

2STIC

# Experimenting with the SCION Internet architecture

Lisa Bruder, Ralph Koning (SIDN Labs)  
Advanced Networking Guest Lecture, UvA/OS3  
Feb 20, 2026

# SIDN is the operator of the .nl TLD

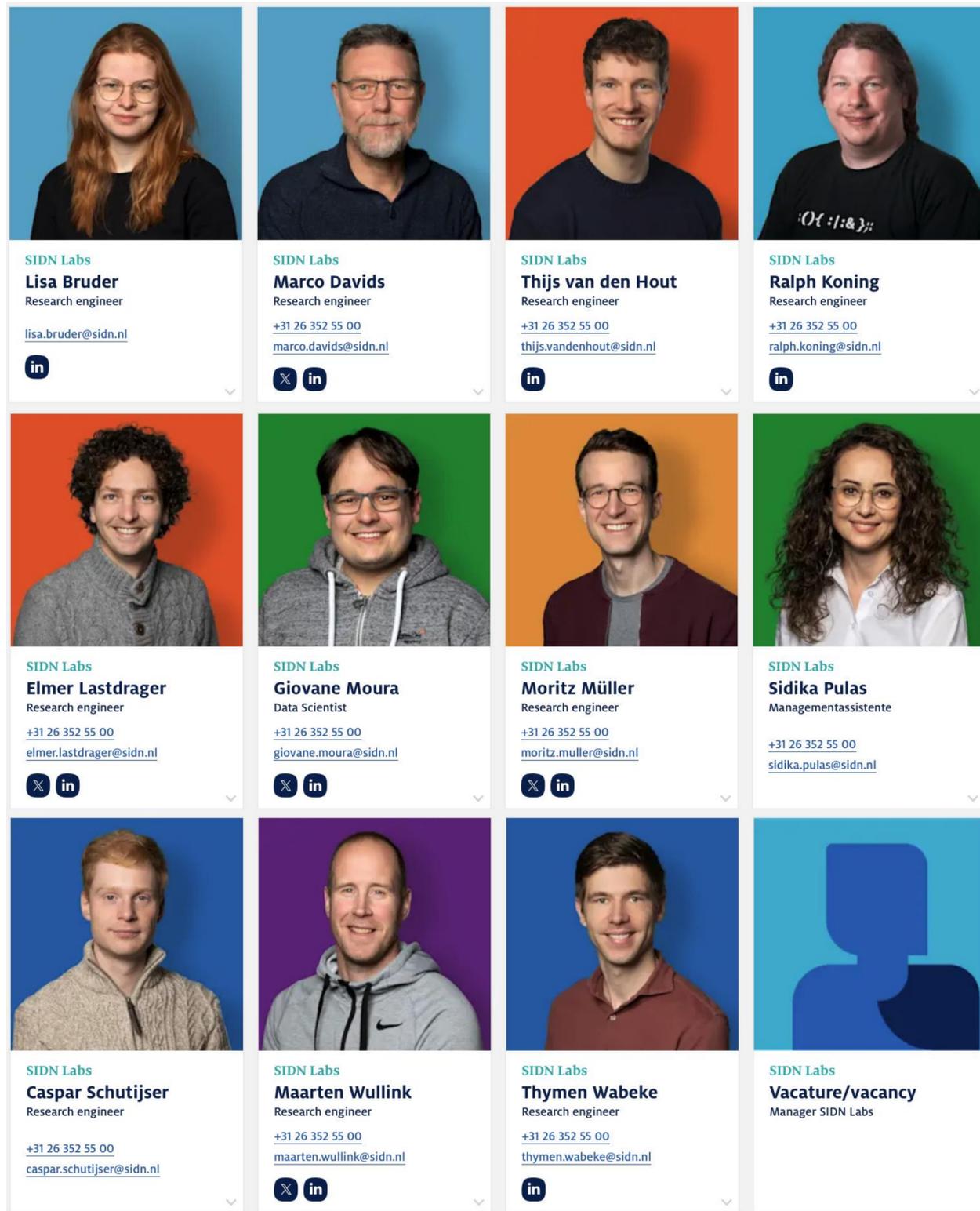
- **Objective:** increase society's confidence in the Internet
- Provide secure and fault-tolerant registry services for .nl
  - Anycasted DNS services with DNSSEC support
  - Registration and domain protection services
- Increase the value of the Internet in the Netherlands and elsewhere
  - Enable safe and novel uses (SIDN Fonds, Yivi/IRMA)
  - Increase infrastructure security and trustworthiness (SIDN Labs)



## **.nl = the Netherlands**

18M inhabitants  
6.1M domain names  
3.8M DNSSEC-signed  
4.0B DNS queries/day  
8.6B NTP queries/day

# SIDN Labs: team



## Goal:

increase security of the Internet infrastructure, special focus on .nl and the Netherlands

## Themes:

1. domain name security
2. infrastructure security
3. *emerging Internet technologies (long term)*

## Applied technical research:

1. large-scale measurements
2. system design
3. prototyping and evaluation
4. standards

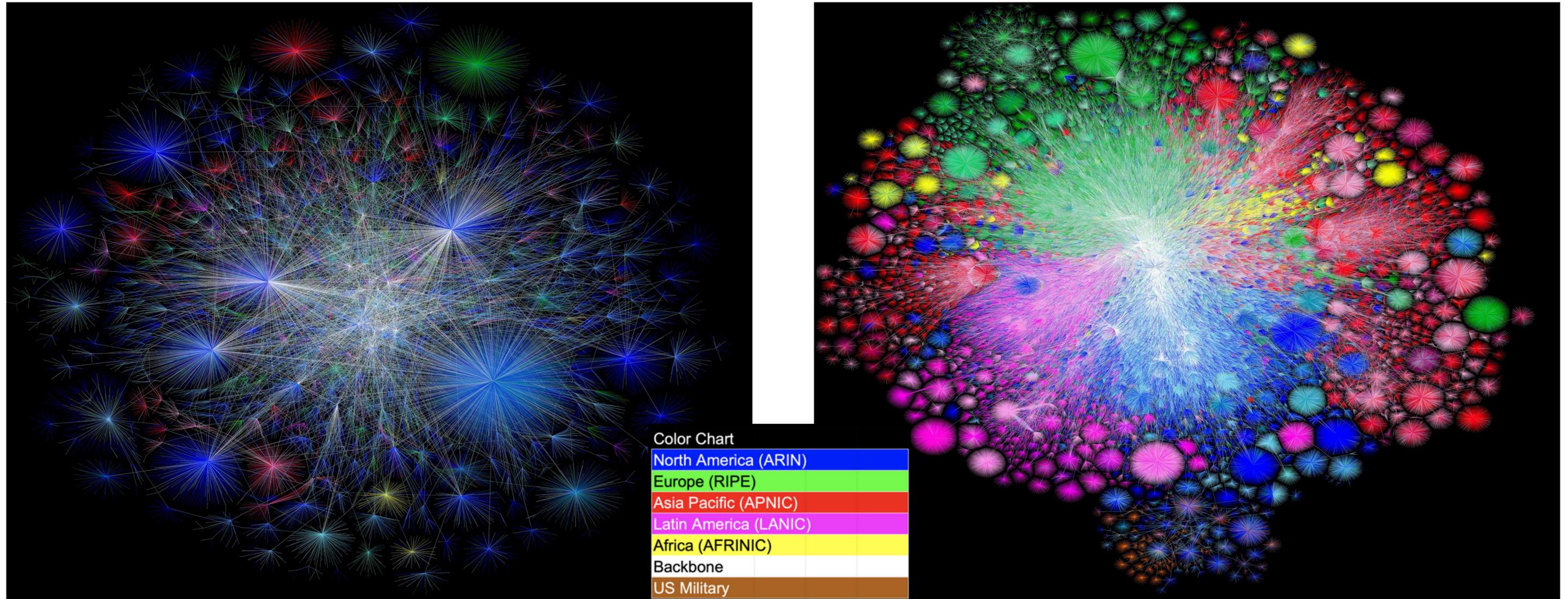


# 2STiC program

Goal: put Dutch and European internet communities in a leading position in the field of secure, stable and transparent inter-network communication



