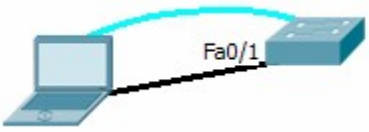
SIECI KOMPUTEROWE – LABORATORIUM 022

Tematyka:

Konfigurowanie przełączników nie rutujących Cisco Catalyst segmentu EDGE: konfigurowanie usług przełączników, Spanning Tree Protocol, EtherChannel

Zadanie A: Konfigurowanie kanałów komunikacyjnych do przełącznika Cisco Catalyst

1. Połącz stację PC z przełącznikiem Ethernet Cisco Catalyst (modele 2950, 2960, 3550, 3560, 3750) przy użyciu kabla TP (*Twisted Pair*) (wykorzystując wybrane gniazda Ethernet). Zamontuj kabel konsoli pomiędzy tymi urządzeniami.



Po nawiązaniu połączenia konsoli pomiędzy przełącznikiem i stacją PC zaktywuj tryb uprzywilejowany (*exec*) CLI przełącznika - komendą *enable* (skrót: *en*). Poprawne przejście do tego trybu zasygnalizuje symbol '*#*'.
Następnie przejdź do trybu konfiguracji przełącznika z wykorzystaniem terminala:
Switch#configure terminal
Switch(config)#
Po przejściu należy skonfigurować adres IP interfejsu VLAN1 przełącznika oraz włączyć (zaktywować) ten interfejs. Przed skonfigurowaniem adresu - sprawdzić (*ping*), czy nie jest on zajęty przez inne urządzenie znajdujące się w lokalnym segmencie sieci IP.
Switch(config)#interface vlan1
Switch (config-if)#ip address 192.168.123.199 255.255.255.0
Switch (config-if)#no shutdown
Adresacja IP dla wszystkich używanych interfejsów musi zostać opracowana samodzielnie i spełniać ogólnie znane reguły (nie należy kopiować dosłownie powyższego przykładu).
Aktywując VLAN sprawdź ustawienia i stan interfejsów IP przełącznika:
Switch#show ip interface brief
Switch#show ip interface vlan 1
lub z trybu konfiguracji:
Switch(config)#do show ip interface brief
Switch(config)#do show ip interface vlan 1
Należy zwrócić uwagę na stan aktywności danych interfejsów (*up/down/administratively down*).

2. Konfigurowanie linii terminali wirtualnych i uruchomienie serwera telnet:
   Oprócz konsoli przełączniki Cisco Catalyst umożliwiają dostęp zdalny (przeznaczony do ich konfigurowania) poprzez terminale wirtualne VTY (jest ich najczęściej 16). Gdy użytkownik zdalny nawiązuje połączenie z przełącznikiem (np. poprzez usługę *telnet*) - przełącznik alokuje dla niego jedną linii VTY. Aby konfiguracja przełącznika pozwoliła na takie połączenie - należy określić ją następującymi komendami:
   Switch(config)#line vty 0 15
   Switch(config-line)#password sieci
   Switch(config-line)#login
   Switch(config-line)#transport input telnet
   Gdzie kolejne wpisy to:
   - Aktywowanie trybu konfiguracji linii (zakres 0-15)
   - Ustanowienie lokalnego hasła
   - Ustanowienie nakazu używania lokalnego hasła przy logowaniu
   - Zezwolenie na ruch *telnet* z wykorzystaniem wybranych linii

   Uwaga: Komenda login będzie blokowana gdy w przełączniku włączono tryb autoryzacji typu new-model (zintegrowany). Należy sprawdzić istnienie wpisu aktywującego ten tryb w konfiguracji przełącznika i ewentualnie usunąć go:
   Switch#show run
   …
   aaa new-model
   …
   Switch(config)#no aaa new-model
   Należy sprawdzić możliwość nawiązania zdalnej sesji telnet z komputera PC do przełącznika. Adres serwera telnet to adres IP interfejsu VLAN1 w przełączniku. Port TCP dla usługi telnet ma wartość standardową: 23.

