SCION, hitting the future Internet road: Next-generation Internet ecosystem and burgeoning opportunities

Jordi Subirà-Nieto, Tilmann Zäschke

What is SCION?

Clean design of an **Inter**-domain **net**work architecture that considers **security from design** to achieve:

- Availability
- Transparency and control
- Reliability and scalability

Open-source project: https://github.com/scionproto/scion

ETH *zürich*

SCiON

Why SCION?

Alternative to our old friend BGP/IP Internet.

SCION incorporates these security requirements from the inception.

Two-napkin original BGP protocol

Why SCION?

The network must provide availability even under the presence
of malicious actors.

Why SCION?

The network must provide availability even under the presence of malicious actors.

Digging into the Orange España Hack

By **Doug Madory** on 26 Jan 2024

Category: Tech matters

Tags: Guest Post, outages, RPKI, security

〈 Blog home

Adapted from Mae Mu's original at Unsplash.

On 3 January 2024, Spain's second-largest mobile operator, Orange España, experienced a national outage spanning multiple hours. The cause? A compromised password and an increasingly robust routing system. It turns out that the network operator's favourite defence tool (RPKI) can be a double-edged sword.

Why SCION?

The network must provide availability even under the presence
of malicious actors.

Digging into the Orange España Hack

By **Doug Madory** on **26 Jan 2024**

Category: Tech matters

Tags: Guest Post, outages, RPKI, security

< Blog home

Adapted from Mae Mu's original at Unsplash.

On 3 January 2024, Spain's second-largest mobile operator, Orange España,
experienced a national outage spanning multiple hours. The cause? A
compromised password and an increasingly robust routing system. It turns
out that the network operator's favourite defence tool (RPKI) can be a
double-edged sword.

Attackers exploit fundamental flaw in the web's security to steal $2 million in cryptocurrency

MARCH 9, 2022 BY HENRY BIRGE-LEE

By Henry Birge-Lee, Liang Wang, Grace Cimaszewski, Jennifer Rexford and Prateek Mittal

Why SCION?

The network must provide availability even under the presence
of malicious actors.

Hungry? Stay for SCION real-world feast

SCION is deployed in practice, **not only** a research project

Yummy desserts:

- Browsing the next-gen Internet
- SCION first-person Shooter
- SCION Walkthrough for Developers

But first the main course...

SCION ecosystem

SCION's distinctive aspects

- **Path-aware** Internet Architecture

- **Scalable trust infrastructure** for the heterogeneous world via Trust Domains

- **Scalable path discovery** for rapid global connectivity

- Highly dense **multipath** for fine-grained path optimization

- **Real-world deployment**

ETH*zürich*

SC:ON
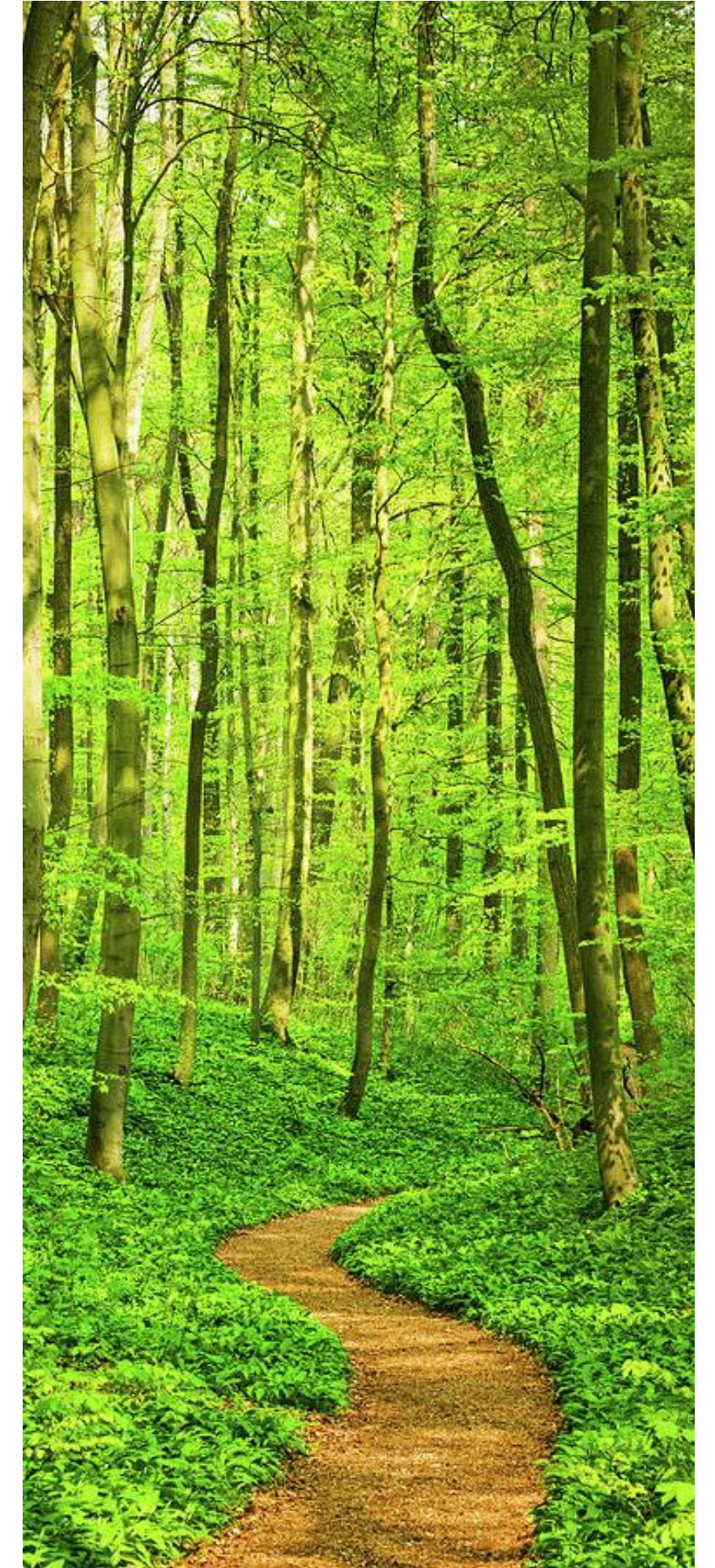
(Trust) Isolation Domains (ISD)

Grouping of Autonomous Systems (AS) that share a common TRC.

Trust Root Configuration (TRC)

- Set of signed certificates and policies

Core AS

- AS that provides ISD connectivity and participates in the TRC management.

