

Protokół VTP (VLAN Trunking Protocol)

Jest to protokół, którego zadaniem jest utrzymywanie aktualnej bazy danych vlanów na wszystkich switchach w ramach całej domeny VTP. Protokół ten jest protokołem firmowym Cisco i występuje w trzech wersjach. Wersja numer 3 pojawiła się stosunkowo niedawno i jest bardzo ciekawym rozwiązaniem, ale może po kolei – najpierw trochę teorii ;-)

Na każdym switchu przechowywana jest baza danych vlanów, które dany switch obsługuje. Jeśli w bazie danych nie ma jakiegoś vlanu, to jest on obsługiwany przez switch.

```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, 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 Gig1/1, Gig1/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Od razu nasuwa się pytanie, po co dodatkowa baza danych, czy switch nie mógł by obsługiwać wszystkich vlanów? Okazuje się, że nie. Dla przykładu switch catalyst 2960 może jednocześnie obsługiwać tylko 255 vlanów. Dla przypomnienia – wszystkich vlanów, które można skonfigurować jest 4094 i są one podzielone na dwa zakresy: podstawowy (1-1005) oraz rozszerzony (1006-4094).

```
Switch#sh vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Server
VTP Domain Name :
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

Dlatego też switch musi wiedzieć, które z vlanów powinien obsługiwać. Musimy też pamiętać, że vlany do bazy danych dodawane są czasem w sposób automatyczny, na przykład wtedy, gdy przypisujemy port do jakiegoś vlanu:

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa 0/16
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
```

A czasem musimy dopisać vlan do bazy danych ręcznie, na przykład wtedy, gdy switch pełni rolę urządzenia tranzytowego dla jakiegoś vlanu:

```
Switch#sh vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, 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
Gig1/1, Gig1/2
1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int ran fa0/16 , fa0/17
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk allowed vlan 20
Switch(config-if-range)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vlan brief

```

VLAN Name	Status	Ports
1 default	active	Fa0/1, 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 Gig1/1, Gig1/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
sh vlan brief

```

VLAN Name	Status	Ports
1 default	active	Fa0/1, 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 Gig1/1, Gig1/2
20 VLAN0020	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Jeśli zapomnimy dodać vlan do bazy danych, to pomimo poprawnej konfiguracji na portach trunk, vlan nie będzie przenoszony przez switch. To, czy vlan będzie przez porty trunk przenoszony poprawnie, czy nie możemy sprawdzić przy użyciu polecenia:

```
S2#show interfaces trunk
```

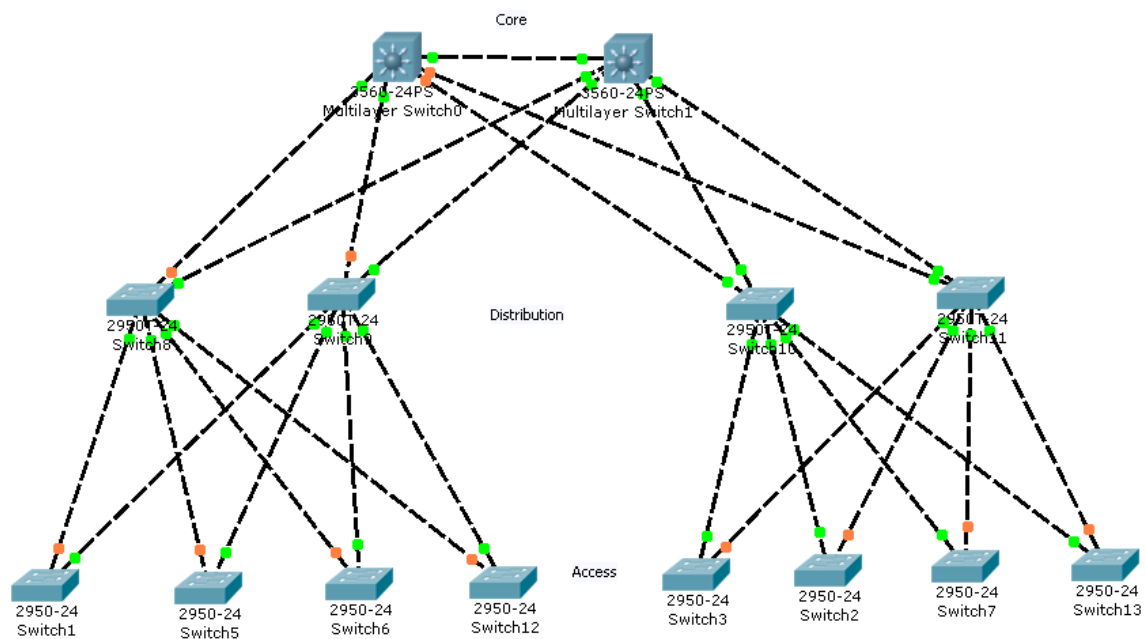
Port	Mode	Encapsulation	Status	Native vlan
Po2	on	802.1q	trunking	99
Po3	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Po2	1-4094
Po3	1-4094

