Stretnutie 6:
Bezpečnosť prepínaných sietí

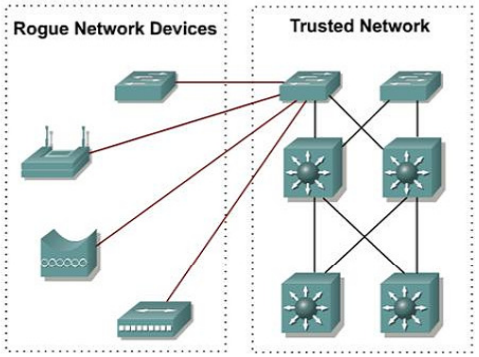
SWITCH Modul 6

Riadenie prístupu do prepínanej siete

Port Security

Riadenie prístupu k prepínanej sieti

- Častým (a často neželaným) javom je nekontrolované pripájanie zariadení k prepínanej sieti
  - Nové notebooky, PC, prístupové body, routery, PDA, ...
- Úlohou prepínačov v prístupovej vrstve je aj ochrana prístupu do siete
- Prepínače Cisco ponúkajú niekoľko mechanizmov na riadenie prístupu k prepínanému portu
  - Port Security
  - Autentifikácia 802.1X
  - Network Admission Control (nie je predmetom tohto kurzu)



Port Security

- Funkcia Port Security umožňuje na porte definovať zoznam tzv. bezpečných (secure) MAC adries
  - Zabezpečený port povolí komunikovať len staniciam, ktorých MAC adresa sa nachádza v zozname
- Bezpečné adresy môžu byť troch druhov:
  - **Static secure MAC**: manuálne nakonfigurovaná adresa
    - Nachádza sa v konfigurácii aj v CAM tabuľke
    - Po reštarte prepínača sa opätovne načíta z uloženej konfigurácie
  - **Dynamic secure MAC**: dynamicky získaná adresa z CAM
    - Nachádza sa len v CAM tabuľke
    - Po odpojení portu alebo reštarte prepínača sa stráca
  - **Sticky secure MAC**: hybrid medzi statickou a dynamickou adresou
    - Získava sa dynamicky, no prepínač automaticky vygeneruje záznam do bežiacej konfigurácie
    - Nachádza sa v konfigurácii aj v CAM tabuľke
    - Po reštarte prepínača sa opätovne načíta z uloženej konfigurácie

Port Security

- Na porte je možné definovať maximálny počet bezpečných adries
  - Statické adresy sa započítavajú do počtu bezpečných adries
  - Prepínač automaticky pridá každú novú neznámu MAC adresu do zoznamu bezpečných adries ako dynamickú resp. sticky
  - Ak by sa však pridaním novej adresy prekročil maximálny počet bezpečných adries, nastáva tzv. porušenie bezpečnosti (security violation)
- Na bezpečnostné porušenie možno zareagovať trojakým spôsobom
  - **Protect**: rámec s nepovolenou MAC adresou sa zahodí
  - **Restrict**: rámec s nepovolenou MAC adresou sa zahodí a zároveň sa incident zaznamená (hláška na konzolu, syslog, SNMP trap...)
  - **Shutdown**: port sa pri prijatí rámca s nepovolenou MAC adresou automaticky uvedie do stavu err-disabled

Konfigurácia Port Security

- Port Security sa konfiguruje individuálne na prepínaných portoch
- Odporúčaný postup:
  - Port nastaviť do režimu „access“ alebo „trunk“
    - Nevyhnutné – Port Security nie je podporovaná na dynamických portoch
  - Nastaviť maximálny povolený počet MAC adries
    - Nepovinné, predvolený počet je 1
  - Definovať statické bezpečné adresy, prípadne sticky learning
    - Nepovinné
  - Určiť reakciu pri porušení bezpečnosti
    - Nepovinné, predvolená reakcia je shutdown
  - Určiť spôsob expirácie bezpečných adries
    - Nepovinné. Bez dodatočného nastavenia statické a sticky adresy neexpirujú vôbec, dynamické expirujú až pri odpojení portu
  - Aktivovať port security
    - Nevyhnutné a často prehliadnuté!

Konfigurácia a kontrola Port Security

```
Sw(config)# interface fa0/2
Sw(config-if)# switchport mode access
Sw(config-if)# switchport port-security maximum 5
Sw(config-if)# switchport port-security mac-address 001c.2320.3a28
Sw(config-if)# switchport port-security violation restrict
Sw(config-if)# switchport port-security aging time 10
Sw(config-if)# switchport port-security
```

```
Sw# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/2             5            3                  0         Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 8192
```

Konfigurácia a kontrola Port Security

```
Sw# show port-security address
          Secure Mac Address Table
----------------------------------------------------------------------------
Vlan    Mac Address       Type                       Ports   Remaining Age
                                                                (mins)
----    -----------       ----                       -----   -------------
   1    0011.2233.4455    SecureConfigured           Fa0/2         -
   1    00e0.4c3b.b787    SecureDynamic              Fa0/2         8
   1    0200.0000.0001    SecureDynamic              Fa0/2         8
----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 8192
```

Konfigurácia a kontrola Port Security

```
Sw# show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 3
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00e0.4c3b.b787:1
Security Violation Count   : 0
```