ETH zürich

SCiON

SCION Control Plane

Path Dissemination for Rapid Global
Connectivity

SCION Control Plane

Path Dissemination for Rapid Global Connectivity

- Beacons (Routing info messages)
- Beacons authenticated at every hop

SCION Control Plane

Path Dissemination for Rapid Global Connectivity

- Beacons (Routing info messages)
- Beacons authenticated at every hop

SCION Control Plane

Path Dissemination for Rapid Global Connectivity

- Beacons (Routing info messages)
- Beacons authenticated at every hop

SCION Control Plane

Path Dissemination for Rapid Global Connectivity

- Beacons (Routing info messages)
- Beacons authenticated at every hop

SCION Control Plane

Path Dissemination for Rapid Global Connectivity

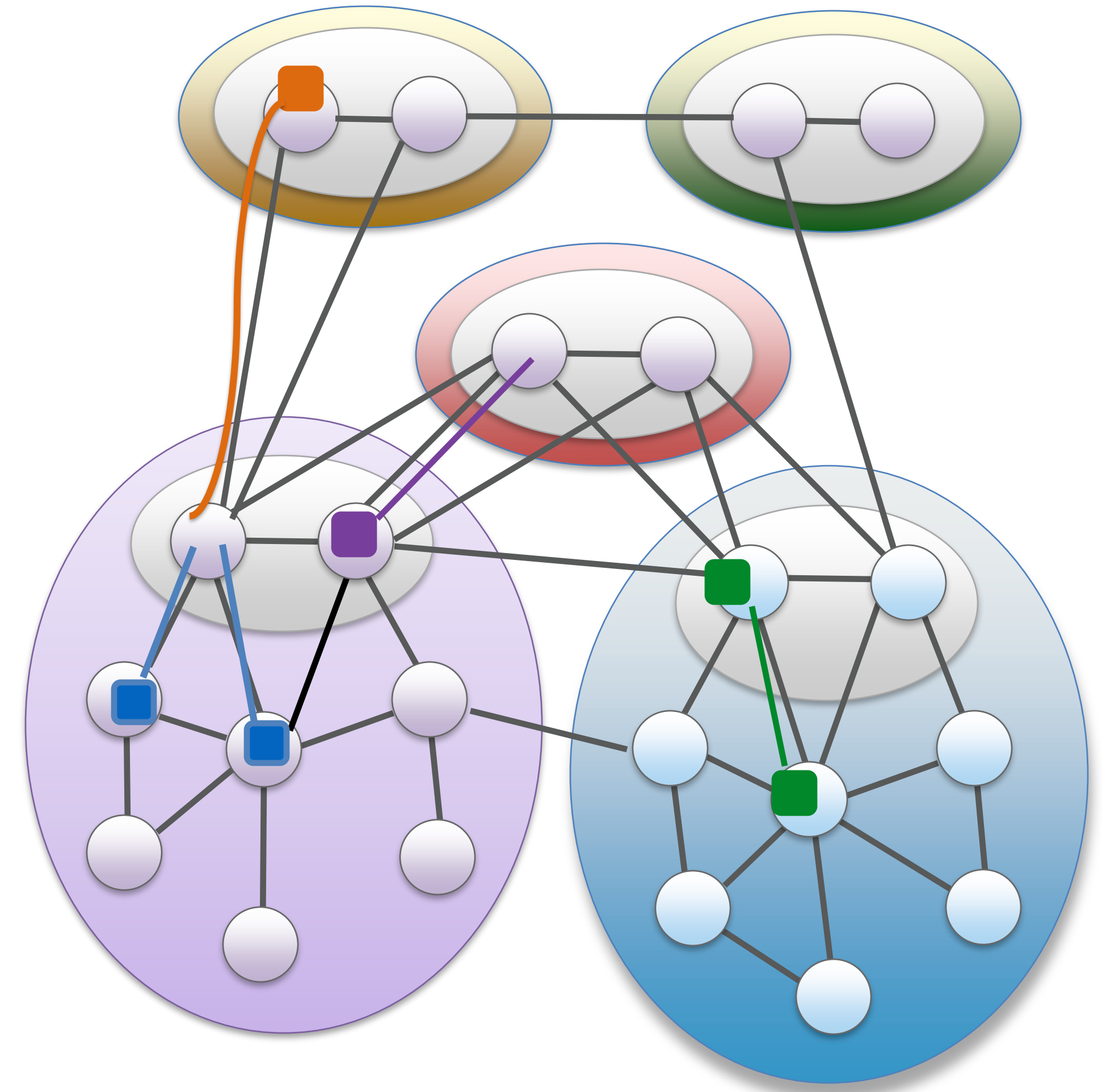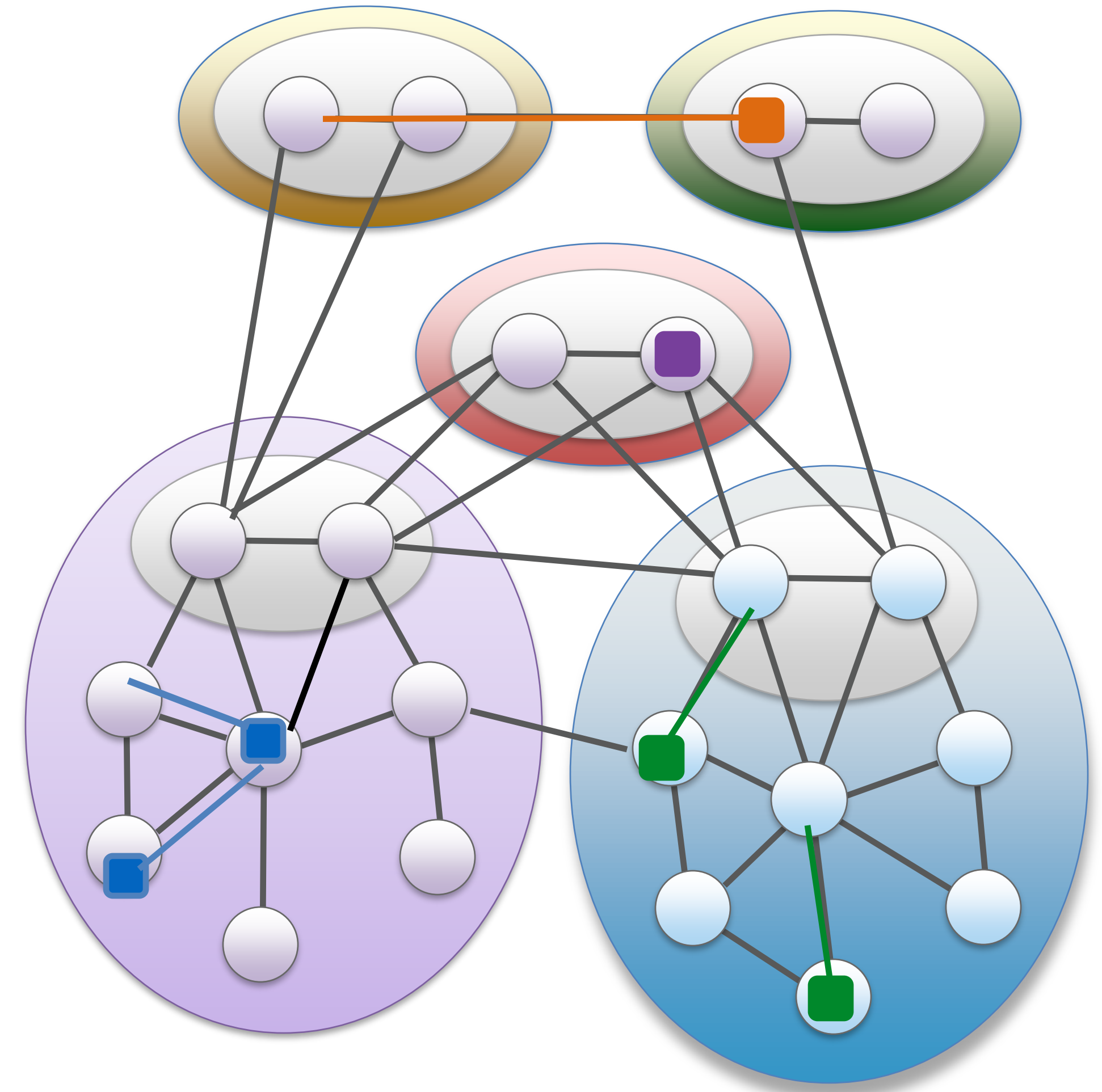- Beacons (Routing info messages)
- Beacons authenticated at every hop
- Remove routing convergence

SCION Control Plane

Path Dissemination for Rapid Global Connectivity

- Beacons (Routing info messages)

- Beacons authenticated at every hop

- Remove routing convergence

To achieve:

- **Rapid path exploration**

- **Scalability** (processing, communication and state overhead)

Exhaustive evaluation:

Deployment and Scalability of an Inter-Domain Multi-Path Routing Infrastructure; Krähenbühl et al.; CoNEXT 2021
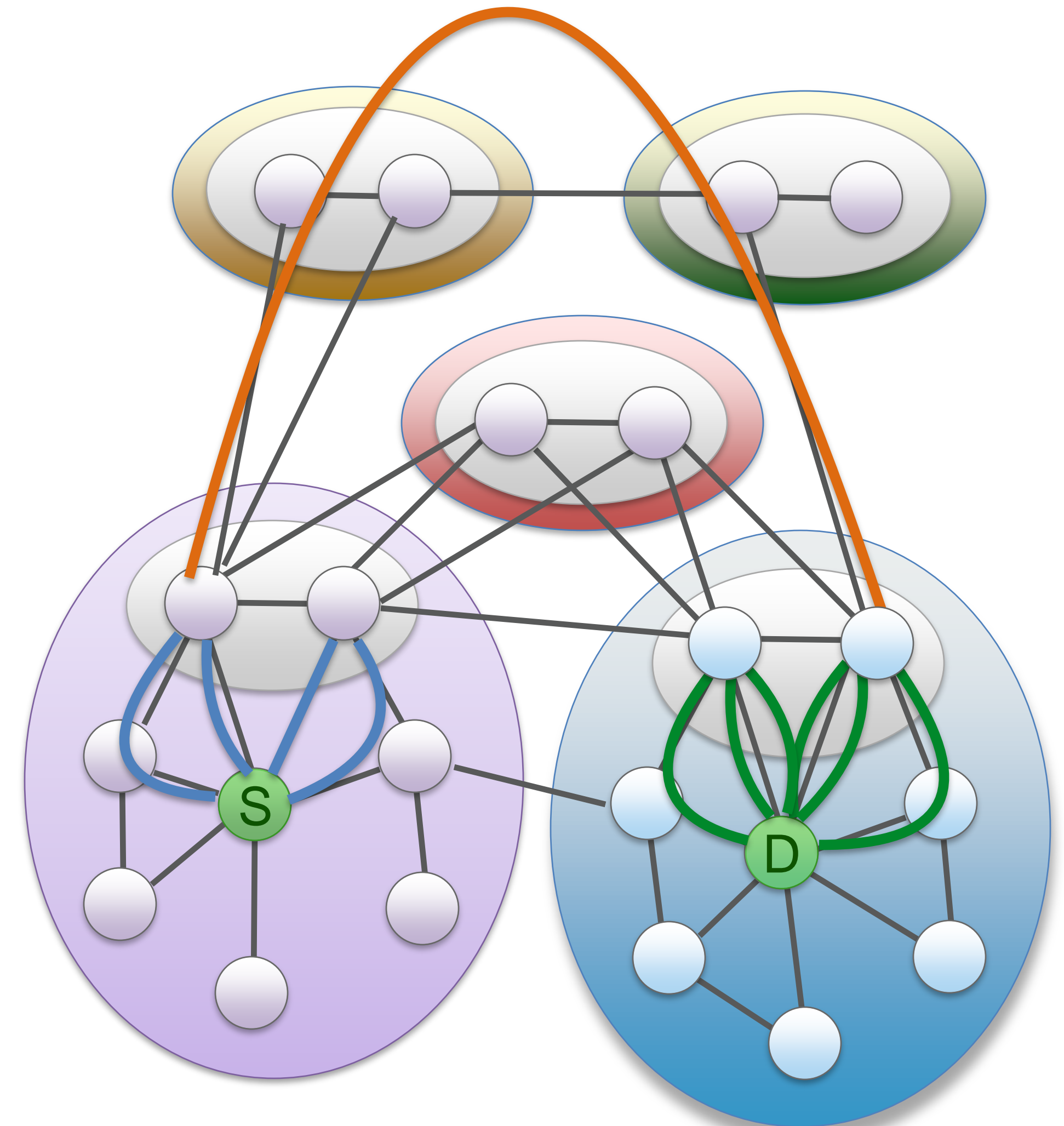
ETH zürich

SCION

Highly dense Multipath

Endhosts benefit from **simultaneous multipath for fine-grained optimization:**

- Low latency, jitter
- High bandwidth
- Privacy, anonymity
- Low CO_2 footprint
- Jurisdiction

