CS5321 Network Security
Week6: Routing Security

Daisuke MASHIMA

2022/23 Sem 2

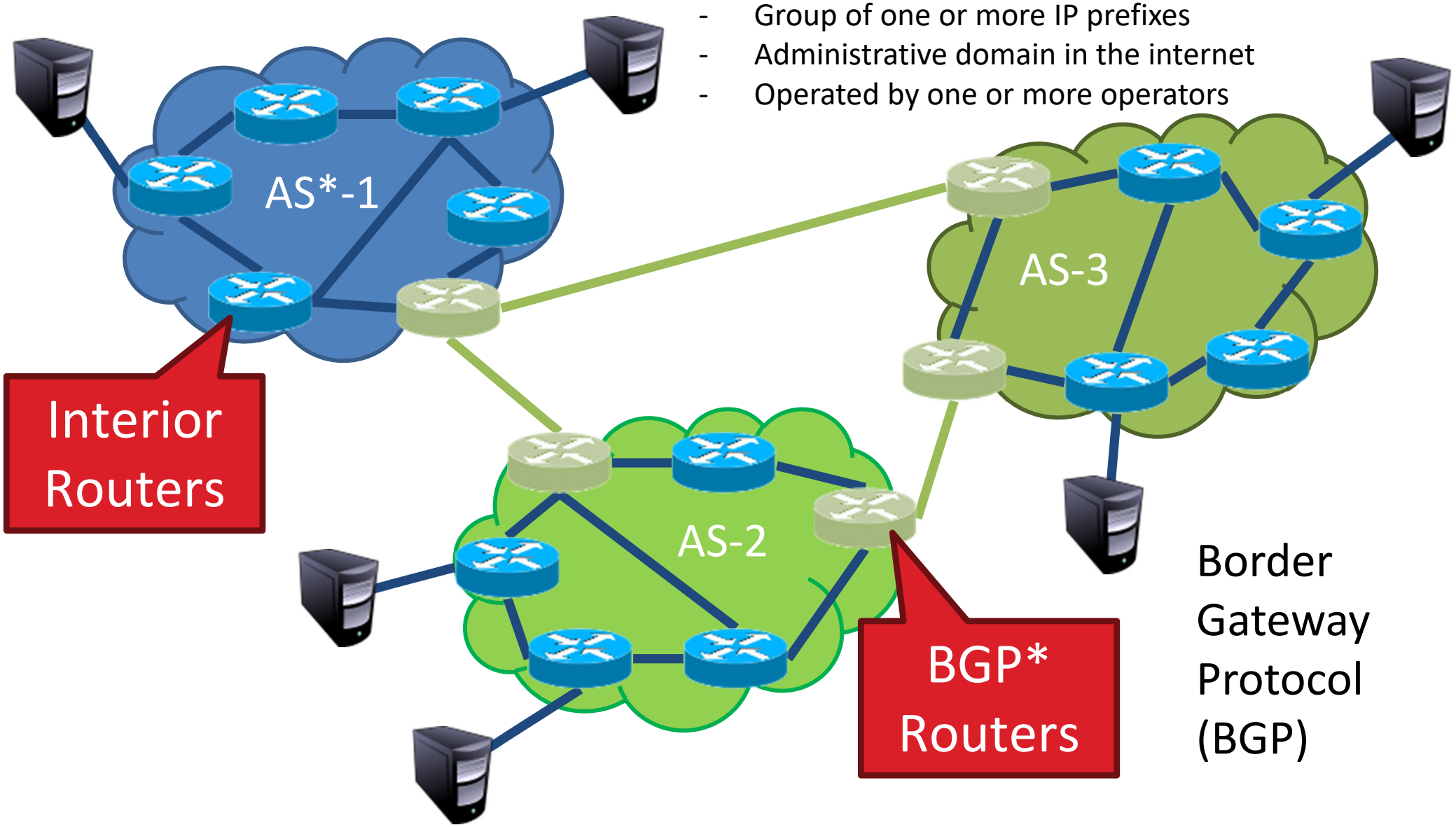
Agenda

- **Inter-domain routing: BGP**
- **Security problems of BGP: Hijacking**
- **BGPSEC/RPKI and their limitations**
- **SCION: redesign the Internet (Guest lecture by Prof Adrian Perrig from ETH Zurich)**

How a packet is delivered across the Internet

Autonomous Systems (ASes)

- Group of one or more IP prefixes
- Administrative domain in the internet
- Operated by one or more operators



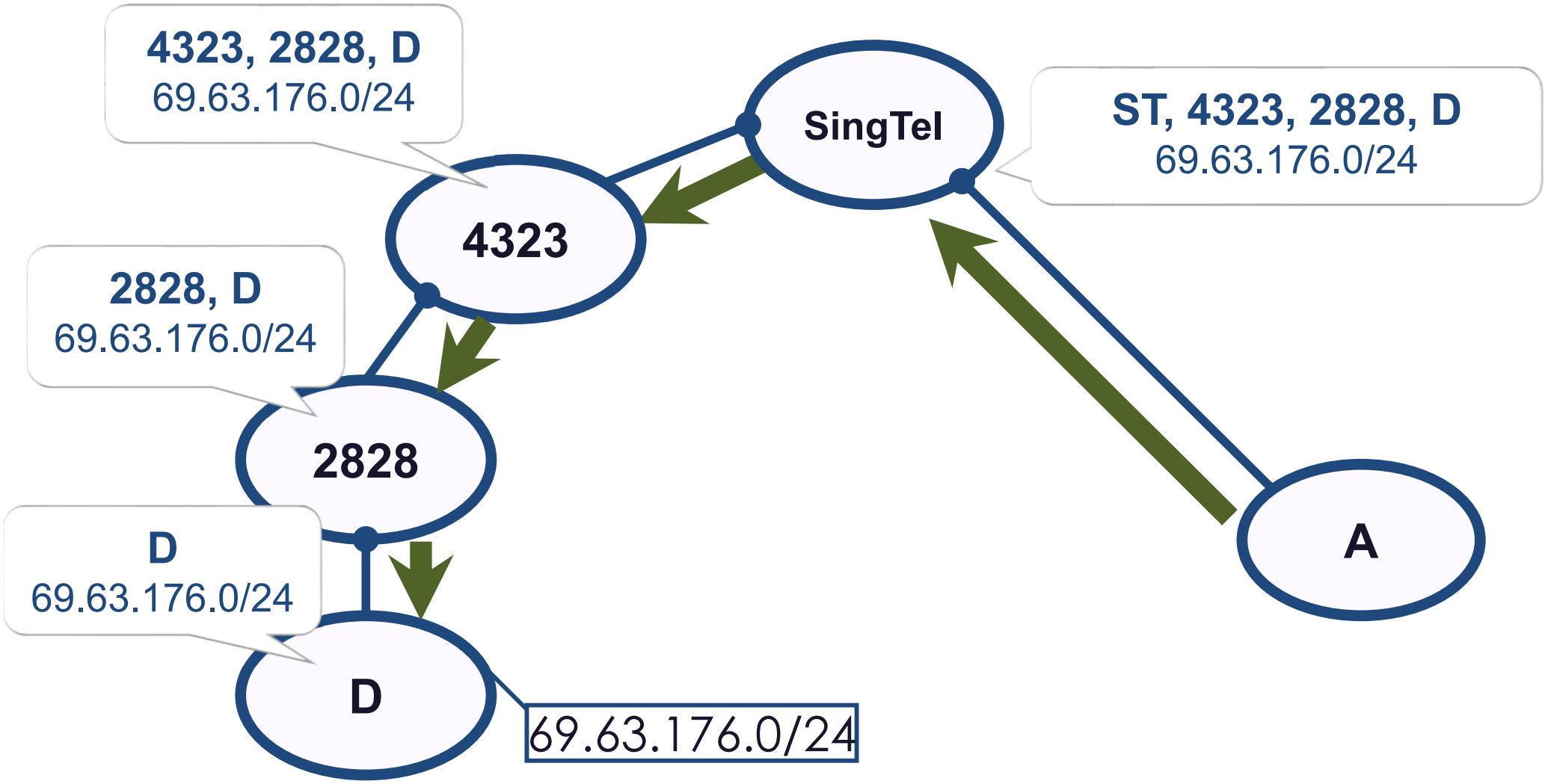
Autonomous System (AS) Numbers

- Each AS identified by an ASN number
  - 16-bit values
  - 64512 – 65535 are reserved
- Currently, there are ~ 60000 ASNs
  - SingTel: 7473
  - Starhub: 4657
  - National Univ of Singapore: 7472
  - Google 15169, 36561, …

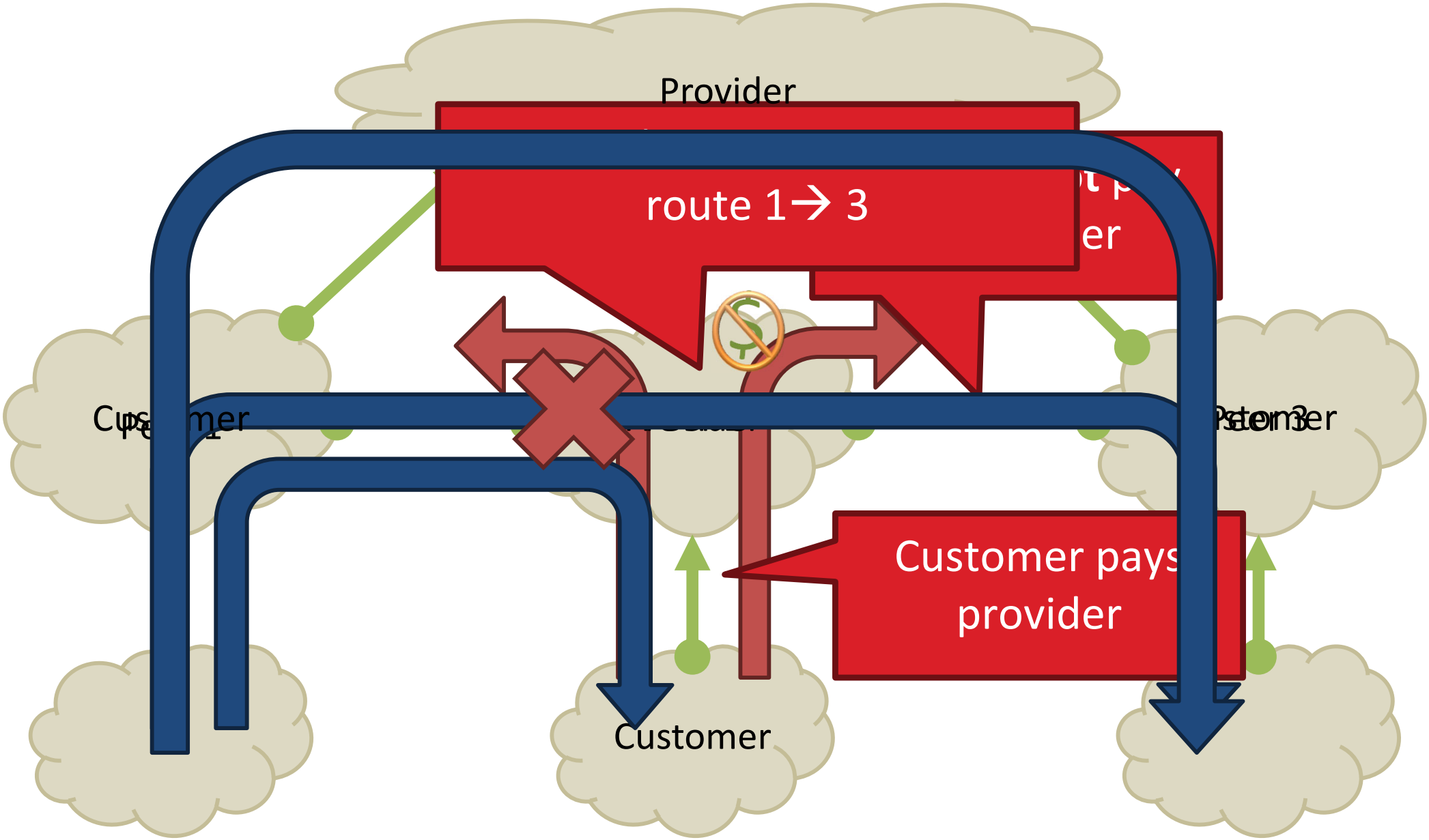
Border Gateway Protocol

- Border Gateway Protocol (BGP)
  - De facto inter-domain routing protocol of the Internet
  - Uses a **path vector** routing
  - **Policy based** routing protocol
- Relatively simple protocol, but…
  - Complex, manual configuration
  - Entire world sees routing advertisements
    - Errors can screw up traffic **globally**
  - Policies driven by **economics**
    - Not by performance (e.g. shortest paths)

