

BGP Communityによる トラフィック制御

1998/7/3

JANOG#2 in KDD新宿

インテリジェント・テレコム株式会社
矢萩 茂樹 (yahagi@itjit.ad.jp)

BGPによる経路制御方法（構成）

- BGP4における経路制御
- communityとは
- communityにより何ができるか
- communityご使用上のご注意
- community制御の限界

BGP4での経路制御 -- 命題！

- AS内は統一したポリシーにより制御可能
- トラフィック出力制御はAS内において好きなように属性をいじれるので、比較的簡単。
- 問題はリターントラフィック制御
「如何にしてその気のない人を自分に都合よく振り向かせるか」

BGP4経路制御に用いる ATTRIBUTE

■ local-preference

- ルートに対して複数出口がある際、どの出口が好ましいかを規定する。
iBGP内(自AS内)で交換され、eBGP(他AS)には伝播しない。

■ MED(Multi-Exit Discriminator)

- 複数のポイントで接続しているASに対してどのルートが好ましいかを伝えるために規定する。隣接ASまでしか伝播しない。

■ as-path (?!)

- 受信した経路がどのASを経由してきたかを現すattribute。ASを通過するたびにそのASの番号が追加されていく。

■ 優先度 : 大 local-pref as-path MED 小

BGP4での経路制御 -- 現状

- AS外のトラフィック制御はそれなりに困難。
 - ASはそれぞれ独立した運営ポリシーを持っており、伝達情報が常にこちらの意図した通りに受け取られるとは限らない。
 - 複数のポイントで相互接続し、MEDで制御しようとしても、先方で内部ルーティングをlocal-preference制御していると無視される！
 - 比較的效果があるのはas-path prepend (as-path長延長)だが、あくまでもCISCO Orientedな機能なので、他のルーターが入ると制御が効かない。
(RFCには規定されていないらしい?!)

BGP4での経路制御 -- 現状(cont.)

- as-path以外のattributeで他ASの戻り経路を制御できるのはMEDとなるが、これは隣接ASまでしか伝播しないため、ASをはさんでしまうと制御ができない。
- では、
 - 伝播範囲を規定しないメッセージの伝達手段を規定し、そのメッセージを理解できる人の間だけで経路制御できるようにしてはどうか。
- BGP Community Attribute !!

Communityとは何か

- RFC-1998
 - "An Application of the BGP Community Attribute in Multi-home Routing"
- BGP Speaker間で共通のポリシーを表現するために規定
- 32bitの数値で表されるポリシーメッセージをBGP経路アナウンスに含めて転送する
- 複数のCommunity Messageを同時に転送可能
- 伝播範囲は規定されない
 - IBGP/EBGP/隣接BGP Speaker/隣接ASまでなどの範囲規定はない
- グローバル領域とプライベート領域を規定
 - 0x00000000 ~ 0x0000FFFF グローバル予約
 - 0x00010000 ~ 0x0000FFFE プライベート領域
 - 0xFFFF0000 ~ 0xFFFFFFFF グローバル予約

Communityとは何か(Cont.)

- well-known communityは2つ (?)
 - 0xFFFFFFFF01 no-export 伝播範囲 -- 隣接AS内
 - 0xFFFFFFFF02 no-advertise 伝播範囲 -- 隣接BGP Speakerまで
 - この他にCISCOではlocal-AS/Internetなるものがある。後者は????
- プライベート領域の意味付けはユーザ依存。
- 最近では上位16bitと下位16bitにフィールドを分割し、上位をAS番号、下位をAS内でのメッセージフィールドとして使用。
10進数で現す表記法が一般的。
 - 表記法 A:M A=AS番号、M=メッセージ番号
ex: 4682:100, 3561:70

Communityにより何ができるか

- Ciscoではroute-mapにて記述する。
- route-mapに記述できる制御の範囲であれば可能。
例えば、
 - announce範囲の限定
 - local-preference制御
 - as-pathの変更
 - その他

