سیسکو به پارسی

مسابقه سیسکو به پارسی – BGP

نوشته:

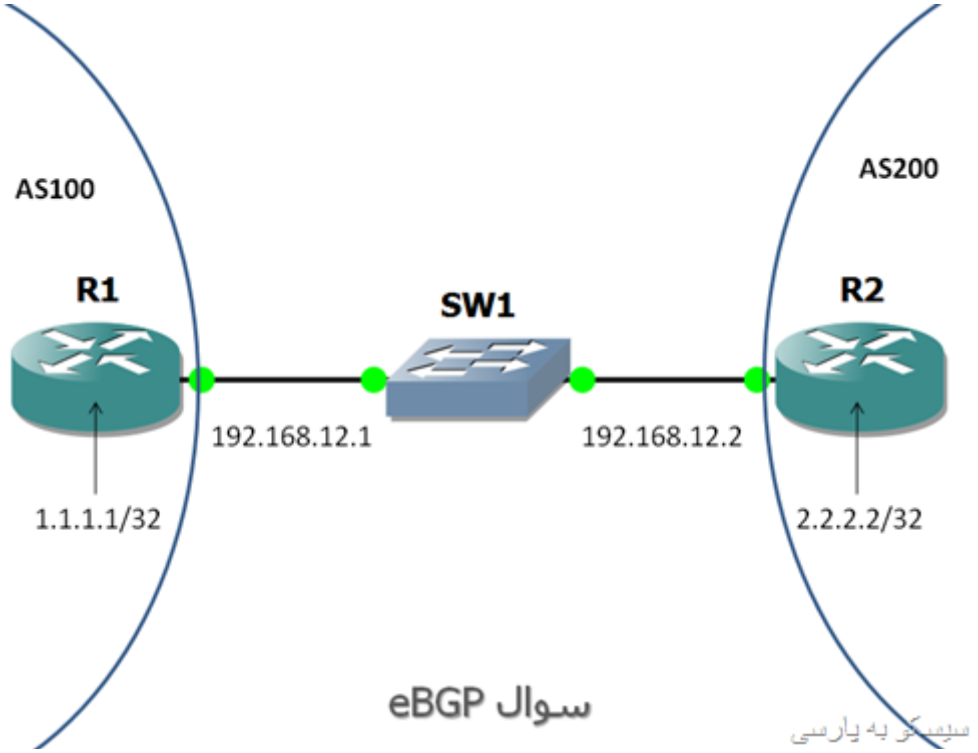
شفق زندی

سایت سیسکو به پارسی http://blog.shafagh.com/persian

انجمن سیسکو به پارسی http://forum.shafagh.com

مسابقه BGP

سوال این هفته در مورد تنظیم پروتکل BGP بین دو Autonomous System بکمک آدرسLoopback است. روترهای R1 و R2 بواسطه یک سوییچ به یکدیگر متصلند. روتر R1 متعلق به AS100 و R2 به AS200 است. آدرس هر دو روتر در شکل زیر نشان داده شده است:



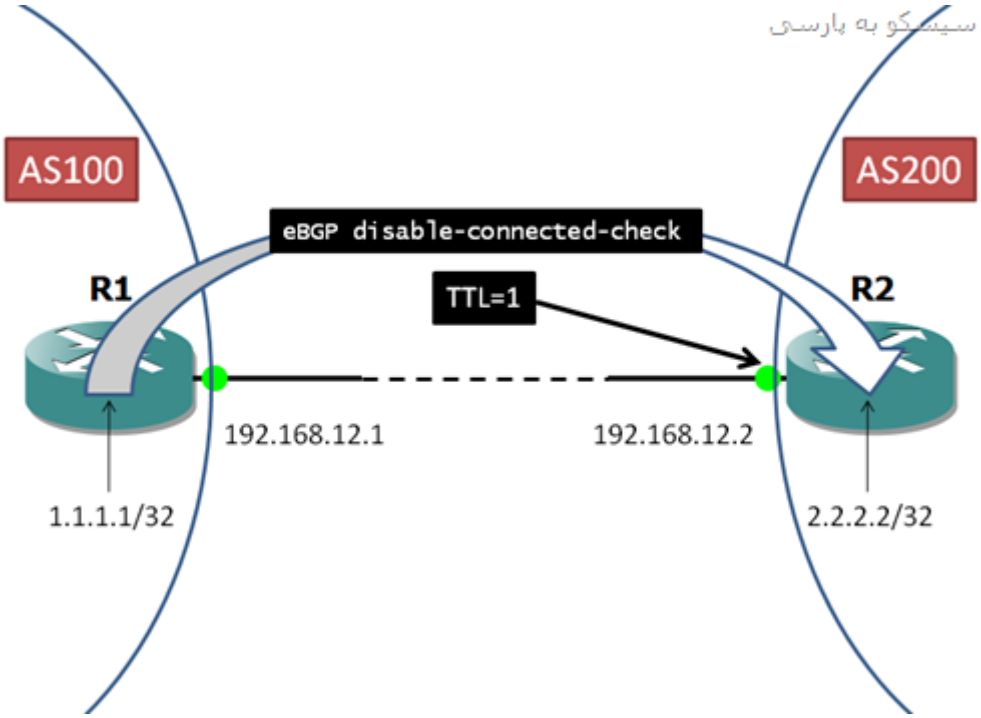
با توجه به شکل یک آدرس Loopback روی هر روتر تنظیم شده است. (۱.۱.۱.۱ و ۲.۲.۲.۲)

