Controlando Tráfego de Trânsito em um AS

GTER27

19/Junho/2009

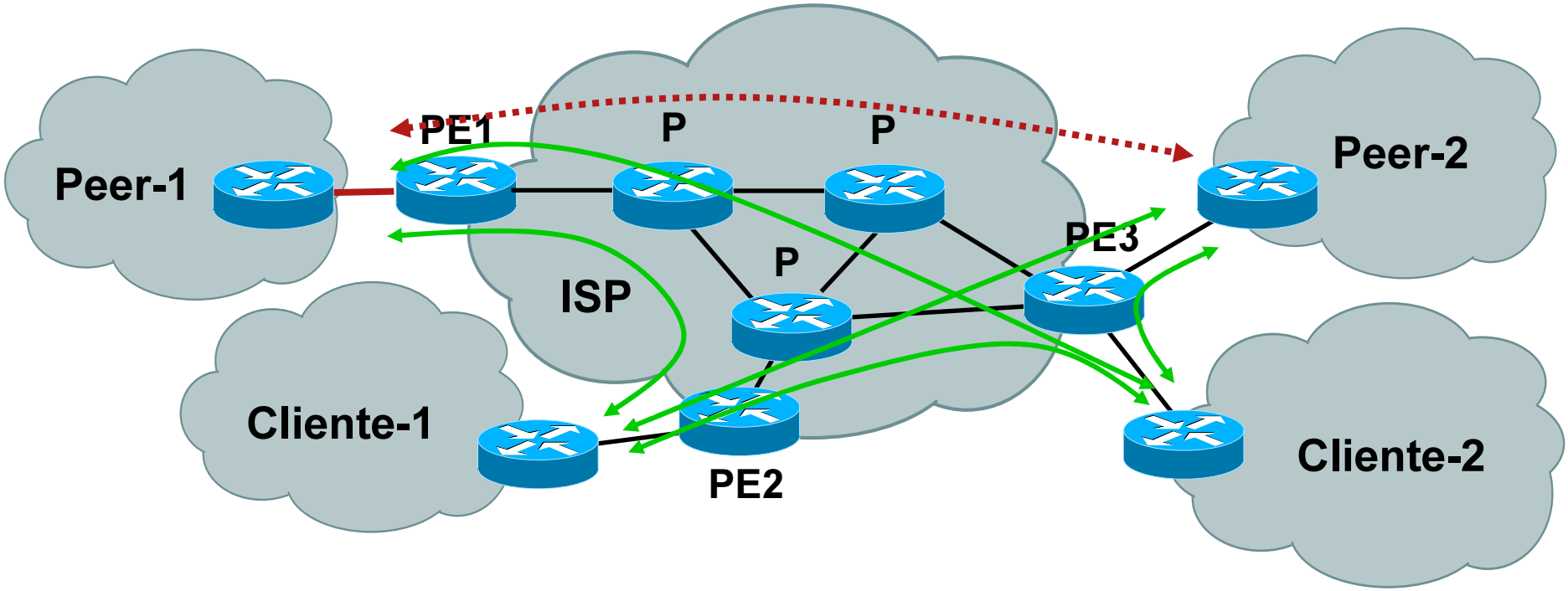
Ana Lúcia Araújo de Faria
aluciade@cisco.com

Network Consulting Engineer

Agenda

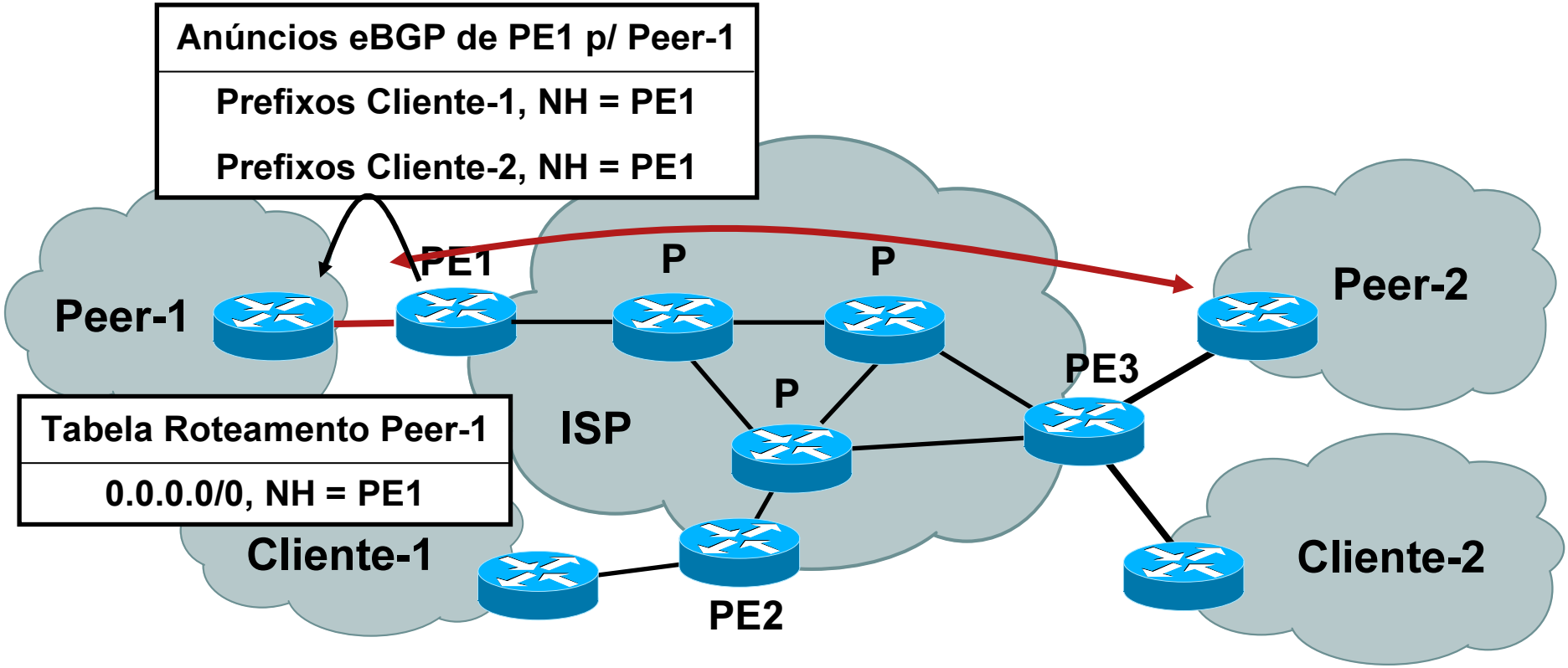
- Apresentação do problema
- Possíveis soluções
- Técnica Proposta
- Implementações
- Detalhamento da Solução

