

Border Gateway Protocol Fundamentals

cisco Live !

Shek Habeebul Haq
Technical Leader, [linkedin.com/in/sheik-habeebul-haq-470877380](https://www.linkedin.com/in/sheik-habeebul-haq-470877380)

Jaivik Shah
Technical Leader, @JaivikSOfficial

Cisco Webex App

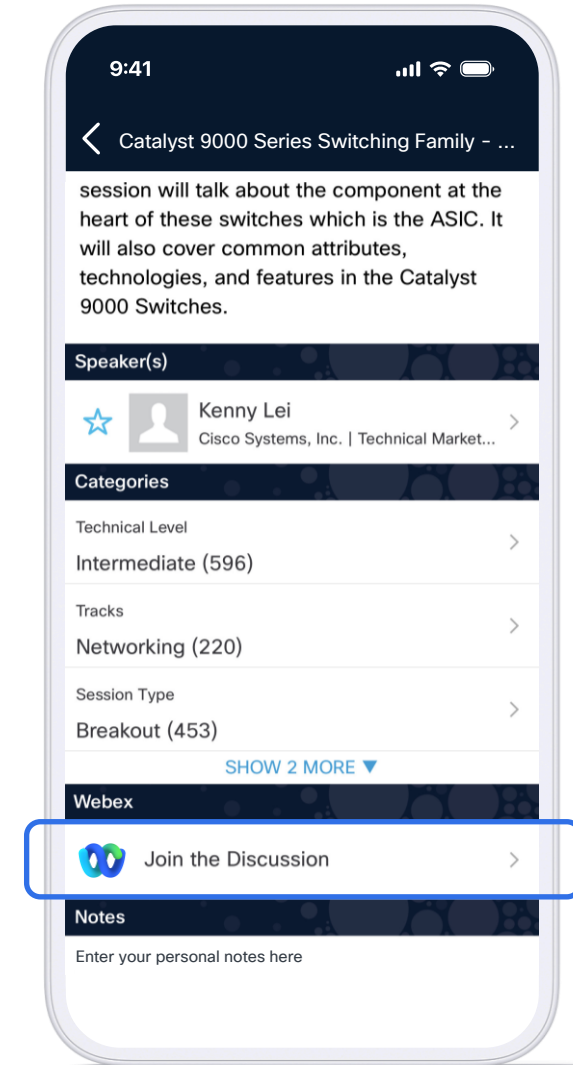
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



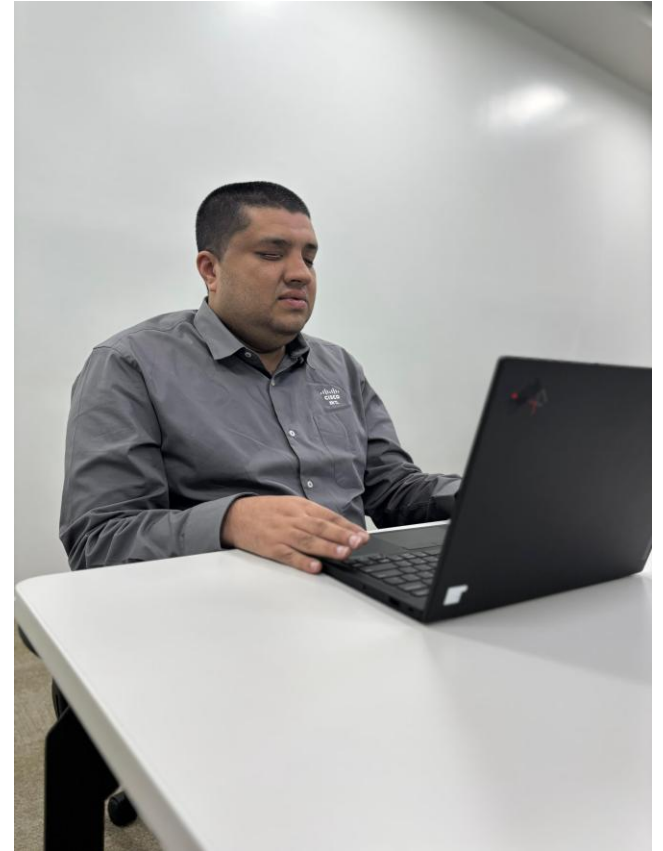
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-1179>

About Hameeb

My career began in a special school for visually challenged students, where Braille was my primary tool for learning. The discovery that screen readers could make computers accessible transformed my perspective—technology became the bridge over barriers I once thought unbreakable. With my first dial-up PC and no dedicated trainers, I taught myself computing through manuals, help files, and relentless trial and error, fuelling a deep curiosity in networking.

Earning a master's in English literature and qualifying as a university professor in India were significant milestones, but joining Cisco in a semi-technical role marked the true turning point. I earned CCNA and CCNP certifications, transitioned fully into networking, and over 11 years rose to Technical Leader in enterprise networking.

Today, I lead teams, mentor others, and champion the fusion of accessibility and automation to create inclusive workplaces, proving that resilience and self-learning can turn unexpected paths into meaningful impact.



About Jaivik

My career in networking began as a CCNA and CCNP trainer, where I empowered corporate teams to master routing and switching. Seeking hands-on challenges while fuelling my learning passion, I transitioned into the corporate world, diving into security, IPv6, and IPsec testing.

This diverse expertise led me to Cisco, where I joined as a High Touch Technical Support Engineer, quickly rising to escalation lead and Technical Leader in the routing domain.

Along the way, I earned dual CCIE certifications in Service Provider and Enterprise, solidifying my reputation as a routing authority.

Beyond the console, I'm a passionate cricketer who has represented my state on the field. Married to a vibrant food blogger and social media enthusiast, we share our lives with our energetic young son, whose boundless curiosity keeps us joyfully occupied.

“Routing isn’t just my job; it’s the art of making the Internet’s bloodstream flow without a single clot.”



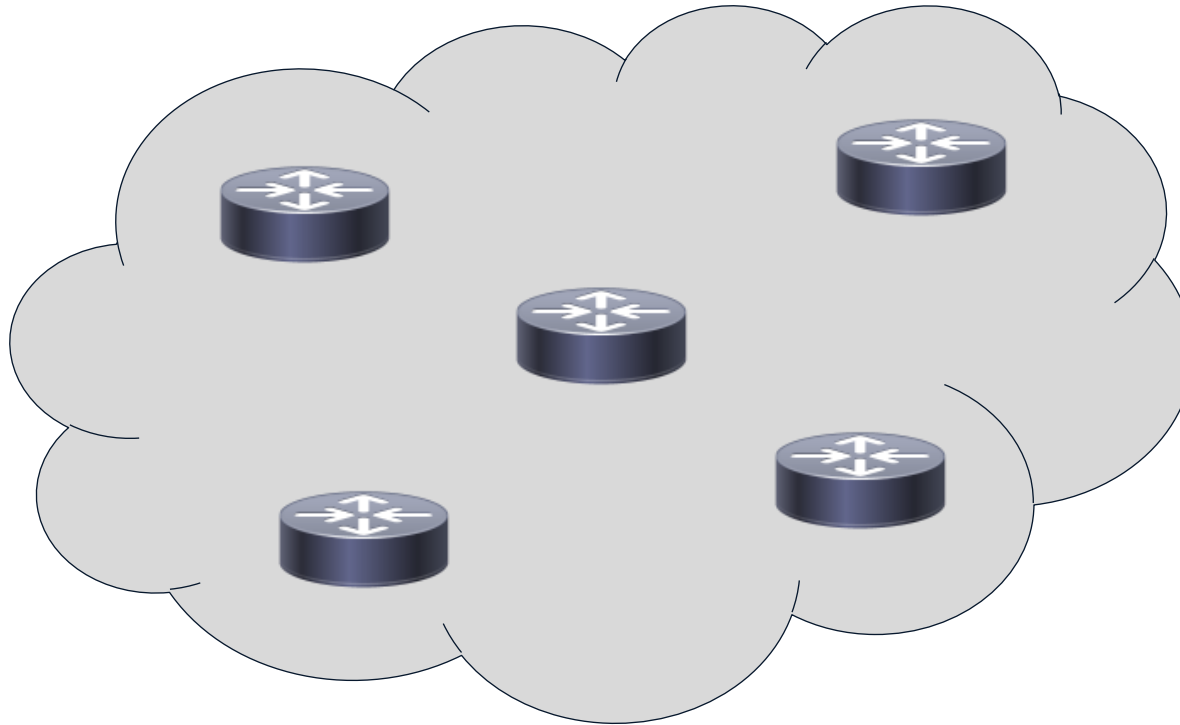
Agenda

- 01 Why BGP?**
- 02 Messages and States**
- 03 Attributes**
- 04 Internal vs External BGP**
- 05 Securing BGP**
- 06 Best Path Selection Algorithm**
- 07 Policy Control and Traffic Engineering**
- 08 Troubleshoot BGP Peering Issues**

Why BGP?

Autonomous System

A group of one or more IP prefixes (lists of IP addresses accessible on a network) run by one or more network operators that maintain a single, clearly-defined routing policy.



Autonomous System (cont'd)

BGP 2-byte ASN RFC1105 (1989)

- 16-bit number
- 0 to 65535
- Private range
64512 to 65534

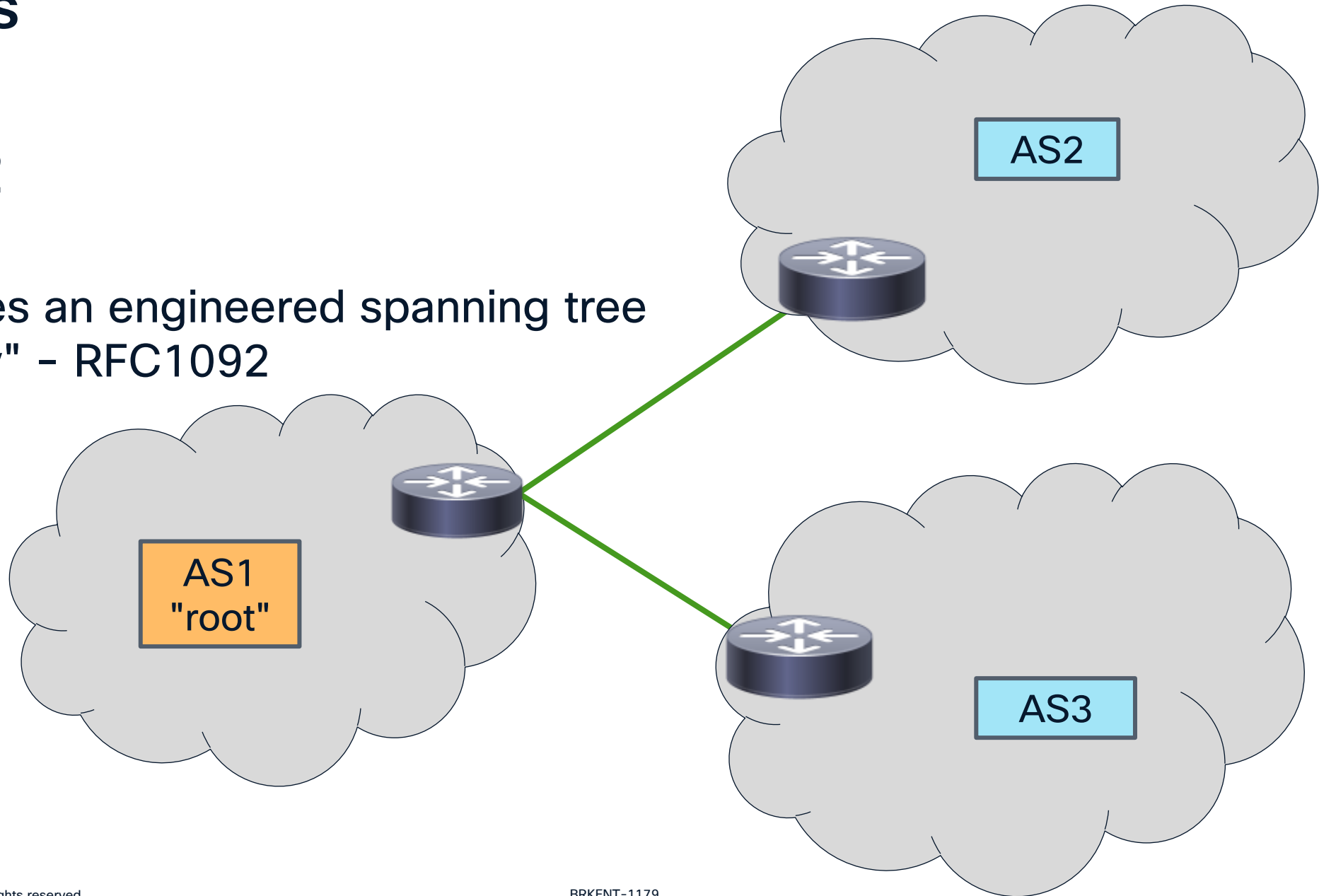
- Created to address 2-byte ASN depletion
- Interoperable with 2-byte ASNs (range includes 2-byte ASNs)
- 32-bit number
- 0 to 4294967295
- Additional private range 4200000000 to 4294967294

BGP 4-byte ASN RFC4893 (2007)

