Switch Cisco Catalyst 2960-Plus

Ogólne

Switche przekierowują ruch do właściwego urządzenia biorąc pod uwagę jego adres MAC. Uzyskują go na podstawie ramki, którą otrzymują od urządzenia. Zapamiętują ten adres i kojarzą go ze swoim portem fizycznym, pod który podczepione jest urządzenie (to skojarzenie przetrzymują w swojej tablicy danych).

Switch Cisco

Porty z prawej strony (góra) to SFP (łącze optyczne). Porty z prawej strony (dół) są portami gigabitowymi i służą do połączenia z siecią zewnętrzną (WAN). Porty z lewej strony są portami FastEthernet (100Mb/s) przeznaczonymi do sieci LAN.

Testowanie urządzeń Cisco można przeprowadzić bez ich fizycznego posiadania. Taką możliwość daje program *PacketTracer*.

Pierwsza konfiguracja musi odbywać się przez port ethernetowy **CONSOLE** (z tyłu obudowy) za pomocą kabla szeregowego **RJ-45 --> RS-232** (w niektórych modelach może to być kabel **RS-232 --> RS-232**).

Domyślne IP: **10.0.0.1** (lub 10.0.0.3 jako zapasowy).

Domyślny użytkownik (konsola oraz www): *cisco* *(lub Switch, lub admin, lub puste pole).*

Domyślne hasło (konsola oraz www): *cisco* *(lub admin, lub puste pole).*

Przywrócenie ustawień fabrycznych: Należy przytrzymać klawisz MODE przez ok. 15 sekund (aż LEDs staną się pomarańczowe) i puścić, gdy zapali się SYST. Inny sposób (przez zwykły port ETH-LAN):

C:\> **telnet 10.0.0.1**

username: *cisco*

password: *cisco*

cisco# **erase startup-config**

lub

RSI-Channel> **en** *(wchodzimy w tryb administratora, czyli Enable Mode)*

RSI-Channel# **write erase**

RSI-Channel# **reload**

lub

Switch> **flash-init**

Switch> **dir flash:** *(przeglądamy pliki konfiguracyjne)*

Switch> **rename flash:config.text flash:config.old**

Switch> **boot**

Enable Password: Hasło dostępu do trybu EXEC (w wierszu poleceń) - prawa dostępu dla poszczególnych użytkowników.

Dostęp do CLI (*Command Line Interface*): za pomocą programu *PuTTY*, *telnet* (*Wiersz Poleceń*).

Polecenia CLI

Ustawienia wstępne

Uwaga: Znak zachęty w postaci ">" oznacza, że jesteśmy w trybie nieuprzywilejowanym, na tzw. koncie zwykłego użytkownika. Nazwa "*Switch*" jest *de facto* nazwą typu *hostname*, czyli nazwą tego konkretnego urządzenia (można tę nazwę zmienić).

Switch> **?** *(tryb pomocy; sprawdzamy, jakie mamy w ogóle dostępne polecenia)*

Switch> **show ?** *(pomoc na temat możliwych danych, które może zaprezentować system; wyjścia z tego trybu dokonujemy za pomocą Ctrl+C)*

Switch> **enable** *(lub też "**en**" przełączamy się w tryb administratora)*

Switch> **exit** *(wychodzimy z trybu administratora)*

Switch# **conf t** *(lub "**configure terminal**" - konfiguracja globalna)*

Switch (config)# *(teraz możemy zmieniać konfigurację globalną)*

Zaczynamy od konfiguracji haseł dostępu:

Switch (config)# **enable secret** *noweHasłoDoTrybuKonfiguracyjnego (o to hasło zostaniemy zapytani, gdy wydamy komendę "enable")*

Switch (config)# **line vty 0 15** *(wchodzimy do ustawień wirtualnych terminali [vty] o numerach 0-15, które służą między innymi do połączeń przez telnet i ssh)*

