Border Gateway Protocol

Jordan Johnson

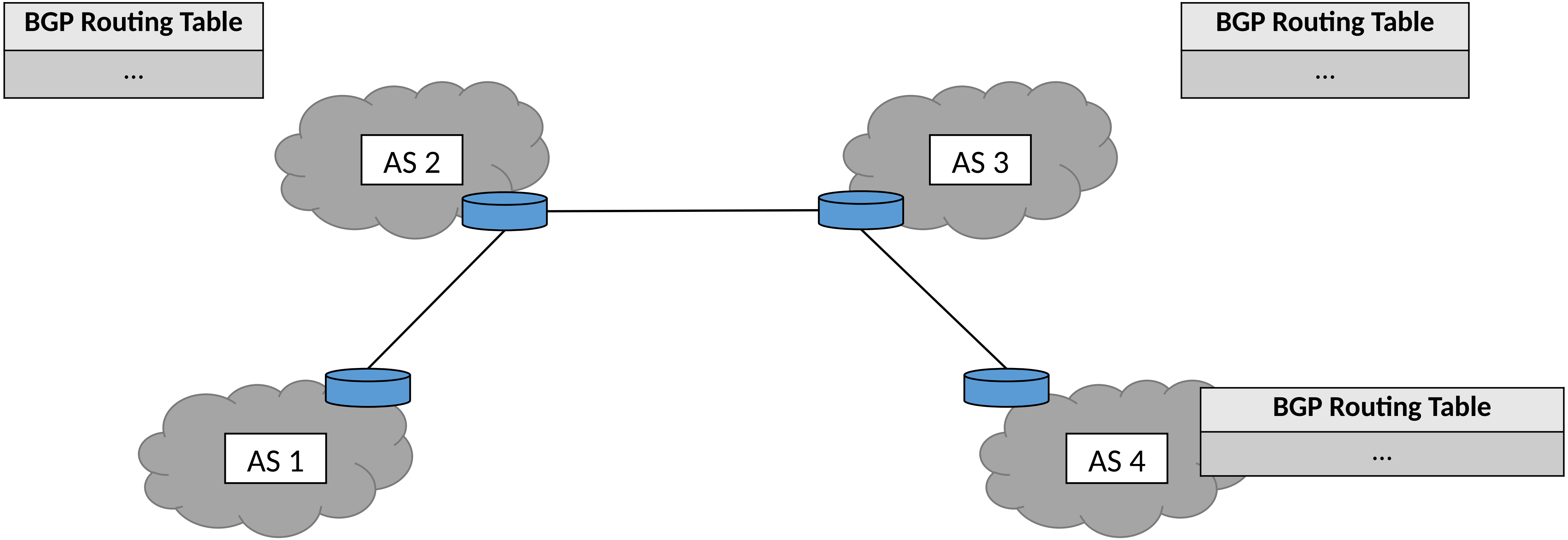
Why should we care about BGP?

- The GPS of the Internet: the method for traffic to know where to go
- Without it, networks would be isolated
- Allow networks to discuss routes with neighbors, known as peers

What is BGP?

- Application layer protocol for interdomain routing
- Interdomain routing occurs between autonomous systems (ASes)
  - Examples: ISPs, large organizations
- Path Vector Routing Protocol
  - Prevents loops
- Uses TCP to maintain connections between peers

