

ASPA and Roles

What's up with that?

@antonis@mastodon.social

RPKI

Resource Public Key Infrastructure

ROA

2a0d:3dc0::/29-29 from AS4601

2a0d:3dc0::/32-48 from AS210312

193.5.16.0/23-32 from AS0

2a0d:3dc0::/29 from AS4601

2a0d:3dc0::/32 from AS210312

193.5.16.0/23 from AS0



ROV

147.189.216.0/22 via 2001:7f8:116::c6b5:1

AS Path: 29529 215405

147.189.216.0/22 via 2001:7f8:116::c6b5:1

AS Path: 29529 215405

147.189.216.0/22 from AS4601

147.189.216.0/22 via 2001:7f8:116::c6b5:1

AS Path: 29529 215405

147.189.216.0/22 from AS4601

147.189.216.0/22 via 2001:7f8:116::c6b5:1

AS Path: 29529 **215405**

147.189.216.0/22 from AS4601

147.189.216.0/22 via 2001:7f8:116::c6b5:1

AS Path: 29529 215405 **4601**

147.189.216.0/22 from AS4601

147.189.216.0/22 via 2001:7f8:116::c6b5:1

AS Path: 29529 215405 **4601**

ASPA

AS4601 providers are AS8298, AS1299

AS8298 providers are AS25091

AS1299 providers are AS0

AS4601 providers are AS8298, AS1299

AS8298 providers are AS25091

AS1299 providers are AS0



147.189.216.0/22 from AS4601

147.189.216.0/22 via 2001:7f8:116::c6b5:1

AS Path: 29529 215405 **4601**

147.189.216.0/22 from AS4601

147.189.216.0/22 via 2001:7f8:116::c6b5:1

AS Path: 29529 **215405** **4601**

AS4601 providers are AS8298

Enhanced Hijack Protection

ASPA

What is ASPA?

ASPA is an emerging standard coming out of the IETF that can help to prevent BGP route leaks, and to a degree improves BGP path security. We recommend to read the documentation below.

[Read the documentation ↗](#)

Watch it explained

We recommend that you watch the presentation given at RIPE 91 before you start.

[Watch the presentation ↗](#)

What providers should I include?

- All your Providers!
- Not your lateral peers
- Unless those peers that can act as your Provider
- Also include non-transparent route servers

Customer ASN	Provider ASNs		
AS4492	AS0	 Edit	 Delete
AS4601	AS8298, AS58115	 Edit	 Delete
AS29529	AS0	 Edit	 Delete
AS210312	AS4601	 Edit	 Delete
AS215405	AS0	 Edit	 Delete
AS219465	AS4492, AS29529, AS215405	 Edit	 Delete

 Edit ASPA



Customer ASN

Provider ASNs

AS4601

AS8298



AS58115



Review

Discard

Who are my providers?

- Everyone who provides you with transit
 - Upstream ISPs (Tier 1, Tier 2, ...)
 - DDoS Mitigation Providers
 - BYOIP Cloud and CDN Providers
- Do NOT add your Peers
 - IXPs, Private Peers, Route Servers
- Do not add your Customers :)

Corner cases?

- For DDoS Mitigation, add your provider(s) in advance
 - Changes in RPKI can take minutes to hour to reach everyone
- Some IXPs are not pure IXPs
 - They provide transit, hide their AS, are not transparent, ...
- Some Peers could also be Providers
 - “Free IPv6 Transit” or pushing your routes to other IXPs you’re not in
- You can always check websites such as bgp.tools to remind you
 - Don’t rely on them, however — it is your network after all, you know it!

<5'

To publish an ASPA object and benefit

2195

ASes have signed ASPA objects already

197

The most providers a single AS has (Cloudflare)

Ingredients

-  3 oz
BINARY BITS
(0s & 1s, well-mixed)
-  1 oz
SYN
(for connection initiation)
-  1 oz
ACK
(to confirm flavor delivery)
-  2 dashes
CHECKSUM
(for integrity)
-  A splash of
DNS
(just to resolve things)
-  1 packet of
UDP
(optional, for a faster kick,
no guarantees)

Serving Notes

-  Best served
connection-oriented.
-  May experience latency
under heavy load.
-  For best results,
avoid congestion
and packet loss.

