

Implementacja technologii VLAN i VxLAN we współczesnych sieciach teleinformatycznych

Dariusz Chaładyniak*
Wojciech Wyrzykowski**

Warszawska Wyższa Szkoła Informatyki

Streszczenie

Artykuł przedstawia analizę ruchu pakietów w sieciach teleinformatycznych z wykorzystaniem technologii VLAN oraz VxLAN. W kolejnych rozdziałach zawarto w nim przygotowanie fizycznego środowiska bazowego, implementację dwóch wybranych rozwiązań, przeprowadzenie testów oraz omówienie uzyskanych wyników.

Słowa kluczowe – technologia VLAN, technologia VxLAN, sieci teleinformatyczne, protokoły sieciowe, routing IP

* E-mail: dchalad@ms.wysi.edu.pl

** E-mail: wojwyr13@gmail.com

Zgłoszono do druku 12 listopada 2022 r.

1. Wstęp

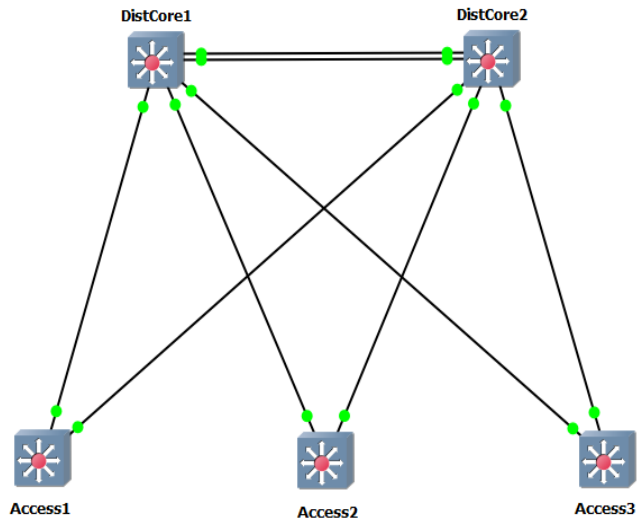
Pierwsze sieci komputerowe wykorzystywały koncentratory, które nie posiadały żadnej logiki sterowania ruchem, a jedynie replikowały dane otrzymane na jednym porcie do wszystkich pozostałych. Ponieważ urządzenia te stanowiły jedną domenę kolizyjną, większa liczba urządzeń w sieci powodowała więcej kolizji, a co za tym idzie, pogorszenie wydajności całej sieci. Odpowiedzią na ten problem były przełączniki, które potrafiły zapamiętać urządzenie osiągalne na danym porcie aby ruch skierowany do niego docierał tylko na ten port. Takie rozwiązanie powodowało, że każdy port przełącznika stanowił oddzielną domenę kolizyjną.

Z czasem, w dużych sieciach, pojawiła się potrzeba unikania pętli, ograniczenia domen rozgłoszeniowy i separacji ruchu. Rozwiązaniem pierwszego problemu stał się protokół drzewa rozpinającego STP, natomiast rozwiązaniem dwóch kolejnych zostały sieci VLAN. Jest to technologia pozwalająca podzielić sieć fizyczną na logiczne segmenty. Obecnie głównie wykorzystywanym standardem opisującym znakowanie ramek VLAN jest standard IEEE 802.1q [1]. Mniejsze segmenty logiczne oznaczają mniej ruchu rozgłoszeniowego do obsłużenia. Separacja logicznych segmentów jest też istotna z punktu widzenia bezpieczeństwa.

Pomimo rozwiązywania wielu problemów, z biegiem czasu STP również ujawniło swoje wady. Nie tylko korzystało z jednego z dostępnych połączeń, pozostawiając pozostałe jako zapasowe, ale dodatkowo czas przełączenia linku zapasowego na aktywny potrafił wynosić nawet 50 sekund [1, 2]. Uwzględniając nowsze wersje tego protokołu, jak RSTP czy MSTP, które skracają czas zbieżności do 10 sekund i pozwalały częściowo zniwelować problem nie wykorzystanych łączy, nadal nie było to rozwiązanie wystarczająco wydajne [3]. Tutaj odpowiedzią stał się model sieci spine-and-leaf, zastępujący tradycyjne modele hierarchiczne, a także technologia VxLAN, która pozwoliła na usunięcie STP [4].

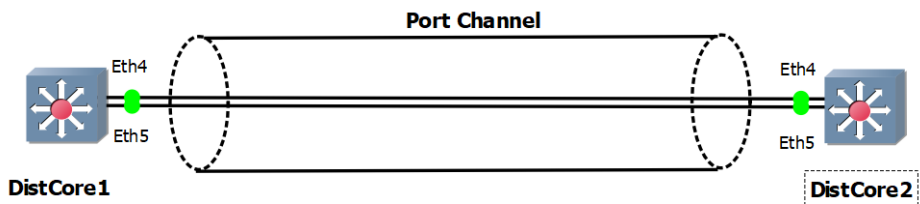
2. Implementacja sieci z wykorzystaniem technologii VLAN

W tym rozwiązaniu wykorzystano model zwiniętego rdzenia (rys. 1), w którym wszystkie przełączniki warstwy dostępowej są połączone z każdym przełącznikiem warstwy rdzenia/dystrybucji [1].



Rysunek 1. Topologia fizyczna badanej sieci

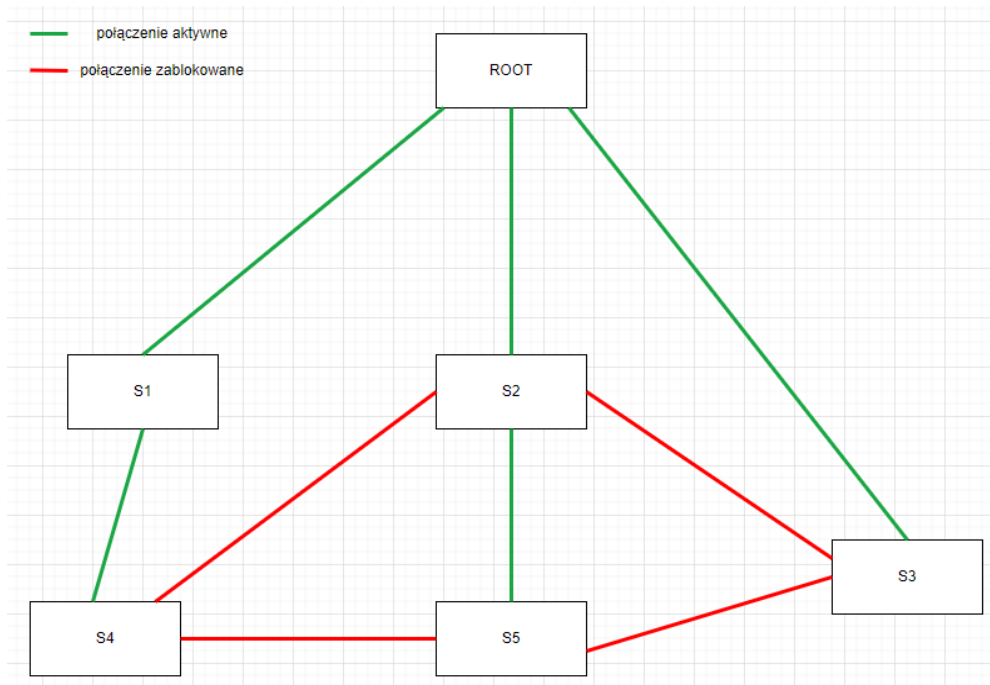
Dla zwiększenia przepustowości pomiędzy przełącznikami wielowarstwowymi warstwy rdzenia/dystrybucji często stosuje się agregację łączy (rys. 2). Polega ona na połączeniu wielu fizycznych łączy w jedno, logiczne nazywane „port channel”. Zbiór interfejsów sieciowych na przełączniku jest określany jako „channel group” i jest powiązany z logicznym interfejsem port channel. Interfejs ten może być konfigurowany prawie tak samo jak zwykły interfejs sieciowy przełącznika, czyli jako L2 lub L3. Interfejs port channel może być również podzielony na podinterfejsy L3 bazujące na znakowaniu VLAN, zgodnie z IEEE 802.1q [1].



Rysunek 2. Agregacja portów

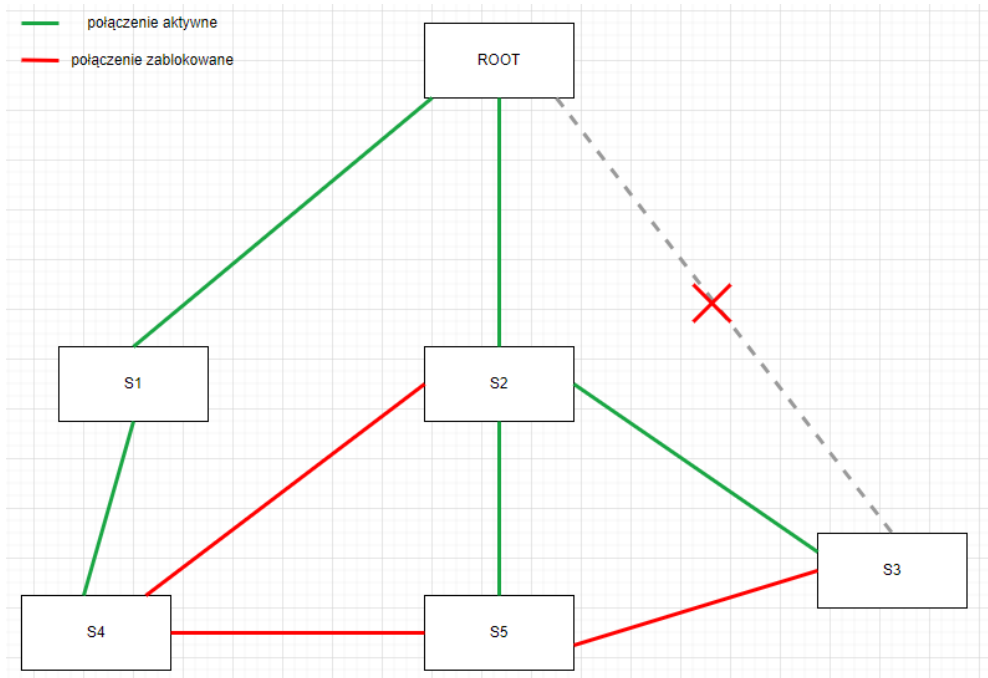
Zadaniem protokołu drzewa opinającego jest zapewnienie braku pętli w warstwie L2. Drzewo opinające jest tworzone przez wyznaczenie przełącznika na szczycie i ustalenie połączeń w dół sieci pozostawiając tylko jedną aktywną trasę do każdego segmentu sieci. Pozostałe, zapasowe łącza są odcinane, aby nie przekazywały ruchu [1, 2].

Schemat przykładowego drzewa STP przedstawiono na rysunku 3.



Rysunek 3. Drzewo STP bez pętli

W przypadku awarii aktywnego połączenia STP aktywuje jeden z łączy zapasowych. Wynik tego działania pokazano na rysunku 4.