# The Internet

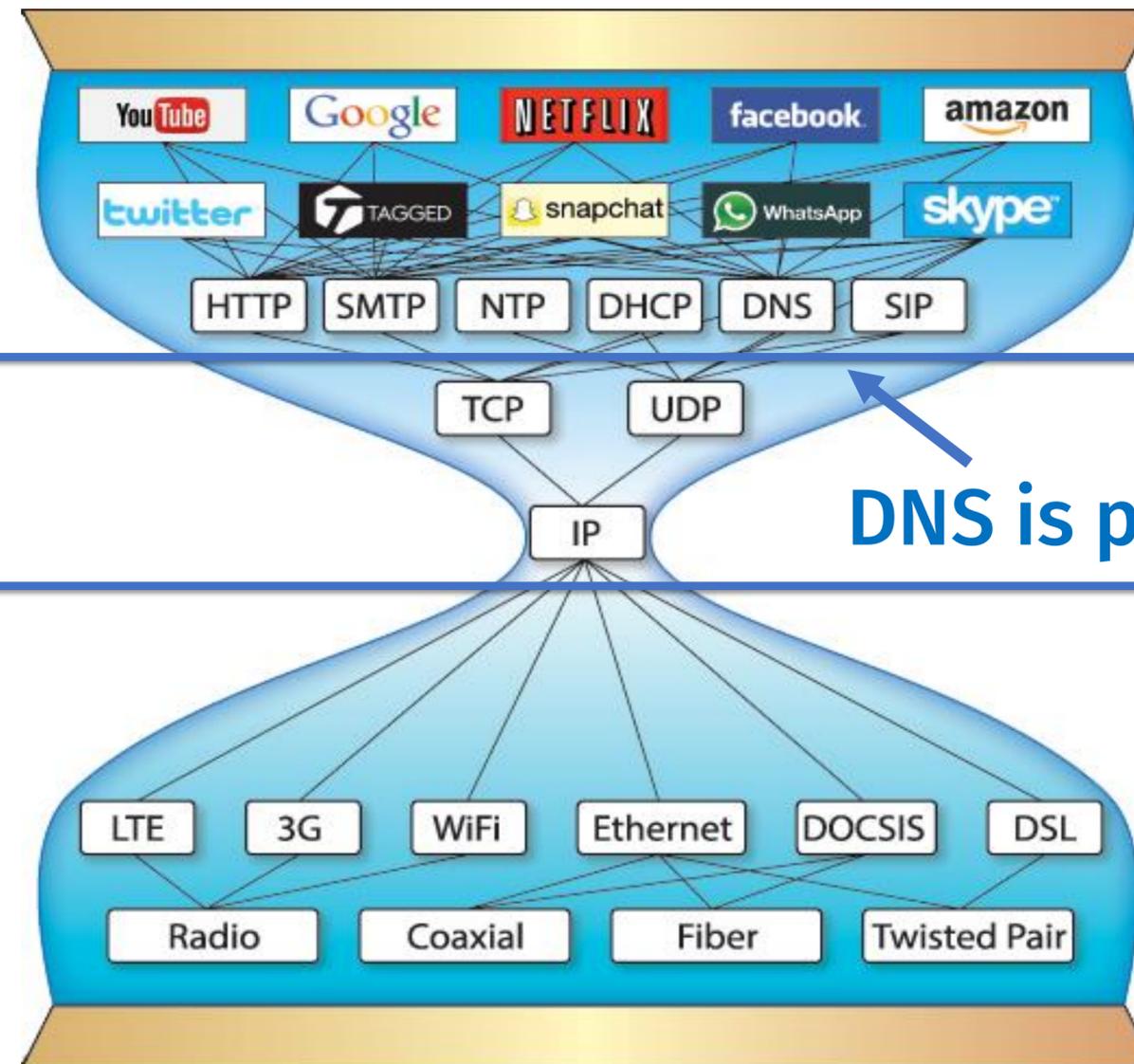


1997

2021

# Rate of change

Fast



Slow!

DNS is pretty slow too

Fast

# New Requirements

- New applications have new **security, stability** and **transparency** requirements
  - More interaction with physical space (e.g., transport, smart grids, drones, remote surgery)
- To provide **trust** and **confidence** in communication we need a **responsible** internet
  - Control over routing and verification of operational behavior
  - Agreements on how to use certain parts of the infrastructure.

SCION  
NDN  
RINA  
ManyNets  
XIA  
MobilityFirst  
Nebula  
Service-centric networking  
FII  
B4  
...

Some new inter-domain  
networked architectures

# Opening up

- Adoption of new protocols in technologies was slow, but network devices are opening up.
- (Onie) Open Network Install Environment offers OS choice on network equipment.
- OpenFlow/SDN offer control plane programmability.
- P4 provides dataplane programmability.

# Potentially promising clean slate architectures

- RINA
  - Everything is IPC (Inter-Process Communication)
  - WIP implementations: ProtoRINA, OpenIRATI
- NDN
  - Data centric
  - Stateful, lots of caching in the network
  - Implementation: [named-data.net](http://named-data.net)
- Extensible Internet
  - Introduces layer 3.5
  - No implementation yet
- **SCION**
  - **Path selection**
  - **Active community**
  - **Implementation: [github.com/scionproto](https://github.com/scionproto)**

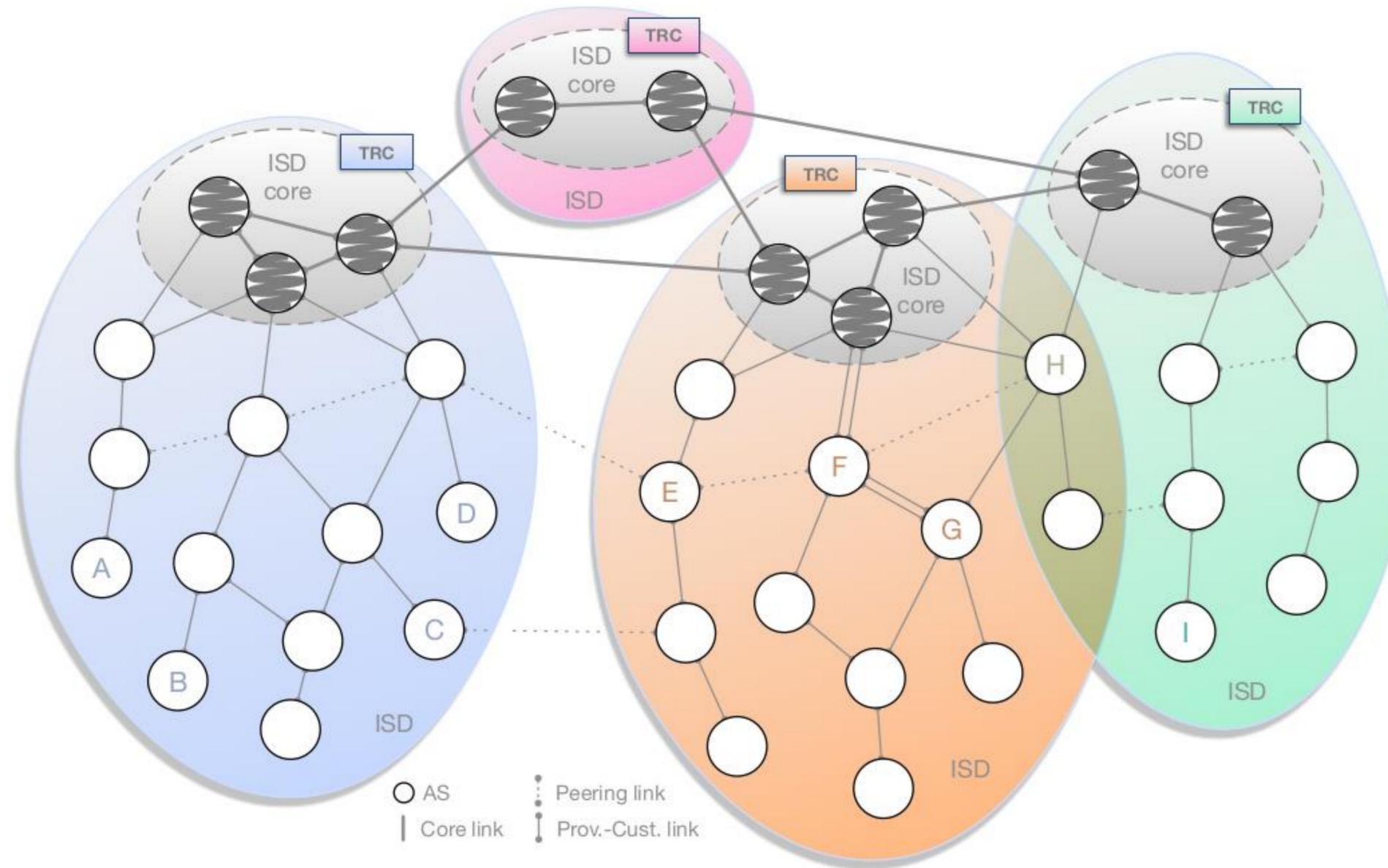
2STIC

SCION

# SCION

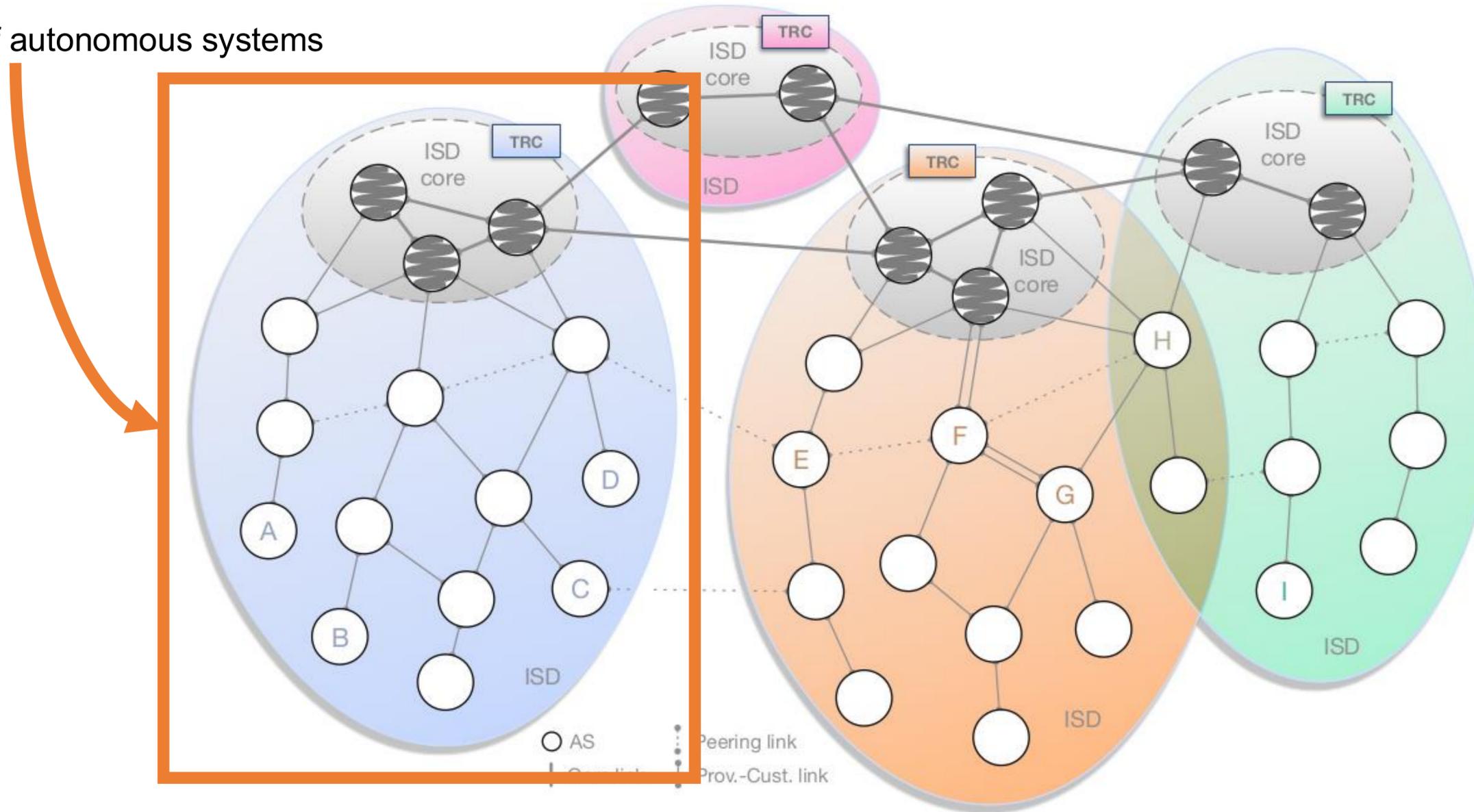
- “**Scalability, Control, and Isolation On Next-generation Networks**”
- Developed by Network Security Group, ETH Zurich
- **Goal:** improve security of inter-domain routing and isolation of compromise
  - Security by design
  - Path-aware networking (Sender selects path)
  - Multi-path communication
  - Existing application can still be used

