

Migratory ASs

Sandra Murphy

sandra.murphy@sparta.com

sponsored by DHS under an Interagency Agreement with AFRL

How to Do That in BGPSEC

Notation

In the following, the notation means:

for the origin BGPSEC signature attribute:

sig(originprefix, <target>, AS of signer, pcount) key

for intermediate BGPSEC signature attributes:

sig(<target>, AS of signer, pcount) key

MIGRATING

333

|

ISP A'

ISP A'

```
CE-1 <---- PE-1 <----- PE-2 <---- CE-2
100      Old_ASN: 300      Old_ASN: 200      400
          New_ASN: 200      New_ASN: 200
```

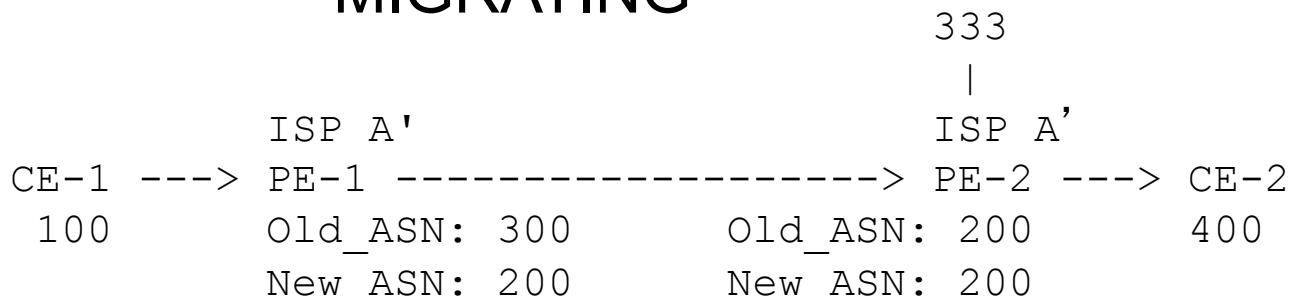
```
CE-2 to PE-2:  sig(origin(N), <200>, 400, pcount=1)K_400-CE2  [sig11]
                AS_PATH=(400)
                length=sum(pcount)=1
```

```
PE-2 to 333:   sig(<333>, 200, sig11, pcount=1, sig11)K_200-PE2  [sig12]
                sig(origin(N), <200>, 400, pcount=1)K_400-CE2  [sig11]
                AS_PATH=(200, 400)
                length=sum(pcount)=2
```

```
PE-2 to PE-1:  sig11
```

```
PE-1 to CE-1:  sig(<100>, 300, pcount=1, sig12)K_300-PE1  [sig13]
                sig(<300>, 200, pcount=0, sig11)K_200-PE2  [sig12]
                sig(origin(N), <200>, 400, pcount=1)K_400-CE2  [sig11]
                AS_PATH=(300, 400)
                length=sum(pcount)=2 (length is NOT 3)
```

MIGRATING



```
PE-1 to CE-1:  sig(<100>,300,pcount=1,sig12)K_300-PE1 [sig13]
               sig(<300>,200,pcount=0,sig11)K_200-PE2 [sig12]
               sig(origin(N),<200>,400,pcount=1)K_400-CE2 [sig11]
               AS_PATH=(300,400)
               length=sum(pcount)=2 (length is NOT 3)
```

Note that PE-1 is adding two signatures to the list.

It is as if PE-1 had an AS hop internally. NOTE: “**AS IF**”
PE-1 adds sig12 and sig13.

sig12 is added as if PE-1 is AS200 and adds the pcount=0.
sig13 is added as if PE-1 is AS300. So “AS300” authorizes
“AS200” to add the pcount=0.

Note that the neighbor of the AS that adds pcount=0 is the one
authorizing - further ASs can not check the authorization.
(For original route server motivation, neighbor **is** authority.)

MIGRATING in Other Direction – Alternative 1

```

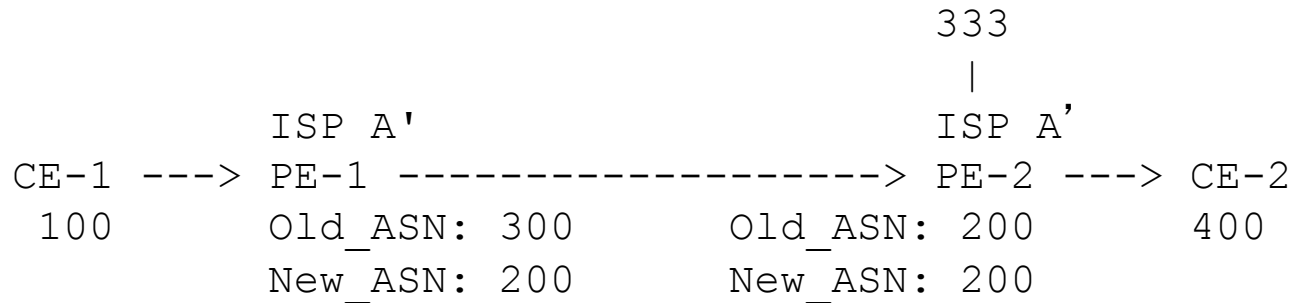
                                     333
                                     |
                                     ISP A'
ISP A'
CE-1 ----> PE-1 -----> PE-2 ----> CE-2
100      Old_ASN: 300      Old_ASN: 200      400
          New_ASN: 200      New_ASN: 200
```

```
CE-1 to PE-1:  sig(origin(N2), <300>, 100, pcount=1)K_100-CE1 [sig21]
AS_PATH=(100)
length=sum(pcount)=1
```

```
PE-1 to PE-2:  sig(<200>, 300, pcount=0, sig21)K_300-PE1 [sig22]
sig(origin(N2), <300>, 100, pcount=1)K_100-CE1 [sig21]
AS_PATH=(300, 100)
length=sum(pcount)=1
```

```
PE-2 to CE-2:  sig(<400>, 200, pcount=1, sig22)K_200-PE2 [sig23]
sig(<200>, 300, pcount=0, sig21)K_300-PE1 [sig22]
sig(origin(N2), <300>, 100, pcount=1)K_100-CE1 [sig21]
AS_PATH=(200, 300, 100)
length=sum(pcount)=2
```

MIGRATING in Other Direction – Alternative 1



```
PE-1 to PE-2:  sig(<200>,300,pcount=0,sig21)K_300-PE1 [sig22]
               sig(origin(N2),<300>,100,pcount=1)K_100-CE1 [sig21]
               AS_PATH=(300,100)
               length=sum(pcount)=1
(P E-2 authorizes PE-1 to use pcount=0)
```

PE-1 is the one doing the migration, so it makes sense that it is the one that has to take special action.
but this is an ibgp session and not normal to be adding bgpsec attrb on ibgp session.
Again, this is working as if there was a ebgp hop internal to PE1, at least as far as the bgpsec attributes are computed

Discussion

- In BGP, this is a non-spec vendor knob
- There's work presented to idr to make a standard way to do this (make vendor knobs consistent)
- Presuming this proves to work
- Do we consider this as advice to vendors making bgpsec versions of their knobs?
- Do we make this part of the bgpsec protocol?
 - (If idr makes this standard, then obviously it should be part of bgpsec protocol.)