Rysunek 4. Efekt działania protokołu STP

Poniżej zawarto opis konfiguracji wszystkich urządzeń sieciowych wykorzystanych do stworzenia środowiska badawczego.

Pierwszym etapem było uruchomienie routingu ip oraz skonfigurowanie i weryfikacja dwóch sieci VLAN o identyfikatorach 10 i 20 (rys. 5).

W kolejnym kroku skonfigurowano porty trunk do przełączników dostępowych oraz interfejs Port-Channel agregując dwa łącza pomiędzy przełącznikami DistCore-1 i DistCore-2 (rys. 6).

```

DistCore-1(config)#vlan 10
DistCore-1(config-vlan-10)#exit
DistCore-1(config)#vlan 20
DistCore-1(config-vlan-20)#exit
DistCore-1(config)#
DistCore-1(config)#sh vlan brief
VLAN  Name                               Status  Ports
-----
1     default                                active  Et6, Et7, Et8, Et9, Et10, Et11
10    VLAN0010                               active  Cpu, Et1, Et2, Et3, Po1
20    VLAN0020                               active  Cpu, Et1, Et2, Et3, Po1
    
```

```

DistCore-2(config)#vlan 10
DistCore-2(config-vlan-10)#exit
DistCore-2(config)#vlan 20
DistCore-2(config-vlan-20)#
DistCore-2(config-vlan-20)#exit
DistCore-2(config)#sh vlan brief
VLAN  Name                               Status  Ports
-----
1     default                                active  Et6, Et7, Et8, Et9, Et10, Et11
10    VLAN0010                               active  Cpu, Et1, Et2, Et3, Po1
20    VLAN0020                               active  Cpu, Et1, Et2, Et3, Po1
    
```

Rysunek 5. Konfiguracja i weryfikacja sieci VLAN

```

DistCore-1(config)#interface Ethernet1
DistCore-1(config-if-Et1)# switchport trunk allowed vlan 10,20
DistCore-1(config-if-Et1)# switchport mode trunk
DistCore-1(config-if-Et1)#!
DistCore-1(config-if-Et1)#interface Ethernet2
DistCore-1(config-if-Et2)# switchport trunk allowed vlan 10,20
DistCore-1(config-if-Et2)# switchport mode trunk
DistCore-1(config-if-Et2)#
DistCore-1(config-if-Et2)#interface Ethernet4
DistCore-1(config-if-Et4)# channel-group 1 mode active
DistCore-1(config-if-Et4)#!
DistCore-1(config-if-Et4)#interface Ethernet5
DistCore-1(config-if-Et5)# channel-group 1 mode active
DistCore-1(config-if-Et5)#!
DistCore-1(config-if-Et5)#interface Port-Channell1
DistCore-1(config-if-Po1)# switchport trunk allowed vlan 10,20
DistCore-1(config-if-Po1)# switchport mode trunk
    
```

```

DistCore-2(config)#interface Ethernet1
DistCore-2(config-if-Et1)# switchport trunk allowed vlan 10,20
DistCore-2(config-if-Et1)# switchport mode trunk
DistCore-2(config-if-Et1)#!
DistCore-2(config-if-Et1)#interface Ethernet2
DistCore-2(config-if-Et2)# switchport trunk allowed vlan 10,20
DistCore-2(config-if-Et2)# switchport mode trunk
DistCore-2(config-if-Et2)#
DistCore-2(config-if-Et2)#interface Ethernet4
DistCore-2(config-if-Et4)# channel-group 1 mode active
DistCore-2(config-if-Et4)#!
DistCore-2(config-if-Et4)#interface Ethernet5
DistCore-2(config-if-Et5)# channel-group 1 mode active
DistCore-2(config-if-Et5)#!
DistCore-2(config-if-Et5)#interface Port-Channell1
DistCore-2(config-if-Po1)# switchport trunk allowed vlan 10,20
DistCore-2(config-if-Po1)# switchport mode trunk
    
```

Rysunek 6. Konfiguracja portów typu trunk

Następnie skonfigurowano interfejsy SVI tworząc jednocześnie grupę VRRP (rys. 7). Adres wirtualny grupy VRRP będzie stanowił domyślną bramę dla urządzeń końcowych.

```
DistCore-1(config)#interface Vlan10
DistCore-1(config-if-Vl10)# ip address 10.10.10.11/24
DistCore-1(config-if-Vl10)# vrrp 1 priority-level 251
DistCore-1(config-if-Vl10)# vrrp 1 ipv4 10.10.10.1
DistCore-1(config-if-Vl10)# vrrp 1 ipv4 version 3
DistCore-1(config-if-Vl10)#
DistCore-1(config-if-Vl10)#interface Vlan20
DistCore-1(config-if-Vl20)# ip address 10.10.20.11/24
DistCore-1(config-if-Vl20)# vrrp 1 priority-level 251
DistCore-1(config-if-Vl20)# vrrp 1 ipv4 10.10.20.1
DistCore-1(config-if-Vl20)# vrrp 1 ipv4 version 3
DistCore-1(config-if-Vl20)#exit
```

```
DistCore-2(config)#interface Vlan10
DistCore-2(config-if-Vl10)# ip address 10.10.10.12/24
DistCore-2(config-if-Vl10)# vrrp 1 priority-level 250
DistCore-2(config-if-Vl10)# vrrp 1 ipv4 10.10.10.1
DistCore-2(config-if-Vl10)# vrrp 1 ipv4 version 3
DistCore-2(config-if-Vl10)#
DistCore-2(config-if-Vl10)#interface Vlan20
DistCore-2(config-if-Vl20)# ip address 10.10.20.12/24
DistCore-2(config-if-Vl20)# vrrp 1 priority-level 250
DistCore-2(config-if-Vl20)# vrrp 1 ipv4 10.10.20.1
DistCore-2(config-if-Vl20)# vrrp 1 ipv4 version 3
DistCore-2(config-if-Vl20)#exit
```

Rysunek 7. Konfiguracja interfejsów SVI oraz grupy VRRP

Ostatecznie zweryfikowano łączność pomiędzy przełącznikami (rys. 8).

```
DistCore-1(config)#ping 10.10.10.12 repeat 3
PING 10.10.10.12 (10.10.10.12) 72(100) bytes of data.
80 bytes from 10.10.10.12: icmp_seq=1 ttl=64 time=55.3 ms
80 bytes from 10.10.10.12: icmp_seq=2 ttl=64 time=64.4 ms
80 bytes from 10.10.10.12: icmp_seq=3 ttl=64 time=76.3 ms

--- 10.10.10.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 22ms
rtt min/avg/max/mdev = 55.311/65.366/76.387/8.636 ms, pipe 3, ipg/ewma 11.390/58.939 ms
DistCore-1(config)#ping 10.10.20.12 repeat 3
PING 10.10.20.12 (10.10.20.12) 72(100) bytes of data.
80 bytes from 10.10.20.12: icmp_seq=1 ttl=64 time=60.3 ms
80 bytes from 10.10.20.12: icmp_seq=2 ttl=64 time=72.1 ms
80 bytes from 10.10.20.12: icmp_seq=3 ttl=64 time=80.5 ms

--- 10.10.20.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 22ms
rtt min/avg/max/mdev = 60.356/71.029/80.551/8.284 ms, pipe 3, ipg/ewma 11.338/64.173 ms
```

Rysunek 8. Weryfikacja łączności pomiędzy przełącznikami

Wszystkie przełączniki warstwy dostępowej zostały skonfigurowane i zweryfikowane w następujący sposób (rys. 9):

- dodano sieci VLAN 10 i 20;
- interfejsy w kierunku warstwy rdzenia/dystrybucji skonfigurowano jako trunk L2;
- interfejsy dostępowe dla urządzeń końcowych skonfigurowano jako interfejsy access.

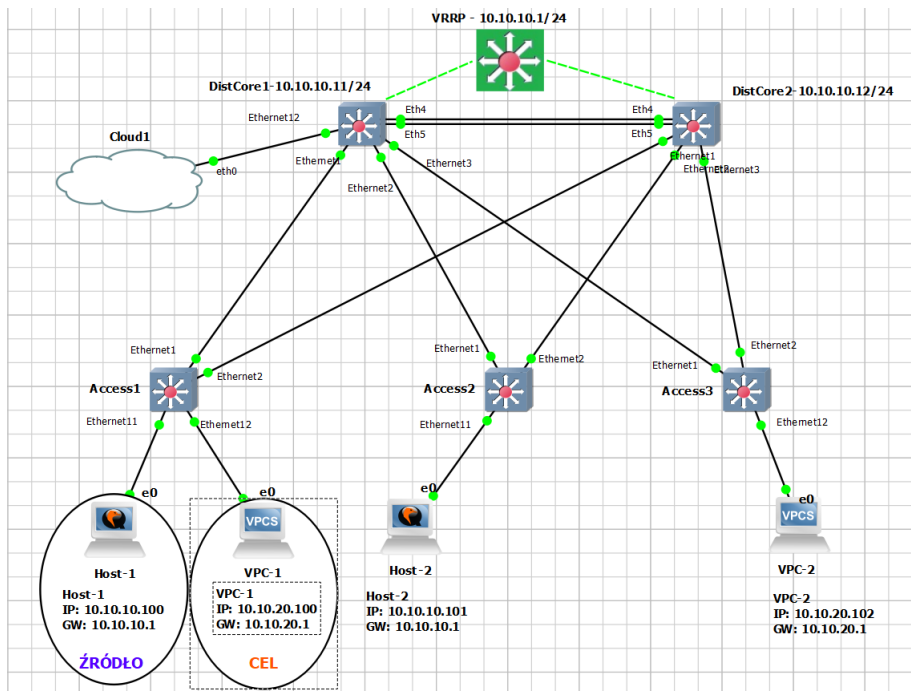
```
Access-1(config)#vlan 10,20
Access-1(config-vlan-10,20)#!
Access-1(config-vlan-10,20)#interface Ethernet1
Access-1(config-if-Et1)#  switchport trunk allowed vlan 10,20
Access-1(config-if-Et1)#  switchport mode trunk
Access-1(config-if-Et1)#!
Access-1(config-if-Et1)#interface Ethernet2
Access-1(config-if-Et2)#  switchport trunk allowed vlan 10,20
Access-1(config-if-Et2)#  switchport mode trunk
Access-1(config-if-Et2)#!
Access-1(config-if-Et2)#interface Ethernet11
Access-1(config-if-Et11)#  switchport access vlan 10
Access-1(config-if-Et11)#!
Access-1(config-if-Et11)#interface Ethernet12
Access-1(config-if-Et12)#  switchport access vlan 20
Access-1(config-if-Et12)#
Access-1(config-if-Et12)#exit
```

Rysunek 9. Konfiguracja przełącznika Access-1

Konfigurację systemów na urządzeniach końcowych przeprowadzono tak, aby do każdego przełącznika dostępowego były podłączone dwa hosty - każdy w oddzielnej sieci VLAN. Bramy domyślne wskazują na wirtualne adresy VRRP skonfigurowane na przełącznikach warstwy wyższej. Taka konfiguracja zapewniła przeprowadzenie testów opisanych poniżej.