3. Aby możliwe było przejście w tryb uprzywilejowany CLI (*exec*) używając klienta telnet lub SSH (czyli w połączeniu zdalnym) konieczne jest zdefiniowanie w przełączniku hasła egzekwowanego standardowo przy takim przejściu (przejście bez podawania hasła dozwolone jest tylko dla lokalnych połączeń konsoli):
   Switch(config)#enable password sieci
   Hasło zdejmujemy komendą:
   Switch(config)#no enable password
   Sprawdź otrzymaną konfigurację:
   Switch#show running-config
   i ponownie nawiąż połączenie poprzez telnet - przechodząc następnie do trybu *exec*.

4. Uruchomienie serwera SSH:
   Określ nazwę domeny internetowej dla przełącznika:
   Switch(config)#ip domain-name domena
   Zmień wartość *hostname* dla przełącznika na inną niż domyślna:
   Switch(config)#hostname Mojhost
   Mojhost#
   Zmiana nazwy hosta nie dotyczy jedynie treści karetki. *Hostname* jako nazwa urządzenia jest propagowana przez sieć, między innymi w protokole CDP (*Cisco Discovery Protocol*)

Wygeneruj klucz RSA i następnie podaj wielkość klucza (360-2048 bitów).
Uwaga: Klient SSH „*Putty*” wymaga klucza o długości 512 bitów:
Switch(config)#crypto key generate rsa
Sprawdź ustawienia:
Switch#show ip ssh
Przełącz tryb autoryzacji użytkowników z opcji "serwera AAA radius" (co jest domyślne) na wykorzystanie lokalne systemu kont:
Switch(config)#aaa new-model
Uwaga: powyższa komenda uniemożliwia użycie komendy:
Switch(config-line)#login
(niemożliwa jest już autoryzacja przy pomocy hasła przypisanego do linii)
Zdefiniuj w przełączniku przynajmniej jednego użytkownika z *loginname* i *hasłem*:
Switch(config)#username sieci priv 15 password 0 sieci
gdzie kod 0 oznacza hasło zadane jawnie tekstem (wartość 7 oznaczałaby hasło szyfrowane), zaś 15 to wartość priorytetu przypisanego temu użytkownikowi (najwyższy).
Dla wybranych linii zablokuj możliwość logowania poprzez nie szyfrowany telnet:
Switch(config)#line vty 0 15
Switch(config-line)#transport input none
lub (w niektórych wersjach CatOS):
Switch(config-line)#no transport input telnet
Aktywuj użytkowanie SSH w liniach:
Switch(config)#line vty 0 15
Switch(config-line)#transport input ssh
Połącz się z przełącznikiem z użyciem dowolnego klienta SSH (np. programu Putty na stacji PC) sprawdzając poprawność funkcjonowania tej usługi (port TCP usługi SSH ma wartość domyślną 22).

5. Ograniczanie dostępu poprzez linie:
   Przetestuj możliwość ograniczenia dostępu - jedynie do określonych adresów IP – tworząc regułę filtrującą ACL (*Access Control List*) o wybranym numerze (w przykładzie poniżej jest to 55):
   Switch(config)#access-list 55 permit 192.168.1.0 0.0.0.255
   Następnie zastosuj tą regułę do logowania przez wybrane linie:
   Switch(config)#line vty 0 15
   Switch(config-line)#access-class 55 in
   Switch(config-line)#exit
   Uwaga: przy definiowaniu użytej w powyższym przykładzie reguły filtrującej ACL wartość maski adresu IP zapisujemy w inwersji bitowej (np. jak powyżej: 0.0.0.255 odpowiada masce 255.255.255.0).
   Połącz się ponownie z przełącznikiem z użyciem klienta SSH i zweryfikuj funkcjonowanie ograniczeń w dostępie do linii.