Port	Vlans allowed and active in management domain
Po2	1,99,111
Po3	1,99,111

Port	Vlans in spanning tree forwarding state and not pruned
Po2	1,99,111
Po3	1,99,111

Porty „Po” to Port-channel. Dodatkowo należy pamiętać, że polecenie to pokazuje status portów trunk, które są w stanie „up”, jeśli na porcie trunk nie ma linku, polecenie nie pokaże jego statusu. Wróćmy do protokołu VTP. Jego zadaniem jest automatyczna synchronizacja baz danych vlanów na wszystkich switchach w ramach domeny VTP. Domena VTP, to switchy, które posługują się taką samą nazwą domenową. Domyślnie protokół VTP jest wyłączony, nazwa domenowa jest ustawiona na pusty ciąg znaków (null), i wszystkie zmiany w bazie danych vlanów muszą być wykonywane ręcznie. Proszę zwrócić uwagę na to ile pracy trzeba włożyć, aby przeciągnąć jeden vlan łączący switchy 1 i 13:



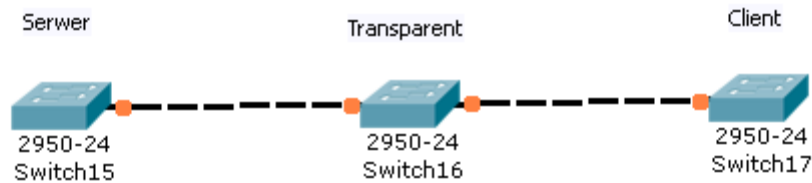
Należy skonfigurować vlan co najmniej na 5 switchach, tyle że nie będziemy mieć wtedy redundancji. Aby uzyskać pełną redundancję musimy skonfigurować vlan na wszystkich 14 urządzeniach. Gdyby wykonać tę konfigurację ręcznie – jest to bardzo czasochłonne. Tutaj właśnie ma nam pomóc protokół VTP.

Protokół VTP umożliwia switchom pracę w jednym z trzech trybów:

Serwer – umożliwia dodawanie nowych vlanów, bądź kasowanie już istniejących w lokalnej bazie danych, dodatkowo zmiany są propagowane na całą domenę VTP. Jeśli dodamy nowy vlan, to jest on dodawany na wszystkich switchach w domenie. Na serwerze vlany są zapisywane w pamięci flash i po restarcie urządzenia mogą być stamtąd odczytane.

Klient – nie pozwala na wprowadzanie żadnych zmian, nie przechowuje bazy danych vlanów w pamięci flash, po restarcie urządzenia musi prosić o przesłanie pełnej bazy danych vlanów z serwera.

Transparent – switch pracujący w tym trybie jest wyłączony z działania protokołu vtp, baza danych vlanów jest przechowywana w pamięci flash, ale jeśli na switchu pracującym w tym trybie dodamy vlan, to zostanie on dodany tylko lokalnie. Jeśli będziemy mieli trzy switchy połączone ze sobą jak niżej:



to switch pracujący w trybie transparent będzie przezroczysty dla protokołu vtp i nie będzie blokował komunikacji serwera z klientem. Dodatkowo praca w trybie transparent umożliwia użycie pełnego zakresu vlanów (1 – 4094), natomiast jeśli switchy pracują w trybie serwer bądź klient, to mogą używać tylko vlanów podstawowych (1 – 1005), wyjątkiem jest vtp v.3, ale tą wersję protokołu chciałbym omówić osobno, bo odbiega ona znacznie od wersji 1 i 2.

