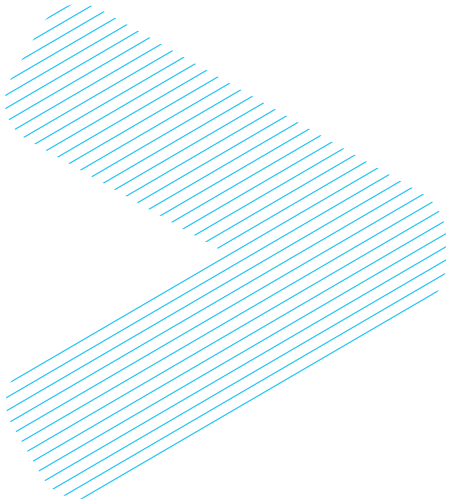
Protect your peering edge - review

Riaan Vos
riaan.vos@is.co.za
Internet Solutions

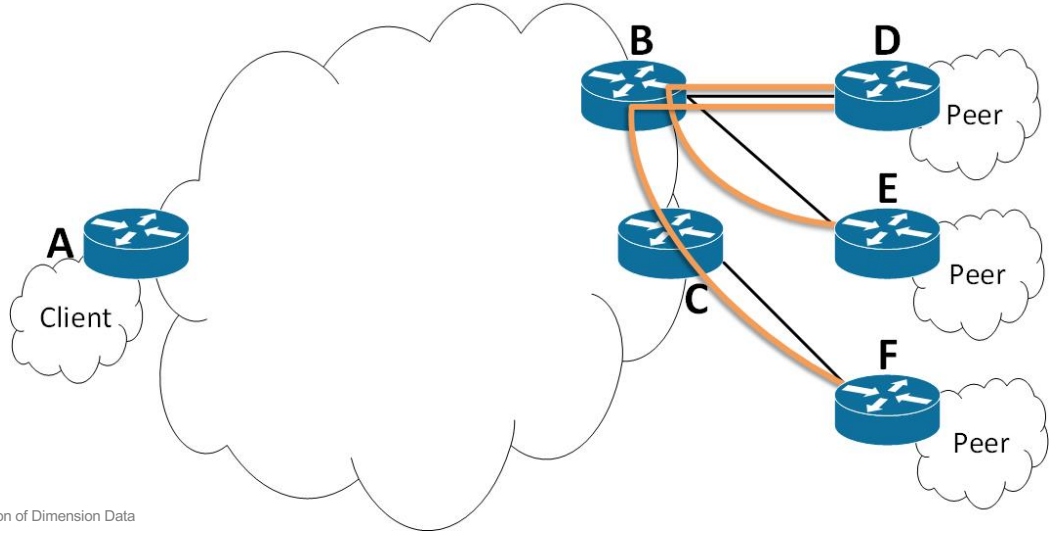
TABLE OF **CONTENTS**



Protect your peering edge - review

Why?

- You will receive traffic not destined for you or your clients.
- To limit the risk of becoming an unintended transit provider.



Protect your peering edge - review

Option 1: “First steps”

- No valid 0/0.
- Partial advertisements from RRs.
- iACLs.
- Split transit and peering layers.

Protect your peering edge - review

Advantages of this approach?

- ✓ Easy to implement.
- ✓ Covering the majority of cases.

Protect your peering edge - review

Disadvantages of this approach?

- ✕ Manual approach.
- ✕ Error prune.
- ✕ No multiservice edge approach.
- ✕ “Trickier” relationships.

Protect your peering edge - review

Option 2: QPPB (QoS Policy Propagation via BGP)

- Cisco, Huawei: QPPB.
- Juniper: SCU/DCU.
- Alcatel, Nokia: QPPB.

