A Taxonomy of Attacks Using BGP Blackholing

Loïc Miller and Cristel Pelsser

September 23, 2019

University of Strasbourg

BGP Blackholing

Blackholing is a **DDoS mitigation** technique signaled via **BGP**[1].

[1] Rekhter, Li, and Hares, **A Border Gateway Protocol 4 (BGP-4)**.

BGP Blackholing

Blackholing is a **DDoS mitigation** technique signaled via **BGP**[1]. Internet is composed of **Autonomous Systems** (AS): one or more networks under the control of a single entity.

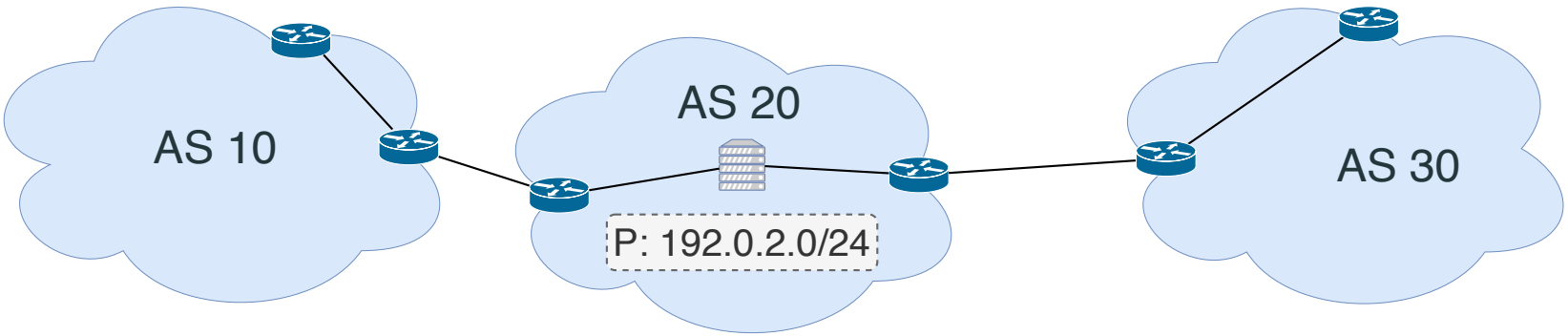


Figure 1: BGP Blackholing

[1] Rekhter, Li, and Hares, **A Border Gateway Protocol 4 (BGP-4)**.

BGP Blackholing

Blackholing is a **DDoS mitigation** technique signaled via **BGP**[1]. Internet is composed of **Autonomous Systems** (AS): one or more networks under the control of a single entity.

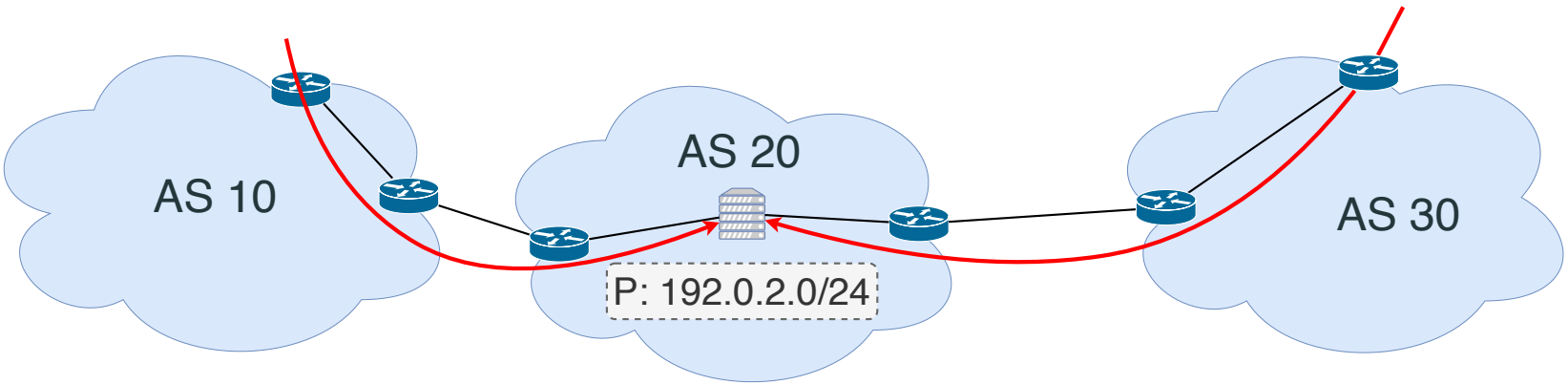


Figure 1: BGP Blackholing

[1] Rekhter, Li, and Hares, **A Border Gateway Protocol 4 (BGP-4)**.

BGP Blackholing

Blackholing is a **DDoS mitigation** technique signaled via **BGP**[1]. Internet is composed of **Autonomous Systems** (AS): one or more networks under the control of a single entity.

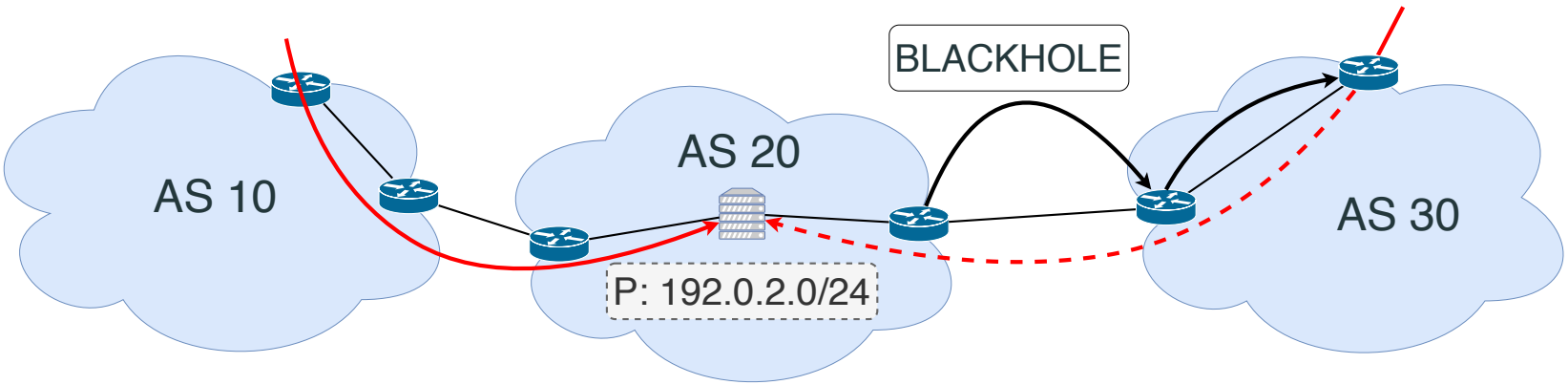


Figure 1: BGP Blackholing

[1] Rekhter, Li, and Hares, **A Border Gateway Protocol 4 (BGP-4)**.

BGP Blackholing

Blackholing is a **DDoS mitigation** technique signaled via **BGP**[1]. Internet is composed of **Autonomous Systems** (AS): one or more networks under the control of a single entity.

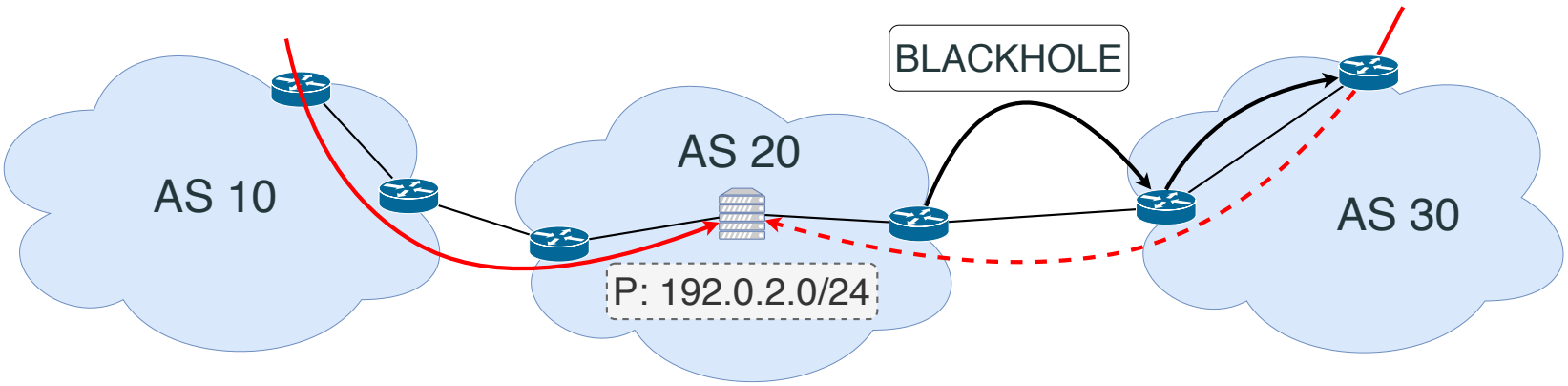


Figure 1: BGP Blackholing

Blackholing has a double-edged sword effect: **all** traffic is dropped.

[1] Rekhter, Li, and Hares, **A Border Gateway Protocol 4 (BGP-4)**.

Objectives

Objectives

Can blackholing be used with malicious intent?

Objectives

Can blackholing be used with malicious intent?

Are there different types of attacks?

Objectives

Can blackholing be used with malicious intent?

Are there different types of attacks?

Are there any existing and relevant security mechanisms?

Objectives

Can blackholing be used with malicious intent?

Are there different types of attacks?

Are there any existing and relevant security mechanisms? Are these mechanisms enough?

Quick BGP Primer

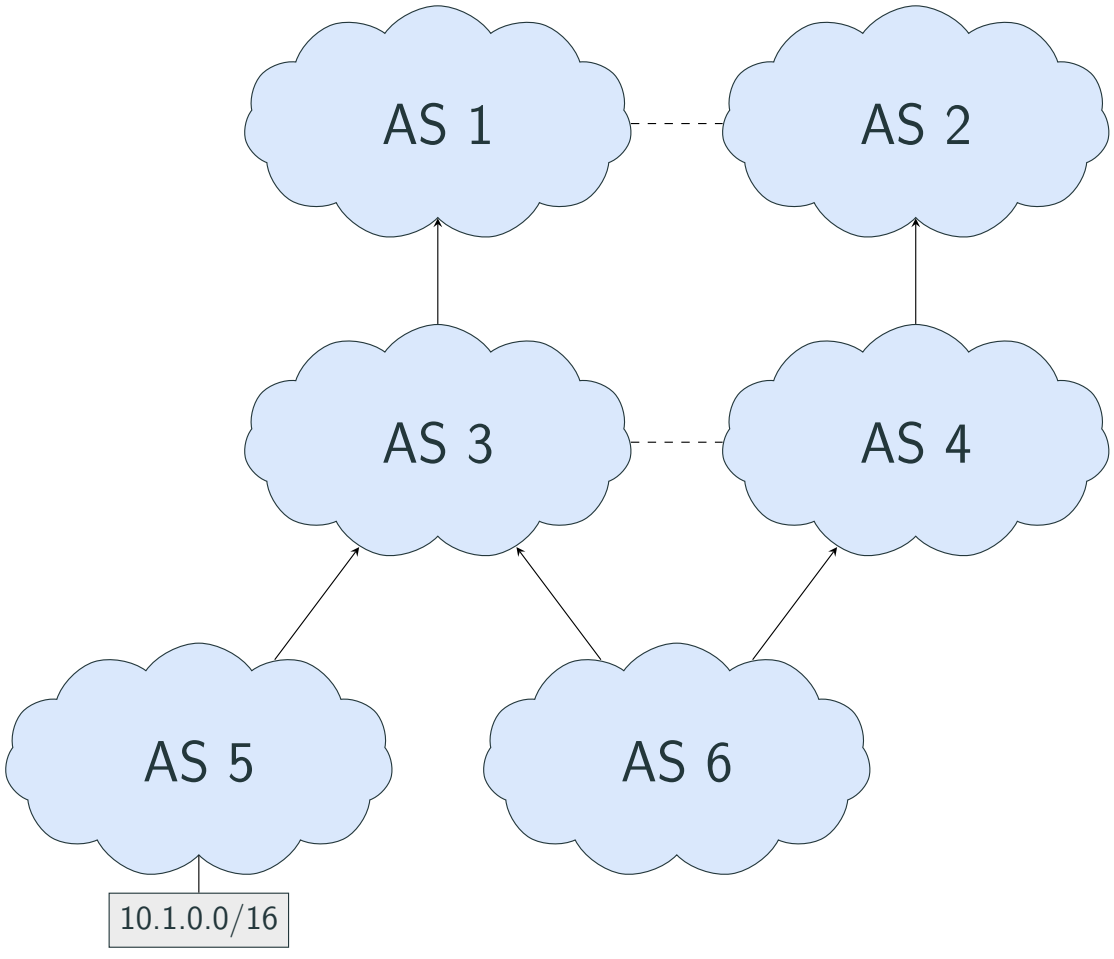


Figure 2: BGP message propagation

Quick BGP Primer

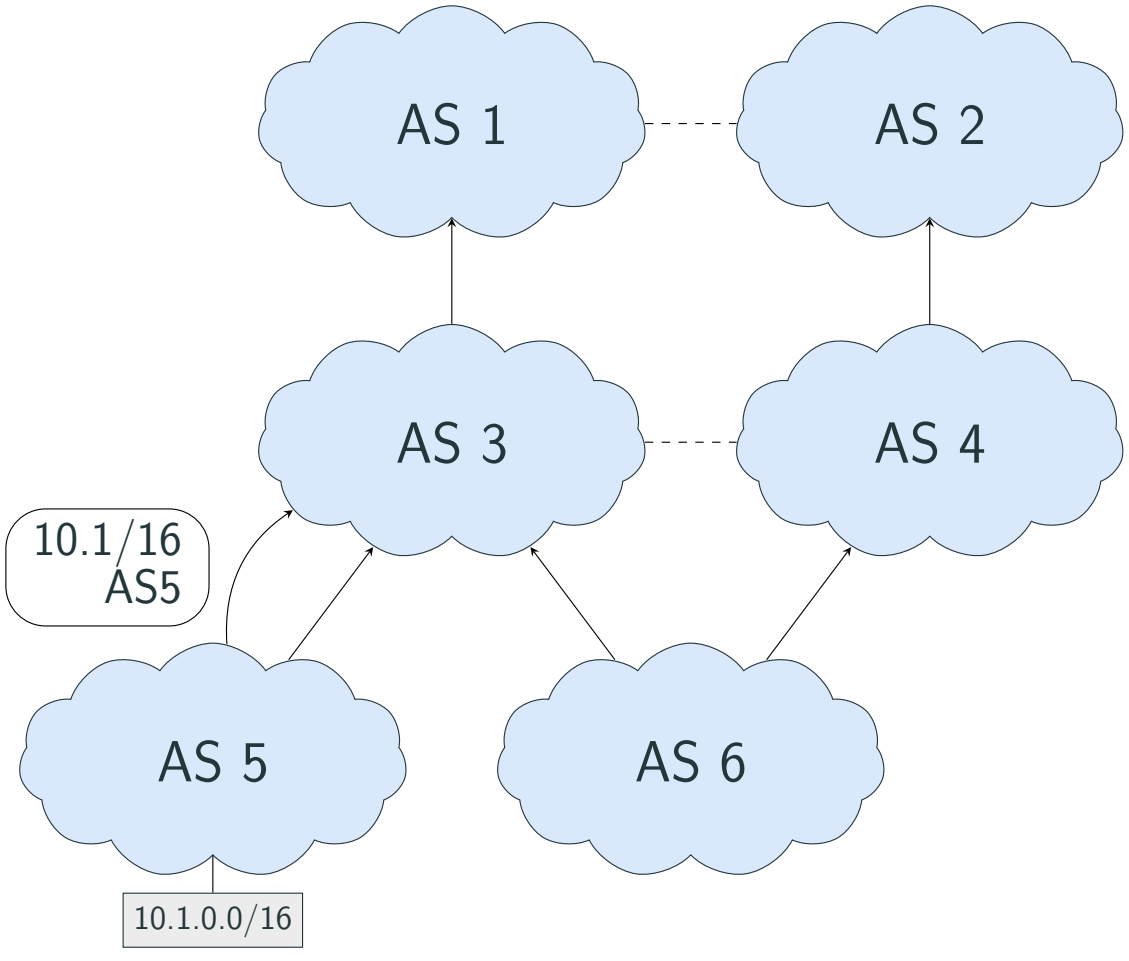


Figure 2: BGP message propagation

Quick BGP Primer

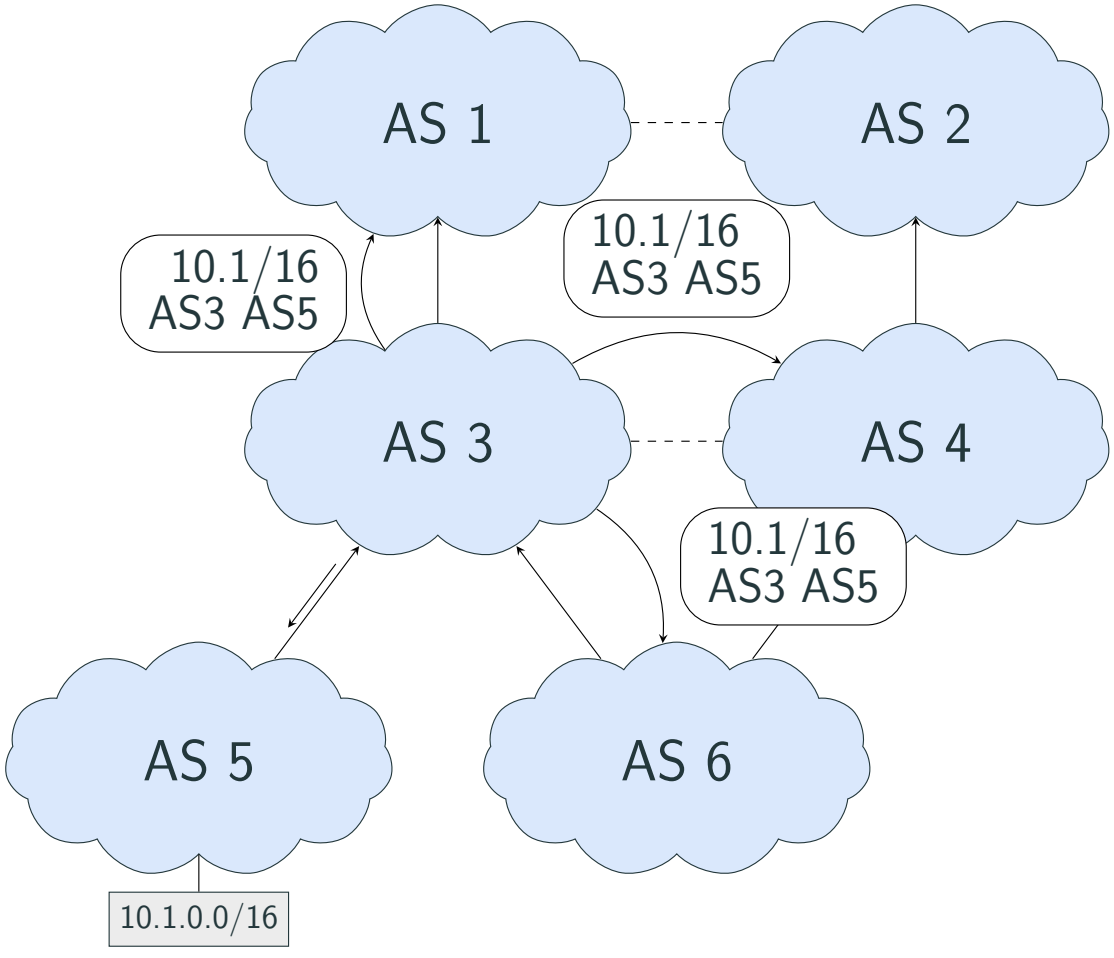


Figure 2: BGP message propagation

Quick BGP Primer

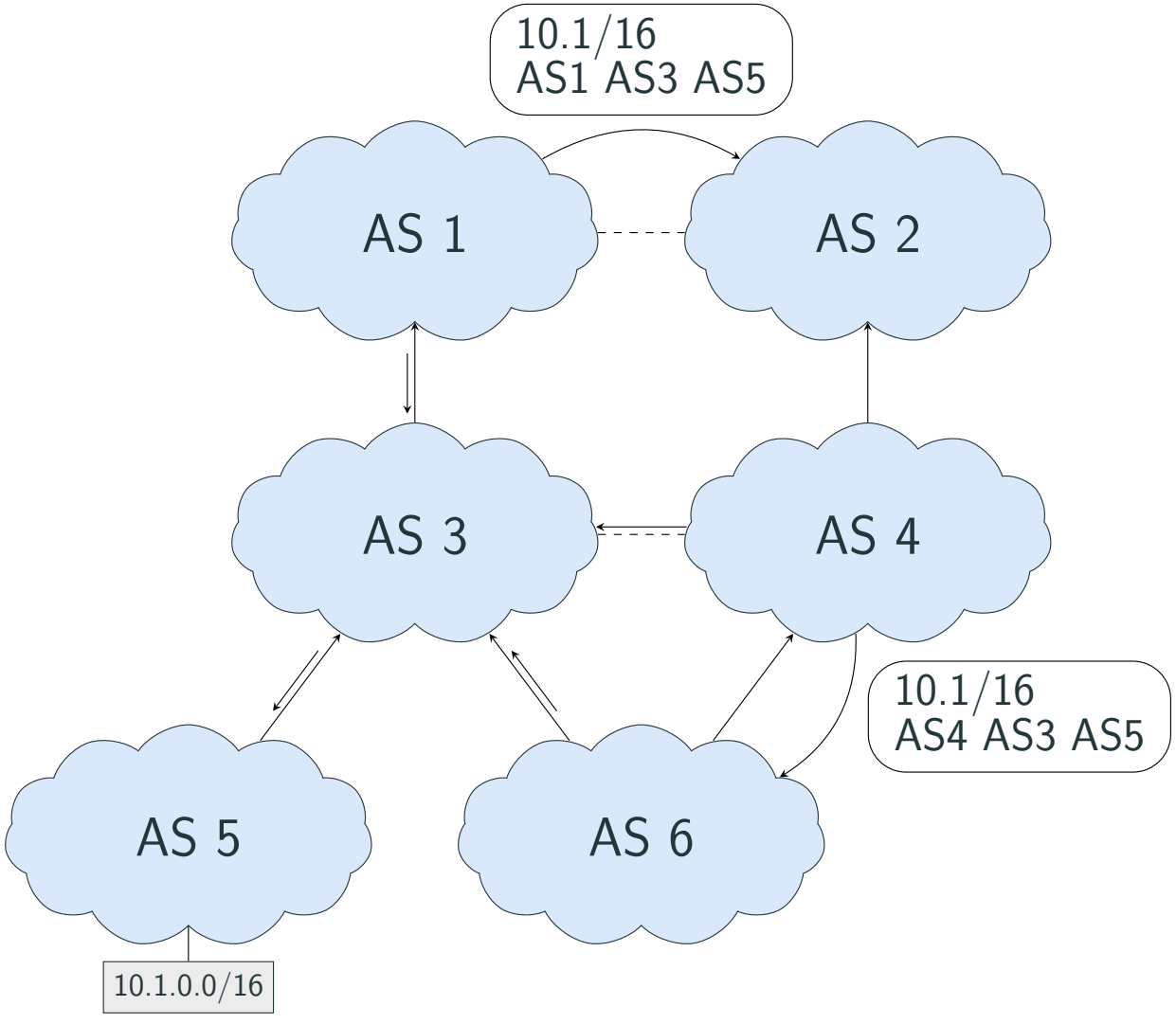


Figure 2: BGP message propagation

Quick BGP Primer

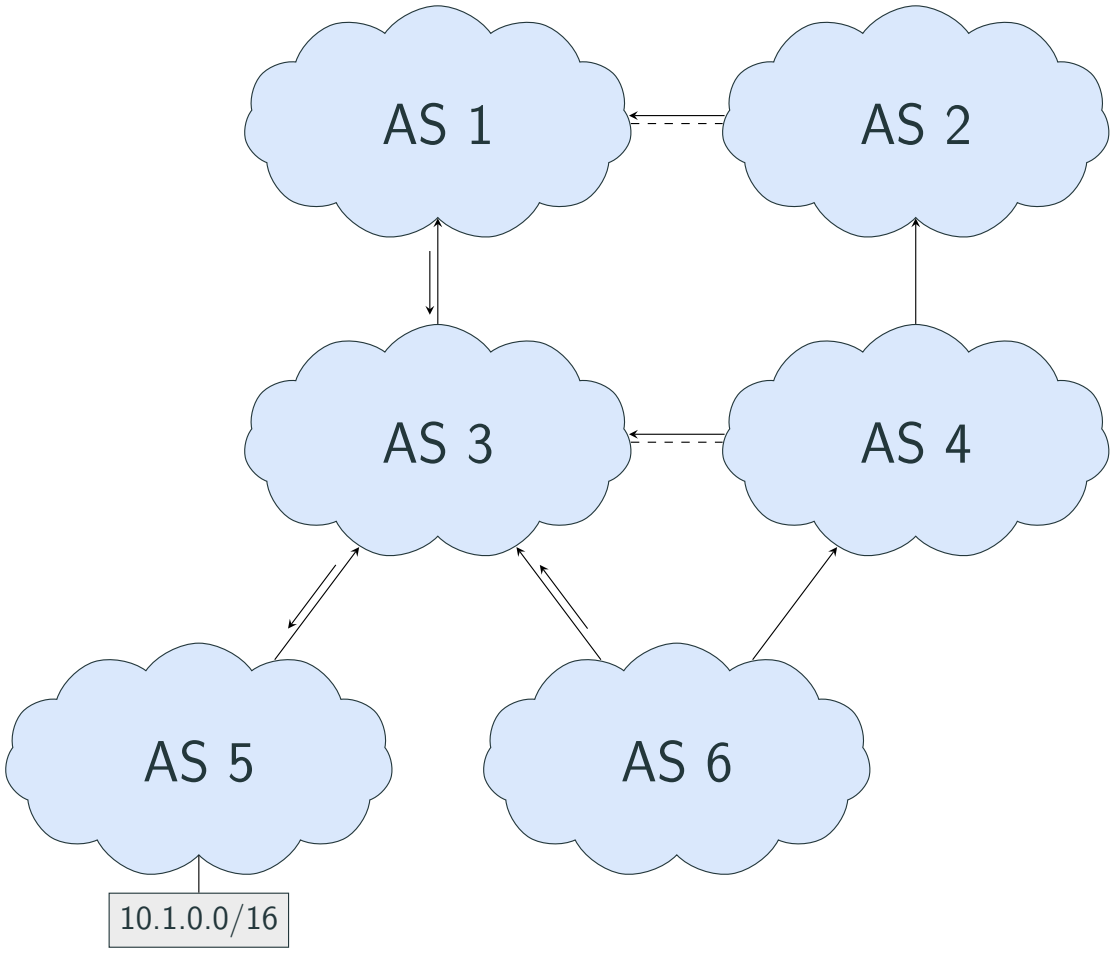


Figure 2: BGP message propagation

BGP Hijacks

As BGP is a distributed protocol, lacking authentication of route origins and verification of paths, ASes can advertise illegitimate routes for prefixes they do not own, attracting some or all of the traffic to these prefixes.

