TP-Link TL-SG105E - switch zarządzalny

Ogólne

Do panelu konfiguracyjnego można dostać się korzystając z przeglądarki internetowej lub przez oprogramowanie załączone na płycie o nazwie *Simple Smart Utility* (lepszy wybór, gdy mamy problem ze znalezieniem naszego *switch'a*, gdyż w tej opcji wysyłane są pakiety UDP na *broadcast* korzystając z portów 29808/29809).

Domyślne IP: DHCP z routera; jeśli brak DHCP, to 192.168.0.1.

Domyślny użytkownik: *admin*

Domyślne hasło: *admin*

Prędkość portów: 1000Mb/s (zielona dioda), 10/100 Mb/s (żółta dioda).

Standardy: IEEE802.3*, IEEE802.1p, IEEE802.1q

Prędkości: Ethernet 10Mb/s (*Half Duplex*) i 20Mb/s (*Full Duplex*); Fast Ethernet 100Mb/s (*Half Duplex*) oraz 200Mb/s (*Full Duplex*); Gigabit Ethernet 2000Mb/s (*Full Duplex*).

Okablowanie: 10Base-T, 100Base-TX, 1000Base-T.

Czym *switch zarządzalny* różni się od routera?

Funkcje	Switch zarządzalny	Router
Serwer DHCP	✗	✔
Dedykowany port WAN	✗	✔
Możliwy moduł AP	✗	✔
Konwersja różnych protokołów	✗	✔
Firewall	✗	✔
Posiada wiele kart sieciowych	✗	✔
Przesyła dane w oparciu o IP (warstwa 3 OSI)	✗	✔

Funkcje

Access Security - umożliwia logowanie się administratora tylko z konkretnego portu po konkretnym protokole: *Control Mode / Port Based: nrPortu*.

Tryb tekstowy:

```
TL-SG105E(config)# interface vlan 1
TL-SG105E(config-if)# user access-control port-based interface gigabitEthernet 1/0/1 http https ssh
```

Port Security - ustawienie pojedynczego portu fizycznego na obsługę tylko jednego konkretnego adresu MAC (do pola „*Max Learned MAC*" wprowadzamy 1, pole „*Learn Mode*" ustawiamy na „*Permanent*", a status na „*Drop*"). Po wpięciu do tego portu zaufanego urządzenia, switch zapamiętuje jego adres MAC (status „*Learned Num*" przyjmuje wartość 1).

Jeśli do tego portu podłączymy potem inne urządzenie (innego laptopa, o innym numerze MAC) - port zostanie zablokowany.

W wersji tekstowej:

TL-SG105E> **enable**

TL-SG105E# **configure**

TL-SG105E(config)# **interface range gigabitEthernet 1/0/4** *(konfigurowany będzie port 4)*

TL-SG105E(config-if-range)# **mac address-table max-mac-count max-number 1 mode permanent status drop** *(tylko jeden adres MAC będzie akceptowany)*

TL-SG105E(config-if-range)# **show mac address-table max-mac-count interface gigabitEthernet 1/0/4** *(po minucie sprawdzamy, czy rzeczywiści adres MAC podpiętego urządzenie został zapisany)*

IGMP Snooping - protokół filtrujący ruch IGMP w wyniku uczenia się / rozpoznawania grup multicastowych, umożliwia kierowanie rozgłoszeń *multicast* tylko do wybranych portów (to one zgłaszają chęć otrzymywania tych pakietów poprzez wysłanie „*join to IP_Nadawcy*”) eliminując niepotrzebny ruch rozgłoszeniowy (np. serwer telewizji internetowej emituje 3 programy o odmiennym IP (*Multicast Table*), każdy z nich kierowany jest przez switch do innego portu fizycznego). Switch nie robi więc rozgłoszenia do wszystkich portów, lecz przekierowuje ten ruch do konkretnych maszyn, które go oczekują. Router w sieci też powinien obsługiwać funkcję IGMP Proxy. W switchu określamy, które porty mają brać udział w IGMP Snooping i tworzymy dla nich VLAN. W praktyce, na przełączniku aktywujemy funckję IGMP Snooping i wybieramy opcję „*Unknown Multicast Frame: Drop / Discard*”. Aktywujemy także opcję „*Querier*”. Funkcja ta nie generuje dodatkowych komunikatów w sieci, a znacząco je redukuje.