Port Security – záverečné poznámky

- Port Security je dobrou ochranou proti MAC floodingu
  - Generovanie rámcov s náhodnými MAC odosielateľa a prepĺňanie CAM
- Akonáhle je na porte aktivovaná Port Security, naučené adresy v CAM sa konvertujú na bezpečné adresy
  - Ak je počet adries na porte v CAM vyšší než povolený počet bezpečných adries, dôjde k bezpečnostnému porušeniu
- Príkaz `no switchport port-sec mac-addr sticky` odstráni z konfigurácie aj všetky sticky MAC adresy
  - V CAM tieto adresy zostanú s povahou dynamic secure MAC adries
- Na portoch, kde je definovaná Voice VLAN, je potrebné nastaviť počet povolených MAC adries aspoň na 2
- Kurikulum uvádza, že statické MAC a sticky learning nie je možné použiť na portoch s Voice VLAN
  - Toto obmedzenie platí pre 2950 vo všetkých verziách IOSu
  - Na 3550 toto obmedzenie neplatí od verzie IOSu 12.2(25)SEB
  - Na 2960 a 3560 toto obmedzenie neplatí od verzie IOSu 12.2(25)SEC

Rozšírené AAA

Authentication, Authorization, Accounting

- AAA je súbor mechanizmov pre autentifikáciu, autorizáciu a účtovanie
  - Autentifikácia: Overenie identity (Kto je to?)
  - Autorizácia: Pridelenie práv (Čo môže robiť?)
  - Účtovanie: Evidencia používania služieb (Koľko zaplatí?)
- Na Cisco zariadeniach sa AAA využíva na rôzne účely
  - Riadenie administratívneho prístupu (EXEC)
  - 802.1X na prepínačoch a access pointoch
  - WPA alebo WPA2 Enterprise
  - PPP, IPSec

Modely AAA

- Na Cisco zariadeniach je možné prepínať sa medzi dvomi modelmi AAA
- Starší model
  - Autentifikácia len voči lokálnej databáze
  - Autorizácia len voči lokálnej databáze
  - Minimálne (ak vôbec nejaké) možnosti pre účtovanie
- Novší model
  - Komplexná konfigurácia, ktorá umožňuje rôzne služby nasmerovať na AAA voči rôznym databázam

Nový model AAA

- Nový model AAA vychádza z týchto predpokladov
  - Na jednej strane máme isté druhy služieb, ktoré vedia pomocou istého mechanizmu riadiť prístup (dot1x, enable, login, ppp)
  - Na druhej strane máme rôzne databázy s evidenciou používateľov a ich práv (RADIUS, TACACS, lokálna databáza)
  - My chceme mať možnosť konkrétnej službe vysvetliť, v akej databáze má používateľa vyhľadať
- Napríklad:
  - Konzolové prihlásenia sa overia voči lokálnej databáze
  - SSH prihlásenia sa overia voči RADIUS serveru s IP 1.2.3.4
  - PPP prihlásenia sa overia voči RADIUS serveru s IP 5.6.7.8
  - Ethernet klienti sa overia voči RADIUS serveru s IP 9.8.7.6

Konfigurácia AAA

- Aktivácia podpory nového AAA:

```
Router(config)# aaa new-model
```

- Vytvorenie zoznamu autentifikačných metód (databáz) pre zvolený typ autentifikácie:

```
Router(config)# aaa authentication { ppp | dot1x | enable
  | login } MENO db [ db … ]
```

- Použitie závisí na konkrétnom druhu aplikácie, napr:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login L_LOCAL local
Router(config)# line vty 0 15
Router(config-line)# login authentication L_LOCAL
```

Konfigurácia AAA

- Pri novom AAA je autentifikácia striktne oddelená od autorizácie
  - Systém vás prihlási, ale nedostanete práva
- Vytvorenie zoznamu autorizačných metód (databáz) pre zvolený typ autorizácie:

```
Router(config)# aaa authorization { exec | network | … }
  MENO db [ db … ]
```

- Použitie závisí na konkrétnom druhu aplikácie, napr:

```
Router(config)# aaa new-model
Router(config)# aaa authorization exec E_LOCAL local
Router(config)# line vty 0 15
Router(config-line)# authorization exec E_LOCAL
```

Príklad konfigurácie

- Využitie lokálnej databázy:

```
aaa new-model
aaa authentication login L_LOCAL local
aaa authorization exec E_LOCAL local
line vty 0 15
 login authentication L_LOCAL
 authorization exec E_LOCAL
```

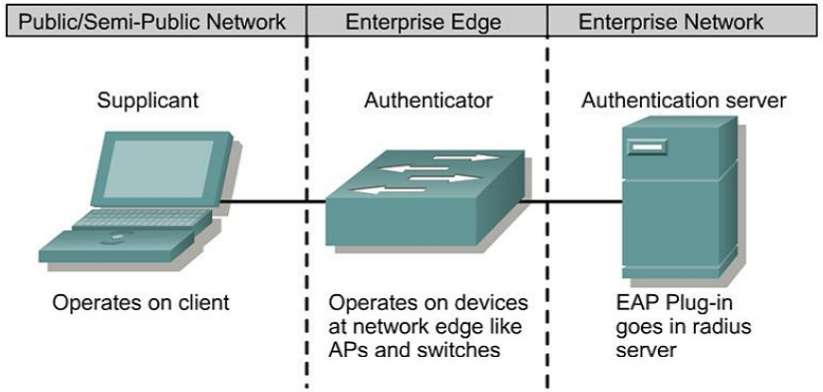
- Využitie RADIUS servera a lokálnej databázy:

```
aaa new-model
aaa authentication login L_RAD+L group radius local
aaa authorization exec E_RAD+L group radius local
radius-server host 1.2.3.4 auth-port 1812 acct-port 1813 key HESLO
line vty 0 15
 login authentication L_RAD+L
 authorization exec E_RAD+L
```

Riadenie prístupu do prepínanej siete

802.1X

Autentifikácia 802.1X



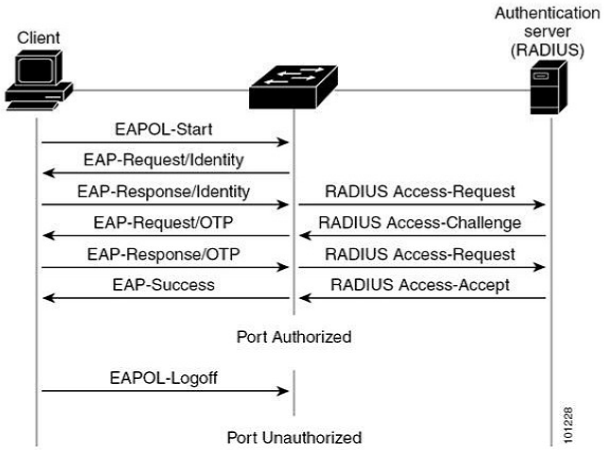
- Autentifikácia 802.1X umožňuje vyžiadať si od používateľa zvolené prihlasovacie údaje
  - Na prepínači sa port odblokuje až po úspešnom prihlásení
  - Pri neúspešnom prihlásení môže port zostať v karanténnej alebo hosťovskej VLAN

Autentifikácia 802.1X

- Autentifikácia 802.1X využíva niekoľko podporných komponentov a protokolov
  - Supplicant: softvérový klient na PC, zodpovedný za odovzdávanie autentifikačných dát
  - Authenticator: zariadenie, ku ktorému sa PC pripája a ktoré vyžaduje, aby sa klient korektne autentifikoval
  - Autentifikačný server: obsahuje databázu informácií o používateľoch
  - Extensible Authentication Protocol (EAP): generický protokol pre odovzdávanie autentifikačných informácií, špecifikovaný v RFC 3748
  - RADIUS: autentifikačný komunikačný protokol medzi prístupovým serverom (Network Access Server) a autentifikačným serverom, špecifikovaný v RFC 2865. Spolupráca RADIUS a EAP je v RFC 3579
  - 802.1X: štandard IEEE popisujúci Port-Based Authentication s využitím EAP správ v Ethernetových rámcoch (EAP over LAN = EAPOL) a protokolu RADIUS

Priebeh 802.1X autentifikácie

- Klient odošle správu EAPOL-Start
- Switch vyžiada od klienta prvotné identifikačné údaje
- EAP odpoveď klienta switch prebalí do RADIUS správy a odošle ju na server
- RADIUS server môže podľa typu okamžite klienta autentifikovať, alebo bude nasledovať niekoľko kôl typu „výzva – odpoveď“
- Po úspešnej autentifikácii RADIUS odošle správu Access-Accept
- Switch na prijatie správy odblokuje port a informuje klienta o úspechu



Príklad konfigurácie pre 802.1x na prepínačoch

```
aaa new-model
aaa authentication dot1x default group radius

! Nasledujúci riadok netreba, ak nechceme dynamicky prideľovať VLAN
aaa authorization network default group radius

radius-server host 1.2.3.4 auth-port 1812 acct-port 1813 key HESLO
dot1x system-auth-control
interface FastEthernet 0/1
 switchport mode access
 dot1x port-control auto
 ! Pre novšie switche namiesto „dot1x port-control auto“ zadať oba:
 ! authentication port-control auto
 ! dot1x pae authenticator
```

- Táto konfigurácia pri vhodnom nastavení RADIUS servera okrem autentifikácie klienta automaticky zaradí port do pridelenej VLAN

802.1X – záverečné poznámky

- Pri 802.1X je možné v konfigurácii definovať viaceré VLAN
  - Guest VLAN – VLAN pre stanice, ktoré nepodporujú 802.1X
  - Restricted VLAN – VLAN pre stanice, ktoré podporujú 802.1X, ale nepodarilo sa im úspešne prihlásiť (tzv. Auth-Fail VLAN)
- 802.1X môže pôsobiť problémy, ak je na port prepínača pripojených viacero staníc
  - Prepínače 2950 a 3550 nevedia autentifikovať individuálne stanice. Port bude otvorený alebo zatvorený pre všetky stanice
  - Prepínače 2960 a 3560 podporujú individuálnu autentifikáciu pre viaceré stanice od verzie IOS 12.2(50)SE (tzv. multiauth mode)
- Pri 802.1X je podstatná (a najzložitejšia) konfigurácia RADIUS servera
  - Pokročilejšie autentifikačné metódy (napr. PEAP alebo EAP-TLS) si vyžadujú vygenerovanie X.509 certifikátu pre server, prípadne aj pre klientov

Ochrana integrity VLAN

Útoky na VTP

- Útoky na VTP sa snažia neautorizovane pozmeniť VLAN databázu prostredníctvom VTP
- VTP (snáď s výnimkou VTPv3) je žiaľ veľmi naivný protokol a Cisco IOS ani neposkytuje veľa možností na jeho ochranu
- Odporúčané kroky:
  - Zabezpečiť VTP doménu netriviálnym heslom
  - Nepripájať stanice k trunk portom
  - Ak je predsa potrebné, aby bol na trunk port pripojený napr. server, ochrániť tento port pomocou MAC ACL
    - Cieľová MAC 01-00-0C-CC-CC-CC
    - Typ 0x2003

VLAN Hopping

- Existuje niekoľko druhov útokov, ktoré sa snažia spôsobiť, aby rámec zo stanice v istej VLAN „pretiekol“ do inej VLAN
  - Nie vždy musí existovať cesta nazad
  - To však nie je nutne problém – napr. pri TCP SYN Flood Attack
- Dva najbežnejšie vektory útoku:
  - Útok na DTP
  - Dvojité značkovanie pri 802.1Q

Útok na DTP

- Útoky na DTP spočívajú v snahe prinútiť dynamický port prejsť do režimu trunk
  - DTP je síce proprietárny, ale nie je ťažké napodobiť jeho paket
- Ochrana je jednoduchá – nepoužívať dynamický režim na portoch a deaktivovať DTP
- DTP je deaktivovaný na portoch, ktoré sú
  - Staticky nastavené ako prístupové
  - Staticky nastavené ako trunkové a DTP je deaktivované príkazom **`switchport nonegotiate`**
  - Nastavené ako smerované porty príkazom **`no switchport`**

Útok na DTP