使用例-1

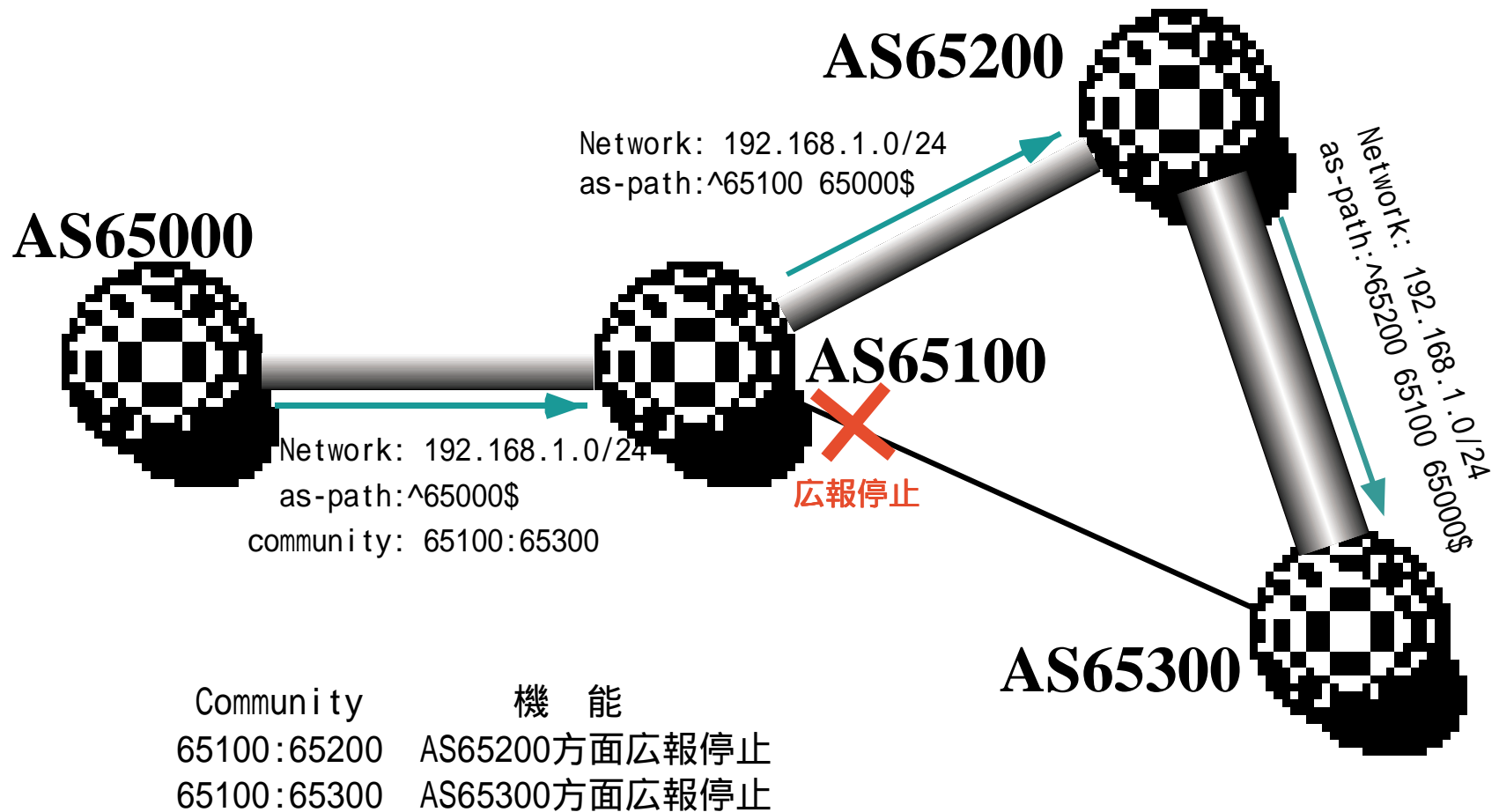
announce範囲限定(1)

■ 広報範囲を限定するAS65000の Config

```
■ router bgp 65000
  neighbor 172.16.0.1 remote-as 65100
  neighbor 172.16.0.1 send-community
  neighbor 172.16.0.1 route-map COM-OUT out
route-map COM-OUT permit 10
  match ip address 1
  set community no-export
access-list 1 permit 172.16.1.0 0.0.0.255
```

使用例-1'

announce範囲限定(2)



使用例-1'

announce範囲限定(2)

