Bezpečnost počítačové sítě kampusu

CCNP SWITCH

Cisco | Networking Academy®
Mind Wide Open™

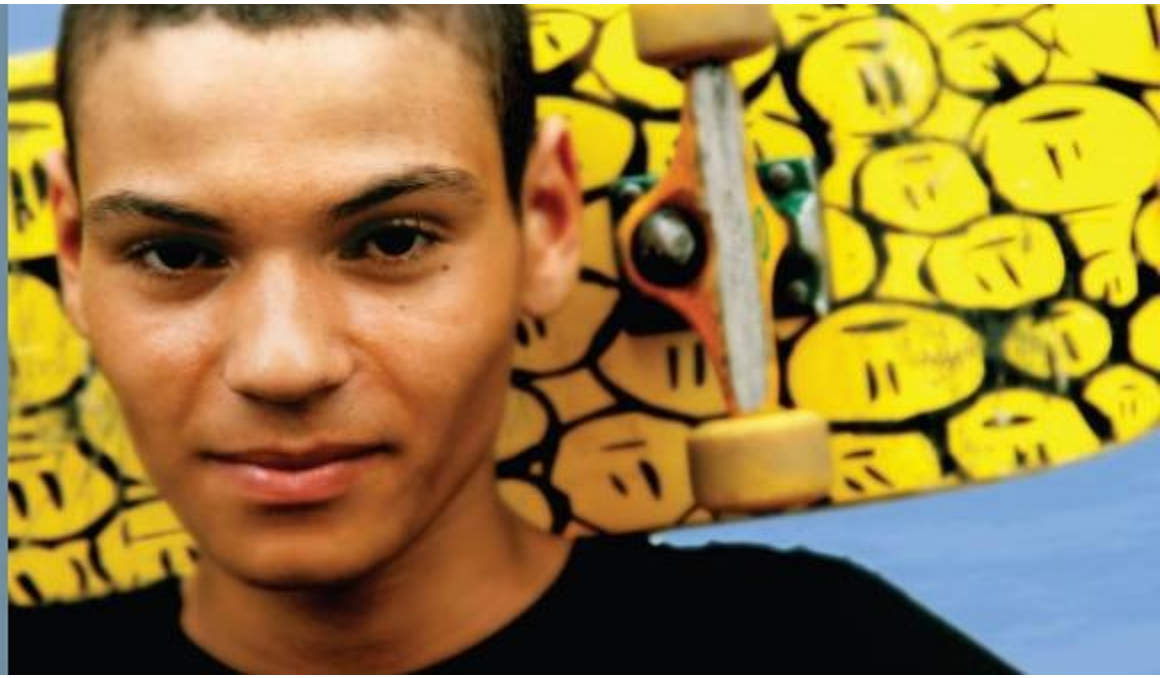
© 2007 – 2016, Cisco Systems, Inc. All rights reserved. Cisco Public

Cíle kapitoly 10

Tato kapitola obsahuje následující témata:

- Přehled otázek bezpečnosti přepínačů
- Požadované osvědčené postupy pro základní bezpečnost přepínačů Catalyst
- Zranitelnosti kampusových sítí
- Bezpečnost portu
- Storm control
- Snižování účinků spoofing útoků
- DHCP snooping, IP Source Guard a dynamická ARP inspekce
- Bezpečné trunky VLAN
- Privátní VLAN

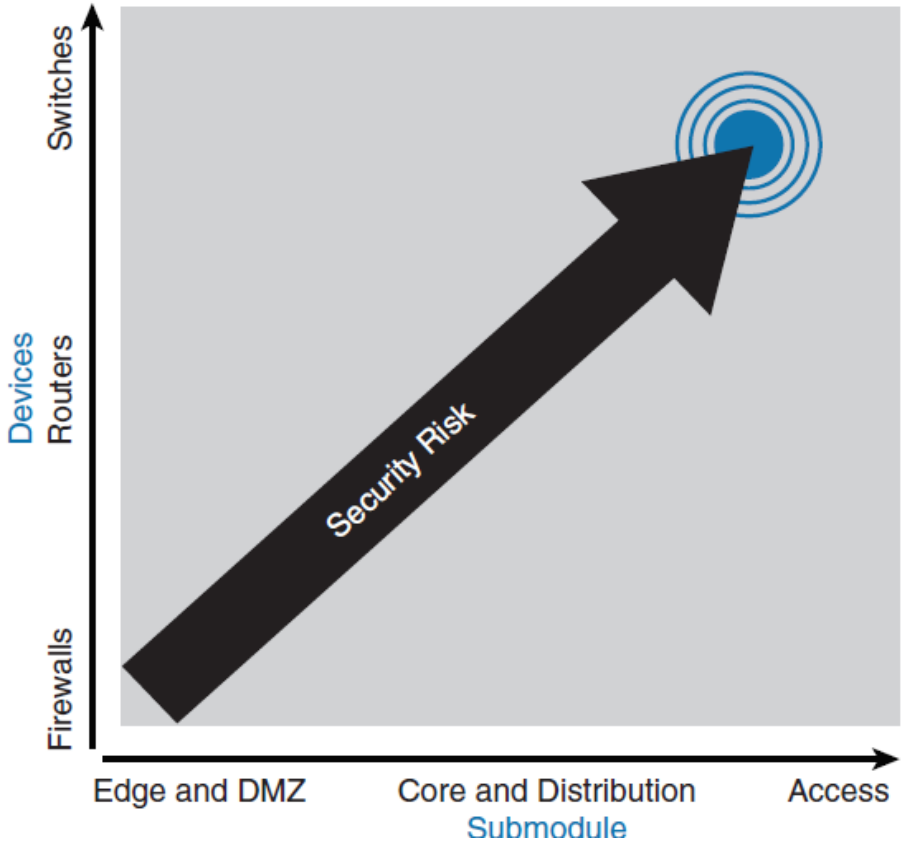
Přehled problémů bezpečnosti přepínačů



© 2007 – 2016, Cisco Systems, Inc. All rights reserved. Cisco Public

Přehled problémů bezpečnosti přepínačů

- Většina pozornosti průmyslu se zaměřuje na bezpečnostní útoky z vnější strany zdí organizace a na horní vrstvy OSI.
- Výchozí stav síťových zařízení zdůrazňuje toto zaměření na vnější ochranu a vnitřní otevřenou komunikaci.
- Pro přepínače a směrovače je k dispozici mnoho funkcí zabezpečení, ale musí být povoleno, aby byly účinné



Přehled problémů s bezpečností přepínačů

Existují důvody pro silnou ochranu infrastruktury podnikového kampusu

- Spoléhání se na bezpečnost, která byla zavedena na okraji podnikové sítě, selže. S několika vrstvami zabezpečení se zvyšuje ochrana podnikového kampusu, kde obvykle sídlí nejstrategičtější aktiva.
- Pokud podnik otevře návštěvníkům své budovy, může útočník potenciálně získat fyzický přístup k zařízením v podnikovém areálu. Spoléhání se na fyzickou bezpečnost nestačí. Velmi často se externí přístup nezastaví na podnikovém okraji.
- Aplikace vyžadují přinejmenším nepřímý přístup k prostředkům podnikového kampusu, což znamená, že je nutná také silná síťová bezpečnost.
- Veřejné a hybridní cloudové architektury představují nová rizika. I když je cloud bezpečný, útoky zevnitř mohou nakonec kompromitovat samotný cloud.

Nejlepší praktiky bezpečnosti Cisco přepínačů

Nejlepší praktiky konfigurace bezpečnosti Cisco přepínačů

- **Zabezpečená hesla**
  - Příkaz pro povolení hesla používá slabé šifrování.
  - Pokud je to možné, použijte tajné heslo.
  - Chcete-li šifrovat všechna hesla, která nelze šifrovat pomocí silného ověřování, použijte globální konfigurační příkaz pro šifrování hesel služby.
  - S externí AAA.

- **Bannery**
  - Cílem je upozornit neoprávněné uživatele, že jejich činnost by mohla být důvodem k pronásledování.
  - Použijte přihlašovací příkaz banneru.

- **Zabezpečený přístup ke konzole**
  - I když jsou přepínače obvykle umístěny v uzamčených skříních a datově řízených datových centrech, je to nejlepší postup pro konfiguraci ověřování na jakékoli konzole.

Nejlepší praktiky konfigurace bezpečnosti Cisco přepínačů

- **Zabezpečení terminálového přístupu**
  - Vždy zabezpečte vty
  - Konfigurujte ACL.

```
access-list 1 permit 10.0.0.234
access-list 1 permit 10.0.0.235
line vty 0 15
access-class 1 in
```

- **Zabezpečení webového rozhraní**
  - `no ip http server`
  - Když už to musí být, pak `ip http secure server` a zase ACL

```
access-list 1 permit 10.100.50.0 0.0.0.255
ip http secure server
ip http access-class 1
```

Nejlepší praktiky konfigurace bezpečnosti Cisco přepínačů

- **Vždy používejte Secure Shell (SSH) a zajistěte, aby byl Telnet server deaktivován**
  - Telnet je snadno ovladatelný, ale není bezpečný. Veškerý text, který je odeslán prostřednictvím relace Telnet, je předán v čistém textu.
  - SSH používá k zabezpečení dat relace silné šifrování. Měli byste použít nejvyšší verzi SSH, která je k dispozici.

- **Zabezpečený přístup k protokolu SNMP**
  - Pokud nepotřebujete přístup pro zápis přes SNMP, zakažte jej.
  - Vždy se doporučuje používat výhradně SNMPv3, který využívá bezpečné ověřování.

Nejlepší praktiky konfigurace bezpečnosti Cisco přepínačů

- **Bezpečný provoz STP**
  - Vždy byste měli povolit funkci BPDU Guard na všech access portech přepínače.
  - Nikdy konfigurovat BPDU Guard a BPDU filtr na stejném portu. Pokud tak učiníte, projeví se pouze filtr BPDU.

- **Secure Cisco Discovery Protocol (CDP)**
  - Všechna zařízení Cisco mají zpravidla ve všech portech povoleno CDP. Je třeba zakázat CDP na portech, které se připojují k vnějším sítím.
  - Navíc vždy vypněte CDP na přístupových (access) portech koncového uživatele.Pakety (advertisements) CDP jsou odesílány v čistém textu a nelze konfigurovat autentizaci.

Opakování Cisco Spanning Tree z kap. 4

Klíčové vlastnosti nástroje Cisco STP Toolkit, které zajišťují stabilitu STP, jsou následující:

BPDU Guard
Zakáže port PortFast, pokud je přijata BPDU

BPDU Filter
Ignoruje BPDU na portech, např. mezi ISO a jeho zákazníkem

Root Guard
Zabraňuje tomu, aby se externí přepínače staly rooty

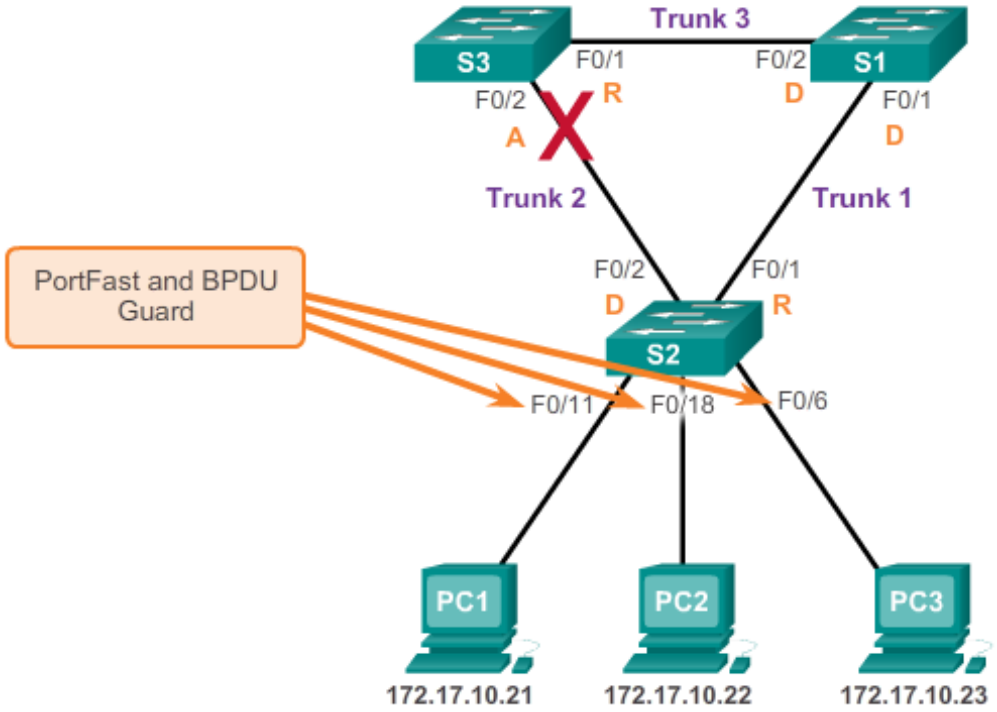
Loop Guard
Zabraňuje tomu, aby se alternativní port stal designated portem, pokud nebudou přijaty žádné BPDU

Rozdíl BPDU Guard a BPDU Filter

- **BPDU Guard** hlídá vstup BPDU do rozhraní. Jakmile je přijata první BPDU, dojde k vypnutí portu.

- **BPDU Filter** filtruje BPDU v obou směrech. Nastavení filtrování BPDU na rozhraní má stejný efekt jako zákaz spanning stromu od nežádoucích zařízení na něm a může způsobit smyčky spanning-tree.

PortFast and BPDU Guard



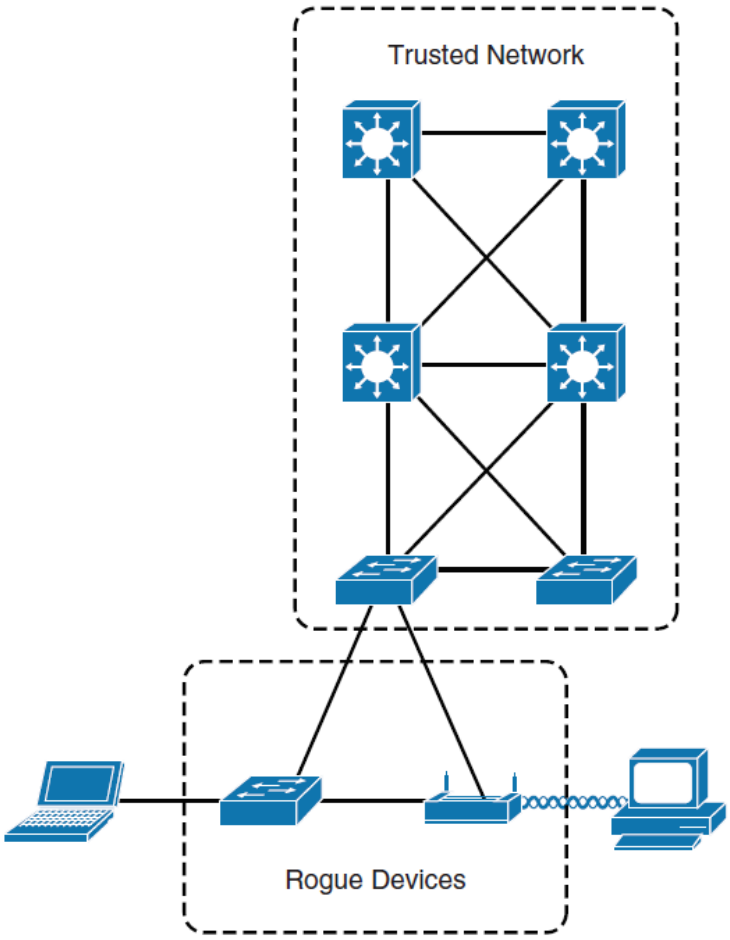

```
S2(config)# interface FastEthernet 0/11
S2(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to
a single host. Connecting hubs, concentrators, switches,
bridges, etc... to this interface  when portfast is enabled,
can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
 have effect when the interface is in a non-trunking mode.
S2(config-if)# spanning-tree bpduguard enable
S2(config-if)# end
```

Nejlepší praktiky konfigurace bezpečnosti Cisco přepínačů

- **Zabezpečte nepoužívané porty přepínačů**
  - Všechny nepoužívané porty přepínačů by měly být vypnuty, aby se zabránilo neoprávněným uživatelům v připojení k síti.
  - Všechny uživatelské porty by měly být konfigurovány s příkazem přístupu k režimu přepínání.
    Všechny nepoužívané porty umístěte do izolované nebo falešné sítě VLAN.

Zranitelnosti kampusových sítí

Nežádoucí přístup



Nežádoucí přístup přichází v několika formách.

- Tato zařízení mohou být vážným porušením zabezpečení sítě, protože mohou být připojena k síťovému portu za firemní bránou firewall.
- Vzhledem k tomu, že zaměstnanci obecně nemají možnost nastavit v přístupovém bodu bezpečnostní opatření, je pro neautorizované uživatele snadné používat přístupový bod k zachycení síťového provozu a únosů klientských relací.

Zranitelnosti útoků

Útoky spuštěné proti přepínačům a ve vrstvě 2 lze seskupit následujícím způsobem:

- Útoky podvrstvy MAC
- Útoky na VLAN
- Spoofing útoky
- Útoky na přepínače

Útoky podvrstvy MAC

- Útok: Záplava (flooding) MAC adresami
  - Rámce s unikátními neplatnými zdrojovými adresami MAC zaplavují přepínač, který vyčerpává tabulkový prostor s adresovatelnou pamětí (CAM - content-addressable memory), což znemožňuje nové položky z platných hostitelů.
- Opatření
  - Zmírnění (mitigation)
  - Zabezpečení portu.
  - přístupové mapy pro MAC adresu VLAN.