The TCP/IP Cocktail



Instructions

-  Initiate the session:
add SYN and wait
for SYN-ACK.
-  Pour in Binary Bits
and shake vigorously
until fully encapsulated.
-  Add Checksum
and verify integrity
before proceeding.
-  If packets are lost
during shaking,
retransmit immediately.
-  Strain into a chilled
Layer 2
header glass.
-  Garnish with
a twist of IP routing.

Warning

-  Do not mix
with firewalls
unless properly configured.
-  Excess consumption
may cause fragmentation.

GRNOG20

where Greek Networkers meet

Ingredients

- 3 oz
BINARY BITS
(0s & 1s, well-mixed)
- 1 oz
SYN
(for connection initiation)
- 1 oz
ACK
(to confirm flavor delivery)
- 2 dashes
CHECKSUM
(for integrity)
- A splash of
DNS
(just to resolve things)
- 1 packet of
UDP
(optional, for a faster
no guarantees)

Serving Notes

- Best served
connection-oriented
- May experience latency
under heavy load.
- For best results,
avoid congestion
and packet loss.

The TCP/IP Cocktail

Instructions

- 1  Initiate the session:
add SYN and wait
for SYN-ACK.
 - 2  Pour in Binary Bits
and shake vigorously
until fully encapsulated.
 - 3  Add Checksum
and verify integrity
before proceeding.
-  If packets are lost
during shaking,
retransmit immediately.
 -  Strain into a chilled
Layer 2
header glass.
 -  Garnish with
a twist of IP routing.

Warning

-  Do not mix
with firewalls
unless properly configured.
-  Excess consumption
may cause fragmentation.

Participant List

184 participants

GRNOG20

where Greek Networkers meet

AS50877 AIRBEAM **AS6777** AMS-IX **AS1200** AMS-IX **AS55064** Arista Networks
AS4601 Antonis **AS41125** Bank of Greece **AS2856** British Telecom **AS5400**
British Telecom **AS215492** Butler **AS109** Cisco **AS13445** Cisco WebEx **AS36692**
Cisco OpenDNS **AS8248** CTI Diophantos **AS6695** DE-CIX **AS3320** Deutsche
Telekom **AS207953** Devoq **AS13038** Euronext Athens **AS21186** Fast Telecom
AS56457 FASTPATH **AS199121** Flexoptix **AS40934** Fortinet **AS51392** Fusioned
AS200561 Gamma Placetel **AS50311** Gloman **AS215804** GRID Telecom **AS5408**
GRNET **AS2914** NTT **AS214618** Hack the Box **AS211275** Thomas **AS24652**
Juniper ;) **AS71** HPE **AS49544** i3D.net **AS16876** ICANN **AS26710** ICANN
AS20144 ICANN **AS3323** NTUA **AS6169** Kentik **AS207063** Kentik **AS204764**
Kyndryl **AS199081** Lancom **AS51185** MainStreaming **AS206529** Metadosis
AS61968 MIX-IT **AS201494** modulus **AS24796** NAMEX **AS2546** NCSR Dimokritos
AS57463 NetIX **AS34224** Neterra **AS1241** NOVA **AS206735** Novelcomm
AS31898 Oracle **AS197515** Orizon Telecom **AS6799** OTE **AS12713** OTEGlobe
AS29247 COSMOTE **AS3491** PCCW **AS9002** RETN **AS202042** Skroutz **AS8499**
Space Hellas **AS8280** Synapsecom **AS16013** UniSystems **AS39505** VESTITEL
AS3329 Vodafone **AS198121** Whalebone **AS209608** Municipality of Athens