BGP Hijacks

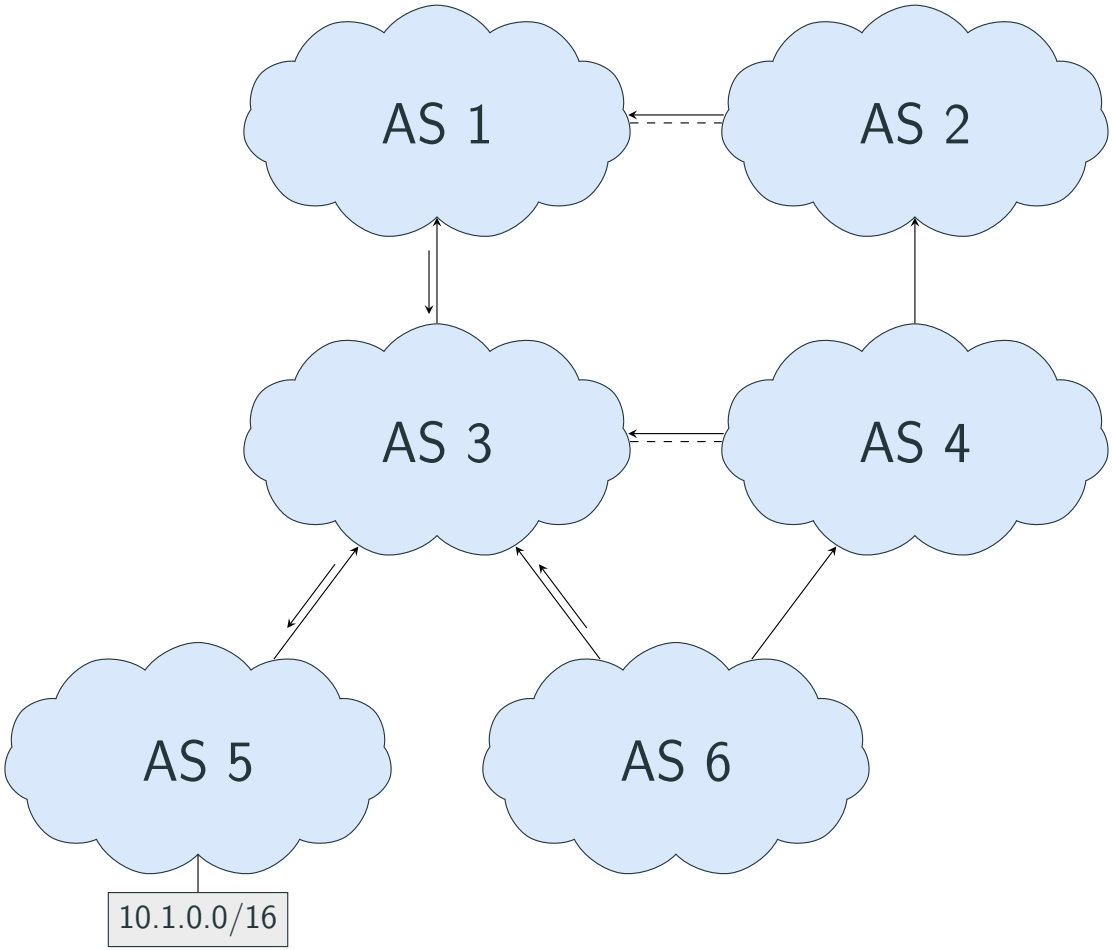


Figure 3: BGP hijack

BGP Hijacks

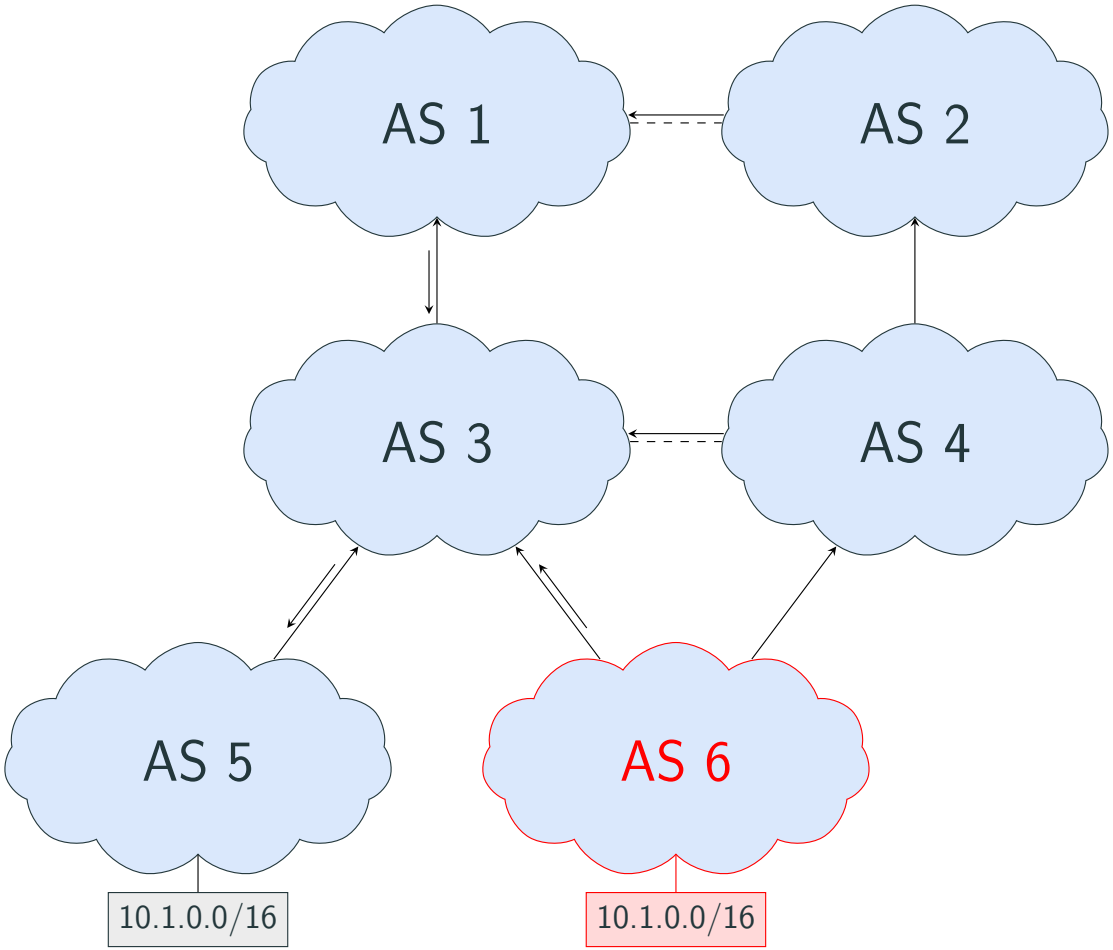


Figure 3: BGP hijack

BGP Hijacks

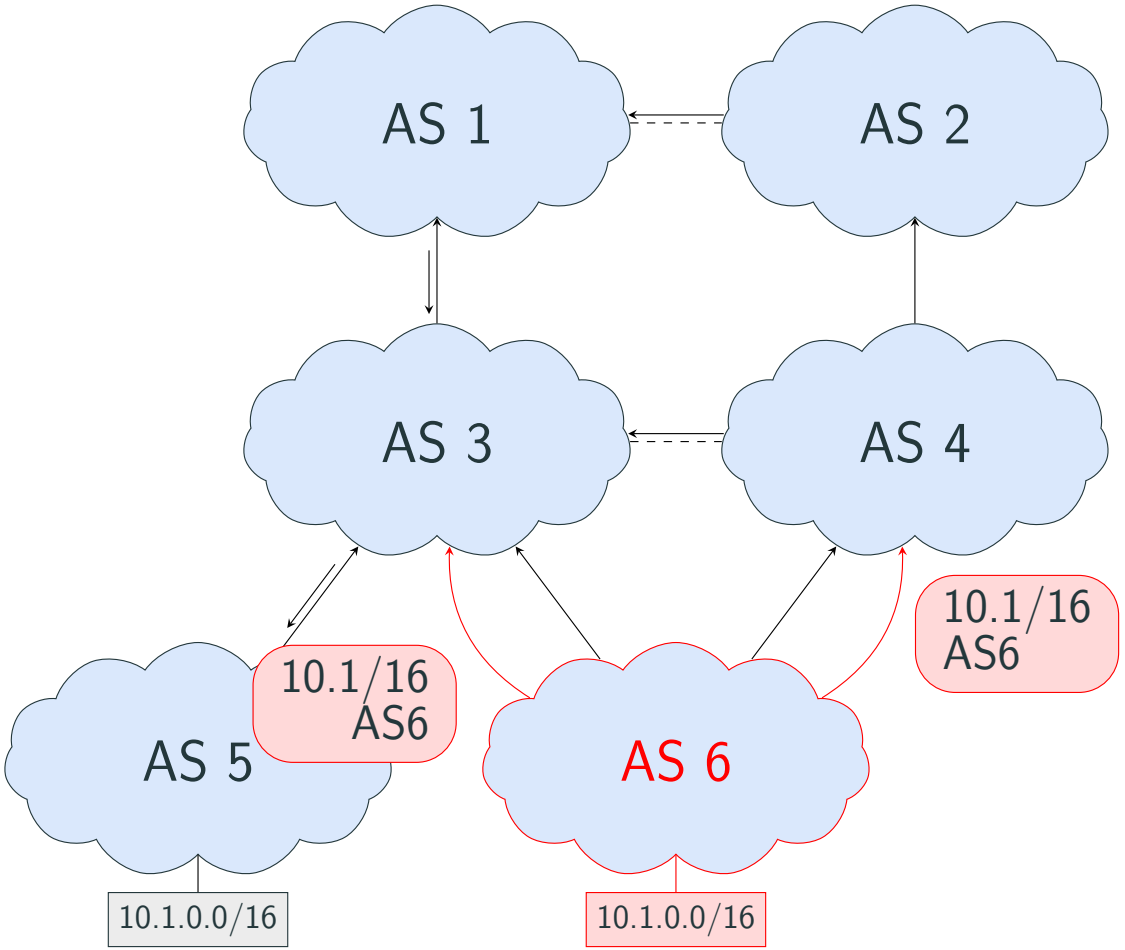


Figure 3: BGP hijack

BGP Hijacks

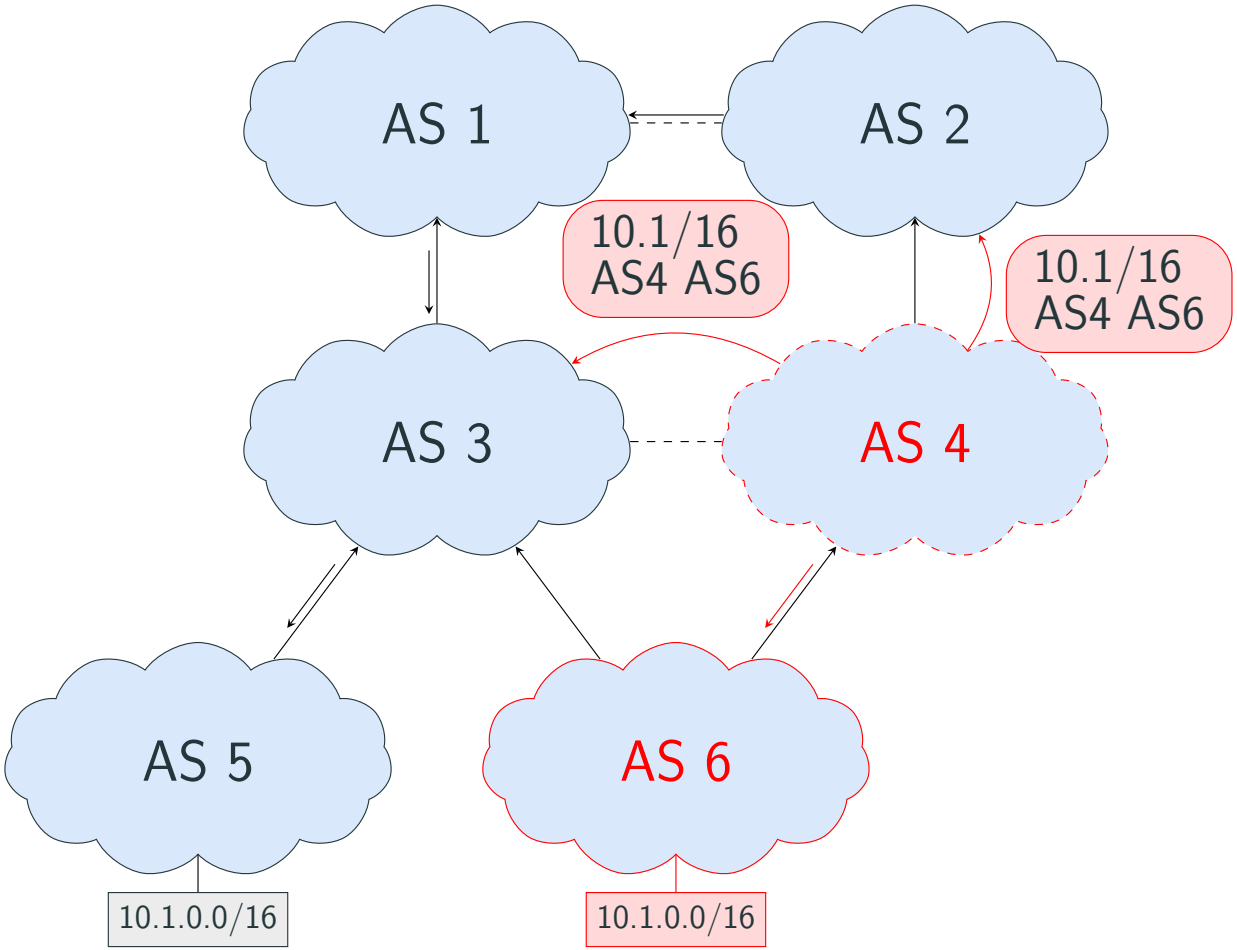


Figure 3: BGP hijack

BGP Hijacks

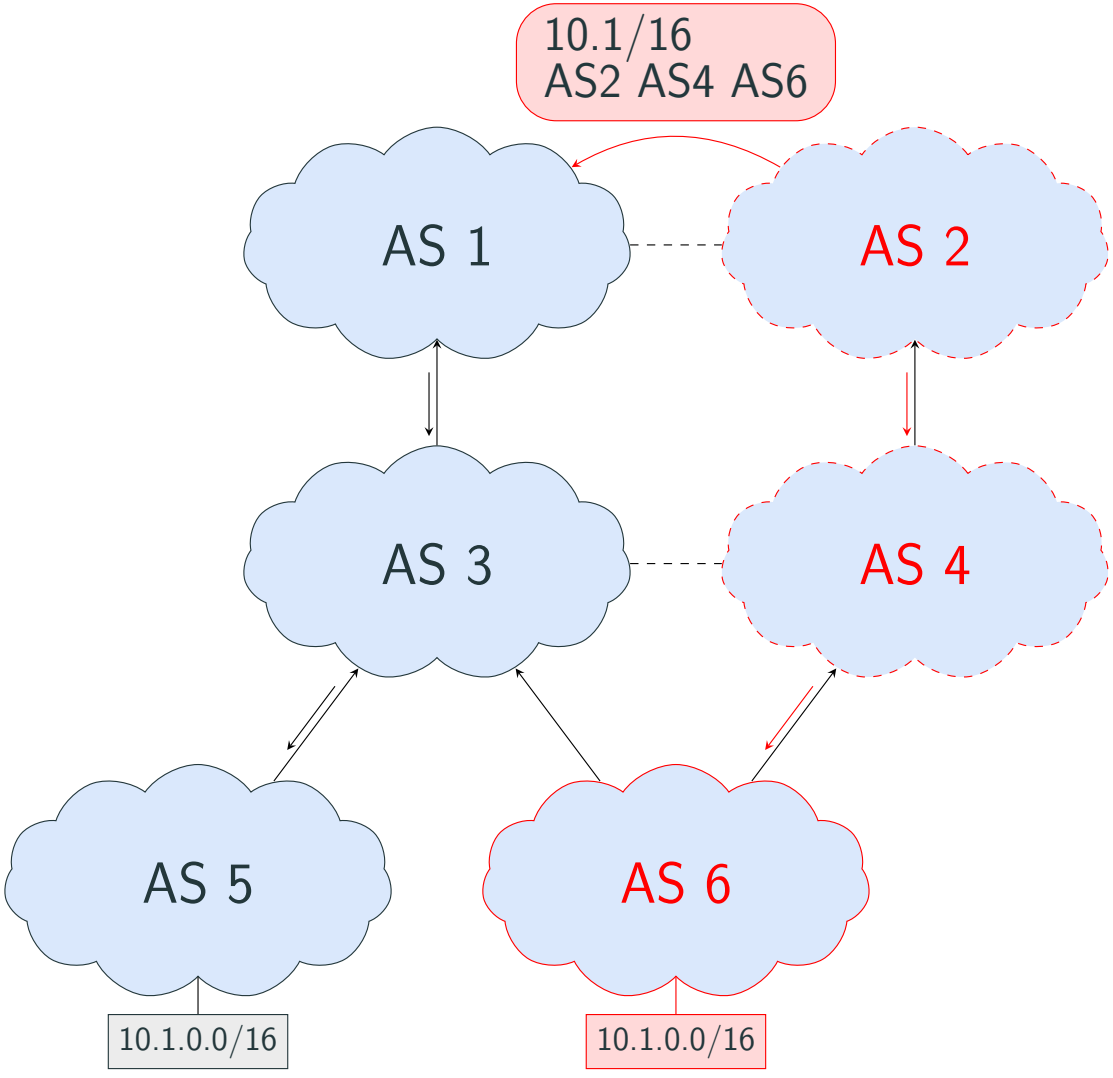


Figure 3: BGP hijack

BGP Hijacks

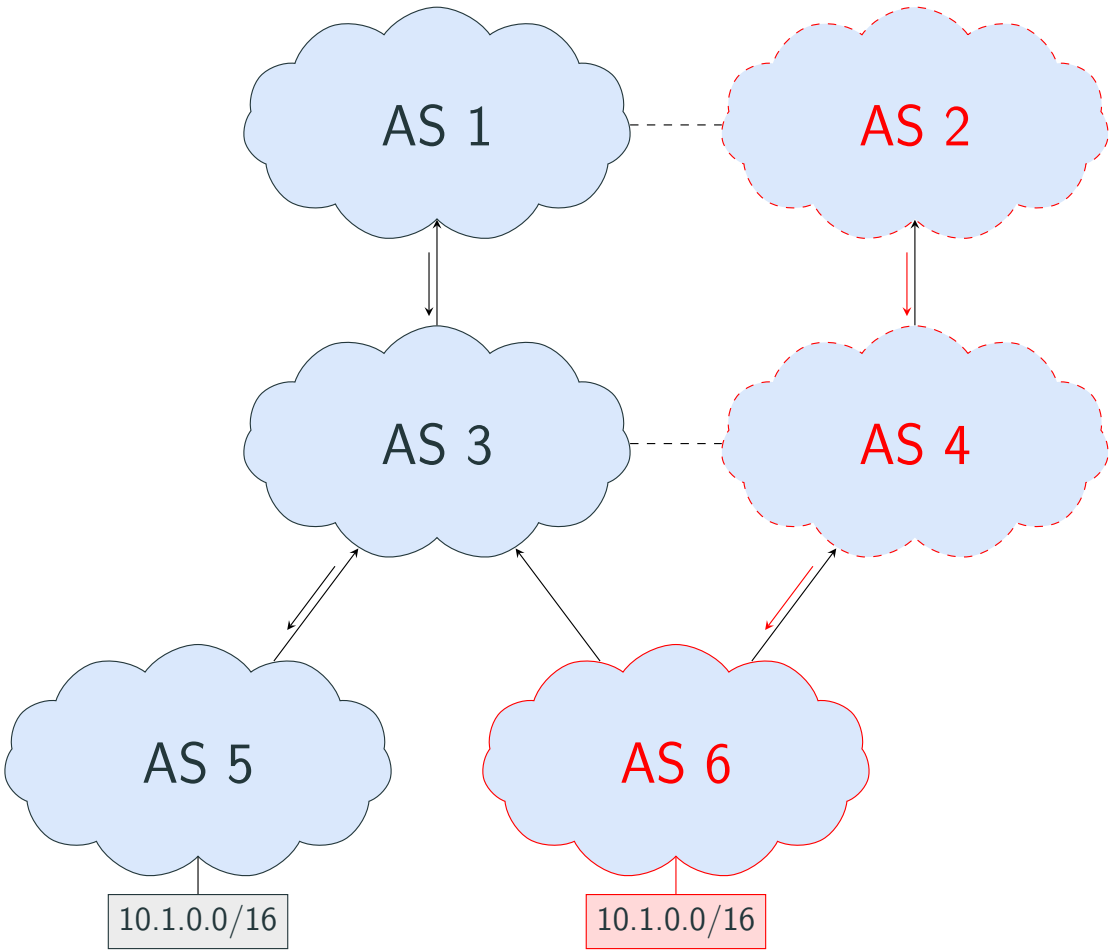


Figure 3: BGP hijack (Type-0[2])

[2]Sermpezis et al., "ARTEMIS: Neutralizing BGP hijacking within a minute".

BGP Hijacks - 5304 routing attacks in 2017 alone[2].

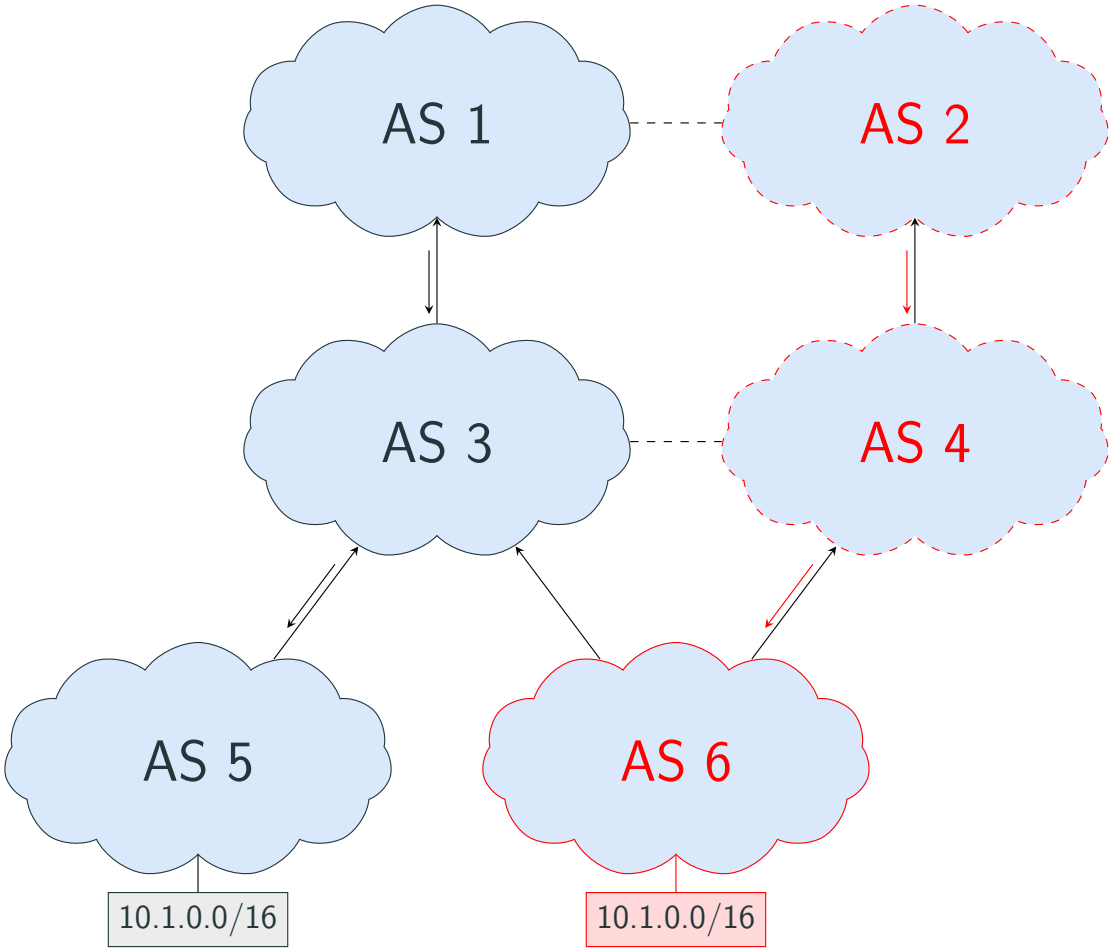


Figure 3: BGP hijack (Type-0)

[2]Robachevsky, **14,000 Incidents: A 2017 Routing Security Year in Review**.

