Rozdział 2: Wprowadzenie do sieci przełączanych

Routing and Switching

Cisco | Networking Academy®
Mind Wide Open™

Rozdział 2

2.0 Wprowadzenie

2.1 Podstawowa konfiguracja przełącznika

2.2 Bezpieczeństwo przełącznika: zarządzanie i wdrażanie

Rozdział 2: Cele

Po zakończeniu tego rozdziału będziesz potrafił:

- wyjaśnić zalety i wady routingu statycznego,
- skonfigurować podstawowe ustawienia na przełączniku Cisco,
- konfigurować porty przełącznika zgodnie z wymogami sieci,
- skonfigurować wirtualny interfejs do zarządzania przełącznikiem,
- opisać podstawowe ataki na bezpieczeństwo w środowisku opartym o przełączniki,
- opisać najlepsze praktyki związane z bezpieczeństwem w środowisku opartym o przełączniki,
- skonfigurować funkcję zabezpieczenia portu, aby ograniczyć dostęp do sieci.

Sekwencja rozruchowa przełącznika

1. Samoczynny test po włączeniu (POST).
2. Uruchomienie oprogramowania boot loader.
3. Boot loader inicjalizuje pracę procesora CPU w trybie niskiego poziomu.
4. Boot loader inicjalizuje system plików dla pamięci flash.
5. Boot loader wyszukuje lokalizację obrazu systemu IOS, ładuje system IOS do pamięci i przekazuje kontrolę nad przełącznikiem do IOS.

Sekwencja rozruchowa przełącznika (cd.)

Aby znaleźć odpowiedni obraz Cisco IOS, przełącznik przechodzi przez następujące etapy:

Krok 1. Przełącznik próbuje automatycznie wykonać rozruch za pomocą zmiennej środowiskowej BOOT.

Krok 2. Jeżeli zmienna BOOT nie jest ustawiona, to przełącznik przeszukuje rekurencyjnie cały system plików pamięci flash w celu znalezienia pierwszego pliku wykonywalnego. Jeśli to możliwe, przełącznik ładuje i wykonuje pierwszy plik wykonywalny.

Krok 3. Po wykonaniu powyższych operacji, system operacyjny IOS inicjalizuje interfejsy w oparciu o polecenia znajdujące się w pliku konfiguracji startowej, która jest zapisana w pamięci NVRAM.

Uwaga: Polecenie **`boot system`** może być używane do ustawienia zmiennej środowiskowej BOOT.

Odzyskiwanie po awarii systemu

- Boot loader może być również wykorzystywany do zarządzania przełącznikiem, jeśli IOS nie może być załadowany.
- Aby uzyskać dostęp do pamięci flash za pomocą boot loadera należy wykonać następujące kroki:

  1. za pomocą kabla konsolowego podłącz komputer do portu konsolowego przełącznika, następnie odłącz kabel zasilający przełącznik;
  2. ponownie podłącz kabel zasilający do przełącznika, a następnie naciśnij i **przytrzymaj** przycisk Mode;
  3. dioda System LED na krótko zmieni kolor na pomarańczowy, następnie na ciągły zielony, wtedy puść **przycisk** Mode.

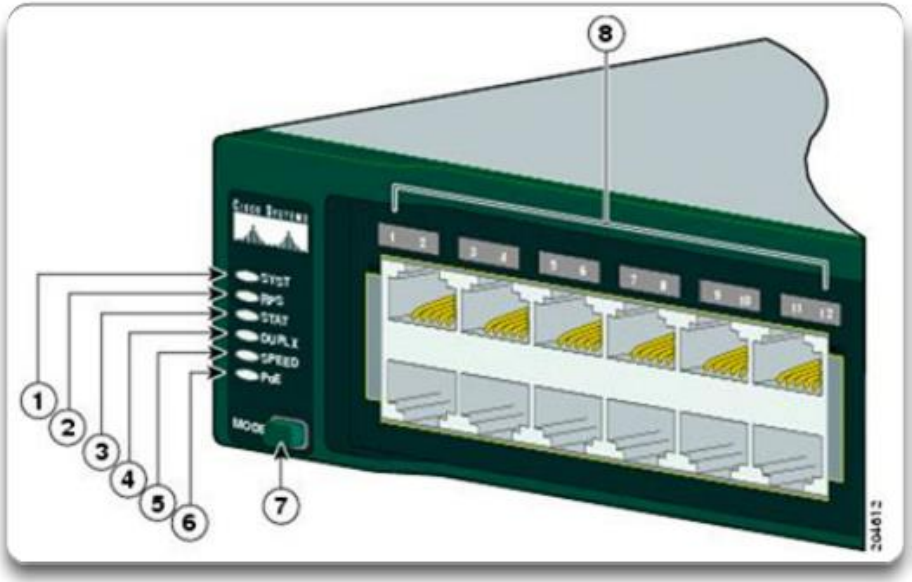
- W oprogramowaniu emulatora terminala na PC pojawia się **`switch:prompt`** programu ładującego.

Diody LED przełącznika

- Każdy port na przełączniku Cisco Catalyst ma diodę, która dostarcza wartościowych informacji związanych z rozwiązywaniem problemów.
- Domyślnie lampki LED pokazują aktywność portu, ale mogą również udzielać informacji na temat przełącznika za pomocą **przycisku** Mode.
- Na przełącznikach Cisco Catalyst 2960 dostępne są następujące tryby:
  - System LED,
  - Redundant Power System (RPS) LED,
  - Port Status LED,
  - Port Duplex LED,
  - Port Speed LED,
  - Power over Ethernet (PoE) Mode LED.

Podstawowa konfiguracja Przełącznika

Tryby przełącznika Cisco Catalyst 2960



Diody LED na przełączniku Catalyst 2960

1	Dioda LED systemowa	5	Dioda LED szybkości portu
2	Dioda LED awaryjnego zasilania RPS (jeśli jest dostępne w przełączniku).	6	Dioda LED statusu PoE (jeśli PoE jest dostępne w przełączniku)
3	Dioda LED statusu portu (tryb domyślny).	7	Przycisk wyboru trybu
4	Dioda LED trybu duplex portu	8	Diody LED portów

Przygotowanie do podstaw zarządzania przełącznikami

- Aby zdalnie zarządzać przełącznikiem, musi on mieć skonfigurowany dostęp do sieci.
- Należy skonfigurować adres IP i maskę podsieci.
- Jeśli zarządzamy przełącznikiem ze zdalnej sieci, musi być skonfigurowana brama domyślna.
- Informacje IP (adres, maska podsieci, brama) mają być przypisane do interfejsu wirtualnego przełącznika (SVI).
- Chociaż te ustawienia IP umożliwiają zdalne zarządzanie i zdalny dostęp do przełącznika, nie pozwalają na routing pakietów w warstwie 3.

Przygotowanie do podstaw zarządzania przełącznikami (cd.)

Konfiguracja interfejsu zarządzania przełącznikiem

Polecenia IOS dla przełącznika Cisco	
Przejdź do trybu konfiguracji globalnej.	`S1# configure terminal`
Przejdź w tryb konfiguracji interfejsu dla SVI.	`S1(config)# interface vlan 99`
Skonfiguruj adres IP interfejsu zarządzania.	`S1(config-if)# ip address 172.17.99.11 255.255.0.0`
Włącz interfejs zarządzania.	`S1(config-if)# no shutdown`
Powróć do trybu uprzywilejowanego EXEC.	`S1(config-if)# end`
Zapisz bieżącą konfigurację do konfiguracji startowej.	`S1# copy running-config startup-config`

Przygotowanie do podstaw zarządzania przełącznikami (cd.)

