BGP - запрещаем прием дефолта

Опубликовано muff в Чт, 2011-04-14 12:29

Довольно часто, если уж используется **BGP**, имеем в наличии несколько аплинков. И уже в зависимости от топологии сети строим маршрутизацию.

Как в таком случае поступать с дефолтом? Оптимальное решение всегда будет зависеть от той же топологии. Довольно часто также возникает необходимость в запрете приема дефолта от какого-то из нейборов. Кстати, к написанию статьи подтолкнула ситуация, возникшая вследствии того, что на роутере моей локалки, прием дефолта не фильтровался. И в один прекрасный момент один из нейборов прислал на этот роутер маршрут к этой самой **0.0.0.0/0** . А поскольку я дефолт как раз и получал по **BGP** (правда от нейбора с меньшим **Weight**), то в результате дефолт перенаправился на другого нейбора (что есть не очень хорошо, в моем случае).

Итак, пора заняться фильтрацией дефолта, чтобы избежать подобных ситуаций в будущем. Согласно таблицы маршрутизации, дефолт сейчас приходит по **BGP** от **192.168.157.85**:

```
router# show ip route
 Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route


B>* 0.0.0.0/0 [20/0] via 192.168.157.85, vlan684, 01:52:18
```

Для сравнения пропишем дефолт еще и статическим маршрутом на этот же IP:

```
router(config)# ip route 0.0.0.0/0 192.168.157.85
```

Проверяем:

```
router# show ip route
 Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.157.85, vlan684
B   0.0.0.0/0 [20/0] via 192.168.157.85, vlan684, 02:01:17
```

А теперь уже можно играться с запрещением дефолта по BGP. Создаем префикс-лист с названием **DENY-DEFAULT-IN**:

```
router(config)# ip prefix-list DENY-DEFAULT-IN seq 5 deny 0.0.0.0/0 le 1
router(config)# ip prefix-list DENY-DEFAULT-IN seq 10 permit 0.0.0.0/0 ge 2
```

Теперь применим этот фильтр к нейбору, от которого нет необходимости получать дефолт:

```
router(config-router)# neighbor 192.168.157.85 prefix-list DENY-DEFAULT-IN in
```

Обновляем список принимаемых от **192.168.157.85** префиксов:

```
router# clear ip bgp 192.168.157.85 soft in
```

Проверяем:

```
router0-zebra# show ip route
 Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.157.85, vlan684
```

Вуаля. Имеем в наличии только статически прописанный дефолт. По **BGP** он уже не приходит. Теперь дело за малым - применить префикс-лист **DENY-DEFAULT-IN** к определенным нейборам. А в моем случае еще и убрать этот префикс-лист с нейбора **192.168.157.85** (поскольку на момент тестирования дефолт приходил только от него) и статический маршрут, созданный в начале статьи.