AS50877 AIRBEAM **AS6777** AMS-IX **AS1200** AMS-IX **AS55064** Arista Networks
AS4601 Antonis **AS41125** Bank of Greece **AS2856** British Telecom **AS5400**
British Telecom **AS215492** Butler **AS109** Cisco **AS13445** Cisco WebEx **AS36692**
Cisco OpenDNS **AS8248** CTI Diophantos **AS6695** DE-CIX **AS3320** Deutsche
Telekom **AS207953** Devoq **AS13038** Euronext Athens **AS21186** Fast Telecom
AS56457 FASTPATH **AS199121** Flexoptix **AS40934** Fortinet **AS51392** Fusioned
AS200561 Gamma Placetel **AS50311** Gloman **AS215804** GRID Telecom **AS5408**
GRNET **AS2914** NTT **AS214618** Hack the Box **AS211275** Thomas **AS24652**
Juniper ;) **AS71** HPE **AS49544** i3D.net **AS16876** ICANN **AS26710** ICANN
AS20144 ICANN **AS3323** NTUA **AS6169** Kentik **AS207063** Kentik **AS204764**
Kyndryl **AS199081** Lancom **AS51185** MainStreaming **AS206529** Metadosis
AS61968 MIX-IT **AS201494** modulus **AS24796** NAMEX **AS2546** NCSR Dimokritos
AS57463 NetIX **AS34224** Neterra **AS1241** NOVA **AS206735** Novelcomm
AS31898 Oracle **AS197515** Orizon Telecom **AS6799** OTE **AS12713** OTEGlobe
AS29247 COSMOTE **AS3491** PCCW **AS9002** RETN **AS202042** Skroutz **AS8499**
Space Hellas **AS8280** Synapsecom **AS16013** UniSystems **AS39505** VESTITEL
AS3329 Vodafone **AS198121** Whalebone **AS209608** Municipality of Athens