Skonfiguruj bramę domyślną przełącznika

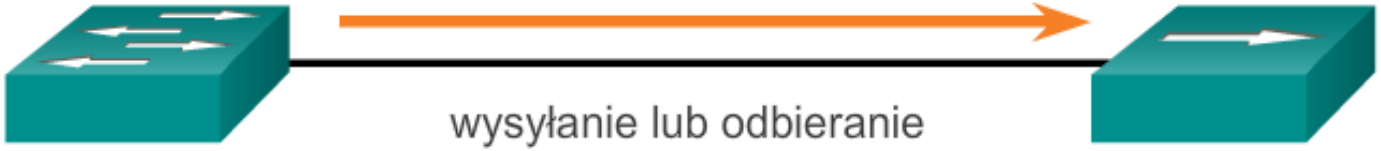
Polecenia IOS dla przełącznika Cisco	
Przejdź do trybu konfiguracji globalnej.	`S1# configure terminal`
Dla przełącznika skonfiguruj bramę domyślną.	`S1(config)# ip default-gateway 172.17.99.1`
Powróć do trybu uprzywilejowanego EXEC.	`S1(config-if)# end`
Zapisz bieżącą konfigurację do konfiguracji startowej.	`S1# copy running-config startup-config`

Konfiguracja portów przełącznika

Komunikacja duplex

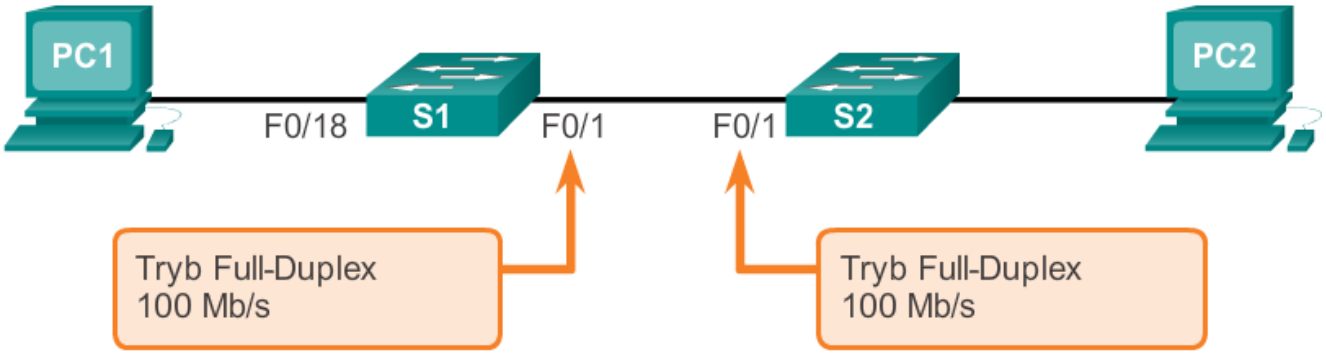
Komunikacja w trybie full duplex

Komunikacja w trybie half duplex



Konfiguracja portów przełącznika

Konfigurowanie trybu dupleksu i szybkości



Polecenia IOS dla przełącznika Cisco	
Przejdź do trybu konfiguracji globalnej.	`S1# configure terminal`
Przejdź do trybu konfigurowania interfejsu.	`S1(config)# interface FastEthernet 0/1`
Skonfiguruj interfejs w trybie duplex.	`S1(config-if)# duplex full`
Skonfiguruj szybkość interfejsu.	`S1(config-if)# speed 100`
Wróć do trybu uprzywilejowanego EXEC.	`S1(config-if)# end`
Zapisz bieżącą konfigurację do konfiguracji startowej.	`S1# copy running-config startup-config`

Funkcja Auto-MDIX

- Do niedawna w przypadku podłączania urządzeń, wymagane były określone rodzaje kabli (proste lub z przeplotem).
- Korzystanie z opcji automatic medium-dependent interface crossover (auto-MDIX) interfejsu umożliwia wyeliminowanie tego problemu.
- Gdy jest włączony auto-MDIX, interfejs automatycznie wykrywa wymagany rodzaj połączenia kablowego i odpowiednio konfiguruje połączenie.
- Podczas korzystania z auto-MDIX na interfejsie, prędkość interfejsu i dupleksu musi być ustawiona na **auto**.

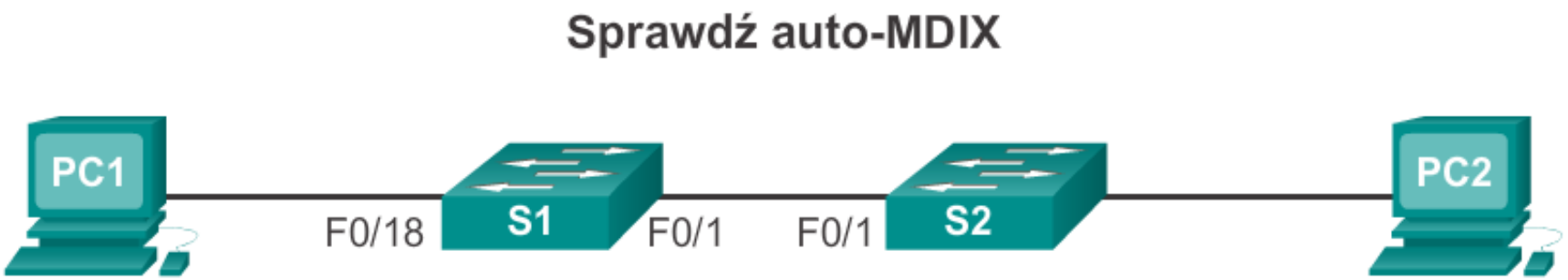
Konfiguracja portów przełącznika

Funkcja Auto-MDIX (cd.)

Sprawdź auto-MDIX

Polecenia IOS dla przełącznika Cisco	
Przejdź do trybu konfiguracji globalnej.	`S1# configure terminal`
Przejdź do trybu konfigurowania interfejsu.	`S1(config)# interface fastethernet 0/1`
Skonfiguruj interfejs do automatycznej negocjacji trybu duplex z podłączonym urządzeniem.	`S1(config-if)# duplex auto`
Skonfiguruj interfejs do automatycznej negocjacji szybkości z podłączonym urządzeniem	`S1(config-if)# speed auto`
Włącz auto-MDIX na interfejsie.	`S1(config-if)# mdix auto`
Wróć do trybu uprzywilejowanego EXEC.	`S1(config-if)# end`
Zapisz bieżącą konfigurację do konfiguracji startowej.	`S1# copy running-config startup-config`

Funkcja Auto-MDIX (cd.)




```
S1# show controllers ethernet-controller fa 0/1 phy | include
Auto-MDIX
 Auto-MDIX      :  On    [AdminState=1    Flags=0x00056248]
S1#
```