BGP Blackjacks - Type-0

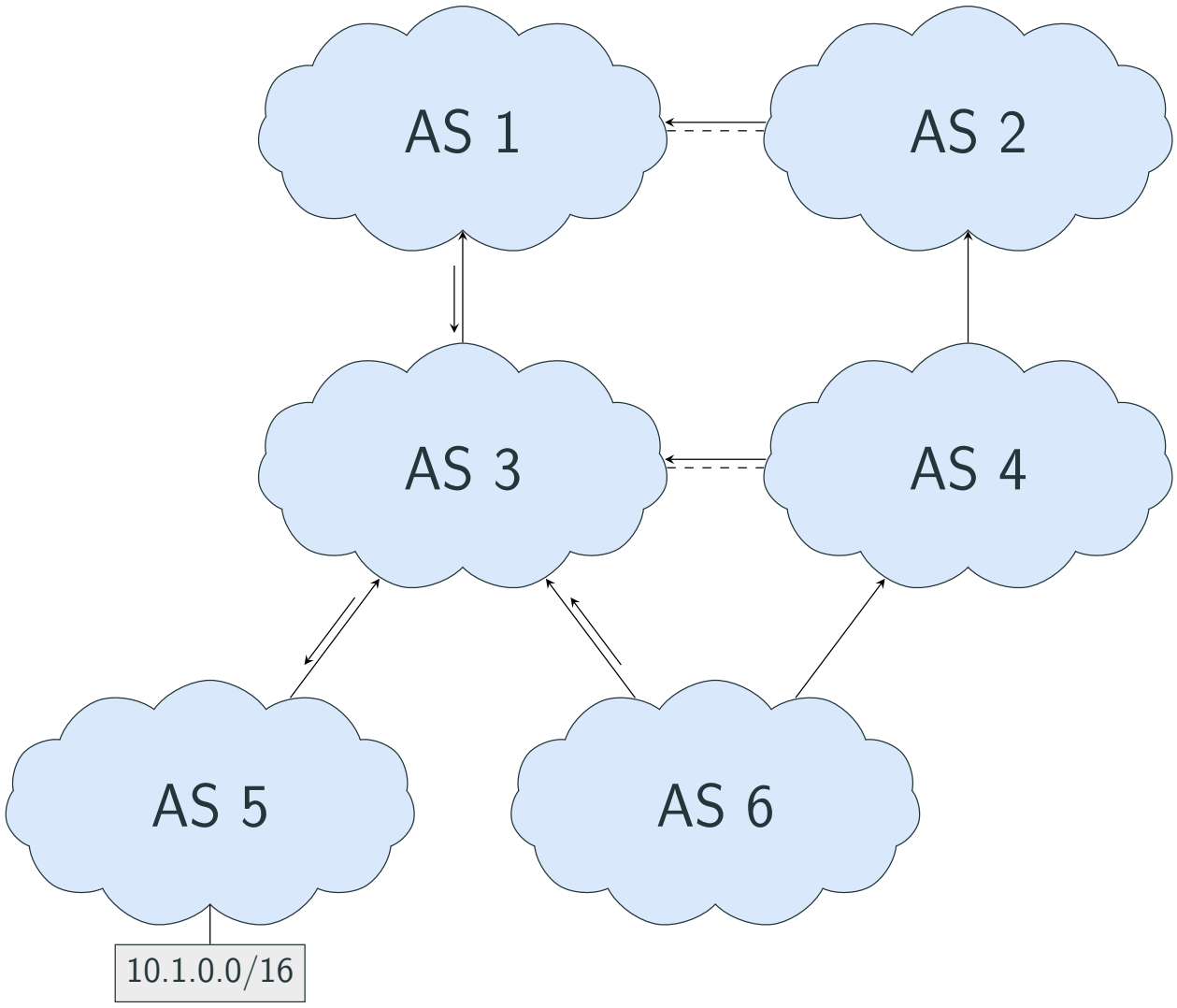


Figure 4: Type-0 blackjack

BGP Blackjacks - Type-0

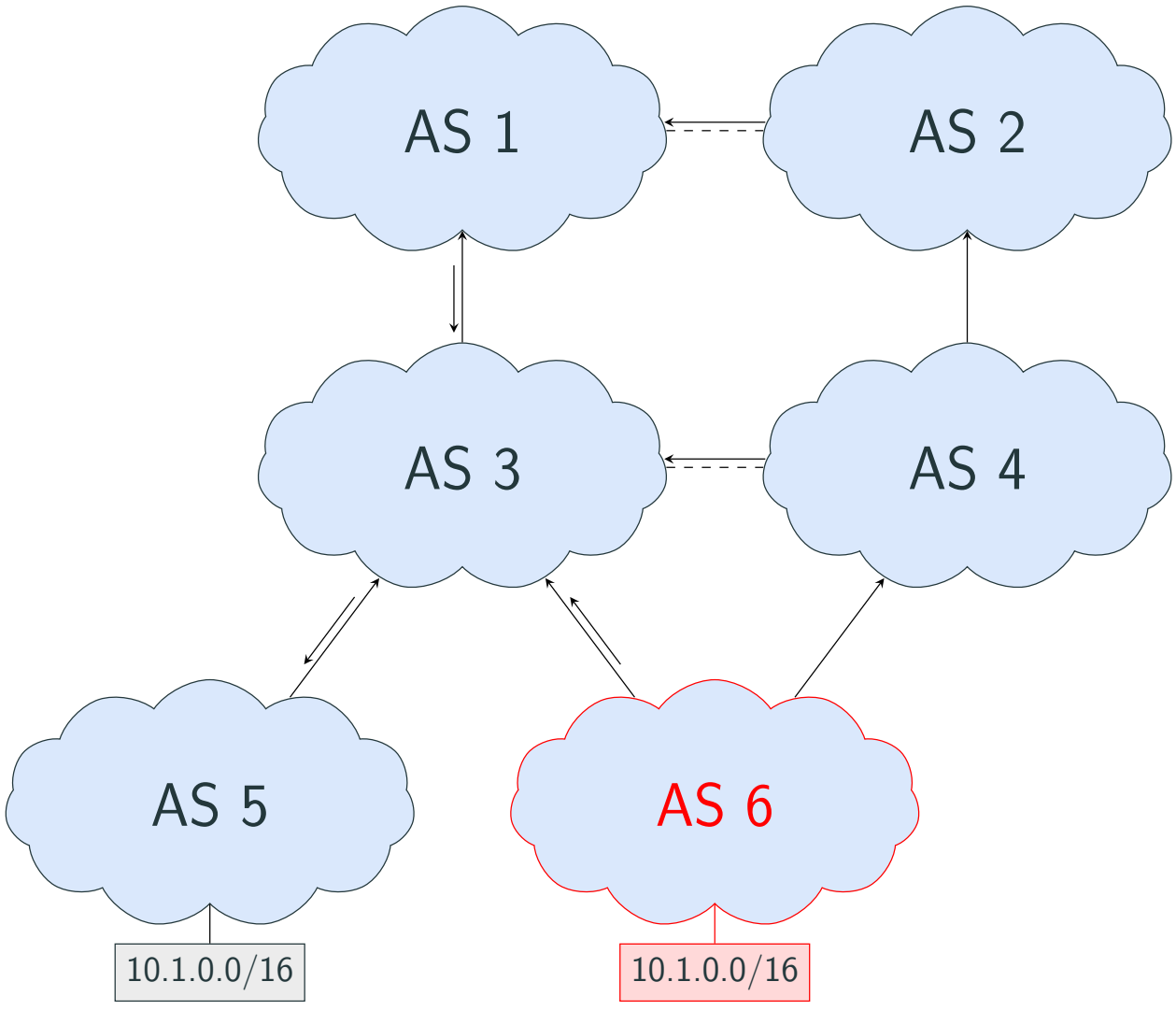


Figure 4: Type-0 blackjack

BGP Blackjacks - Type-0

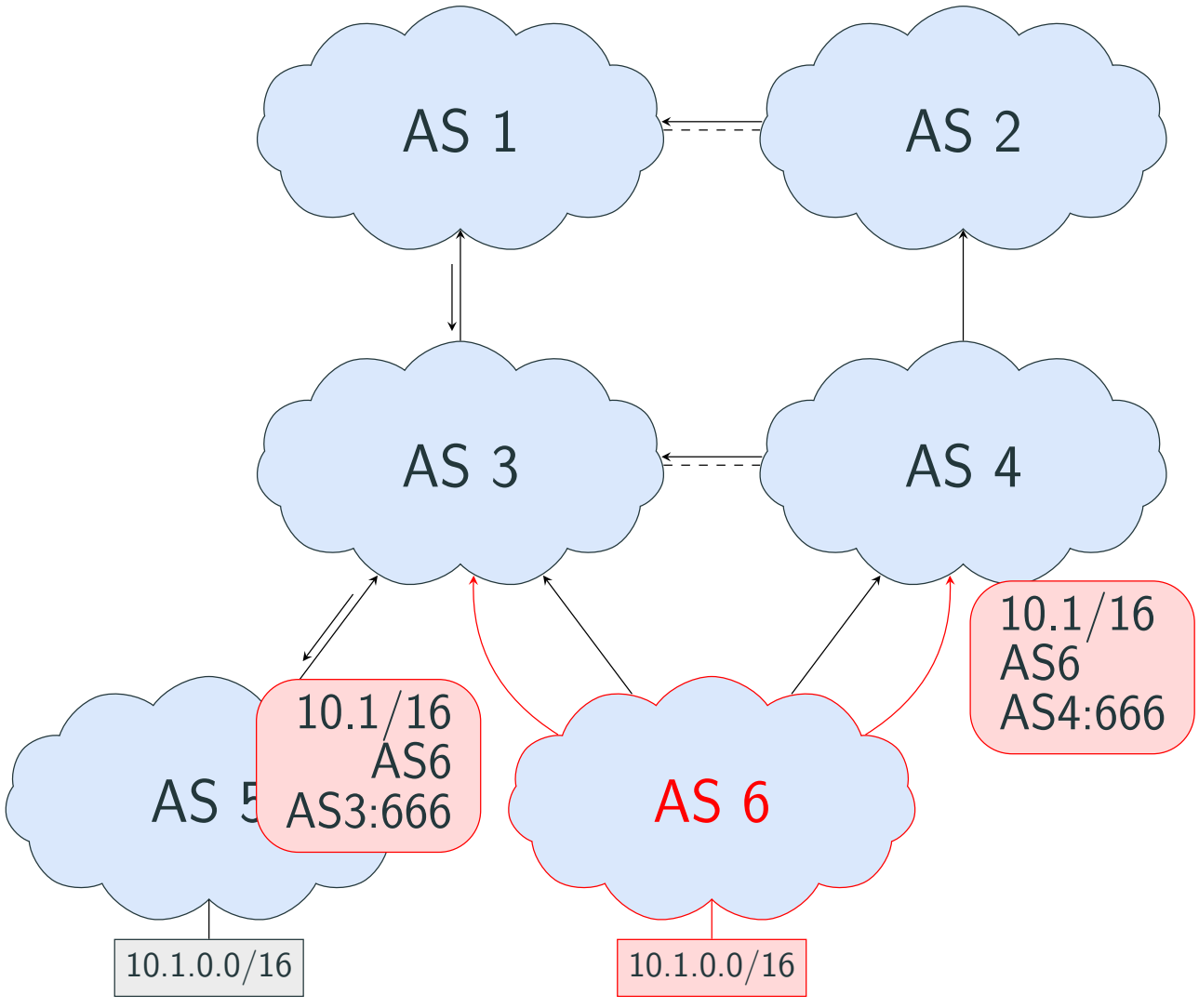


Figure 4: Type-0 blackjack

BGP Blackjacks - Type-0

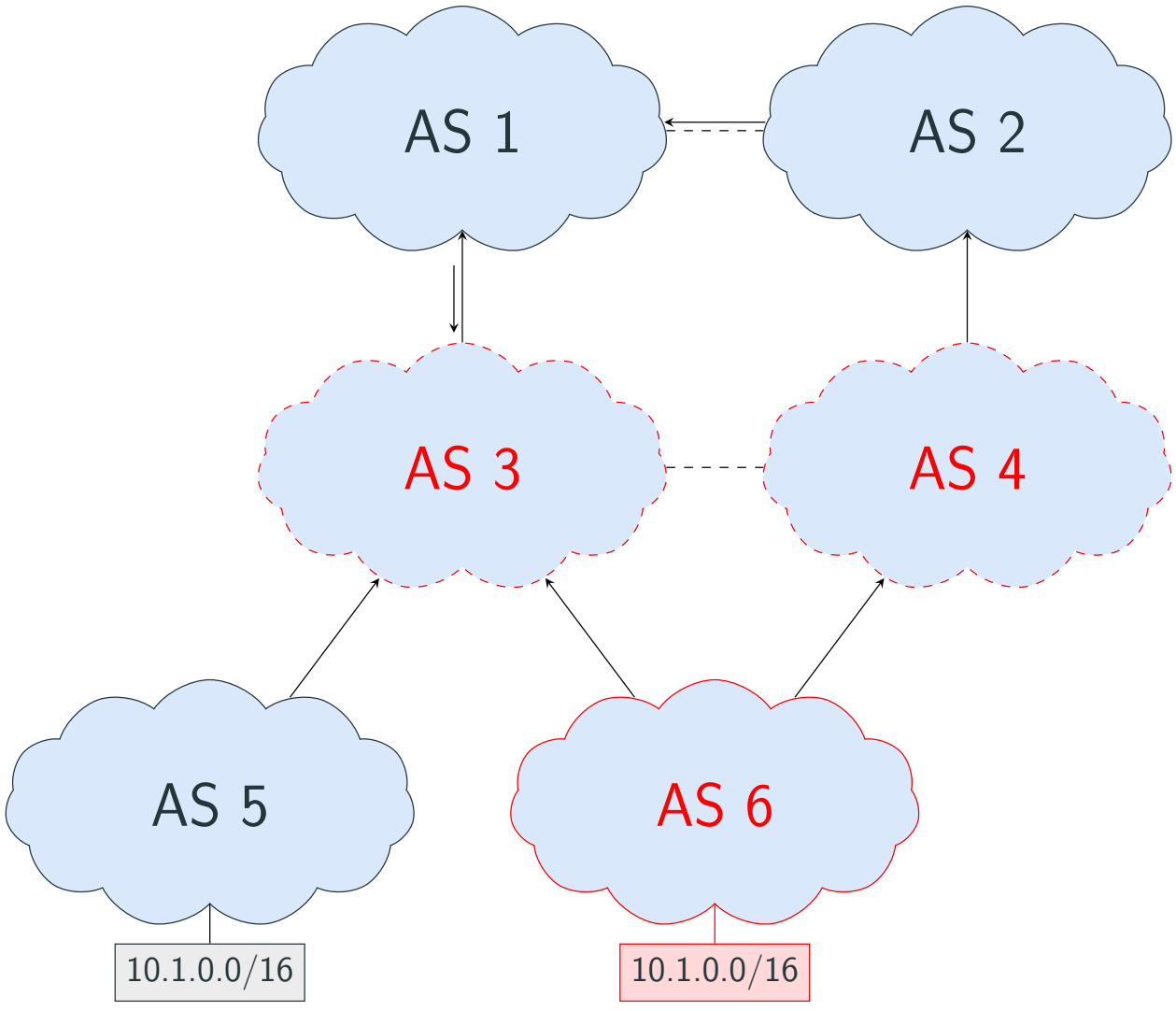


Figure 4: Type-0 blackjack

Best practices for legitimate blackholing empower blackjacks

Best Practices for blackholing[3]

Give a **higher priority** to blackholing.

Do **not propagate** the advertisement across AS borders.

[3] Cisco, **Remotely Triggered Black Hole Filtering - Destination Based and Source Based**.

Best practices for legitimate blackholing empower blackjacks

Best Practices for blackholing[3]

Give a **higher priority** to blackholing.

Do **not propagate** the advertisement across AS borders.

Advantages of blackjacks

Reach: Precedence over AS path length. Even ASes far away are vulnerable.

No propagation: More disruption.

Stealth: The attacker is not dropping traffic himself.

---

[3] Cisco, **Remotely Triggered Black Hole Filtering - Destination Based and Source Based**.

RPKI - Resource Public Key Infrastructure[4]

The RPKI is a distributed, hierarchic public key infrastructure. It allows prefix holders to emit digitally signed objects attesting that a given AS is **authorized to originate** routes for a set of prefixes.

[4] Lepinski and Kent, **An Infrastructure to Support Secure Internet Routing**.

