# Adresacja i podział na podsieci

Router R1

|  |
| --- |
| enable  configure terminal  hostname R1  ip name-server 8.8.8.8  interface fa0/0  ip address 192.168.1.1 255.255.255.0  no shutdown  exit  interface se2/0  ip address 192.168.10.1 255.255.255.252  no shutdown  exit  interface se3/0  ip address 192.168.10.5 255.255.255.252  no shutdown  exit |

Router R2

|  |
| --- |
| enable  configure terminal  hostname R2  ip name-server 8.8.8.8  interface fa0/0  ip address 192.168.2.1 255.255.255.0  no shutdown  exit  interface se2/0  ip address 192.168.10.2 255.255.255.252  no shutdown  exit  interface se3/0  ip address 192.168.10.9 255.255.255.252  no shutdown  exit |

Router R3

|  |
| --- |
| enable  configure terminal  hostname R3  ip name-server 8.8.8.8  interface fa0/0  ip address 192.168.3.1 255.255.255.0  no shutdown  exit  interface se2/0  ip address 192.168.10.6 255.255.255.252  no shutdown  exit  interface se3/0  ip address 192.168.10.10 255.255.255.252  no shutdown  exit |

Następnie dla każdej z podsieci ustalono statyczne **adresy IP, Default Gateway oraz Subnet Mask**. Aby to ustawić na urządzeniach w danej podsieci trzeba było wejść w **PC ->** **Desktop** **->** **IP Configuration**.

**Default Gateway** to adres IP routera z którym połączony jest Switch, czyli dla:

* S1 – 192.168.1.1
* S2 - 192.168.2.1
* S3, S4 – 192.168.3.1

**Subnet Mask** wszędzie jest 255.255.255.0

Adresy IP urządzeń zostały przydzielone jako kolejne adresy po DefaultGateway, czyli dla urządzeń połączonych z S1 było to: 192.168.1.2, 192.168.1.3, itd.

# VLANy

Switch S1

|  |
| --- |
| **Utworzenie Vlanów na Switchu S1** |
| enable  configure terminal  vlan 10  name PC\_VLAN  vlan 20  name Laptop\_VLAN  vlan 30  name Printer\_VLAN  vlan 40  name DHCP\_VLAN  exit |
| **Konfiguracja portów na Switchu S1** |
| interface range fa0/2-3  switchport mode access  switchport access vlan 10  exit  interface fa0/4  switchport mode access  switchport access vlan 20  exit  interface fa0/5  switchport mode access  switchport access vlan 40  exit  interface fa0/6  switchport mode access  switchport access vlan 30  exit |

Switch S2

|  |
| --- |
| **Utworzenie Vlanów na Switchu S2** |
| enable  configure terminal  vlan 10  name PC\_VLAN  vlan 20  name Laptop\_VLAN  vlan 30  name Printer\_VLAN  vlan 40  name DHCP\_VLAN  exit |
| **Konfiguracja portów na Switchu S2** |
| interface range fa0/2-3  switchport mode access  switchport access vlan 10  exit  interface fa0/4  switchport mode access  switchport access vlan 20  exit  interface fa0/5  switchport mode access  switchport access vlan 30  exit  interface fa0/6  switchport mode access  switchport access vlan 40  exit |

Switch S3

|  |
| --- |
| **Utworzenie Vlanów na Switchu S3** |
| enable  configure terminal  vlan 10  name PC\_VLAN  vlan 20  name Laptop\_VLAN  vlan 30  name Printer\_VLAN  vlan 40  name DHCP\_VLAN  exit |
| **Konfiguracja portów na Switchu S3** |
| interface fa0/4  switchport mode access  switchport access vlan 10  exit  interface fa0/3  switchport mode access  switchport access vlan 20  exit  interface fa0/5  switchport mode access  switchport access vlan 30  exit  interface fa0/2  switchport mode access  switchport access vlan 40  exit |
| **Konfiguracja uplink do Sniffera (port Fa0/6) - łączy S3 z S4 przez Sniffer** |
| interface fa0/6  switchport mode trunk  exit |

Switch S4

|  |
| --- |
| **Konfiguracja portów na Switchu S4** |
| interface fa0/2  switchport mode access  switchport access vlan 10  exit  interface fa0/3  switchport mode access  switchport access vlan 30  exit |
| **Konfiguracja uplink do Sniffera (port Fa0/1) - łączy S4 z S3 przez Sniffer** |
| interface fa0/1  switchport mode trunk  exit |

**Podsumowanie konfiguracji VLAN**

1. VLANy zostały zorganizowane według kategorii urządzeń:

* VLAN 10 (PC\_VLAN): Wszystkie komputery PC we wszystkich switchach.
* VLAN 20 (Laptop\_VLAN): Wszystkie laptopy.
* VLAN 30 (Printer\_VLAN): Wszystkie drukarki.
* VLAN 40 (DHCP\_VLAN): Wszystkie serwery DHCP.