Weryfikowanie konfiguracji portów przełącznika

Polecenia sprawdzające

Polecenia IOS dla przełącznika Cisco	
Wyświetla informacje o stanie i konfiguracji interfejsu.	S1# **show interfaces** [*interface-id*]
Wyświetla konfigurację startową.	S1# **show startup-config**
Wyświetla bieżącą konfigurację.	S1# **show running-config**
Wyświetla informację o systemie plików pamięci flash.	S1# **show flash**
Wyświetla status sprzętu i oprogramowania.	S1# **show version**
Wyświetla historię wprowadzonych poleceń.	S1# **show history**
Wyświetla informacje związane z adresem IP interfejsu.	S1# **show ip** [*interface-id*]
Wyświetla tablicę adresów MAC przełącznika.	S1# **show mac-address-table** lub S1# **show mac address-table**

Problemy w warstwie dostępu do sieci

Wyświetlanie informacji o stanie i statystyce interfejsu.

```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is upHardware is Fast
Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)MTU
1500 bytes, BW 100000 Kbit, DLY 100 usec,
<wyniki pominięto>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 0 runts, 0 giants, 0
  throttles
  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 68 multicast, 0 pause input
  0 input packets with dribble condition detected
  3594664 packets output, 436549843 bytes, 0 underruns
  8 output errors, 1790 collisions, 10 interface resets
  0 unknown protocol drops
  0 babbles, 235 late collision, 0 deferred
<wyniki pominięto>
```

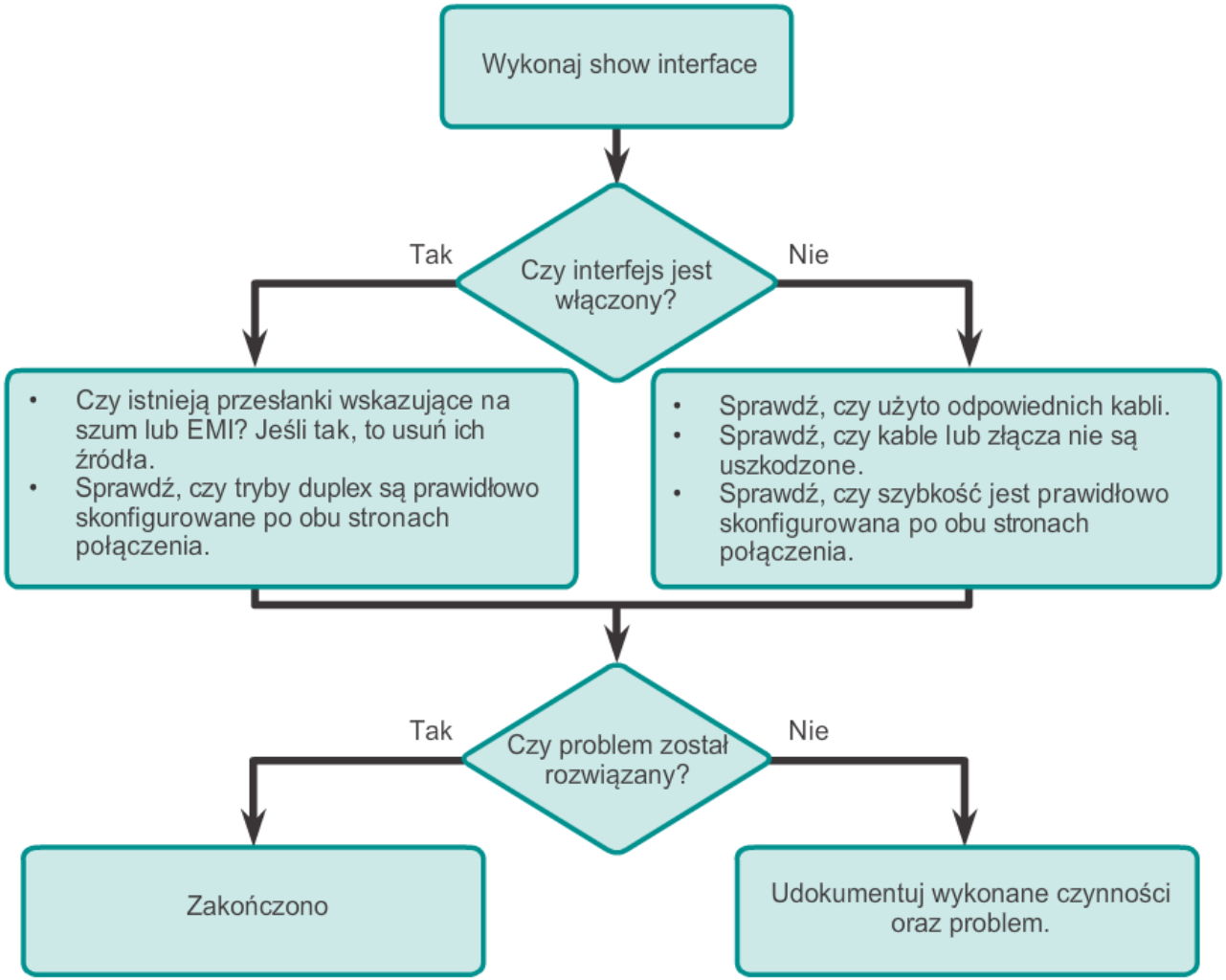
Problemy w warstwie dostępu do sieci (cd.)

Problemy związane z warstwą dostępu do sieci

Typ błędu	Opis
Błędy wejścia	Ogólna liczba błędów. Zawiera błędy o za krótkich (runts) i za długich (giants) ramkach, nie zbuforowanych ramkach, CRC, błędach ramki, liczniki nadpisania (overrun) i zignorowania ramki (ignored).
Runts	Pakiety są pomijane, ponieważ są mniejsze niż minimalny rozmiar pakietu dla danego medium. Na przykład, każdy pakiet Ethernet, który jest mniejszy niż 64 bajty jest uważany za "runt".
Giants	Pakiety są pomijane, ponieważ są większe niż maksymalny rozmiar pakietu dla danego medium. Na przykład, każdy pakiet Ethernet, który jest większy niż 1,518 bajtów jest uważany za "giant".
CRC	Błędy CRC są generowane gdy obliczona suma kontrolna nie jest taka sama jak suma kontrolna otrzymana.
Output Errors	Suma wszystkich błędów, które uniemożliwiły ostateczne przekazywanie datagramów z interfejsu, który jest sprawdzany.
Collisions	Liczba komunikatów retransmitowanych z powodu kolizji w sieci Ethernet.
Late Collisions	Kolizje które występują po 512 bitach ramki która została przesłana.

Rozwiązywanie problemów

Rozwiązywanie problemów związanych z mediami przełączanymi



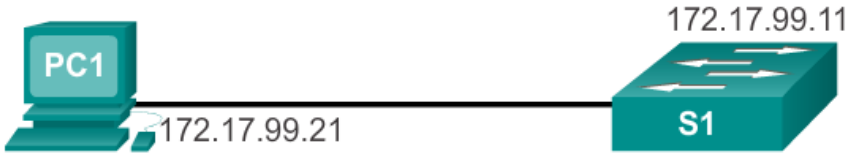
Bezpieczny zdalny dostęp

Obsługa SSH

- Secure Shell (SSH) jest protokołem zapewniającym bezpieczne (zaszyfrowane) połączenie do zdalnego zarządzania urządzeniem.
- SSH jest powszechnie stosowany w systemach UNIX.
- Oprogramowanie Cisco IOS również obsługuje protokół SSH.
- Aby włączyć protokół SSH w przełączniku Catalyst 2960, przełącznik musi używać wersji oprogramowania IOS zawierającego (zaszyfrowane) funkcje i możliwości kryptograficzne.
- Ze względu na silne właściwości szyfrowania protokół SSH powinien zastąpić Telnet przy zarządzaniu połączeniami.
- Domyślnie protokół SSH korzysta z TCP port 22. Telnet korzysta z TCP port 23.