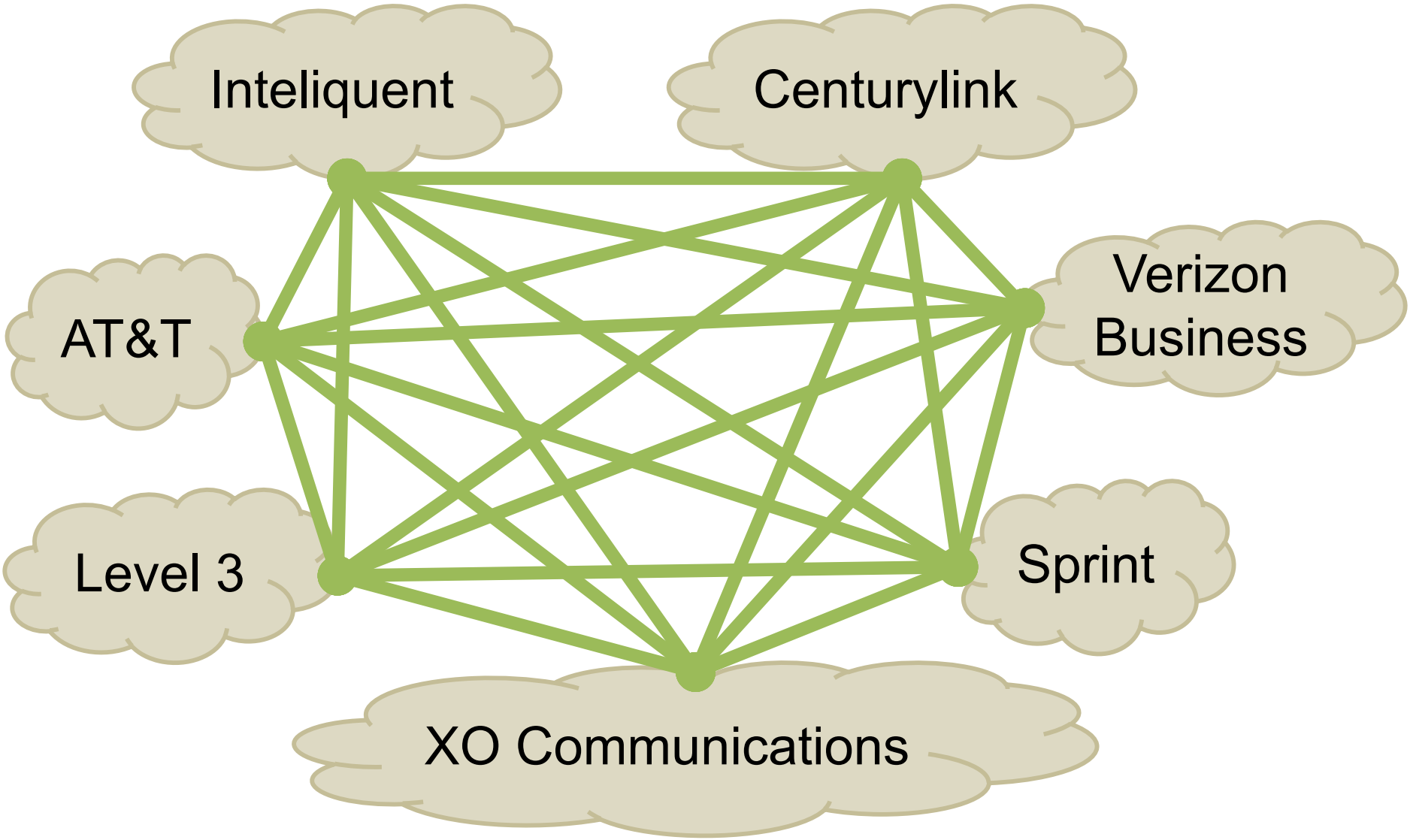
BGP



BGP's Business Relationships

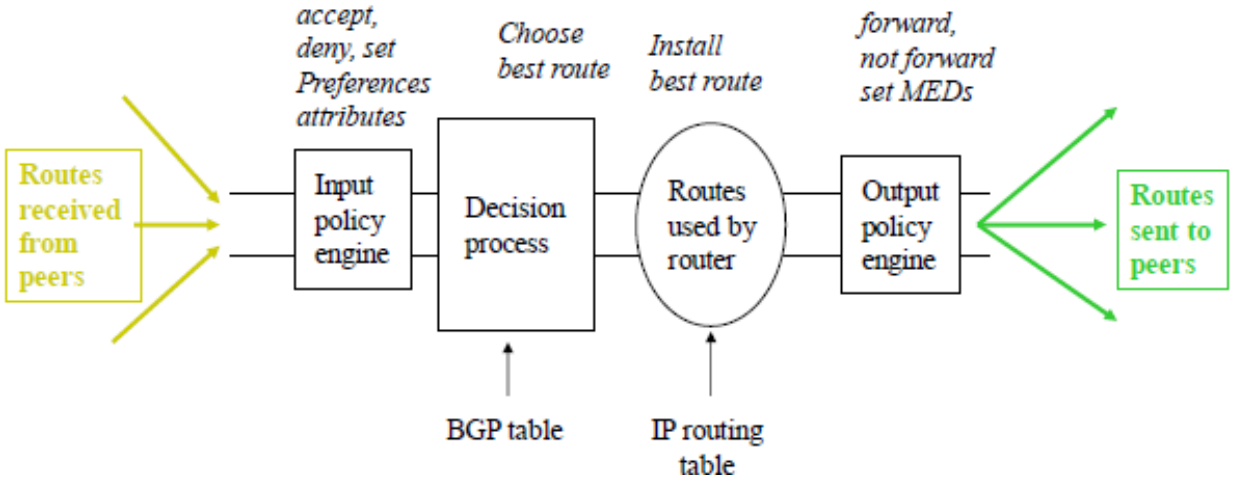


Tier-1 ISP Peering



Route Selection Summary

- AS selects one "best" route to use/advertise for each IP prefix



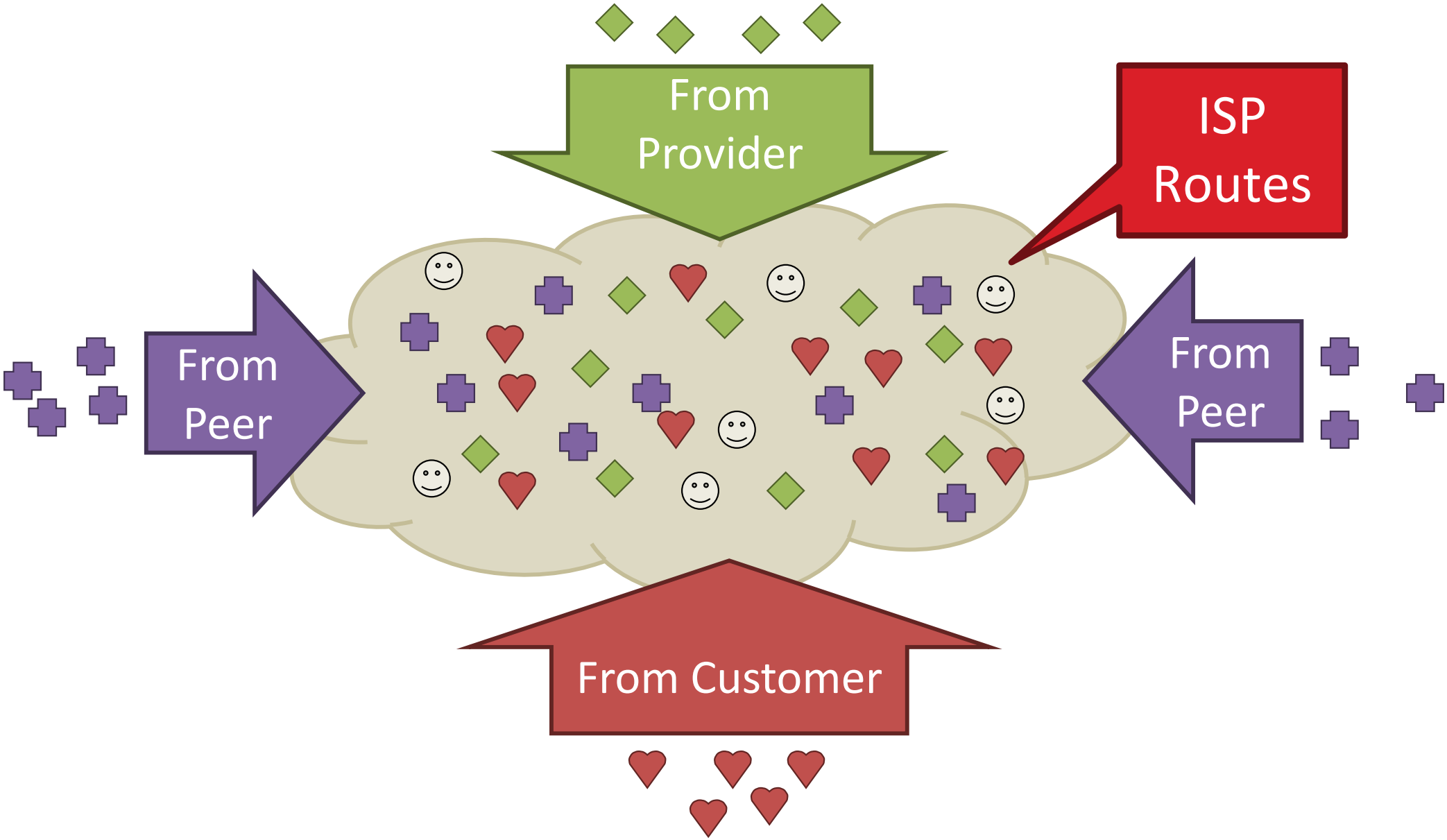
Highest Local Preference — Enforce relationships

Shortest AS Path

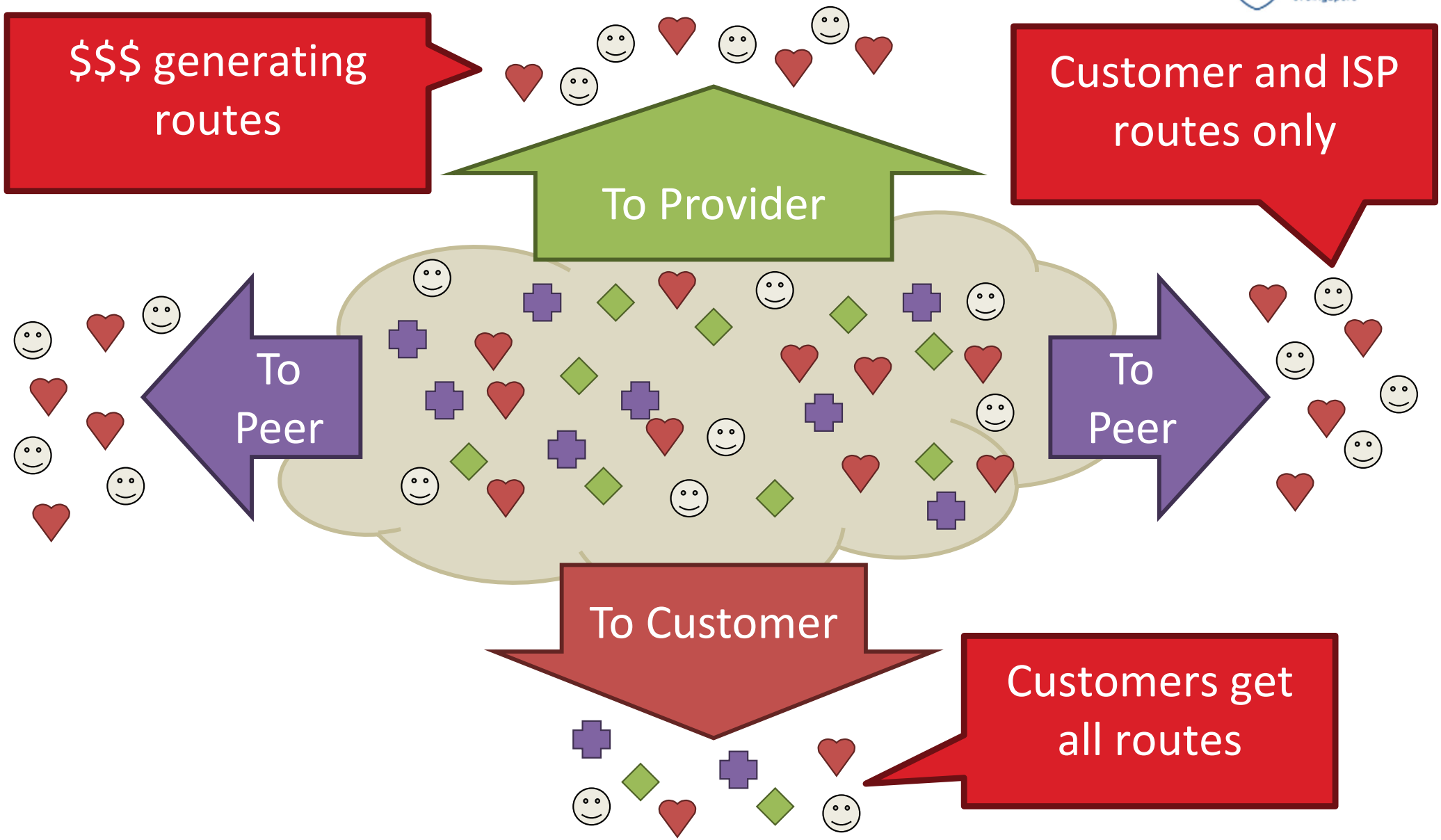
Lowest IGP (Interior Gateway Protocol) — Traffic engineering: **Cost to BGP Egress**

