Making BGP filtering a habit: Impact on policies

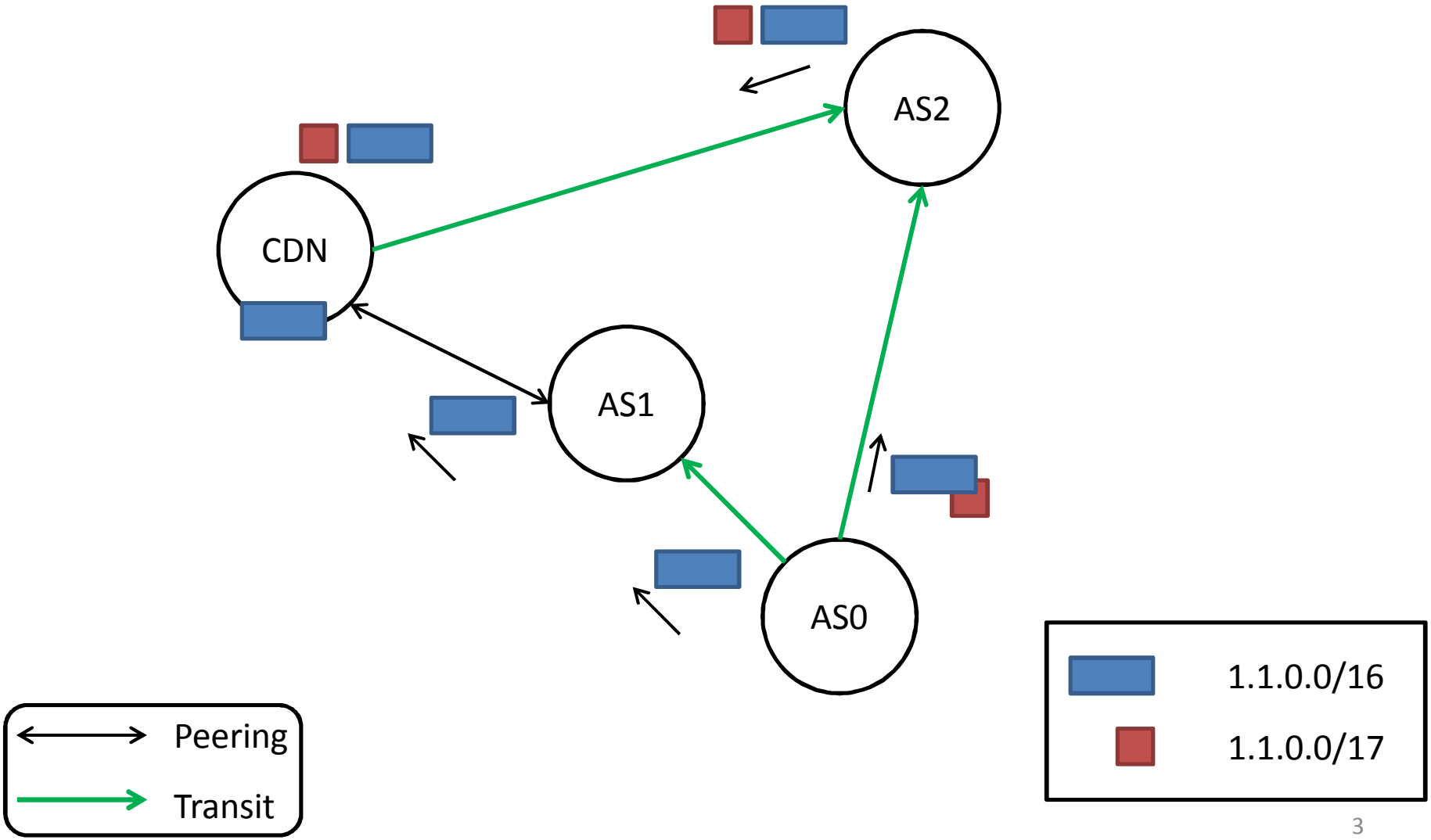
JuanCamilo.Cardona@imdea.org
Pierre.Francois@imdea.org
IMDEA Networks

draft-cardona-filtering-threats-01

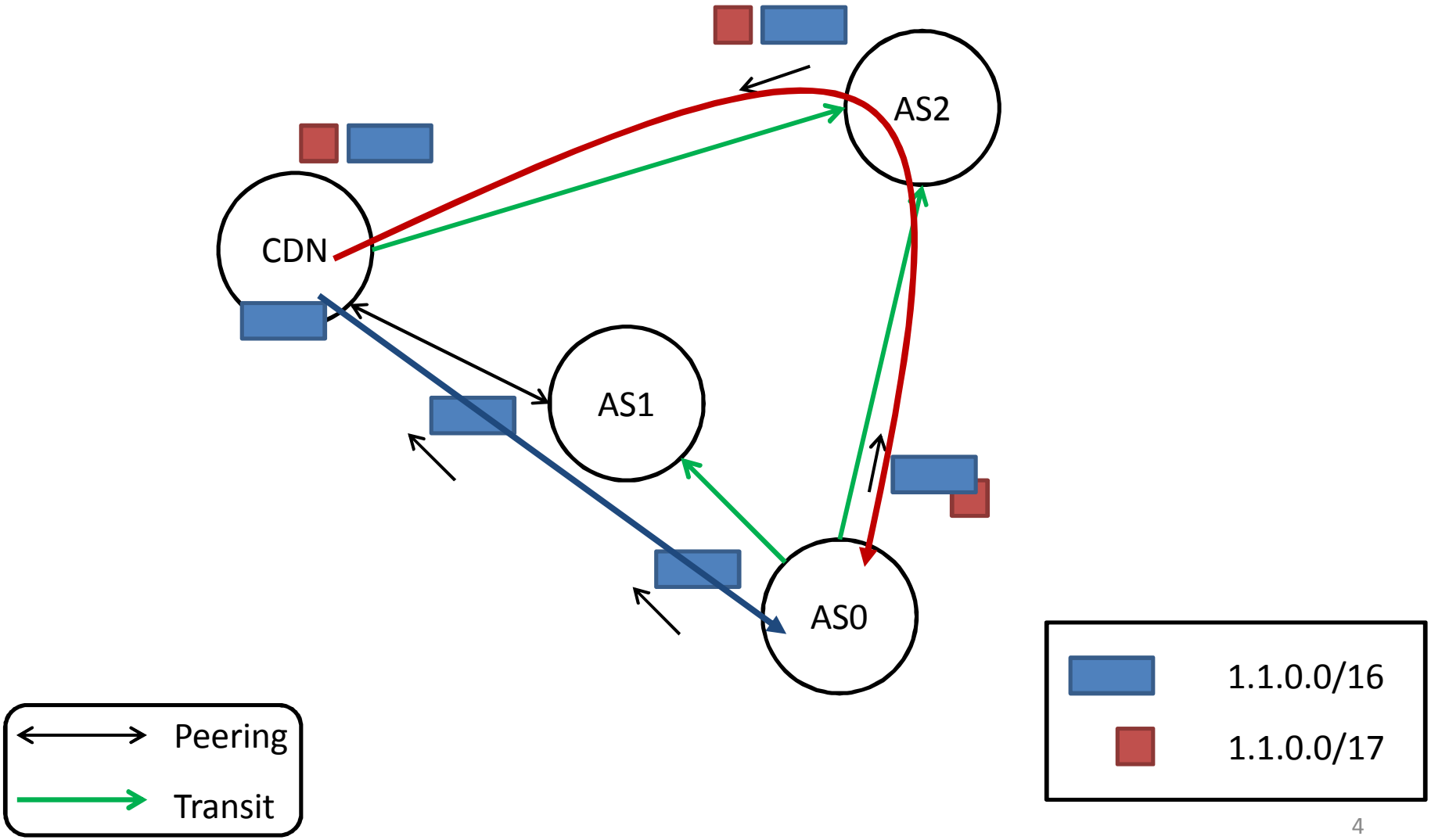
Motivation
Filtering overlapping prefixes