■ Community送信側 (AS65000)の Config

```
■ router bgp 65000
  neighbor 172.16.0.1 remote-as 65100
  neighbor 172.16.0.1 send-community
  neighbor 172.16.0.1 route-map AS65000-OUT out
route-map AS65000-OUT permit 10
  match ip address 1
  set community 65100:65300
access-list 1 permit 192.168.10.0 0.0.0.255
```

使用例-1'

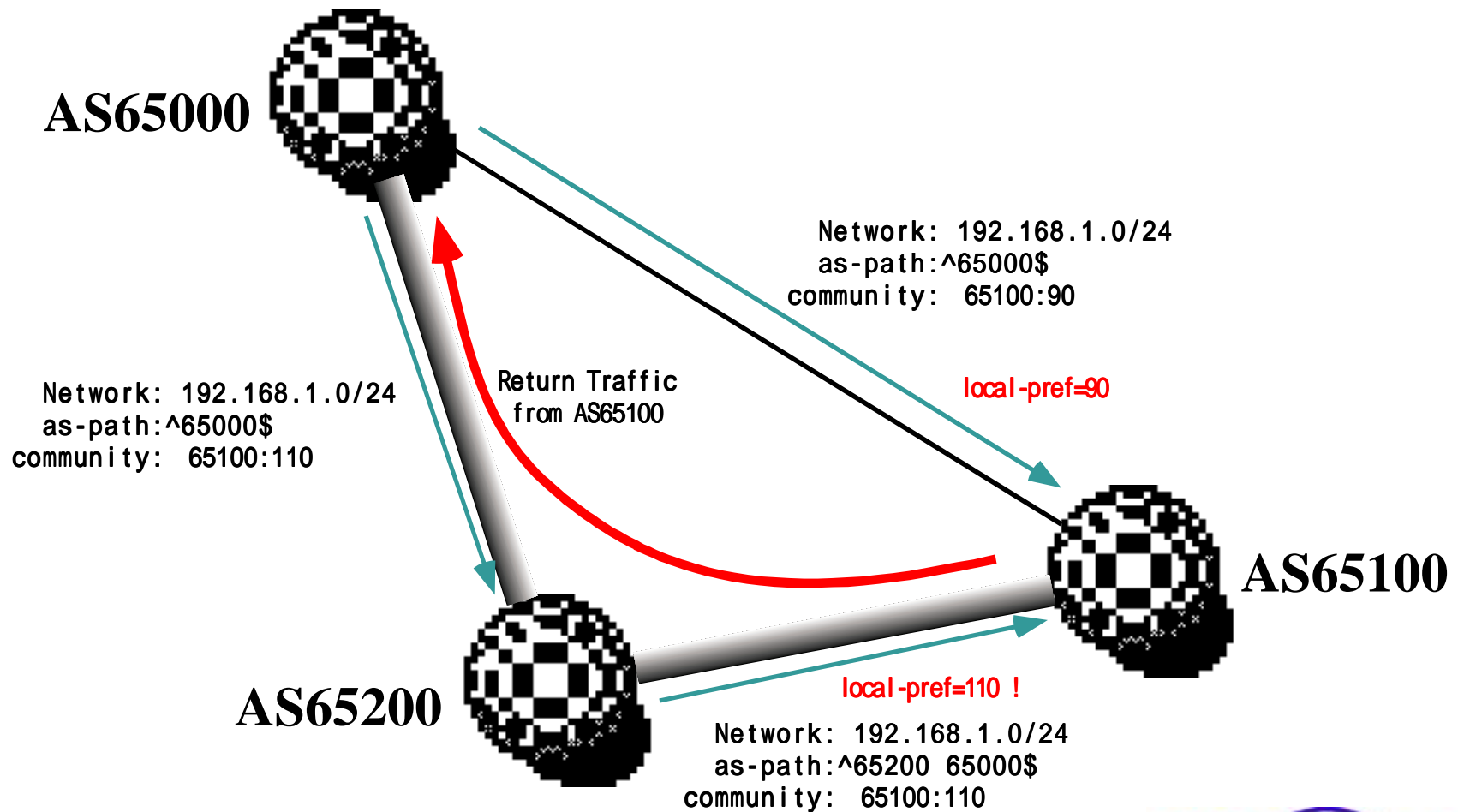
announce範囲限定(2)