1. Uplinki pomiędzy switchami (S3 i S4 oraz Sniffer) zostały skonfigurowane jako trunk, aby przesyłać dane z różnych VLANów.
2. Switch S4 i urządzenia podłączone do niego są traktowane jako część tej samej podsieci i VLANów co urządzenia S3.

# Serwer DHCP

Poniżej jest konfiguracja wszystkich serwerów DHCP w sieci

|  |  |  |
| --- | --- | --- |
| **DHCP1** | **DHCP2** | **DHCP3** |
| Serwer DHCP -> Desktop -> IP Configuration | | |
| IP Address: **192.168.1.6**  Subnet Mask: **255.255.255.0**  Default Gateway: **192.168.1.1**. | IP Address: **192.168.2.6**  Subnet Mask: **255.255.255.0**  Default Gateway: **192.168.2.1**. | IP Address: **192.168.3.7**  Subnet Mask: **255.255.255.0**  Default Gateway: **192.168.3.1**. |
| Serwer DHCP -> Services -> DHCP | | |
| Service: **ON**  Pool Name: **DHCP1\_Pool**  Default Gateway: **192.168.1.1**  DNS Server: **8.8.8.8**  Subnet Mask: **255.255.255.0**  Start IP: **192.168.1.100**  Max users: **156** | Service: **ON**  Pool Name: **DHCP2\_Pool**  Default Gateway: **192.168.2.1**  DNS Server: **8.8.8.8**  Subnet Mask: **255.255.255.0**  Start IP: **192.168.2.100**  Max users: **156** | Service: **ON**  Pool Name: **DHCP3\_Pool**  Default Gateway: **192.168.3.1**  DNS Server: **8.8.8.8**  Subnet Mask: **255.255.255.0**  Start IP: **192.168.3.100**  Max users: **156** |

# Konfiguracja urządzeń pod kątem dostępu SSH

Dane logowania

Login: admin

Hasło: cisco1234

Router R1

|  |
| --- |
| enable  configure terminal  hostname R1  ip domain-name wdc\_projekt.local  username admin privilege 15 password cisco1234  line vty 0 4  transport input ssh  login local  exit  crypto key generate rsa  1024 |

Router R2

|  |
| --- |
| enable  configure terminal  hostname R2  ip domain-name wdc\_projekt.local  username admin privilege 15 password cisco1234  line vty 0 4  transport input ssh  login local  exit  crypto key generate rsa  1024 |

Router R3

|  |
| --- |
| enable  configure terminal  hostname R3  ip domain-name wdc\_projekt.local  username admin privilege 15 password cisco1234  line vty 0 4  transport input ssh  login local  exit  crypto key generate rsa  1024 |

# Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS

NTP służy do synchronizacji czasu na wszystkich urządzeniach sieciowych. Dzięki temu logi, raporty i zdarzenia są spójne czasowo. Konfiguracja NTP przebiega jak poniżej:

1. Zidentyfikuj serwer NTP  
   Można wykorzystać publiczny serwer NTP, np. pool.ntp.org, lub skonfigurować jeden z routerów jako lokalny serwer NTP. **My wybieramy publiczny serwer.**
2. Konfiguracja routerów oraz switchy jako klientów NTP

**WAŻNE:** Aby urządzenie mogło zinterpretować serwer po nazwie, to musi mieć skonfigurowany DNS. Najczęściej używany DNS to 8.8.8.8. To właśnie z takich korzystają nasze routery oraz inne urządzenia, np. PC, laptopy, DHCP, drukarki.

Router R1

|  |
| --- |
| enable  configure terminal  ntp server pool.ntp.org prefer  ntp update-calendar  exit |

Pozostałe routery (R2, R3) i wszystkie switche (S1, S2, S3, S4)

|  |
| --- |
| enable  configure terminal  ntp server pool.ntp.org  ntp update-calendar  exit |

Dla routera R1 jest użyte słowo kluczowe „prefer”, które oznacza, że pozostałe urządzenia będą synchronizowały czas w pierwszej kolejności do serwera z tego urządzenia. Przy takim samym serwerze na każdym urządzeniu nie ma to większego znaczenia, ale w przypadku, gdy różne urządzenia mają różne serwery NTP jest to dosyć przydatne.

