Konfiguracja Switcha

poniedziałek, 14 stycznia 2019
08:29

Podstawowa konfiguracja:
- Zmiana nazwy

Konfiguracja dostępu:
- Konsola
- Telnet

Zabezpieczenie switcha:
- Enable
- Szyfrowanie haseł

Ustawienie ip dla switcha:
- Ustawienie IP
- Ustawienie bramy

Tworzenie Vlan:
- Tworzenie nowego vlan
- Nazwa vlan
- Przypisanie vlan do 1 portu
- Przypisanie vlan do wielu portów

Ustawienie portu w tryb pracy TRUNK

Ustawienie VTP:
- Ustawienie trybu pracy
- Ustawienie hasła
- Ustawienie domeny
- Konieczna zmiana nazwy switcha

Ustawienie Port-Security

Ustawienie Port Mirroring

Ustawienie EtherChannel

Dodatkowo SSH

Konfiguracja switcha cz.1
Aby przejść do trybu EXEC:
Enable

Wejście do trybu konfiguracji:
Configure terminal

Ustawienie nazwy dla urządzenia:
Hostname NAZWA - gdzie NAZWA to nowa nazwa dla urządzenia

Ustawienie hasła na enable:
Enable secret cisco

Ustawienie hasła na console:
Line con 0
Password cisco
Login

Ustawienie hasła na telnet:
Line vty 0 4
Password cisco
Login

Szyfrowanie haseł:
Service password-encryption

Zapisywanie aktualnej konfiguracji jako startową:
Copy runn start

Konfiguracja Switcha cz. 2

Tworzenie VLAN-ów
W trybie konfiguracji wydajemy polecenie:
vlan 10– gdzie 10 to numer vlanu
Name Biuro – ustawienie nazwy dla vlan 10

Przypisanie pojedynczego portu do VLAN'u:
W trybie konfiguracji wydajemy polecenie:
Interface fastethernet 0/1 - konkretny interfejs do którego chcemy się odwołać
Switchport mode access - włączenie trybu dostępu
Switchport access vlan 10 – przypisanie dostępu dla vlan 10

Przypisanie Vlanu do wielu portów na raz:
W trybie konfiguracji wydajemy polecenie:
Interface range fastethernet 0/1 - 10 - interfejsy od 1 do 10 do których chcemy się odwołać
Switchport mode access - włączenie trybu dostępu
Switchport access vlan 10 – przypisanie dostępu dla vlan 10

Ustawienie protokołu VTP (w trybie konfiguracji):
VTP pracuje w 3 trybach: server, client, transparent
Vtp mode server – ustawienie switcha w trybi VTP-server
Vtp domain sala3.tzn - ustawienie nazwy domeny dla vtp
Vtp password cisco – ustawienie hasła cisco dla vtp

Przypisanie portu w tryb trunk – do przesyłania różnych vlan'ów
(w trybie konfiguracji)
Int gig 0/1 - wejście na interfejs gigabitowy 0/1
Switchport mode trunk – ustawienie trybu trunk

Konfiguracja switcha cz. 3

Ustawienie parametrów połączenia dla interfejsu, np. Fastethernet 0/1 (w config t)
Int fast 0/1
Duplex half – ustawienie trybu pracy halfduplex lub full dla fullduplex
Speed 10 – ustawienie przepustowości na 10 Mb/s

Konfiguracja związana z adresami MAC:
Show mac-address-table - wyświetla tablicę adresów MAC urządzenia
Clear mac-address-table - czyści tablicę adresów MAC urządzenia
Mac-address-table static 001c.c012.3456 interface fastEthernet 0/1 vlan 10 – ustawienie adresu statycznego MAC dla interfejsu fastethernet 0/1 w Vlanie 10

Konfiguracja statyczna bezpiecznych adresów MAC:
Ustawienie statyczne adresu 001c.c012.3456 jako 1 bezpiecznego adresu Mac na interfejsie 0/1

Int fast 0/1
Switchport mode access
Switchport port-security
Switchport port-security mac-address 001c.c012.3456
Switchport port-security max 1

EtherChannel
EtherChannel - łączenie w sposób logiczny kilku fizycznych interfejsów. Maksymalna ilość fizycznych łączy - 8. Wszystkie muszą mieć taką samą przepustowość. Przykład 1 dla ruch

tylko vlan 10, przykład 2 dla wszystkich vlanów (trunk). Konfiguracja musi zostać wykonana na obu końcach połączenia.
Dwa tryby pracy - PAgP oraz LACP
PAgP – ustawienia trybu w stanie {auto | desirable | on}
LACP - ustawienia trybu w stanie {active | passive}