Zadanie B: Spanning Tree Protocol

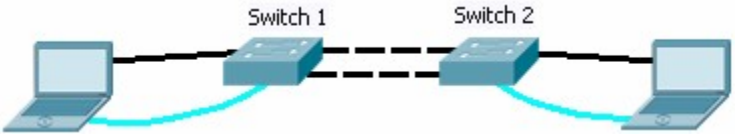
1. Procesy automatycznego eliminowania pętli w segmencie sieci opartym o Ethernet są prowadzone w większości zaawansowanych przełączników Ethernet. Odpowiada za nie *Spanning Tree Protocol*. Definiuje on jeden przełącznik

wyróżniony (tzw. *root bridge*). Każdy z przełączników nie posiadający statusu poszukuje możliwych połączeń z *root bridge* nanosząc je w strukturze drzewa (*Spanning tree*). Deaktywuje jednocześnie wszelkie (najczęściej gorsze) połączenia redundantne – eliminując tym samym pętle w sieci.

2. Przygotuj do pracy drugi przełącznik Ethernet Cisco Catalyst i połącz go kablem Ethernet z poprzednim oraz kablem konsoli z drugim PC.

Aby sprawdzić stan *Spanning tree* budowanego przez przełączniki (w tym także status *root bridge* przełącznika, wartości BID BPDU /*Bridge Protocol Data Unit*/ dla portów itp.) należy posłużyć się komendą:
Switch#show spanning-tree
Switch#show spanning-tree detail
Switch#show spanning-tree vlan 1-10
Po sprawdzeniu należy zidentyfikować (w obydwu przełącznikach):
- status *root bridge,*
- *Root ID* (określa dane *root bridge* - może dotyczyć bieżącego przełącznika lub innego, który ma status *root bridge*)
- *Bridge ID* (określa dane bieżącego przełącznika)
- *Root port*
- *Designated ports*

Następnie należy dodać drugie połączenie pomiędzy przełącznikami (tworząc niedozwoloną w tej topologii pętlę fizyczną).



Po odczekaniu, aż nastąpi przebudowa *Spanning tree* ponownie należy sprawdzić w obydwu przełącznikach stan *Spanning tree*, identyfikując:
- *root bridge*
- *Root Port*
- *Designated ports*
- *Alternative ports (czy powstały?)*

3. Po ustaleniu połączenia pomiędzy przełącznikami wybranego przez STP jako aktywne należy je wyłączyć, np.:
Switch(config)#interface fa 0/5
Switch(config-if)#shutdown
i znów przeanalizować sytuację.
Ponowne uruchomienie aktywności portu:
Switch(config-if)#no shutdown
Należy uruchomić diagnostykę przebudowy drzewa *Spanning tree*:
Switch#debug spanning-tree events
następnie ponownie usunąć oraz dodać łącze.
Zatrzymanie diagnostyki:
Switch#no *debug spanning-tree events*

4. Wyłączenie akceptowania ramek PBDU: Funkcja ta jest przeznaczona do blokowania możliwości ingerowania ze strony *End-stations* spreparowanymi ramkami PBDU w *Spanning Tree* przełącznika. Nie należy jej używać wobec portów podłączonych do innych przełączników:
   Switch(config-if)#spanning-tree bpduguard disable

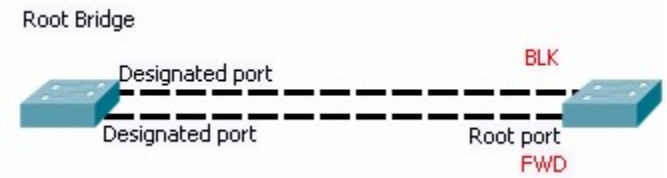
5. W przełącznikach Cisco protokół STP funkcjonuje domyślnie w trybie *per-VLAN* (istnieje wtedy osobne *Spanning tree* dla każdego izolowanego VLAN). Nawet gdy VLAN nie zostały skonfigurowane, zawsze istnieje VLAN 1, którego mogą dotyczyć czynności konfiguracyjne STP. Zatem w samych opcjach konfigurowania VLAN także będą zlokalizowane dalsze komendy STP.
   Aby przenieść status STP *root bridge* dla wybranego VLAN do własnego przełącznika należy użyć komendy:
   Switch(config)#spanning-tree vlan 1 root primary
   Komenda ta powoduje takie manipulowanie wartością *priority*, aby doszło do przeniesienia *root bridge* do bieżącego przełącznika. Inny wariant komendy:
   Switch(config)#spanning-tree vlan 1 root secondary
   określa *priority* jako wartość „drugą najlepszą" – powodując przejęcie funkcji *root bridge* gdy obecny *root bridge* ulegnie awarii.
   Należy przenieść status STP *root bridge* do przeciwległego niż obecnie przełącznika ponownie sprawdzić stan STP w przełącznikach.
   Należy sprawdzić stan STP:
   Switch#show spanning-tree
   Switch#show spanning-tree summary
   Switch#show spanning-tree vlan 1 detail
   Switch#show spanning-tree int fa 0/1 detail