RPKI - Resource Public Key Infrastructure

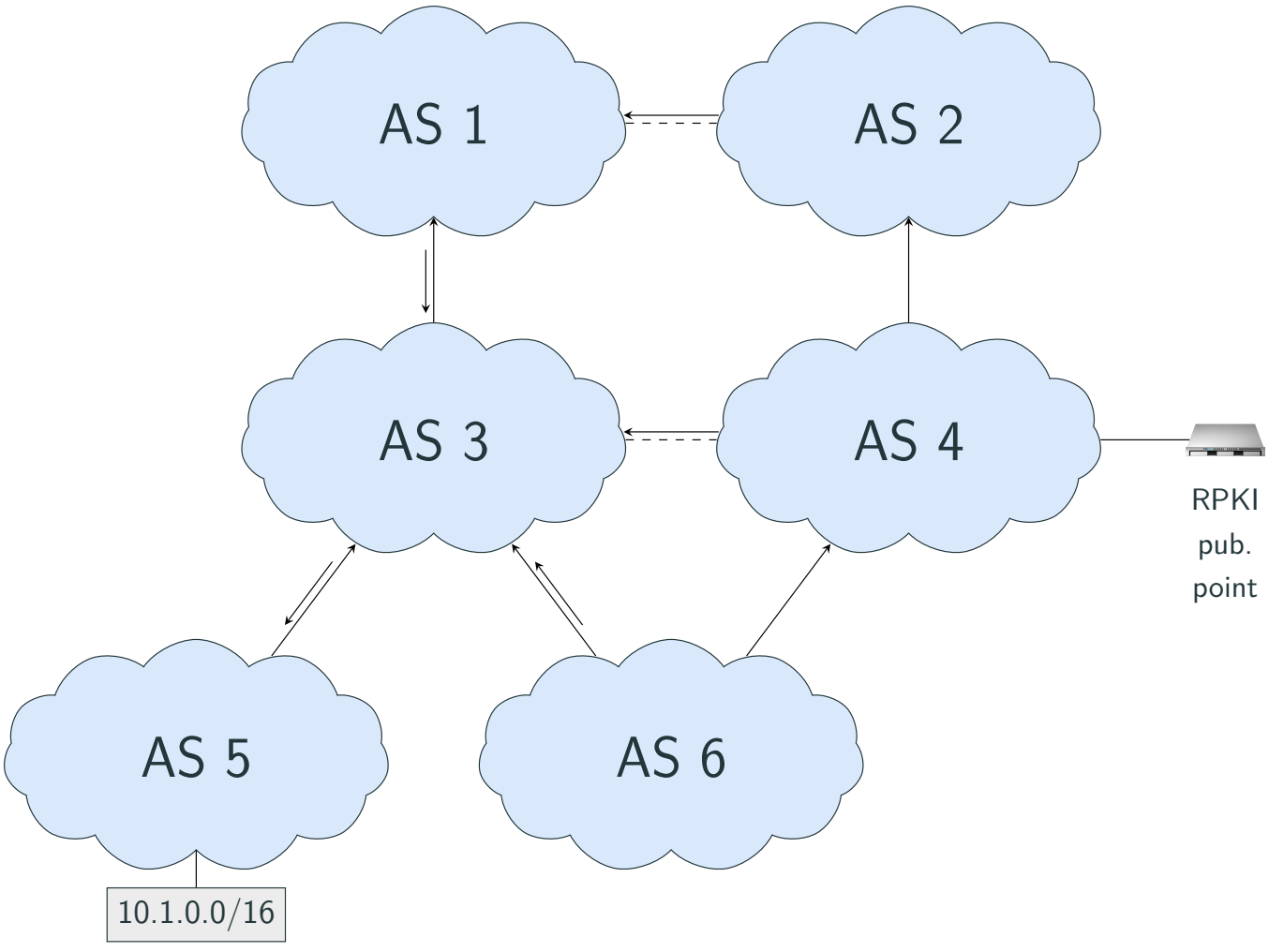


Figure 5: RPKI usage

RPKI - Resource Public Key Infrastructure

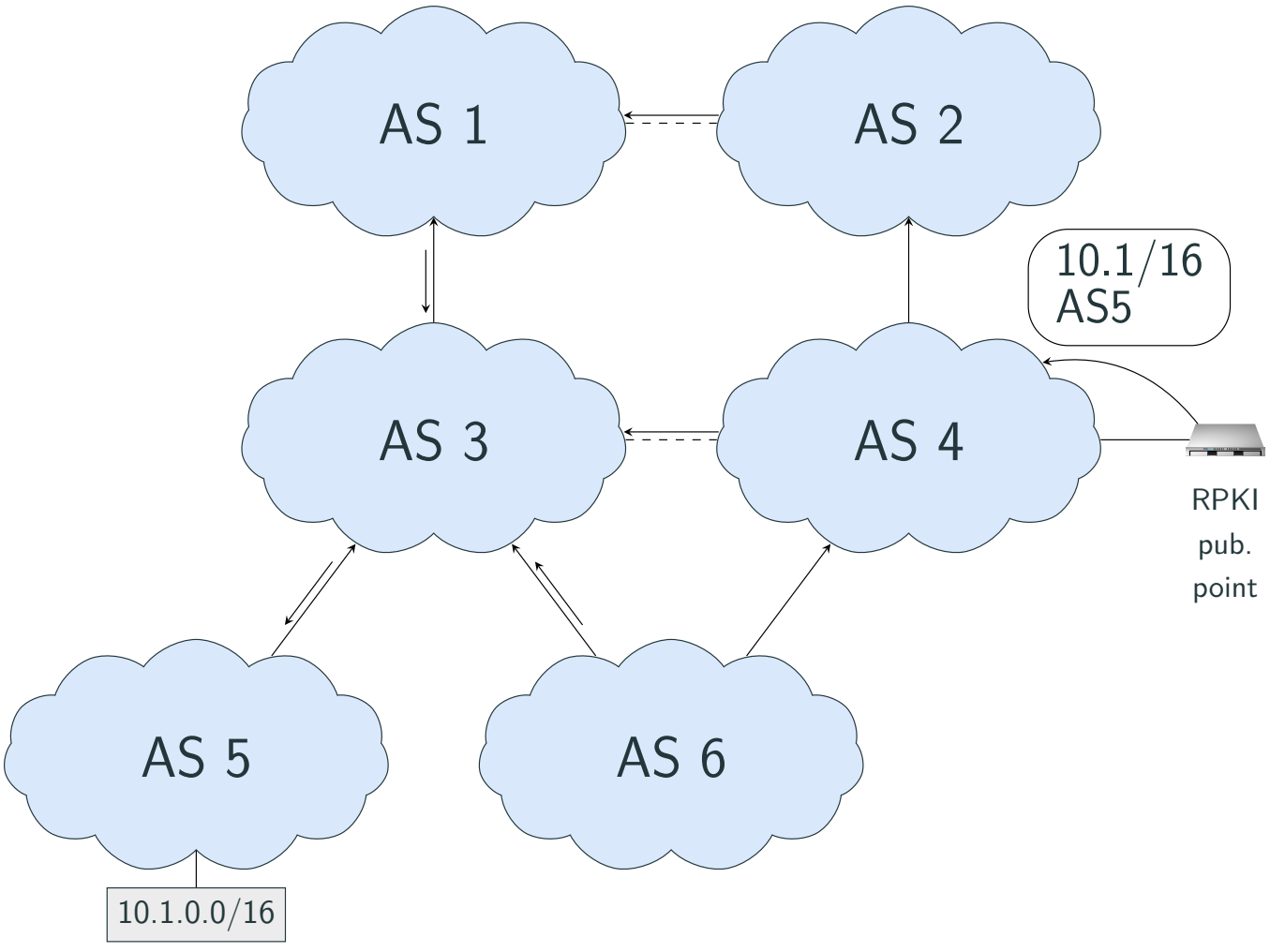


Figure 5: RPKI usage

RPKI - Resource Public Key Infrastructure

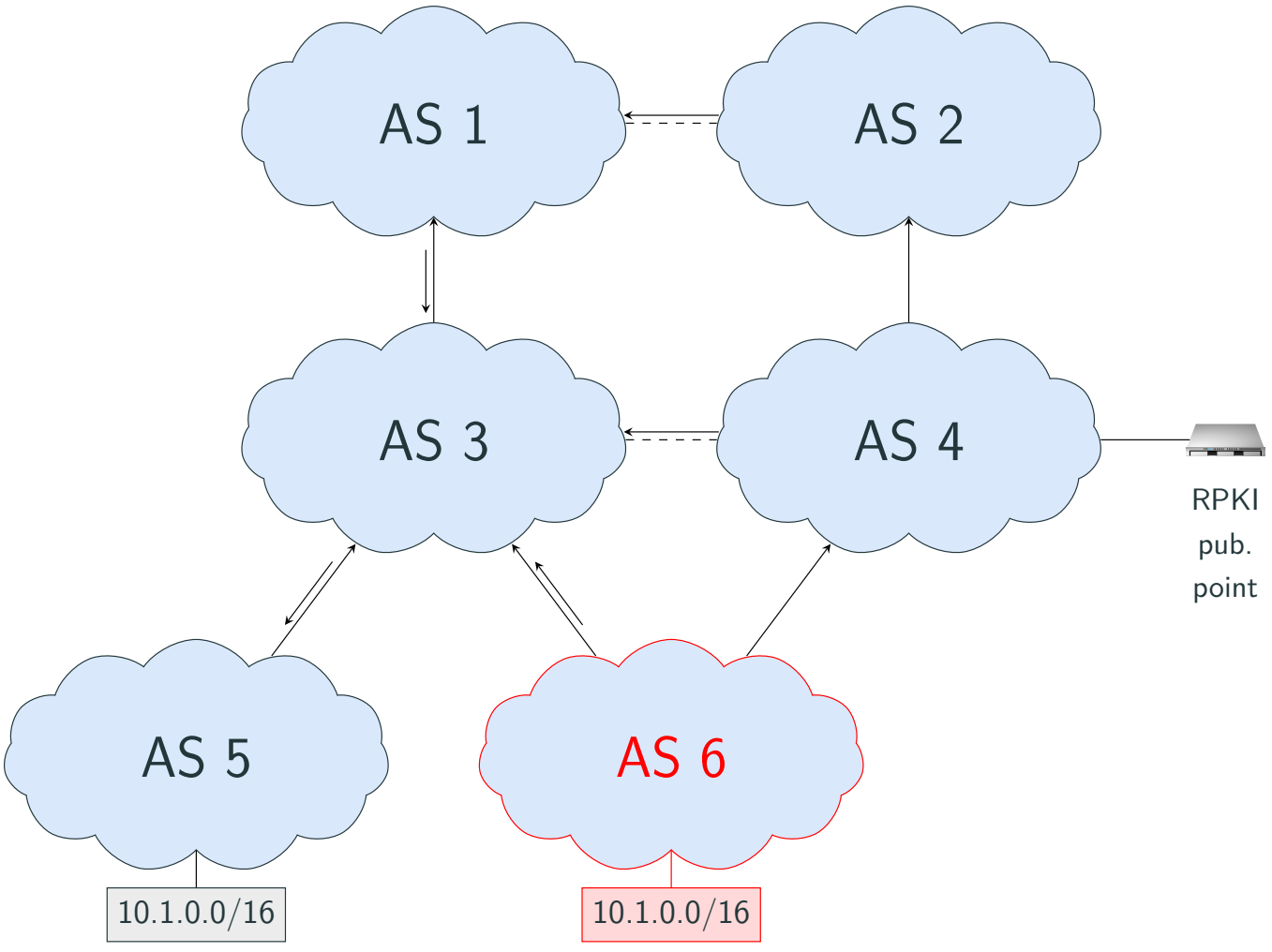


Figure 5: RPKI usage

RPKI - Resource Public Key Infrastructure

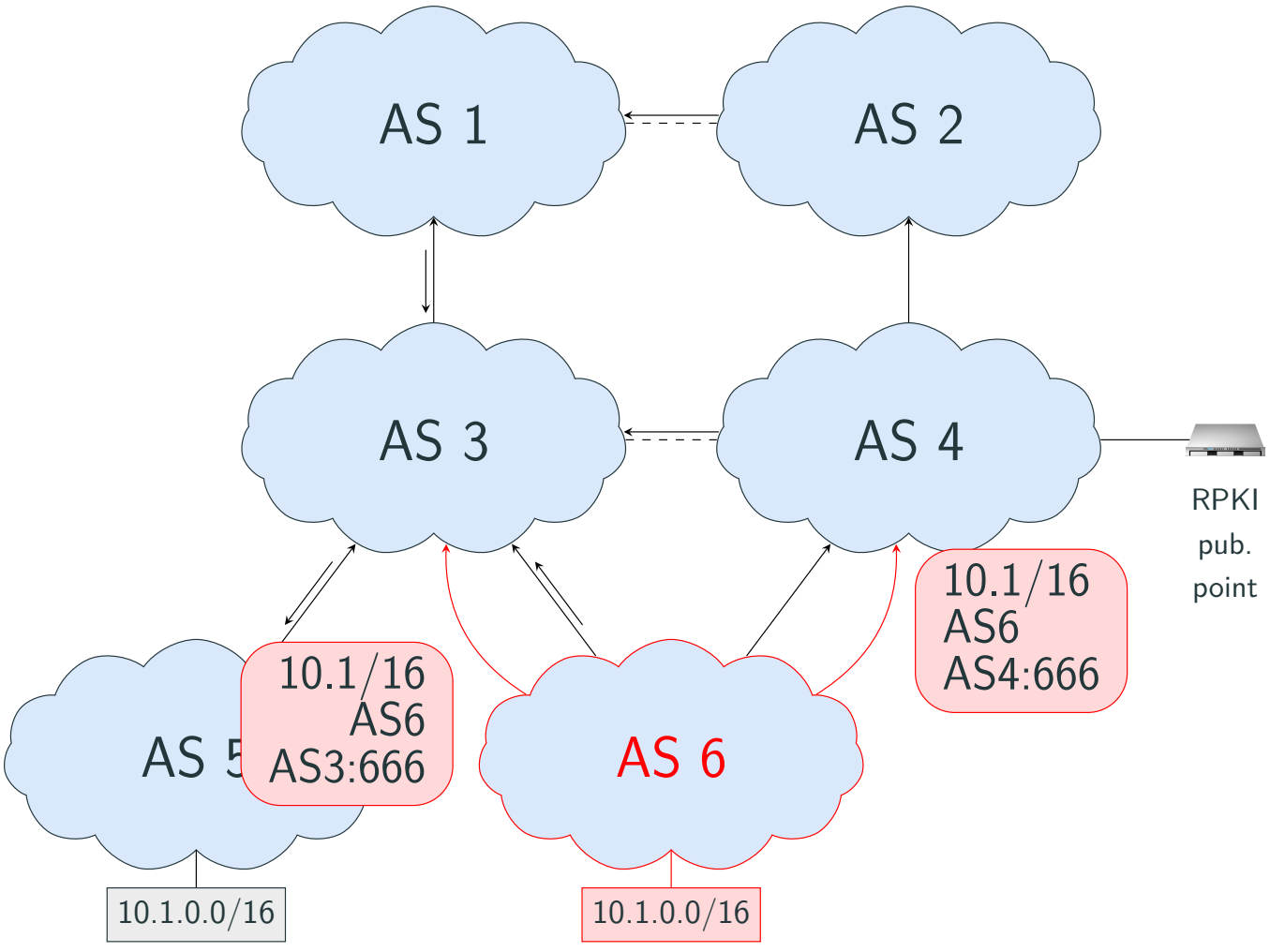


Figure 5: RPKI usage

RPKI - Resource Public Key Infrastructure

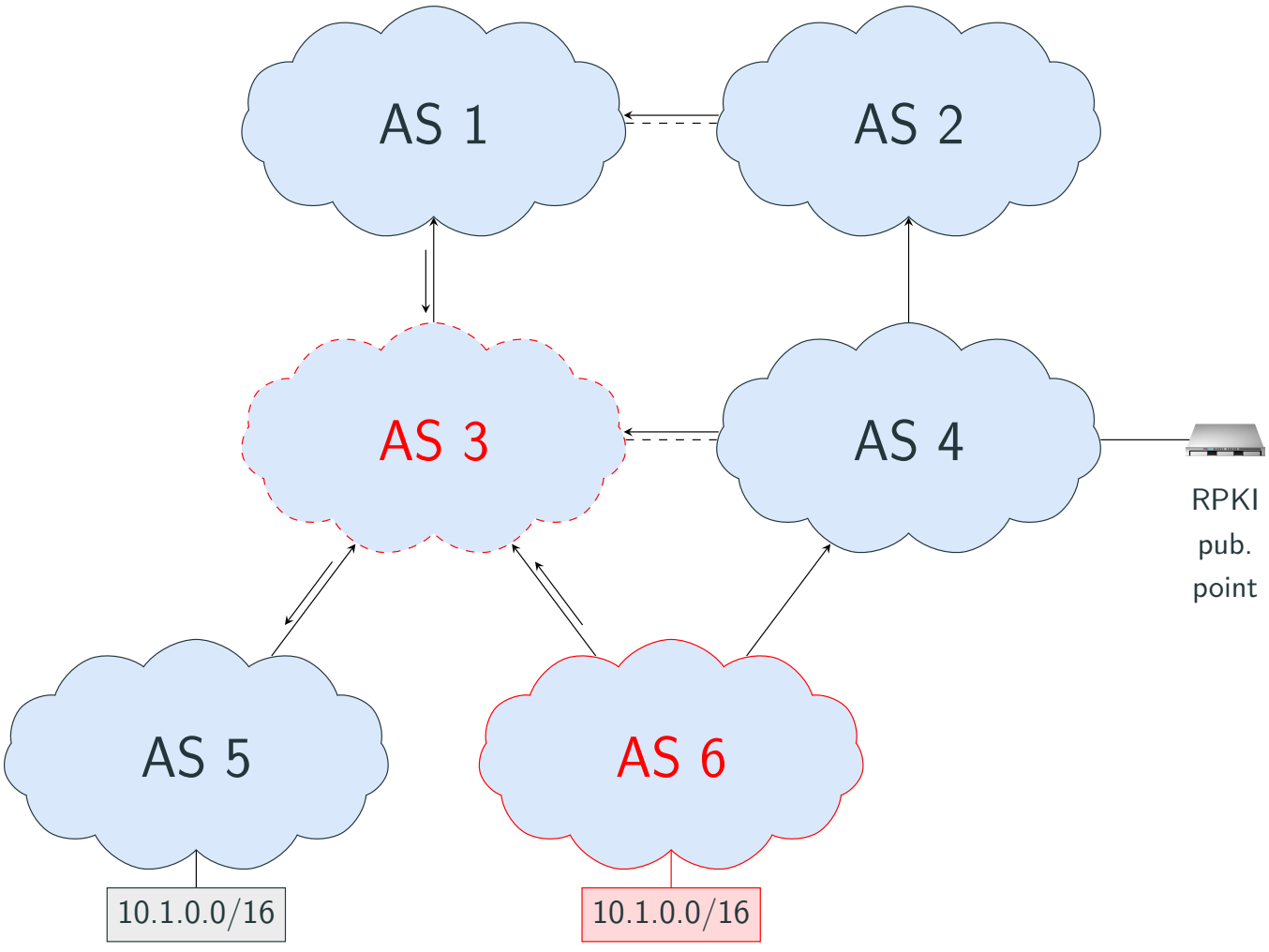


Figure 5: RPKI usage

BGP Blackjacks - Type-N

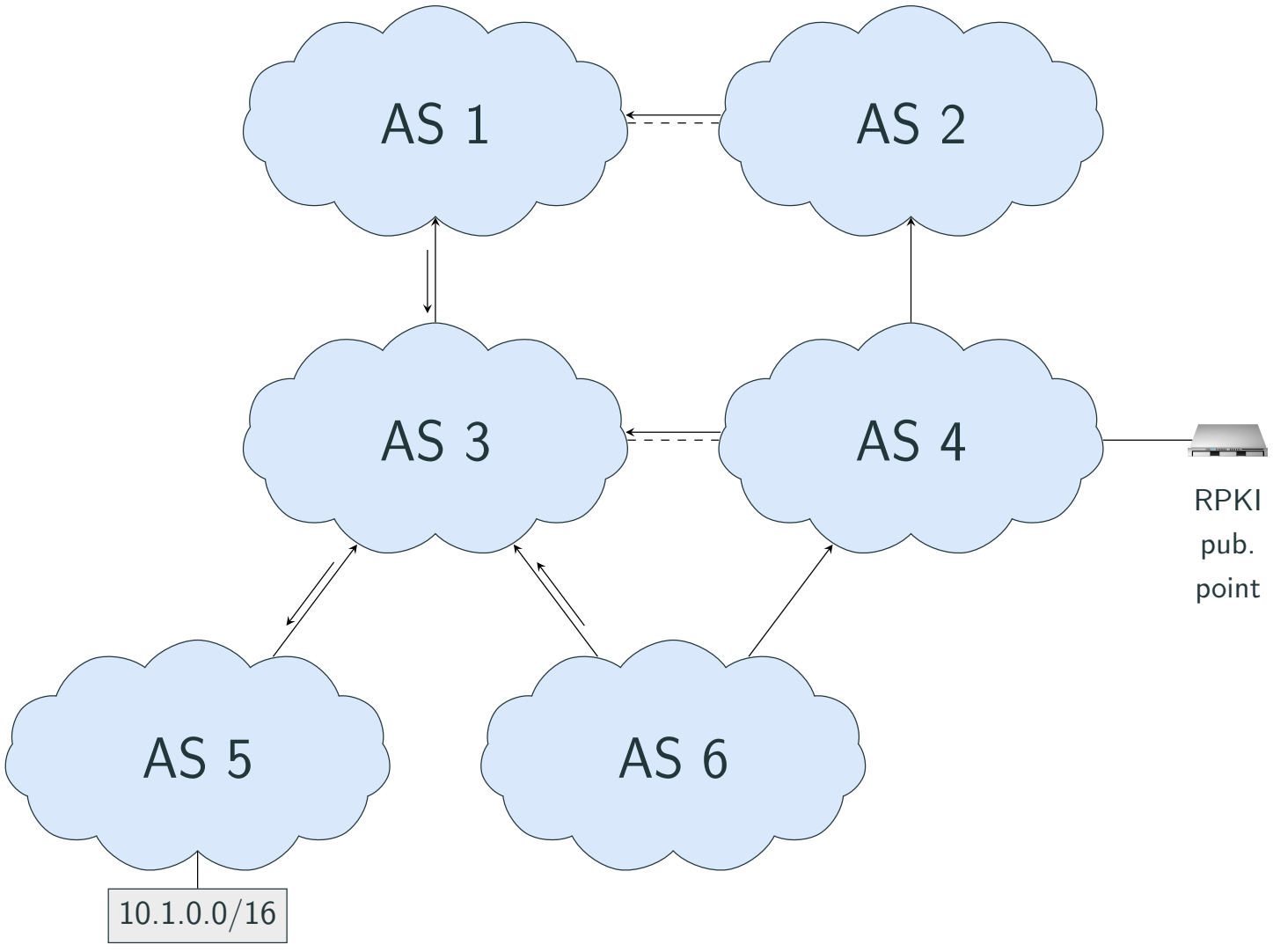


Figure 6: Type-N blackjack

BGP Blackjacks - Type-N

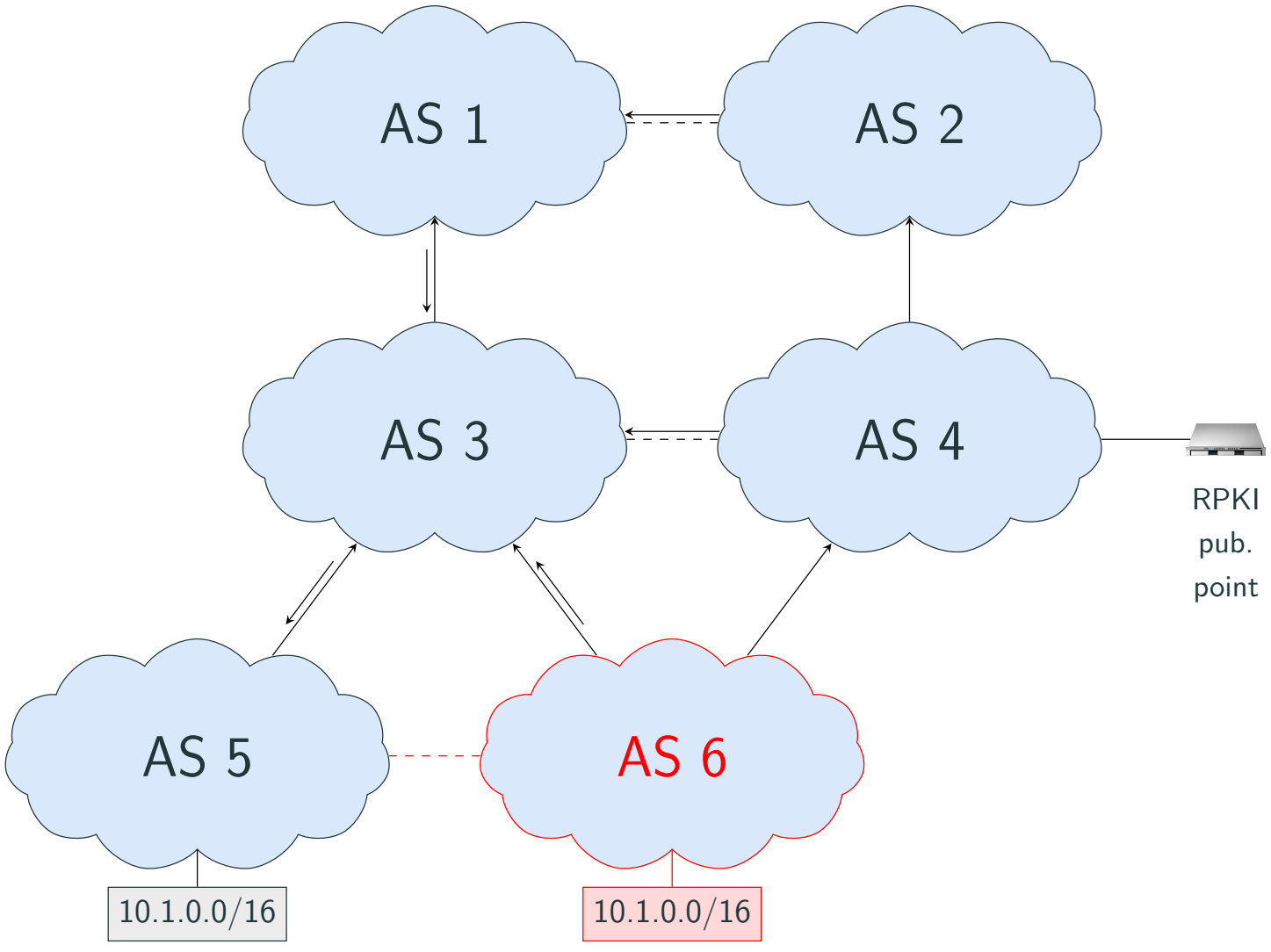


Figure 6: Type-N blackjack

BGP Blackjacks - Type-N

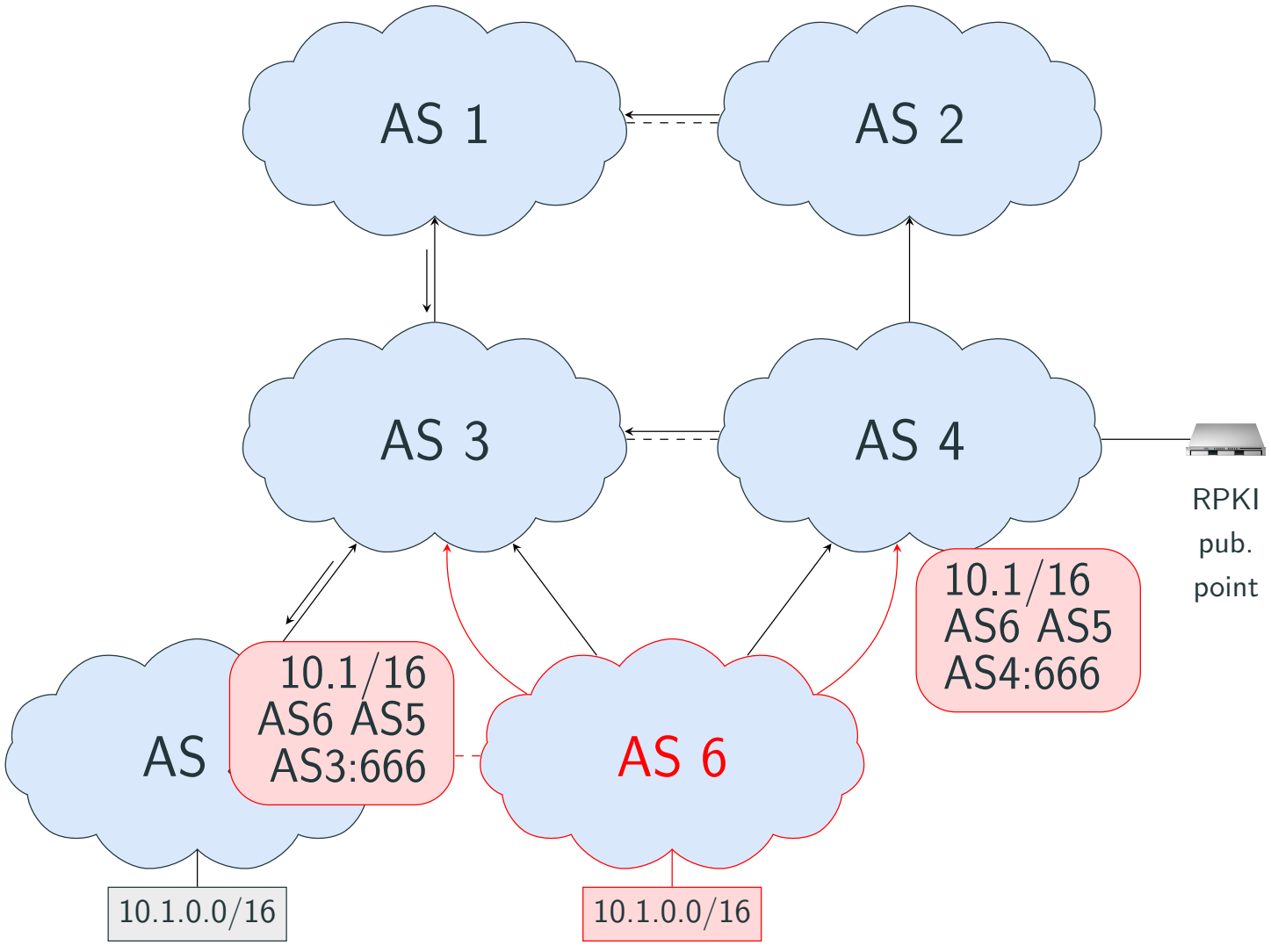


Figure 6: Type-N blackjack

BGP Blackjacks - Type-N

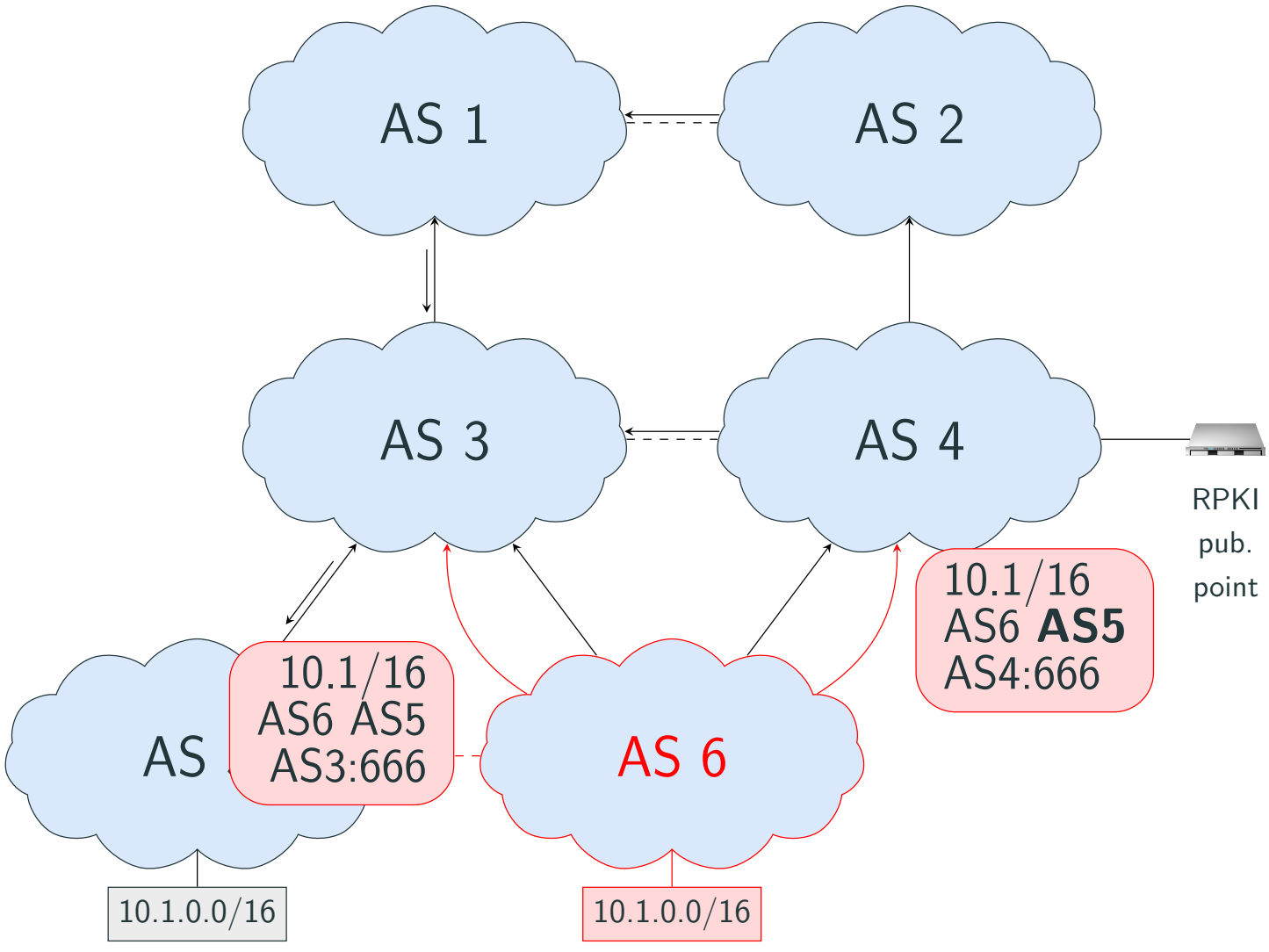


Figure 6: Type-N blackjack

BGP Blackjacks - Type-N

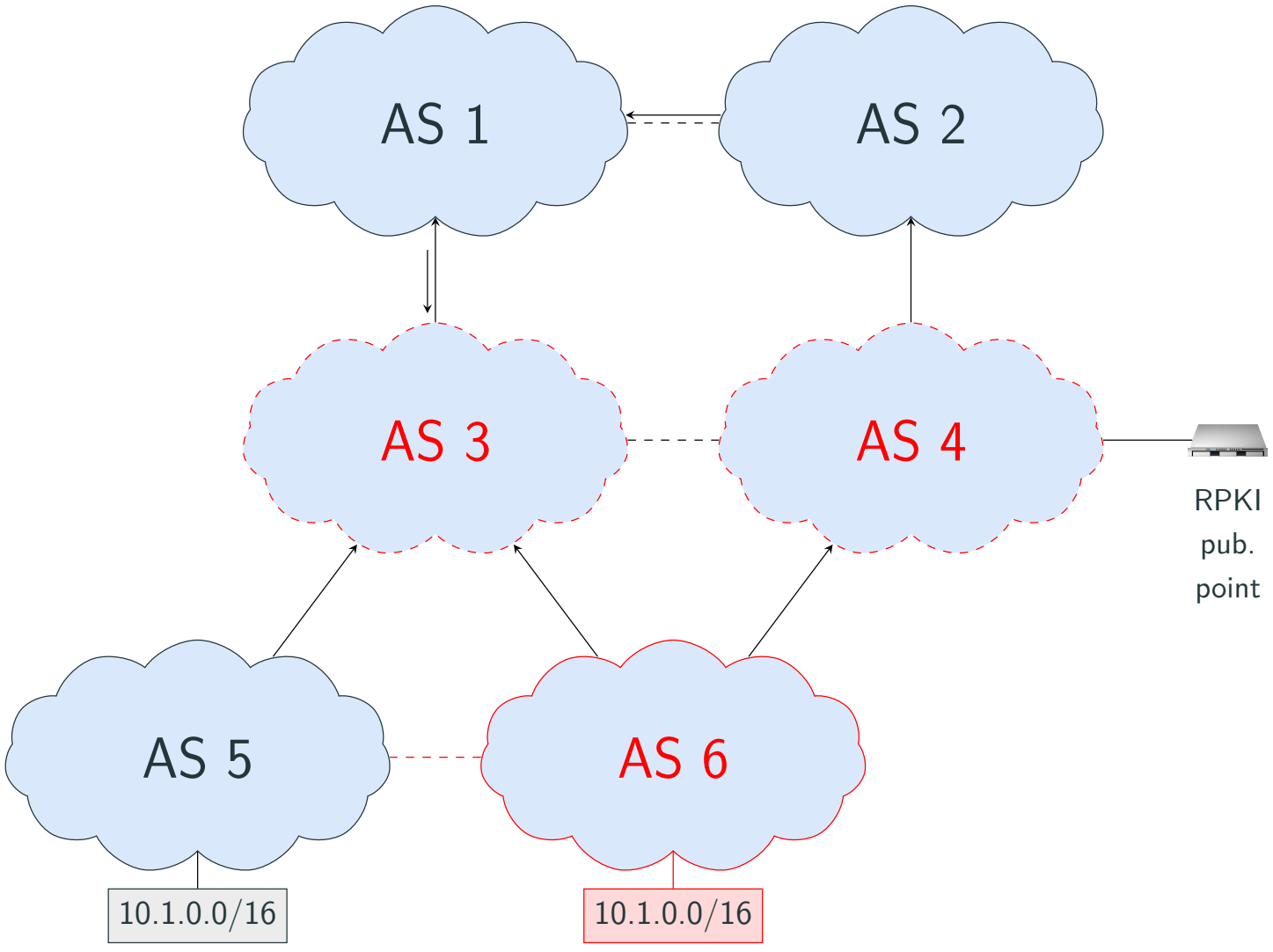


Figure 6: Type-N blackjack

BGPsec[5]

BGPsec modifies BGP to allow ASes to **sign** advertisements. This guarantees the AS path reflects the **actual path** the advertisement went through.

[5] Lepinski and Sriram, **BGPsec Protocol Specification**.