■ Community受信側 (AS65100) の Config

```
router bgp 65100
  neighbor 172.16.0.2 remote-as 65000
  neighbor 172.16.1.2 remote-as 65200
  neighbor 172.16.1.2 route-map AS65200-OUT out
  neighbor 172.16.2.2 remote-as 65300
  neighbor 172.16.2.2 route-map AS65300-OUT out
  route-map AS65200-OUT deny 10
    match community 1
  route-map AS65300-OUT deny 10
    match community 2
  ip community-list 1 permit 65100:65200
  ip community-list 2 permit 65100:65300
```

使用例-2

local-preference制御



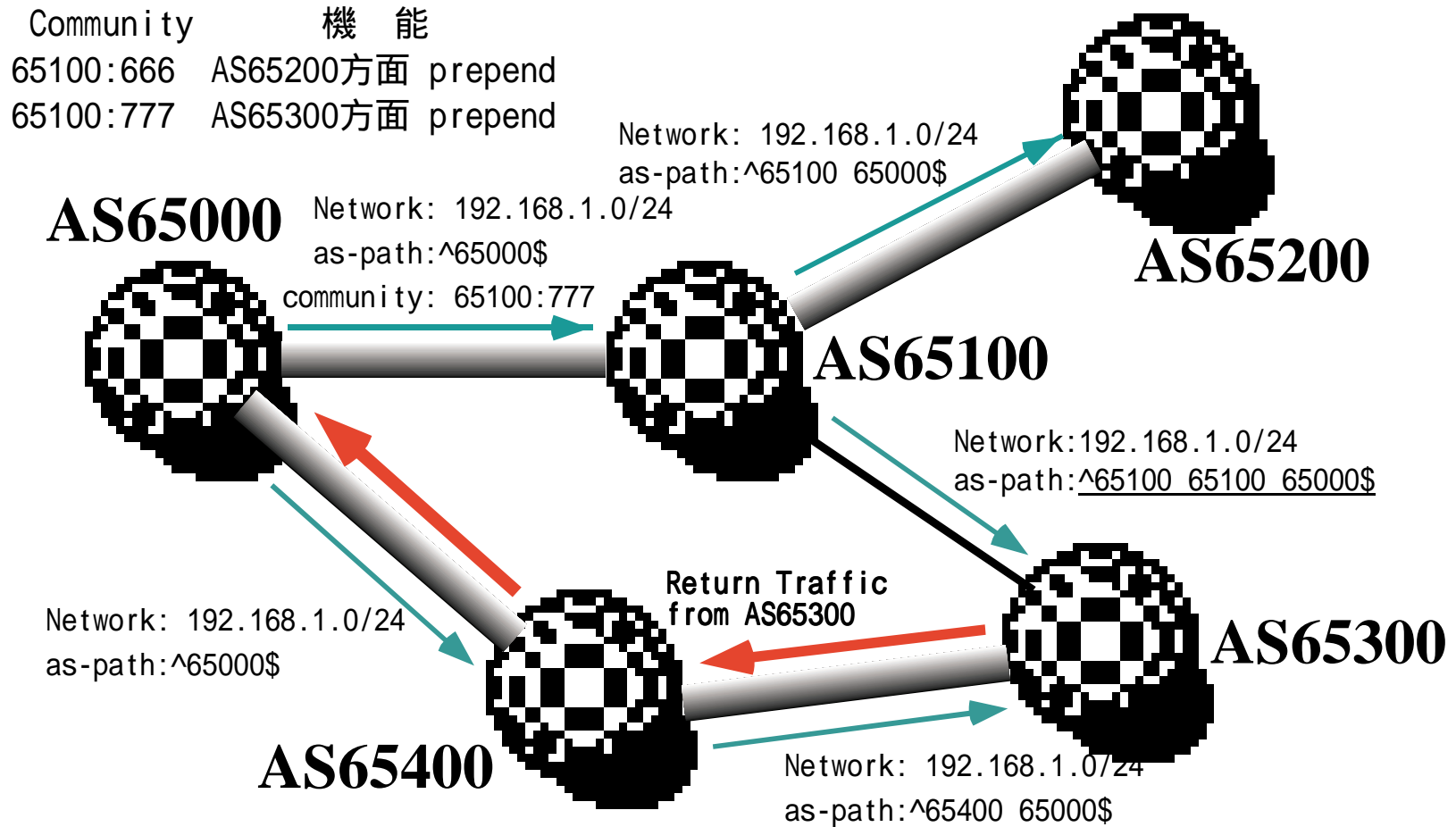
使用例-2

local-preference制御

■ Community受信側 (AS65100) の Config

```
router bgp 65100
  neighbor 172.16.0.2 remote-as 65000
  neighbor 172.16.1.2 remote-as 65200
  neighbor 172.16.1.2 route-map COM-IN in
  neighbor 172.16.2.2 remote-as 65300
  neighbor 172.16.2.2 route-map COM-IN in
route-map COM-IN permit 10
  match community 1
  set local-preference 90
route-map COM-IN permit 20
  match community 2
  set local-preference 110
ip community-list 1 permit 65100:90
ip community-list 2 permit 65100:110
```


使用例-3 as-pathの変更



使用例-3 as-pathの変更

■ Community受信側 (AS65100) の Config

```
router bgp 65100
  neighbor 172.16.0.2 remote-as 65000
  neighbor 172.16.1.2 remote-as 65200
  neighbor 172.16.1.2 route-map AS65200-OUT out
  neighbor 172.16.2.2 remote-as 65300
  neighbor 172.16.2.2 route-map AS65300-OUT out
  route-map AS65200-OUT permit 10
    match community 1
    set as-path prepend 65100
  route-map AS-65300-OUT permit 10
    match community 2
    set as-path prepend 65100
  ip community-list 1 permit 65100:666
