded-address 192.168.99.1
ip dhcp excluded-address 192.168.99.2
ip dhcp excluded-address 192.168.99.254
ip dhcp excluded-address 192.168.99.255
```

```

ip dhcp excluded-address 192.168.99.100
ip dhcp excluded-address 192.168.99.101
ip dhcp excluded-address 192.168.99.102
ip dhcp excluded-address 192.168.99.103
ip dhcp excluded-address 192.168.99.104
ip dhcp excluded-address 192.168.99.200
ip dhcp excluded-address 192.168.99.201
ip dhcp excluded-address 192.168.40.1
ip dhcp excluded-address 192.168.40.2
ip dhcp excluded-address 192.168.40.254
ip dhcp excluded-address 192.168.40.255
ip dhcp excluded-address 192.168.40.3
!
ip dhcp pool vlan10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.254
ip dhcp pool vlan20
network 192.168.20.0 255.255.255.0
default-router 192.168.20.254
ip dhcp pool vlan30
network 192.168.30.0 255.255.255.0
default-router 192.168.30.254
ip dhcp pool vlan99
network 192.168.99.0 255.255.255.0
default-router 192.168.99.254
ip dhcp pool vlan40
network 192.168.40.0 255.255.255.0
default-router 192.168.40.254
!
!
aaa new-model
!
aaa authentication login default group tacacs+ local
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Wiktoria secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
username admin secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
!
!
!

```



```

!
!
!
!
!
no ip domain-lookup
ip domain-name kisiegarnia.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0/0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
standby 1 ip 192.168.10.254
standby 1 priority 150
standby 1 preempt
!
interface GigabitEthernet0/0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
standby 2 ip 192.168.20.254
standby 2 priority 150
standby 2 preempt
!
interface GigabitEthernet0/0/0.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
standby 3 ip 192.168.30.254
standby 3 priority 150
standby 3 preempt
!
interface GigabitEthernet0/0/0.40
encapsulation dot1Q 40
ip address 192.168.40.1 255.255.255.0
standby 4 ip 192.168.40.254
!
interface GigabitEthernet0/0/0.99
encapsulation dot1Q 99
ip address 192.168.99.1 255.255.255.0

```

```

standby 5 ip 192.168.99.254
!
interface GigabitEthernet0/0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
ip address 10.0.0.1 255.255.255.252
!
interface Serial0/1/1
ip address 10.0.0.5 255.255.255.252
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
network 192.168.10.0
network 192.168.20.0
network 192.168.30.0
network 192.168.99.0
network 192.168.40.0
network 10.0.0.0 0.0.0.3
network 10.0.0.4 0.0.0.3
auto-summary
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
ip access-list extended ADMIN_SSH
permit tcp 192.168.99.0 0.0.0.255 any eq 22
permit tcp 192.168.70.0 0.0.0.255 any eq 22
deny tcp any any eq 22
!
banner motd ^CNieupowaznionym wstep wzbroniony^C

```

```

!
tacacs-server host 192.168.40.3
tacacs-server key GA_haslo
!
!
snmp-server community admin RW
!
logging 192.168.40.3
line con 0
password 7 082048430017544541
!
line aux 0
!
line vty 0 4
access-class ADMIN_SSH in
password 7 08204843001745464058
transport input ssh
line vty 5 15
password 7 08204843001745464058
!
!
ntp authentication-key 1 md5 082048430017544541 7
ntp authenticate
ntp trusted-key 1
ntp server 192.168.40.3
!
end

```

5.2. DS1

```

Current configuration : 3444 bytes
!
version 16.3.2
service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname DS1
!
login block-for 120 attempts 3 within 60
!
enable secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
!
!
!
!
!
aaa new-model
!
aaa authentication login default group tacacs+ local
!

```