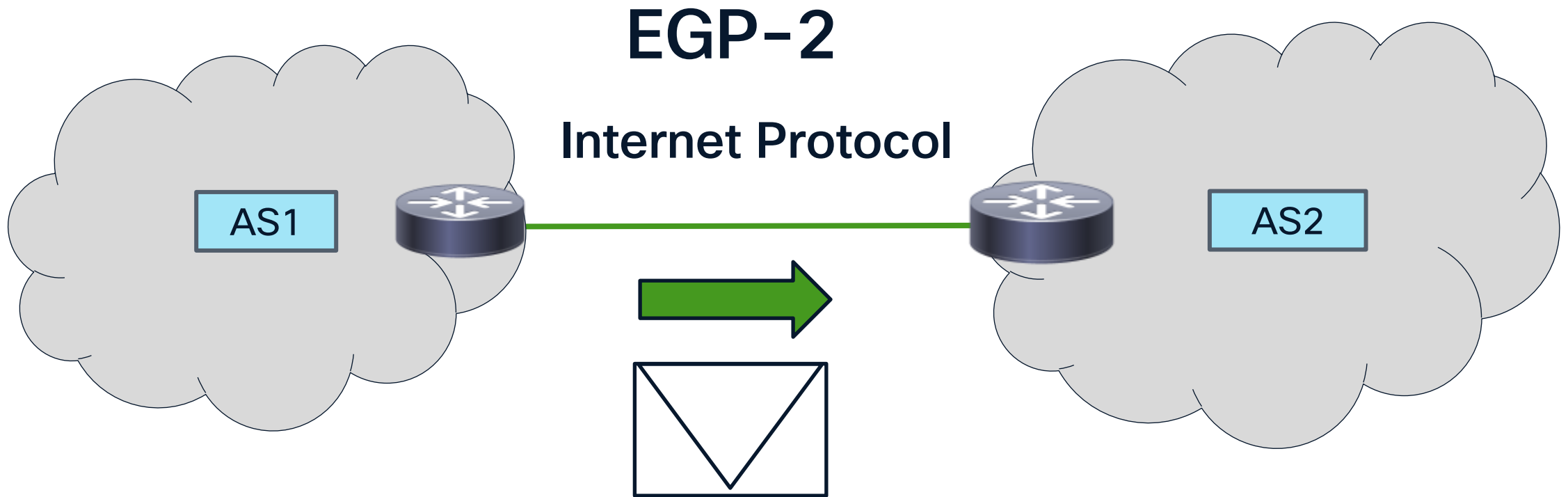
Late 80's

EGP-2

"Assumes an engineered spanning tree topology" - RFC1092



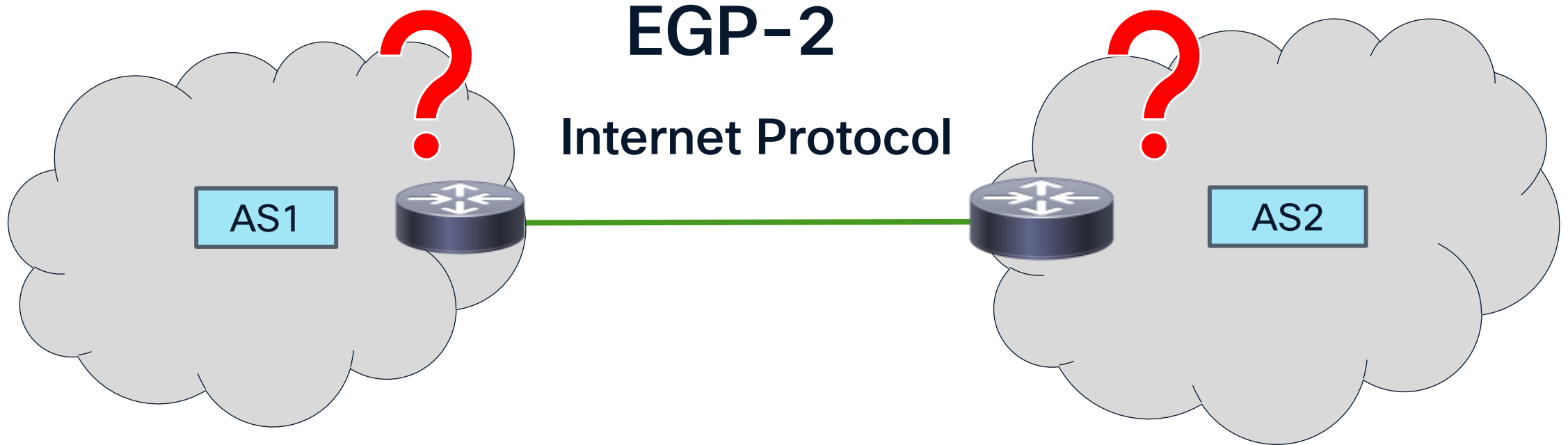
Late 80's



Late 80's

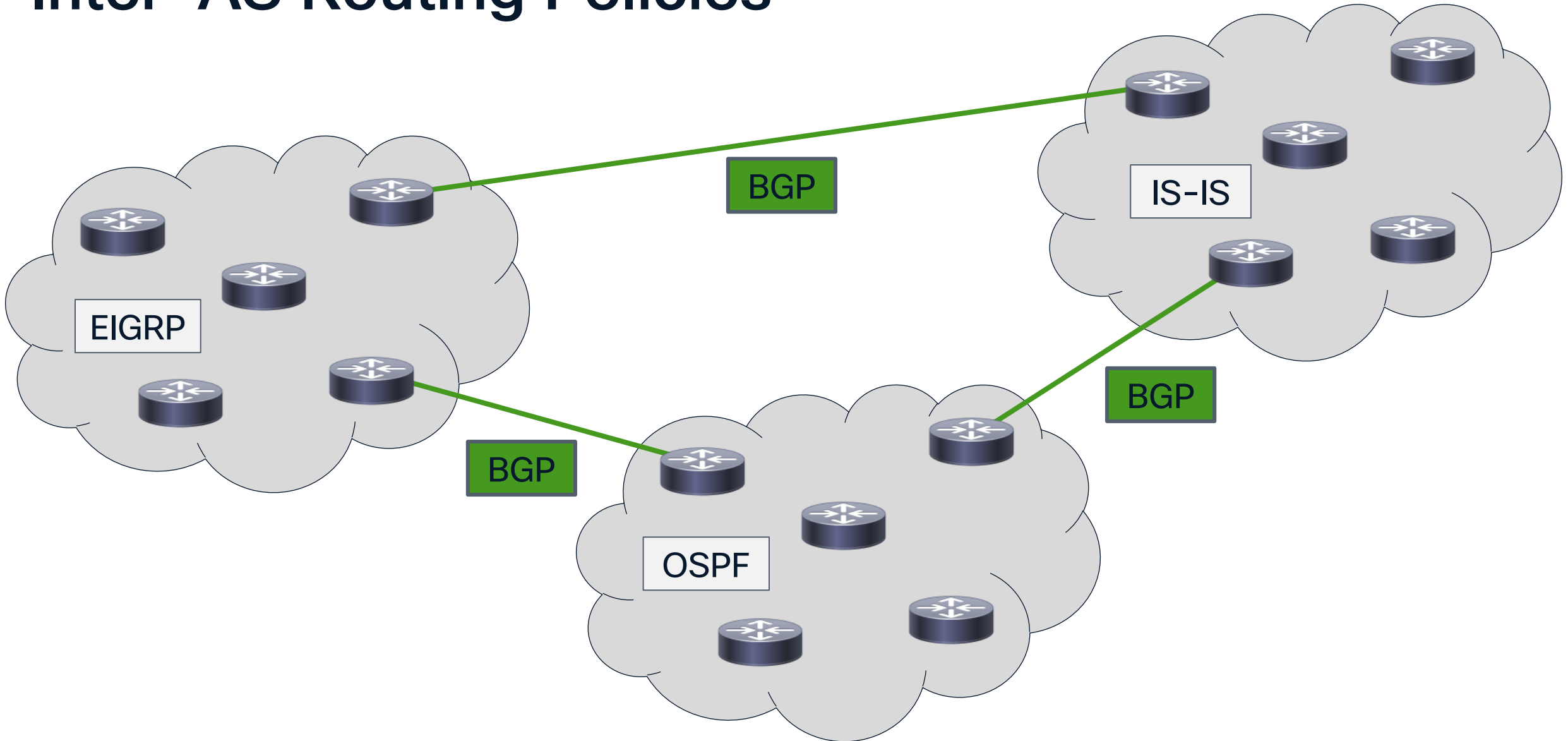


Late 80's



No reliable retransmission mechanism

Inter-AS Routing Policies



Border Gateway Protocol

- Border Gateway Protocol
 - Large scale, robust and stable routing protocol designed to operate between autonomous systems
 - Based on TCP, listens on port 179
 - Fundamentally a distance vector protocol
 - Does not have the concept of a simple metric
 - Strong control over advertised routes and their attributes

Route Scale & Control Plane Stability

```
route-views> show bgp ipv4 unicast summary | ex never|Active|Idl
```

```
BGP router identifier 128.223.51.103, local AS number 6447
```

```
BGP table version is 2813468887, main routing table version 2813468887
```

```
Path RPKI states: 7708169 valid, 10262796 not found, 14390 invalid
```

```
962240 network entries using 238635520 bytes of memory
```

```
<Output omitted...>
```

```
BGP using 3360540172 total bytes of memory
```

```
BGP activity 71481761/70340753 prefixes, 3122764440/3095983216 paths, scan  
interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
4.68.4.46	4	3356	5325851	83510	2813468729	12	0	3w5d	905347
12.0.1.63	4	7018	5117677	19250	2813468729	124	0	1w5d	906235

```
<Output omitted...>
```

BGP Stability Considerations

- Network events burst.
- Fast reaction: better convergence, more churn.
- Delayed reaction: more stability, slower convergence.
- BGP prioritizes stability.
- Delays updates to reduce churn, combines changes.
- Sends only incremental updates.

Route Scale & Control Plane Stability

```
R1# show bgp ipv4 unicast neighbors 10.1.1.2
```

```
BGP neighbor is 10.1.1.2, remote AS 65500, external link
```

```
BGP version 4, remote router ID 10.1.1.2
```

```
BGP state = Established, up for 00:48:19
```

```
Last read 00:00:14, last write 00:00:03, hold time is 180, keepalive interval is 60  
seconds
```

```
<Output omitted>
```

```
Default minimum time between advertisement runs is 30 seconds
```

```
<Output omitted>
```

Network Layer Reachability Information Exchange

```
R1(config)# router bgp 64512
R1(config-router)# address-family ?
  ipv4      Address family
  ipv6      Address family
  l2vpn     Address family
  nsap      Address family
  vpnv4     Address family
  vpnv6     Address family
```

Prefix/Length

```
route-views> show bgp all neighbors 4.68.4.46 | i family
For address family: IPv4 Unicast
  Address family IPv4 Unicast: advertised and received
  Address family IPv4 Multicast: advertised and received
For address family: IPv6 Unicast
For address family: IPv4 Multicast
  Address family IPv4 Unicast: advertised and received
  Address family IPv4 Multicast: advertised and received
For address family: L2VPN E-VPN
For address family: MVPNv4 Unicast
```

Messages

BGP Message Types

- BGP runs on TCP:
 - Byte stream-oriented
 - Unicast only
 - Connection-oriented and reliable
 - Provides flow and congestion control
- BGP message format aligns with TCP specifics:
 - Message markers
 - Length indications (lots of!)

BGP Message Types

BGPv4 uses (only) 5 message types

- OPEN
- UPDATE
- NOTIFICATION
- KEEPALIVE
- ROUTE-REFRESH

BGP OPEN Message

- BGP speakers use OPEN to advertise configuration and capabilities after TCP session starts:
 - Version
 - Autonomous System Number
 - Hold Time (advertise/negotiation)
 - BGP Router ID
 - Optional Capabilities (advertise/negotiation)
- Incompatible configurations terminate peering and close TCP session.

BGP OPEN Message

Border Gateway Protocol - OPEN Message

Marker: ffffffffffffffffffffffffffffffffffffffff

Length: 57

Type: OPEN Message (1)

Version: 4

My AS: 64512

Hold Time: 180

BGP Identifier: 10.255.255.1

Optional Parameters Length: 28

- Optional Parameters

‣ Optional Parameter: Capability

‣ Optional Parameter: Capability

‣ Optional Parameter: Capability

‣ Optional Parameter: Capability

- Optional Parameter: Capability

  Parameter Type: Capability (2)

  Parameter Length: 6

  ‣ Capability: Support for 4-octet AS number capability

BGP NOTIFICATION Message

- NOTIFICATION message sent for unrecoverable conditions to terminate peering.
- Sender closes session after NOTIFICATION.
- Contents useful for diagnostics.

```
Border Gateway Protocol - NOTIFICATION Message
Marker: ffffffffffffffffffffffffffffffffffffffff
Length: 21
Type: NOTIFICATION Message (3)
Major error Code: Cease (6)
Minor error Code (Cease): Administratively Shutdown (2)
```

BGP KEEPALIVE Message

- BGP uses KEEPALIVE instead of TCP keepalives to show liveliness.
- KEEPALIVE is sent:
 - Immediately after an agreeable OPEN message.
 - Periodically, default is one-third of Hold Time.

Border Gateway Protocol - KEEPALIVE Message

Marker: ffffffffffffffffffffffffffffffffffffffff

Length: 19

Type: KEEPALIVE Message (4)

BGP ROUTE-REFRESH Message

- Original BGP lacked a way to request prefix resend.
 - Needed for inbound route policy changes.
 - Vendors used "Soft Reconfiguration" to store unfiltered routes.
- RFC 2918 introduced ROUTE-REFRESH to request route resend for any address family.

Border Gateway Protocol - ROUTE-REFRESH Message

Marker: ffffffffffffffffffffffffffffffffffffffff

Length: 23

Type: ROUTE-REFRESH Message (5)

Address family identifier (AFI): IPv4 (1)

Subtype: Normal route refresh request [RFC2918] with/without ORF [RFC5291] (0)

Subsequent address family identifier (SAFI): Unicast (1)

BGP UPDATE Message

- UPDATE message is BGP's workhorse.
- Advertises reachable NLRI with attributes.
- Withdraws unreachable NLRI.
- Designed for maximum efficiency:
 - Path attributes included once, followed by NLRI sharing them.
 - Each NLRI contains only the network prefix (with padding if needed).

BGP Update Message – New/Updated Routes

Border Gateway Protocol - UPDATE Message

Marker: ffffffffffffffffffffffffffffffffffffffff

Length: 67

Type: UPDATE Message (2)

Withdrawn Routes Length: 0

Total Path Attribute Length: 28

- Path attributes

▸ Path Attribute - ORIGIN: IGP

▸ Path Attribute - AS_PATH: empty

▸ Path Attribute - NEXT_HOP: 10.255.255.1

▸ Path Attribute - MULTI_EXIT_DISC: 1234

▸ Path Attribute - LOCAL_PREF: 100

- Network Layer Reachability Information (NLRI)

▸ 192.168.0.0/24

▸ 192.168.1.0/24

▸ 192.168.2.0/24

▸ 192.168.3.0/24

BGP Update Message – Withdrawn Routes

```
Border Gateway Protocol - UPDATE Message
Marker: ffffffffffffffffffffffffffffffffffffffff
Length: 27
Type: UPDATE Message (2)
Withdrawn Routes Length: 4
- Withdrawn Routes
  ▸ 192.168.3.0/24
Total Path Attribute Length: 0
```

States

Active, Idle, Connect

1174	17:39:50.701103	10.1.1.2	10.1.1.1	TCP	60	52565 → 179	[SYN] Seq=0 Win=16384
1175	17:39:50.724304	10.1.1.1	10.1.1.2	TCP	60	179 → 52565	[SYN, ACK] Seq=0 Ack=
1176	17:39:50.761402	10.1.1.2	10.1.1.1	TCP	60	52565 → 179	[ACK] Seq=1 Ack=1 Win=16384

> Frame 1174: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 0

> Ethernet II, Src: ca:02:9f:44:00:00 (ca:02:9f:44:00:00), Dst: ca:01:5f:3a:00:00 (ca:01:5f:3a:00:00)

> Internet Protocol Version 4, Src: 10.1.1.2, Dst: 10.1.1.1

> Transmission Control Protocol, Src Port: 52565, Dst Port: 179, Seq: 0, Len: 0

Source Port: 52565

Destination Port: 179

[Stream index: 4]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 3742606240

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

0110 = Header Length: 24 bytes (6)

> Flags: 0x002 (SYN)

Window: 16384

[Calculated window size: 16384]

Checksum: 0xf164 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> Options: (4 bytes), Maximum segment size

> [Timestamps]

Open Sent & Open Confirmed

1177	17:39:50.792164	10.1.1.2	10.1.1.1	BGP	112	OPEN Message
1178	17:39:50.815234	10.1.1.1	10.1.1.2	BGP	112	OPEN Message
1179	17:39:50.815297	10.1.1.1	10.1.1.2	BGP	73	KEEPALIVE Message
1180	17:39:50.873147	10.1.1.2	10.1.1.1	BGP	73	KEEPALIVE Message
> Frame 1177: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface -, id 0						
> Ethernet II, Src: ca:02:9f:44:00:00 (ca:02:9f:44:00:00), Dst: ca:01:5f:3a:00:00 (ca:01:5f:3a:00:00)						
> Internet Protocol Version 4, Src: 10.1.1.2, Dst: 10.1.1.1						
> Transmission Control Protocol, Src Port: 52565, Dst Port: 179, Seq: 1, Ack: 1, Len: 58						
v Border Gateway Protocol - OPEN Message						
Marker: ffffffffffffffffffffffffffffffffff						
Length: 58						
Type: OPEN Message (1)						
Version: 4						
My AS: 65500						
Hold Time: 180						
BGP Identifier: 10.1.1.2						
Optional Parameters Length: 29						
v Optional Parameters						
v Optional Parameter: Capability						
Parameter Type: Capability (2)						
Parameter Length: 6						
> Capability: Multiprotocol extensions capability						
v Optional Parameter: Capability						
Parameter Type: Capability (2)						
Parameter Length: 2						
> Capability: Route refresh capability (Cisco)						
v Optional Parameter: Capability						
Parameter Type: Capability (2)						
Parameter Length: 2						
> Capability: Route refresh capability						

Established

```
R1# show bgp ipv4 unicast summary
```

```
BGP router identifier 10.1.1.1, local AS number 64512
```

```
BGP table version is 1, main routing table version 1
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.1.2	4	65500	15	15	1	0	0	00:10:49	0

Attributes

BGP Attributes

- An attribute is an additional piece of information accompanying an advertised NLRI
- BGP uses attributes in multiple ways
 - Prevents routing loops
 - Performs best path selection
 - Filters or sorts routes
 - ... and many more
- Basic BGP specification recognizes only a handful of attributes
- Several new have been added over time for various applications and uses

BGP Attribute Types

- **Well-known:** Every BGP implementation must support it
 - Well-known mandatory: Must always be included with a NLRI
 - Well-known discretionary: May be included with a NLRI as needed
- **Optional:** BGP implementations do not need to support it
 - Optional transitive: When advertising a learned NLRI, keep the attribute with the NLRI even if not recognized
 - Optional non-transitive: When advertising a learned NLRI, remove the attribute from the NLRI if not recognized

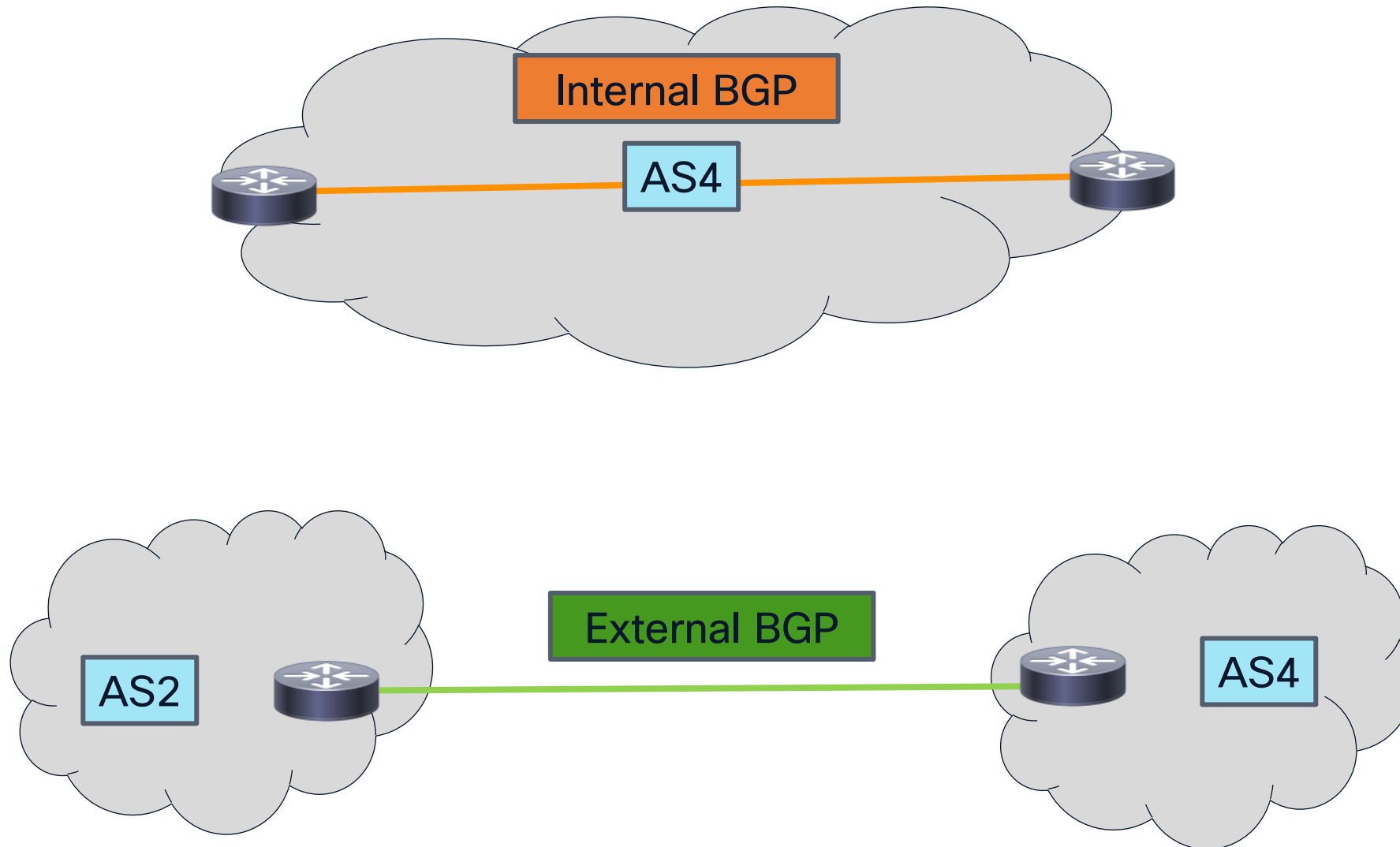
Note: All well-known attributes are transitive