6. Inną metodą wpływania na kształt *Spanning tree* jest bezpośrednie manipulowanie priorytetem przełącznika (jako mostka). Jak wiadomo - przełącznik sam definiuje priorytet *BID* (*Bridge ID*) BPDU - można jednak określić wartość czterech najstarszych bitów BID:
   Switch(config)#spanning-tree vlan 1 priority 16384
   Domyślna wartość priorytetu to 32768. W praktyce poprzednie komendy zawierające frazy *root primary* i *root secondary* obniżały wartość *priority* przełącznika do odpowiednio 32768-4096 oraz 32768-4096-4096 gdy wszystkie inne przełączniki były skonfigurowane domyślnie (możliwe do przypisania wartości są wielokrotnością liczby 4096).
   Korygując priorytety przełączników (niższy ma pierwszeństwo) należy spowodować powrót statusu *root bridge* do pierwotnego przełącznika.

   Możliwe jest zablokowanie utraty statusu *root bridge* przez przełącznik poprzez wybrane łącze (więc komenda dotyczy konfiguracji portu, przez który prowadzony jest ruch):
   Switch(config-if)#spanning-tree guard root
   Zablokuj port powyższą komendą, następnie dokonaj próby przejęcia statusu *root bridge (jak poprzednio)* przez przeciwległy przełącznik. Sprawdź czy doszło do kolizji *root bridge* pomiędzy przełącznikami (*root inconsistency*) i czy w

konsekwencji wykrycia tej kolizji port skonfigurowany z opcją *guard root* został przez przełącznik zablokowany i wykluczony z STP (broken - BKN):
Switch#show spanning-tree vlan 1
Switch#show log
Uwaga: W obecnej konfiguracji sama próba przejęcia statusu *root bridge* nadal się powiedzie, ponieważ w instalacji pozostaje drugie połączenie pomiędzy przełącznikami, które nie zostało zablokowane. Zostanie ono uruchomione po zablokowaniu

7. Manipulowanie wartością *port priority*
   Aby wpłynąć na wybór jednego z wielu alternatywnych połączeń pomiędzy dwoma przełącznikami (obecnie mamy dwa) - konieczne jest manipulowanie priorytetami portów lub kosztem łącza. Domyślna wartość priorytetu portu to 128 przy granulacji 16.



   Wartość ta jest przesyłana przez ramki BPDU do drugiego przełącznika, który będzie szukał najlepszej ścieżki do *root bridge* i podejmie decyzje o wyborze łącza na podstawie tego priorytetu. Zatem aby to wykazać, należy konfigurować priorytet portu w *root bridge*, aby *root bridge* wysłał informację o priorytecie do drugiego przełącznika, który wybierze dopiero drogę:
   Switch(config)#int fa 0/1
   Switch(config-if)#spanning-tree port-priority 64
   lub jedynie dla konkretnego VLAN (i portu):
   Switch(config)#int fa 0/1
   Switch(config-if)#spanning-tree vlan 1port-priority 64
   gdzie pierwszeństwo ma ustawienie wartości dla VLAN (dzięki temu port może mieć różne priorytety - w zależności od użytkowanego VLAN).
   Przy pomocy powyższej komendy przenieś aktywność na drugie z istniejących łącz. Sprawdź skutek działania w obydwu przełącznikach:
   Switch(config)#show spanning-tree
   Uwaga: Pole *priority* w liście portów STP zawiera wartość wysyłaną, a nie odebraną (więc zmieni się tylko w przypadku *root bridge*). Aby w drugim przełączniku sprawdzić wartość priorytetu, należy posłużyć się komendą np.:
   Switch(config)#show spanning-tree vlan 1 detail
   i odszukać informację na temat *designated port* w kierunku *root bridge*