BGPsec

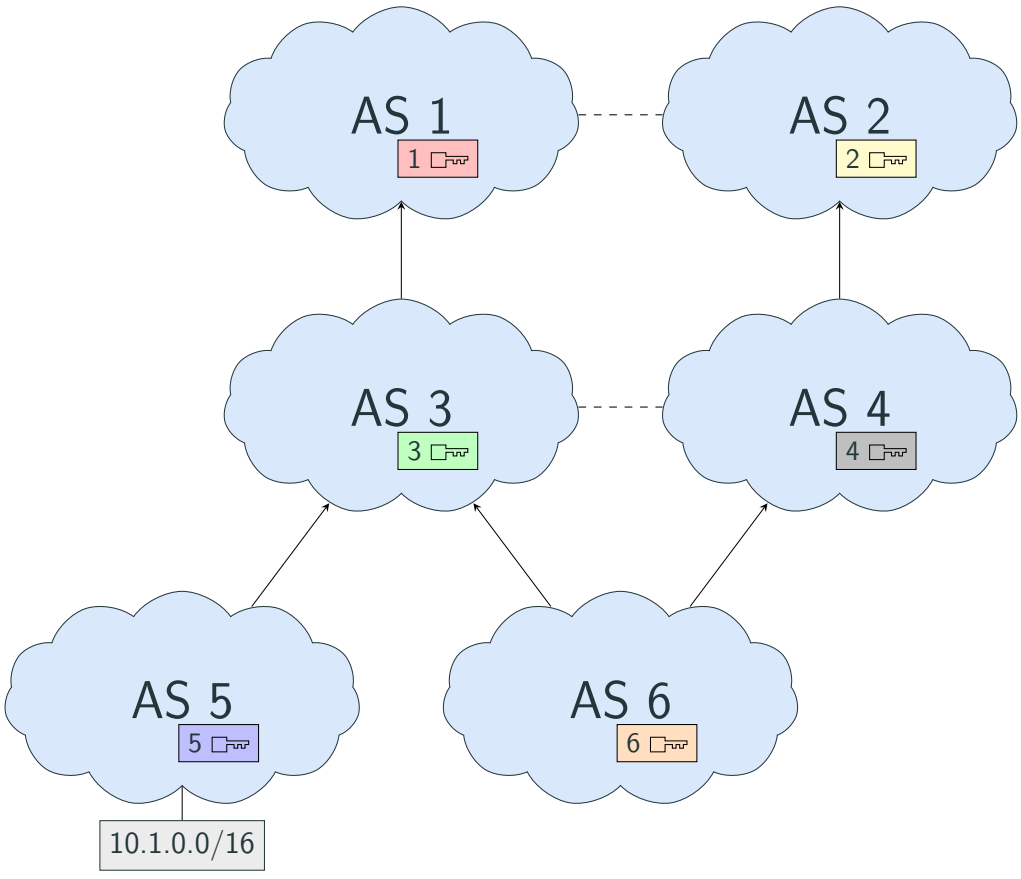


Figure 7: BGPsec message propagation

BGPsec

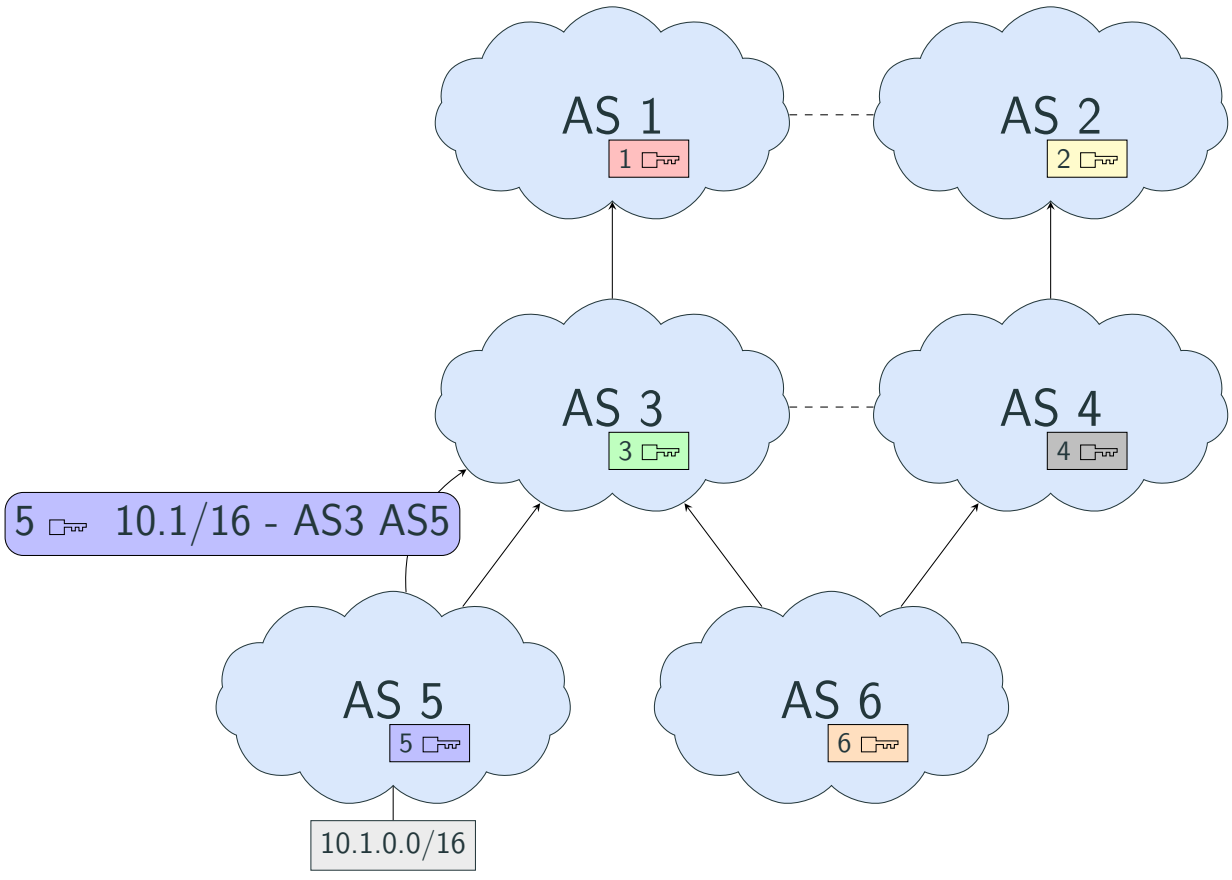


Figure 7: BGPsec message propagation

BGPsec

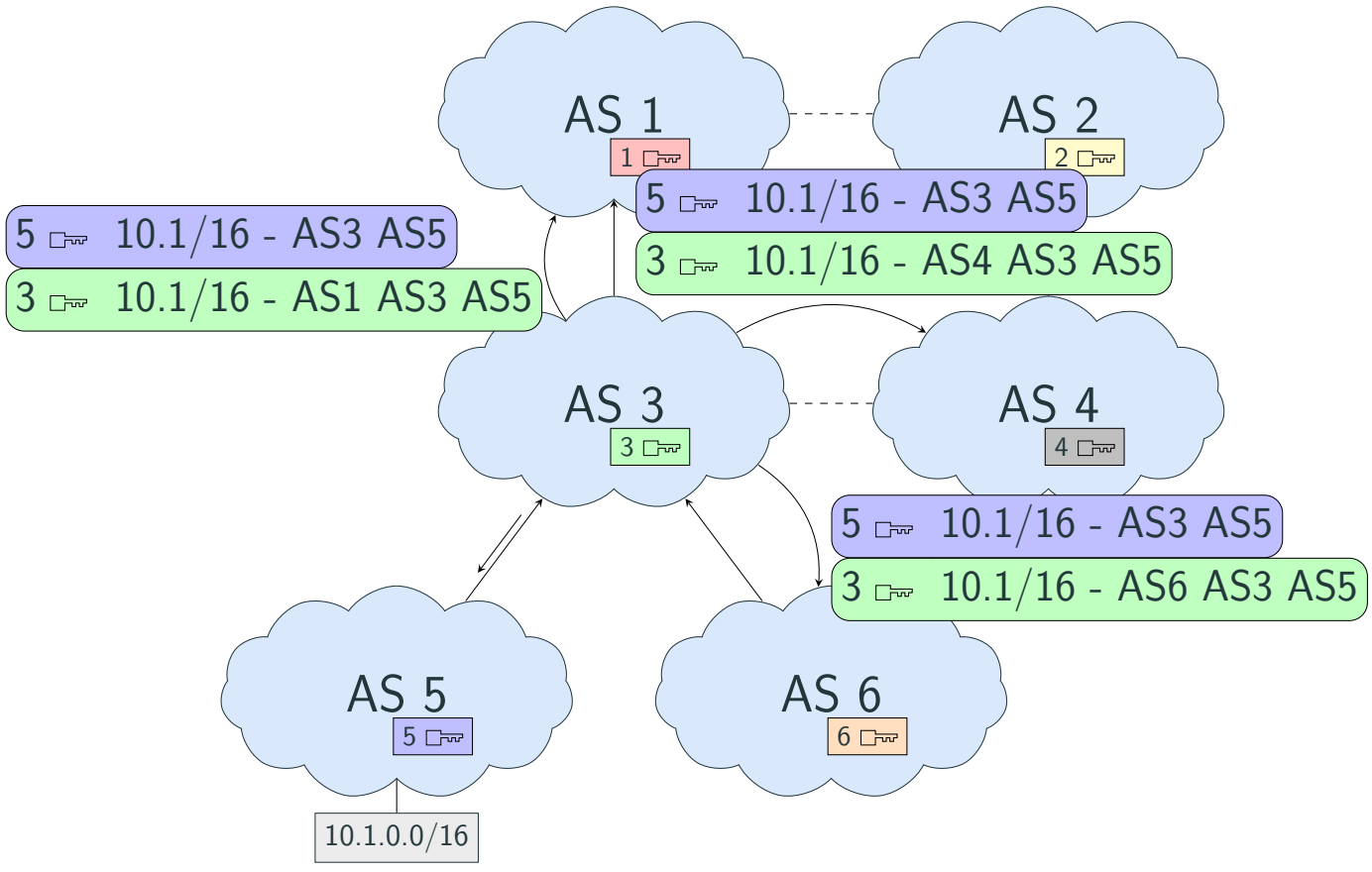


Figure 7: BGPsec message propagation

BGPsec

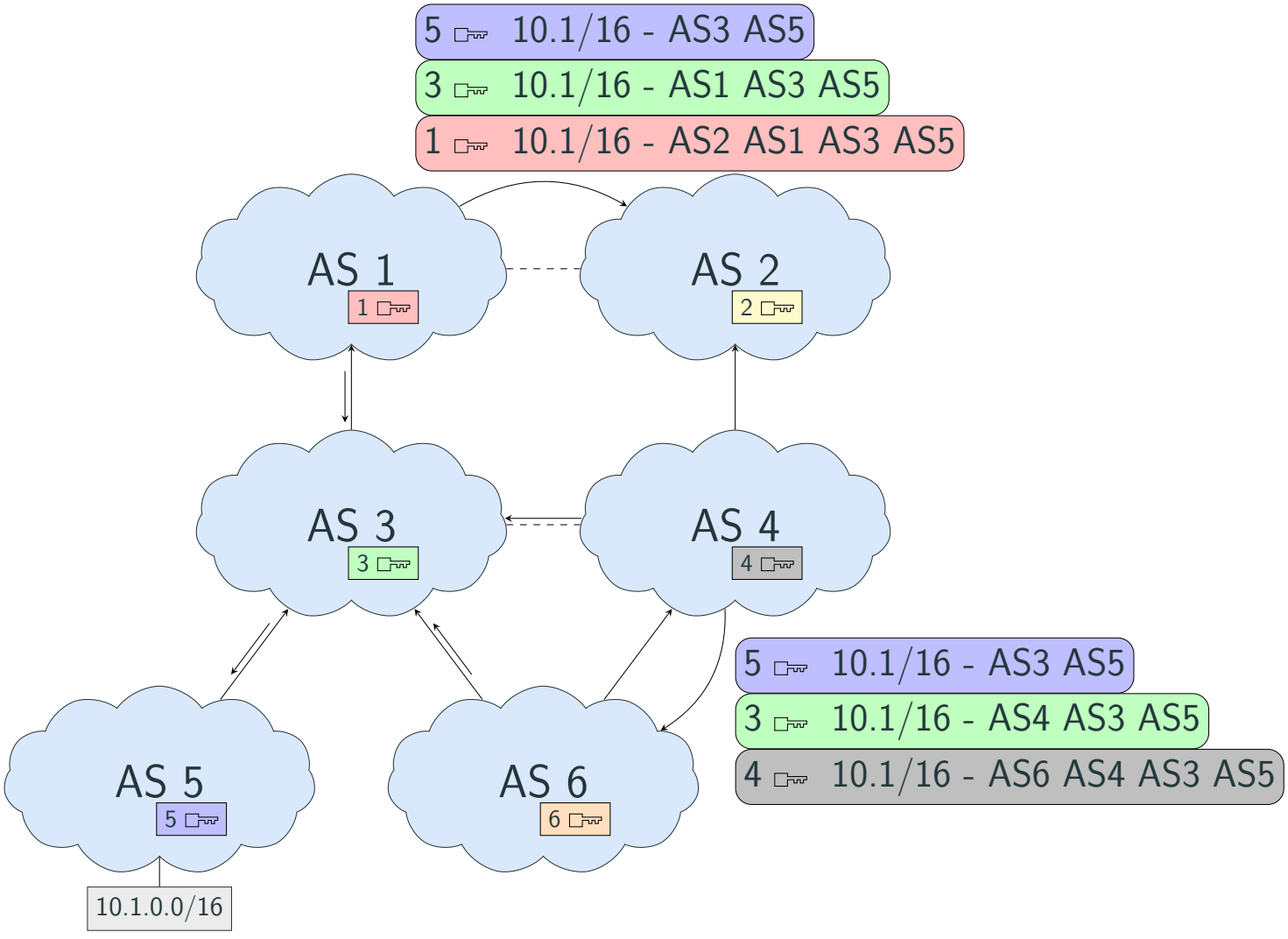


Figure 7: BGPsec message propagation

BGPsec

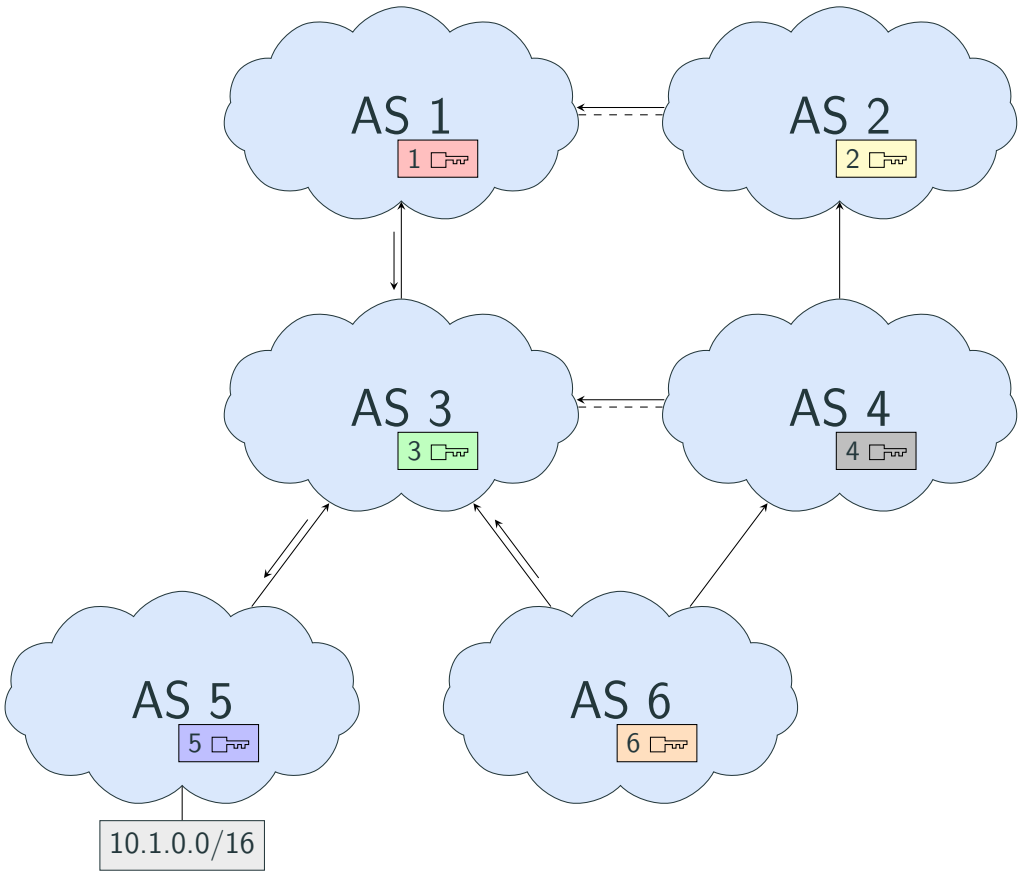


Figure 7: BGPsec message propagation

BGP Blackjacks - Type-N

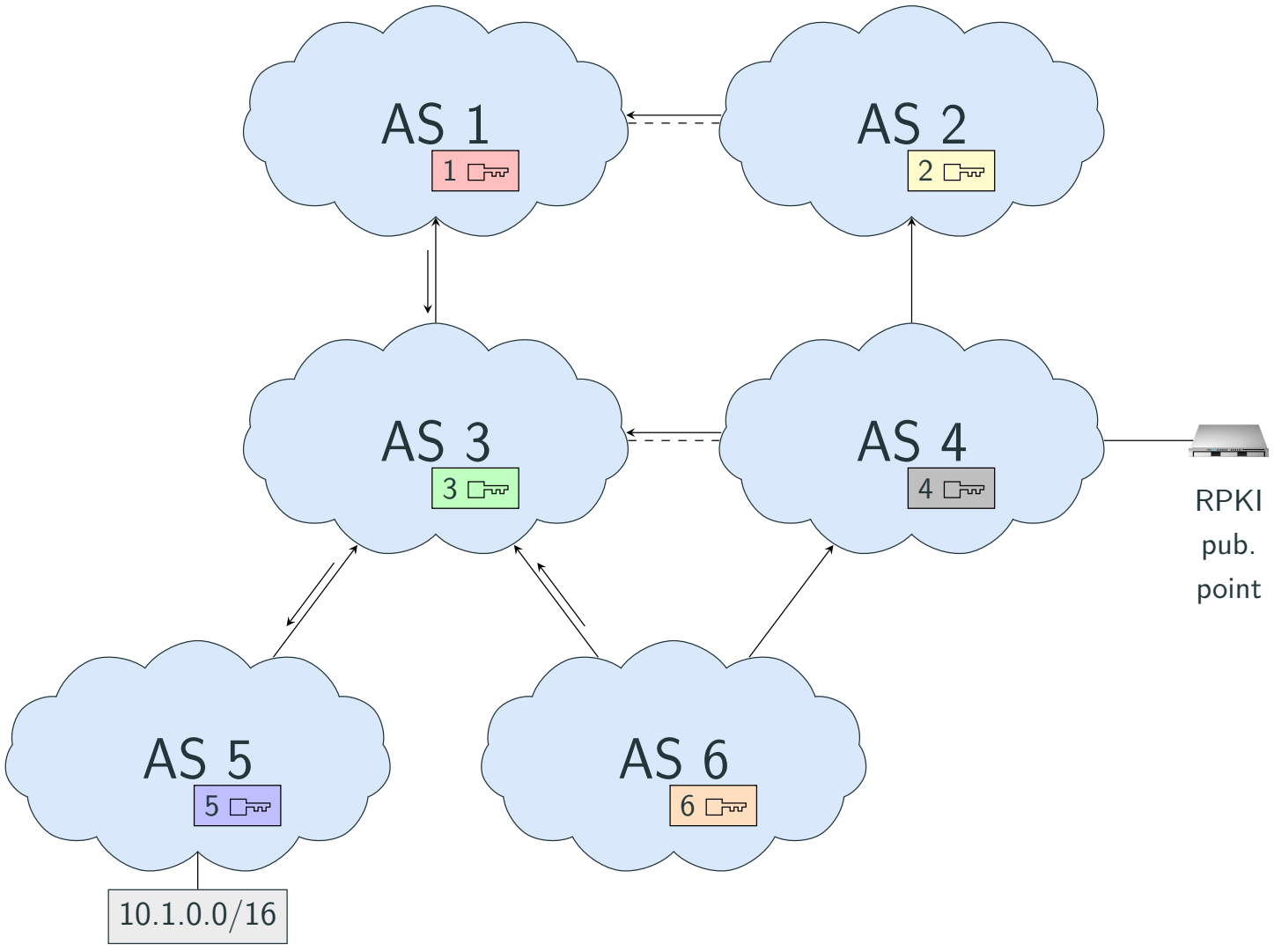


Figure 8: Type-N blackjack

BGP Blackjacks - Type-N

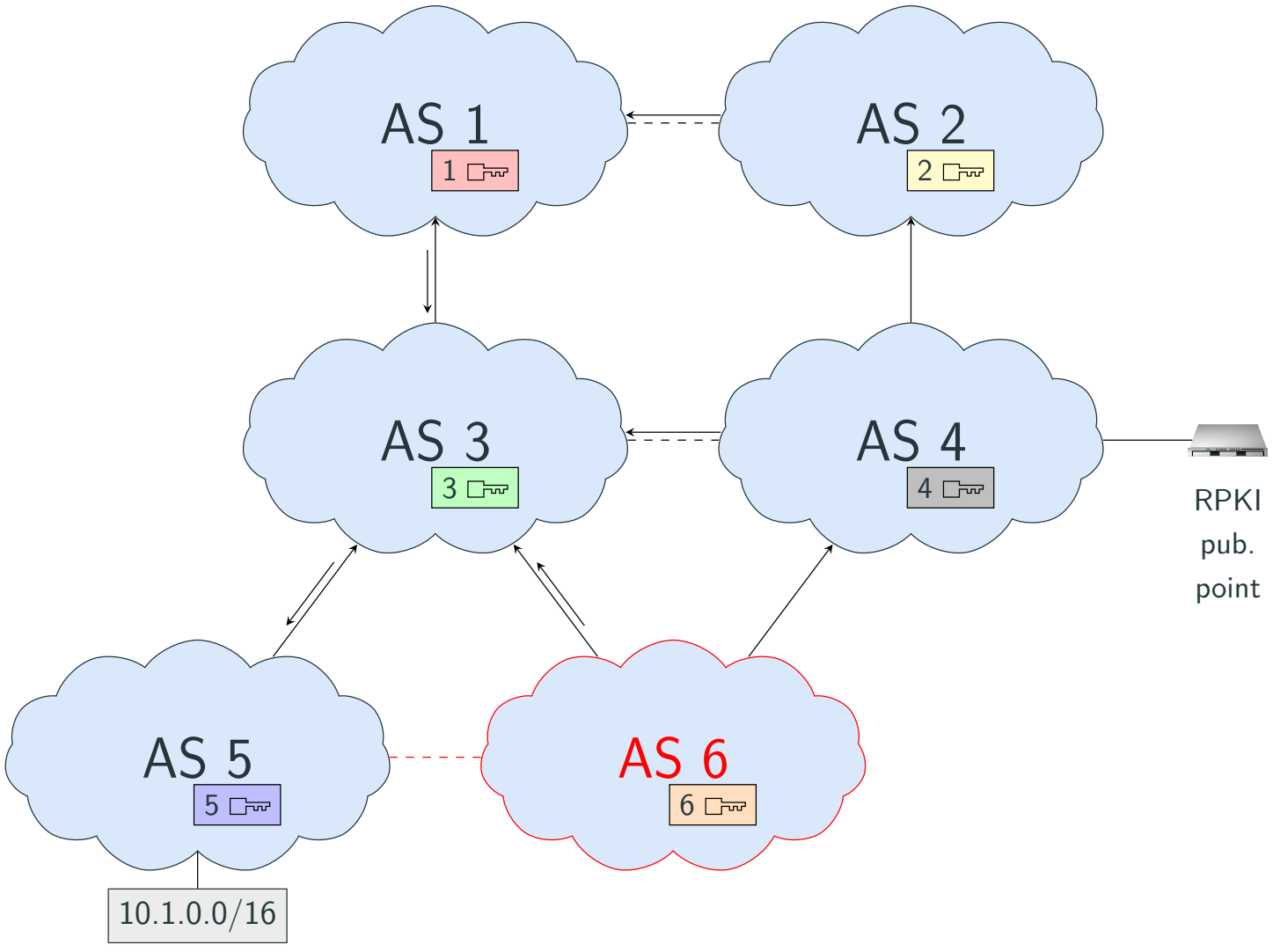


Figure 8: Type-N blackjack

BGP Blackjacks - Type-N

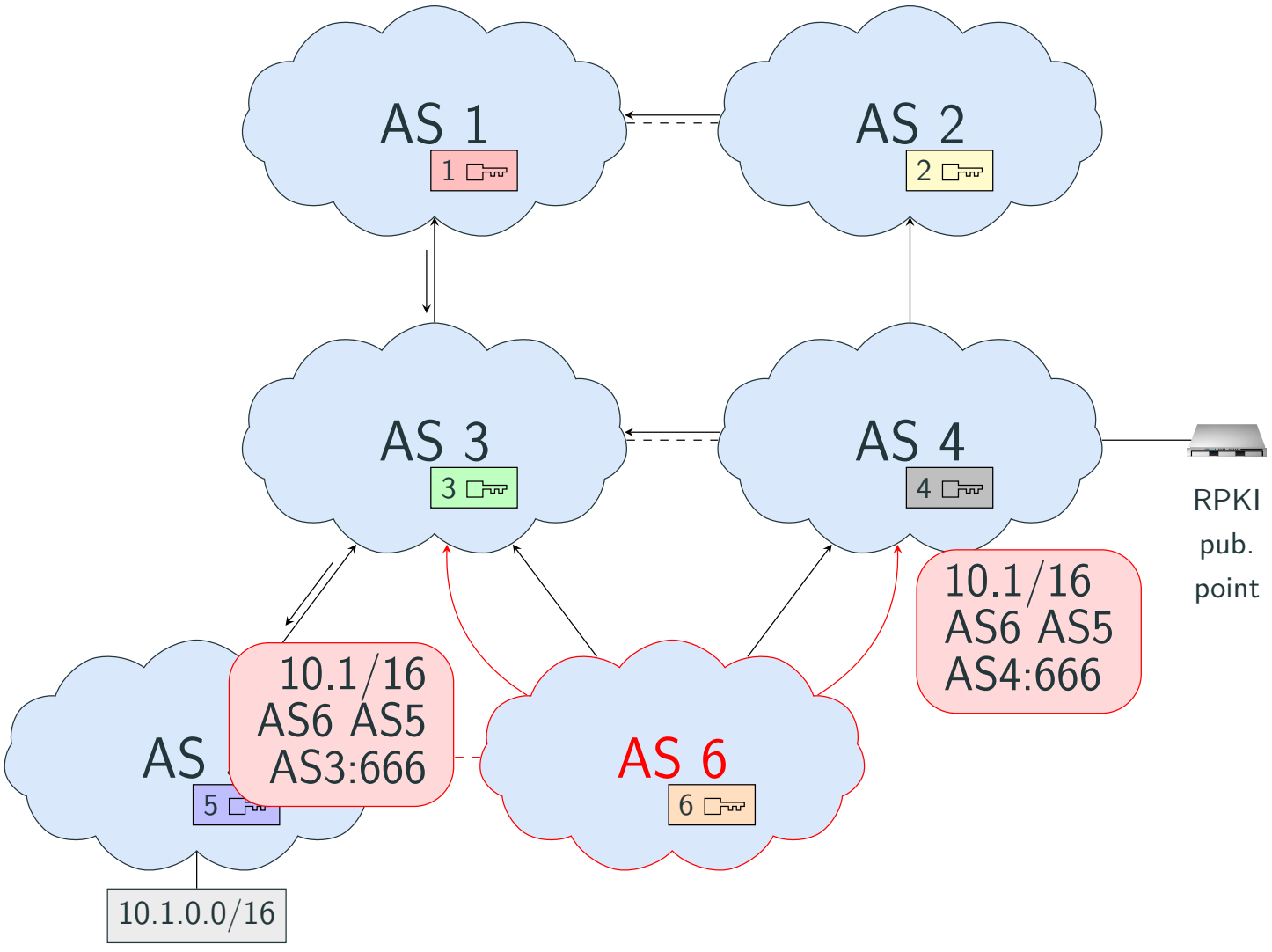


Figure 8: Type-N blackjack

BGP Blackjacks - Type-N

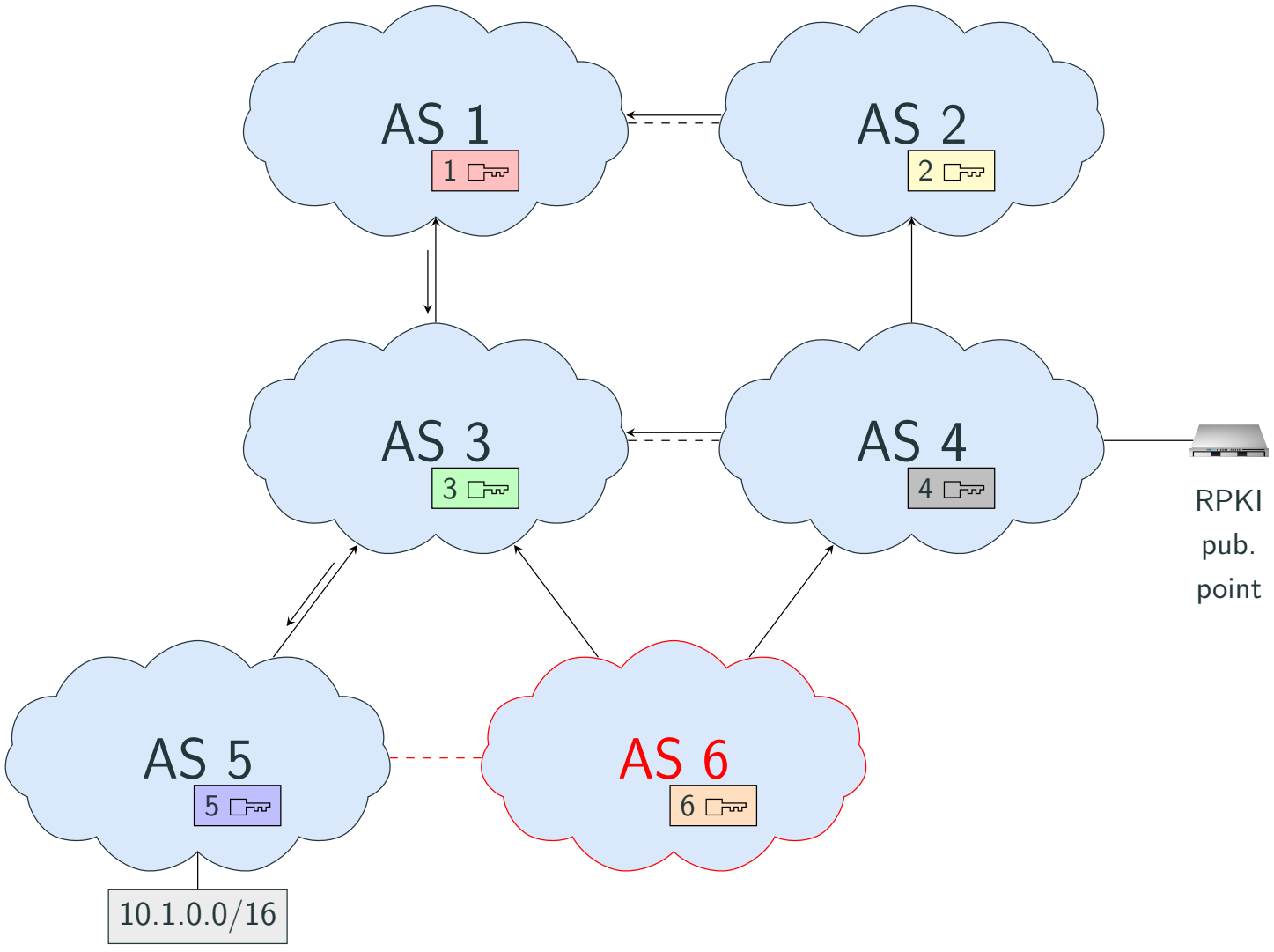


Figure 8: Type-N blackjack

BGP Blackjacks - On Path

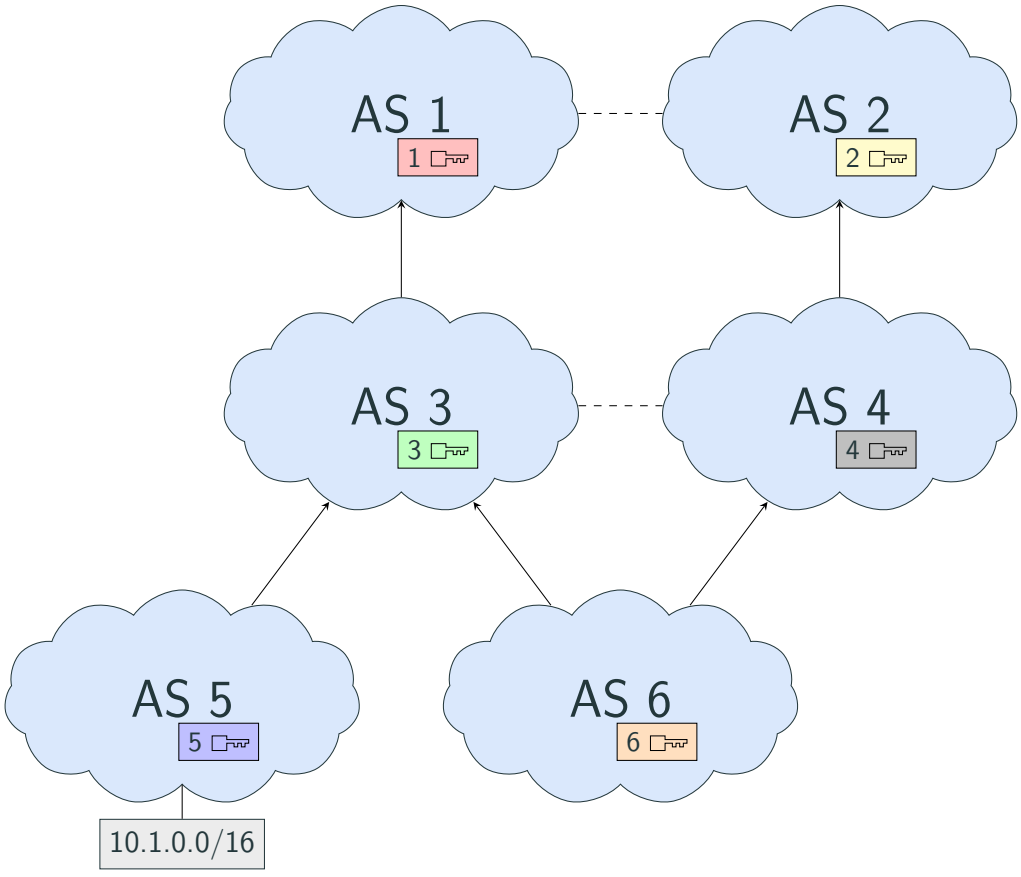


Figure 9: On Path blackjack

BGP Blackjacks - On Path

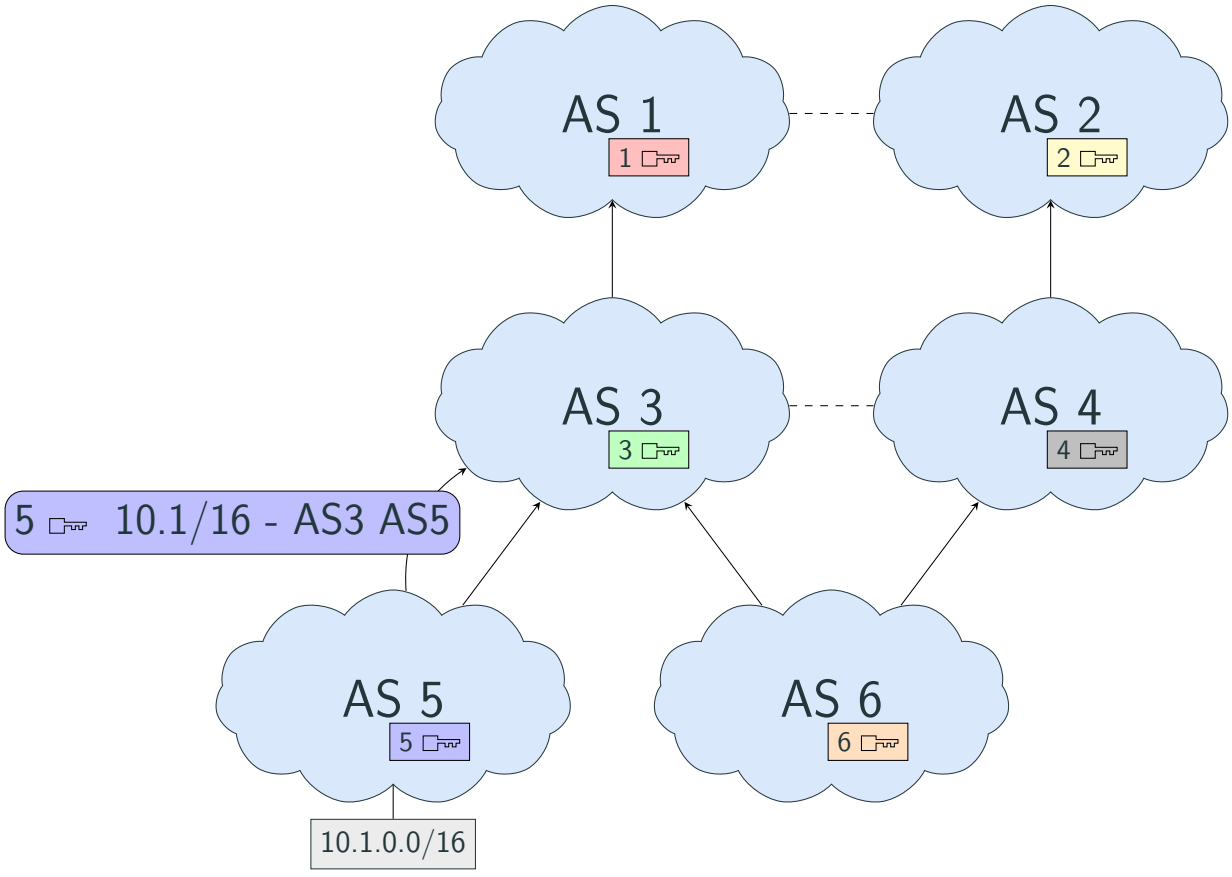


Figure 9: On Path blackjack