BGP Attributes

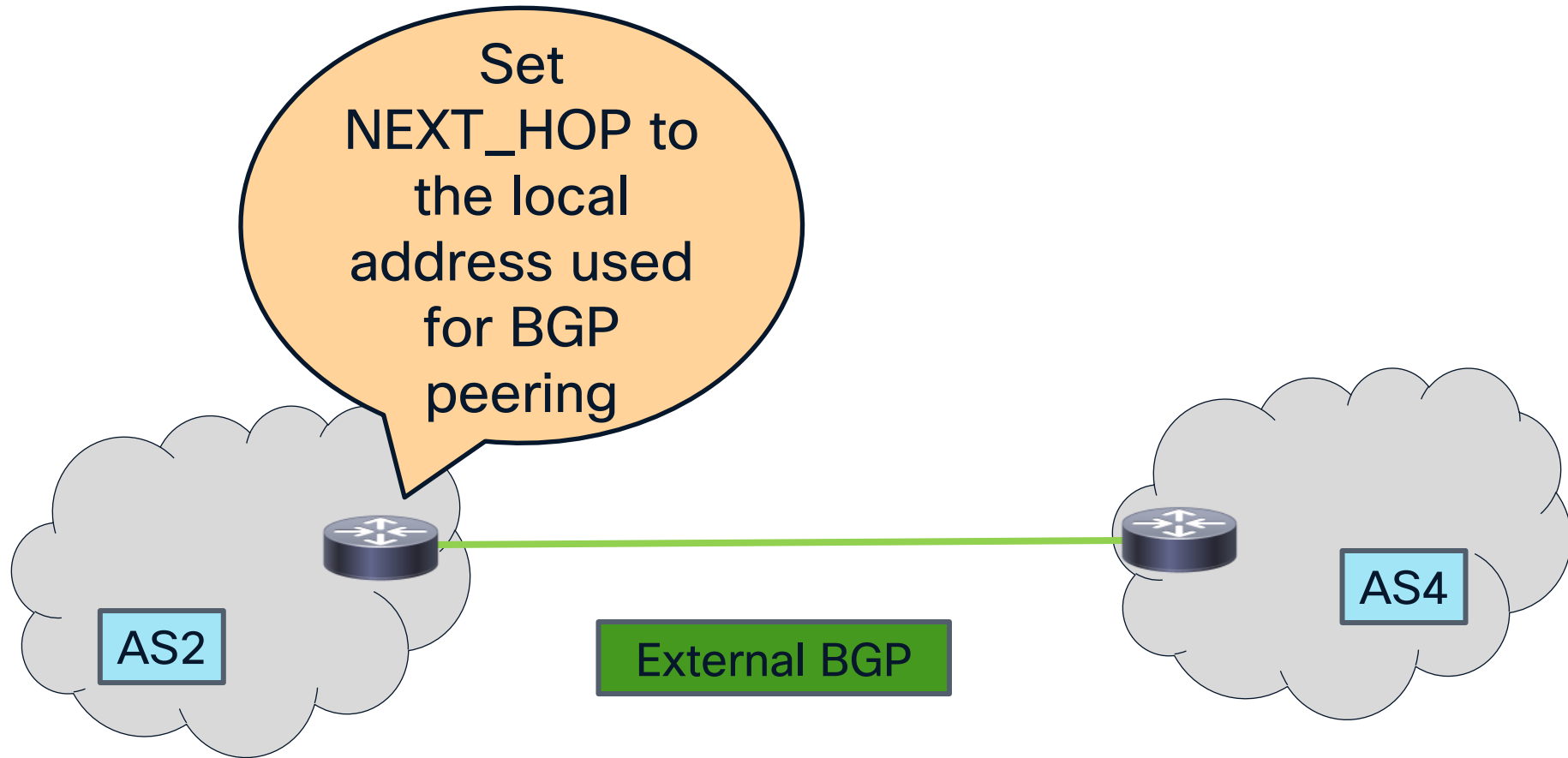
- Well-known mandatory
 - AS_PATH
 - NEXT_HOP
 - ORIGIN
- Well-known discretionary
 - LOCAL_PREF
 - ATOMIC_AGGREGATE
- Optional transitive
 - AGGREGATOR
 - COMMUNITIES
 - EXTENDED_COMMUNITIES
- Optional non-transitive
 - MULTI_EXIT_DISC
 - CLUSTER_LIST

