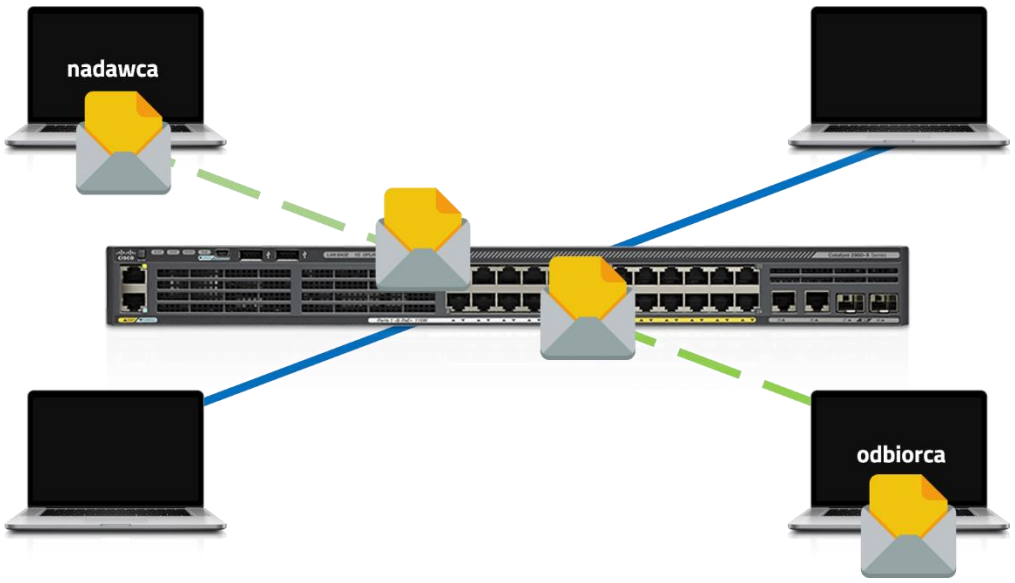
pasja-informatyki.pl

Sieci komputerowe – Konfiguracja przełącznika CISCO – hasła dostępu, Port Security, DHCP Snooping