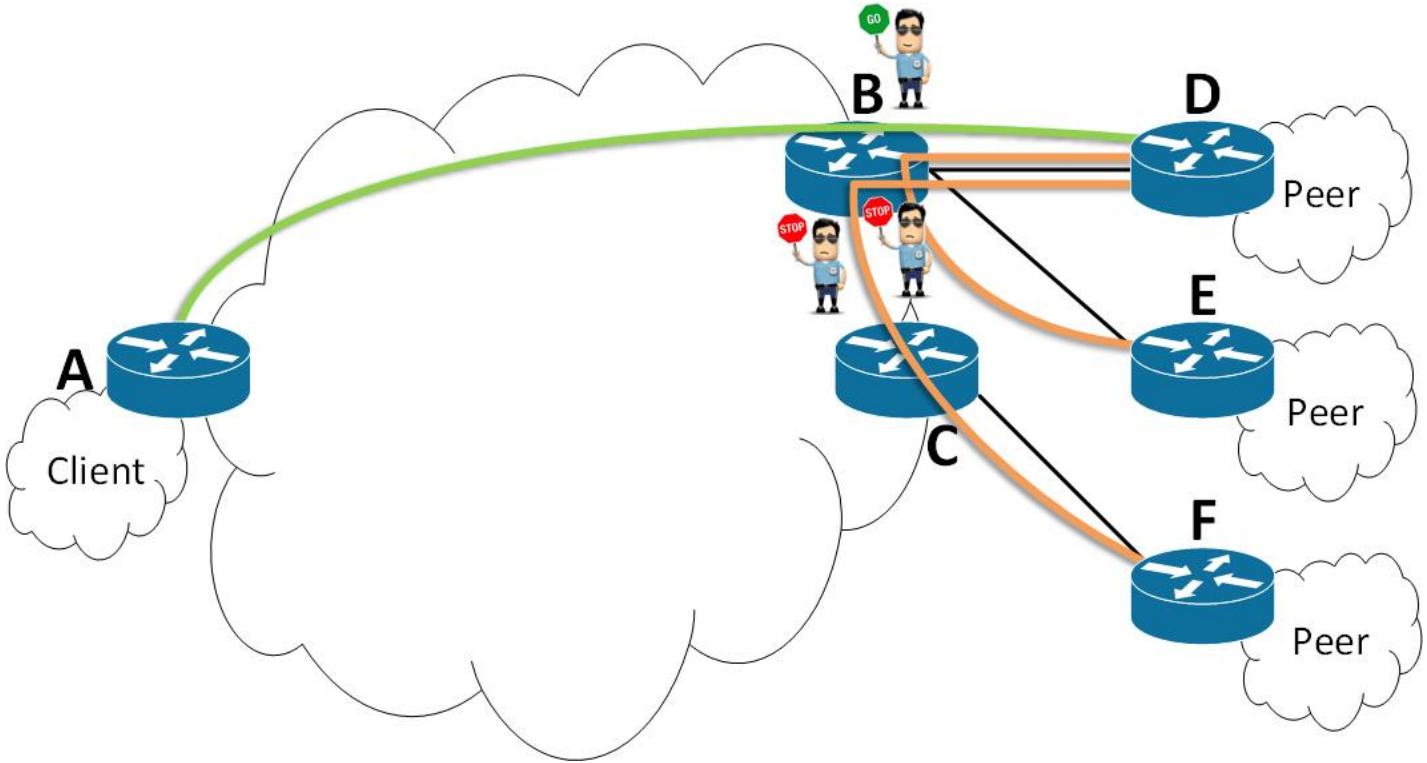
Protect your peering edge - review

What is QPPB?

- QPPB: QoS Policy Propagation via BGP.
- BGP advertisement classification.
- The BGP advertisement inherits the classification of the associated BGP session.
- **Any ingress packet will get the same classification as the destination.**

Protect your peering edge - review

What is QPPB? (2)



Protect your peering edge - review

How does QPPB work?

Step 1: Tag peer prefixes uniquely within BGP and FIB tables.

- Mark peer prefixes with community attribute (P) and tag (P).
- Mark transit prefixes with community attribute (P) and tag (P).
- Mark client prefixes with community attribute (C) and tag (C).

```
route-policy qosgroup_map
if community matches-any P-comm
then
set qos-group 7
else
set qos-group 1
endif
end-policy
!
router bgp <your ASN>
address-family ipv4 unicast
table-policy qosgroup_map
```

Protect your peering edge - review

How does QPPB work? (2)

Step 2: Tag external packets at peering locations based upon longest prefix matching within FIB.

- Received from peer/transit and destined to peer/transit: tag as (P).
- Received from peer/transit and destined to client: tag as (C).

int gi0/0/0
ipv4 bgp policy propagation input qos-group destination

Protect your peering edge - review

How does QPPB work? (3)

Step 3: Packet classification via MQC.

```
class-map match-any EXT
 match qos-group 7
 end-class-map
!
policy-map qppb_set_dscp
 class EXT
  police rate percent 1
   conform-action drop
  !
 class class-default
  set dscp af11
 end-policy-map
!
int gi0/0/0
service-policy input qppb_set_dscp
```

Protect your peering edge - review

Advantages of QPPB?