ETHzürich

SCiON
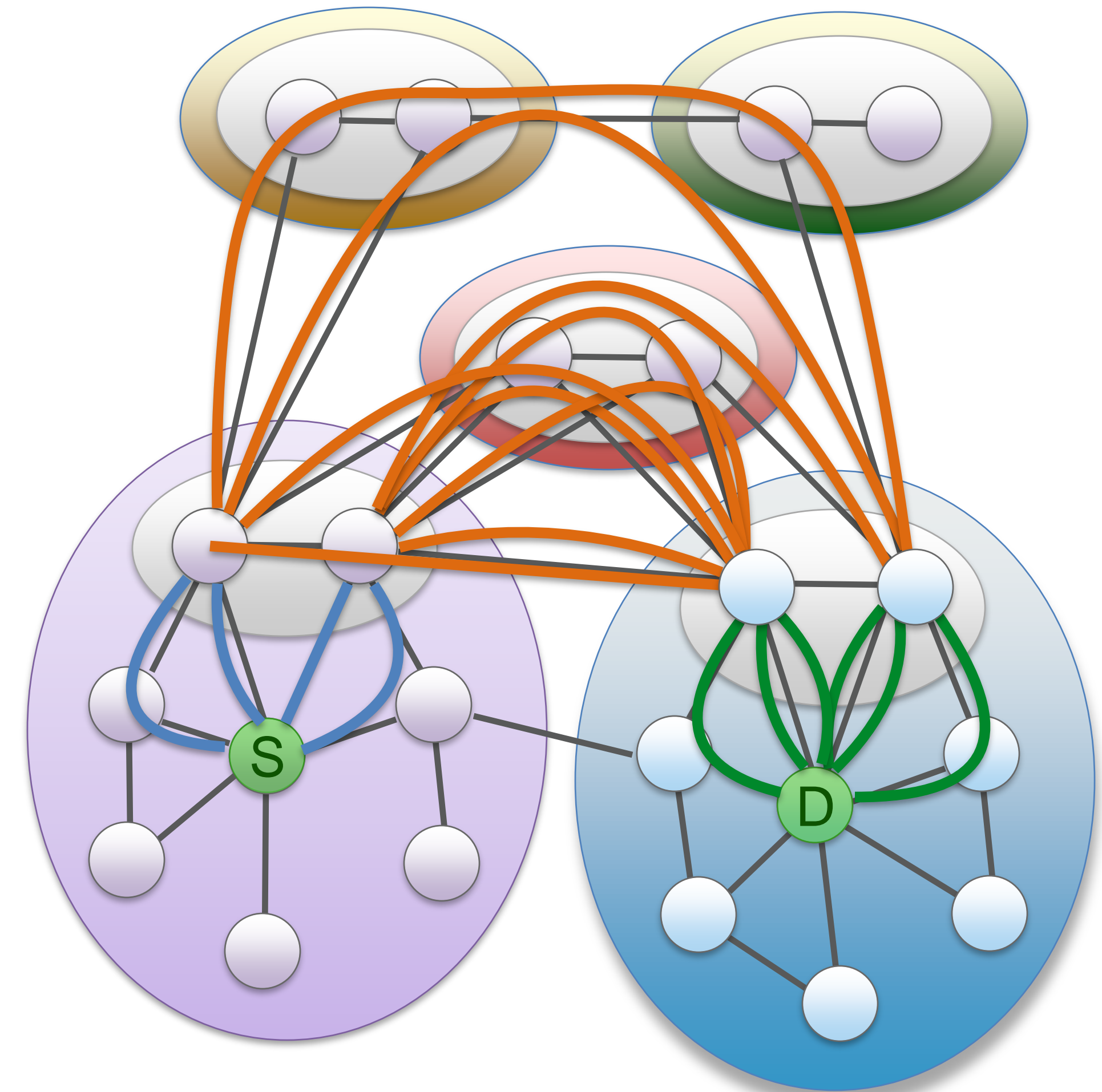
Highly dense Multipath

Endhosts benefit from **simultaneous multipath for fine-grained optimization:**

- Low latency, jitter
- High bandwidth
- Privacy, anonymity
- Low CO_2 footprint
- Jurisdiction

Dozens or even **100+ different** paths in the **production SCION Network**

- Likely to find the best path

ETHzürich
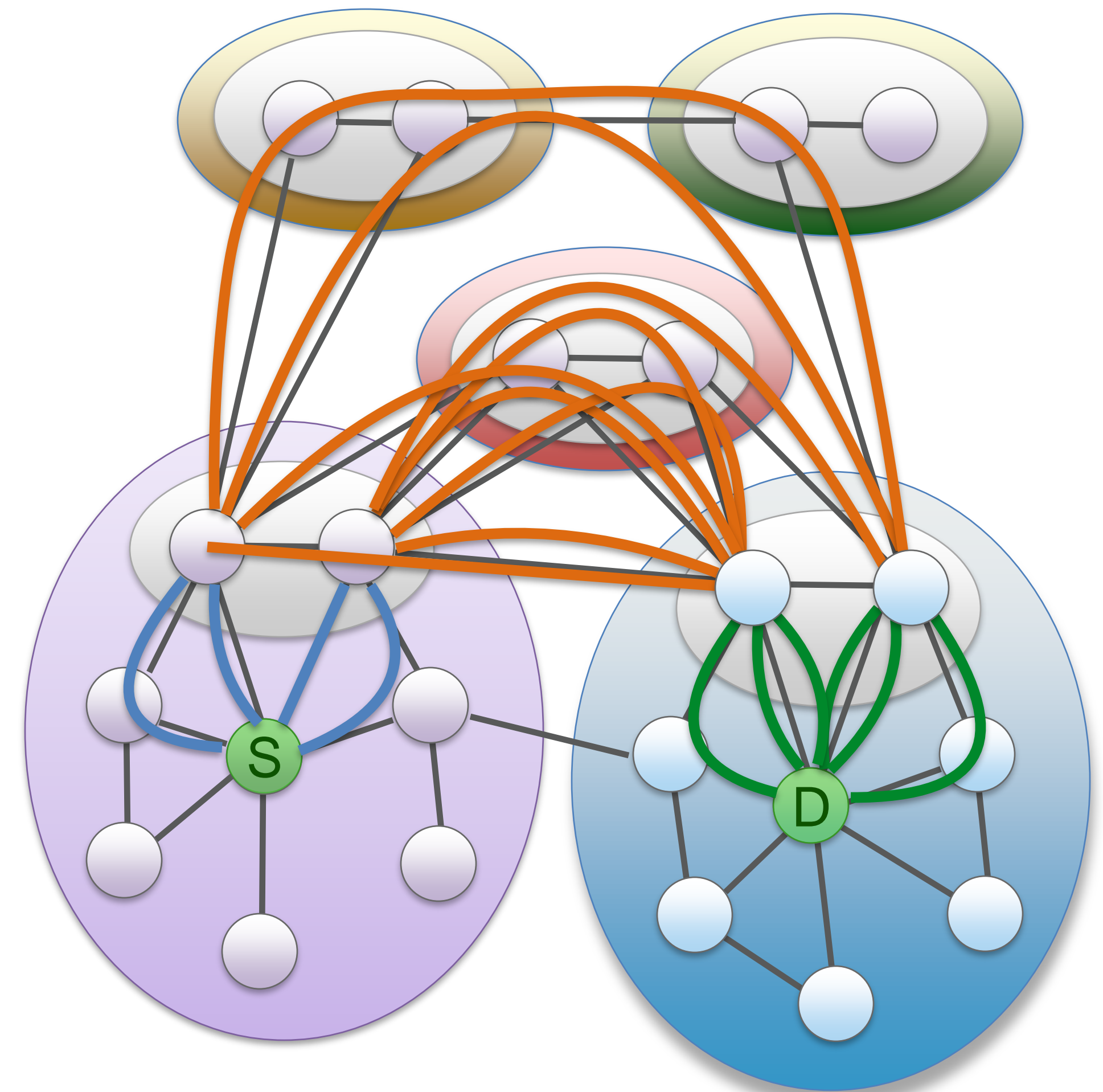
SCiON

SCION CP & DP

💡 **Path-based Network Architecture**

Control Plane - Routing

❖ Path information discovery (as seen previously)