2.1. Przeskoki pomiędzy sieciami VLAN

Test ten ma na celu określenie liczby przeskoków pakietów od źródła podłączonego do przełącznika Access-1 i umieszczonego w sieci VLAN 10 do celu podłączonego do tego samego przełącznika dostępowego, ale umieszczonego w sieci VLAN 20. Umiejscowienie stacji w infrastrukturze pokazano na rysunku 10.



Rysunek 10. Umieszczenie źródła i celu w testowanej sieci

Test przeprowadzono przy pomocy narzędzia konsolowego „MTR”, a wynik przedstawiono na rysunku 11.

```

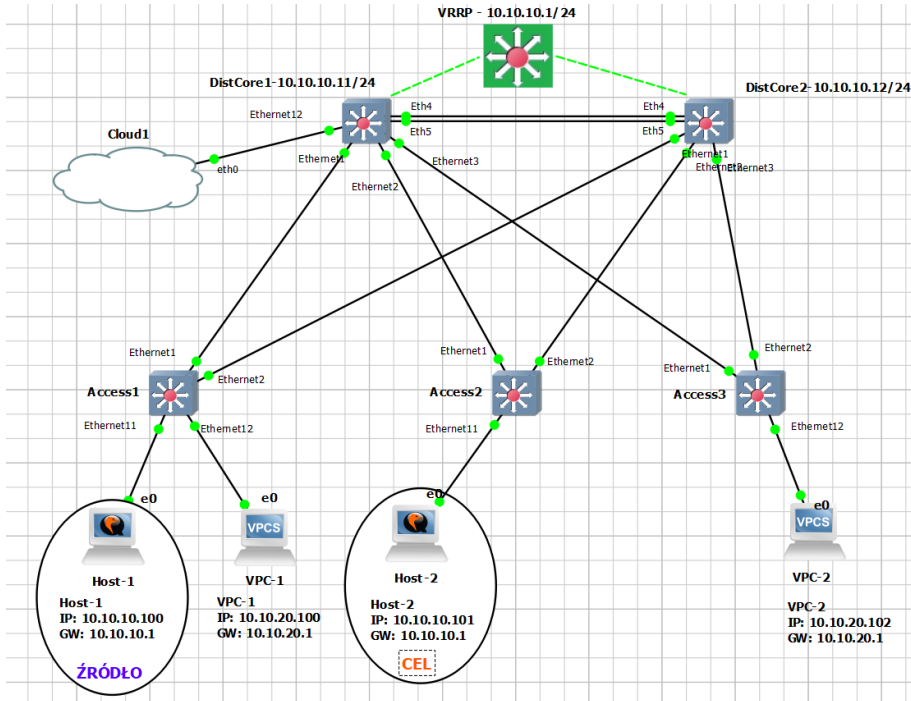
My traceroute [v0.85]
centos (0.0.0.0) Sat Dec 18 23:27:32 2021
Keys: Help Display mode Restart statistics Order of fields quit
          Packets
Host      Loss%  Snt  Last  Avg  Best  Wrst StDev
 1. 10.10.10.11      0.0%   6   69.7  76.3  45.2 135.3  33.5
 2. 10.10.20.100    0.0%   6  130.1 105.5  68.1 175.3  42.7
    
```

Rysunek 11. Wynik testu liczby przeskoków

2.2. Rozłożenie ruchu na połączeniach pomiędzy warstwami

Badanie to ma zidentyfikować rozłożenie ruchu ze źródła do celu pomiędzy łączami redundantnymi, zarówno w górę jak i w dół sieci. Umieszczenie źródła i celu w infrastrukturze przedstawiono na rysunku 12. Ponieważ w modelu wykorzystano

MSTP, przeprowadzono analizę stanu portów na urządzeniach znajdujących się na trasie pakietów (rys. 13 oraz rys. 14.).



Rysunek 12. Umieszczenie źródła i celu w testowanej sieci

```

Access-2#sh spanning-tree vlan 10
Spanning tree instance for vlan 10
MST0
  Spanning tree enabled protocol mstp
  Root ID    Priority    8192
            Address      0c61.1361.596d
            Cost        0 (Ext) 2000 (Int)
            Port        1 (Ethernet1)
            Hello Time  2.000 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    32768 (priority 32768 sys-id-ext 0)
            Address      0c1a.633d.647f
            Hello Time  2.000 sec Max Age 20 sec Forward Delay 15 sec

Interface    Role        State        Cost        Prio.Nbr Type
-----
Et1          root       forwarding   2000        128.1    P2p
Et2          alternate discarding   2000        128.2    P2p
Et11         designated forwarding 2000        128.11   P2p Edge
    
```

Rysunek 13. Stan portów w przełączniku Access-1

```

Access-1(config)#sh spanning-tree vlan 10
Spanning tree instance for vlan 10
MST0
  Spanning tree enabled protocol mstp
  Root ID    Priority    8192
            Address    0c61.1361.596d
            Cost      0 (Ext) 2000 (Int)
            Port      1 (Ethernet1)
            Hello Time 2.000 sec Max Age 20 sec Forward Delay 15 sec

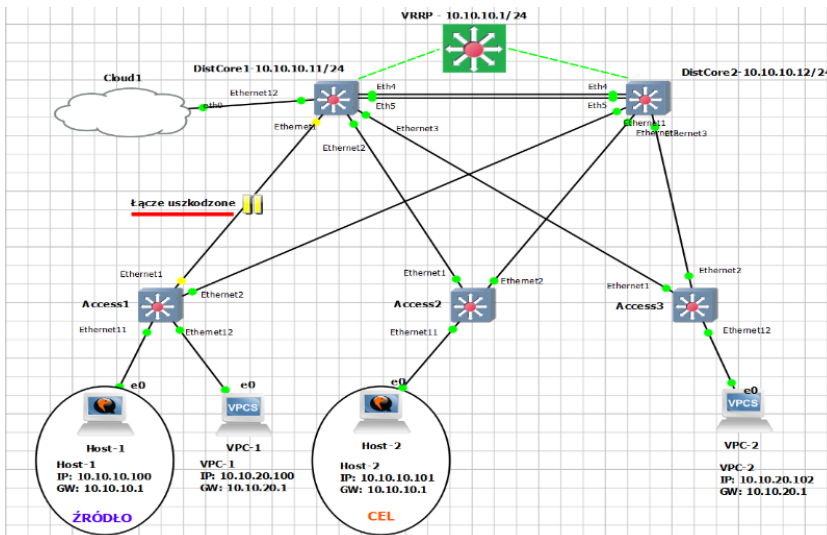
  Bridge ID  Priority    32768 (priority 32768 sys-id-ext 0)
            Address    0c2c.794b.080a
            Hello Time 2.000 sec Max Age 20 sec Forward Delay 15 sec

Interface    Role        State        Cost        Prio.Nbr Type
-----
Et1          root       forwarding   2000        128.1   P2p
Et2          alternate discarding   2000        128.2   P2p
Et11         designated forwarding 2000        128.11  P2p Edge
    
```

Rysunek 14. Stan portów w przełączniku Access-2

2.3. Awaria jednego łącza w górę sieci

Badanie ma określić czas potrzebny na osiągnięcie zbieżności sieci po zasymulowaniu awarii aktywnego połączenia pomiędzy przełącznikiem Access-1, a warstwą wyższą. W tym celu zbadano liczbę utraconych pakietów ICMP wysyłanych w jednosekundowych odstępach ze źródła do celu. Umieszczenie źródła, celu i uszkodzenia połączenia pokazano na rys. 15.



Rysunek 15. Umieszczenie źródła, celu oraz uszkodzonego łącza w testowanej sieci

Wyniki przeprowadzonego badania przedstawiono na rysunku 16. Badanie przeprowadzono w dwóch etapach: podczas awarii i podczas odzyskania sprawności.

```
[root@centos ~]# ping 10.10.10.101
PING 10.10.10.101 (10.10.10.101) 56(84) bytes of data.
64 bytes from 10.10.10.101: icmp_seq=1 ttl=64 time=116 ms
64 bytes from 10.10.10.101: icmp_seq=2 ttl=64 time=41.2 ms
64 bytes from 10.10.10.101: icmp_seq=3 ttl=64 time=161 ms
64 bytes from 10.10.10.101: icmp_seq=4 ttl=64 time=49.8 ms
64 bytes from 10.10.10.101: icmp_seq=5 ttl=64 time=48.8 ms
64 bytes from 10.10.10.101: icmp_seq=6 ttl=64 time=241 ms
64 bytes from 10.10.10.101: icmp_seq=7 ttl=64 time=45.7 ms
64 bytes from 10.10.10.101: icmp_seq=8 ttl=64 time=47.0 ms
64 bytes from 10.10.10.101: icmp_seq=9 ttl=64 time=181 ms
64 bytes from 10.10.10.101: icmp_seq=10 ttl=64 time=52.6 ms
64 bytes from 10.10.10.101: icmp_seq=11 ttl=64 time=37.1 ms
64 bytes from 10.10.10.101: icmp_seq=12 ttl=64 time=154 ms
64 bytes from 10.10.10.101: icmp_seq=13 ttl=64 time=44.4 ms
64 bytes from 10.10.10.101: icmp_seq=14 ttl=64 time=43.6 ms
64 bytes from 10.10.10.101: icmp_seq=21 ttl=64 time=212 ms
64 bytes from 10.10.10.101: icmp_seq=22 ttl=64 time=53.4 ms

--- 10.10.10.101 ping statistics ---
22 packets transmitted, 16 received, 27% packet loss, time 21025ms
rtt min/avg/max/mdev = 37.197/95.731/241.501/68.452 ms
[root@centos ~]# ping 10.10.10.101
PING 10.10.10.101 (10.10.10.101) 56(84) bytes of data.
64 bytes from 10.10.10.101: icmp_seq=1 ttl=64 time=180 ms
64 bytes from 10.10.10.101: icmp_seq=2 ttl=64 time=78.8 ms
64 bytes from 10.10.10.101: icmp_seq=3 ttl=64 time=52.8 ms
64 bytes from 10.10.10.101: icmp_seq=4 ttl=64 time=58.9 ms
64 bytes from 10.10.10.101: icmp_seq=5 ttl=64 time=59.2 ms
64 bytes from 10.10.10.101: icmp_seq=6 ttl=64 time=60.0 ms
64 bytes from 10.10.10.101: icmp_seq=9 ttl=64 time=66.1 ms
64 bytes from 10.10.10.101: icmp_seq=10 ttl=64 time=52 ms
64 bytes from 10.10.10.101: icmp_seq=11 ttl=64 time=102 ms
64 bytes from 10.10.10.101: icmp_seq=12 ttl=64 time=50.1 ms
64 bytes from 10.10.10.101: icmp_seq=13 ttl=64 time=37.9 ms

--- 10.10.10.101 ping statistics ---
14 packets transmitted, 11 received, 21% packet loss, time 13019ms
rtt min/avg/max/mdev = 37.967/72.755/180.717/37.730 ms
```