Lowest Router ID — When all else fails, break ties

IMPORTING ROUTES

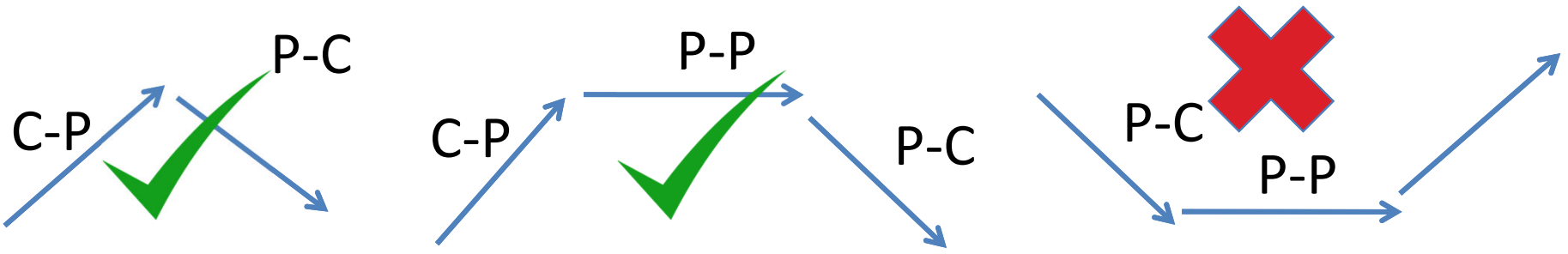


EXPORTING ROUTES



Modeling BGP

- **Gao-Rexford model**
  - AS prefers to use customer path, then peer, then provider
    - Follow the money!
  - **Valley-free** property for traversal and advertisement
    - A downhill path followed by another uphill path is NOT allowed.
    - Invalid patterns: P -> C -> Peer, P -> C -> P, Peer -> Peer, Peer -> P



Lack of security mechanisms in BGP

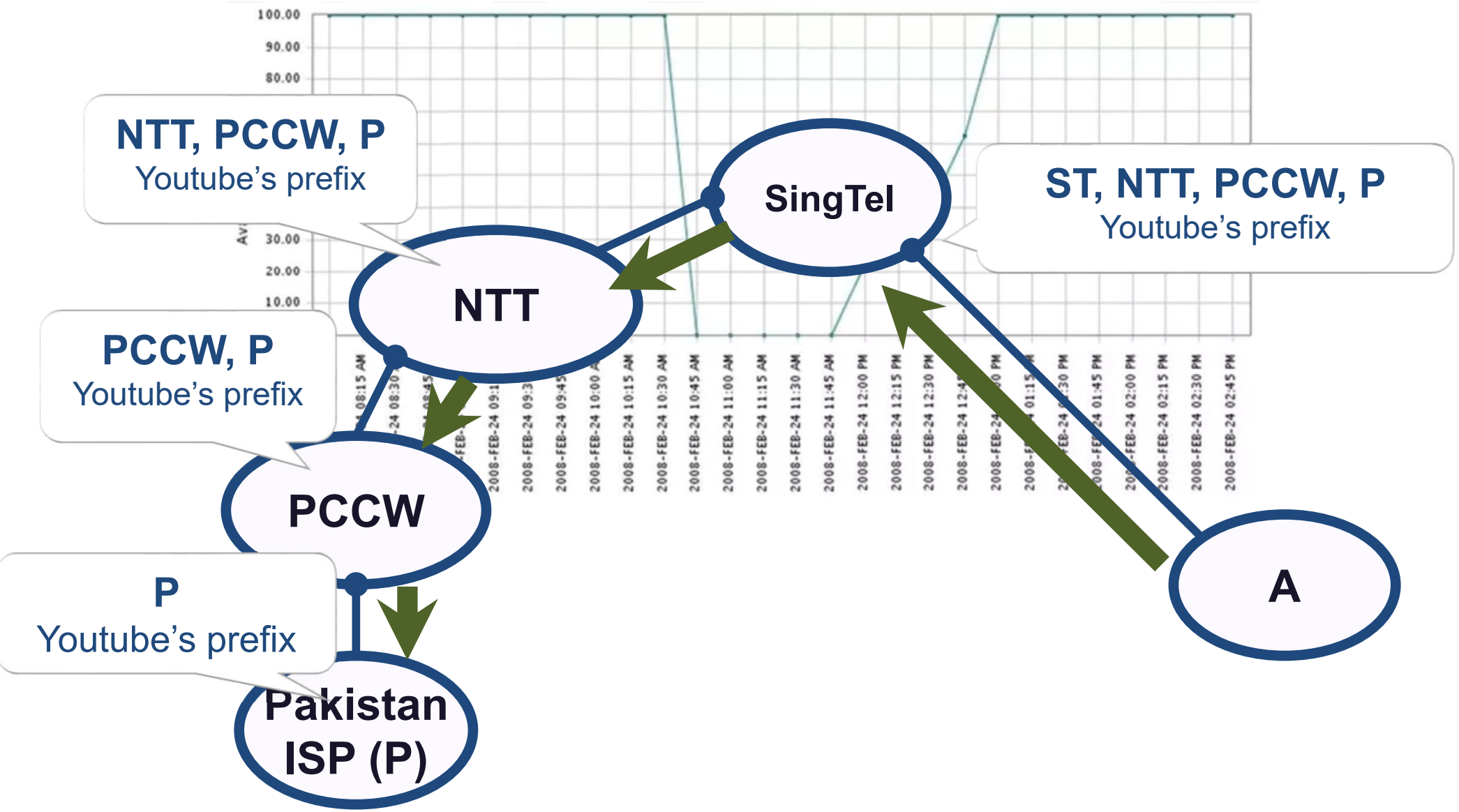
- *Confidentiality?*
- *Integrity?*
- *Availability?*

- **BGP has none!**

- Three major BGP attacks:
  - Prefix theft
  - AS path truncation
  - AS path alteration

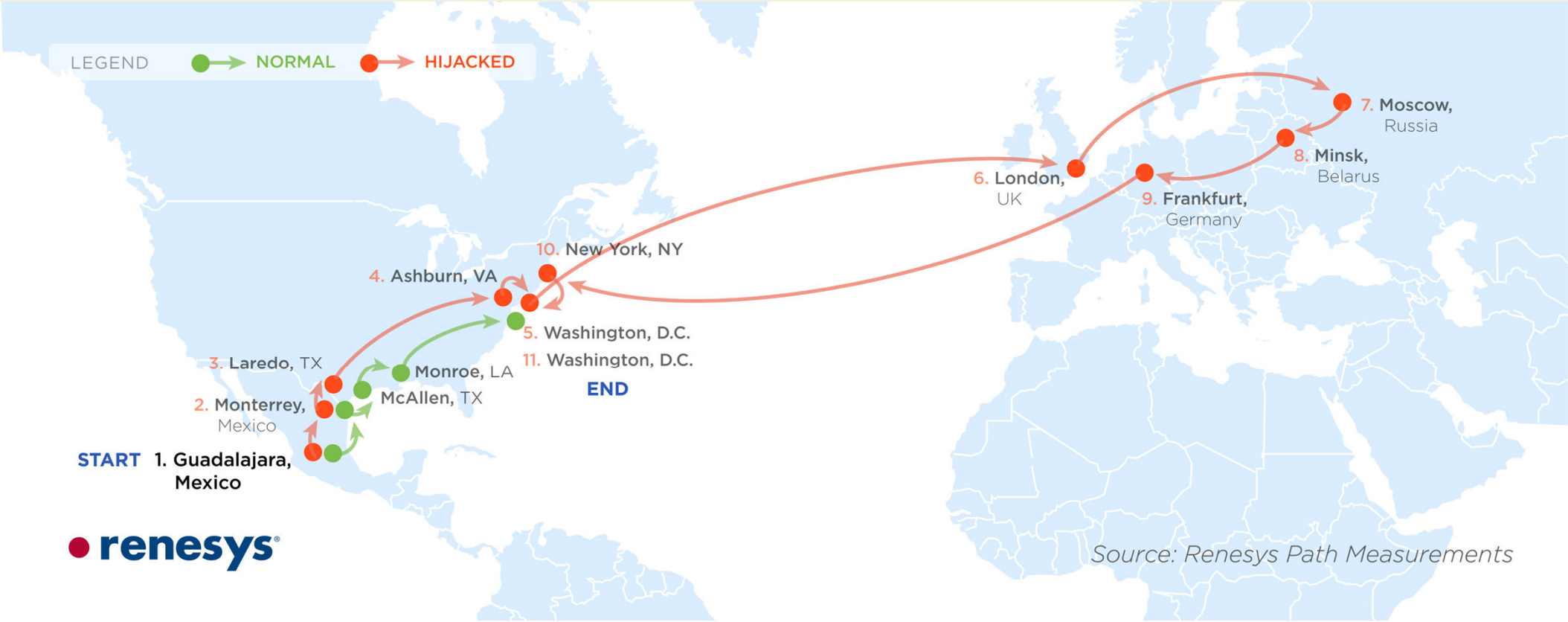
BGP ***Hijacking*** and ***Interception***

Pakistan Youtube Outage Event (2008)