- A lot of overlapping prefixes in BGP
- Traffic enforced over the overlapping prefix
- Overlapping prefixes can be partially propagated
  - *“They make me forward to my transit instead of my peer/customer”*
  - *“I’m loosing money due to their games”*
- Natural reaction: Filter them

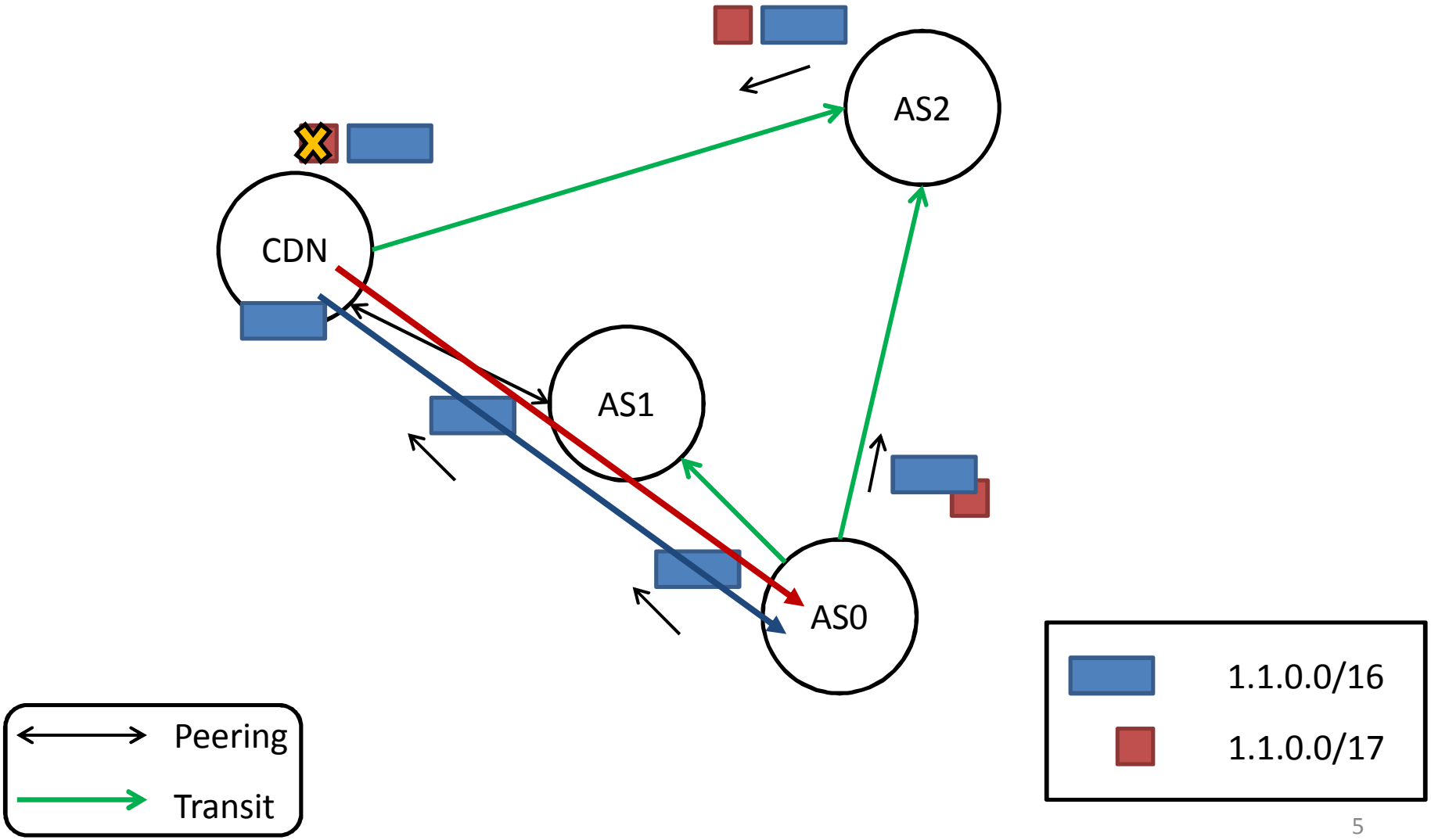
Example (local filtering)



Example (local filtering)



Example (local filtering)