8. Manipulowanie wartością *cost*
   Omawiany w poprzednim punkcie parametr *port priority* ma znaczenie tylko w sytuacji, gdy dla danej instancji STP obliczone sumaryczne wartości kosztu alternatywnych tras do *root bridge* są takie same. Wartość kosztu zależy od prędkości łącza. W domyślnym 16-bitowym wariancie wynosi: 10Mbps = 100, 100Mbps = 19, 1Gbps = 4, 10Gbps = 2. Możemy manipulować wartością *cost* dla odcinka bezpośrednio podłączonego do danego przełącznika - rezygnując lokalnie z powyższego porządku
   Switch(config)#int fa 0/1
   Switch(config-if)#spanning-tree cost 13

lub jedynie dla konkretnego VLAN (i portu):
Switch(config)#int fa 0/1
Switch(config-if)#spanning-tree vlan 1cost 13
gdzie ponownie pierwszeństwo ma ustawienie wartości dla VLAN.
Przy pomocy tej komendy przenieś aktywność na drugie z istniejących łącz – obniżając jego koszt. Sprawdź skutek działania w obydwu przełącznikach:
Switch(config)#show spanning-tree

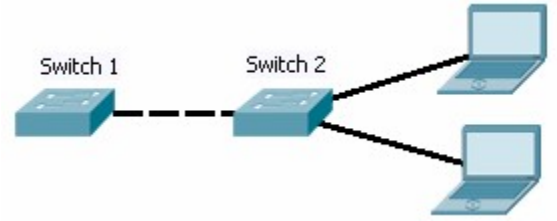
9. Wersje STP.
   Przełączenie aktywnej wersjiRapid protokołu STP jest możliwe (konsekwentnie w obydwu przełącznikach) za pośrednictwem komendy:
   Switch(config)# spanning-tree mode pvst
   lub
   Switch(config)# spanning-tree mode rapid-pvst
   gdzie pvst to per-VLAN spanning tree.
   Sprawdzenie aktywnej wersji (w raporcie zobaczymy wpis o treści "*ieee compatible STP*" lub "*rstp compatible STP*"):
   Switch#sh spanning-tree detail

10. Aby wyłączyć całkowicie funkcjonowanie STP dla przełącznika należy użyć komendy:
    Switch(config)#spanning-tree portfast default
    Aby wyłączyć STP jedynie dla fizycznego portu przełącznika:
    Switch(config-if)#spanning-tree portfast

    UWAGA!!: Zbudowanie pętli z użyciem portów przełącznika nie realizujących STP może spowodować zapętlenie przekazywania tej samej ramki Ethernet i zablokowanie sieci.

Zadanie C: Zarządzanie adresami MAC i filtrowanie ramek Ethernet na podstawie tych adresów.

1. Do niniejszych doświadczeń należy zbudować instalację analogiczną do przedstawionej na rysunku:



W przełącznikach Layer 2 (nie rutujących) nie jest możliwe przypisanie reguły ACL do interfejsu Ethernet. Można jednak zdefiniować globalną tablicę adresów MAC i reguły postępowania po natrafieniu na te adresy w ramkach Ethernet np.:
Switch(config)#mac address-table static 0013.72b9.89fe vlan 1 drop
lub (zależnie od wersji IOS):
Switch(config)#mac-address-table static 0013.72b9.89fe vlan 1 drop
gdzie 1 to identyfikator VLAN (w przykładzie wartość domyślnego VID, czyli 1)

Zablokuj w przełączniku **Switch 2** przy użyciu powyższej komendy wybraną stację PC. Sprawdź funkcjonowanie tego ograniczenia, następnie przywróć ruch.