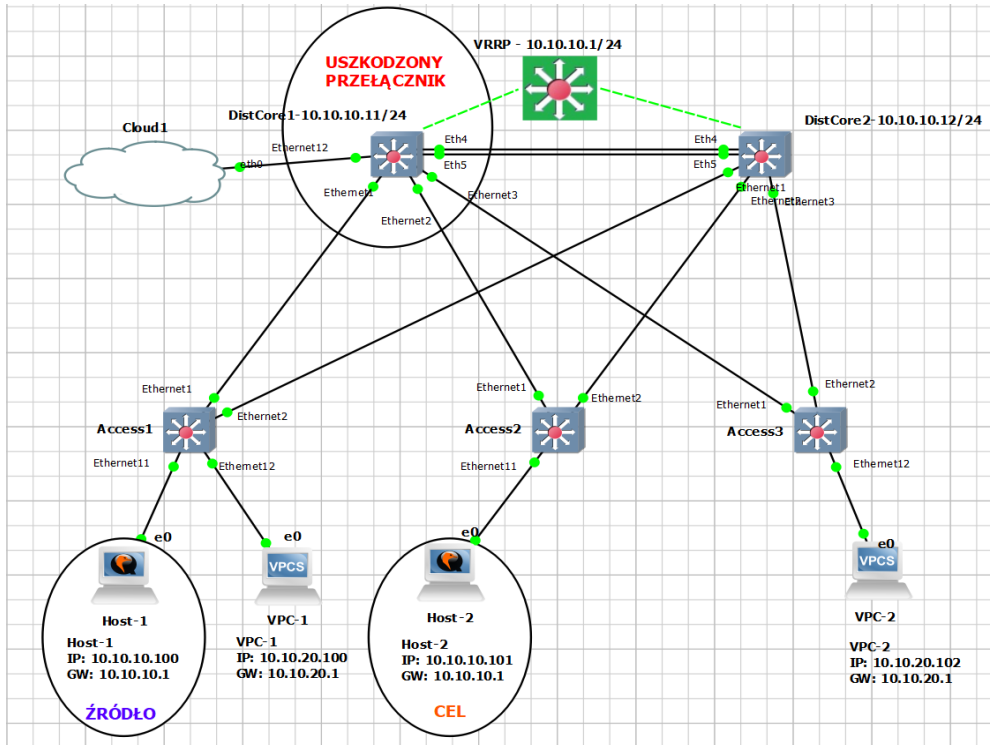
Rysunek 16. Wynik badania symulowanej awarii i przywrócenia łącza

2.4. Awaria przełącznika warstwy rdzenia/dystrybucji

Ostatnie badanie pokazuje jak długa była przerwa w transmisji podczas awarii przełącznika warstwy rdzenia/dystrybucji do którego prowadzi aktywne łącze z niższej warstwy. Umieszczenie źródła, celu i uszkodzonego przełącznika pokazano na rysunku 17.

Badanie przeprowadzono w sposób analogiczny do poprzedniego. Ze źródła do celu wysyłano pakiety ICMP ping w jednosekundowych odstępach. Rezultat badania

przedstawiono na rysunku 18. Przeprowadzono je również w dwóch etapach: podczas awarii i podczas odzyskania sprawności.



Rysunek 17. Umieszczenie źródła i celu uszkodzonego przełącznika

```
64 bytes from 10.10.10.101: icmp_seq=12 ttl=64 time=50.8 ms
64 bytes from 10.10.10.101: icmp_seq=13 ttl=64 time=52.7 ms
64 bytes from 10.10.10.101: icmp_seq=14 ttl=64 time=47.5 ms
64 bytes from 10.10.10.101: icmp_seq=15 ttl=64 time=55.0 ms
64 bytes from 10.10.10.101: icmp_seq=22 ttl=64 time=166 ms
64 bytes from 10.10.10.101: icmp_seq=23 ttl=64 time=88.0 ms
64 bytes from 10.10.10.101: icmp_seq=24 ttl=64 time=89.9 ms

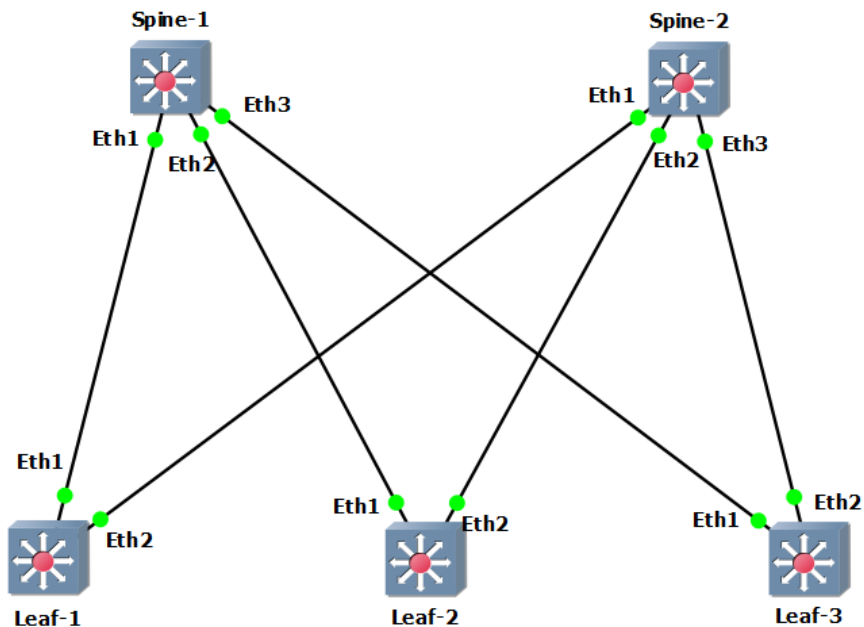
64 bytes from 10.10.10.101: icmp_seq=398 ttl=64 time=43.4 ms
64 bytes from 10.10.10.101: icmp_seq=399 ttl=64 time=36.7 ms
64 bytes from 10.10.10.101: icmp_seq=400 ttl=64 time=42.9 ms
64 bytes from 10.10.10.101: icmp_seq=401 ttl=64 time=43.3 ms
64 bytes from 10.10.10.101: icmp_seq=402 ttl=64 time=43.0 ms
64 bytes from 10.10.10.101: icmp_seq=408 ttl=64 time=488 ms
64 bytes from 10.10.10.101: icmp_seq=409 ttl=64 time=212 ms
64 bytes from 10.10.10.101: icmp_seq=410 ttl=64 time=113 ms
```

Rysunek 18. Wyniki badania po awarii przełącznika

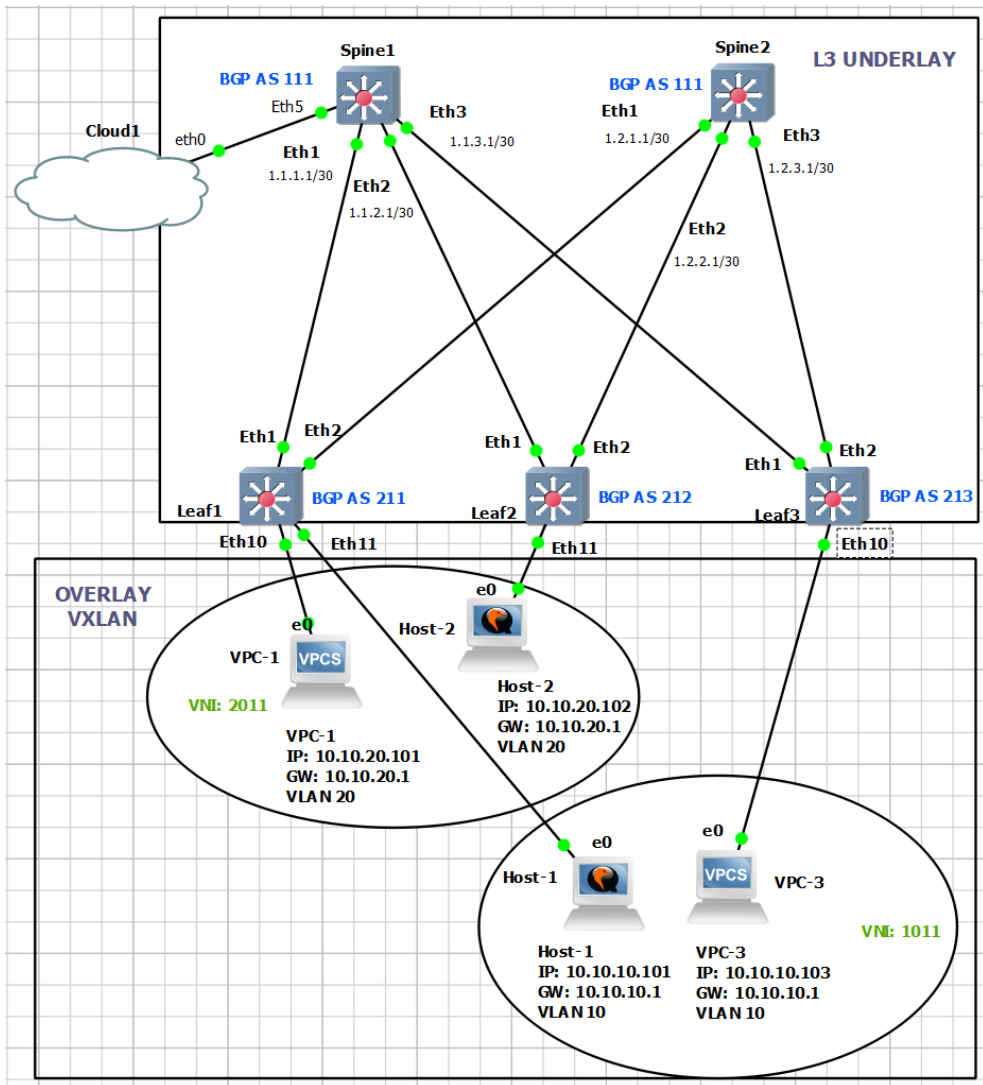
3. Implementacja sieci z wykorzystaniem technologii VxLAN

W rozdziale tym opisano proces budowy sieci wykorzystującej model spine-and-leaf oraz technologię VxLAN (rys. 19). Model spine-and-leaf w opracowywanym rozwiązaniu korzysta z tych samych urządzeń co rozwiązanie VLAN opisane w rozdziale 2. Każdy przełącznik warstwy niższej jest połączony ze wszystkimi przełącznikami warstwy wyższej (rys. 20). Jednak różnica dotyczy dwóch poniższych założeń:

- przełączniki Spine pracują tylko w trybie L3, a przełączniki Leaf w trybie L2/L3;
- brak połączenia pomiędzy przełącznikami Spine.