ارتباط eBGP دو روتر را بصورتی تنظیم کنید که ارتباط از Loopback یک روتر به Loopback دیگری برقرار گردد. (بسته های BGP از ۱.۱.۱.۱ به ۲.۲.۲.۲ و برعکس آن ردوبدل شوند)

تنظیم بخش router bgp روتر R1 خود را بصورت comment ذکر کنید. قبل از پاسخگویی حتما جواب خود را با GNS3 یا روی روترهای Lab خود، تست کنید. چون ممکن است راه حل شما در عمل کار نکند.

پاسخ مسابقه BGP

همانطور که انتظار میرفت پس از طرح سوالBGP نیز پاسخ های بسیاری خوبی از دوستان دریافت کردیم.
برای مشخص کردن Source بسته های BGP از دستور neighbor x update-source استفاده میکنیم. با کمک دستور فوق به R1 میگوییم که با آدرسLoopback ، بسته های TCP را به سمت همسایه ارسال کند (همانطور که میدانید، BGPاز پروتکل TCP برای ارتباط با همسایگانش استفاده میکند. جهت اطلاعات بیشتر به پست BGP رجوع کنید.) همین تنظیم در سمت مقابل نیز انجام میشود.



نکته مهم سوال، تنها استفاده از Loopback Address نیست بلکه براساس RFC، پروتکل BGP در ارتباط با همسایگان خارجی خود eBGP بصورت Default تنها با همسایگانی که مستقیما (Directly) متصل هستند ارتباط برقرار میکند و علاوه بر آن TTL بسته های خود را برابر با یک ست میکند. پس اگر همسایه ای با آدرسی جدا از آدرس مستقیما متصل یا چند Hop دورتر از همسایه دیگر باشد، ارتباط بصورت نرمال برقرار نخواهد شد. این یک ویژگی امنیتی در eBGP است. در iBGP قانون TTL صدق نمیکند و میتوان ارتباط را براحتی بین همسایگانی که از هم فاصله دارند برقرار کرد. برای ارتباط بین Loopback ها باید Route بین دو همسایه وجود داشته باشد:

```
R1(config)# ip route 2.2.2.2 255.255.255.255 192.168.12.2
R2(config)# ip route 1.1.1.1 255.255.255.255 192.168.12.1
```

به سه روش میتوان مساله فوق را حل کرد:

راه حل یک

```
router bgp 100
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 disable-connected-check
neighbor 2.2.2.2 update-source Loopback1
```

در سناریو ما، این بهترین راه حل است. چون به TTL دست نمیزنیم. بدین صورت روتر از حملات Session-Hijackingدر امان می ماند و باTTL=1 با همسایه ارتباط برقرار میکند.

راه حل دو

```
router bgp 100
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 ttl-security hops 2
neighbor 2.2.2.2 update-source Loopback1
```

Cisco in Persian

دستور ttl-security برای امنیت ارتباط، TTLبسته های ارسالی و دریافتی را بصورت Maximum در نظر میگیرد یعنی وقتی برابر با حداکثر دو Hop تنظیم شود، بسته های ارسالی را با TTL=255 میفرستد و از طرف مقابل تا حداکثر TTL=253 انتظار دارد تا پاسخ دریافت کند. با کمک این دستور Connected-Check نیز انجام نمیشود و دو همسایه که مستقیم بهم متصل نیستند میتوانند با هم ارتباط برقرار کنند.

راه حل سه

```
router bgp 100
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 ebgp-multihop 2
neighbor 2.2.2.2 update-source Loopback1
```

در این روش eBGP بخاطر دستور ebgp-multihop متوجه میشود که همسایه مستقیم متصل نبوده و بهمین دلیل Connected-Check را انجام نمیدهد. در مثال ما بسته های BGP با TTL=2 ارسال میشوند. هر چه تعداد hop در ebgp-multihop را بزرگتر در نظیر بگیریم ریسک امنیتی ارتباط BGP نیز افزایش می یابد و برای Attackاز فواصل دورتر مهیا میگردد.

برندگان مسابقه:

ایمان کرد

آرش مظلومی

محمد حسینی

علی a.zamanian@*****.com

bleeed_it_out@*****.com

Saeid-Alekhamiss

saman

محسن عفیف پور

طاها (dotnet)

سپیده

morteza

مهدی دهقان

اما بهترین پاسخ را Saeid-Alekhamiss ارسال کردند که به هر سه روش فوق اشاره شده، هرچند که با بی دقتی شماره AS Number را اشتباه تنظیم کردند، اما قابل تقدیر است. قبلا هم اشاره کردم که در پاسخ دقت کنید و تنها مواردی که در سوال از شما خواسته شده را انجام دهید بهمین دلیل برخی از پاسخ ها قابل قبول نیستند: دو نفر از دوستان از Default Route برای دسترسی به طرف دیگر استفاده کرده اند که متاسفانه پاسخ آنها مورد قبول قرار نمیگیرد.

Cisco in Persian