Data Plane - Packet forwarding

❖ Combine Path Segments to Path

❖ Packets contain Path

❖ Routers forward packets based on Path
  ▷ Simple routers, stateless operation

Packet P1

| F→C→A |
| A→I→J→M |
| M→P→S |
| Payload |

Packet P2

| F→D→B |
| B→K→L |
| L→O→S |
| Payload |
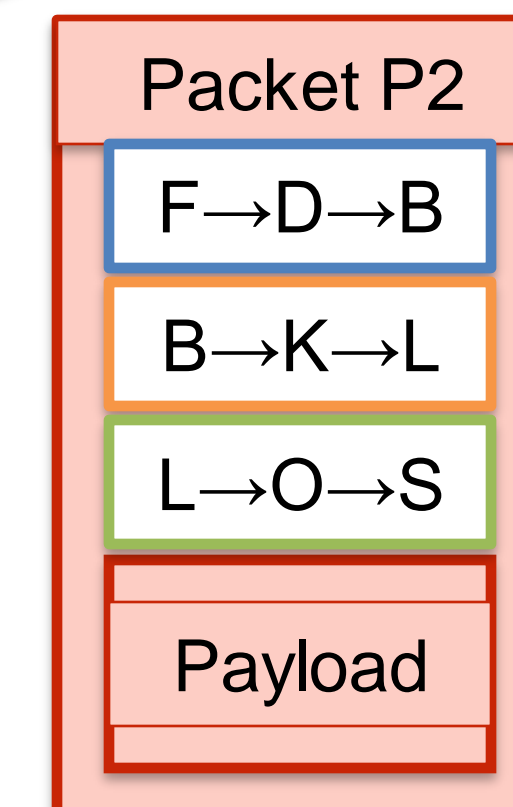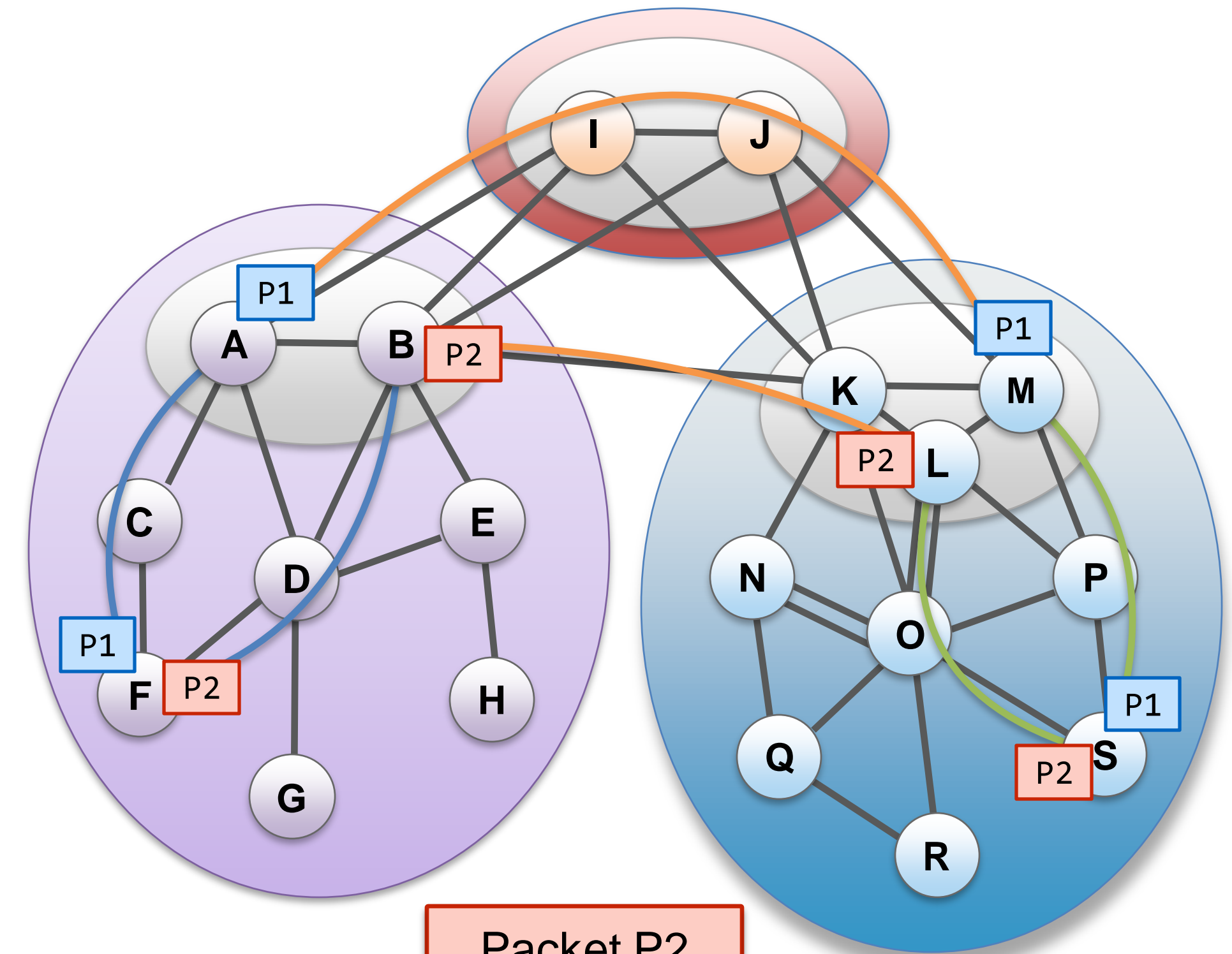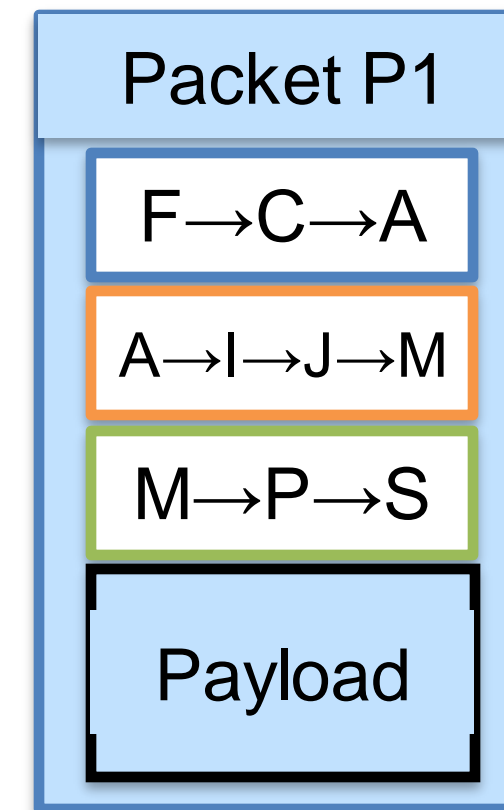
Real-world Deployment

Global SCION Internet (some parts):

- SCIERA: SCION Education, Research and Academic Network
- Secure and resilient communication fabric for industries
  - SSFN
  - SSHN
- ...

SCIONLab Testbed Network

SCION Production Network

BGP-free global communication (Not an overlay!)

- BGP fault independent

- Deployment with international ISPs around 100+ ASes

  - CH, EU, NA, Asia,...

- **SCION cloud-based access** offered by some CSP (currently AWS).

SCIERA: Education & Research ISD

Universities:
- Princeton University, OVGU Magdeburg, KAUST, Korea University, University of Virginia, NCSR-Demokritos

SCIERA: Education & Research ISD

Universities:

- Princeton University, OVGU Magdeburg, KAUST, Korea University, University of Virginia, NCSR-Demokritos

Research institutions:

- SIDN, CSCS, KISTI, CyberEX

SCIERA: Education & Research ISD

Universities:

- Princeton University, OVGU Magdeburg, KAUST, Korea University, University of Virginia, NCSR-Demokritos

Research institutions:

- SIDN, CSCS, KISTI, CyberEX

Research and Education Networks:

- SWITCH, GÉANT, KREONET, RNP, WACREN, BRIDGES
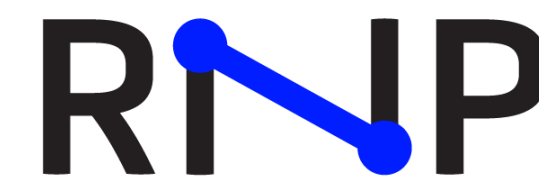
SCIERA: Education & Research ISD

Main networks providing connectivity: GÉANT, Kreonet, SWITCH

Deployed
Deployment

SCION Industry Networks

SSFN: Secure Swiss Finance Network

Launched in 2021 by SIX and SNB.

Facilitates sound Interbank Payments, phasing out previous Finance IPNet by June 2024 and connecting **~120 participants**
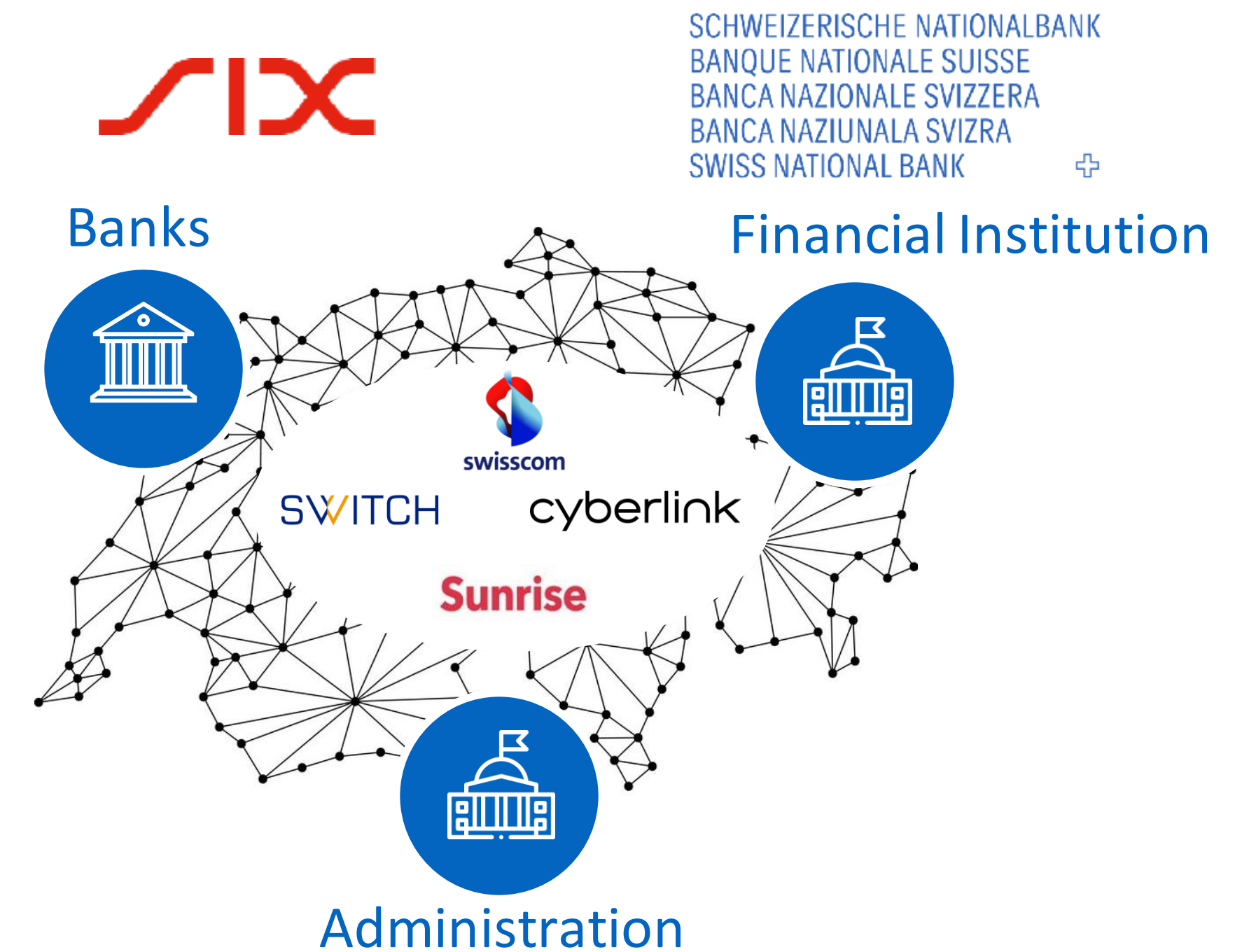
SCION Industry Networks