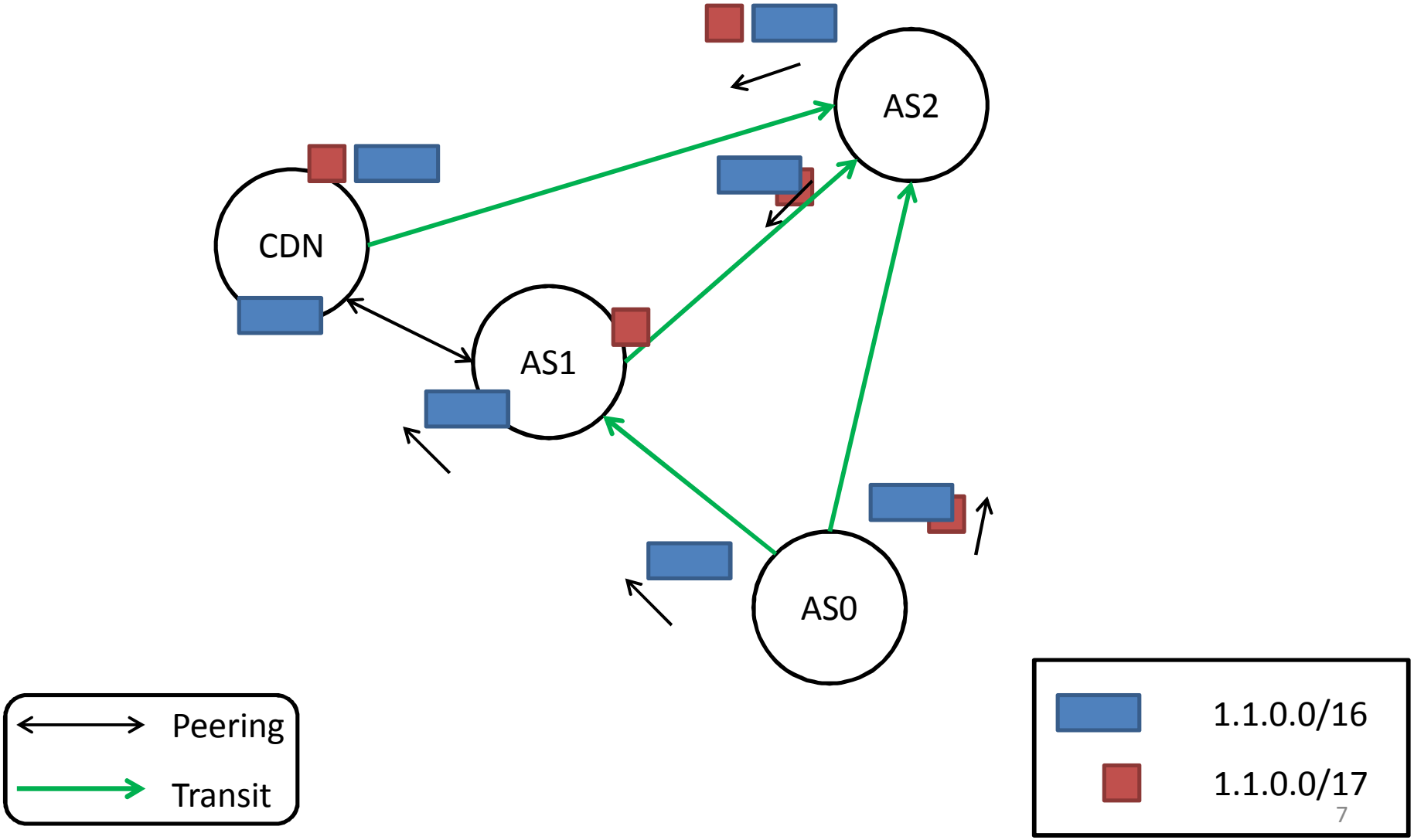


Motivation

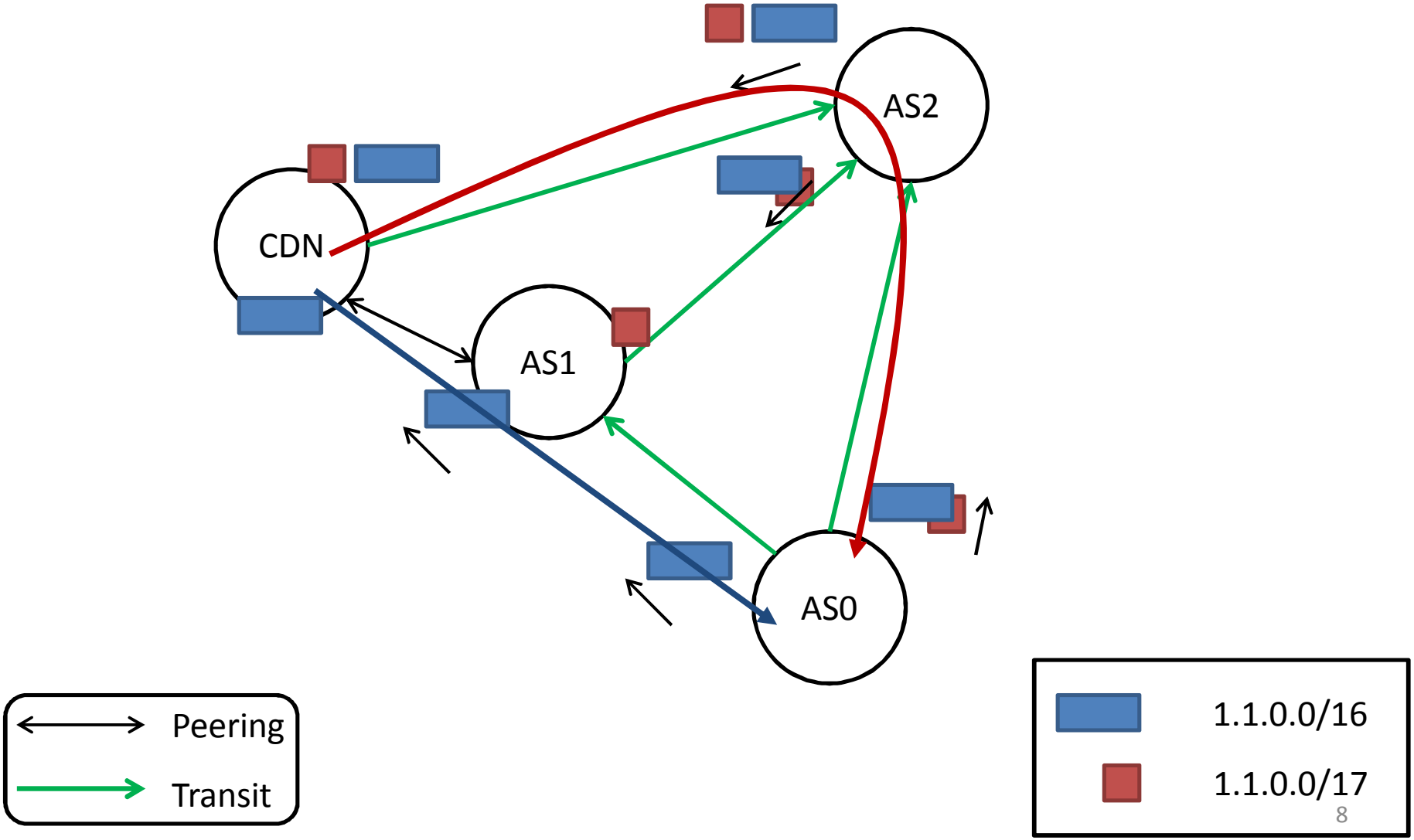
- ISPs have announced this practice
  - See INIT7 talk at RIPE63
- Requests for automatic filtering mechanisms

