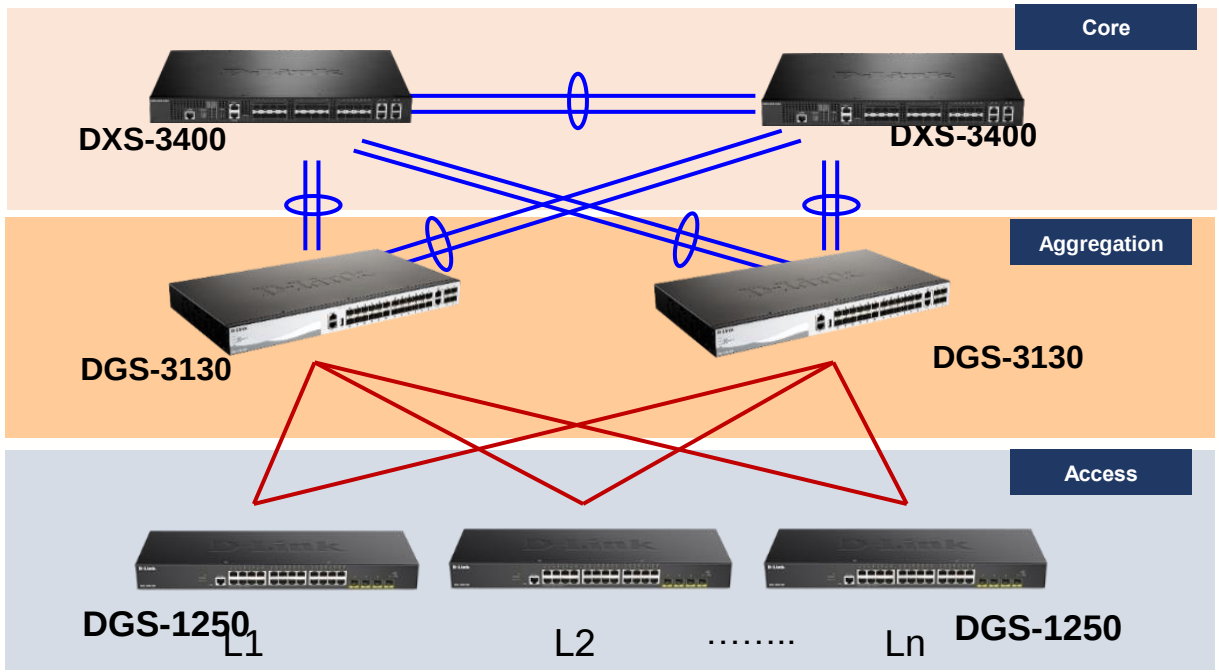
Wybrane mechanizmy bezpieczeństwa w przełącznikach dostępowych

Maciej Dąbrowski
Pre-sales Engineer

Bezpieczeństwo w sieciach dostępowych

- Warstwa dostępowa jak nazwa wskazuje ma nam zapewnić dostęp do sieci.
- Na tym poziomie musimy być najlepiej zabezpieczeni
- Wszystko złe co dzieje się potem może być konsekwencją braku zabezpieczeń w warstwie dostępowej
- Cała sieć jest tak bezpieczna jak jej najsłabsze ogniwo
- Ataki na sieć od wewnątrz są trudne do zdiagnozowania
- Narażamy się na utratę poufnych informacji jak i na zagrożenie przestoju pracy całej sieci
- Często skupiamy się na ochronie sieci od strony zewnętrznej (WAN) zapominając od sieci LAN
- Musimy pamiętać nie tylko o bezpieczeństwie dostępu do sieci ale także o zabezpieczeniu urządzeń sieciowych
- Przełączniki L2 posiadają mechanizmy bezpieczeństwa skutecznie chroniące nas przed najczęstszymi atakami:
  (Port Security, DHCP snooping, Loopback Detection, IMPB, DAI, IP Source Guard, BPDU Guard, Safeguard Engine, DoS Attack Prevention, Storm Control, 802.1X…)



Mechanizmy bezpieczeństwa w przełącznikach dostepowych

DGS-1100 Series

- 802.1Q 128 Vlans
- Management Vlan
- Loopback Detection
- Traffic Segmentation
- Storm Control
- SSL
- D-Link Safeguard

DES-1210 Series

- 802.1Q 256 Vlans
- Management Vlan
- Loopback Detection
- Traffic Segmentation
- Storm Control
- SSL
- D-Link Safeguard
- ACL in (1280)
- 802.1X
- DHCP Server Screening
- Port Security
- DoS Attack Prevention
- ARP Spoofing Prevention
- SSHv2

DGS-1210 Series

- 802.1Q 256 Vlans
- Management Vlan
- Loopback Detection
- Traffic Segmentation
- Storm Control
- TLS
- D-Link Safeguard
- ACL in (768)
- 802.1X (local, Radius)
- DHCP Server Screening
- Port Security
- DoS Attack Prevention
- ARP Spoofing Prevention
- SSHv2
- IMPB

DXS-1210 Series

- 802.1Q 4K Vlans
- Management Vlan
- Loopback Detection
- Traffic Segmentation
- Storm Control
- TLS
- D-Link Safeguard
- ACL in/out (1536)
- 802.1X (local, Radius)
- Guest VLan
- DHCP Server Screening
- Port Security
- DoS Attack Prevention
- ARP Spoofing Prevention
- SSHv2
- IMPB
- DAI
- IPSG
- Trusted Host
- Console Port
- Full Cli
- Password Encryption

DGS-1250 Series

- 802.1Q 4K Vlans
- Management Vlan
- Loopback Detection
- Traffic Segmentation
- Storm Control
- TLS
- D-Link Safeguard
- ACL in (768)
- 802.1X (local, Radius, host based)
- Guest VLan
- DHCP Server Screening
- Port Security
- DoS Attack Prevention
- ARP Spoofing Prevention
- SSHv2
- IMPB
- Trusted Host
- Console Port
- Full Cli

DGS-2000 Series

- 802.1Q 256 Vlans
- Management Vlan
- Loopback Detection
- Traffic Segmentation
- Storm Control
- TLS
- D-Link Safeguard
- ACL in (200)
- 802.1X Radius, Host based,)
- Guest VLan
- DHCP Server Screening
- Port Security
- DoS Attack Prevention
- ARP Spoofing Prevention
- SSHv2
- IMPB
- Trusted Host
- Console Port
- Full Cli
- Password Encryption

DGS-1510 Series

- 802.1Q 4K Vlans
- Management Vlan
- Loopback Detection
- Traffic Segmentation
- Storm Control
- TLS
- D-Link Safeguard
- ACL in (768)
- 802.1X Radius, Host basedCompund Auth,)
- MAC,WAC
- Guest VLan
- DHCP Server Screening
- Port Security
- DoS Attack Prevention
- ARP Spoofing Prevention
- SSHv2
- IMPB (DAI, IPSG)
- Trusted Host
- Console Port
- Full Cli
- Password Encryption

DGS-1520 Series

- 802.1Q 4K Vlans
- Management Vlan
- Loopback Detection
- Traffic Segmentation
- Storm Control
- TLS
- D-Link Safeguard
- ACL in/out (1536)
- 802.1X Radius, Host basedCompund Auth,)
- MAC,WAC
- Guest VLan
- DHCP Server Screening
- Port Security
- DoS Attack Prevention
- ARP Spoofing Prevention
- SSHv2
- IMPB (DAI, IPSG)
- Trusted Host
- Console Port
- Full Cli
- Password Encryption

D-Link®
Building Networks for People

Bezpieczeństwo dostępu do urządzenia

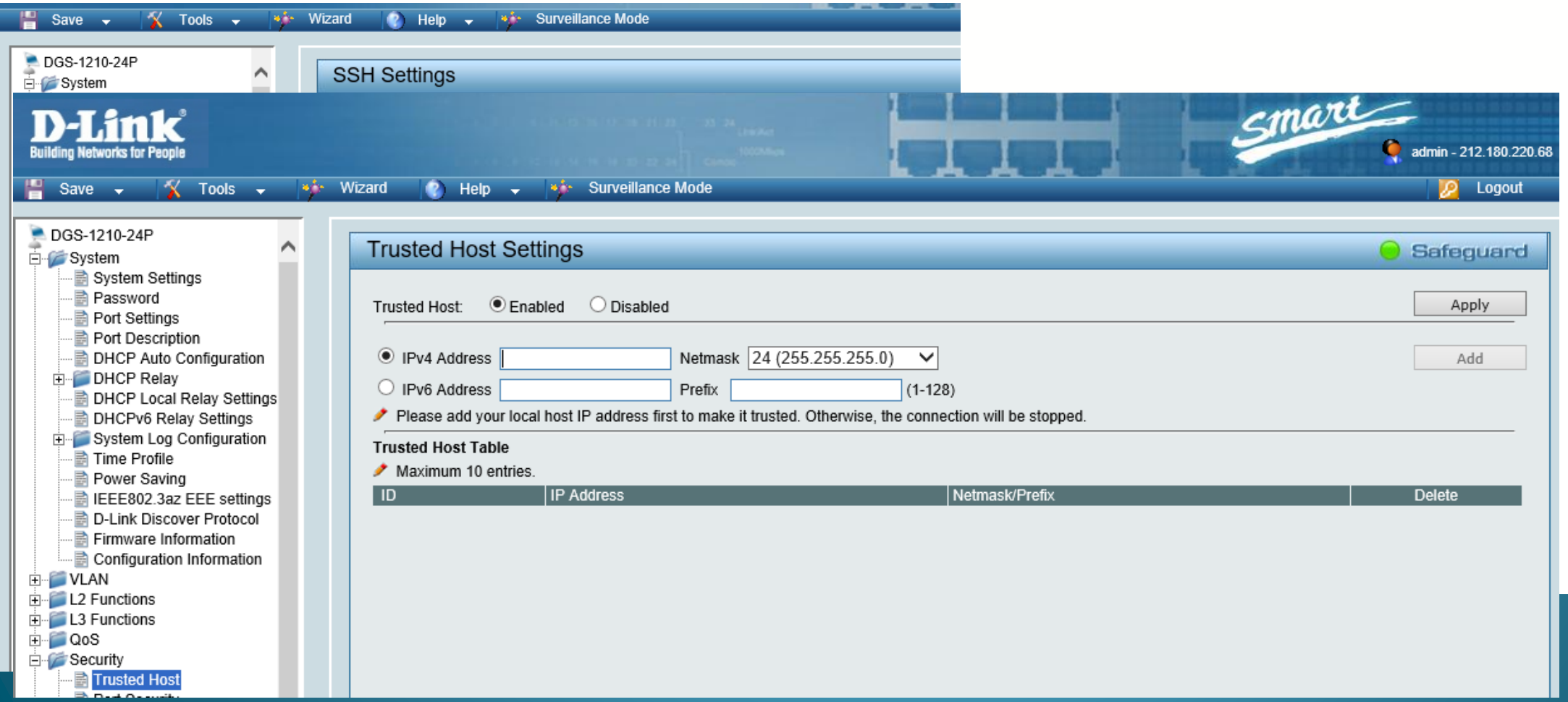
- Domyślny adres przełącznika: 10.90.90.90, username: admin password: admin
- Włączone protokoły telnet (dla przełączników z cli) i http dla przełączników WEB Ui
- Niezabezpieczony hasłem interfejs console
- Wszystkie porty należą do Vlan 1 (możliwość zarządzania ze wszystkich portów)

Jak dokonać podstawowego zabezpieczenia urządzenia:

1. Zmień hasło do konta administratora na wszystkich interfejsach (Web, Cli, Console)
2. Tam gdzie możliwie zaszyfruj hasło w pliku konfiguracyjnym (service password-encryption)
3. Zmień domyślny adres IP przełącznika
4. Ustaw Interfejs zarządzający przełącznika na osobnym Vlanie
5. Usuń porty klienckie z Vlanu management
6. Wyłącz niezabezpieczone protokoły (HTTP, Telnet)
7. Włącz protokoły SSL/TLS i SSH
8. Tam gdzie możliwe ustaw listy ACL dla interfejsów zarządzających (Funkcja Trusted Host)
9. Utwórz dodatkowe konto na mniejszych prawach na jeśli ktoś z zewnątrz potrzebuje dostępu
10. Wykonuj cykliczne backupy konfiguracji na wypadek konieczności resetu urządzenia

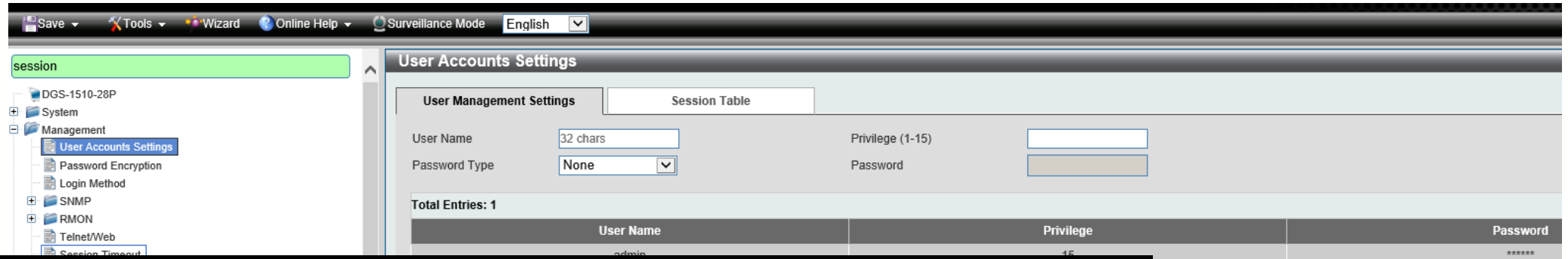
Podstawowe bezpieczeństwo DGS-1210

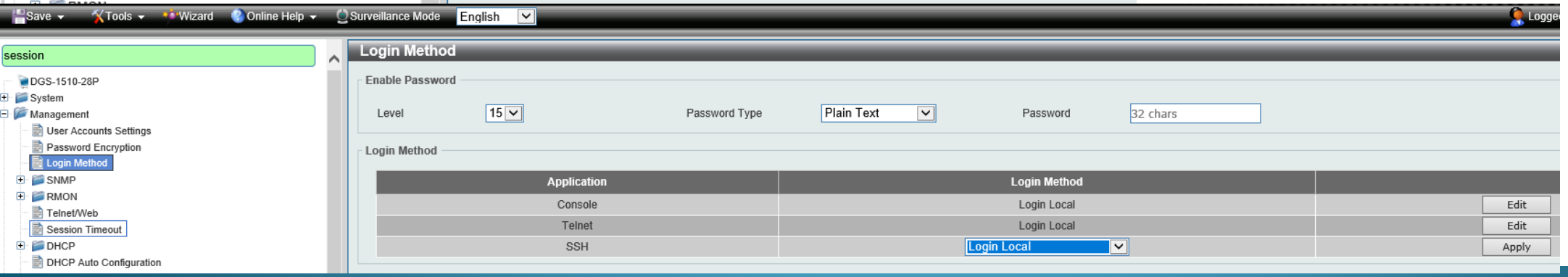
Jedno konto na prawach administratora do wszystkich interfejsów, z możliwością zmiany hasła
Włączenie SSL/TLS
Włączenie SSH
Trusted Host dla zwiększenia bezpieczeństwa