Internal vs External BGP

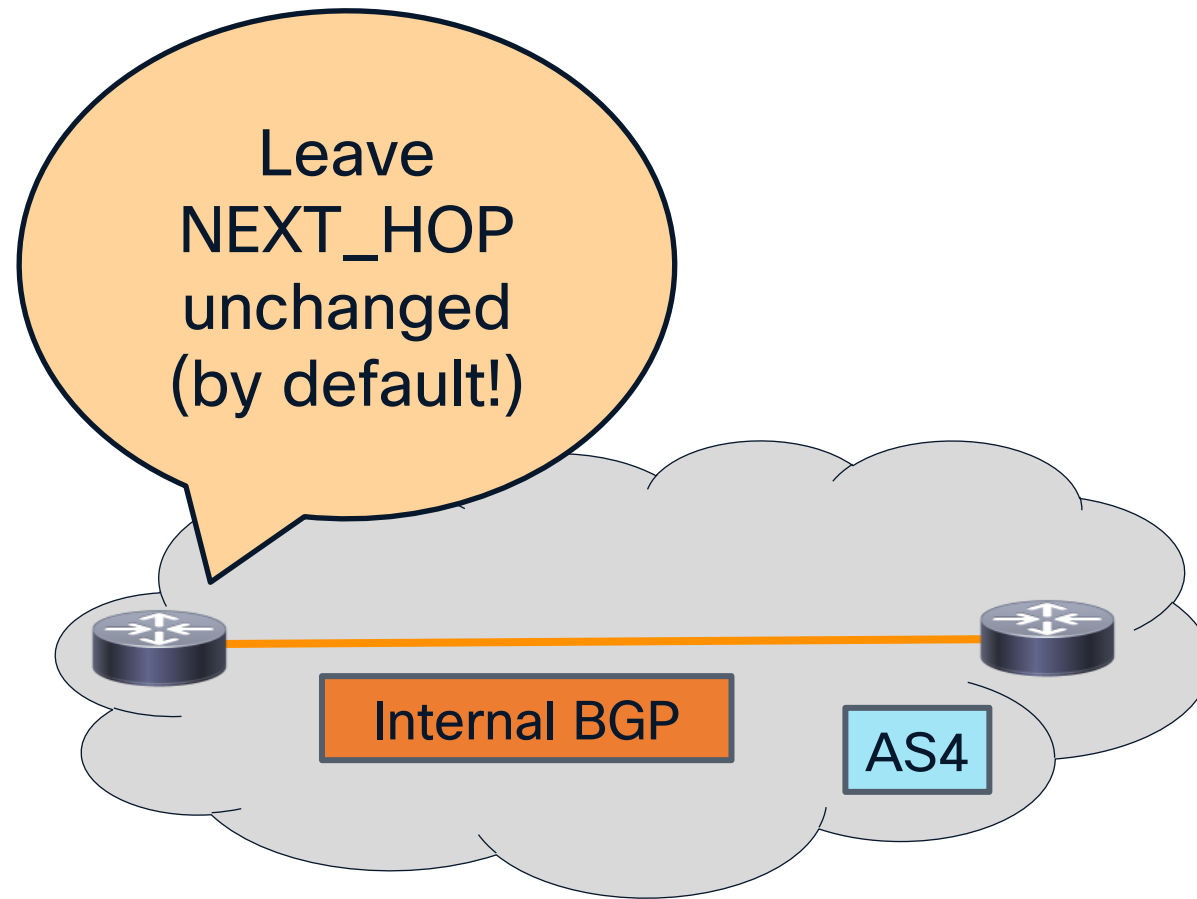
Internal vs External BGP



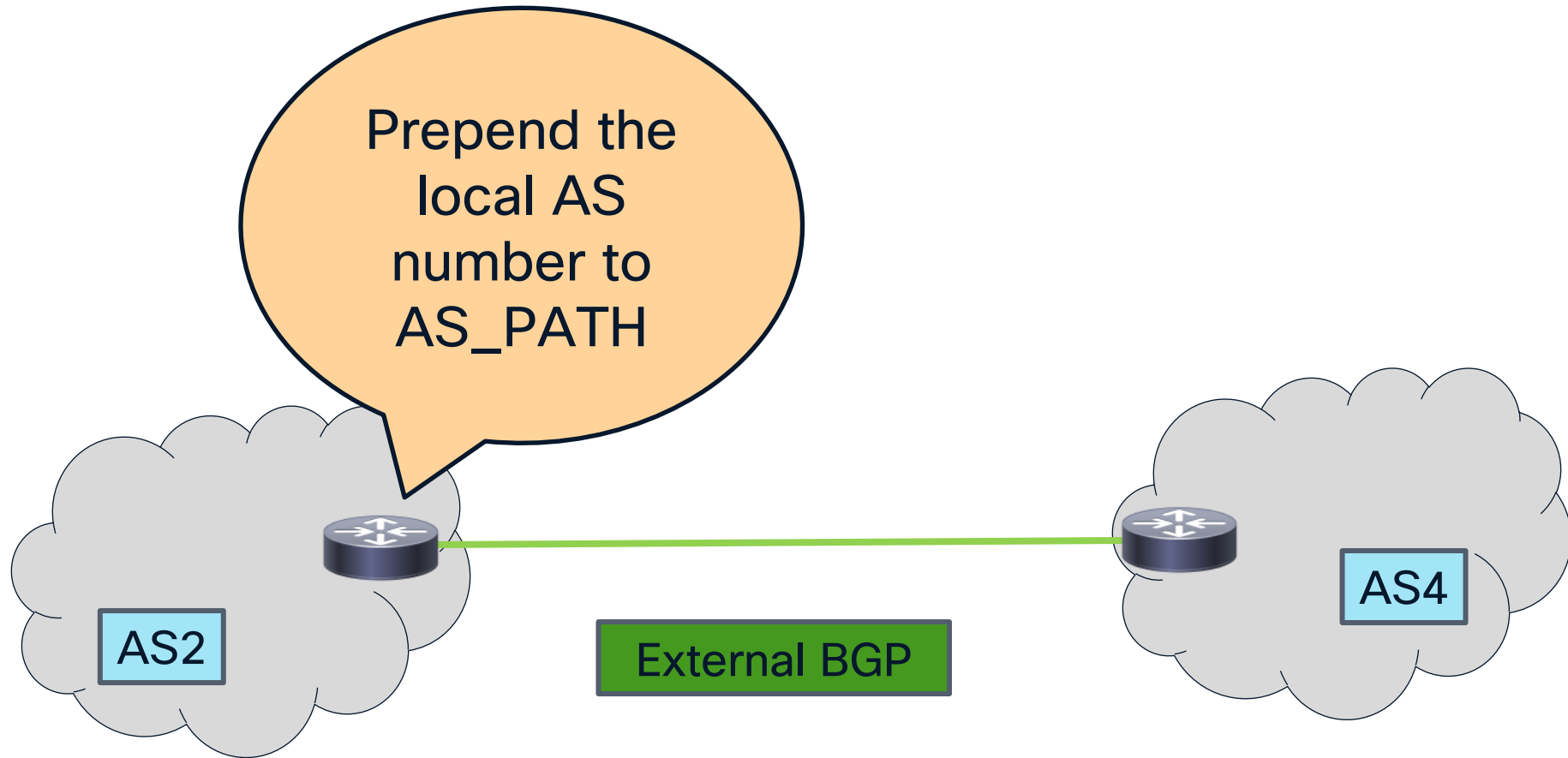
NEXT_HOP in eBGP



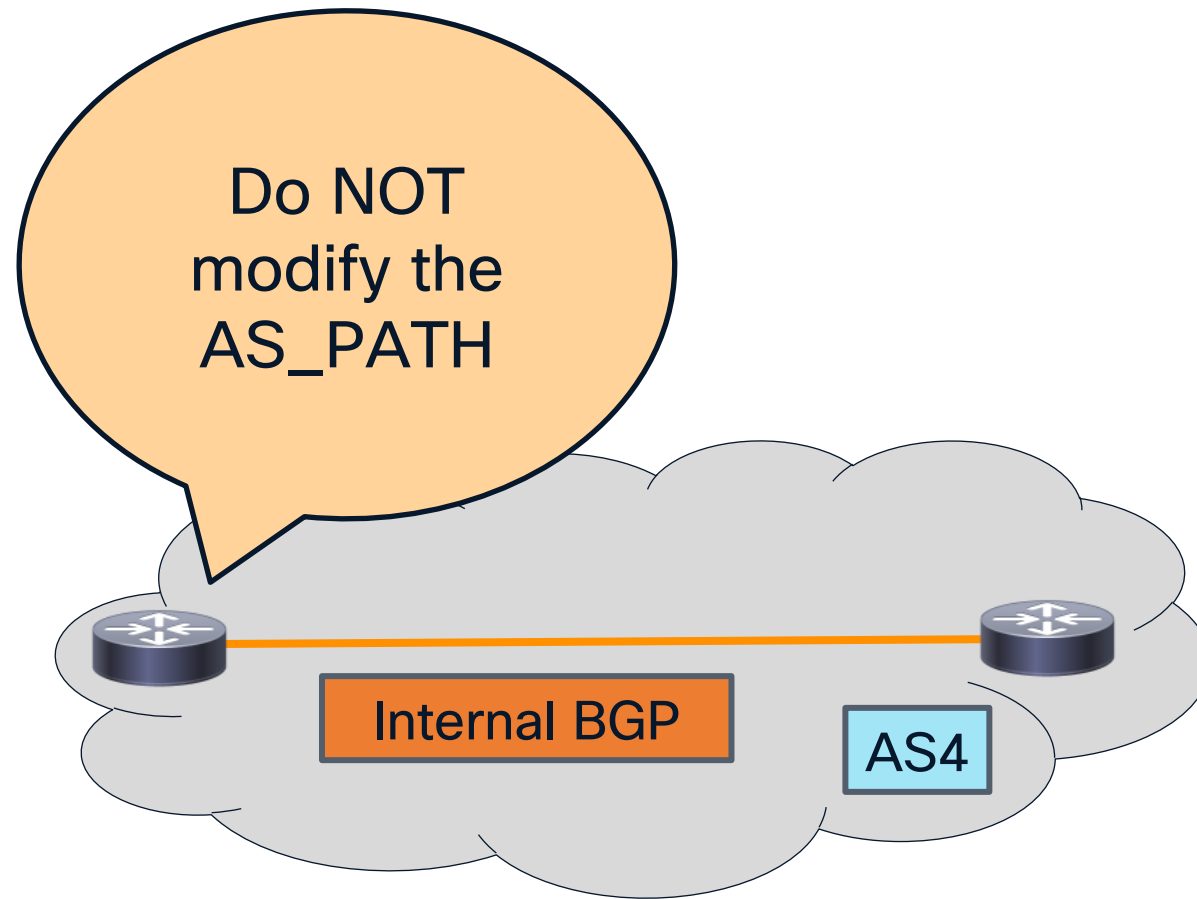
NEXT_HOP in iBGP



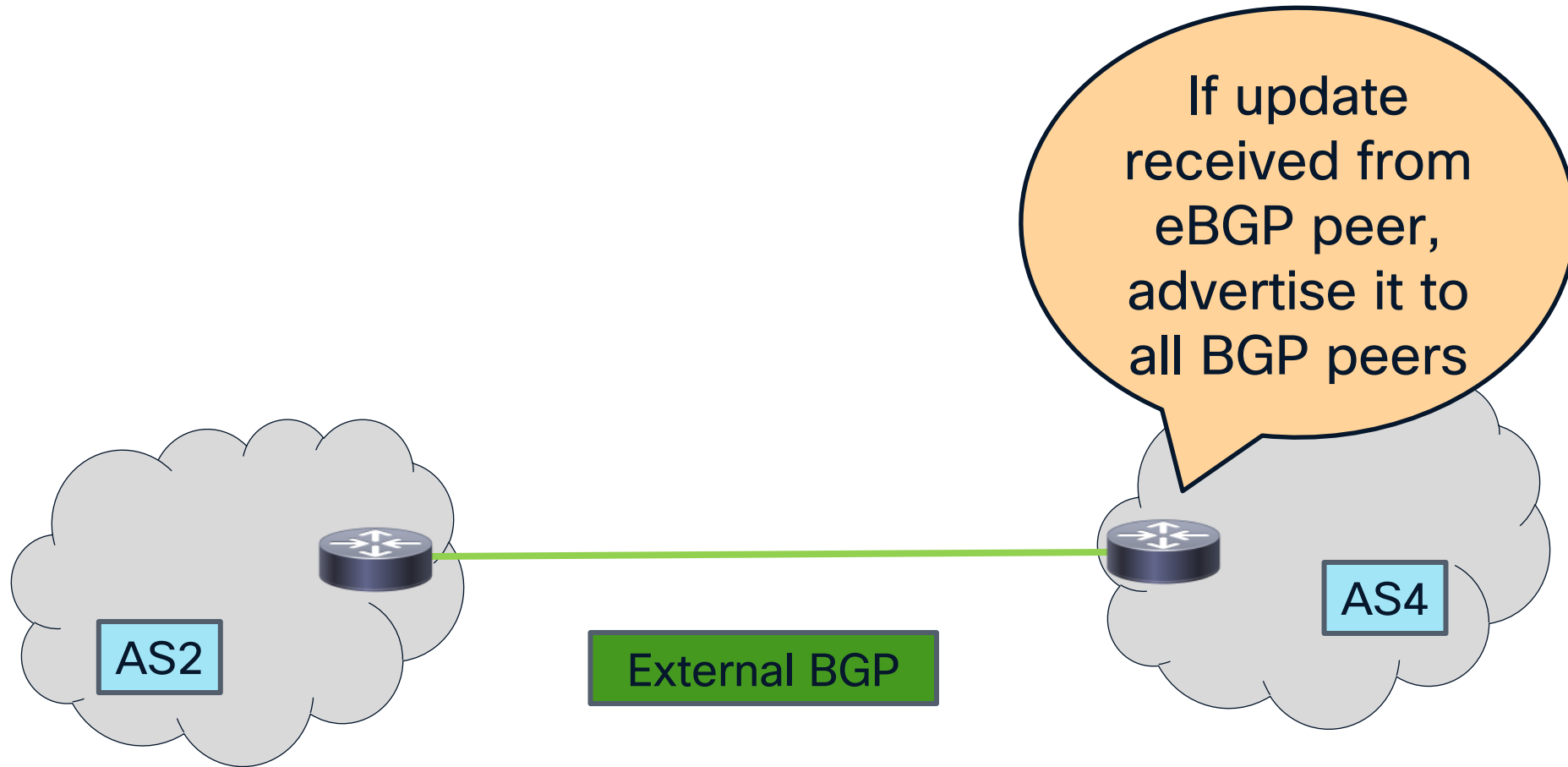
AS_PATH in eBGP



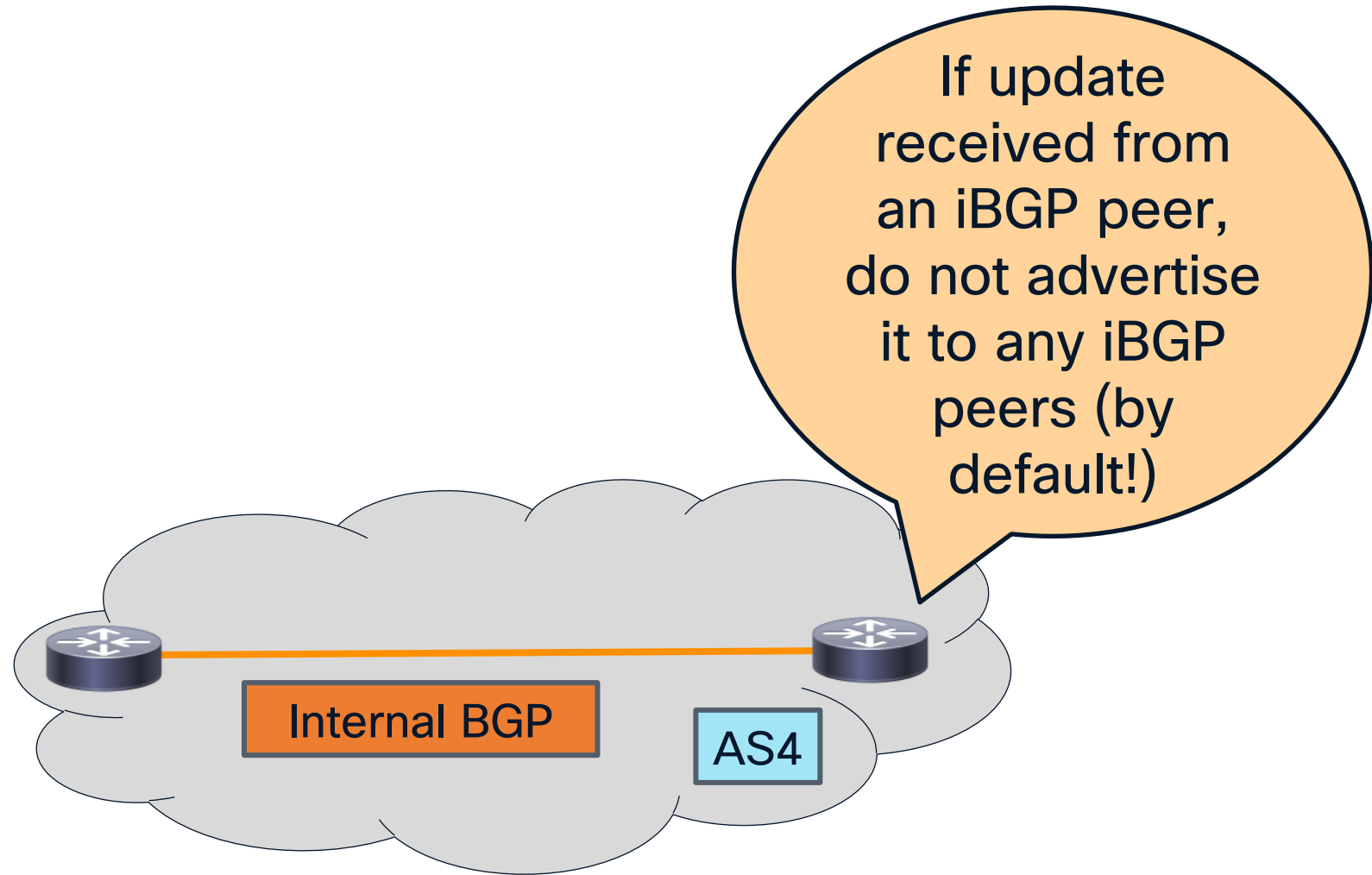
AS_PATH in iBGP



Updates in eBGP



Updates in iBGP



Securing BGP

TCP Authentication Option

- BGP relies on TCP support to provide optional authentication
- Initially, TCP only supported MD5-based hash (RFC 2385)
- RFC 5925 brings in TCP Authentication Option (TCP-AO)
- Cryptographically stronger protection based on hash message authentication codes; does not prescribe any particular hash function
- IOS XE supports
 - hmac-sha-1
 - hmac-sha-256
 - aes-128-cmac

Configuring BGP authentication with TCP-AO

- Configuring BGP authentication with TCP-AO
- Parameters of the TCP Authentication Option need to be configured in a specialized key chain of the “tcp” type

```
key chain bgpkeys tcp
key 1
send-id 123
recv-id 123
cryptographic-algorithm aes-128-cmac
key-string s3cr3tP4ss
```

- The key chain then must be applied to the neighbor

```
router bgp 64512
neighbor ... ao bgpkeys
```

Secure eBGP Default Policy

- RFC 8212 stipulates a strict default behaviour for eBGP
 - If no explicit inbound policy for a peer is configured, ignore any received routes from this peer
 - If no explicit outbound policy for a peer is configured, do not advertise any routes to this peer
- This serves multiple purposes
 - Preventing a router from inadvertently becoming a transit router
 - Preventing a router from advertising unintended routes
 - Preventing a router from having its existing routing inadvertently changed
 - Preventing a router from crashing due to receiving too many routes

Secure eBGP policy in IOS XE

- This has been the default behavior in IOS-XR since day one
- In IOS XE, this behaviour can be activated by:

router bgp 64512

bgp safe-ebgp-policy

- Both IOS-XR and IOS XE implement RFC 8212 with a quirk
- An eBGP neighbor must be explicitly configured with both inbound and outbound policy, otherwise no routes will be exchanged with it

Best Path Selection Algorithm

Best Path Selection in BGP

BGP selects the best path based on several constraints:

- Loop-free
- Shortest AS path
- Exits the local AS quickly as possible
- Avoids unnecessary updates for insignificant changes
- Allows admin override

BGP aims to choose one best path per NLRI for local use and advertisement to peers.

10,000 Miles View at BGP Best Path Selection

When a BGP speaker learns multiple paths for an NLRI, it selects the best path as follows:

1. Choose the first variant as the initial best path.
2. Compare each subsequent variant to the current best path.
3. Update the best path if a better variant is found.
4. Continue until all variants are inspected.

Before Getting to the Nitty Gritty...



Router selecting the best path



Generic router (unspecific)



The resulting next hop



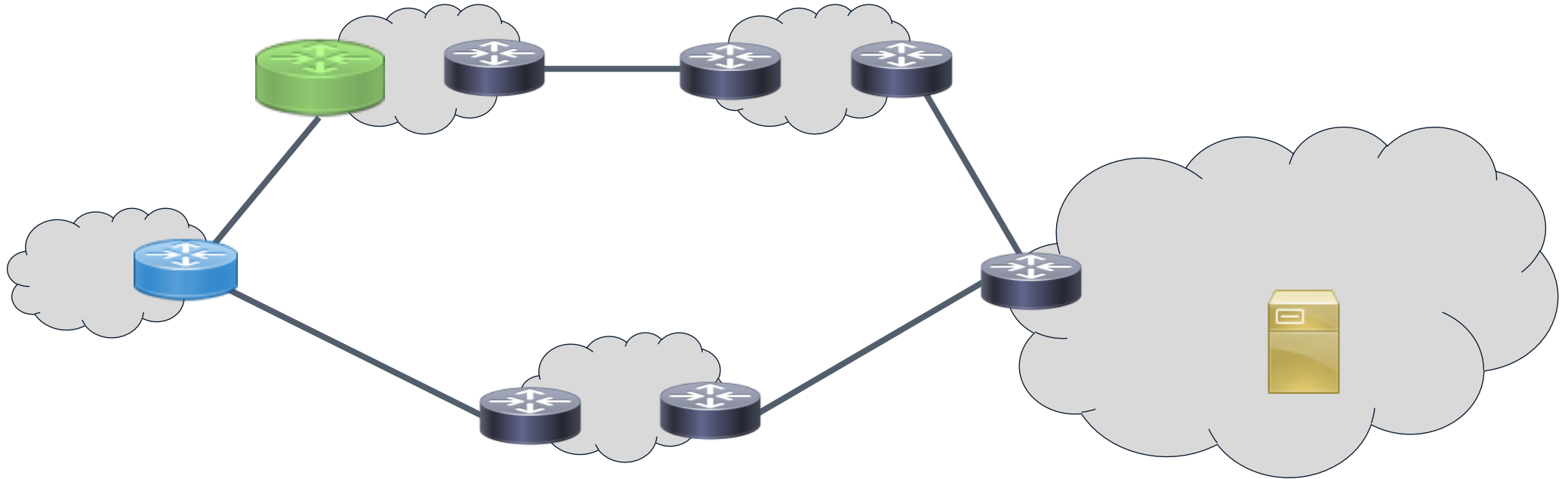
Destination (NLRI)

Before diving into the BGP best path algorithm steps, keep in mind:

- For every NLRI, BGP always compares the current best path to a variant in its database (injected locally or learned from peers)
- The best path is both used locally (if it makes sense) and advertised to other peers, subject to the advertisement rules and policies

In upcoming slides, the diagrams demonstrate typical scenarios but are not exhaustive

The logic behind BGP best path selection (1)

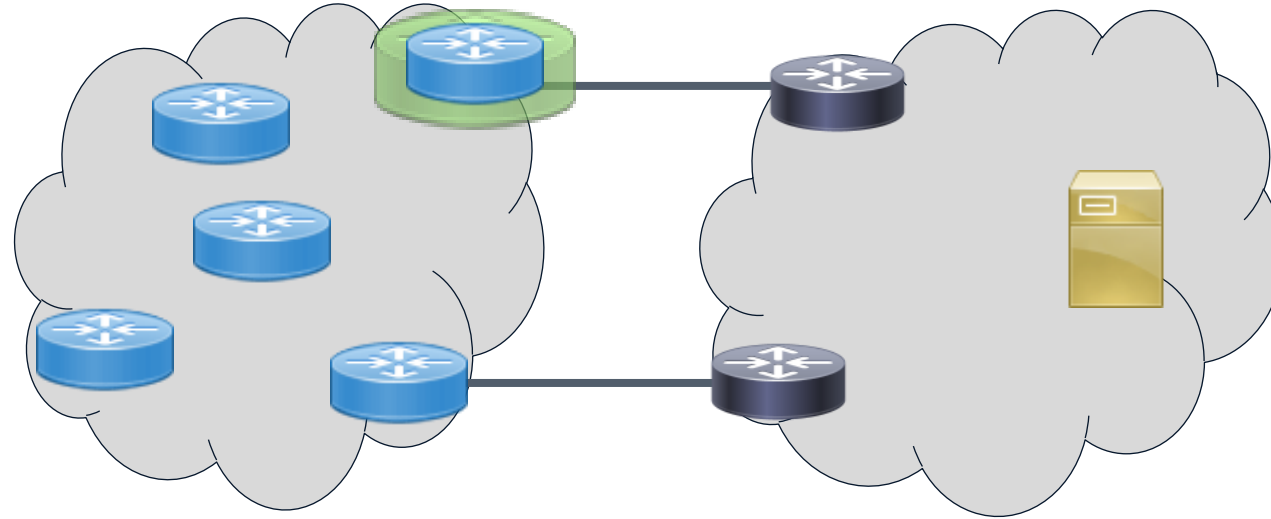


Step 1: Prefer the path with the higher WEIGHT

Rationale: Always have means to **override** the path choice **locally**

Note: This is an override rule

The logic behind BGP best path selection (2)

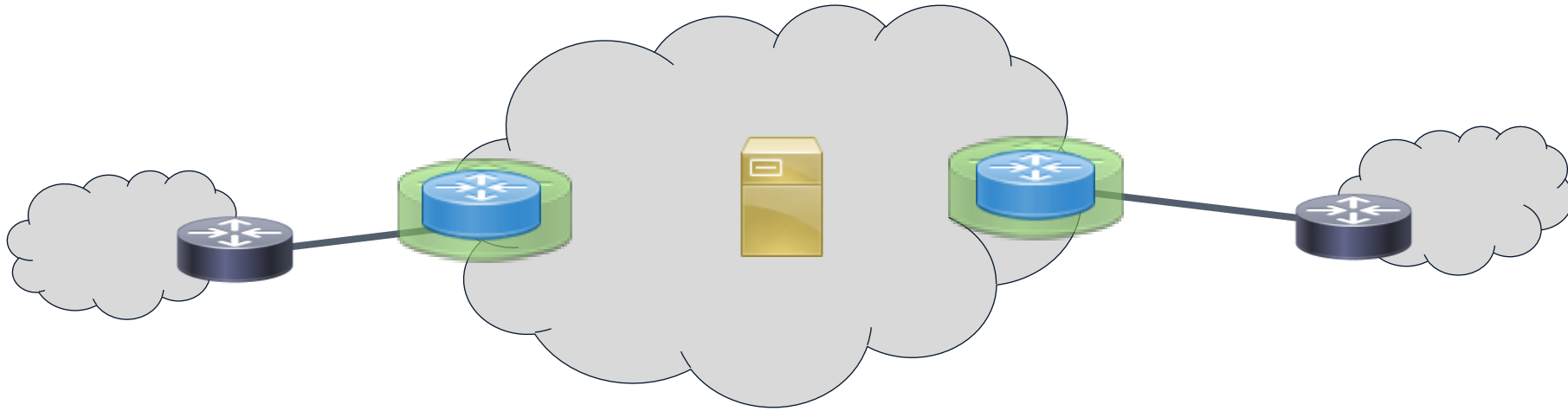


Step 2: Prefer the path with the higher LOCAL_PREF

Rationale: Have means to **override** the best path **for the entire AS** from a single exit point