Zaleca się, aby w sieci przełączanej były co najmniej dwa switchy skonfigurowane jako serwer, w przeciwnym razie awaria serwera spowoduje, że nie będziemy w stanie kontrolować bazy danych vlanów, a klienci nie będą mieli skąd pobrać aktualnej bazy danych na przykład po restarcie klienta. Zmiany wprowadzone na dowolnym serwerze propagowane są do wszystkich klientów oraz do pozostałych serwerów. Aby ustalić kto ma najświeższą wersję bazy danych stosowany jest numer rewizyjny:

```

Switch#sh vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode        : Server
VTP Domain Name           :
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
  
```

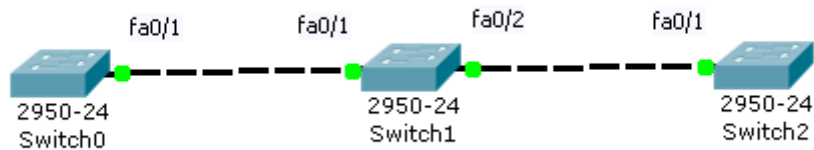
Startuje on od 0, a następnie każda zmiana wprowadzona do bazy danych vlanów powoduje jego zwiększenie o 1. Każdy serwer rozsyła zawartość swojej bazy danych vlanów oraz aktualny numer rewizyjny. Jako najświeższa baza danych uznawana jest ta, która ma najwyższy numer rewizyjny. Niestety taka metoda postępowania niesie też pewne ryzyko. Jeśli ktoś podłączy do naszej sieci switch, który będzie skonfigurowany jako serwer, będzie miał skonfigurowaną taką samą nazwę domeny vtp i będzie miał wyższy numer rewizyjny niż urządzenia w naszej sieci, to nadpisze on aktualną bazę danych na wszystkich urządzeniach w naszej sieci. Sytuacja taka może się zdarzyć także wtedy, gdy switch pracujący w naszej sieci odłączymy do celów testowych, a następnie podłączymy go z powrotem. Bardzo ważne jest sprawdzenie na switchu, który chcemy podłączyć do naszej sieci jaki ma numer rewizyjny. Numer ten możemy zresetować zmieniając nazwę domeny vtp na inną, a potem powracając do poprzedniej nazwy.

Domyślnie protokół VTP jest wyłączony na switchu, poprzez ustawienie nazwy domeny na pusty ciąg znaków:

```

Switch#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode        : Server
VTP Domain Name           :
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
  
```

Domyślny tryb pracy to serwer. Nasza przykładowa sieć wygląda następująco:



Po pierwsze pamiętajmy o tym, że protokół vtp do działania wymaga, aby switche były połączone portami typu trunk. Jeśli link łączący switche będzie w trybie Access protokół vtp nie będzie działał. Zatem zaczynamy konfigurację od ustawienia portów do pracy w trybie trunk:

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch0(config)#int fa 0/1
Switch0(config-if)#switchport mode dynamic desirable
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch0(config-if)#^Z
Switch0#sh interfaces trunk
Port          Mode          Encapsulation  Status      Native vlan
Fa0/1         auto          n-802.1q       trunking   1

Port          Vlans allowed on trunk
Fa0/1         1-1005

Port          Vlans allowed and active in management domain
Fa0/1         1

Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         none

Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#int fa 0/1
Switch1(config-if)#switchport mode dynamic desirable
Switch1(config-if)#int fa 0/2
Switch1(config-if)#switchport mode dynamic desirable
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
^Z
%SYS-5-CONFIG_I: Configured from console by console
Switch1#sh int 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         1-1005
Fa0/2         1-1005

Port          Vlans allowed and active in management domain
Fa0/1         1
Fa0/2         1

Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         none
Fa0/2         none
Switch1#

Switch2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#int fa 0/1
Switch2(config-if)#switchport mode dynamic desirable
```

Teraz definiujemy wersje protokołu vtp, który chcemy używać, nazwę domeny vtp oraz role, które będą pełniły poszczególne switchy. Wystarczy, że domenę vtp skonfigurujemy na jednym z urządzeń, a ponieważ domyślnie jest ono serwerem – roześle skonfigurowaną nazwę na całą sieć. Dobrym pomysłem jest też ustawienie hasła, które zabezpieczy nas przed próbą podłączenia nieautoryzowanych urządzeń do naszej sieci.

