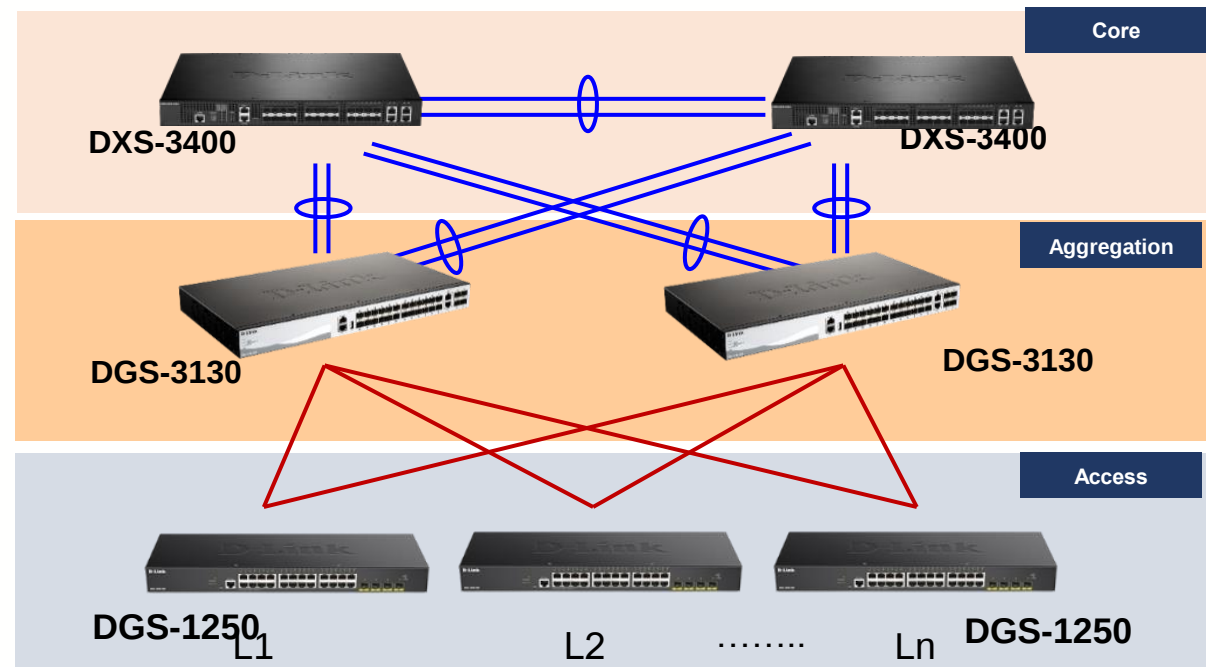


Wybrane mechanizmy bezpieczeństwa w przełącznikach dostępowych



Bezpieczeństwo w sieciach dostępowych

- Warstwa dostępową 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

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 możliwe 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

The screenshot displays the D-Link web management interface for a DGS-1210-24P switch. The top navigation bar includes 'Save', 'Tools', 'Wizard', 'Help', and 'Surveillance Mode'. The left sidebar shows a tree view of configuration options, with 'Trusted Host' selected under the 'Security' category. The main content area is titled 'Trusted Host Settings' and features a 'Safeguard' status indicator. The 'Trusted Host' toggle is set to 'Enabled'. Below this, the 'IPv4 Address' field is active, with a 'Netmask' dropdown set to '24 (255.255.255.0)'. An 'Add' button is present next to the IPv4 settings. A message states: 'Please add your local host IP address first to make it trusted. Otherwise, the connection will be stopped.' The 'Trusted Host Table' section indicates a maximum of 10 entries and contains an empty table with columns for ID, IP Address, Netmask/Prefix, and Delete.

ID	IP Address	Netmask/Prefix	Delete
----	------------	----------------	--------

Konta użytkowników DGS-1510

The image displays three screenshots of the D-Link DGS-1510-28P web interface, showing the configuration of user accounts and login methods.

Top Screenshot: User Accounts Settings

The interface shows the "User Accounts Settings" page. The "User Management Settings" tab is active. The "Session Table" tab is also visible. The "User Name" field is set to "32 chars". The "Privilege (1-15)" field is set to "15". The "Password Type" is set to "None". The "Password" field is empty. The "Total Entries: 1" is displayed. Below the settings, a table shows the user account configuration:

User Name	Privilege	Password
admin	15	*****

Middle Screenshot: Password Encryption

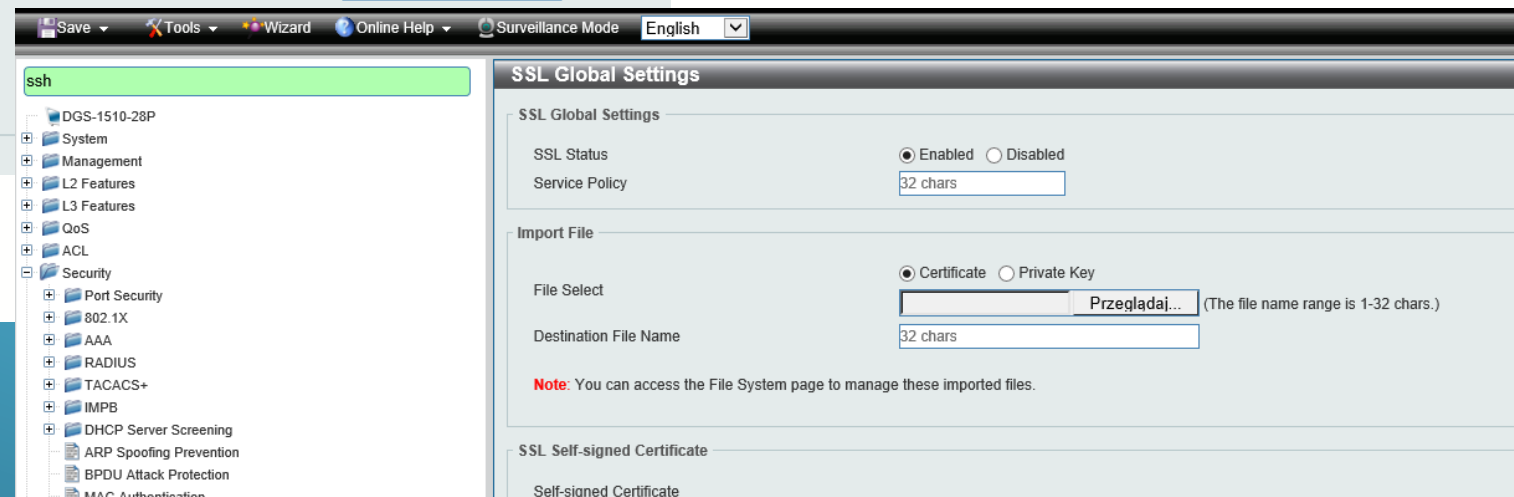
The interface shows the "Password Encryption" page. The "Password Encryption Settings" tab is active. The "Password Encryption State" is set to "Enabled". The "Password Type" is set to "Encrypted-SHA1".