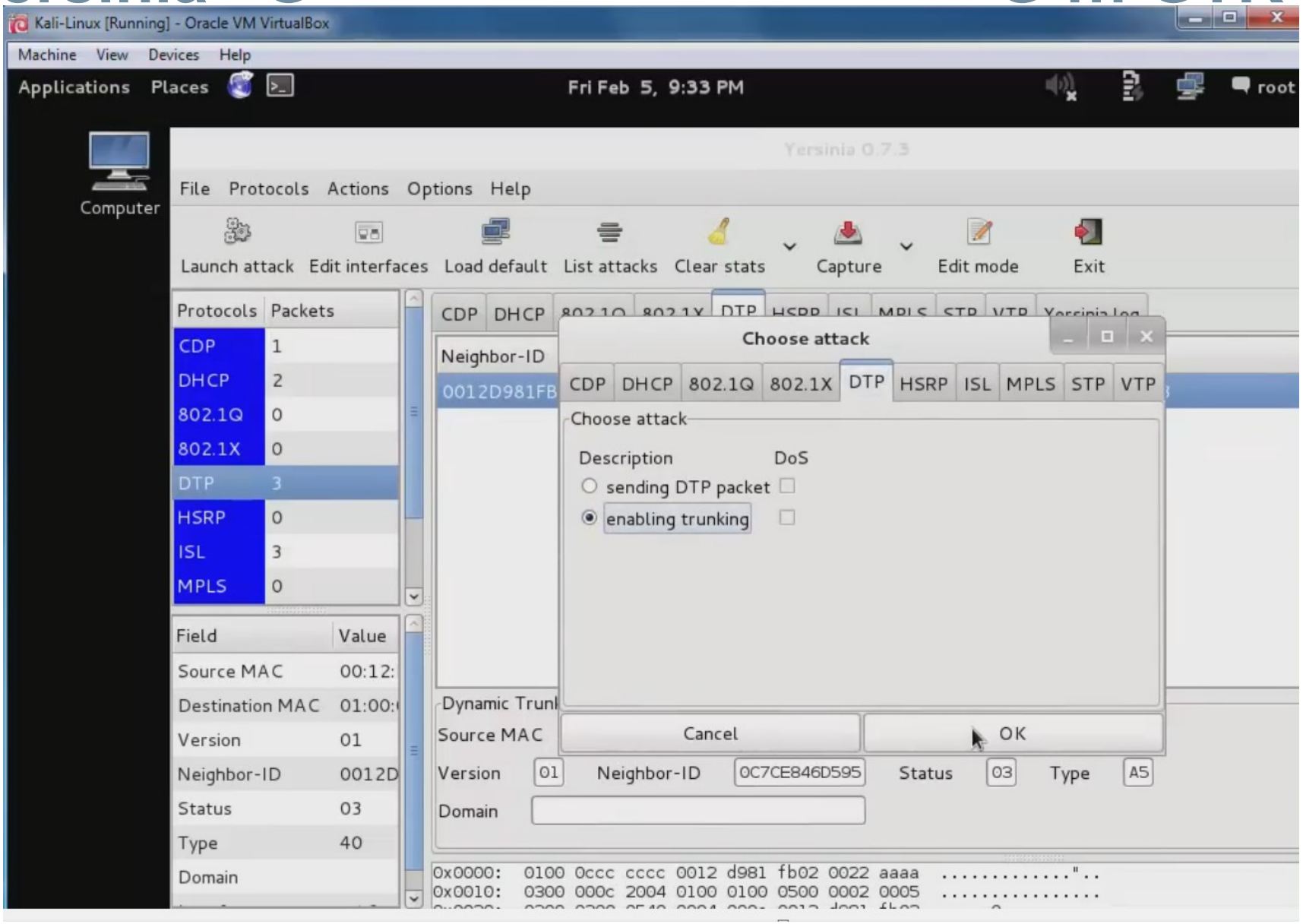
Útoky na VLANy

- **VLAN Hopping**
  - Změnou VLAN ID na paketech, které jsou zapouzdřeny pro trunking, útočící zařízení může posílat pakety na různých VLANs, vynechávající bezpečnostní opatření vrstvy 3.
  - **Zmírnění**
    Zpřísněte konfiguraci trunků a stav vyjednávání nevyužitých portů. Vypněte nepoužívané porty. Nepoužité porty umístěte do společné sítě VLAN.

- **Útoky mezi zařízeními na společné VLAN**
  - Zařízení mohou potřebovat vzájemnou ochranu, i když jsou na společné VLANě. To platí zejména o segmentech poskytovatele služeb, které podporují zařízení od více zákazníků.
  - **Zmírnění**
    Implementujte privátní VLAN (PVLANs).

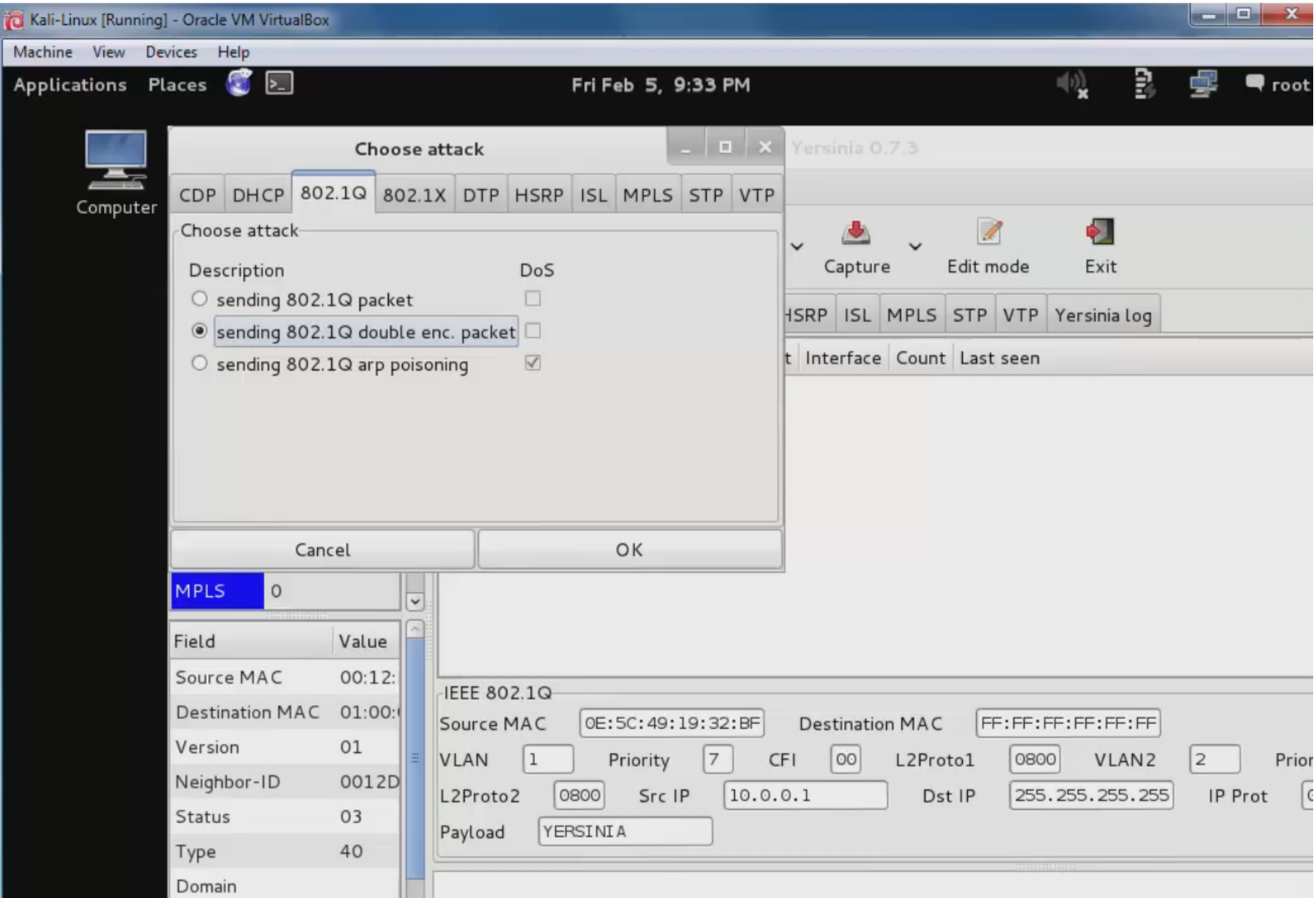
yersinia –G

G … GTK



https://github.com/tomac/yersinia další Mausezahn a Scapy

Generování rámce se dvěma VLAN záhlavími



Obrana před VLAN hoppingem s příklady

- Nastavte nativní VLAN tranku na falešný nebo nepoužívaný VLAN ID.
  - Nepoužité porty umístěte do falešné sítě VLAN
  - Omezit nativní VLAN z obou konců tranku.
  - Zakažte DTP

Např.

```
Switch(config)# vlan 800
Switch(config-vlan)# name falesny_native
Switch(config-vlan)# exit
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk native vlan 800
Switch(config-if)# switchport trunk allowed vlan remove 800
Switch(config-if)# switchport mode trunk
```

Jinou alternativou je vynutit, aby všechny tagy 802.1Q spadly do rámců pro nativní VLAN, neboli po

```
Switch(config)#switchport trunk native vlan 800   se dá
Switch(config)# vlan dot1q tag native
```

Útoky typu Spoofing (předstírání identity)

- **DHCP Starvation a DHCP Spoofing**
  - Útočící zařízení může po určitou dobu vyčerpat adresový prostor, který je k dispozici pro servery DHCP, nebo se může stát útočným serverem DHCP.

    Opatření

    - Použijte snooping (sledování, špehování) DHCP.
- **Kompromitovaný spanning tree**
  - Útočící zařízení spoofuje kořenový most v topologii protokolu STP (Spanning Tree Protocol). Pokud je úspěšný, síťový útočník může vidět řadu rámců.

    Opatření

    - Proaktivně konfigurujte primární a záložní kořenová zařízení.
    - Nastavit Root Guard.

Útoky typu Spoofing (předstírání identity)

- **MAC Spoofing**
  - Útočící zařízení spoofuje MAC adresu platného hostitele, který je právě v tabulce CAM. Přepínač pak předá útočícímu zařízení všechny rámce, které jsou určeny pro platného hostitele.

  Opatření
  - Použijte snooping DHCP, zabezpečení portu.

- **ARP spoofing**
  - Útočící zařízení krade odpovědi na protokol (ARP) určené pro platné hostitele. Adresa MAC útočícího zařízení se pak stane cílovou adresou, která se nachází v rámcích vrstvy 2, které byly odeslány platným síťovým zařízením.

  Opatření
  - Použijte DAI.
  - Použijte snooping DHCP, port security.

Útoky na zařízení switch

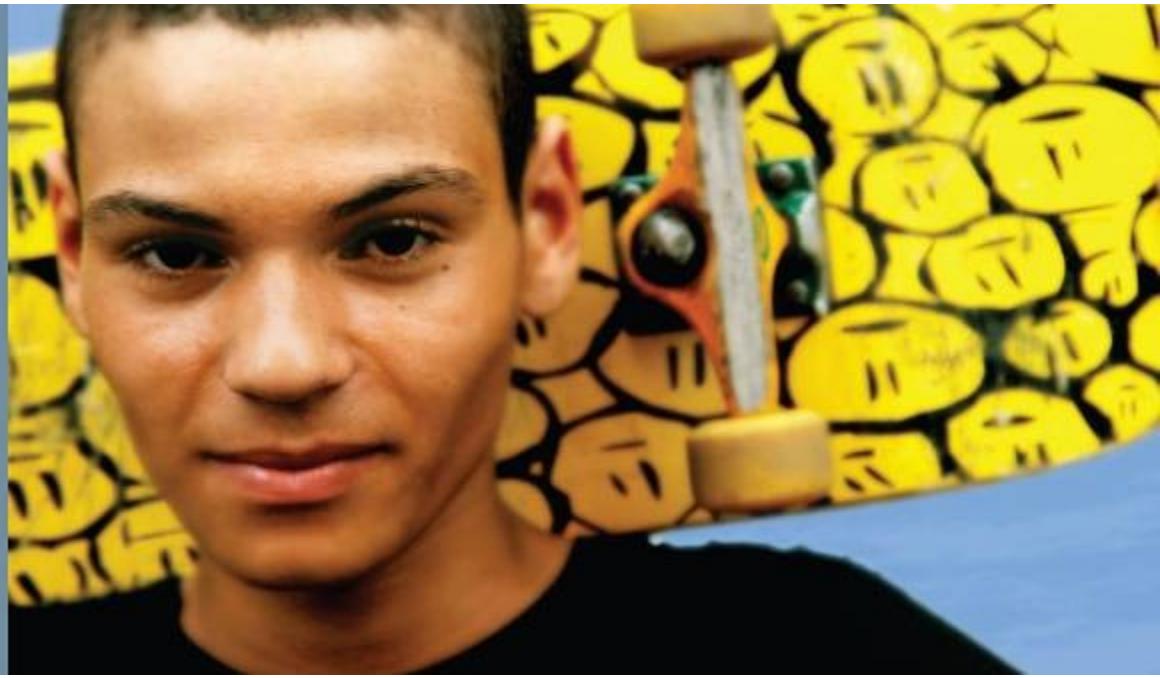
- **Cisco Discovery Protocol (manipulace s CDP)**
- Informace odeslané prostřednictvím CDP jsou přenášeny v jasném textu a nejsou ověřeny, což umožňuje jejich zachycení a zpřístupnění informací o topologii sítě.

  Opatření
  - Zakažte protokol Cisco Discovery Protocol ve všech portech, kde není úmyslně používán.

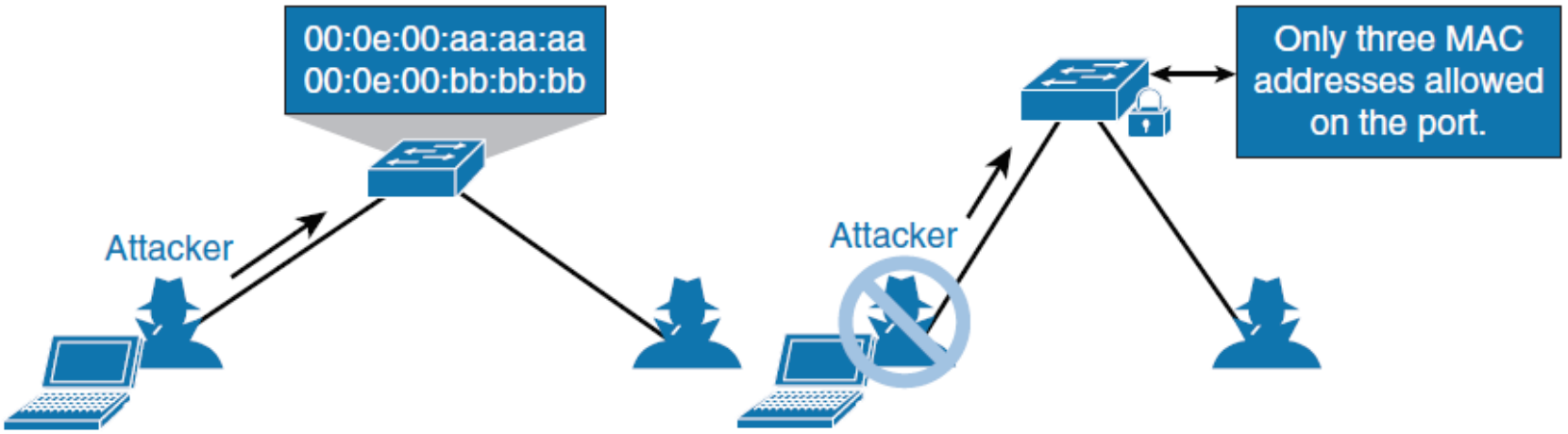
- **SSH protokol a útoky Telnetu**
  - Telnet pakety lze číst v čistém textu. SSH je správná volba, ale ve verzi 1 má bezpečnostní problémy.

  Opatření
  - Použijte SSH verze 2.
  - Použijte vty ACL.

Port Security



Port Security



- Zabezpečení portu omezuje port přepínače na konkrétní sadu nebo počet adres MAC.
- Tyto adresy lze naučit dynamicky nebo konfigurovat staticky.
- Port pak poskytne přístup k rámcům pouze z těchto adres.

Kroky Port Security 1/2

1. **Konfigurace bezpečnost portu.**
   - Konfigurujte bezpečnost portu tak, aby umožňoval pouze požadovaný počet připojení na portu.
   - Nakonfigurujte položku pro každou z těchto povolených adres MAC.
   - Tato konfigurace ve skutečnosti naplní tabulku adres MAC novými položkami pro tento port a zabraňuje se dynamicky další položky.

2. **Zpracovány jsou pouze povolené rámce.**
   - Když přijdou rámce na port přepínače, jejich zdrojová adresa MAC je zkontrolována proti tabulce adres MAC.
   - Pokud adresa MAC zdroje rámce odpovídá položce v tabulce pro daný port, jsou rámce předány přepínači, který má být zpracován jako všechny ostatní rámce na přepínači.

Fungování Port Security 2/2

3. **Nové adresy neumožňují vytvářet nové položky adres MAC adres.**
   - Když na port přijdou rámce s nepovolenou adresou MAC, přepínač určí, že adresa není v aktuální tabulce adres MAC a nevytváří dynamickou položku pro tuto novou adresu MAC, protože počet povolených adres byl omezen.

4. **Přepínač provede akci v reakci na nepotvrzené rámce.**
   - Přepínač znemožní přístup k portu a provede jednu z těchto akcí závislých na konfiguraci:

     ✓celý port přepínače může být zablokován,

     ✓přístup může být odepřen pouze pro tuto MAC adresu a může být generována chyba protokolu nebo

     ✓přístup může být odepřen pro danou MAC adresu, ale bez generování logovací zprávy.

Konfigurace Port Security

- **`switchport port-security maximum`** *`value`*
  - Omezení počtu připojených MAC adres. Rozpětí *value* je od 1 do 3072; defaultní hodnota je 1.
- **`switchport port-security violation { protect | restrict | shutdown }`**
  - Volitelně nastavuje režim narušení, akci, která má být provedena, když je zjištěno narušení zabezpečení, jako jednu z těchto:
    - **restrict** Je omezen přenos dat, zvýšen čítač SecurityViolation a odeslána zpráva SNMP.
    - **shutdown** rozhraní je err-disabled .
- **`switchport port-security limit rate invalid-source-mac`**
  - Nastaví limit rychlosti pro špatné pakety.

RSE kapitola 5

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

```
Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
Switch(config-if)#switchport port-security violation
```

Konfigurace Port Security (pokračování)

- **`switchport port-security mac-address`** *`mac-address`*
  - Volitelně zadá bezpečnou adresu MAC rozhraní.
  - Pomocí tohoto příkazu můžete zadat maximální počet zabezpečených adres MAC. Pokud nakonfigurujete méně bezpečných MAC adres než je maximum, zbývající adresy MAC budou dynamicky naučeny.
- **`switchport port-security mac-address sticky`**
  - Volitelně umožňuje sticky učení na rozhraní.

1. Příklad Port Security

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet 3/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end

Switch# show port-security interface gigabitethernet 3/12
Port Security              :Enabled
Port Status                :Secure-up
Violation Mode             :Shutdown
Aging Time                 :0
Aging Type                 :Absolute
SecureStatic Address Aging :Enabled
Maximum MAC Addresses      :5
Total MAC Addresses        :0
Configured MAC Addresses   :0
Sticky MAC Addresses       :11
Last Source Address        :0000.0000.0401
Security Violation Count   :0
```

2. Příklad Port Security

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet 5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 10
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# end
Switch# show port address
Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age
                                                              (mins)
----    -----------       ----                      -----   -------------
   1    0000.0000.0001    SecureSticky              Gi5/1         -
   1    0000.0000.0002    SecureSticky              Gi5/1         -
   1    0000.0000.0003    SecureConfigured          Gi5/1         -

-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 1024
```

Podmínky chybového stavu portu 1/2

Následující seznam uvádí nejběžnější situace, kdy port přejde do stavu s chybou - err-disabled state:

- **Narušení bezpečnosti portu**
  - Když se na portu naučí neplatná adresa MAC nebo nebo se registruje příliš mnoho MAC adres, přepínač může volitelně umístit port do stavu err-disabled.
- **Porušení Spanning-tree BPDU guard**
  - Když máte chybně nakonfigurován PortFast v kombinaci s BPDU Guard.
- **Chybná konfigurace EtherChannel**
  - Všechny parametry musí být stejné pro všechny porty na obou stranách svazku
- **Neshoda duplexu**
  - Duplexní režim musí být stejný na obou stranách spoje;

Podmínky chybového stavu portu 2/2

- **Podmínka UDLD**
  - UDLD (Unidirectional Link Detection) zajišťuje, že spojení je vždy obousměrné; Když tedy detekuje jednosměrné spojení, umístí port do stavu, který je zakázán.
- **Spanning-tree Root Guard**
  - Pokud port s podporou root guardu obdrží nadřazenou BPDU od těch, které odeslal aktuální root bridge.
- **Link flapping**
  - Když je stav spojení překlopen mezi stavy up a down, je port umístěn do stavu err-disabled.
- **Další důvody**
  - Jiné důvody zahrnují pozdní kolizní detekci, Layer 2 Tunneling Protokol Guard, DHCP snooping rate-limit, nesprávné gigabit interface convert (GBIC), a ARP inspekce.