```
Sw# configure terminal
Sw(config)# int gi0/1
Sw(config-if)# switchport mode access
Sw(config-if)# int gi0/23
Sw(config-if)# switchport mode trunk
Sw(config-if)# end
…
Sw# show int gi0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
…
Sw# show int gi0/23 switchport
Name: Gi0/23
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
```

Útok na DTP

```
Sw# configure terminal
Sw(config)# int gi0/23
Sw(config-if)# switchport mode trunk
Sw(config-if)# switchport nonegotiate
Sw(config-if)# end
…
Sw# show int gi0/23 switchport
Name: Gi0/23
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
```

Útok dvojitým značkovaním

- Existencia natívnej VLAN v 802.1Q umožňuje ďalší druh pomerne sofistikovaného útoku
- Predstavme si najprv túto situáciu:

- Ako bude na Gi0/2 označkovaný rámec, ktorý...
  - ... vošiel cez Gi0/1 bez značky?

Útok dvojitým značkovaním

- Existencia natívnej VLAN v 802.1Q umožňuje ďalší druh pomerne sofistikovaného útoku
- Predstavme si najprv túto situáciu:

- Ako bude na Gi0/2 označkovaný rámec, ktorý...
  - ... vošiel cez Gi0/1 bez značky?
    - → **Značkou 10**
  - ... vošiel cez Gi0/1 so značkou 10?
    - → **Značkou 10**
  - ... vošiel cez Gi0/1 so značkou 15?
    - → **Značkou 15**
  - ... vošiel cez Gi0/1 so značkou 20?
    - → **Bez značky**

Útok dvojitým značkovaním

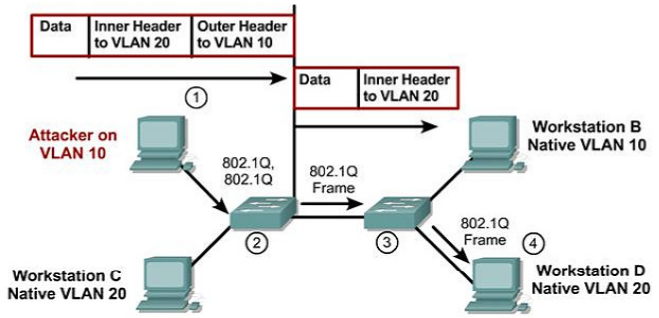
- Hoci to nie je známka správneho dizajnu, v sieti môžu individuálne trunkové prepoje mať navzájom rôzne natívne VLAN
  - VLAN, do ktorej rámec patrí, sa na vstupnom trunkovom porte určí buď podľa hodnoty 802.1Q značky alebo podľa natívnej VLAN portu, ak značka chýba
  - Na výstupnom trunkovom porte sa musí rámec správne označkovať, t.j.:
    - Ak **nepatrí** do VLAN, ktorá je na výstupnom porte natívna, potom rámec musí mať značku. Ak ju doposiaľ nemal, switch ju pridá
    - Ak **patrí** do VLAN, ktorá je na výstupnom porte natívna, potom rámec nemá mať značku. Ak ju mal, switch ju odstráni
- Posledný bod je kľúčový pre útok dvojitým značkovaním

Útok dvojitým značkovaním

- Aj na prístupových portoch sú za určitých okolností akceptované označkované rámce
  - Rámec musí mať značku buď s číslom VLAN 0 (rámec s 802.1p prioritou) alebo s číslom VLAN, do ktorej patrí
  - Novšie switche (2960, 3560) naviac vyžadujú, aby na porte bola definovaná (nejaká) Voice VLAN
- Pre označkovaný rámec, ktorý vošiel prístupovým portom a odchádza trunkom, platia analogické pravidlá:
  - VLAN, do ktorej rámec patrí, sa na vstupnom porte určí podľa nastavenia access VLAN na porte. Ak rámec mal značku, musí mať vhodnú hodnotu (0 alebo číslo access VLAN)
  - Na výstupnom trunkovom porte sa musí rámec správne označkovať:
    - Ak **nepatrí** do VLAN, ktorá je na výstupnom porte natívna, potom rámec musí mať značku. Ak ju doposiaľ nemal, switch ju pridá