Sprawdzenie synchronizacji NTP na routerze lub switchu

|  |
| --- |
| show ntp status  show clock |

# Implementacja lokalnego SPAN

Konfiguracja Sniffera na Switchu S3

|  |
| --- |
| enable  configure terminal  monitor session 1 source vlan 10  monitor session 1 destination interface fa0/6 |

# Implementacja co najmniej jednej listy kontroli dostępu ACL wewnątrz zabezpieczonej sieci

Lista ACL została skonfigurowana na Routerze R1. Póki co jest to tylko lista ACL blokująca ruch do VLAN30, jednak nie jestem pewien czy nie trzeba tu stworzyć ZBF opartego na strefach internal i external tak jak w instrukcji na labach.

|  |
| --- |
| enable  configure terminal  access-list 100 deny ip any 192.168.1.0 0.0.0.255  access-list 100 permit ip any any  interface fa0/0  ip access-group 100 in |

# Kompletna konfiguracja urządzeń z projektu od Kuby

R1 PEŁNA KONFIGURACJA

|  |
| --- |
| enable  configure terminal  hostname R1  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip cef  no ipv6 cef  ip ssh version 2  ip domain-name michal.com  username admin password cisco  aaa new-model  aaa authentication login auth group tacacs+ local  tacacs-server host 192.168.10.2 key key  ntp server 192.168.10.2  interface FastEthernet0/0  ip address 192.168.1.1 255.255.255.192  ip access-group 1 in  ip access-group 1 out  duplex auto  speed auto  exit  interface FastEthernet0/0.20  encapsulation dot1Q 20  ip address 192.168.10.1 255.255.255.0  ip access-group 1 in  exit  interface FastEthernet1/0  no ip address  duplex auto  speed auto  shutdown  exit  interface Serial2/0  no ip address  clock rate 2000000  shutdown  exit  interface Serial3/0  no ip address  clock rate 2000000  shutdown  exit  interface FastEthernet4/0  ip address 192.168.2.1 255.255.255.0  exit  interface FastEthernet5/0  ip address 192.168.3.1 255.255.255.0  exit  ip route 192.168.1.64 255.255.255.192 192.168.2.2  ip route 192.168.1.128 255.255.255.192 192.168.3.2  ip route 192.168.20.0 255.255.255.0 192.168.2.2  ip route 192.168.30.0 255.255.255.0 192.168.3.2  access-list 1 deny host 192.168.10.3  access-list 1 permit any  logging 192.168.10.2  line con 0  login authentication auth  exit  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit  ip flow-export version 9  router rip  exit  ip classless  exit |

R2 PEŁNA KONFIGURACJA

|  |
| --- |
| enable  configure terminal  hostname R2  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip cef  no ipv6 cef  ip ssh version 2  ip domain-name michal.com  username admin password cisco  aaa new-model  aaa authentication login auth group tacacs+ local  tacacs-server host 192.168.20.2 key key  ntp server 192.168.20.2  interface FastEthernet0/0  ip address 192.168.1.65 255.255.255.192  duplex auto  speed auto  exit  interface FastEthernet0/0.30  encapsulation dot1Q 30  ip address 192.168.20.1 255.255.255.0  exit  interface FastEthernet1/0  no ip address  duplex auto  speed auto  shutdown  exit  interface Serial2/0  no ip address  clock rate 2000000  shutdown  exit  interface Serial3/0  no ip address  clock rate 2000000  shutdown  exit  interface FastEthernet4/0  ip address 192.168.2.2 255.255.255.0  exit  interface FastEthernet5/0  ip address 192.168.4.1 255.255.255.0  exit  ip route 192.168.1.0 255.255.255.192 192.168.2.1  ip route 192.168.1.128 255.255.255.192 192.168.4.2  ip route 192.168.10.0 255.255.255.0 192.168.2.1  ip route 192.168.30.0 255.255.255.0 192.168.4.2  logging 192.168.20.2  line con 0  login authentication auth  exit  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit  ip flow-export version 9  router rip  exit  ip classless  exit |

R3 PEŁNA KONFIGURACJA

|  |
| --- |
| enable  configure terminal  hostname R3  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip cef  no ipv6 cef  ip ssh version 2  ip domain-name michal.com  username admin password cisco  aaa new-model  aaa authentication login auth group tacacs+ local  tacacs-server host 192.168.30.2 key key  ntp server 192.168.30.2  interface FastEthernet0/0  ip address 192.168.1.129 255.255.255.192  ip access-group 101 in  ip access-group 101 out  duplex auto  speed auto  exit  interface FastEthernet0/0.40  encapsulation dot1Q 40  ip address 192.168.30.1 255.255.255.0  ip access-group 101 in  ip access-group 101 out  exit  interface FastEthernet1/0  no ip address  duplex auto  speed auto  shutdown  exit  interface Serial2/0  no ip address  clock rate 2000000  shutdown  exit  interface Serial3/0  no ip address  clock rate 2000000  shutdown  exit  interface FastEthernet4/0  ip address 192.168.3.2 255.255.255.0  ip access-group 1 in  ip access-group 1 out  exit  interface FastEthernet5/0  ip address 192.168.4.2 255.255.255.0  ip access-group 100 in  ip access-group 100 out  exit  ip route 192.168.1.0 255.255.255.192 192.168.3.1  ip route 192.168.1.64 255.255.255.192 192.168.4.1  ip route 192.168.10.0 255.255.255.0 192.168.3.1  ip route 192.168.20.0 255.255.255.0 192.168.4.1  logging 192.168.30.2  ip flow-export version 9  access-list 100 permit tcp 192.168.20.0 0.0.0.255 any eq 22  access-list 100 deny ip any any  access-list 101 deny tcp any any eq 22  access-list 101 permit ip any any  line con 0  login authentication auth  exit  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit  ip classless  exit |