Stav portu Err-Disable

- Ve výchozím nastavení je pro všechny tyto příčiny povolena detekce zakázaných chyb.
- Lze nastavit další důvody pro vypnutí portu.
- Pomocí následujícího příkazu určete příčiny:

- `Switch(config)# errdisable detect cause [ all | cause-name ]`

Automatická obnova ze stavu Err-Disabled

- Po odstranění příčiny stavu err-disabled je třeba dát shut / no shut.
- Protože podmínka chybového stavu je idstraněna, nedojde k aktivaci err-disable.
- Aby bylo možné snížit administrativní režii, může být port přepínače nakonfigurován tak, aby byl po určité době automaticky znovu aktivován.
- Samozřejmě, pokud je chybový stav stále přítomen, port se okamžitě vrátí do stavu, kdy je chybný stav.

```
Switch(config)# errdisable recovery cause psecure-violation
Switch(config)# errdisable recovery interval 60
```

Port Access List (PACL)

- Port access lists (PACLs) je další způsob jak aplikovat bezpečnost v kampusových sítích.
- Standardní access control lists (ACL) jsou aplikovány na provoz procházející přes rozhraní Layer 3.
- Funkce PACL poskytuje možnost provádět řízení přístupu na konkrétním portu 2. vrstvy.
- Port Layer 2 je fyzický přístup nebo port trunk, který patří do VLAN.
- Funkce ACL portu je podporována pouze v hardwaru. (Port ACL nejsou aplikovány na žádné pakety směrované v softwaru)
- Funkce PACL neovlivňuje řídicí pakety vrstvy 2, jako například CDP, VTP, DTP a STP, přijaté na portu.

Port Access List

- Jsou dva typy PACL:
- **IP access list**
  - Filtruje IPv4 a IPv6 pakety na Layer 2 portu.
- **MAC access list**
  - Filtruje pakety nepodporovaného typu (ne IP, ARP nebo MPLS) na základě polí ethernetového rámce.
  - Seznam přístupů MAC není použit pro zprávy IP, MPLS nebo ARP.
  - Můžete definovat pouze pojmenované přístupové seznamy MAC

Port Access Lists

Interakce PACL s jinými typy ACL závisí na nakonfigurovaném režimu:

- V **preferovaném módu** portů PACL nabývá účinku a potlačuje účinek jiných ACL. Tento režim je jediný režim, který je povolen při použití PACL na trunku.
- V **režimu sloučení (merge)** jsou PACL, VACL a standardní ACL sloučeny ve směru vstupu. Toto je **defaultní režim**.
- IP a MAC ACL mohou být aplikovány na fyzická rozhraní vrstvy 2. Jsou podporovány standardní (číslované, pojmenované) a rozšířené (číslované, pojmenované) IP ACL a rozšířené jmenné seznamy MAC ACL.

Port Access Lists

Konfigurujte MAC ACL a aplikujte na rozhraní Layer 2:

- SW(config)# **mac access-list extended** *acl-name*
- SW(config-ext-macl)# **permit host** [*source-mac* | **any**] [*destination-mac* | **any**]
- SW(config-ext-macl)# **interface** *interface-slot/number*
- SW(config-if)# **mac access-group** *acl-name* **in**

Konfigurujte IP ACL a aplikujte na rozhraní Layer 2:

- SW(config)# **ip access-list** *acl-type acl-name*
- SW(config-ext-nacl)# **permit** *protocol* [*source-address* | **any**] [*destination-address* | **any**]
- SW(config-ext-nacl)# **interface** *interface-slot/number*
- SW(config-if)# **ip access-group** *acl-name* **in**

Příklad PACL

Switch(config)#ip access-list extended jednoduchy-ip-acl
Switch(config-ext-nacl)#permit tcp any any
Switch(config-ext-nacl)#end

Switch(config)#mac access-list extended **jednoduchy -mac-acl**
Switch(config-ext-macl)#permit host 000.000.011 any
Switch(config-ext-macl)#end

Switch(config)# interface fa 0/1
Switch(config-if)#ip access-group **jednoduchy -ip-acl** in
Switch(config-if)#mac access-group **jednoduchy-mac-acl** out

PACL's Group Mode

Konfiguruje způsob access group na Layer 2 rozhraní:

- `SW(config)# **interface** *interface-slot/number*`
- `SW(config-if)# **access-group mode** [ **prefer port** | **merge** ]`

- Poznámka: Tento příkaz není podporován na všech platformách.

Storm Control

Storm Control

- Popište, co je to traffic storm a jak ji ovládat.
- Konfigurujte a ověřte storm control.

Úvod do Storm Control

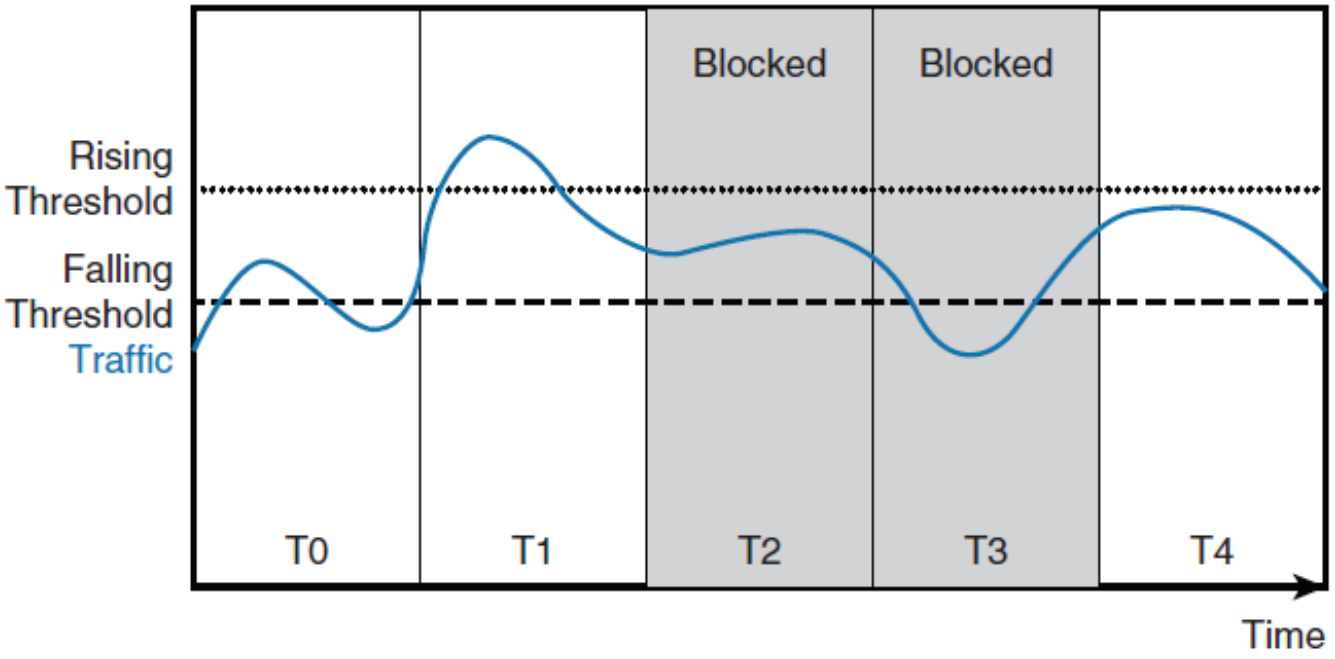
- Traffic storm nastane, když pakety zaplaví LAN, což vytváří nadměrný provoz a snižuje výkon sítě.
- Funkce traffic storm brání tomu, aby porty LAN byly zahlušeny broadcasty, multicasty nebo unicast provozem na fyzických rozhraních.

Chování Storm Control

- Během intervalu porovnává úroveň provozu s konfigurovanou prahovou úrovní traffic stormu.
- Úroveň řízení traffic stormu je buď absolutní počet bitů nebo paketů za sekundu nebo procento celkové dostupné šířky pásma portu.
- Lze nakonfigurovat dva prahy.
- Když přenos překročí stoupající prahovou úroveň, traffic stormu blokuje port.
- Jakmile provoz klesne pod práh pádu (falling threshold), ovládání bouře odstraní blok.
- Konfigurace dolní prahové hodnoty je volitelná.

Chování Storm Control

- Volitelně lze rozhraní zablokovat (shutdown), pokud je porušena prahová úroveň nebo je odeslán SNMP trap.
- Storm control je konfigurováno na každé rozhraní pro každý typ provozu (unicast, multicast, broadcast) zvlášť.



Konfigurace a verifikace Storm Control na rozhraní

- Switch(config)# **interface** *interface-slot/int*
- Switch(config-if)# **storm-control** [**broadcast** | **multicast** | **unicast**] **level** { *risingpercent* | **bps** *rising-bps* | **pps** *rising-pps* } [*falling-percent*|*falling-bps*|*falling-pps*]
- Switch(config)# **interface** *interface-slot/int*
- Switch(config-if)# **storm-control action** { **shutdown**|**trap** }

```
Switch(config)# interface GigabitEthernet 0/0/1
Switch(config-if)# storm-control broadcast level 40 25
Switch(config-if)# storm-control multicast level pps 50k 25k
Switch(config-if)# storm-control unicast level bps 20m
Switch(config-if)# storm-control action shutdown
Switch(config-if)# storm-control action trap
```

Verifikace konfigurace Storm Control

```
Switch# show storm-control
Interface  Filter State   Upper         Lower         Current
---------  -------------  ------------  ------------  ----------
Gi0/1      Forwarding       40.00%        25.00%        3.50%
```

```
Switch# show storm-control multicast
Interface  Filter State   Upper         Lower         Current
---------  -------------  ------------  ------------  ----------
Gi0/1      Blocking        50m pps       25m pps       34m pps
```

```
Switch# show storm-control unicast
Interface  Filter State   Upper         Lower         Current
---------  -------------  ------------  ------------  ----------
Gi0/1      Blocking          20m bps       20m bps       37m bps
```

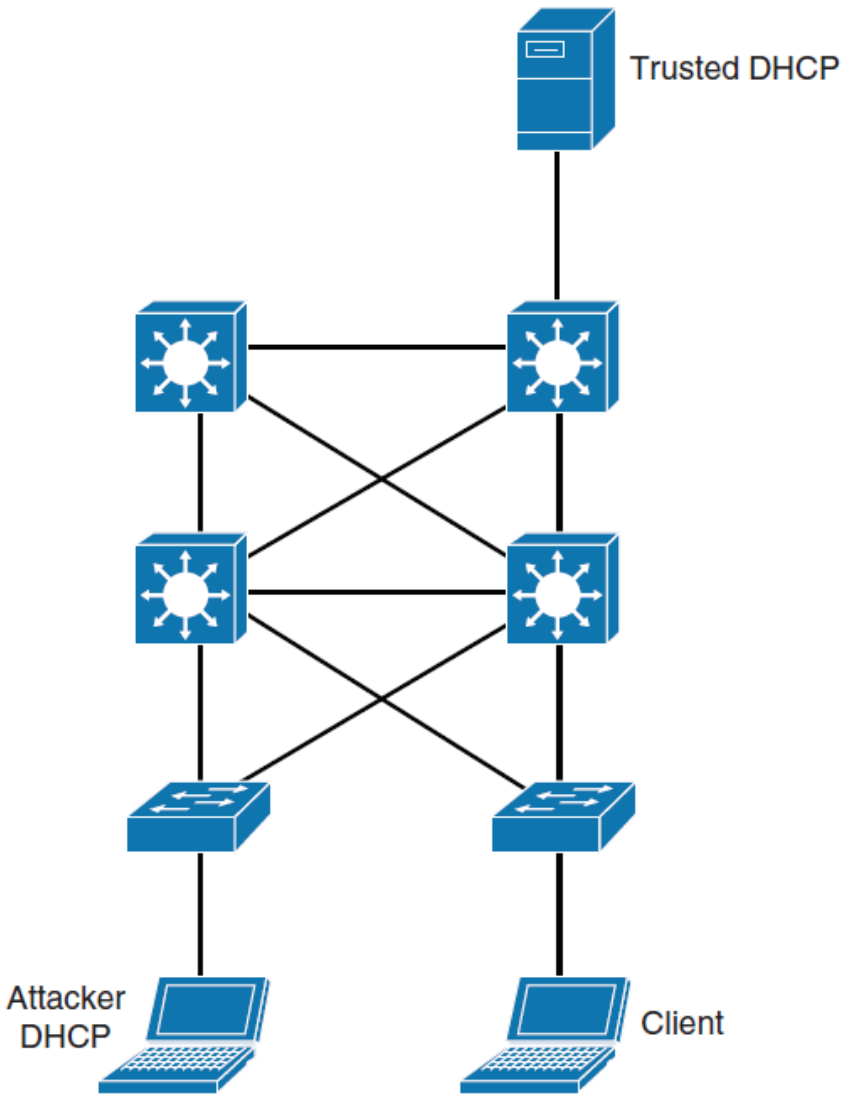
Opatření proti spoofingu (Mitigating Spoofing Attacks)

© 2007 – 2016, Cisco Systems, Inc. All rights reserved. Cisco Public

Zmírňující útoky spoofingu

- Jak může poškozený server DHCP poškodit vaši síť
- Falšování DHCP
- Konfigurace a ověřování snoopingu DHCP
- Co je IP Source Guard a proč ji potřebujete
- Konfigurace ochrany IP zdroje
- Spoofing ARP
- Jak DAI funguje
- Konfigurace DAI (Dynamic ARP Inspection)

Útok DHCP Spoofing



- Nejčastějším příkladem falešného DHCP serveru je, když je počítač nakonfigurován jako DHCP server v síti kampusu.
- Pokud odpověď odesílatele DHCP serveru dorazí nejdříve na klienta DHCP, klient tuto odpověď použije.
- Protože tato první odpověď z podvodného serveru je falešná, klient nebude moci získat správné připojení k síti a může mít přesměrovaný provoz na falešnou výchozí bránu.

Proces vytvoření falešného serveru DHCP

1. Útočník je hostitelem falešného serveru DHCP mimo port přepínače do stejné podsítě jako klienti.
2. Klient vysílá požadavek na informace o konfiguraci DHCP.
3. Nežádoucí server DHCP reaguje před legitimním serverem DHCP a přiřazuje informace o konfiguraci IP definované útočníkem.
4. Hostitelské pakety jsou přesměrovány na adresu útočníka, protože emulují výchozí bránu pro chybnou IP adresu, která je klientovi poskytována prostřednictvím DHCP.

DHCP Snooping (kontrola)

Funkce DHCP Snooping konfiguruje dva typy portů:

- **Důvěryhodné (trusted) porty**
  - Hostování serveru DHCP nebo může být uplink směrem k serveru DHCP.
- **Nedůvěryhodné porty**
  - Jsou ty, které nejsou explicitně nakonfigurovány jako důvěryhodné.
  - Z pohledu snooping DHCP by porty nedůvěryhodného přístupu neměly odesílat žádné odpovědi serveru DHCP, například DHCPOFFER, DHCPACK nebo DHCPNAK.
  - Pokud se zařízení na nedůvěryhodném portu pokusí odeslat do sítě paket odpovědí DHCP, port se vypne.
    - ✓ Tato funkce může být spojena s možností 82 DHCP, ve které mohou být informace o přepínači, jako je ID portu požadavku DHCP, vloženy do paketu požadavku DHCP.

