Směrování mezi autonomními systémy

eBGP pro IPv4

BGP je exterior směrovací protokol a zatímco u OSPF určujeme číslo procesu (které je lokální a míří směrem dovnitř routeru), u BGP určujeme číslo ASN. Zde budeme používat čísla z testovacího rozsahu.

Pro RouterID platí u BGP totéž co u OSPF – buď ho stanovíme ručně ve směrovacím procesu, nebo se použije nejvyšší adresa nasazená na některém loopbacku, nebo nejvyšší adresa nasazená na některém běžném rozhraní (priorita podle tohoto pořadí).

Pokud se použije adresa loopbacku, její role je identifikace daného routeru vzhledem k ostatním BGP peerům, ale ve skutečnosti se dá využít i pro posílání BGP komunikace (nastavení je mimo rámec tohoto předmětu). Výhodou je, že loopback IP adresa je vždy aktivní a funkční, i když některé z fyzických rozhraní přestane fungovat, komunikace je tedy stabilnější.

Předpokládejme tedy, že RouterID řešíme pomocí loopbacku, který už máme vytvořený a nastavený. Nejdřív ve směrovacím procesu (určeném číslem ASN) definujeme sousedy a jejich ASN:

```
router bgp 64500
       neighbor 12.0.0.2 remote-as 64501
       …
```

Postupně pro všechny BGP sousedy (nemusejí nutně mít adresu z téže podsítě). U každého uvádíme ASN, které logicky bude jiné než to, které jsme napsali k směrovacímu procesu (jsme zatím u eBGP, sousedi jsou z jiných autonomních systémů).

Sousedství si můžeme ověřit příkazem

```
sh ip bgp neighbors
```

Vrátíme se do směrovacího procesu a použijeme příkaz network. Ten má trochu jiný význam než u vnitřních protokolů – u vnitřího protokolu se zadaná síť porovná s adresami na připojených rozhraních a síť za rozhraním je propagována sousedům. U BGP se zadaná síť (včetně masky) porovnává s obsahem směrovací tabulky, a pokud je tam nalezena, bude propagována sousedům. Z toho vyplývá, že propagovat můžeme i takovou síť, která není přímo připojená (může být do směrovací tabulky umístěna jiným směrovacím protokolem). Syntaxe:

```
network 12.0.0.0
network 12.128.0.0 mask 255.255.0.0
```

Masku uvádíme, pokud neodpovídá třídě.

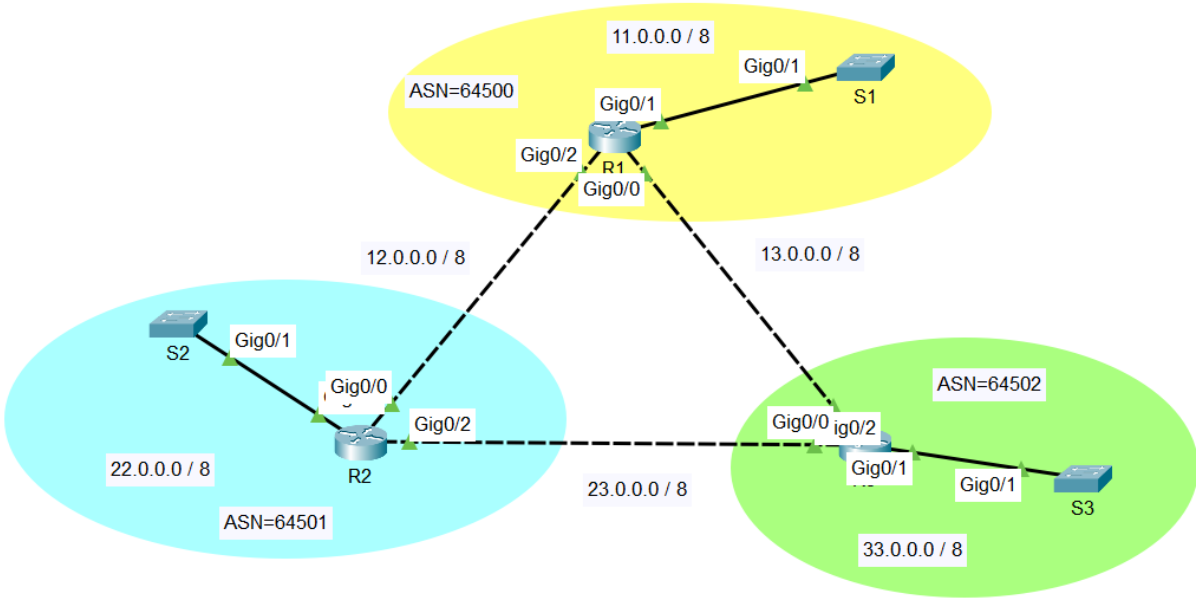
Shrňme si show příkazy pro protokol BGP:

```
sh run
sh ip protocol
sh ip bgp           ; zobrazí BGP tabulku, ze které se určí položky do směrovací tabulky
sh ip bgp neighbors
sh ip bgp summary
sh ip route
debug ip bgp
no debug ip bgp
```

Protokol BGP má poměrně dlouhou dobu konvergence, do směrovacích tabulek se změny promítají někdy až po několika minutách.