Rysunek 19. Topologia fizyczna sieci VxLAN



Rysunek 20. Architektura sieci z zastosowaniem technologii VxLAN

Projekt zawiera dwa przełączniki Spine-1 i Spine-2, które pracują w trybie L3. Pierwszym etapem było uruchomienie routingu ip oraz skonfigurowanie interfejsów L3 w dół sieci nadając im adresację z maskami /30 (rys. 21 oraz rys. 22).

```

Spine1(config)#interface Ethernet1
Spine1(config-if-Et1)# description to Leaf1
Spine1(config-if-Et1)# no switchport
Spine1(config-if-Et1)# ip address 1.1.1.1/30
Spine1(config-if-Et1)#!
Spine1(config-if-Et1)#interface Ethernet2
Spine1(config-if-Et2)# description to Leaf2
Spine1(config-if-Et2)# no switchport
Spine1(config-if-Et2)# ip address 1.1.2.1/30
Spine1(config-if-Et2)#!
Spine1(config-if-Et2)#interface Ethernet3
Spine1(config-if-Et3)# description to Leaf3
Spine1(config-if-Et3)# no switchport
Spine1(config-if-Et3)# ip address 1.1.3.1/30
Spine1(config-if-Et3)#sh ip interface brief

```

Interface	IP Address	Status	Protocol	MTU	Address Owner
Ethernet1	1.1.1.1/30	up	up	1500	
Ethernet2	1.1.2.1/30	up	up	1500	
Ethernet3	1.1.3.1/30	up	up	1500	

Rysunek 21. Konfiguracja i weryfikacja portów L3 w przełączniku Spine-1

```

Spine2(config)#interface Ethernet1
Spine2(config-if-Et1)# description to Leaf1
Spine2(config-if-Et1)# no switchport
Spine2(config-if-Et1)# ip address 1.2.1.1/30
Spine2(config-if-Et1)#!
Spine2(config-if-Et1)#interface Ethernet2
Spine2(config-if-Et2)# description to Leaf2
Spine2(config-if-Et2)# no switchport
Spine2(config-if-Et2)# ip address 1.2.2.1/30
Spine2(config-if-Et2)#!
Spine2(config-if-Et2)#interface Ethernet3
Spine2(config-if-Et3)# description to Leaf3
Spine2(config-if-Et3)# no switchport
Spine2(config-if-Et3)# ip address 1.2.3.1/30
Spine2(config-if-Et3)#sh ip interface brief

```

Interface	IP Address	Status	Protocol	MTU	Address Owner
Ethernet1	1.2.1.1/30	up	up	1500	
Ethernet2	1.2.2.1/30	up	up	1500	
Ethernet3	1.2.3.1/30	up	up	1500	

Rysunek 22. Konfiguracja i weryfikacja portów L3 w przełączniku Spine-2

Następnie skonfigurowano router BGP, sąsiedztwa do przełączników Leaf, redundancję tras ECMP oraz redystrybucję tras podłączonych bezpośrednio (rys. 23 oraz rys. 24).


```
Spine1(config)#router bgp 111
Spine1(config-router-bgp)#neighbor 1.1.1.2 remote-as 211
Spine1(config-router-bgp)#neighbor 1.1.2.2 remote-as 212
Spine1(config-router-bgp)#neighbor 1.1.3.2 remote-as 213
Spine1(config-router-bgp)#maximum-paths 2 ecmp 2
Spine1(config-router-bgp)#redistribute connected
Spine1(config-router-bgp)#sh bgp instance
BGP instance information for VRF default
BGP Local AS: 111, Router ID: 1.1.3.1
Total peers: 3
  Static peers: 3
  Dynamic peers: 0
  Disabled peers: 0
  Established peers: 3
Four Octet ASN mode enabled
Graceful restart helper mode enabled
Graceful restart mode disabled
End of rib timer timeout: 00:05:00
Attributes of the reflected routes are not preserved
Number of Adj-RIB-Ins awaiting cleanup: 0
Maximum paths: 2 Maximum ECMP: 2
UCMP mode: disabled
Peer mac resolution timeout: 00:00:00
BGP Convergence timer is inactive
BGP Convergence based update synchronization is disabled
BGP Convergence slow-peer timeout: 00:01:30
BGP Listen Port Status: listening on port 179
BGP Convergence information:
  BGP has converged: yes, Time taken to converge: 00:00:40
  Outstanding EORs: 0, Outstanding Keepalives: 0
  Convergence timeout: 00:05:00
Address family IPv4 Unicast:
  Additional-paths installation is disabled
  Extended next-hop capability is disabled
Address family IPv6 Unicast:
  Additional-paths installation is disabled
```

Rysunek 23. Konfiguracja i weryfikacja protokołu BGP w przełączniku Spine-1

```
Spine2(config)#router bgp 111
Spine2(config-router-bgp)#neighbor 1.2.1.2 remote-as 211
Spine2(config-router-bgp)#neighbor 1.2.2.2 remote-as 212
Spine2(config-router-bgp)#neighbor 1.2.3.2 remote-as 213
Spine2(config-router-bgp)#maximum-paths 2 ecmp 2
Spine2(config-router-bgp)#redistribute connected
Spine2(config-router-bgp)#sh bgp instance
BGP instance information for VRF default
BGP Local AS: 111, Router ID: 1.2.3.1
Total peers: 3
  Static peers: 3
  Dynamic peers: 0
  Disabled peers: 0
  Established peers: 3
Four Octet ASN mode enabled
Graceful restart helper mode enabled
Graceful restart mode disabled
End of rib timer timeout: 00:05:00
Attributes of the reflected routes are not preserved
Number of Adj-RIB-Ins awaiting cleanup: 0
Maximum paths: 2 Maximum ECMP: 2
UCMP mode: disabled
Peer mac resolution timeout: 00:00:00
BGP Convergence timer is inactive
BGP Convergence based update synchronization is disabled
BGP Convergence slow-peer timeout: 00:01:30
BGP Listen Port Status: listening on port 179
BGP Convergence information:
  BGP has converged: yes, Time taken to converge: 00:00:40
  Outstanding EORs: 0, Outstanding Keepalives: 0
  Convergence timeout: 00:05:00
Address family IPv4 Unicast:
  Additional-paths installation is disabled
  Extended next-hop capability is disabled
Address family IPv6 Unicast:
  Additional-paths installation is disabled
```

Rysunek 24. Konfiguracja i weryfikacja protokołu BGP w przełączniku Spine-2.

Wszystkie trzy przełączniki Leaf pracują w trybie L2/L3 i zostały skonfigurowane zgodnie z poniższym schematem (rys. 25 oraz rys. 26):

- dodanie sieci VLAN 10 i 20;
- konfiguracja portów L3 w górę sieci;
- konfiguracja interfejsu lokalnego Loopback1;
- uruchomienie routingu i konfiguracja protokołu BGP;
- konfiguracja interfejsu VxLAN;
- konfiguracja portów dostępowych L2;
- konfiguracja SVI oraz adresu anycast IP.

```
Leaf1(config)#interface Ethernet1
Leaf1(config-if-Et1)# description to Spine1
Leaf1(config-if-Et1)# no switchport
Leaf1(config-if-Et1)# ip address 1.1.1.2/30
Leaf1(config-if-Et1)#!
Leaf1(config-if-Et1)#interface Ethernet2
Leaf1(config-if-Et2)# description to Spine2
Leaf1(config-if-Et2)# no switchport
Leaf1(config-if-Et2)# ip address 1.2.1.2/30
Leaf1(config-if-Et2)#
Leaf1(config-if-Et2)#interface Loopback1
Leaf1(config-if-Lo1)# ip address 211.1.1.1/32
Leaf1(config-if-Lo1)#
Leaf1(config-if-Lo1)#vlan 10,20
Leaf1(config-vlan-10,20)#int eth10
Leaf1(config-if-Et10)# switchport mode access
Leaf1(config-if-Et10)# switchport access vlan 10
Leaf1(config-if-Et10)#int eth11
Leaf1(config-if-Et11)# switchport mode access
Leaf1(config-if-Et11)# switchport access vlan 20
Leaf1(config-if-Et11)#
Leaf1(config-if-Et11)#sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et3, Et4, Et5, Et6, Et7, Et8 Et9, Et12
10	VLAN0010	active	Cpu, Et10, Vx1
20	VLAN0020	active	Cpu, Et11, Vx1

```
Leaf1(config-if-Et11)#sh ip interface brief
```

Interface	IP Address	Status	Protocol	MTU	Address Owner
Ethernet1	1.1.1.2/30	up	up	1500	
Ethernet2	1.2.1.2/30	up	up	1500	
Loopback1	211.1.1.1/32	up	up	65535	
Management1	unassigned	down	down	1500	

Rysunek 25. Konfiguracja i weryfikacja interfejsów w przełączniku Leaf-1