Política de Interconexão (*Peering*) Internet



- Peers devem ter conectividade IP com prefixos de Clientes
- Peers não devem usar ISP como trânsito para acessar um ao outro

Controle da Política de *Peering* Baseado em BGP

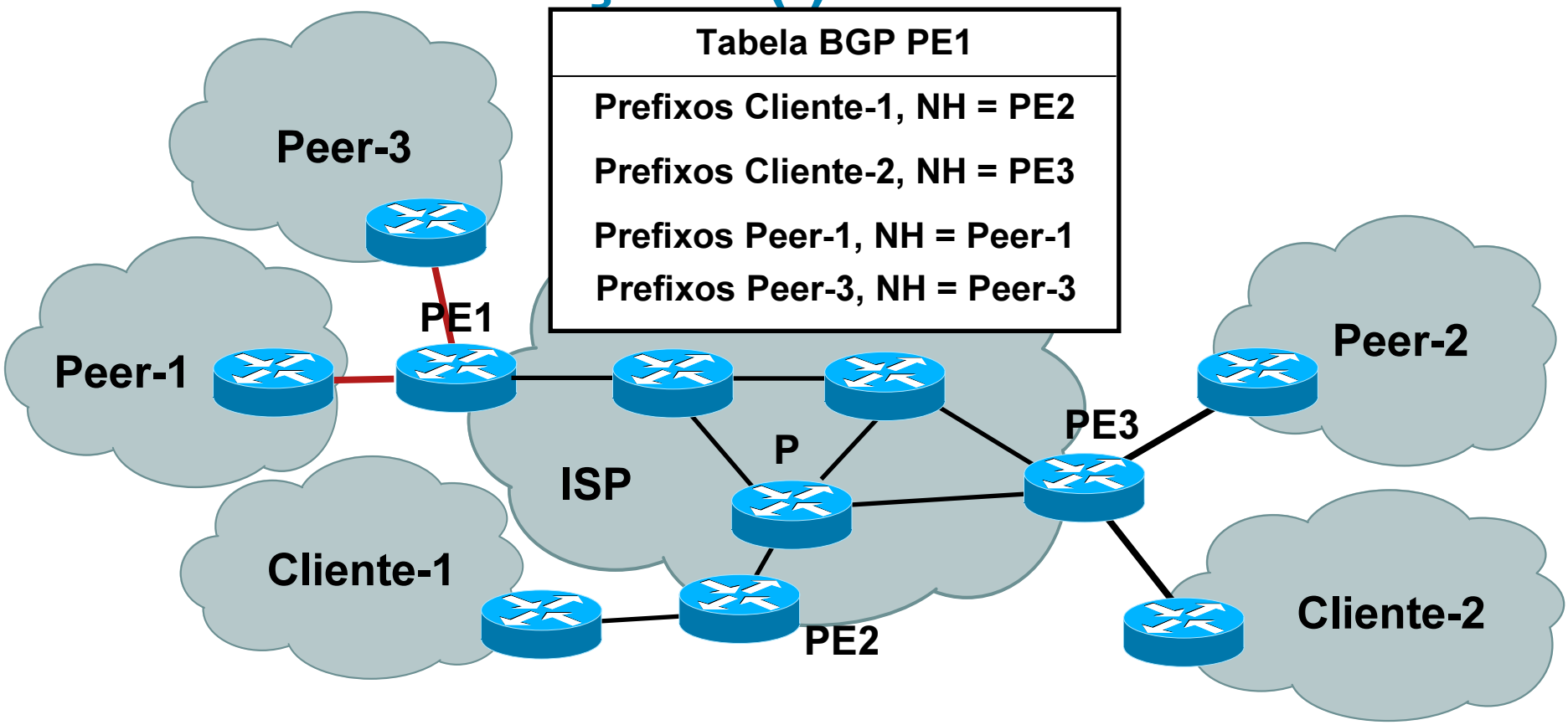


- **Política BGP garante *control plane***
  - **Técnicas disponíveis para filtrar anúncios de prefixos**
- **Política BGP não age no *data plane***
  - **Pacote destinado ao Peer-2 enviados pelo Peer-1 serão encaminhados pela FIB**