- Blindly filtering can affect neighboring ASes

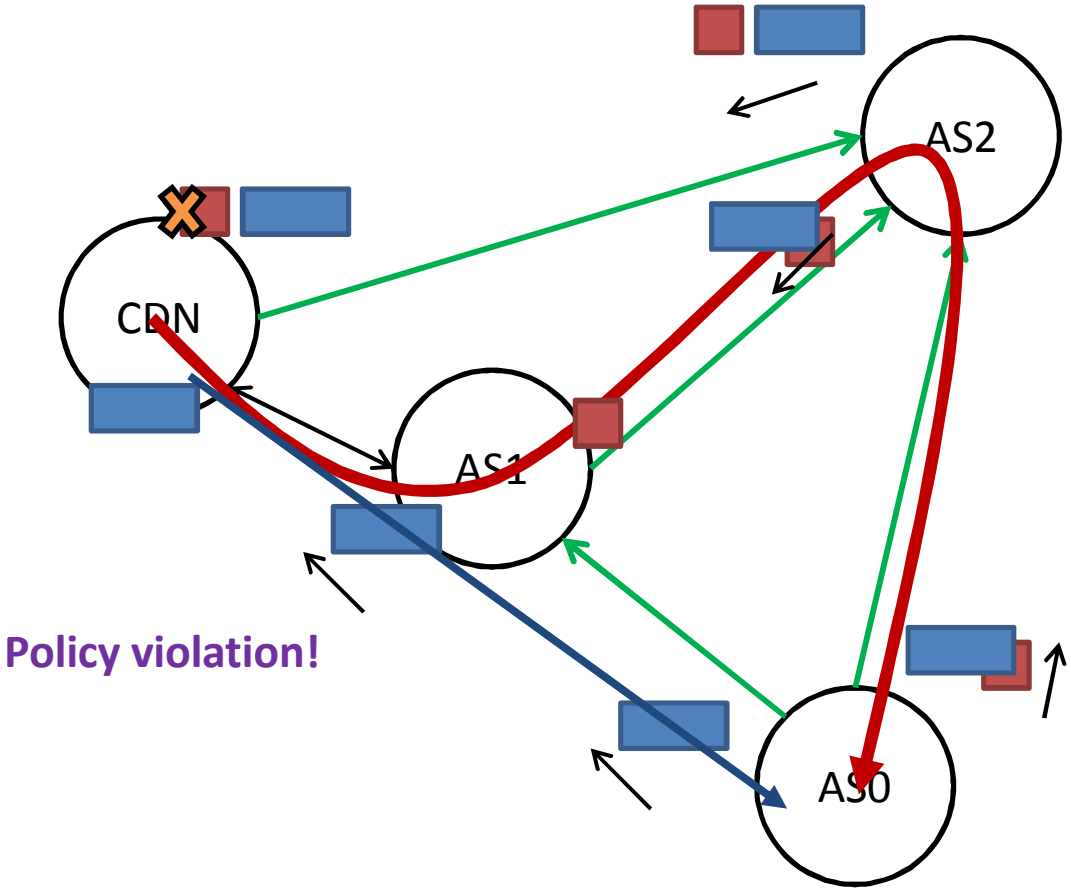
Local filtering
Policy violation

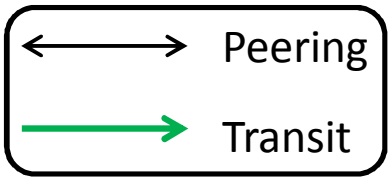


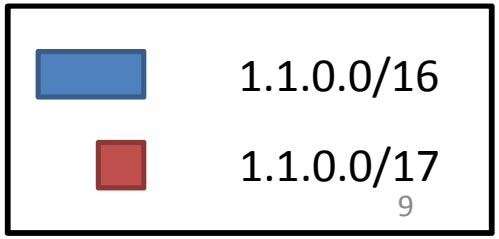
Local filtering
Policy violation



Local filtering
Policy violation







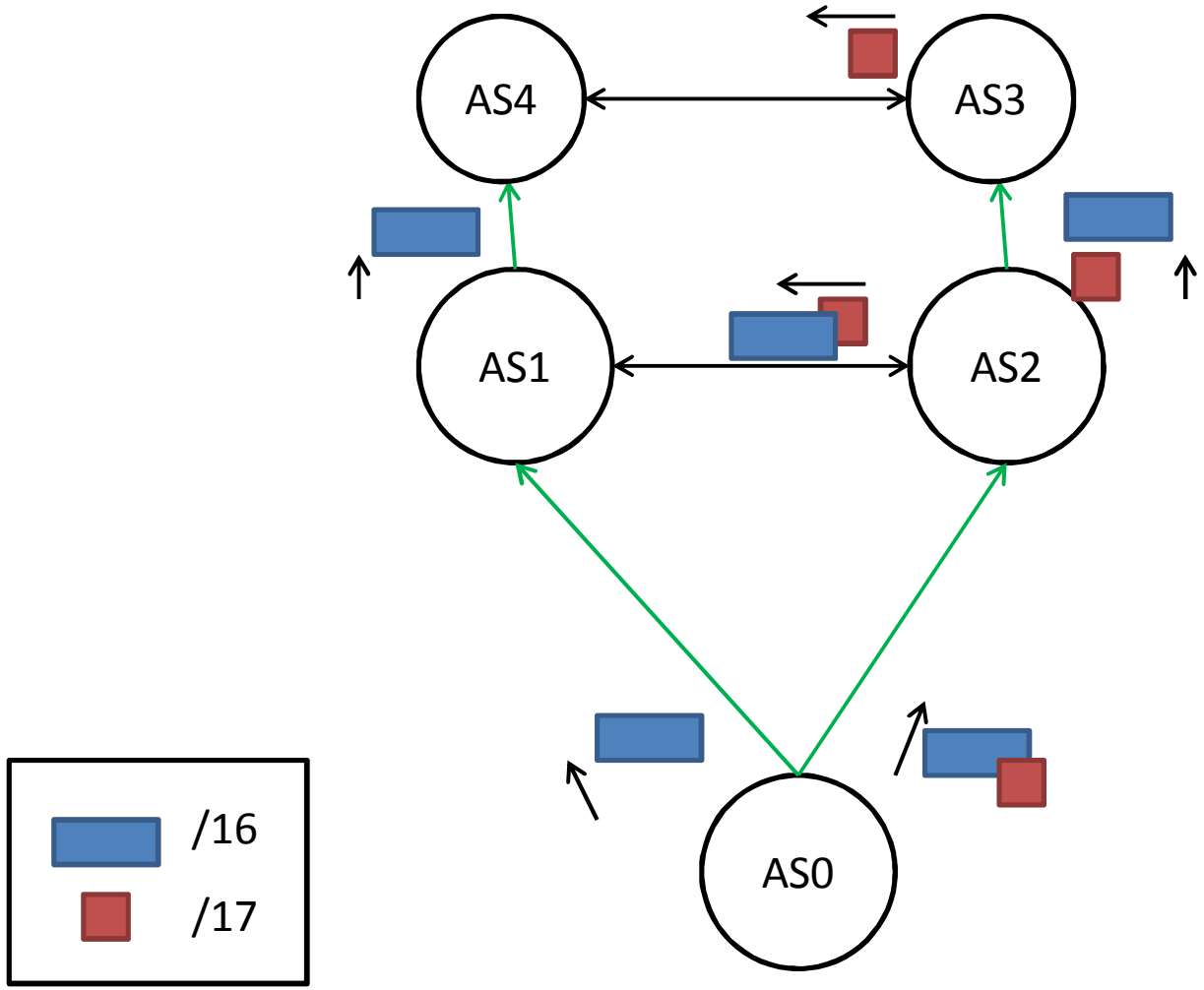
Local filtering
Conclusions

- Local filtering can be beneficial for you
  - But can violate the policies of neighboring ASes
  - It is impossible for the “culprit” to distinguish among the cases without gathering external data
- A similar effect can be obtained when remote filtering is performed