```
Leaf1(config)#ip routing
Leaf1(config)#router bgp 211
Leaf1(config-router-bgp)#neighbor 1.1.1.1 remote-as 111
Leaf1(config-router-bgp)#neighbor 1.2.1.1 remote-as 111
Leaf1(config-router-bgp)#maximum-paths 2 ecmp 2
Leaf1(config-router-bgp)#redistribute connected
Leaf1(config-router-bgp)#
Leaf1(config-router-bgp)#int vxlan 1
Leaf1(config-if-Vx1)# vxlan source-interface loopback 1
Leaf1(config-if-Vx1)# vxlan vlan 20 vni 2011
Leaf1(config-if-Vx1)# vxlan vlan 10 vni 1011
Leaf1(config-if-Vx1)# vxlan flood vtep 212.1.1.1 213.1.1.1
Leaf1(config-if-Vx1)# no shutdown
```

Rysunek 26. Konfiguracja protokołu BGP oraz VxLAN w przełączniku Leaf-1

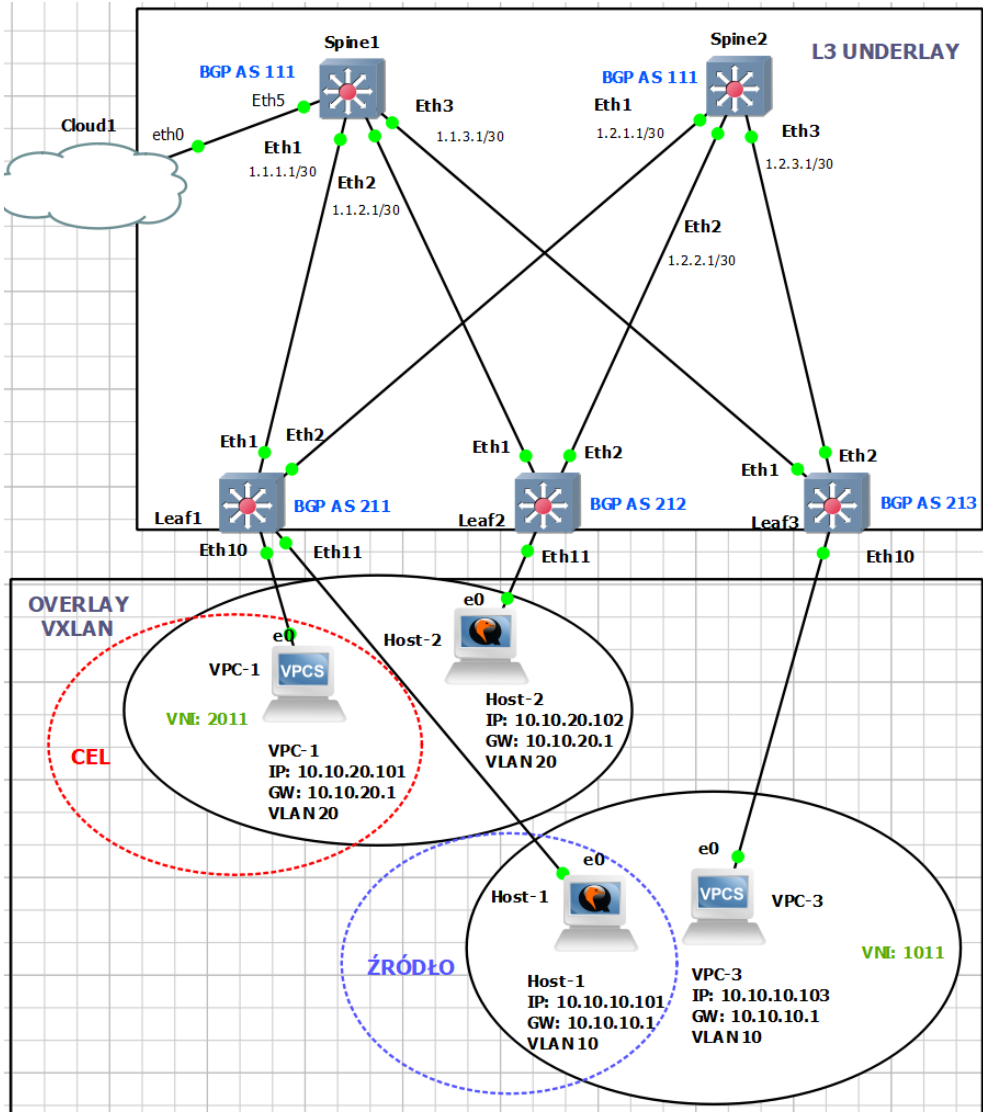
```
Leaf1(config)#sh ip bgp summary
BGP summary information for VRF default
Router identifier 1.2.1.2, local AS number 211
Neighbor Status Codes: m - Under maintenance
  Neighbor      V AS      MsgRcvd  MsgSent  InQ  OutQ  Up/Down State  PfxRcd PfxAcc
  1.1.1.1       4 111      447      444     0    0 07:18:41 Estab   9      9
  1.2.1.1       4 111      445      448     0    0 07:18:33 Estab   7      7
Leaf1(config)#sh vxlan vni
VNI to VLAN Mapping for Vxlan1
VNI      VLAN      Source      Interface      802.1Q Tag
-----
1011     10        static      Ethernet10     untagged
          Vxlan1     10
2011     20        static      Ethernet11     untagged
          Vxlan1     20
VNI to dynamic VLAN Mapping for Vxlan1
VNI      VLAN      VRF      Source
-----
Leaf1(config)#sh vxlan vtep detail
Remote VTEPS for Vxlan1:
VTEP      Learned Via      MAC Address Learning      Tunnel Type(s)
-----
212.1.1.1 control plane    datapath                    flood
213.1.1.1 control plane    datapath                    flood
Total number of remote VTEPS: 2
```

Rysunek 27. Weryfikacja BGP, map VLAN do UNI oraz VTEP-ów w przełączniku Leaf-1

Konfigurację systemów na urządzeniach końcowych przeprowadzono w taki sposób, aby do każdego przełącznika dostępowego były podłączone dwa hosty – każdy w oddzielnej sieci VLAN. Bramy domyślne wskazują na adresy IP anycast skonfigurowane na każdym VTEP'ie (rys. 27). Taka konfiguracja umożliwiła przeprowadzenie testów opisanych poniżej.

3.1. Przeskoki pomiędzy sieciami VLAN

Test miał na celu określenie liczby przeskoków pakietów od źródła podłączonego do przełącznika Leaf-1 i umieszczonego w sieci VLAN 10 do celu podłączonego do tego samego przełącznika, ale umieszczonego w sieci VLAN 20. Umiejscowienie stacji w infrastrukturze pokazano na rysunku 28.



Rysunek 28. Umiejscowienie źródła i celu w testowanej sieci

Test przeprowadzono przy pomocy narzędzia konsolowego „MTR”, a wynik przedstawiono na rysunku 29.

```
centos (0.0.0.0) My traceroute [v0.85] Sun Dec 19 18:47:17 2021
Keys: Help Display mode Restart statistics Order of fields quit
          Packets                               Pings
Host      Loss%  Snt   Last   Avg    Best  Wrst  StDev
1. 10.10.10.1    0.0%   21   21.7  26.5  11.9  76.7  20.0
2. 10.10.20.101 0.0%   20   31.4  32.9  23.3  139.8 25.2
```

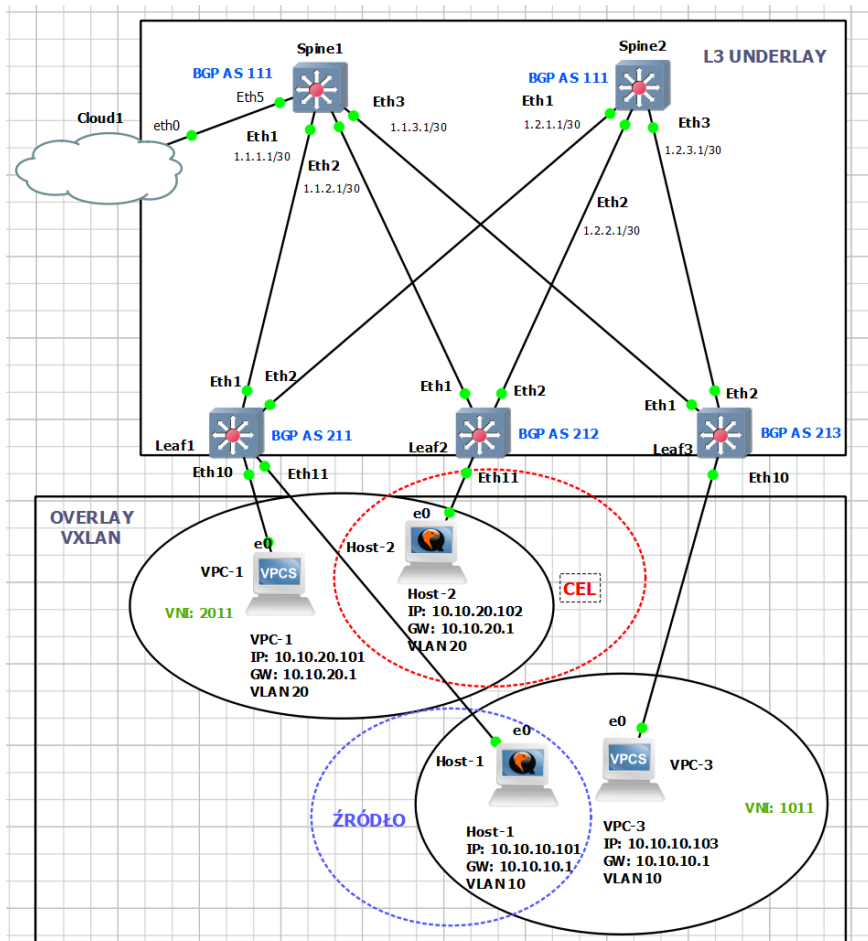
Rysunek 29. Wynik testu liczby przeskoków

3.2. Rozłożenie ruchu na połączeniach pomiędzy warstwami

Badanie pokazuje rozłożenie ruchu ze źródła do celu pomiędzy łączami redundantnymi zarówno w górę jak i w dół sieci. Ponieważ w modelu wykorzystano funkcję ECMP, przeprowadzono analizę tablic routingu na urządzeniach znajdujących się na trasie pakietów.

Umieszczenie źródła i celu w infrastrukturze przedstawiono na rysunku 30.

Topologia omawianej sieci pozwala na analizę tras na przełącznikach Leaf. Wynik testu przedstawiono na rysunkach 31 i 32.



Rysunek 30. Umieszczenie źródła i celu w teście rozłożenia ruchu sieciowego

```

C      1.1.1.0/30 is directly connected, Ethernet1
B E   1.1.2.0/30 [200/0] via 1.1.1.1, Ethernet1
B E   1.1.3.0/30 [200/0] via 1.1.1.1, Ethernet1
C      1.2.1.0/30 is directly connected, Ethernet2
B E   1.2.2.0/30 [200/0] via 1.2.1.1, Ethernet2
B E   1.2.3.0/30 [200/0] via 1.2.1.1, Ethernet2
C      10.10.10.0/24 is directly connected, Vlan10
C      10.10.20.0/24 is directly connected, Vlan20
B E   10.48.150.0/24 [200/0] via 1.1.1.1, Ethernet1
C      211.1.1.1/32 is directly connected, Loopback1
B E   212.1.1.1/32 [200/0] via 1.1.1.1, Ethernet1
      via 1.2.1.1, Ethernet2
B E   213.1.1.1/32 [200/0] via 1.1.1.1, Ethernet1
      via 1.2.1.1, Ethernet2
    
```

Rysunek 31. Tablica routingu w przełączniku Leaf-1

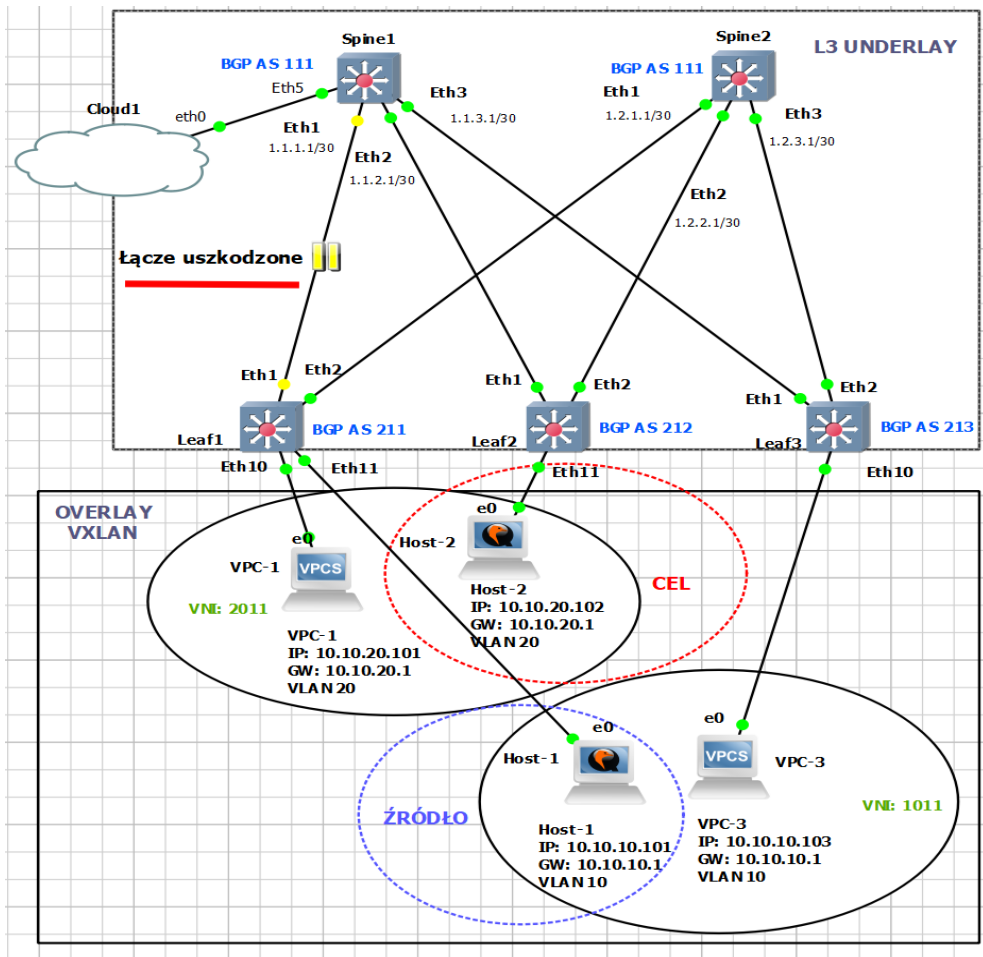
```
B E 1.1.1.0/30 [200/0] via 1.1.2.1, Ethernet1
C   1.1.2.0/30 is directly connected, Ethernet1
B E 1.1.3.0/30 [200/0] via 1.1.2.1, Ethernet1
B E 1.2.1.0/30 [200/0] via 1.2.2.1, Ethernet2
C   1.2.2.0/30 is directly connected, Ethernet2
B E 1.2.3.0/30 [200/0] via 1.2.2.1, Ethernet2
C   10.10.10.0/24 is directly connected, Vlan10
C   10.10.20.0/24 is directly connected, Vlan20
B E 10.48.150.0/24 [200/0] via 1.1.2.1, Ethernet1
B E 211.1.1.1/32 [200/0] via 1.1.2.1, Ethernet1
                        via 1.2.2.1, Ethernet2
C   212.1.1.1/32 is directly connected, Loopback1
B E 213.1.1.1/32 [200/0] via 1.1.2.1, Ethernet1
                        via 1.2.2.1, Ethernet2
```

Rysunek 32. Tablica routingu w przełączniku Leaf-2

3.3. Awaria jednego łącza w górę sieci

Poniższe badanie miało na celu określenie czasu potrzebnego na osiągnięcie zbieżności sieci po zasymulowaniu awarii aktywnego połączenia pomiędzy przełącznikiem Leaf-1 a warstwą wyższą. W tym celu została zbadana liczba utraconych pakietów ICMP wysyłanych w jednosekundowych odstępach ze źródła do celu.

Umieszczenie źródła, celu i uszkodzenia połączenia przedstawiono na rysunku 33, a wyniki badania na rysunku 34.



Rysunek 33. Umieszczenie źródła, celu i uszkodzonego łącza