Bottom Screenshot: Login Method

The interface shows the "Login Method" page. The "Enable Password" section is active. The "Level" is set to "15". The "Password Type" is set to "Plain Text". The "Password" field is set to "32 chars". The "Login Method" section is active. Below the settings, a table shows the login method configuration:

Application	Login Method	
Console	Login Local	Edit
Telnet	Login Local	Edit
SSH	Login Local	Apply

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
```

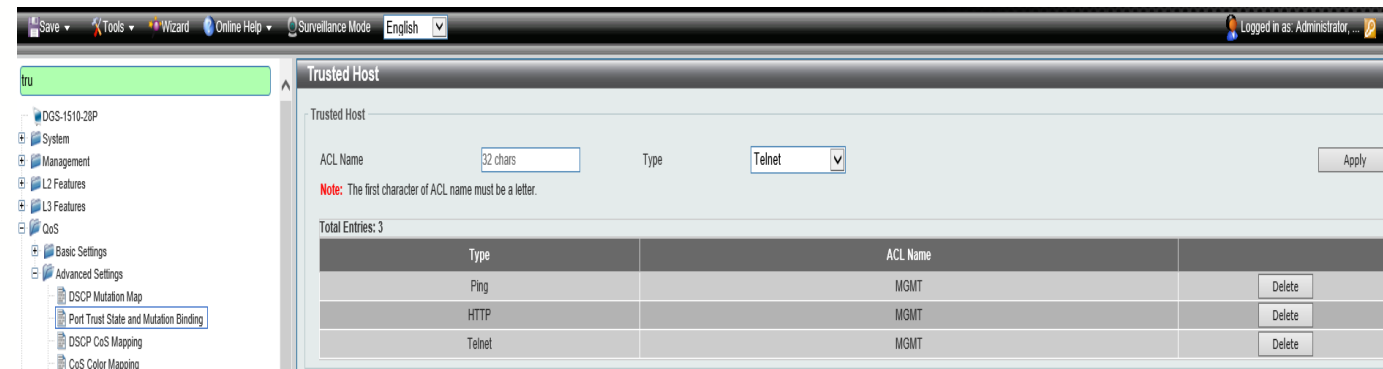
```
access-class MGMT
```

```
exit
```

```
endconfig t
```

```
ip http access-class MGMT
```

```
ip https access-class MGMT
```



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 połączenie 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 się 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 adresację.	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 cały ruch dedykowany do niego 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 doбором 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 możliwości podsłuchania transmisji unicastowej na innych portach przełącznika
- ❑ Aging – Podtrzymywanie i usuwanie adresów MAC z tablicy przełącznika na podstawie liczników.

Komunikacja na przełączniku L2

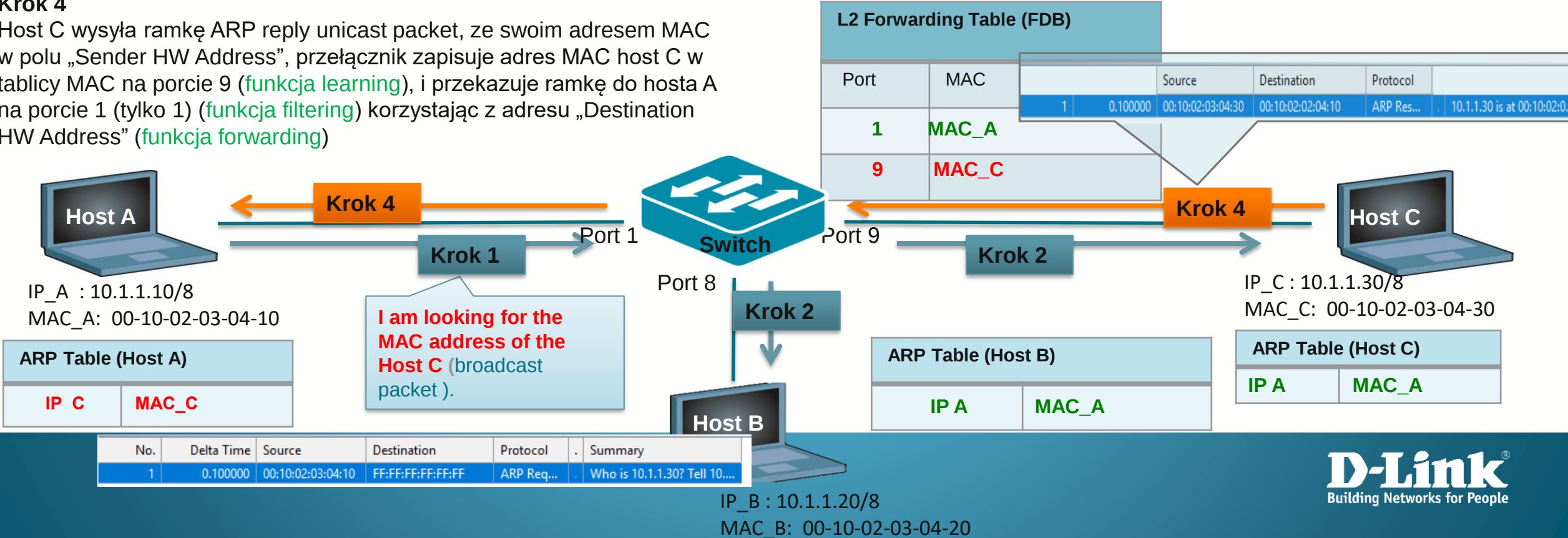
Scenariusz: Host A z Host B

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**)



Scenariusz: Host A z Host B cd

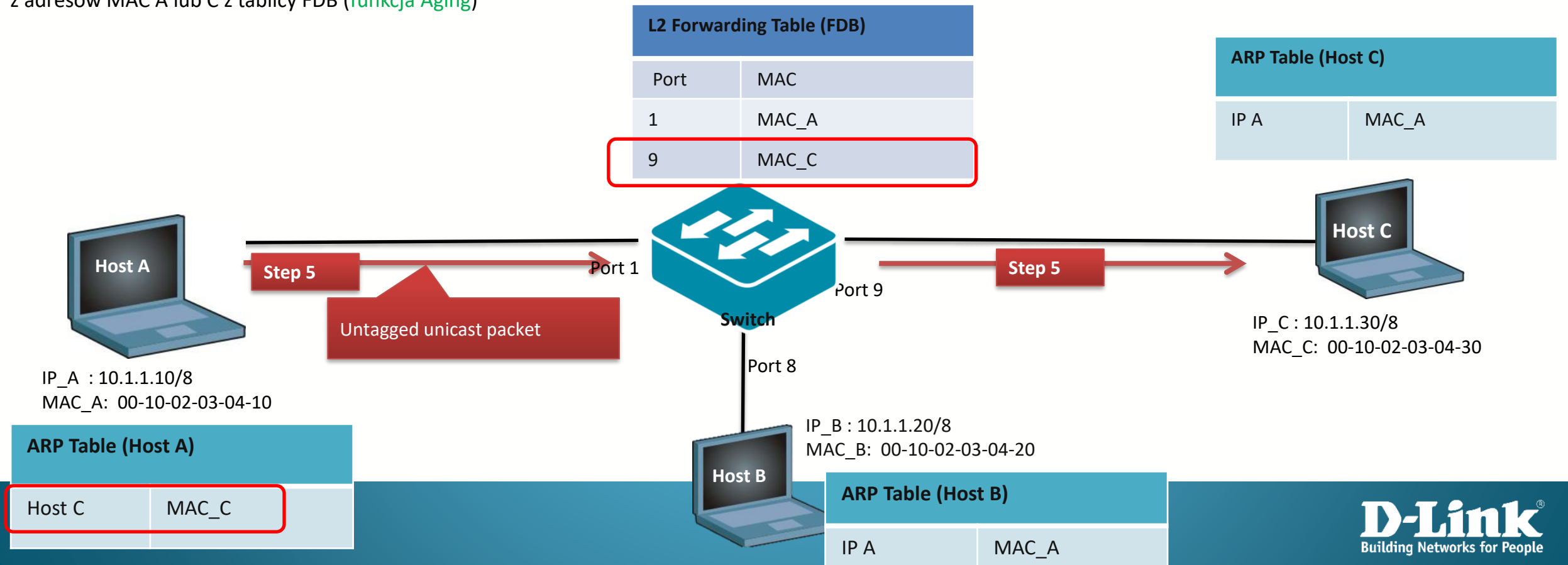
Krok 5

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 momentu 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**)



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 zapelnienia 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

Port Security

From Port: 01 To Port: 28 Admin State: Disabled Max Learning Address (0-64): 0 Apply

Port	Admin State	Max Learning Address
01	Disabled	0
02	Disabled	0
03	Enabled	1

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

System Log

Maximum 500 entries.

ID	Time	Log Description	Severity
18	Jun 12 07:04:52	Port security violation (Port: 3, Vid: 1, MAC: 00-26-5A-81-9B-28)	warning
17	Jun 12 07:04:50	Port security violation (Port: 3, Vid: 1, MAC: 00-26-5A-81-9B-28)	warning
16	Jun 12 07:04:48	Port security violation (Port: 3, Vid: 1, MAC: 00-26-5A-81-9B-28)	warning

MAC Address Table

Port	01	02	03	04	05	06	07	08	09
Learning	✓	✓	✓	✓	✓	✓	✓	✓	✓
Port	15	16	17	18	19	20	21	22	23
Learning	✓	✓	✓	✓	✓	✓	✓	✓	✓

Add Static MAC Address

Port: 01 MAC Address: VID: 1

Static MAC Address Lists

Maximum 256 entries.

ID	Port	MAC Address	VID
1	3	00-26-5A-81-9B-28	1

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

Port Security DGS-1510

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

The screenshot shows the 'Port Security Port Settings' configuration page. The top navigation bar includes 'Save', 'Tools', 'Wizard', 'Online Help', 'Surveillance Mode', and a language dropdown set to 'English'. The user is logged in as 'Administrator'. The left sidebar shows the 'L2 Features' tree with 'FDB' expanded, showing 'Static FDB' and 'VLAN' sub-menus. The main content area is titled 'Port Security Port Settings' and contains a form with the following fields: 'From Port' (eth1/0/1), 'To Port' (eth1/0/1), 'State' (Disabled), 'Maximum (0-6556)' (32), 'Violation Action' (Protect), 'Security Mode' (Delete-on-Timeout), 'Aging Time (0-1440)' (empty), and 'Aging Type' (Absolute). An 'Apply' button is at the bottom right. Below the form is a table showing the configuration for four ports.

Port	Maximum	Current No.	Violation Action	Violation Count	Security Mode	Admin State	Current State	Aging Time	Aging Type
eth1/0/1	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/2	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/3	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/4	3	3	Restrict	0	Delete-on-Timeout	Enabled	Forwarding	50	Absolute

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

The screenshot shows the 'Port Security Address Entries' configuration page. The top navigation bar is identical to the previous screenshot. The left sidebar shows the 'L2 Features' tree with 'FDB' expanded, showing 'Static FDB' and 'VLAN' sub-menus. The main content area is titled 'Port Security Address Entries' and contains a form with the following fields: 'Port' (eth1/0/1), 'MAC Address' (00-84-57-00-00-00), and a checkbox for 'Permanent'. A 'VID (1-4094)' field is also present. 'Add', 'Delete', and 'Clear by Port' buttons are at the bottom right. Below the form is a table showing the configuration for three entries.

Port	VID	MAC Address	Address Type	Remaining Time (mins)
eth1/0/4	1	00-26-5A-81-9B-28	Delete-on-Timeout	50
eth1/0/4	1	E4-54-E8-A6-8D-98	Permanent	-
eth1/0/4	1	E4-54-E8-A8-08-9C	Permanent	-

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
-----
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 security violation on Ethernet1/0/4.
```

```
#43653 2000-01-09 23:42:34 WARN(4) MAC address 00-26-5A-81-9B-28 causes port security 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
```

