SCION: A Secure Internet Architecture

Adrian Perrig

Network Security Group, ETH Zürich

Anapaya Systems

ETH zürich

SCION

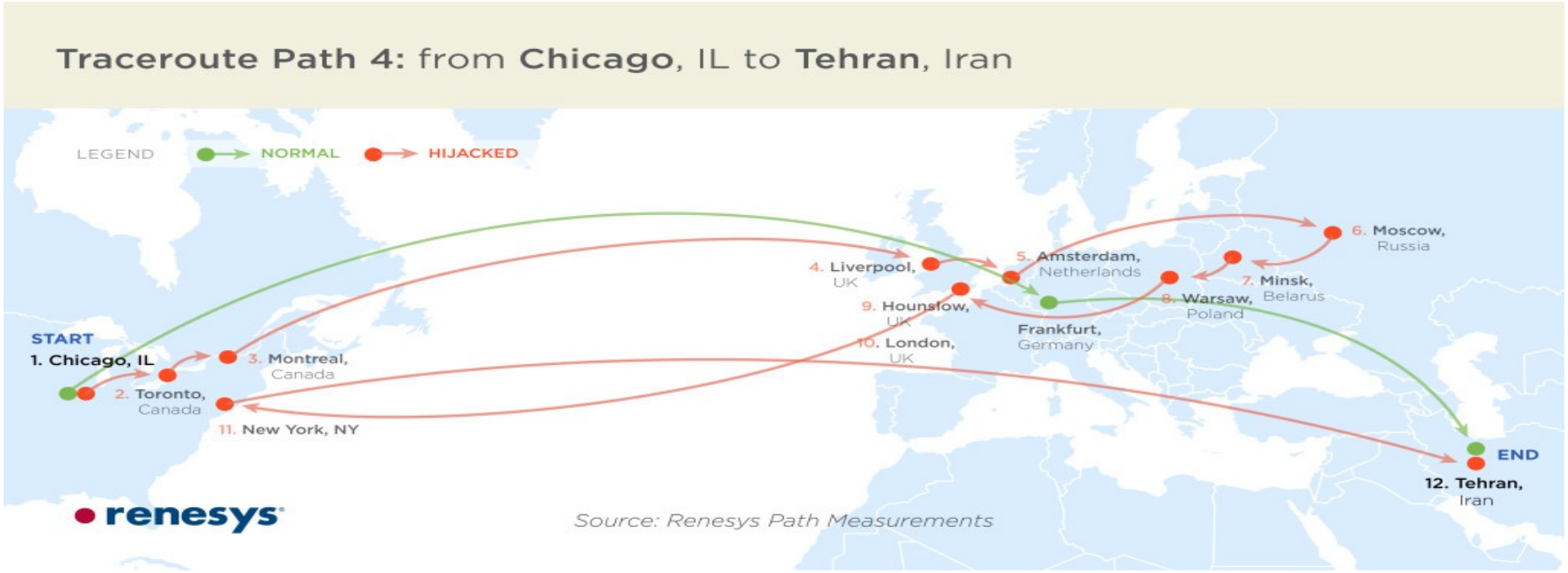
anapaya systems

Internet Weakness: DoS and DDoS Attacks

- Expensive and difficult to protect against DoS und DDoS attacks
- Despite large investments, attacks continue to be successful
  - **November 2015: Protonmail attacked during 1 week**
  - **March 2016: CH e-commerce under attack: Digitec, Galaxus, SBB, Migros, etc.** (Hackers demanded 25 Bitcoins to stop attacks)
  - **Fall 2016: Global Mirai botnet attacks, e.g., OVH, Dyn, russian banks**
  - June 2017: Northkorea “Hidden Cobra” botnet uncovered
  - September 2017: Global airport chaos, DDoS paralyzes checkin systems
- **Can we reliably defend against DDoS attacks?**

Internet Weakness: Communication Path Hijacking

- Sender und receiver have limited control over routing paths
- Attacks can hijack and relay paths
- **How can we guarantee communication paths?**



ETH zürich

SCION

Internet Weakness: Kill Switch ruptures Sovereignty

- Current Internet suffers from several “Kill Switches”, which can halt communication within a geographical area
- Several attack avenues exist: DDoS, BGP hijacking, DNS redirection, BGPSEC / DNSSEC / TLS certificate revocation
- Example August 2017: An erroneous route injected by Google prevents communication for 50% of Internet in Japan during 40 minutes
- **Can we construct an Internet without Kill Switches?**

SCION Architecture Design Goals

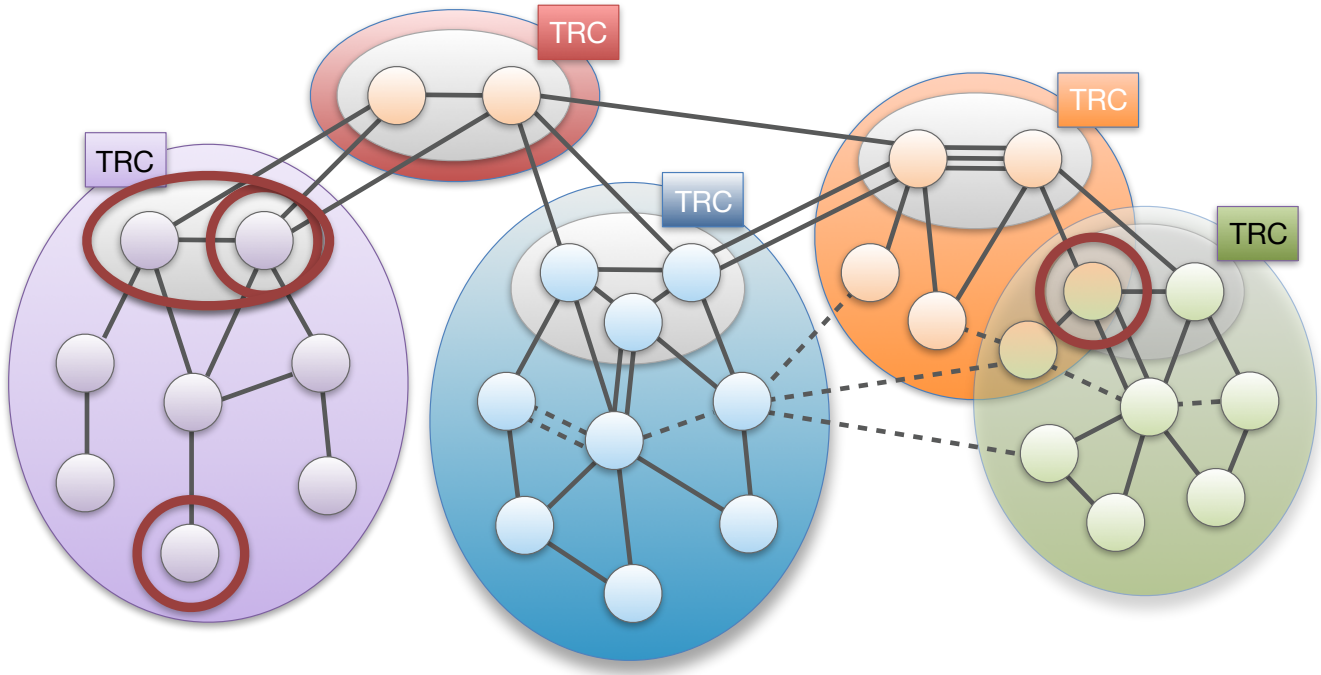
- High availability, even for networks with malicious parties
  - Adversary: access to management plane of router
  - Communication should be available if adversary-free path exists
- Secure entity authentication
  that scales to global heterogeneous (dis)trusted environment
- Flexible trust: enable selection of trust roots
- Transparent operation: clear what is happening to packets and whom needs to be relied upon for operation
- Balanced control among ISPs, senders, and receivers
- Scalability, efficiency, flexibility