BGP Example



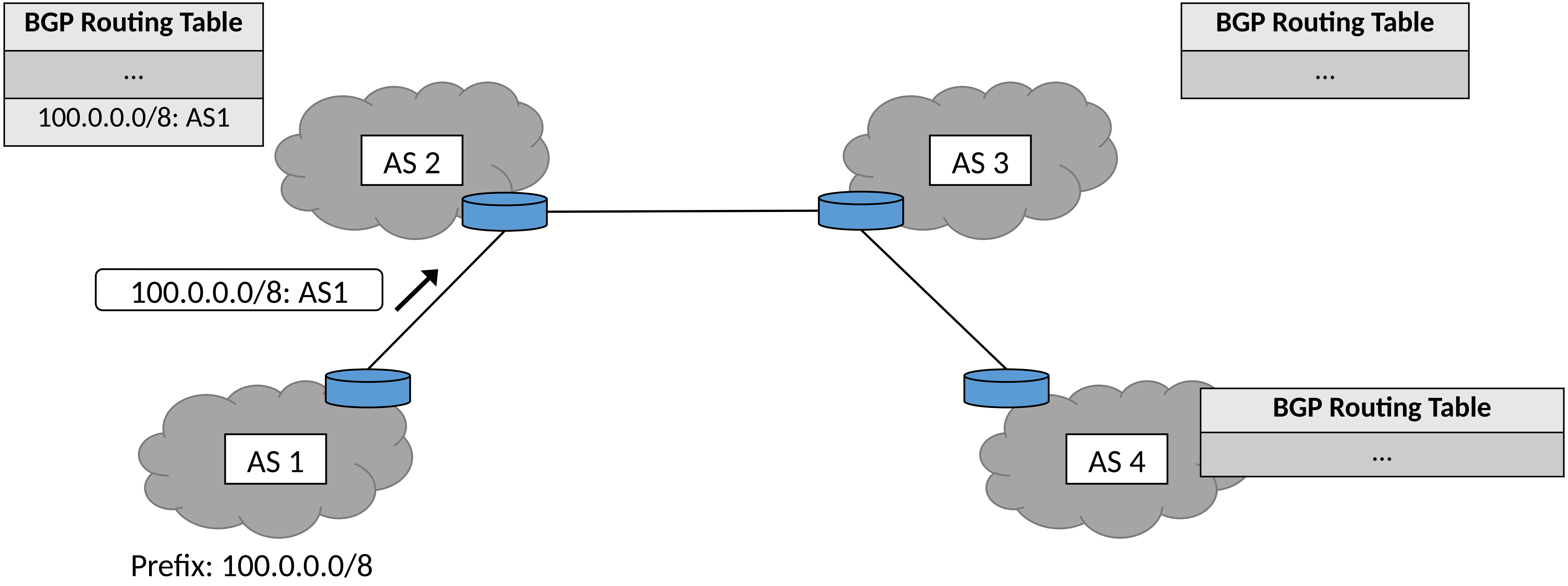
BGP Routing Table
…

BGP Routing Table
…

BGP Routing Table
…

Prefix: 100.0.0.0/8

BGP Example

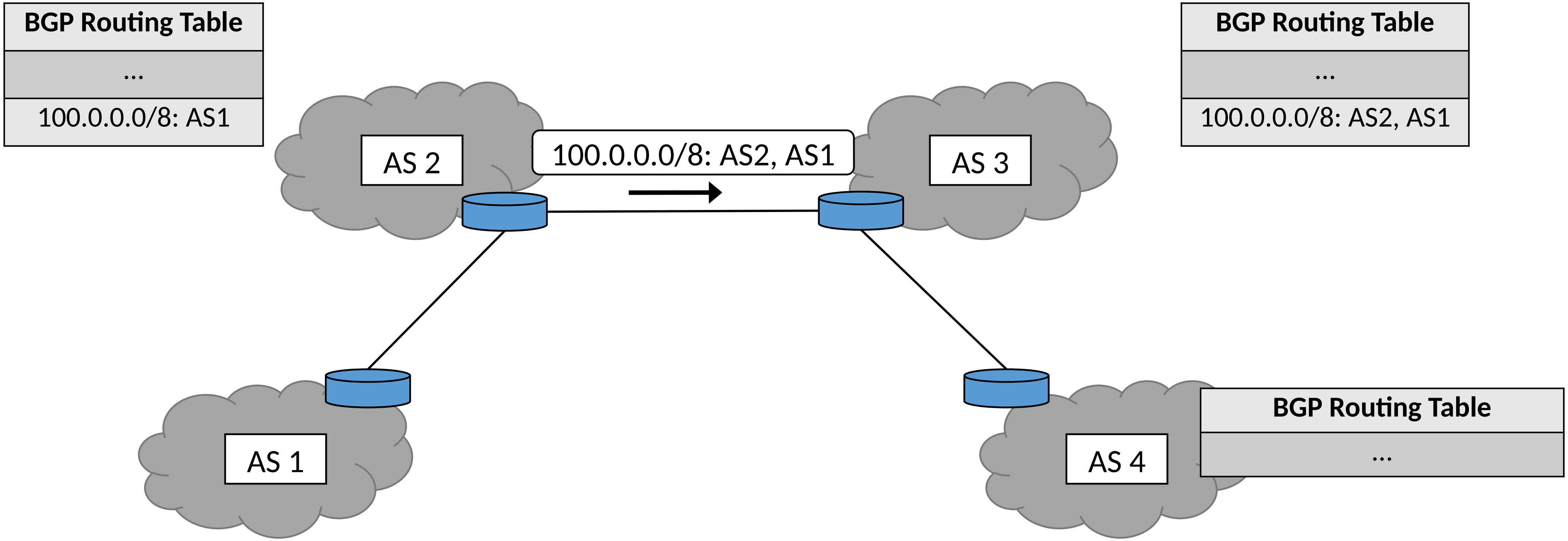


BGP Routing Table
…
100.0.0.0/8: AS1

BGP Routing Table
…

BGP Routing Table
…

BGP Example



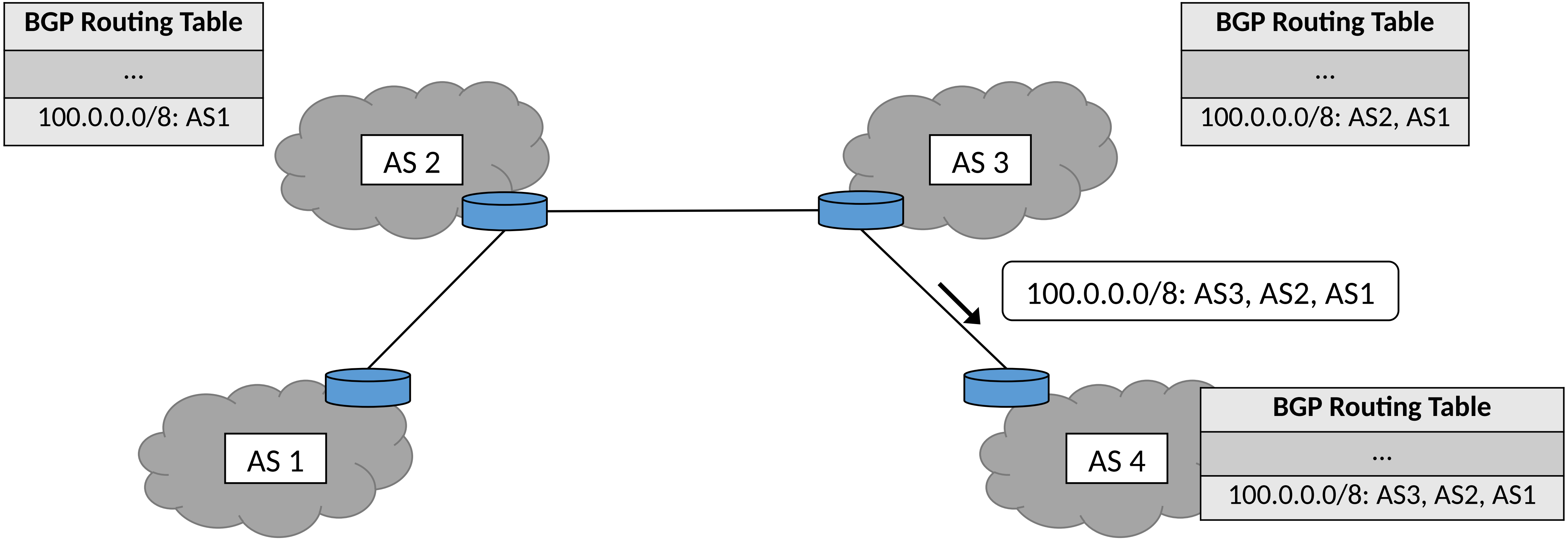
BGP Routing Table
…
100.0.0.0/8: AS1

BGP Routing Table
…
100.0.0.0/8: AS2, AS1

BGP Routing Table
…

Prefix: 100.0.0.0/8

BGP Example



BGP Routing Table
…
100.0.0.0/8: AS1

BGP Routing Table
…
100.0.0.0/8: AS2, AS1

100.0.0.0/8: AS3, AS2, AS1

BGP Routing Table
…
100.0.0.0/8: AS3, AS2, AS1

Prefix: 100.0.0.0/8

BGP is heavily influenced by policy

- Each AS has its own goals and relationships with other ASes

- Shortest path length is not guaranteed
    - Intra-domain path lengths are not going to be the same
    - ASes will prefer paying customers
    - Traffic engineering (typically done with AS prepending)

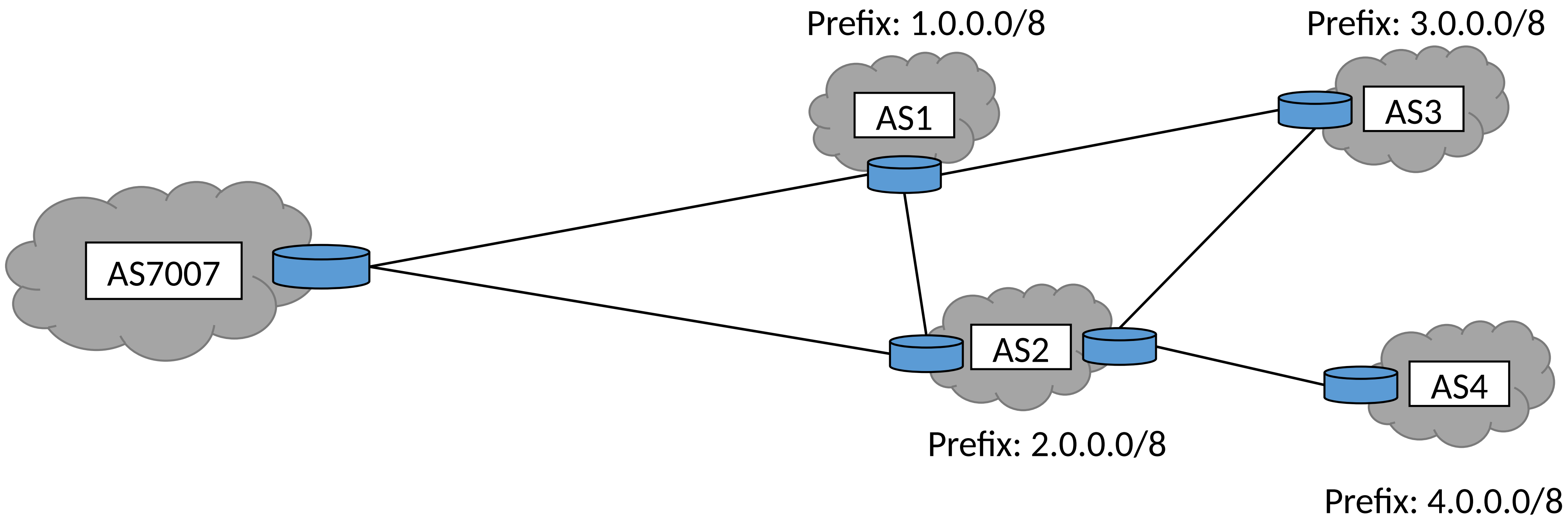
- Each AS will have its own set of import and export policies
    - Example: don’t allow prefixes longer than /24

What are the issues with BGP?