```
Switch0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch0(config)#vtp version 2
Switch0(config)#vtp mode server
Device mode already VTP SERVER.
Switch0(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
Switch0(config)#vtp password cisco
Setting device VLAN database password to cisco
Switch0(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Switch0#sh vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode        : Server
VTP Domain Name           : cisco
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Enabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0xFE 0x47 0xC1 0x5D 0x1E 0x2A 0x53 0x49
Configuration last modified by 0.0.0.0 at 3-1-93 00:38:11
Local updater ID is 0.0.0.0 (no valid interface found)
```

Zanim zmienimy konfiguracje na pozostałych switchach – sprawdzimy jaki status ma obecnie protokół vtp:

```
Switch1#sh vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode        : Server
VTP Domain Name           : cisco
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Enabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0xAA 0xB9 0x0C 0xCD 0xD7 0xE8 0xA6 0xE0
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#vtp password cisco
Setting device VLAN database password to cisco
Switch1(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch1(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Switch1#sh vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode        : Client
VTP Domain Name           : cisco
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Enabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0xFE 0x47 0xC1 0x5D 0x1E 0x2A 0x53 0x49
Configuration last modified by 0.0.0.0 at 3-1-93 00:38:11
```

Jak widać, nazwa domeny vtp oraz wersja protokołu zostały już automatycznie rozpropagowane na całą sieć przez pierwszy ze skonfigurowanych switchy. Pozostało nam ustawić hasło oraz zmienić tryb

pracy switcha. Te same zmiany wprowadzamy na switchu 2. Proszę zwrócić uwagę na jeszcze jeden ciekawy szczegół, chodzi mianowicie o fakt użycia do zestawienie połączeń trunk trybu „dynamic desirable”. Porty pracujące w tym trybie przejdą w tryb trunk jedynie wtedy, gdy na obu switchach spiętych ze sobą skonfigurowana zostanie ta sama domena VTP, w przeciwnym razie porty pozostaną w trybie Access. Od teraz jeśli będziemy chcieli dodać jakiś vlan do bazy danych vlanów na każdym switchu w sieci, wystarczy, że dodamy go na switchu skonfigurowanym jako serwer.

```
Switch0#sh vlan brief
```

VLAN Name	Status	Ports
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

```
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

```
Switch0#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch0(config)#vlan 111
```

```
Switch0(config-vlan)#name stojedenascie
```

```
Switch0(config-vlan)#vlan 112
```

```
Switch0(config-vlan)#name stodwanascie
```

```
Switch0(config-vlan)#^Z
```

```
Switch0#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
sh vlan brief
```

VLAN Name	Status	Ports
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

```
111 stojedenascie active
112 stodwanascie active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

```
Switch0#
```

Pamiętajmy, że na switchach skonfigurowanych jako klienci nie możemy dodawać, ani kasować vlanów. Możemy to robić tylko z poziomu serwera.

```
Switch2#sh vlan brief
```

VLAN Name	Status	Ports
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

```
111 stojedenascie active
112 stodwanascie active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

```
Switch2#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch2(config)#vlan 113
```