ETH zürich

SCION

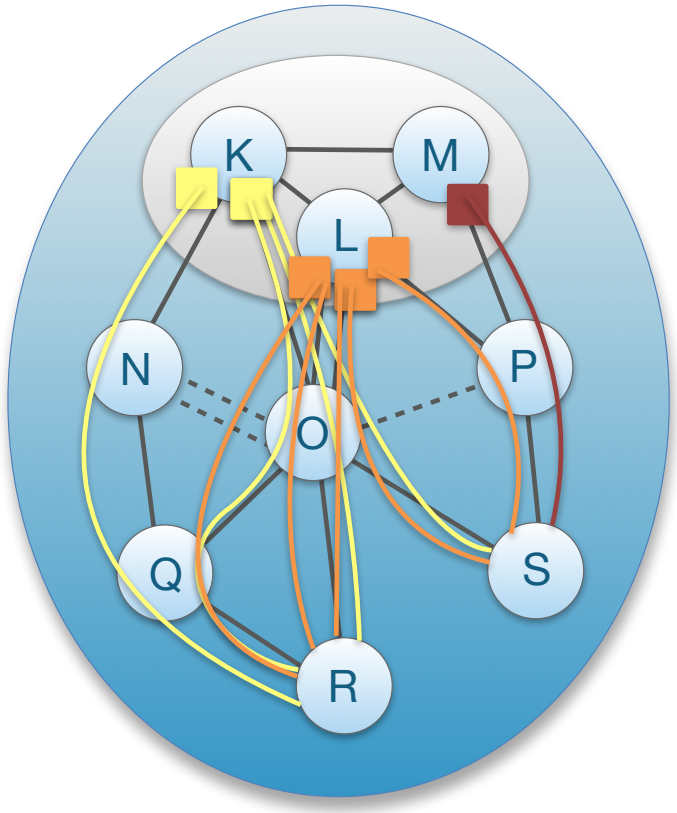
Approach for Scalability: Isolation Domain (ISD)

- Isolation Domain (ISD): grouping of ASes
- ISD core: ASes that manage the ISD
- Core AS: AS that is part of ISD core
- Control plane is organized hierarchically
  - Inter-ISD control plane
  - Intra-ISD control plane



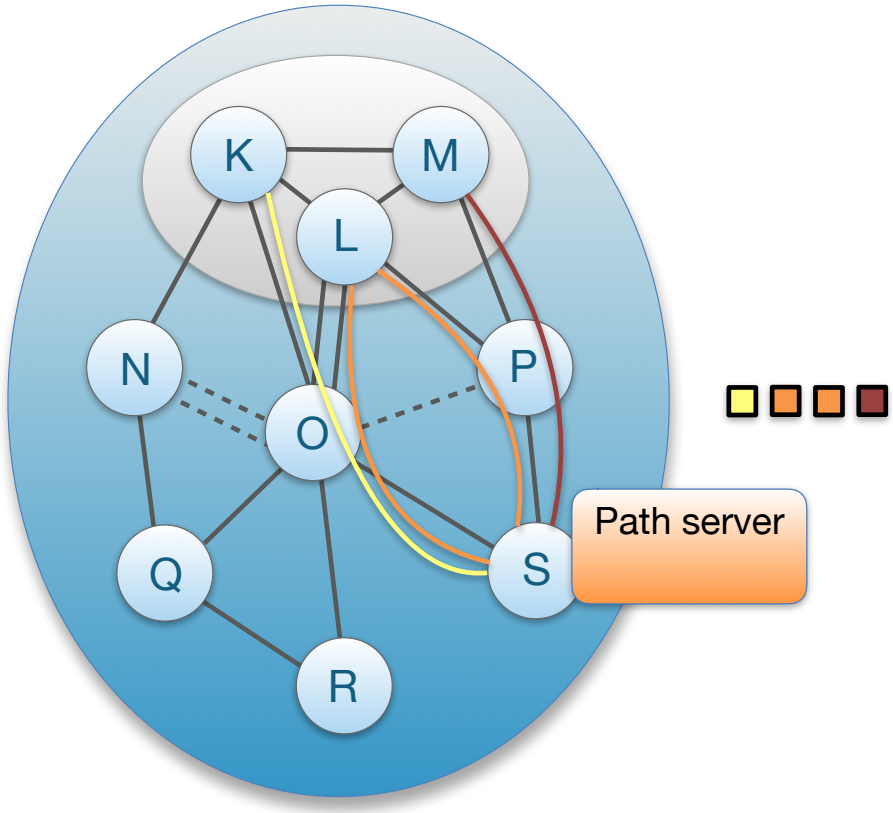
Intra-ISD Path Exploration: Beaconing

- Core ASes K, L, M initiate Path-segment Construction Beacons (PCBs), or "beacons"
- PCBs traverse ISD as a flood to reach downstream ASes
- Each AS receives multiple PCBs representing path segments to a core AS



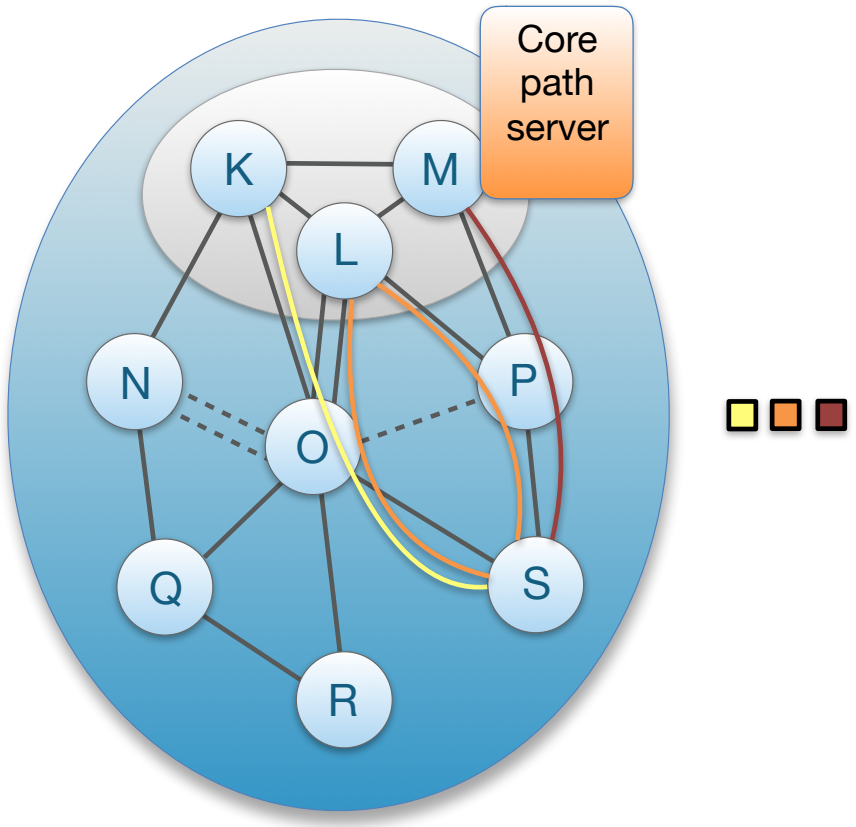
Up-Path Segment Registration

- AS selects path segments to announce as up-path segments for local hosts
- Up-path segments are registered at local path servers