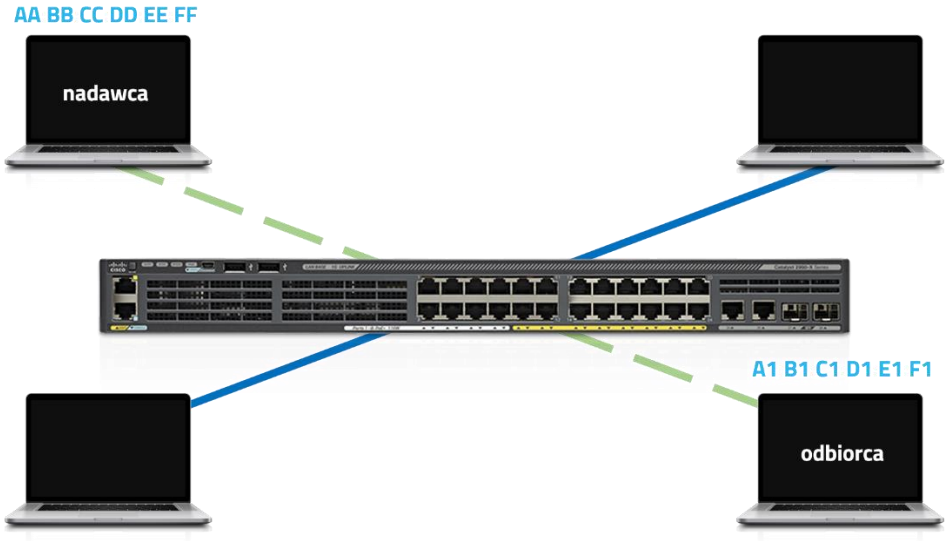
Damian Stelmach

Spis treści

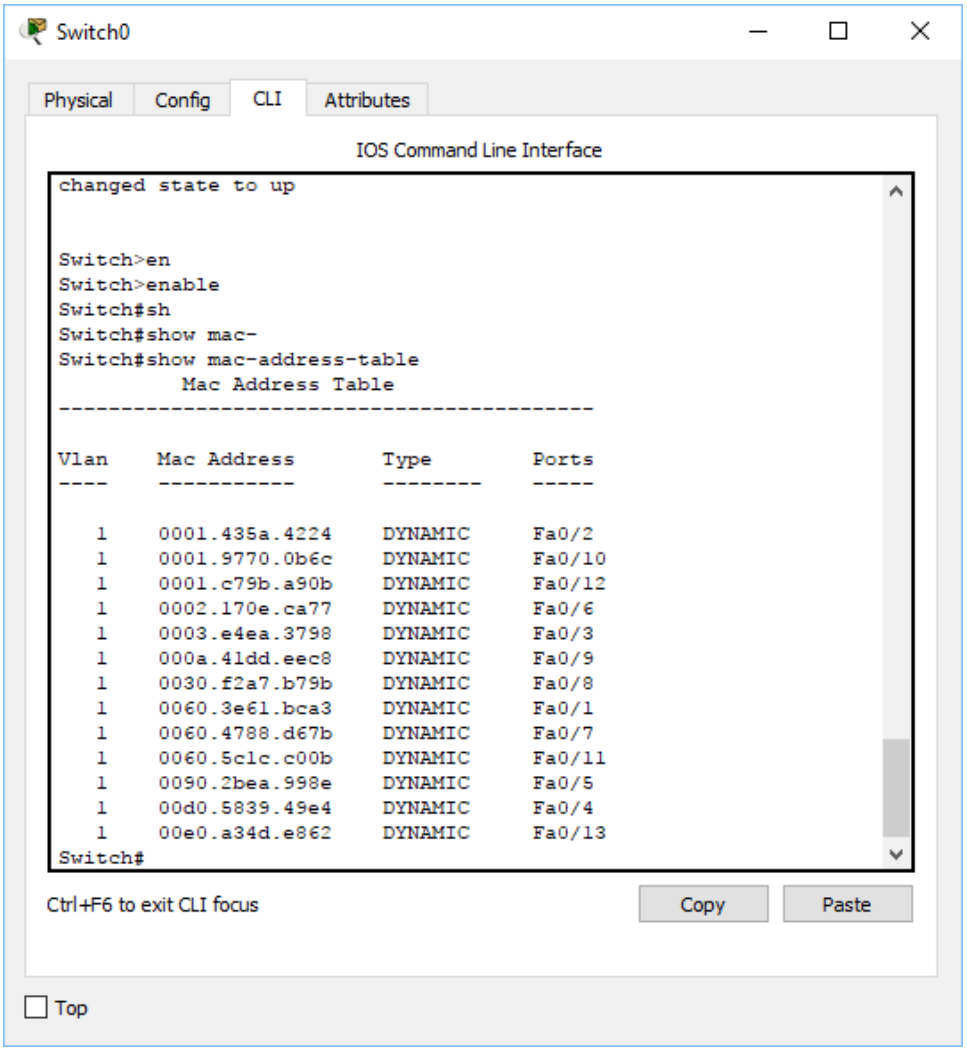
Przełączniki sieciowe (ang. Switches), są to urządzenia pracujące w **drugiej warstwie modelu OSI**, czyli w warstwie **łącza danych**. Ich podstawową funkcją **jest pośrednictwo** w wymianie danych pomiędzy **urządzeniami końcowymi**, czyli komputerami czy drukarkami pracującymi w sieciach lokalnych. Tak więc można powiedzieć, że switch'e są swoistymi łącznikami pomiędzy urządzeniami końcowymi. Zasada ich działania jest ogólnie dość prosta, odbierają dane na jednym porcie, są to dane od nadawcy i przekazują je na port, do którego podłączony jest odbiorca danych.



Parametrem, na podstawie którego przełącznik wie, na jaki port przekazać dane jest **fizyczny adres karty sieciowej** urządzenia końcowego, czyli adres **MAC**. Po podłączeniu każdego urządzenia końcowego do sieci, przełącznik uczy się jego adresu MAC i zapisuje go w swojej pamięci. Proces ucznia się nazywany jest **zalewaniem** (omówiony został w odcinku dotyczącym funkcji warstwy łącza danych).