S1 PEŁNA KONFIGURACJA

|  |
| --- |
| enable  configure terminal  hostname S1  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip ssh version 2  ip domain-name michal.com  username admin privilege 1 password cisco  aaa new-model  aaa authentication login auth group tacacs+ local  ntp server 192.168.10.2  spanning-tree mode pvst  spanning-tree extend system-id  interface FastEthernet0/1  switchport mode trunk  exit  interface FastEthernet0/2  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/3  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/4  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/5  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/6  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/7  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/8  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/9  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/10  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/11  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/12  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/13  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/14  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/15  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/16  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/17  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/18  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/19  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/21  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/22  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/23  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/24  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface GigabitEthernet0/1  exit  interface GigabitEthernet0/2  exit  interface Vlan1  no ip address  shutdown  exit  interface Vlan20  ip address 192.168.10.20 255.255.255.0  exit  logging 192.168.10.2  tacacs-server host 192.168.1.2 key key  tacacs-server host 192.168.10.20 key key  tacacs-server host 192.168.10.2 key key  line con 0  login  exit  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit  monitor session 1 source interface Fa0/3  monitor session 1 destination interface Fa0/4  exit |

S2 PEŁNA KONFIGURACJA

|  |
| --- |
| enable  configure terminal  hostname S2  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip ssh version 2  ip domain-name michal.com  username admin privilege 1 password cisco  aaa new-model  aaa authentication login auth group tacacs+ local  ntp server 192.168.20.2  spanning-tree mode pvst  spanning-tree extend system-id  interface FastEthernet0/1  switchport mode trunk  exit  interface FastEthernet0/2  switchport access vlan 30  switchport mode access  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/3  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/4  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/5  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/6  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/7  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/8  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/9  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/10  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/11  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/12  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/13  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/14  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/15  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/16  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/17  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/18  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/19  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/21  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/22  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/23  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/24  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface GigabitEthernet0/1  exit  interface GigabitEthernet0/2  exit  interface Vlan1  no ip address  shutdown  exit  interface Vlan30  ip address 192.168.20.30 255.255.255.0  exit  logging 192.168.20.2  tacacs-server host 192.168.20.2 key key  line con 0  login  exit  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit  monitor session 1 source interface Fa0/3  monitor session 1 destination interface Fa0/4  exit |

S3 PEŁNA KONFIGURACJA

|  |
| --- |
| enable  configure terminal  hostname S3  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip ssh version 2  ip domain-name michal.com  username admin privilege 1 password cisco  aaa new-model  aaa authentication login auth group tacacs+ local  ntp server 192.168.30.2  spanning-tree mode pvst  spanning-tree extend system-id  interface FastEthernet0/1  switchport mode trunk  exit  interface FastEthernet0/2  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/3  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/4  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/5  switchport access vlan 40  switchport mode access  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/6  switchport access vlan 40  switchport mode trunk  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/7  switchport access vlan 40  exit  interface FastEthernet0/8  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/9  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/10  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/11  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/12  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/13  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/14  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/15  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/16  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/17  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/18  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/19  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/21  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/22  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/23  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/24  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface GigabitEthernet0/1  exit  interface GigabitEthernet0/2  exit  interface Vlan1  no ip address  shutdown  exit  interface Vlan40  ip address 192.168.30.40 255.255.255.0  exit  logging 192.168.30.2  tacacs-server host 192.168.30.2 key key  line con 0  login  exit  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit  monitor session 1 source interface Fa0/3  monitor session 1 destination interface Fa0/4  exit |

S4 PEŁNA KONFIGURACJA

|  |
| --- |
| enable  configure terminal  hostname S4  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip ssh version 2  ip domain-name michal.com  username admin privilege 1 password cisco  aaa new-model  aaa authentication login auth group tacacs+ local  ntp server 192.168.30.2  spanning-tree mode pvst  spanning-tree extend system-id  interface FastEthernet0/1  switchport access vlan 2  switchport mode trunk  exit  interface FastEthernet0/2  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/3  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/4  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/5  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/6  switchport access vlan 2  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/7  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/8  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/9  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/10  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/11  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/12  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/13  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/14  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/15  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/16  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/17  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/18  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/19  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/21  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/22  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/23  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/24  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface GigabitEthernet0/1  exit  interface GigabitEthernet0/2  exit  interface Vlan1  no ip address  shutdown  exit  interface Vlan40  ip address 192.168.30.41 255.255.255.0  exit  logging 192.168.30.2  tacacs-server host 192.168.10.2 key key  tacacs-server host 192.168.40.2 key key  tacacs-server host 192.168.30.2 key key  line con 0  login  exit  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit  exit |