SSFN: Secure Swiss Finance Network

Launched in 2021 by SIX and SNB.

Facilitates sound Interbank Payments, phasing out previous Finance IPNet by June 2024 and connecting **~120 participants**
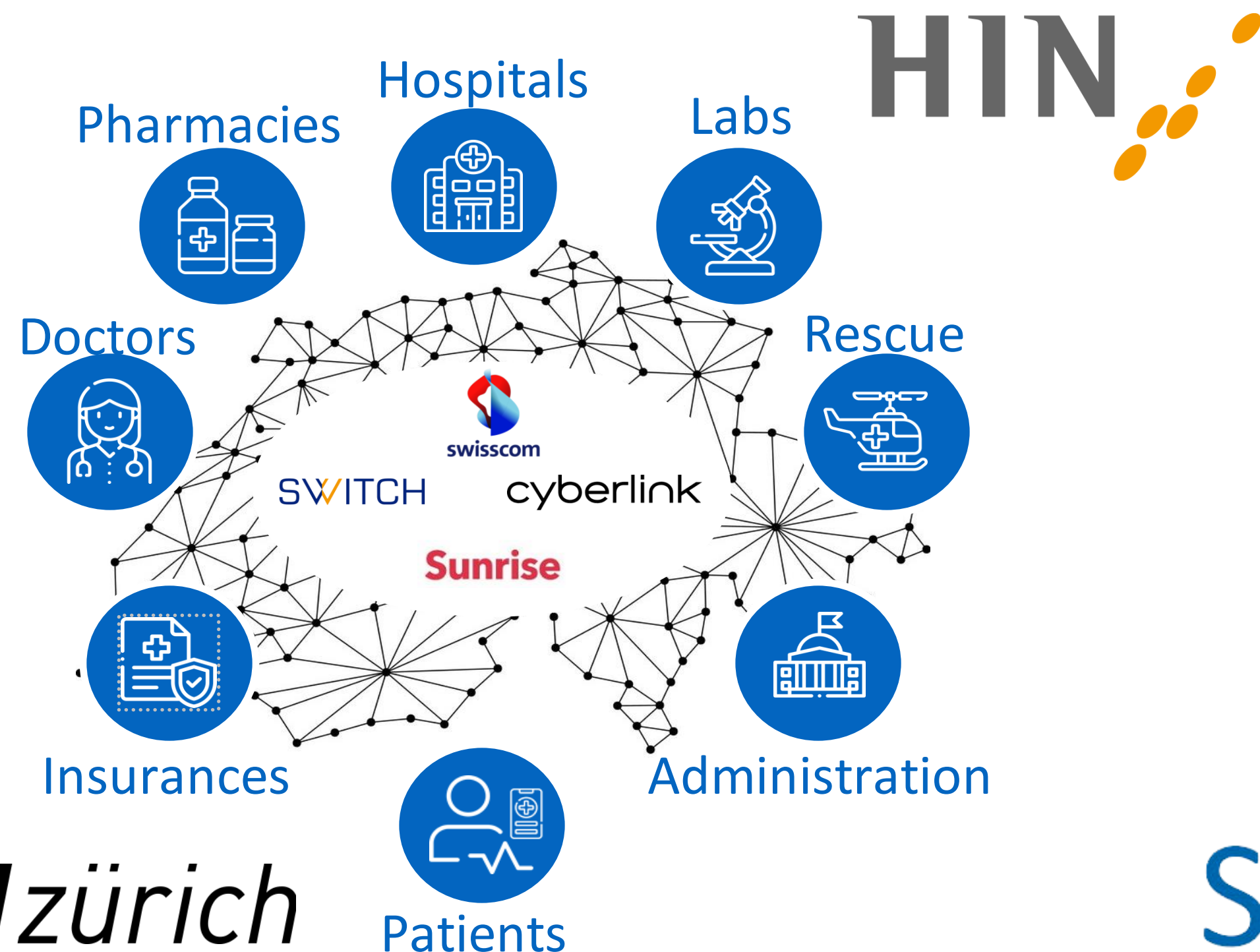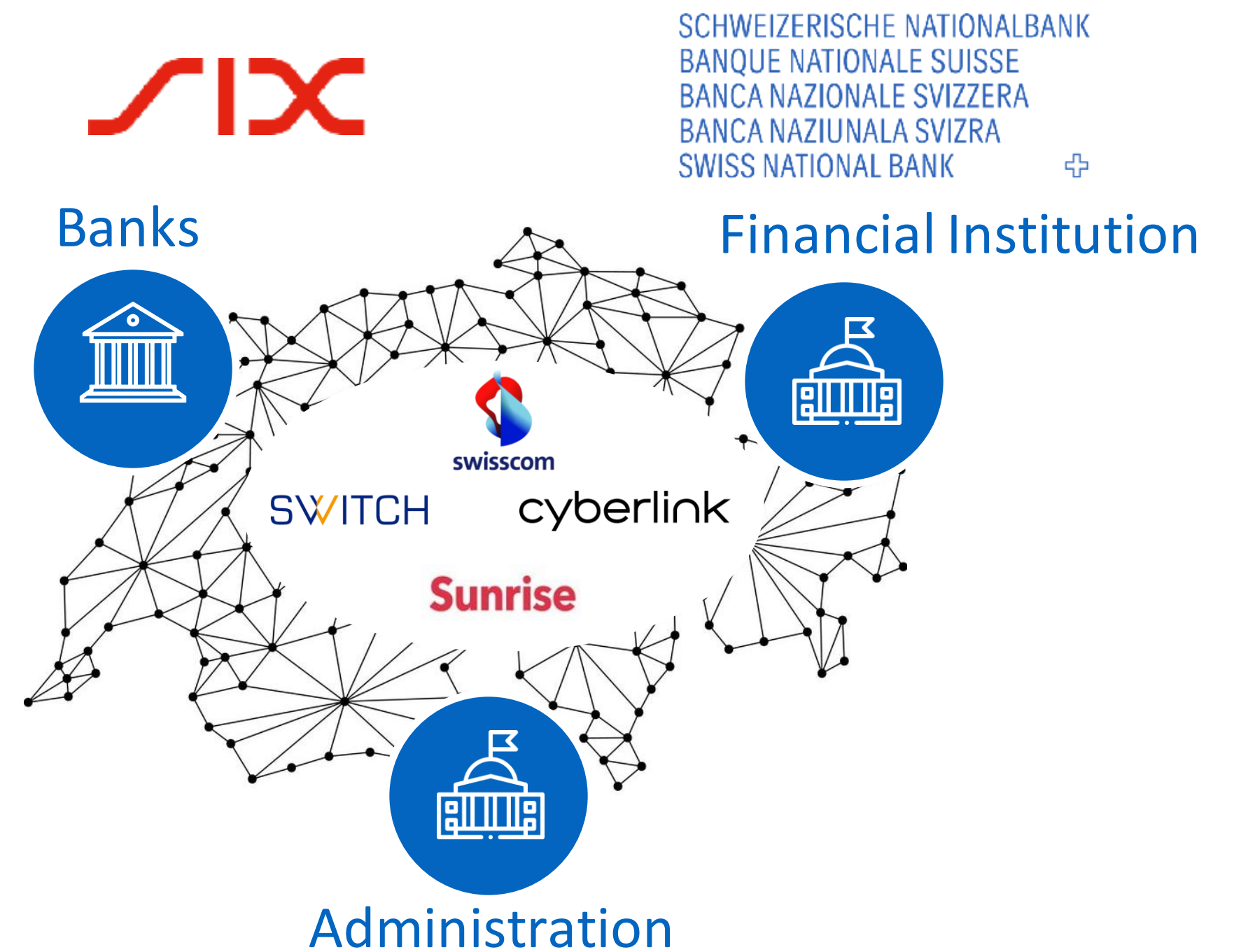
SSHN: Secure Swiss Healthcare Network

HIN Trust Circle (HIN Vertrauensraum) provides connectivity based on SCION to **~50,000 health professionals** since December 2022