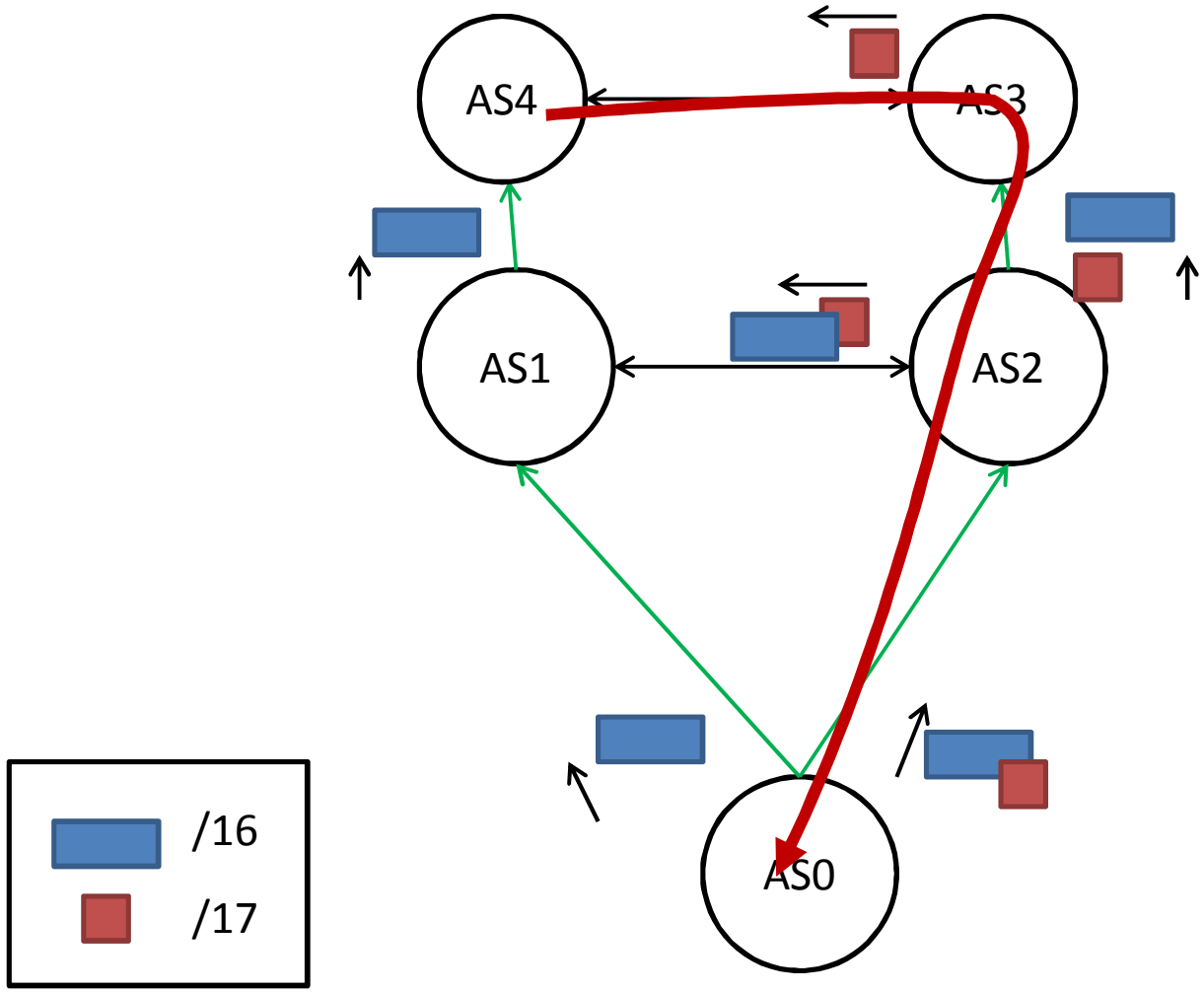
Remote triggered filtering Background

- Some large ISPs offer remote route propagation control using BGP communities

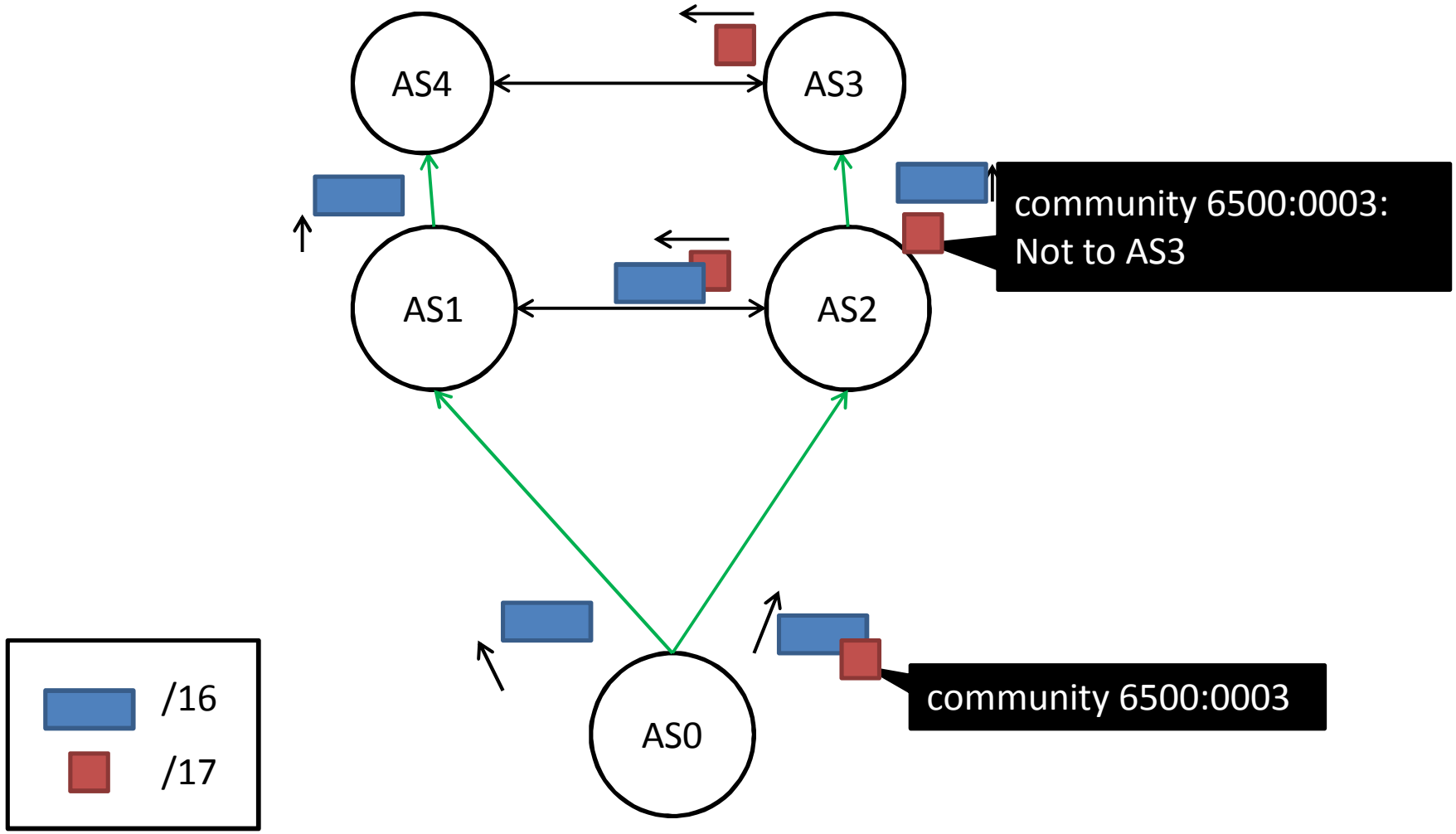
Remote triggered filtering



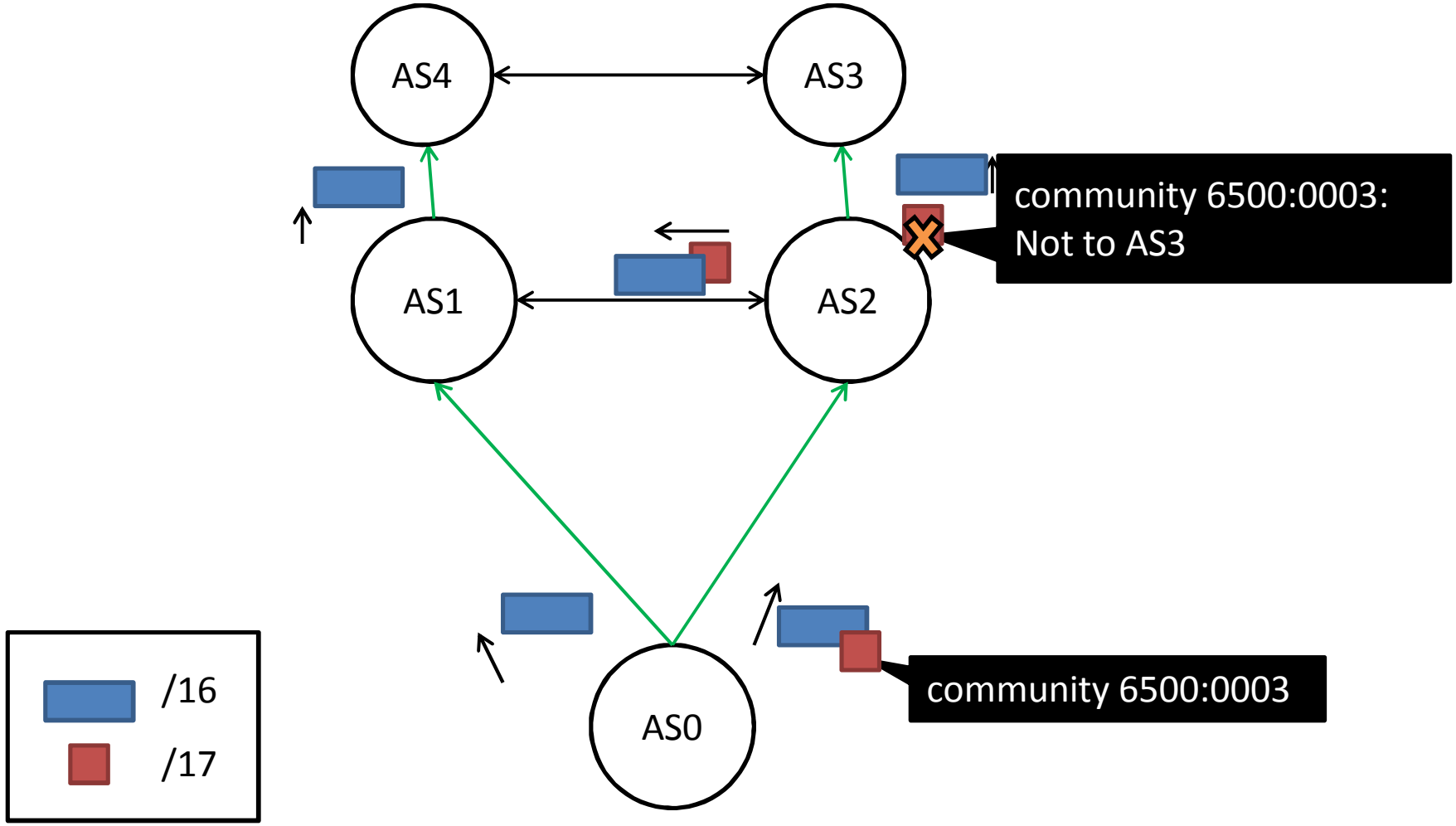
Remote triggered filtering



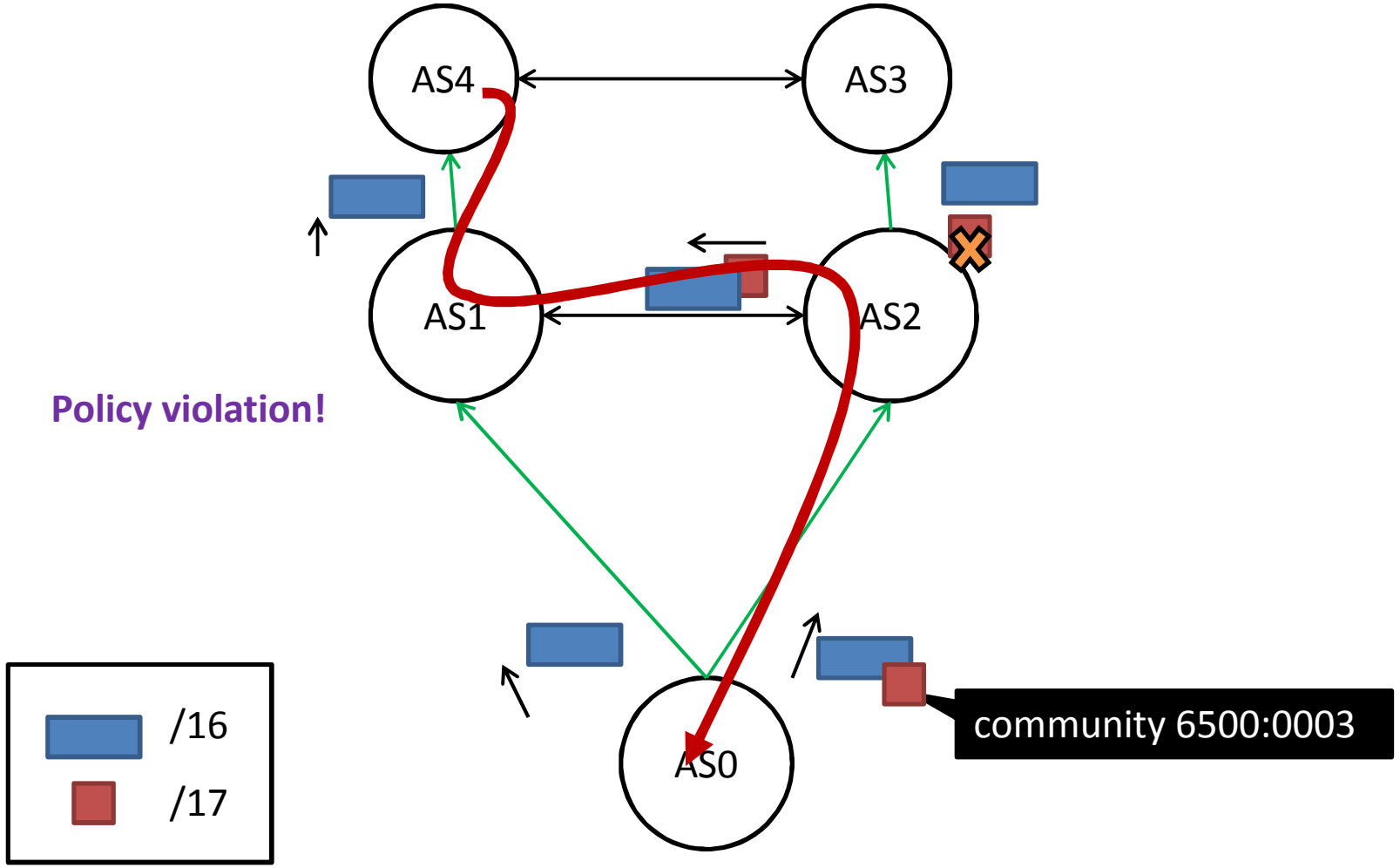
Remote triggered filtering