D-Link
Building Networks for People

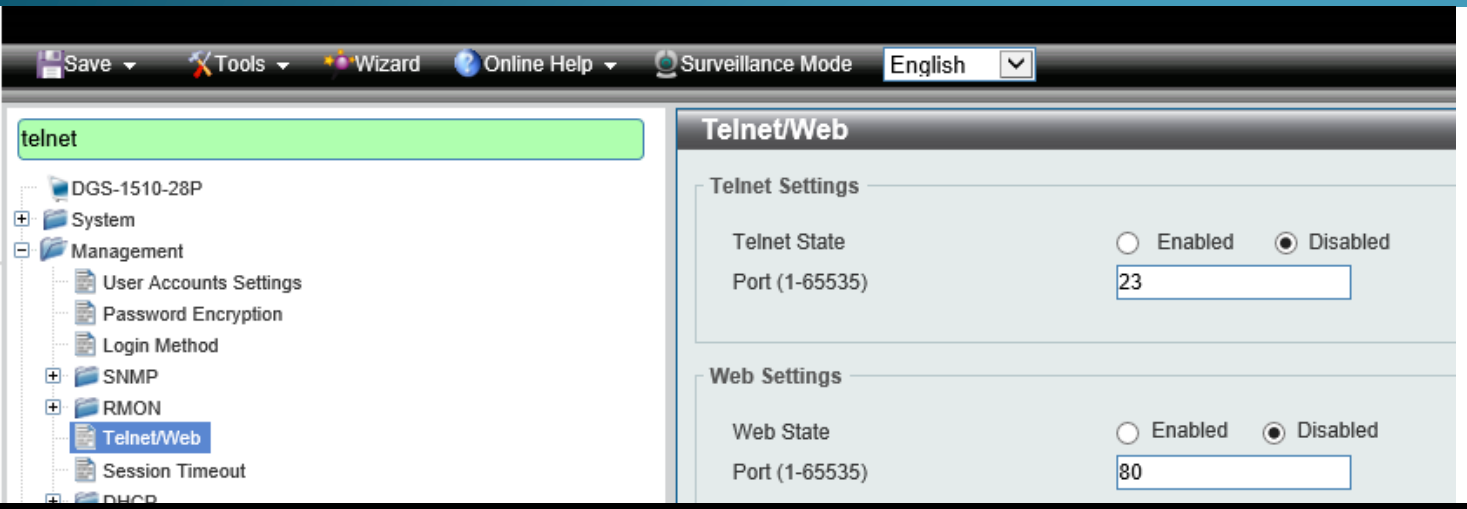
Konta użytkowników DGS-1510

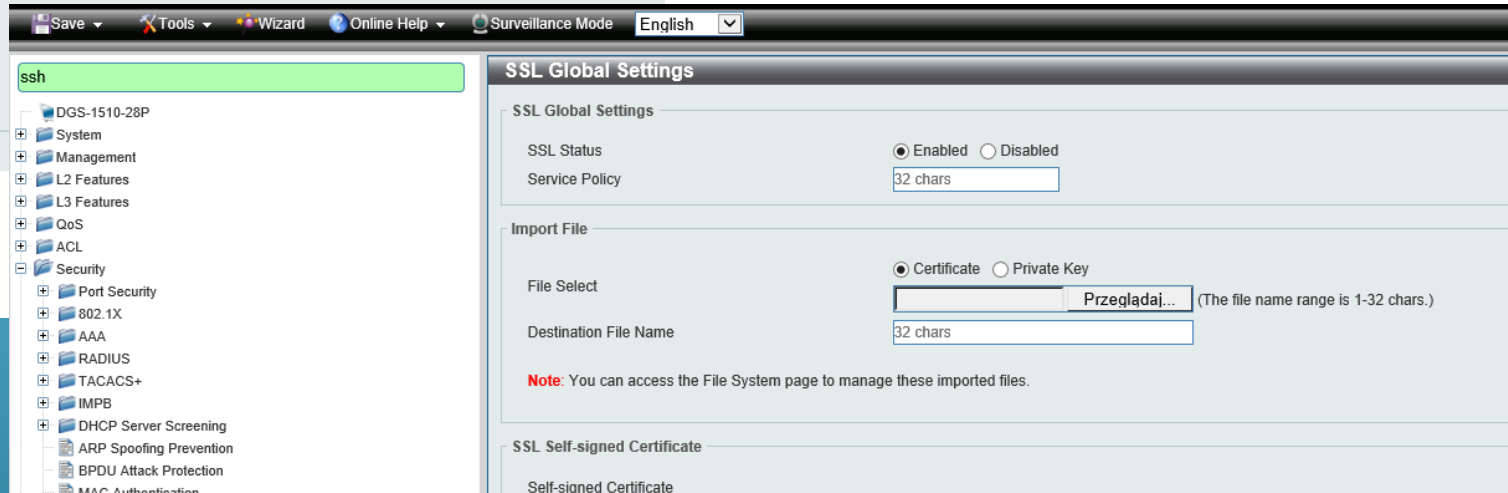




D-Link®
Building Networks for People

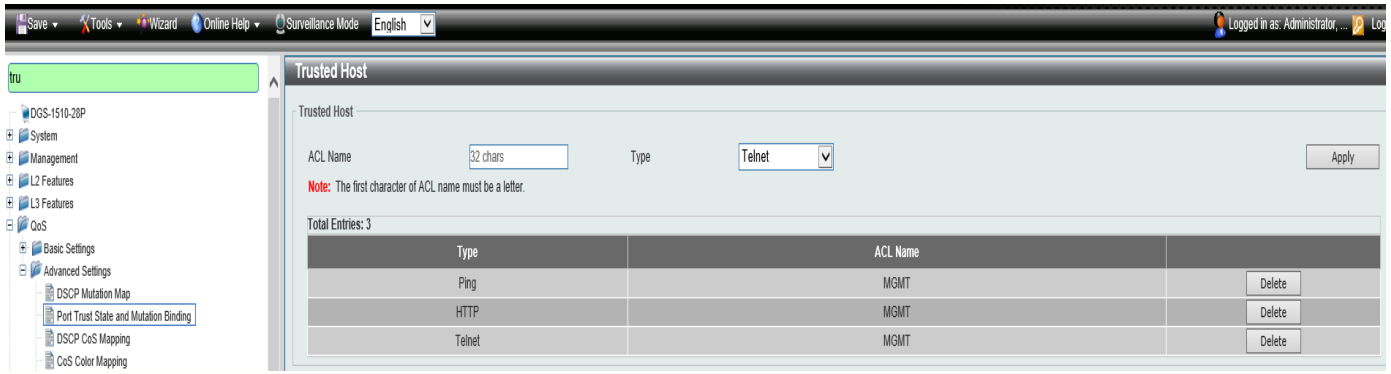
Bezpieczne zarządzanie DGS-1510





Ograniczony dostęp do przełącznika – Trusted Host

- Utwórz listę ACL dla wymaganego dostępu
- Podepnij listę ACL do danego interfejsu zarządzającego



Access to the switch only from Vlan 1 and WAN side. (Limit Access from Vlan 2 and Vlan3)
[Topology]
PC1(192.168.1.100)----(P1) **DGS-1510** (P2) ---- PC2 (192.168.2.100)
PC3(192.168.3.100)----(P3)

Interface Vlan1: 192.168.1.1
Interface Vlan2: 192.168.2.1
Interface Vlan3: 192.168.3.1

ip access-list MGMT 1
10 deny 192.168.2.1 0.0.0.255 any
20 deny 192.168.3.1 0.0.0.255 any
30 permit any any
line telnet
access-class MGMT
login local
end
config t
line ssh
access-class MGMT
exit
endconfig t
ip http access-class MGMT
ip https access-class MGMT

D-Link®
Building Networks for People

Rodzaje ataków w sieciach L2

Rodzaj Ataku	Opis	Zapobieganie
MAC Layer Attacks		
MAC Address Flooding Przeładowanie tablicy MAC	Zalanie przełącznika ramkami z różnymi adresami source MAC i przeładowanie tablicy MAC przełącznika, brak możliwości nauki nowych adresów MAC i w konsekwencji przekazywanie ramek typu unicast na wszystkie porty.	Port security. Storm Control
VLAN Attacks		
Ataki pomiędzy urządzeniami w tym samym Vlanie	Urządzenia z tego samego Vlanu mogą wymagać separacji względem siebie w celu uniknięcia możliwości komunikacji. Przypadek spotykany w sieciach dostawców lub w sieciach z portami współdzielonymi	Private Vlan Assymetric Vlan Traffic Segmentation
Pętle w sieci		
Pętle w warstwie L2 na portach klienckich	Utworzenie pętli na portach klienckich, poprzez połaczenie dwóch portów na tym samym przełączniku, lub podłączenie na porcie przełącznika innego przełącznika/Huba z pętlą poniżej. Na skutek pętli w sieci, cały segment sieci LAN z pętlą staje się nieużyteczny, brak komunikacji jak również brak dostępu do urządzeń aktywnych na ich interfejsie IP	STP/RSTP Loopback Detection

Rodzaje ataków w sieciach L2

Rodzaj Ataku	Opis	Zapobieganie
Spoofing Attacks		
DHCP Starvation and DHCP Spoofing (blokowanie serwera DHCP lub podszywanie sie pod serwer)	Atakujący może doprowadzić do wyczerpania się puli adresów na serwerze DHCP poprzez wysyłanie dużej ilości zapytań DHCP jak również podszyć się pod nasz serwer i rozdawać niepoprawną adresacje.	DHCP snooping. DHCP server screening
Spanning-tree Compromises Podszywanie się pod Root Bridge poprzez fałszywe ramki BPDU	Atakujący może dostarczyć do sieci sfałszowane ramki BPDU z informacją o błędnym przełączniku root, przez co doprowadzić do zmian w topologii sieci.	Root Guard BPDU protection
Podszywanie się pod konkretny adres MAC	Atakujący może sfałszować swój adres MAC, przez co przełącznik wskutek błędnego wprowadzenia adresu do tablicy MAC może przekazywać ramki dedykowane do konkretnego hosta na niepoprawny port	Port Security IMPB+DHCP Snooping
Address Resolution Protocol (ARP) Spoofing Fałszowanie pakietów ARP w sieci	Atakujący odpowiada fałszywym pakietem ARP reply na wysłane z sieci zapytanie ARP przez co powoduje błędne odwzorowanie w tablicy ARP u pytającego hosta, podszywając się pod hosta docelowego i przekierowując całych dedykowany do niego ruch na siebie	Dynamic ARP Inspection (DAI), DHCP snooping ARP Spoofing Prevention

Komunikacja w sieci L2 - przełączniki

Przełącznik sieciowy - urządzenie łączące segmenty sieci komputerowej pracujące głównie w drugiej warstwie modelu OSI (łącza danych), jego zadaniem jest przekazywanie ramek między segmentami sieci z doborem portu przełącznika, na który jest przekazywana. Przełączniki L2 działają w oparciu o adresy MAC w ramce Ethernet

Główne funkcje przełącznika:

- Learning - uczenie się i wypełnianie tablicy MAC na podstawie otrzymywanych ramek na danym porcie przełącznika, realizowane na podstawie źródłowego adresu MAC
- Flooding – przekazywanie ramek typu broadcast, unknown unicast na wszystkie porty przełącznika z pominięciem portu na którym ramka została otrzymana, funkcja umożliwiająca komunikację pomiędzy urządzeniami bez odwzorowań w tablicy MAC przełącznika
- Forwarding –Przekazywanie ramek do odpowiedniego portu przełącznika na podstawie docelowego MAC adresu, ramki unicast ze znanym adresem docelowym MAC są przekazywane tylko do konkretnego portu odbiorcy
- Filtering – Przekazywanie ramek tylko do portu na którym widnieje docelowy adres MAC ramki, brak możliwość podsłuchania transmisji unicastowej na innych portach przełącznika
- Aging – Podtrzymywanie i usuwanie adresów MAC z tablicy przełącznika na podstawie liczników.

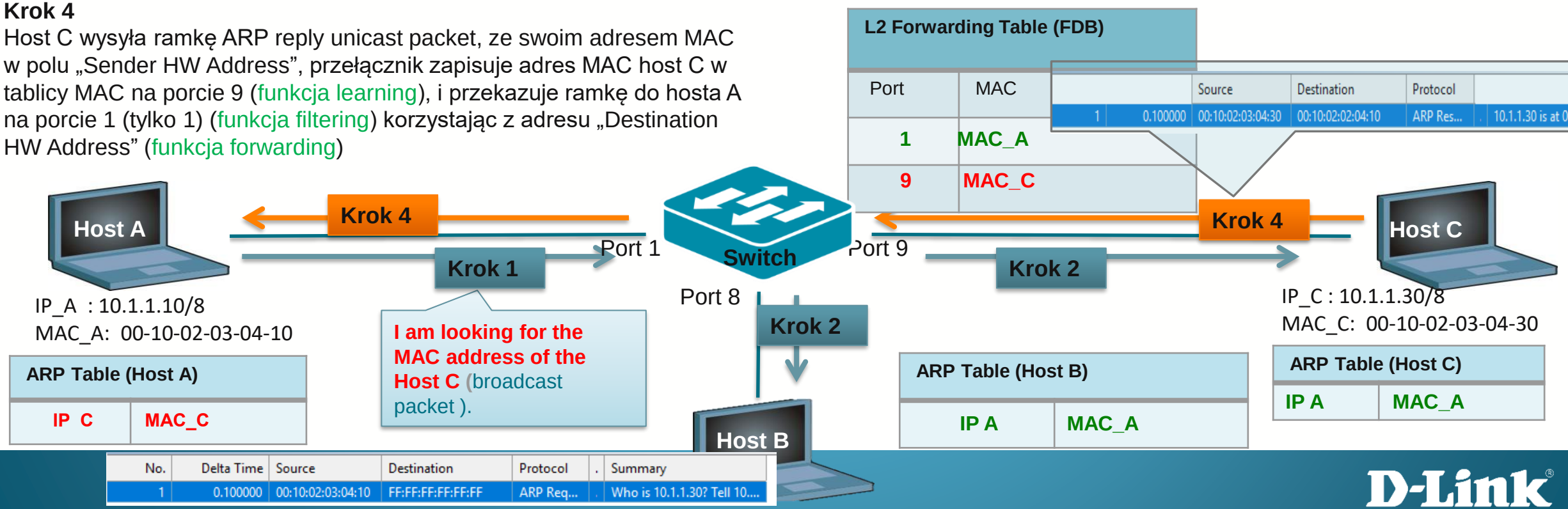
Komunikacja na przełączniku L2
Scenariusz: Host A z Host B

Krok 1.
Host A sprawdza swoją tablicę ARP czy posiada MAC adres hosta C.
Jako że tablica ARP hosta A nie posiada wpisu z MAC adresem hosta C, host A wysyła pakiet ARP request, w celu poznania adresu MAC hosta C.