```
PING 10.10.20.102 (10.10.20.102) 56(84) bytes of data.  
64 bytes from 10.10.20.102: icmp_seq=1 ttl=63 time=256 ms  
64 bytes from 10.10.20.102: icmp_seq=2 ttl=63 time=64.1 ms  
64 bytes from 10.10.20.102: icmp_seq=4 ttl=63 time=178 ms  
64 bytes from 10.10.20.102: icmp_seq=5 ttl=63 time=78.8 ms  
64 bytes from 10.10.20.102: icmp_seq=6 ttl=63 time=85.0 ms  
64 bytes from 10.10.20.102: icmp_seq=7 ttl=63 time=202 ms  
64 bytes from 10.10.20.102: icmp_seq=8 ttl=63 time=76.5 ms  
64 bytes from 10.10.20.102: icmp_seq=9 ttl=63 time=84.7 ms  
64 bytes from 10.10.20.102: icmp_seq=10 ttl=63 time=190 ms  
64 bytes from 10.10.20.102: icmp_seq=11 ttl=63 time=80.9 ms  
64 bytes from 10.10.20.102: icmp_seq=12 ttl=63 time=81.0 ms  
64 bytes from 10.10.20.102: icmp_seq=13 ttl=63 time=215 ms  
64 bytes from 10.10.20.102: icmp_seq=14 ttl=63 time=79.2 ms  
64 bytes from 10.10.20.102: icmp_seq=15 ttl=63 time=90.6 ms  
64 bytes from 10.10.20.102: icmp_seq=16 ttl=63 time=191 ms  
64 bytes from 10.10.20.102: icmp_seq=17 ttl=63 time=78.1 ms  
64 bytes from 10.10.20.102: icmp_seq=18 ttl=63 time=123 ms  
64 bytes from 10.10.20.102: icmp_seq=19 ttl=63 time=176 ms  
64 bytes from 10.10.20.102: icmp_seq=20 ttl=63 time=82.9 ms  
64 bytes from 10.10.20.102: icmp_seq=21 ttl=63 time=103 ms  
64 bytes from 10.10.20.102: icmp_seq=22 ttl=63 time=176 ms  
64 bytes from 10.10.20.102: icmp_seq=23 ttl=63 time=106 ms  
64 bytes from 10.10.20.102: icmp_seq=24 ttl=63 time=87.9 ms  
64 bytes from 10.10.20.102: icmp_seq=25 ttl=63 time=177 ms
```

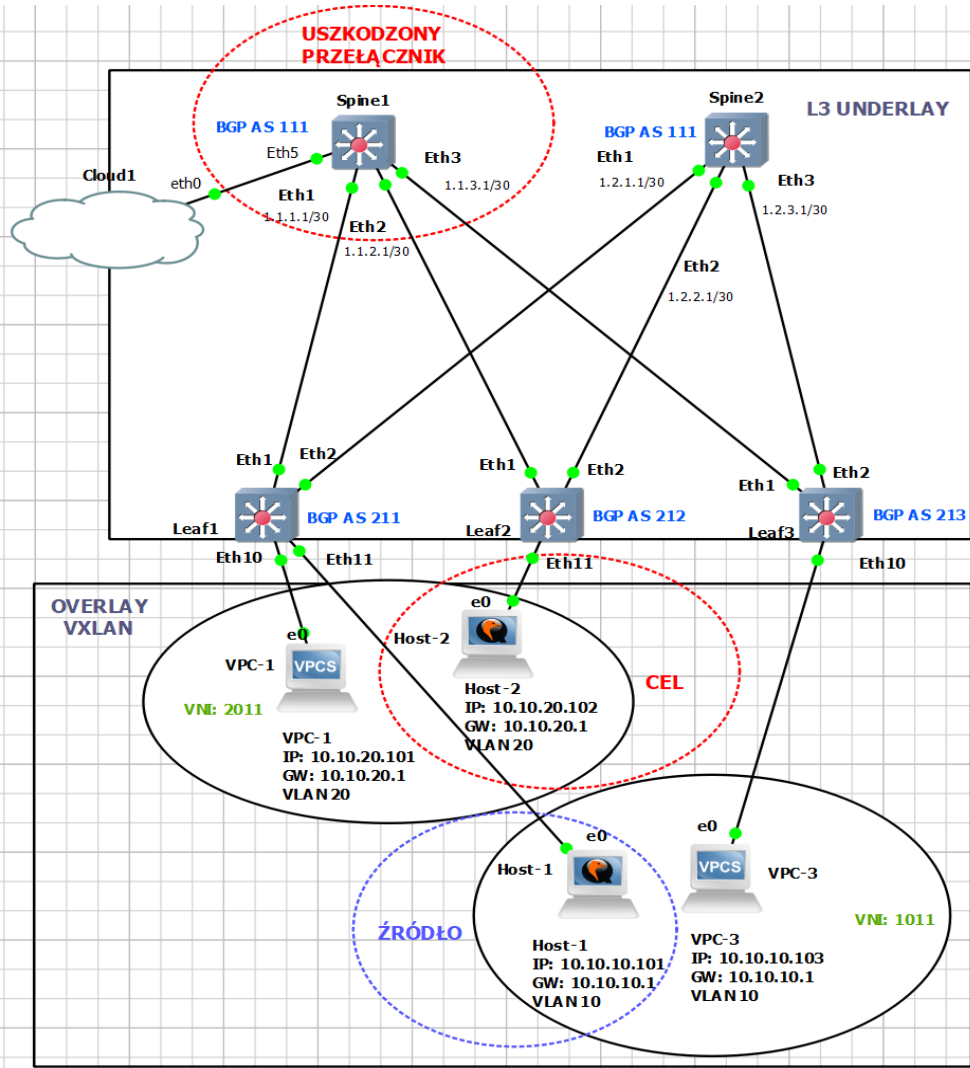
Rysunek 34. Wyniki badania zasymulowanej awarii łącza

3.4. *Awaria przełącznika Spine1*

Ostatnie badanie pokazuje, jak długa przerwa nastąpi w transmisji podczas awarii przełącznika Spine1, do którego prowadzi łącze z niższej warstwy. Umieszczenie źródła, celu i uszkodzonego przełącznika pokazano na rysunku 35.

Badanie przeprowadzono w sposób analogiczny do poprzedniego. Ze źródła do celu wysyłano pakiety ICMP ping w jednosekundowych odstępach. Badanie przeprowadzono również w dwóch etapach: podczas awarii i podczas odzyskania sprawności.

Rezultat badania przedstawiono na rysunkach 36 i 37.



Rysunek 35. Umieszczenie źródła, celu i uszkodzonego przełącznika Spine1

```
[root@centos ~]# ping 10.10.20.102 -i 1
PING 10.10.20.102 (10.10.20.102) 56(84) bytes of data.
64 bytes from 10.10.20.102: icmp_seq=1 ttl=63 time=121 ms
64 bytes from 10.10.20.102: icmp_seq=2 ttl=63 time=91.3 ms
64 bytes from 10.10.20.102: icmp_seq=3 ttl=63 time=103 ms
64 bytes from 10.10.20.102: icmp_seq=4 ttl=63 time=83.9 ms
64 bytes from 10.10.20.102: icmp_seq=5 ttl=63 time=84.9 ms
64 bytes from 10.10.20.102: icmp_seq=7 ttl=63 time=87.6 ms
64 bytes from 10.10.20.102: icmp_seq=8 ttl=63 time=207 ms
```

Rysunek 36. Wynik testu w czasie awarii