Switch (config-line)# **password** *noweHasłoDoTerminaliWirtualnych*

Switch (config-line)# **login** *(hasło będzie potrzebne do zalogowania się)*

Switch (config)# **line console 0** *(przechodzimy do ustawień portu CONSOLE)*

Switch (config-line)# **password** *noweHasłoDoPortuCONSOLE (zmieniamy lub ustanawiamy hasło do portu konsolowego; jest to hasło do konta zwykłego użytkownika; zostaniemy o nie zapytani już na samym początku przy próbie wejścia do trybu konsoli)*

Switch (config-line)# **login** *(hasło będzie potrzebne do logowania)*

Odzyskiwanie hasła

1. Będąc połączonym przez PuTTY ze switchem, wyłącz switch z prądu (tzw. *power cycle*).

2. Wciśnij przycisk MODE znajdujący się na obudowie i włącz zasilanie. Trzymaj go wciśnięty przez około 5 sekund aż zacznie migać dioda SYST na kolor zielony/pomarańczowy. Na ekranie powinny pojawić się informacje o bootowaniu systemu.

3. Wpisz komendy:

switch: **flash_init**

switch: **load_helper**

switch: **dir flash:** *(na wykazie plików powinien pojawić się "config.text", który jest de facto plikiem "start-up config")*

switch: **rename flash:/config.text flash:/config.old** *(zmieniamy jego nazwę)*

switch: **reset**

Uwaga: Podczas ponownego uruchamiania, system nie znajduje w pamięci FLASH pliku startowego (start-up configuration), więc uruchamia "System Configuration Dialog" (należy tę sekcję pominąć odpowiadając "n" na wszystkie pytania).

Switch> **enable**

Switch# **dir flash:** *(upewniamy się, że na wykazie widnieje nasz plik "config.old")*

Uwaga: Mamy w tym momencie dwie możliwości: albo przywracamy starą (pierwotną) konfigurację poprzez zmianę nazwy pliku z "*config.old*" na "*config.text*", albo tworzymy świeżą konfigurację poprzez wydanie polecenia:

Switch# **copy run start-up** *(tworzy plik "config.text")*

lub

Switch# **rename flash:/config.old flash:/config.text**
Switch# **dir flash:** *(upewniamy się, że plik "config.text" jest na dysku)*
Switch# **copy config.text run** *(przywracamy ustawienia do RAM-u)*
Switch# **show run** *(upewniamy się, że teraz jest wszystko w porządku)*
Switch# **conf t**
Switch (config)# **enable secret noweHasło** *(opcjonalnie)*
Switch (config)# **end**
Switch# **copy run start** *(zapisujemy całość do pliku startowego)*

Uwaga: W trybie konfiguracji szczegółowej można ustawić oddzielne hasło dostępu na każdym porcie fizycznym:
Switch (config)# **line vty 0 4**
Switch (config-line)# **password** *twojeHasło*
lub
Switch (config)# **line aux 0**
Switch (config-line)# **password** *twojeHasło*
lub
Switch (config)# **line con 0**
Switch (config-line)# **password** *twojeHasło*

Uwaga: Należy pamiętać, że hasła utworzone za pomocą komendy "password" można złamać (szukaj w Internecie: "Cisco password cracker online").

Zabezpieczenie fizycznych portów

Switch (config)# **interface fastEthernet 0/1** *(będziemy konfigurować port fizyczny nr 1)*
Switch (config-if)# **switchport mode access** *(zmieniamy tryb pracy portu nr 1)*
Switch (config-if)# **switchport port-security** *(zmieniamy zabezpieczenia portu nr 1)*
Switch (config-if)# **switchport port-security mac-address sticky** *(uaktywniamy filtrację MAC: tylko obecny MAC urządzenia podpiętego do portu nr 1 będzie przez port obsługiwany; inne MACi zostaną zignorowane)*
Switch (config-if)# **switchport port-security maximum 1** *(tylko ten jeden adres MAC może być przypisany do tego portu)*
Switch (config-if)# **shutdown** *(można także całkowicie wyłączyć port nr 1; służy to także do restartu portu z nowymi ustawieniami)*
Switch (config-if)# **no shutdown** *(można go także ponownie włączyć)*