# Kompletna konfiguracja urządzeń z projektu od Kuby z podziałem na urządzenia

R1

|  |
| --- |
| **1. Adresacja:** |
| enable  configure terminal  hostname R1  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip cef  no ipv6 cef  ip domain-name michal.com  interface FastEthernet0/0  ip address 192.168.1.1 255.255.255.192  duplex auto  speed auto  exit  interface FastEthernet0/0.20  encapsulation dot1Q 20  ip address 192.168.10.1 255.255.255.0  exit  interface FastEthernet4/0  ip address 192.168.2.1 255.255.255.0  exit  interface FastEthernet5/0  ip address 192.168.3.1 255.255.255.0  exit  ip route 192.168.1.64 255.255.255.192 192.168.2.2  ip route 192.168.1.128 255.255.255.192 192.168.3.2  ip route 192.168.20.0 255.255.255.0 192.168.2.2  ip route 192.168.30.0 255.255.255.0 192.168.3.2 |
| **2. Podział na podsieci:** |
| enable  configure terminal  ip route 192.168.1.64 255.255.255.192 192.168.2.2  ip route 192.168.1.128 255.255.255.192 192.168.3.2  ip route 192.168.20.0 255.255.255.0 192.168.2.2  ip route 192.168.30.0 255.255.255.0 192.168.3.2 |
| **3. VLANy:** |
| enable  configure terminal  interface FastEthernet0/0.20  encapsulation dot1Q 20  ip address 192.168.10.1 255.255.255.0  exit |
| **4. Serwer DHCP:** |
| Brak konfiguracji serwera DHCP w dostarczonym fragmencie. |
| **5. Konfiguracja urządzeń pod kątem dostępu SSH:** |
| enable  configure terminal  ip ssh version 2  ip domain-name michal.com  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit |
| **6. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS:** |
| enable  configure terminal  ntp server 192.168.10.2  logging 192.168.10.2 |
| **7. Implementacja lokalnego SPAN:** |
| Brak konfiguracji lokalnego SPAN w dostarczonym fragmencie. |
| **8. Implementacja co najmniej jednej listy kontroli dostępu ACL wewnątrz zabezpieczonej sieci:** |
| enable  configure terminal  access-list 1 deny host 192.168.10.3  access-list 1 permit any |
| **9. Implementacja zabezpieczeń STP:** |
| Brak konfiguracji zabezpieczeń STP w dostarczonym fragmencie. |
| **10. Konfiguracja uwierzytelniania AAA na serwerze przy użyciu TACACS+ lub RADIUS:** |
| enable  configure terminal  aaa new-model  aaa authentication login auth group tacacs+ local  tacacs-server host 192.168.10.2 key key |
| **11. Zaprojektowanie zapory sieciowej typu Private and Public:** |
| Brak szczegółowej konfiguracji zapory sieciowej w dostarczonym fragmencie. |

R2

|  |
| --- |
| **1. Adresacja:** |
| enable  configure terminal  hostname R2  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip cef  no ipv6 cef  ip domain-name michal.com  interface FastEthernet0/0  ip address 192.168.1.65 255.255.255.192  duplex auto  speed auto  exit  interface FastEthernet0/0.30  encapsulation dot1Q 30  ip address 192.168.20.1 255.255.255.0  exit  interface FastEthernet4/0  ip address 192.168.2.2 255.255.255.0  exit  interface FastEthernet5/0  ip address 192.168.4.1 255.255.255.0  exit  ip route 192.168.1.0 255.255.255.192 192.168.2.1  ip route 192.168.1.128 255.255.255.192 192.168.4.2  ip route 192.168.10.0 255.255.255.0 192.168.2.1  ip route 192.168.30.0 255.255.255.0 192.168.4.2 |
| **2. Podział na podsieci:** |
| enable  configure terminal  ip route 192.168.1.0 255.255.255.192 192.168.2.1  ip route 192.168.1.128 255.255.255.192 192.168.4.2  ip route 192.168.10.0 255.255.255.0 192.168.2.1  ip route 192.168.30.0 255.255.255.0 192.168.4.2 |
| **3. VLANy:** |
| enable  configure terminal  interface FastEthernet0/0.30  encapsulation dot1Q 30  ip address 192.168.20.1 255.255.255.0  exit |
| **4. Serwer DHCP:** |
| Brak konfiguracji serwera DHCP w dostarczonym fragmencie. |
| **5. Konfiguracja urządzeń pod kątem dostępu SSH:** |
| enable  configure terminal  ip ssh version 2  ip domain-name michal.com  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit |
| **6. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS:** |
| enable  configure terminal  ntp server 192.168.20.2  logging 192.168.20.2 |
| **7. Implementacja lokalnego SPAN:** |
| Brak konfiguracji lokalnego SPAN w dostarczonym fragmencie. |
| **8. Implementacja co najmniej jednej listy kontroli dostępu ACL wewnątrz zabezpieczonej sieci:** |
| Brak konfiguracji ACL w dostarczonym fragmencie. |
| **9. Implementacja zabezpieczeń STP:** |
| Brak konfiguracji zabezpieczeń STP w dostarczonym fragmencie. |
| **10. Konfiguracja uwierzytelniania AAA na serwerze przy użyciu TACACS+ lub RADIUS:** |
| enable  configure terminal  aaa new-model  aaa authentication login auth group tacacs+ local  tacacs-server host 192.168.20.2 key key |
| **11. Zaprojektowanie zapory sieciowej typu Private and Public:** |
| Brak szczegółowej konfiguracji zapory sieciowej w dostarczonym fragmencie. |

