SMĚROVANÉ A PŘEPÍNANÉ SÍTĚ
SEMESTRÁLNÍ PROJEKT

DHCP
snooping

Petr Gurecký
gur020

15. května 2006 LS 2005/2006

Obsah

1 Cíl projektu

Cílem projektu bylo prakticky ukázat fungování DHCP snoopingu spuštěném na switchi. Tedy zabránit tomu, aby nedošlo k narušení přidělování IP adres stanicím díky tomu, že byl do sítě připojen druhý DHCP server, označený jako falešný.

2 Jak DHCP snooping funguje

V sítích, ve kterých jsou stanicím IP adresy přidělovány dynamicky prostřednictvím DHCP serveru, existuje nebezpečí, že se zde připojí útočník takovým způsobem, že bude představovat DHCP server a bude přidělovat stanicím jiné IP adresy. Taktéž může v DHCP odpovědi klientovi poslat svou IP adresu jako adresu výchozí brány. Potom bude veškerý provoz od klienta směřovaný ven ze sítě procházet přes útočníkův počítač. Jde tedy o „Man-in-the-Middle“ útok, protože útočník pak může pakety přeposílat na správnou cílovou adresu, ale přitom může prozkoumat každý paket, který takto zachytil.

Některé switche Cisco Catalyst nabízejí možnost využití DHCP snoopingu, abychom takovýmto útokům zabránili. Je-li DHCP snooping anktivován, jsou porty switche rozděleny na důvěryhodné a nedůvěryhodné. Pravé DHCP servery jsou připojeny na porty označené jako důvěryhodné, zatímco všechny stanice jsou připojeny na nedůvěryhodné porty.

Switch pak zachytává všechny DHCP požadavky, které přicházejí na nedůvěryhodné porty, předtím, než je rozesílá po celém VLANu[1]. Všechny DHCP odpovědi, které přicházejí na nedůvěryhodné porty, jsou zahozeny, protože zjevně musí pocházet z falešného DHCP serveru.

DHCP snooping také udržuje informace o vazbách, kdy klient obdržel „pravou“ DHCP odpověď. Jde o tabulku vazeb, která obsahuje MAC adresu, IP adresu, čas vypršení platnosti záznamu, čas přidání záznamu, číslo VLANu a jméno rozhraní, které je označeno jako nedůvěryhodné. Tabulka nenese žádné informace ohledně stanic připojených na důvěryhodná rozhraní.

3 Konfigurace DHCP snoopingu na switchi

Konfigurací DHCP snoopingu na switchi říkáme switchi, že má rozlišovat mezi důvěryhodnými a nedůvěryhodnými rozhraními. Chceme-li DHCP snooping provozovat na VLANu, musíme jej nejprve zapnout globálně. Můžeme tak učinit nezávisle na jiných DHCP službách.

Tabulka 1 vyjadřuje implicitní nastavení pro DHCP snooping.

Volba	Implicitní hodnota/stav
DHCP snooping	Disabled
DHCP snooping information option	Enabled
DHCP snooping limit rate	Infinite (žádná omezení)
DHCP snooping trust	Untrusted
DHCP snooping vlan	Disabled

Tabulka 1: Implicitní hodnoty pro DHCP snooping

Vysvětlení některých voleb:

- DHCP snooping information option – Pokud je DHCP požadavek zachycen na nedůvěryhodném portu, switch do něj přidá svou MAC adresu a identifikaci portu. Požadavek je pak přeposlán na pravý DHCP server. Podle RFC 3046[2] je číslo této volby 82.
- DHCP snooping limit rate – Limit určující, kolik DHCP paketů za sekundu může daným rozhraním projít. To se týká DHCP dotazů i odpovědí.

[1] DHCP požadavky vysílají stanice jako multicast.
[2] Request for Comments

- DHCP snooping trust – Označení daného portu jako důvěryhodného.
- DHCP snooping vlan – Určení VLANu, na kterém bude DHCP snooping spuštěn.

3.1 Aktivace DHCP snoopingu

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

Tento příkaz globálně zapne DHCP snooping. Pro vypnutí stačí předřadit klíčové slovo „no“.

```
Switch(config)# ip dhcp snooping vlan (číslo)
```

Zapne DHCP snooping na VLANu s příslušným číslem. Lze zadat také dvě čísla, která pak znamenají dolní a horní mez rozmezí všech VLANů.

```
Switch(config)# ip dhcp snooping information option
```

Zapne DHCP volbu č. 82 (viz výše).

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

Nastaví příslušné rozhraní jako důvěryhodné (připojené k pravému DHCP serveru).

```
Switch(config-if)# ip dhcp snooping limit rate (číslo)
```

Nastaví kolik DHCP paketů může rozhraní přijmout za sekundu (pps). Obvykle se neudává hodnota větší než 100 pps. Obyčejně se limit udává na nedůvěryhodných rozhraních. Chceme-li jej použít na rozhraní důvěryhodné, musíme vzít na vědomí, že přes tato rozhraní prochází veškerý DHCP provoz ve switchi, a proto bychom měli použít větší hodnotu limitu.

```
Switch# show ip dhcp snooping
```

Zobrazí aktuální konfiguraci DHCP snoopingu na daném switchi.