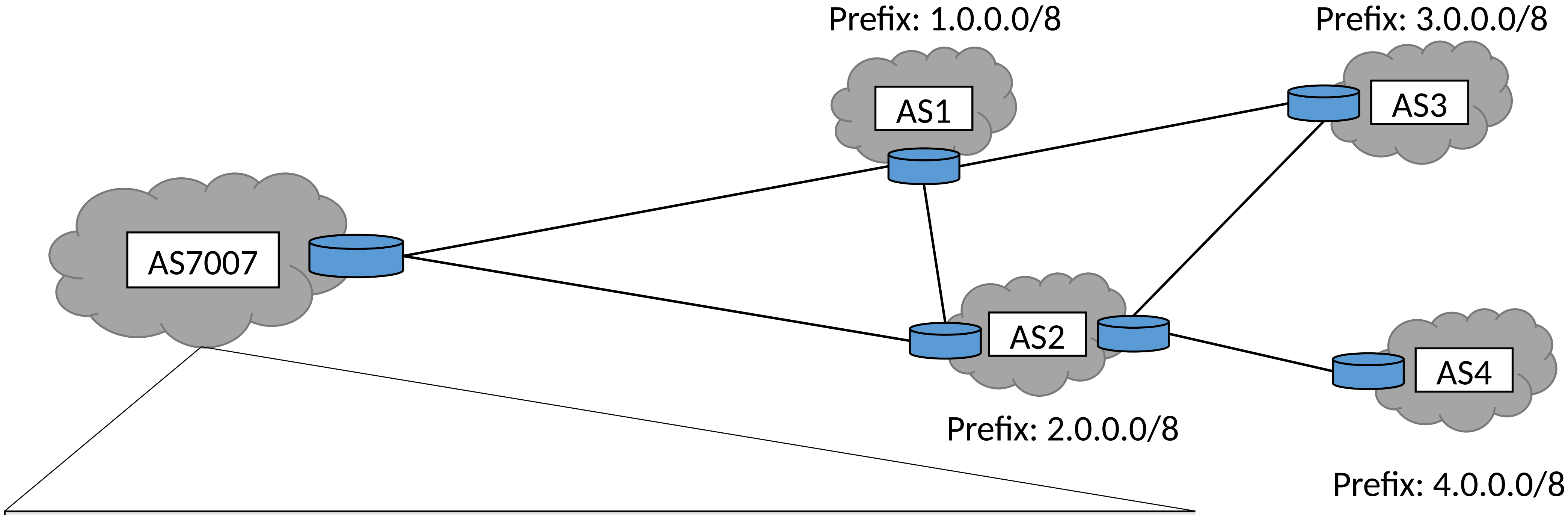
- Long Convergence Times [1]
  - Especially for route failovers
  - This makes the following issues even worse…

- Misconfigurations [2]
  - 1997: AS7007 in Virginia announces bad routes for most of the Internet
  - 2001: AS3561 propagates false routes from downstream customer
  - 2004: Turkish network provider announces bad routes for most of the Internet
  - 2008: Pakistan Telecom takes down YouTube
  - And many more…

AS7007 Misconfiguration Event [5]

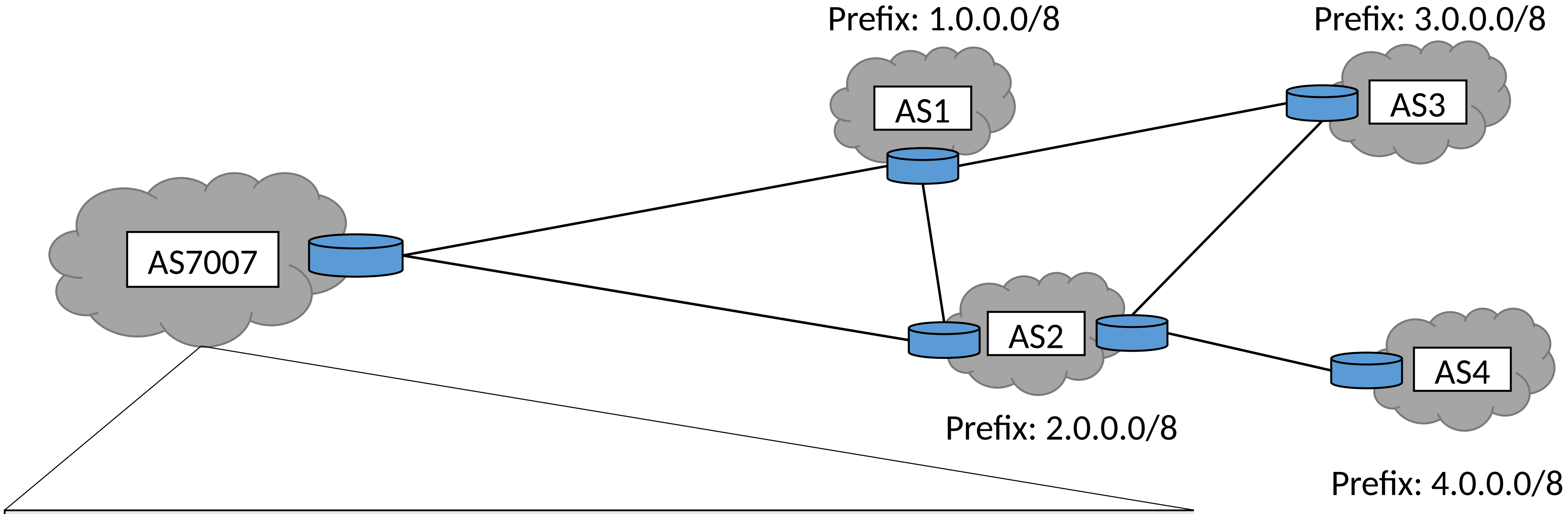


AS7007 Misconfiguration Event [5]



BGP Routing Table			
1.0.0.0/8: AS1	2.0.0.0/8: AS2	3.0.0.0/8: AS1, AS3	4.0.0.0/8: AS2, AS4