Obsługa SSH (cd.)

Połączenie SSH do zdalnego zarządzania przełącznikiem



172.17.99.11 - PuTTY

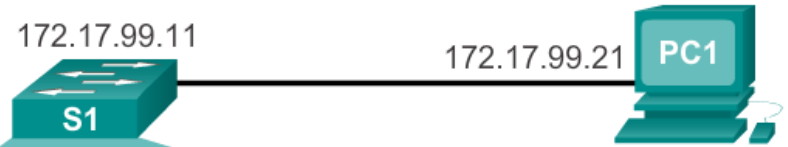
```
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1>enable
Password:
S1#
```

Bezpieczny zdalny dostęp

Konfigurowanie SSH

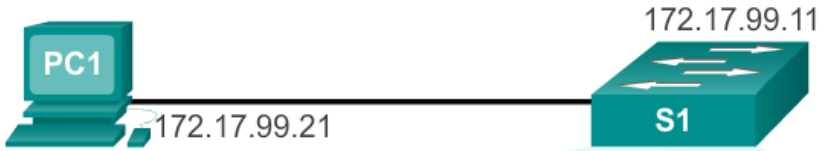
Konfigurowanie SSH do zdalnego zarządzania przełącznikiem




```
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin secret ccna
S1(config-line)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2
S1(config)# exit
S1#
```

Weryfikacja SSH

Sprawdzanie ustawień i stanu SSH




```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption  Hmac       State         Username
0          2.0     IN   aes256-cbc  hmac-sha1 Session started admin
0          2.0     OUT  aes256-cbc  hmac-sha1 Session started admin
%No SSHv1 server connections running.
S1#
```

Zalewanie adresami MAC

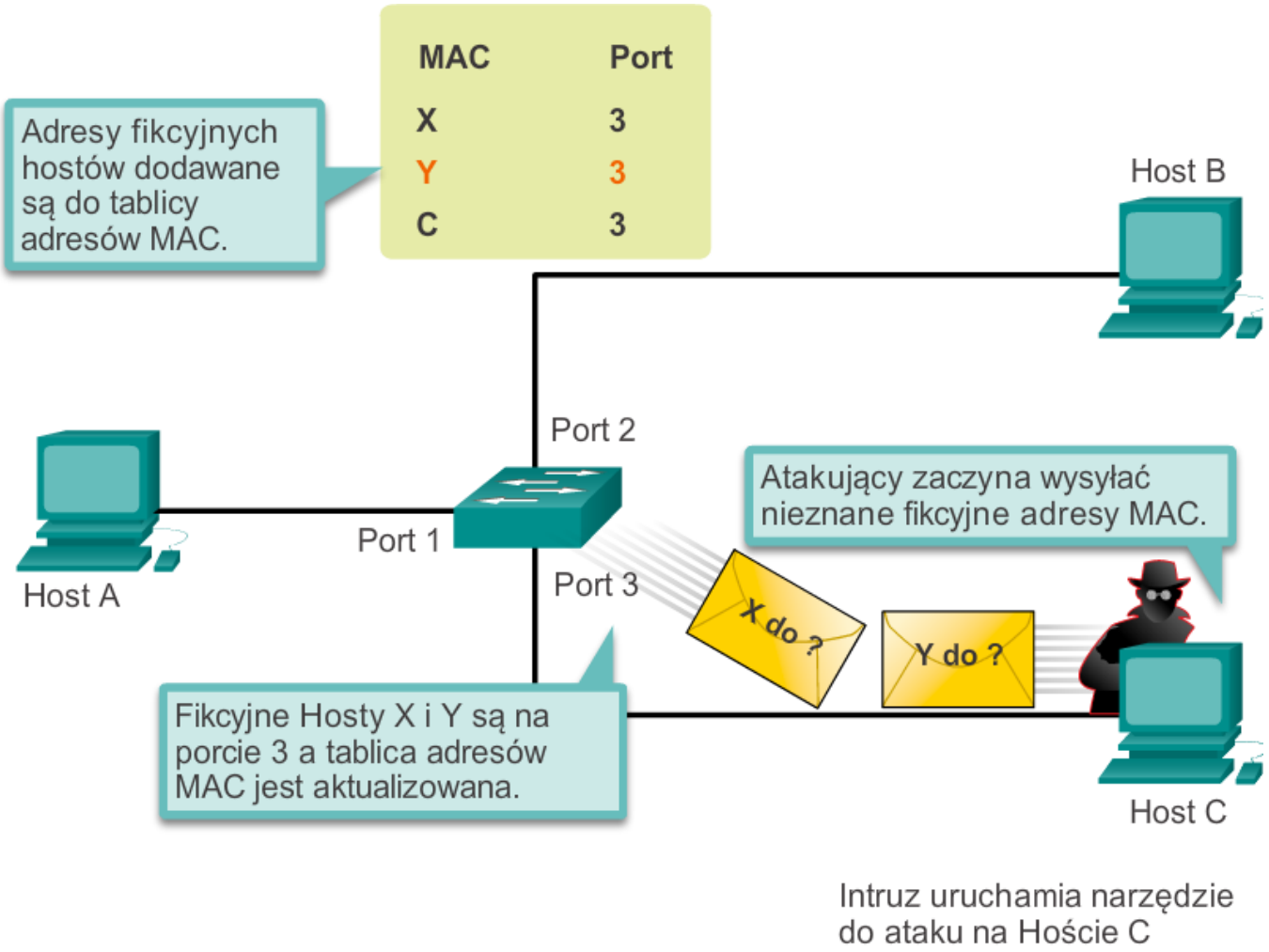
- Przełączniki automatycznie wypełniają swoje tabele CAM, obserwując ruch wprowadzany do ich portów.
- Przełączniki przesyłają ruch przez wszystkie porty, jeśli nie mogą znaleźć docelowego adresu MAC w swojej tablicy CAM.
- W takich warunkach przełącznik działa jako koncentrator. Ruch unicast może być identyfikowany przez wszystkie urządzenia podłączone do przełącznika.
- Dokonujący ataku może wykorzystać ten problem, aby uzyskać dostęp do normalnie kontrolowanego ruchu przez przełącznik za pomocą komputera, by uruchomić narzędzie do zalewania adresów MAC.

Zalewanie adresami MAC (cd.)

- Takie narzędzie jest programem stworzonym do generowania i wysyłania ramek z fałszywego źródła adresów MAC do portu przełącznika.
- Gdy ramki te dotrą do przełącznika, dodaje on fałszywy adres MAC do swojej tablicy CAM, odnotowując port, z którego przybyły ramki.
- Ostatecznie tabela CAM wypełnia się fałszywymi adresami MAC.
- Tabela CAM nie ma obecnie miejsca na właściwe urządzenia obecne w sieci, a zatem nie znajduje ich adresów MAC w tabeli CAM.
- Wszystkie ramki są teraz przekazywane do wszystkich portów, co pozwala dokonującemu atak na dostęp do ruchu innych hostów.