```
64 bytes from 10.10.20.102: icmp_seq=180 ttl=63 time=115 ms
64 bytes from 10.10.20.102: icmp_seq=181 ttl=63 time=68.3 ms
64 bytes from 10.10.20.102: icmp_seq=182 ttl=63 time=67.5 ms
64 bytes from 10.10.20.102: icmp_seq=183 ttl=63 time=198 ms
64 bytes from 10.10.20.102: icmp_seq=184 ttl=63 time=82.0 ms
64 bytes from 10.10.20.102: icmp_seq=185 ttl=63 time=168 ms
64 bytes from 10.10.20.102: icmp_seq=186 ttl=63 time=218 ms
64 bytes from 10.10.20.102: icmp_seq=187 ttl=63 time=87.1 ms
64 bytes from 10.10.20.102: icmp_seq=188 ttl=63 time=200 ms
64 bytes from 10.10.20.102: icmp_seq=189 ttl=63 time=149 ms
64 bytes from 10.10.20.102: icmp_seq=190 ttl=63 time=84.6 ms
```

Rysunek 37. Wynik testu po przywróceniu sprawności

4. Podsumowanie

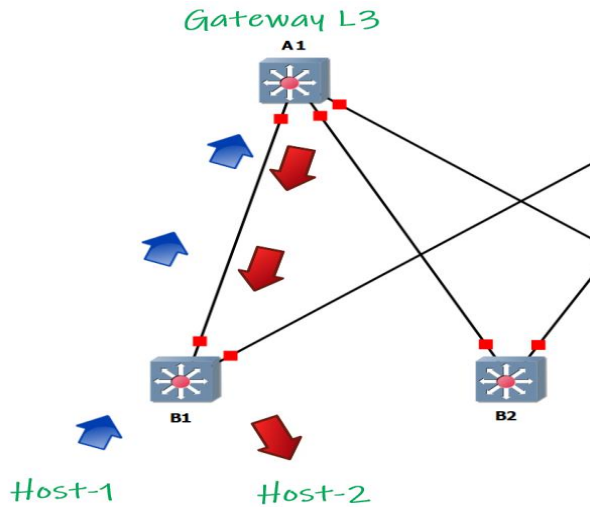
W poprzednich rozdziałach przeprowadzono testy wydajności sieci w dwóch modelach. Pierwszy to sieć bazująca na klasycznych rozwiązaniach, takich jak model hierarchiczny, protokół drzewa opinającego i VLAN.

Drugi model wykorzystuje nowsze technologie takie jak spine-and-leaf, redundancję bazującą na funkcjonalności ECMP oraz Anycast Gateway, będącą częścią technologii VXLAN.

Wyniki przeprowadzonych testów są wyszczególnione poniżej.

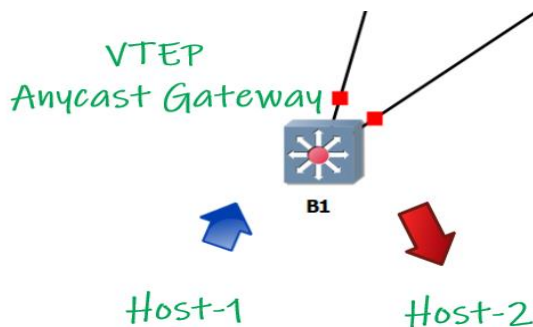
4.1. Przeskoki pomiędzy sieciami VLAN

W pierwszym przypadku liczba przeskoków wyniosła dwa. Zatem pakiet z hosta enkapsulowany w ramkę trafia na przełącznik dostępowy. Dalej trafia na przełącznik dystrybucyjny gdzie następuje deenkapsulacja, routing, ponowna enkapsulacja i odsyłanie ramki ponownie do przełącznika dostępowego, skąd dociera do hosta docelowego. Trasę pakietu przedstawiono na rysunku 38.



Rysunek 38. Trasa pakietu w modelu z siecią VLAN

W drugim przypadku, liczba przeskoków również wyniosła dwa. Jednak tutaj urządzeniem pierwszego skoku jest to, do którego bezpośrednio są podłączone hosty docelowy i źródłowy. Routing odbywa się bezpośrednio na tym urządzeniu. Poniżej na rys. 39 pokazano trasę pakietu.



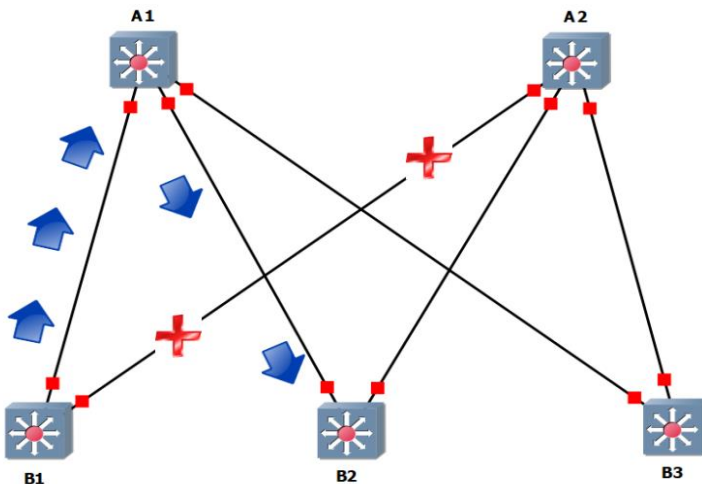
Rysunek 39. Trasa pakietu w modelu z siecią VxLAN

Porównując oba wyniki, w modelu VxLAN trasa jest skracana o co najmniej dwa przeskoki, do i z urządzenia warstwy wyższej. Został skrócony czas, w jakim pakiet pokonuje trasę ze źródła do celu, a ponadto nie jest zajmowana przepustowość łącza do warstwy wyższej.

4.2. Rozłożenie ruchu na połączeniach pomiędzy warstwami

Wyniki badania w pierwszym modelu wykazały, że protokół MSTP ustawił w stan blokowania po jednym łączu z przełączników dostępowych do przełączników wyższej warstwy. Aktywne pozostały tylko łącza do jednego przełącznika dystrybucyjnego. I chociaż jest to właściwe zachowanie MSTP, to jednak ogranicza możliwą przepustowość o połowę. MSTP daje możliwość utworzenia oddzielnego drzewa dla każdej sieci VLAN lub ich grupy, co pozwala zniwelować ten problem. Jednak wymaga to dużej uwagi i uwzględniania tego czynnika przy zmianach w sieci.

Rysunek 40 przedstawia rozłożenie ruchu w modelu z siecią VLAN.

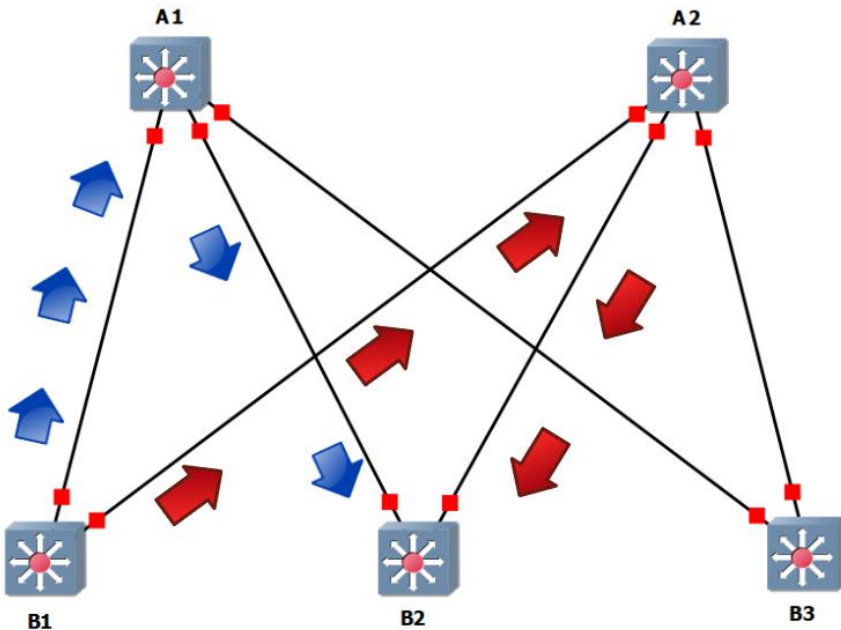


Rysunek 40. Rozłożenie ruchu pakietów w modelu z siecią VLAN

Badanie wykazało, że w rozwiązaniu w modelu z siecią VxLAN powyższy problem nie występuje. Wiele tras o tym samym koszcie, które są przekazywane do tablicy routingu, pozwala na wykorzystanie wszystkich łączy w zrównoważony sposób bez „sztywnego” konfigurowania tras. Algorytmy dostępne do wykorzystania podczas

balansowania ruchu pomiędzy łączami są zależne od producenta i sprzętu. Wydaje się jednak, że nawet najprostszy algorytm rozkładający ruch równo pomiędzy łączami jest bardziej elastyczny od wymuszonej, stałej konfiguracji.

Rysunek 41 przedstawia rozłożenie ruchu na dwa łącza w modelu z siecią VxLAN.



Rysunek 41. Rozłożenie ruchu pakietów w modelu z siecią VxLAN

4.3. *Awaria jednego łącza w górę sieci*

Badanie miało na celu ustalenie czasu, przez jaki pakiety nie są przekazywane w sieci. W pierwszym przypadku przerwa w trakcie wystąpienia awarii trwała około 6 sekund. Tyle potrzebował protokół MSTP na przełączenie łącza zapasowego w stan aktywny. Zbadano też czas niedostępności w momencie ustąpienia awarii, który wyniósł 2 sekundy. Daje to łącznie 8 sekund niedostępności w trakcie nawet krótkiej awarii. Co prawda nie są to wartości tak wysokie, jak w przypadku zwykłego STP,

jednak 8 sekund nadal jest dużą wartością w kontekście dużych sieci korporacyjnych. Obecnie nie są znane metody przyspieszenia zbieżności dla sieci wykorzystujących protokoły z rodziny STP.

Jak wykazało badanie modelu z siecią VxLAN, sieć bazująca na połączeniach L3 potrzebuje znacznie mniej czasu na osiągnięcie stanu zbieżności. Podczas awarii łącza, czas niedostępności wynosił około 1 sekundy, natomiast w chwili jej ustąpienia nie wystąpiła żadna przerwa. Jest to charakterystyczne dla ruchu opartego o połączenia L3 z routingiem dynamicznym. W momencie awarii protokołów routingu potrzebuje czasu na uznanie trasy za uszkodzoną, usunięcie jej z tablicy routingu i rozpropagowanie tej informacji. Zanim to się stanie trasa jest w tablicy routingu jako prawidłowa i wszystkie pakiety przekazane na jej podstawie trafiają do „czarnej dziury” – stąd chwilowa niedostępność. Kiedy połączenie zostanie naprawione, trasa pojawia się w tablicy routingu i jest w tym momencie w pełni prawidłowa. Pakiety, które z niej skorzystają, są przekazywane do następnego skoku. Z tego powodu nie pojawia się żadna niedostępność w momencie ustąpienia awarii.

4.4. Awaria przełącznika wyższej warstwy

Badanie miało na celu ustalenie czasu, przez jaki pakiety nie są przekazywane w sieci. Jego rezultaty były zbliżone do wyników poprzedniego badania. Model z siecią VxLAN zarejestrował jednosekundową przerwę w momencie wystąpienia awarii i pracował bezprzerwowo w czasie usunięcia usterki. Różnica pojawiła się w modelu z siecią VLAN – podczas usunięcia usterki czas niedostępności okazał się o 3 sekundy dłuższy i wyniósł 5 sekund.

5. Literatura

- [1] G.A. Donahue, *Arista Warrior: A Real-World Guide to Understanding Arista Switches and EOS*, O'Reilly Media, 2019.
- [2] S. Maloo, A. Firas, *CCNP and CCIE Data Center Core DCCOR 350-601 Official Cert Guide*, Cisco Press, 2020.
- [3] M. Al-shawi, *CCDE Study Guide*, Cisco Press, 2015.
- [4] D. Jansen, L. Krattiger, S. Kapadia, *Building Data Centers with VXLAN BGP EVPN: A Cisco NX-OS Perspective*, Cisco Press, 2017.

VLAN and VxLAN Technologies Implementation in Contemporary ICT Networks

Abstract

The article presents an analysis of packet traffic in ICT networks with the use of VLAN and VxLAN technologies. The following chapters include the preparation of the physical base environment, the implementation of two selected solutions, testing and discussion of the results obtained.

Keywords: *VLAN technology, VxLAN technology, ICT networks, network protocols, IP routing*