Agenda

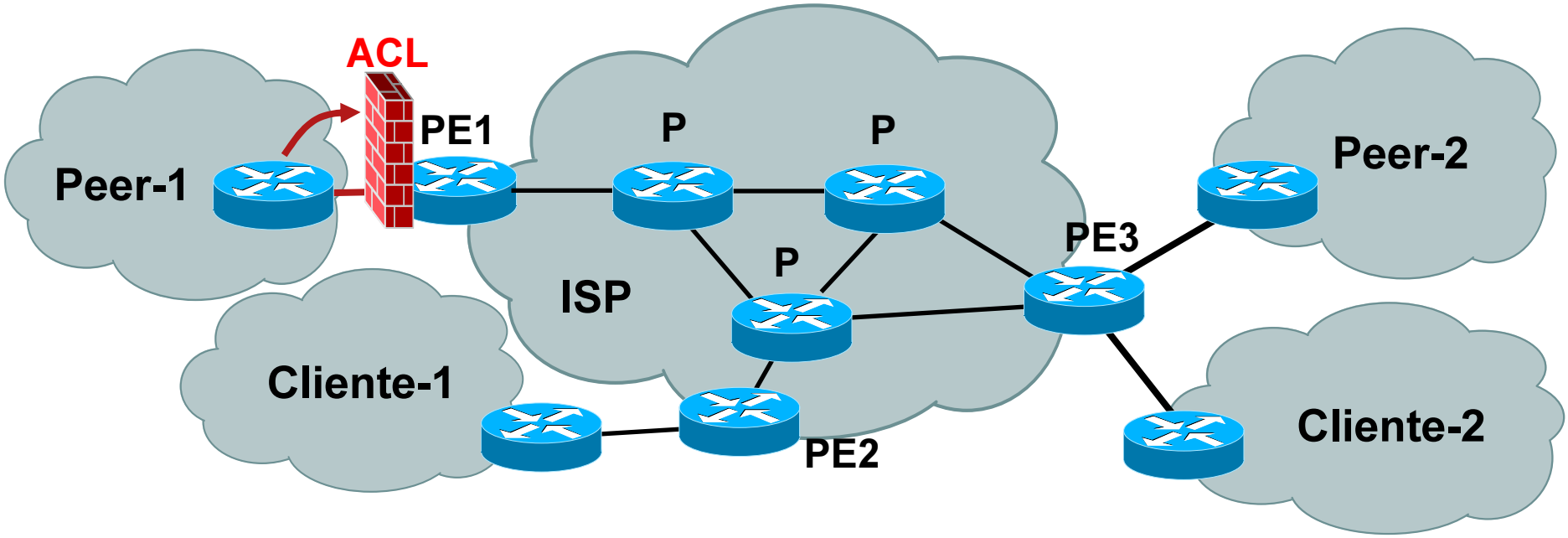
- Apresentação do problema
- Possíveis soluções
- Técnica Proposta
- Implementações
- Detalhamento da Solução

Possíveis Soluções (i)