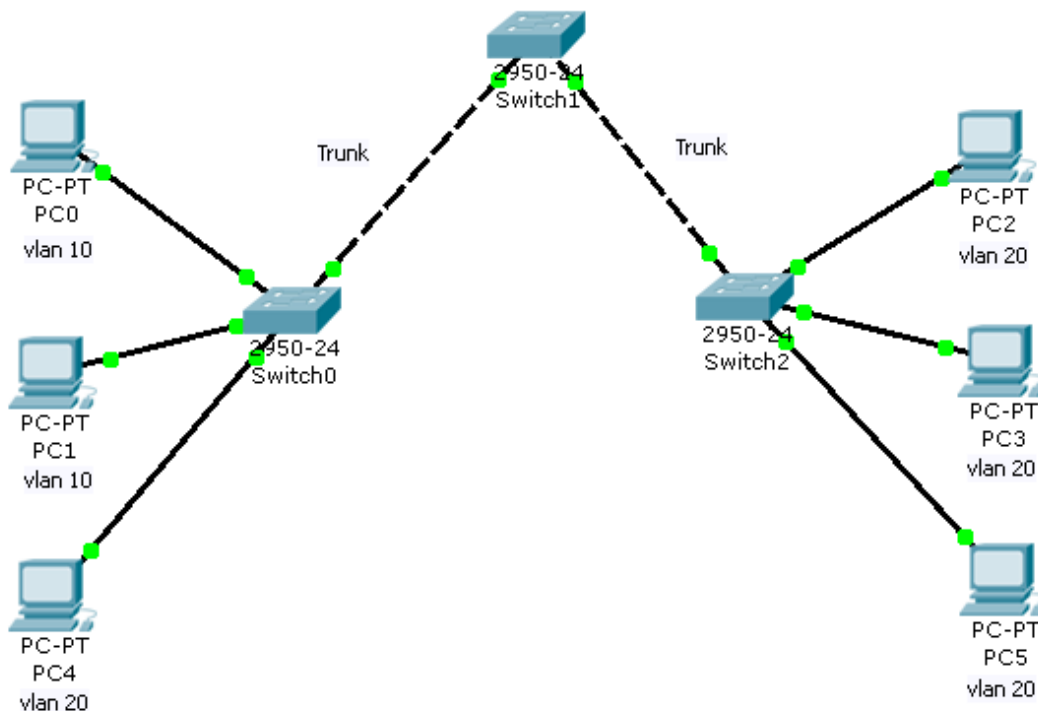
```
VTP VLAN configuration not allowed when device is in CLIENT mode.
```

```

Switch2(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Switch2#sh vtp status
VTP Version                : 2
Configuration Revision     : 4
Maximum VLANs supported locally : 255
Number of existing VLANs   : 7
VTP Operating Mode        : Client
VTP Domain Name           : cisco
VTP Pruning Mode          : Disabled
VTP V2 Mode                : Enabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0x91 0x22 0xC1 0xA7 0xCF 0x5D 0x79 0x05
Configuration last modified by 0.0.0.0 at 3-1-93 00:46:00

```

Bardzo ciekawą funkcjonalnością, którą oferuje nam protokół vtp jest funkcjonalność vtp pruning. Jest ona domyślnie wyłączona i aby z niej skorzystać należy ją świadomie włączyć. Funkcjonalność ta pozwala ograniczyć transmisję broadcastów tylko do części sieci, w której są one niezbędne. Rozpatrzmy poniższy przypadek:



Jeśli pojawi się ramka broadcast wygenerowana przez host PC0, to zostanie ona dostarczona do PC1, oraz zostanie przesłana przez port trunk pomiędzy Switch0 oraz Switch1 a następnie przez port trunk pomiędzy Switch1 a Switch2, pomimo tego, że ani na Switch1, ani na Switch2 nie ma żadnych hostów w vlanie 10. Jest to marnotrawienie dostępnego pasma. Funkcjonalność vtp pruning ma zapobiegać tego typu zjawiskom. Switche wymieniają między sobą informacje o tym, czy w danym vlanie znajdują się jacyś odbiorcy, do których należy przesyłać ruch broadcast, jeśli nie to ruch nie jest przesyłany. Innymi słowy, jeśli włączymy funkcjonalność vtp pruning, to ramka broadcast wygenerowana przez host PC0 dotrze tylko do PC1, natomiast na port trunk już nie zostanie wysłana.

```

S2#sh vtp status
VTP Version capable        : 1 to 3
VTP version running       : 3
VTP Domain Name           : ccie
VTP Pruning Mode          : Disabled
VTP Traps Generation      : Disabled
Device ID                  : 000a.b8df.7a00

```



```

S2(config)#vtp pruning
Pruning switched on
S2(config)#^Z
*Mar 1 02:09:52.832: %SYS-5-CONFIG_I: Configured from console by consoleat
S2#sh vtp status
VTP Version capable          : 1 to 3
VTP version running          : 3
VTP Domain Name              : ccie
VTP Pruning Mode             : Enabled
VTP Traps Generation         : Disabled
Device ID                    : 000a.b8df.7a00

Feature VLAN:
-----
VTP Operating Mode           : Server
Number of existing VLANs    : 7
Number of existing extended VLANs : 0
Configuration Revision      : 11
Primary ID                  : 000a.b8df.7a00
Primary Description         : S2
MD5 digest                  : 0x62 0x76 0x83 0x40 0xF7 0xE5 0x3E 0x28
                             0x0D 0xBF 0x99 0xB3 0x6A 0x75 0xF1 0x52