- ✓ Sustainable option.
- ✓ Multiservice functionality can be done.
- ✓ No need to do filtering on RRes.

Protect your peering edge - review

Disadvantages of QPPB?

- Difficult to understand.
- Still prune to configuration errors (”human factor”):
  - Blackholing.
  - Missing enforcement.
- Only granular to a BGP level.

Protect your peering edge - review

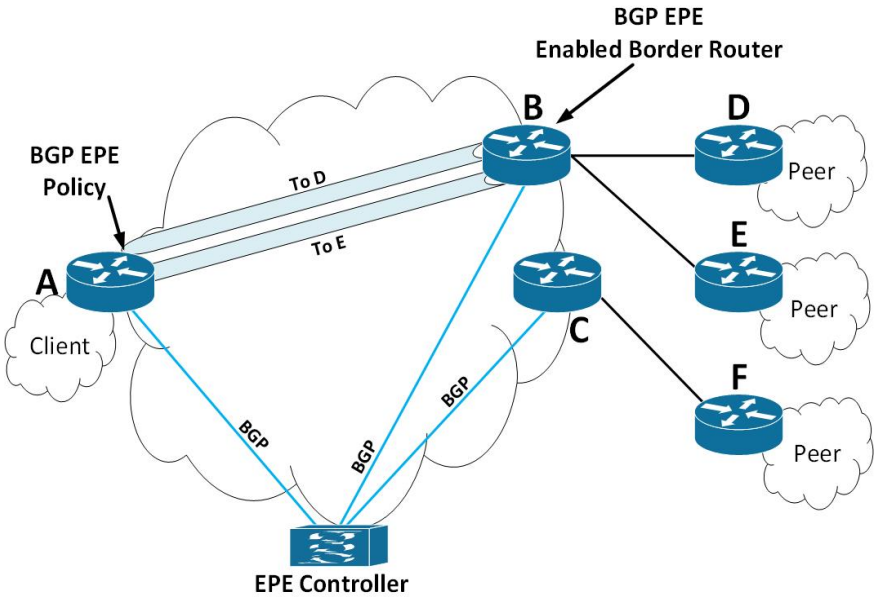
Option 3: BGP EPE

- Based on a Segment Routing (SR) implementation.
- SR will bring you benefits such as the following:
  - Less protocols.
  - Programmability.
  - Scaling.
  - Better granular control.
- Tutorials on SR: http://www.segment-routing.net/tutorials/

Protect your peering edge - review

BGP EPE (Egress Peer Engineering)

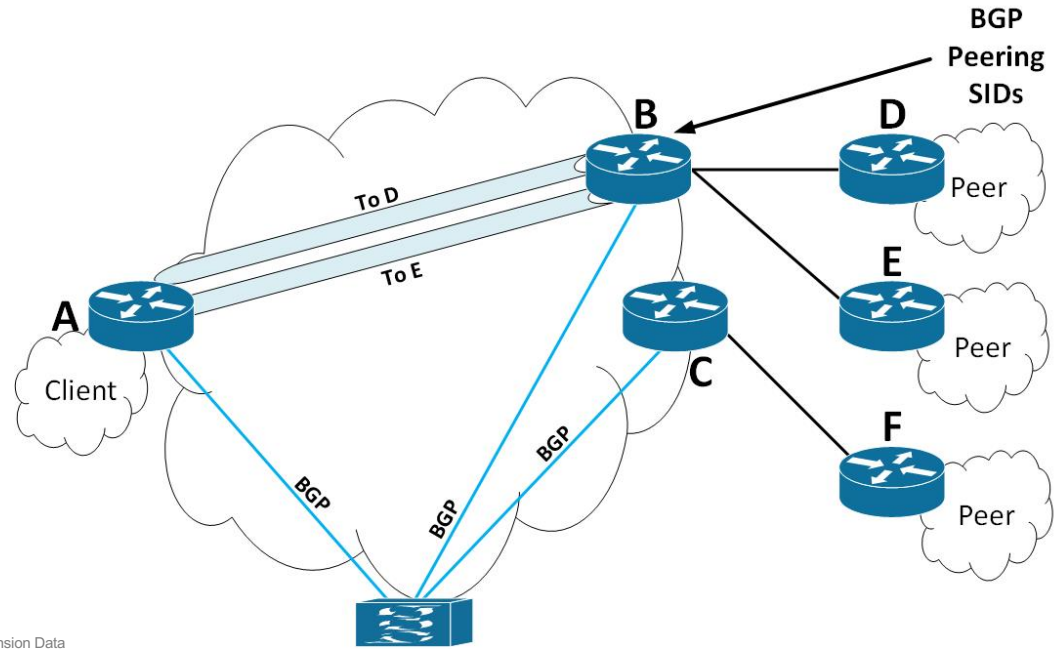
- Problem statement (RFC7855): “A centralized controller should instruct ingress PE to use a specific egress PE.”
- ”**How To**”: draft-ietf-spring-segment-routing-central-epe.