Router okresowo odpytuje komputery (*IGMP Query* wysyłane na 224.0.0.1, czyli do wszystkich hostów), czy nadal są zainteresowane członkostwem w danej grupie multicastowej. Komputery odpowiadają za pomocą *IGMP Report* (w przypadku braku odpowiedzi przez pewien czas, router usuwa komputer z grupy). Komputer może także sam opuścić grupę poprzez wysłanie „*IGMP Leave IP_Grupy*” na adres 224.0.0.2 (wszystkie routery).

Switch> **show ip igmp group** *(wyświetla grupę IGMP)*

DHCP Snooping - zapobiega sytuacji, w której haker unieszkodliwia nasz serwer DHCP i wystawia w sieci swój własny serwer DHCP. W konfiguracji należy podać numer VLAN (jeśli nie mamy VLAN-ów, wpisujemy 1), a w sekcji „*Port Config*” należy zaznaczyć port do którego podpięty jest zaufany serwer DHCP („*Trusted Port: Enable*”). Na pozostałych portach ustawiamy limit możliwych do wysyłania żądań do serwera DHCP („*Rate Limit*”) na 10/s (aby uniknąć paraliżu w przypadku ataku).

W trybie tekstowym:

TL-SG105E(config)# **ip dhcp snooping**

TL-SG105E(config)# **ip dhcp snooping vlan 1**

TL-SG105E(config)# **interface gigabitEhternet 1/0/4**

TL-SG105E(config-if)# **ip dhcp snooping trust**

TL-SG105E(config)# **interface range gigabitEhternet 1/0/1-3**

TL-SG105E(config-if-range)# **ip dhcp snooping limit rate 10**

TL-SG105E(config)# **interface range gigabitEhternet 1/0/5-8**

TL-SG105E(config-if-range)# **ip dhcp snooping limit rate 10**

TL-SG105E(config-if-range)# **show ip dhcp snooping interface** *(podsumowanie konfiguracji)*

LAG (*Link Aggregation Group*) - łączenie kilku fizycznych portów w jeden logiczny port, np. dwa switche możemy połączyć ze sobą za pomocą dwóch niezależnych kabli w celu zapewnienia redundancji (nadmiaru, na wypadek awarii). Połączone (zagregowane) porty muszą obsługiwać tę samą szybkość i być w trybie *full-duplex*. Połączenie może być ustawione statycznie (Static LAG) lub dynamicznie (przez protokół LACP - *Link Aggregation Control Protocol*). Tę samą operację (te same porty) należy zagregować na drugim switch'u.

W trybie tekstowym:

TL-SG105E(config)# **interface GigabitEthernet 1/0/7-8**

TL-SG105E(config-if-range)# **channel-group 1 mode on**

TL-SG105E(config-if-range)# **show etherchannel 1 summary** *(sprawdzamy, czy wszystko jest OK)*

Zastosowanie dwóch kabli zwiększa przepustowość łącza (ramki nie są powielane na każdym kablu, więc nie jest to dublowanie ruchu). W przypadku awarii jednego kabla, drugi automatycznie przejmuje jego rolę, choć mamy wtedy prędkość standardową.

Port Mirroring - funkcja zwana niekiedy SPAN (***S****witched* ***P****ort* ***An****alyzer*), umożliwia kopiowanie ruchu (wychodzącego i przychodzącego) z jednego portu na inny (jego dublowanie) w celu przechwycenia jego ruchu lub diagnostyki tego ruchu, na przykład za pomocą programu *Wireshark*. Port kopiowany to „*Mirrored Port*" (ruch wychodzący TX [*Ingress*] / ruch przychodzący RX [*Engress*]), a port na który ruch jest kopiowany to „*Mirroring Port*". Jeden *Mirroring Port* może monitorować kilka *Mirrored Port*.