SCIONLab testbed

Globally distributed testbed to conduct experiments and test deployments

Anyone can **join the network only downloading a VM.**
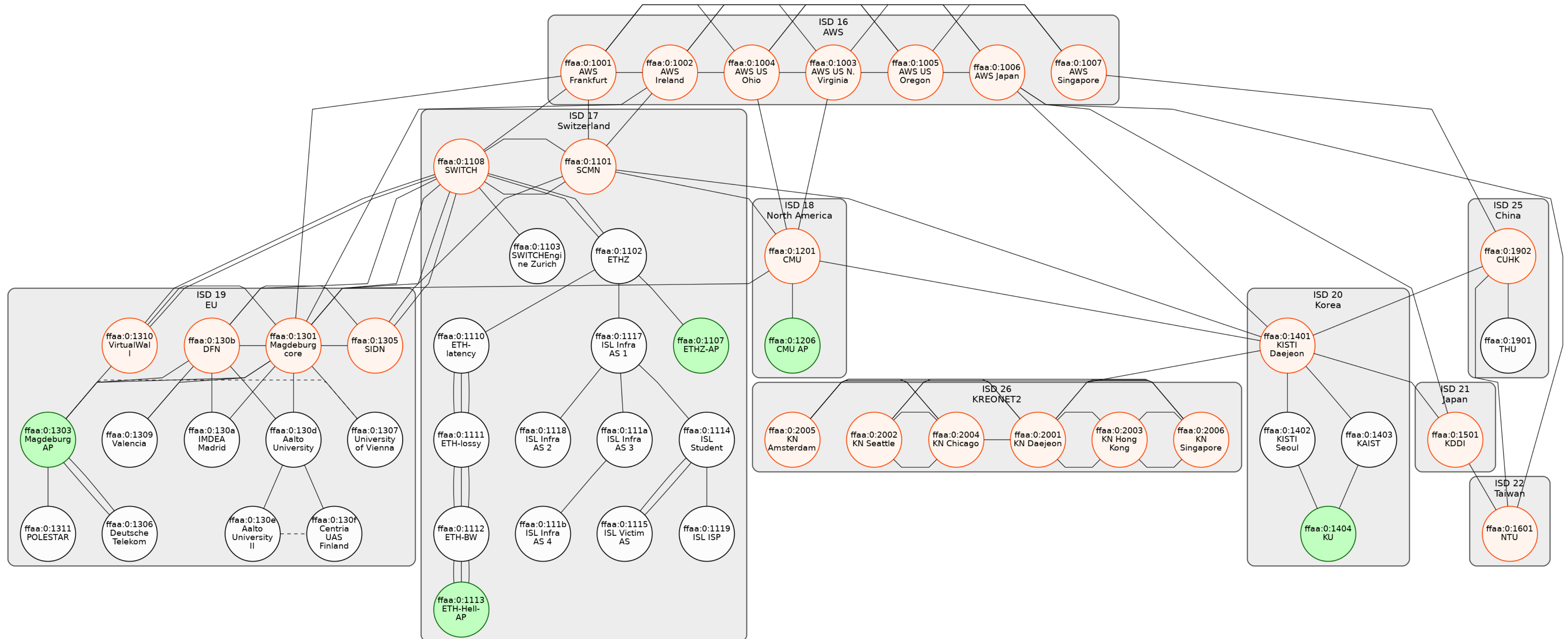
For you, developers!

SCION is getting awesome

- Curated list of awesome SCION projects
  (https://github.com/scionproto/awesome-scion)

SCION is getting awesome

- Curated list of awesome SCION projects
  (https://github.com/scionproto/awesome-scion)
  - Infrastructure
    - Tofino SCION Router, eXpress router (XDP/P4),...

ETH zürich

SCION is getting awesome

- Curated list of awesome SCION projects
  (https://github.com/scionproto/awesome-scion)
  - Infrastructure
    - Tofino SCION Router, eXpress router (XDP/P4),...
  - Applications
    - Browser-extension, (SCION-aware) QUAKE III,...

ETH zürich

SCION

SCION is getting awesome

- Curated list of awesome SCION projects
  (https://github.com/scionproto/awesome-scion)
  - Infrastructure
    - Tofino SCION Router, eXpress router (XDP/P4),...
  - Applications
    - Browser-extension, (SCION-aware) QUAKE III,...
  - Libraries
    - Go, Java (WIP), Rust, Bindings

SCION is getting awesome

- Curated list of awesome SCION projects
  (https://github.com/scionproto/awesome-scion)
  - Infrastructure
    - Tofino SCION Router, eXpress router (XDP/P4),...
  - Applications
    - Browser-extension, (SCION-aware) QUAKE III,...
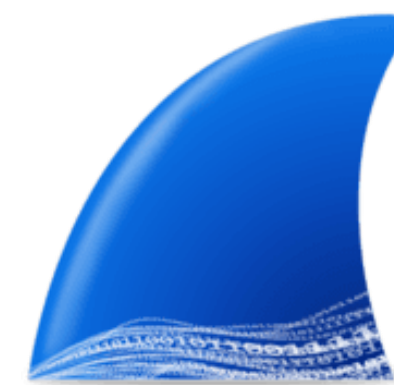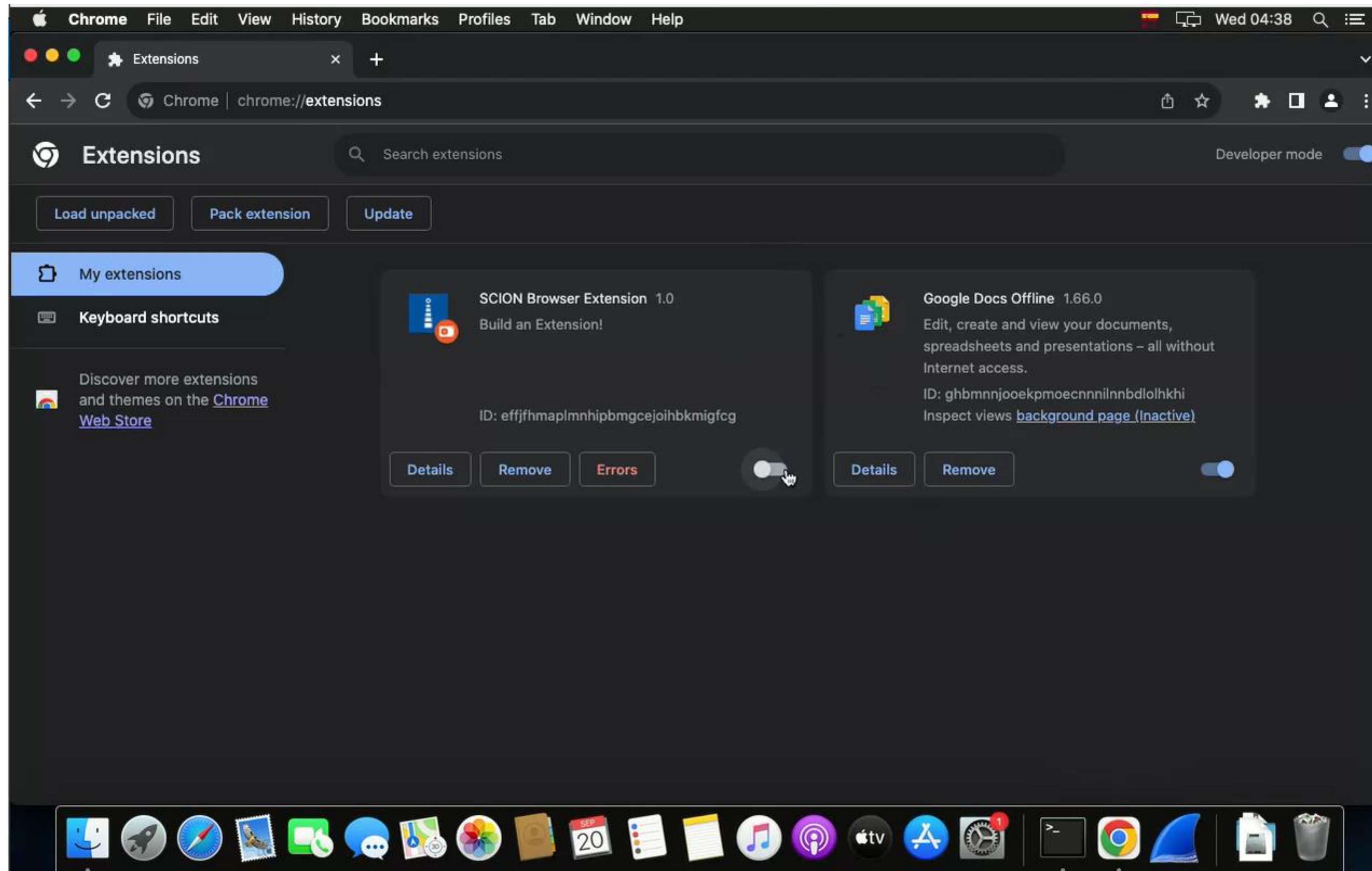 - Libraries
    - Go, Java (WIP), Rust, Bindings
  - Tools
    - SEED Emulator, scapy library, Wireshark

SCION-enabled Browser Demo on macOS

SCION-aware QUAKE III?

CONNECTING TO 19-FFAA:1:1087,10.255.255.1:27960

AWAITING CHALLENGE...1

Getting started – Your own project

- Go API: https://pkg.go.dev/github.com/netsec-ethz/scion-apps/pkg/pan#DialUDP

func DialUDP

```
func DialUDP(ctx context.Context, local netaddr.IPPort, remote UDPAddr,
    policy Policy, selector Selector) (Conn, error)
```

DialUDP opens a SCION/UDP socket, connected to the remote address. If the local address, or either its IP or port, are left unspecified, they will be automatically chosen.

DialUDP looks up SCION paths to the destination AS. The policy defines the allowed paths and their preference order. The selector dynamically selects a path among this set for each Write operation. If the policy is nil, all paths are allowed. If the selector is nil, a DefaultSelector is used.