Inne wybrane polecenia admina:
Switch# **copy running-config startup-config** *(zapis bieżącej konfiguracji, tj. skopiowanie bieżącej konfiguracji do pliku startowego)*
Switch# **show mac-address-table** *(pokazuje MACi podpiętych urządzeń i porty, do których są podpięte)*
Switch> **show interface fastethernet 0/5** *(pokazuje parametry portu nr 5)*
Switch (config)# **hostname** *nowaNazwaUrządzenia (zmiana nazwy switcha)*
Switch (config-if)# **ip dhcp snooping trust** *(tylko na tym fizycznym porcie [wcześniej trzeba określić na jakim] może działać serwer DHCP [jego MAC]; ten serwer staje się zaufanym; zapobiega to podszyciu się pod ten serwer innego obcego serwera DHCP)*
Switch (config)# **interface range fastEthernet 0/1 - 16** *(zakres konfigurowanych portów będzie obejmował porty 1-16)*
Switch (config-if-range)# **ip dhcp snooping limit rate 10** *(każdy z klientów podpiętych do konkretnych portów może poprosić serwer DHCP tylko 10 razy o przyznanie adresu IP za jednym razem)*

Switch (config-if-range)# **show ip dhcp snooping** *(pokazuje porty, które mają ustawiony limit żądań przydziału DHCP w jednej serii)*

Switch# **show vtp status** *(pokazuje status mechanizmu VTP oraz informację, czy dany switch pracuje w trybie serwera VTP czy w trybie klienta)*

Switch# **vtp domain 3bird** *(tworzymy domenę VTP, która będzie scalać serwer VTP z klientami VTP)*

Switch# **vtp password** *hasłoDlaDomenyVTP*

Switch# **vtp mode client** *(na innym switchu ustawiamy tryb klienta)*

Switch# **vtp domain 3bird** *(podłączamy do istniejącej domeny VTP)*

Switch# **vtp password** *hasłoDlaDomenyVTP (na innym switchu ustawiamy tryb klienta)*

Aby klient mógł się komunikować z serwerem, port do serwera musi być typu TRUNK:

Switch# **conf t**

Switch (config)# **interface gigabitEthernet 0/1**

Switch (config)# **switchport mode trunk**

Switch (config)# **end**

Uwaga: Na switchu, który jest klientem VTP, nie można tworzyć sieci VLAN. On służy do pobierania definicji z serwera VTP.

VLAN-y

Wszystkie komputery podpięte do switcha mogą mieć jedną grupę IP, np. 192.168.0.1-24... ale nie będą mogły się ze sobą komunikować, jeśli będą w różnych VLAN-ach. Aby utworzyć sieć VLAN, switch musi obsługiwać standard 802.1Q.

Zastrzeżone (predefiniowane) numery VLAN to: 1 (wszystkie porty), 1002 (fddi), 1003 (token-ring), 1004, 1005.

- **TRUNK (TAG VLAN)** - port fizyczny, który może transportować pakiety z różnych VLAN-ów (gdyby nie był otagowany, mógłby transportować dane tylko jednego VLAN-a). Użyteczne w sytuacji, gdy jeden przełącznik zarządzalny posiadający VLAN-y, podpinamy pod drugi przełącznik zarządzalny posiadający także VLAN-y (czyli łączymy ze sobą dwa przełączniki poprzez gigabitowe porty LAN). Ramki przepływające przez te porty mają dodatkowe dwa znaczniki (są tagowane), tj. **TPID** (*Tag Protocol Identifier*, o stałej wartości 0x8100, które mówią, że ramka jest w standardzie 802.1Q) oraz **TCI** (*Tag Control Information* - zawiera numer sieci VLAN, priorytet ramki, standard sieci, np. 0 oznacza sieć *ethernet*). Tagi te mówią nam, że ramka opuszczając przełącznik została przez niego zmodyfikowana i oznaczona tymi tagami (opakowana dodatkowo do tych tagów). Na podstawie tego tagu, drugi switch (który otrzyma taką ramkę), będzie wiedział do jakiej sieci ją przekierować. Przed wysyłką pozbawia ją jednak ten ramki, gdyż nie będzie ona już potrzebna.
- **UNTAGED** - gdy VLAN-y utworzone są na jednym fizycznym przełączniku. Ramki nie potrzebują wtedy dodatkowych znaczników (tagów).
- **VTP** (*VLAN Trunking Protocol*) - serwer zainstalowany na jednym ze switchy (pozostałe są klientami VTP), który automatycznie rozsyła informacje o istniejących VLAN-ach, ich numerach i nazwach (protokół VTP). Nie rozsyła jednak informacji o przypisanych do VLAN-u portów (te trzeba ręcznie dodać na kliencie). Używany w dużych sieciach z dużą ilością switchy. W małych sieciach - niezalecany. Same VLAN-y można tworzyć tylko na serwerze, nie jest w takiej sytuacji możliwe tworzenie VLAN-ów na klientach.