Note: This is an override rule

The logic behind BGP best path selection (3)

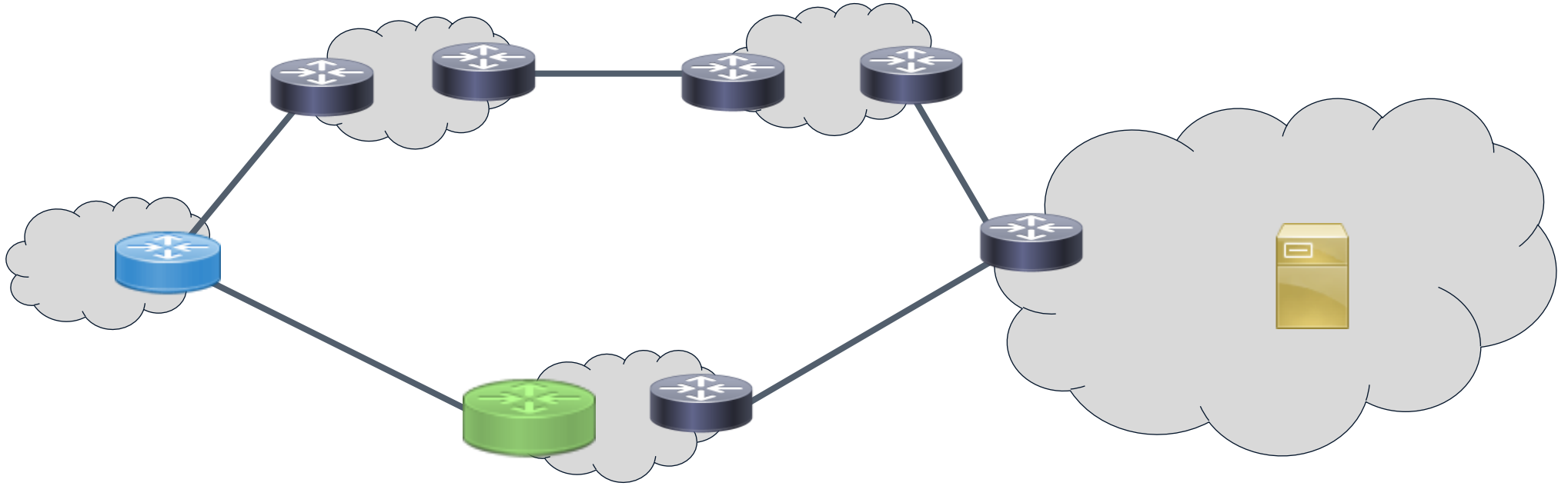


Step 3: Prefer the locally originated path (network, redistribution, aggregation)

Rationale: I get a chance to **speak on behalf of my own local AS**

Note: The best route is not just for me to use but also to advertise to **others** so that **they know**

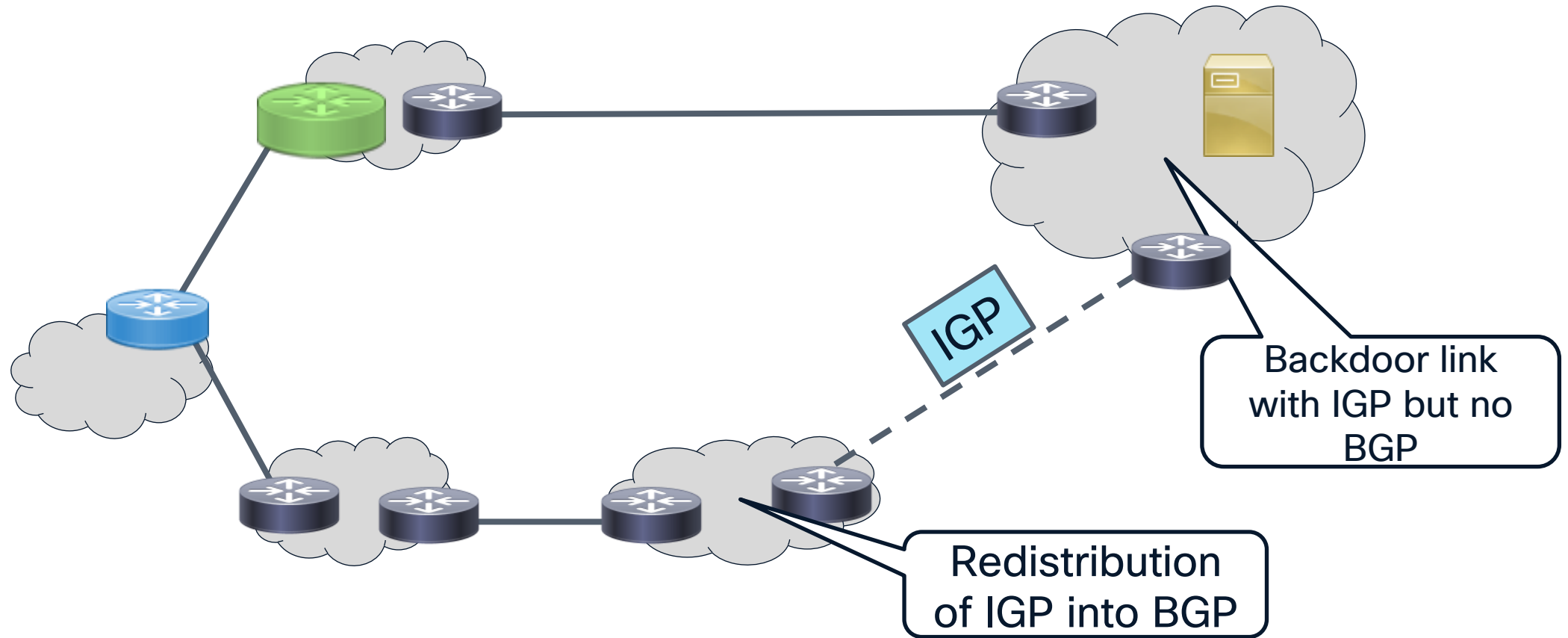
The logic behind BGP best path selection (4)



Step 4: Prefer the path with the shortest AS_PATH / AS4_PATH

Rationale: Traverse the **least amount of autonomous systems**

The logic behind BGP best path selection (5)

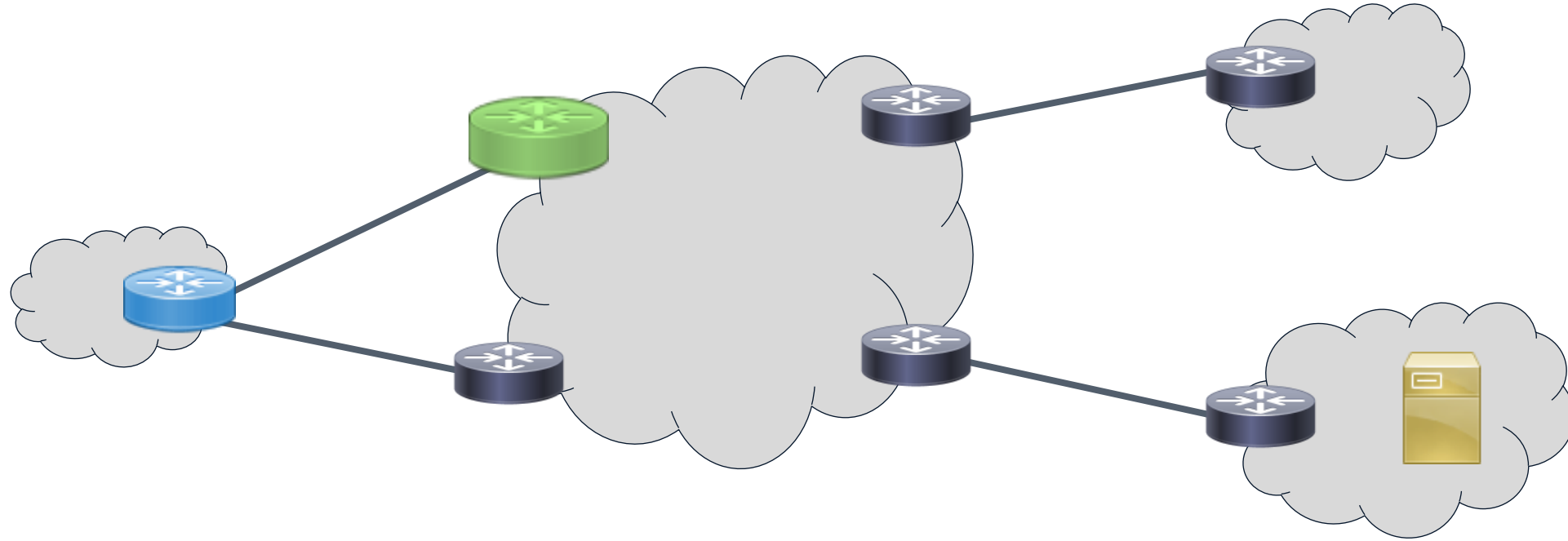


Step 5: Prefer the path with the lower ORIGIN code

Rationale: Take the *most trustworthy* path

Note: IGP is lower than EGP, EGP is lower than Incomplete

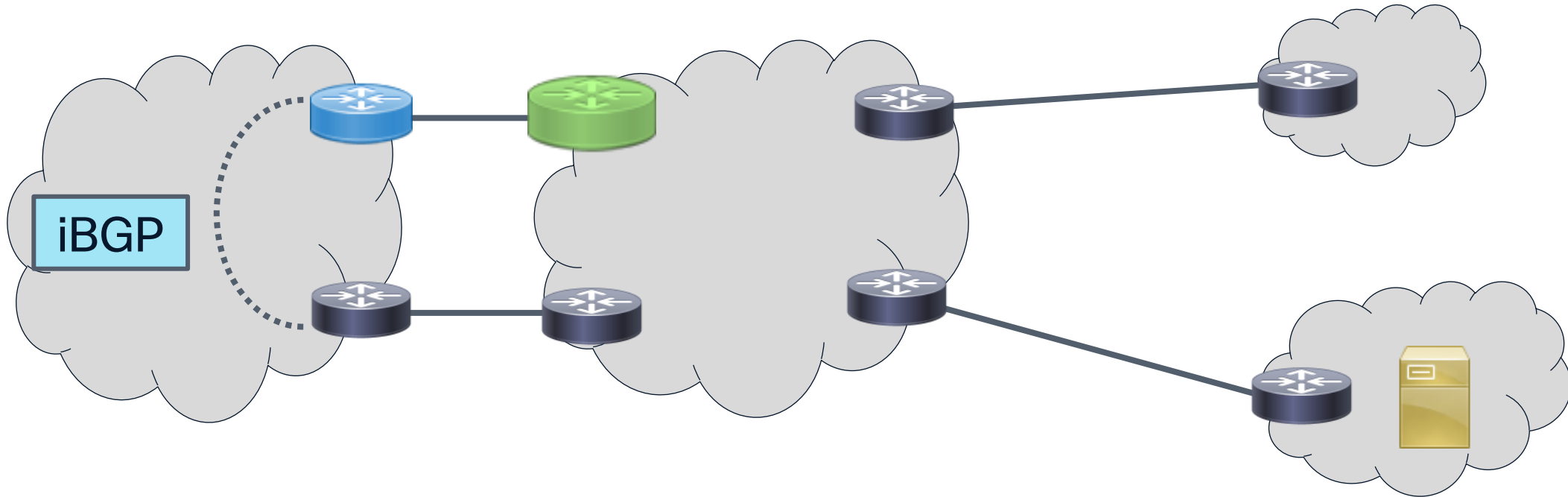
The logic behind BGP best path selection (6)



Step 6: Prefer the path with the lower MULTI_EXIT_DISC

Rationale: Respect the *preferred path hint* indicated by the neighbor AS

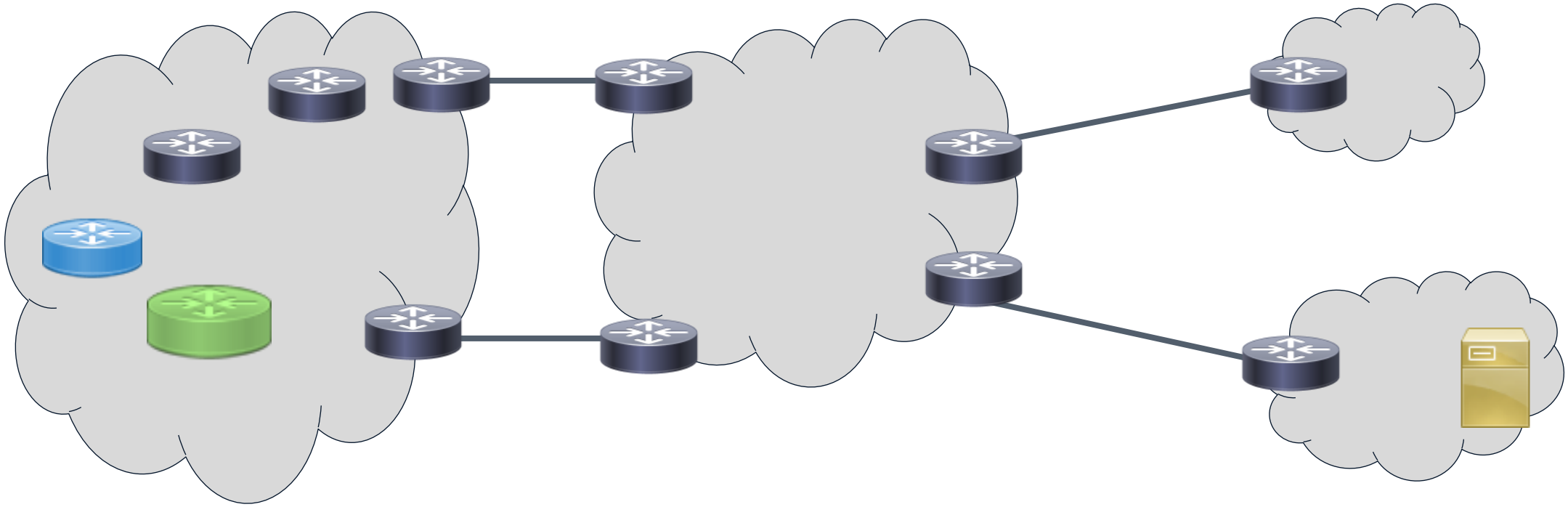
The logic behind BGP best path selection (7)



Step 7: Prefer eBGP-learned path over iBGP-learned one

Rationale: If you need to *leave* the local AS, *leave right away if you can*

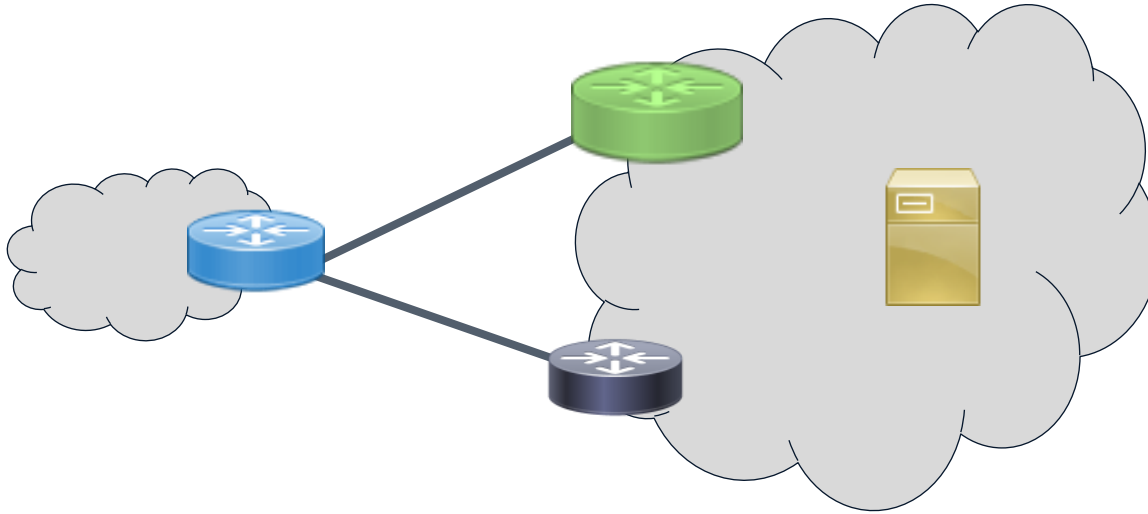
The logic behind BGP best path selection (8)



Step 8: Prefer the path with the lower IGP metric to the next hop

Rationale: If you need to *traverse* the local AS but *can't leave* right away,
just *take the shortest path toward the exit*