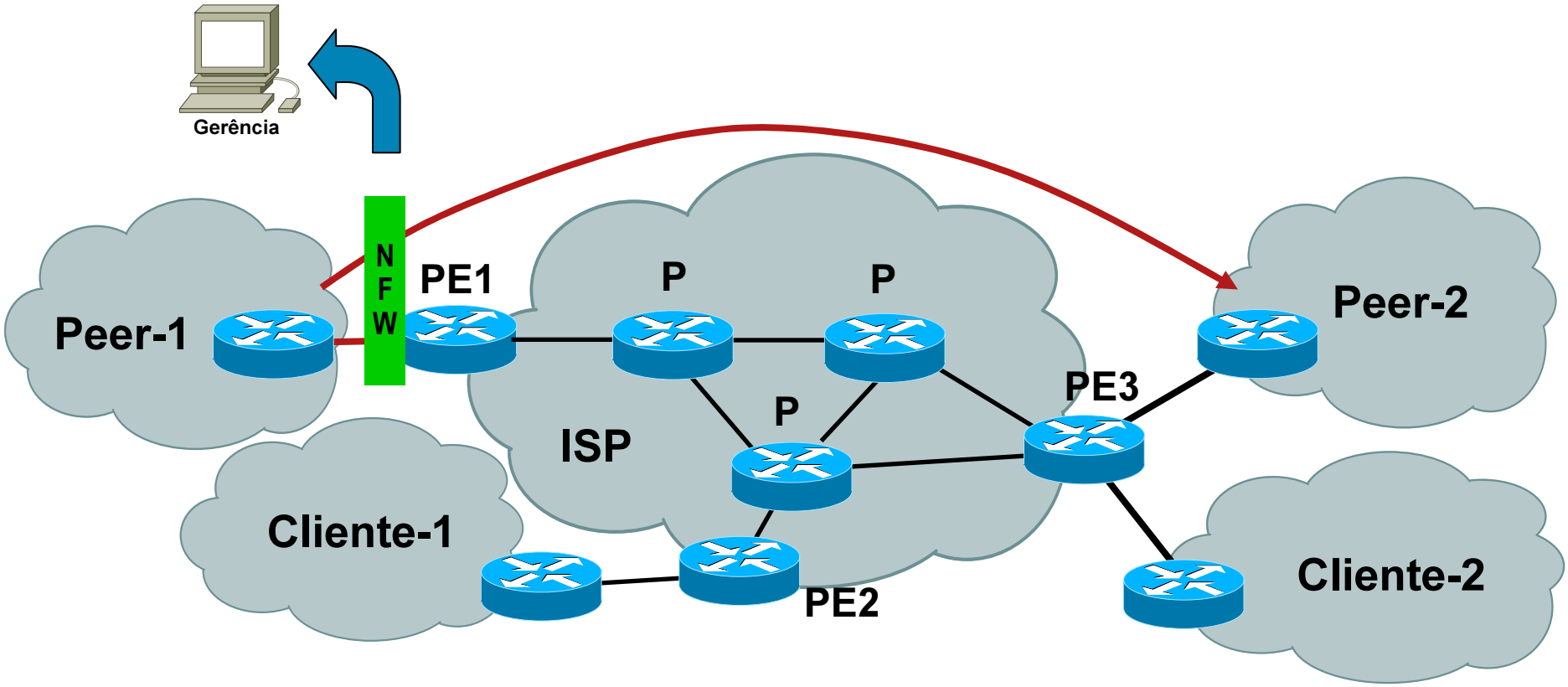
i. **Roteador de borda de conexão com *peers* com tabela BGP parcial**
   - Não evita trânsito entre *peers* conectados no mesmo roteador de borda

Possíveis Soluções (ii)



ii. **Lista de acesso na interface de entrada dos *peers***
   - Solução não escalável e ineficiente operacionalmente

Possíveis Soluções (iii)

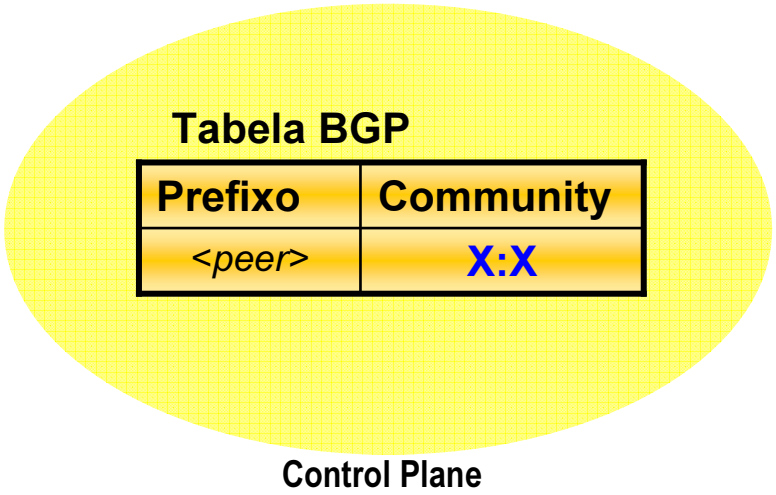


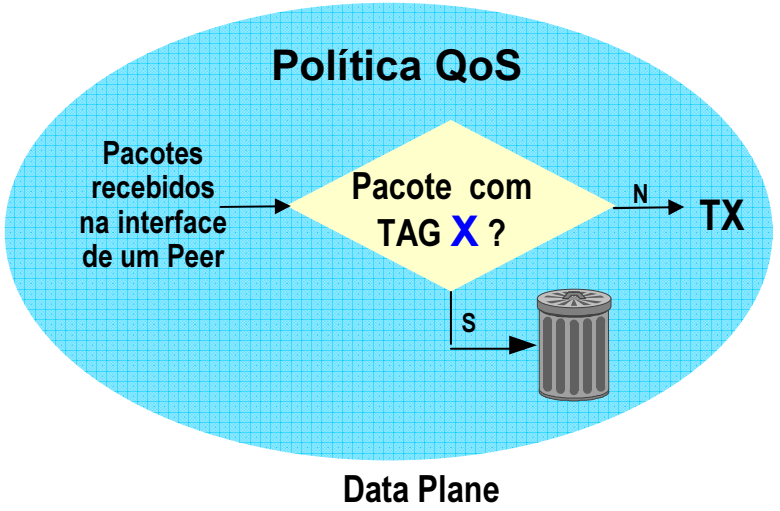
iii. **Monitoramento e verificação *offline* de falta de conformidade da política**
  – Solução reativa