Krok 2.
Przełącznik otrzymuje pakiet ARP typu broadcast, odczytuje z niego MAC adres źródłowy i zapisuje go w swojej tablicy MAC (funkcja learning), jako że jest to pakiet rozgłoszeniowy przekazuje go na wszystkie porty z wyjątkiem portu z którego pakiet otrzymał (funkcja flooding)

Krok 3
Ramka dociera do hostów B i C natomiast tylko host C odpowiada (adres IP w zapytaniu ARP), host B ignoruje ramkę

Krok 4
Host C wysyła ramkę ARP reply unicast packet, ze swoim adresem MAC w polu „Sender HW Address", przełącznik zapisuje adres MAC host C w tablicy MAC na porcie 9 (funkcja learning), i przekazuje ramkę do hosta A na porcie 1 (tylko 1) (funkcja filtering) korzystając z adresu „Destination HW Address" (funkcja forwarding)

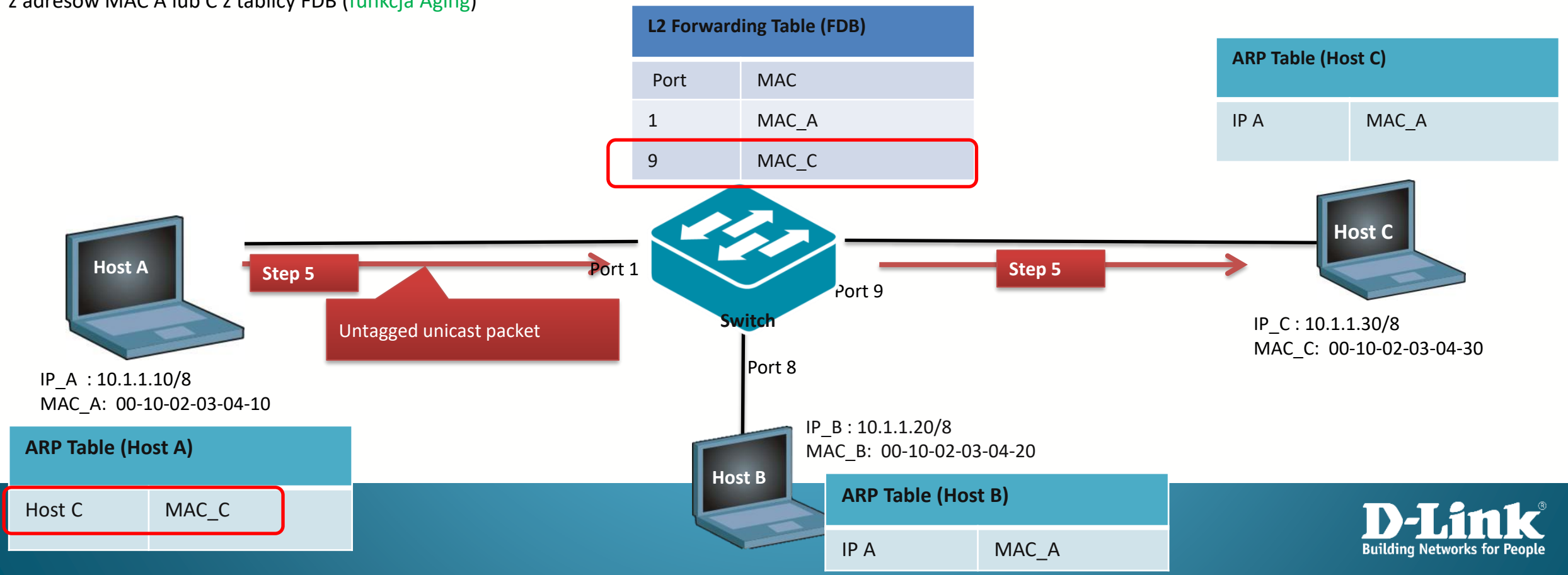


D-Link
Building Networks for People

Scenariusz: Host A z Host B cd

Krok 5
Jako że host A zna już adres MAC hosta C może wysłać do niego bezpośrednio zaadresowany pakiet

Krok 6
Przełącznik dostarcza pakiet bezpośrednio do portu na którym jest host C na podstawie zbudowanej tablicy MAC i informacji DMAC z nagłówka pakietu
Od tego mementu możliwa jest komunikacja dwustronna na portach 1 i 9 z wykorzystaniem funkcji filtering aż do momentu usunięcia któregoś z adresów MAC A lub C z tablicy FDB (funkcja Aging)



D-Link
Building Networks for People

Port security

- Każdy przełącznik posiada określony rozmiar tablicy MAC
- Pakiety unicast są przekazywane tylko na port na którym znajduje się docelowy MAC adres z otrzymanej ramki
- Pakiety broadcast, unknown unicast przekazywane są na wszystkie porty
- W przypadku zapełnienia tablicy MAC kolejne, wysyłane pakiety Unicast przesyłane są na wszystkie porty - brak funkcji filtrowania

Potencjalny atak polegający na zalaniu przełącznika i wypełnienie jego tablicy MAC może skutkować wyciekiem danych w sieci lokalnej i spowolnieniem całej sieci

Port Security ma na celu:

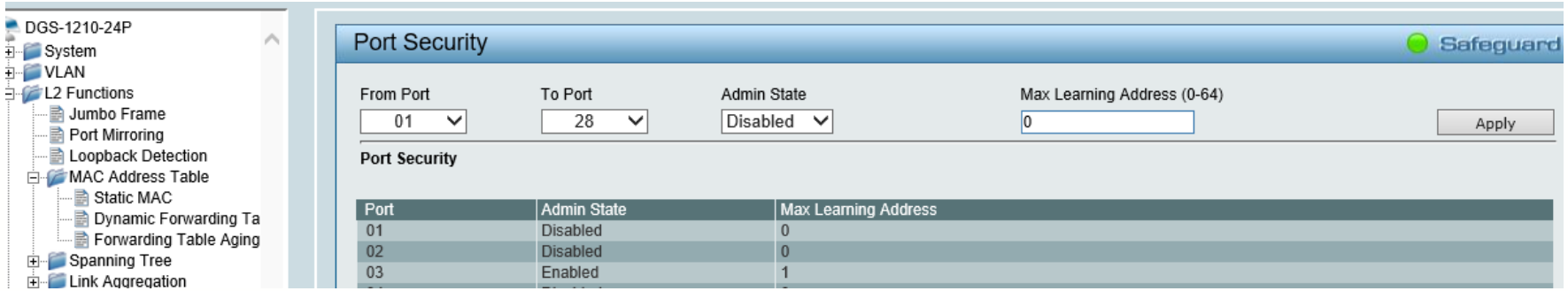
- Uniemożliwić zapisywanie adresów MAC na danym porcie poza określony przez administratora próg
- Odrzucanie wszystkich przychodzących ramek poza określonym progiem
- Zdefiniowanie konkretnych adresów MAC na konkretnym porcie
- Poinformowanie administratora o próbie ataku w postaci loga systemowego lub SNMP Trap

Ograniczenia Port Security:

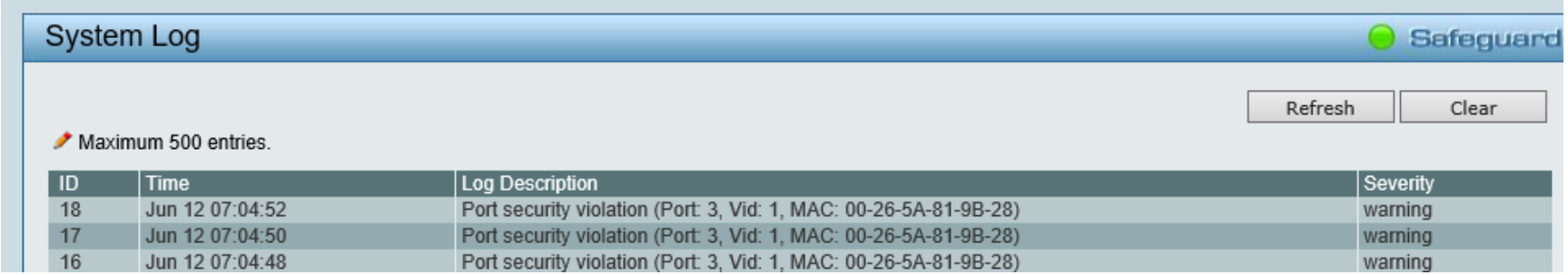
- IMPB
- 802.1X
- Link Aggregation

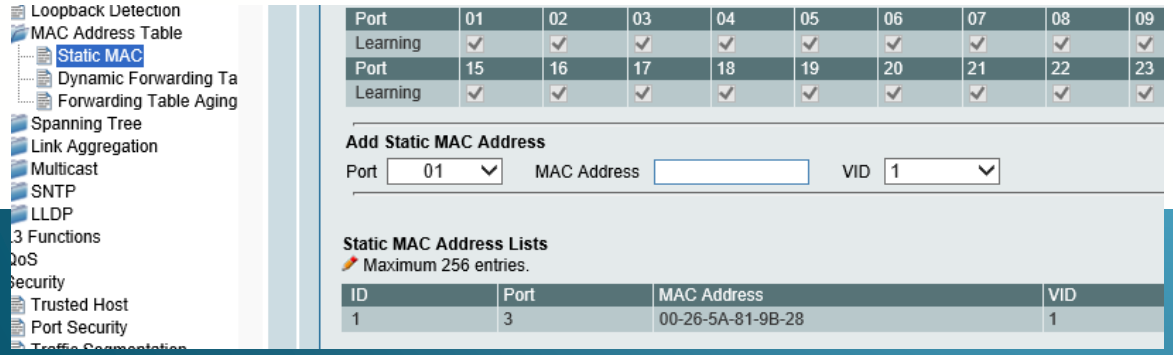
Port Security DGS-1210

Włącz Port Security na danym porcie i ustaw maksymalną liczbę dopuszczalnych MAC Adresów



Podłączenie większej ilości adresów MAC od zdefiniowanej, generuje Log o naruszeniu Port Security i blokuje ruch z tych adresów



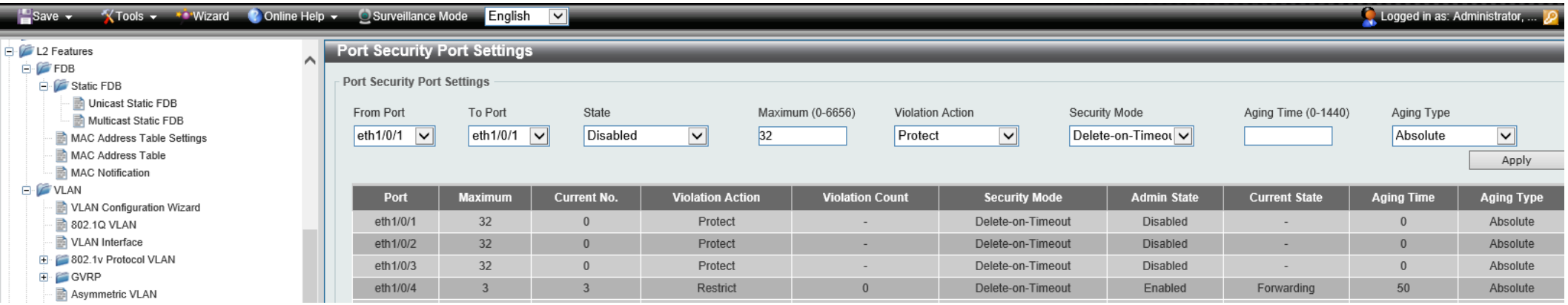


- W celu zdefiniowania konkretnych adresów MAC na danym porcie, utwórz statyczny wpis w tablicy MAC.
- Wpis statyczny ma wyższy priorytet niż mechanizm Por Security

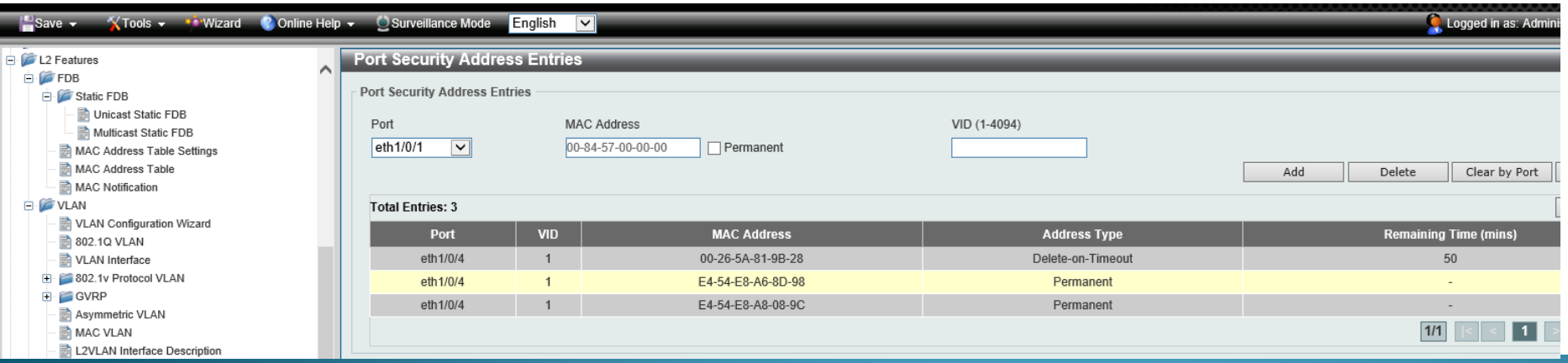
D-Link®
Building Networks for People

Port Security DGS-1510

- Możliwość skonfigurowania akcji dla naruszenia mechanizmu na porcie
- Wybranie trybu zabezpieczenia: Delete on Timeout lub Permanent



- Opcja dodawania statycznych adresów MAC dla danych portów (adresy statyczne wchodzą w pulę liczby maksymalnie obsługiwanych adresów na porcie)