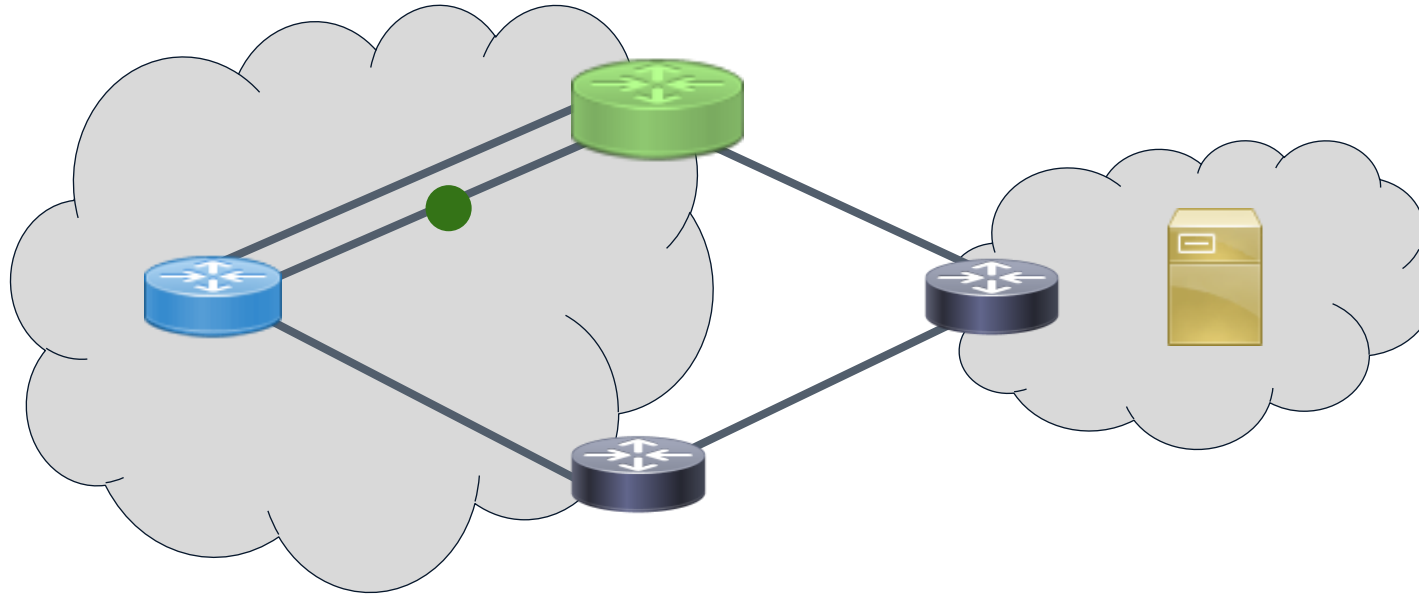
The logic behind BGP best path selection (9)



Step 9: If both paths are learned via eBGP, prefer the older one

Rationale: The eBGP paths are, by this point, **effectively equal** – so **don't bother** updating anything

The logic behind BGP best path selection (10-12)



Steps 10-12: Prefer the path learned from the BGP peer with the lower Router ID,

then with the shorter CLUSTER_LIST,

then from the BGP peer with the lower peering IP address

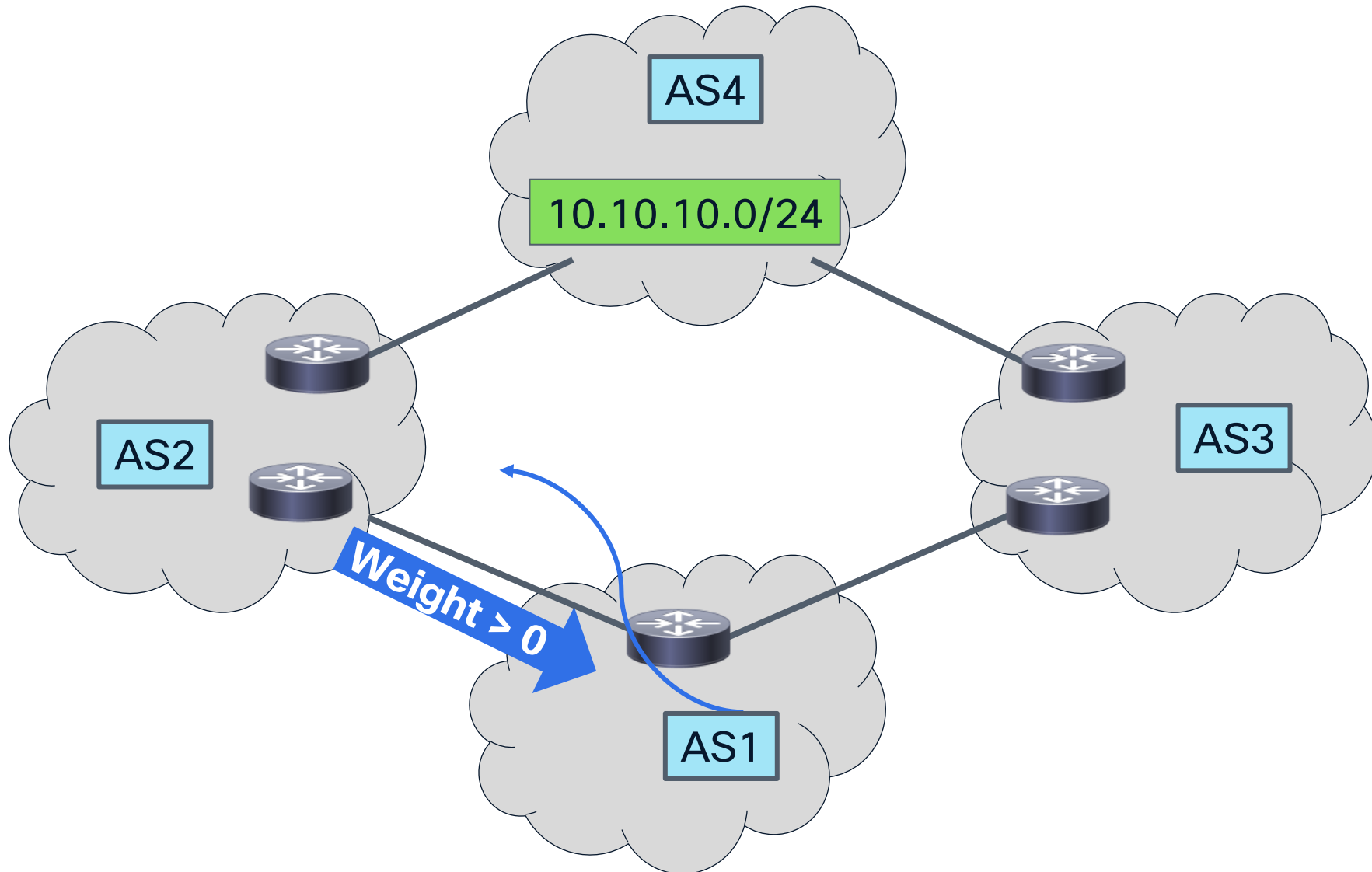
Rationale: Technical tiebreakers to arrive at *exactly one best path*

Quick Recap of Best Path Selection in BGP

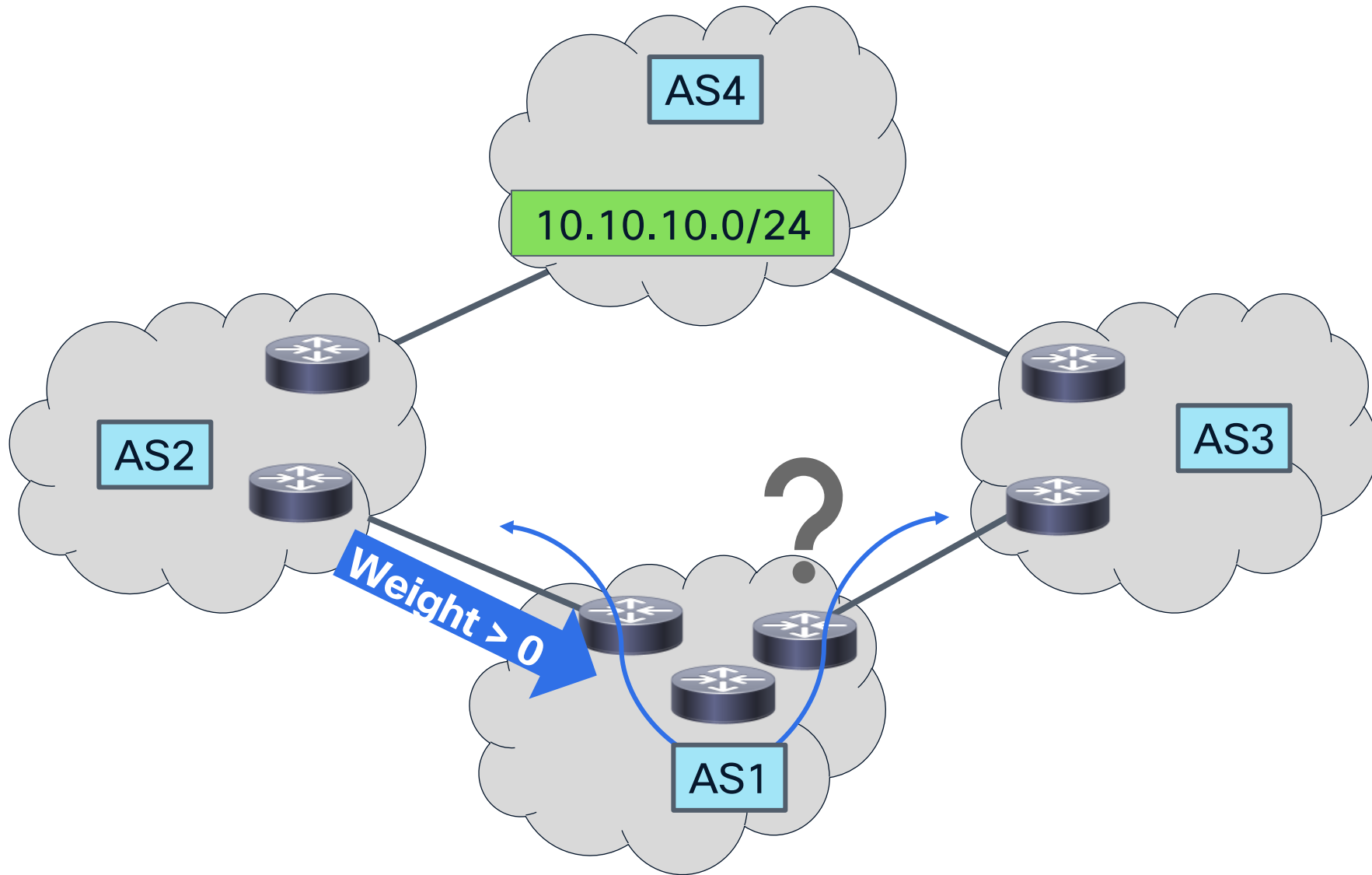
Attributes	Explanation
Next-hop must be accessible	Next-hop in forwarding table
Weight	Local to the router
Local preference	Spread within AS
Originated locally	Via redistribute or network statement
AS-path	Number of ASes in the AS-path attribute
Origin	IGP < EGP < INCOMPLETE
MED	Between paths from same AS
Path type	EBGP over IBGP
Router ID	Lower is preferred.