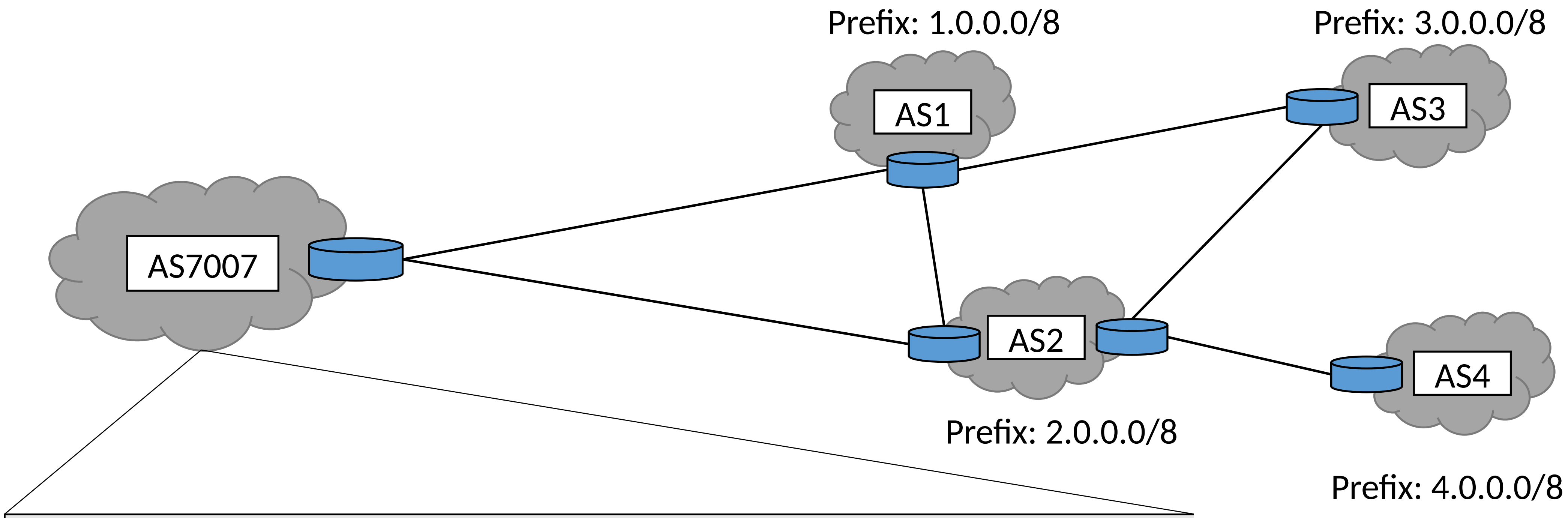
AS7007 Misconfiguration Event [5]



BGP Routing Table			
1.0.0.0/24: AS1	2.0.0.0/24: AS2	3.0.0.0/24: AS1, AS3	4.0.0.0/24: AS2, AS4
1.0.1.0/24: AS1	2.0.1.0/24: AS2	3.0.1.0/24: AS1, AS3	4.0.1.0/24: AS2, AS4
…	…	…	…

AS7007 *deaggregates* prefixes to /24

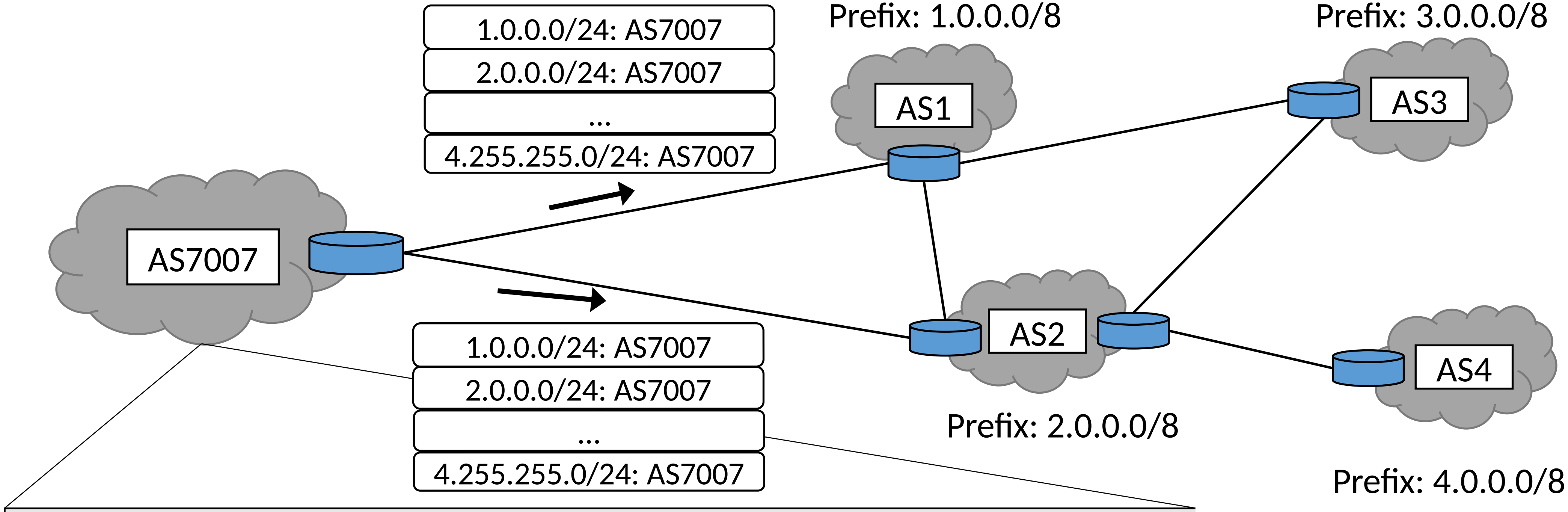
AS7007 Misconfiguration Event [5]



BGP Routing Table			
1.0.0.0/24: ~~AS1~~	2.0.0.0/24: ~~AS2~~	3.0.0.0/24: ~~AS1, AS3~~	4.0.0.0/24: ~~AS2, AS4~~
1.0.1.0/24: ~~AS1~~	2.0.1.0/24: ~~AS2~~	3.0.1.0/24: ~~AS1, AS3~~	4.0.1.0/24: ~~AS2, AS4~~
…	…	…	…

AS7007 strips AS paths

AS7007 Misconfiguration Event [5]



BGP Routing Table

1.0.0.0/24: ~~AS1~~	2.0.0.0/24: ~~AS2~~	3.0.0.0/24: ~~AS1, AS3~~	4.0.0.0/24: ~~AS2, AS4~~
1.0.1.0/24: ~~AS1~~	2.0.1.0/24: ~~AS2~~	3.0.1.0/24: ~~AS1, AS3~~	4.0.1.0/24: ~~AS2, AS4~~
…	…	…	…

AS7007 announces specific routes with best path to peers

What are the security issues with BGP?

- BGP was not designed with security in mind
  - No authentication of route updates
  - Who can you trust? Your peers? Your peers' peers?

- Issues with securing BGP:
  - BGP is everywhere, it is the glue of the Internet
  - Proposed solutions are too computationally expensive and difficult to deploy
  - Route filters are difficult to configure and don't have a full view

BGP Attacks [3]

- TCP attacks
  - Confidentiality: passive eavesdropping
  - Integrity: man in the middle or message replay attacks
  - Availability: SYN flooding or link cutting attacks

- Path attribute manipulation
  - Sending a route update with false attributes to influence path selection
  - Examples: path length, fake loops, extra long paths

BGP Attacks [3]

- No authentication of AS number or prefix origins
  - Any AS can advertise an AS number, path, or prefix regardless of ownership
  - Can lead to prefix or traffic hijacking
  - Interception: loss of integrity or confidentiality
  - Blackhole: loss of availability

What is Traffic Hijacking?