Roles & OTC

147.189.216.0/22 from AS4601

147.189.216.0/22 via 2001:7f8:116::c6b5:1

AS Path: 29529 **215405** **4601**

AS4601 providers are AS8298

Me

AS29529

AS215405

AS4601



Me

AS29529

AS215405

AS4601

AS8298



Me

AS29529

AS215405

AS4601

AS8298



Me



AS29529

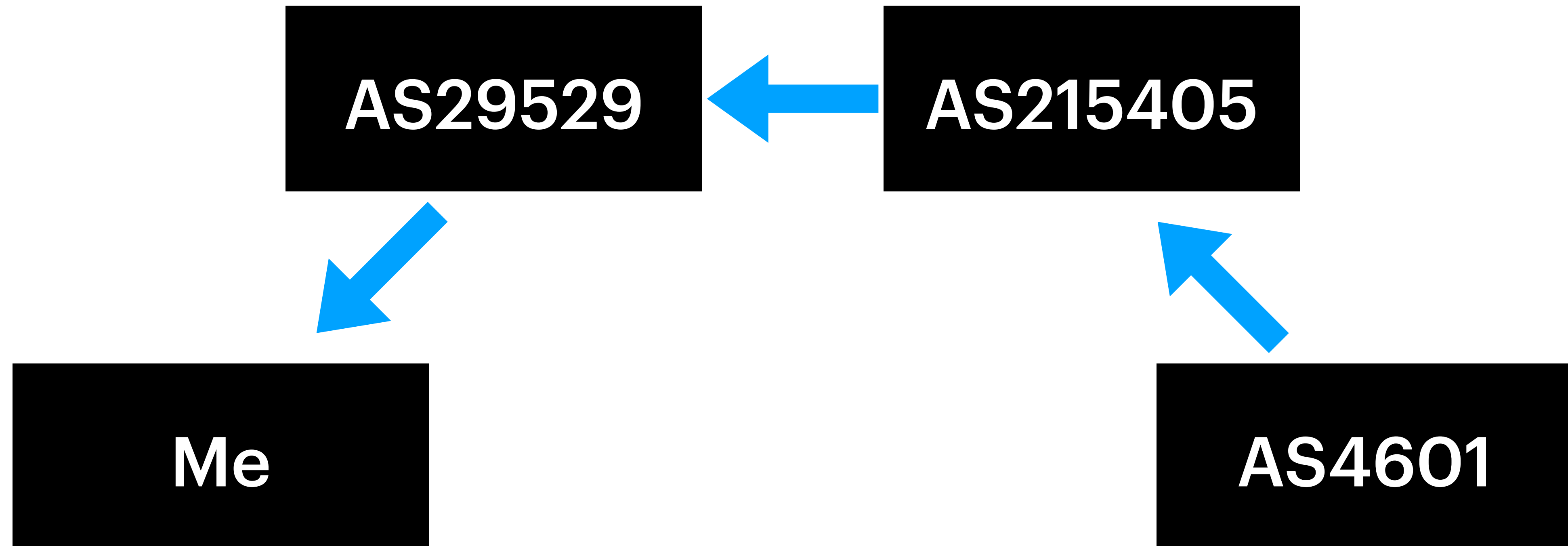


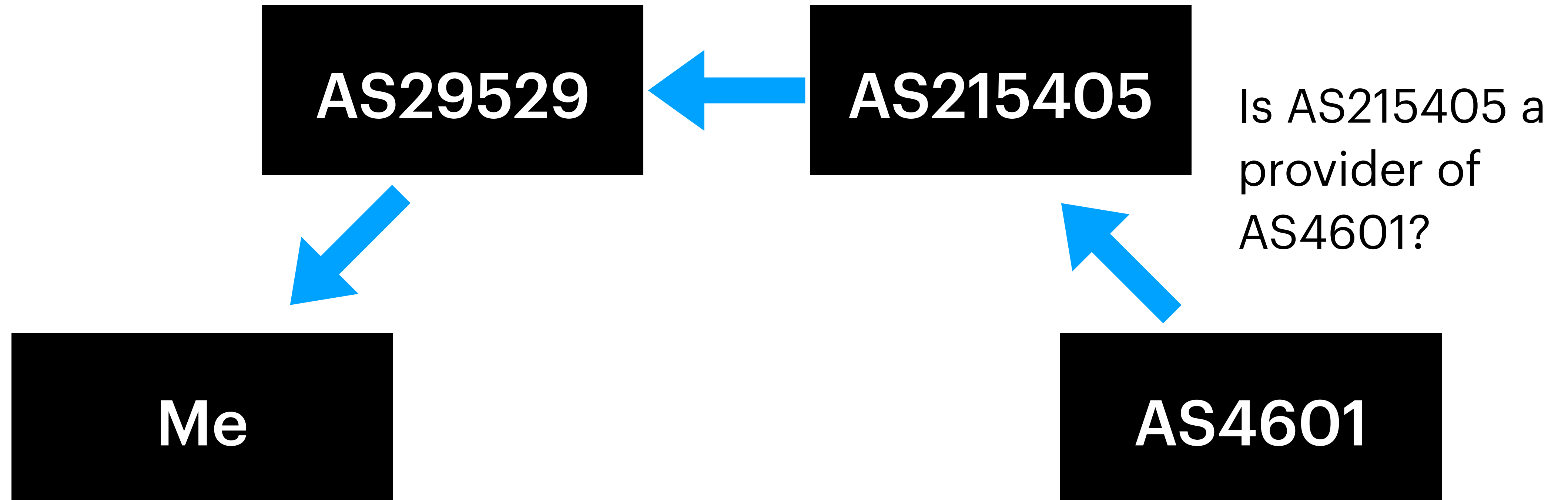
AS215405

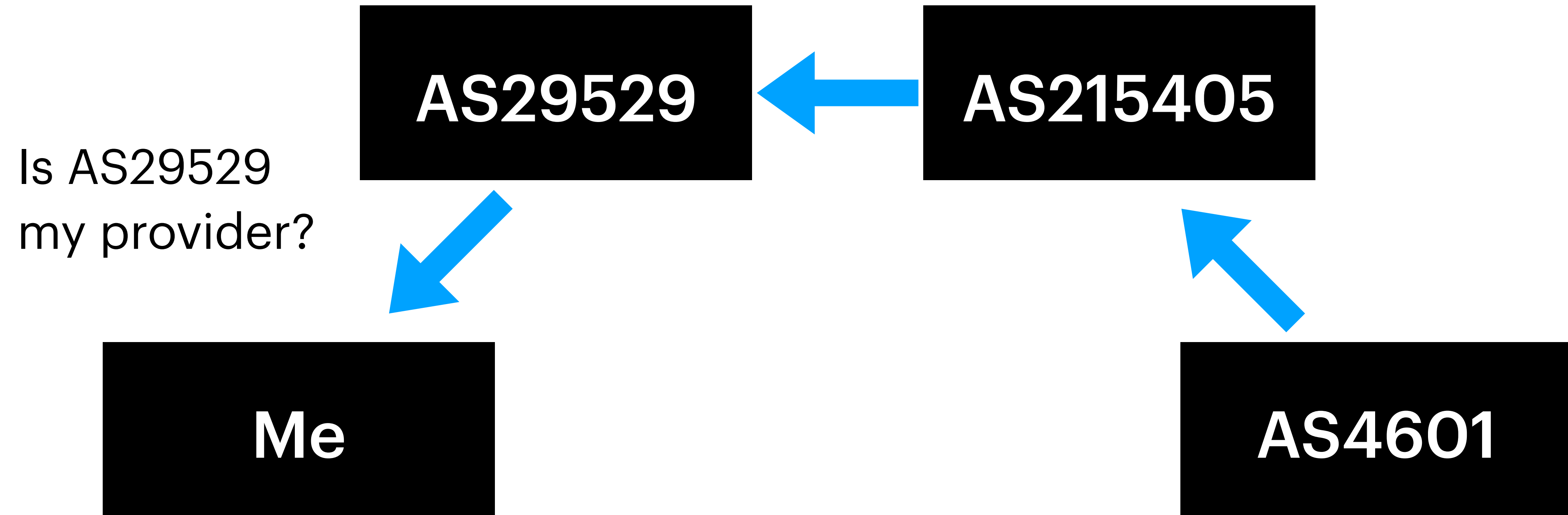


AS4601

AS8298







Valley-free Principle

The Internet is hierarchical :(

Why?



The Internet is* valley-free

- Due to the business / financial model of the Internet:
 - Who pays whom dictates the traffic direction
 - Relationships are set and enforced with filters
 - Each network you connect to is either a Peer, Customer, or Upstream
 - Customers must never give you connectivity
 - Peers must only give connectivity to their customers
 - Upstreams are the only ones carrying you to the Internet

The “simple” rules

- One or more “uphill” steps, up to one side step, one on more “downhill”
- You can go up to one step sideways (to a peer)
 - If I peer with an AS, they must not send my routes to their peers
- If you stop going up, you cannot go up again
 - My peers & their customers must not send my routes to their upstreams