Policy Control and Traffic Engineering

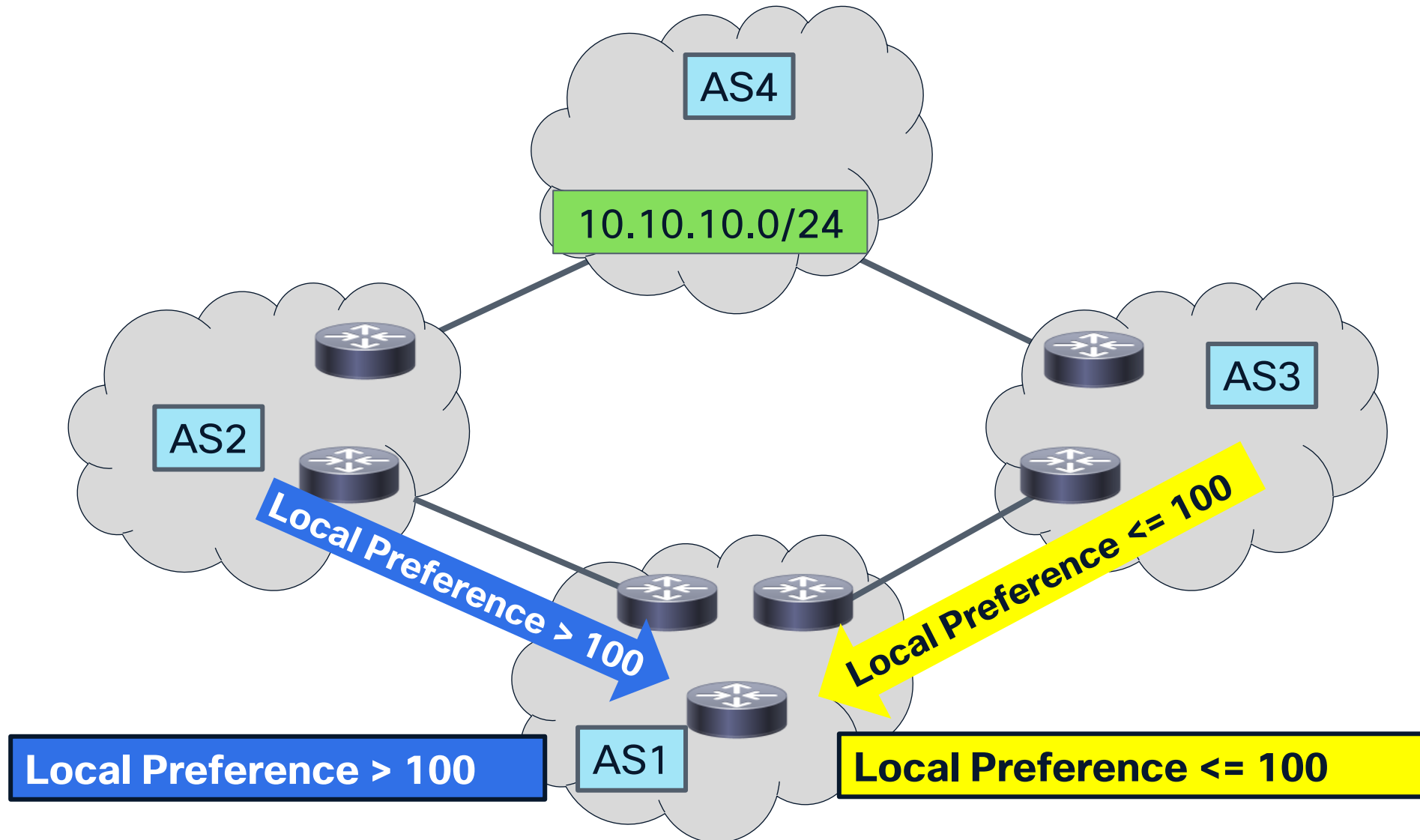
Outbound Traffic - Weight



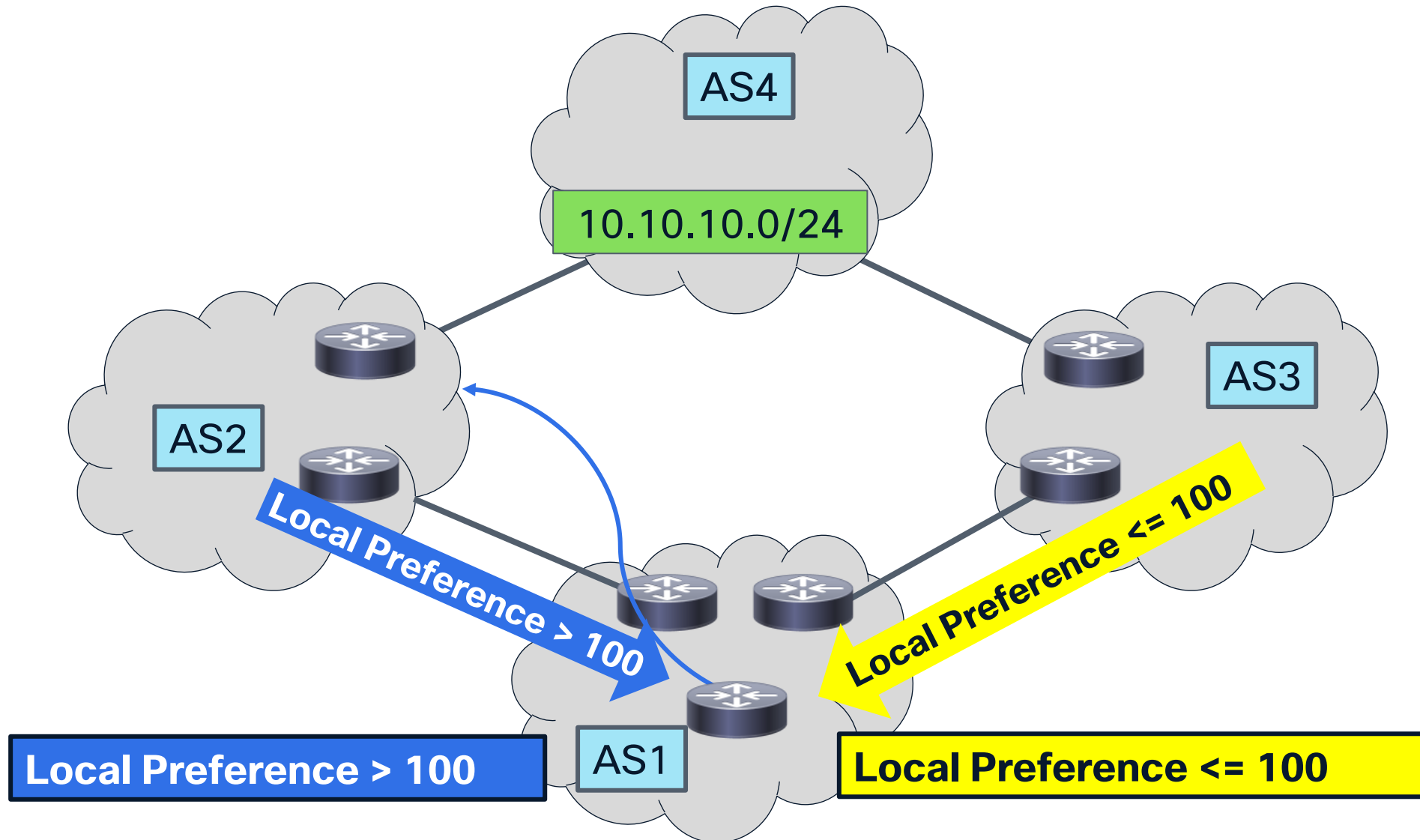
Outbound Traffic - Weight



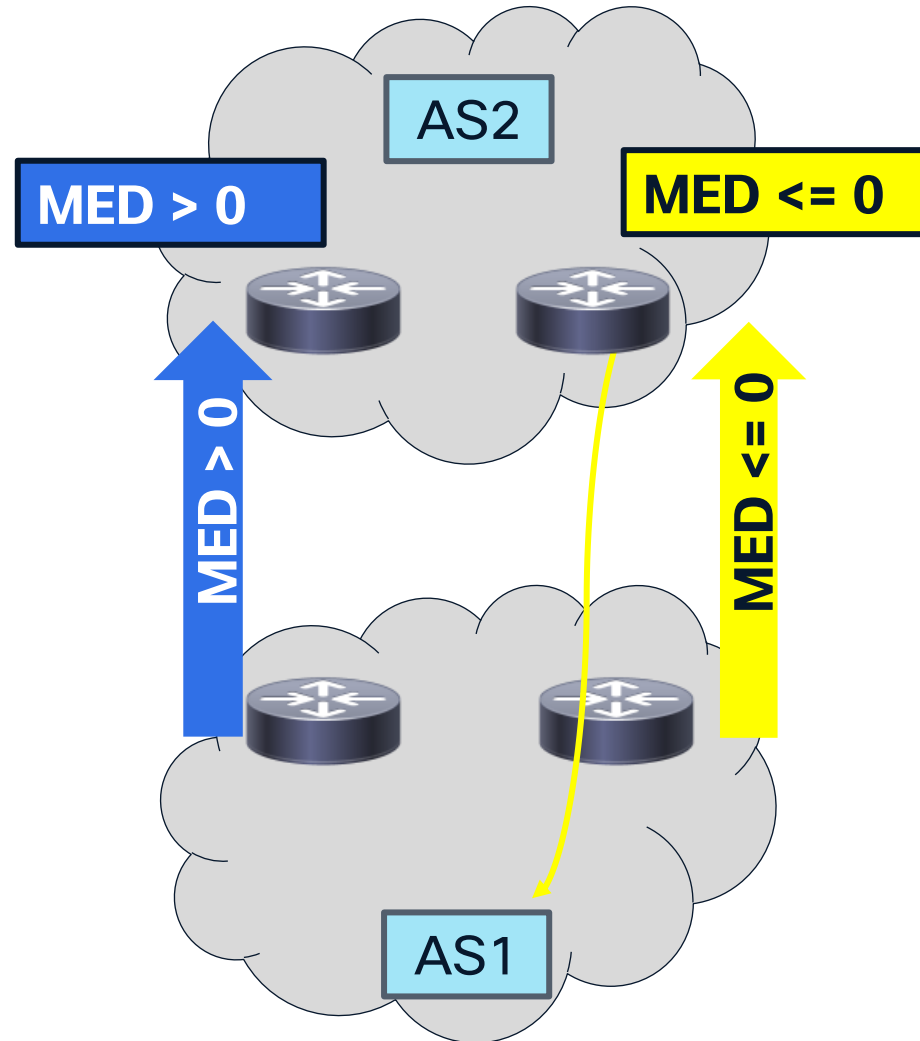
Outbound Traffic – LOCAL_PREF



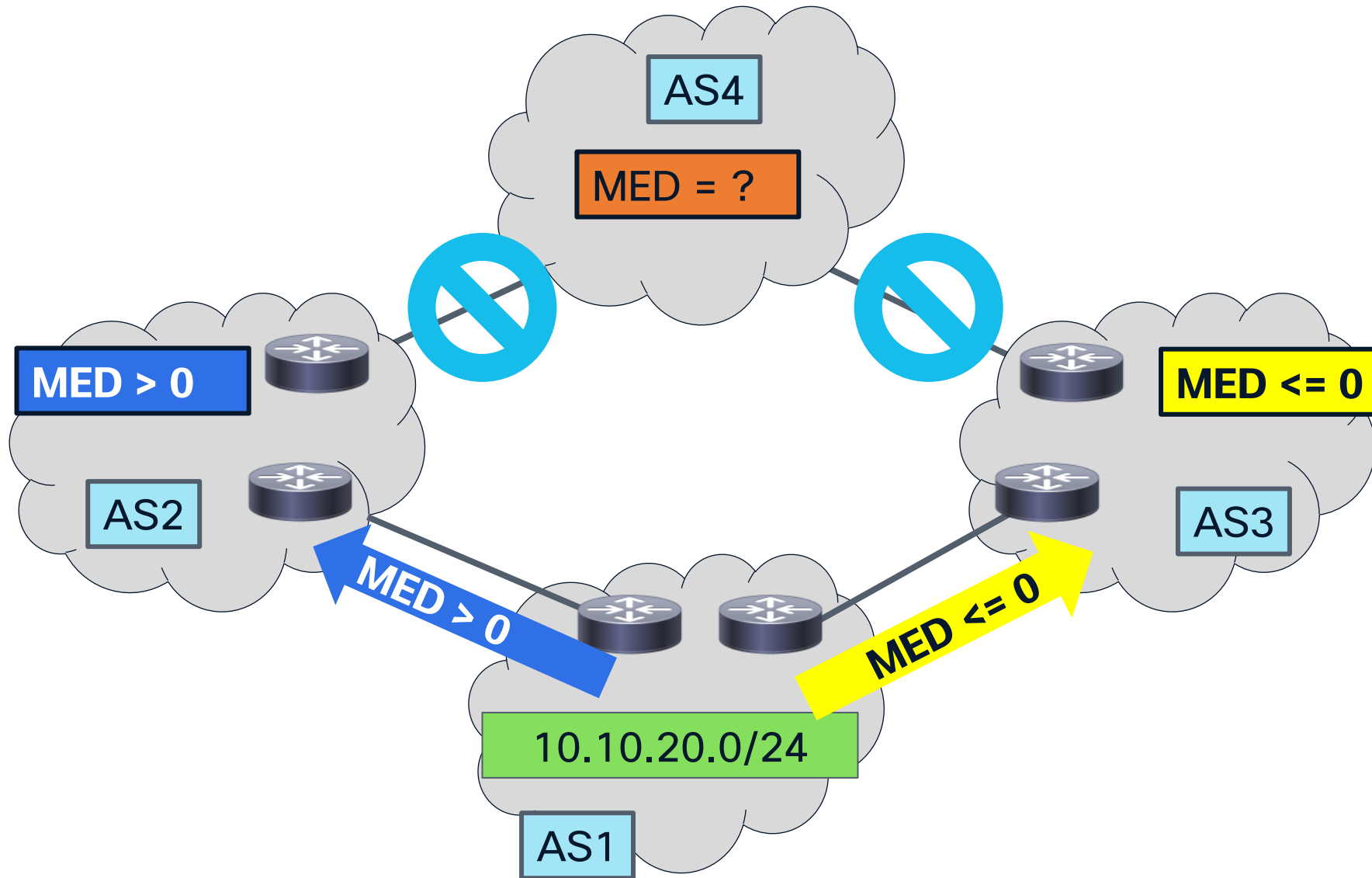
Outbound Traffic – LOCAL_PREF



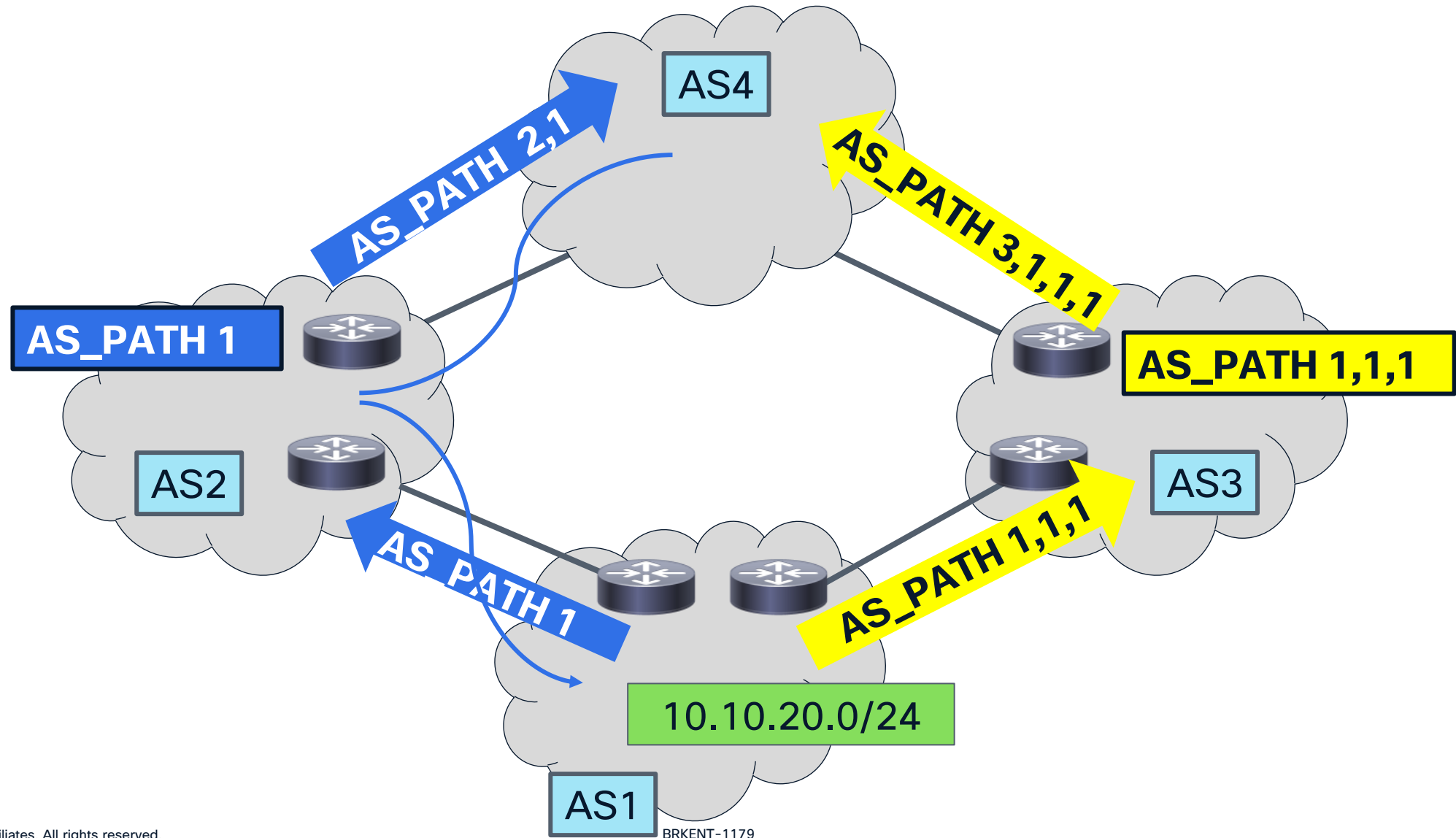
Inbound Traffic – MULTI_EXIT_DISC



Inbound Traffic – MULTI_EXIT_DISC



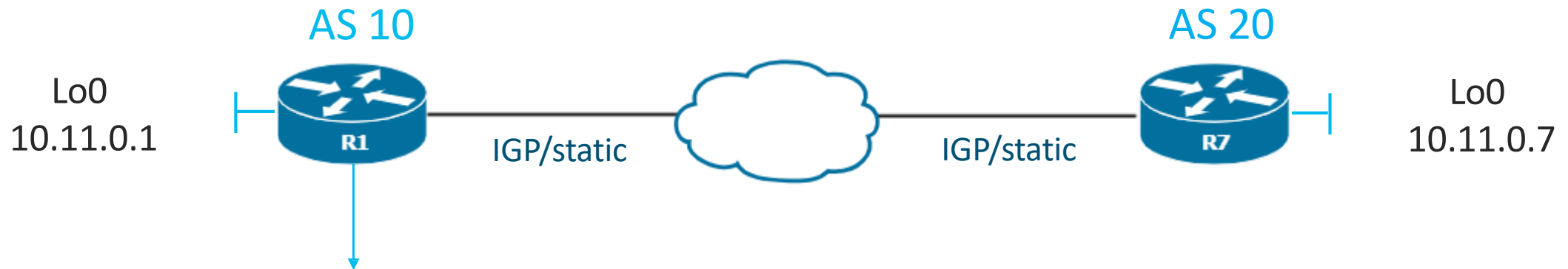
Inbound Traffic - AS_PATH



Troubleshoot BGP Peering Issues

Troubleshoot Peering issues

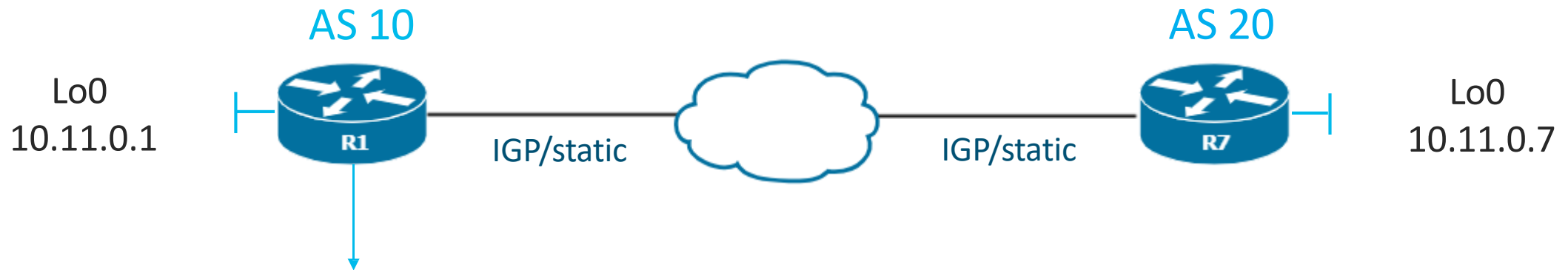
Verify Layer 3 connectivity



```
R1# ping 10.11.0.7 source 10.11.0.1
Sending 5, 100-byte ICMP Echos to 10.11.0.7, timeout is 2 seconds: Packet
sent with a source address of 10.11.0.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 m
```

Troubleshoot Peering issues

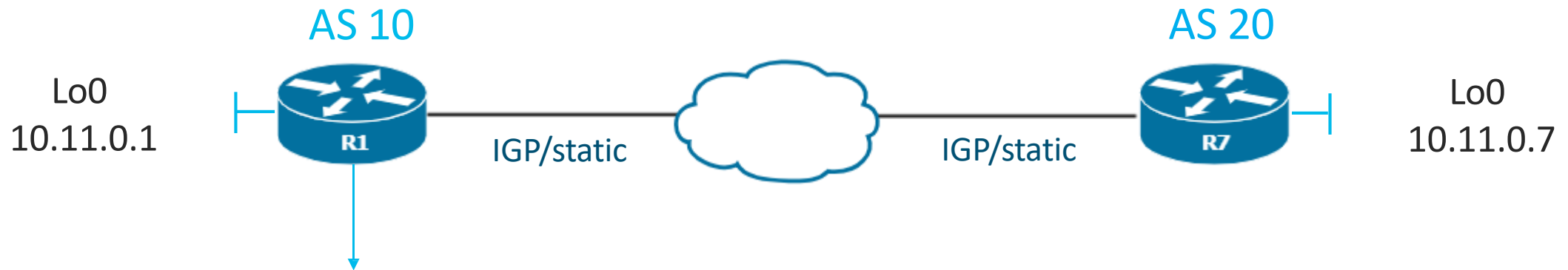
Verify Layer 4 connectivity



```
R1# telnet 10.11.0.7 179 /source-interface Loopback0
Trying 10.11.0.7, 179 ... Open
```