Příklad

Na následujícím obrázku je (poněkud nepravděpodobná) síť se třemi autonomními systémy, ke stažení je předpřipravený soubor (na webu ten první na eBGP). Na všech rozhraních jsou nasazeny IP adresy, na routeru R2 je provedena celá základní konfigurace eBGP (peers a sítě), na routeru R1 je zatím částečná konfigurace (zjistěte, co chybí, dokončete), na routeru R3 je nutno nakonfigurovat BGP. Nezapomeňte ověřit, jestli existují loopbacky se správnými adresami.



Pro zjednodušení budeme chtít, aby všechny přítomné sítě byly propagovány přes BGP, třebaže to není nutné a ani to není zvykem. Po dokončení konfigurace ověřte dostupnost jednotlivých sítí a vyzkoušejte různé show příkazy.

Další vlastnosti a možnosti eBGP

Sumarizace

V BGP je defaultně vypnuta sumarizace, ta se samozřejmě dá zapnout, sumarizuje se podle třídy. K tomu slouží příkaz `auto-summary` v subkonfiguračním směrovacím módu.

Také je možné zajistit agregaci jen určitých adresních rozsahů, k tomu slouží příkaz `aggregate-address` použitý ve směrovacím subkonfiguračním módu. Tento příkaz má především jako parametr agregovaný rozsah adres, ale I další parametry, jejich vysvětlení najdeme například na https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5441-aggregation.html

Redistribuce směrovací informace jiného protokolu

Jak bylo výše uvedeno, BGP propaguje sítě převzaté z vlastní směrovací tabulky, nebere je z rozhraní. Takže není problém distribuovat peerům záznam ze směrovací tabulky pocházející od jiného směrovacího protokolu, například od OSPF. Ovšem mělo by se jednat o veřejné adresy, nikoliv soukromé. Můžeme do směrovacího procesu přímo zadat příkaz network s danou sítí (včetně masky, pokud je jiná než pro třídu), nebo se dá použít příkaz pro redistribuci adresních rozsahů (například `redistribute ospf 1 match external` distribuuje externí cesty protokolu OSPF).

Taktéž je možné určit adresy pro redistribuci přesněji, a to pomocí ACL, příklad najdeme například na https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/6500-bgp-pix.html (asi tak v polovině stránky).

BGP umí také předávat default route. Nejdřív vytvoříme nulovou cestu a nasměrujeme do zařízení Null0, pak propagujeme přes BGP:

```
ip route 0.0.0.0 0.0.0.0 null0
router BGP xxxxx
       network 0.0.0.0
```

Použití loopbacku také pro posílání směrovacích informací a zvýšení hodnoty TTL

Směrovací informace BGP může být posílána na IP adresu síťového rozhraní (například router R2 na obrázku výše bude posílat směrovací informace pro router R1 přes TCP spoj na adresu 12.0.0.1), nebo se dá nakonfigurovat posílání na adresu loopbacku použitou jako RouterID (zde 1.1.1.1). V Packet Traceru je s tím problém, ale na reálném zařízení bychom to provedli takto – nejdřív zprovoznit loopback na routeru R1:

```
int lo0
       ip addr 1.1.1.1 255.255.255.255
       exit
```

Pak na routeru R2 sdělíme, že I pro TCP spojení pro BGP informace se má používat loopback na R1:

```
router bgp 64501
       neighbor 1.1.1.1 remote-as 64500
       neighbor 1.1.1.1 update-source Loopback0
       neighbor 1.1.1.1 ebgp-multihop 2       ; číslo větší než 1, použije se jako TTL
```

Výhodou je větší odolnost komunikace proti výpadkům sítě, a také možnost použít tutéž IP adresu při přístupu do zařízení přes různé cesty. Ale pozor: eBGP standardně používá TTL=1, jenže pokud router přijme BGP segment přes fyzické síťové rozhraní a cílová adresa je jeho loopback, pak uvnitř routeru proběhne směrování, při kterém se TTL sníží o 1, a až potom se PDU dostane na loopback, pokud ovšem TTL >0. Proto je nutné použít příkaz `ebgp-multihop` a nastavit takto TTL na hodnotu vyšší než 1.