A

B

C

D

E

F

G

H

A

B

C

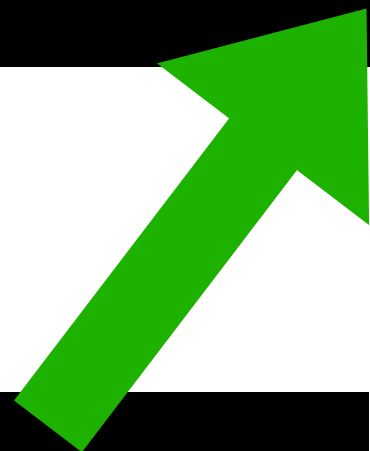
D

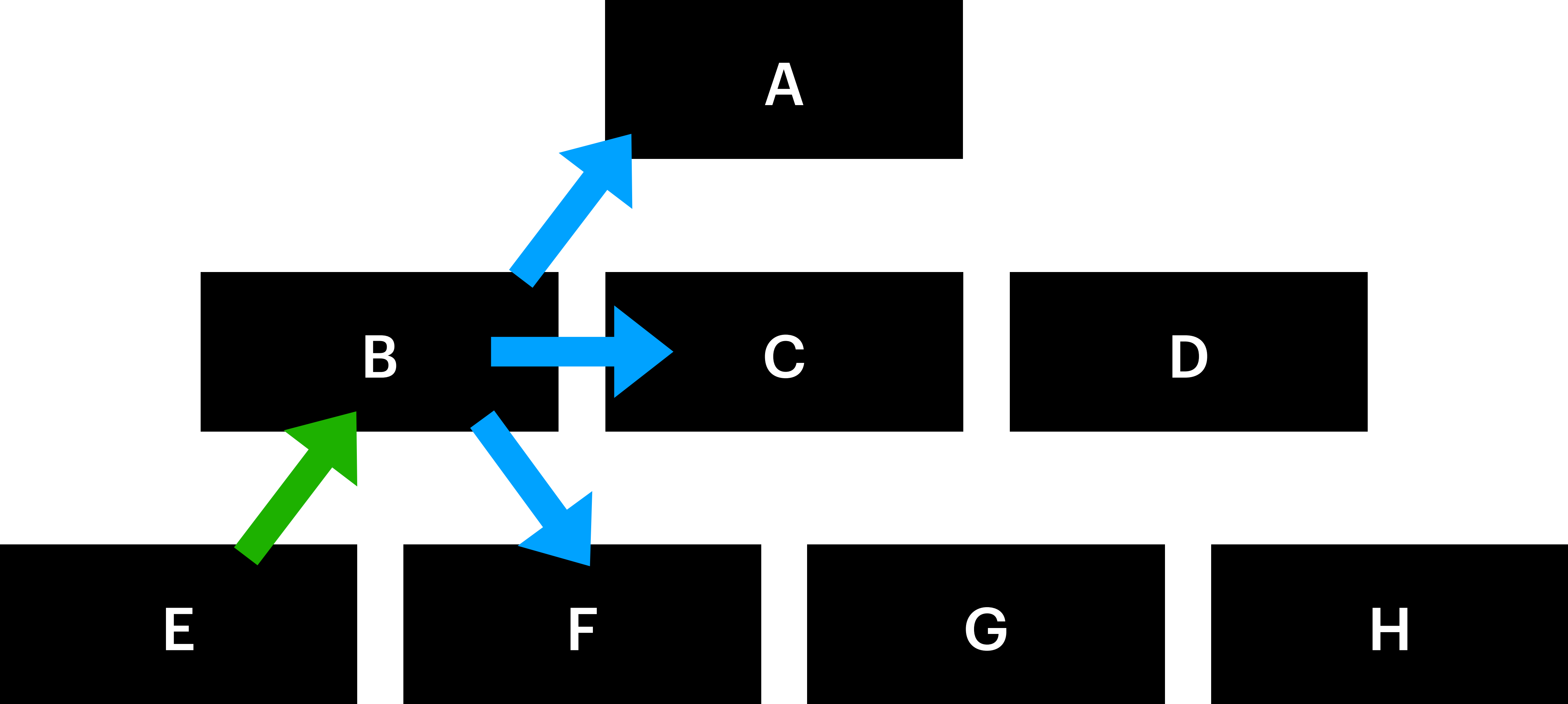
E

F

G

H





A

B

C

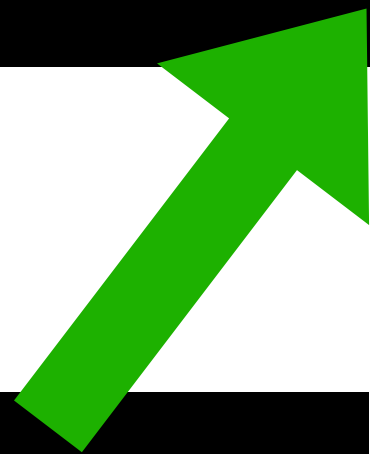
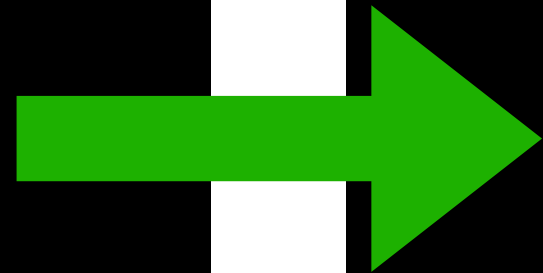
D