Protect your peering edge - review

BGP EPE (2)

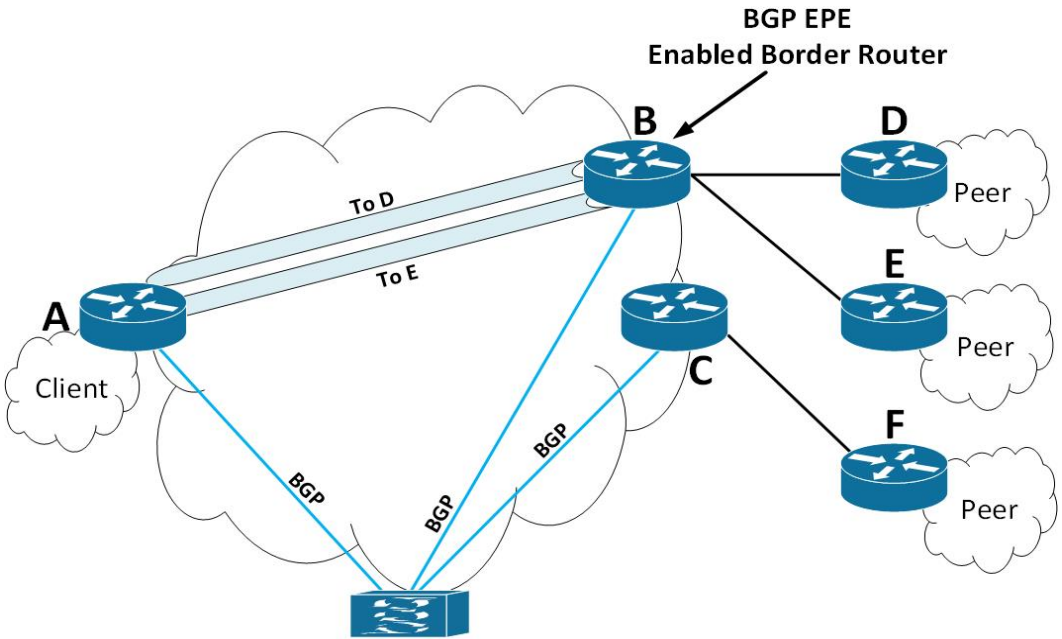
- BGP Peering SIDs.
  - Locally assigned labels to identify eBGP peers.



Protect your peering edge - review

BGP EPE (3)