# Isolation domains



# Isolation domains

ISD: Group of autonomous systems

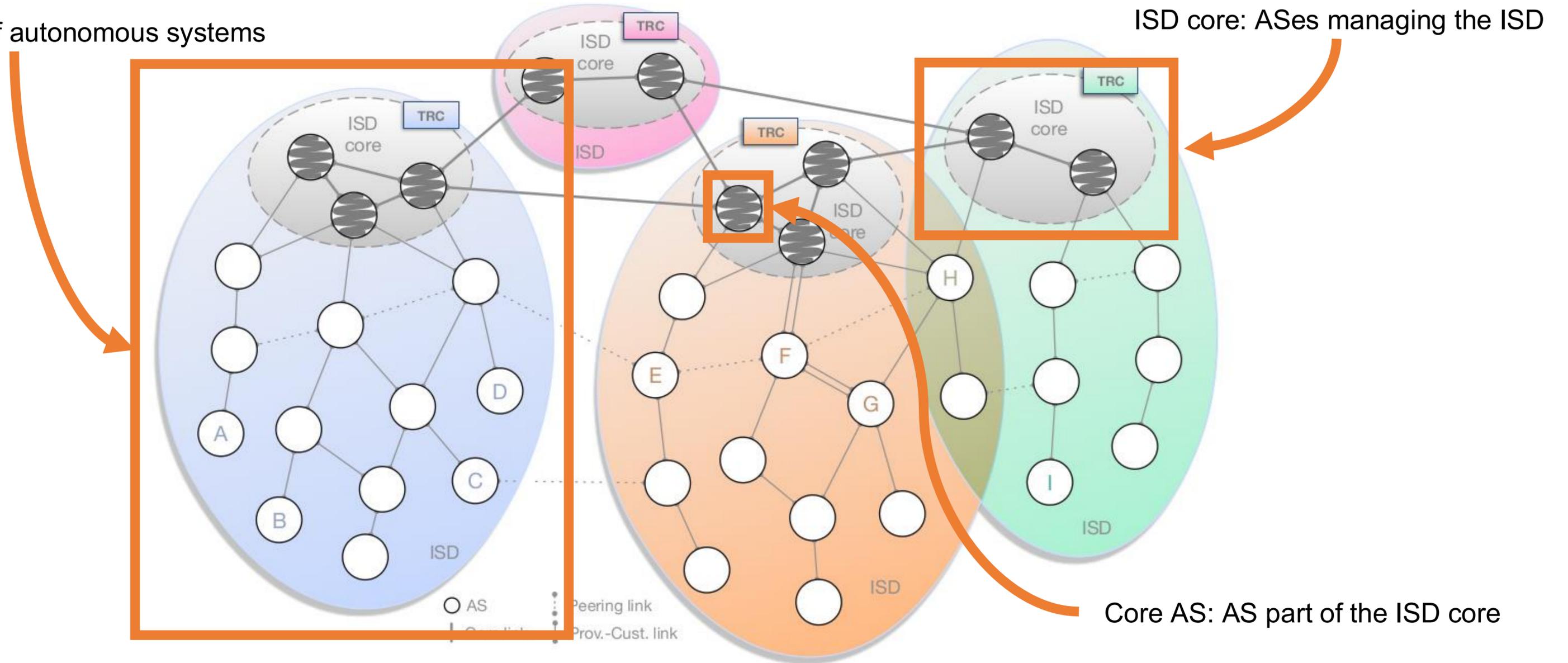




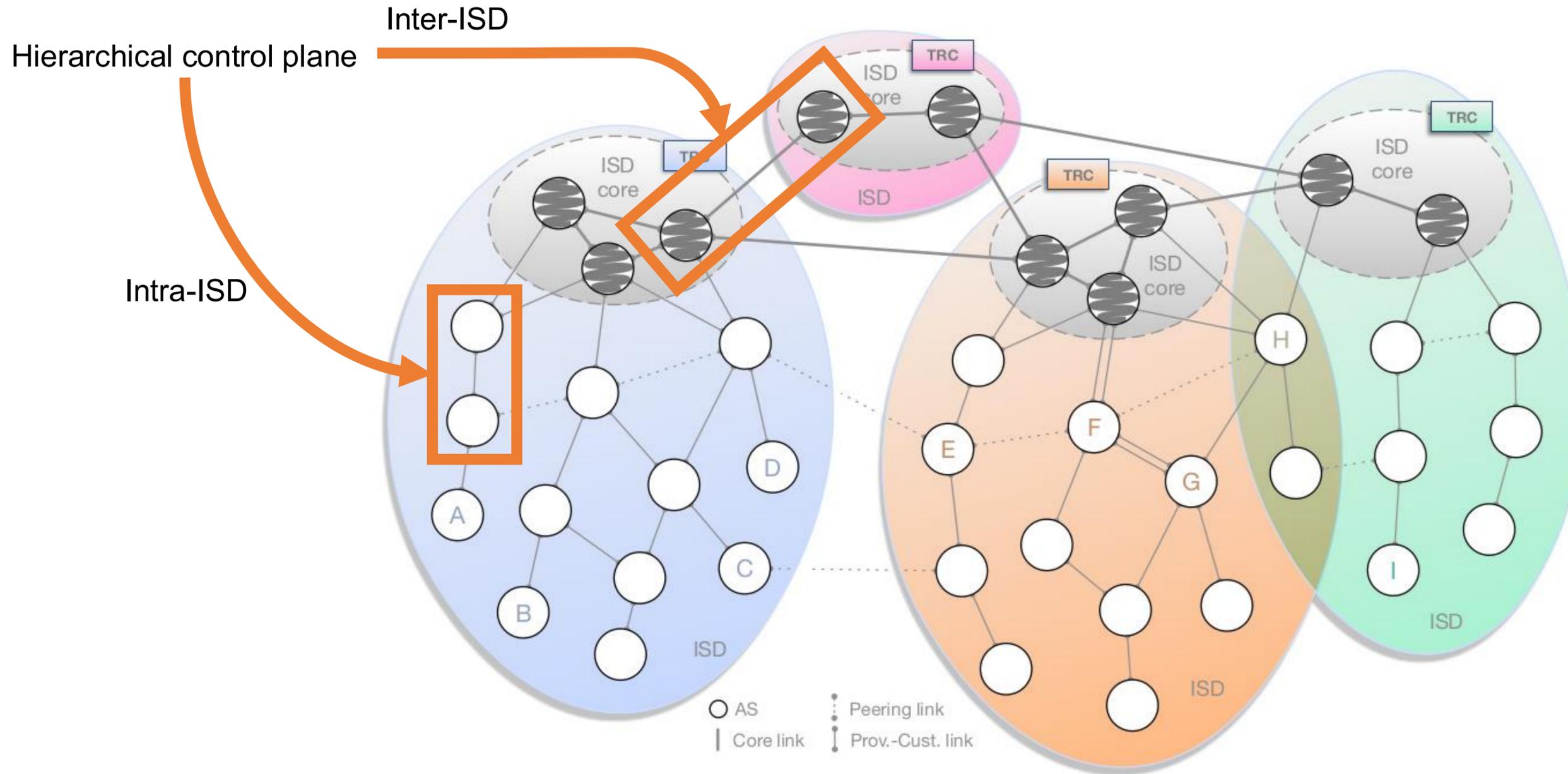
# Isolation domains

ISD: Group of autonomous systems

ISD core: ASes managing the ISD



# Isolation domains



# ISD and AS numbering

## **ISD-AS, address**

16-bit identifier (decimal)

# ISO and AS numbering

48-bit (hexadecimal)

**73-AS, address**

# ISO and AS numbering

or decimal if  $\leq 32$  bits



48-bit (hexadecimal)

**73-0:3:4830, address**

# ISD and AS numbering

**73-215088, address**

does not need to be globally unique!