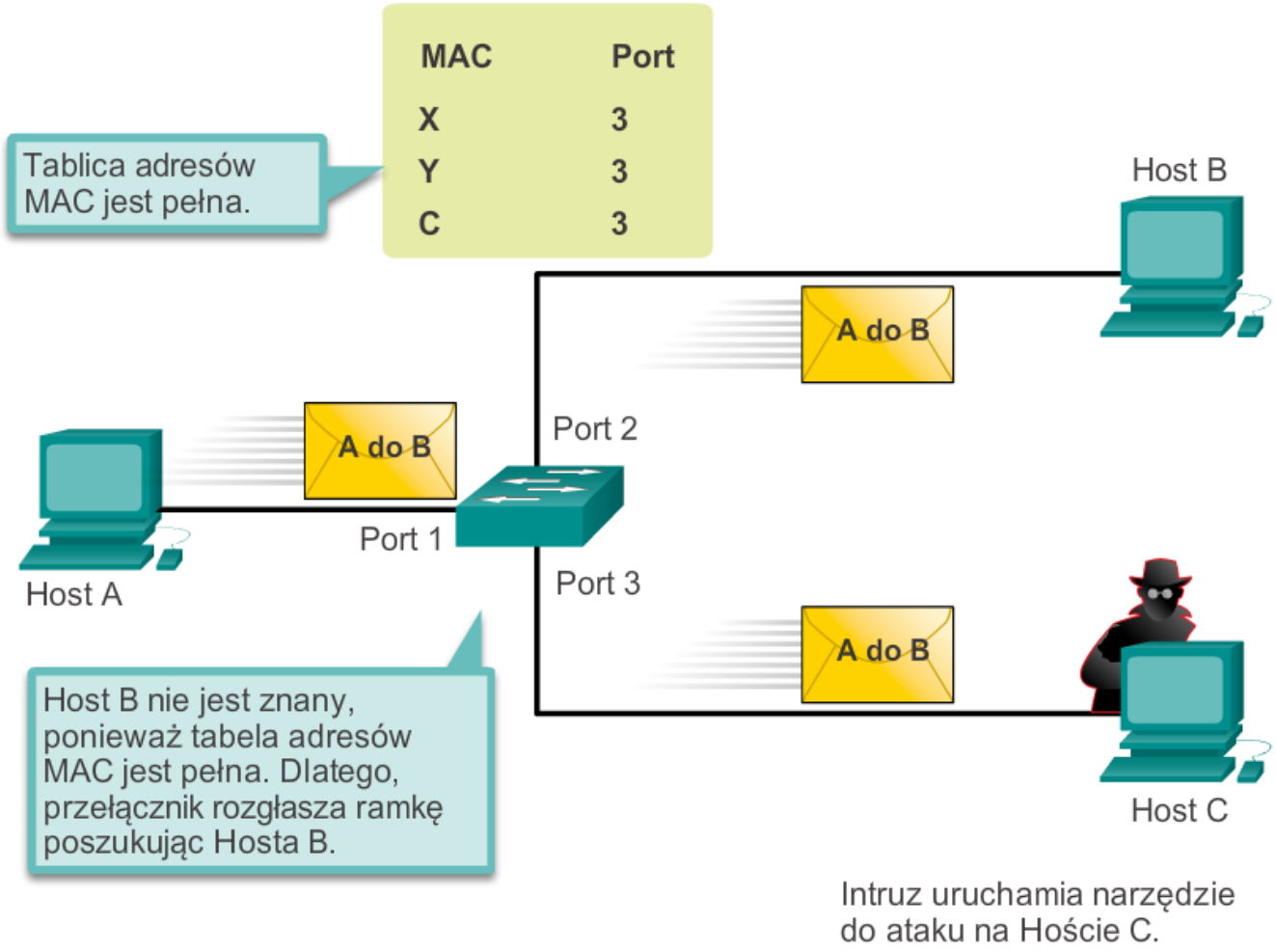
Zalewanie adresami MAC (cd.)

Dokonujący ataku zapełnia tabelę MAC fałszywymi wpisami.



Zalewanie adresami MAC (cd.)

Przełącznik teraz zachowuje się jak koncentrator.