- Adversarial route causes traffic to be dropped or intercepted
- Dropped traffic results in a denial of service (DoS)
- Intercepted traffic could lead to eavesdropping and man in the middle attacks

Hypothesis: BGPsec Mitigates Traffic Hijacking

- Goal: an adversarial or misconfigured AS cannot drop or intercept traffic that would not normally traverse it by announcing a false BGP route

- But what is BGPsec?

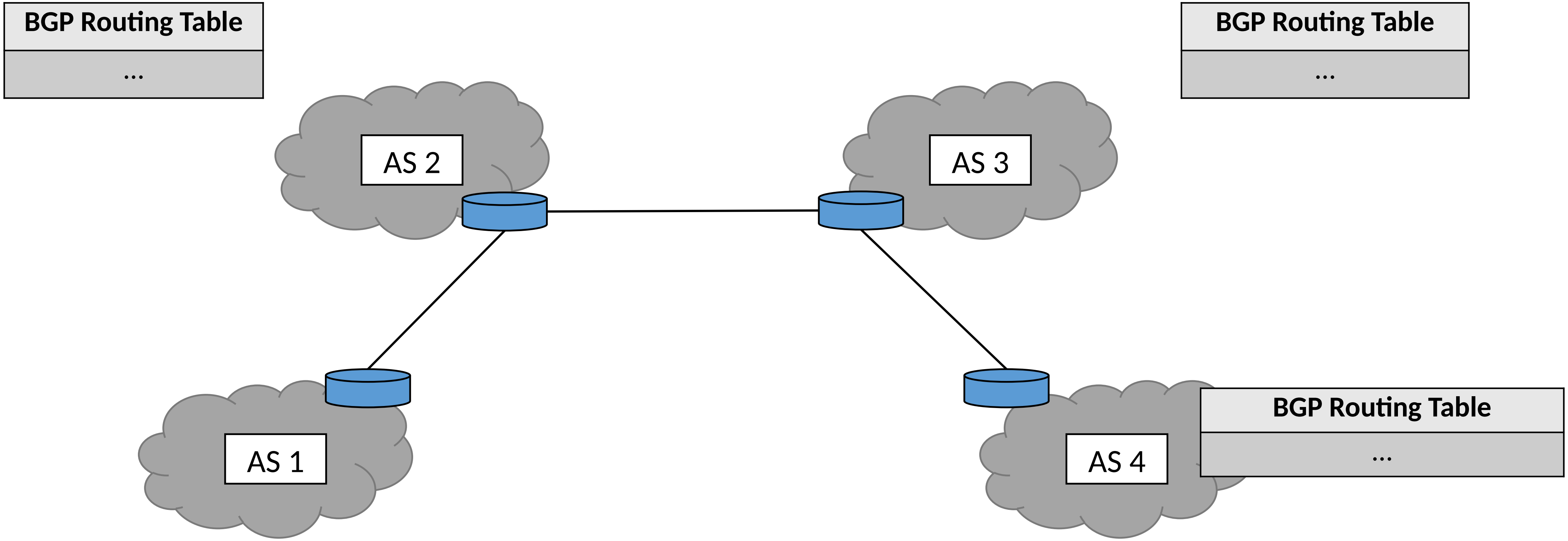
What is BGPsec? [4]

- Modification of BGP using RPKI to authenticate both prefix origins and route paths
  - Does not provide confidentiality

- Resource Public Key Infrastructure (RPKI) is the provision of certificates for authenticating AS numbers and prefix origins
  - Certificates known as resource origin authorizations (ROAs)
  - Distributed by regional Internet registries (RIRs)

- RPKI first used to authenticate origins, BGPsec also validates paths

BGPsec Example [4]



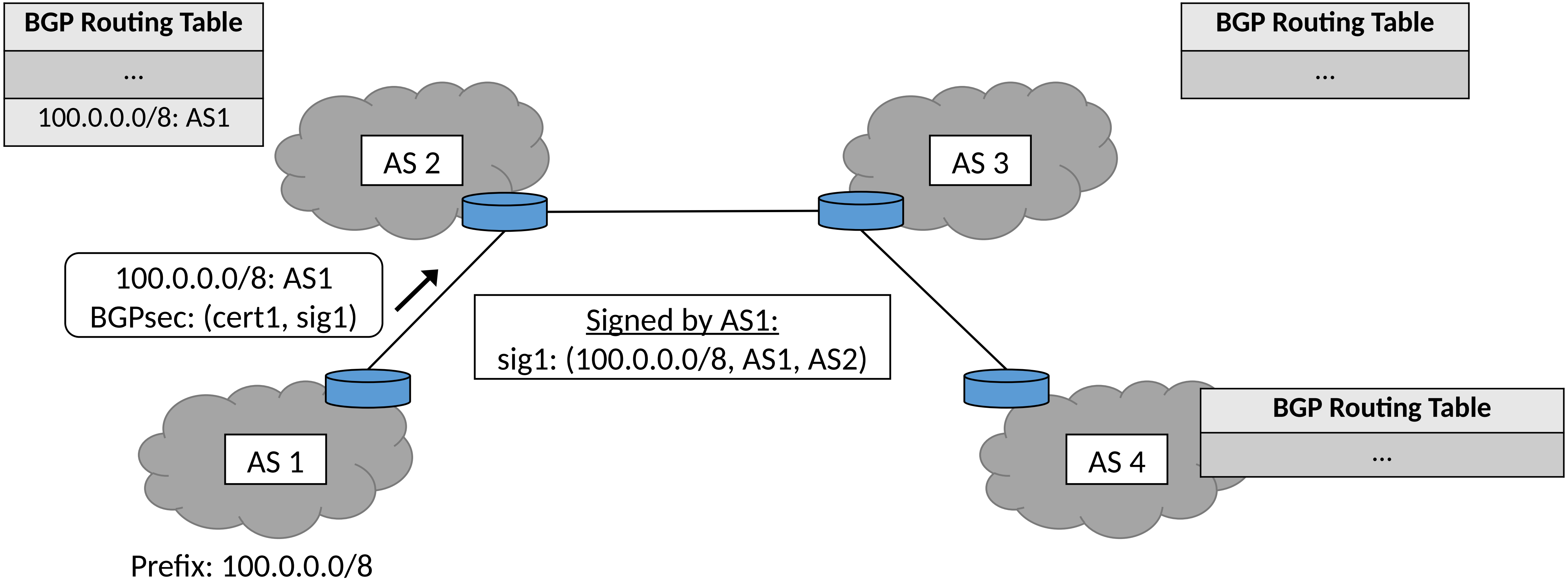
BGP Routing Table
…

BGP Routing Table
…

BGP Routing Table
…

Prefix: 100.0.0.0/8

BGPsec Example [4]