Zbiór adresów fizycznych, zapisanych w pamięci przełącznika nazywany jest **tablicą adresów MAC**. Przykładową tablicę wyjętą ze switcha pracującego w sieci lokalnej widać poniżej.



Tablica **zawiera informacje o adresie MA**C urządzanie podłączonego do danego portu oraz **o sposobie uzyskania takiej informacji**. Kiedy **ramka** trafia do przełącznika (porcja danych w warstwie łącza danych to właśnie ramka), ten odczytuje z niej adres fizyczny **odbiorcy**, porównuje go ze swoją tablicą adresów fizycznych i wysyła dane na ten port, do którego podłączone jest urządzenie o takim samy adresie, jaki jest w ramce.

Obecnie dostępne switch'e oferują zacznie szerszy zakres funkcjonalności, **niż tylko przełączanie ramek**. Spotkać możemy, np. przełączniki, które posiadają funkcjonalności **zbliżone do ruterów**, potrafiące realizować również procesy rutingu. O takim przełączniku, mówi się wówczas, że jest on **przełącznikiem warstwy trzeciej**, ponieważ realizuje również zadania związane z **warstwą sieci modelu OSI**. Zwyczajne przełączniki, realizujące tylko zadania warstwy drugiej, podzielić możemy na dwie grupy, na przełączniki **niezarządzalne** oraz **zarządzalne**. Te pierwsze po prostu wyjmujemy z

kartonu, podłączamy do prądu i działamy. Nie wymagają one żadnej konfiguracji, działają od razu po uruchomieniu. **Przełączniki zarządzalne**, również mogą pracować zaraz po podłączeniu do sieci zasilającej, oferują one jednak możliwość konfiguracji i to w całkiem sporym zakresie.

Większość obecnie pracujących sieci lokalnych oparta jest właśnie o przełączniki sieciowe. O takiej sieci mówimy wówczas, że jest to **sieć przełączana**, a nazwa ta wywodzi się oczywiście od urządzeń, które te przełączanie realizują. Najbardziej popularnym standardem w takich sieciach jest oczywiście **Ethernet** oraz wszelkie jego odmiany, dlatego też możecie czasami spotkać się z pojęciem **przełącznika ethernetowego**.

Urządzenia sieciowe marki CISCO są **dość drogie**, dlatego zanim podejmiemy się ich zakupu, warto skorzystać z symulatora **CISCO Packet Tracer**, który pozwoli nam nauczyć się podstaw konfiguracji urządzeń tej firmy, bez konieczności wydawania na nie fortuny. Program ten jest **symulatorem sieciowym**, który pozwala tworzyć **zaawansowane topologie** oraz konfigurować urządzenia bez większych ograniczeń.

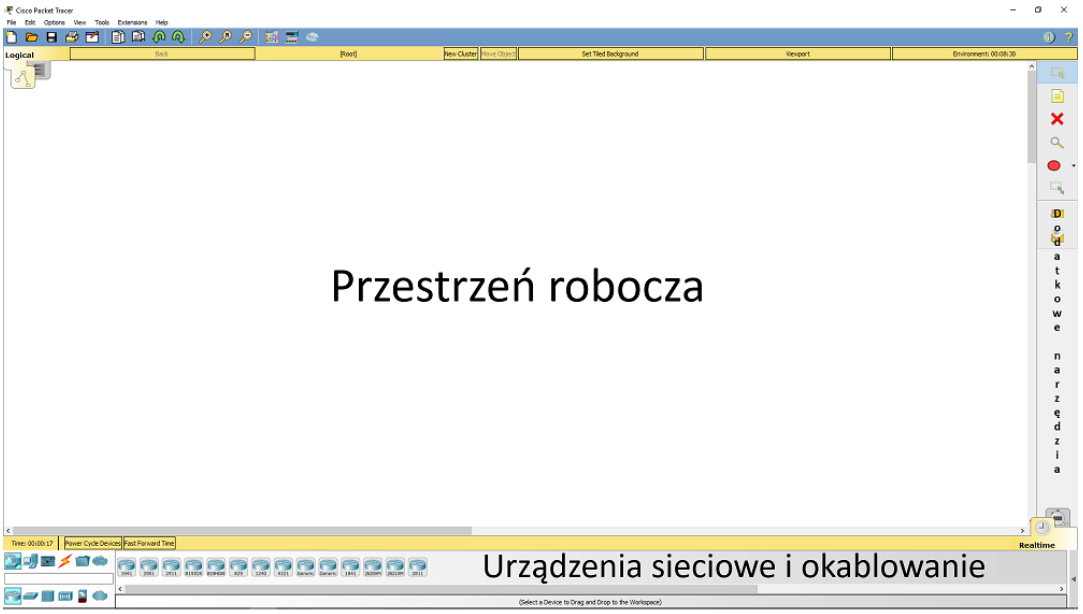
Jest to narzędzie, które bezpłatnie możemy pobrać z oficjalnej strony **akademii CISCO**, znajdującej się pod adresem:

https://www.netacad.com

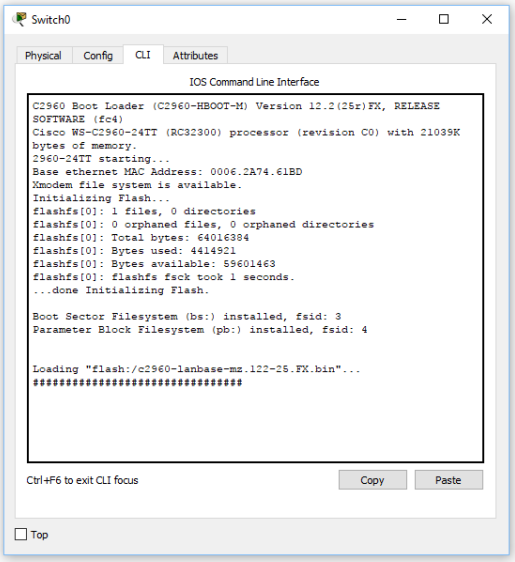
Aby korzystać z pełnej funkcjonalności programu, **należy zarejestrować się w akademii**. Można też aplikacje pobrać z innych stron, natomiast podczas uruchamiania programu trzeba podać **login i hasło**, dlatego tak czy inaczej na stronę akademii CISCO zajrzeć trzeba. Polecam też korzystać właśnie z niej, gdyż tam zawsze znajdziecie najbardziej aktualną wersję programu. Dotarcie do formularza rejestracyjnego możliwe jest poprzez wejście do menu:

COURSES -> PACKET TRACER -> INTRODUCTION TO PACKET TRACER -> ENROLL NOW

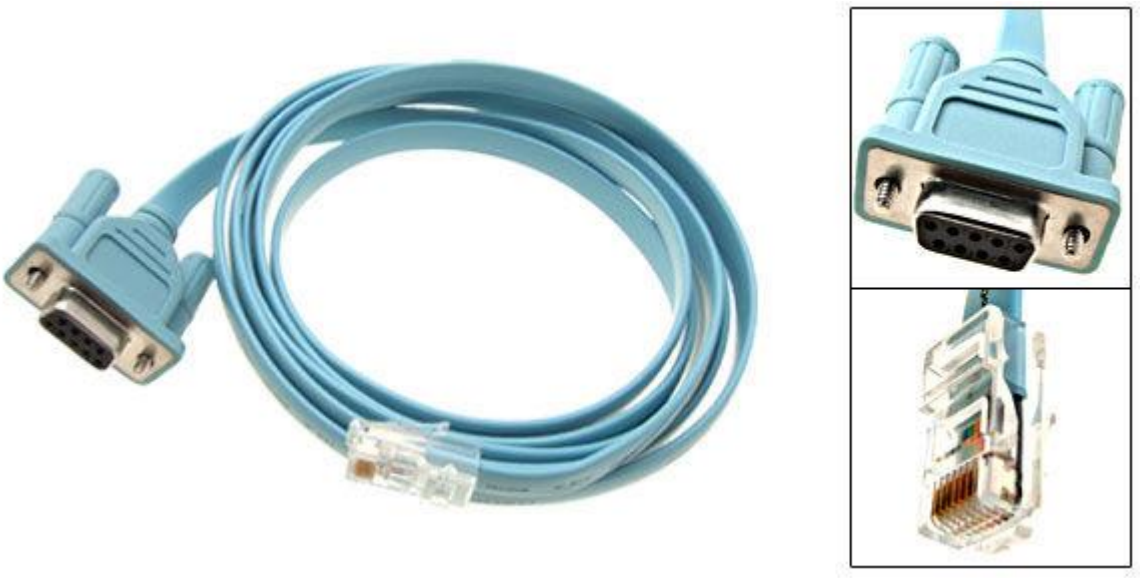
Po uruchomieniu programu, do dyspozycji mamy **przestrzeń do tworzenia topologii**, **pogrupowane urządzenia**, które możemy wykorzystać do tworzenia topologii wraz z **okablowaniem** oraz **dodatkowe narzędzia**.