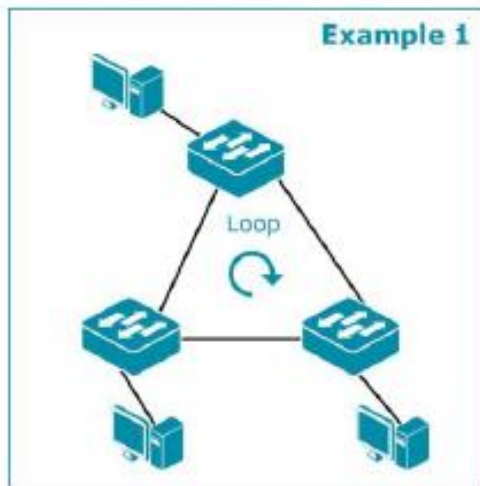
```
Total number of buffered messages:10000
```

```
#43658 2000-01-09 23:46:58 WARN(4) MAC address 00-26-5A-81-9B-28 causes port security violation on Ethernet1/0/4.
```

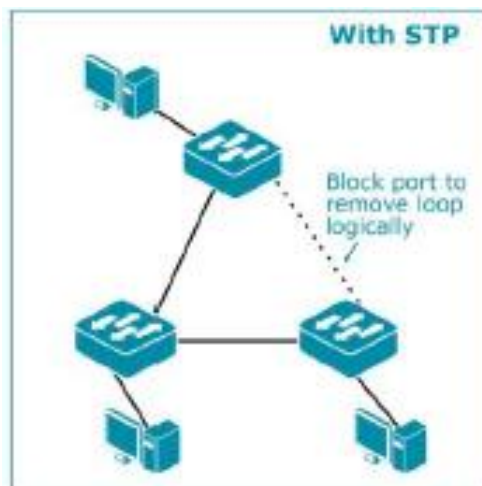
```
#43657 2000-01-09 23:46:58 WARN(4) Port <1/0/4> enters error disable state due to Port Security violation
```