W trybie tekstowym:

Switch(config)# **monitor session 1 source interface fastEthernet 0/2** *(jako źródło można także podać VLAN, np. source vlan 30)*

Switch(config)# **monitor session 1 destination interface fastEthernet 0/10**

MTU VLAN Configuration - nie ma nic wspólnego z MTU (*Maximum Transmission Unit*), lecz raczej oznacza (*Multi Tenant Unit*); izoluje ruch z poszczególnych portów, aby nie mogły się ze sobą bezpośrednio komunikować i przekazuje cały ruch na port *Uplink*, aby to router decydował o ich wzajemnej komunikacji.

Port Isolation - okrojona wersja VLAN-ów; nawet jeśli porty są we wspólnej grupie IP, nie będą się widzieć, jeśli włączona jest izolacja; Port: 1 (port źródłowy) wysyła dane (*Forward Portlist*) do konkretnych portów (wszystkie inne są izolowane).

Port Based VLAN Configuration - typowe tworzenie wirtualnym grup LAN-ów (VLAN-ów). Domyślnie są to porty z separacją (bez znakowania / tagowania).

W trybie tekstowym:

Switch# **show vlan brief** *(skrócona lista VLAN-ów)*

802.1Q VLAN Configuration - tutaj możemy określić, które porty są tagowane, a które nie są. Jeśli chcemy połączyć ze sobą dwa switch'e zarządzalne i scalić ich porty fizyczne we wspólny VLAN, porty te należy otagować. Tagi umieszczane są wewnątrz ramki po adresie źródłowym. Pierwsza część tagowania to TPID, którego wartość zawsze wynosi 0x8100 (informacja, że ramka została otagowana zgodnie ze standardem 802.1q). Drugie pole to TCI zawierające identyfikator sieci VLAN, priorytet oraz standard sieci LAN (np. 0 = Ethernet). W konfiguracji switcha należy pamiętać o nadaniu VLAN-om odpowiedniego numeru PVID.

Porty TRUNK - połączenie pomiędzy dwoma switchami (zwane także magistralą 802.1q), które pozwala na przenoszenie całej komunikacji między VLAN-ami poprzez jedno łącze fizyczne (np. na obu switchach mamy VLAN-y „uczniowie" oraz „nauczyciele", które będą się ze sobą komunikować). Ramki przesyłane przez port TRUNK są automatycznie tagowane, dzięki czemu switche są w stanie określić do jakiego VLAN-u je kierować. Jeśli ramka nie jest otagowana, jest kierowana do natywnego VLAN-u (może istnieć tylko jeden natywny VLAN).

Tworzenie portu trunk na wybranym interfejsie:

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

Switch(config-if)# **switchport trunk encapsulation dot1q**

Switch(config-if)# **switchport trunk native vlan 99** *(tworzymy tzw. „czarną dziurę", domyślny port natywny VLAN1 zmieniamy na VLAN99, który nie istnieje)*

Switch(config-if)# **switchport trunk allowed vlan 10,14,18** *(port trunk będzie obsługiwał VLAN 10/14/18)*

Switch(config-if)# **no shutdown**

Tryby portów

- **general** - zwykły, może mieć przypisanych wiele VLAN-ów;
- **access** - zwykły (nigdy *trunk*) do obsługi ramek nieotagowanych, może mieć przypisany tylko jeden VLAN; jeśli natrafi na ramkę otagowaną, odrzuci ją;
- **nonnegotiate** - zawsze *trunk*;
- **dynamic auto** - port zmienia się automatycznie w *trunk* jeśli na drugim końcu będzie port *trunk* lub *desirable* *(oczekuje inicjatywy tego drugiego portu)*;
- **dynamic desirable** - aktywnie stara się zmienić na port *trunk* jeśli na drugim końcu także będzie *desirable* / *trunk*.