BGP Routing Table
…
100.0.0.0/8: AS1

BGP Routing Table
…

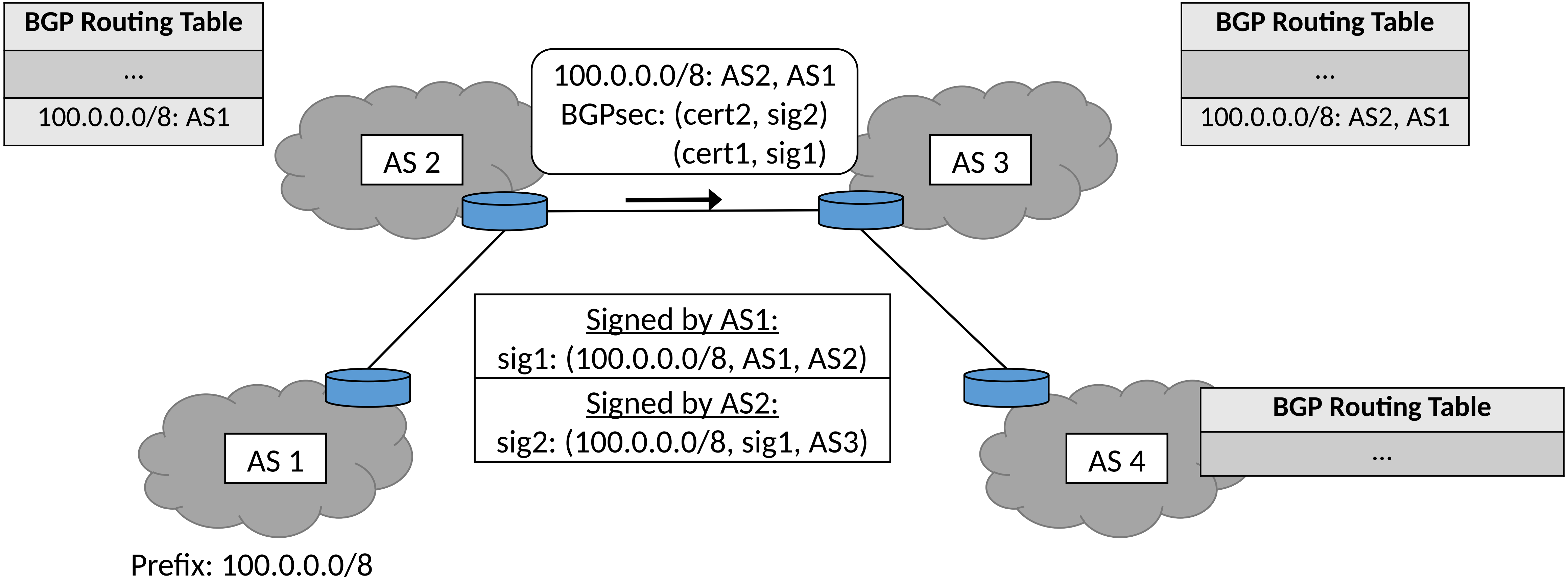
BGP Routing Table
…

100.0.0.0/8: AS1
BGPsec: (cert1, sig1)

Signed by AS1:
sig1: (100.0.0.0/8, AS1, AS2)

Prefix: 100.0.0.0/8

BGPsec Example [4]



BGP Routing Table
…
100.0.0.0/8: AS1

100.0.0.0/8: AS2, AS1
BGPsec: (cert2, sig2)
(cert1, sig1)

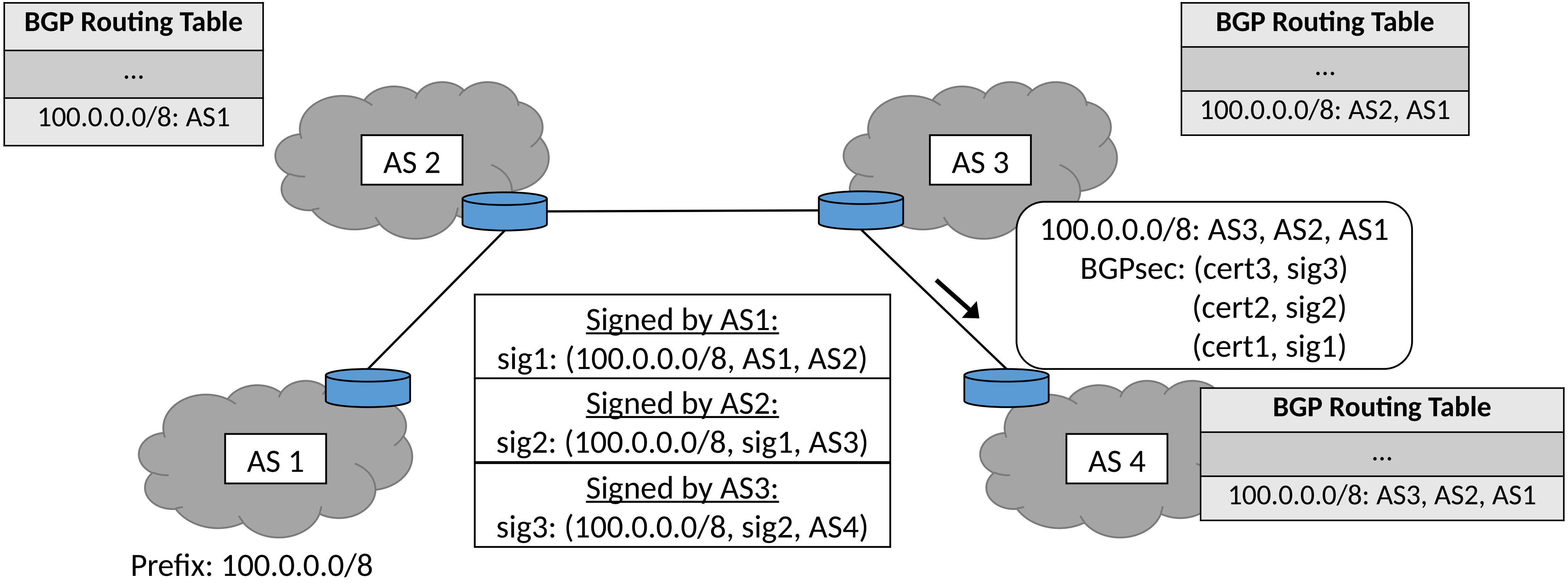
BGP Routing Table
…
100.0.0.0/8: AS2, AS1

Signed by AS1:
sig1: (100.0.0.0/8, AS1, AS2)
Signed by AS2:
sig2: (100.0.0.0/8, sig1, AS3)

BGP Routing Table
…

Prefix: 100.0.0.0/8

BGPsec Example [4]



BGP Routing Table
…
100.0.0.0/8: AS1

BGP Routing Table
…
100.0.0.0/8: AS2, AS1

100.0.0.0/8: AS3, AS2, AS1
BGPsec: (cert3, sig3)
(cert2, sig2)
(cert1, sig1)

Signed by AS1:
sig1: (100.0.0.0/8, AS1, AS2)

Signed by AS2:
sig2: (100.0.0.0/8, sig1, AS3)

Signed by AS3:
sig3: (100.0.0.0/8, sig2, AS4)

BGP Routing Table
…
100.0.0.0/8: AS3, AS2, AS1

Prefix: 100.0.0.0/8

Notes on BGPsec [7]

- BGPsec only works if both peers speak BGPsec
    - For a complete chain of updates, every AS in the path must support BGPsec
    - BGPsec support is communicated during a BGP peer session’s startup