DHCP snooping

1. Zapnutí funkce

```
SWITCH(config)#ip dhcp snooping
```

2. Na daném interface uvedení důvěryhodných portů

```
SWITCH(config-if)#ip dhcp snooping trust
```

3. Specifikace, na kterých VLANách bude funkce zapnuta

```
SWITCH(config)#ip dhcp snooping vlan 1 - 999
```

můžeme definovat jednu VLANu, seznam VLAN oddělený čárkou nebo rozsah

Příklad DHCP Spoofing


```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#int fa0/4
Switch(config-if)#ip dhcp snooping ?
  limit   DHCP Snooping limit
  trust   DHCP Snooping trust config
  vlan    DHCP Snooping vlan

Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#do show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is operational on following VLANs:
1
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted     Rate limit (pps)
-------------------------  -------     ----------------
FastEthernet0/4            yes         unlimited
Switch(config-if)#
```

Rozhraní fa0/4 je nastaveno jako důvěryhodné

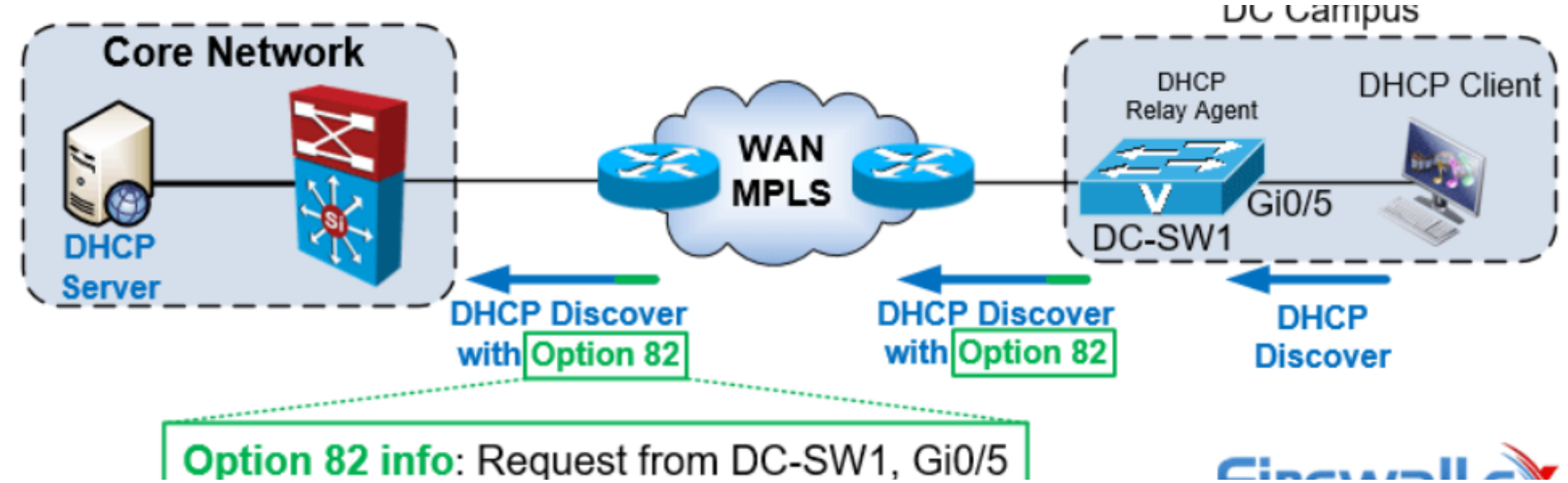
```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/4
Switch(config-if)#ip verify source
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#do show mac address-table int fa0/4
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    1c75.08ab.1d47    DYNAMIC     Fa0/4
Total Mac Addresses for this criterion: 1

Switch(config)#ip source binding 1c75.08ab.1d47 vlan 1 10.0.0.13 int fa0/4
```

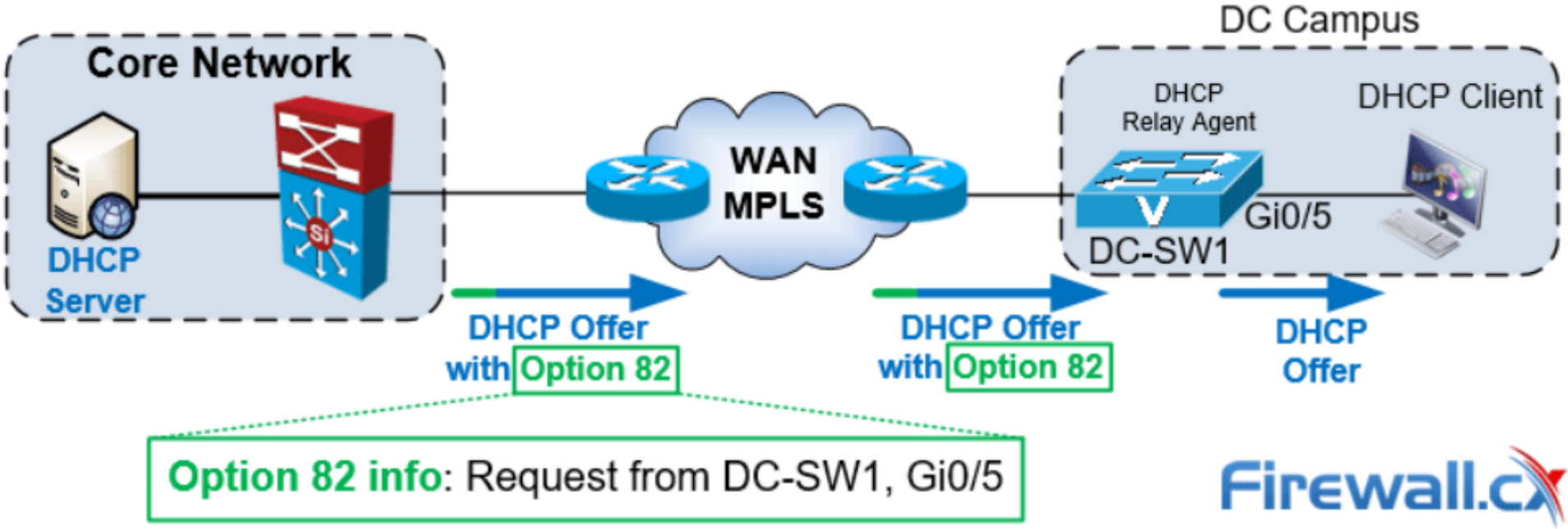
Blíže: http://ccnp300-115.blogspot.com/2016/09/ip-source-guard.html

DHCP 82

- Jak bylo uvedeno v předchozí části, možnost DHCP 82 poskytuje dodatečné zabezpečení, pokud se DHCP používá k přidělení síťových adres. Tato funkce umožňuje agentu DHCP relay zahrnout informace o sobě a připojeném klientovi do rámců požadavků DHCP při předávání požadavků DHCP z klienta DHCP na server DHCP.
- Server DHCP pak může tyto informace použít k přiřazení adres IP, provádění řízení přístupu a nastavení zásad kvality služby (QoS) a zásad zabezpečení (nebo jiných politik přiřazování parametrů) pro každého účastníka sítě poskytovatele služeb.
- Někteří kabeloví operátoři používají možnost DHCP 82 s kabelovými modemy, aby zajistili kontrolu přístupu a kvalitu serveru pro uživatele podnikových tříd mezi domácími uživateli.
- Alternativně, pokud informace nejsou přítomny nebo nesprávné, server DHCP by mohl požadavek ignorovat. Volba DHCP 82 spolu se snoopingem DHCP jsou osvědčenými postupy pro sítě kampusů jako další bezpečnostní opatření.

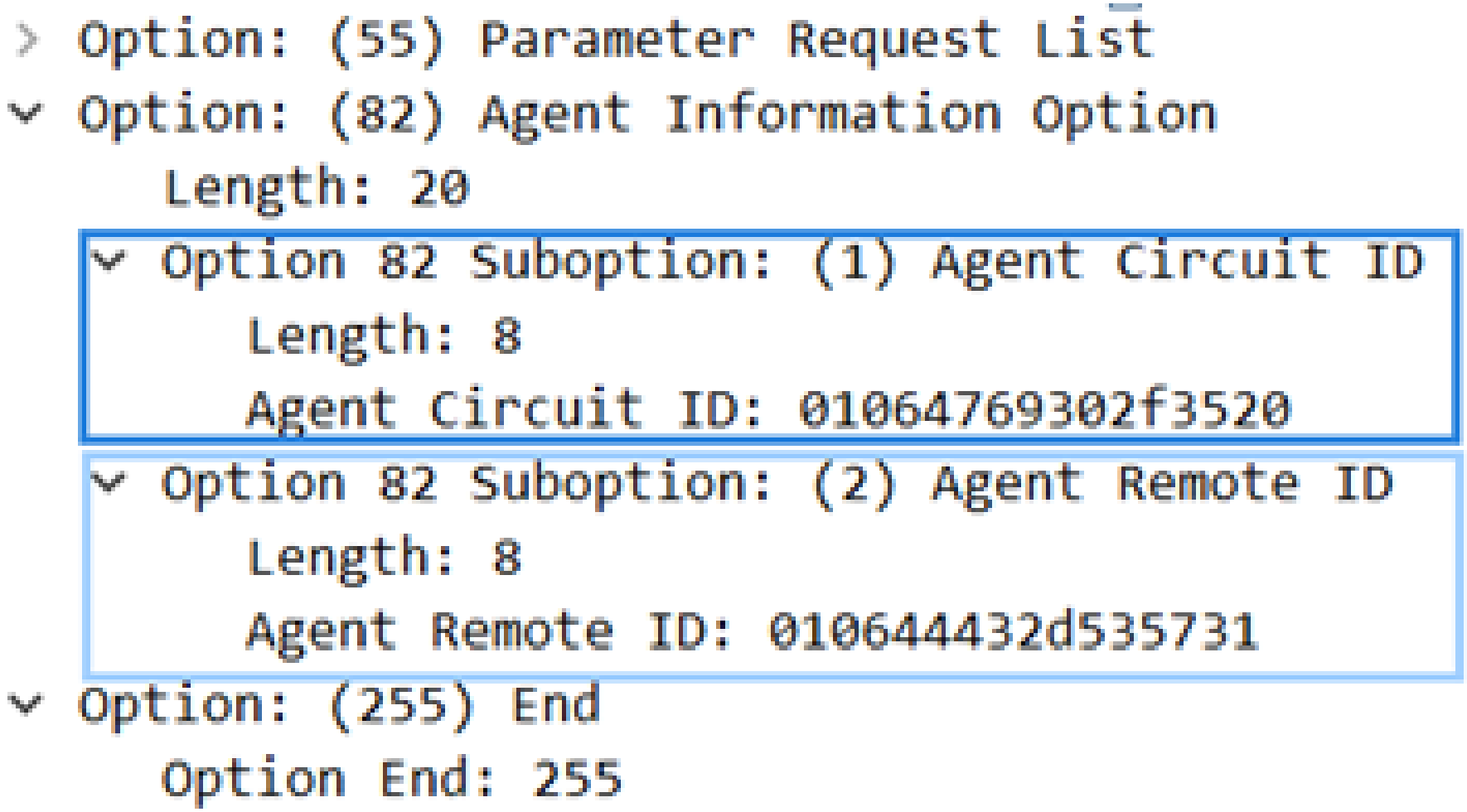
DHCP 82



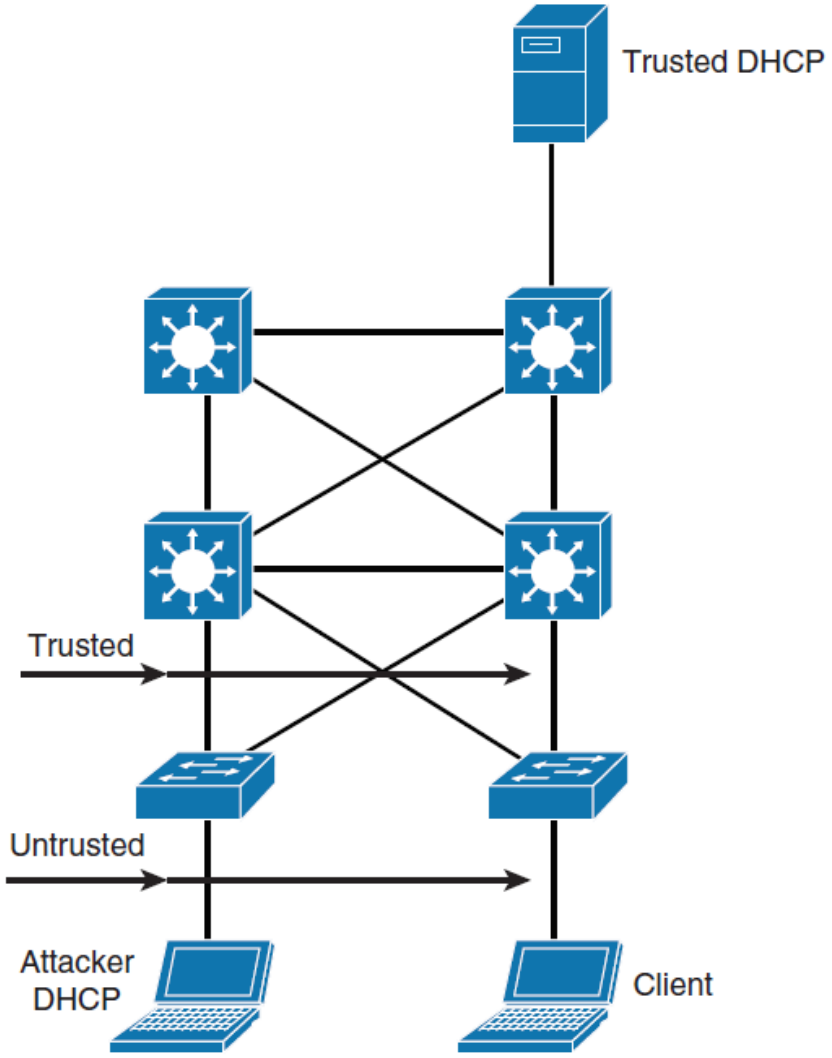


Firewall.cx

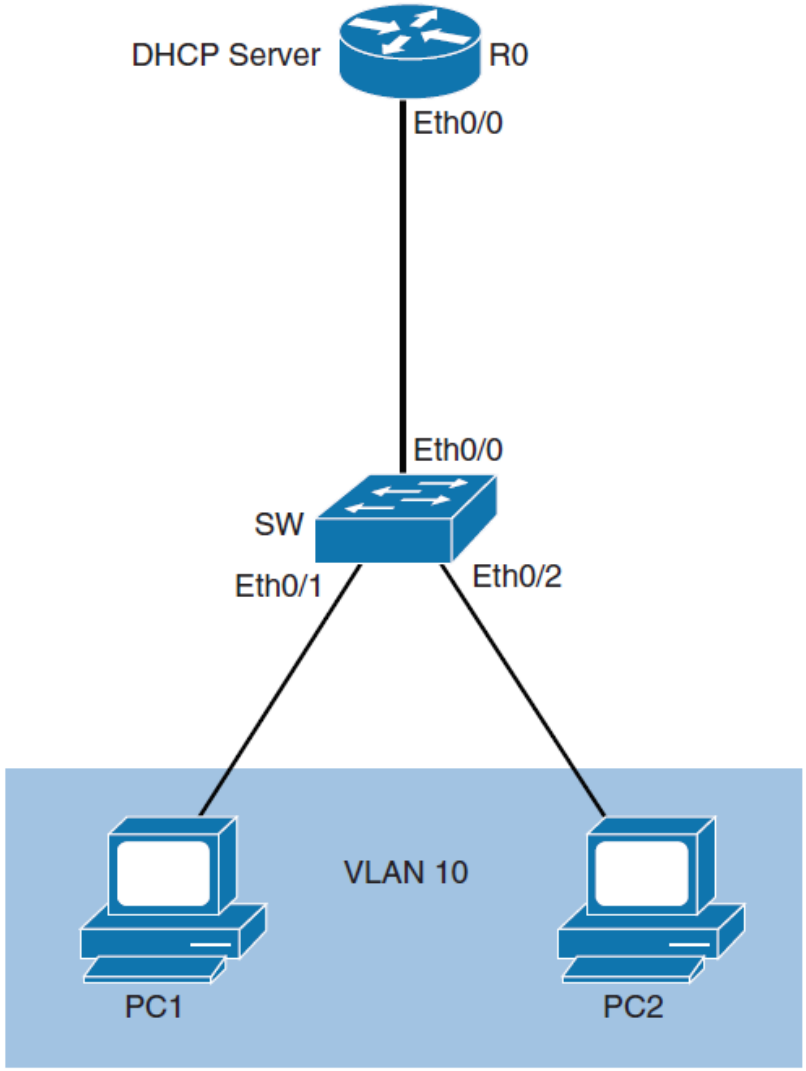
Struktura TLV v rámci DHCP 82



DHCP Snooping



Příklad konfigurace DHCP Snoopingu



Příklad konfigurace DHCP Snoopingu

- Kroky pro povolení DHCP snooping pro VLAN 10 se serverem DHCP v síti Ethernet 0/0:
  Krok 1. Globálně povolte snooping DHCP.
  Krok 2. Zapněte snooping DHCP na vybraných VLAN.
  Krok 3. Konfigurace důvěryhodných rozhraní, protože nedůvěryhodné jsou výchozí.
  Krok 4. Nakonfigurujte rychlostní limit požadavků DHCP na nedůvěryhodných portech.
  Krok 5. Konfigurujte volbu informací pomocí volby DHCP 82.

```
SW(config)# ip dhcp snooping
SW(config)# ip dhcp snooping VLAN 10
SW(config)# interface Ethernet 0/0
SW(config-if)# ip dhcp snooping trust
```

Poskytnutí více informací o klientovi: **ip dhcp snooping information option 82**

Verifikace konfigurace DHCP Snoopingu

```
SW# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0024.f9c6.1a80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
Ethernet0/0                 yes       yes             unlimited
```

Verifikace konfigurace DHCP Snoopingu

```
SW# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ----------
----------
00:24:13:47:AF:C2   192.168.1.4      85858       dhcp-snooping   10     Ethernet0/1
00:24:13:47:7D:B1   192.168.1.5      85859       dhcp-snooping   10     Ethernet0/2
Total number of bindings: 2
```

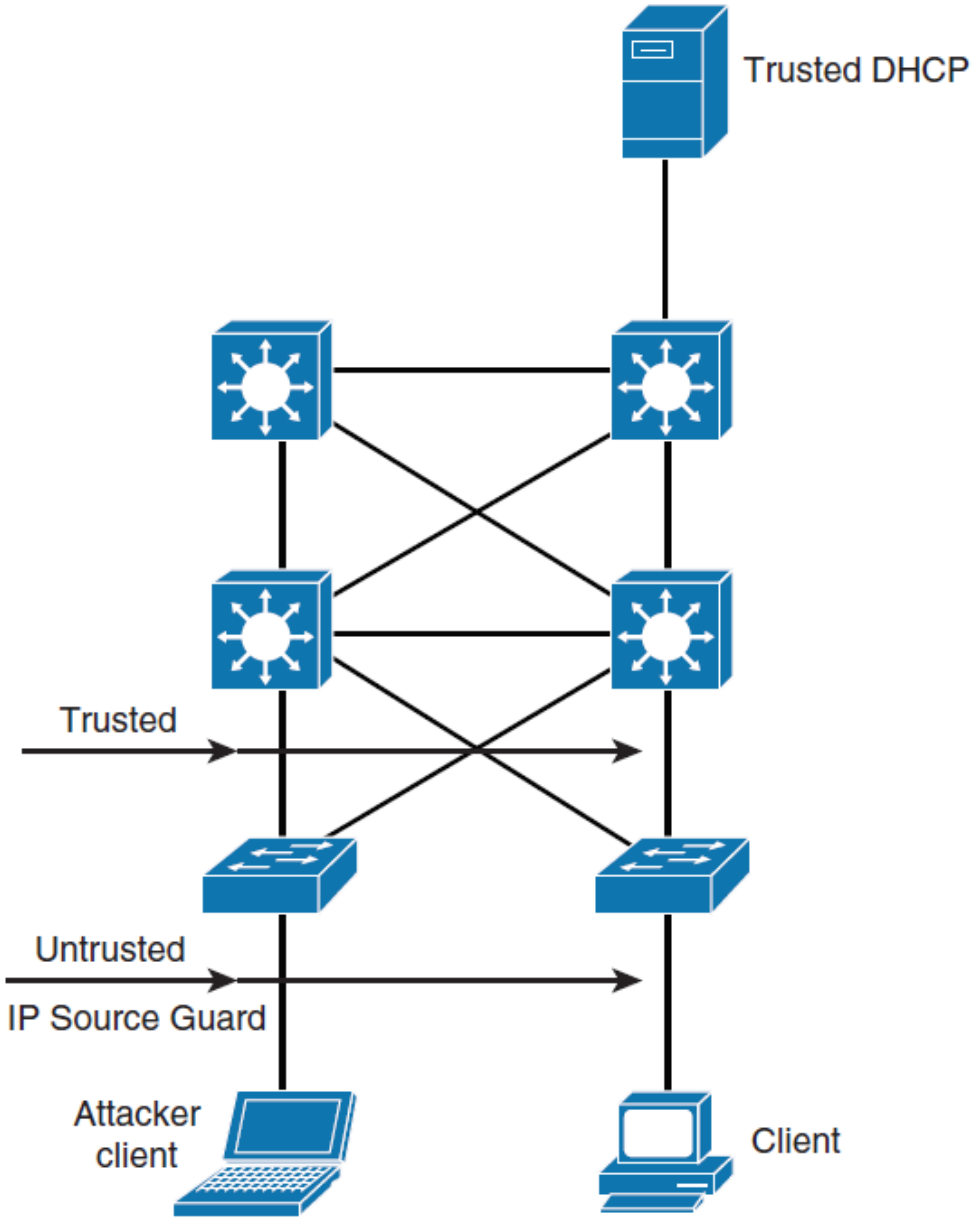
DHCP Snooping Command Review

- **ip dhcp snooping**
  - Umožňuje globálně snooping DHCP. Ve výchozím nastavení není tato funkce povolena.
- **ip dhcp snooping information option**
  - Povolí volbu DHCP 82. Tato volba je volitelná pro to, aby předaný paket požadavků DHCP obsahoval informace o portu přepínače, ze kterého pochází.
  - Tato možnost je ve výchozím nastavení povolena.
- **ip dhcp snooping vlan vlan-id [vlan-id]**
  - Identifikuje sítě VLAN, které budou předmětem snoopingu DHCP.
- **ip dhcp snooping trust**
  - Konfiguruje důvěryhodný port.
  - Použijte žádné klíčové slovo pro návrat k nedůvěryhodným.
  - Tento příkaz použijte v režimu konfigurace rozhraní.
- **ip dhcp snooping limit rate *rate***
  - Konfiguruje počet paketů DHCP za sekundu, které rozhraní může přijímat.
  - To zajišťuje, že provoz DHCP nepřekoná servery DHCP. Normálně platí, že limit rychlosti platí pro nedůvěryhodná rozhraní.
  - Tento příkaz použijte v režimu konfigurace rozhraní.
- **show ip dhcp snooping**
  - Ověřuje konfiguraci.