D-Link®
Building Networks for People

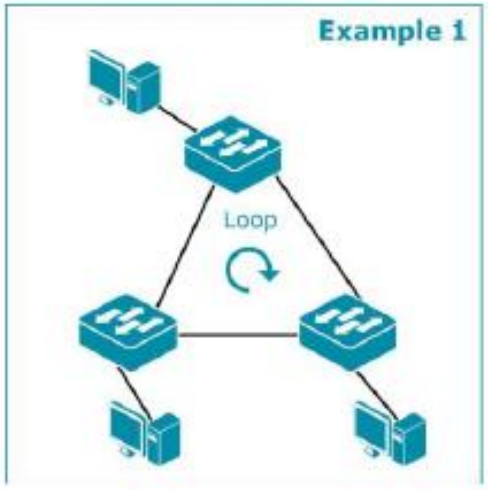
Port Security DGS-1510

```
Switch#show port-security interface e1/0/4

 D:Delete-on-Timeout  P:Permanent
 Interface     Max  Curr  Violation     Violation   Security Admin  Current
 No.           No.   No.    Act.          Count        Mode  State   State
 ------------ ----- ----- -------- -------------------- -- -------- ------------
 eth1/0/4      2     2     Restrict 1491                 D  Enabled  Forwarding

Switch#show po
Switch#show port-security address

 Interface    VLAN ID MAC Address       Address Type      Remaining Time
                                                              (mins)
 ------------ ------- ----------------- ----------------- -------------
 eth1/0/4      1       E4-54-E8-A6-8D-98 Permanent         -
 eth1/0/4      1       E4-54-E8-A8-08-9C Permanent         -

 Total Entries: 2

Switch#show logging

Total number of buffered messages:10000

#43654 2000-01-09 23:43:42 WARN(4) MAC address 00-26-5A-81-9B-28 causes port sec
urity violation on Ethernet1/0/4.
#43653 2000-01-09 23:42:34 WARN(4) MAC address 00-26-5A-81-9B-28 causes port sec
urity violation on Ethernet1/0/4.
```

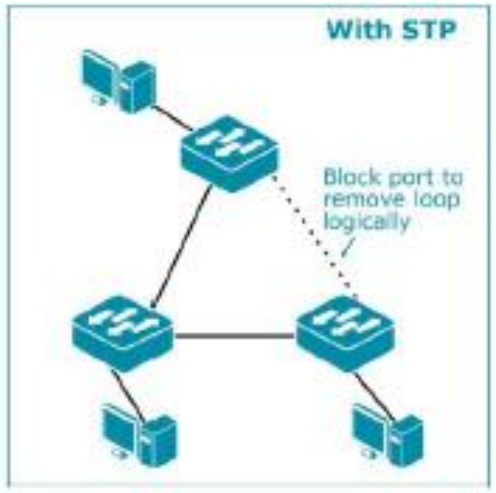
```
Switch#show port-security interface e1/0/4

 D:Delete-on-Timeout  P:Permanent
 Interface     Max  Curr  Violation     Violation   Security Admin  Current
 No.           No.   No.    Act.          Count        Mode  State   State
 ------------ ----- ----- -------- -------------------- -- -------- ------------
 eth1/0/4      2     2     Shutdown -                    D  Enabled  Err-disabled

Switch#show logging

Total number of buffered messages:10000

#43658 2000-01-09 23:46:58 WARN(4) MAC address 00-26-5A-81-9B-28 causes port security vio
lation on Ethernet1/0/4.
#43657 2000-01-09 23:46:58 WARN(4) Port <1/0/4> enters error disable state due to Port Se
curity violation
```

Pętle w sieciach L2 – Loopback detection

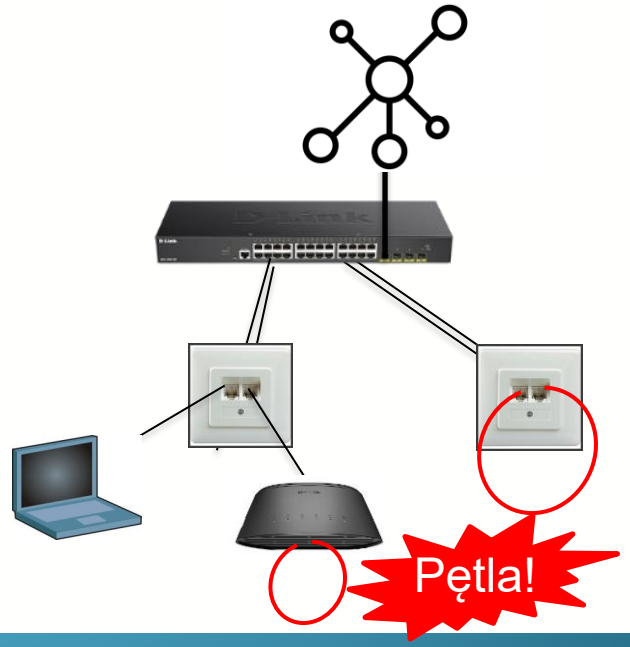
- Pętle w sieciach L2, powstają najczęściej „przez przypadek” na skutek źle połączonej infrastruktury sieciowej.
- Brak wbudowanego mechanizmu unikania pętli w warstwie 2
- Jeden pakiet typu broadcast, multicast, unknown unicast może zablokować cała sieć.
- Dążymy do nadmiarowej topologii fizycznej przy zachowaniu pętli w topologii logicznej.
- Nie zawsze kontrolujemy połączenia do klientów gdzie może pojawić się pętla na skutek podłączenia niepożądanych urządzeń.
- W większych sieciach (kilka, kilkanaście przełączników), trudno szybko znaleźć źródło pętli.
- Pętla w jednym segmencie sieci (na jednym urządzeniu) powoduje przerwę pracy całej sieci L2 (domeny rozgłoszeniowej)
- Różne protokoły unikania pętli (dla różnych zastosowań): STP, RSTP, MSTP, ERPS, Loopback Detection, LACP



Topologia fizyczna



Topologia logiczna



Loopback Detection

Zabezpiecza przed:

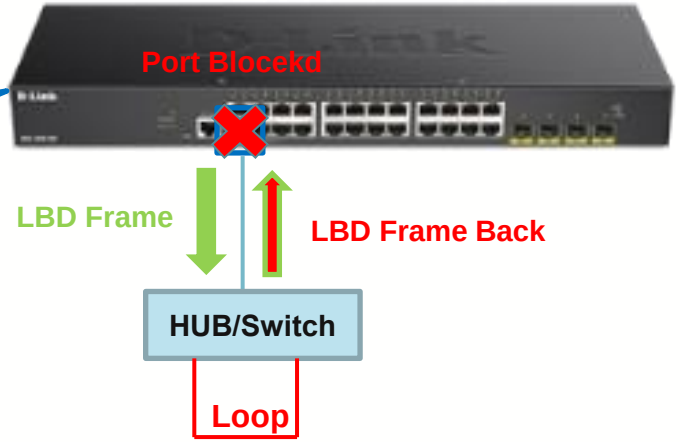
- ✓ Pętlą na pojedynczym porcie przełącznika (przy pomocy dodatkowego urządzenia)
- ✓ Pętlą pomiędzy dwoma portami

- Funkcjonalność niezależna od protokołów Spanning Tree – Nie mogą działać jednocześnie na tym samym porcie
- Może działać na zasadzie port based lub vlan based

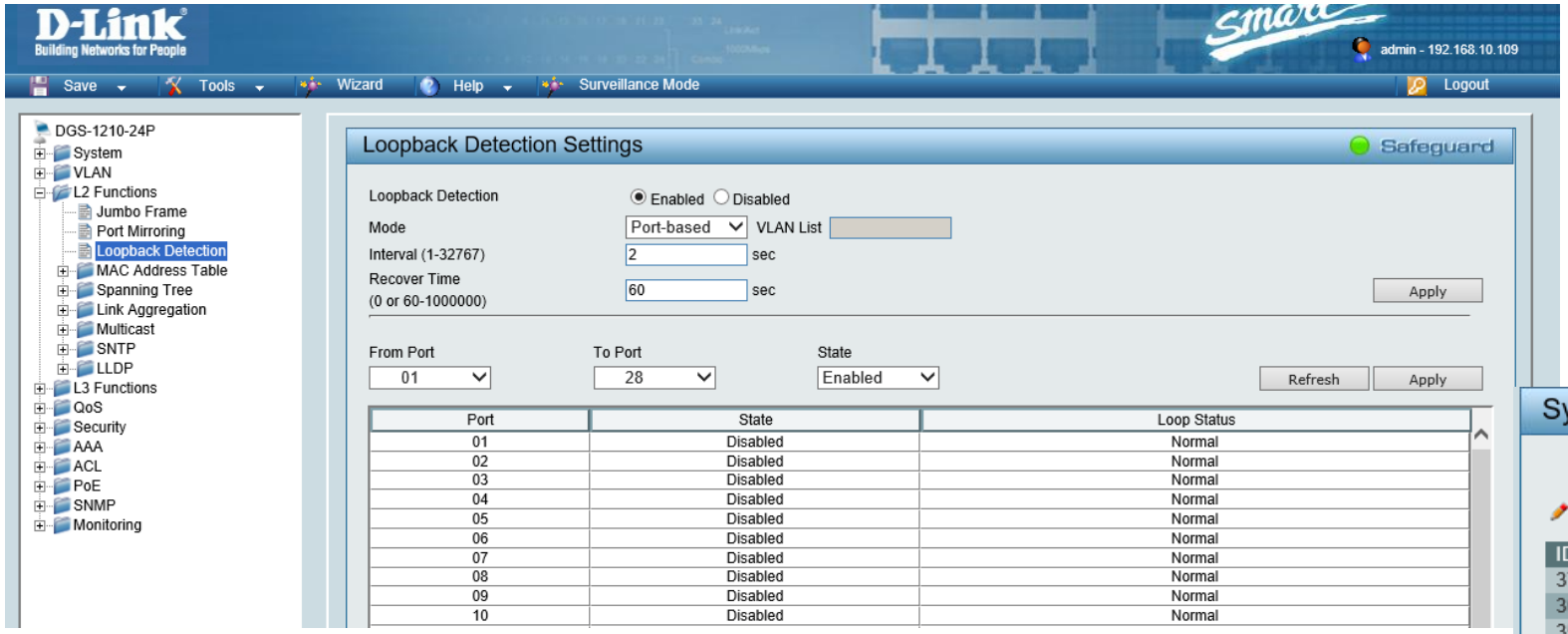
Zasada działania:

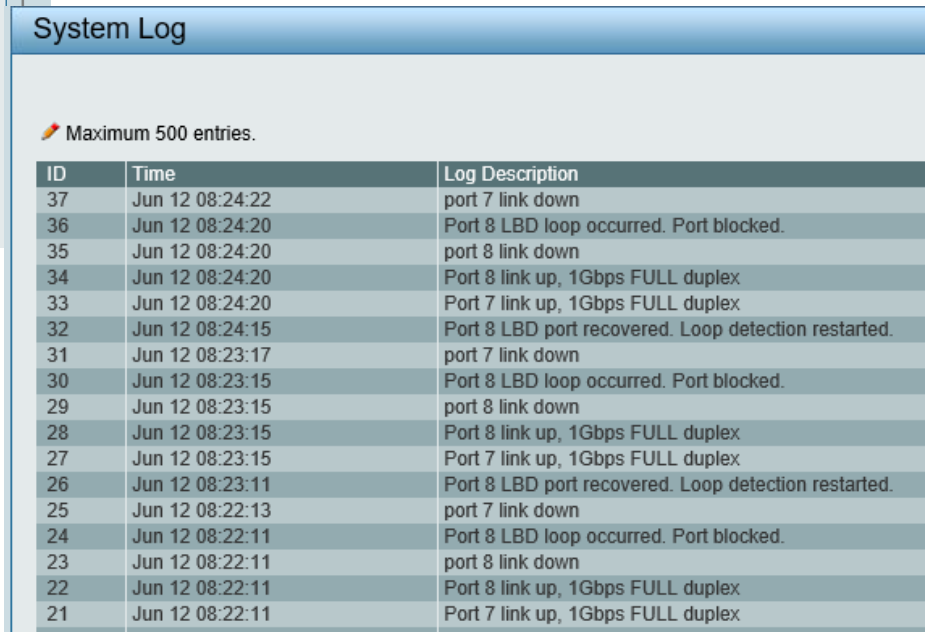
1. Wysyłanie zdefiniowanej ramki kontrolnej typu multicast lub broadcast na porcie z włączonym loopback detection.
2. Nasłuchiwanie czy ramka ta nie powróciła na tym samym lub innym porcie tego urządzenia.
3. Jeśli przełącznik odbierze taką ramkę na tych portach, port wysyłający taką ramkę zostaje zablokowany (RX/TX).
4. Otrzymujemy powiadomienie o takim zdarzeniu w logach
5. Możliwe automatyczne lub manualne przywrócenie tak wyłączonego portu (errdisable)

```
Switch#
#43662 2000-01-10 01:11:32 WARN(4) Port <1/0/11> enters error disable state due to Loopback Detection
#43663 2000-01-10 01:11:32 CRIT(2) Ethernet1/0/11 LBD loop occurred.
#43664 2000-01-10 01:11:32 WARN(4) Port <1/0/9> enters error disable state due to Loopback Detection
#43665 2000-01-10 01:11:32 CRIT(2) Ethernet1/0/9 LBD loop occurred.
Switch#show logging
```

