

Modular Campus Network Design with VLANs, Trunks and PVST+

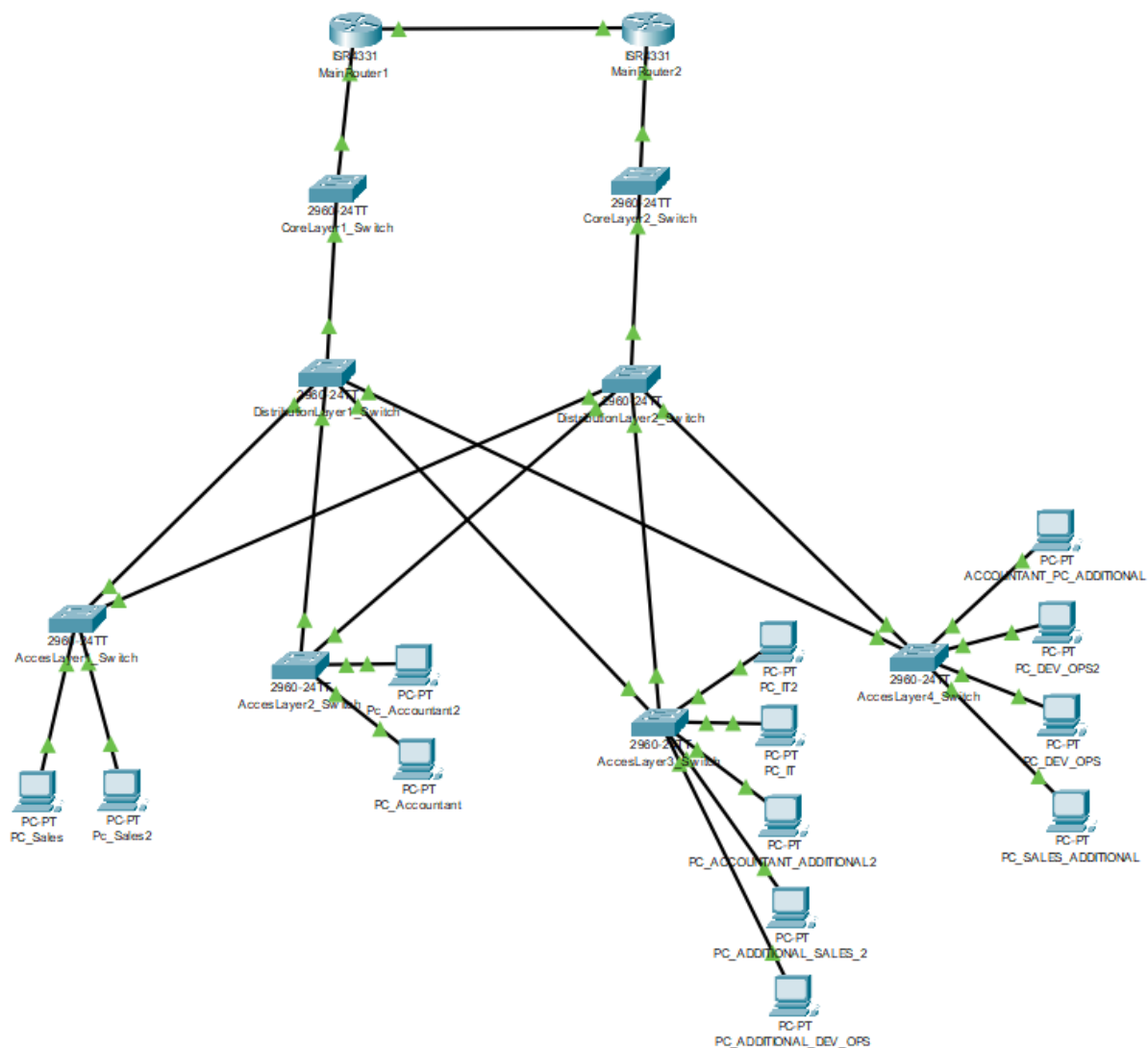
Założenia:

W projekcie chciałem ująć tematyki związane z Vlana-mi, HSRP oraz STP.

1. Topologia sieci.

Postanowiłem że zastosuję topologię kampusową. Pominąłem wdrożenie routerów ISP, z uwagi na to że laboratoria z routingu nie są celem tej pracy. Sieć Składa się z 2 głównych routerów (docelowo każdy router byłby podłączony do osobnego dostawcy internetu – zabieg mający na celu zabezpieczenie w przypadku awarii u jednego z dostawców. Rozwiązanie kosztowne, sugerowane firmom dla których wysoki wskaźnik availability jest istotny. Sugestia: warto w takiej sytuacji rozważyć główne łącze o przepustowości 1 Gbps oraz łącze zapasowe o niższej przepustowości, np. 300 Mbps. Dlaczego? Ponieważ zapasowe łącze gigabitowe generuje zbyt duże koszty w stosunku do swojej roli, którą pełni jedynie w przypadku awarii.