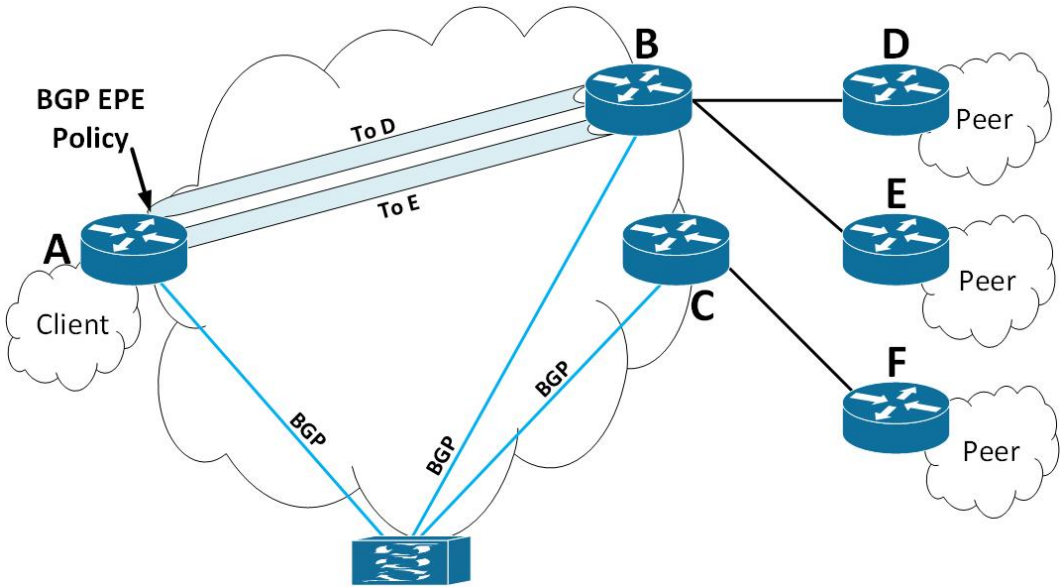
- BGP EPE enabled border routers.
  - Border device compiling the BGP Peering SIDs.



Protect your peering edge - review

BGP EPE (4)

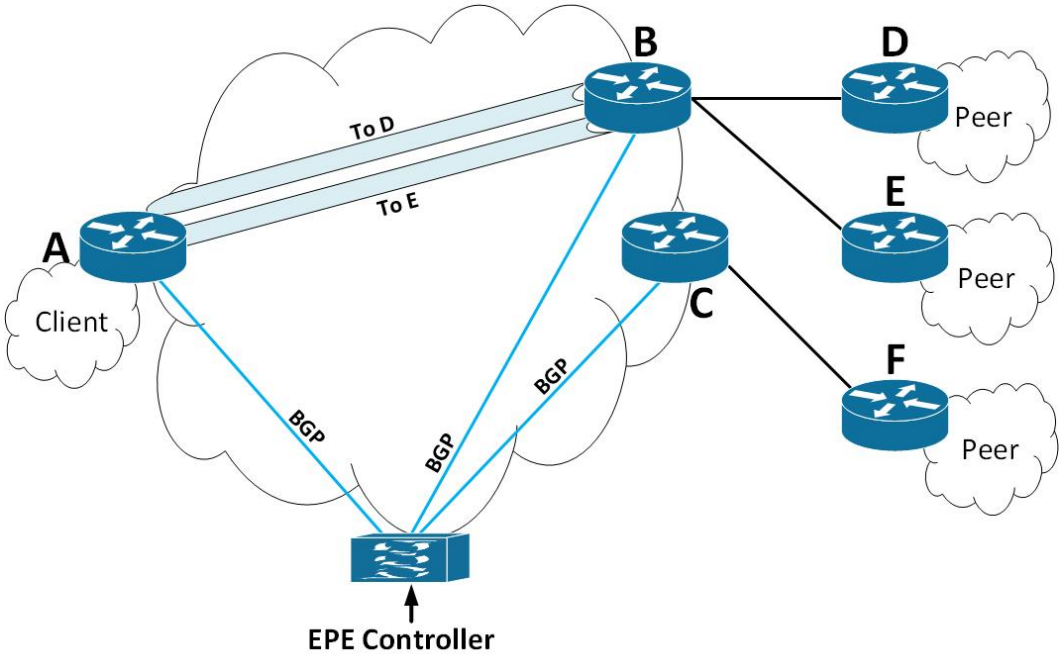
- BGP EPE ingress policy.
  - Program path to BGP EPE edge router.



Protect your peering edge - review

BGP EPE (5)