- Go API also has C, C++ and Python bindings

- Rust API: https://github.com/MystenLabs/scion-rs

- Java API (alpha) : https://github.com/netsec-ethz/scion-java-client

ETH zürich   SCION

SCION Java client

- 100% pure Java client
- API similar to `DatagramChannel`
  (and `DatagramSocket`)
- API for path inspection and selection
- SCMP echo & traceroute (ICMP for SCION)

ETHzürich

SCION

Basic Java client

SCION **DatagramChannel** can be used (exactly) as Java nio **DatagramChannel**:

```
InetSocketAddress addr = new InetSocketAddress("ethz.ch", 80);
try (DatagramChannel channel = DatagramChannel.open()) {
    channel.configureBlocking(true);
    channel.connect(addr);
    channel.write(ByteBuffer.wrap("Hello Scion".getBytes()));
    ...
    ByteBuffer response = ByteBuffer.allocate(1500);
    channel.read(response);
}
```

ETH zürich

SCiON

Java client with PathPolicy

SCION **DatagramChannel** with **PathPolicy**:

```
InetSocketAddress addr = new InetSocketAddress("ethz.ch", 80);
try (DatagramChannel channel = DatagramChannel.open()) {
  channel.configureBlocking(true);
  channel.connect(addr);
  channel.setPathPolicy(PathPolicy.MAX_BANDWIDTH);
  channel.write(ByteBuffer.wrap("Hello Scion".getBytes()));
  ...
  ByteBuffer response = ByteBuffer.allocate(1500);
  channel.read(response);
}
```

ETH *zürich*

SCiON

Java server

SCION **DatagramChannel** can be used similarly to JDK **DatagramChannel**:

```
try (DatagramChannel channel = DatagramChannel.open()) {

  ...

  ByteBuffer request = ByteBuffer.allocate(1500);
  Path pathToClient = channel.receive(request);   // SCION specific

  ...

  ByteBuffer response = ... ;
  channel.send(response, pathToClient);
}
```

receive() returns a **Path** that can be used for **send()**

PathPolicy

Predefined
algorithms

- FIRST

- MIN_HOP

- MIN_LATENCY*

- MAX_BANDWIDTH*

- IsdAllow

- IsdDisallow

PathPolicy

Predefined
algorithms

- FIRST
- MIN_HOP
- MIN_LATENCY*
- MAX_BANDWIDTH*
- IsdAllow
- IsdDisallow

Example:
geofencing

ISD 125
ISD 120
ISD 99
ISD 110
ISD 130

ETH *zürich*

SC:ON

PathPolicy

Predefined algorithms

- FIRST
- MIN_HOP
- MIN_LATENCY*
- MAX_BANDWIDTH*
- IsdAllow
- IsdDisallow

Example: geofencing

ISD 125
ISD 120
ISD 99
ISD 110
ISD 130
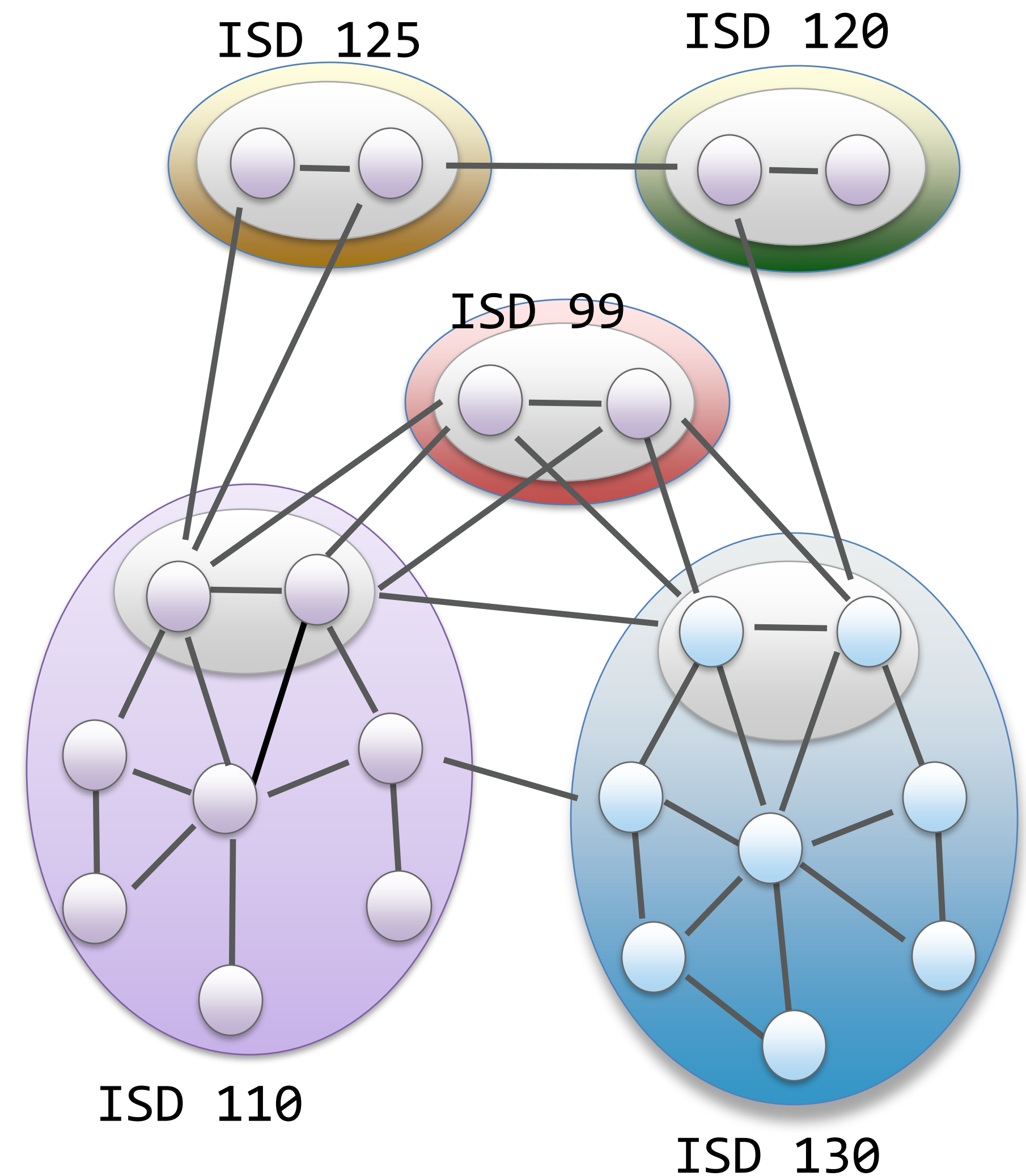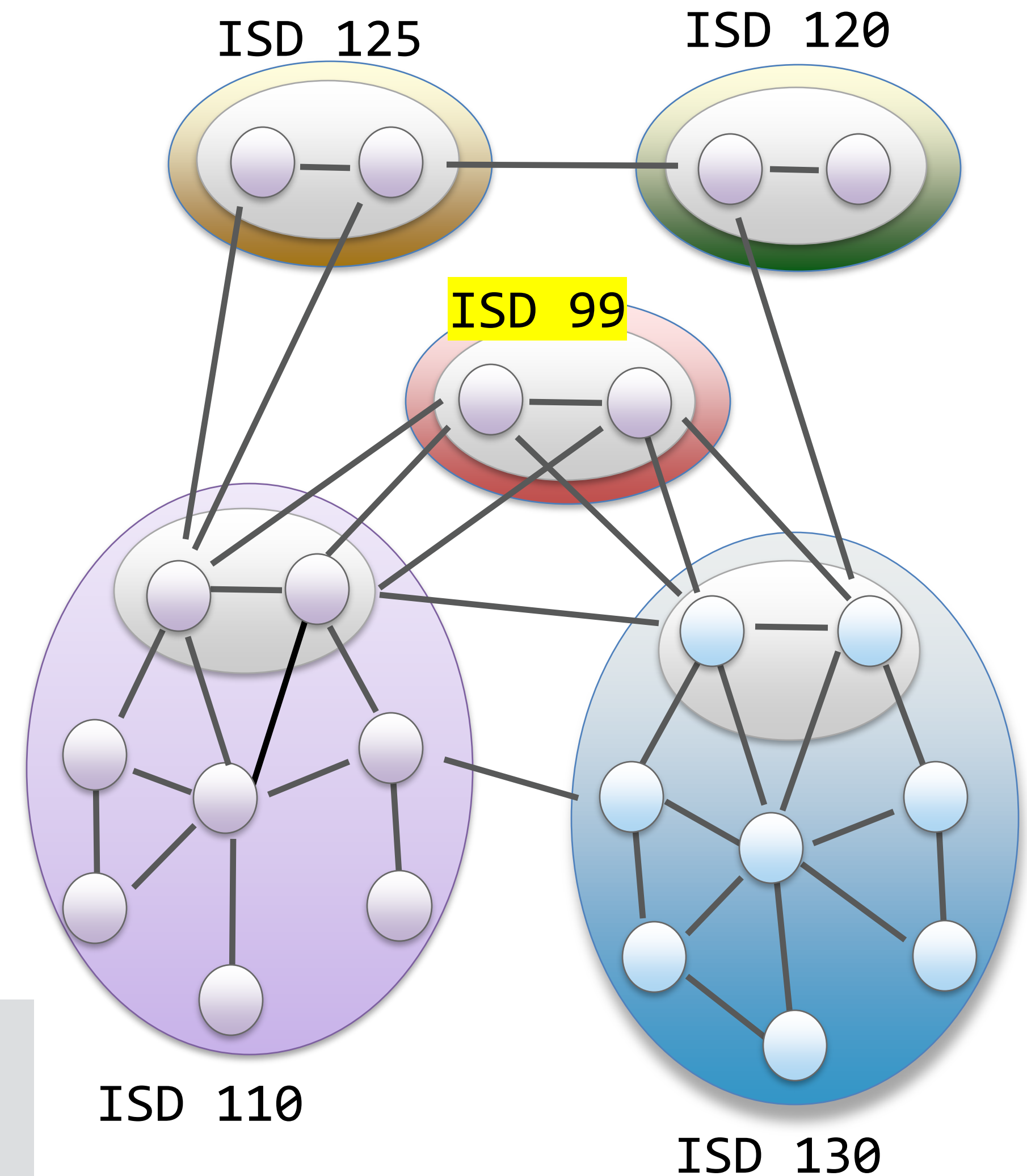
```
PathPolicy geoFence  = new IsdDisallow(99);
channel.setPathPolicy(geoFence);
```