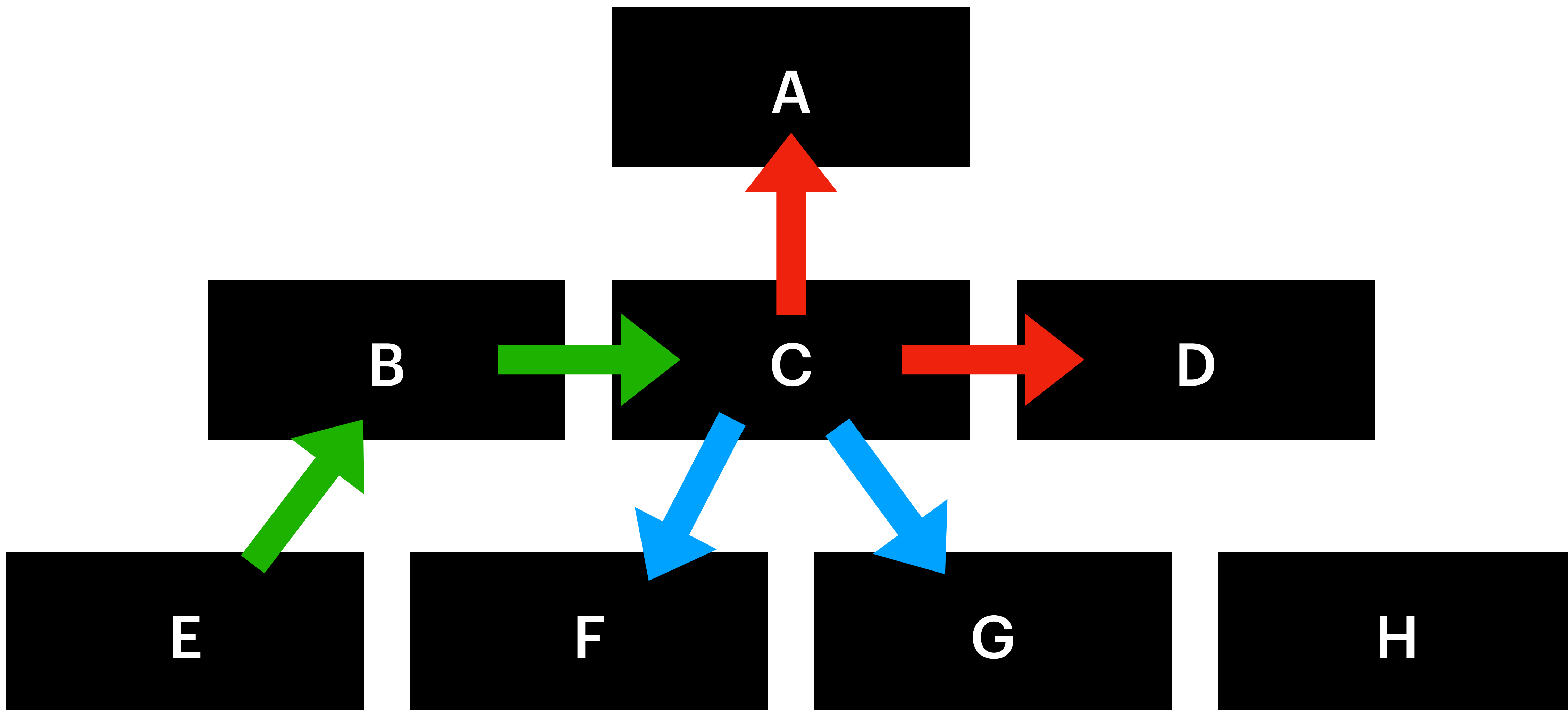
E

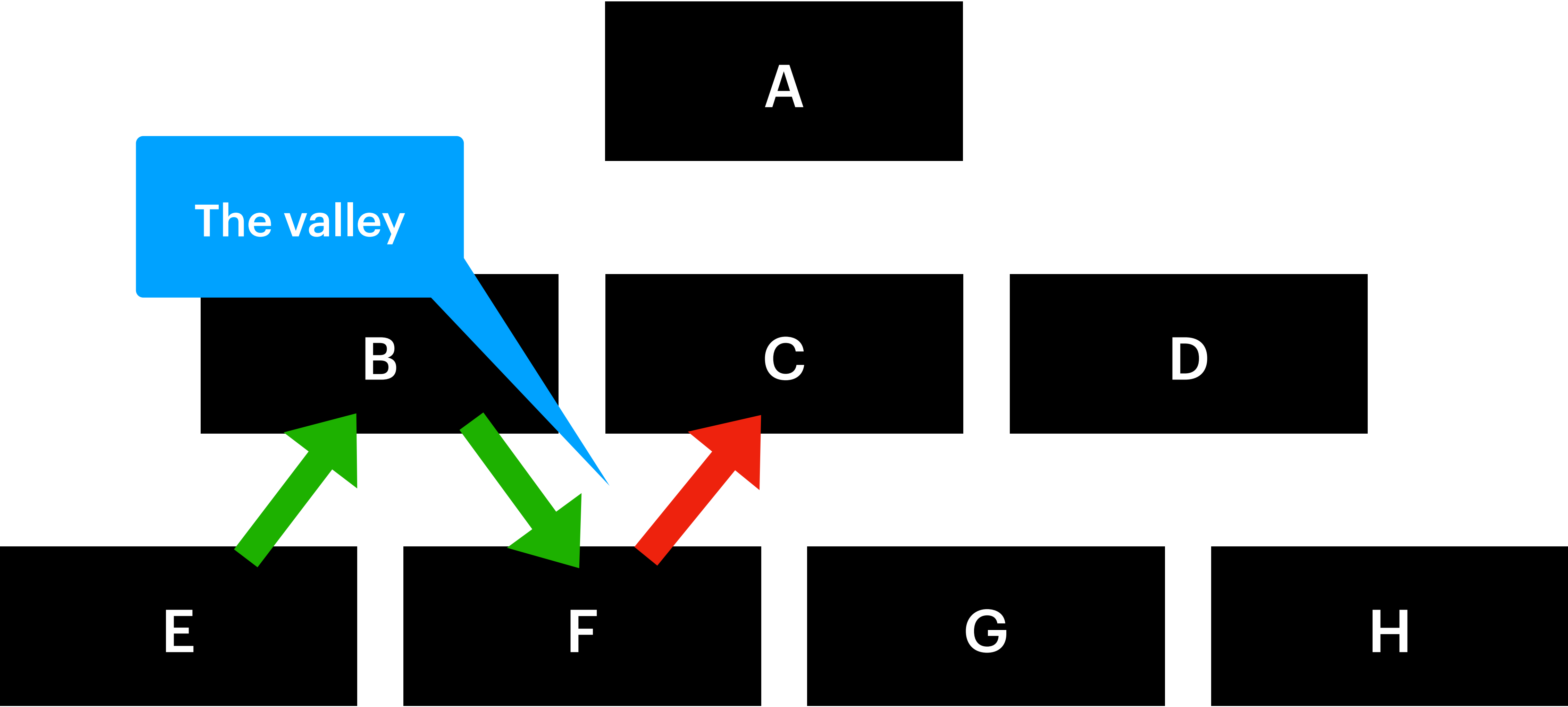
F

G

H







Enough graph theory!

Roles

- On each BGP Session / Group / Template, you set a “Role”:
 - Provider, Customer, Peer, Route Server, Route Server Client
- If the other party sets one too, they must be pairs
 - You cannot both use “Provider”, it must be “Provider” & “Customer”
- Your BGP stack can now automatically prevent Route Leaks*!
 - It knows what it can send where, filtering things for you:
 - It will never send Provider prefixes to Providers or Peers or RS
 - It will never send Peer prefixes to Providers or other Peers [...]

OTC (Only To Customer)

- Your BGP stack will receive and add this “tag” to all routes
- Your router will “tag” all routes to Customers or Peers with OTC
- The presence signifies that this prefix has been sent to a Customer or Peer
 - (It is already in the “off-ramp”)
- It will not propagate it to Providers, Peers, or Route Servers
 - (It will not go uphill or sideways again)
- You avoid causing route leaks for you, your customers, and everyone else

ASPA

BGP Roles

OTC Attribute

ASPA and Roles

What's up with that?