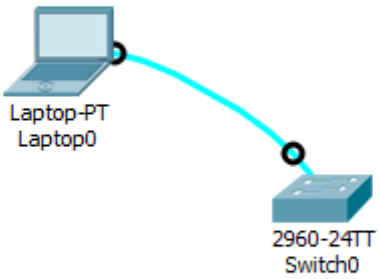


Konfiguracja urządzeń sieciowych odbywać się może z wykorzystaniem **wielu kanałów**. Można połaczyć się z urządzeniem wykorzystując **port konsolowy** (ang. Console), znajdujący się najczęsciej w tylnej części obudowy, jak również poprzez **termianle wirtualne** z wykorzystaniem protokołów zdalnego dostępu takich jak **SSH** czy **Telent**. To w realnej sieci. W przypadku symulatora, mamy <u>również</u> możliwość uruchomienia trybu konfuigracyjnego klikając po prostu w urzadzenia znajduące się w przestrzeni roboczej i wybranie zakładki **CLI** (ang. **Command Line Interface**)



Aby jednak zasymulować **prawdziwą sieć**, warto dodać do przestrzeni roboczej **komputer**, może być laptop i podłączyć się do **konsoli konfiguracyjnej** urządzenia poprzez komputer, z wykorzystaniem **kabla konsolowego** oraz portu **COM** (zwanego RS232). Kabel taki widoczny jest poniżej, z jednej strony posiada końcówkę **RJ45**, którą podłączamy do portu konsolowego w urządzeniu, a z drugiej port **COM**, który podłączamy do komputera.





Chcąc dostać się do konsoli CLI przełącznika, klikamy w ikonę komputera, wybieramy **DESKTOP -> TERMINAL -> OK.** Od teraz mamy już dostęp do konsoli poleceń przełącznika i możemy przystąpić do jego konfiguracji. W realnej sieci, na fizycznym komputerze skorzystalibyśmy z bezpłatnej aplikacji **PUTTY**, która pozwala m.in. na łączenie się z urządzeniami sieciowymi.

Pierwszy, dostępny tryb to **tryb użytkownika**. Uruchamiany jest po wciśnieciu klawisza **ENTER** na klawiaturze. Dostępność tego trybu potwierdzona jest znakiem zachęty w postaci **znaku większości**:

```
SWITCH>
```

Jest to tryb, który nie pozwala na dokonywanie żadnej konfiguracji, a lista dostępnych w nim opcji jest **mocno ograniczona**. Z poziomu tego trybu możemy natomiast przejrzeć np. informacje o dostępnych interfejsach, wydając takie polecenie:

```
Switch>show ip interface brief
```

Lista dostępnych na danym poziomie opcji wyświetla się kiedy na klawiaturze wprowadzimy symbol **znaku zapytania**. Wyświetlanie dostępnych opcji za pomocą znaku zapytania **działa na wszystkich poziomach konfiguracji**

```
Switch>?
Exec commands:
  connect        Open a terminal connection
  disable        Turn off privileged commands
  disconnect     Disconnect an existing network connection
  enable         Turn on privileged commands
  exit           Exit from the EXEC
  logout         Exit from the EXEC
  ping           Send echo messages
  resume         Resume an active network connection
  show           Show running system information
  telnet         Open a telnet connection
  terminal       Set terminal line parameters
  traceroute     Trace route to destination
```

