



Průzkum možností generátoru a vyhodnocovače provozu v Cisci
IOS Pagent Image

Vladimír Jarotek, Filip Břuska

Abstrakt: Cílem tohoto projektu je prozkoumání možností generátoru a vyhodnocovače provozu v Cisco IOS Pagent Image.

Klíčová slova: Cisco, IOS, Pagent, TGN, Router

1	Cisco IOS.....	2
2	Pagent.....	2
3	Pagent nástroje.....	2
3.1	Topologie.....	3

1 Cisco IOS

IOS je zkratka pro **Internetwork Operating System**, což je operační systém, který používá většina switchů a routerů firmy Cisco. IOS je propracovaný a na míru provedený systém, nabízí velké množství možností pro konfiguraci, je to vlastně balíček směrovacích, přepínacích, propojovacích a telekomunikačních funkcí pevně integrovan do multitaskingového operačního systému. Celý IOS je uložen v jednom image souboru s příponou *bin*.

2 Pagent

Pagent je množina testovacích nástrojů založených na CISCO IOS vytvořený CISCEm. Testovací nástroje jsou včleněny do speciálního IOS Pagent image.

Tyto nástroje nejsou schopné provádět testy na 2. vrstvě (spojové) ISO modelu. Nemohou ovlivňovat kontrolní součet rámců, injektovat hardwarové chyby atd.

Dále je zde omezení na rychlost vysílání a přijímání paketů, záleží na CPU. Pagent programy jsou používány na testování 3. vrstvy a výše. Emulace routerovacích protokolů, multicastu, TCP sessions, http sessions.

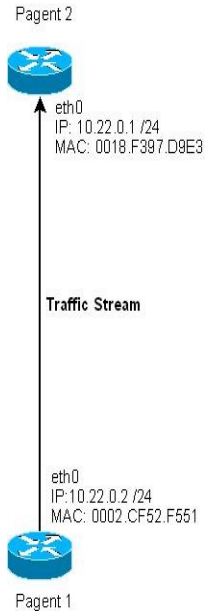
3 Pagent nástroje

- TGN (Traffic Generator)
Se používá k definování a odesílání paketů jakékoliv kombinace podporovaných interfaců na routeru. Program má předdefinované šablony pro podporu definování specifických typů paketů. Délka paketů a data v hlavičce mohou být nastaveny na konstantní, inkrementální, nebo náhodné hodnoty. Definice paketů mohou být importovány z PKTS programového zachycovacího bufferu.
- PKTS (Packet Count and Capture)
Může zachytit a zobrazit příchozí nebo odchozí pakety z jakékoliv kombinace interfaců na routeru. PKTS podporuje vytvoření filterů, které dovolují selektivní počítání, zachycování nebo zobrazování.
- RVT a CVT (Router Verified Traffic) a (Control Verified Traffic)
Jsou používány společně pro testování bridgů a routerů. CVT může automaticky vytvořit několik traffic streamů mezi několika interfaci Pagent routerů pro několik různých LAN síťových protokolů.
- PMOD
Dovoluje Pagent routerům aby byly vloženy do testované sítě, takže test provozu bude procházet skrze router a bude možno pakety provozu modifikovat. Tento nástroj může zahazovat, upravovat, zpožd'ovat nebo vkládat časovou značku do paketů.
- TCP session emulator
Je nástroj sloužící pro vytvoření TCP provozu. Nástroj poskytuje konfigurovatelné vlastnosti, které umožňují uživateli emulovat různé TCP aplikační dialogy mezi TCP klientem a TCP serverem.
- HTTP session emulator
Nástroj pro vytvoření http provozu. Emuluje několik http klientů otevirajících http spojení k http serveru. Umožňuje vytvářet všechny typy http spojení včetně všech typů http požadavků a http odpovědí.
- FTP session emulator
Je TCP aplikace pro přenášení souborů. FTPSE klient emulátor vytváří skutečný ftp provoz a emuluje klientské sessions, které musí komunikovat se skutečným FTP serverem. Současně podporuje FTPSE pouze klientskou stranu v pasivním modu.