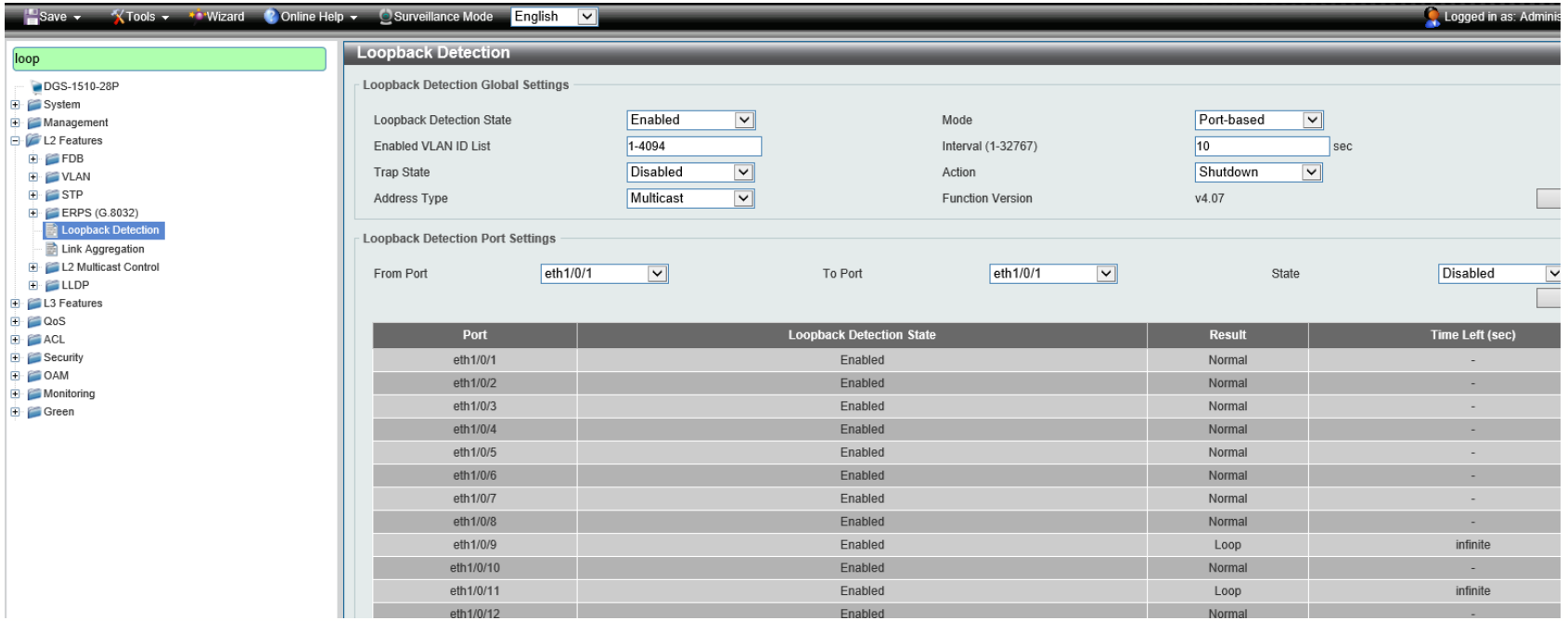


Loopback Detection - Konfiguracja





Loopback Detection - Konfiguracja

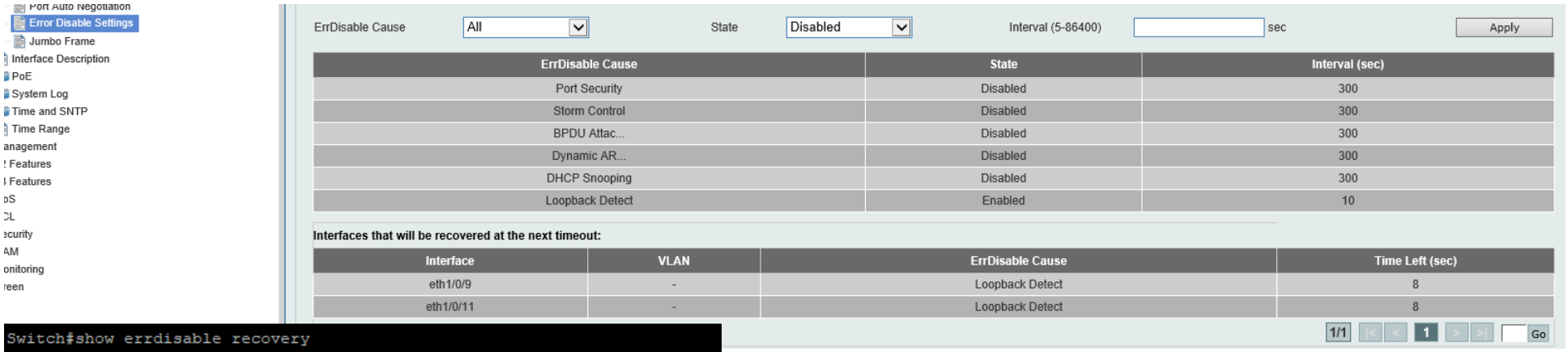


Port	Loopback Detection State	Result	Time Left (sec)
eth1/0/1	Enabled	Normal	-
eth1/0/2	Enabled	Normal	-
eth1/0/3	Enabled	Normal	-
eth1/0/4	Enabled	Normal	-
eth1/0/5	Enabled	Normal	-
eth1/0/6	Enabled	Normal	-
eth1/0/7	Enabled	Normal	-
eth1/0/8	Enabled	Normal	-
eth1/0/9	Enabled	Loop	infinite
eth1/0/10	Enabled	Normal	-
eth1/0/11	Enabled	Loop	infinite
eth1/0/12	Enabled	Normal	-

```
Switch#
#43662 2000-01-10 01:11:32 WARN(4) Port <1/0/11> enters error disable state due to Loopback Detection
#43663 2000-01-10 01:11:32 CRIT(2) Ethernet1/0/11 LBD loop occurred.
#43664 2000-01-10 01:11:32 WARN(4) Port <1/0/9> enters error disable state due to Loopback Detection
#43665 2000-01-10 01:11:32 CRIT(2) Ethernet1/0/9 LBD loop occurred.
Switch#show logging
```

D-Link®
Building Networks for People

Loopback Detection - Przywracanie portu

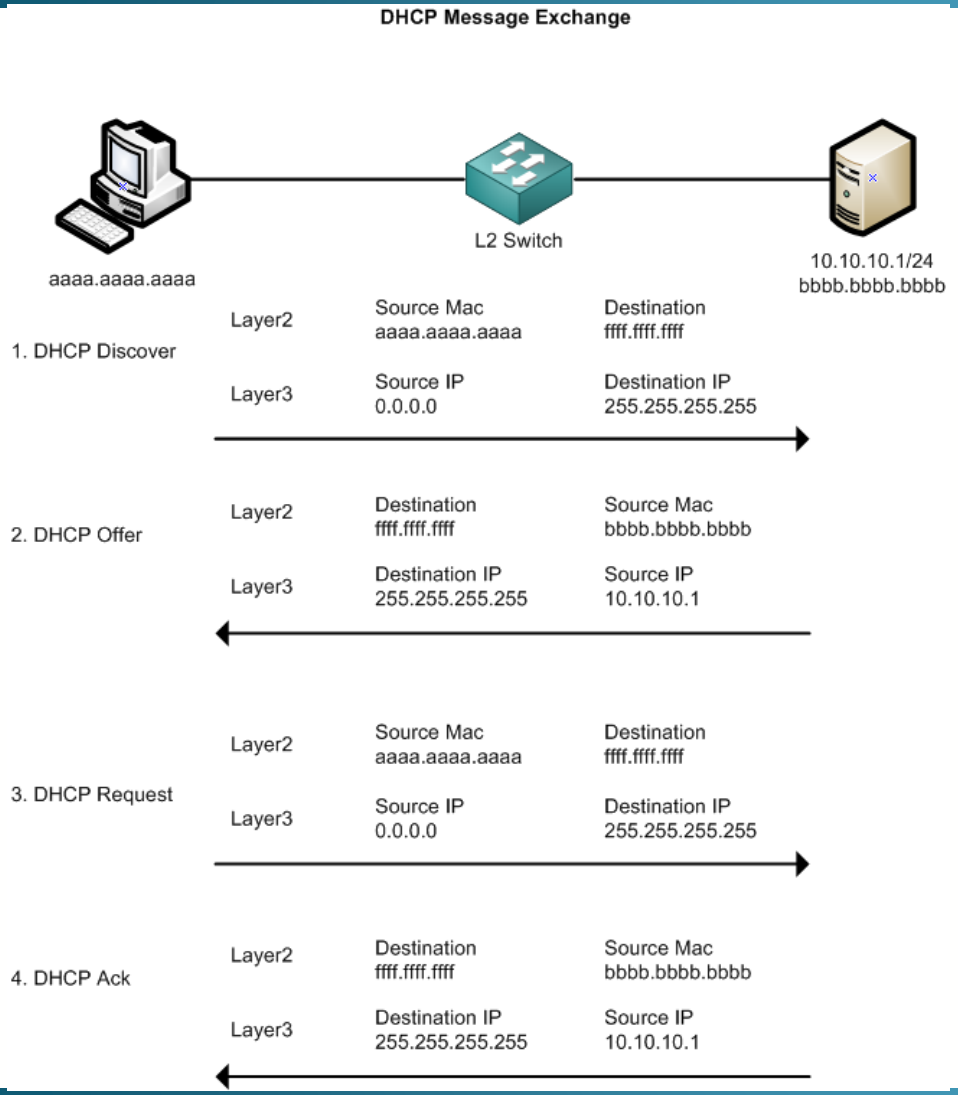



```
Switch#show errdisable recovery

ErrDisable Cause                  State         Interval
--------------------------------  ------------  -------------
Port Security                     disabled      300 seconds
Storm Control                     disabled      300 seconds
BPDU Attack Protection            disabled      300 seconds
Dynamic ARP Inspection            disabled      300 seconds
DHCP Snooping                     disabled      300 seconds
Loop Detection                    enabled       10 seconds

Interfaces that will be recovered at the next timeout:

Interface    Errdisable Cause                   Time left(sec)
---------    --------------------------------   --------------
eth1/0/9     Loop Detection                     4
eth1/0/11    Loop Detection                     4
```

```
#43666 2000-01-10 01:13:22 WARN(4) Port <1/0/9> leaves the error disable state which is previously caused by Loopback Detection
#43667 2000-01-10 01:13:22 CRIT(2) Ethernet1/0/9 LBD loop recovered.
#43668 2000-01-10 01:13:22 WARN(4) Port <1/0/11> leaves the error disable state which is previously caused by Loopback Detection
#43669 2000-01-10 01:13:22 CRIT(2) Ethernet1/0/11 LBD loop recovered.
#43670 2000-01-10 01:13:32 WARN(4) Port <1/0/11> enters error disable state due to Loopback Detection
#43671 2000-01-10 01:13:32 CRIT(2) Ethernet1/0/11 LBD loop occurred.
#43672 2000-01-10 01:13:32 WARN(4) Port <1/0/9> enters error disable state due to Loopback Detection
#43673 2000-01-10 01:13:32 CRIT(2) Ethernet1/0/9 LBD loop occurred.
#43674 2000-01-10 01:13:41 WARN(4) Port <1/0/11> leaves the error disable state which is previously caused by Loopback Detection
```

D-Link
Building Networks for People

Zagrożenia związane z DHCP



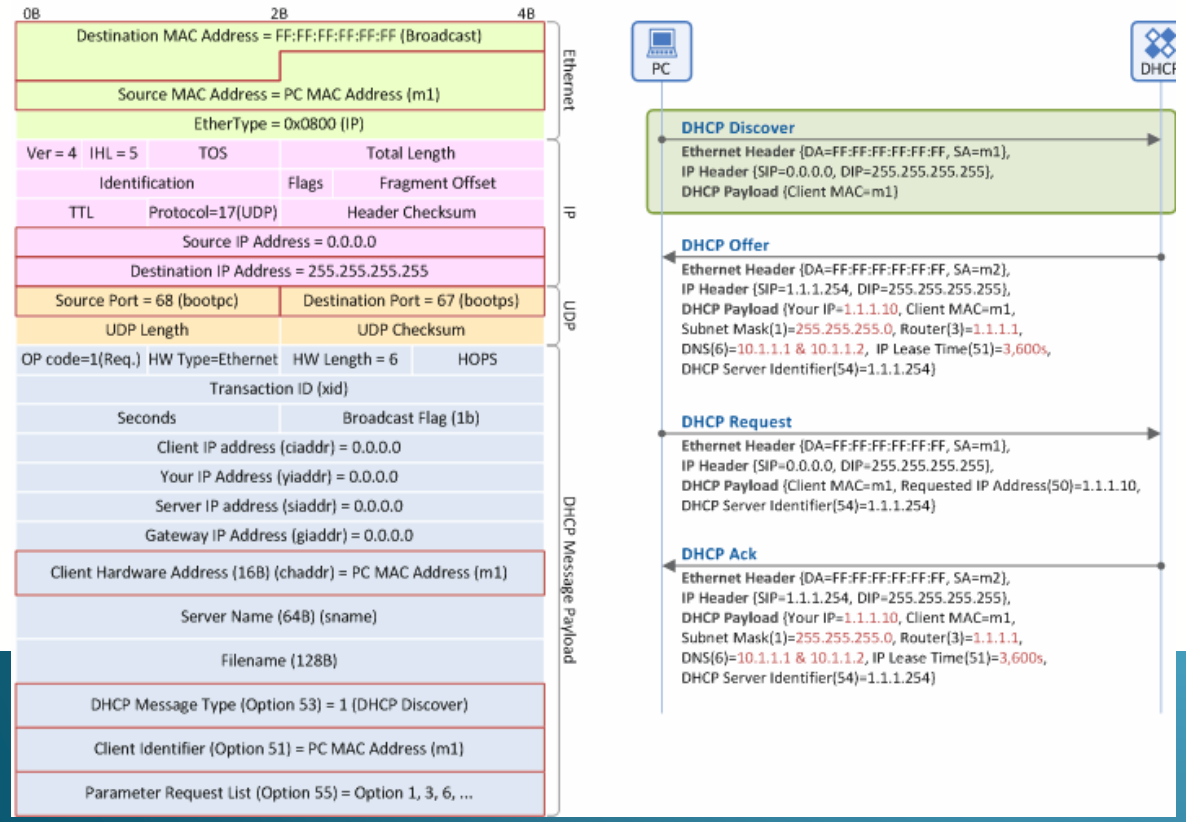
- Serwer DHCP ma za zadania w sposób dynamiczny i automatyczny przyznać adresacje IP wraz z dodatkowymi informacjami
- Standardowo serwer DHCP przyznaje: IPv4, maskę podsieci, adres bramy domyślnej, adresy serwerów DNS, informacje o czasie dzierżawy adresu
- Standardowo pakiety w ramach wymiany DHCP client-serwer to otwarta komunikacja typu broadcast
- Przełączniki L2 przekazują takie ramki na wszystkie porty co czyni tą komunikację łatwą do podsłuchania i podatną na ataki. ,
- Najczęściej urządzenia klienckie korzystają z protokołu DHCP do uzyskania adresacji
- Dzięki nasłuchiwaniu pakietów DHCP możemy dowiedzieć się dużo o samej sieci
- Zagrożenie dla bezpieczeństwa sieci w przypadku podłączenia nieautoryzowanego serwera DHCP
- Bałagan i problemy w komunikacji sieciowej przy podłączeniu osobnego serwera DHCP „przez przypadek”
- Główne typy ataków to atak typu Dos i atak typu MITM
- Można uniknąć zagrożenia dzięki mechanizmom DHCP Snooping, DHCP Server Screening.