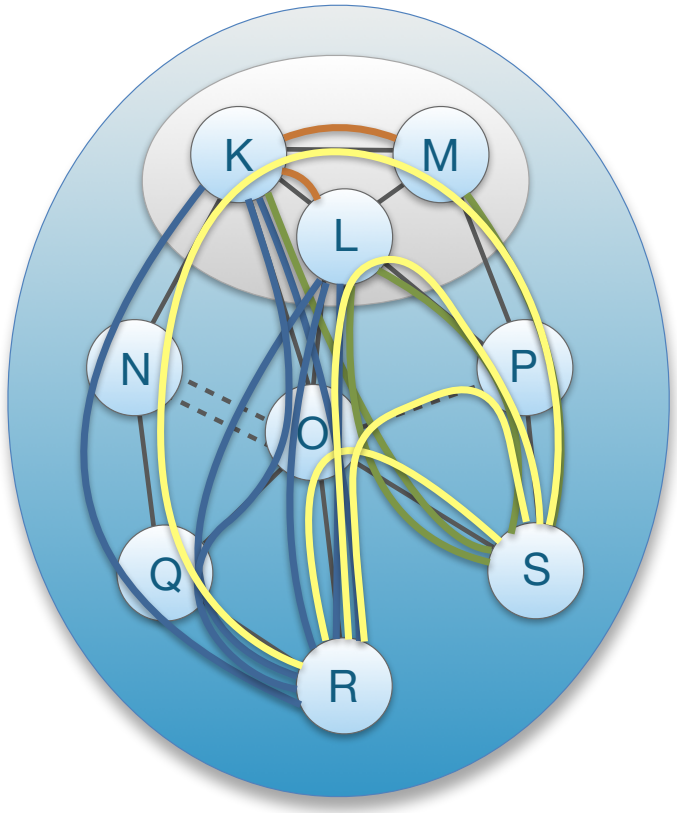
Down-Path Segment Registration

- AS selects path segments to announce as down-path segments for others to use to communicate with AS
- Down-path segments are uploaded to core path server in core AS

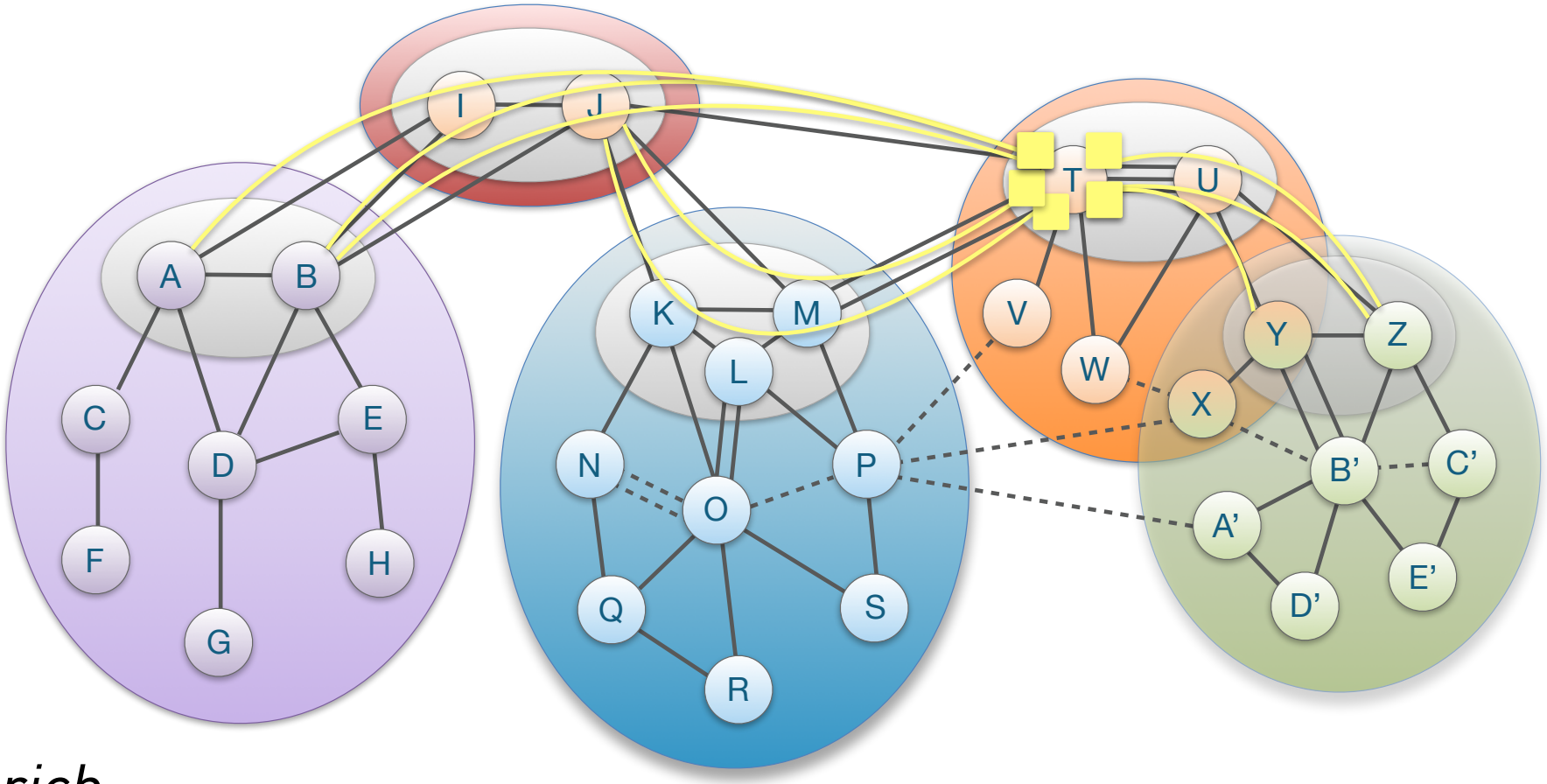


Path Creation: Local ISD

- Client requests path segments to <ISD, AS> from local path server
- If down-path segments are not locally cached, local path server send request to core path server
- Local path server replies
  - Up-path segments to local ISD core ASes
  - Down-path segments to <ISD, AS>
  - Core-path segments as needed to connect up-path and down-path segments