R3

|  |
| --- |
| **1. Adresacja:** |
| enable  configure terminal  hostname R3  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip cef  no ipv6 cef  ip domain-name michal.com  interface FastEthernet0/0  ip address 192.168.1.129 255.255.255.192  ip access-group 101 in  ip access-group 101 out  duplex auto  speed auto  exit  interface FastEthernet0/0.40  encapsulation dot1Q 40  ip address 192.168.30.1 255.255.255.0  ip access-group 101 in  ip access-group 101 out  exit  interface FastEthernet4/0  ip address 192.168.3.2 255.255.255.0  ip access-group 1 in  ip access-group 1 out  exit  interface FastEthernet5/0  ip address 192.168.4.2 255.255.255.0  ip access-group 100 in  ip access-group 100 out  exit  ip route 192.168.1.0 255.255.255.192 192.168.3.1  ip route 192.168.1.64 255.255.255.192 192.168.4.1  ip route 192.168.10.0 255.255.255.0 192.168.3.1  ip route 192.168.20.0 255.255.255.0 192.168.4.1 |
| **2. Podział na podsieci:** |
| enable  configure terminal  ip route 192.168.1.0 255.255.255.192 192.168.3.1  ip route 192.168.1.64 255.255.255.192 192.168.4.1  ip route 192.168.10.0 255.255.255.0 192.168.3.1  ip route 192.168.20.0 255.255.255.0 192.168.4.1 |
| **3. VLANy:** |
| enable  configure terminal  interface FastEthernet0/0.40  encapsulation dot1Q 40  ip address 192.168.30.1 255.255.255.0  ip access-group 101 in  ip access-group 101 out  exit |
| **4. Serwer DHCP:** |
| Brak konfiguracji serwera DHCP w dostarczonym fragmencie. |
| **5. Konfiguracja urządzeń pod kątem dostępu SSH:** |
| enable  configure terminal  ip ssh version 2  ip domain-name michal.com  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit |
| **6. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS:** |
| enable  configure terminal  ntp server 192.168.30.2  logging 192.168.30.2 |
| **7. Implementacja lokalnego SPAN:** |
| Brak konfiguracji lokalnego SPAN w dostarczonym fragmencie. |
| **8. Implementacja co najmniej jednej listy kontroli dostępu ACL wewnątrz zabezpieczonej sieci:** |
| enable  configure terminal  access-list 100 permit tcp 192.168.20.0 0.0.0.255 any eq 22  access-list 100 deny ip any any  access-list 101 deny tcp any any eq 22  access-list 101 permit ip any any |
| **9. Implementacja zabezpieczeń STP:** |
| Brak konfiguracji zabezpieczeń STP w dostarczonym fragmencie. |
| **10. Konfiguracja uwierzytelniania AAA na serwerze przy użyciu TACACS+ lub RADIUS:** |
| enable  configure terminal  aaa new-model  aaa authentication login auth group tacacs+ local  tacacs-server host 192.168.30.2 key key |
| **11. Zaprojektowanie zapory sieciowej typu Private and Public:** |
| Brak szczegółowej konfiguracji zapory sieciowej w dostarczonym fragmencie. |