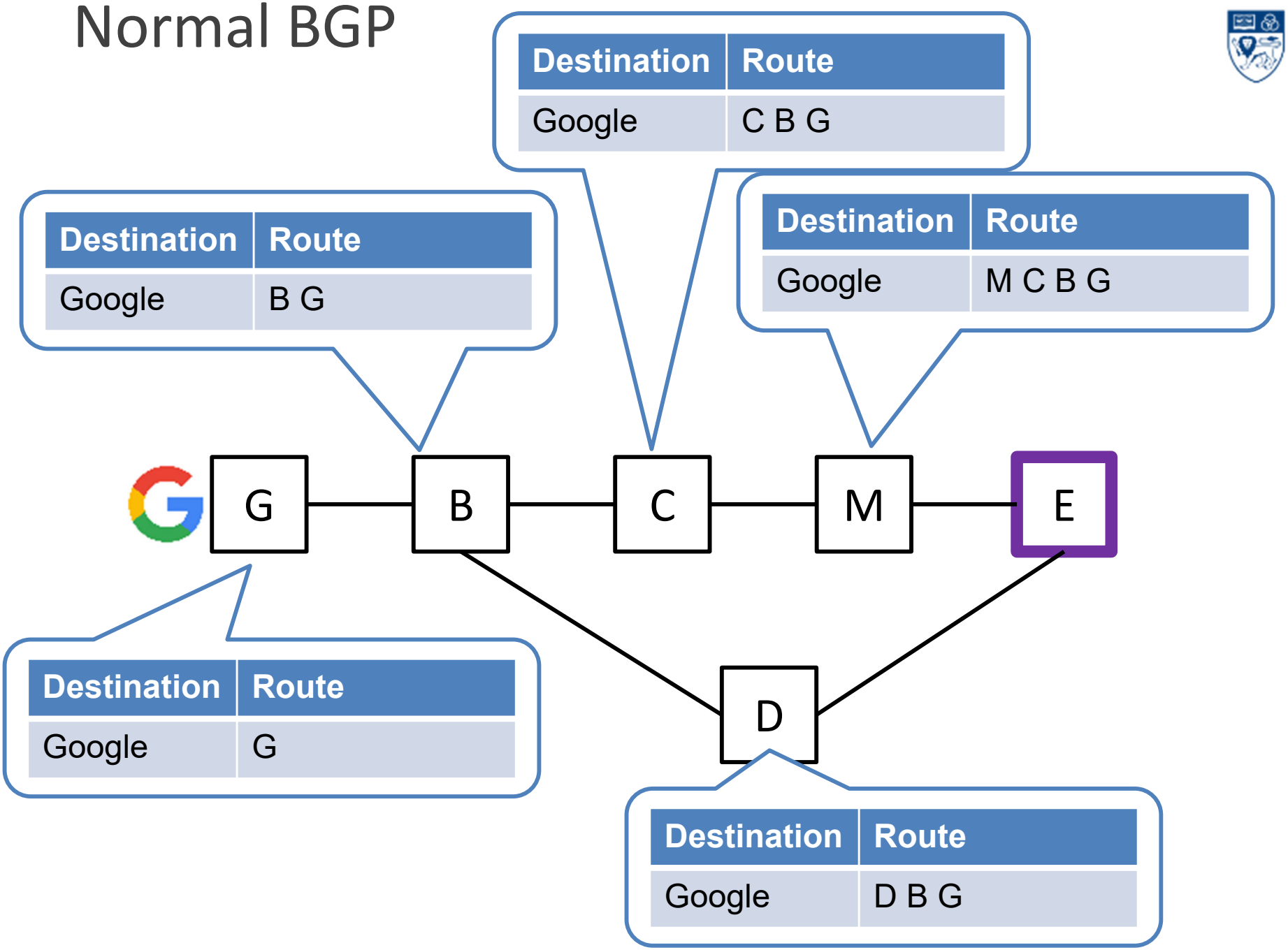


Interception in real world

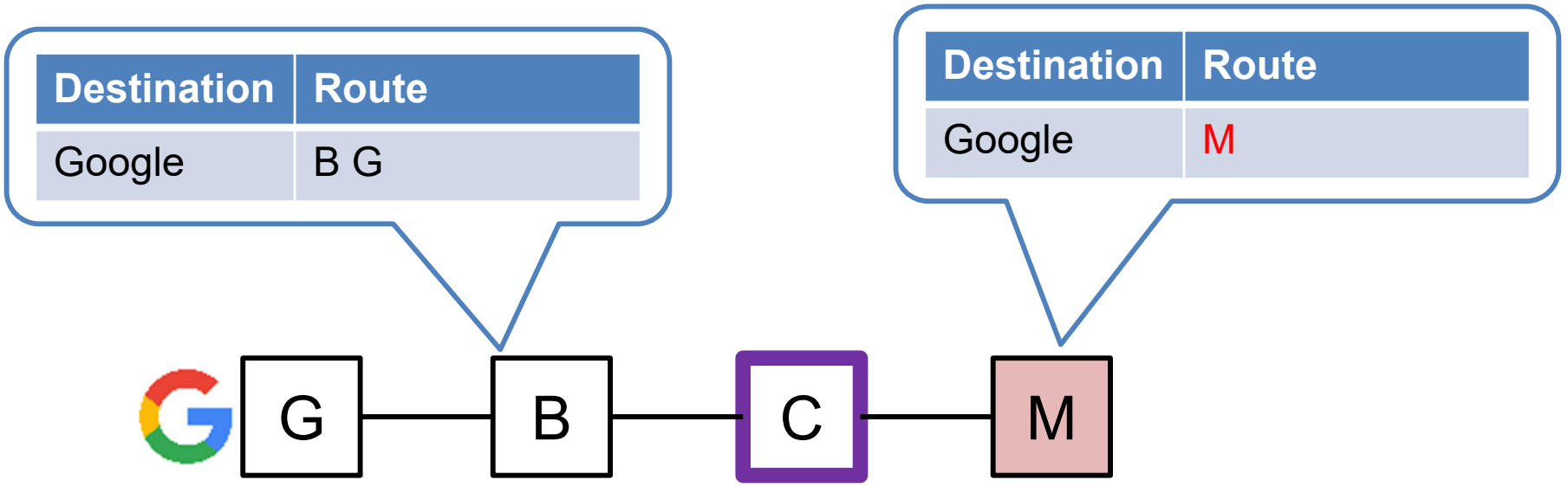
Traceroute Path 1: from **Guadalajara**, Mexico to **Washington**, D.C. via ***Belarus***



Normal BGP

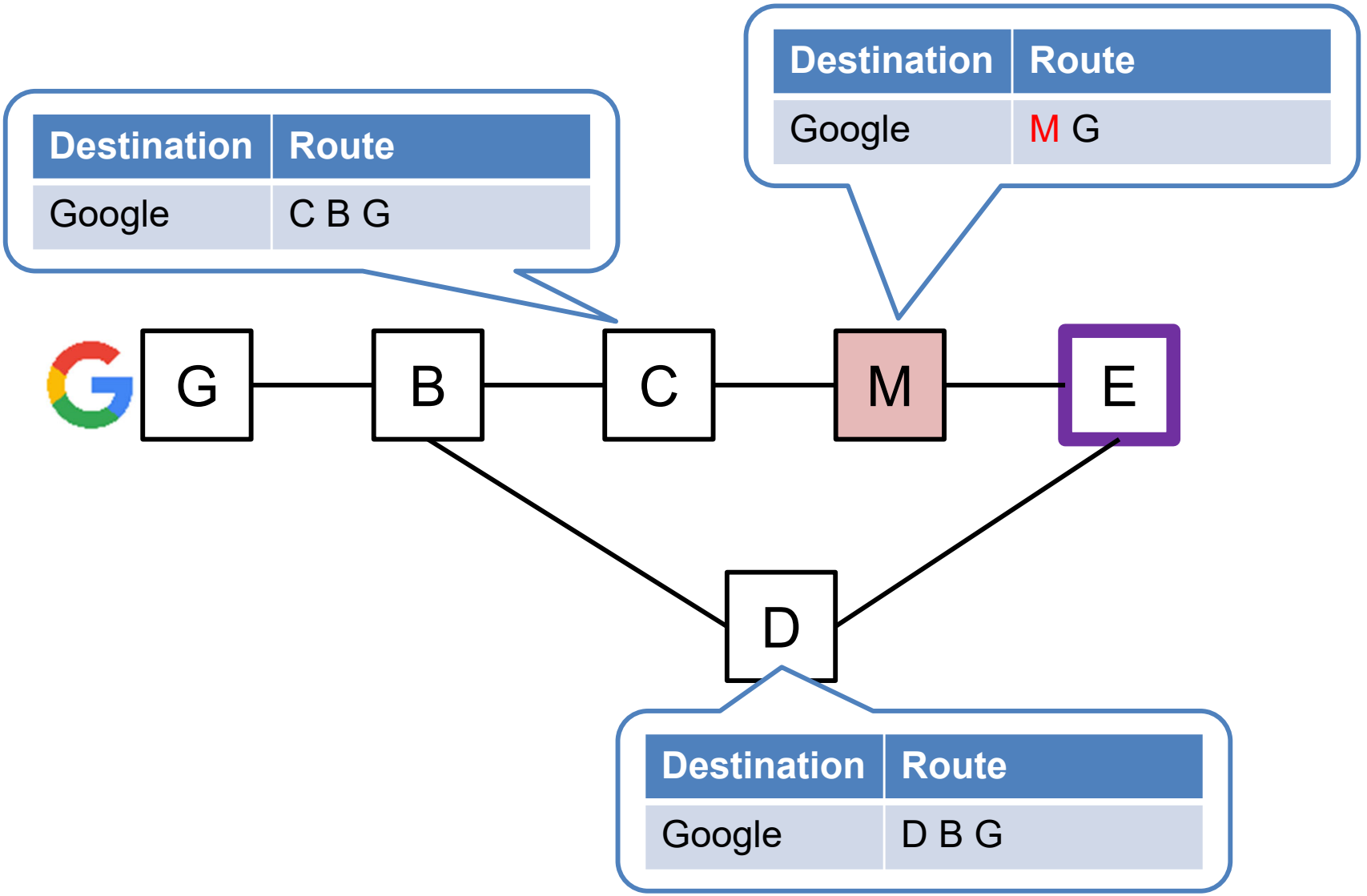


1) Prefix hijacking (invalid origin)



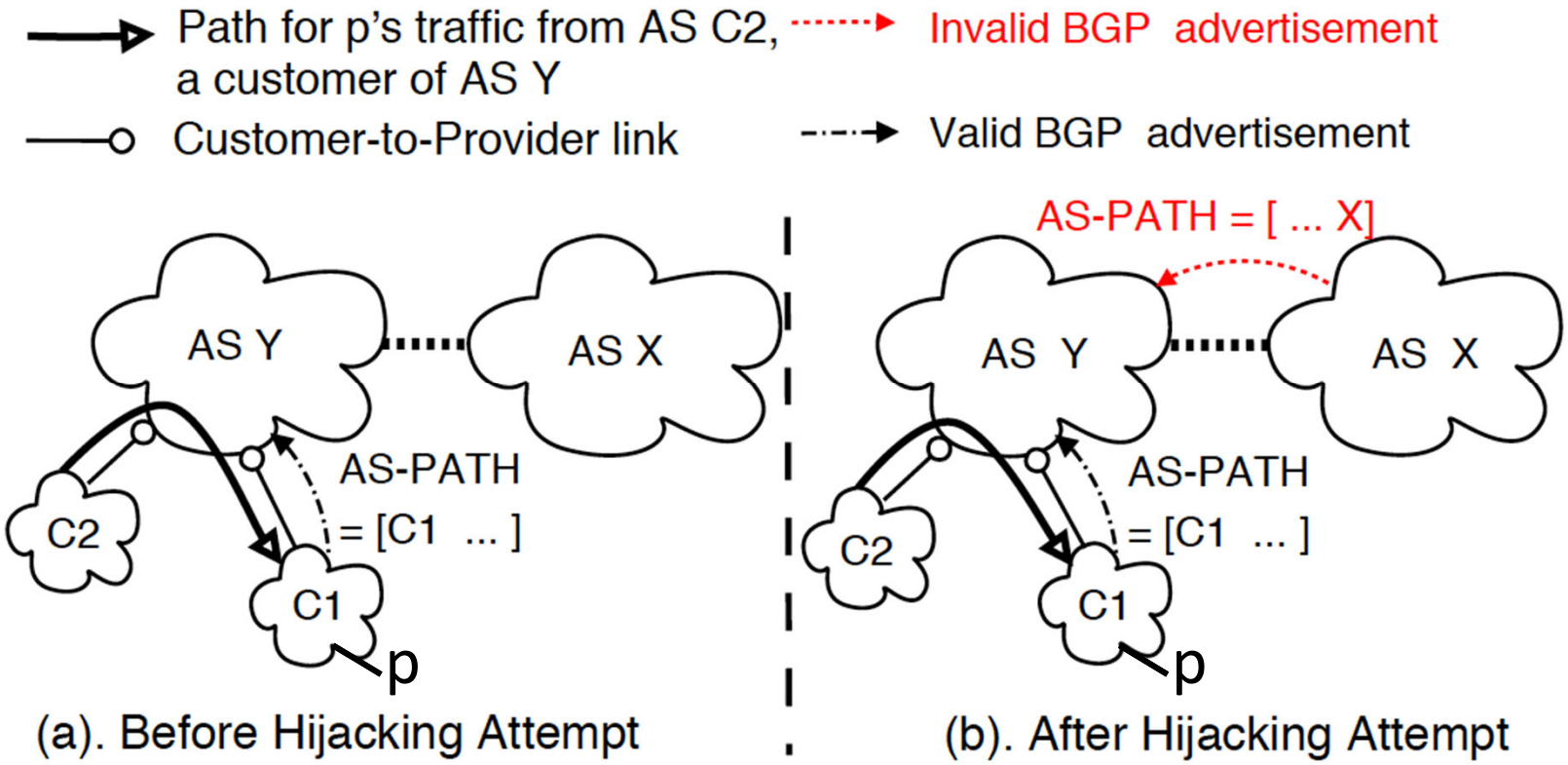
This attack causes “multiple origin AS (MOAS) anomaly”
And thus can be detected.

2) One-hop prefix hijacking (invalid next hop)



BGP Hijacking and Interception

- AS X hijacks traffic to C1 from AS Y
- If AS X forward traffic to C1, we call it **interception**.



- ✓ ***Will AS Y accept the invalid BGP advertisement for path for p? (Hijacking)***
- ✓ ***Can AS X always forward traffic to C1? (Interception)***

Effectiveness of Hijacking

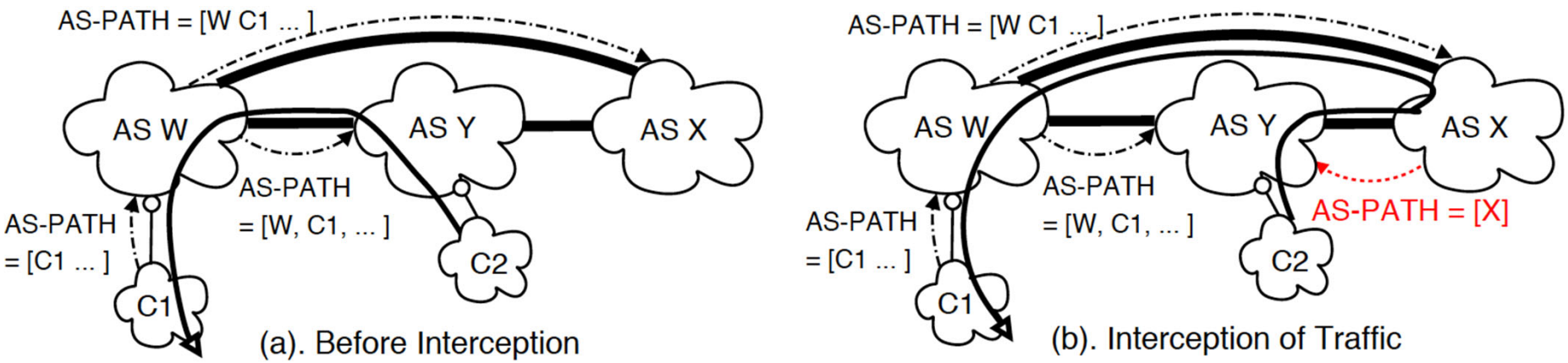
- AS Y accepts the invalid BGP update only when the new (invalid) route is **cheaper** than the original (valid) route

Table 1: AS Y's traffic to prefix p can (✓), cannot (✗) or can partly (–) be hijacked depending on its existing route and the invalid route.