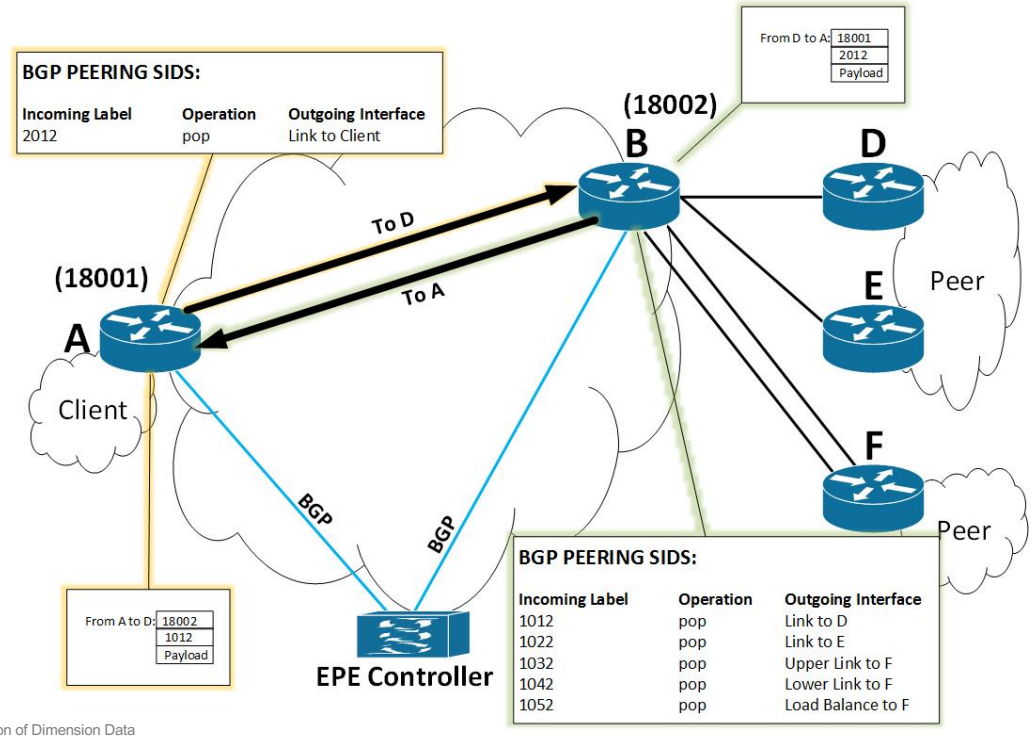
- BGP EPE Controller.
  - PCE based.



Protect your peering edge - review

BGP EPE (6)

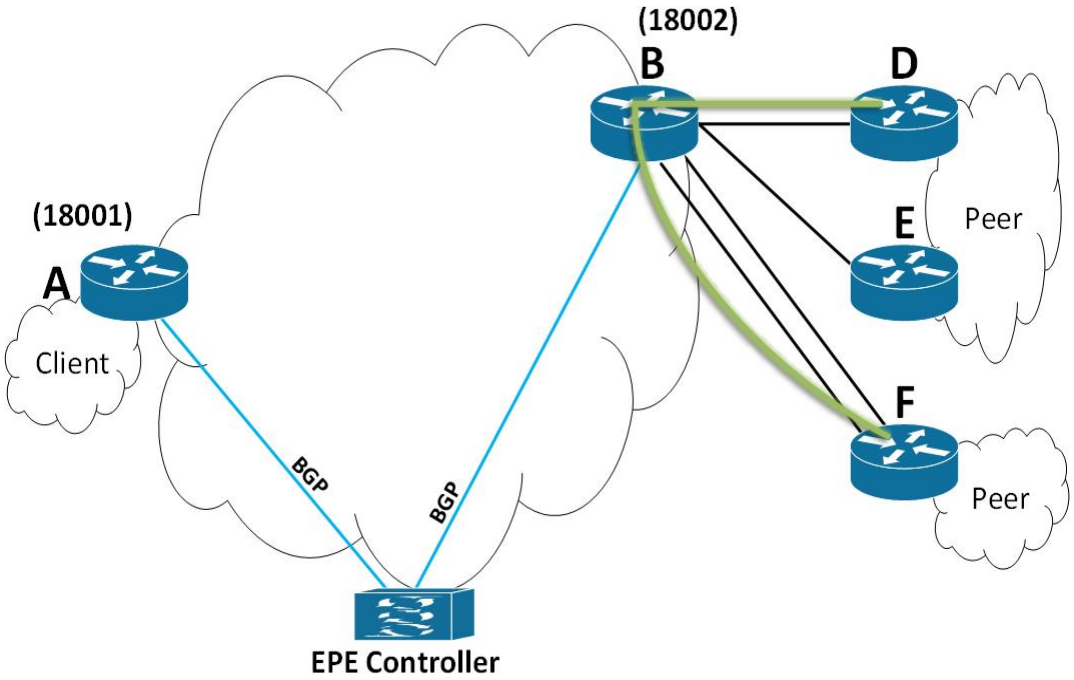
- Example 1: Traffic from A to D.