Problém s navýšením TTL také řešíme, pokud mezi dvěma eBGP sousedy je ještě jiné L3 zařízení. Také musíme nastavit hodnotu TTL na vyšší číslo. Protokol iBGP tento problém nemá, tam je defaultní hodnota TTL větší než 1.

Příklad

Na webu je předpřipravený soubor 08c_routing-BGP2a.pkt (druhý odkaz pro BGP). Přímo v souboru jsou instrukce, co je třeba udělat. Nezapomeňte nakonfigurovat také propagování default route přes BGP. Všimněte si, jakým způsobem je z propagován rozsah pro veřejnou síť z AS 64501 a uvědomte si, proč je v tomto AS také protokol OSPF (které rozhraní je pasivní?). Zobrazte si také směrovací tabulky různých routerů.

Filtrování v BGP

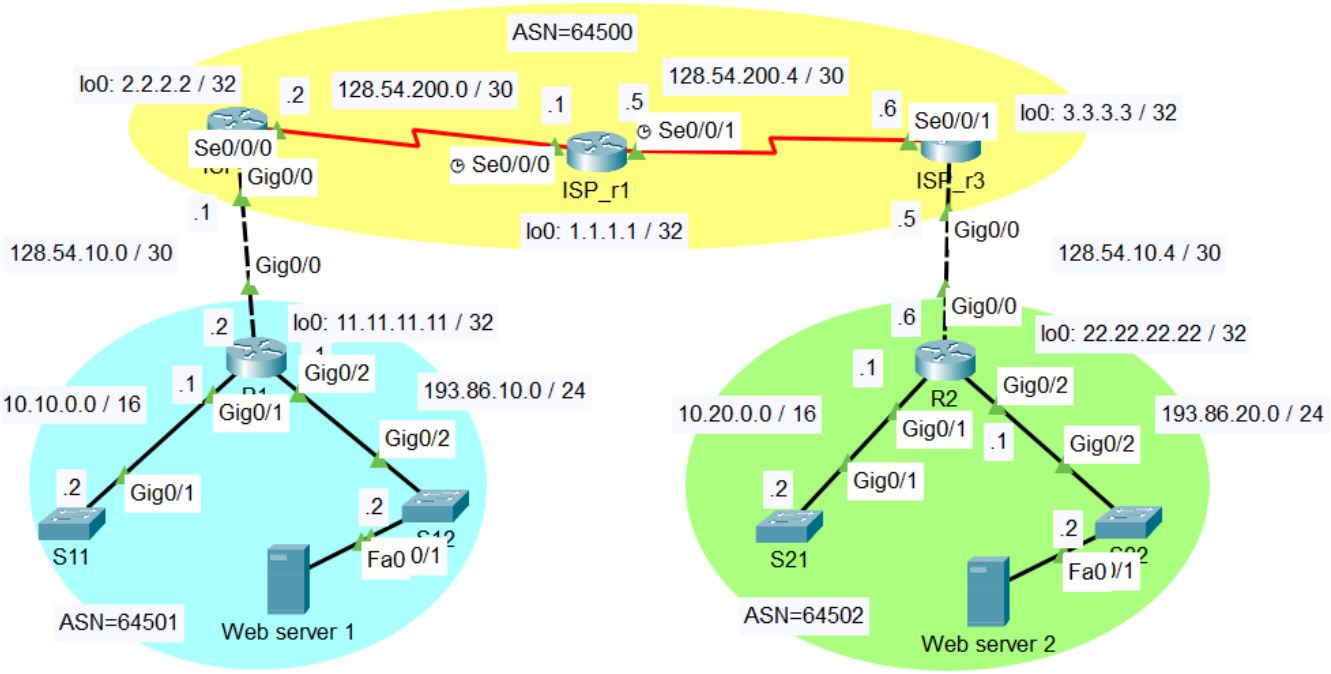
Jak víme, BGP dokáže propagovat peerům cokoliv, co najde ve směrovací tabulce, ovšem ne vše z tabulky je vhodné poslat do světa. V předchozím příkladu jsme zajistili propagování jedné veřejné sítě v každém stub AS, kdežto soukromé rozsahy zůstaly soukromými, ale ve skutečnosti je několik možností jak vyfiltrovat sítě pro propagování:

- vytvoříme standardní nebo extended ACL a ve směrovacím procesu použijeme příkaz
  `neighbor soused distribute-list označení_ACL out    ; k sousedovi půjde pouze toto`
  `neighbor soused distribute-list označení_ACL in     ; od souseda přijmu pouze toto`
- použijeme příkaz `ip prefix-list název permit adresa_sítě` (při určení sítě použijeme CIDR zápis, tedy s délkou prefixu), pak ve směrovacím procesu použijeme příkaz
  `neighbor soused prefix-list název in` (nebo `out`, podle toho, který směr konfigurujeme)
- další možností je využít příkaz `route-map`, případně další.

iBGP – směrování uvnitř AS

Zatímco eBGP předpokládá, že BGP sousedi mají různá čísla ASN, iBGP se používá tehdy, když BGP sousedi mají totéž číslo ASN (patří do téže autonomní oblasti). Rozdíl v konfiguraci není až tak velký, taktéž se používá příkaz `neighbor xxxx remote-as yyyy`, ale za klíčovým slovem remote-as je stejné číslo ASN jako u označení BGP procesu.