Przykład 1.
Switch# configure terminal
Switch(config)# interface range gigabitethernet 0/1 - 2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end

Przykład 2.
Switch# configure terminal
Switch(config)# interface range gigabitethernet 0/1 -2
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end

Port Mirroring
Dublowanie portów jest używane w przełączniku sieciowym do wysyłania kopii pakietów sieciowych widocznych na jednym porcie przełącznika (lub całej sieci VLAN) do połączenia monitorowania sieci na innym porcie przełącznika. Jest to powszechnie stosowane w przypadku urządzeń sieciowych, które wymagają monitorowania ruchu sieciowego, takich jak system wykrywania wtargnięcia , pasywna sonda lub technologia monitorowania rzeczywistego użytkownika (RUM), która jest używana do obsługi zarządzania wydajnością aplikacji (APM). Dublowanie portów na przełączniku Cisco Systems jest ogólnie określane jako Switched Port Analyzer (SPAN) lub Zdalny analizator portów (RSPAN).
Inżynierowie sieci lub administratorzy używają dublowania portów do analizowania i debugowania danych lub diagnozowania błędów w sieci. Pomaga administratorom w bacznym śledzeniu wydajności sieci i ostrzega ich, gdy wystąpią problemy. Może być używany do odbijania ruchu przychodzącego lub wychodzącego (lub obu) w jednym lub wielu interfejsach.

Konfiguracja odbywa się w trybie konfiguracji globalnej (conf t)
monitor session 1 source interface fastethernet 0/5
- przypisanie sesji źródłowej na port 5 switcha
monitor session 1 destination interface fastethernet 0/3
- przypisanie sesji przeznaczenia na port 3 switcha

polecenie do podglądu sesji:
show monitor session 1

Session 1

Source Ports:
RX Only: None
TX Only: None
Both: Fa0/5
Destination Ports: Fa0/3

Port Security
konfiguracja portów do obsługi wybranych adresów MAC
Sposób ten zabezpiecza fizycznie dostęp do zasobów naszej sieci komputerowej, poprzez takie ustawienia przełącznika CISCO, aby mógł on obsługiwać tylko wskazane adresy MAC na danym porcie (przełączniki na podstawie tego parametru przesyłają dane w sieci), każdorazowe podłączenie urządzenia z innym adresem fizycznym niż ten zapisane w konfiguracji, spowoduje zablokowanie portu i uniemożliwi korzystanie z sieci.

Lista aktualnie dostępnych adresów MAC na urządzeniu:

show mac-address-table
W wyniku wykonania polecenia zostanie wyświetlona tabela z adresami MAC przypisanym do danego
interfejsu np:

Vlan	Mac-Address	Type	Ports
1	0001.9666.099c	DYNAMIC	Fa0/1
1	0060.3ed6.41eb	DYNAMIC	Fa0/2
1	0060.5c52.b33e	DYNAMIC	Fa0/3

Konfiguracja PortSecurity odbywa się na konkretnym interfejsie np.:FastEthernet 0/1:
configure terminal
interfacefastEthernet 0/1
W tym miejscu wykonamy polecenia, które przypiszą adres MAC wybranego komputera do tego interfejsu:
switchport mode access
switchport port-security
switchport port-security violation shutdown (do wyboru - protect/restrict/shutdown)
switchport port-security maximum 1
switchport port-security mac-address sticky - (uczy się adresów MAC tylu ile wskazuje parametr powyżej)
switchport port-security mac-address 0001.9666.099c
exit

Od teraz każdorazowe podłączenie do portu urządzenia z innym adresem MAC niż ten przypisane spowoduje zablokowanie interfejsu lub inną reakcję. Aby go odblokować należy w trybie konfiguracji interfejsu wykonać polecenie shutdown / no shutdown
---
Dodanie adresu MAC do tablicy adresów MAC na Switchu:

mac-address-table static 001c.c011.2233 vlan 10 interface fastethernet 0/1

Polecenie to przypisuje w sposób trwały adres MAC 001c.c011.2233 do interfejsu 0/1 w Vlan'ie 10

Dodatkowo:
Konfiguracja SSH
show ip ssh - sprawdzam czy działa ssh
konfiguracja SSH
Aby konfiguracja ssh zadziałała musimy ustawić :
inną nazwę urządzenia niż domyślna
oraz nazwę domeny

ip domain-name [nazwa domeny]
hostname [nazwa switcha]

generowanie klucza – zalecane 1024 bity
crypto key generate rsa
stworzenie użytkownika i hasła
username Waldek secret 0 cisco
Uruchomienie ssh na vty 0 4
line vty 0 4
login local
transport input ssh
komenda logowania z innego switcha
ssh -l cisco [ip switcha]