BGP Blackjacks - On Path

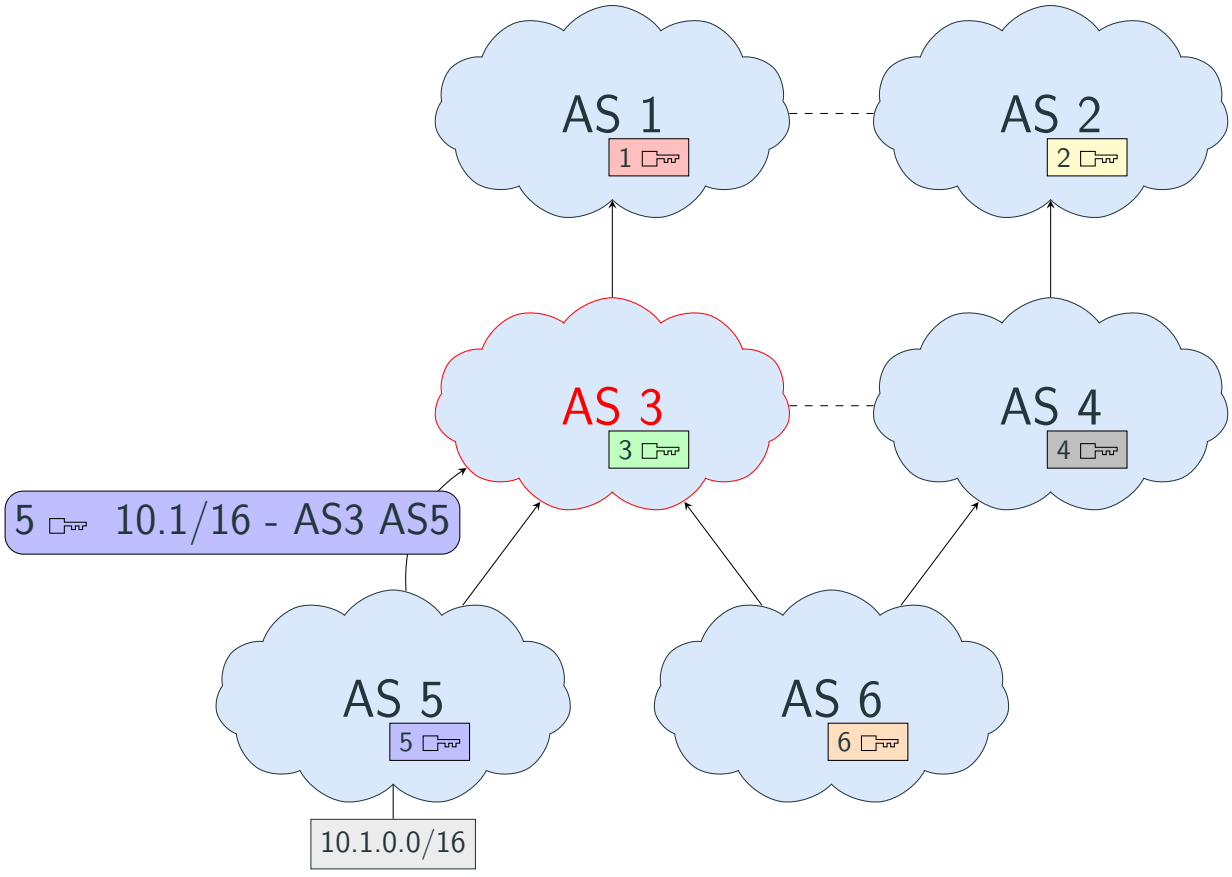


Figure 9: On Path blackjack

BGP Blackjacks - On Path

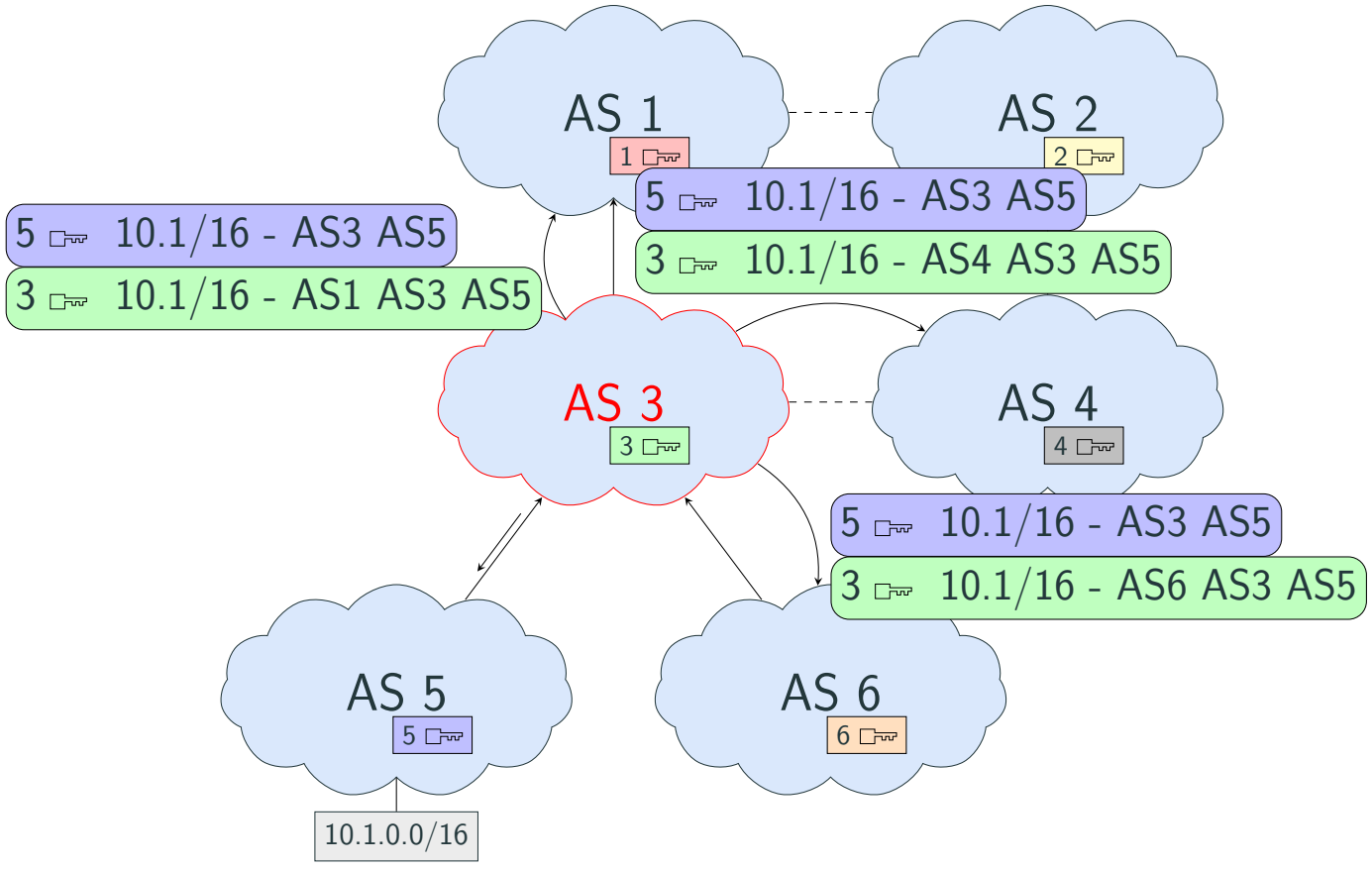


Figure 9: On Path blackjack

BGP Blackjacks - On Path

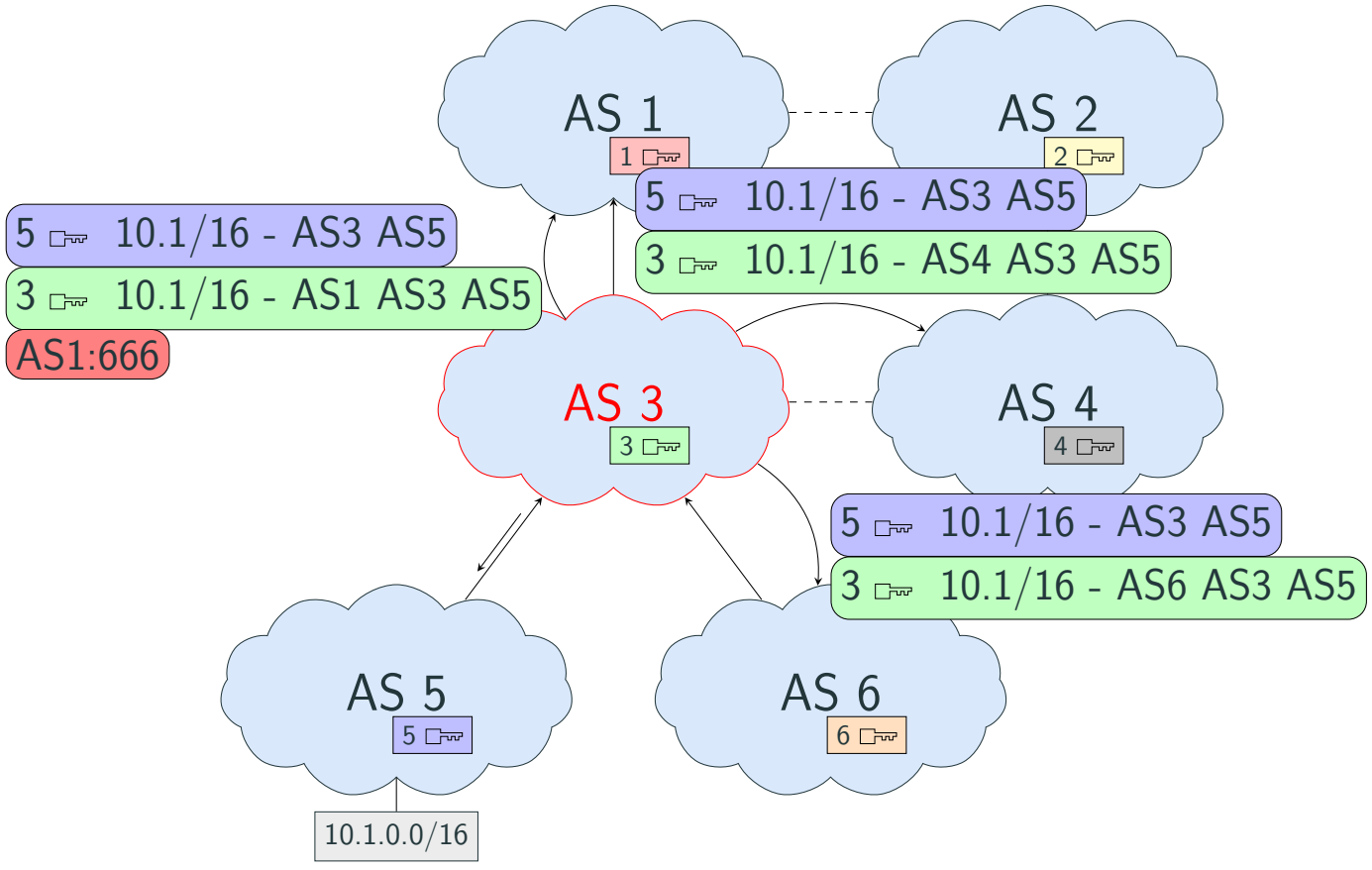


Figure 9: On Path blackjack

BGP Blackjacks - On Path

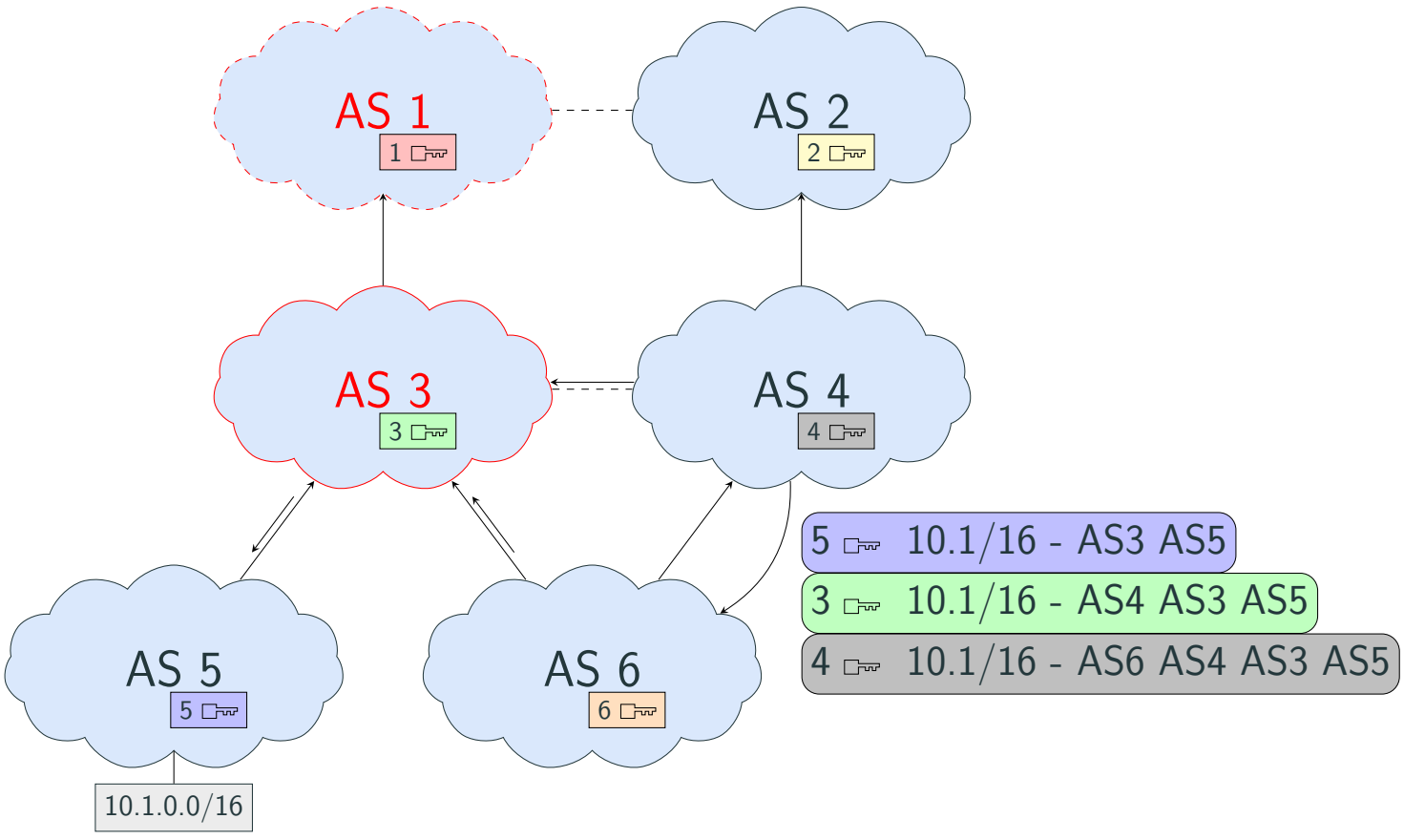


Figure 9: On Path blackjack

BGP Blackjacks - On Path

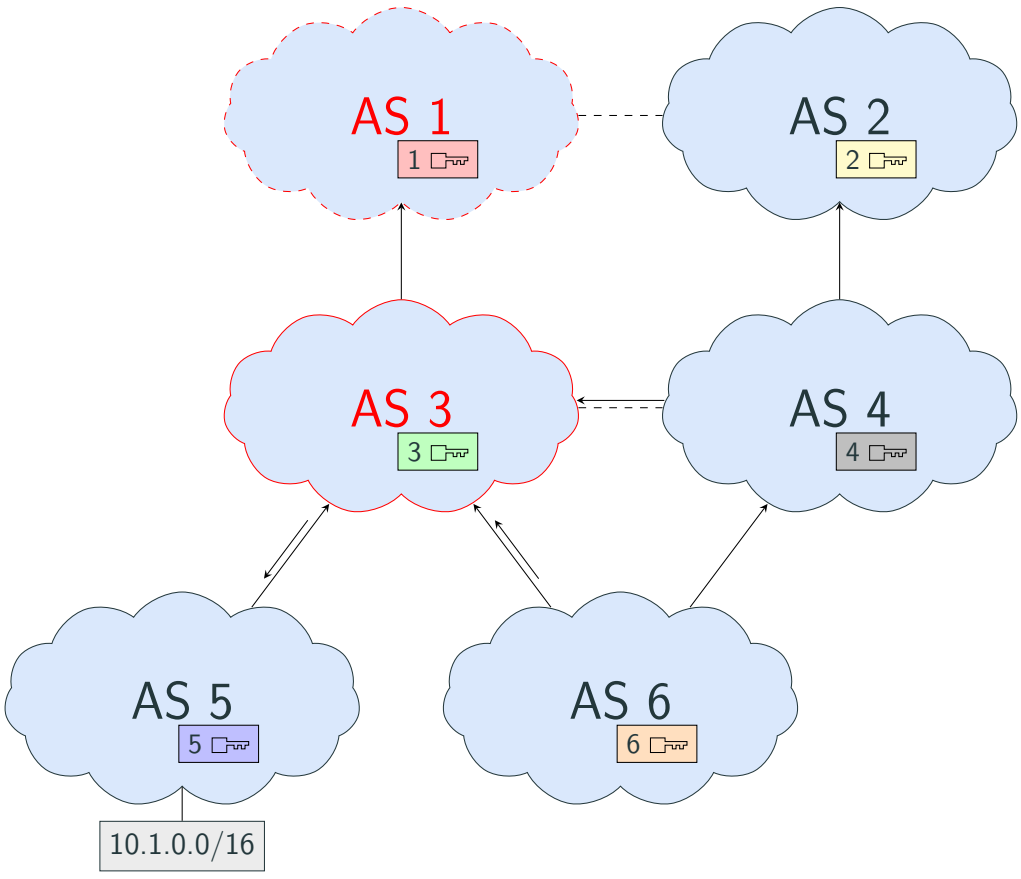


Figure 9: On Path blackjack

Attack Taxonomy

Security Deployment	Type-0	Type-N	NOP	OP	OP-GRV
BGPsec (full)	■	■	■	□	□
BGPsec (partial)	◪	◪	◪	□	□
RPKI (full)	■	□	□	□	□
RPKI (partial)	◪	□	□	□	□
No security	□	□	□	□	□

Table 1: Security deployments against exact prefix blackjacks

Attack Taxonomy

Security Deployment	Type-0	Type-N	NOP	OP	OP-GRV
BGPsec (full)	■	■	■	□	□
BGPsec (partial)	◪	◪	◪	□	□
RPKI (full)	■	□	□	□	□
RPKI (partial)	◪	□	□	□	□
No security	□	□	□	□	□

Table 1: Security deployments against exact prefix blackjacks

BGPsec: not yet deployed.