# ISO and AS numbering

73-215088, 127.0.0.1

# ISD and AS numbering

73-215088, ::1

# Routing: overview

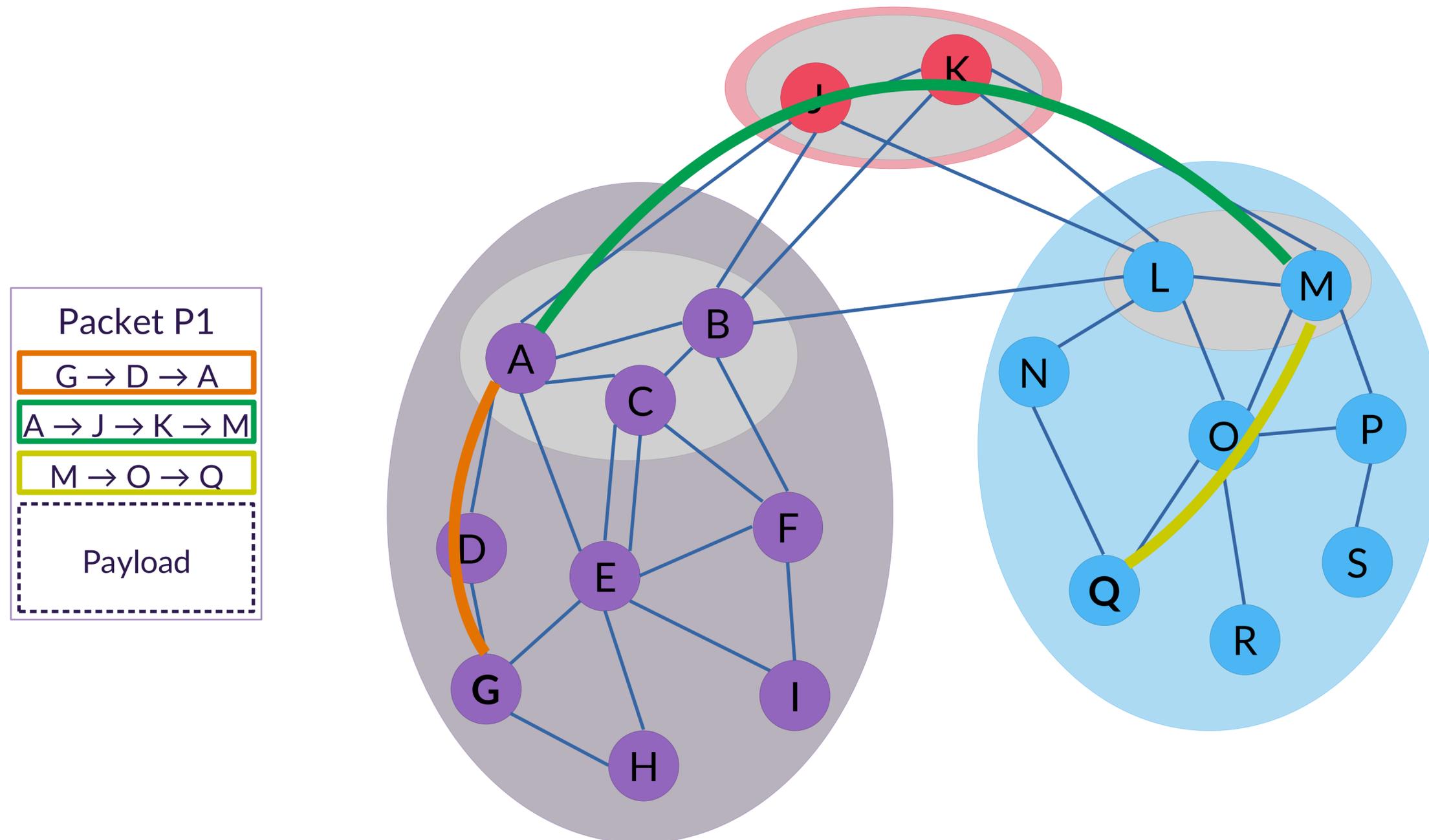
## Control plane

- Construct and disseminate path segments

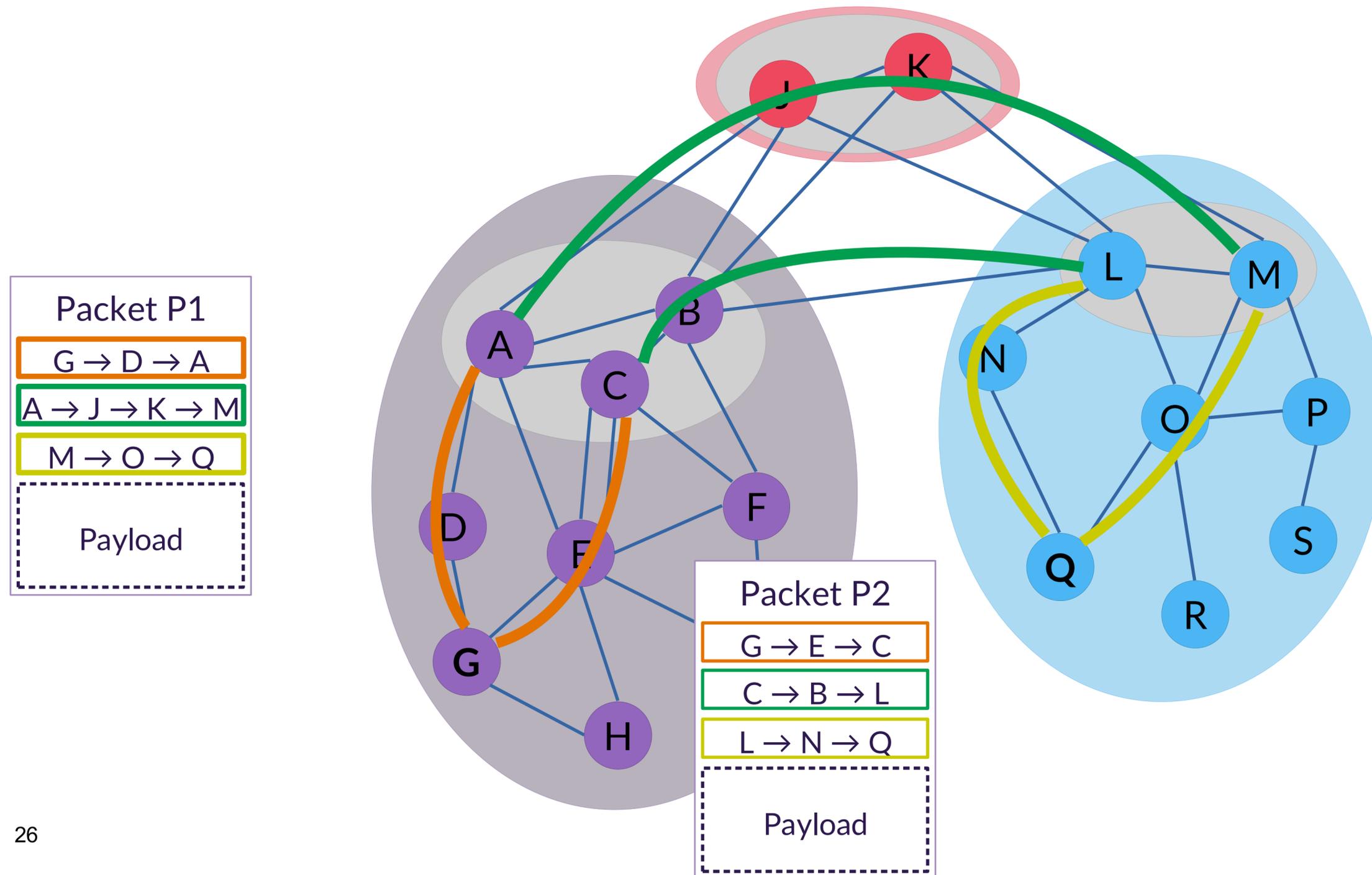
## Data plane

- Combine path segments to path
- Packets contain path
- Routers forward packets based on path (stateless)

# Data Plane: Segments



# Data Plane: Path combination



# Control plane: path exploration

## Inter-ISD

- Performed by Core ASes
- Flooding similar to BGP
- Less ASes involved (only core)