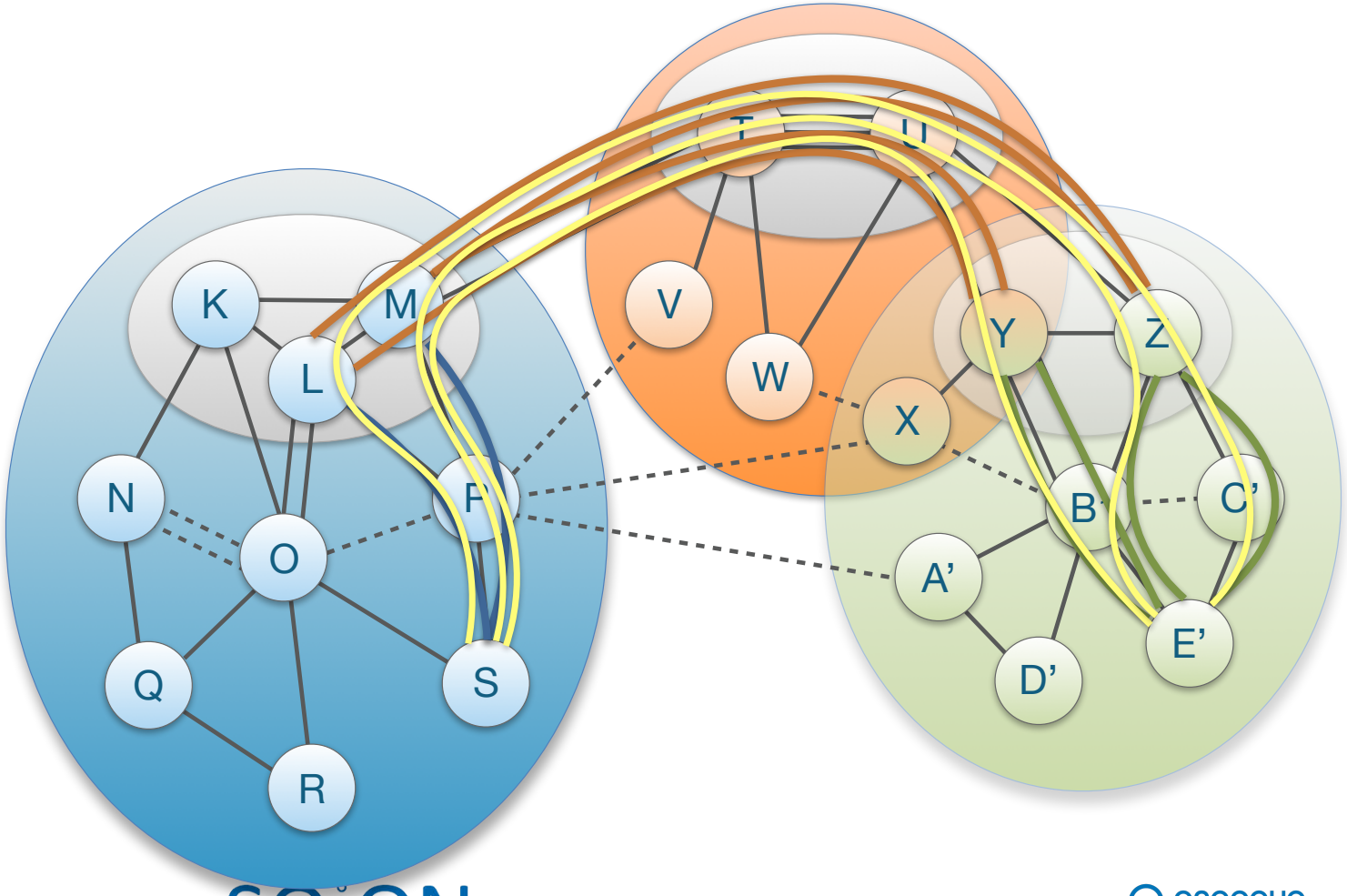
Inter-ISD Path Exploration: Sample Core-Path Segments from AS T



ETH zürich

Path Creation: Remote ISD

- Host contacts local path server requesting <ISD, AS>
- If path segments are not cached, local path server will contact core path server
- If core path server does not have path segments cached, it will contact remote core path server
- Finally, host receives up-, core-, and down-segments



ETH zürich

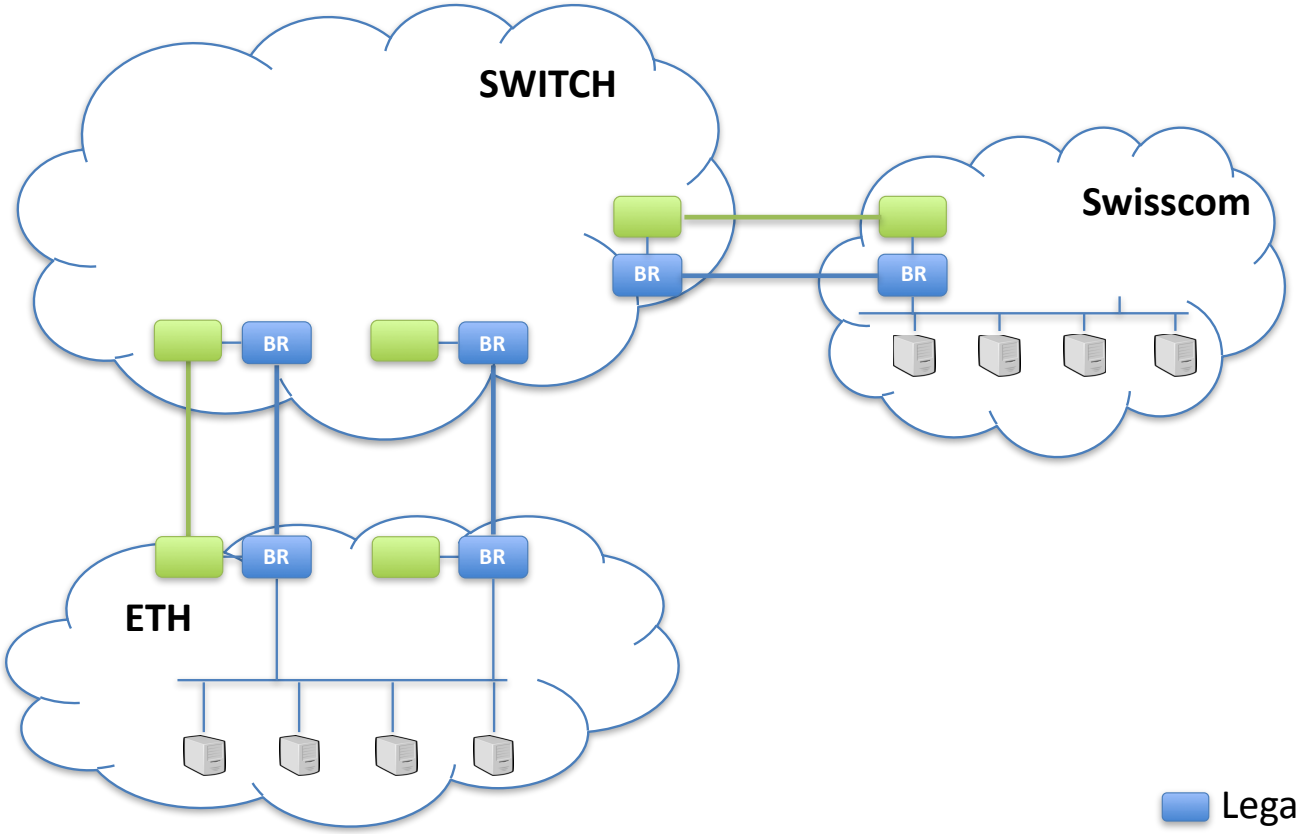
SCION

anapaya systems

No Global Coordination Required for Adoption

- SCION re-uses current local network infrastructure
- Requires setup of routers and servers (commodity HW)
  - SCION border router
  - Beacon, certificate, and path servers
- Border routers of different ASes connect natively or using as overlay over the Internet
- For fault tolerance, multiple servers and border routers can be set up
- Minimal deployment: single commodity host per domain, implementing border router and all servers