2. Konfiguracja urządzeń.



Mamy klasyczną sieć kampusową. Switche warstwy dostępowej zapewniają połączenie hostom. Każdy switch warstwy access podłączony do 2 switchy warstwy distribution (Zapewnienie redundancji łącza).

Switch acc1:

Na tym switchu ustawiłem jeden vlan (10), mając na uwadze fakt że są tam podłączone urządzenia tylko z działu sales któremu ten vlan jest docelowo przypisany

```

1      default      active      Fa0/3, Fa0/4, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gig0/1, Gig0/2
10     VLAN_SALES   active      Fa0/5, Fa0/6, Fa0/7, Fa0/8
1002   fddi-default active
1003   token-ring-default active
1004   fddinet-default active
1005   trnet-default active
Switch#

```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/2	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa0/1	10,20,30,40			
Fa0/2	10,20,30,40			
Port	Vlans allowed and active in management domain			
Fa0/1	10			
Fa0/2	10			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa0/1	10			
Fa0/2	10			

Na switchu 3 i 4 doszło jednak do anomalii. W trakcie prac uznano że jednak do pokoju należy dokooptować ludzi z innych działów. Więc dodano stanowiska które docelowo powinny znajdować się na innym piętrze. Przykładowa konfiguracja switcha acc4:

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig0/1, Gig0/2
10	VLAN_SALES	active	Fa0/16
20	VLAN_ACCOUNTANT	active	Fa0/15
30	VLAN_IT	active	Fa0/17
40	VLAN_DevOps	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0

Switch#show interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	auto	n-802.1q	trunking	1
Fa0/2	auto	n-802.1q	trunking	1

Port Vlans allowed on trunk

Fa0/1	10,20,30,40
Fa0/2	10,20,30,40

Port Vlans allowed and active in management domain

Fa0/1	10,20,30,40
Fa0/2	10,20,30,40

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1	10,20,30,40
Fa0/2	10,20,30,40

Konfiguracja switcha warstwy distribution layer:

VLAN	Name	Status	Ports
1	default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10	VLAN0010	active	
20	VLAN_ACCOUNTANT	active	
30	VLAN_IT	active	
40	VLAN_DEV_OPS	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0

--More--

//błąd administratora. Nie została ustawiona nazwa dla Vlanu 10.

```
Switch#show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Fa0/1     on        802.1q         trunking     1
Fa0/2     on        802.1q         trunking     1
Fa0/3     on        802.1q         trunking     1
Fa0/4     on        802.1q         trunking     1
Fa0/5     on        802.1q         trunking     1

Port      Vlans allowed on trunk
Fa0/1     10,20,30,40
Fa0/2     10,20,30,40
Fa0/3     10,20,30,40
Fa0/4     10,20,30,40
Fa0/5     10,20,30,40

Port      Vlans allowed and active in management domain
Fa0/1     10,20,30,40
Fa0/2     10,20,30,40
Fa0/3     10,20,30,40
Fa0/4     10,20,30,40
Fa0/5     10,20,30,40
```

Konfiguracja switcha nr 2 w warstwie distribution taka sama.

Switche warstwy core. Tutaj nie zachodzi redundancja między łączem distribution a core. Nie jest konieczna, co wynika z samej topologii.

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Gig0/1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	10,20,30,40
Gig0/1	10,20,30,40

Port	Vlans allowed and active in management domain
Fa0/1	10,20,30,40
Gig0/1	10,20,30,40

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	10,20,30,40
Gig0/1	10,20,30,40

1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/2
10	VLAN0010	active	
20	VLAN_ACCOUNTANT	active	
30	VLAN_IT	active	
40	VLAN_DEV_OPS	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0

--More-- |

Teraz przejdzie HSRP (Hot standby router protocol).

Na routerach zastosowano HSRP. Jaki jest tego cel? Wprowadzenie load balancingu między podsieciami. Router 1 pełni rolę Active dla vlanów 10 i 20. Jest w trybie standby dla vlanów 30 i 40. Natomiast na routerze standby dla vlanów 10 i 20 oraz active dla 30 i 40.

Odnosnie protokołu STP. Root bridgem dla vlanów 10 i 20 został ręcznie wybrany switch core layer nr 1. Jest to częsty zabieg stosowany w sieciach kampusowych. Switchy warstwy core powinny pełnić rolę root bridgea. U mnie podział jest 50/ 50. Switch core 1 pełni rolę bridge-a dla 2 vlanów, dla pozostałych 2 jest secondary. Odwrotna sytuacja na switchu core layer 2.

```
VLAN0010
Spanning tree enabled protocol ieee
Root ID    Priority    24586
           Address    00D0.97BE.D116
           This bridge is the root
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    24586 (priority 24576 sys-id-ext 10)
           Address    00D0.97BE.D116
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 20

Interface   Role Sts Cost      Prio.Nbr Type
-----
Gi0/1       Desg FWD 4        128.25  P2p
Fa0/1       Desg FWD 19       128.1   P2p

VLAN0020
Spanning tree enabled protocol ieee
Root ID    Priority    24596
           Address    00D0.97BE.D116
           This bridge is the root
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    24596 (priority 24576 sys-id-ext 20)
           Address    00D0.97BE.D116
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 20

Interface   Role Sts Cost      Prio.Nbr Type
-----
Gi0/1       Desg FWD 4        128.25  P2p
Fa0/1       Desg FWD 19       128.1   P2p
```