Pętle w sieciach L2 – Loopback detection

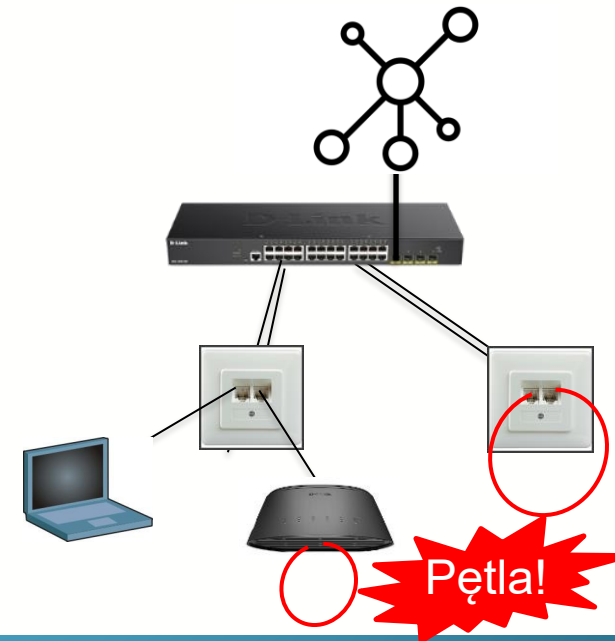
- Pętle w sieciach L2, powstają najczęściej „przez przypadek” na skutek źle połączonych infrastruktury sieciowej.
- Brak wbudowanego mechanizmu unikania pętli w warstwie 2
- Jeden pakiet typu broadcast, multicast, unknown unicast może zablokować całą sieć.
- Dążymy do nadmiarowej topologii fizycznej 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

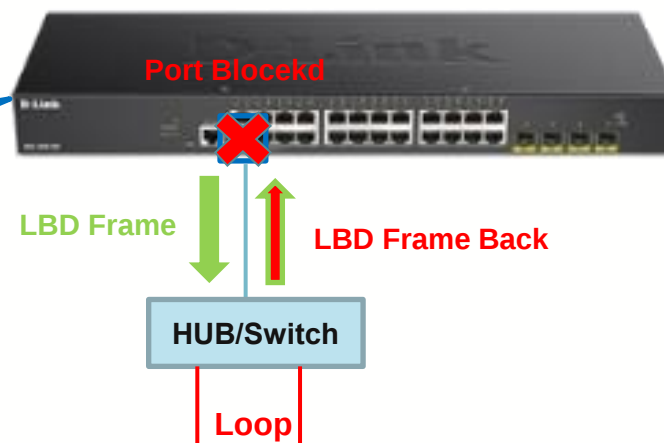
Zabezpiecza przed:

- ✓ 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 wyłączanego 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

D-Link
Building Networks for People

admin - 192.168.10.109

Save Tools Wizard Help Surveillance Mode Logout

Loopback Detection Settings Safeguard

Loopback Detection ☒ Enabled ☐ Disabled

Mode Port-based VLAN List

Interval (1-32767) 2 sec

Recover Time (0 or 60-1000000) 60 sec Apply

From Port 01 To Port 28 State Enabled Refresh Apply

Port	State	Loop Status
01	Disabled	Normal
02	Disabled	Normal
03	Disabled	Normal
04	Disabled	Normal
05	Disabled	Normal
06	Disabled	Normal
07	Disabled	Normal
08	Disabled	Normal
09	Disabled	Normal
10	Disabled	Normal

System Log

Maximum 500 entries.

ID	Time	Log Description
37	Jun 12 08:24:22	port 7 link down
36	Jun 12 08:24:20	Port 8 LBD loop occurred. Port blocked.
35	Jun 12 08:24:20	port 8 link down
34	Jun 12 08:24:20	Port 8 link up, 1Gbps FULL duplex
33	Jun 12 08:24:20	Port 7 link up, 1Gbps FULL duplex
32	Jun 12 08:24:15	Port 8 LBD port recovered. Loop detection restarted.
31	Jun 12 08:23:17	port 7 link down
30	Jun 12 08:23:15	Port 8 LBD loop occurred. Port blocked.
29	Jun 12 08:23:15	port 8 link down
28	Jun 12 08:23:15	Port 8 link up, 1Gbps FULL duplex
27	Jun 12 08:23:15	Port 7 link up, 1Gbps FULL duplex
26	Jun 12 08:23:11	Port 8 LBD port recovered. Loop detection restarted.
25	Jun 12 08:22:13	port 7 link down
24	Jun 12 08:22:11	Port 8 LBD loop occurred. Port blocked.
23	Jun 12 08:22:11	port 8 link down
22	Jun 12 08:22:11	Port 8 link up, 1Gbps FULL duplex
21	Jun 12 08:22:11	Port 7 link up, 1Gbps FULL duplex

Loopback Detection - Konfiguracja

loop

DGS-1510-28P

System

Management

L2 Features

FDB

VLAN

STP

ERPS (G.8032)

Loopback Detection

Link Aggregation

L2 Multicast Control

LLDP

L3 Features

QoS

ACL

Security

OAM

Monitoring

Green

Loopback Detection

Loopback Detection Global Settings

Loopback Detection State: Enabled

Enabled VLAN ID List: 1-4094

Trap State: Disabled

Address Type: Multicast

Mode: Port-based

Interval (1-32767): 10 sec

Action: Shutdown

Function Version: v4.07

Loopback Detection Port Settings

From Port: eth1/0/1 To Port: eth1/0/1 State: Disabled

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
```

Loopback Detection - Przywracanie portu

PORT Auto Negotiation

Error Disable Settings

Jumbo Frame

Interface Description

PoE

System Log

Time and SNTP

Time Range

Management

! Features

! Features

oS

oL

Security

AM

Monitoring

reen

ErrDisable Cause

All

State

Disabled

Interval (5-86400)

sec

Apply

ErrDisable Cause	State	Interval (sec)
Port Security	Disabled	300
Storm Control	Disabled	300
BPDU Attac...	Disabled	300
Dynamic AR...	Disabled	300
DHCP Snooping	Disabled	300
Loopback Detect	Enabled	10

Interfaces that will be recovered at the next timeout:

Interface	VLAN	ErrDisable Cause	Time Left (sec)
eth1/0/9	-	Loopback Detect	8
eth1/0/11	-	Loopback Detect	8

1/1<<1>>Go