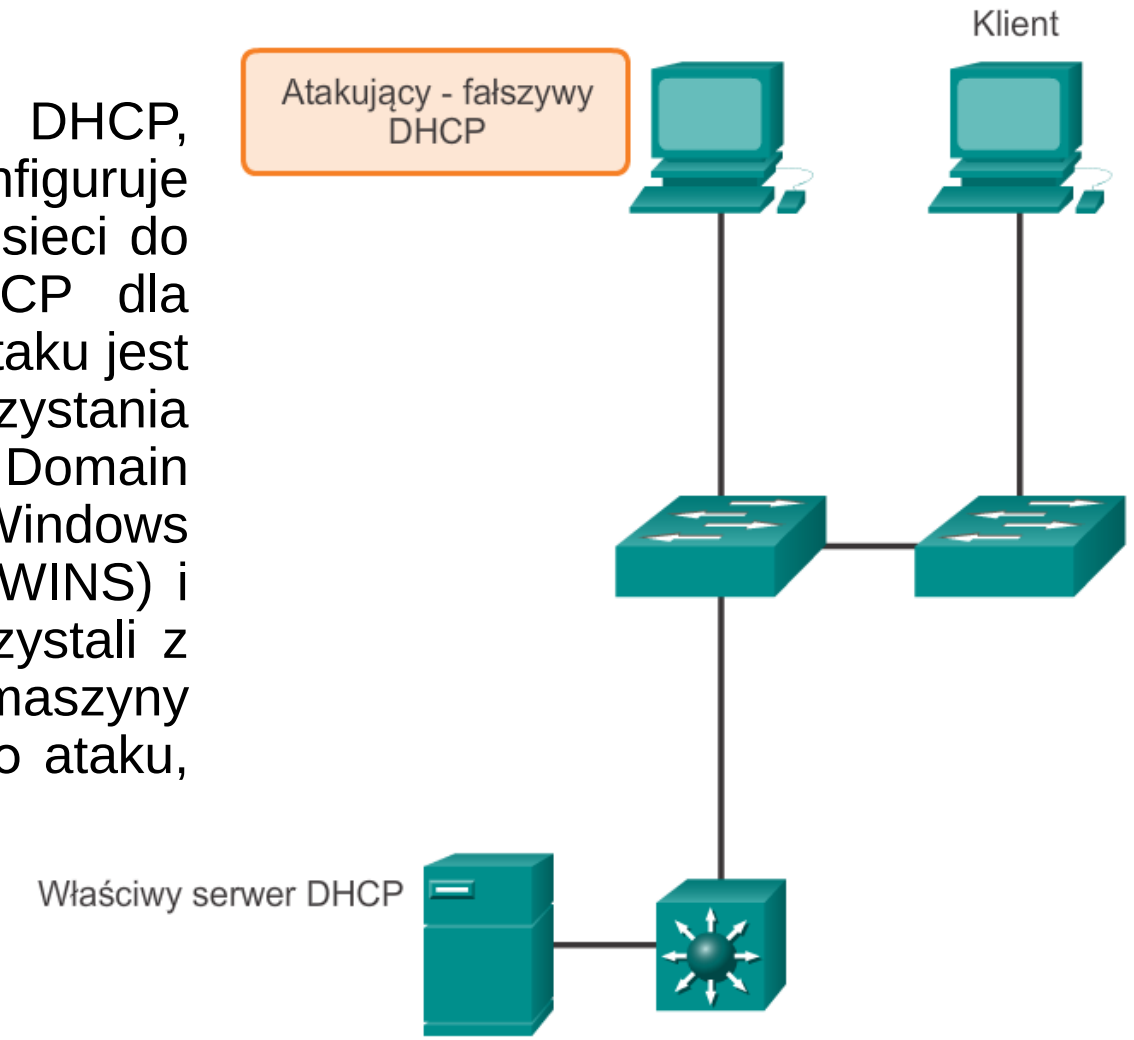


DHCP Spoofing

- DHCP to protokół sieciowy używany do automatycznego przypisywania informacji IP.
- Istnieją dwa typy ataków DHCP:
  - DHCP spoofing,
  - DHCP starvation.
- W ataku typu DHCP spoofing w sieci umieszczony jest fałszywy serwer DHCP do wydawania adresów DHCP dla klientów.
- Atak DHCP starvation jest często używany przed fałszowaniem DHCP, by odmówić usługi do uprawnionego serwera DHCP.

Atak DHCP Spoofing

W atakach fałszowania DHCP, dokonujący ataku konfiguruje fałszywy serwer DHCP w sieci do wydawania adresów DHCP dla klientów. Powodem tego ataku jest zmuszenie klientów do korzystania z fałszywych serwerów Domain Name System (DNS) lub Windows Internet Naming Service (WINS) i sprawienie, by klienci korzystali z dokonującego ataku lub maszyny pod kontrolą dokonującego ataku, jako bramy domyślnej.



Wykorzystywanie protokołu Cisco Discovery

- Cisco Discovery Protocol jest protokołem firmy Cisco, który umożliwia gromadzenie informacji o bezpośrednio połączonych urządzeniach Cisco.
- Protokół Cisco Discovery jest zaprojektowany tak, aby umożliwić urządzeniom do auto-konfiguracji ich połączenia.
- Jeśli dokonujący ataku nasłuchuje wiadomości protokołu Cisco Discovery, może on dowiedzieć się o istotnych informacjach o modelu urządzenia i bieżącej wersji oprogramowania.

Uwaga: Cisco zaleca wyłączenie CDP, jeżeli nie jest używany.

Wykorzystywanie protokołu Telnet

- Protokół Telnet jest niebezpieczny i powinien zostać zastąpiony przez protokół SSH.
- Dokonujący ataku może użyć protokołu Telnet w ramach innych ataków:
  - atak Brute Force Password,
  - atak Telnet DOS.
- Gdy hasło nie może zostać przechwycone, dokonujący ataku wypróbuje tyle kombinacji znaków, ile to tylko możliwe. Ta próba odgadnięcia hasła jest znana jako atak brute force password.
- Telnet może być zastosowany w celu przetestowania odgadniętego hasła przeciw systemowi.

Wykorzystywanie protokołu Telnet (cd.)

- W ataku Telnet DoS sprawca wykorzystuje lukę w oprogramowaniu serwera Telnet, który działa na przełączniku i sprawia, że usługa Telnet jest niedostępna.
- Ten rodzaj ataku uniemożliwia administratorowi funkcje zarządzania zdalnego dostępu do przełącznika.
- Może on być połączony z innymi bezpośrednimi atakami na sieć w ramach skoordynowanej próby uniemożliwienia dostępu administratorowi sieci do podstawowych urządzeń podczas ataku.
- Luki w usłudze Telnet, które pozwalają na przeprowadzanie ataków DoS, są zazwyczaj eliminowane w poprawkach dodawanych do nowych wydań systemu Cisco IOS.

Najlepsze praktyki w bezpieczeństwie

10 najlepszych praktyk:

- opracuj pisemną politykę bezpieczeństwa dla organizacji,
- wyłącz zbędne usługi i porty,
- używaj silnych haseł i zmieniaj je często,
- kontroluj fizyczny dostęp do urządzenia,
- użyj protokołu HTTPS zamiast HTTP,
- wykonuj kopię zapasową na bieżąco,
- edukuj pracowników o atakach socjotechnicznych,
- szyfruj i zabezpieczaj hasłem dane poufne,
- zastosuj zapory firewall,
- aktualizuj oprogramowanie na bieżąco.

Narzędzia bezpieczeństwa sieci

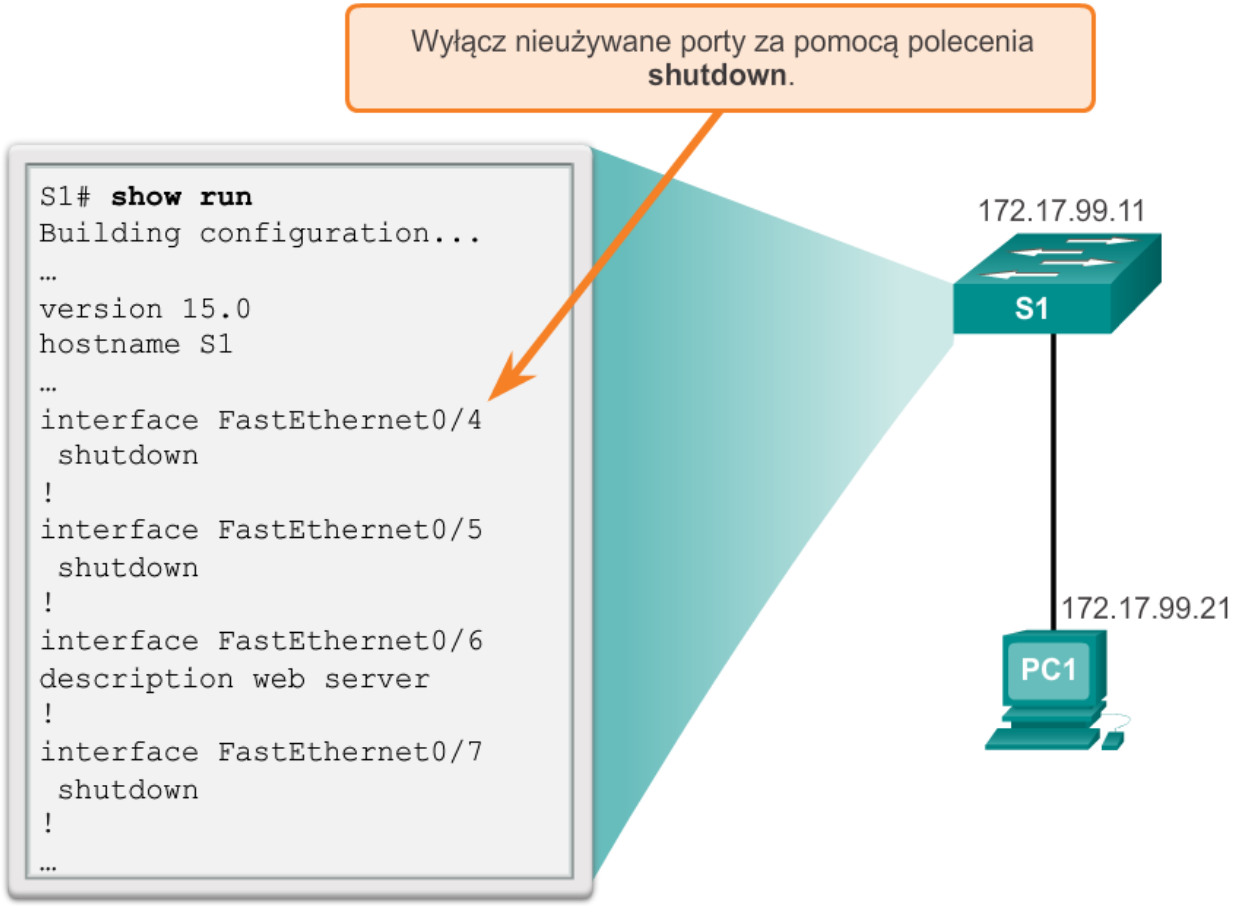
- Narzędzia bezpieczeństwa sieci są ważne dla administratorów sieci.
- Narzędzia bezpieczeństwa sieci umożliwiają administratorowi sprawdzenie siły zastosowanych środków bezpieczeństwa.
- Administrator może przypuścić atak na sieć i przeanalizować wyniki oraz określić, jak dostosować zasady bezpieczeństwa w celu ograniczenia tych rodzajów ataków.
- Inspekcja zabezpieczeń i testy penetracyjne to dwie podstawowe funkcje wykonywane przez narzędzia testujące bezpieczeństwo sieci.