```

A na koniec krótki opis protokołu VTP w wersji 3. Różnice w stosunku do wersji 1 oraz 2 są dość spore. Przede wszystkim jest to protokół, który ma służyć do synchronizacji nie tylko bazy danych vlanów, ale też innych baz danych. Może służyć np. do synchronizacji bazy danych protokołu MST - IEEE802.1s (Multiple Spanning Tree), nie jest ograniczony tylko do jednego zadania. Oczywiście vtp v.3 pozwala korzystać ze wszystkich 4094 vlanów, pozwala również na zdefiniowanie tych samych funkcji switchy, co poprzednie wersje, to jest: serwer, klient oraz transparent, ale rola serwera nieco się zmieniła. Nadal baza danych vlanów jest przechowywana na serwerze w pamięci flash, nadal możemy mieć w sieci kilka serwerów, ale zmiany możemy wprowadzać tylko na jednym, wskazanym serwerze, tak zwanym „primary server”. Domyślnie żaden switch nie jest w tym trybie włączony, więc aby dodać nowy vlan – trzeba się przełączyć do tego trybu. Aby tego dokonać – musimy znać hasło ustawione dla protokołu vtp, bo zostaniemy o nie zapytani.

```

S2#sh vtp status
VTP Version capable          : 1 to 3
VTP version running          : 3
VTP Domain Name              : ccie
VTP Pruning Mode             : Enabled
VTP Traps Generation         : Disabled
Device ID                    : 000a.b8df.7a00

Feature VLAN:
-----
VTP Operating Mode           : Server
Number of existing VLANs    : 7
Number of existing extended VLANs : 0
Configuration Revision      : 11
Primary ID                  : 000a.b8df.7a00
Primary Description         : S2
MD5 digest                  : 0x62 0x76 0x83 0x40 0xF7 0xE5 0x3E 0x28
                             0x0D 0xBF 0x99 0xB3 0x6A 0x75 0xF1 0x52

Feature MST:
-----
VTP Operating Mode           : Off

Feature UNKNOWN:
-----
VTP Operating Mode           : Off

S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#vlan 112
VTP VLAN configuration not allowed when device is not the primary server for vlan 112
S2(config)#^Z
*Mar 1 02:21:44.529: %SYS-5-CONFIG_I: Configured from console by consolevtp
S2#vtp primary

```

```

This system is becoming primary server for feature vlan
Enter VTP Password:
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
*Mar  1 02:22:29.098: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: 000a.b8df.7a00
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 112
S2(config-vlan)#^Z
S2#
*Mar  1 02:22:53.735: %SYS-5-CONFIG_I: Configured from console by console

```

Takie podejście eliminuje problem z podłączeniem switcha z wyższym numerem rewizyjnym. Nawet, jeśli taki switch zostanie podłączony i nawet jeśli będzie ustawiony w tryb „primary”, to wszystkie urządzenia w domenie vtp będą słuchać tylko jednego serwera „primary” i będą pamiętały jego mac-address, więc taki switch nie będzie w stanie wyrządzić żadnej szkody.

```

S2#show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.

VTP Feature   Conf Revision Primary Server Device ID      Device Description
-----
VLAN          No      12      000a.b8df.7a00 001b.5477.6b80 S3
VLAN          No      12      000a.b8df.7a00 8843.e1a4.0d40 S1

```

Jeśli zdecydujemy się na przeniesienie „primary serwera” na inny switch, to bieżący „primary serwer” straci swój status, a nowy switch, który stanie się „primary serwerem” musi ogłosić swój mac-address w sieci. Pamiętajmy też o tym, że switch może stracić status „primary serwer” jeśli zajdzie jedna z poniższych sytuacji:

- switch zostanie zrestartowany,
- nastąpi przełączenie między kartami procesorowymi na switchu (w przypadku redundancji),
- inny switch przejmie rolę „primary serwera”,
- nastąpi jakakolwiek zmiana konfiguracji vtp (inna nazwa domeny, inne hasło, etc.)

Protokół vtp v.3 pojawił się stosunkowo niedawno, ale daje ogromne możliwości, które są naprawdę godne polecenia. Oczywiście niniejszy artykuł nie wyczerpuje tematu protokołu vtp, jego celem jest jedynie wskazanie wygodnego narzędzia, które ma usprawnić proces zarządzania siecią. Zainteresowane osoby odsyłam do dokumentacji na stronie Cisco ;-) i życzę udanej konfiguracji (uwaga na numer rewizyjny ;-P)

Kucharczyk Paweł