Deployment @ ETH



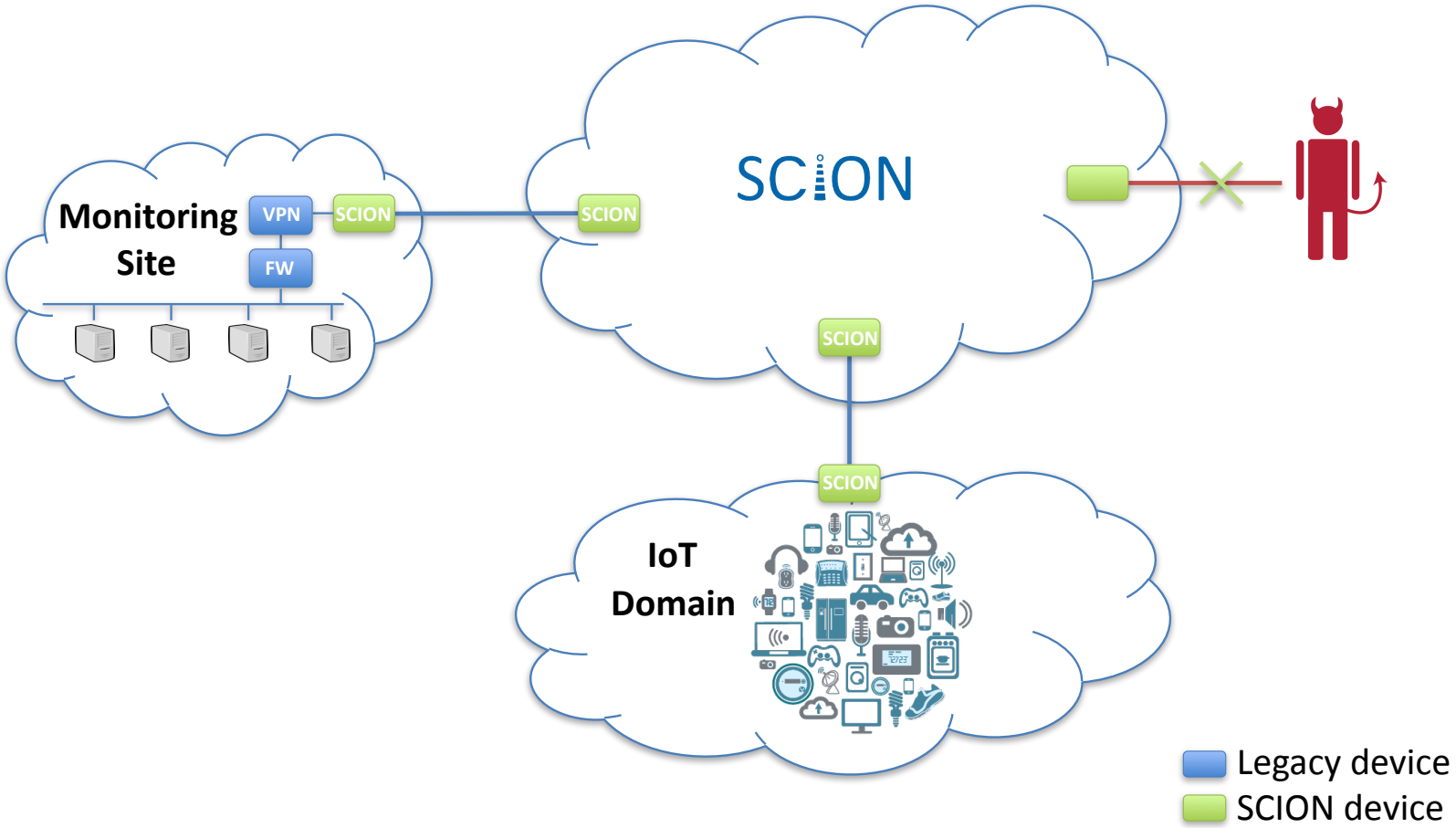
Legacy device
SCION border router

ETH zürich

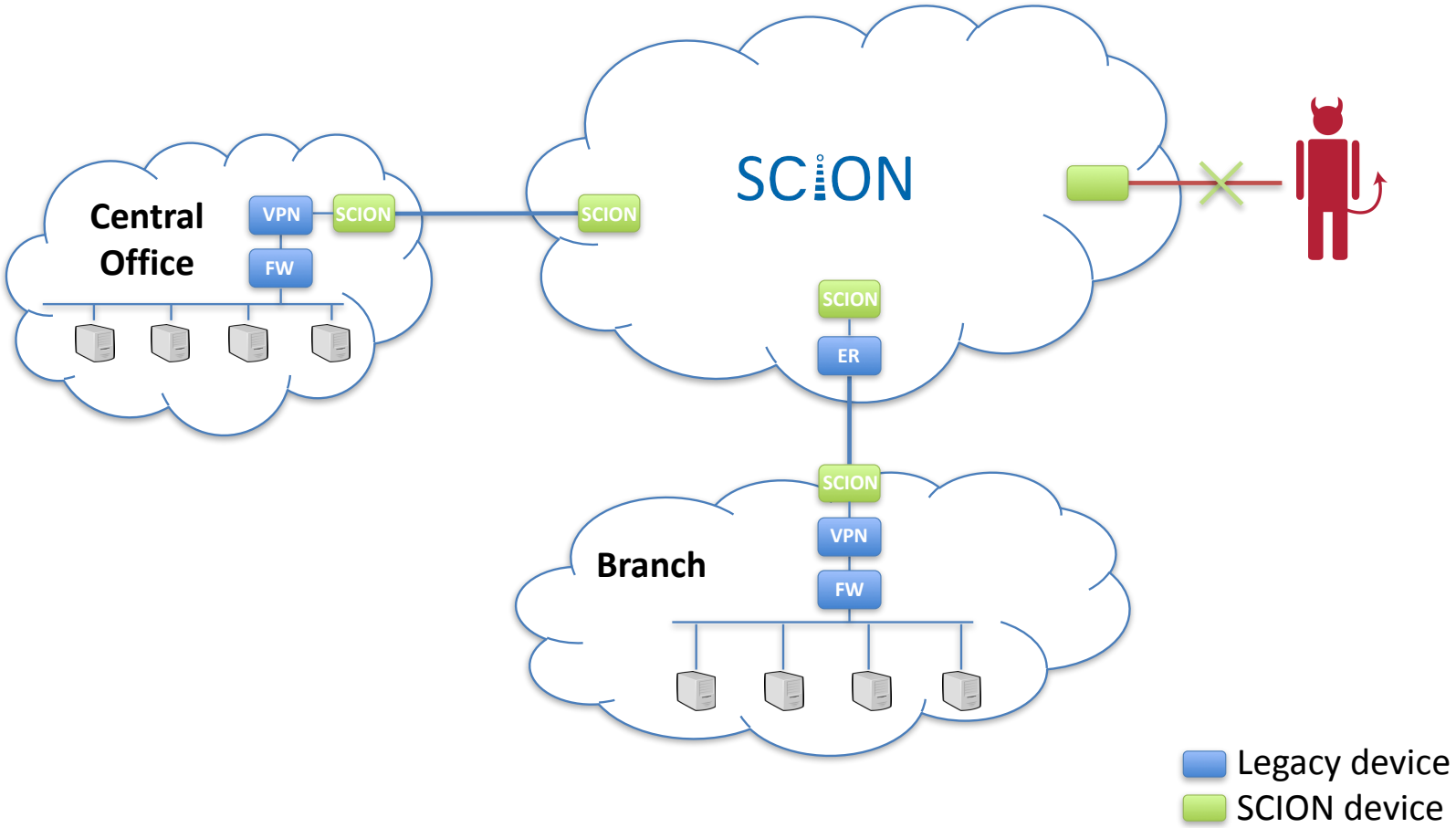