Agenda

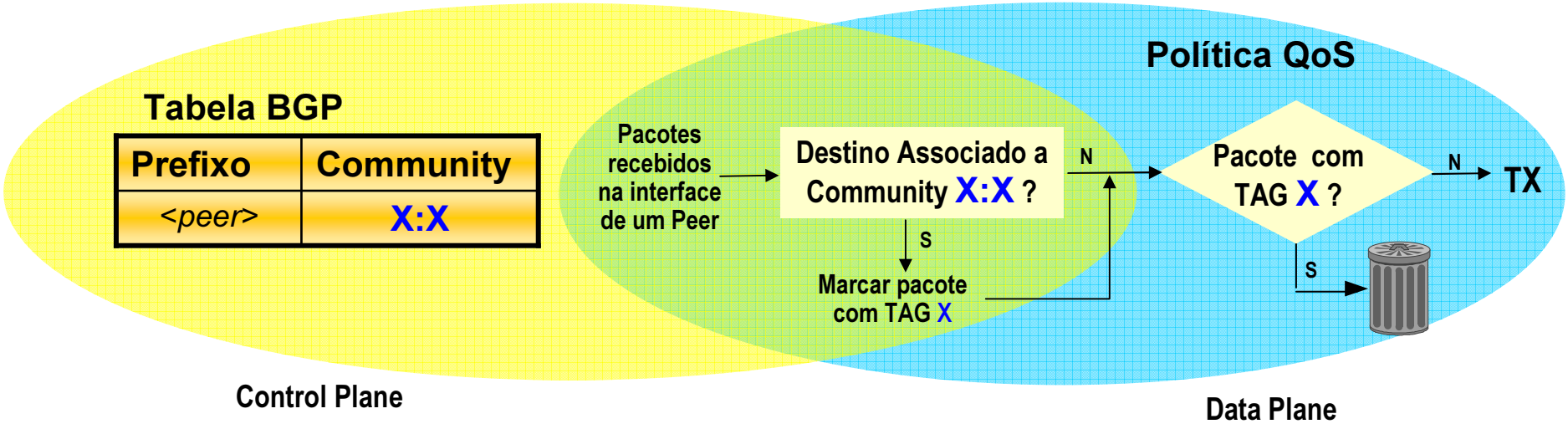
- Apresentação do problema
- Possíveis soluções
- **Técnica Proposta**
- Implementações
- Detalhamento da Solução

Técnica Proposta





Técnica Proposta



1. **Ação no *Control Plane***
   - Prefixos de peer identificados na tabela BGP através de um atributo BGP (ex: **Community X:X**)
   - Prefixos de peer associados a um **TAG X** ao ser instalado na FIB
2. **Interação entre *Control Plane* e *Data Plane***
   - Pacotes recebidos de um peer e destinado a prefixos da FIB com **TAG X** são marcados com **TAG X**
3. **Ação no *Data Plane***
   - Pacotes marcados com **TAG X** descartados pela política de QoS

Agenda

- Apresentação do problema
- Possíveis soluções
- Técnica Proposta
- **Implementações**
- Detalhamento da Solução

Implementações

- **Cisco**

  QPPB (*Qos Policy Propagation via BGP*)

  http://www.cisco.com/en/US/docs/ios/11_1/feature/guide/bgppropp.html

- **Juniper**

  Destination Class Policing

  http://kb.juniper.net/index?page=content&id=KB9298&actp=search&searchid=1245336388580&smlogin=true

Agenda

- Apresentação do problema
- Possíveis soluções
- Técnica Proposta
- Implementações
- Detalhamento da Solução