Invalid route ⇒ Existing route	Length	Customer	Peer	Provider
Customer	<n	✗	✗	✗
	=n	–	✗	✗
	>n	✓	✗	✗
Peer	<n	✓	✗	✗
	=n	✓	–	✗
	>n	✓	✓	✗
Provider	<n	✓	✓	✗
	=n	✓	✓	–
	>n	✓	✓	✓

Interception = Hijacking + Forwarding

- Attacker may want to be stealthy. Thus, instead of backhauling, it forwards packets to original receiver



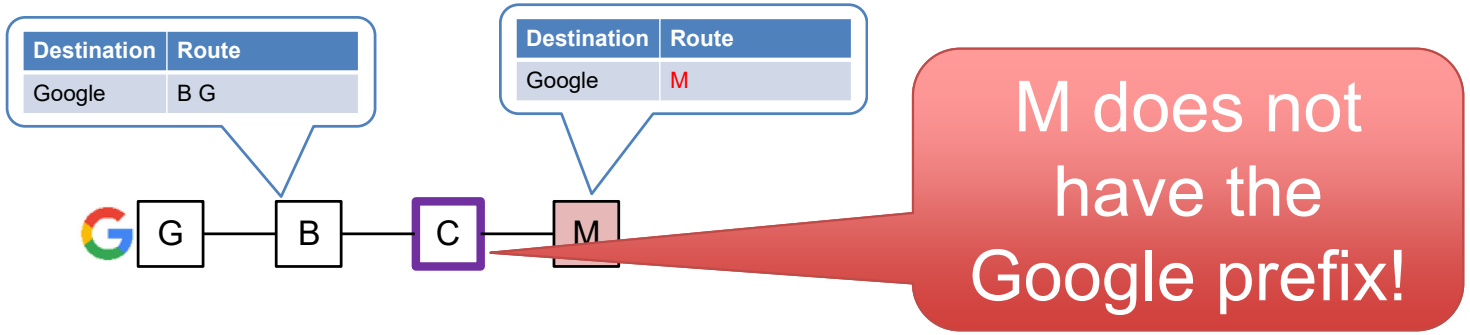
- ***Is forwarding always possible once path is hijacked?***

  Safety condition (condition for hijacking AS to successfully forward)
  None of the ASes along the route to prefix p used by the hijacking AS should choose the invalid route advertised by it over their existing route to p.

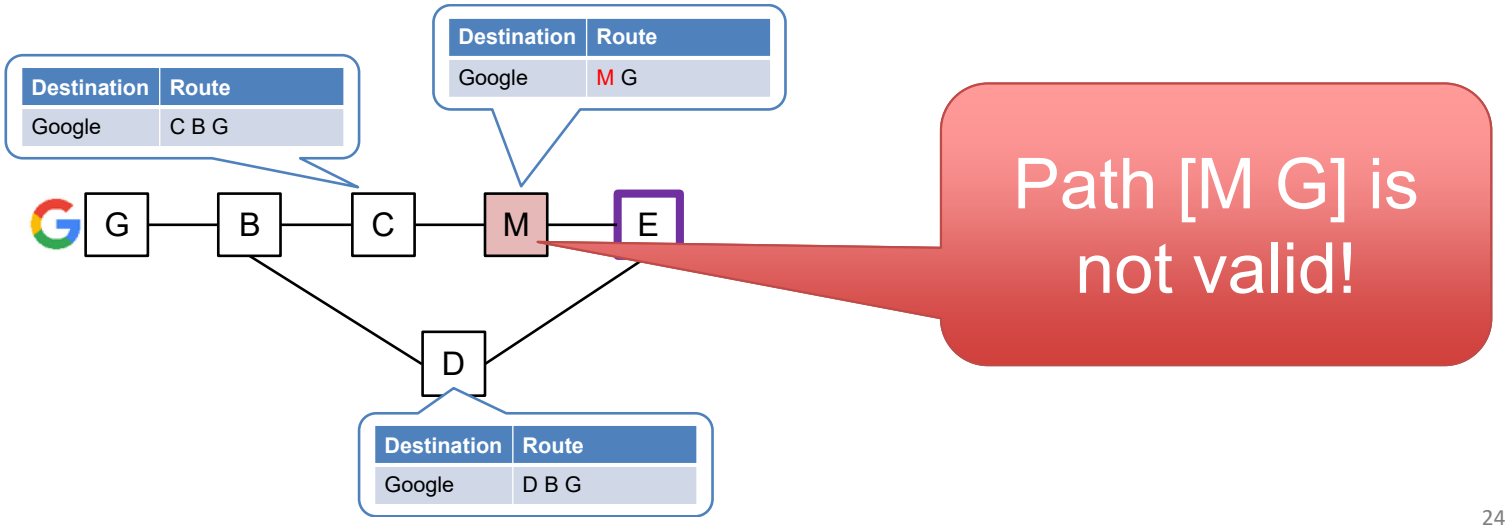
Solutions to BGP Hijacking

RPKI and BGPSEC

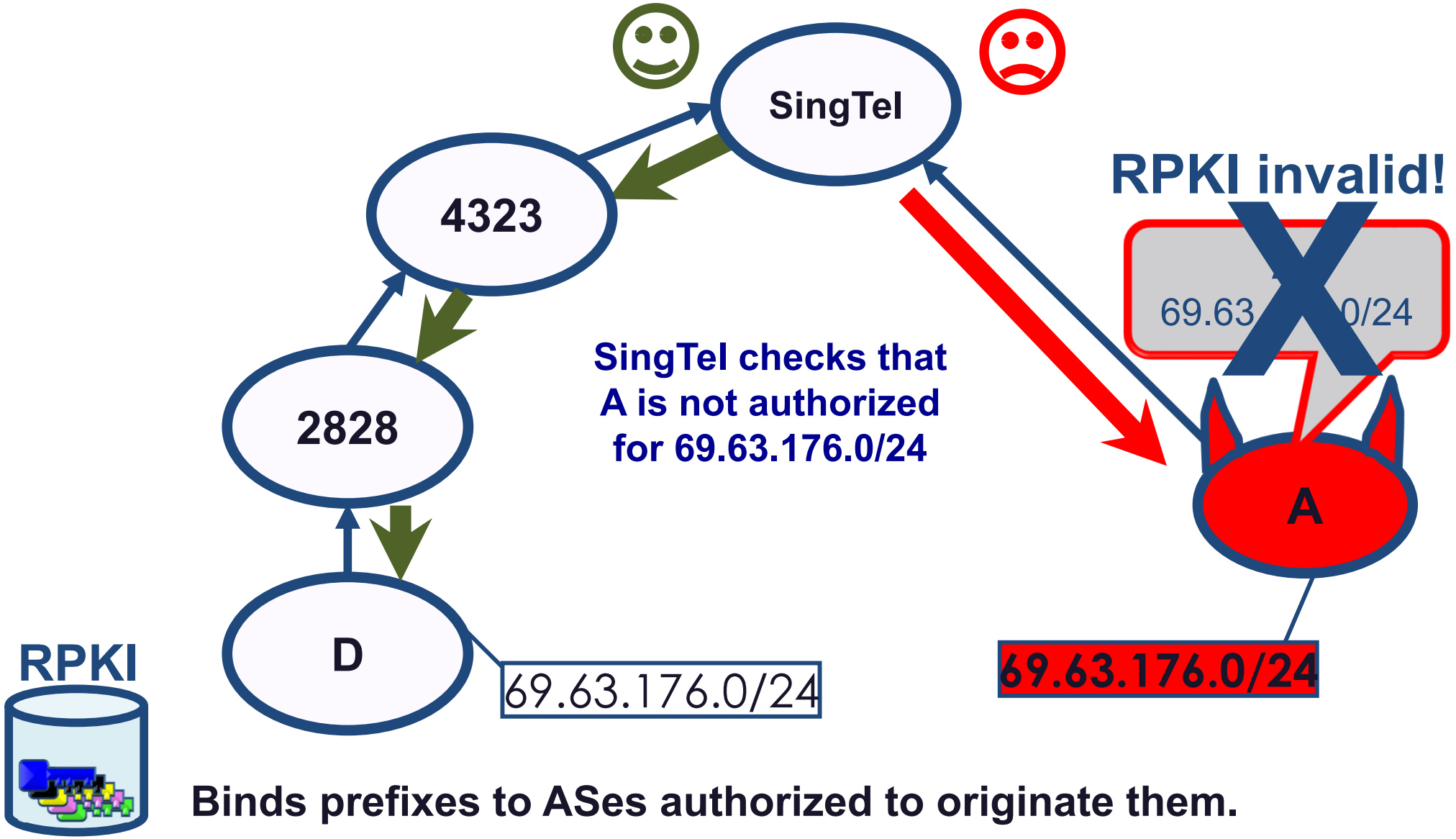
- Resource Public Key Infrastructure (RPKI)
  - Ensures particular AS owns particular address blocks