Propagacja wiedzy na temat adresów MAC stacji podłączonych do danego segmentu sieci musi następować także pomiędzy przełącznikami. W powyższym przykładzie **Switch 1** musi pozyskać wiedzę na temat adresów stacji PC od przełącznika **Switch 2**. Sprawdź zawartość tablicy MAC przełącznika **Switch 1**, porównując adresy MAC z adresami stacji PC. Należy posłużyć się tu komendą:
Switch1#show mac address-table
lub (zależnie od wersji IOS):
Switch1#show mac-address-table
Aby sprawdzić listę adresów MAC, do których droga prowadzi przez konkretny interfejs należy użyć przykładowo komendy:
Switch1#show mac-address-table interface fa 0/1
Ile adresów MAC znalazło się w tablicy przełącznika **Switch 1**?
UWAGA: Adresy MAC zostaną rozpropagowane dopiero po przeprowadzeniu sesji ARP pomiędzy stacjami PC. Sesję można przyspieszyć (np. poprzez użycie komendy ping ze stacji)

Możliwe jest definiowanie własnych (dowolnych) MAC dla interfejsów przełącznika (przypisanych do VLAN). Zdefiniowanie statycznego adresu MAC dla wybranego portu i VLAN1 (czyli do interfejsu konfiguracyjnego przełącznika):
Switch2(config)#mac-address-table static 1111.2222.3333 vlan 1 int fa0/5

Zadanie D: Agregowanie portów - EtherChannel

1. Zadanie polega na zagregowaniu (połączeniu w całość) kilku portów przełącznika - tworząc z nich w jedno łącze logiczne. Takie łącze, poprowadzone pomiędzy przełącznikami, umożliwi zwielokrotnienie dostępnej przepustowości. Aby zestawić *EtherChannel* należy stworzyć jego konfigurację w obydwu przełącznikach. Konfiguracja *EtherChannel* w tych przełącznikach musi angażować w logicznym łączu taką samą liczbę portów Ethernet. W zadaniu wykorzystaj instalację z zadania poprzedniego – tworząc jednak kilka fizycznych łącz pomiędzy przełącznikami (będą teraz pełniły rolę składowych *EtherChannel*).

2. W obydwu przełącznikach zdefiniuj nowy interfejs typu *Port-Channel*, obrazujący logiczną agregację portów Ethernet:
Switch(config)#interface Port-channel 1
Sprawdź konfigurację:
Switch #show ip int brief
UWAGA: Aby możliwe było zestawienie *EtherChannel* cecha *port mode* dla wszystkich zaangażowanych portów (w obydwu przełącznikach), oraz dla interfejsu *Port-channel*, do którego porty są przypisane musi mieć identyczną wartość (np. *access*):
Switch(config-if)#switchport mode access

3. Zanim przystąpisz do przypisywania portów przełącznika do *EtherChannel* - odłącz je tymczasowo od przeciwległego przełącznika. Gdy skonfigurowana zostanie tylko jedna strona *Etherchannel* (druga jeszcze nie jest skonfigurowana), a łącze funkcjonuje – przełączniki wykryją niespójność konfiguracji i trwale wyłączą porty (*err-disabled*).
4. Przypisz wybrane porty Ethernet przełącznika do tzw. *channel-group* i zdefiniuj spójny dla nich tryb pracy (*port mode*), np.:
   *Switch(config)#*interface range FastEthernet 0/1 - 2
   Switch(config-if)#switchport mode access
   Switch(config-if)#channel-group 1 mode on
   przy czym *channel group* musi być identyfikowana numerem (w przykładzie jest to 1) takim samym jak zdefiniowany wcześniej interfejs *Port-Channel* (zbieżność tej wartości stanowi sprzęg pomiędzy grupą portów a interfejsem). Po skonfigurowaniu przypisań portów – połącz z powrotem kablami przełączniki obserwując proces zestawiania *EtherChannel*.