S1

|  |
| --- |
| **1. Adresacja:** |
| enable  configure terminal  hostname S1  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip ssh version 2  ip domain-name michal.com  interface Vlan20  ip address 192.168.10.20 255.255.255.0  exit |
| **2. Podział na podsieci:** |
| Brak konfiguracji podziału na podsieci w dostarczonym fragmencie. |
| **3. VLANy:** |
| enable  configure terminal  spanning-tree mode pvst  spanning-tree extend system-id  interface FastEthernet0/1  switchport mode trunk  exit  interface FastEthernet0/2  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/3  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/4  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/5  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/6  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/7  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/8  switchport access vlan 20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/9  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/10  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/11  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/12  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/13  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/14  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/15  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/16  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/17  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/18  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/19  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/21  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/22  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/23  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/24  spanning-tree portfast  spanning-tree bpduguard enable  exit |
| **4. Serwer DHCP:** |
| Brak konfiguracji serwera DHCP w dostarczonym fragmencie. |
| **5. Konfiguracja urządzeń pod kątem dostępu SSH:** |
| enable  configure terminal  ip ssh version 2  ip domain-name michal.com  username admin privilege 1 password cisco  line con 0  login  exit  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit |
| **6. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS:** |
| enable  configure terminal  ntp server 192.168.10.2  logging 192.168.10.2 |
| **7. Implementacja lokalnego SPAN:** |
| enable  configure terminal  monitor session 1 source interface Fa0/3  monitor session 1 destination interface Fa0/4  exit |
| **8. Implementacja co najmniej jednej listy kontroli dostępu ACL wewnątrz zabezpieczonej sieci:** |
| Brak konfiguracji ACL w dostarczonym fragmencie. |
| **9. Implementacja zabezpieczeń STP:** |
| enable  configure terminal  spanning-tree mode pvst  spanning-tree extend system-id |
| **10. Konfiguracja uwierzytelniania AAA na serwerze przy użyciu TACACS+ lub RADIUS:** |
| enable  configure terminal  aaa new-model  aaa authentication login auth group tacacs+ local  tacacs-server host 192.168.1.2 key key  tacacs-server host 192.168.10.20 key key  tacacs-server host 192.168.10.2 key key |
| **11. Zaprojektowanie zapory sieciowej typu Private and Public:** |
| Brak szczegółowej konfiguracji zapory sieciowej w dostarczonym fragmencie. |

S2

|  |
| --- |
| **1. Adresacja:** |
| enable  configure terminal  hostname S2  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip ssh version 2  ip domain-name michal.com  interface Vlan30  ip address 192.168.20.30 255.255.255.0  exit |
| **2. Podział na podsieci:** |
| Brak konfiguracji podziału na podsieci w dostarczonym fragmencie. |
| **3. VLANy:** |
| enable  configure terminal  spanning-tree mode pvst  spanning-tree extend system-id  interface FastEthernet0/1  switchport mode trunk  exit  interface FastEthernet0/2  switchport access vlan 30  switchport mode access  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/3  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/4  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/5  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/6  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/7  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/8  switchport access vlan 30  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/9  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/10  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/11  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/12  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/13  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/14  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/15  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/16  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/17  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/18  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/19  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/21  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/22  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/23  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/24  spanning-tree portfast  spanning-tree bpduguard enable  exit |
| **4. Serwer DHCP:** |
| Brak konfiguracji serwera DHCP w dostarczonym fragmencie. |
| **5. Konfiguracja urządzeń pod kątem dostępu SSH:** |
| enable  configure terminal  ip ssh version 2  ip domain-name michal.com  username admin privilege 1 password cisco  line con 0  login  exit  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit |
| **6. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS:** |
| enable  configure terminal  ntp server 192.168.20.2  logging 192.168.20.2 |
| **7. Implementacja lokalnego SPAN:** |
| enable  configure terminal  monitor session 1 source interface Fa0/3  monitor session 1 destination interface Fa0/4  exit |
| **8. Implementacja co najmniej jednej listy kontroli dostępu ACL wewnątrz zabezpieczonej sieci:** |
| Brak konfiguracji ACL w dostarczonym fragmencie. |
| **9. Implementacja zabezpieczeń STP:** |
| enable  configure terminal  spanning-tree mode pvst  spanning-tree extend system-id |
| **10. Konfiguracja uwierzytelniania AAA na serwerze przy użyciu TACACS+ lub RADIUS:** |
| enable  configure terminal  aaa new-model  aaa authentication login auth group tacacs+ local  tacacs-server host 192.168.20.2 key key |
| **11. Zaprojektowanie zapory sieciowej typu Private and Public:** |
| Brak szczegółowej konfiguracji zapory sieciowej w dostarczonym fragmencie. |