Protect your peering edge - review

BGP EPE (7)

- Example 2: Traffic from D to F.



Protect your peering edge - review

Advantages of BGP EPE

- ✓ No longer solely dependent on the classification of BGP.
- ✓ Controller is responsible for classification.
- ✓ Flexibility to override general rules.

Protect your peering edge - review

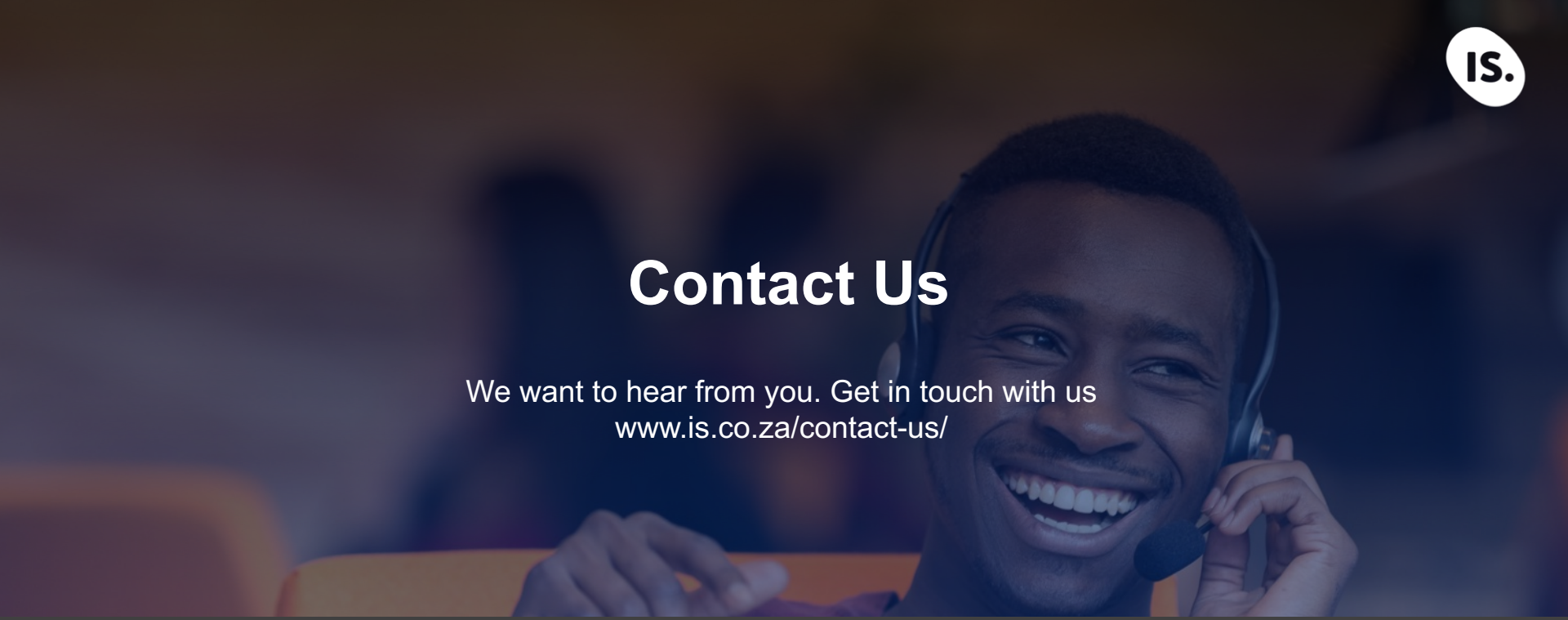
Disadvantages of BGP EPE

- Does need a controller.
- Complexity is moved from network to a controller.
- SR needs to be in use by operator.
- Only limited efficiency (i.e. when labels can be imposed).

Protect your peering edge - review

Summary

- BGP EPE:
  - More suitable for typical traffic steering implementation.
- QPPB:
  - Currently the best option for protecting your peering edge.



Contact Us

We want to hear from you. Get in touch with us
www.is.co.za/contact-us/

PHONE
+2711 575 1000

EMAIL
riaan.vos@is.co.za

WEBSITE
www.is.co.za