```
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
```

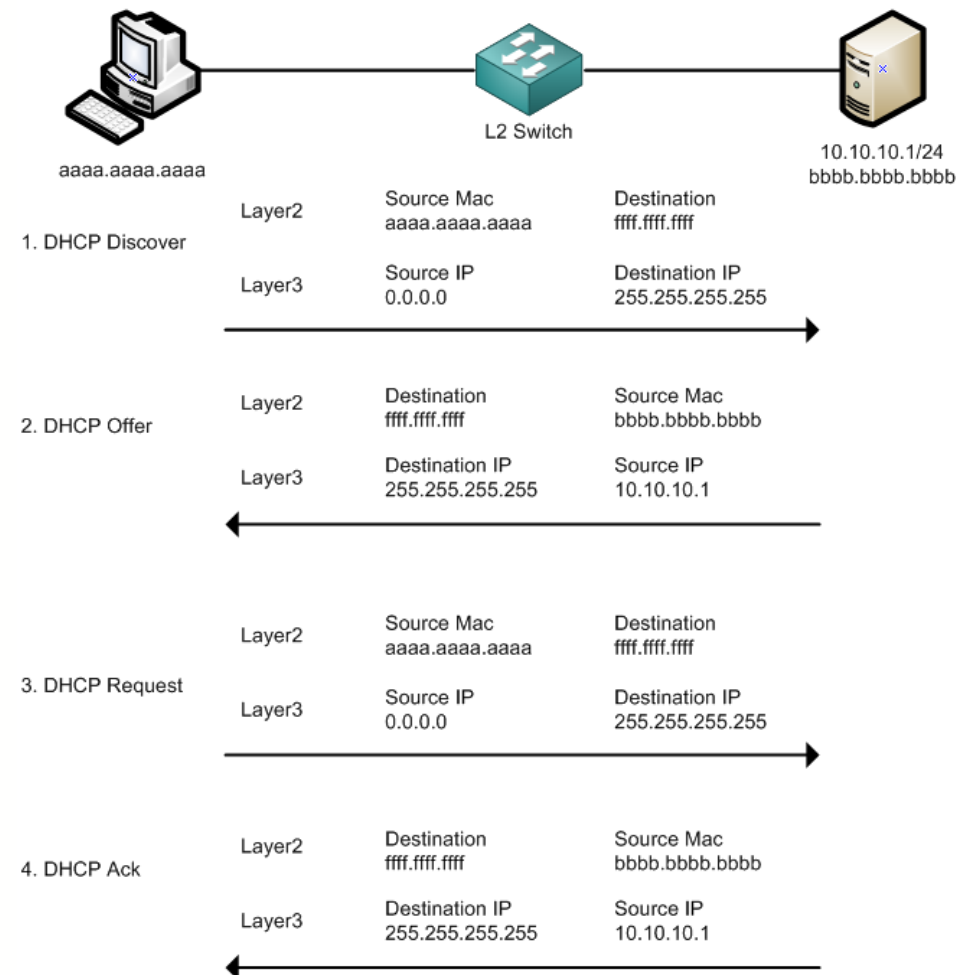
```
Interfaces that will be recovered at the next timeout:
```