5. Sprawdź konfigurację analizując status portów w *EtherChannel* (*D-down, P-port-channel, d-default*):
   Switch#show etherchannel summary
   W stacji PC podłączonej do przełącznika uruchom program ping w trybie ciągłym (sprawdzając łączność z dowolnym interfejsem IP po przeciwległej stronie *EtherChannel*). Następnie rozłącz jeden z kabli pomiędzy portami i ponownie sprawdź status *EtherChannel*. Czy wystąpiły przerwy w przełączaniu ramek? Podłącz ponownie kabel. Zauważ, że po podłączeniu nie przebiega już procedura uczenia MAC oraz sesja STP - port aktywuje się natychmiast. Nie przechodzi w stan *Listening* i *Learning* - dołączając od razu do *EtherChannel*. Sprawdź stan STP przy aktywnym *EtherChannel*:
   Switch#show spanning-tree
   Łącze *EtherChannel* powinno figurować na liście łącz danej instancji STP jako port *Po1*, gdzie *1* to numer *channel-group* (powinno też mieć obliczony koszt zależny od liczby aktywnych portów w *channel-group*).Zwróć uwagę na koszt łącza (*cost*) wyliczony przez STP dla *Po1*.
   Diagnostyka ogólna *EtherChannel*:
   Switch#debug etherchannel
   W przypadku problemów z uruchomieniem (błędy typu *misconfig*) wyłącz i włącz ponownie interfejsy Port channel, np.:
   Switch(config)#int Po 1
   Switch(config)#shut
   Switch(config)#no shut

Zadanie E: Inne podstawowe czynności konfiguracyjne przełączników Cisco Catalyst

1. Gdy przy wpisywaniu komendy popełniona zostanie literówka, przełącznik automatycznie poszukuje adresu IP wpisanego "błędnego symbolu", interpretując go jako nazwę hosta (skoro nie-komendę). Powoduje to chwilowe zablokowanie konsoli (oczekiwanie na DNS). Aby usunąć takie zachowanie należy użyć

komendy:
Switch(config)#no ip domain-lookup

2. Definiowanie nazwy hosta dla przełącznika:
   S*witch(config)#hostname s0*
   s0(config)#
   gdzie *s0* to nowa nazwa.
3. Sprawdzenie aktualnej konfiguracji przełącznika:
   Switch#show running-config
4. Utrwalenie w pamięci *FLASH* obecnych ustawień (nie należy tego obecnie robić, gdyż w *zadaniu A* założyliśmy w przełączniku hasła):
   Switch#write memory
5. Kasowanie ustawień zapisanych w pamięci *FLASH* (z przejściem do ustawień fabrycznych):
   Switch#write erase
6. Wyjście po ścieżce konsoli o jeden poziom w górę:
   Switch(config-line)#exit
   Switch(config)#
7. Wyjście po ścieżce ustawień na samą górę:
   Switch(config-line)#end
   Switch#
8. Analiza zachowania rozmaitych procesów zachodzących w systemie operacyjnym przełącznika - polega aktywowaniu lub de-aktywowaniu procesu ich monitorowania w prowadzonego czasie rzeczywistym i skutkujących generowaniem komunikatów o zdarzeniach w konsoli terminala:
   Switch# debug ip icmp
   Uwaga: proces monitorowania może generować bardzo dużą liczbę komunikatów, co zakłóci korzystanie z konsoli (na przykład, gdy dotyczy on monitorowania ruchu datagramów).
   Wyłączenie wszelkich procesów monitorowania:
   Switch#no debug all

Zadanie F: Zarządzanie przełącznikiem poprzez WWW

1. Włącz przeglądarkę WWW i przy jej pomocy zaloguj się do przełącznika (używając zdefiniowanego wcześniej adresu IP interfejsu VLAN 1). Sprawdź możliwość dokonania wszystkich ustawień konfiguracyjnych opisanych we wcześniejszych zadaniach poprzez interfejs WWW.