IP Source Guard (IPSG)

- IPSG pracuje tak, že dynamicky udržuje VLAN ACL dle portů na základě naučených vazeb IP-to-MAC-to-switch-port.
- Když je IPSG povoleno, přepínač blokuje veškerý provoz IP do portu, s výjimkou paketů DHCP zachycených procesem snooping DHCP.
- Po dokončení procesu DHCP a přijetí platné adresy IP ze serveru DHCP (nebo pokud uživatel nakonfiguruje vazbu statického zdroje IP), je na portu nainstalován ACL na portu a VLAN (PVACL). dynamicky.
- Tento proces omezuje vstup IP klienta na příslušném portu na zdrojovou adresu IP nakonfigurovanou ve vazbě.
- Jakýkoli provoz IP s jinou zdrojovou adresou IP, než je adresa ve vazbě zdroje IP, bude odfiltrován.

IPSG Topology Layout

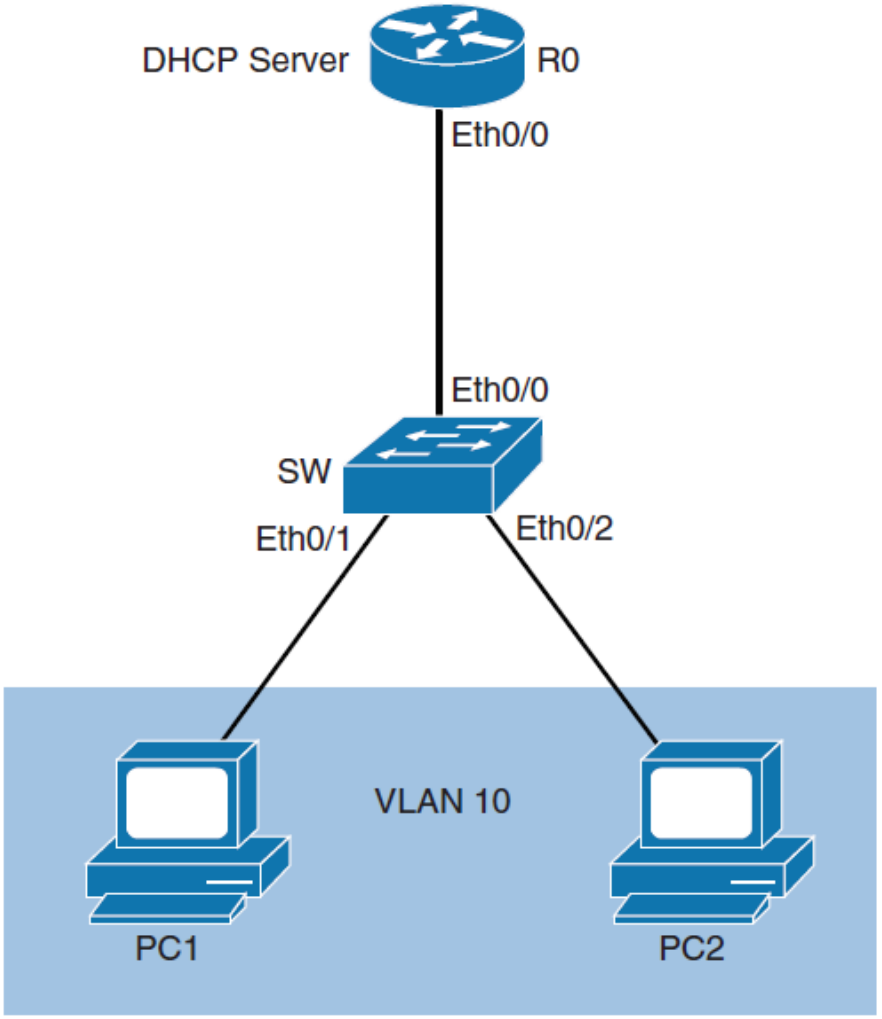


Filtry IPSG

- Pro každý nedůvěryhodný port existují dvě možné úrovně filtrování zabezpečení protokolu IP:
- **Source IP address filter**
- IP provoz je filtrován na základě jeho zdrojové IP adresy. Je povolen pouze provoz IP se zdrojovou adresou IP, která odpovídá položce vazby zdroje IP. Filtr zdrojové adresy IP se změní, když je v portu vytvořena nová vazba vstupu zdroje IP nebo odstraněna.
- **Source IP and MAC address filter**
- IP provoz je kromě své MAC adresy ještě filtrován na základě jeho zdrojové IP adresy; povolen je pouze provoz IP se zdrojovými adresami IP a MAC, které odpovídají položce vazby IP zdroje.

Musí být předtím zapnut DHCP snooping

Konfigurace IPSG



Konfigurace IPSG

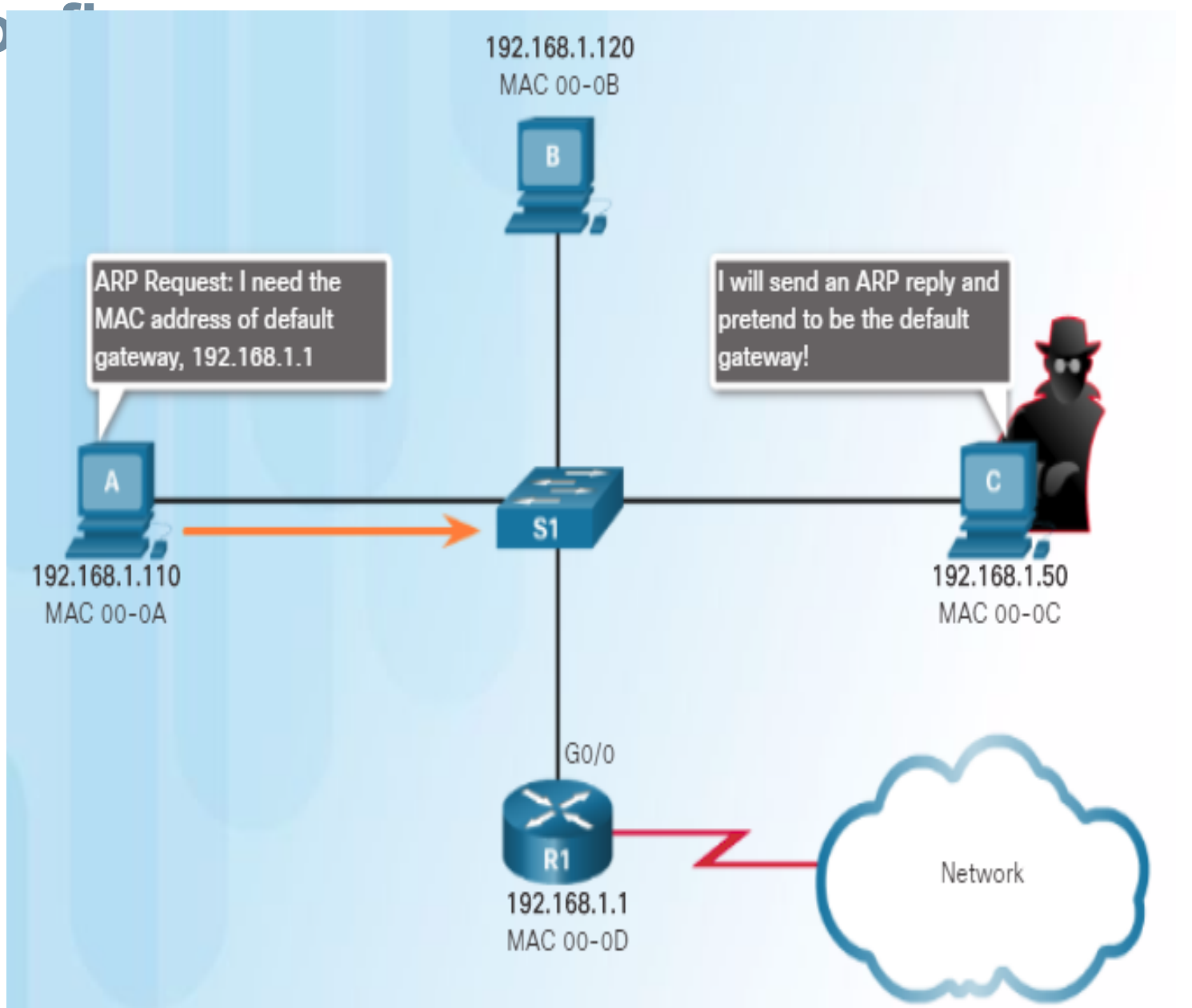
- Pro nastavení IPSG na portu použijte pro nastavení filtru IP adresy příkaz na rozhraní **`ip verify source`**
- Pro nastavení filtru na bázi MAC a IP adresy použijte na rozhraní příkaz **`ip verify source port-security`** .

```
SW(config)# interface Ethernet 0/1
SW(config-if)# ip verify source
SW(config-if)# ip verify source port-security
SW(config-if)# interface Ethernet0/2
SW(config-if)# ip verify source
SW(config-if)# ip verify source port-security
```

Konfigurace IPSG a verifikace stavu

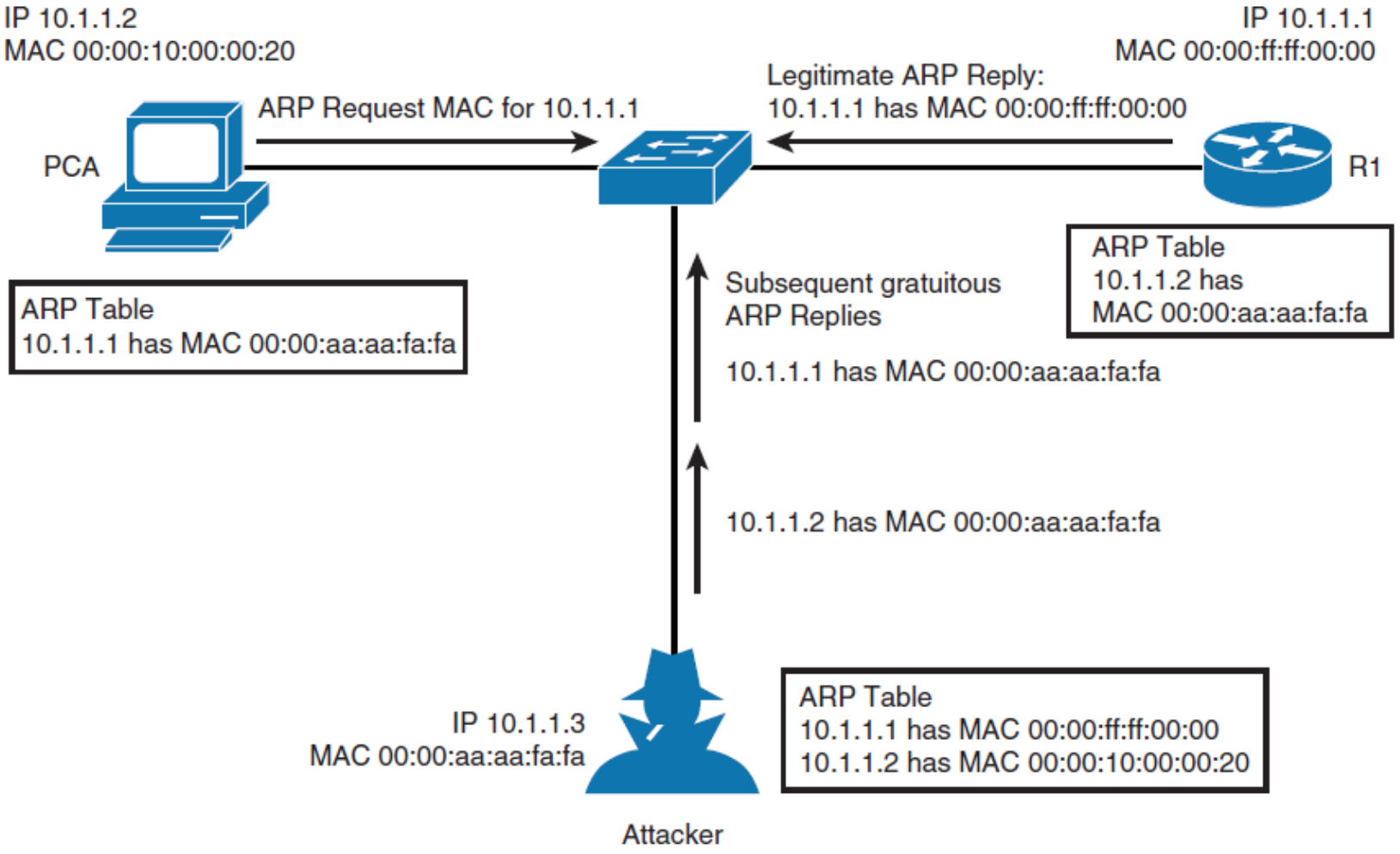
```
SW# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Et0/1      ip           active       192.168.1.4                         10
Et0/2      ip           active       192.168.1.5                         10
```

ARP Spo



Note: MAC addresses are shortened for demonstration purposes.

ARP Spoofing



ARP Spoofing

Krok 1. PCA pošle ARP požadavek na MAC adresu R1.

Krok 2. R1 odpovídá své MAC a IP adrese. Aktualizuje také cache ARP.

Krok 3. PCA váže MAC adresu R1 na R1 IP adresu v ARP cache.

Krok 4. Útočník odešle svou odpověď ARP na PCA, vázající jeho MAC adresu na IP adresu R1.

Krok 5. PCA aktualizuje ARP cache s MAC adresou útočníka vázaného na IP adresu R1.

Krok 6. Útočník odešle svou odpověď ARP na R1, čímž je jeho MAC adresa vázána na IP PCA.

Krok 7. R1 aktualizuje ARP cache s MAC adresou útočníka vázaného na IP adresu PCA.

Krok 8. Pakety jsou přesměrovány přes útočníka.

Dynamická ARP Inspection

- Dynamická inspekce ARP (DAI) pomáhá předcházet takovým útokům tím, že nepřenáší neplatné nebo bezdůvodné odpovědi ARP do jiných portů ve stejné síti VLAN.
- DAI zachytí všechny požadavky ARP a všechny odpovědi na nedůvěryhodné porty.
- Každý zachycený paket je ověřen na platné vazby IP-to-MAC podobné IPSG.
- Odpovědi ARP přicházející z neplatných zařízení jsou buď vypnuty nebo zaprotokolovány přepínačem pro auditování, takže útokům na otravu ARP poissoning je zabráněno.
- Můžete také použít DAI pro hodnocení limitů paketů ARP a poté, pokud je rychlost překročena, rozhraní zakázáno.
- DAI určuje platnost paketu ARP na základě platné databáze vázeb adres MAC-to-IP, která je vytvořena snoopingem DHCP.
- Navíc, pro zpracování hostitelů, kteří používají staticky nakonfigurované adresy IP, může DAI ověřit pakety ARP proti uživatelem nakonfigurovaným ARP ACL.

Konfigurace Dynamic ARP Inspection (DAI) x ARP Spoofingu

1. Zapnutí DAI se provede vyjmenováním VLAN, kde se má povolit.

```
SWITCH(config)#ip arp inspection vlan 100,200
```

2. Důvěryhodné porty musíme přepnout do trust stavu.

```
SWITCH(config-if)#ip arp inspection trust
```

3. Pokud chceme použít statické záznamy, tak musíme nakonfigurovat pravidlo ARP ACL.

```
SWITCH(config)#arp access-list ARPtest
SWITCH(config-arp-acl)#permit ip host
192.168.1.10 mac host 0011.70f1.e051
```

4. Po nakonfigurování ARP ACL pravidlo musíme aplikovat pro určitou VLANu.

```
SWITCH(config)#ip arp inspection filter ARPtest
vlan 100
```

Příkazy, které zobrazí různé informace o DAI

```
SWITCH#show ip arp inspection interfaces
SWITCH#show ip dhcp snooping binding
SWITCH#show ip arp inspection vlan 100,200
SWITCH#show ip arp inspection statistics vlan 100,200
```

arpspoof

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
arpspoof -i eth0 -t 192.168.1.63 -r 192.168.1.254
```

arpspoof a driftnet

```
root@P4ND4:~# netdiscover -r 192.168.243.0/24
```

```
root@P4ND4:~# arpspoof -i eth0 -t 192.168.243.129 192.168.243.2
0:c:29:be:39:e2 0:c:29:44:d:6a 0806 42: arp reply 192.168.243.2 is-at 0:c:29:be:
39:e2
```

```
root@P4ND4:~# arpspoof -i eth0 -t 192.168.243.2  192.168.243.129
0:c:29:be:39:e2 0:50:56:e7:b3:7f 0806 42: arp reply 192.168.243.129 is-at 0:c:29
:be:39:e2
0:c:29:be:39:e2 0:50:56:e7:b3:7f 0806 42: arp reply 192.168.243.129 is-at 0:c:29
:be:39:e2
0:c:29:be:39:e2 0:50:56:e7:b3:7f 0806 42: arp reply 192.168.243.129 is-at 0:c:29
:be:39:e2
0:c:29:be:39:e2 0:50:56:e7:b3:7f 0806 42: arp reply 192.168.243.129 is-at 0:c:29
:be:39:e2
0:c:29:be:39:e2 0:50:56:e7:b3:7f 0806 42: arp reply 192.168.243.129 is-at 0:c:29
:be:39:e2
```

```
0:c:29:be:39:e2 0:c:29:44:d:6a 0806 42: arp reply 192.168.243.2 is-at 0:c:29:be:
39:e2
0:c:29:be:39:e2 0:c:29:44:d:6a 0806 42: arp reply 192.168.243.2 is-at 0:c:29:be:
39:e2
0:c:29:be:39:e2 0:c:29:44:d:6a 0806 42: arp reply 192.168.243.2 is-at 0:c:29:be:
```