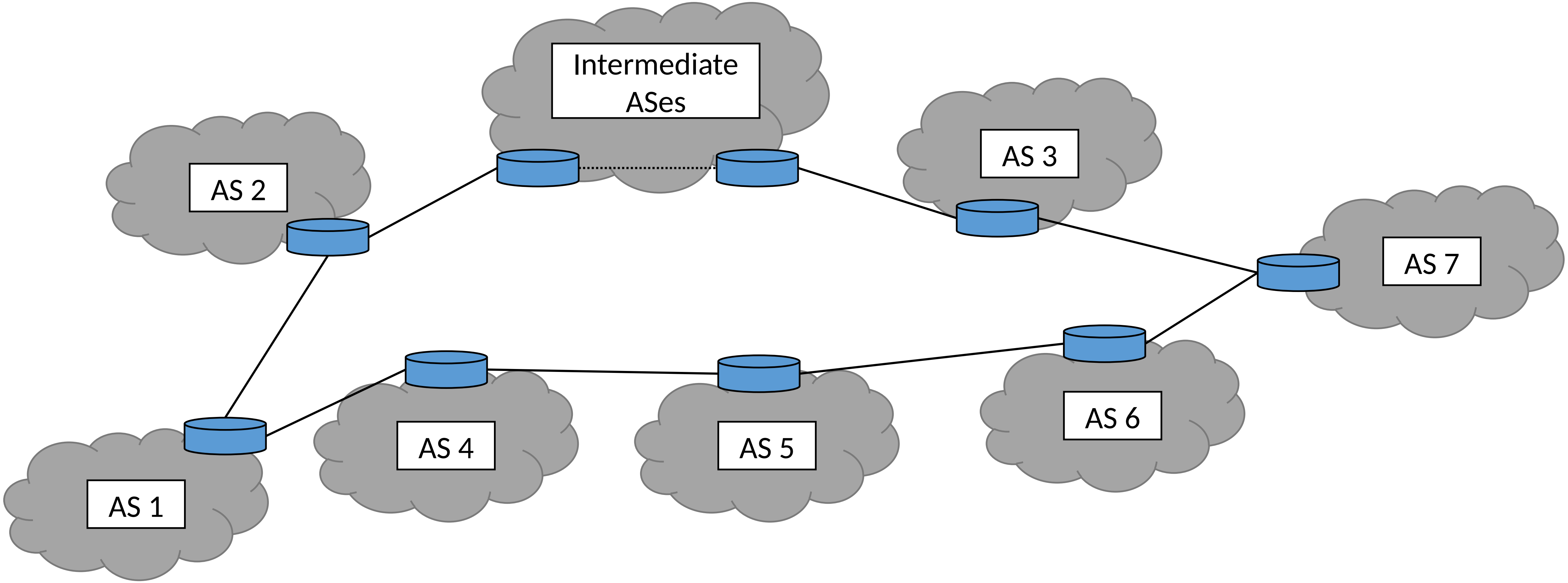
- RIRs must provide ROAs to each AS

So BGPsec protects against traffic hijacking?

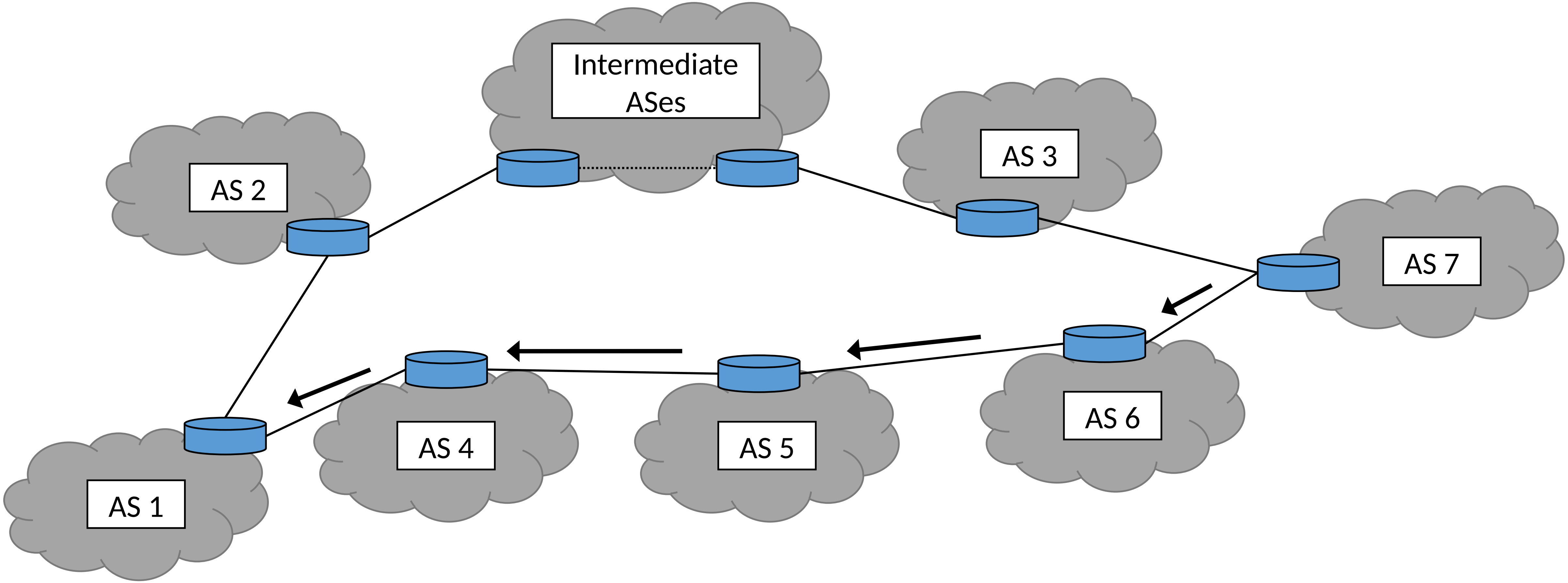
- BGPsec authenticates the entire path, so there should not be a way to hijack traffic, right?