Drugi tryb, to **tryb uprzywilejowany**, uruchamiamy go wprowadzając polecenie **ENABLE**. Przejście do tego trybu potwierdzone jest **hashtagiem** po nazwie urządzenia:

```
Switch>enable
Switch#
```

W tym trybie możemy również przeglądać konfigurację portów, mamy natomiast również możliwość dokonywania **podstawowych zmian konfiguracyjnych**, takich jak wyświetlana **nazwa urządzenia**, jak również na zapisywanie **aktualnej konfiguracji.**

Trzeci tryb, to **tryb konfiguracji globalnej**. Uruchomiony zostaje po wprowadzeniu polecenia **CONFIGURE TERMIAL** lub też **CONF T**:

```
Switch#configure terminal
Switch(config)#
```

To jest tryb pozwalający na **dokonywanie właściwej konfiguracji urządzenia**, jak również jest to tryb, z którego można dostać się do ostatniego dostępnego trybu, tzw. **trybu konfiguracji szczegółowej**, który dotyczy już konkretnych funkcjonaliści. W dalszej części dokumentu omawiał będę poszczególne funkcjonaliści wraz z opisem każdej z komend.

Pierwszą czynnością jaką powinniśmy wykonać zanim zaczniemy konfigurować konkretne funkcjonalności powinno być nadanie **haseł dostępu** do **trybu użytkownika** oraz **trybu uprzywilejowanego**. Jeśli konfigurujemy przełącznik (lub też ruter CISCO) poprzez **kabel konsolowy**, zabezpieczenie hasłem do **trybu użytkownika** wykonamy stosując następujące polecenia:

```
Switch>enable                          /przejście do trybu uprzywilejowanego
Switch#configure terminal              /przejście do trybu konfiguracji globalnej
Switch(config)#line console 0          /wybór portu konsolowego
Switch(config-line)#password cisco     /nadanie hasła cisco
Switch(config-line)#login              /wymaganie hasła podczas logowania
```

Następnie należy utworzyć hasło wymagane podczas przejścia do trybu uprzywilejowanego. Wykonujemy następujące polecenia:

```
Switch(config-line)#exit               /wyjście z trybu konfiguracji portu konsolowego
Switch(config)#enable password cisco   /nadanie hasła cisco dla trybu uprzywilejowanego
```

Hasło przejścia do **trybu uprzywilejowanego** nadane zostało zaraz po tym, jak utworzone zostało hasło do **trybu użytkownika**, dlatego też zanim nadaliśmy to drugie hasło, trzeba było **wyjść z trybu konfiguracji szczegółowej** (w tym wypadku konfiguracji portu konsolowego) stąd zastosowywanie polecenie **EXIT** na początku drugiego listingu.

Podana wyżej konfiguracja hasła, wymaganego przy wejściu do trybu użytkownika dotyczyła portu konsolowego, za pomocą którego my podłączyliśmy się do przełącznika. Jeśli ktoś korzysta natomiast z konfiguracji poprzez protokoły **Telnet** lub **SSH**, wówczas należy nadać odrębne hasła dla tych połączeń. Będąc w trybie konfiguracji globalnej (**Switch(config)#**), wydajemy następujące polecenia:

```
Switch(config)#line vty 0 15           /wybór termianli wirtualnych – od 0 do 15 – tyle
                                       ich jest w przełączniku serii 2960
Switch(config-line)#password cisco     /nadanie hasła cisco
Switch(config-line)#login              /wymaganie hasła podczas logowania
```

Hasła nadane, możemy teraz przystąpić do konfiguracji funkcjonalności związanych z **bezpieczeństwem sieci**.