- BGPSEC
  - Provides AS path integrity

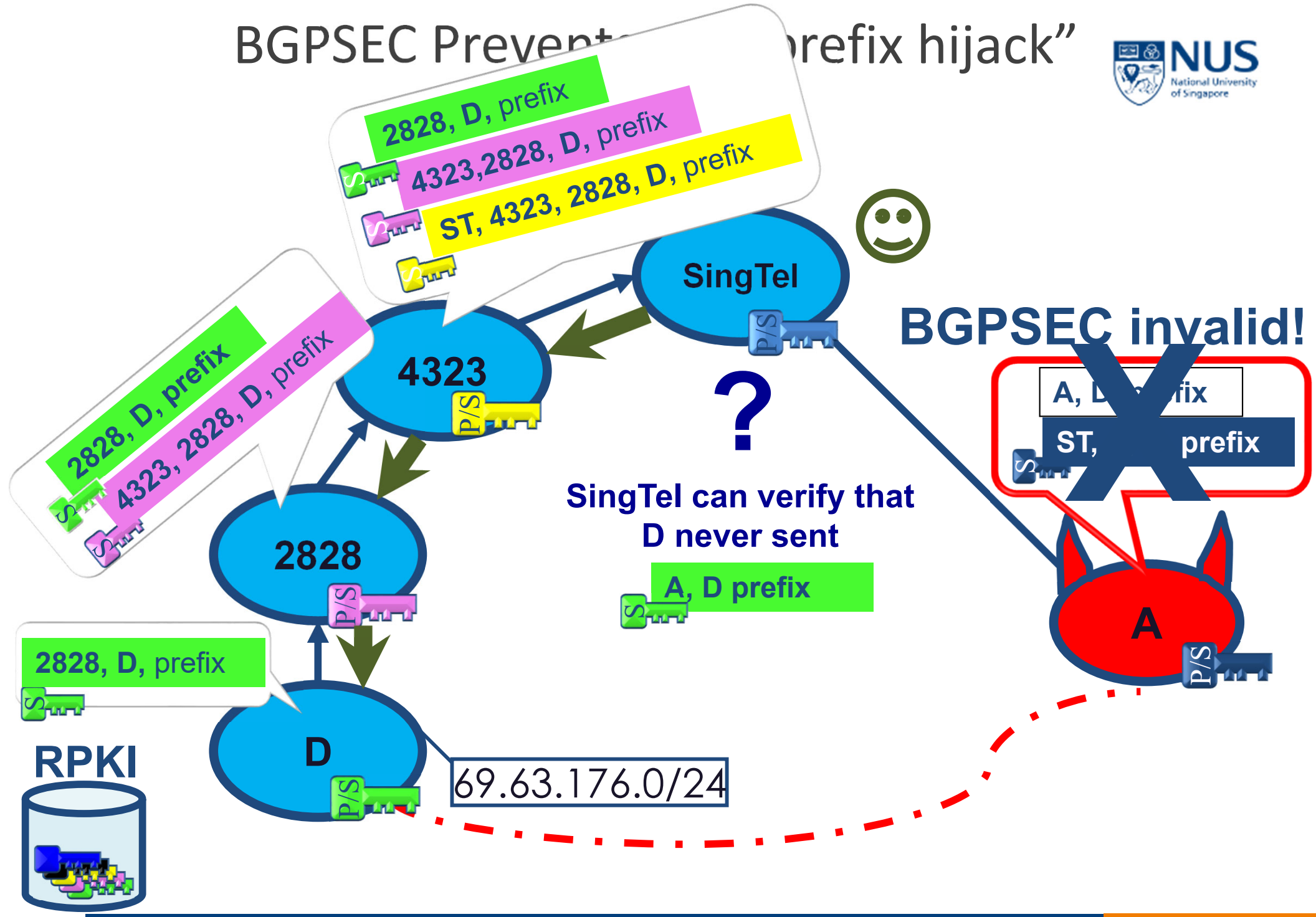


RPKI Prevents Prefix Hijacks

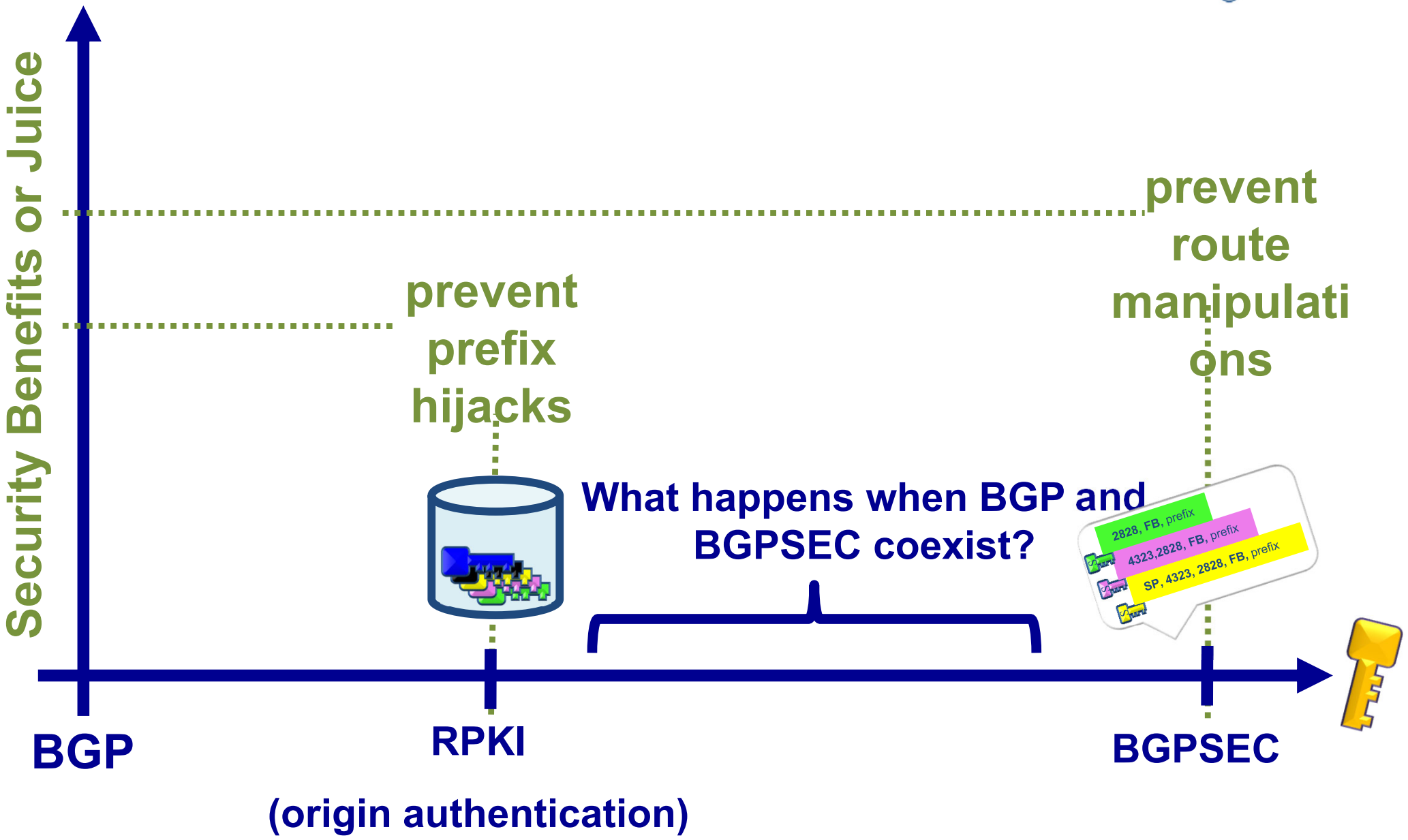


Binds prefixes to ASes authorized to originate them.

BGPSEC Prevent[illegible]refix hijack”

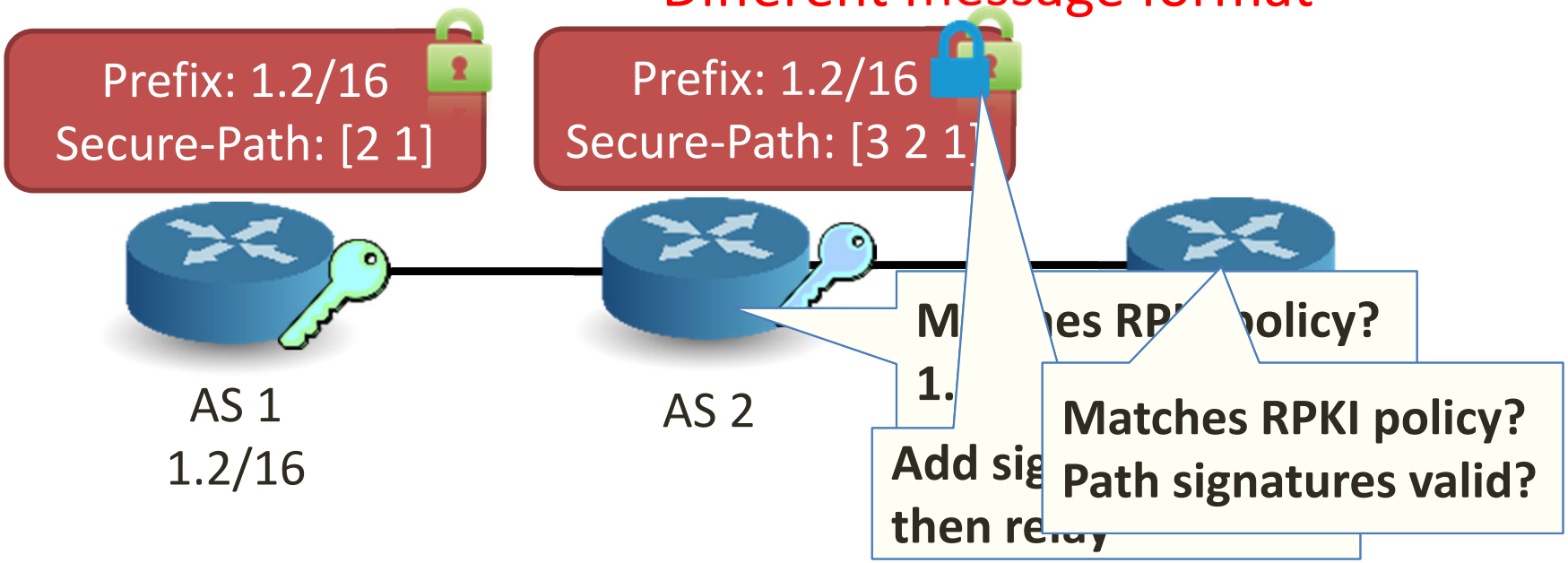


Partial Landscape of BGP Defenses



Current paradigm: a two step solution

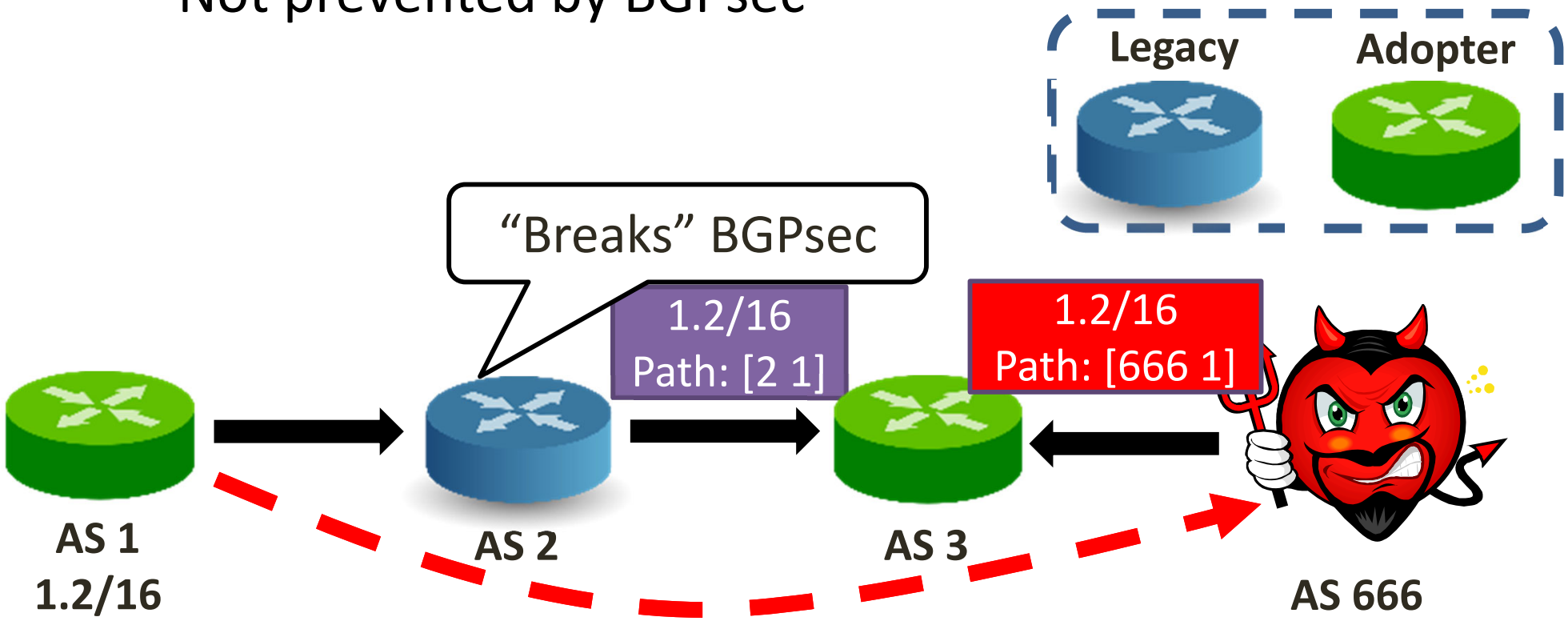
- First, RPKI against invalid origin
- Then, add BGPsec
  - Protects against false paths (e.g., next-AS attacks)
  - Deployment challenge: •Real-time signature and validation
    •Different message format



BGPsec in partial adoption?