Uwaga: Port *trunk* (np. nr 1) musi znaleźć się w poszczególnych VLAN-ach, które go potrzebują (np. VLAN#20 [**1**-4,9], VLAN#30 [**1**,5-9]), a do połączeń switch'a z Internetem (port 9) należy utworzyć osobny VLAN i wciągnąć do niego wszystkie porty w tym *trunk* [1-**9**].

VPT - to własnościowy protokół firmy Cisco do zarządzania wieloma VLAN-ami na jednym wspólnym łączu fizycznym.

QoS Basic - możemy tutaj określić, które fizyczne porty mają najwyższy priorytet (*Port Based*), a więc przydzielić go połączeniom głosowym i video. Należy także w tym przypadku wyłączyć funcję „*NAT Boost*" (nie może działać razem z QoS). Priorytety możemy także powiązać z poszczególnymi protokołami, urządzeniami lub programami, np. FTP, HTTP, Facebook, POP3, telefon VoIP.

Bandwidth Control Settings - oprócz korzystania z QoS, możemy alternatywnie na „sztywno" określić przepustowość na poszczególnych portach w kb/s (*Ingress Rate* [przychodzące] / *Egress Rate* [wychodzące]). Port odbierający dane wysyła do nadawcy po prostu „ramkę pauzy" (i ustawia jej czas trwania) po odebraniu określonej ilości danych (lub wtedy, gdy otrzymuje więcej danych niż jest w stanie przetworzyć). Nadawca nie tylko zwalnia transmisję do konkretnego odbiorcy, ale zwalnia transmisję do wszystkich odbiorców (i to jest duża wada). Ramka po pewnym czasie „wygasa" i karta sieciowa ponownie odbiera zbuforowane dane nadawcy. „Ramki pauzy" nie są wysyłane bezpośrednio do drugiego komputera, ale do switch'a (a switch może wysyłać takie ramki do komputerów). Nie można używać tej funkcji jednocześnie z QoS (i jest ona gorsza niż QoS).

Sterowanie przepływem danych Ethernet jest na niższym poziomie OSI niż sterowanie przepływem danych TCP (protokół ten zwiększa powoli szybkość przepływu, a gdy segmenty TCP zaczynają być gubione / tracone, wtedy zaczyna tę szybkość zmniejszać i robi retransmisję segmentów). Nakładanie się tych obu mechanizmów nie jest dobrym pomysłem (spowalnia drastycznie sieć). Nie należy włączać tej opcji!

Storm Control Settings - czasami rozsyłane wiadomości wymagają od odbiorców odpowiedzi (potwierdzenia), a te odpowiedzi wymagają kolejnych potwierdzeń i tworzy się efekt kuli śnieżnej (złośliwe oprogramowanie, uszkodzona karta sieciowa). Funkcja filtruje ruch rozgłoszeniowy, tutaj można ograniczyć przepustowość tego ruchu, ale tylko dla określonych typów ramek (*broadcast / multicast*). Innymi słowy: jeśli ruchu rozgłoszeniowego jest zbyt dużo (przekroczono określony poziom), zostaje on ograniczony, aby nie zapchać sieci. Ograniczenie polega albo na porzucaniu ramek, albo na czasowym wyłączeniu interfejsów.

Switch(config)# **interface FastEthernet0/1**

Switch(config-if)# **storm-control broadcast level ?** *(może być broadcast / multicast / unicast)*

Cable Test - testowanie kabli pod względem błędów, ale także problemów wynikających ze zbyt dużego dystansu.

Loop Prevention Settings - wykrywa zapętlenie w sieci (także VLAN) w oparciu o protokół SLPP (*Simple Loop Prevention Protocol*, małe pakiety *Hello*). W przypadku wykrycia zapętlenia, port jest wyłączany. Opcja przydatna w przypadku problemów w zastanej / obcej sieci (nie

znamy jej). Jeśli doskonale znamy sieć i jej okablowanie, opcja powinna być wyłączona, aby nie obciążać sieci.