```
root@P4ND4:~# driftnet -i eth0
```

Příklad konfigurace ARP ACL

```
CORE-SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE-SW(config)#arp access-list ARP-ACL-01
CORE-SW(config-arp-nacl)#permit ip host 192.168.10.250 mac host aabb.c
CORE-SW(config-arp-nacl)#exit
CORE-SW(config)#do show arp access-list
ARP access list ARP-ACL-01
    permit ip host 192.168.10.250 mac host aabb.cc00.0831
```

Přiřazení ARP-ACL-01 na VLAN 10

```
CORE-SW(config)#ip arp inspection filter ARP-ACL-01 vlan 10
CORE-SW(config)#do show ip arp inspection vlan 10

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Stat
 ----     -------------    ---------   ---------          ----
   10     Enabled          Active      ARP-ACL-01         No
```

Konfigurační kroky DAI

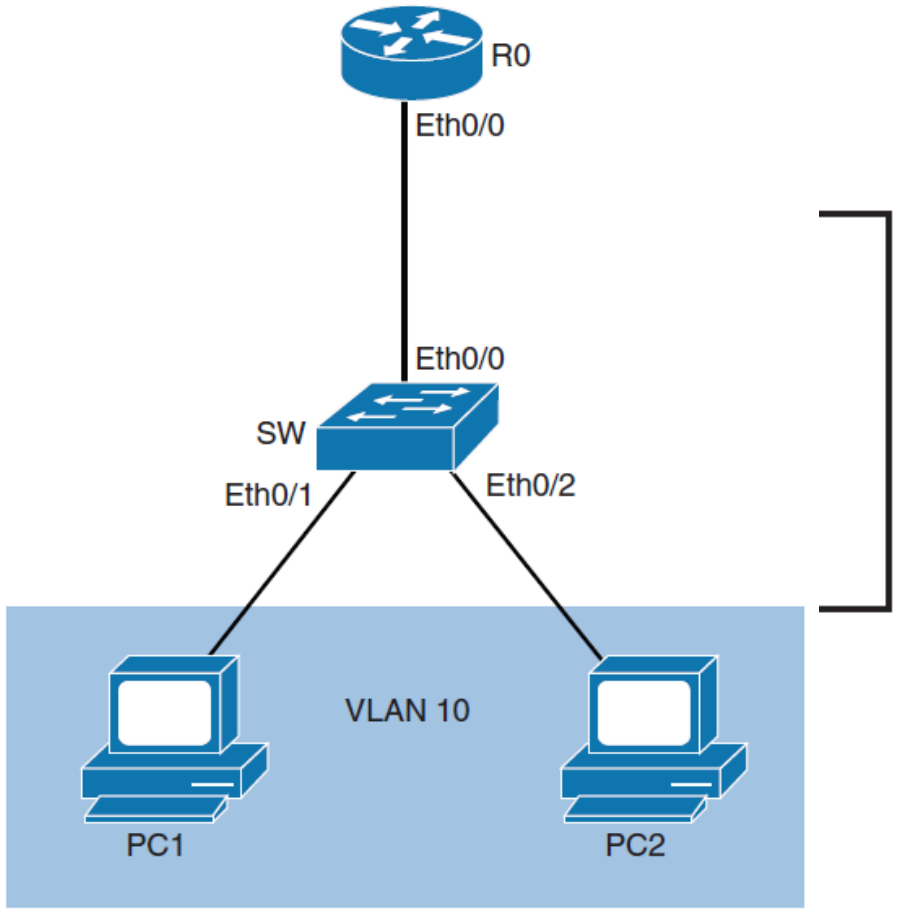
Krok 1. Implementujte ochranu proti spoofingu DHCP:
- Globálně povolte snooping DHCP.
- Povolte snooping DHCP na vybraných VLAN.

Krok 2. Zapněte DAI: Povolte kontrolu ARP na vybraných VLAN.

Krok 3. Konfigurace důvěryhodných rozhraní pro snooping DHCP a kontrolu ARP (výchozí nastavení je nedůvěryhodné).

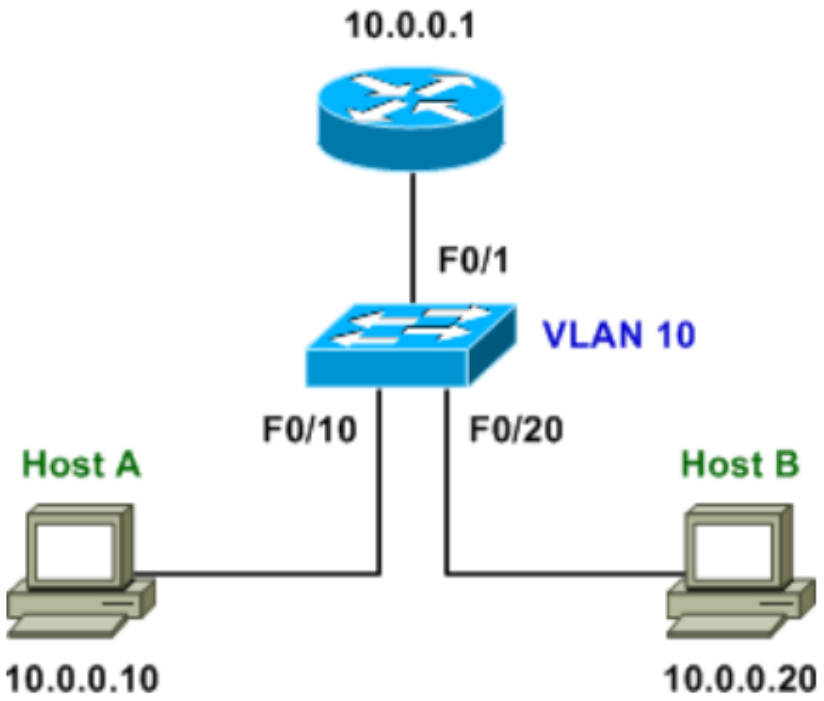
Konfigurace DAI

```
SW(config)# ip dhcp snooping
SW(config)# ip dhcp snooping vlan 10
SW(config)# ip arp inspection vlan 10
SW(config)# interface Ethernet 0/0
SW(config-if)# ip dhcp snooping trust
SW(config-if)# ip arp inspection trust
```



Příklad: static IP source address bindings

```
Switch(config)# interface f0/10
Switch(config-if)# ip verify source
Switch(config-if)# interface f0/20
Switch(config-if)# ip verify source
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10

Switch# show mac address-table int f0/10
          Mac Address Table
-------------------------------------------
Vlan      Mac Address         Type          Ports
10        001d.60b3.0add      DYNAMIC       Fa0/10
Total Mac Addresses for this criterion: 1

Switch#show mac address-table int f0/20
Mac Address Table
-------------------------------------------
Vlan      Mac Address         Type          Ports
10        0023.7d00.d0a8      DYNAMIC       Fa0/20
Total Mac Addresses for this criterion: 1

Switch# conf t
Switch(config)# ip source binding 001d.60b3.0add vlan 10 10.0.0.10 interface f0/10
Switch(config)# ip source binding 0023.7d00.d0a8 vlan 10 10.0.0.20 interface f0/20
```



Verifikace řešení

```
Switch(config)# do sh ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ----
Fa0/10     ip           active       10.0.0.10                        10
Fa0/20     ip           active       10.0.0.20                        10
```

Fajn, adresy jsou nakonfigurované.

```
Host_B$ ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=64 time=0.465 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=64 time=0.297 ms
64 bytes from 10.0.0.10: icmp_seq=3 ttl=64 time=0.385 ms
```

Z 20.0.0.20 ping na 10.0.0.10 funguje.

```
Host_B# scapy
Welcome to Scapy (2.0.0.11 beta)
>>> sendp(Ether()/IP(src='1.2.3.4', dst='10.0.0.10')/ICMP(), iface='eth0')
.
Sent 1 packets.
```

Že je odpověď na 1.2.3.4 a ne na 10.0.0.20 zjistíme z B pomocí Wiresharku.
Zapracovalo, že jsme napsali „důvěřuj zdroji“ – ip verify source.

Příkazy DAI

- **ip arp inspection vlan** *vlan-id* [**,** *vlan-id*]
  - Nastavuje DAI na VLAN nebo rozpětí VLAN
- **ip arp inspection trust**
  - Nastavuje rozhraní jako trusted
- **ip arp inspection validate** {[*src-mac*] [*dst-mac*] [*ip*]}
  - Konfiguruje DAI tak, aby v případě, že jsou adresy IP neplatné, zrušil pakety ARP, rovněž tak pokud adresy MAC v těle paketů ARP neodpovídají adresám zadaným v záhlaví sítě Ethernet

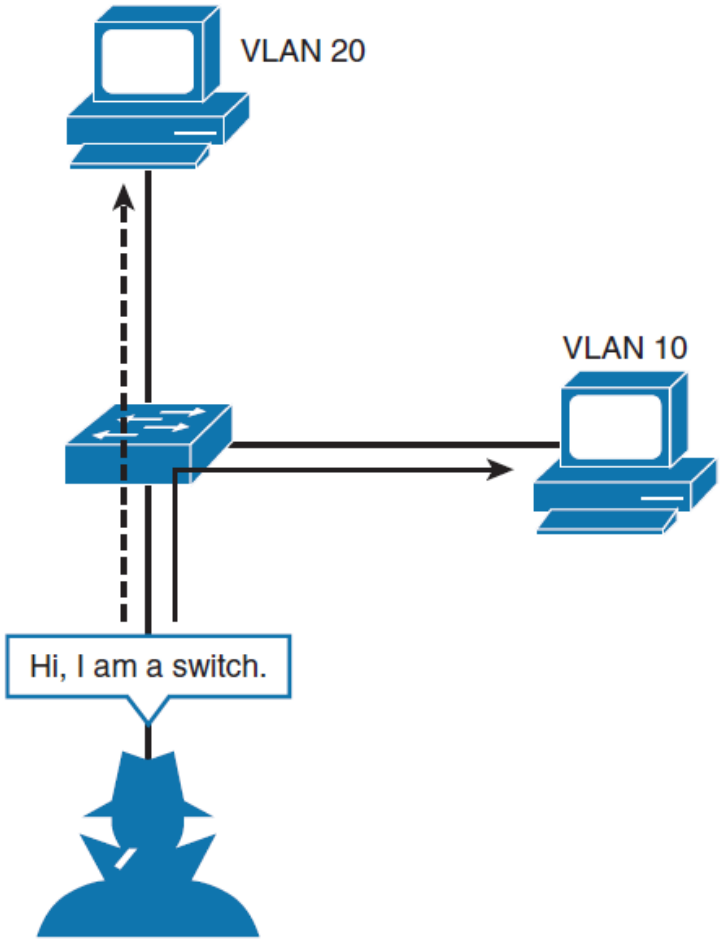
Bezpečnost VLAN Trunků

© 2007 – 2016, Cisco Systems, Inc. All rights reserved. Cisco Public

Bezpečnost VLAN trunků

- Popište spoofing útok spojený s VLAN trunky přepínače
- Chraňte svou síť před switch spoofingu
- Popište VLAN hopping útok
- Chraňte svou síť proti útoku VLAN hopping
- Popište potřebu VLAN ACL
- Popište, jak VLAN ÄCL komunikují se standardními a portů ACL
- Konfigurace VLAN ACL

Switch Spoofing



- Existuje několik mechanismů nebo osvědčených postupů, které minimalizují autorizovaný přístup k trunkovým portům a switch spoofing, včetně následujících
  - Ruční konfigurace
  - Shut down nepoužívaných rozhraní
  - Omezení VLANs na trunk portech

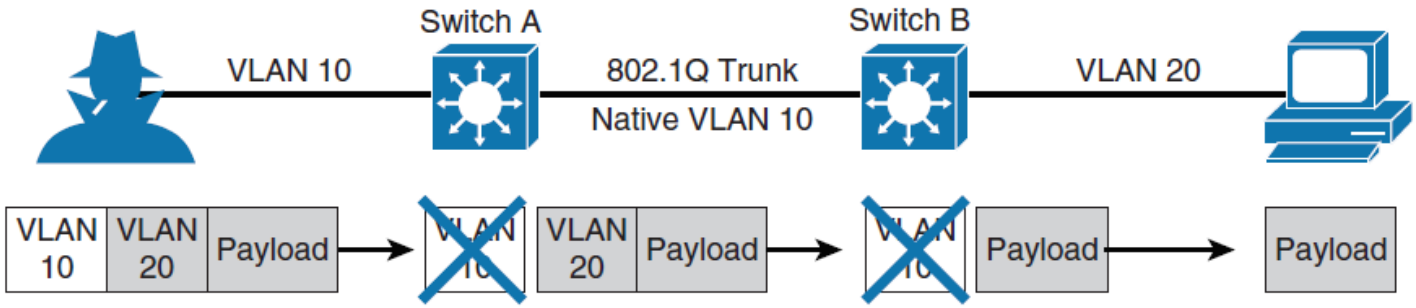
Switch Spoofing

```
SW(config)# interface interface-slot/number
SW(config-if)# switchport mode access
SW(config-if)# switchport access vlan vlan-id
```

```
SW(config)# interface interface-slot/number
SW(config-if)# shutdown
```

```
SW(config)# interface interface-slot/number
SW(config-if)# switchport trunk allowed vlan vlan-list
```

VLAN Hopping



- Zařízení s podporou IP, které útočník používá, musí být připojeno k access portu.
- Zařízení s podporou protokolu IP musí odeslat rámec s dvěmi tagy.
- Přepínač prvního skoku musí být nakonfigurován tak, aby přijímal rámce 802.1Q.
- Přepínač prvního skoku musí být připojen k jinému přepínači s trunkem 802.1Q a jeho nativní VLAN musí odpovídat vnějšímu VLAN tagu útočníků.

Ochrana proti VLAN Hoppingu

- Protože port VLAN útočníku musí odpovídat nativnímu VLAN trunku, jednoduchým řešením je nakonfigurovat nativní VLAN všech trunk portů na nevyužitou VLAN.`SW(config)# **interface** *interface-slot/number*`
- `SW(config-if)# **switchport trunk native** vlan *vlan-id*`
- `SW(config-if)# **switchport trunk allowed vlan remove** *vlan-id*`

- Další možností je defaultně označit všechny rámce na trunk portech jako tag. Příkaz ke konfiguraci této volby je následující:
- `SW(config)# **vlan dot1q tag native**`

  netagovaný provoz je pak vyhazován

VLAN Access Lists (VACL)

- VACL mohou poskytovat řízení přístupu pro všechny pakety, které jsou přemostěny v rámci sítě VLAN nebo pakety, které jsou směrovány do nebo z VLAN nebo rozhraní WAN.
- VACL lze konfigurovat pro provoz na vrstvách IP nebo MAC s určitými omezeními v závislosti na platformě a verzi softwaru.
- Přístupové seznamy VLAN (VACL) na přepínačích Catalyst slouží k následujícím dvěma odlišným účelům:
  - S určitými omezeními filtrujte provoz ve vrstvě 2.
  - Překonává omezení VLAN Switch Port Analyzer (SPAN) pomocí funkce Capture Port.

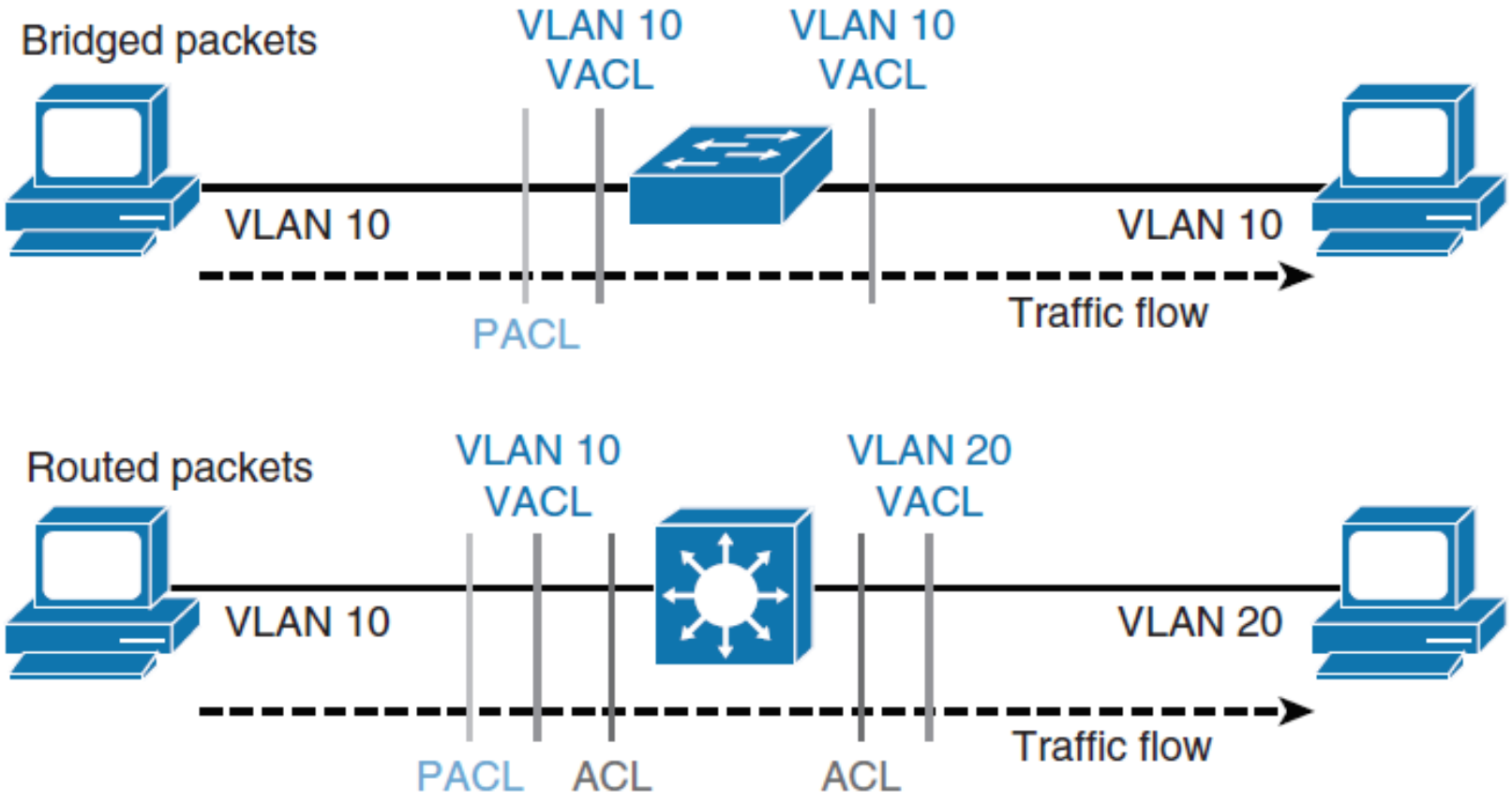
Proces VACL

- Každá přístupová mapa VLAN se může skládat z jedné nebo více mapových sekvencí; každá posloupnost má klauzuli o shodě a klauzuli o akci.
- Klauzule shody specifikuje IP nebo MAC ACL pro filtrování provozu a klauzule akce specifikuje akci, která má být provedena, když nastane shoda.
- Když tok odpovídá vstupu ACL povolení, je provedena příslušná akce a tok není zkontrolován proti zbývajícím sekvencím.
- Když se tok shoduje s položkou odmítnutí ACL, bude zkontrolován proti dalšímu ACL ve stejné sekvenci nebo následující sekvenci.
- Pokud tok neodpovídá žádné položce ACL a pro tento typ paketu je nakonfigurován alespoň jeden ACL, paket je vyhozen.

Výhody capture portu VACL Capture Port nad VSPAN

- **Analýza granuality provozu**
  - VACL mohou odpovídat na základě zdrojové IP adresy, cílové IP adresy, typu protokolu vrstvy 4, zdrojových a cílových portů vrstvy 4 a dalších informací.
  - **Počet relací**
    - VACLs jsou realizovány v hardwaru
- **Oversubscription cílového portu**
  - Identifikace granulárního provozu snižuje počet rámců, které mají být předávány do cílového portu, a tím minimalizuje pravděpodobnost jejich překročení.
- **VACL jsou realizovány v hardwaru**

Interakce VACL s ACL a PACL



Konfigurace VACLs

- SW(config)# **mac access-list extended** *acl-name*
- SW(config-ext-macl)# **permit host** [*source-mac* | **any**] [*destination-mac* | **any**]
- SW(config)# **ip access-list** *acl-type acl-name*
- SW(config-ext-nacl)# **permit protocol** [*source-address* | **any**] [*destination-address* | **any**]

- SW(config)# **vlan access-map** *map-name*
- SW(config-access-map)# **match** [**mac** | **ip**] **address** *acl-name*
- SW(config-access-map)# **action** [**drop**|**forward**|**redirect**][**log**]

- SW(config)# **vlan filter** *map-name* **vlan-list** [*vlan-list* | **all**]

Příkazy VACL