## Intra-ISD

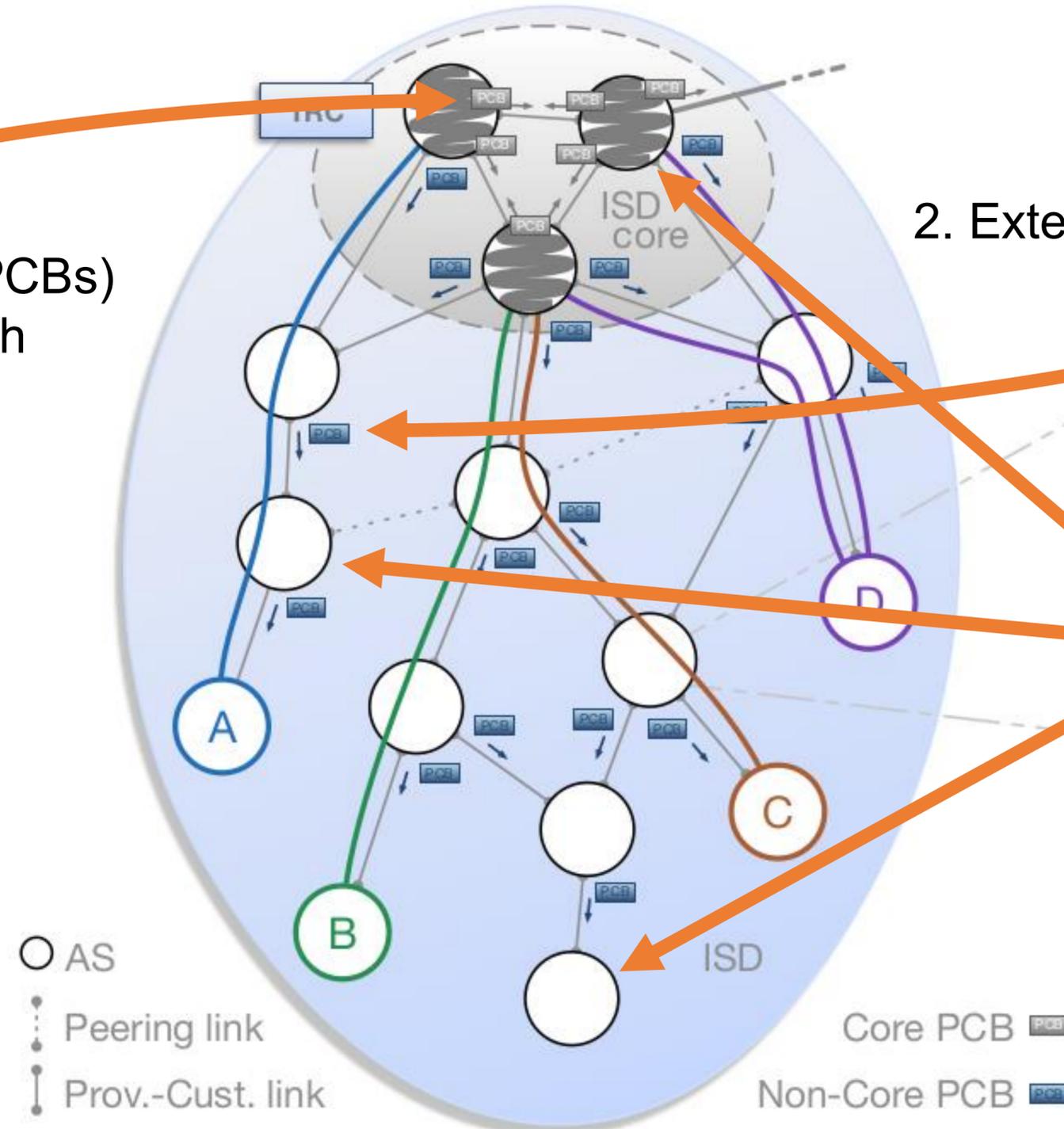
- Downstream multi-path flooding

# Control plane: Intra-ISD path exploration

1. Path Construction Beacons (PCBs) sent downstream using multi-path flooding

2. Extended and forwarded by other ASes

3. Path registration



# Routing: policies

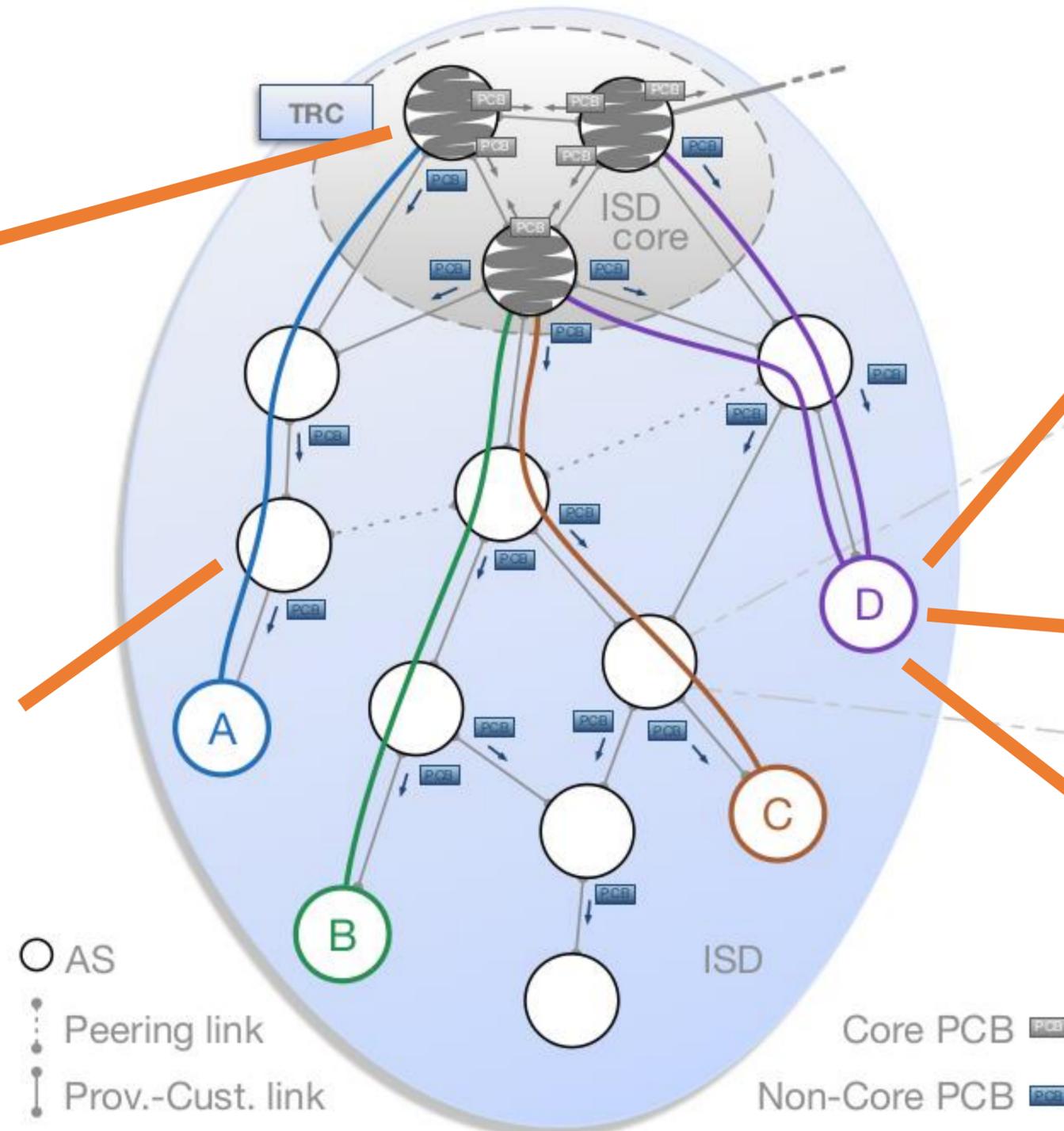
**Core AS:**  
What do I offer to the local path server of this AS?

**Up-stream AS:**  
To where do I forward the received PCBs?

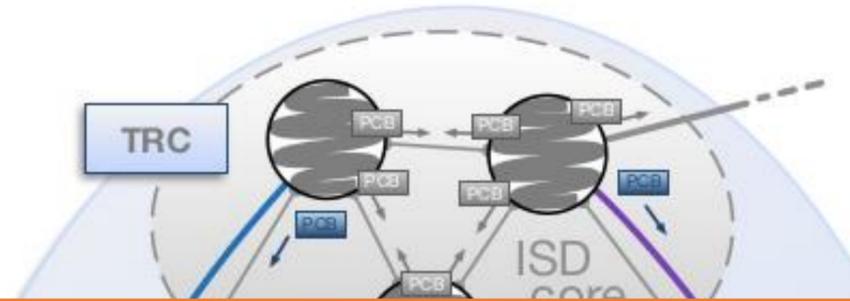
**Local AS:**  
Which down-path segments do I offer to the ISD core?

**Local AS:**  
Which path segments do I offer to my clients?

**Client:**  
How do I combine segments offered by the local path server?

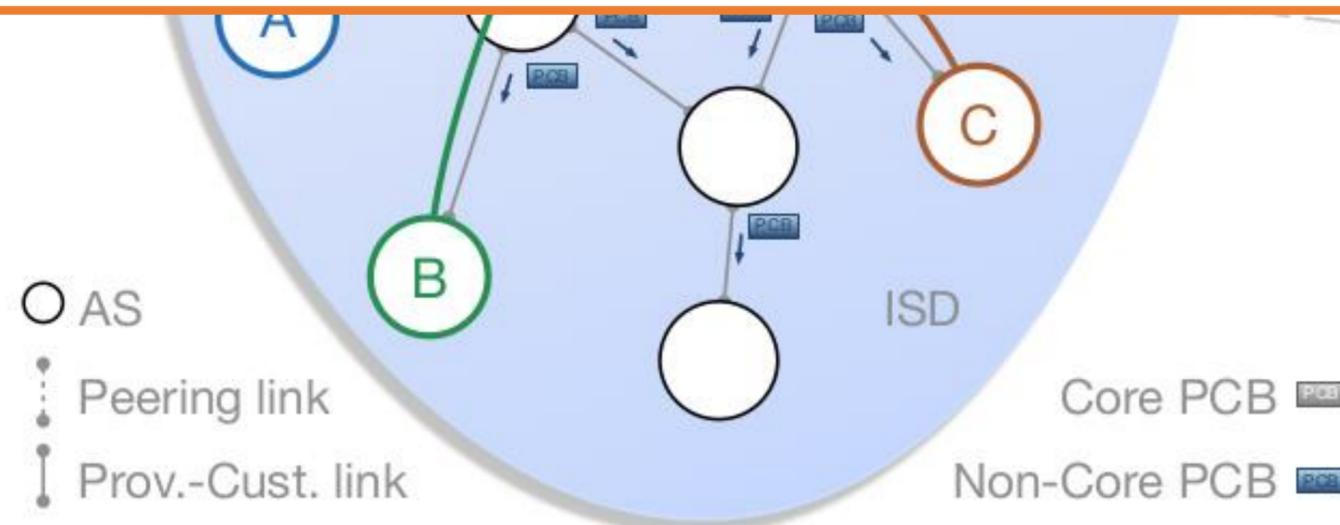


# Routing: policies



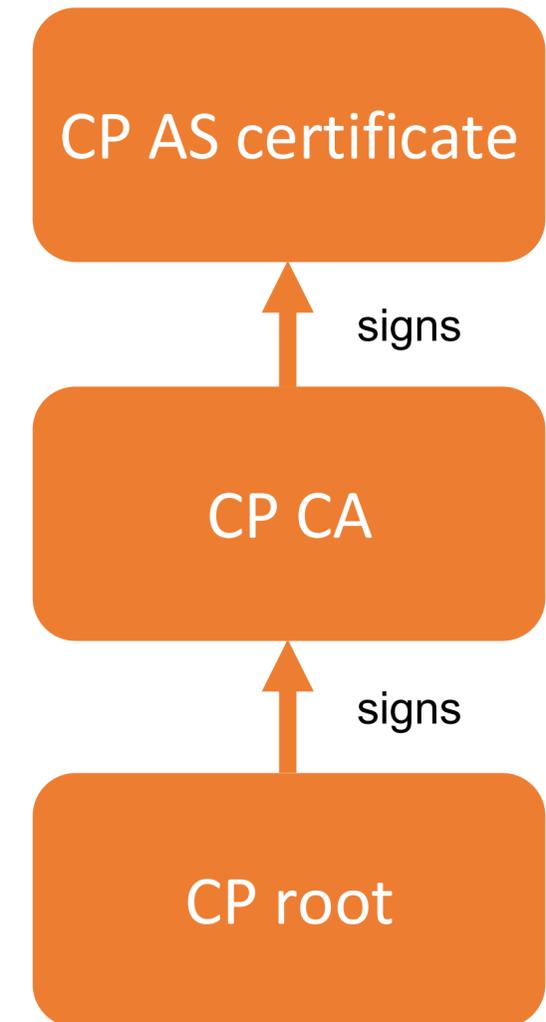
More on routing policies: RP report “**A Comparative Analysis of Routing Policies in BGP and SCION by Kaj Koole, Martyna Pawlus, (2023).**”