    - Ak **patrí** do VLAN, ktorá je na výstupnom porte natívna, potom rámec nemá mať značku. Ak ju mal, switch ju odstráni

Útok dvojitým značkovaním

- Trunk medzi switchmi má natívnu VLAN 10
- Útočník vo VLAN 10 odošle rámec, ktorý má dva tagy
  - Vrchný má VID 10
  - Spodný má VID 20
- Switch akceptuje tento rámec
- Pretože rámec patrí do VLAN 10, ale tá je na trunku natívna, switch odstráni vrchný tag
- Na ďalší switch dorazí rámec s tagom 20
- Nič netušiaci switch ho spracováva vo VLAN 20



Ochrana proti útoku dvojitým značkovaním

- Tento problém vzniká vtedy, ak je útočník v tej istej VLAN, ktorá je zároveň na nejakom trunku natívna
- Spôsoby ochrany sú viaceré
  - Na trunkoch používať rovnakú natívnu VLAN, ktorá nikdy nebude nikde použitá ako access alebo voice VLAN
  - Na switchoch vyšších radov existuje v globálnom konfiguračnom režime príkaz `vlan dot1q tag native` aktivujúci tagovanie všetkých VLAN na trunku vrátane natívnej
  - Používať ISL ☺ (trápne až tristné riešenie)

ACL na prepínačoch

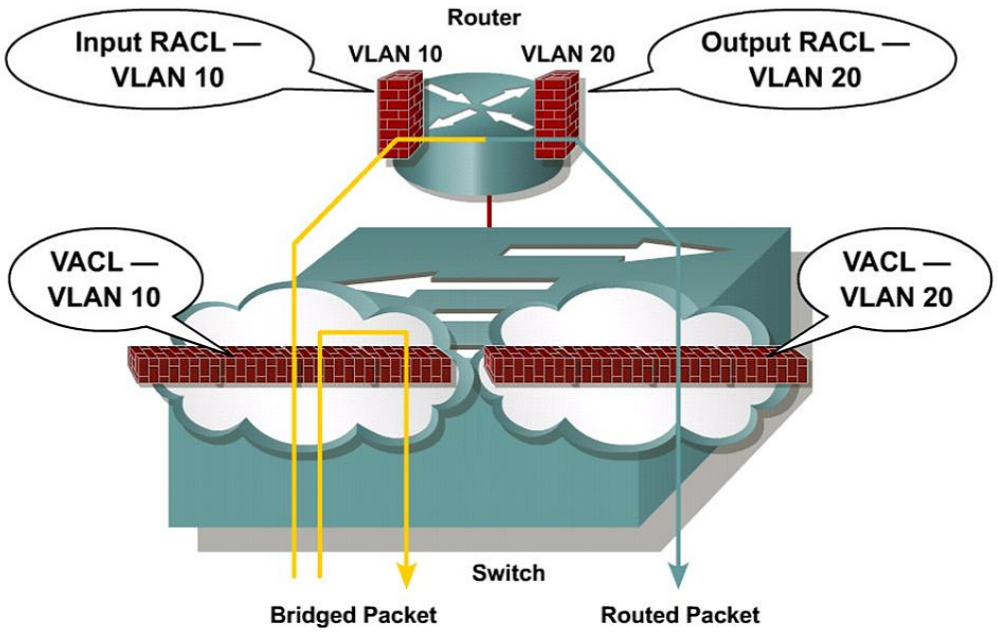
ACL na prepínačoch

- Prepínače Cisco podporujú viaceré druhy ACL
  - Klasické IP ACL, ktoré môžu byť umiestnené na smerovaných alebo prepínaných portoch (Router ACL alebo Port ACL, na prepínaných portoch iba inbound smer)
  - MAC ACL, ktoré môžu byť umiestnené na prepínaných portoch (Port ACL, iba inbound smer)
    - **MAC ACL na novších switchoch platia len na non-IP pakety!**
    - **Nutné konzultovať dokumentáciu!**
  - VLAN ACL (takisto nazývané VLAN map), ktoré sú aplikované na VLAN ako celok (nemajú smer, interne využívajú IP alebo MAC ACL)
- VACL sú podporované na 35x0 a vyšších radoch

ACL na prepínačoch

- ACL na multilayer switchoch sú kompilované a ukladané v TCAM
  - Pretože TCAM má obmedzenú veľkosť a zdieľa sa aj pre iné účely, existujú aj obmedzenia na počet a celkovú veľkosť použitých ACL
  - Pomocou príkazu `sdm prefer TYP` v globálnom konfiguračnom režime je možné zmeniť rozdelenie TCAM medzi jednotlivé aplikácie
  - Veľmi sa odporúča preštudovať podrobnosti o TCAM šablónach v Configuration Guide k danému typu switcha – „Configuring SDM Templates“
  - S SDM šablónami je potrebné manipulovať napr. aj vtedy, ak treba na switchi aktivovať IPv6 alebo Policy-Based Routing. Štandardná šablóna „Desktop“ bežne tieto funkcie nepodporuje

ACL na prepínačoch



VLAN ACL

- VLAN ACL sa hodia na plošnú aplikáciu bezpečnostných pravidiel na zvolenú VLAN
- Základným stavebným prvkom VACL je tzv. **VLAN map**
  - Má veľmi podobnú filozofiu ako route-map
  - Môže mať niekoľko blokov
  - V každom bloku sa definuje nejaký test (odkaz na existujúce ACL) a akcia – forward alebo drop (niekde aj redirect)
  - Na konci platí klasické „deny any“, ale len pre použitý protokol (IP alebo MAC)
- Postup tvorby VACL
  - Vytvoriť ACL
  - Vytvoriť VLAN map s použitím definovaných ACL
  - Aplikovať VLAN map na zvolené VLAN

VLAN ACL