SCION

anapaya systems

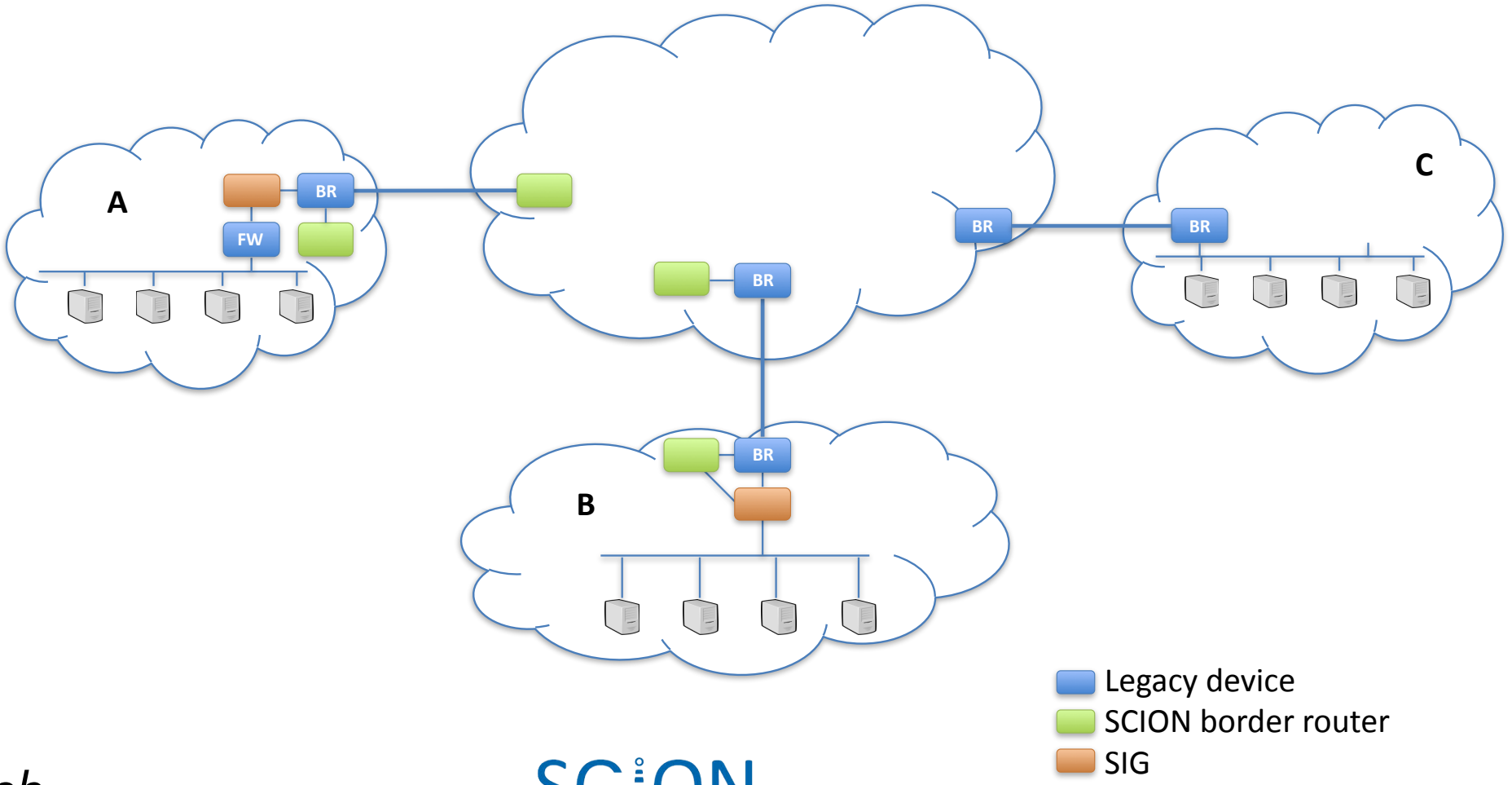
Use Case: IoT Protection through Default Off