[https://2stic.nl/downloads/routing\\_policies\\_koole\\_pawlus.pdf](https://2stic.nl/downloads/routing_policies_koole_pawlus.pdf)



# Cryptography

- PCBs are signed by every AS along the path
- ISD's CA is responsible for issuing certificates for all ASes
- CP root key is embedded in the **Trust Root Configuration (TRC)**



# TRC

Signed collection of

- CP root and voting certificates and
- ISD policy information (defines roles within the ISD)

# Routing summary

- Path information included in packet headers
- Sender selects the path
- Recipient address no longer used to route between autonomous systems

# Security

- Path information authenticated in control plane and data plane
- Control plane
  - Beacons authenticated using digital signatures
  - No route hijacks
- Data plane
  - User combines authenticated path segments from the control plane
  - Hop fields in path are authenticated through a cryptographic Message Authentication Code (MAC)

# Security

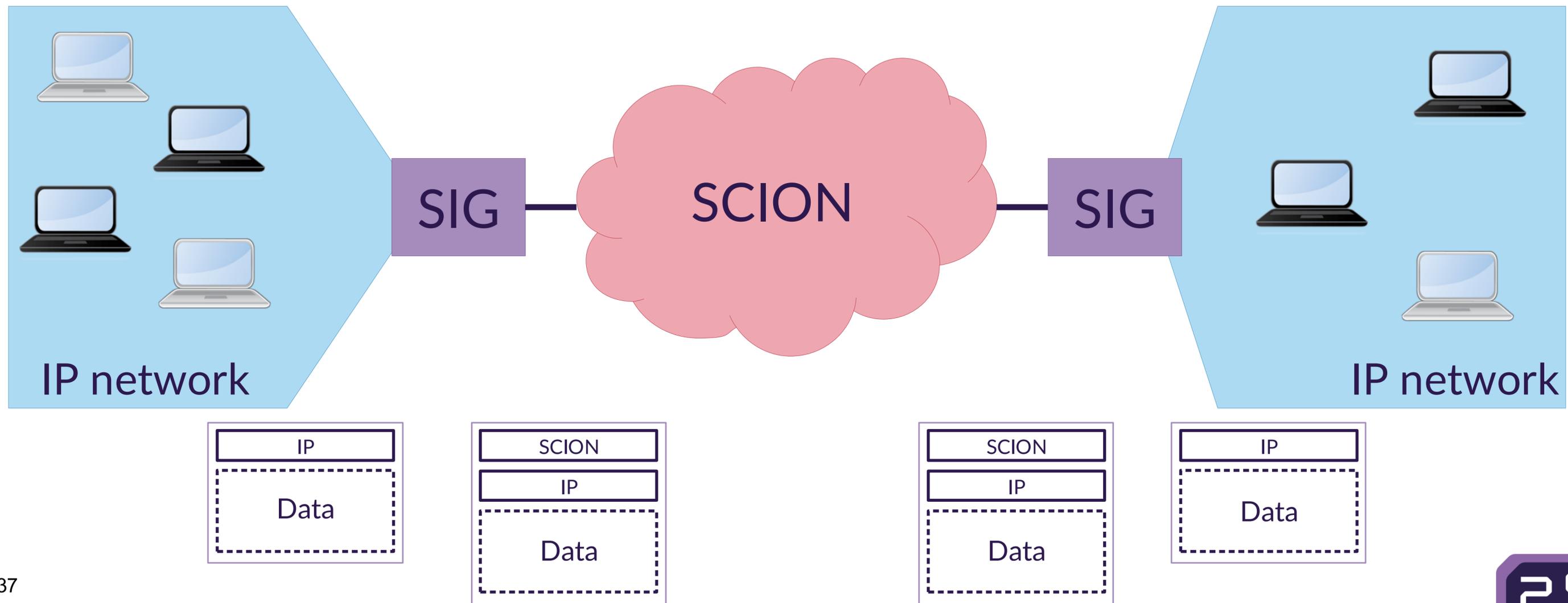
- Address spoofing no longer possible on AS-level
  - Protects against reflection attacks
  - Reduces impact of DDoS attacks
- Hidden paths
  - Path information not published
  - Can only be used by parties that know the relevant hop fields
- EPIC (Every Packet Is Checked) is a data plane extension that offers additional security and transparency

# Reliability and QoS

- Redundancy through use of multi-path communication
- Fast failover in case of link failure
  - No waiting for convergence
- Possible to add latency information to beacons
  - Path selection based on latency
- Hummingbird extension
  - Minimum bandwidth reservation

# Transitioning to SCION

Can be combined with existing applications using SCION-IP Gateway (SIG)

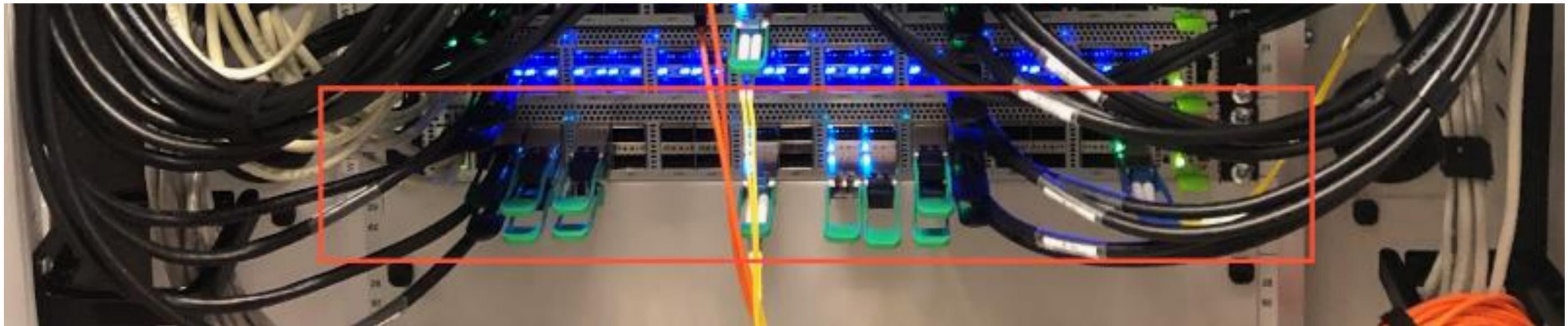


2STIC

Project: SCION in P4

# A new internet architecture in P4

- We implemented the SCION internet architecture in P4 for the Intel Tofino
- Determine feasibility of running a new architecture on switch hardware and evaluate performance



# P4

“Programming Protocol-independent Packet Processors (P4) is a domain-specific language for network devices, specifying how data plane devices (switches, NICs, routers, filters, etc.) process packets.”

Source: [www.p4.org](http://www.p4.org)

# Intel Tofino

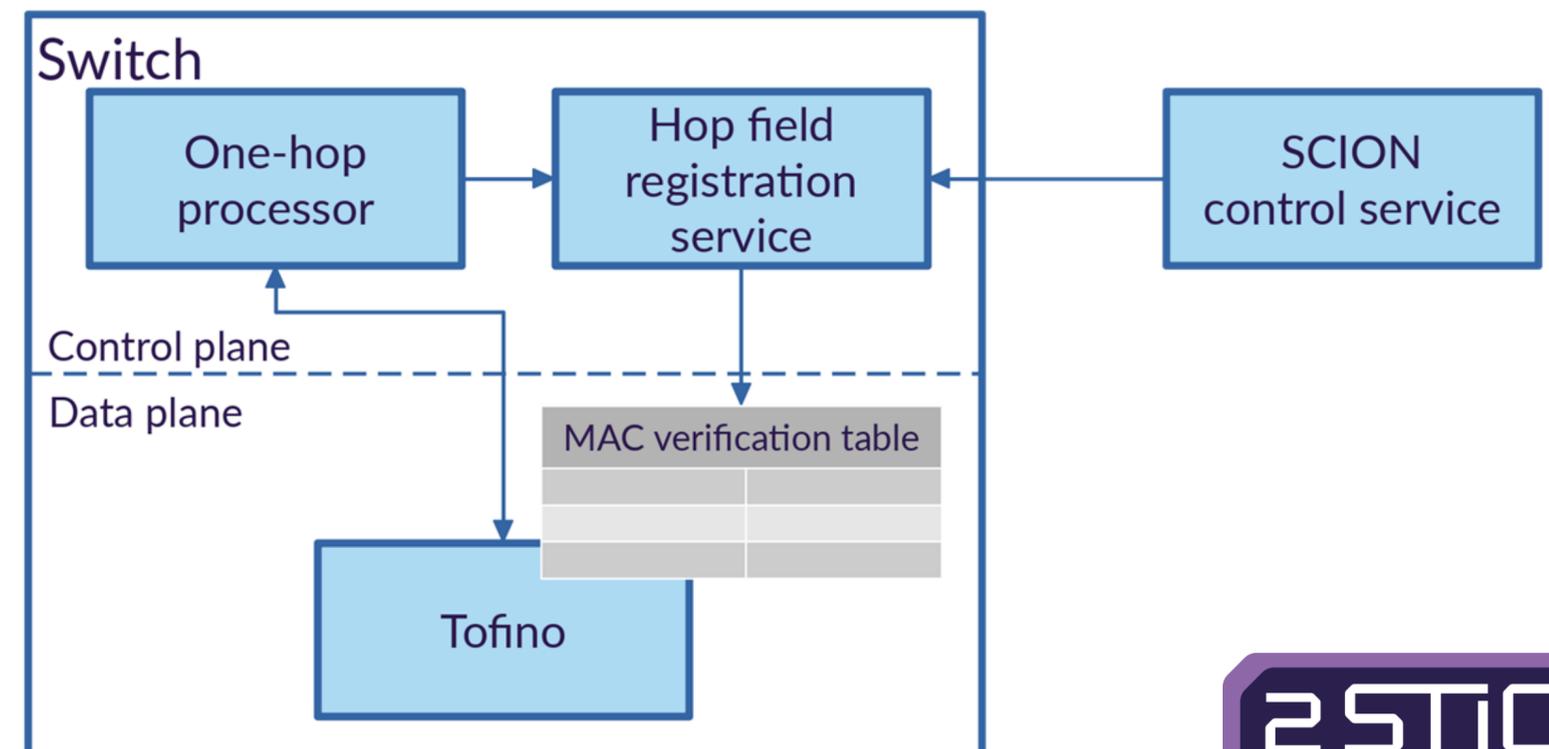
- P4-programmable Ethernet switch ASIC
- Switches available with e.g., 32 or 64 100 Gbit/sec ports