```
SW(config)# mac access-list extend simple-mac-acl
SW(config-ext-macl)# permit host 0000.001c.2014 any
SW(config-ext-macl)# exit
SW(config)# ip access-list extended simple-ip-acl
SW(config-ext-nacl)# permit ip host 192.168.1.1 any
SW(config-ext-nacl)# exit
SW(config)#
SW(config)# vlan access-map simple-vlan-map
SW(config-access-map)# match mac address simple-mac-acl
SW(config-access-map)# match ip address simple-ip-acl
SW(config-access-map)# action forward
SW(config-access-map)# exit
SW(config)# vlan filter simple-vlan-map vlan-list 2-10

SW(config)# end
```

Příklad VACL 1

mac access-list extended test

permit any host 0023.2343.5679

vlan access-map **test1** 10

match mac address test

action drop

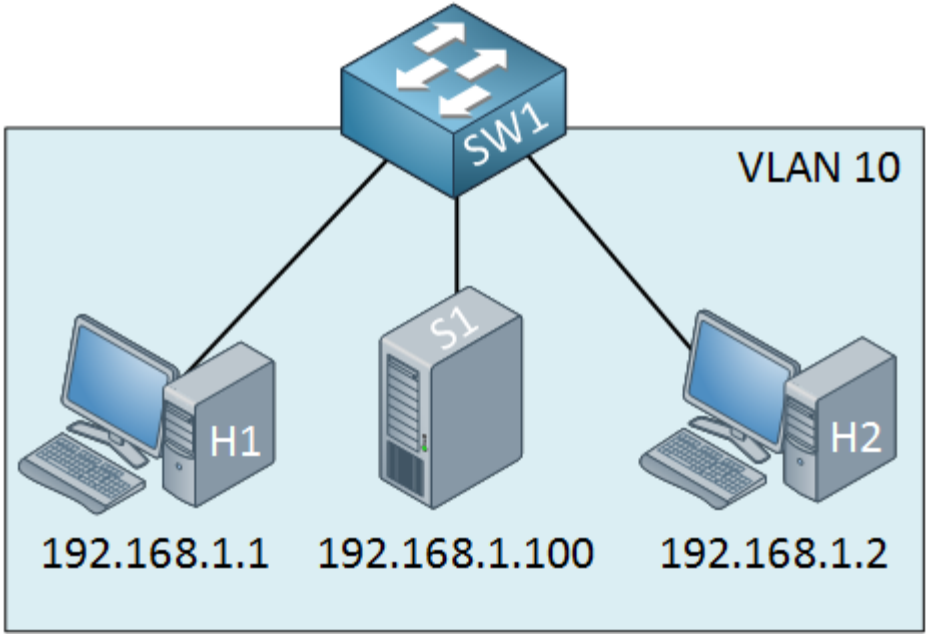
vlan access-map **test1** 20

action forward

vlan filter **test1** vlan-list 1 (všechny porty přepínače jsou v default vlan 1)

Příklad VACL 2

PC z VLAN mají zablokovaný přístup k serveru, ostatní komunikace je povolena



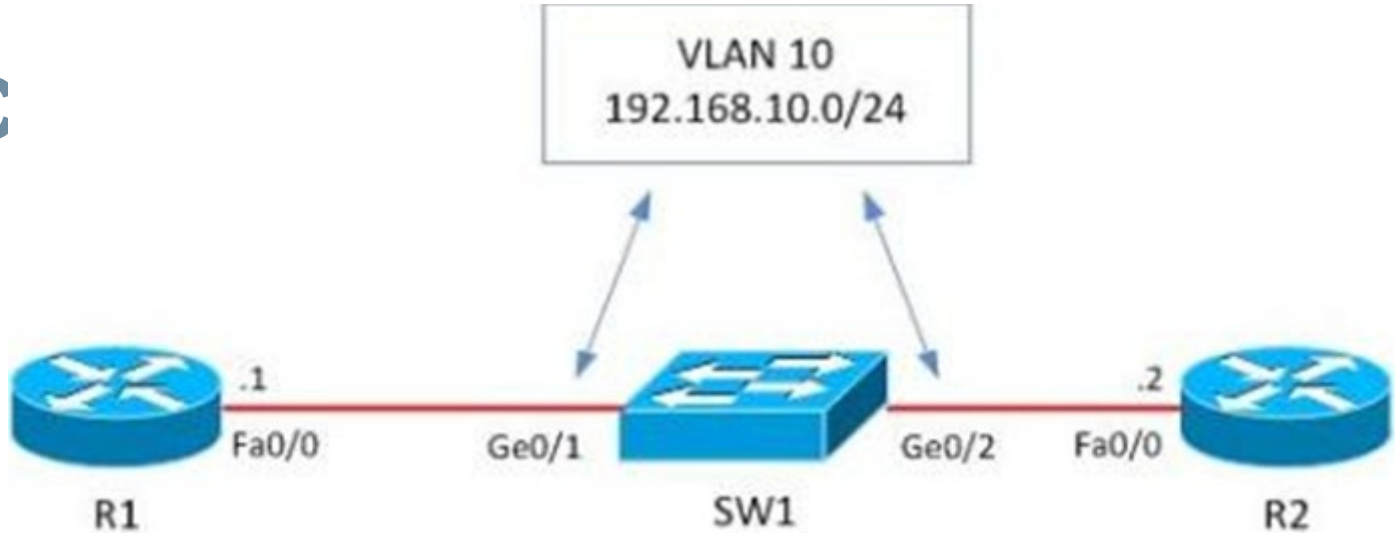
SW1(config)#**access-list 100 permit ip any host 192.168.1.100**

SW1(config)#**vlan access-map NOT-TO-SERVER 10**
SW1(config-access-map)#**match ip address 100**
SW1(config-access-map)#**action drop**
SW1(config-access-map)#**vlan access-map NOT-TO-SERVER 20**
SW1(config-access-map)**#action forward**

SW1(config)#**vlan filter NOT-TO-SERVER vlan-list 10**

P59klad VAC

Zákaz telnetu od R1, vše ostatní povoleno.

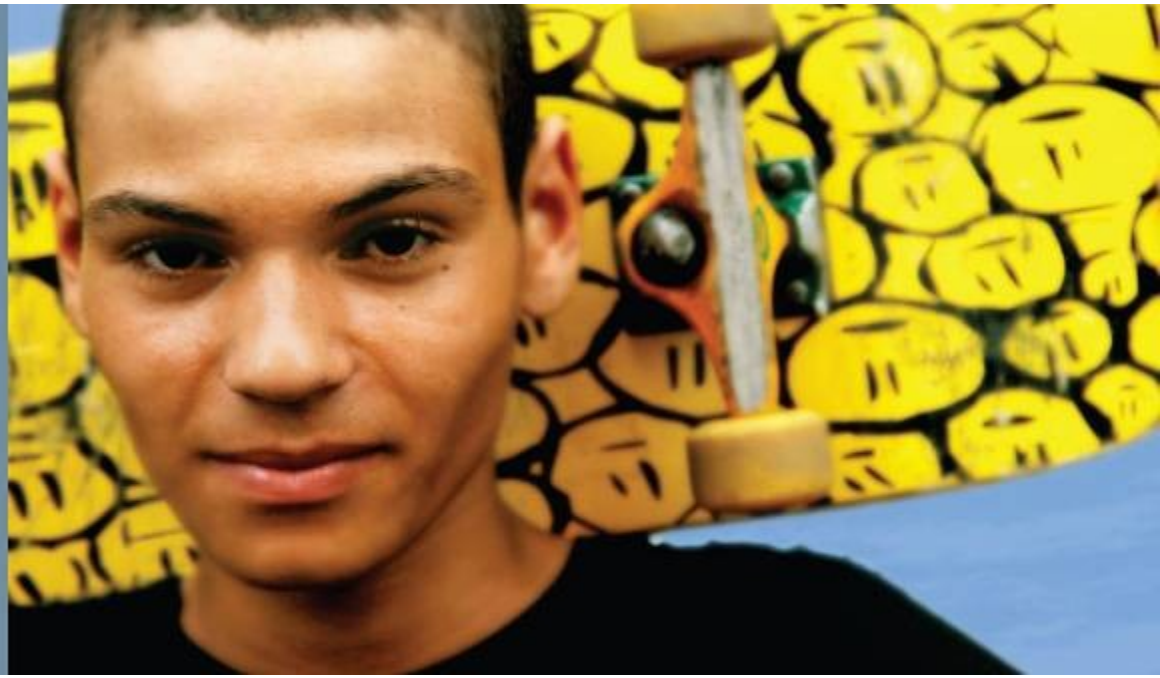


switch(config)#**ip access-list extended restrict_telnet_R2**
switch(config-ext-nacl)#**permit tcp host 192.168.10.1 host 192.168.10.2 eq 23**

switch(config-ext-nacl)#**vlan access-map VACL 10**
switch(config-access-map)#**action drop**
switch(config-access-map)#**match ip address restrict_telnet_R2**
switch(config-access-map)#**vlan access-map VACL 20**
switch(config-access-map)#**action forward**

switch(config)#**vlan filter VACL vlan-list 10**

Privátní VLANy



Privátní VLANy

- Úvod do privátních VLAN
- Popište privátní funkci VLAN
- Popište typy privátních portů VLAN
- Konfigurace privátních sítí VLAN
- Ověřte privátní konfiguraci VLAN
- Popište privátní VLAN přes více přepínačů
- Popište funkci chráněného portu

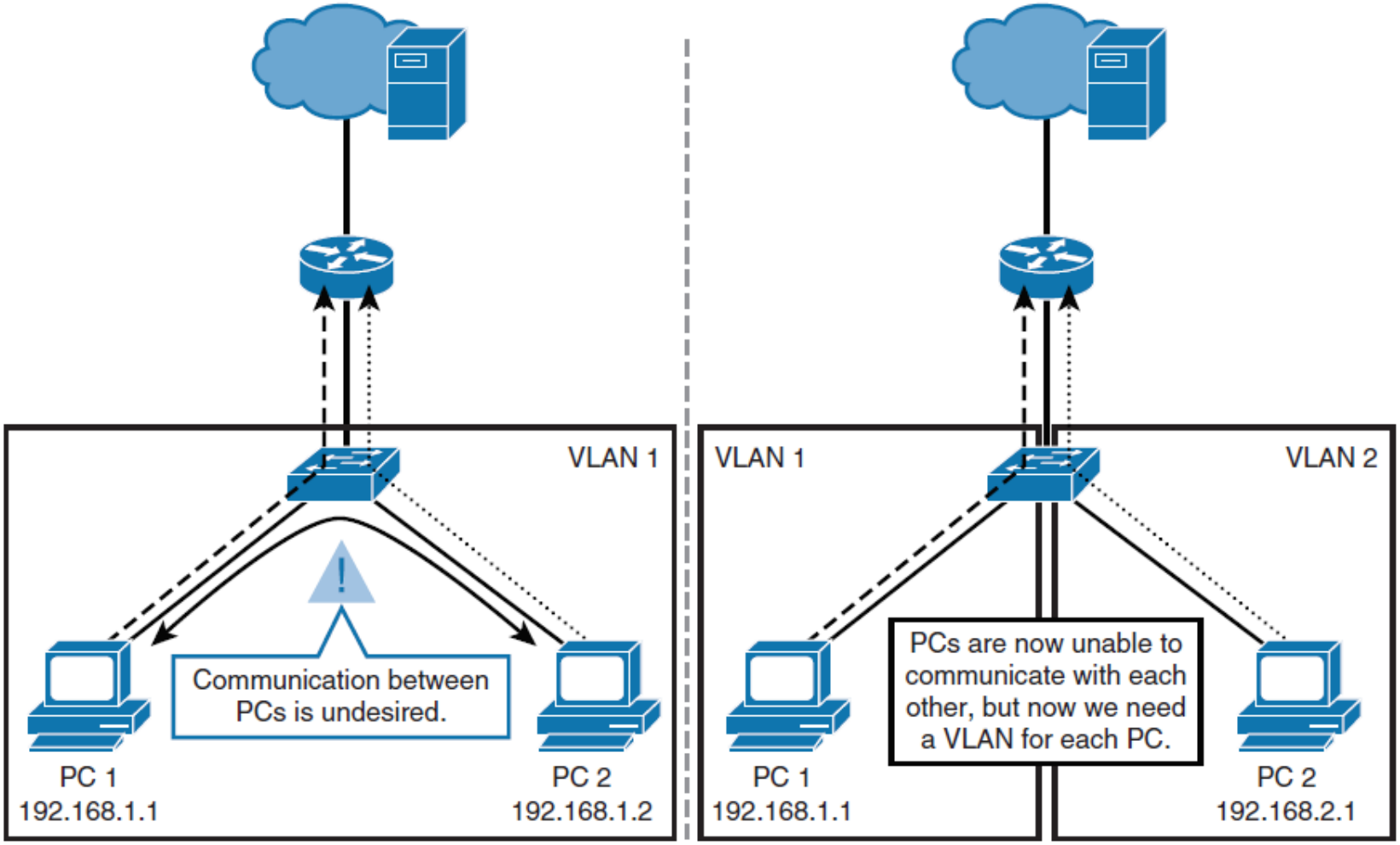
Úvod do PVLAN

- PVLAN omezují koncová zařízení, jako jsou počítače a mobilní zařízení, od vzájemné komunikace, ale přesto umožňují komunikaci s porty směrovačů a síťovými službami.
- Zařízení koncového uživatele se budou chovat normálně, ale nebudou moci komunikovat s jinými zařízeními ve stejné doméně vrstvy 2.
- Tento mechanismus poskytuje úroveň bezpečnosti.
- Přiřazení každého jednotlivého koncového zařízení jeho vlastní VLAN by provedlo stejnou bezpečnostní metodu jako PVLAN; přepínače však mají omezený počet podporovaných VLAN a velký počet VLAN vytváří problémy se škálovatelností.

Úvod do PVLAN

- PVLAN jsou v podstatě VLAN uvnitř VLAN.
- Pro směrování paketů mezi různými PVLANy je zapotřebí zařízení vrstvy 3.
- Když je VLAN rozdělena do PVLAN, zařízení v různých PVLAN stále patří do stejné IP podsítě, ale nejsou schopny vzájemně komunikovat na vrstvě 2.
- PVLANs jsou elegantním řešením, když potřebujete udržet více zařízení ve stejné podsíti IP a zároveň zajistit izolaci portu na vrstvě 2.

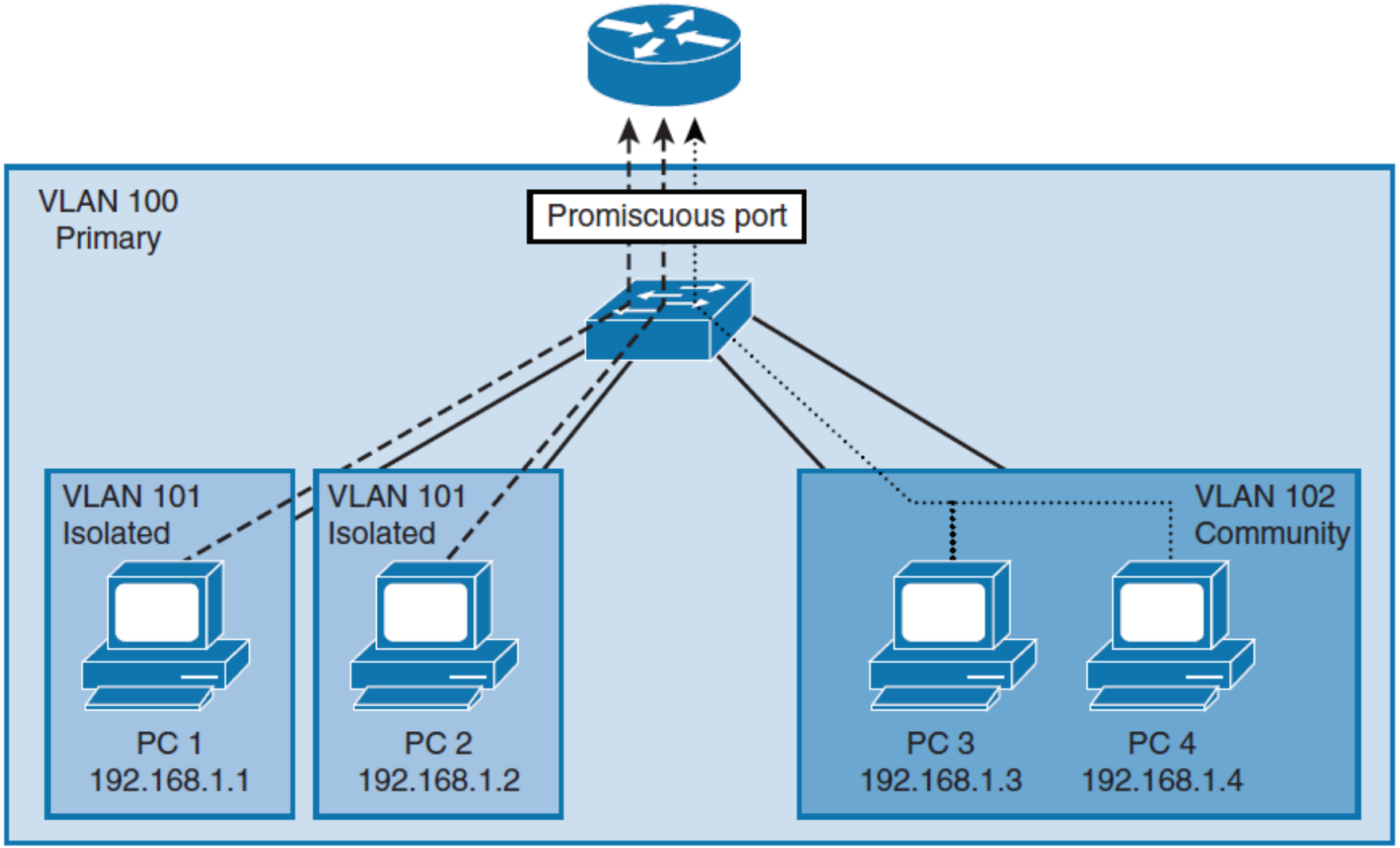
Úvod do PVLAN



Typy portů PVLAN

- Doména PVLAN má jednu **primární VLAN**.
- Každý port v privátní VLAN doméně je členem primární VLAN; primární VLAN je celá soukromá VLAN doména.
- **Sekundární VLAN** jsou subdomény, které zajišťují izolaci mezi porty v rámci stejné privátní domény VLAN.
- Existují dva typy sekundárních VLAN: izolované VLAN a komunitní VLAN.
  - **Izolované VLAN** obsahují izolované porty, které mezi sebou nemohou komunikovat v izolovaném VLAN.
  - **Komunitní VLAN** obsahují komunitní porty, které mohou komunikovat mezi sebou v komunitní VLAN.

Typy portů PVLAN



Typy portů PVLAN

- **Promiskuitní**
  - Promiskuitní port patří do primární VLAN a může komunikovat se všemi mapovanými porty v primární VLAN, včetně komunitních a izolovaných portů.
  - V primární síti VLAN může být více promiskuitních portů.
- **Izolovaný**
  - Izolovaný port je hostitelský port, který patří do izolovaného sekundárního VLAN.
  - Izolovaný port je od ostatních portů zcela izolovaný, s výjimkou přidružených promiskuitních portů.
  - V určeném izolovaném VLAN můžete mít více než jeden izolovaný port.
- **Komunitní**
  - Komunitní port je hostitelský port, který patří do sekundární VLAN komunity.
  - Komunitní porty komunikují s ostatními porty ve stejné VLAN komunity as přidruženými promiskuitními porty.
  - Jsou izolovány od všech portů v jiných komunitních VLANs a všech izolovaných portech.

Konfigurace PVLAN

- VTP musí být nastaven jako transparentní nebo vypnutý.
- Nakonfigurujte primární VLAN.
- Nakonfigurujte sekundární VLAN a aplikujte konfiguraci těchto PVLAN jako izolované nebo komunitní.
- Připojte (asociujte) primární VLANy k sekundárním VLANům.