Meager benefits [Lychev et al., SIGCOMM'13]

- AS 666 launches a next-AS attack against AS 1
  - Not prevented by BGPsec

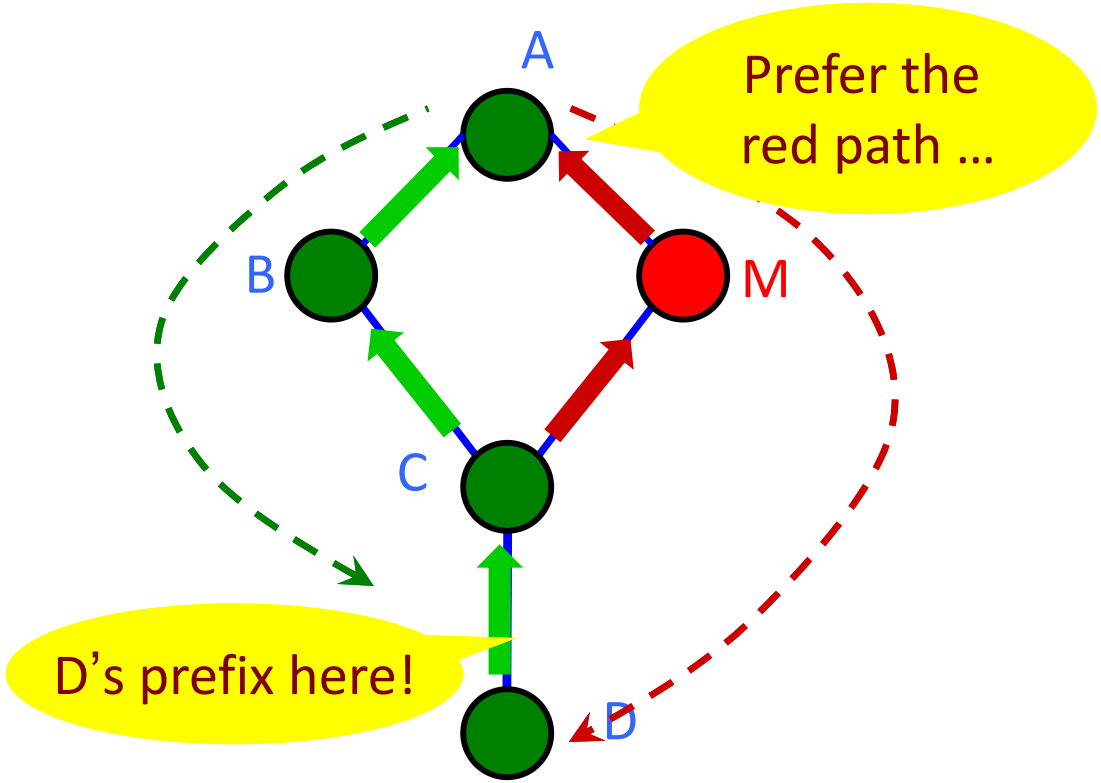


A ***clean-slate*** approach: SCION

(Following slides are from 2022 for reference)

Limitations of the Current Internet

- Too little *path control* by end points
  - Destination has too little control over inbound paths

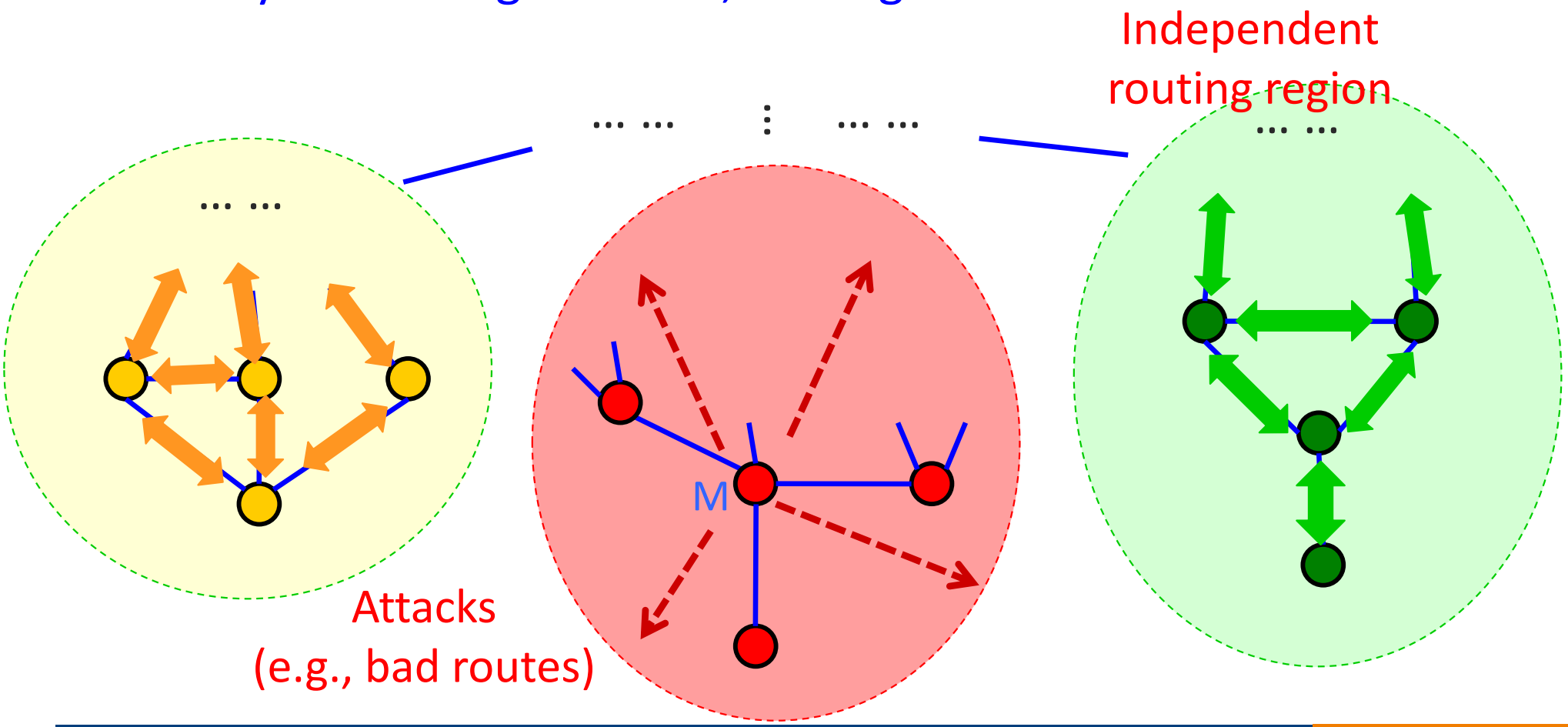


Limitations of the Current Internet

- Too little *path control* by end points
  - Destination has too little control over inbound paths
- Lack of routing isolation
  - A failure/attack can have global effects
  - Global visibility of paths is not scalable
- Lack of route freshness
  - Current BGP enables replaying of obsolete paths
- Huge routing/forwarding table size

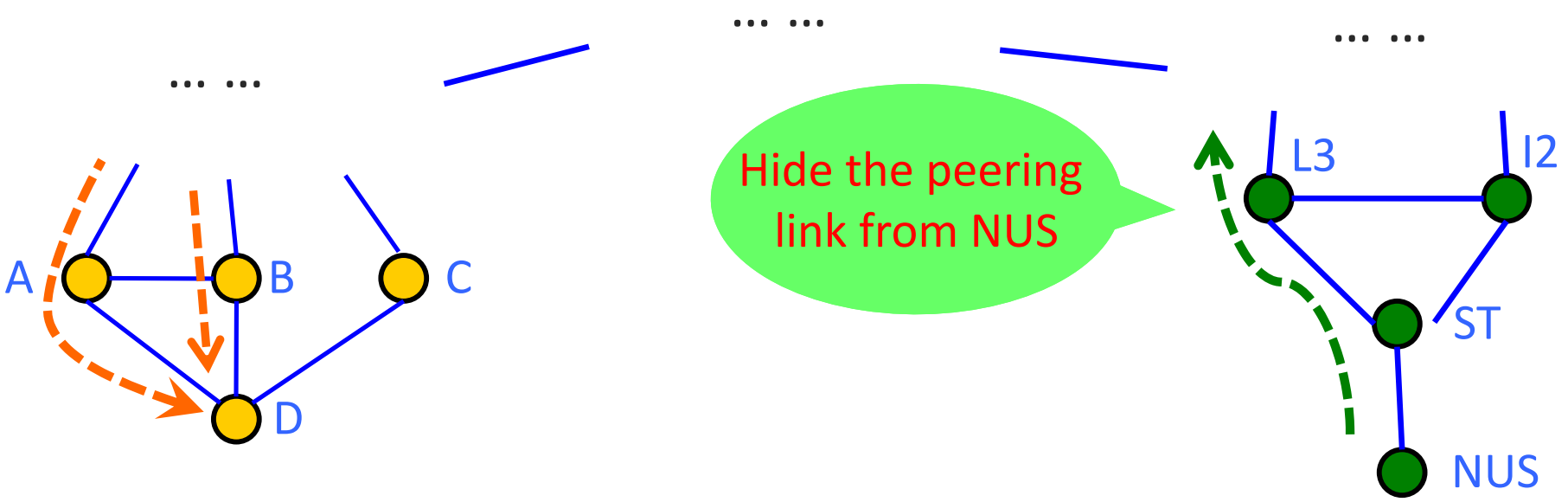
Wish List (1): Isolation

- Localization of attacks
- Mutually distrusting domains, no single root of trust



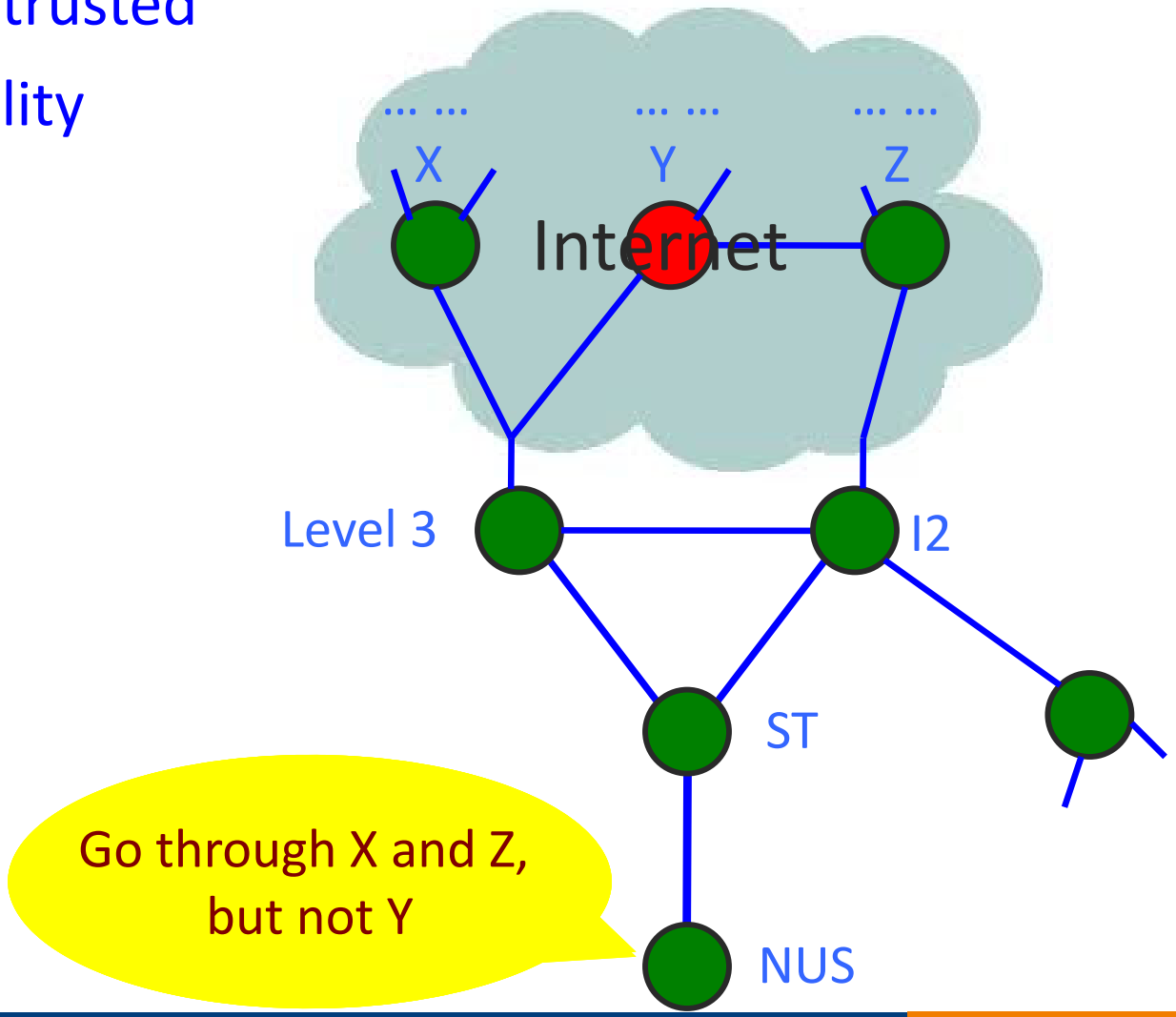
Wish List (2): Balanced Control

- Source, destination, transit ISPs all have path control
- Support rich policies and DDoS defenses