```
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
```

Zagrożenia związane z DHCP

DHCP Message Exchange



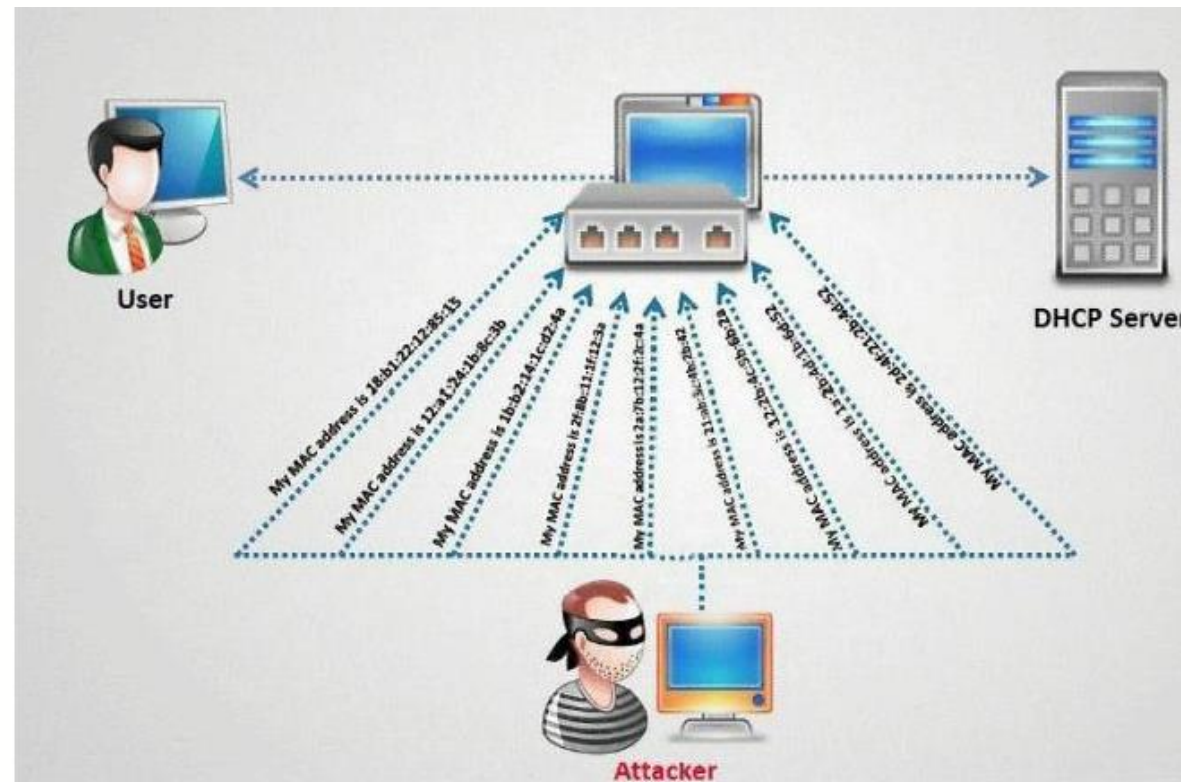
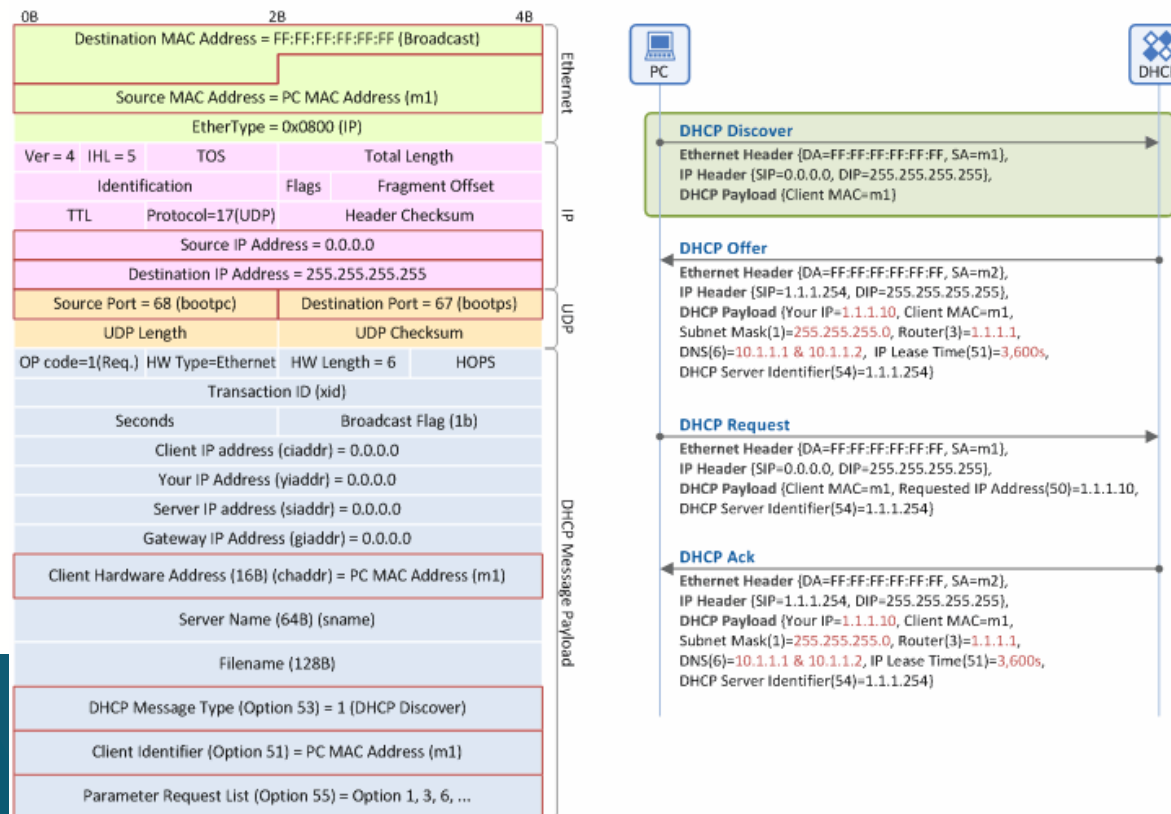
- Serwer DHCP ma za zadania w sposób dynamiczny i automatyczny przyznać adresację IP wraz z dodatkowymi informacjami
- Standardowo serwer DHCP przyznaje: IPv4, maskę podsieci, adres bramy domyślnej, adresy serwerów DNS, informacje o czasie dzierżawy adresu
- Standardowo pakiety w ramach wymiany DHCP 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 nasłuchiowaniu 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

DHCP Snooping Global Settings

DHCP Snooping Global Settings

- | | | |
|------------------------------------|--|---|
| DHCP Snooping | ☒ Enabled | ☐ Disabled |
| Information Option Allow Untrusted | ☐ Enabled | ☒ Disabled |
| Source MAC Verification | ☒ Enabled | ☐ Disabled |
| Station Move Deny | ☐ Enabled | ☒ Disabled |

Surveillance Mode English Logged in as: Administrator

DHCP Snooping Port Settings

DHCP Snooping Port Settings

From Port: eth1/0/2

To Port: eth1/0/2

Entry Limit (0-1024): ☒ No Limit

Rate Limit (1-300): ☐ No Limit

Trusted: No

Port	Trusted	Rate Limit	Entry Limit
eth1/0/1	No	No Limit	No Limit