Příklad konfigurace a ověření nastavení na VLANech s čísly 10 až 100:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 100
Switch(config)# ip dhcp snooping information option
Switch(config)# interface FastEthernet2/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# exit
Switch(config)# exit
Switch# show ip dhcp snooping
DHCP Snooping is configured on the following VLANs:
    10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface           Trusted        Rate limit (pps)
---------           -------        ----------------
FastEthernet2/1     yes            100
FastEthernet2/2     yes            none
FastEthernet3/1     no             20
Switch#
```

4 Zobrazení informací o DHCP snoopingu

Je možné si zobrazit tabulku vazeb DHCP snoopingu a také konfiguraci kteréhokoliv portu na daném switchi.

4.1 Zobrazení vazební tabulky

Tabulka pro DHCP snooping obsahuje vazební informace, které se týkají nedůvěryhodných portů.

Příklad zobrazení vazebních informací DHCP snoopingu na switchi:

```
Switch# show ip dhcp snooping binding

MacAddress      IP Address    Lease (seconds)    Type     VLAN   Interface
-----------     -----------   ----------------   -----    -----  ------------
0000.0100.0201  10.0.0.1      1600               dynamic  100    FastEthernet2/1
```

Pole	Popis
Mac Address	hardwarová MAC adresa klienta
IP Address	klientova IP adresa přidělená DHCP serverem
Lease (seconds)	doba platnosti IP adresy
Type	typ vazby; dynamicky/staticky
VLAN	číslo VLANu na klientském rozhraní
Interface	rozhraní připojené k DHCP klientovi

Tabulka 2: Popis hodnot polí z výpisu příkazu `show ip dhcp snooping binding`

4.2 Zobrazení konfigurace

Následující příklad ukazuje, jak zobrazit informace o konfiguraci DHCP snoopingu na switchi.

```
Switch# show ip dhcp snooping
DHCP Snooping is configured on the following VLANs:
    10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface           Trusted        Rate limit (pps)
---------           -------        ----------------
FastEthernet2/1     yes            100
FastEthernet2/2     yes            none
FastEthernet3/1     no             20
Switch#
```

Z výpisu můžeme vyčíst následující informace:

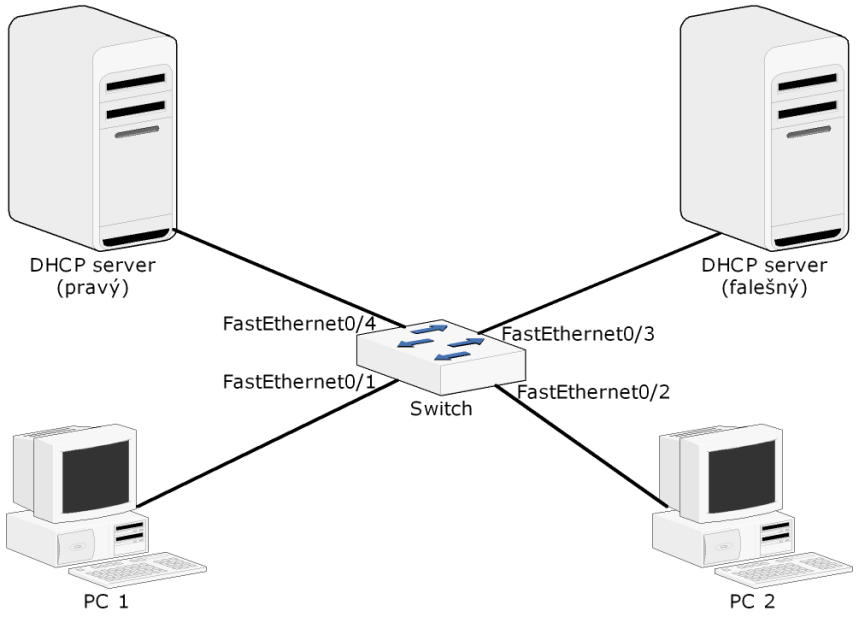
- DHCP snooping byl aktivován na VLANech č. 10, 30 až 40, 100, 200 až 220.
- `Insertion of option 82 information is enabled.` – Zachycené DHCP požadavky na nedůvěryhodných portech budou přeposlány na pravý DHCP server s tím, že do nich switch přidá svou MAC adresu a identifikaci portu.
- Rozhraní `FastEthernet2/1` a `FastEthernet2/2` jsou nastavena jako důvěryhodná, tj. jsou připojena k DHCP serveru. Navíc na rozhraní `FastEthernet2/1` je nastaven limit, že za sekundu může projít maximálně 100 DHCP paketů. Rozhraní `FastEthernet3/1` není sice nastaveno jako důvěryhodné, ale je mu přidělen limit, že za sekundu zdu může projít maximálně 20 DHCP paketů.

5 Praktické zapojení

V praktickém zapojení šlo o to, ukázat, jak účinný bude DHCP snooping spuštěný na switchi. Zapojení bylo provedeno tak, aby v jednu chvíli byly aktivní dva DHCP servery, oba nabízející připojeným stanicím své adresy. Každý z DHCP serverů měl nastaven jiný adresní rozsah, aby na stanicích bylo možné rozeznat, ze kterého DHCP serveru, má stanice přiřazenou adresu. Schéma zapojení je znázorněno na obrázku 1.

Použitý hardware:

- Switch Cisco Catalyst 2950
- 2 × pracovní stanice s Linux Debian 2.4
- 2 × DHCP server spuštěný na Linux Debian 2.4



Obrázek 1: Schéma praktického zapojení

5.1 Konfigurační soubory

Pravý i falešný DHCP server byly nakonfigurovány téměř stejně. Lišily se ve jméně a především v rozsahu IP adres, které přidělovaly klientům, aby bylo vůbec možné testovat chování celé sítě. Pravý server (na portu FastEthernet0/4) přiděloval adresy z rozsahu 192.168.1.10 – 192.168.1.20 a falešný (na portu FastEthernet0/3) z rozsahu 192.168.1.110 – 192.168.1.120.

Konfigurace pravého DHCP serveru (soubor dhcpd.conf):