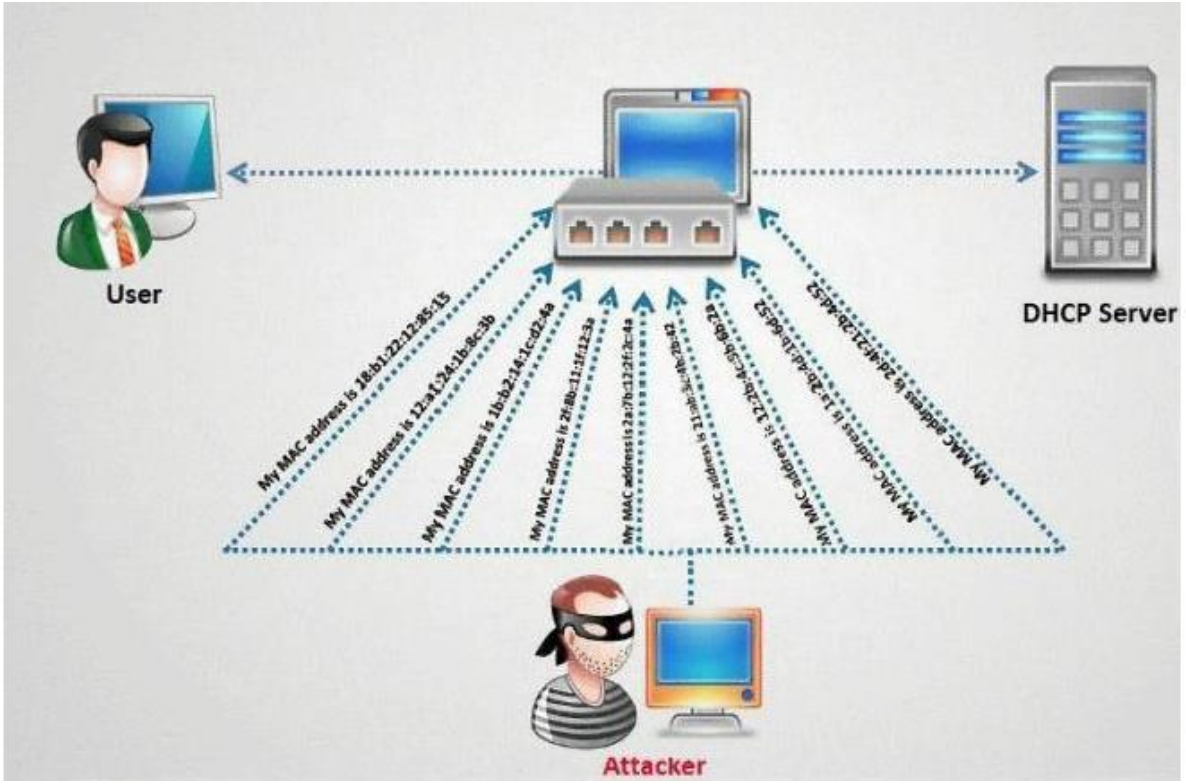
DHCP Starvation – DoS Attack

- Atakujący wysyła bardzo dużo zapytań do serwera DHCP (fałszując pakiety), przez co następuje wyczerpanie puli dostępnych adresów na serwerze.
- Usługa DHCP jest niedostępna dla innych „właściwych” klientów

Zapobieganie:

- ✓ **Port Security** z ograniczeniem liczby MAC adresów na porcie (tylko w przypadku wykorzystania innych adresów MAC przez atakującego)
- ✓ Ograniczenie zapytań DHCP na porcie – DHCP Snooping

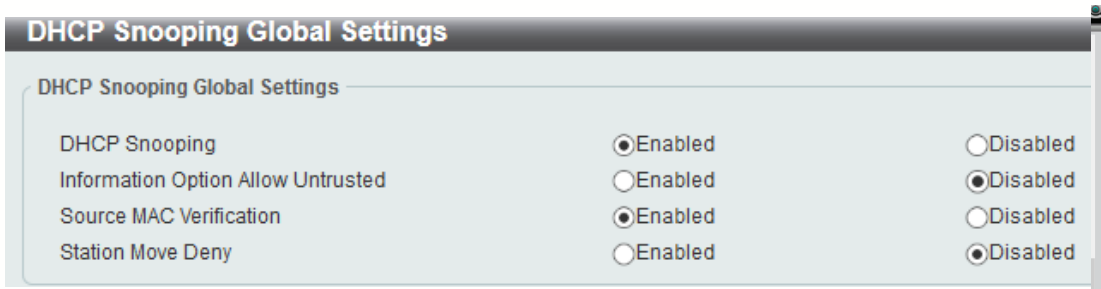




DHCP Snooping Limit Rate

- Ograniczenie pakietów DHCP na porcie klienckim.
- Przełącznik z włączonym DHCP snooping na porcie nasłuchuje pakietów DHCP i wykonuje odpowiednie akcje
- Opcja Limit Rate, ogranicza ilość dozwolonych pakietów DHCP na danym porcie do zdefiniowanej wartości (dhcp/sec)
- Po przekroczeniu progu port przechodzi w stan error disable, i otrzymujemy loga o tym zdarzeniu'

1. Włącz DHCP snooping globalnie
2. Włącz DHCP snooping na porcie
3. Określ liczbę dozwolonych pakietów DHCP na porcie



Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping verify mac-address

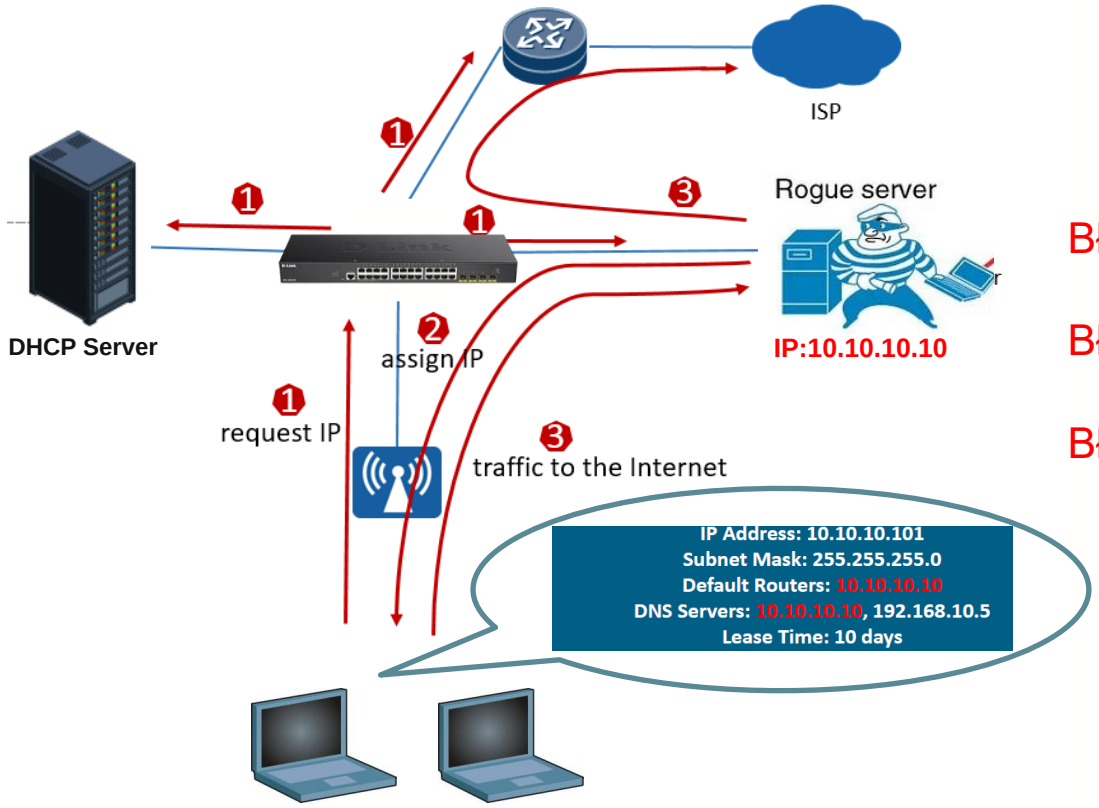
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# ip dhcp snooping limit rate 5

D-Link®
Building Networks for People

DHCP Spoofing Attack

- Zainstalowanie w sieci fałszywego serwera DHCP i alokacja niepoprawnych adresacji w sieci (skutek MITM)
- Podłączenie „przez przypadek” serwera DHCP, skutkiem czego może być brak dostępu do sieci na niektórych hostów

Co może zrobić atakujący jako serwer DHCP



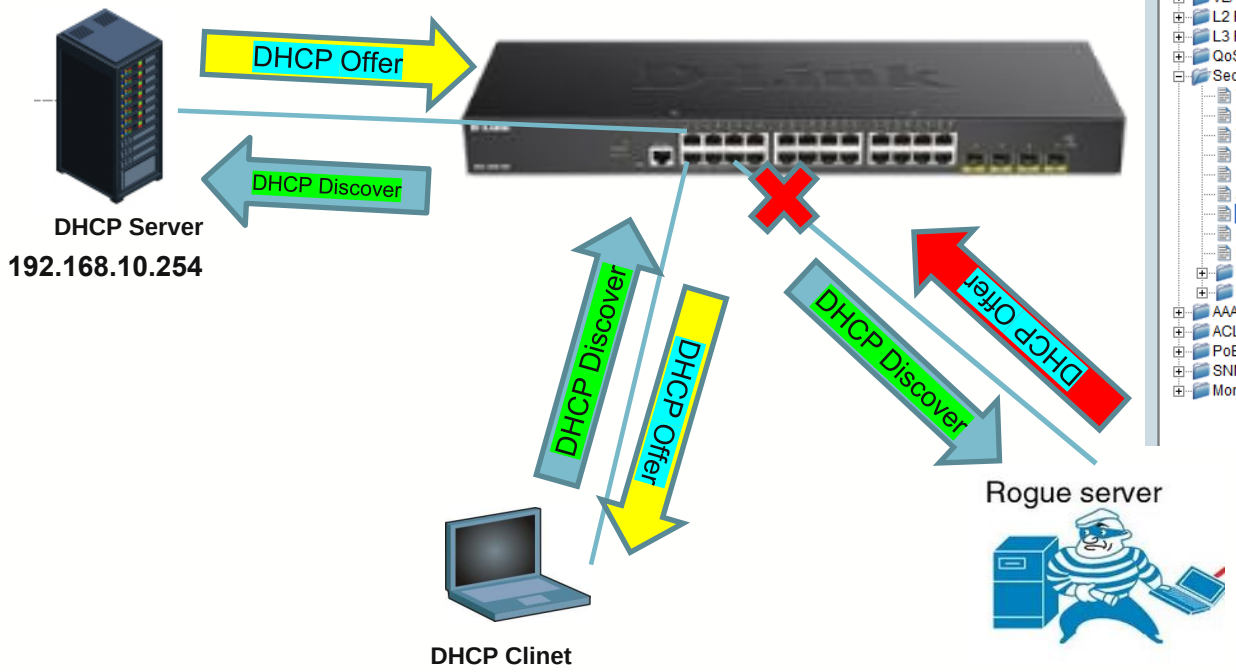
Błędny adres bramy domyślnej – Atakujący udaje bramę domyślną

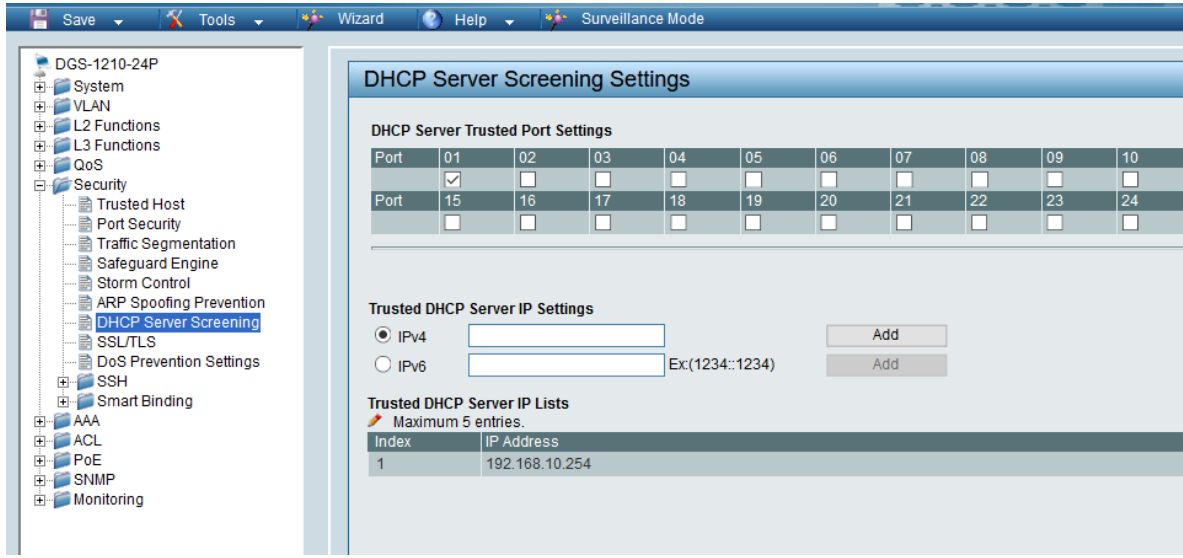
Błędny adres DNS – Atakujący udaje serwer DNS

Błędny adres IP – Atakujący powoduje DoS z błędnym adresem IP dla klienta

DHCP Server Screening

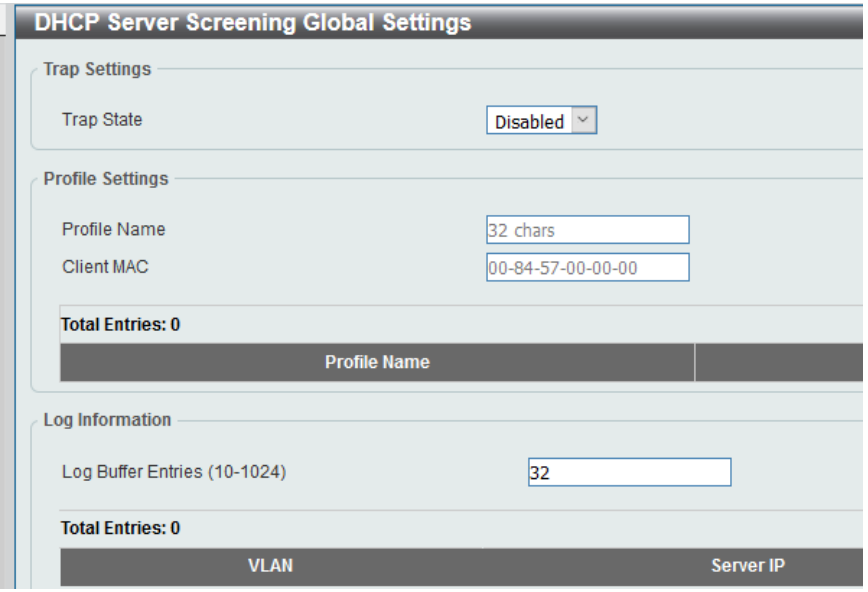
- Funkcja DHCP Server Screening pozwala na filtrowanie pakietów DHCP Server (DHCP Offer, DHCP Ack, DHCPNAK)
- Pakiety tego typu wysłane na port przełącznika z włączoną opcją DHCP Server Screening są filtrowane
- Możliwość skonfigurowania adresu IP serwera DHCP na porcie typu trust (zaufanym), tylko pakiety z tym adresem źródłowym będą przez port przekazywane