```

!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Wiktoria secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
username admin secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
!
!
!
!
!
!
!
!
!
!
!
ip dhcp snooping vlan 10,20,30,40,99
ip dhcp snooping
!
ip domain-name kisiegarnia.com
!
!
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30 priority 24576
spanning-tree vlan 40,99 priority 28672
!
!
!
!
!
!
!
interface Port-channel1
switchport mode trunk
!
interface GigabitEthernet1/0/1
ip dhcp snooping trust
switchport trunk native vlan 99
switchport mode trunk
spanning-tree guard root
!
interface GigabitEthernet1/0/2
ip dhcp snooping trust
switchport trunk native vlan 99
switchport mode trunk

```

```
spanning-tree guard root
!
interface GigabitEthernet1/0/3
ip dhcp snooping trust
switchport trunk native vlan 99
switchport mode trunk
spanning-tree guard root
!
interface GigabitEthernet1/0/4
ip dhcp snooping trust
switchport trunk native vlan 99
switchport mode trunk
spanning-tree guard root
!
interface GigabitEthernet1/0/5
ip dhcp snooping trust
switchport trunk native vlan 99
switchport mode trunk
spanning-tree guard root
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
```

```

interface GigabitEthernet1/0/21
ip dhcp snooping trust
switchport mode trunk
!
interface GigabitEthernet1/0/22
ip dhcp snooping trust
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/23
ip dhcp snooping trust
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/24
ip dhcp snooping trust
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
mac-address 00e0.f77d.d601
ip address 192.168.99.200 255.255.255.0
!
ip default-gateway 192.168.99.1
ip classless
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
ip access-list extended ADMIN_SSH
permit tcp 192.168.99.0 0.0.0.255 any eq 22
permit tcp 192.168.70.0 0.0.0.255 any eq 22
deny tcp any any eq 22

```

```

!
banner motd ^CNieupowaznionym wstep wzbroniony^C
!
tacacs-server host 192.168.40.3
tacacs-server key DS1_haslo
!
!
!
logging 192.168.40.3
line con 0
password 7 082048430017544541
!
line aux 0
!
line vty 0 4
access-class ADMIN_SSH in
password 7 08204843001745464058
transport input ssh
line vty 5 15
password 7 08204843001745464058
!
!
!
ntp authentication-key 1 md5 082048430017544541 7
ntp authenticate
ntp trusted-key 1
ntp server 192.168.40.3
!
end

```

5.3. HR

```

Current configuration : 5576 bytes
!
version 15.0
service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname HR
!
enable secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
!
!
!
no ip domain-lookup
ip domain-name kisiegarnia.com
!
username Wiktoria secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
!
!

```

```
ip dhcp snooping vlan 10,99
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 10
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/2
switchport access vlan 10
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/3
switchport access vlan 10
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/5
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/6
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
```



```

!
interface FastEthernet0/7
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/8
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/9
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/10
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/11
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/12
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/13

```

```
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/14
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/15
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/16
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/17
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/18
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/19
switchport access vlan 999
ip dhcp snooping limit rate 10
```

```

switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/20
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/21
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/22
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/23
switchport access vlan 999
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface FastEthernet0/24
switchport access vlan 99
ip dhcp snooping limit rate 10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
shutdown
!
interface GigabitEthernet0/1
switchport trunk native vlan 99
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate

```

```

!
interface GigabitEthernet0/2
switchport trunk native vlan 99
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
ip address 192.168.99.100 255.255.255.0
!
ip default-gateway 192.168.99.1
!
banner motd ^CNieupowaznionym wstep wzbroniony^C
logging 192.168.40.3
!
!
!
ip access-list extended ADMIN_SSH
permit tcp 192.168.99.0 0.0.0.255 any eq 22
permit tcp 192.168.70.0 0.0.0.255 any eq 22
deny tcp any any eq 22
line con 0
password 7 082048430017544541
login
!
line vty 0 4
access-class ADMIN_SSH in
password 7 08204843001745464058
login local
transport input ssh
line vty 5 15
password 7 08204843001745464058
login
!
!
!
ntp authenticate
ntp trusted-key 1
ntp server 192.168.40.3
!
end

```