VLAN0030

Spanning tree enabled protocol ieee

Root ID Priority 24606
 Address 00D0.BA4C.6581
 Cost 76
 Port 1(FastEthernet0/1)
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 28702 (priority 28672 sys-id-ext 30)
 Address 00D0.97BE.D116
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Gi0/1	Desg	FWD	4	128.25	P2p
Fa0/1	Root	FWD	19	128.1	P2p

VLAN0040

Spanning tree enabled protocol ieee

Root ID Priority 24616
 Address 00D0.BA4C.6581
 Cost 76
 Port 1(FastEthernet0/1)
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 28712 (priority 28672 sys-id-ext 40)
 Address 00D0.97BE.D116
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Gi0/1	Desg	FWD	4	128.25	P2p
Fa0/1	Root	FWD	19	128.1	P2p

GigabitEthernet0/0/1.10 - Group 1

State is Active

12 state changes, last state change 01:18:07

Virtual IP address is 192.168.5.1

Active virtual MAC address is 0000.0C07.AC01

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

Hello time 3 sec, hold time 10 sec

Next hello sent in 0.707 secs

Preemption enabled

Active router is local

Standby router is 192.168.5.3, priority 90 (expires in 7 sec)

Priority 110 (configured 110)

Group name is hsrp-Gig-1 (default)

GigabitEthernet0/0/1.20 - Group 1

State is Active

11 state changes, last state change 01:17:48

Virtual IP address is 192.168.6.1

Active virtual MAC address is 0000.0C07.AC01

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

Hello time 3 sec, hold time 10 sec

Next hello sent in 1.407 secs

Preemption enabled

Active router is local

Standby router is 192.168.6.3, priority 90 (expires in 7 sec)

Priority 110 (configured 110)

Group name is hsrp-Gig-1 (default)

```
Group name is hsrp-Gig-1 (default)
GigabitEthernet0/0/1.30 - Group 1
State is Standby
  19 state changes, last state change 02:14:34
Virtual IP address is 192.168.7.1
Active virtual MAC address is 0000.0C07.AC01
  Local virtual MAC address is 0000.0C07.AC01 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.507 secs
Preemption enabled
Active router is 192.168.7.3, priority 110 (expires in 7 sec)
  MAC address is 0000.0C07.AC01
Standby router is local
Priority 90 (configured 90)
Group name is hsrp-Gig-1 (default)
GigabitEthernet0/0/1.40 - Group 1
State is Standby
  18 state changes, last state change 02:01:42
Virtual IP address is 192.168.8.1
```

3. Test działania.

Wykorzystano podstawowe narzędzia diagnostyczne w postaci polecenia ping oraz traceroute.

Wynik:

Physical Config **Desktop** Programming Attributes

Command Prompt

```
C:\>ping 192.168.8.30

Pinging 192.168.8.30 with 32 bytes of data:

Reply from 192.168.8.30: bytes=32 time<1ms TTL=127
Reply from 192.168.8.30: bytes=32 time<1ms TTL=127
Reply from 192.168.8.30: bytes=32 time=10ms TTL=127
Reply from 192.168.8.30: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.8.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

```
C:\>tracert 192.168.8.30

Tracing route to 192.168.8.30 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.5.2
  2  0 ms    0 ms    0 ms    192.168.8.30

Trace complete.
```

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.6.20

Pinging 192.168.6.20 with 32 bytes of data:

Request timed out.
Reply from 192.168.6.20: bytes=32 time=11ms TTL=127
Reply from 192.168.6.20: bytes=32 time=1ms TTL=127
Reply from 192.168.6.20: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.6.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 4ms

C:\>
```

```
C:\>tracert 192.168.7.10

Tracing route to 192.168.7.10 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.8.3
  2  0 ms    0 ms    0 ms    192.168.7.10

Trace complete.
```

4. Wnioski końcowe.

Ku mojemu zdziwieniu w topologii nie pojawiły się żadne porty typu blocked (alternate). Dopiero po weryfikacji wersji protokołu STP moim oczom ukazał się PVST+. Tworzy on osobne instancje „drzewa” dla każdego vlanu, co jak widzimy eliminuje powstanie ewentualnych pętli. Stosując bazową wersję protokołu STP (802.1d) zobaczylibyśmy w topologii pomarańczowe kropki, symbolizujące zablokowane porty.