# 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 |