Narzędzia bezpieczeństwa sieci

- Narzędzia bezpieczeństwa sieci mogą być wykorzystane do badania sieci.
- Poprzez monitorowanie sieci administrator może ocenić, jakiego rodzaju informacje atakujący będzie w stanie zebrać. Na przykład atakując i zalewając tabelę CAM przełącznika, administrator może dowiedzieć się, które porty przełącznika są narażone na zalewanie MAC i może skorygować ten problem.
- Narzędzia do ochrony sieci mogą być również stosowane do testowania penetracji sieci. Testy penetracyjne symulują atak na sieć w celu określenia wrażliwości sieci na prawdziwy atak.
- Uchybienia w konfiguracji urządzeń sieciowych można zidentyfikować na podstawie wyników testów penetracji.
- Mogą być dokonywane zmiany, by urządzenia były bardziej odporne na ataki.
- Takie testy mogą uszkodzić sieć i powinny być przeprowadzane w kontrolowanych warunkach.
- Idealny do tego celu jest test off-line, który naśladuje aktualnie pracującą rzeczywistą sieć.

Zabezpieczenie nieużywanych portów

Skuteczną i prostą wytyczną dotyczącą bezpieczeństwa jest wyłączenie nieużywanych portów.

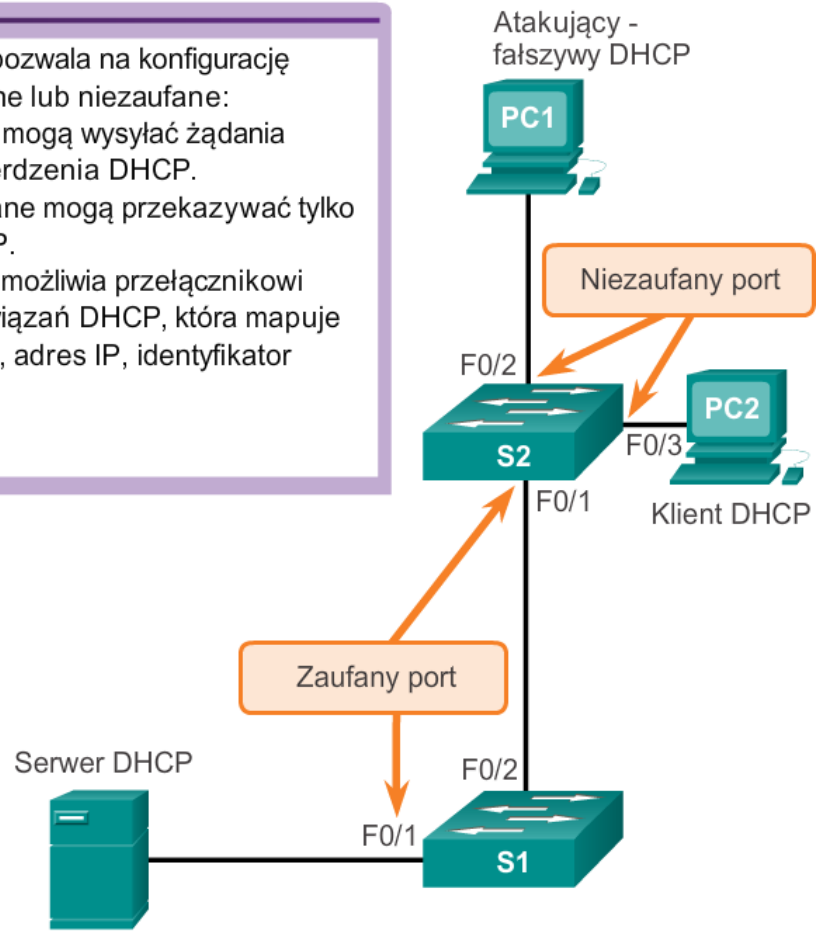


Zabezpieczenia portów przełącznika

DHCP Snooping

Funkcja ingerencji w DHCP właściwa dla przełączników Cisco Catalyst pozwala określić, które porty mogą odpowiadać na żądania DHCP.

- Snooping DHCP pozwala na konfigurację portów jako zaufane lub niezaufane:
  - Zaufane porty mogą wysyłać żądania DHCP i potwierdzenia DHCP.
  - Porty niezaufane mogą przekazywać tylko żądania DHCP.
- DHCP snooping umożliwia przełącznikowi budowę tabeli powiązań DHCP, która mapuje adres MAC klienta, adres IP, identyfikator VLAN i ID portu.




```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20
S1(config)# interface fastethernet 0/1
S1(config-if)# ip dhcp snooping trust
S1(config)# interface fastethernet 0/2
S1(config-if)# ip dhcp limit rate 5
```

Zabezpieczenia portów (operacje)

- Zabezpieczenia portu ograniczają liczbę poprawnych adresów MAC obsługiwanych przez port.
- Tylko autoryzowane adresy MAC mają dostęp do sieci, podczas gdy inne adresy MAC są odrzucane.
- Wszystkie dodatkowe próby połączenia przez nieznane adresy MAC naruszają zasady bezpieczeństwa.
- Bezpieczne adresy MAC mogą być skonfigurowany na wiele sposobów:
  - bezpieczne statyczne adresy MAC,
  - bezpieczne dynamiczne adresy MAC,
  - przyklejone (ang. sticky) adresy MAC.

Zabezpieczenia portów (tryby naruszenia)

- IOS uzna naruszenie zasad bezpieczeństwa w przypadku wystąpienia jednej z tych sytuacji:
  - maksymalna liczba bezpiecznych adresów MAC dla tego interfejsu została dodana do CAM oraz stacji, której adres MAC nie znajduje się w tablicy adresów, próbując uzyskać dostęp do interfejsu,
  - rozpoznany lub skonfigurowany adres na zabezpieczonym interfejsie pojawi się na innym zabezpieczonym interfejsie w tej samej sieci VLAN.
- Istnieją trzy możliwe działania podejmowane w przypadku wykrycia naruszenia zasad bezpieczeństwa:

  chronić, ograniczać, zamknąć.