Attack Taxonomy

Security Deployment	Type-0	Type-N	NOP	OP	OP-GRV
BGPsec (full)	■	■	■	□	□
BGPsec (partial)	◪	◪	◪	□	□
RPKI (full)	■	□	□	□	□
RPKI (partial)	◪	□	□	□	□
No security	□	□	□	□	□

Table 1: Security deployments against exact prefix blackjacks

BGPsec: not yet deployed.

RPKI: 16.44% of prefixes.

Attack Taxonomy

Security Deployment	Type-0	Type-N	NOP	OP	OP-GRV
BGPsec (full)	■	■	■	□	□
BGPsec (partial)	◪	◪	◪	□	□
RPKI (full)	■	□	□	□	□
RPKI (partial)	◪	□	□	□	□
No security	□	□	□	□	□

Table 1: Security deployments against exact prefix blackjacks

BGPsec: not yet deployed.

RPKI: 16.44% of prefixes.

ROV: 84 ASes ($0.005 < \textit{certainty} < 1$)[6]

[6] Reuter et al., "Towards a rigorous methodology for measuring adoption of RPKI route validation and filtering".

Attack Taxonomy

Security Deployment	Type-0	Type-N	NOP	OP	OP-GRV
BGPsec (full)	■	■	■	□	□
BGPsec (partial)	◪	◪	◪	□	□
RPKI (full)	■	□	□	□	□
RPKI (partial)	◪	□	□	□	□
No security	□	□	□	□	□

Table 1: Security deployments against exact prefix blackjacks

BGPsec: not yet deployed.

RPKI: 16.44% of prefixes.

ROV: 84 ASes ($0.005 < \textit{certainty} < 1$)[6] - 0.13% of ASes[7].

[6] Reuter et al., "Towards a rigorous methodology for measuring adoption of RPKI route validation and filtering".

[7] Bates, Smith, and Huston, **CIDR REPORT for 22 Sep 19**.

Attack Taxonomy

Security Deployment	Type-0	Type-N	NOP	OP	OP-GRV
BGPsec (full)	■	■	■	□	□
BGPsec (partial)	◪	◪	◪	□	□
RPKI (full)	■	□	□	□	□
RPKI (partial)	◪	□	□	□	□
No security	□	□	□	□	□

Table 1: Security deployments against exact prefix blackjacks

BGPsec: not yet deployed.

RPKI: 16.44% of prefixes.

ROV: 84 ASes ($0.005 < \textit{certainty} < 1$)[6] - 0.13% of ASes[7].

[6] Reuter et al., "Towards a rigorous methodology for measuring adoption of RPKI route validation and filtering".

[7] Bates, Smith, and Huston, **CIDR REPORT for 22 Sep 19**.

Suggested Best Practices

Authorized origin: RPKI.

Valid path: BGPsec.

It is not enough!

Suggested Best Practices

Authorized origin: RPKI.
Valid path: BGPsec.

Direct connection: The AS sending the blackhole advertisement is directly connected to the local AS: only one AS in the AS path.

Suggested Best Practices

Direct connection: The AS sending the blackhole advertisement is directly connected to the local AS: only one AS in the AS path.

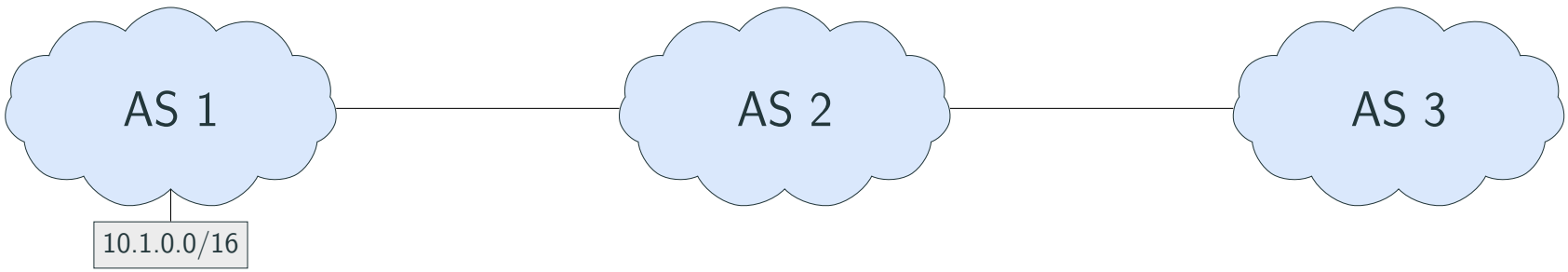


Figure 10: Suggested Best Practices

Suggested Best Practices

Direct connection: The AS sending the blackhole advertisement is directly connected to the local AS: only one AS in the AS path.

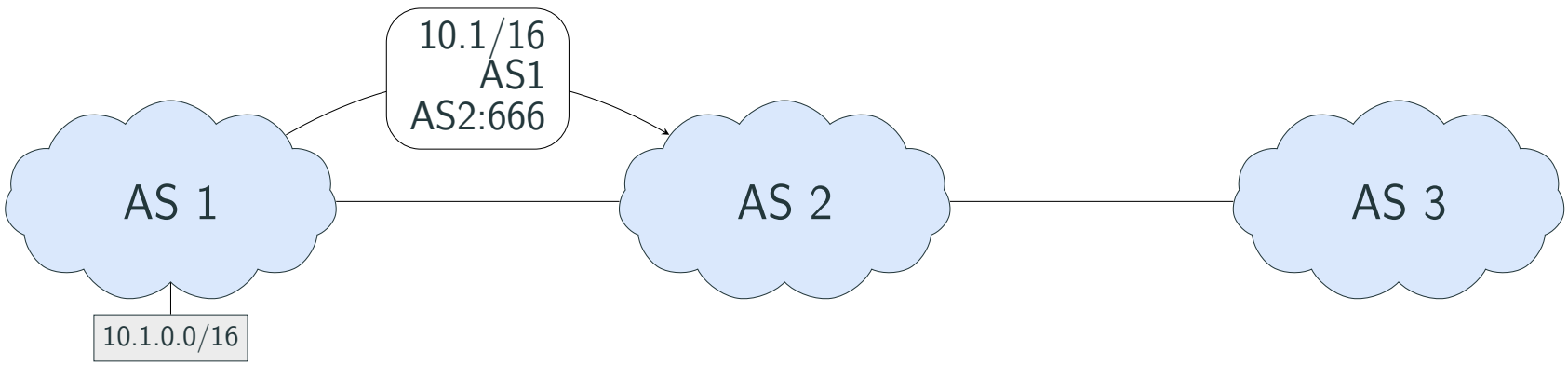


Figure 10: Suggested Best Practices

Suggested Best Practices

Direct connection: The AS sending the blackhole advertisement is directly connected to the local AS: only one AS in the AS path.

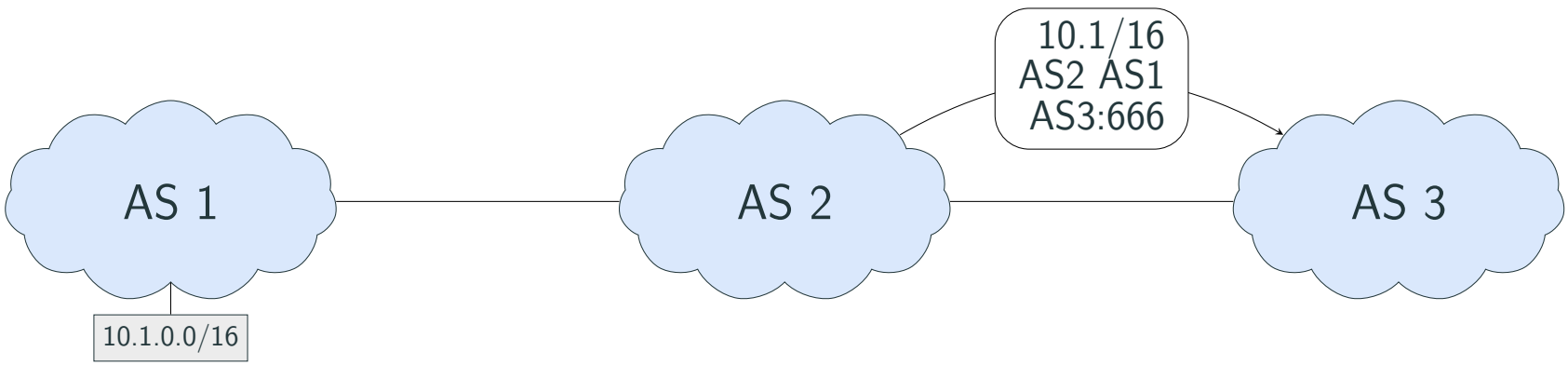


Figure 10: Suggested Best Practices

Suggested Best Practices

Direct connection: The AS sending the blackhole advertisement is directly connected to the local AS: only one AS in the AS path.

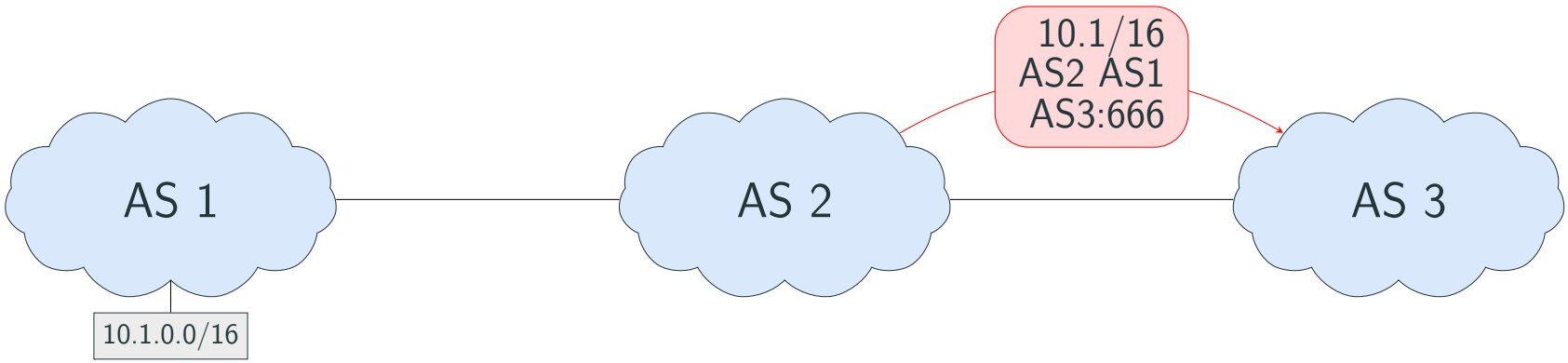


Figure 10: Suggested Best Practices

Suggested Best Practices

Direct connection: The AS sending the blackhole advertisement is directly connected to the local AS: only one AS in the AS path. Limits possible attacks to Type-0 and NOP blackjacks.

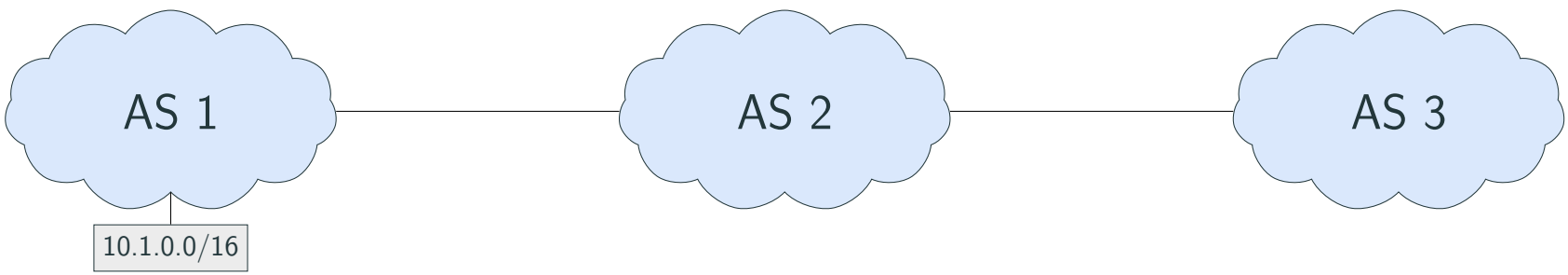


Figure 10: Suggested Best Practices

Suggested Best Practices

Direct connection: The AS sending the blackhole advertisement is directly connected to the local AS: only one AS in the AS path. Limits possible attacks to Type-0 and NOP blackjacks.

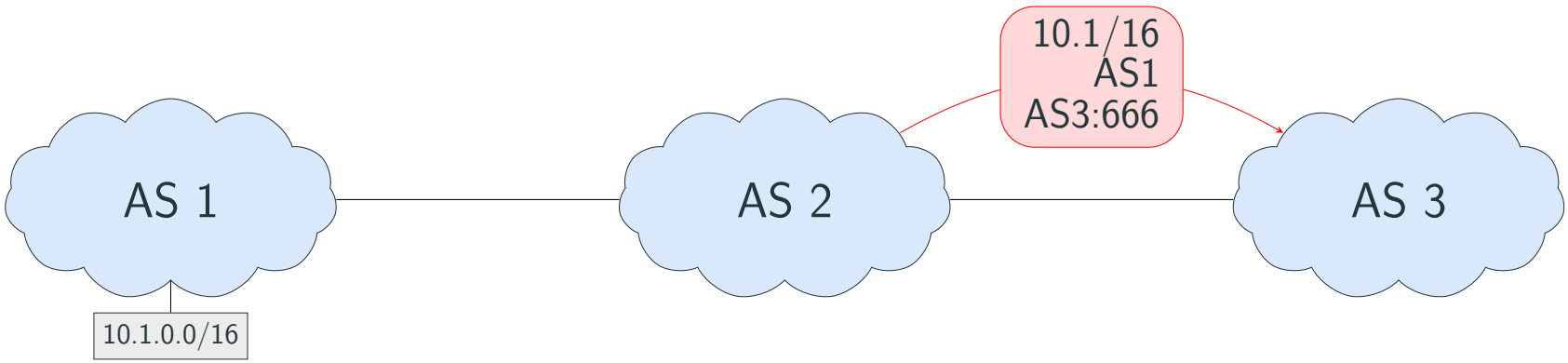


Figure 10: Suggested Best Practices

Suggested Best Practices

Legitimate peer: The peer sending the blackhole advertisement is legitimate if the leftmost AS in the AS path is the ASN specified in the BGP OPEN message that created the session.

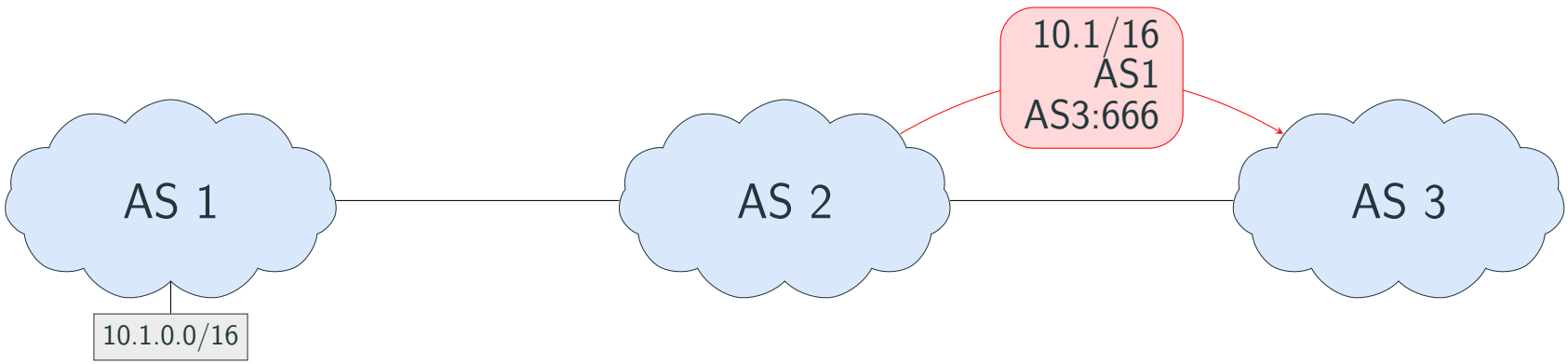


Figure 10: Suggested Best Practices

A BGPsec solution - Associate communities to ASes.

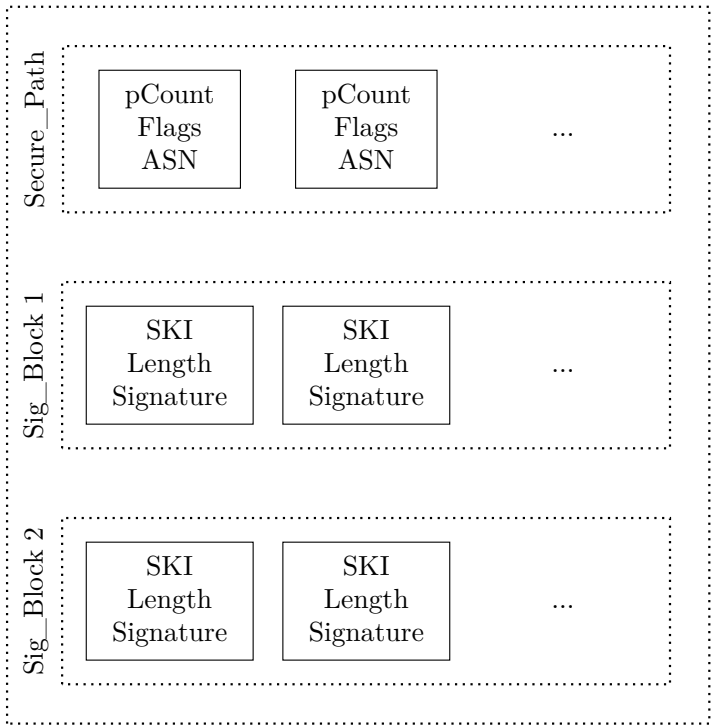


Figure 11: BGPsec_PATH attribute

A BGPsec solution - Associate communities to ASes.

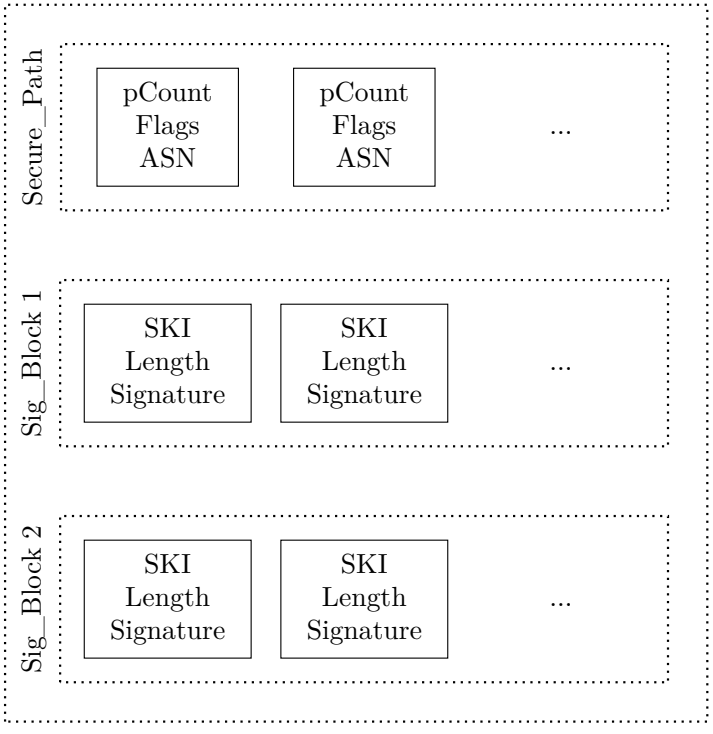


Figure 11: BGPsec_PATH attribute

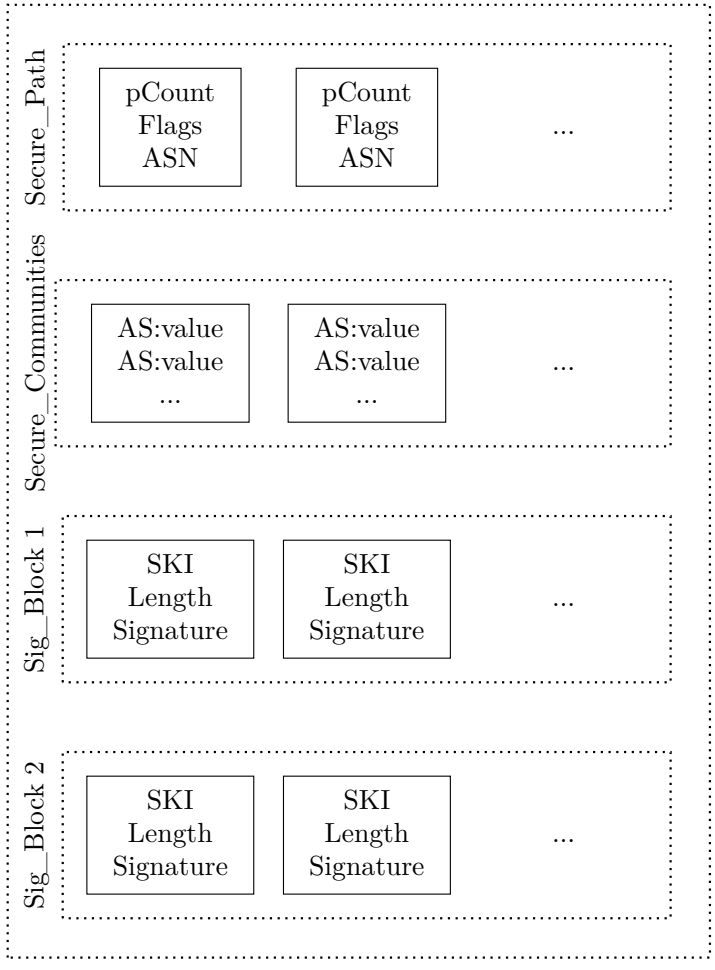


Figure 12: Modified attribute

A BGPsec solution - Associate communities to ASes.

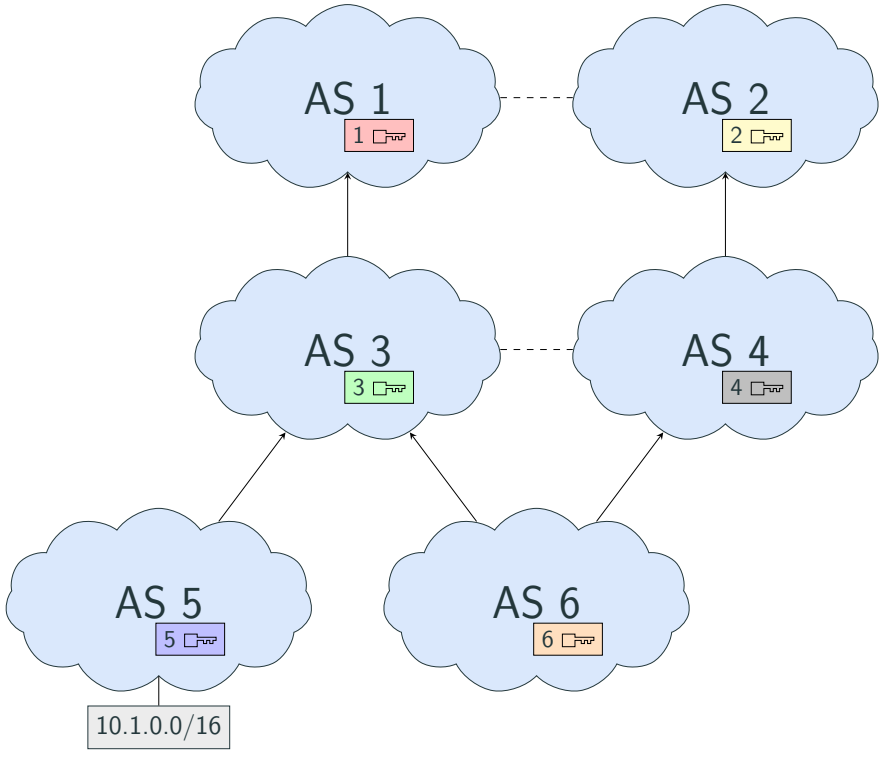


Figure 13: BGPsec message propagation (modified)

A BGPsec solution - Associate communities to ASes.