Remote triggered filtering



Remote triggered filtering



Impact of filtering

- Filtering can be useful for an ISP
  - We are not questioning this
- Might violate policies of neighboring ASes
- It should be done with care
- Not only for those who filter:
  - Contracts should cover such considerations
  - Detecting violations is not simple

What can ISPs do?

- How to detect a Policy violation:
  - Monitoring traffic
  - Analyze BGP data
- How to solve it:
  - Filter out traffic
  - Forward differently
  - Human interaction

Conclusion

- Filtering of overlapping prefixes can do harm
- It’s needed and used
- Let’s be aware and conscious about it

Next steps

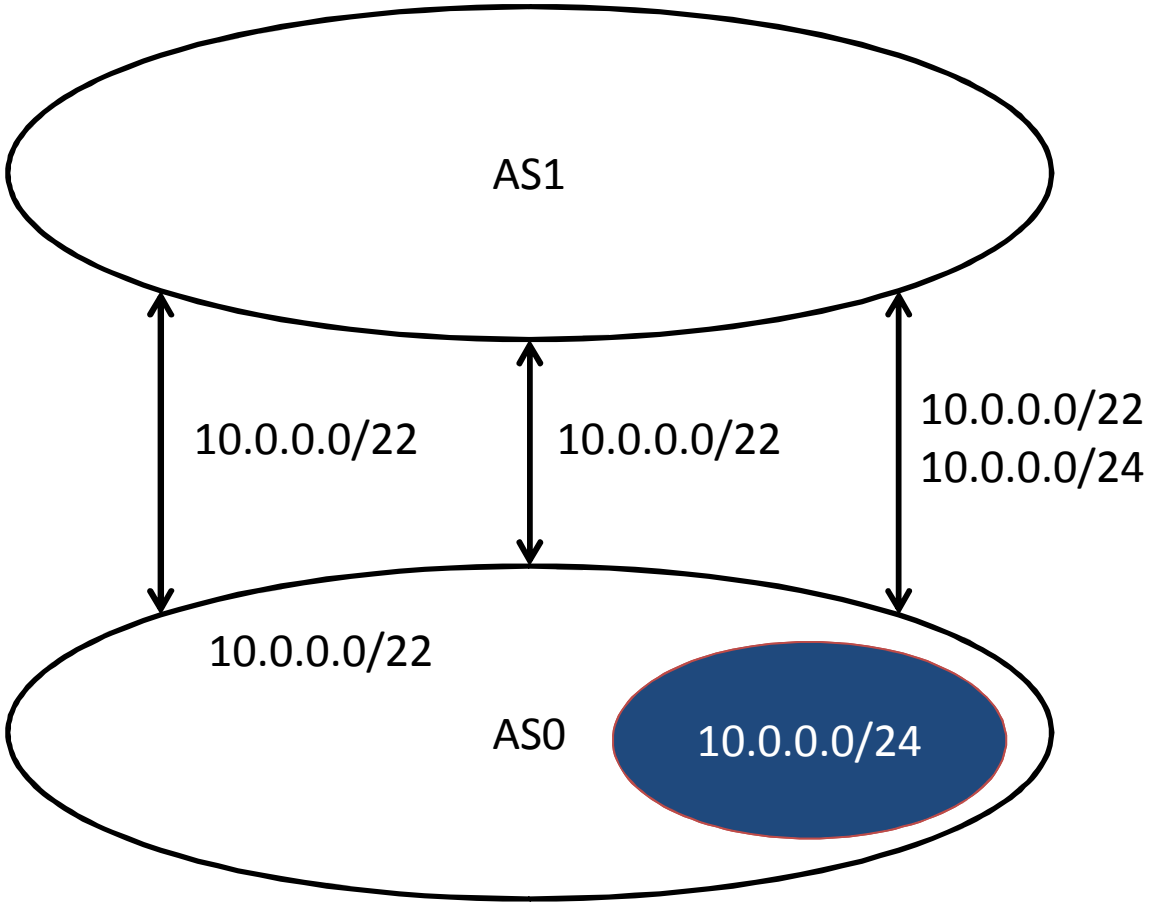
- Consider feedback
- WG DOC?

Questions?