- Unfortunately, there is still a way: wormhole attacks

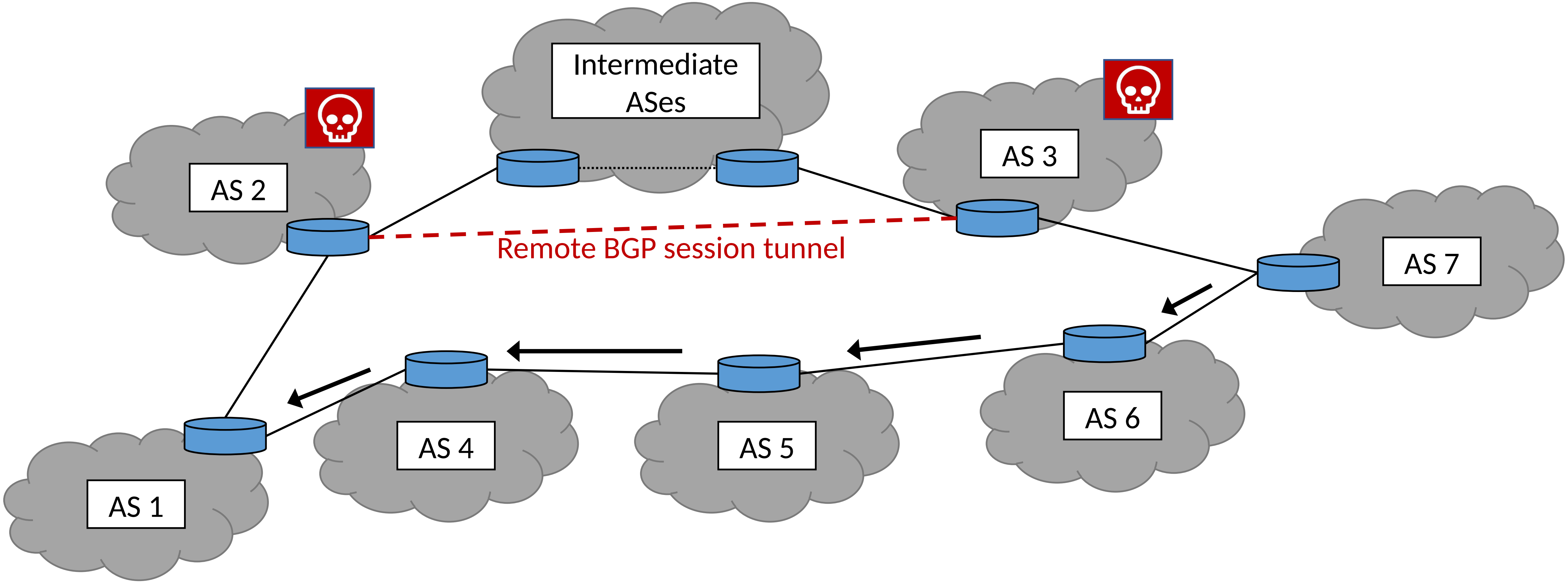
Example of Hijacking: Wormhole Attack [4]



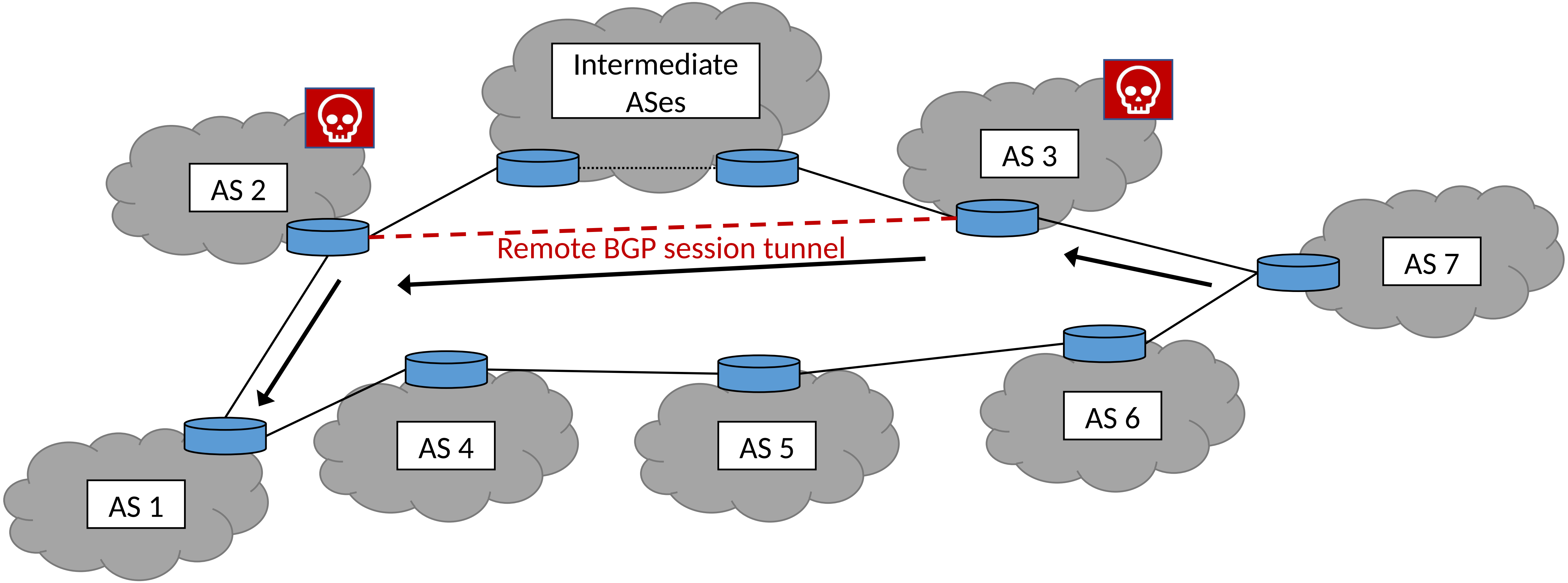
Example of Hijacking: Wormhole Attack [4]



Example of Hijacking: Wormhole Attack [4]



Example of Hijacking: Wormhole Attack [4]



BGPsec Does Not Mitigate Traffic Hijacking [4]

- Two adversarial ASes can use tunneling to reduce announced path length
- May not always work due to AS policies
- [4] lists additional methods to hijack traffic
  - Protocol manipulation attacks

How can BGPsec improve? [4]

- Instead of certifying AS prefixes, certify physical link prefixes
  - Can track the physical links being used to prevent false path lengths
  - Adds additional complexity

- Use trusted processor architectures in BGP routers
  - An AS can verify its peers’ configurations and the routes it uses
  - Adds additional complexity
  - Forces peers to agree on “good” configurations

Further Issues [3, 4, 6]

- Cryptography is computationally expensive
  - RPKI is no exception
  - BGPsec requires multiple signatures to be verified
  - A solution like path-end validation [6] could reduce computation cost

- Router registries must be correct and up-to-date

- Requires routers to be reconfigured or replaced
  - There are a lot of routers
  - Higher chance of misconfigurations

Conclusion

- BGP has security issues

- BGPsec does not provide complete protection against traffic hijacking

- Is BGPsec the right solution?

Questions?

References

1. Labovitz, Craig, et al. "Delayed Internet routing convergence." ACM SIGCOMM Computer Communication Review 30.4 (2000): 175-187.
2. Mahajan, Ratul, David Wetherall, and Tom Anderson. "Understanding BGP misconfiguration." ACM SIGCOMM Computer Communication Review 32.4 (2002): 3-16.
3. Butler, Kevin, et al. "A survey of BGP security issues and solutions." Proceedings of the IEEE 98.1 (2009): 100-122.
4. Li, Qi, et al. "BGP with BGPsec: Attacks and countermeasures." IEEE Network 33.4 (2018): 194-200.
5. Bono, Vincent J. “7007 Explanation and Apology.” Nanog, 26 Apr. 1997, seclists.org/nanog/1997/Apr/444.
6. Cohen, Avichai, et al. "One hop for RPKI, one giant leap for BGP security." Proceedings of the 14th ACM Workshop on Hot Topics in Networks. 2015.
7. Lepinski, Matthew, and Kotikalapudi Sriram. “RFC8205: BGPsec Protocol Specification.” Request for Comments (RFC), Internet Engineering Task Force (IETF), Sept. 2017, datatracker.ietf.org/doc/html/rfc8205.