# Some challenges

- No support for cryptographic operations in Intel Tofino
- Protocol not designed for hardware
  - Complex headers

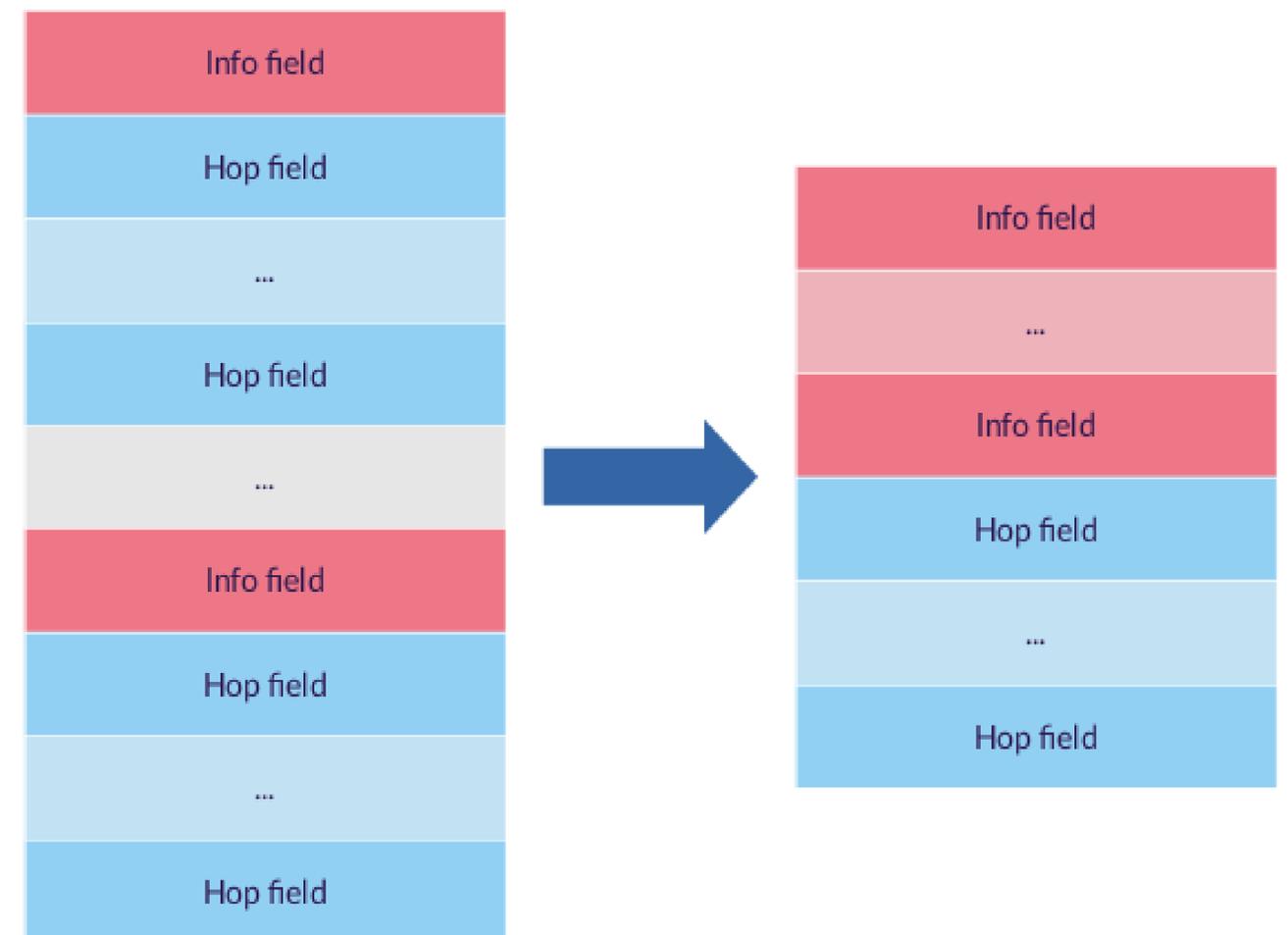
# No cryptographic operations

- MACs verified using table containing all currently valid values
- Populated from control plane when MACs are generated
  - In the SCION control plane
  - At the switch
- Invalid entries removed



# Complex header fields

- For example: forwarding path consisted of nested lists
- Flattening the structure provides for more efficient parsing

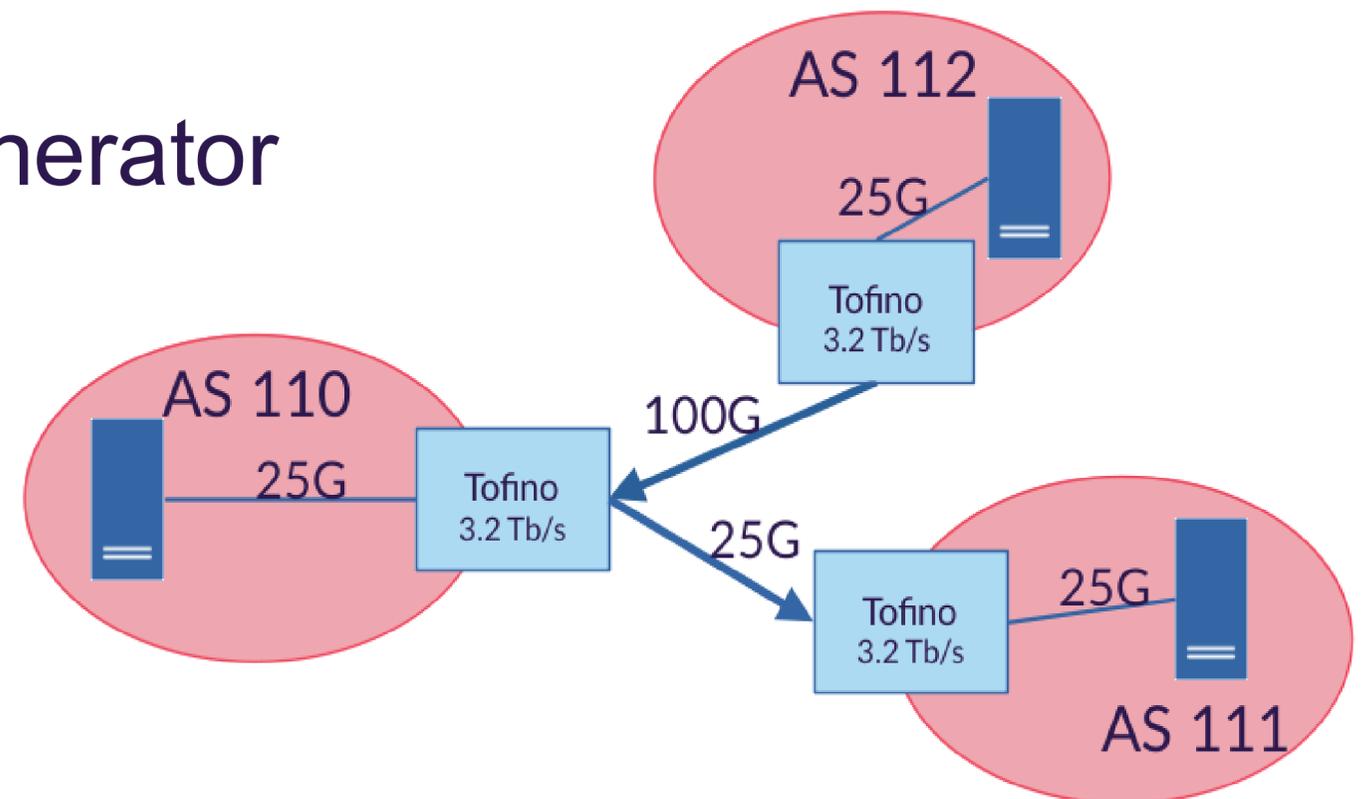


# Lessons learned

- When designing a protocol with hardware in mind
  - use explicit lengths
  - do not use absolute offsets
  - limit the usage of variable length fields
  - do not use complex data structures such as nested lists

# Evaluation

- Edgecore switches with 32 100 Gbps ports
- Tested functionality with topology where all border routers ran on switches
- Tested performance using packet generator for different path lengths
- Achieved near line-rate for almost all tested path lengths



# Conclusion

- SCION can be implemented for switch hardware and run on high speeds
- Several lessons learned regarding protocol design
- Code is open source and available at [github.com/SIDN/p4-scion](https://github.com/SIDN/p4-scion)
- Netsys Lab continued developing it for Intel Tofino 2: <https://github.com/netsys-lab/scion-p4>