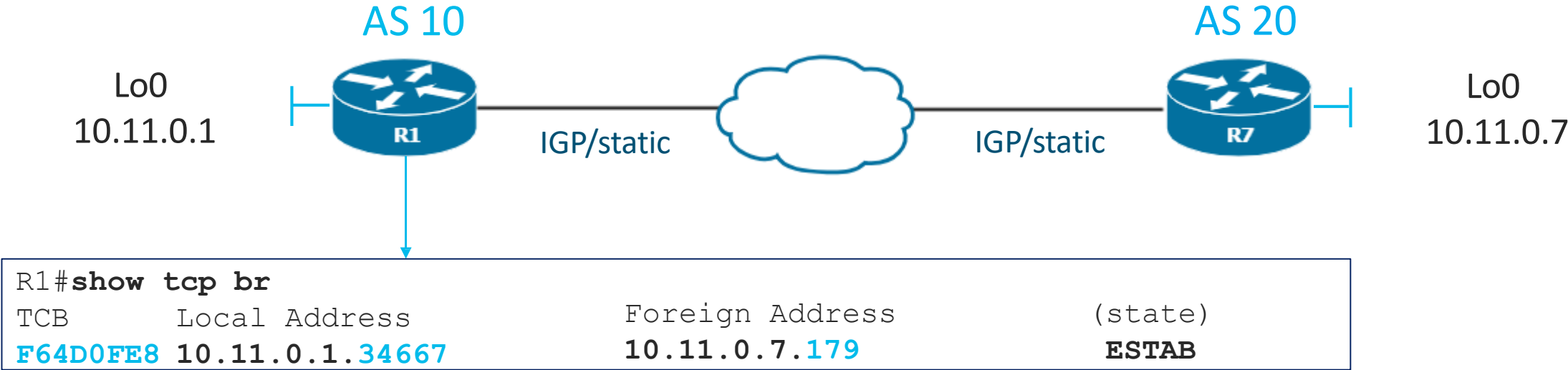
Troubleshoot Peering issues

Verify **Layer 4** connectivity



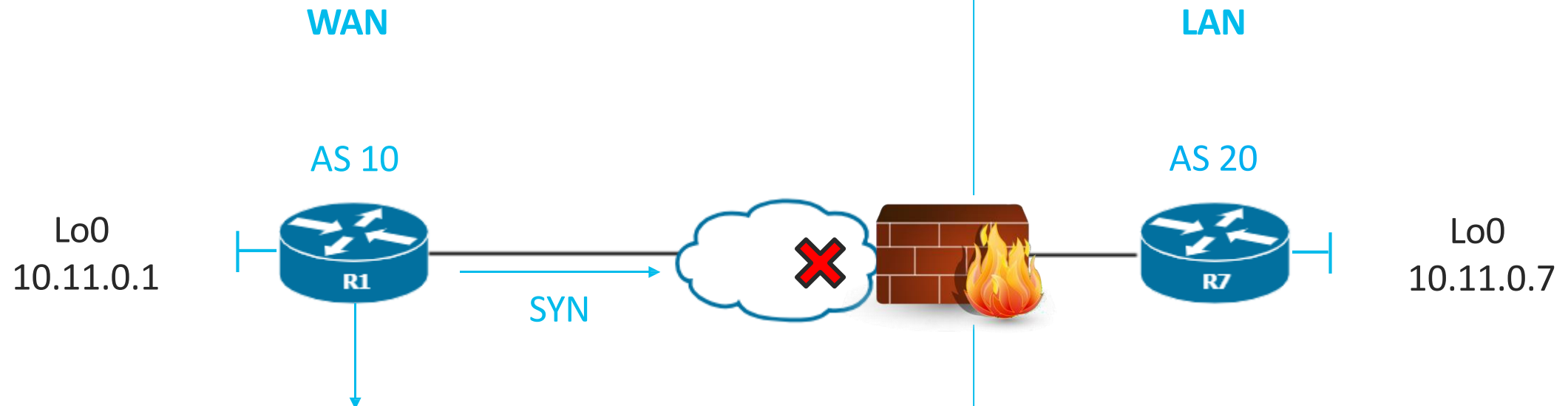
```
R1# telnet 10.11.0.7 179 /source-interface Loopback0
Trying 10.11.0.7, 179 ... Open
```

Verify TCP connection



Verify TCP connection

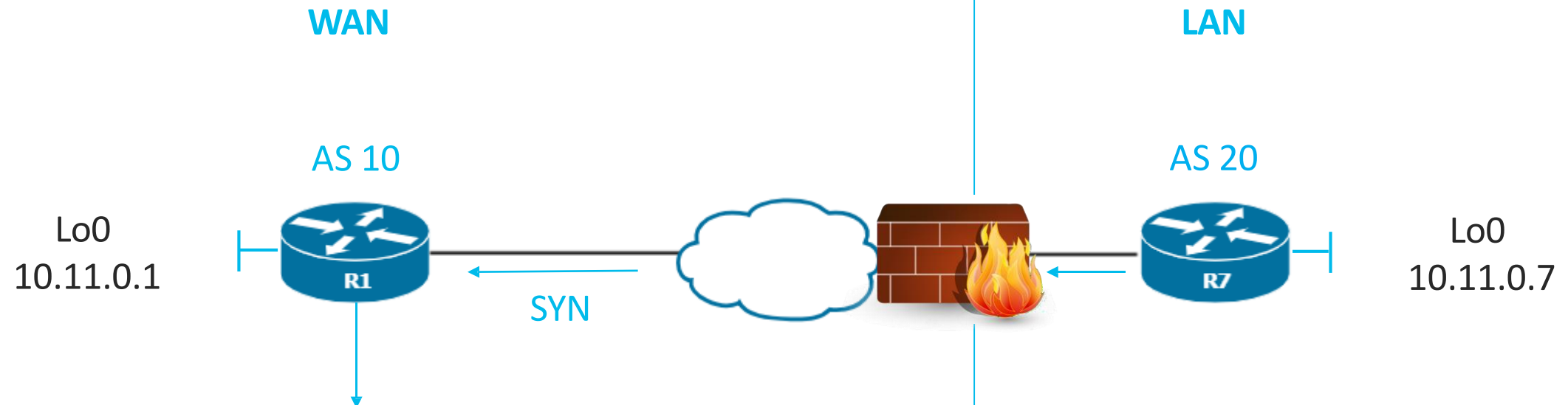
Change transport connection mode to **passive**



```
R1#show tcp tcb F64D0FE8
Local host: 10.11.0.1, Local port: 34667
Foreign host: 10.11.0.7, Foreign port: 179
Status Flags: active open
Option Flags: nagle, path mtu capable
```

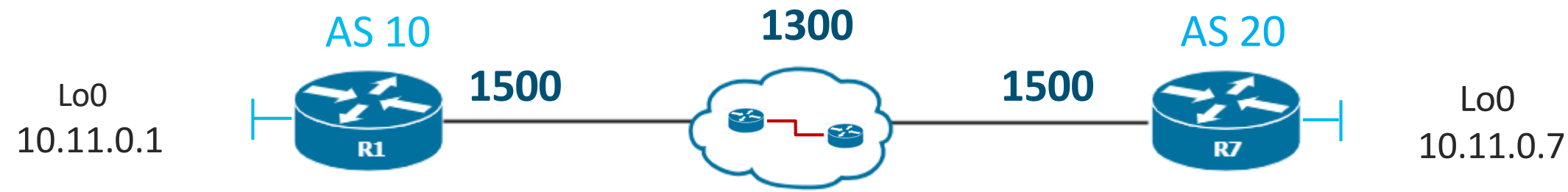
Verify TCP connection

Change transport connection mode to **passive**

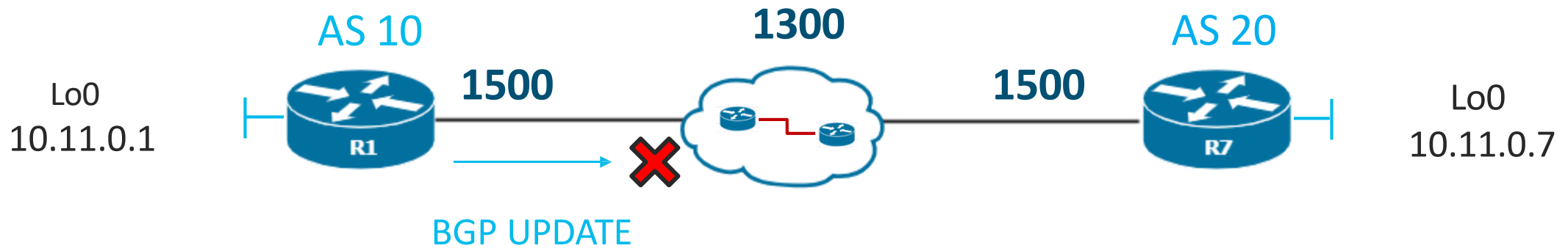


```
R1#show tcp tcb F64D0C60
Local host: 10.11.0.1, Local port: 179
Foreign host: 10.11.0.7, Foreign port: 64440
Status Flags: passive open, gen tcbs
Option Flags: nagle, path mtu capable
```

Troubleshoot MTU issues

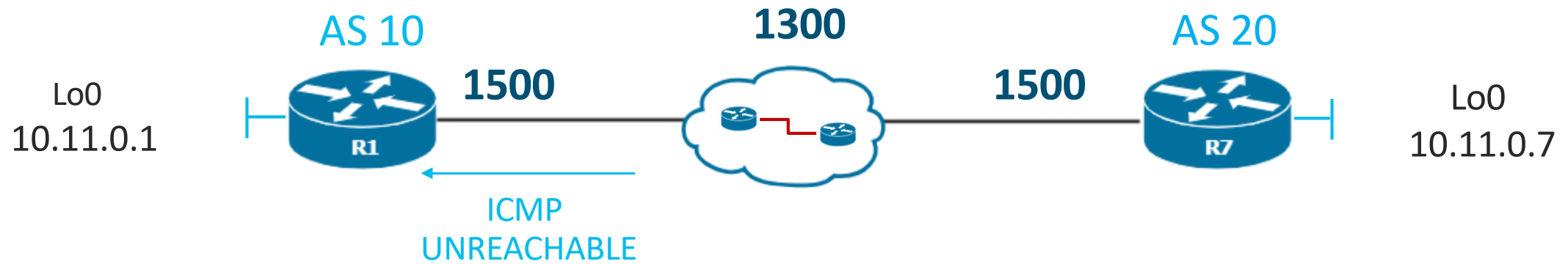


Troubleshoot MTU issues



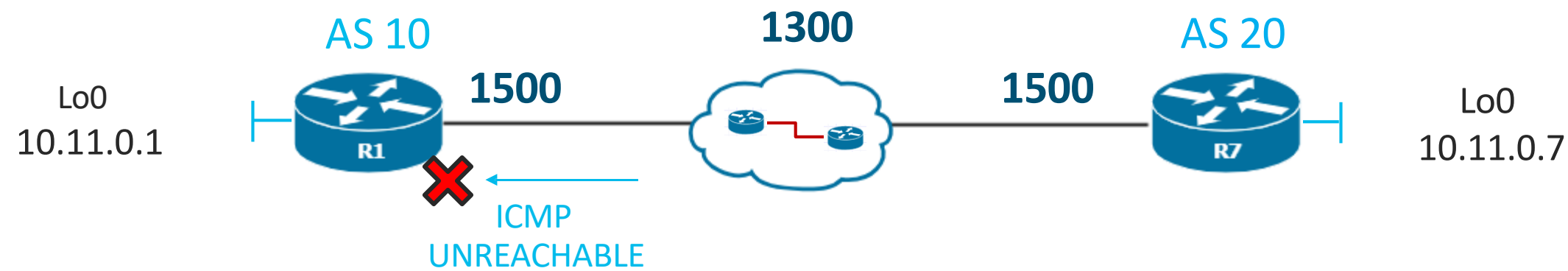
- BGP UPDATE packets are sent with the DF-bit set
- BGP relies on PTMUD to identify the largest packet size which can be sent without fragmentation

Troubleshoot MTU issues

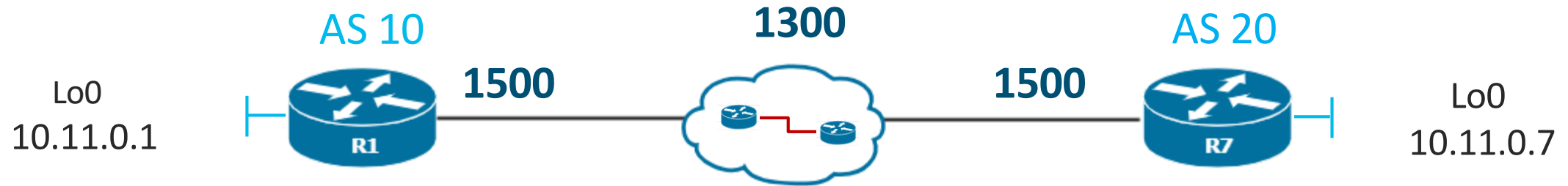


- **PTMUD** uses on ICMP to inform BGP of the **lowest MTU** in the transit path

Troubleshoot MTU issues



Troubleshoot MTU issues



- Perform **df-bit ping** to identify **highest MTU without fragmentation** in **path**
- **ip tcp mss**
- **ip tcp adjust-mss**
- **Disable PTMUD** to allow BGP to establish with a lower MSS

Keepalive and Holdtime

- Holdtime is negotiated via OPEN messages

180 seconds is default

- KEEPALIVE transmitted every 60s

3 seconds: Lowest non-zero setting

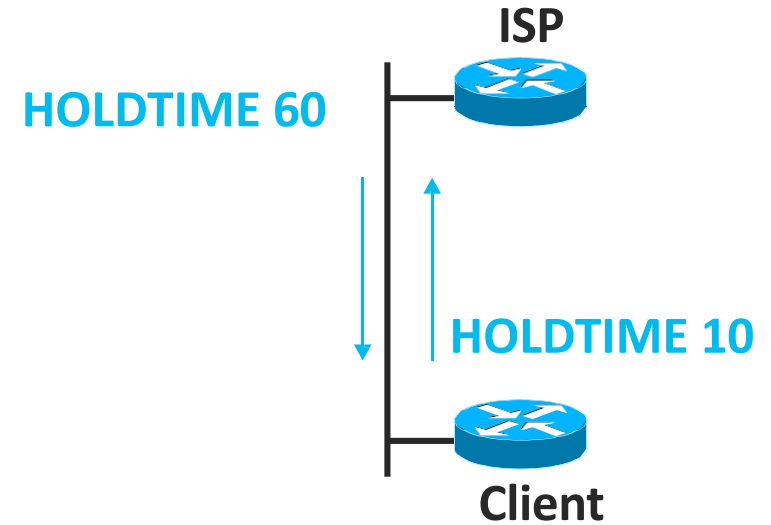
```
ISP(config-router)# neighbor x.x.x.x timers X Y
```

```
  X. (0-65535) is keepalive
```

```
  Y. (0-65535) is holdtime
```

Keepalive and Holdtime

- Holdtime is negotiated via **OPEN** messages
- **Lowest holdtime wins**



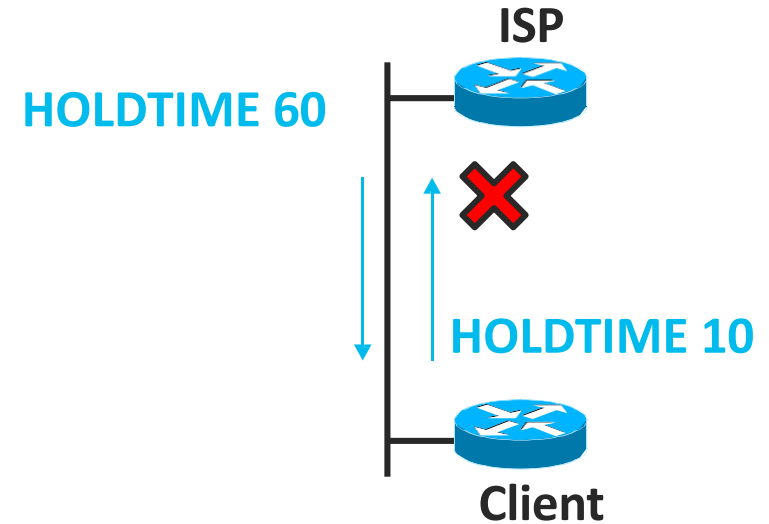
```
ISP(config-router)# neighbor x.x.x.x timers X Y
```

```
  X. (0-65535) is keepalive
```

```
  Y. (0-65535) is holdtime
```

Keepalive and Holdtime

- Holdtime is negotiated via **OPEN** messages
- Lowest holdtime wins



```
ISP(config-router)# neighbor x.x.x.x timers X Y Z
```

```
X. (0-65535) is keepalive
```

```
Y. (0-65535) is holdtime
```

```
Z. (0-65535) minimum acceptable holdtime
```

BGP Peers

show ip bgp neighbours - AFI independent BGP info

```
R1#show ip bgp neighbors 2.2.2.2
BGP neighbor is 2.2.2.2, remote AS 200, external
link BGP version 4, remote router ID 2.2.2.2
BGP state = Established, up for 00:02:07
Last read 00:00:06, last write 00:00:13, hold time is 180,
keepalive
interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Address family IPv4 Unicast: advertised and
received Message statistics:
  InQ depth is 0
  OutQ depth is 0

```

	Sent	Rcvd
Opens:	6	6
Notifications:	0	0
Updates:	4	0
Keepalives:	175	177
Route Refresh:	0	0
Total:	185	183

```
Default minimum time between advertisement runs is 30 seconds
```

Concluding Remarks

BGPv4 is ~30 years old but its core is still the same – a credit to its well-thought design

BGP is a world on its own – where to learn more?

- Cisco Press textbooks
- Cisco Communities, Cisco Learning Network
- IETF RFCs
- Wireshark
- Hands-on experience is key



BGP

**Be Guided by
Policy, Prudence and Precision**

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