- LNE (Large Network Emulator)
Zahrnuje 6 programů pro podporu 6ti routerovacích protokolů: BGP, OSPF, ISIS, EIGRP, IGRP a RIP

3.1 TGN

Následující konfigurační příkazy vytvoří dopravní proud z routeru PAGENT1. Router PAGENT2 zastává roli ARP respondera poskytujícího MAC adresy pro ARP požadavky.



Nastavení routeru (Pagent 2) jako ARP responder

```
#interface fastethernet 0/0
#ip address 10.22.0.1 255.255.255.0
#no shutdown

#tgn                               //skočí do TGN konfiguračního modu
fastethernet 0/0                   //volba interfacu
add arp responder
ip-address 10.22.0.2 to 10.22.0.253
mac-address 00B0.D086.BBF7        //nastavení MAC adresy interfacu fe 0/0
```

Nastavení routeru (Pagent 1) pro vytvoření 64 bytového toku

```
#interface fastethernet 0/0
#ip address 10.21.0.254 255.255.255.0
#mac-address 000C.299C.B333
#no shutdown

#tgn
fastethernet 0/0
add ip
name "PAGENT1-to-PAGENT2-64byte"
rate 70
length 64
l2-encapsulation arpa
l2-dest-addr 00B0.D086.BBF7        //adresa PAGENTu 2
l2-src-addr 000C.299C.B333        //adresa PAGENTu 1
l2-protocol 0x0800
l3-tos random 0x00 to 0x07
l3-dest-addr random 10.22.0.2 to 10.22.0.253
l3-src-addr random 10.21.0.2 to 10.21.0.253
```

Nastavení routeru (Pagent 1) pro vytvoření 570 bytového toku

```
#tgn
fastethernet 0/0
add ip
name "PAGENT1-to-PAGENT2-570byte"
rate 40
length 570
l2-encapsulation arpa
l2-dest-addr 00B0.D086.BBF7 //adresa PAGENTu 2
l2-src-addr 000C.299C.B333 //adresa PAGENTu 1
l2-protocol 0x0800
l3-tos random 0x00 to 0x07
l3-dest-addr random 10.22.0.2 to 10.22.0.253
l3-src-addr random 10.21.0.2 to 10.21.0.253
```

Nastavení routeru (Pagent 1) pro vytvoření 1518 bytového toku

```
#tgn
fastethernet 0/0
add ip
name "PAGENT1-to-PAGENT2-1518byte"
rate 10
length 1518
l2-encapsulation arpa
l2-dest-addr 00B0.D086.BBF7 //adresa PAGENTu 2
l2-src-addr 000C.299C.B333 //adresa PAGENTu 1
l2-protocol 0x0800
l3-tos random 0x00 to 0x07
l3-dest-addr random 10.22.0.2 to 10.22.0.253
l3-src-addr random 10.21.0.2 to 10.21.0.253
```

```
PAGENT1(TGN:ON,Fa0/0:8/8)# start //spuštění generování provozu
```

```
PAGENT1(TGN:ON,Et0/0:4/4)#show rate //ukáže výsledky po vygenerování provozu
```

ts#	template	state	repeat	interval/rate	interval/rate	packets_sent
2	IP	on	1	70 pps	3.216	134071
3	IP	on	1	40 pps	3.216	134068
4	IP	on	1	10 pps	3.216	134067

```
Totals for Ethernet 0/0 9.649 402206
```

Ukázková konfigurace pro využití PAGENTu jako generátoru BGP paketů

BGP konfigurační proces na Pagent routeru:

```
#interface 0/0
#ip address 173.200.14.10 255.255.255.0
#router bgp 100
#network 173.200.0.0
#neighbor 173.200.14.101 remote-as 101
```

Následující příkazy jsou:

- Přiřazení IP adres k BGP procesu
- Identifikování IP adresy cílového routeru
- Přiřazení čísla autonomního systému k BGP procesu
- Identifikování čísla autonomního systému vzdáleného nebo cílového routeru
- Přidání skupiny sítí mezi inzerované