```
ip access-list standard Machine100
 permit 192.0.2.100

ip access-list extended WinServ
 permit tcp any any range 135 139
 permit udp any any range 135 139
 permit tcp any any eq 445
 permit udp any any eq 445
 permit udp any any eq 1900

mac access-list extended IPX
 permit any any 0x8137 0x0
 permit any any lsap 0xFFFF 0x0
 permit any any lsap 0xE0E0 0x0
```

```
vlan access-map V50 10
 match ip address Machine100
 action forward

vlan access-map V50 20
 match ip address WinServ
 match mac address IPX
 action drop

vlan access-map V50 30
 action forward

vlan filter V50 vlan-list 50
```

- Vyhodnocovanie blokov VACL je závislé od poradia
- V bloku VLAN map môže byť match na IP aj na MAC ACL, akceptujú sa ako logické OR
- Viaceré ACL rovnakého typu sa píšu do jedného riadku match za sebou (ako v route-map)

Spoofing a ochrana pred ním

Spoofing

- Spoofing je snaha tváriť sa, že som niekto, kto nie som
- Existuje množstvo druhov podľa použitých protokolov
- My sa pozrieme na tri druhy spoofingu:
  - DHCP Spoofing
  - ARP Spoofing
  - IP Spoofing
- V súčasnosti používané prepínače Catalyst 2950/2960 a vyššie bežne dokážu poskytnúť ochranu proti DHCP spoofingu
  - Proti ARP a IP spoofingu mali ochranu donedávna iba prepínače Catalyst 3550/3560 a vyššie
  - Od verzie IOSu 12.2(50)SE je ochrana proti ARP a IP spoofingu dostupná aj na Catalyst 2960

DHCP Spoofing

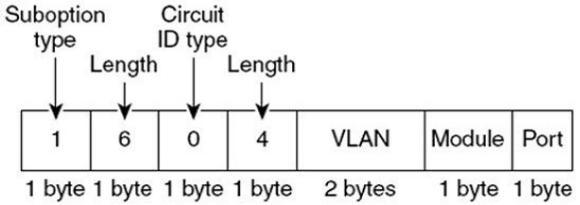
- DHCP spoofing je zapojenie neautorizovaného DHCP servera do siete
  - Môže sa jednať o zlomyseľnú aktivitu
  - Mnohokrát však ide skôr o nedbalosť – vlastný access point, notebook so sieťovým softvérom a podobne
- Zabezpečenie DHCP by malo riešiť tieto nedostatky:
  - Správy od klienta (DISCOVER, REQUEST, DECLINE) sú spravidla posielané ako broadcast, takže ich dostanú všetci v spoločnej VLAN, nielen server
  - Správa od servera (OFFER, ACK) môže byť odoslaná ako broadcast alebo cieľová MAC nemusí byť na prepínači známa, a tak sa opäť môže dostať k nepatričným staniciam
  - Do siete možno bez problémov, častokrát nepozorovane pridávať nové DHCP servery
  - DHCP správy možno podstrkávať alebo vytvárať ich nezmyselné

Ochrana – DHCP snooping

- DHCP Snooping je podpora na prepínačoch Catalyst, ktorá sleduje a riadi tok DHCP správ
- DHCP Snooping rozoznáva dôveryhodné a nedôveryhodné porty
  - Na nedôveryhodných portoch sa nachádzajú stanice
  - Na dôveryhodných portoch alebo za nimi sa nachádzajú DHCP servery
  - Predvolený typ portu je nedôveryhodný
- DHCP Snooping si podľa DHCP komunikácie na nedôveryhodných portoch vytvára databázu
  - V databáze si switch zaznamenáva MAC stanice, pridelenú IP, čas výpožičky, VLAN a port
  - Túto databázu neskôr využíva DHCP Snooping i ďalšie ochranné mechanizmy
- Ak DHCP Snoopingom prejde DHCP správa od klienta, vloží sa do nej DHCP Option-82
  - Informačné pole, ktoré identifikuje, na ktorom switchi a ktorom jeho porte je tento klient pripojený

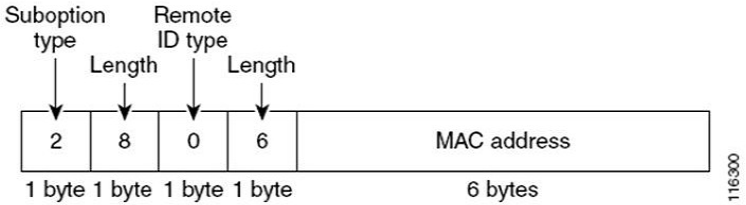
DHCP Option-82

Circuit ID Suboption Frame Format



- DHCP Option-82 má dve časti
  - **Circuit ID** – identifikuje rozhranie, kde je klient pripojený
  - **Remote ID** – identifikuje zariadenie, kde je klient pripojený

Remote ID Suboption Frame Format



Ochrana – DHCP Snooping

- Ako DHCP Snooping **zahadzuje** DHCP správy:
  - Správy od DHCP servera (OFFER, ACK, NAK, LEASEQUERY) prijaté na nedôveryhodnom porte
  - Správy od DHCP klienta, v ktorých sa hodnota poľa chaddr v DHCP správe nezhoduje s MAC adresou odosielateľa
  - Správy RELEASE, DECLINE od DHCP klienta, ktorého MAC adresa v databáze je na inom porte, než ktorým správa prišla
  - Správy prijaté na nedôveryhodnom porte, v ktorých je adresa DHCP Relay agenta iná než 0.0.0.0 alebo v ktorých sa nachádza DHCP Relay Option-82
- Ako DHCP Snooping **preposiela** DHCP správy:
  - Správa od DHCP klienta, ktorú switch nezahodil, bude odoslaná iba cez dôveryhodný port
  - Správa od DHCP servera, ktorú switch nezahodil, bude na základe Option-82 odoslaná len tomu klientovi, pre koho je určená (t.j. aj ak by bol príjemca broadcast alebo neznámy)

Konfigurácia DHCP Snoopingu

- DHCP Snooping sa jednak musí aktivovať na globálnej úrovni, jednak sa musí zapnúť pre zvolenú VLAN
- Všetky porty v danej VLAN budú nedôveryhodné. Porty vrátane trunkov, za ktorými sa nachádzajú DHCP servery, treba označiť ako dôveryhodné
  - Typicky budú teda ako dôveryhodné porty označené všetky trunkové porty na prístupových aj distribučných switchoch, ktorými sú switche navzájom prepojené
  - Porty k jednotlivým klientským staniciam zostanú nedôveryhodné