2STIC

# Deployments and Apps

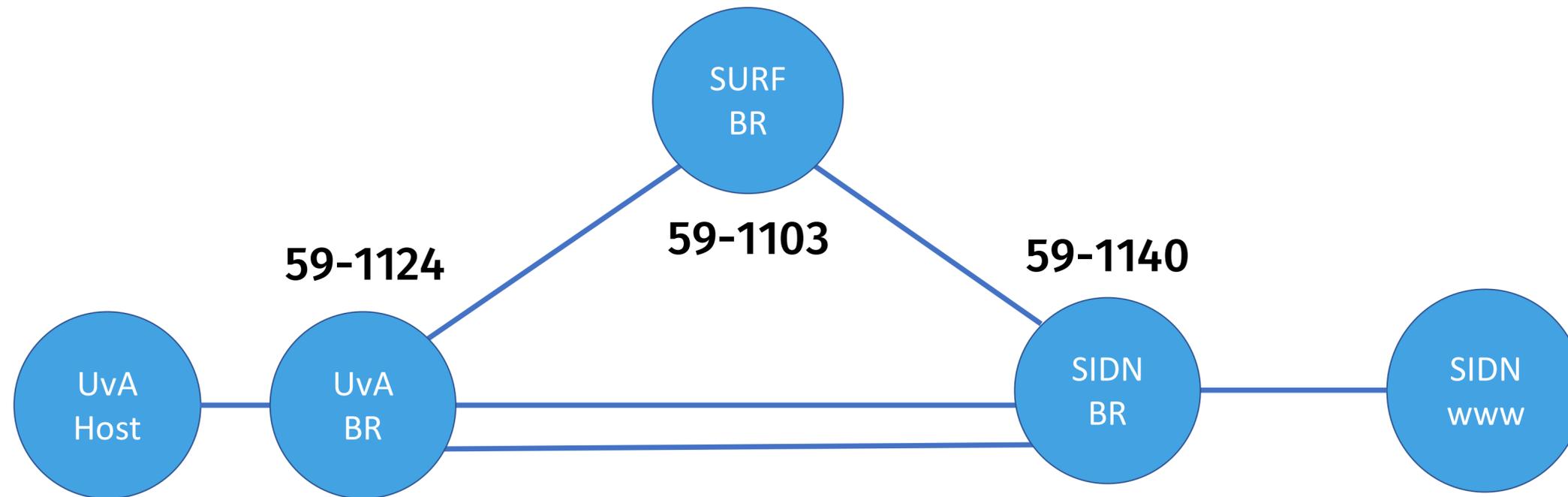
# Using SCION

- Open-source implementation of SCION:  
<https://github.com/scionproto/scion>
- Contains code for 7 binaries (router, control, dispatcher, daemon, ...)
- **scion-orchestrator** for “easy” configuration and setup:  
<https://github.com/scionproto-contrib/scion-orchestrator>
- List of SCION tools, applications, libraries:  
<https://github.com/scionproto/awesome-scion>

# Using SCION

- *Anapaya Systems* builds SCION capable software and network hardware
- In use at banks, government and hospitals (in .ch)

# 2STiC: SCION-nl testbed



# 2STiC: SCION-nl testbed

The screenshot shows a web browser window with the address bar displaying 'sidnlabs.nl'. The website content includes the 'SIDN LABS' logo and a large heading 'Zorgeloos' (Carefree) over a background image of a person at a computer. Below the heading, there is text: 'Het internet is grootser dan ooit voorzien. Om er zorgeloos te zijn, moet het internet van...'. A teal button labeled 'Over SIDN LABS' is visible. On the right side of the browser, a SCION overlay panel is open, displaying the following information:

- All resources loaded via SCION**
  - ✓ www.sidnlabs.nl
  - ✓ ip6.sidnlabs.nl
  - ✓ servfail.sidnlabs.nl
  - ✓ images.ctfassets.net
- SCION preference for www.sidnlabs.nl:  Strict
- [Manage Preferences...](#)
- [Path Usage...](#)
- + www.alotof.it
- www.sidnlabs.nl
  - Strategy:** Shortest Path
  - Usage:** 3.6 MiB
  - ISDs:**
    -  (2STiC)
  - **Path:** 59-1124 -> 59-1140

# 2STiC: SCION-nl testbed

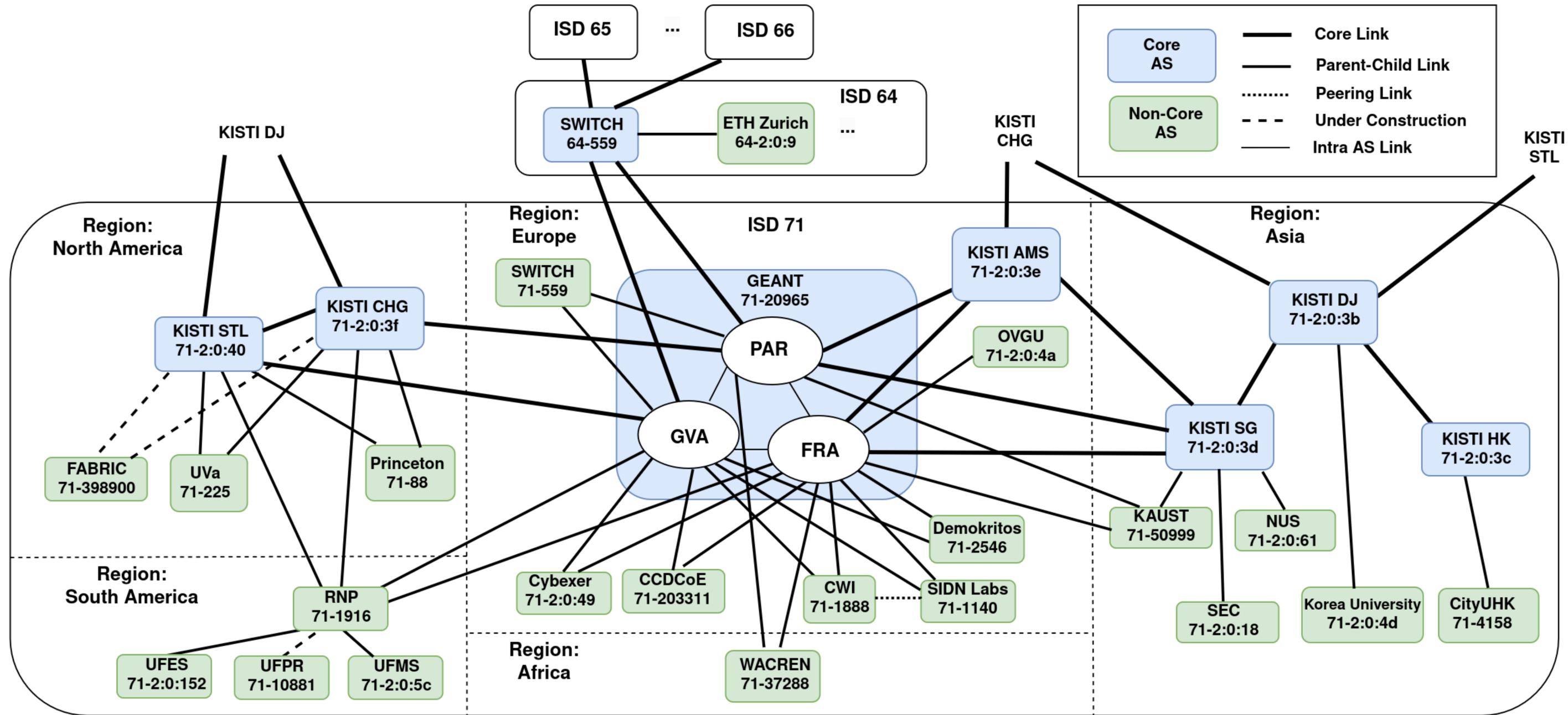
With SCION-nl we can experiment with user controllable routing:  
A user can choose to *only use routes* that have the **GDPR** label.

```
59-1124$ python3 path_query.py 59-1140 asis,gdpr
PATH id: 0 size: 1 path: ['59-1124 1>1']
59-1124 ['gdpr: True']
59-1140 ['asis: https://asis.sidnlabs.nl:18080', 'gdpr: True']

PATH id: 1 size: 1 path: ['59-1124 3>4']
59-1124 ['gdpr: True']
59-1140 ['asis: https://asis.sidnlabs.nl:18080', 'gdpr: True']

PATH id: 2 size: 2 path: ['59-1103 1>2', '59-1140 2>2']
59-1124 ['gdpr: True']
59-1103 ['gdpr: True']
59-1140 ['asis: https://asis.sidnlabs.nl:18080', 'gdpr: True']
```

# SCI ERA: SCION Education Research and Academic





Den Haag, 30 januari 2025

# Odido Business en Anapaya introduceren nieuwe security-technologie SCION in Nederland

SCION is de nieuwe generatie internetinfrastructuur, ontworpen voor bedrijven en overheden met vitale infrastructuren.

Als eerste provider in Nederland introduceert Odido de nieuwe beveiligingsoplossing SCION van Zwitserse softwarebedrijf Anapaya voor de zakelijke markt in Nederland. Dit SCION-beveiligingsprotocol, dat is ontwikkeld door het Federal Institute of Technology Zurich, is de nieuwe standaard op het gebied van veiligheid en specifiek ontworpen voor bedrijven en overheden met vitale internetinfrastructuren. Met de samenwerking met Anapaya is Odido de eerste provider in Nederland die deze nieuwe technologie aanbiedt aan klanten met kritieke infrastructuren.

**Nieuwe en extra bescherming**

[← Voorpagina newsroom](#)

**Deel deze  
release**

**2STIC**

TUESDAY, MAY 19, 2026

# SCION DAY 2026 – BENELUX EDITION

SCION DAY 2026 – Benelux edition, for the first time this SCION flagship event will be held in the Netherlands, on May 19, 2026.

SCION technology is an Internet protocol deployed across critical infrastructure in Switzerland to increase security and cyber resilience. It enables network optionality by allowing users to choose which infrastructure their data is forwarded through, thereby reducing the attack surface of critical IT networks.

Today, this market-ready technology is also available to businesses and critical sectors in the Benelux region.

Join us to hear first-hand from SCION customers how they are deploying this technology to reduce the risk of cyberattacks and strengthen their approach to sovereignty and cyber resilience. Beyond security, SCION represents a strategic approach to compliance with EU regulations such as DORA and NIS2.

 Amsterdam & online

 12:00 - 6:30 PM CET

 19.05.2026

We'll open registrations soon



2STIC

DISCUSSION

# Discussion

To recap, today we've seen:

- Programmable network hardware;
- A new internet architecture;
- An active community.

With these developments in mind, we wonder:  
**how do you see the future of the Internet?**

# Discussion

## Routing transparency

- Do users need this much transparency and control?
- 3rd parties can tell a lot about how you are connected to the internet by looking at the headers in a single packet, is this desirable?

## Isolation Domains

- What is a sustainable governance structure for an ISD? Should this be government controlled or not?
- Will ISDs (and extensions) violate net neutrality?

2STIC

Thanks for your attention!

Lisa Bruder, Ralph Koning

[sidnlabs.nl](http://sidnlabs.nl)

[2stic.nl](http://2stic.nl)