Detalhamento da Solução via QPPB

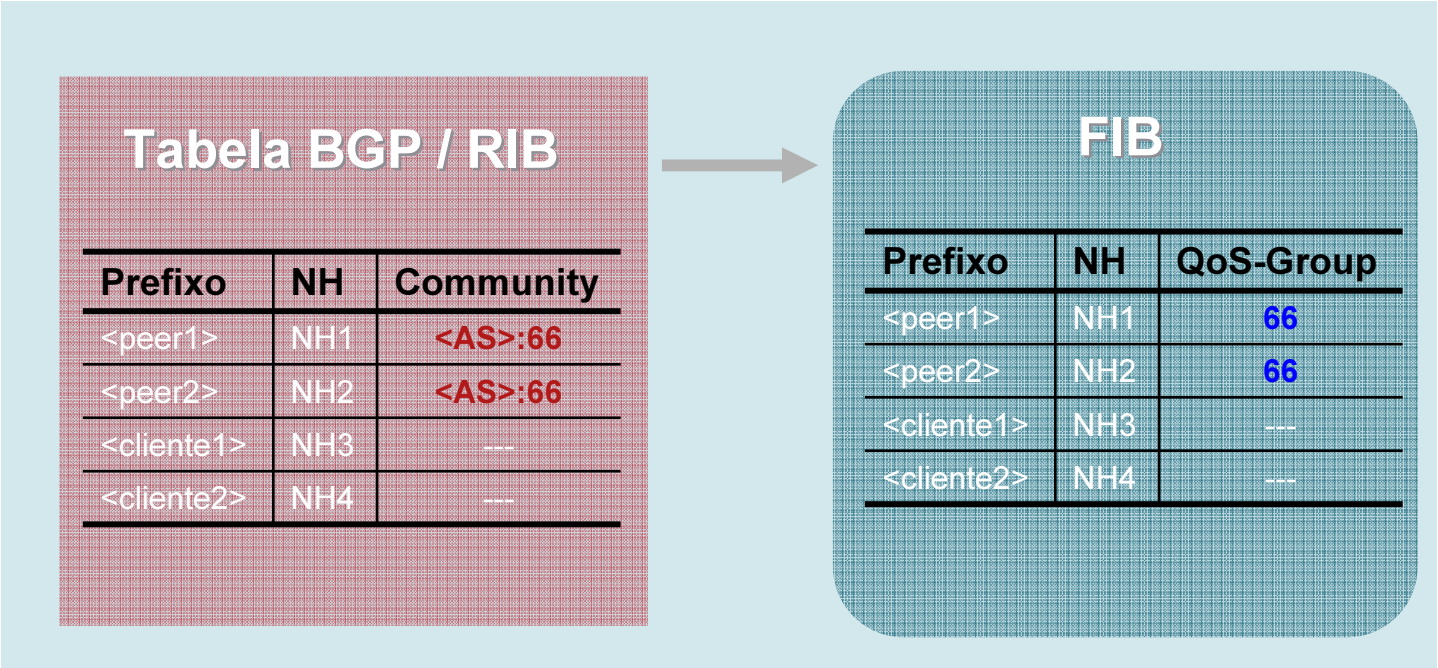
- **Configuração do Roteador**

1. Associação de TAG ao prefixo na FIB via BGP
   IOS CLI **table-map**

2. Associação de TAG a pacote recebido no roteador via QPPB
   IOS CLI **bgp-policy**

3. Classificação e descarte de pacote via QoS
   IOS CLI **service-policy**

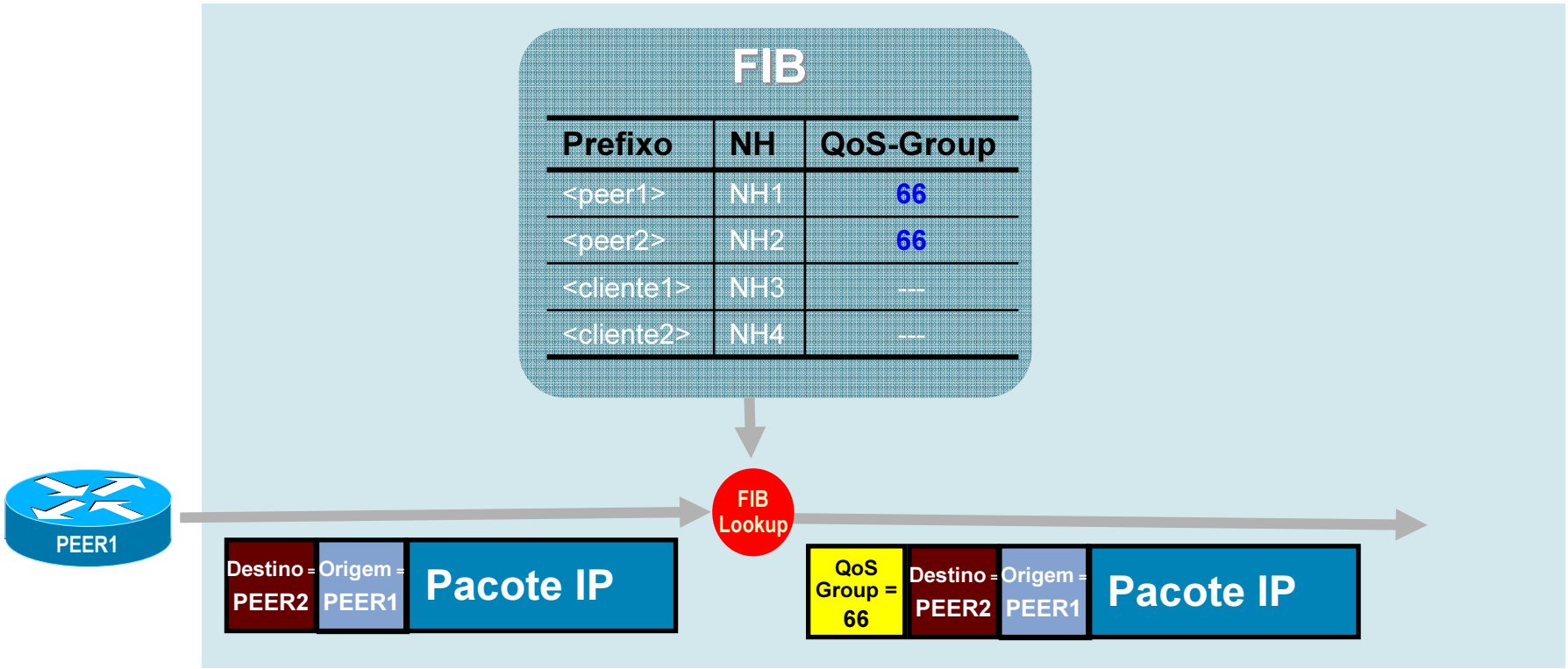
(1) Associação de TAG na FIB via BGP




```
!
ip bgp-community new-format
router bgp <AS>
  :
  table-map set-prefix-type
```