```
Sw# configure terminal
Sw(config)# ip dhcp snooping
Sw(config)# ip dhcp snooping vlan 1
Sw(config)# interface fa0/24
Sw(config-if)# ip dhcp snooping trust
Sw(config-if)# end
```

Konfigurácia DHCP Snoopingu

```
Sw# 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 default format: vlan-mod-port
   remote-id: 001d.e5be.e380 (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)
-----------------------    -------    ------------    ----------------
FastEthernet0/24           yes        yes             unlimited
  Custom circuit-ids:
```

Konfigurácia DHCP Snoopingu

```
Sw# show ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type            VLAN  Interface
------------------  ----------      ----------  -------------   ----  ---------
00:E0:4C:41:3C:E9   10.0.0.4        84960       dhcp-snooping   1     Fa0/11
00:E0:4C:3B:B7:87   10.0.0.6        85042       dhcp-snooping   1     Fa0/1
Total number of bindings: 2
```

Problémy s Option-82

- Ak je DHCP server v inej VLAN než klienti (a na bráne je teda nastavená služba DHCP Relay), potom všetko bude fungovať
- Ak je DHCP server v tej istej VLAN, vznikne problém
  - DHCP server prestane prideľovať adresy a v debug výpisoch na DHCP serveri sa objaví:

```
Router# debug ip dhcp server packet
*Sep 9 01:59:40: DHCPD: inconsistent relay information.
*Sep 9 01:59:40: DHCPD: relay information option exists, but giaddr is zero
```

  - Dôvod: Switch si do DHCP správ vkladá Option-82, avšak nevypĺňa IP adresu relay agenta, a routeru je to podozrivé
  - Riešenie: dovoliť DHCP serveru akceptovať aj takéto DHCP správy, buď globálne alebo iba na vstupnom rozhraní

```
Router(config)# ip dhcp relay information trust-all ! Globálne…
Router(config)# int fa0/1 ! Iba na routed rozhrania (SVI, no switchport)
Router(config-if)# ip dhcp relay information trusted ! … alebo na rozhraní
```

Problémy s Option-82

- V istých prípadoch sa môže objaviť situácia, že prístupový switch vie vkladať Option-82, ale nevie robiť DHCP Snooping, a preto sa rozhodneme robiť DHCP Snooping na nadradenom switchi
  - Mnohokrát v service-provider prostredí (FTTx, PON, Metro Ethernet...)
  - Klientské zariadenie pre svoju identifikáciu a pre identifikáciu klienta realizuje vkladanie Option-82, nemá však logiku pre DHCP Snooping
- Tu vzniká problém, ako na nadradenom (tzv. agregačnom) switchi nastaviť režim portov pre DHCP Snooping
  - Ak budú untrusted, potom zahodia DHCP správy, ktoré majú vyplnenú adresu relay agenta alebo prítomnú Option-82 (filtrovacie pravidlo 4)
    - Také však budú podľa predpokladu všetky správy od klientov ☹
  - Ak budú trusted, nebudú z DHCP správ napĺňať databázu (nie sú pre DHCP snooping zaujímavé)
    - To zasa nerieši našu snahu zabezpečiť DHCP komunikáciu ☹

Problémy s Option-82

- Uvedený problém sa rieši pridaním príkazu na agregačný switch buď globálne alebo len na vybranom nedôveryhodnom rozhraní:

```
AggSw(config)# ip dhcp snooping option allow-untrusted ! Globálne
AggSw(config)# int fa0/1
AggSw(config-if)# ip dhcp snooping option allow-untrusted ! Len rozhranie
```

- Samozrejme, všetky problémy s Option-82 sa dajú odstrániť aj tým, že na prístupovom switchi zakážeme jej pridávanie:

```
Sw(config)# no ip dhcp snooping information option
```

- Toto riešenie je však trápne a ochudobňuje DHCP Snooping o podstatnú časť jeho schopností

Ochrana proti DHCP DoS

- DHCP Snooping doposiaľ dokázal sieť ochrániť pred nepovolanými DHCP servermi a príliš zvedavými DHCP klientmi
- Ak však príde klient, ktorý rad zaradom vystrieda rôzne MAC a na každú si vyžiada novú IP, môže vyčerpať voľné IP adresy na DHCP serveri
- Tento problém rieši DHCP Snooping Limit Rate
  - Na porte je možné definovať maximálny počet prijatých DHCP správ za sekundu
  - Ak sa tento počet prekročí, port sa deaktivuje (err-disabled)

```
Sw(config)# int fa0/1
Sw(config-if)# ip dhcp snooping limit rate 5
```

IP Spoofing

- IP Spoofing je ukradnutie IP adresy inej stanice
- DHCP Snooping môže výrazne pomôcť
  - Vytvára si databázu MAC a IP adries podľa DHCP správ
  - Táto databáza sa dá využiť na kontrolu, či sa na porte neobjavila stanica s inou IP adresou
- Ochranou proti IP Spoofingu je IP Source Guard
  - IP adresu stanici pridelí DHCP server. Vďaka DHCP Snoopingu sa MAC adresa stanice a pridelená IP zaznačí do databázy
  - IP Source Guard kontroluje, či IP adresa odosielateľa na porte, prípadne dokonca MAC adresa odosielateľa, zodpovedá záznamu v databáze

Konfigurácia IP Source Guard

- Predpokladom pre konfiguráciu IP Source Guard je funkčný DHCP Snooping
- Samotný IP Source Guard s kontrolou IP adresy odosielateľa sa konfiguruje jednoducho:

```
Sw(config)# int fa0/1
Sw(config-if)# ip verify source
```

- IP Source Guard s kontrolou IP aj MAC adresy odosielateľa sa konfiguruje podobne – na kontrolu MAC adresy sa využíva mechanizmus Port Security:

```
Sw(config)# int fa0/1
Sw(config-if)# switchport port-security
Sw(config-if)# ip verify source port-security
```

- Vloženie statického mapovania v prípade potreby:

```
Sw(config)# ip source binding 0200.1122.3344 vlan 1 10.0.0.10 int fa0/1
```

ARP Spoofing

- ARP Spoofing je odosielanie nevyžiadaných (gratuitous) ARP správ, v ktorých mapujeme zvolenú IP na inú než skutočnú MAC adresu
  - Denial of Service: mapovaním IP na neexistujúcu MAC
  - Man-In-The-Middle: mapovaním cudzej IP na moju MAC
- Aj tu môže pomôcť databáza DHCP Snoopingu
- Mechanizmus ochrany proti ARP Spoofingu sa volá Dynamic ARP Inspection (DAI)
  - Každá ARP správa obsahuje o. i. polia
    - Source MAC a Source IP
    - Target MAC a Target IP
  - DAI kontroluje, či si tieto údaje v ARP správach podľa databázy z DHCP Snoopingu navzájom zodpovedajú
  - DAI môže dodatočne kontrolovať aj správnosť ďalších údajov

Dynamic ARP Inspection

- DAI rozdeľuje porty na dôveryhodné a nedôveryhodné
  - Na nedôveryhodných portoch switch kontroluje obsah prichádzajúcich ARP správ oproti DHCP Snooping databáze
  - Nevyhovujúce ARP správy zahodí
  - Predvolený typ je nedôveryhodný
- Konfigurácia DAI predpokladá funkčný DHCP Snooping

```
Sw(config)# ip arp inspection vlan 1
Sw(config)# int fa0/1
Sw(config-if)# ip arp inspection trust
```

- Typicky, porty k iným switchom a k routerom budú dôveryhodné, porty k staniciam budú nedôveryhodné

Dynamic ARP Inspection

- Dodatočnou možnosťou DAI je validácia ARP správ

```
Sw(config)# ip arp inspection validate { [src-mac] [dst-mac]
                                         [ip [allow-zeros] ] }
```

- Možnosti:
  - **src-mac**: Zdrojová MAC rámca sa musí zhodovať so zdrojovou MAC v tele ARP správy. Kontrolujú sa queries aj replies
  - **dst-mac**: Cieľová MAC rámca sa musí zhodovať s cieľovou MAC v tele ARP správy. Kontrolujú sa iba replies
  - **ip**: IP adresy v tele ARP správy musia byť iné ako 0.0.0.0, 255.255.255.255 a nesmú byť multicastové. Kontrolujú sa queries aj replies, cieľová IP adresa sa kontroluje iba v replies
  - **allow-zeros**: Pri kontrole „ip“ sa povoľuje, aby zdrojová IP mohla byť 0.0.0.0

Záverečné poznámky

- DAI dovoľuje definovať maximálny počet ARP správ za sekundu
  - Štandardne je 15 vstupujúcich správ za sekundu na nedôveryhodnom porte, dôveryhodný port je bez obmedzení
  - Pri prekročení počtu správ bude port deaktivovaný (err-disabled)
- Ak nie je použité DHCP, je možné definovať tzv. ARP ACL, v ktorom staticky vymenujeme IP a ich MAC, a toto ACL použiť v DAI

```
Switch(config)# arp access-list ARP-V1
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 0201.0203.0405
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter ARP-V1 vlan 1
```


CISCO