```
SW(config)# vlan 100
SW(config-vlan)# private-vlan primary
SW(config)# vlan 101
SW(config-vlan)# private-vlan isolated
SW(config)# vlan 102
SW(config-vlan) private-vlan community
SW(config) vlan 100
SW(config-vlan) private-vlan association 101, 102
```

Přiřazení portů

- Promiskuidní Porty
- SW(config)# **interface** *interface-slot/number*
- SW(config-if)# **switchport mode private-vlan promiscuous**
- SW(config-if)# **switchport private-vlan mapping** *primary-vlan-id* **add** *secondary-vlanid* {, *secondary-vlan-id* }

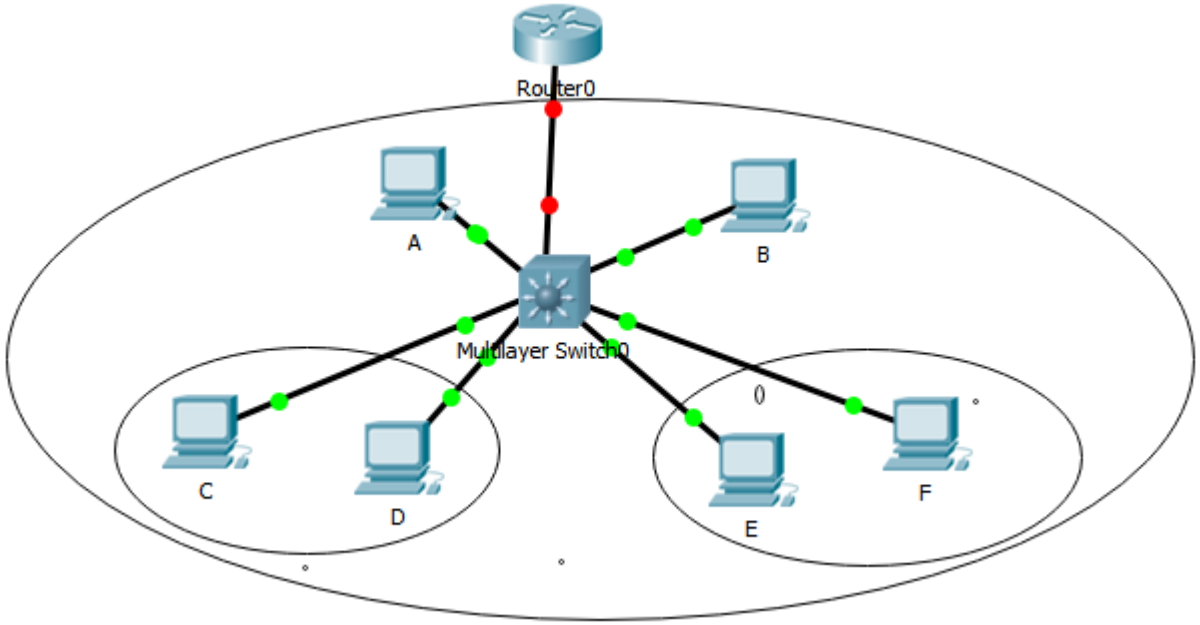
- Komunitní nebo izolované porty
- SW(config)# **interface range** *interface-range*
- SW(config-if-range)# **switchport mode private-vlan host**
- SW(config-if-range)# **switchport private-vlan host-association** *primary-vlan-id secondary-vlan-id*

Přiřazení portů

```
SW(config)# interface GigabitEthernet 0/1
SW(config-if)# switchport description Interface-to-Router
SW(config-if)# switchport mode private-vlan promiscuous
SW(config-if)# switchport private-vlan mapping 100 add 101, 102
SW(config-if)# interface range GigabitEthernet 0/2-3
SW(config-if-range)# switchport description End-User-Ports-In-Isolated-PVLAN
SW(config-if-range)# switchport mode private-vlan host
SW(config-if-range)# switchport private-vlan host-association 100 101
SW(config-if)# interface range GigabitEthernet 0/4-5
SW(config-if-range)# switchport description End-User-Ports-In-Community-PVLAN
SW(config-if-range)# switchport mode private-vlan host
SW(config-if-range)# switchport private-vlan host-association 100 102
```

Příklad 1
Zadání:
A, B izolovaná 101,
C, D komunitní 102,
E, F komunitní 104
R0 promiskuitní,
A, B, C, D sekundární VLAN, všechny v primární VLAN 100

A nemůže komunikovat s B
C může komunikovat s D

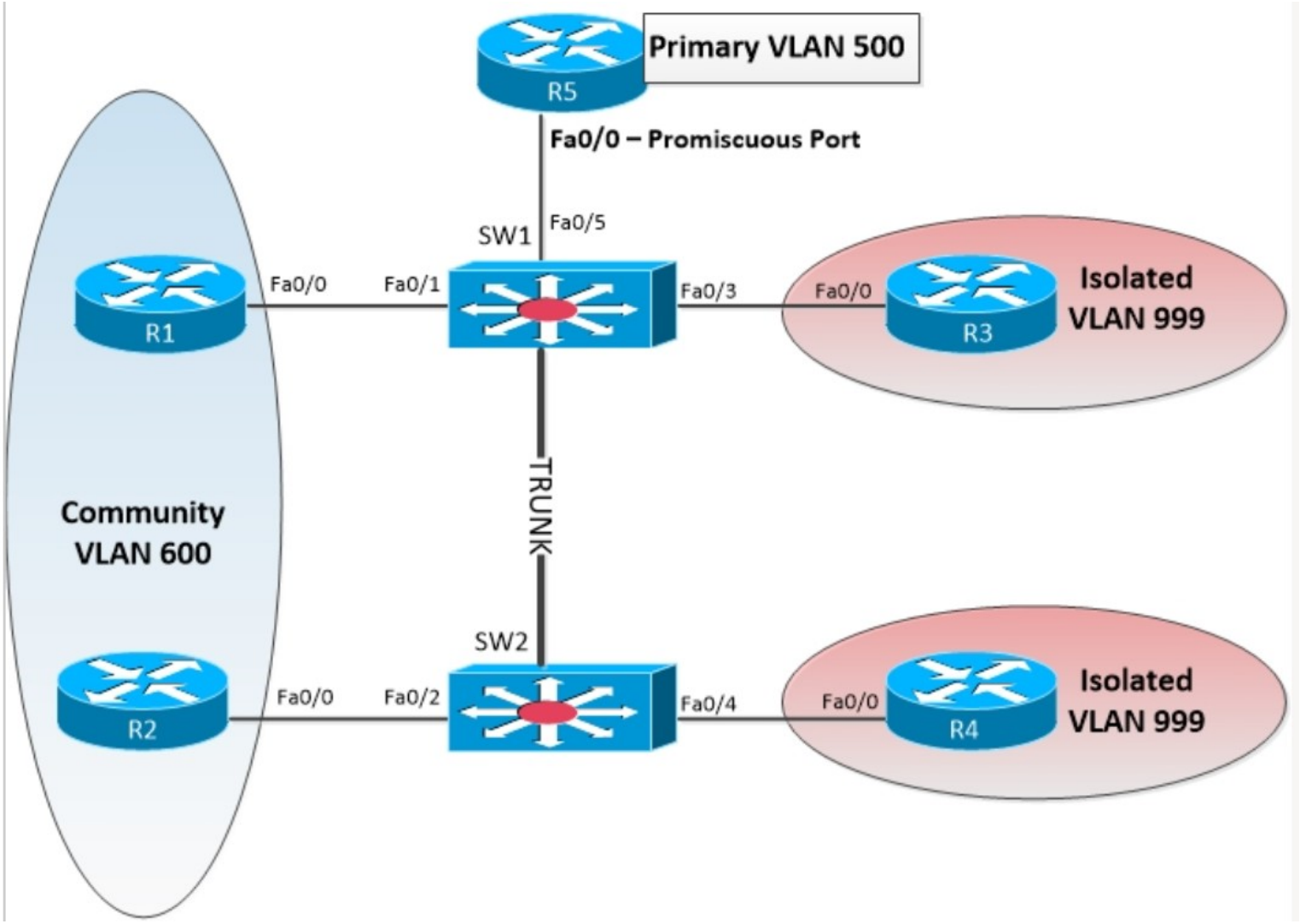


Konfigurace

Switch(config)**#vtp mode transparent**
Switch(config)**#vlan 101**
Switch(config-vlan)**#private-vlan isolated**
Switch(config-vlan)**#vlan 102**
Switch(config-vlan)**#private-vlan community**
Switch(config-vlan)**#vlan 103**
Switch(config-vlan)**#private-vlan community**
Switch(config-vlan)**#vlan 100**
Switch(config-vlan)**#private-vlan primary**
Switch(config-vlan)**#private-vlan association 101,102,103**
Switch(config)**# interface f0/1**
Switch(config-if)**# switchport mode private-vlan promiscuous**
Switch(config-if)**# switchport private-vlan mapping 100 101,102,103**
Switch(config)**# interface range f0/2 – 0/3** //connect to host A and B
Switch(config-if)**# switchport mode private-vlan host**
Switch(config-if)**# switchport private-vlan host-association 100 101**
Switch(config-if)**# interface range f0/3 -0/4** //connect to host C and D
Switch(config-if)**# switchport mode private-vlan host**
Switch(config-if)**# switchport private-vlan host-association 100 102**
Switch(config-if)**# interface f0/5 – 0/6** //connect to host E and F
Switch(config-if)**# switchport mode private-vlan host**
Switch(config-if)**# switchport private-vlan host-association 100 103**

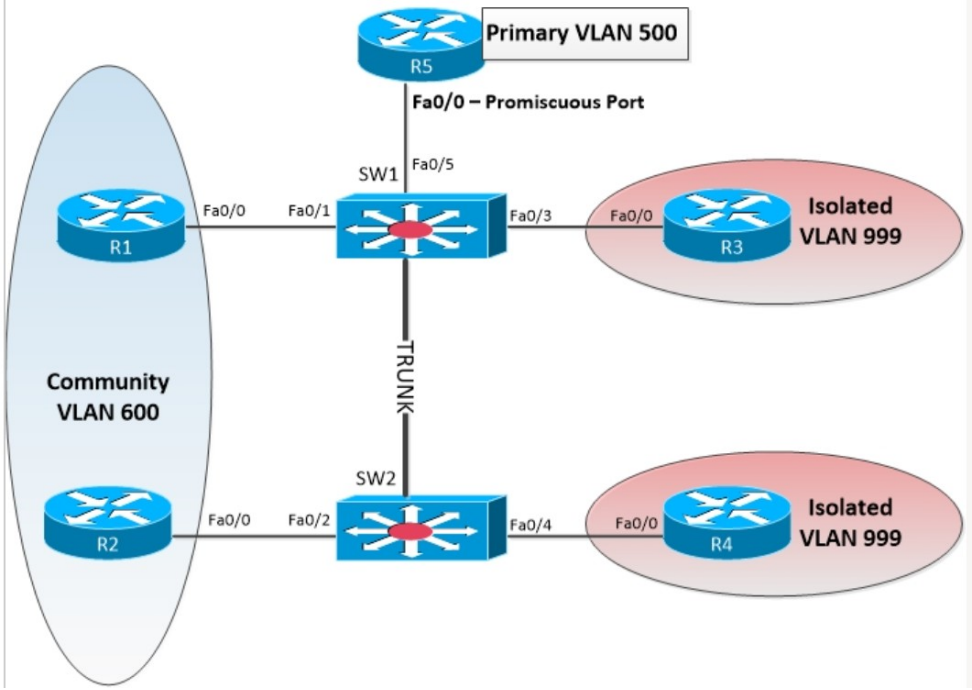
Switch(config)**#vtp mode transparent**
Switch(config)**#vlan 101**
Switch(config-vlan)**#private-vlan isolated**
Switch(config-vlan)**#vlan 102**
Switch(config-vlan)**#private-vlan community**
Switch(config-vlan)**#vlan 103**
Switch(config-vlan)**#private-vlan community**
Switch(config-vlan)**#vlan 100**
Switch(config-vlan)**#private-vlan primary**
Switch(config-vlan)**#private-vlan association 101,102,103**
Switch(config)**# interface f0/1**
Switch(config-if)**# switchport mode private-vlan promiscuous**
Switch(config-if)**# switchport private-vlan mapping 100 101,102,103**
Switch(config)**# interface range f0/2 – 0/3** //connect to host A and B
Switch(config-if)**# switchport mode private-vlan host**
Switch(config-if)**# switchport private-vlan host-association 100 101**
Switch(config-if)**# interface range f0/3 -0/4** //connect to host C and D
Switch(config-if)**# switchport mode private-vlan host**
Switch(config-if)**# switchport private-vlan host-association 100 102**
Switch(config-if)**# interface f0/5 – 0/6** //connect to host E and F
Switch(config-if)**# switchport mode private-vlan host**
Switch(config-if)**# switchport private-vlan host-association 100 103**

Zadání příkladu 2



© 2007 – 2016, Cisco Systems, Inc. All rights reserved. Cisco Public

Řešení příkladu 2




```
SW1(config)#vtp mode transparent
SW2(config)#vtp mode transparent

SW1(config)#vlan 500,600,999
SW2(config)#vlan 500,600,999

SW1(config-vlan)#private-vlan primary
SW1(config)#vlan 600
SW1(config-vlan)#private-vlan community
SW1(config)#vlan 999
SW1(config-vlan)#private-vlan isolated
SW1(config)#vlan 500
SW1(config-vlan)#private-vlan association 600,999

SW2(config)#vlan 500
SW2(config-vlan)#private-vlan association 600,999
```

Pokračování řešení příkladu 2

```
SW1(config)#int fa0/1
SW1(config-if)#description to R1
SW1(config-if)#switchport private-vlan host-association 500 600
SW1(config-if)#switchport mode private-vlan host
SW1(config-if)#spanning-tree portfast
SW2(config)#int fa0/2
SW2(config-if)#description to R2
SW2(config-if)#switchport private-vlan host-association 500 600
SW2(config-if)#switchport mode private-vlan host
SW2(config-if)#spanning-tree portfa
SW1(config)#int fa0/3
SW1(config-if)#description to R3
SW1(config-if)#switchport private-vlan host-association 500 999
SW1(config-if)#spanning-tree portfast
SW1(config)#int fa0/4
SW2(config-if)#description to R4
SW2(config-if)#switchport private-vlan host-association 500 999
SW2(config-if)#spanning-tree portfast
```

Kontrola výsledku příkladu 2

- SW2(config-if)#spanning-tree portfast
- SW1#sh vlan private-vlan
-
- Primary Secondary Type Ports
- ------- --------- ---------- ----------
- 500 600 community Fa0/1
- 500 999 isolated Fa0/3
-
- SW1#sh vlan private-vlan type
- Vlan Type
- ---- ----------
- 500 primary
- 600 community
- 999 isolated

Použití Protected portů

- Funkce PVLAN není dostupná na všech přepínačích.
- Chráněný port, známý také jako PVLAN edge, je funkce, která má (na rozdíl od PVLAN) pouze lokální význam pro přepínač.
- Chráněné porty nepředávají žádný provoz do chráněných portů na stejném přepínači.

- `SW(config)# interface interface-slot/number`
- `SW(config-if)# switchport protected`

Souhrn kapitoly 10

- Konfigurujte zabezpečení portu, abyste omezili a filtrovali adresy MAC na portech; zabezpečení portů podporuje funkce, které snižují režii při přidělování adres MAC na jeden port.
- Použijte PVLAN pro omezení provozu v rámci VLAN s jednoduchou konfigurací.
- Chcete-li zabránit útokům spoofingu, využijte snooping DHCP, DAI a IPSG.
- Zvažte VACL, je-li to vhodné pro blokování zbytečného provozu a známých útoků.
- Na všech zařízeních Cisco vždy dodržujte základní konfigurace zabezpečení, například AAA.
- Zůstaňte v kontaktu se všemi zranitelnostmi a bezpečnostními upozorněními od společnosti Cisco.
- Udržujte aktuální informace o verzích softwaru Cisco Catalyst, protože nové verze softwaru řeší známé bezpečnostní chyby.

Chapter 10 Labs

- **CCNPv7.1 SWITCH Lab 10.1 Securing Layer2**
- **CCNPv7.1 SWITCH Lab 10.2 Securing VLANs**
- **https://slideplayer.com/slide/3561082/**

© 2007 – 2016, Cisco Systems, Inc. All rights reserved. Cisco Public