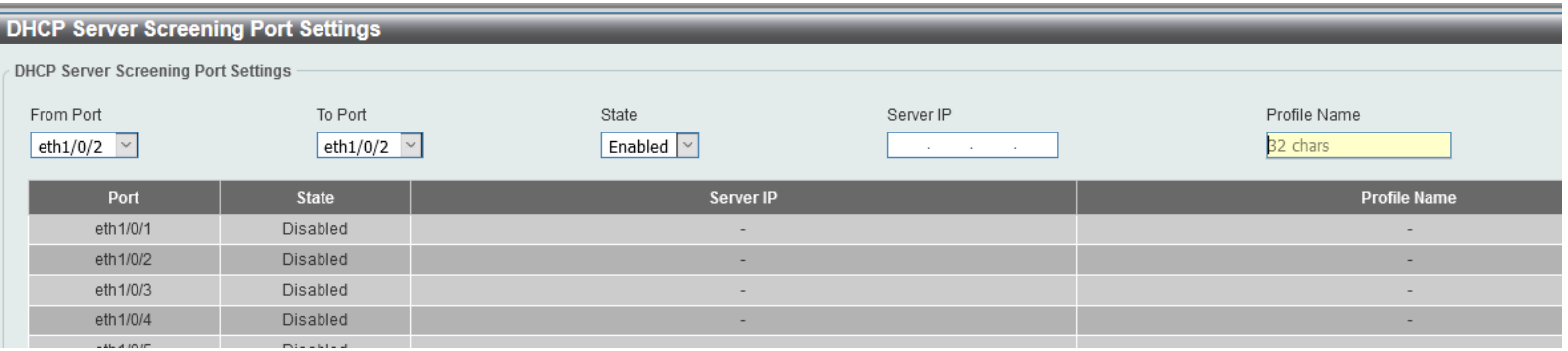




DHCP Server Screening –DGS-1510

Możliwość konfiguracji profili dla określonych MAC adresów klientów





D-Link®
Building Networks for People

DHCP Server Screening - konfiguracja

Sernario 1

[Topology]
DHCP Client---(p3)DGS-1510(p1)---L2 Switch---Rogue DHCP Server(MAC:F4-8C-EB-70-A6-00)
---Trust DHCP Server(MAC:00:AD:24:EC:AC:00)

*DHCP Client MAC 00-00-00-00-00-01
*Rogue DHCP Server IP 10.90.90.90
*Trust DHCP Server IP 10.90.90.89

[Command example]
config t
interface range ethernet 1/0/1
ip dhcp snooping server-screen **/enable server-screen on port**
ip dhcp snooping server-screen 10.90.90.89 **/configure trusted DHCP Server**
exit

==========

Above command is an example to block all untrusted DHCP Server's packet but only permit specific trusted DHCP Server's packet (Ex: 10.90.90.89)

[Verify]
Switch#show log

Total number of buffered messages: 47

#47 2000-01-01 00:05:08 WARN(4) Conflict IP was detected with this device (IP: 10.90.90.90, MAC: f4:8c:eb:70:a6:00, Interface: VLAN 1)

As we can see, rogue Server f4:8c:eb:70:a6:00 will be detected by server-screen

Sernario 2

[Topology]
DHCP Client---(p3)DGS-1510(p1)---L2 Switch---Rogue DHCP Server(MAC:F4-8C-EB-70-A6-00)
---Trust DHCP Server(MAC:00:AD:24:EC:AC:00)

*DHCP Client MAC 00-00-00-00-00-02
*Rogue DHCP Server IP 10.90.90.90
*Trust DHCP Server IP 10.90.90.89

To restrict that only specific servers are allowed to offer addresses to specific clients (In this case , just permit client 00-00-00-00-00-01 to get IP from DHCP Servr(10.90.90.89)

[Command]
config t
dhcp-server-screen profile TEST
based-on hardware-address 00-00-00-00-00-01 **// Assign permitted client's MAC**
exit

interface range ethernet 1/0/1
ip dhcp snooping server-screen **//Enable server-screen on port**
ip dhcp snooping server-screen 10.90.90.89 profile *TEST* **//Allow specific client to get IP from trusted DHCP**
exit

Switch#show ip dhcp server-screen log

Total log buffer size: 32

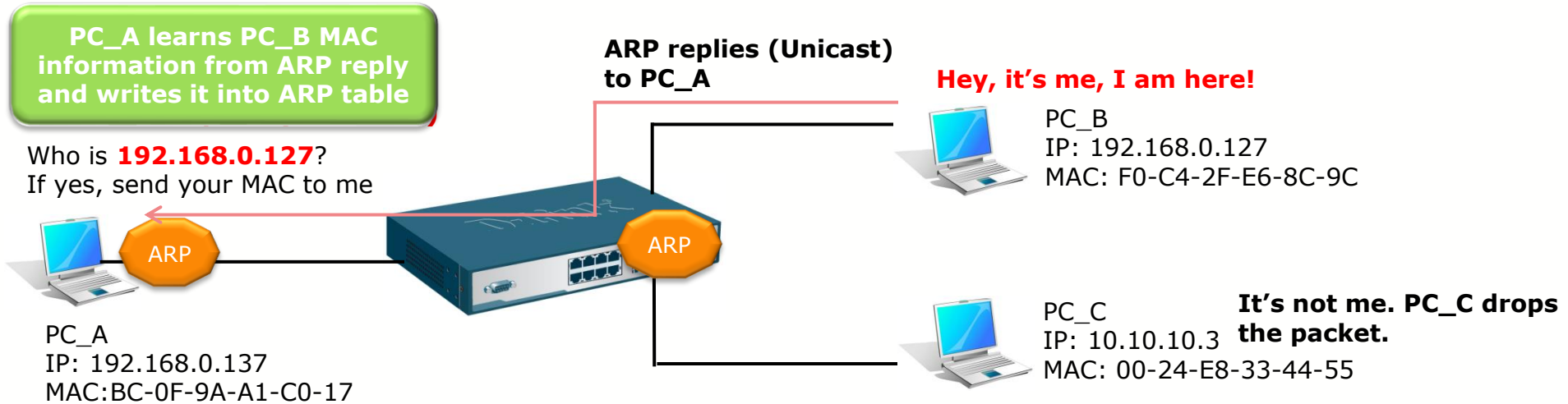
VLAN	Server IP	Client MAC	Occurrence
1	10.90.90.89	00-00-00-00-00-02	1:54:28, 2000-1-1

As we can see , Client 00-00-00-00-00-02 can be blocked by server-screening fuction

D-Link®
Building Networks for People

ARP Spoofing Attacks – zasada działania ARP

ARP spoofing – atak sieciowy w sieci Ethernet pozwalający atakującemu przechwytywać dane przesyłane w obrębie segmentu sieci lokalnej. Przeprowadzony tą metodą atak polega na rozsyłaniu w sieci LAN odpowiednio spreparowanych pakietów ARP zawierających fałszywe adresy MAC. W efekcie pakiety danych wysyłane przez inne komputery w sieci zamiast do adresata trafiają do osoby atakującej pozwalając jej na podsłuchiwanie komunikacji.



ARP Request

```
C:\Windows\system32>arp -a

Interface: 192.168.0.137 --- 0xc
  Internet Address      Physical Address      Type
  192.168.0.1           78-32-1b-6c-4f-58     dynamic
  192.168.0.127         f0-c4-2f-e6-8c-9c     dynamic
  192.168.0.177         6c-72-20-02-c6-df     dynamic
```

```
› Frame 748: 42 bytes on                                                    A64871-6CA8-4328-AC77-0B4D2BE468DA}, id 0
⌄ Ethernet II, Src: D-Li
  › Destination: Broadca
  › Source: D-LinkIn_a1:
    Type: ARP (0x0806)
⌄ Address Resolution Pro
    Hardware type: Ether
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: D-LinkIn_a1:c0:17 (bc:0f:9a:a1:c0:17)
    Sender IP address: 192.168.0.137
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.127
```

ARP Reply

```
› Frame 758: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{4FA64
⌄ Ethernet II, Src: HuaweiDe_e6:8c:9c (f0:c4:2f:e6:8c:9c), Dst: D-LinkIn_a1:c0:17 (bc:0f:9a:a1:c0:17)
  › Destination: D-LinkIn_a1:c0:17 (bc:0f:9a:a1:c0:17)
  › Source: HuaweiDe_e6:8c:9c (f0:c4:2f:e6:8c:9c)
    Type: ARP (0x0806)
  › Trailer: 00000000000000000000000000019a9dd9b
⌄ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: HuaweiDe_e6:8c:9c (f0:c4:2f:e6:8c:9c)
    Sender IP address: 192.168.0.127
    Target MAC address: D-LinkIn_a1:c0:17 (bc:0f:9a:a1:c0:17)
    Target IP address: 192.168.0.137
```

ARP -Słabości

- ❑ Brak mechanizmu autentykacji w pakietach ARP – Atakujący może podać dowolne dane adresowe (IP i MAC) w pakiecie ARP reply
- ❑ Brak mechanizmu sesji czy nawiązywania połączenia – Hosty akceptują pakiety ARP reply nawet jeśli nie wysyłały zapytania ARP request
- ❑ Bardzo szybko w sieci L2 możemy zorientować się o użytkownikach i bramie domyślnej na podstawie biernego nasłuchiwania zapytań ARP
- ❑ Atak ARP spoofing jest bardzo łatwy do przeprowadzenia (darmowe proste w obsłudze programy)

Udany atak ARP spoofing to bardzo duże zagrożenie dla działania sieci i jej bezpieczeństwa:

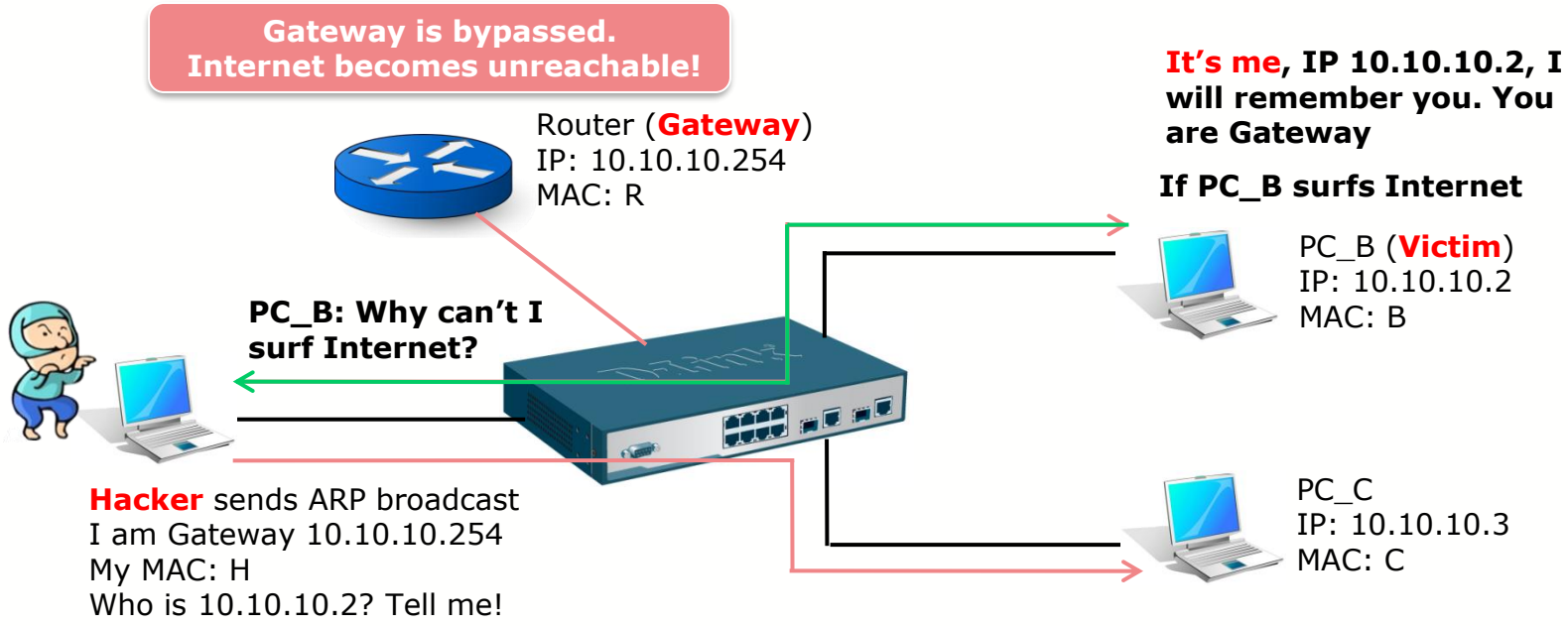
- ❑ Brak dostępu do sieci (LAN,WAN) na hoście z błędnie odwzorowaną tablicą ARP – Atak typu DOS
- ❑ Narażenie się na wyciek danych w sieci LAN – atak typu MITM

Trzy popularne metody ataku Arp Spoofing na zatrzymanie dostępu do sieci WAN (Internet):

- ✓ Haker podszywa się pod adres IP bramy z błędnym adresem MAC (nieistniejącym)
- ✓ Haker podszywa się pod adres IP bramy ze swoim adresem MAC
- ✓ Haker podszywa się pod adres IP bramy z adresem MAC bramy