  ip community-list 2 permit 65100:777
```

Community ご使用上のご注意

(Read Me First編)

- ガードしましょう、自分が処理するCommunity以外は。
 - どこからどんなもんが入ってくるかわからない。
- とんりのBGP SpeakerがCommunityを隣接に伝播してくれるとは限らない。メッセージが伝わらない?!
 - Cisco defaultは転送しない。
neighbor x.x.x.x send-community
- 必ず届く保証はない。
 - 使いたいときには 間の人たち とご相談 (^ ^;

Community ご使用上のご注意 (CISCOをお使いの方へ)

- 一度に1パターンのcommunityしか処理できない。
 - route-map内でcontinueとうつと、次のroute-map条件判断にいくとか
- exact-matchでは、他ASが追加した転送communityまでは盛り込めない。
 - extended community-listなる正規表現が使えるものが有るらしい。
 - マニュアル自体にこれの存在自体がないので使い方がわからない。使えない。(T_T)
- 特定communityの削除処理がないので、未処理communityのみの転送を実現できない。
 - route-map HOGE-IN permit 10
remove community hoge:geho とか
- この実装ではBGP CommunityはInternet Wideには使えない！ (1998/7/3 JANOG2 11.1.18CA現在 :-P)

おまけ - Communityの可能性

- example : CISCOの機能拡張
 - "Quality of Service Policy Propagation via Border Gateway Protocol"
 - <http://www.cisco.com/univercd/cc/td/doc/product/software/ios11/cc111/bgpprop.htm>
- BGP CommunityによりQoSパラメータを指定できるようにし、**広報経路単位**にService Qualityを伝達できるようにする。
- route-map内にて以下の設定が入力可能
 - set ip precedence priority
 - set ip precedence immediate
 - set ip precedence flash
 - set ip precedence flash-override
 - set ip precedence critical
 - etc.....

まとめ

- BGPでの経路制御の3つの方法
 - local-preference/MED/as-path prepend
- 他ASに対するリターントラフィック制御
 - 異なるポリシー間の調整の難易性
- BGP Communityの特徴と使用例
 - 範囲を限定すればそれなりに有効！
- BGP Communityによる制御の限界
 - 確実には使えない。協調運用が基本。基本は同じ
- 遊んでみましょう。(^^;
 - 自ASの中だけでのポリシー伝達にも使えるので



■ ご静聴ありがとうございました。

and



■ See you, soon. ;^)

■ Next Session --

"Do you need NetNews!?"