```
option domain-name "pravy_dhcp";
option routers 192.168.1.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;

default-lease-time 3600;
```

```
max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.10 192.168.1.20;
}
```

Konfigurace falešného DHCP serveru (soubor dhcpd.conf):

```
option domain-name "falesny_dhcp";
option routers 192.168.1.5;
option subnet-mask 255.255.255.0;

default-lease-time 3600;
max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.120;
}
```

Konfigurace samotného DHCP snoopingu na switchi spočívala v jeho globálním zapnutí a nastavení důvěryhodného portu, na kterém byl připojen pravý DHCP server.

Výtah z konfiguračního souboru switche (zobrazeny jen ručně nastavené položky):

```
ip dhcp snooping
ip dhcp snooping vlan 1

interface FastEthernet0/4
 ip dhcp snooping trust
```

Fungování přidělování IP adres DHCP serverem si můžeme demonstrovat přímo na výpisu switche v debug režimu (zapnutý příkazem `debug ip dhcp snooping`):

```
00:20:29: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthe
  rnet0/1)
00:20:29: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER
00:20:29: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
00:20:29: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF,
   packet is flooded to ingress VLAN: (1)
00:20:29: DHCP_SNOOPING_SW: bridge packet send packet to port: FastEthernet0/4.
00:20:29: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthe
  rnet0/4)
00:20:29: DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER
00:20:29: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0
  /1.
00:20:29: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthe
  rnet0/1)
00:20:29: DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST
00:20:29: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
00:20:29: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF,
   packet is flooded to ingress VLAN: (1)
00:20:29: DHCP_SNOOPING_SW: bridge packet send packet to port: FastEthernet0/4.
00:20:29: DHCP_SNOOPING: received new DHCP packet from input interface (FastEth
  ernet0/4)
00:20:29: DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK
00:20:29: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet
  0/1.
```

DHCP rozšiřuje BOOTP[3] protokol, se kterým je zpětně kompatibilní. Klient vysílá do sítě multicast UDP požadavek DHCPDISCOVER. Server zachytí požadavky a zašle zprávu DHCPOFFER (opět multicast). Klient si vybere ze všech odpovědí tu nejvhodnější a pošle DHCPREQUEST. Server, který klient oslovuje, vše buď potvrdí (DHCPACK), nebo ne (DHCPNAK). Klient si to může ještě rozmyslet (DHCPDECLINE). Po vypršení lhůty (nebo pokud klient skončí před lhůtou a pošle DHCPRELEASE) se adresa může poskytnout jinému zájemci.

5.2 Zhodnocení praktického zapojení

Při spuštění obou DHCP serverů, aniž by byl na switchi aktivován DHCP snooping, docházelo na stanicích k periodickému střídání IP adres. Příkazem pump získá stanice IP adresu z DHCP serveru. Po opakovaném použití tohoto příkazu se adresa stále měnila. Tedy jedna stanice stále střídala IP adresy 192.168.1.10 a 192.168.1.100 a druhá 192.168.1.11 a 192.168.1.101.

Po zapnutí DHCP snoopingu již obě stanice získaly správnou IP adresu, tedy z pravého DHCP serveru, který se nacházel na důvěryhodném portu switche (v tomto případě FastEthernet0/4).

Ve výpisu z debug-režimu switche se neobjevila žádná DHCP zpráva z rozhraní FastEthernet0/3, což naznačuje, že switch všechny DHCP požadavky směřoval na rozhraní (FastEthernet0/4), kde se nacházel pravý DHCP server a DHCP odpovědi přicházely taktéž z tohoto rozhraní.

[3]Bootstrap Protocol

Reference

[1] <http://www.cisco.com/>

[2] <http://www.cisco.cz/>

[3] Zapletal, Lukáš: *Linux jako DHCP server* [online], <http://www.root.cz/clanky/linux-jako-dhcp-server/>

[4] RFC 3046 (RFC3046) [online], <http://www.faqs.org/rfcs/rfc3046.html>