S3

|  |
| --- |
| **1. Adresacja:** |
| enable  configure terminal  hostname S3  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip ssh version 2  ip domain-name michal.com  interface Vlan40  ip address 192.168.30.40 255.255.255.0  exit |
| **2. Podział na podsieci:** |
| Brak konfiguracji podziału na podsieci w dostarczonym fragmencie. |
| **3. VLANy:** |
| enable  configure terminal  spanning-tree mode pvst  spanning-tree extend system-id  interface FastEthernet0/1  switchport mode trunk  exit  interface FastEthernet0/2  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/3  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/4  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/5  switchport access vlan 40  switchport mode access  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/6  switchport access vlan 40  switchport mode trunk  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/7  switchport access vlan 40  exit  interface FastEthernet0/8  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/9  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/10  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/11  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/12  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/13  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/14  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/15  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/16  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/17  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/18  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/19  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/21  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/22  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/23  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/24  spanning-tree portfast  spanning-tree bpduguard enable  exit |
| **4. Serwer DHCP:** |
| Brak konfiguracji serwera DHCP w dostarczonym fragmencie. |
| **5. Konfiguracja urządzeń pod kątem dostępu SSH:** |
| enable  configure terminal  ip ssh version 2  ip domain-name michal.com  username admin privilege 1 password cisco  line con 0  login  exit  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit |
| **6. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS:** |
| enable  configure terminal  ntp server 192.168.30.2  logging 192.168.30.2 |
| **7. Implementacja lokalnego SPAN:** |
| enable  configure terminal  monitor session 1 source interface Fa0/3  monitor session 1 destination interface Fa0/4  exit |
| **8. Implementacja co najmniej jednej listy kontroli dostępu ACL wewnątrz zabezpieczonej sieci:** |
| Brak konfiguracji ACL w dostarczonym fragmencie. |
| **9. Implementacja zabezpieczeń STP:** |
| enable  configure terminal  spanning-tree mode pvst  spanning-tree extend system-id |
| **10. Konfiguracja uwierzytelniania AAA na serwerze przy użyciu TACACS+ lub RADIUS:** |
| enable  configure terminal  aaa new-model  aaa authentication login auth group tacacs+ local  tacacs-server host 192.168.30.2 key key |
| **11. Zaprojektowanie zapory sieciowej typu Private and Public:** |
| Brak szczegółowej konfiguracji zapory sieciowej w dostarczonym fragmencie. |
| **12. Konfiguracja zapisywania logów** |
| enable  configure terminal  logging 192.168.30.2 |

S4

|  |
| --- |
| **1. Adresacja:** |
| enable  configure terminal  hostname S4  enable secret class  service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  ip ssh version 2  ip domain-name michal.com  interface Vlan40  ip address 192.168.30.41 255.255.255.0  exit |
| **2. Podział na podsieci:** |
| Brak konfiguracji podziału na podsieci w dostarczonym fragmencie. |
| **3. VLANy:** |
| enable  configure terminal  spanning-tree mode pvst  spanning-tree extend system-id  interface FastEthernet0/1  switchport access vlan 2  switchport mode trunk  exit  interface FastEthernet0/2  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/3  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/4  switchport access vlan 40  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/5  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/6  switchport access vlan 2  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/7  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/8  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/9  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/10  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/11  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/12  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/13  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/14  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/15  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/16  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/17  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/18  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/19  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/20  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/21  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/22  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/23  spanning-tree portfast  spanning-tree bpduguard enable  exit  interface FastEthernet0/24  spanning-tree portfast  spanning-tree bpduguard enable  exit |
| **4. Serwer DHCP:** |
| Brak konfiguracji serwera DHCP w dostarczonym fragmencie. |
| **5. Konfiguracja urządzeń pod kątem dostępu SSH:** |
| enable  configure terminal  ip ssh version 2  ip domain-name michal.com  username admin privilege 1 password cisco  line con 0  login  exit  line vty 0 4  login authentication auth  transport input ssh  exit  line vty 5 15  transport input ssh  exit |
| **6. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS:** |
| enable  configure terminal  ntp server 192.168.30.2  logging 192.168.30.2 |
| **7. Implementacja lokalnego SPAN:** |
| enable  configure terminal  monitor session 1 source interface Fa0/1  monitor session 1 destination interface Fa0/2  exit |
| **8. Implementacja co najmniej jednej listy kontroli dostępu ACL wewnątrz zabezpieczonej sieci:** |
| Brak konfiguracji ACL w dostarczonym fragmencie. |
| **9. Implementacja zabezpieczeń STP:** |
| enable  configure terminal  spanning-tree mode pvst  spanning-tree extend system-id |
| **10. Konfiguracja uwierzytelniania AAA na serwerze przy użyciu TACACS+ lub RADIUS:** |
| enable  configure terminal  aaa new-model  aaa authentication login auth group tacacs+ local  tacacs-server host 192.168.10.2 key key  tacacs-server host 192.168.40.2 key key  tacacs-server host 192.168.30.2 key key |
| **11. Zaprojektowanie zapory sieciowej typu Private and Public:** |
| Brak szczegółowej konfiguracji zapory sieciowej w dostarczonym fragmencie. |
| **12. Konfiguracja zapisywania logów** |
| enable  configure terminal  logging 192.168.30.2 |