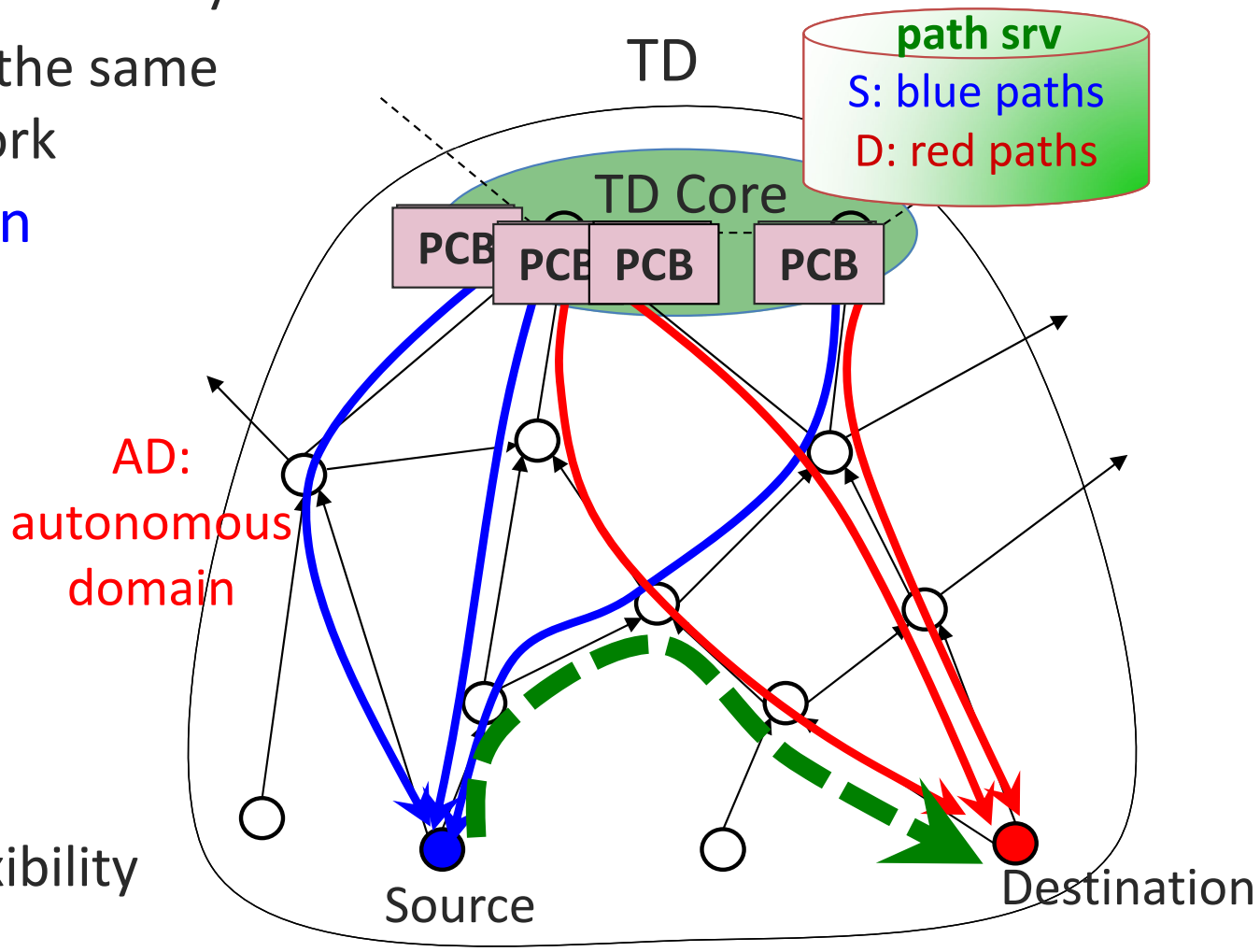
Wish List (3): Explicit Trust

- Know who needs to be trusted
- Enforceable accountability



SCION Architecture Overview

- Trust domain (TD)s
  - Isolation and scalability
  - Regulated by the same legal framework
- Path construction
  - scalability
- Path resolution
  - Control
  - Explicit trust
- Route joining (shortcuts)
  - Efficiency, flexibility

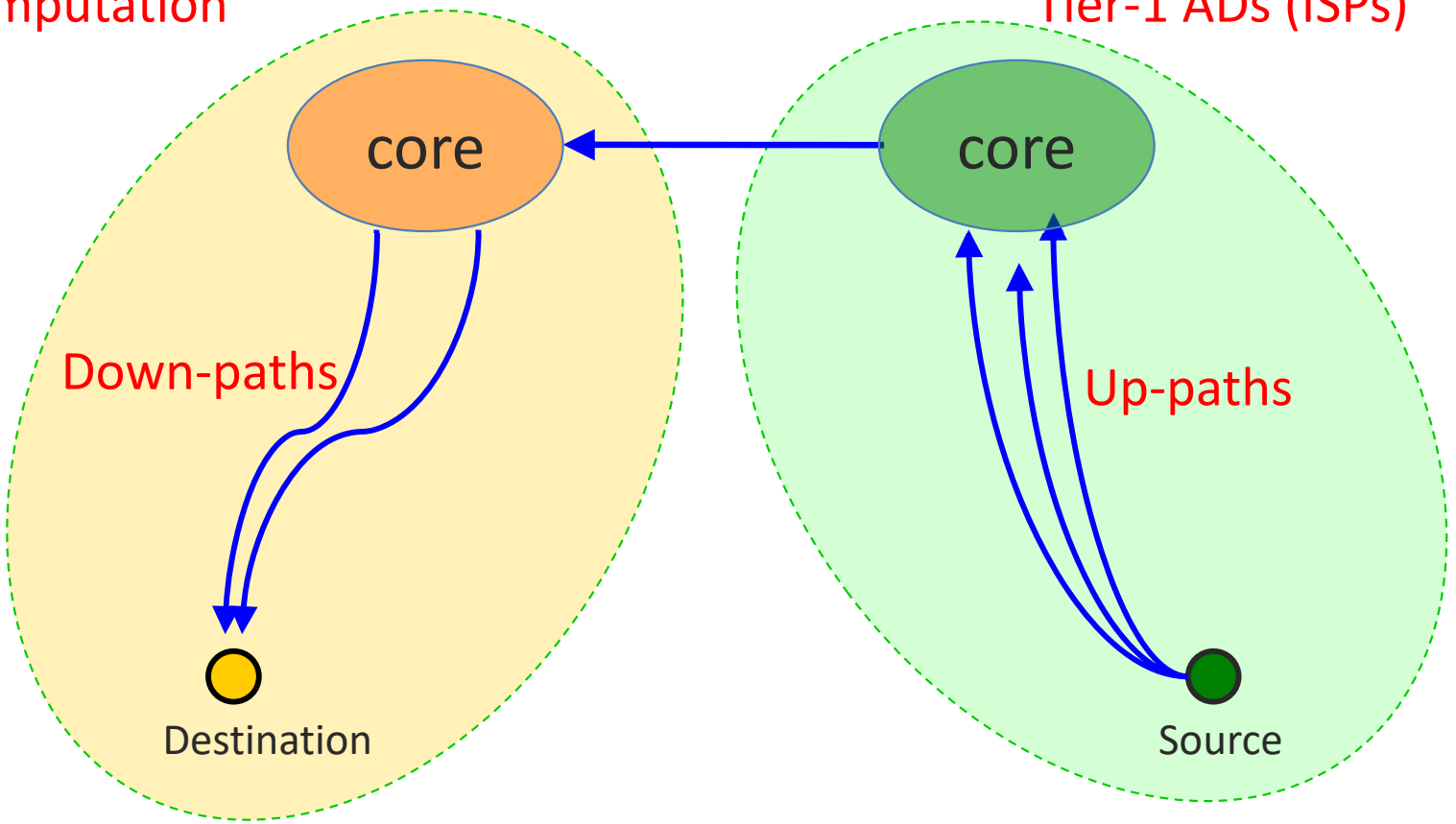


Logical Decomposition

❖ Split the network into a set of trust domains (TD)

TD: isolation of route computation

TD cores: interconnected Tier-1 ADs (ISPs)

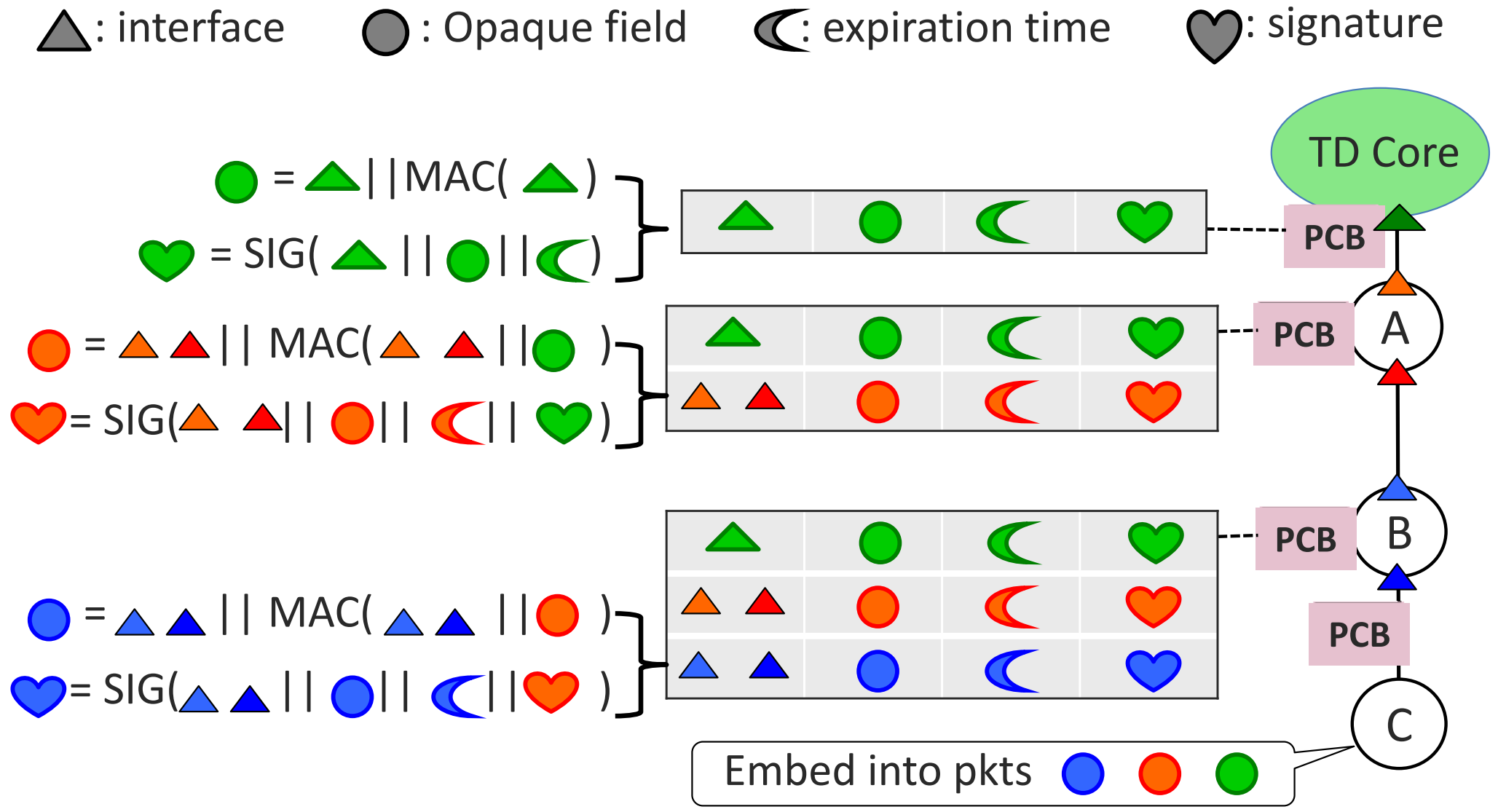


Path Construction

Goal: each endpoint learns multiple verifiable paths to its core

- Discovering paths via **Path Construction Beacons (PCBs)**
  - ✓ TD Core periodically initiates PCBs
  - ✓ Providers advertise upstream topology to peering and customer ADs
- ADs perform the following operations
  - ✓ Collect PCBs
  - ✓ For each neighbor AD, select which *k* PCBs to forward
  - ✓ Update cryptographic information in PCBs
- Endpoint AD will receive up to *k* PCBs from each upstream AD, and select *k* down-paths and up-paths

Path Construction Beacons (PCBs)



Forwarding

- Down-path contains all forwarding decisions (AD traversed) from endpoint AD to TD core
  - ✓ Ingress/egress points for each AD, authenticated in opaque fields
  - ✓ ADs use internal routing to send traffic from ingress to egress point
- Joined end-to-end route contains full forwarding information from source to destination
  - ✓ No routing / forwarding tables needed!

SCION Security Benefits

		BGPSEC etc	SCION
Isolation	Scalability, freshness		
	Path replay attack		
	Collusion attack		
	Single root of trust		
Trusted Computing Base		Whole Internet	TD Core and on-path ADs
Path Control	Source	End-to-end control	Only up-path
	Destination	No control	Inbound paths
	DDoS	Open attacks	Enable defenses

Performance Benefits

- Scalability
  - Routing updates are scoped within the local TD
- Flexibility
  - Transit ISPs can embed local routing policies in opaque fields
- Simplicity and efficiency
  - No interdomain forwarding table
  - Current network layer: routing table explosion
  - Symmetric verification during forwarding
  - Simple routers, energy efficient, and cost efficient

Routing Attacks (= BGP Attacks)

- BGP *is* the routing protocol of the Internet
- But hijacking and interception of BGP routes are very easy

- Approach 1: BGPSEC/RPKI
  - Several practical issues. Not widely deployed.
- Approach 2: SCION
  - Can we really re-design the Internet?

Questions?