Domyślne zabezpieczenia portów dynamicznych

Cecha	Ustawienie domyślne
Zabezpieczenie portów	Wyłączone na porcie
Maksymalna liczba bezpiecznych adresów MAC	1
Rodzaju akcji w przypadku naruszenia zasad bezpieczeństwa	shutdown Port wyłącza się, gdy zostanie przekroczona maksymalna liczba bezpiecznych adresów MAC.
"Przyklejanie" adresów	wyłączone

Konfiguracja zabezpieczeń portów dynamicznych

Konfigurowanie trybu Dynamic Port Security

Linia poleceń Cisco IOS	
Określ interfejs do konfiguracji zabezpieczenia portu.	`S1(config)# interface fastethernet 0/18`
Ustaw tryb dostępowy interfejsów.	`S1(config-if)# switchport mode access`
Włącz funkcję port security na interfejsie.	`S1(config-if)# switchport port-security`

Zabezpieczenia portów przełącznika

Konfiguracja zabezpieczeń portów przyklejonych

Konfiguracja funkcji Sticky Port Security

Linia poleceń Cisco IOS	
Określ interfejs do konfiguracji zabezpieczenia portu.	`S1(config)# interface fastethernet 0/19`
Ustaw tryb dostępowy interfejsów.	`S1(config-if)# switchport mode access`
Włącz funkcję port security na interfejsie.	`S1(config-if)# switchport port-security`
Ustaw maksymalną liczbę dozwolonych bezpiecznych adresów na porcie.	`S1(config-if)# switchport port-security maximum 50`
Włącz funkcję sticky learning.	`S1(config-if)# switchport port-security mac-address sticky`

Zabezpieczenia portów przełącznika

Weryfikacja zabezpieczeń portów przyklejonych

Sprawdzanie przyklejonego adresu MAC

```
S1# show port-security interface fastethernet 0/19
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 10
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0025.83e6.4b02:1
Security Violation Count   : 0
```

Weryfikacja zabezpieczeń portów przyklejonych - działająca konfiguracja

Sprawdzanie przyklejonego adresu MAC w konfiguracji bieżącej

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 10
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

Weryfikacja zabezpieczeń portów - bezpieczne adresy MAC

Sprawdzanie bezpiecznych adresów MAC

```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type              Ports   Remaining Age
                                                      (mins)
----    -----------       ----              -----   -------------
1       0025.83e6.4b01    SecureDynamic     Fa0/18       -
1       0025.83e6.4b02    SecureSticky      Fa0/19       -
------------------------------------------------------------------
```

Porty w stanie wyłączenia po błędzie

- Port z naruszeniem bezpieczeństwa przechodzi w stan wyłączenia po błędzie.
- Gdy port jest wyłączony z powodu błędu, jest on wyłączony w OIS.
- Przełącznik przekazuje zdarzenia za pośrednictwem komunikatów z konsoli.

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

Porty w stanie wyłączenia po błędzie (cd.)

Polecenie **`show interface`** pokazuje również port przełącznika w stanie wyłączenia po błędzie.

```
S1# show interface fa0/18 status
Port Name   Status         Vlan   Duplex   Speed    Type
Fa0/18      err-disabled   1      auto     auto     10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.292b.4c75:1
Security Violation Count   : 1
```

Porty w stanie wyłączenia po błędzie (cd.)

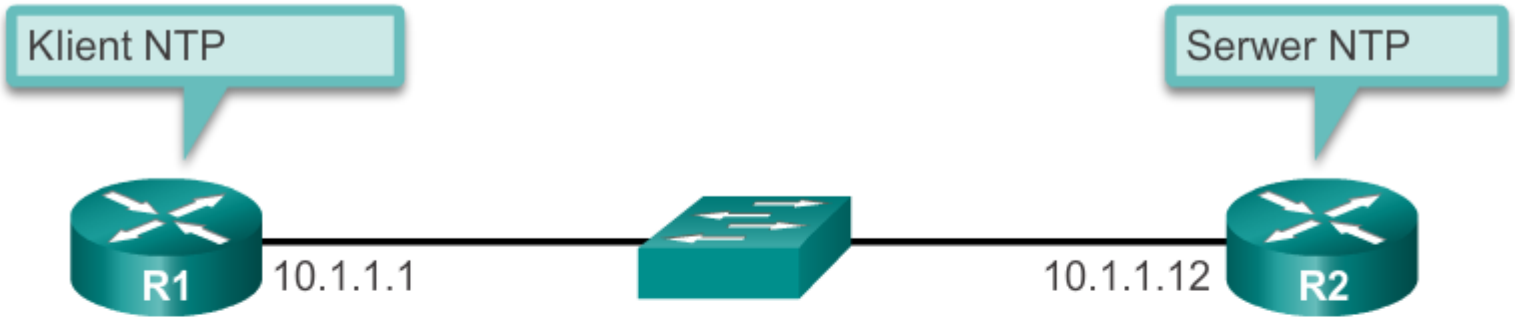
Polecenie **shutdown** lub **no shutdown** musi być wykonane ponownie w trybie konfiguracji interfejsu, by ponownie włączyć port.

```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to up
```

Network Time Protocol

- Network Time Protocol (NTP) jest używany do synchronizacji zegarów w sieci danych systemów komputerowych.
- NTP może uzyskać prawidłowy czas z wewnętrznego lub zewnętrznego źródła czasu.
- Źródłem czasu może być:
  - lokalny zegar wzorcowy,
  - internetowy zegar wzorcowy,
  - GPS lub zegar atomowy.
- Urządzenie sieciowe może być skonfigurowane jako serwer NTP lub klient NTP.
- Przejrzyj notatki ze slajdów, aby uzyskać więcej informacji na temat NTP.

Konfiguracja NTP




```
R1(config)# ntp master 1
```

```
R2(config)# ntp server 10.1.1.1
```

Weryfikacja NTP

```
R2# show ntp associations
  address         ref clock       st   when   poll reach   delay   offs
*~10.1.1.1        .LOCL.           1     13     64   377    1.472   6.07
sys.peer,    # selected,    + candidate, - outlyer,   x falsetick
```

```
R2# show ntp status
Clock is synchronized, stratum 2, reference is 10.1.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz,
precision is 2**17reference time is D40ADC27.E644C776
(13:18:31.899 UTC Mon Sep 24 2012)clock offset is 6.0716
msec,
root delay is 1.47 msecroot dispersion is 15.41 msec,
peer dispersion is 3.62 msecloopfilter state is 'CTRL'
(Normal Controlled Loop), drift is 0.000000091 s/ssystem poll
interval is 64, last update was 344 sec ago.
```

Rozdział 2: Podsumowanie

W tym rozdziale nauczyłeś się:

- o sekwencji rozruchowej przełącznika,
- o trybach lampek LED przełącznika,
- jak uzyskać zdalny dostęp i zarządzać przełącznikiem za pośrednictwem bezpiecznego połączenia,
- o trybach duplexu przełącznika,
- o zabezpieczeniach portu przełącznika, trybach jego naruszenia i działania.
- o najlepszych praktykach dla sieci przełączanych.