Use Case: VPN-based Deployment



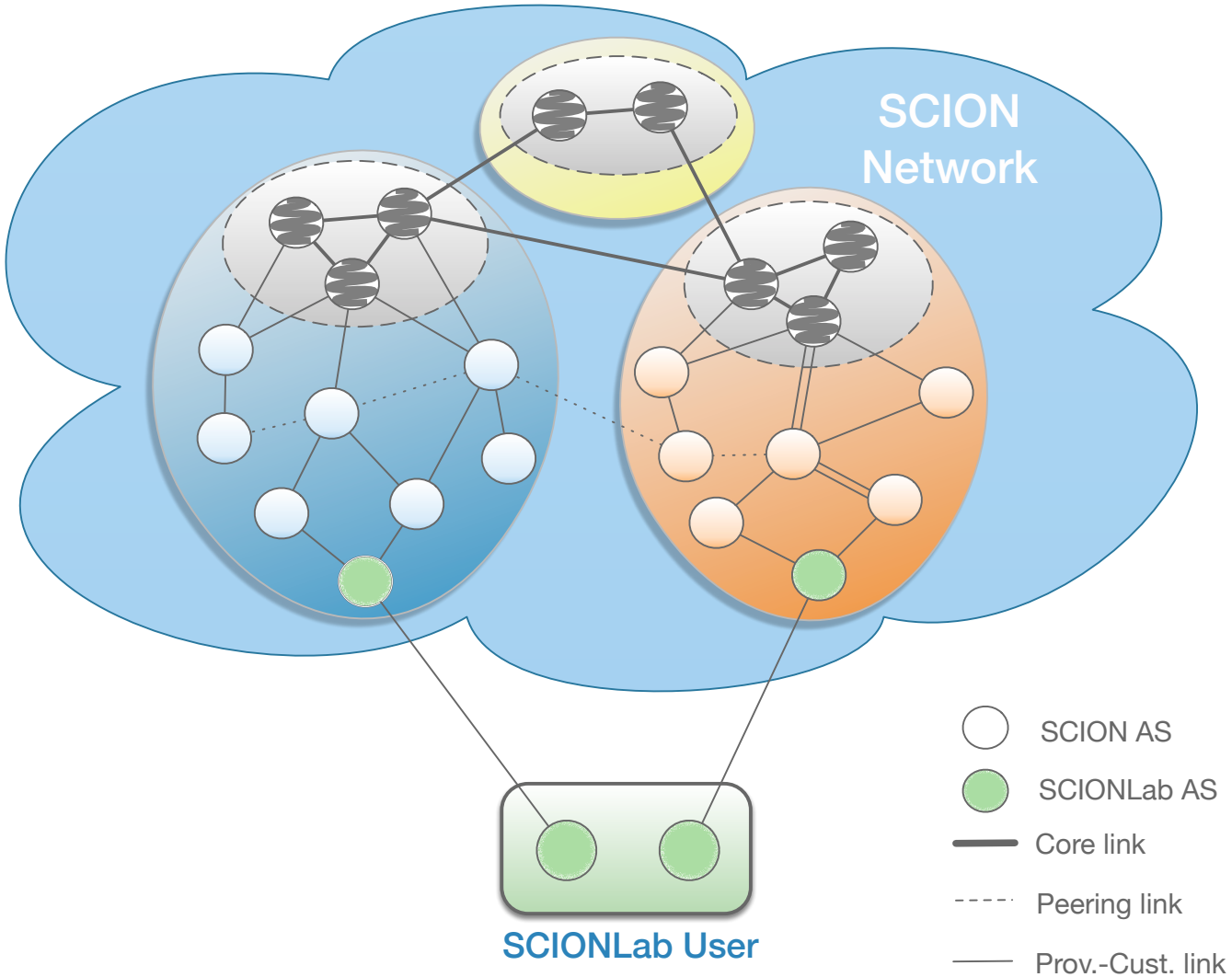
SCION-IP Gateway (SIG) Deployment



ETH zürich

SCION

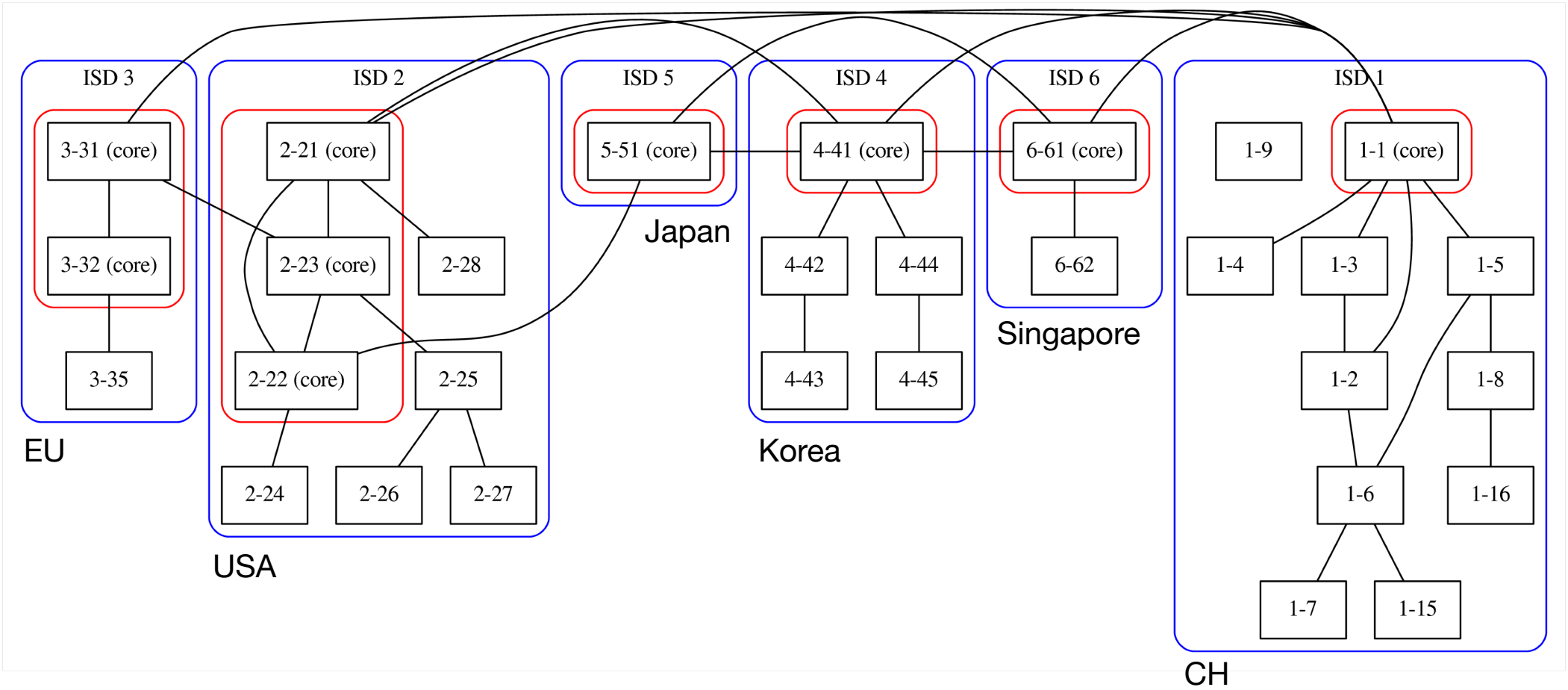
SCIONLab



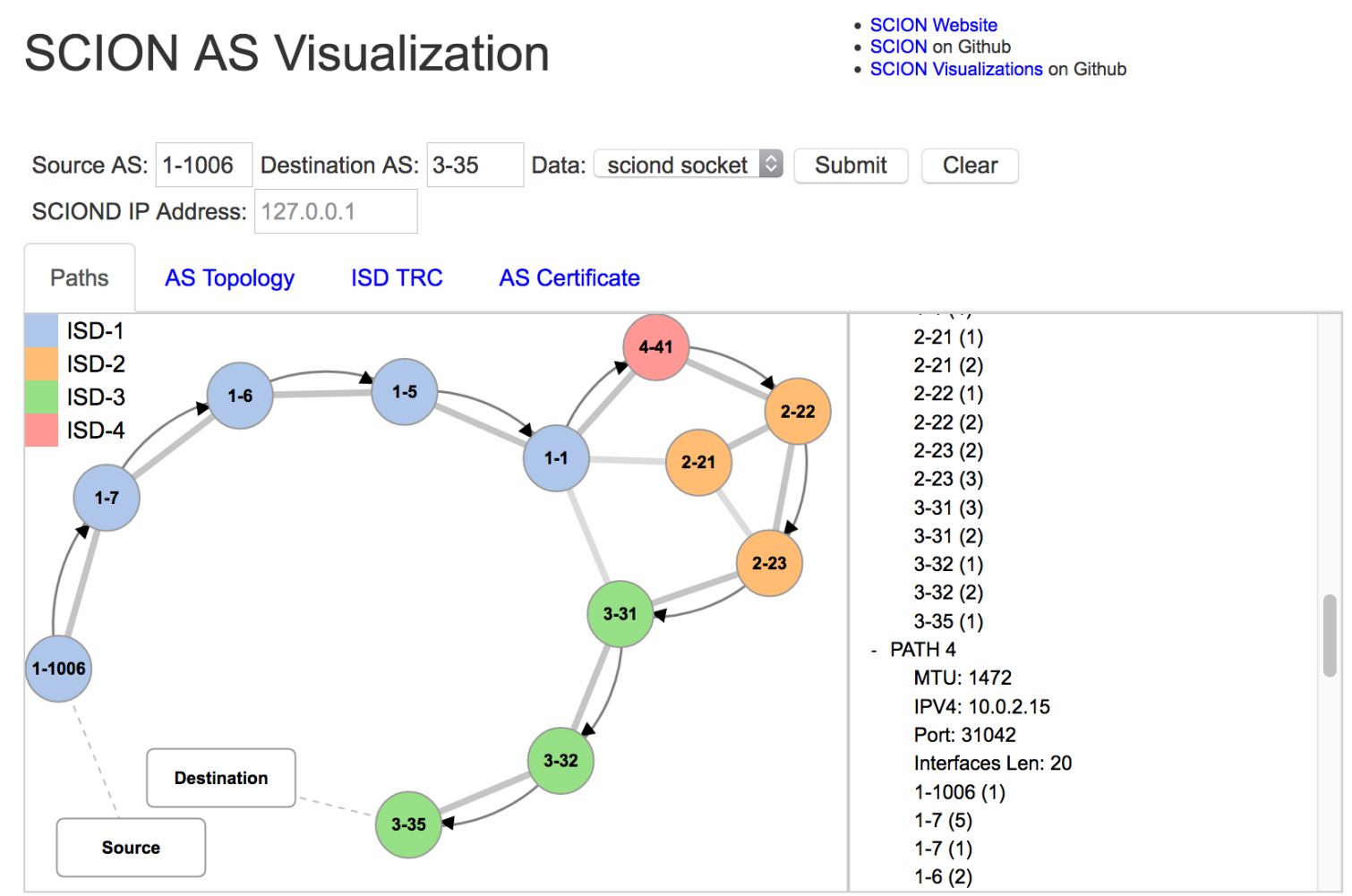
ETH zürich

anapaya systems

Global SCIONLab Network



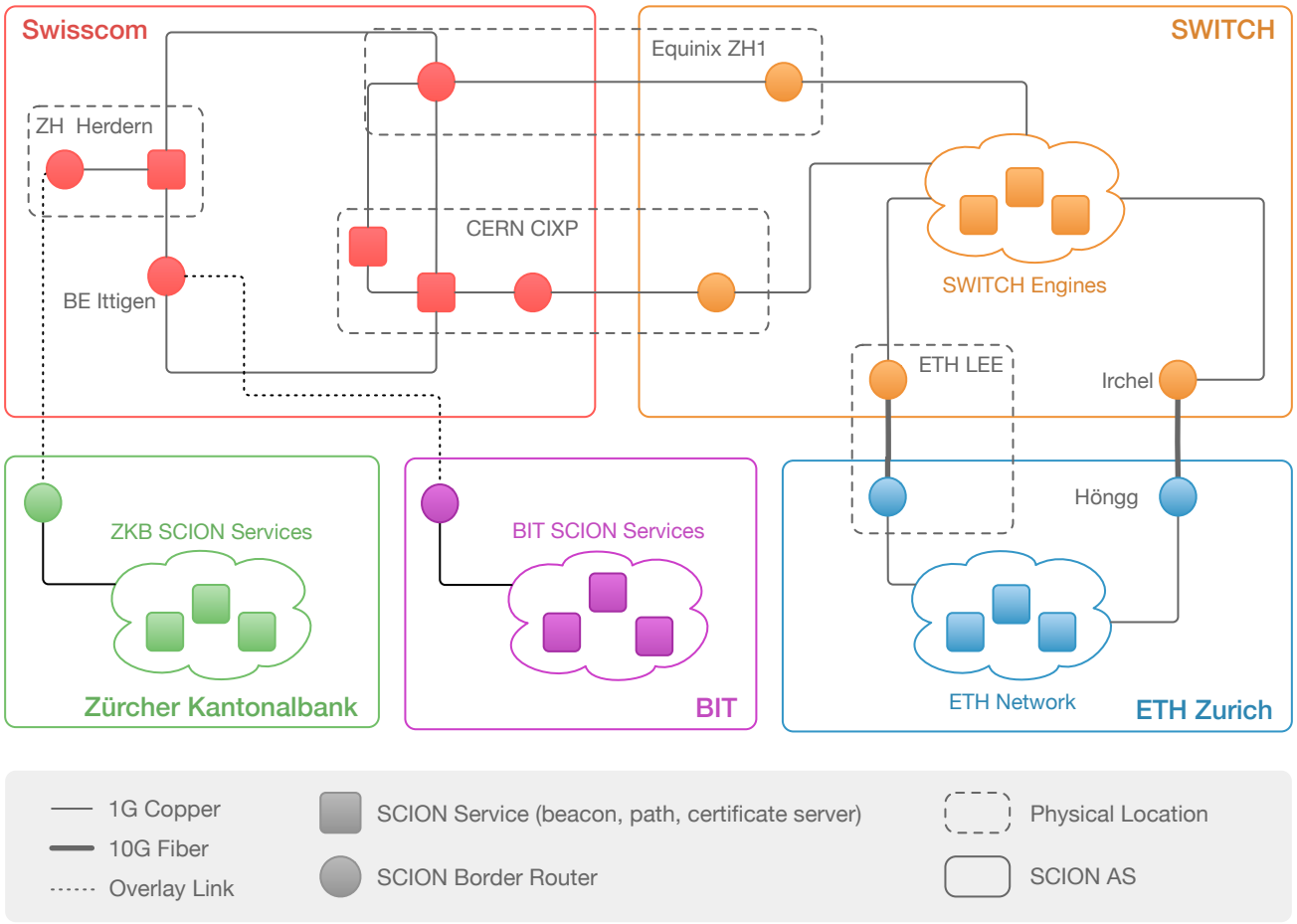
SCION Visualization System



ETH zürich

SCION

Swiss SCION Network



swisscom

SWITCH

Zürcher Kantonalbank

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

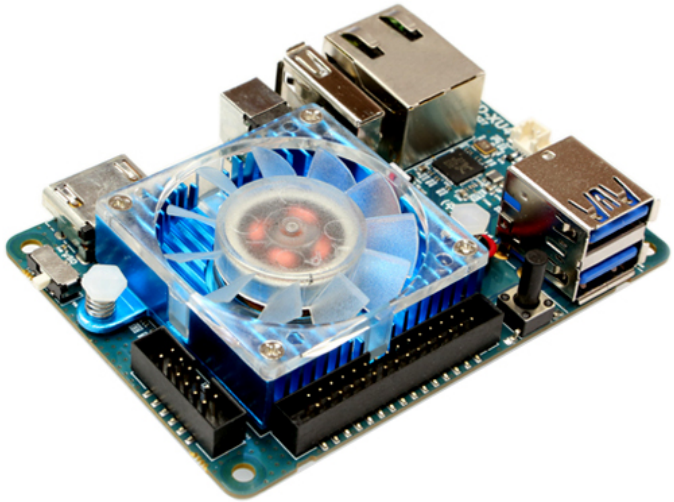
ETH zürich

SCION

anapaya systems

SCION AS runs on ODROID and Raspberry Pi

ODROID
Hardkernel



Raspberry Pi

Belief that Internet is Immutable

- Evidence appears overwhelming that Internet is immutable: IPv6, BGPSEC, DNSSEC, etc.
- However, benefits are limited, esp. for early deployers
- Our goal: provide many benefits, even for early adopters, such that one cannot turn back

Conclusions

- SCION is a secure Internet architecture that we can start using **today**
- Many use cases
  - Cost savings with replacement of leased lines
  - Business continuity: high-speed failover
  - Highly secure communication network