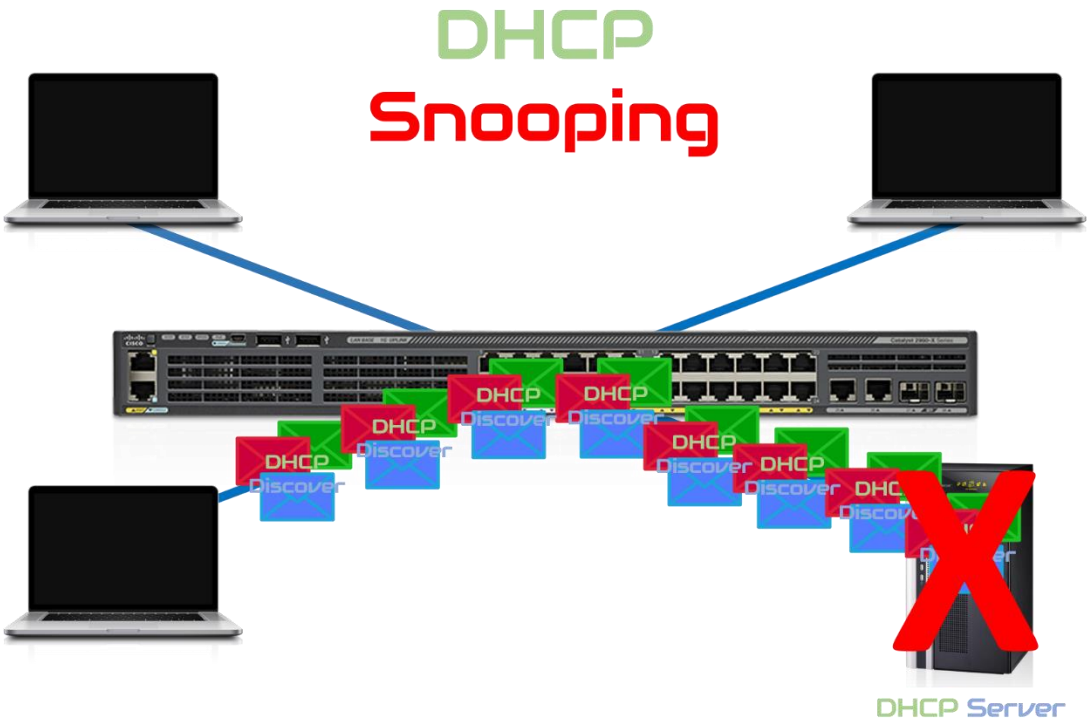
Port Security to **rodzaj zabezpieczenia**, które pozwala **przekazywać ramki**, tylko **zaufanych urządzeń**, a **nie każdego**, które do przełącznika podłączymy. Dzięki odpowiedniej konfiguracji tej funkcjonalności, zabezpieczymy sieć w taki sposób, że **tylko jeden komputer będzie mógł korzystać z danego portu**. Kiedy jakiś intruz będzie chciał dostać się do naszej sieci, np. poprzez próbę podłączenia swojego komputera, przełącznik zareaguje i zablokuje ruch na tym porcie. Zablokuje ponieważ **adres MAC** urządzenia intruza, **nie będzie zaufany** dla naszego przełącznika. W trybie konfiguracji globalnej wykonujemy następujące polecenia:

```
Switch(config)#interface fastEthernet 0/1     /przejście do trybu konfiguracji szczegółowej 1 interfejsu przełącznika
Switch(config-if)#switchport mode access      /zmiana trybu pracy portu przełącznika z dynamicznej na dostępową – wymagane do uruchomiania port security
Switch(config-if)#switchport port-security    /uruchomienie funkcjonalości port Security na 1 porcie
Switch(config-if)#switchport port-security mac-address sticky /przypisanie do port security adresu mac podłączonego komputera
Switch(config-if)#switchport port-security maximum 1      /przypisanie do port security tylko jednego, zaufanego adresu MAC
```

Należy pamiętać, że w przypadku symulatora CISCO Packet Tracer, **wymagane jest wymuszenie ruchu pomiędzy urządzeniami**, aby przełącznik **zapisał adresy MAC poszczególnych komputerów jako zaufane**. Można to zrobić wybierając z dodatkowych narzędzi symbol **koperty** i umieścić na ikonach komputerów (oczywiście muszą mieć przypisane adresy IP). Zasymuluje to działanie polecenia **PING** i pozwoli zapamiętać adresy MAC komputerów jako zaufane. W realnej sieci nie ma takiej konieczności, gdyż ruch wówczas na pewno sam zostanie wygenerowany. Pamiętajcie również o tym, że podobne zabezpieczenie należy skonfigurować na **wszystkich portach przełącznika**, a jeśli któreś z nich są **nieużywane to należy je wyłączyć**. Służy do tego polecenie **SHUTDOWN**, wykonane na poziomie konfiguracji danego interfejsu.