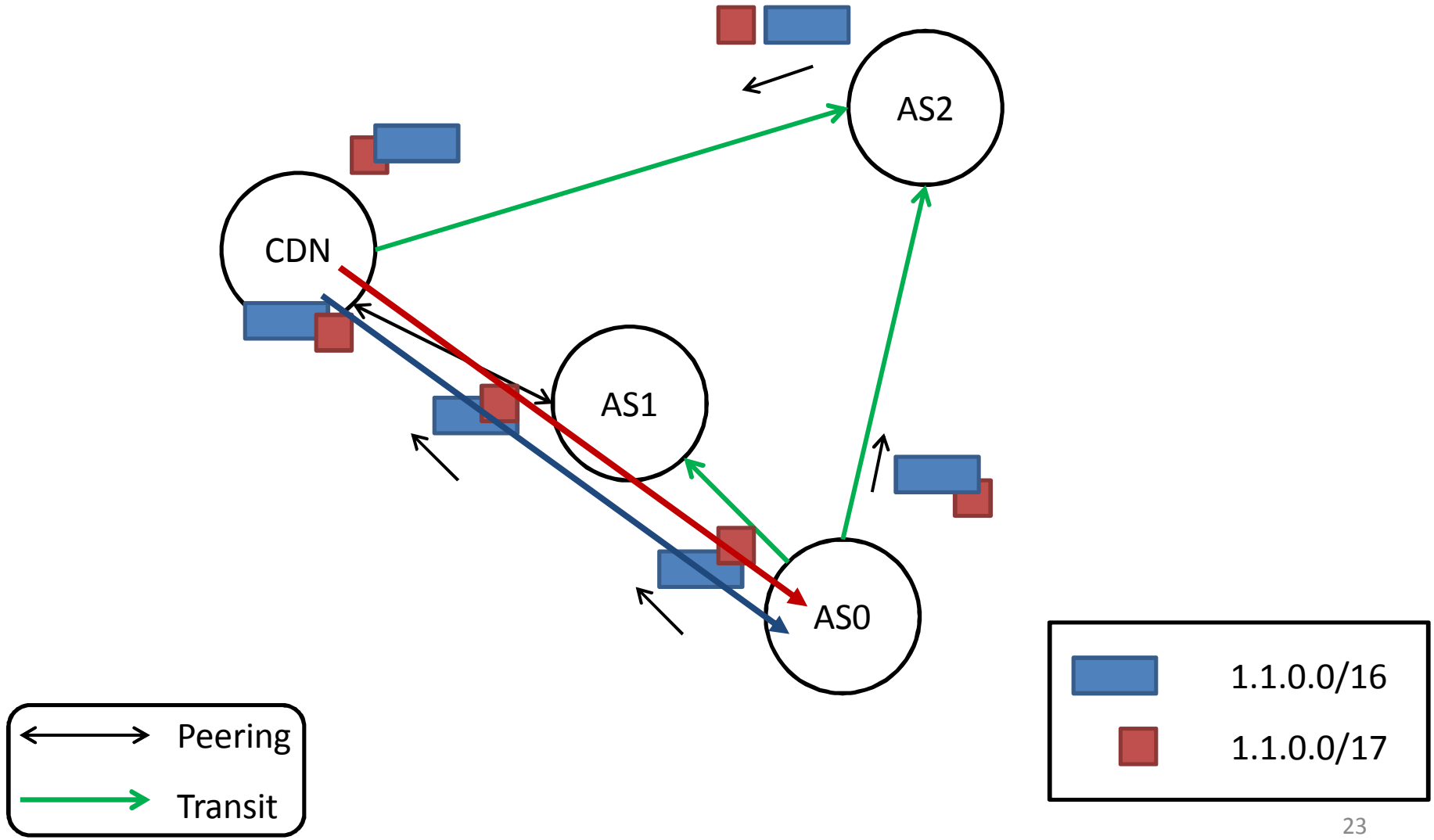
Juan Camilo Cardona
Pierre Francois
IMDEA Networks

draft-cardona-filtering-threats-01

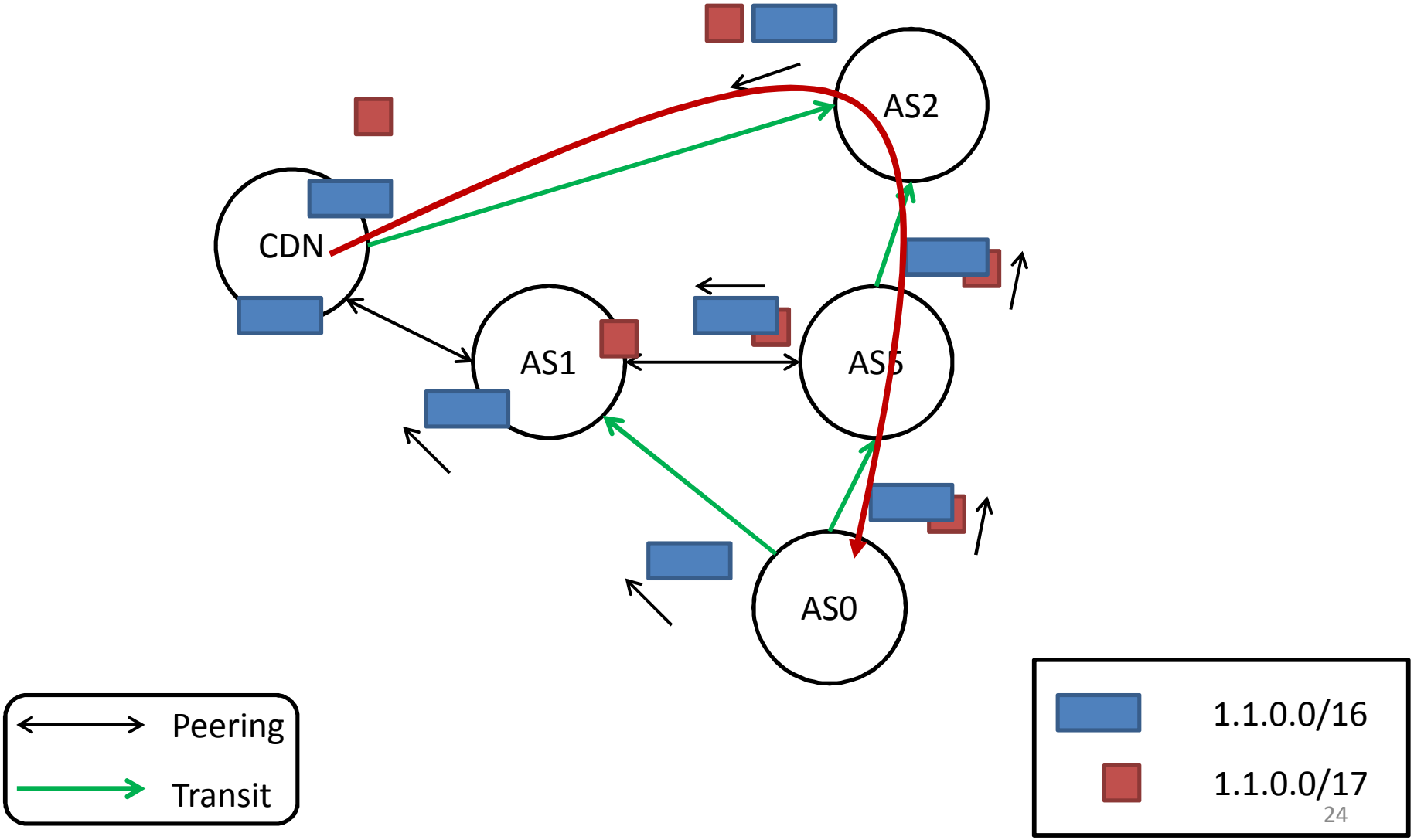
Motivation & Background
Local filtering to enforce policy



Motivation & Background
Local filtering to reduce FIB size



Local filtering
From Peer to Peer



Local filtering
From Peer to Peer