eth1/0/2	No	5	No Limit

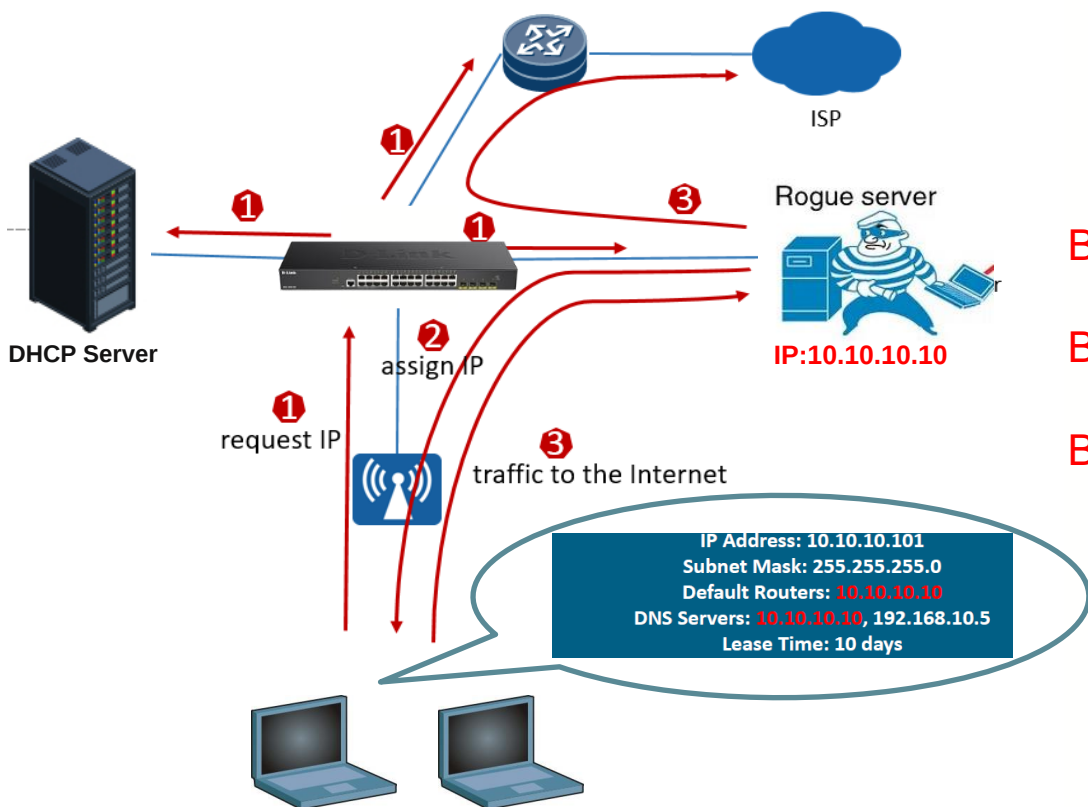
```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping verify mac-address
```

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

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



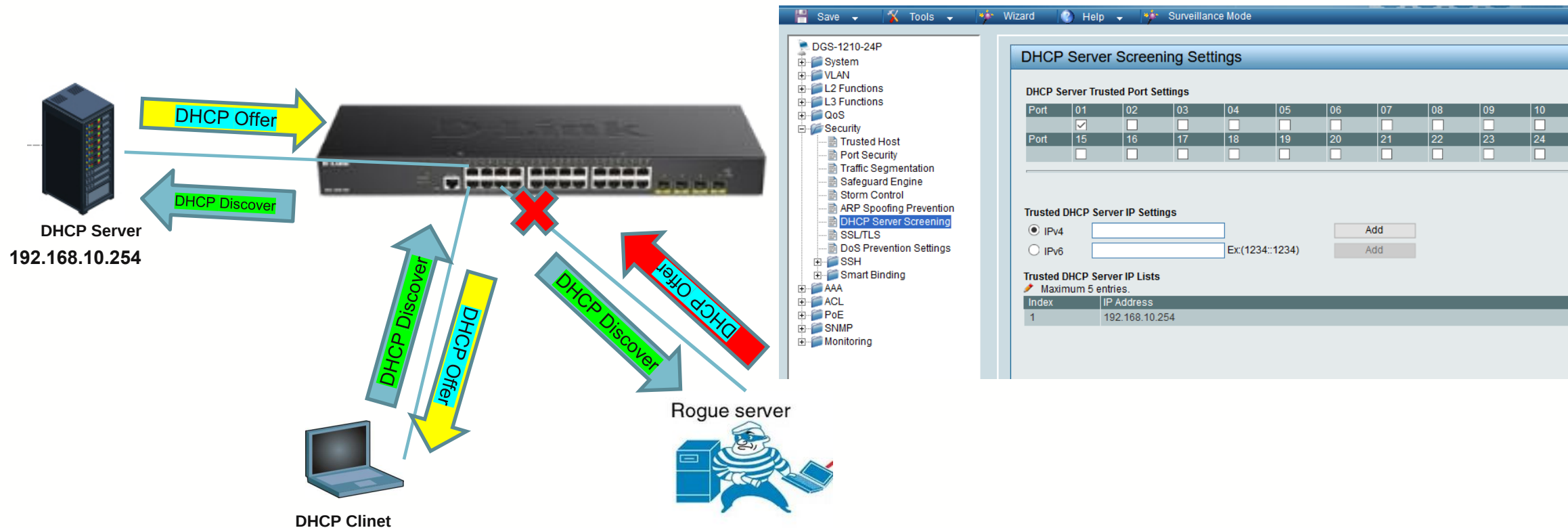
Błędny adres bramy domyślnej – Atakujący udaje bramę domyślną

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

DHCP Server Screening Global Settings

Trap Settings

Trap State

Disabled

Profile Settings

Profile Name

32 chars

Client MAC

00-84-57-00-00-00

Total Entries: 0

Profile Name

Log Information

Log Buffer Entries (10-1024)

32

Total Entries: 0

VLAN	Server IP
------	-----------

DHCP Server Screening Port Settings

DHCP Server Screening Port Settings

From Port

eth1/0/2

To Port

eth1/0/2

State

Enabled

Server IP

- . .

Profile Name

32 chars

Port	State	Server IP	Profile Name
eth1/0/1	Disabled	-	-
eth1/0/2	Disabled	-	-
eth1/0/3	Disabled	-	-
eth1/0/4	Disabled	-	-
eth1/0/5	Disabled	-	-

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

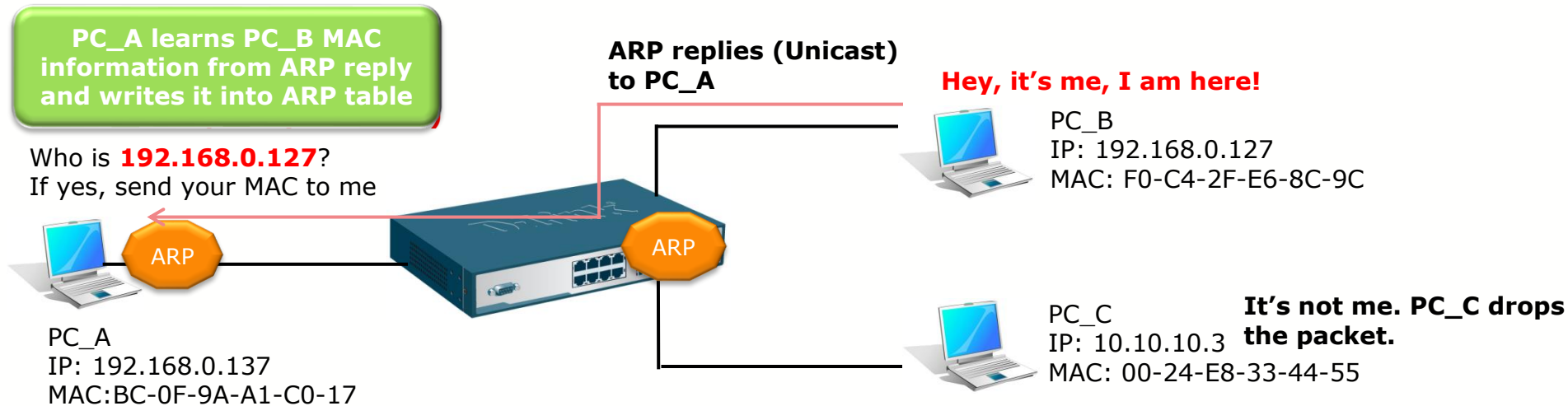
Total log buffer size: 32

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

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
```