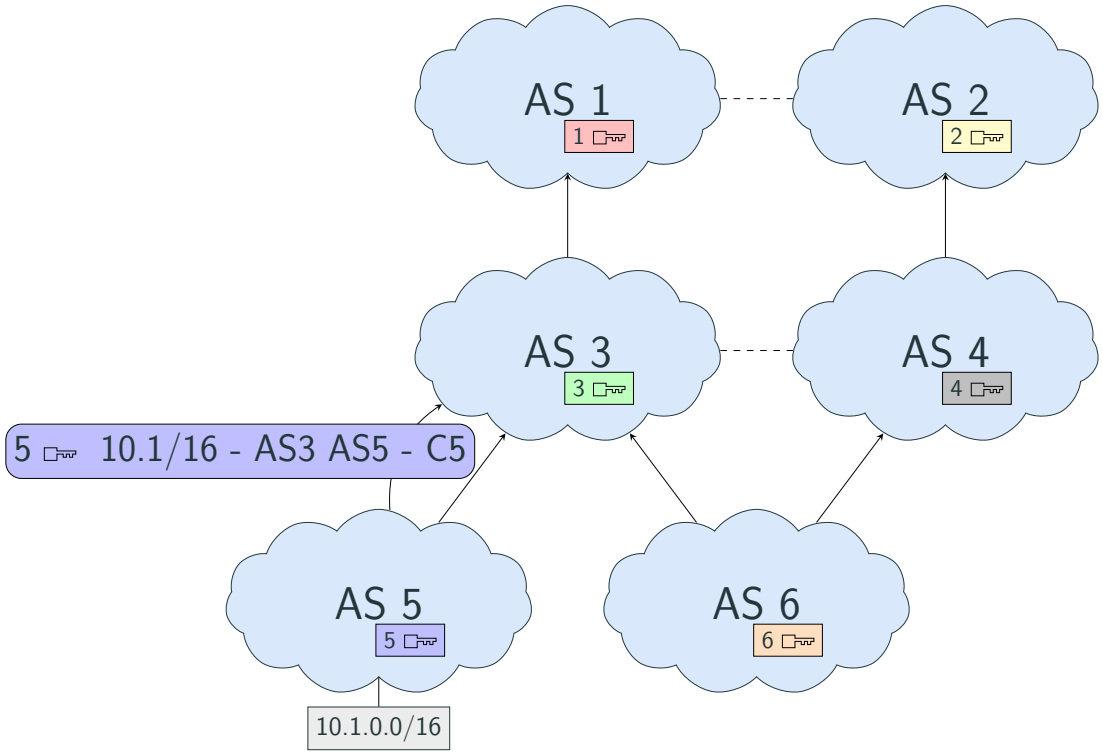


Figure 13: BGPsec message propagation (modified)

A BGPsec solution - Associate communities to ASes.

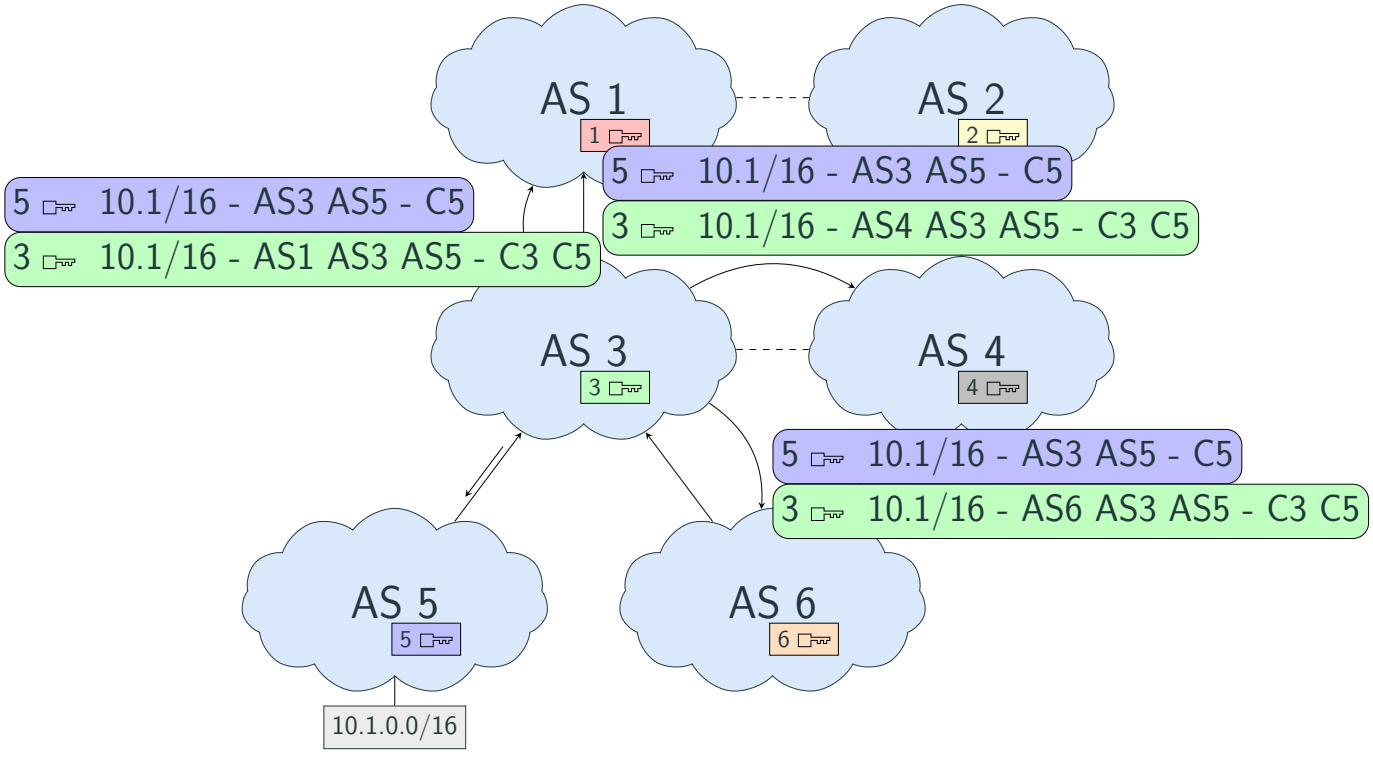


Figure 13: BGPsec message propagation (modified)

A BGPsec solution - Associate communities to ASes.

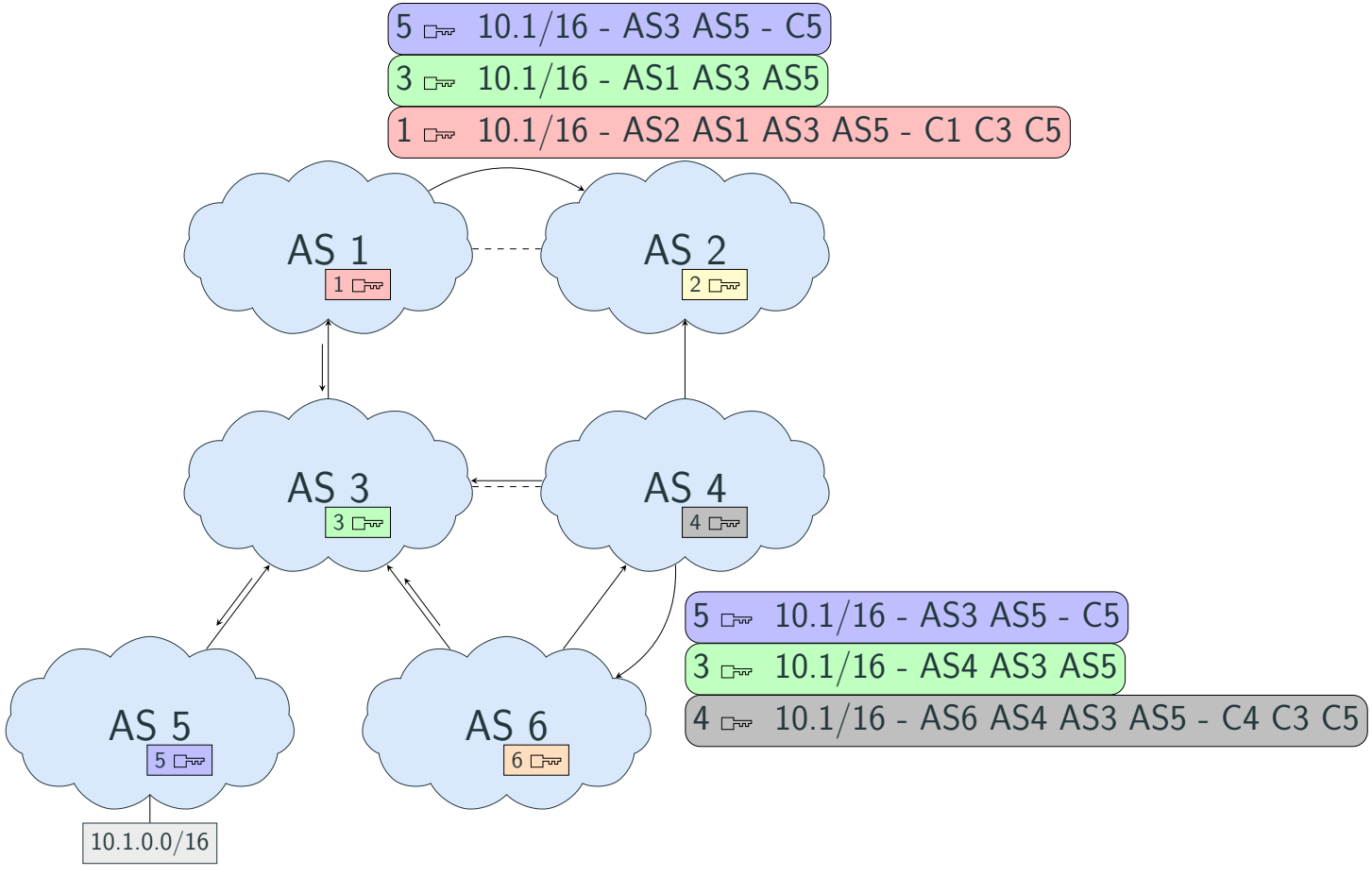


Figure 13: BGPsec message propagation (modified)

A BGPsec solution - Associate communities to ASes.

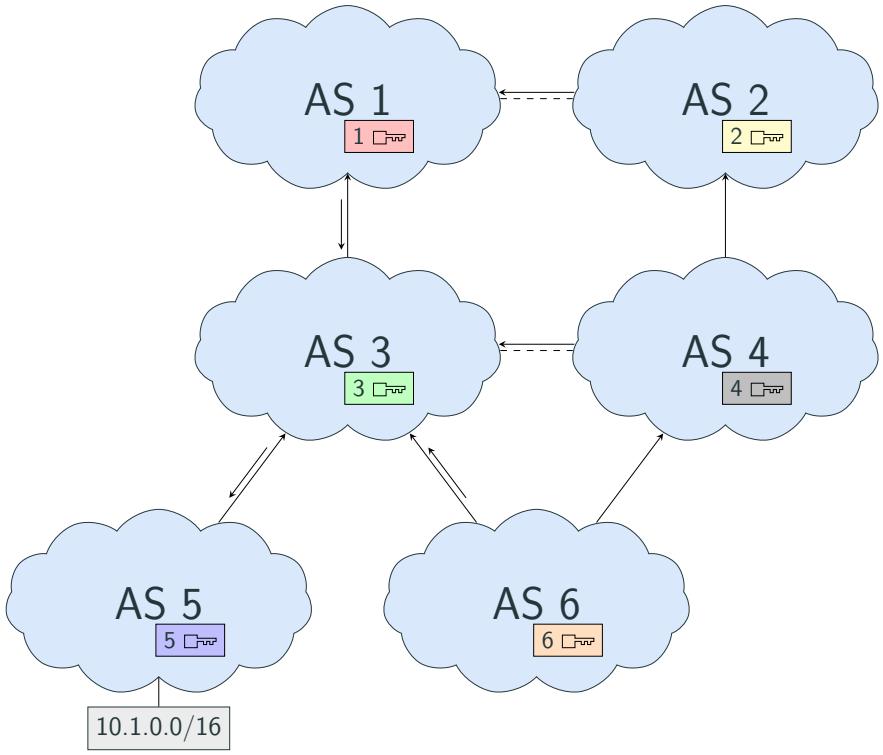


Figure 13: BGPsec message propagation (modified)

Perspectives

Test remaining[8] attacks in a real world setting.

[8] Streibelt et al., "BGP Communities: Even more Worms in the Routing Can".

Perspectives

Test remaining[8] attacks in a real world setting.

Investigate ASes proposing blackholing services.

[8] Streibelt et al., "BGP Communities: Even more Worms in the Routing Can".

Perspectives

Test remaining[8] attacks in a real world setting.

Investigate ASes proposing blackholing services.

Extend the attack model.

[8] Streibelt et al., "BGP Communities: Even more Worms in the Routing Can".

Takeway message

New BGP attacks: BGP blackjacks.

Takeway message

New BGP attacks: BGP blackjacks.

Blackjack attack taxonomy.

Takeway message

New BGP attacks: BGP blackjacks.

Blackjack attack taxonomy.

Existing routing security mechanisms do not provide complete protection.

Takeway message

New BGP attacks: BGP blackjacks.

Blackjack attack taxonomy.

Existing routing security mechanisms do not provide complete protection.

Additional mechanisms to properly defend against or mitigate those attacks.

Thank you!

[1] Tony Bates, Philip Smith, and Geoff Huston. **CIDR REPORT for 22 Sep 19**. 2019. URL: https://www.cidr-report.org/as2.0/ (visited on 09/22/2019).

[2] Cisco. **Remotely Triggered Black Hole Filtering - Destination Based and Source Based**. 2005. URL: https://www.cisco.com/c/dam/en/us/products/collateral/security/ios-network-foundation-protection-nfp/prod%5C_white%5C_paper0900aecd80313fac.pdf (visited on 09/22/2019).

[3] M. Lepinski and S. Kent. **An Infrastructure to Support Secure Internet Routing**. RFC 6480. RFC Editor, Feb. 2012. URL: http://www.rfc-editor.org/rfc/rfc6480.txt.

[4] M. Lepinski and K. Sriram. **BGPsec Protocol Specification**. RFC 8205. RFC Editor, Sept. 2017.

[5] Y. Rekhter, T. Li, and S. Hares. **A Border Gateway Protocol 4 (BGP-4)**. RFC 4271. http://www.rfc-editor.org/rfc/rfc4271.txt. RFC Editor, Jan. 2006. URL: http://www.rfc-editor.org/rfc/rfc4271.txt.

[6] Andreas Reuter et al. "Towards a rigorous methodology for measuring adoption of RPKI route validation and filtering". In: **ACM SIGCOMM Computer Communication Review** 48.1 (2018), pp. 19–27.

[7] Andrei Robachevsky. **14,000 Incidents: A 2017 Routing Security Year in Review**. 2018. URL: https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/ (visited on 09/22/2019).

[8] Pavlos Sermpezis et al. "ARTEMIS: Neutralizing BGP hijacking within a minute". In: **IEEE/ACM Transactions on Networking (TON)** 26.6 (2018), pp. 2471–2486.

[9] Florian Streibelt et al. "BGP Communities: Even more Worms in the Routing Can". In: **Proceedings of the Internet Measurement Conference 2018**. ACM. 2018, pp. 279–292.

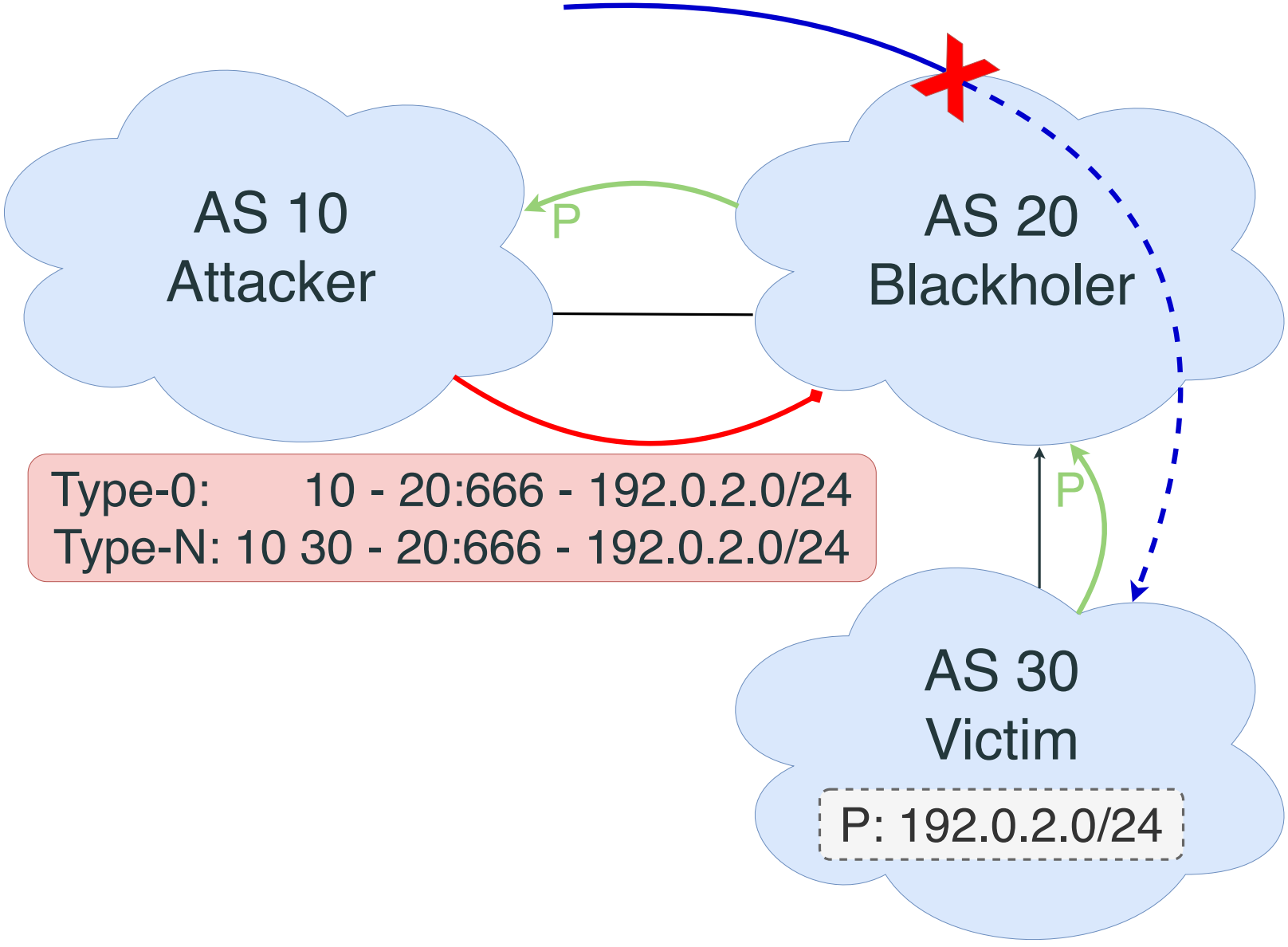


Figure 14: Type-0 and Type-N blackjacks

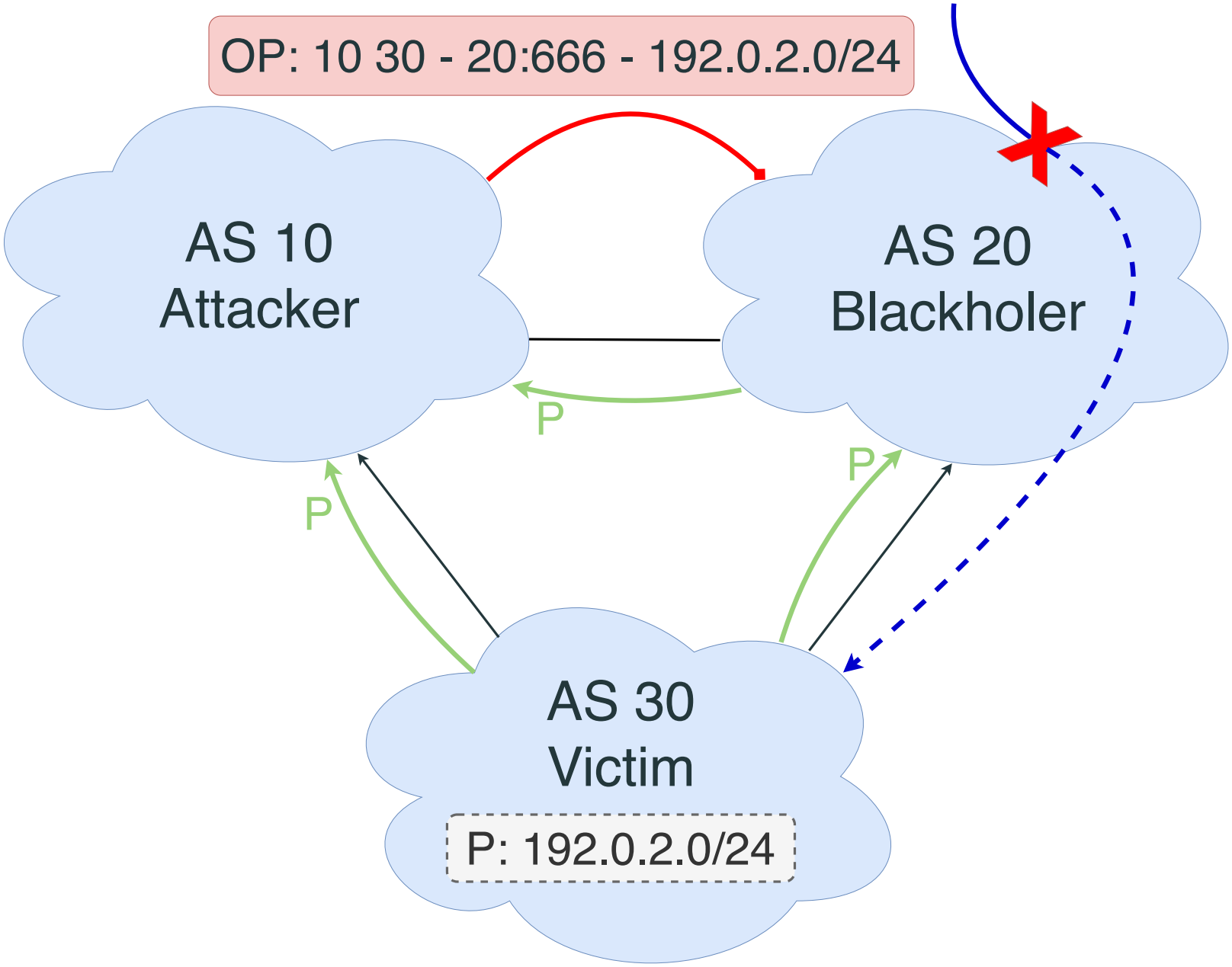
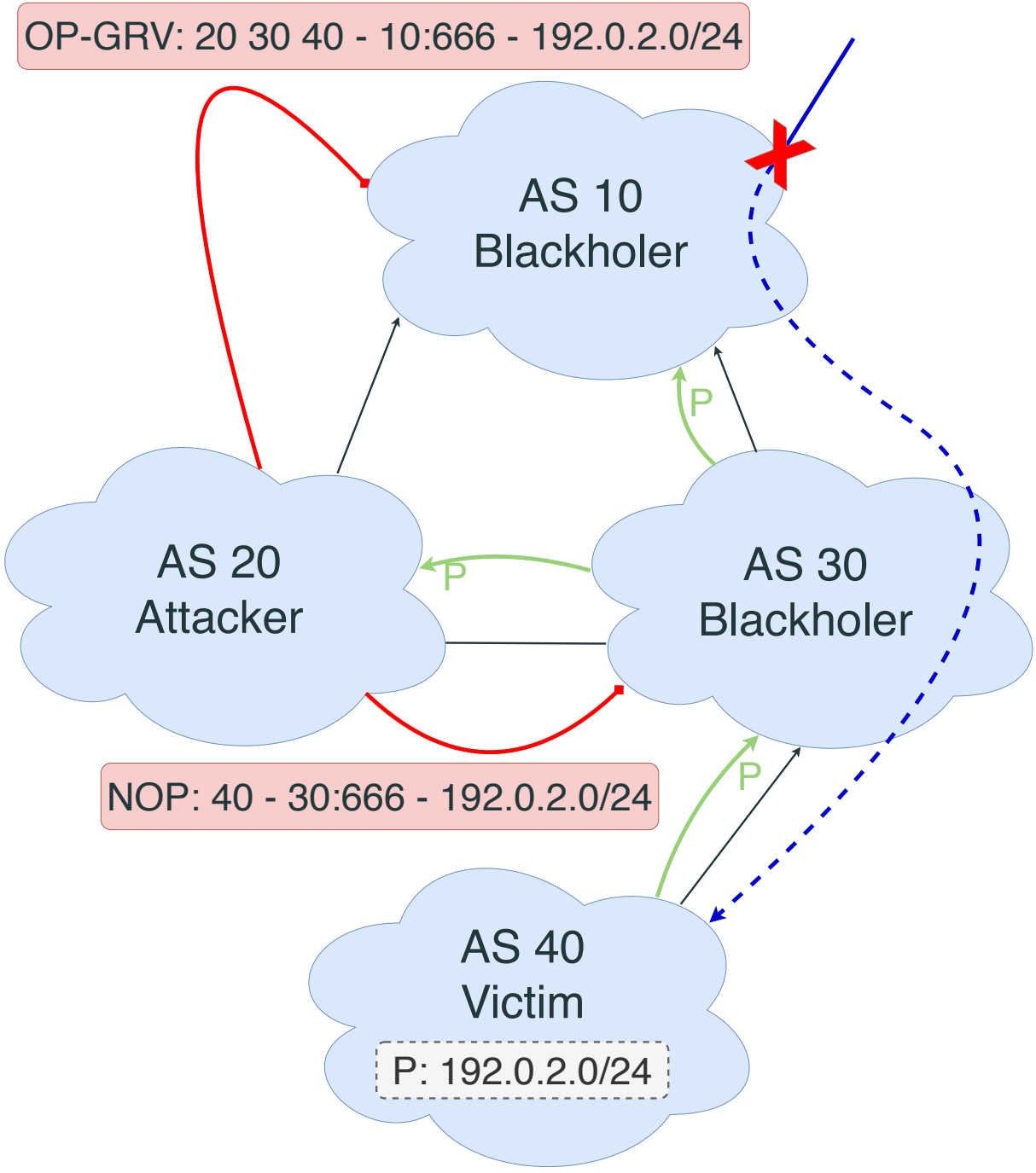


Figure 15: On Path blackjacks


OP-GRV: 20 30 40 - 10:666 - 192.0.2.0/24
AS 10
Blackholer
AS 20
Attacker
AS 30
Blackholer
AS 40
Victim
P: 192.0.2.0/24
P
P
P
NOP: 40 - 30:666 - 192.0.2.0/24

Security Deployment	Type-0	Type-N	NOP	OP	OP-GRV
BGPsec (full)	■	■	■	■	■
BGPsec (partial)	◪	◪	◪	■	■
RPKI (full)	■	■	■	■	■
RPKI (partial)	◪	◪	◪	■	■
No security	□	□	□	■	■

Table 2: Security deployments against sub-prefix blackjacks