VLAN - tryb graficzny

Identyfikator Data VLAN: np. **10** *(przesyłanie danych)*

Identyfikator Voice VLAN: np. **20** *(opuszczamy to pole, gdy nie chcemy wykorzystywać sieci do przesyłania głosu)*

Domyślne IP: **10.0.0.1**.

Nowe IP: np. **192.168.10.1** *(jest to IP pod którym będzie dostępny panel administratora po skończonej konfiguracji)*

Access Port: wybrać porty tworzące sieć VLAN (opuszczamy to pole, jeśli nie chcemy tworzyć sieci VLAN).

Konfiguracja VLAN rozpoczyna się w kreatorze "*Express Setup*", znajduje się także w sekcji "*Management interface*" / "*Network Assistant*".

VLAN w CLI

Switch> **enable** *(lub "en"; przełączamy się w tryb administratora: **En**able Mode)*

Switch# **show flash** *(czy istnieje plik "vlan.dat" z konfiguracją VLAN?)*

Switch# **conf t** *(lub "configure terminal" lub "config terminal"; konfiguracja globalna)*

Switch (config)# **vlan 10** *(tworzymy VLAN o numerze 10)*

Switch (config-vlan)# **name sekretariat** *(nadajemy mu nazwę "Sekretariat")*

Switch (config-vlan)# **vlan 20** *(tworzymy drugi VLAN o numerze 20)*

Switch (config-vlan)# **name marketing** *(nadajemy mu nazwę "Marketing")*

Switch (config-vlan)# **end**

Switch# **show vlan** *(sprawdzamy, czy vlan-y zostały utworzone)*

Teraz musimy dodać poszczególne porty do tych vlan-ów:

Switch# **conf t** *(konfiguracja globalna)*

Switch (config)# **interface range fastEthernet 0/1-3**

Switch (config-if-range)# **switchport access vlan** *[id]* *(przypisujemy porty 1-3 do konkretnego VLAN; jako ID podać numer VLAN, np. 10)*

Możemy także połączyć ze sobą dwa switche. Musimy wtedy na obu utworzyć VLAN-y o tej samej nazwie i identyfikatorze. Dane, które będą przechodzić między tymi dwoma switchami, muszą być jednak otagowane. Aby otagować ramki w przypadku połączenia dwóch switchy (najlepiej przez port gigabitowy, choć nie jest to konieczność):

Switch (config)# **interface gigabitEthernet 0/1** *(będziemy ustawiać właściwości portu GE nr 1)*

Switch (config-if)# **switchport mode trunk** *(port ten definiujemy jako trunk)*

Switch (config-if)# **switchport trunk allowed vlan 10,20** *(pozwalamy temu portowi typu TRUNK transportować ramki z VLAN nr 10 oraz VLAN nr 10)*

Switch (config-if)# **end** *(wychodzimy z trybu konfiguracji interfejsów)*

Switch# **show interfaces trunk** *(pokaż zdefiniowane porty typu TRUNK)*

Ostatnia aktualizacja: 23 grudnia 2018.