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 wire (336 bits), 42 bytes captured (336 bits) on interface {A64871-6CA8-4328-AC77-0B4D2BE468DA}, id 0
```

Ethernet II, Src: D-LinkIn_a1:c0:17 (bc:0f:9a:a1:c0:17), Dst: D-LinkIn_a1:c0:17 (bc:0f:9a:a1:c0:17), Type: ARP (0x0806)

Address Resolution Protocol (request (1))

Hardware type: Ethernet (1)
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: 0000000000000000000000000000000019a9dd9b

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 nasłuchiwanie 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:

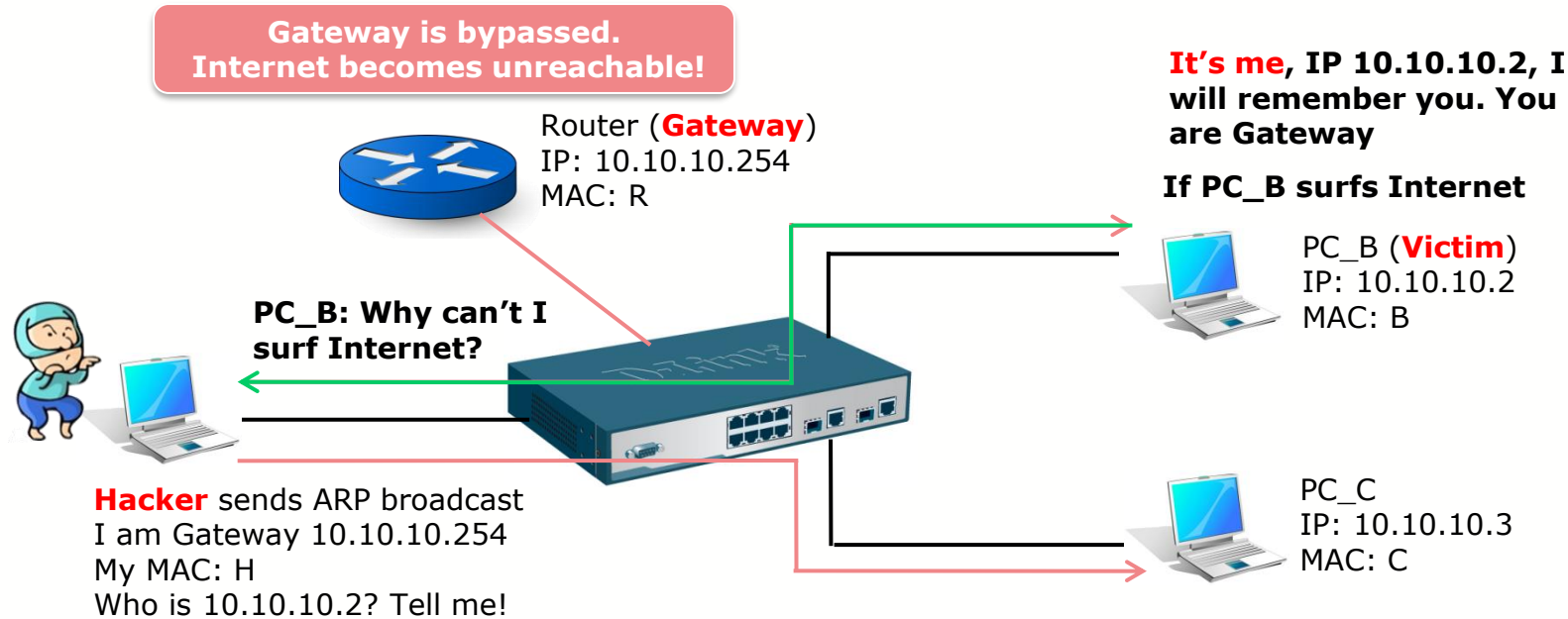
- ❑ Brak dostępu do sieci (LAN,WAN) na hoście z błędnie odwzorowaną tablicą ARP – Atak typu DOS
- ❑ Narażenie się na wyciek danych w sieci LAN – atak typu MITM

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

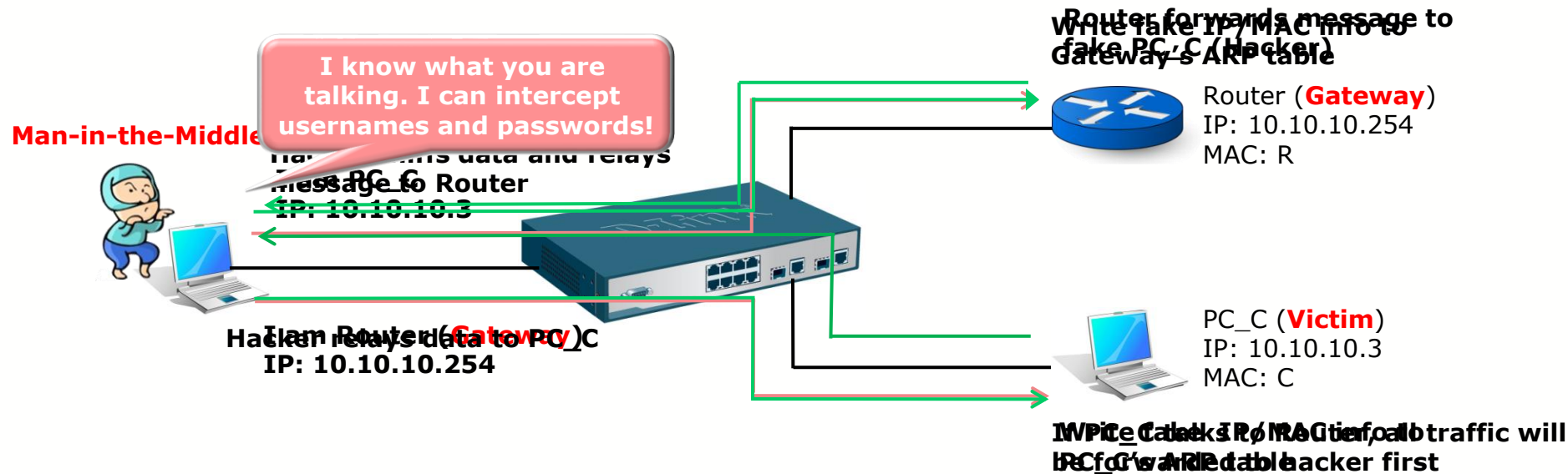
ARP Spoofing Attack

Brak dostępu do sieci zewnętrznej – Atak typu DoS



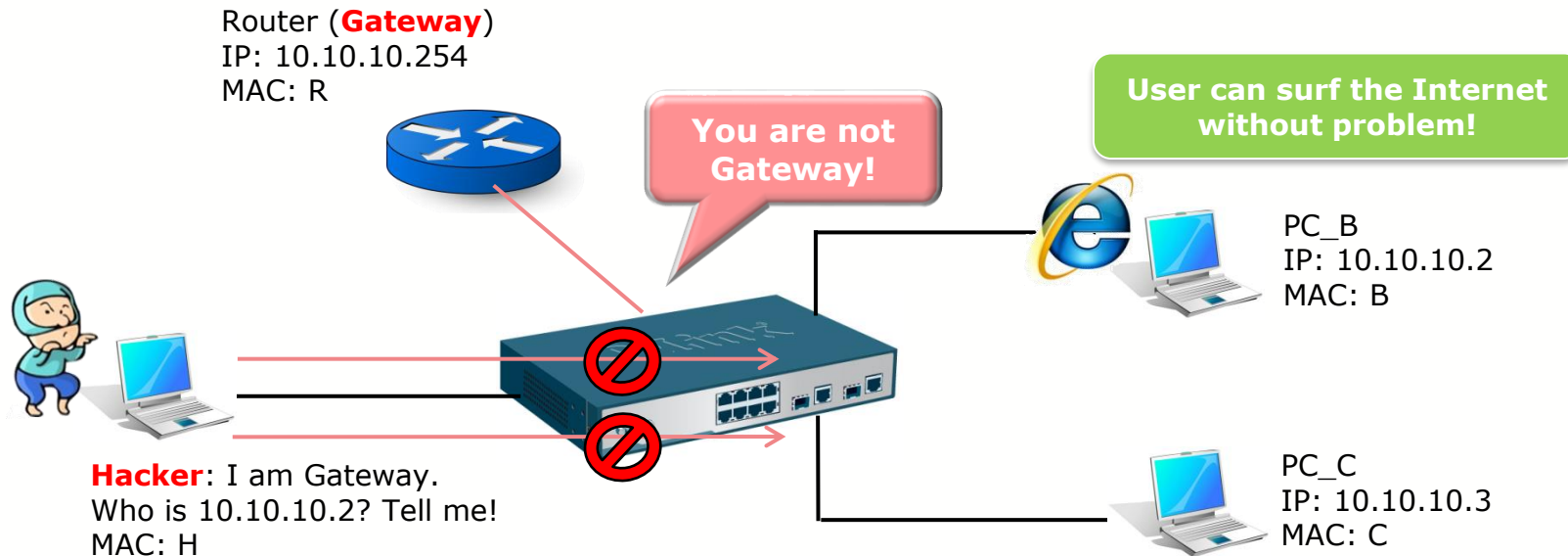
ARP Spoofing Attack

Podśluchiwanie 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

ARP Spoofing Prevention Setting Safeguard

Router / Gateway IP Address:
Router / Gateway MAC Address:
Ports: ☐ All Ports

Total Entries: 1
(Note: 64 Entries Maximum.)

Router / Gateway IP Address	Router / Gateway MAC Address	Ports
192.168.1.1	84-C9-B2-37-C5-32	1

ARP Spoofing Prevention

ARP Spoofing Prevention Logging State: ☒ Enabled ☐ Disabled

ARP Spoofing Prevention

From Port: To Port:
Gateway IP: Gateway MAC:

Total Entries: 1

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

```
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
```

Podsumowanie

- ✓ Zawsze zabezpieczaj urządzenia sieciowe silnymi hasłami
- ✓ Przechowuj hasła w formie szyfrowanej w pliku konfiguracyjnym
- ✓ Nie używaj niezabezpieczonych protokołów komunikacyjnych do zarządzania przełącznikami (HTTP, Telnet)
- ✓ Wyłączaj nieużywane porty w celu kontroli dostępu do sieci
- ✓ Wydziel osobny Vlan do zarządzania infrastrukturą sieciową (osobny od vlanu klienckiego)
- ✓ Ustaw port security tam gdzie to konieczne (porty klienckie) z ograniczoną liczbą 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 ostatnią używaną i działającą 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



Value in Partnership+

KORZYŚCI	REGISTERED D-Link	BRONZE D-Link	SILVER D-Link	GOLD D-Link
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				✓



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





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