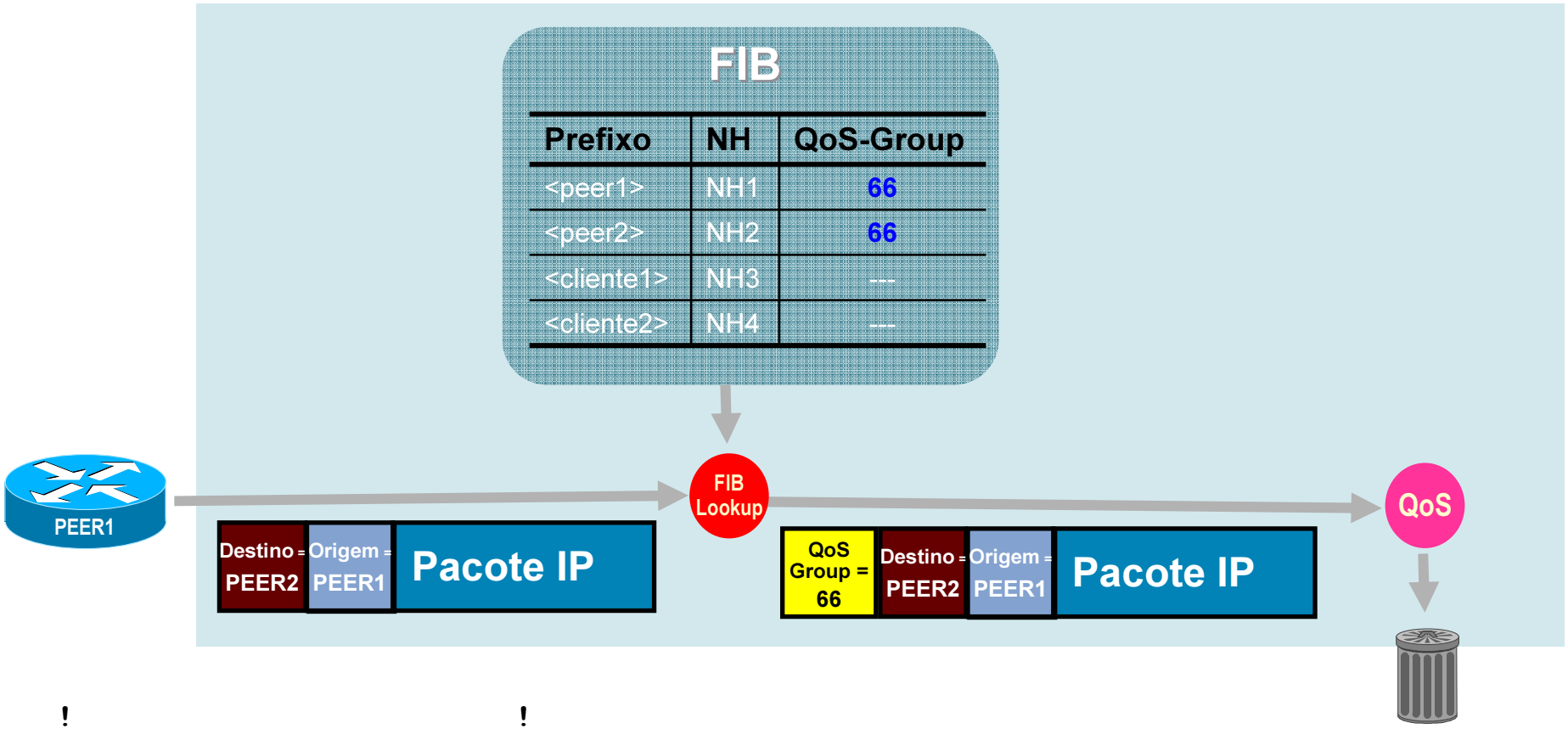
```
!
ip community-list 1 permit <AS>:66
!
route-map set-prefix-type permit 10
  match community 1
  set ip qos-group 66
!
```

(2) Associação de TAG a pacote via QPPB




```
!
interface <ID da interface com Peer1>
  description Interface conectada ao Peer1
  bgp-policy destination ip-qos-map
```