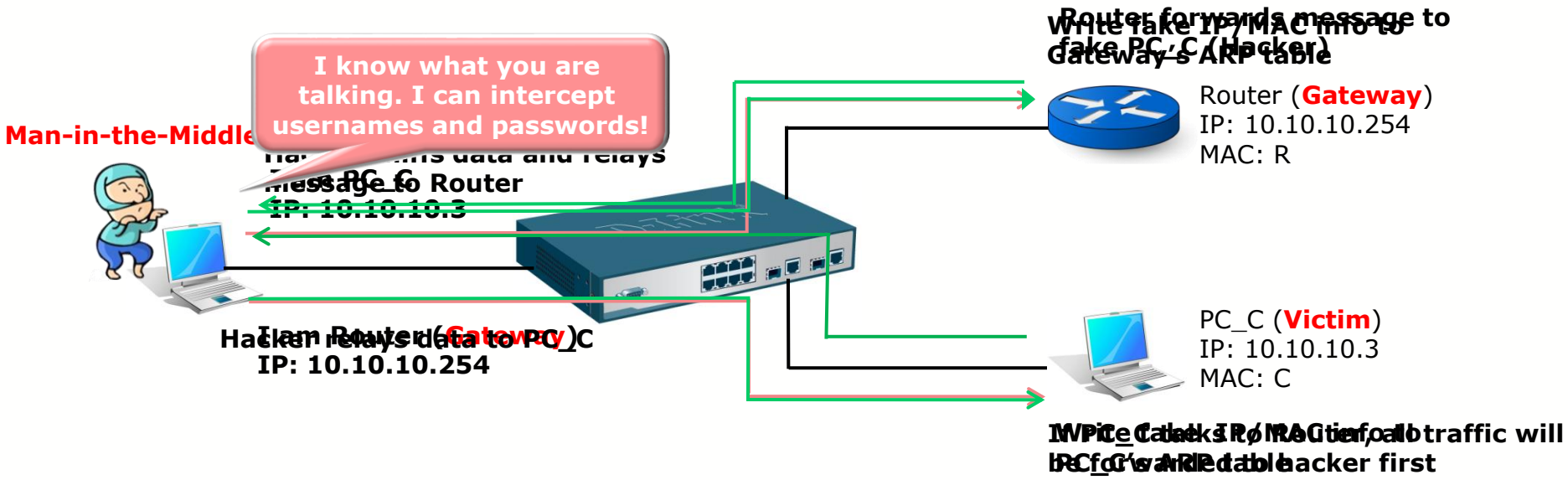
ARP Spoofing Attack

Brak dostępu do sieci zewnętrznej – Atak typu DoS



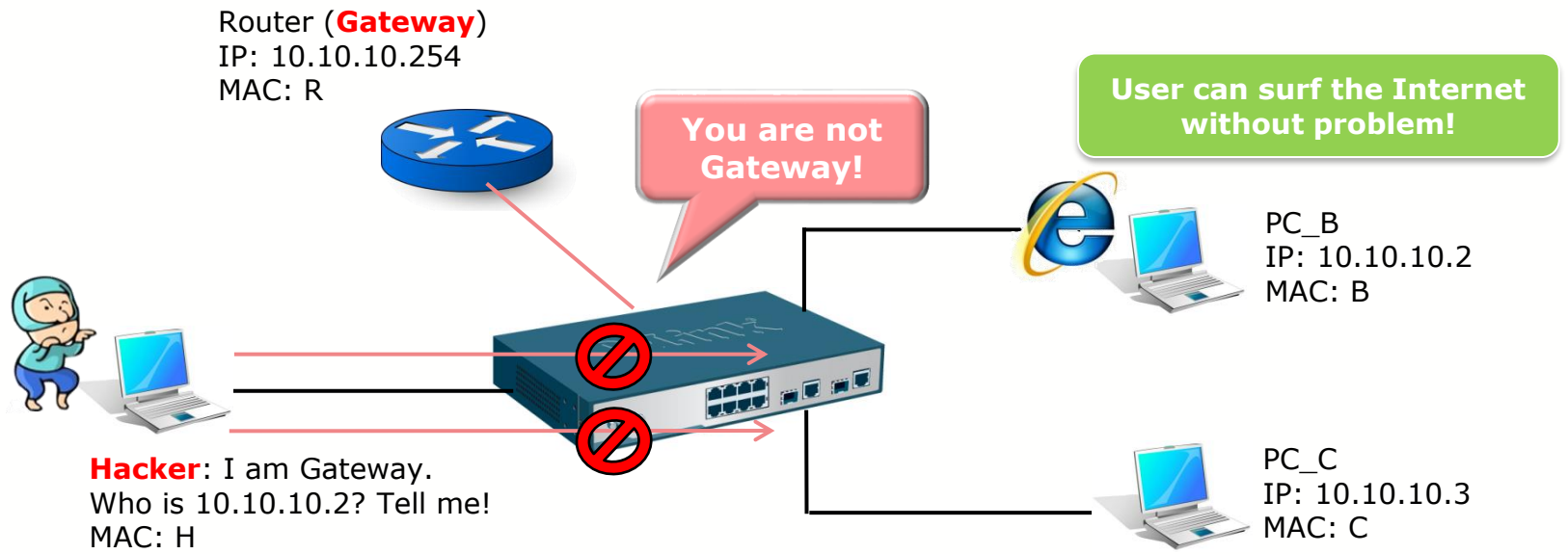
ARP Spoofing Attack

Podsłuchiwanie ruchu w sieci i wyciek danych – zachowany dostęp do sieci. Atak typu MITM

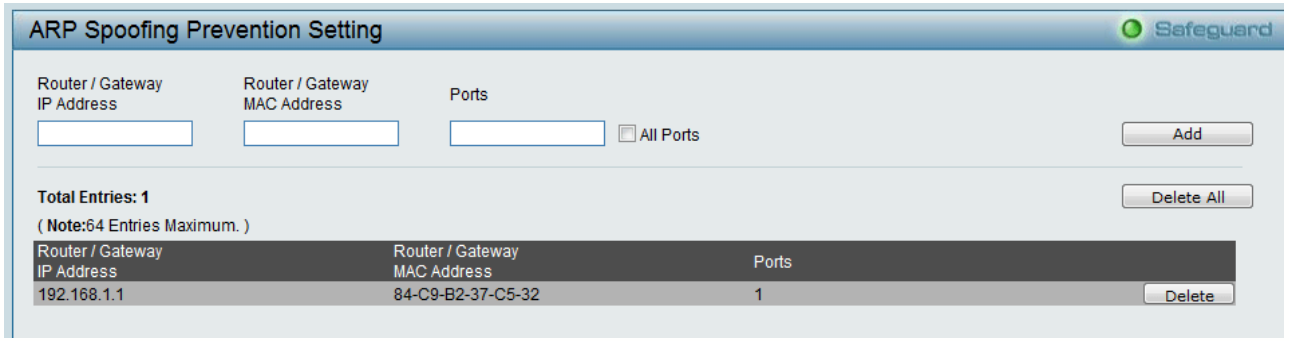


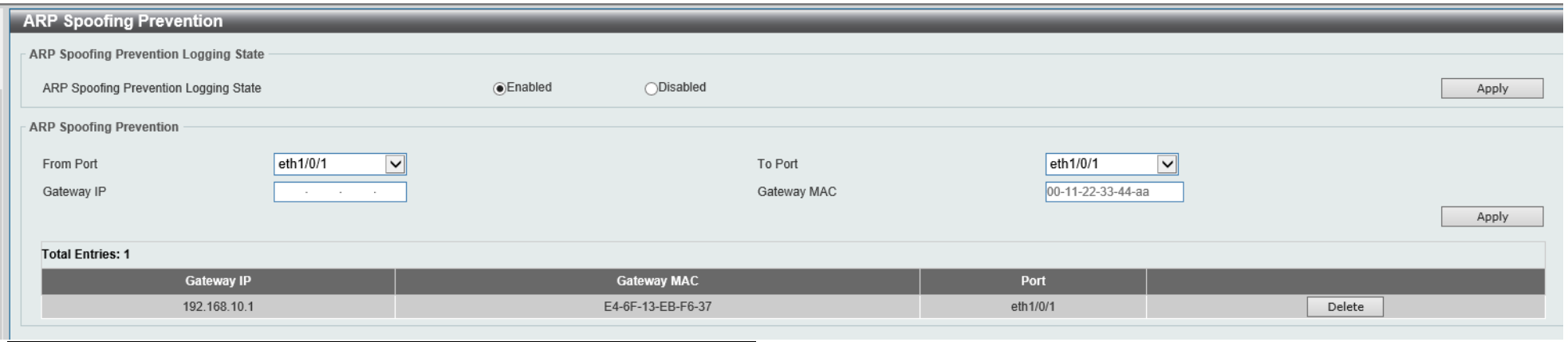
ARP Spoofing prevention

- Mechanizm zapobiegania podszywania się pod bramę domyślną w spreparowanych pakietach ARP.
- Po wykryciu adresu IP bramy w pakiecie ARP przełącznik sprawdza czy MAC adres oraz numer portu jest zgodny z wprowadzoną konfiguracją.
- W przypadku błędnego adresu MAC lub numeru portu pakiet ARP jest przez przełącznik odrzucany
- Pakiety z innym adresem niż adres skonfigurowanej bramy nie są poddawane inspekcji
- Zapobieganie możliwości zainfekowania hostów fałszywymi odwzorowaniami ARP bramy dośmyślnej w tablicach ARP



ARP spoofing prevention - konfiguracja






```
Switch#show ip arp spoofing-prevention

IP              MAC               Interfaces
--------------- ----------------- --------------------------
192.168.10.1    E4-6F-13-EB-F6-37 eth1/0/1

Total Entries: 1

Switch#
```

```
Switch#sh log
Switch#sh logging

Total number of buffered messages:102

#102    2014-06-13 18:38:59 WARN(4) Gateway 10.90.90.9 is under attack by 00-00-00-00-00-02 from eth1/0/1
#101    2014-06-13 18:38:59 WARN(4) Gateway 10.90.90.9 is under attack by 00-00-00-00-00-02 from eth1/0/1
#100    2014-06-13 18:38:59 WARN(4) Gateway 10.90.90.9 is under attack by 00-00-00-00-00-02 from eth1/0/1
#99     2014-06-13 18:38:59 WARN(4) Gateway 10.90.90.9 is under attack by 00-00-00-00-00-02 from eth1/0/1
#98     2014-06-13 18:38:59 WARN(4) Gateway 10.90.90.9 is under attack by 00-00-00-00-00-02 from eth1/0/1
#97     2014-06-13 18:38:59 WARN(4) Gateway 10.90.90.9 is under attack by 00-00-00-00-00-02 from eth1/0/1
#96     2014-06-13 18:38:59 WARN(4) Gateway 10.90.90.9 is under attack by 00-00-00-00-00-02 from eth1/0/1
#95     2014-06-13 18:38:59 WARN(4) Gateway 10.90.90.9 is under attack by 00-00-00-00-00-02 from eth1/0/1
#94     2014-06-13 18:38:59 WARN(4) Gateway 10.90.90.9 is under attack by 00-00-00-00-00-02 from eth1/0/1
#93     2014-06-13 18:38:59 WARN(4) Gateway 10.90.90.9 is under attack by 00-00-00-00-00-02 from eth1/0/1
```

D-Link®
Building Networks for People

Podsumowanie

- ✓ Zawsze zabezpieczaj urządzenia sieciowe silnymi hasłami
- ✓ Przechowuj hasła w formie szyfrowanej w pliku konfiguracyjnym
- ✓ Nie używaj niezabezpieczonych protokołów komunikacyjnych do zarzadzania przełącznikami (HTTP, Telnet)
- ✓ Wyłączaj nieużywane porty w celu kontroli dostępu do sieci
- ✓ Wydziel osobny Vlan do zarządzania infrastruktura sieciową (osobny od vlanu klienckiego)
- ✓ Ustaw port security tam gdzie to konieczne (porty klienckie) z ograniczoną liczba mac adresów
- ✓ Zabezpiecz serwer DHCP poprzez opcje DHCP server screening
- ✓ W celu uniknięcia pętli włącz mechanizm loopback detection na używanych portach klienckich
- ✓ Zabezpiecz swoją bramę domyślną poprzez mechanizm ARP Spoofing prevention
- ✓ Przechowuj w bezpiecznym miejscu pliki z ostatnia używaną i działająca konfiguracją
- ✓ Wykonuj backupy po zmianach w konfiguracji
- ✓ Używaj aktualnych wersji firmware na urządzeniach
- ✓ Dokonuj zmian w sieci w trakcie okien serwisowych

Value in Partnership+

Korzyści dla Partnerów D-Link zarejestrowanych w programie VIP+:

- Szkolenia i system certyfikacji technicznej
- Narzędzia online dla inżynierów i działu sprzedaży
- Rabaty posprzedażne
- Materiały sprzedażowe
- Fundusze na działania marketingowe
- Priorytetowe wsparcie techniczne
- Program NFR
- Dedykowane promocje

D-Link
Building Networks for People

Value in Partnership+

KORZYŚCI	REGISTERED	BRONZE	SILVER	GOLD
Status zarejestrowanego partnera	✔	✔	✔	✔
Dostęp do portalu partnerskiego	✔	✔	✔	✔
Miesięczny biuletyn VIP+	✔	✔	✔	✔
Dostęp do warsztatów i webinarów	✔	✔	✔	✔
Narzędzia online	✔	✔	✔	✔
Materiały techniczno-sprzedażowe	✔	✔	✔	✔
Rejestracja projektów	✔	✔	✔	✔
Możliwość otrzymania ceny projektowej	✔	✔	✔	✔
Dedykowane promocje	✔	✔	✔	✔
Zakup produktów NFR	✔	✔	✔	✔
Priorytetowa obsługa techniczna		✔	✔	✔
Finansowanie szkolenia w ramach Akademii D-Link		✔ (50%)	✔ (100%)	✔ (100%)
Dedykowany opiekun handlowy			✔	✔
Współfinansowanie działań marketingowych (do 50%)			✔	✔
Obecność na stronie dlink.com (sekcja Gdzie kupić?)			✔	✔
Rabaty posprzedażne				✔

D-Link®
Building Networks for People

Zarejestruj się

vipplus.dlink.com

NBDS– Nowa usługa gwarancyjna dla produktów kategorii business

- Standardowa gwarancja Limited Lifetime (+5 lat od zakończenia produkcji) na produkty biznesowe
- Nowy sposób realizacji gwarancji dla wszystkich produktów kategorii biznes
- Next Business Day Service jako usługa standardowa dla produktów objętych gwarancją min 5 lat.
- Produkty z ważnymi kontraktami DAS realizowane na podstawie poprzedniej usługi.
- Sposób zgłaszania i realizacji gwarancji w analogiczny sposób jak dotychczas
- Zabezpieczenie usługi kartą kredytową – środki pobieranie w przypadku braku odsyłki urządzenia w trakcie 15 dni od realizacji zgłoszenia reklamacyjnego

D-LinkAssist
Next Business Day Service

D-Link
Building Networks for People

Dziękujemy za uwagę!

Pytania techniczne:

Maciej Dąbrowski (maciej.dabrowski@dlink.com)

Pytania handlowe:

Rafał Bystrek (rafal.bystrek@dlink.com)

Wioletta Włodarczyk-Kowalik (wioletta.wlodarczyk@dlink.com)

D-Link