Port Statistics - pokazuje czy port jest aktywny oraz w jakim trybie prędkości połączenia znajduje się obecnie, oraz czy występują nieprawidłowe ramki. Należy tutaj zwrócić uwagę, że „*Jumbo Packets*" będzie tutaj notowany zarówno jako błędny (*TxBadPkt*), jak i jako dobry (*TxGoodPkt*).

Jumbo Frame - jeśli chcemy wdrożyć przepuszczanie ramek Jumbo, powinniśmy to ustawić nie tylko na routerze / switchu (domyślnie jest aktywne), ale także na kartach sieciowych komputerów: *Właściwości Karty / Konfiguruj... / Advanced / Property: Jumbo Frame [9KB MTU]*. Aby sprawdzić czy taka komunikacja działa: **ping 192.168.0.23 –f –l 9000**.

Tryb tekstowy

Switchem można zarządzać za pomocą systemu bardzo podobnego do IOS (połączenie przez telnet lub SSH).

TL-SG105E> **enable**

TL-SG105E# **configure**

TL-SG105E(config)#

Aby włączyć logowanie się za pomocą SSH: System / Access Security / SSH Config. W trybie tekstowym:

TL-SG105E(config)# **ip ssh server**

TL-SG105E(config)# **show ip ssh** *(upewniamy się)*

Uwaga*: Jeśli będziemy łączyć się za pomocą PuTTY, program poprosi nam o stworzenie „fingerprint" (potwierdzenie, że ufamy zdalnemu switchowi).*

Bezpieczeństwo

1. Należy usunąć domyślnego administratora „*admin*", utworzyć nowego z inną nazwą: *System / User Managment*. W trybie tekstowym:

   TL-SG105E(config)# **user name robert privilege admin secret** *mojeHasło*

   TL-SG105E(config)# **no user name admin** *(usuwamy konto „admin", oczywiście po zalogowaniu się na nowe konto)*

   TL-SG105E(config)# **show user account-list** *(upewniamy się, że wszystko jest OK)*
2. Należy zmienić domyślne IP switcha: *Routing / Interface*. W trybie tekstowym:

   TL-SG105E(config)# **interface vlan 1**

   TL-SG105E(config-if)# **ip address 192.168.100.200 255.255.255.0**
3. Jeśli nie zamierzamy wykorzystywać **natywnego** *VLAN #1* do jakiegoś konkretnego celu, dobrze jest przenieść go do innej **nieistniejącej** sieci (np. do 99).

   TL-SG105E(config-if)# **switchport trunk native vlan 99**

   TL-SG105E# **show interface trunk** *(upewniamy się)*
4. Administrator powinien utworzyć dedykowany VLAN tylko dla siebie, na potrzeby konfiguracji.
5. Nieużywane porty należy dodać do fałszywego VLAN-u (tzw. czarna dziura), który nie ma do niczego dostępu i niczemu nie służy.

Luki bezpieczeństwa

- Hasło przesyłane jest przez *http* jawnym tekstem. Switch nie ma obsługi *https*. Rozwiązaniem jest nie łączyć się zbyt często z panelem konfiguracyjnym (skonfigurować go raz na początku i zamknąć).
- Oprogramowanie *Simple Smart Utility* wykrywa IP nawet izolowanych VLAN-ów.
- W niektórych przypadkach stwierdzono, że autoryzacja nie jest oparta o sesję, ale o numer IP (więc każdy taki sam numer IP w sieci będzie mieć dostęp do panelu konfiguracyjnego switch’a).
- Można wymusić *reboot* switcha (będzie niedostępny około 30 sekund) poprzez wysłanie mu zbyt długiego loginu:

```
curl -d "username =
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx & logon = Login "-X POST
http://192.168.0.1/logon.cgi
```

Uwaga: W niektórych sytuacjach (zależy od długości loginu) przełącznik zawiesi się po prostu (jedyna możliwość: ręczne odłączenie go od zasilania).

Ostatnia aktualizacja: 26 listopada 2020.