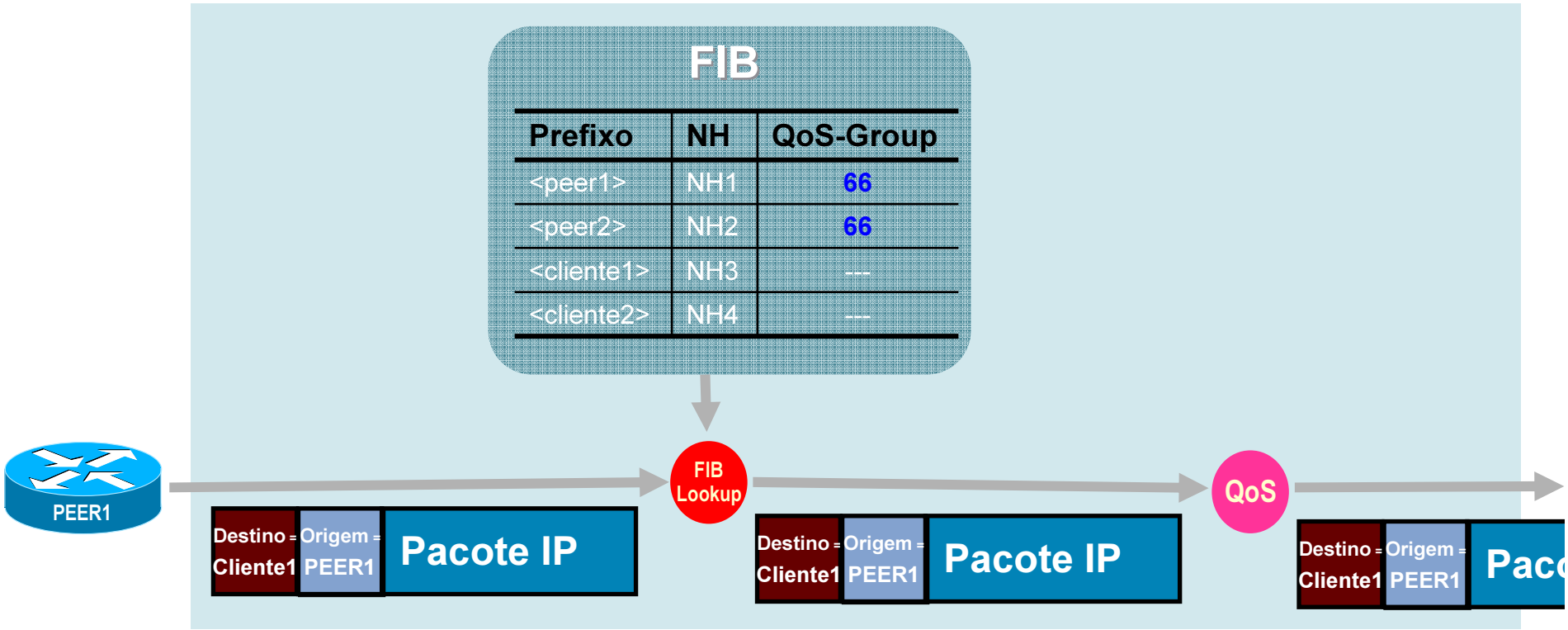
(3) Classificação e descarte de pacote via QoS




```
!
class-map peer-prefix
  match qos-group 66
!
policy peer-in
  class peer-prefix
    drop
```

```
!
interface <ID da interface com Peer1>
  description Interface conectada ao Peer1
  bgp-policy destination ip-qos-map
  service-policy input peer-in
```

(3) Encaminhamento de Pacotes para Clientes




```
!
class-map peer-prefix
  match qos-group 66
!
policy peer-in
  class peer-prefix
    drop
```

```
!
interface <ID da interface com Peer1>
  description Interface conectada ao Peer1
  bgp-policy destination ip-qos-map
  service-policy input peer-in
```

Benefícios da Técnica Proposta

- **Protege contra violações da política de *peering* BGP**
  - Tráfego recebido de um *peer* e destinado a outro *peer* (local ou remoto) é descartado
  - Tráfego recebido de um *peer* e destinado a um cliente é encaminhado normalmente
- **Facilidade operacional**
  - Não são necessárias listas de acesso
  - Associação de TAG na FIB (prefixos de *peers* versus prefixos de clientes) é possível através de política BGP padrão
  - Mudanças na política BGP são refletidas automaticamente no *data plane*
  - Política QoS permite monitoração e registro de violações da política de *peering*
- **Técnica complementa outras aplicações do plano de controle BGP como RTBH**

Q&A

Configuração Juniper
1 – Definição do *destination-class* baseado no BGP

```
routing-options {
        forwarding-table {
            export set-destination-class;
        }
    }
    policy-options {
        policy-statement set-destination-class {
            term 1 {
                from community low-priority-traffic;
                then destination-class dcu-1;
            }
            term 2 {
                then accept;
            }
        }
        community low-priority-traffic members 100:1000;
```

Configuração Juniper
2 – Classificação CoS baseado no *destination-class*

```
interfaces {
    so-0/1/0 {
        unit 0 {
            family inet {
                filter {
                    output differentiate-forwarding-class;
                }
                address 1.1.1.1/30;
            }
        }
    }
}
firewall {
    filter differentiate-forwarding-class {
        term low-priority-traffic {
            from {
                destination-class dcu-1;
            }
            then {
                loss-priority high;
                forwarding-class low-priority;
            }
        }
        term others {
            then accept;
        }
    }
}
```

Configuração Juniper
3 – Descarte baseado no CoS

```
class-of-service {
    forwarding-classes {
        queue 0 best-effort;
        queue 1 low-priority;
        queue 3 network-control;
    }
    interfaces {
        so-0/1/0 {
            scheduler-map juniper;
        }
    }
    scheduler-maps {
        juniper {
            forwarding-class best-effort scheduler 95-95-high;
            forwarding-class low-priority scheduler 0-0-low;
            forwarding-class network-control scheduler 5-5-stright-high;
        }
    }
    schedulers {
        5-5-stright-high {
            buffer-size percent 5;
            priority strict-high;
        }
        0-0-low {
            buffer-size percent 0;
            priority low;
        }
        95-95-high {
            transmit-rate percent 95;
            buffer-size percent 95;
            priority high;
        }
    }
}
```