Defaultně, skupina inzeruje 100 sítí nebo cest do sítí. Náš příklad: Hodnota bude snížena na 10 sítí. Níže jsou příkazy používané k vytvoření a konfigurování tohoto BGP procesu:

```
#lne bgp
(BGP:OFF,Et0:none)#ethernet1
(BGP:OFF,Et1:none)#add bgp
(BGP:OFF,Et1:1)#ip source 173.200.14.101
(BGP:OFF,Et1:1)#ip destination 173.200.14.10
(BGP:OFF,Et1:1)#autonomous-system 101
(BGP:OFF,Et1:1)#remote-as 100
(BGP:OFF,Et1:1)#add group
(BGP:OFF,Et1:1-Grp1)#advert 10
```

Výsledná konfigurace:

```
(BGP:OFF,Et1:1-Grp1)#sh
BGP Process 1 of 1 with 1 group(s) advertising 10 networks
name ""
on
datalink lne-defined
ip source 173.200.14.101
ip destination 173.200.14.10
autonomous-system 101
remote-as 100
!
random-as-range 200 to 65535
disallow duplicate-as on
disallow own-as on
!
router-flap off
router-flap duration on 600 to 1200 seconds
router-flap duration off 300 to 600 seconds
verbose on
flapping on
header-definition off
!
group 1
group name ""
advertise 10 networks
network start 34.1.1.0
network subnetmask 255.255.255.0
network per-nlri 10
next-hop ip-source
origin EGP Flap off
AS_SEQ 3 to 7 Flap off
AS_SET 0 to 3 Flap off
MED 1000 to 3000 Flap off
Pref 10000 to 100000 Flap off
withdraw Flap off
define AS_SEQ off
define AS_SET off
```

```
atomic-aggregate off
aggregator off
community attribute off
originator-id off
cluster-list attribute off
freeform attribute off
```

Když spustím LNE BGP, tak se zobrazí:

```
(BGP:OFF,Etl:1-Grp1)#start
- ON: BGP Processes Started.
```

```
(BGP:ON,Etl:1-Grp1)#
BGP 173.200.14.101: Starting process #1 on Ethernet1.
BGP 173.200.14.101: Send Arp Request.
BGP 173.200.14.101: Send TCP SYN.
BGP 173.200.14.101: Send TCP SYN.
BGP 173.200.14.101: Send BGP Open.
BGP 173.200.14.101: Recv BGP Open from 173.200.14.10
BGP 173.200.14.101: Send Group 1 Updates.
BGP 173.200.14.101: Recv BGP Update from 173.200.14.10
```

Pokud vložíte příkaz *show ip route bgp* na konzoli během testování, tak byste měli vidět 10 cest nebo podsítí, které byly inzerovány pomocí LNE BGP procesu.

Ukázka:

```
#show ip route bgp
34.0.0.0/24 is subnetted, 10 subnets
B 34.1.3.0 [20/2311] via 173.200.14.101, 00:00:03
B 34.1.2.0 [20/2311] via 173.200.14.101, 00:00:03
B 34.1.1.0 [20/2311] via 173.200.14.101, 00:00:03
B 34.1.7.0 [20/2311] via 173.200.14.101, 00:00:03
B 34.1.6.0 [20/2311] via 173.200.14.101, 00:00:03
B 34.1.5.0 [20/2311] via 173.200.14.101, 00:00:03
B 34.1.4.0 [20/2311] via 173.200.14.101, 00:00:03
B 34.1.10.0 [20/2311] via 173.200.14.101, 00:00:03
B 34.1.9.0 [20/2311] via 173.200.14.101, 00:00:04
B 34.1.8.0 [20/2311] via 173.200.14.101, 00:00:04
```

Zastavení BGP:

```
(BGP:ON,Etl:1-Grp1)#stop
--- Please wait until all BGP TCP circuits are closed.
BGP 173.200.14.101: Send TCP FIN #1.
BGP 173.200.14.101: Recv TCP Close from 173.200.14.10
- OFF: BGP Processes Stopped.
(BGP:OFF,Etl:1-Grp1)#
```