Jeśli podczas testowania funkcjonalności Port Security **zablokujecie port** (podłączenie komputera z innym **adresem MAC** niż zaufany i wykonanie komunikacji zablokuje port), to należy w konfiguracji tego portu wykonać polecenia **NO SHUTDOWN** – to wyłączy port całkowicie, następnie wykonujemy polecenie **SHUTDOWN,** to ponownie uruchomi port i po podłączeniu właściwego komputer będzie już możliwa komunikacja.

Teraz zajmiemy się **kolejną funkcjonalnością** oferowaną przez urządzanie Cisco, a mianowicie **DHCP Snooping**. Usługa DHCP powinna być już wszystkim dobrze znana, **jej głównym zadaniem jest automatyczne przydzielanie adresacji IP** dla urządzeń pracujących w sieci. Praktycznie nie ma na świecie sieci komputerowych, które nie korzystały by z serwerów DHCP. DHCP to **usługa bazująca na transmisji broadcastowej**, czyli rozgłoszeniowej i w związku z tym narażona jest na różnego rodzaju ataki. Korzystając z odpowiednich narzędzi, można spowodować, że serwer zostanie zalany komunikatami **DHCP Discover** i przestanie działać.



Podłączony wówczas do **sieci niezaufany serwer** można zacząć przydzielać **swoje adresy IP**. Funkcjonalność **DHCP snooping**, polega na **przypisaniu do konkretnego portu zaufanego serwera DHCP**, a co za tym idzie, uniemożliwi podłączenie „lewego" serwera, do któregoś z innych portów. Dodatkowo funkcjonalność pozwala na ograniczenie ilości możliwych do wysłania z inny portów komunikatów – żądań **DHCP Discover**, co uniemożliwi wykonanie ataku. Zaczniemy od przypisania **portu 24 jako zaufanego dla DHCP**. W trybie konfiguracji globalnej wykonujemy następujące polecenia:

```
Switch(config)#interface fastEthernet 0/24    /przejście do trybu konfiguracji szczegółowej 24 interfejsu przełącznika
Switch(config-if)#ip dhcp snooping trust      /oznaczenie portu 24 jako zaufanego dla serwera DHCP
```

Switch(config-if)#exit	/wyjście z trybu konfiguracji szczegółowej 24 interfejsu, do trybu konfiguracji globalnej
Switch(config)#ip dhcp snooping vlan 1	/uruchomienie funkcjonalności DHCP Snooping dla vlan'u pierwszego (obecnie cały przełącznik pracuje w vlan'ie pierwszym)
Switch(config)#ip dhcp snooping	/potwierdzenie uruchomienia funkcjonalności DHCP Snooping

Teraz musimy dokonać konfiguracji **pozostałych portów przełącznika**, tak aby **ilość możliwych do wysłania żądań DHCP była jak najmniejsza**, wymagana **tylko do tego aby komputery w sieci faktycznie adres mogły otrzymać**, a **nie zalać serwer rzeką komunikatów**. Dzięki temu próba wysłania większej liczby żądań aniżeli ilość zdefiniowana podczas konfiguracji spowoduje zablokowanie portu. W trybie konfiguracji globalnej wykonujemy następujące polecenia:

Switch(config)#interface range fastEthernet 0/1 – 23	/przejście do zbiorczej konfiguracji interfejsów od 1 do 23
Switch(config-if-range)#ip dhcp snooping limit rate 10	/ograniczenie do 10, ilości możliwych komunikatów DHCP Discover, mogących zostać wysłanych z portów

Należy zawsze pamiętać o zapisaniu konfiguracji urządzenia po dokonaniu zmian.

Aby zapisać aktualną konfigurację do pliku konfiguracji startowej, w trybie uprzywilejowanym należy wykonać polecenie:

Switch#copy running-config startup-config