Následující příklad budeme řešit jen v teoretické rovině, protože Packet Tracer nepodporuje iBGP 😊.



Z obrázku je patrné, že ISP propojuje dvě firmy (nebo to mohou být dvě pobočky téže firmy), z nichž každá má svůj autonomní systém. Pokud chce ISP zprostředkovávat cesty mezi „podřízenými“ AS a posílat si je přes své routery, musí použít iBGP (nebo mít ve své síti OSPF a redistribuovat mezi BGP a OSPF). Na routeru ISP_r2 (v žluté zóně vlevo) by byla tato posloupnost příkazů:

```
int lo0
      2.2.2.2 255.255.255.255
      no shut
      exit
router bgp 64500
      neighbor 128.54.200.1 remote-as 64500        ; iBGP
      neighbor 128.54.10.2 remote-as 64501         ; eBGP
```

V případě použití iBGP se pravděpodobněji budou řešit různé možnosti filtrování směrovacích informací (určitým peerům budeme posílat jen částečné updaty směrovacích informací, ne celou tabulku, případně opačně – od určitých peerů nebudeme chtít vše, ale jen část směrovacích informací). Důvodem je jak bezpečnost (zejména v prvním případě) nebo třídění veřejných a soukromých sítí, ale také ochrana před zbytečným zahlcováním směrovacích tabulek, určování optimálnějších cest a ochrana před smyčkami.

Ve směrovací tabulce má iBGP 10× horší AD než eBGP (najděte tabulku ve skriptech pro přednášky a ověřte).

IP SLA ICMP Echo

Pokud si se svým ISP dohodneme ve smlouvě SLA určité podmínky, asi budeme chtít mít možnost si kontrolovat plnění. Typickou podmínkou například bývá neustálá dostupnost připojení (24/7). K tomu slouží funkce IP SLA.

```
ip sla 20                ; číslo operace, nějaké zvolíme
      icmp-echo adresa-druhé-strany    ; můžeme taky přidat označení odchozího rozhraní:
                                       ;  icmp-echo xxxx source-int g0/0
      frequency 30       ; v sekundách – jak často bude posílán ping
      exit
ip sla schedule 20 start-time now life forever
```

Existuje také show příkaz:

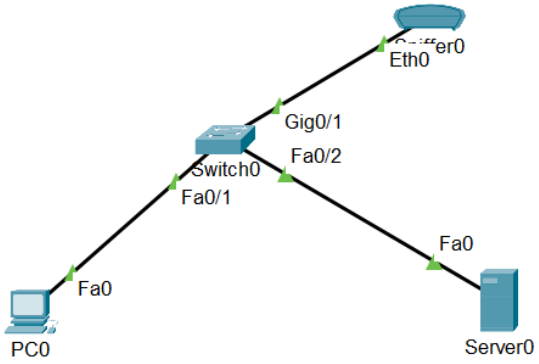
```
sh ip sla configuration
sh ip sla statistics
```

Kromě toho, že si můžeme „ručně“ zobrazit statistiku, je možné tento mechanismus napojit například na SNMP a v případě problémů bude generován SNMP trap.

IP SLA není v Packet Traceru podporována. Můžeme si ji procvičit jen na reálných zařízeních, například tak, že propojíme dva routery, z nichž jeden bude simulovat ISP.

Port Mirroring (SPAN – Switch Port Analyzer)

Použijte switch, PC, server a sniffer (v Packet Traceru ho najdete u koncových zařízení). Na PC nastavte adresu 10.0.0.2/8, na serveru 10.0.0.1/8.



Na snifferu zkontrolujte, jestli je zapnuto zachytávání, a ve filtrech nechte zapnuté pouze ICMP a TCP.

Na switchi proveďte následující (v globálním configu):

```
monitor session 10 source int f0/1
monitor session 10 dest int g0/1
```

Tím vytvoříte monitorovací proces 10, jehož zdrojový port (tedy ten, který je odposloucháván) je f0/1, cílový port (na který se posílá zrcadlený provoz) je g0/1. Nastavení se dá zkontrolovat příkazem

```
sh monitor
```

Pingněte z PC na server, pak si na PC zobrazte webovou stránku pro IP adresu serveru. Pak zkontrolujte, co sniffer zachytil.