    - Strong defense against DDoS attacks, with communication guarantee
    - Path guarantee, attacker cannot re-route traffic
    - No external kill switches, regaining Internet Sovereignty

SCION Projekt Team

- Netsec: Daniele Asoni, Laurent Chuat, Sergiu Costea, Sam Hitz, Mike Farb, Tobias Klausmann, Jonghoon Kwon, Tae-Ho Lee, Sergio Monroy, Chris Pappas, Juan Pardo, Adrian Perrig, Benjamin Rotenberger, Stephen Shirley, Jean-Pierre Smith, Brian Trammell
- Infsec: David Basin, Tobias Klenze, Ralf Sasse, Christoph Sprenger, Thilo Weghorn
- Programming Methodology: Marco Eilers, Peter Müller

ETH zürich

SCION Commercialization

- To commercialize SCION, we have founded Anapaya Systems in June 2017
  - 4 Founders: Prof. David Basin, Sam Hitz (CEO), Prof. Peter Müller, Prof. Adrian Perrig
- We already have several bank and ISP customers
- We are starting to seek investors
- Visit us at: **www.anapaya.net**

Additional Information

- https://www.scion-architecture.net
  - Book
  - Papers
  - Videos
  - Tutorials
  - Newsletter signup
- https://www.anapaya.net
  - Commercializing SCION equipment
- https://github.com/scionproto/scion
  - Source code