ETH *zürich*

SC:ON

Getting started – Testing

Run a local network with the reference implementation

- Code: https://github.com/scionproto/scion

- Docs: https://docs.scion.org/en/latest/dev/run.html

ETH zürich

SCiON

Getting started – Testing

Run a local network with the reference implementation

- Code: https://github.com/scionproto/scion

- Docs: https://docs.scion.org/en/latest/dev/run.html

```
$ ./scion.sh topology -c your_topology.topo
```

ETH zürich

SCiON

Getting started – Testing

Run a local network with the reference implementation

- Code: https://github.com/scionproto/scion

- Docs: https://docs.scion.org/en/latest/dev/run.html

```
$ ./scion.sh topology -c your_topology.topo
$ ./scion.sh topodot your_topology.topo
```
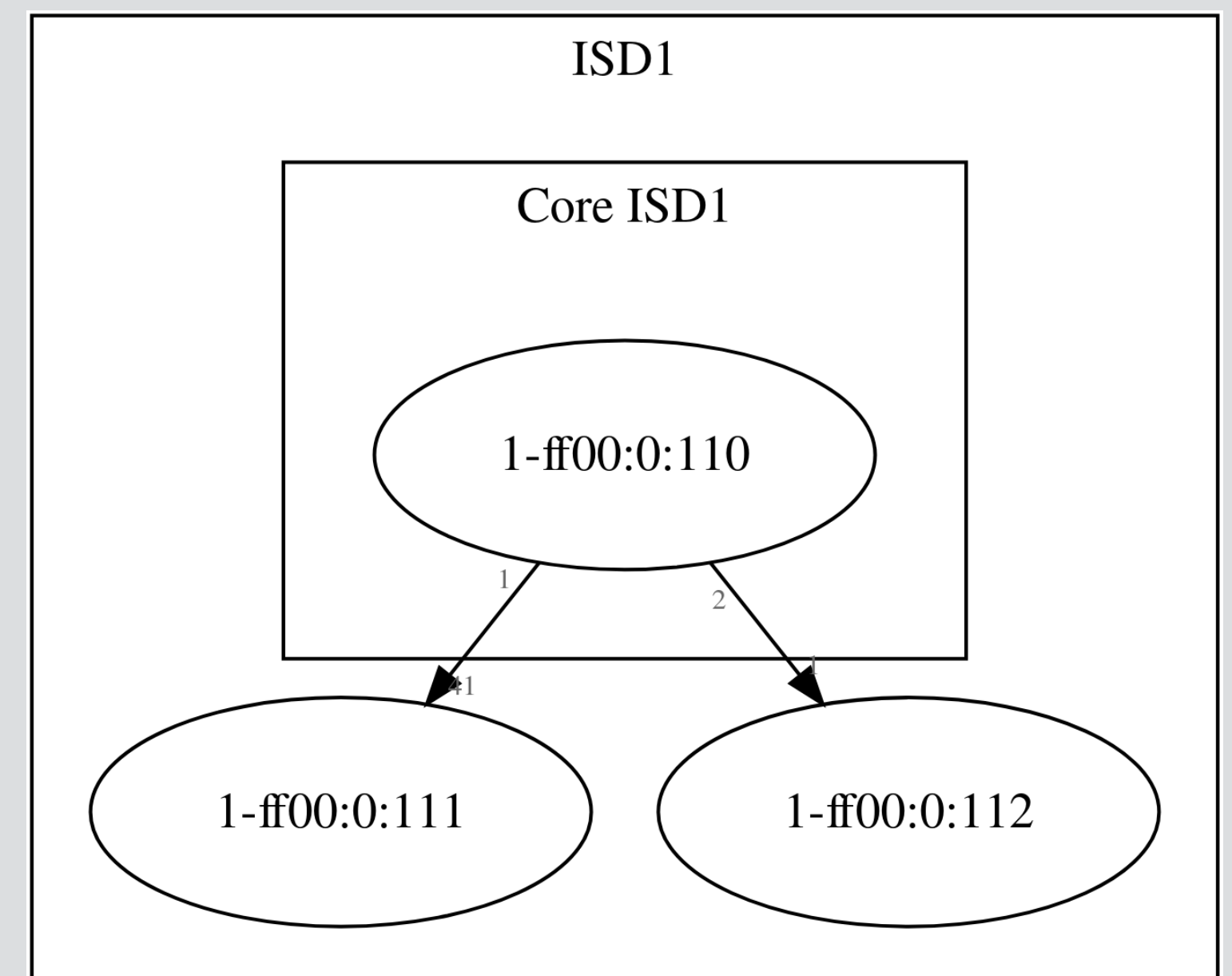
Getting started – Testing

Run a local network with the reference implementation

- Code: https://github.com/scionproto/scion

- Docs: https://docs.scion.org/en/latest/dev/run.html

```
$ ./scion.sh topology -c your_topology.topo

$ ./scion.sh topodot your_topology.topo



$ ./scion.sh run
```


ETH zürich

SCiON

Getting started – Testing

Run a local network with the reference implementation

- Code: https://github.com/scionproto/scion
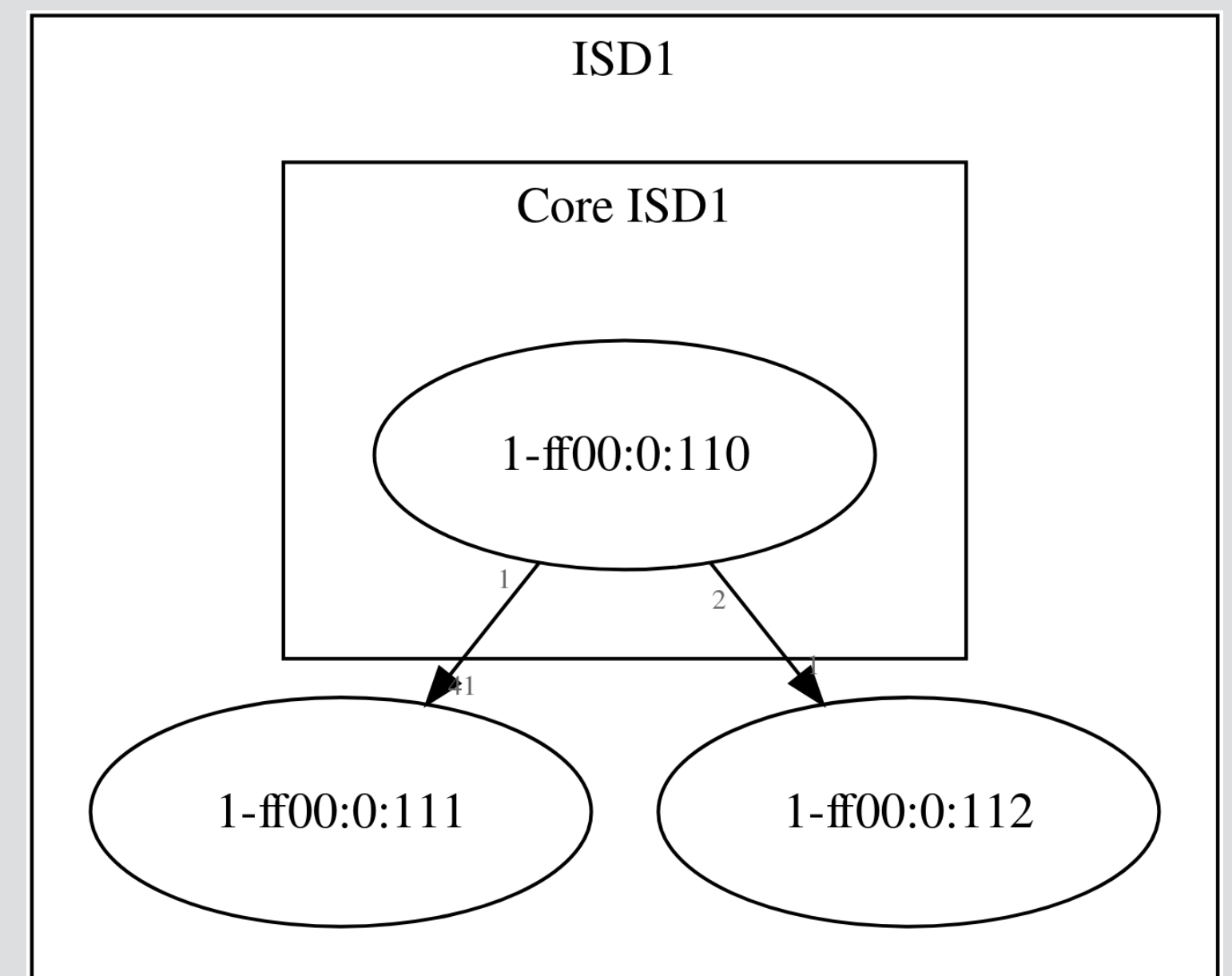
- Docs: https://docs.scion.org/en/latest/dev/run.html
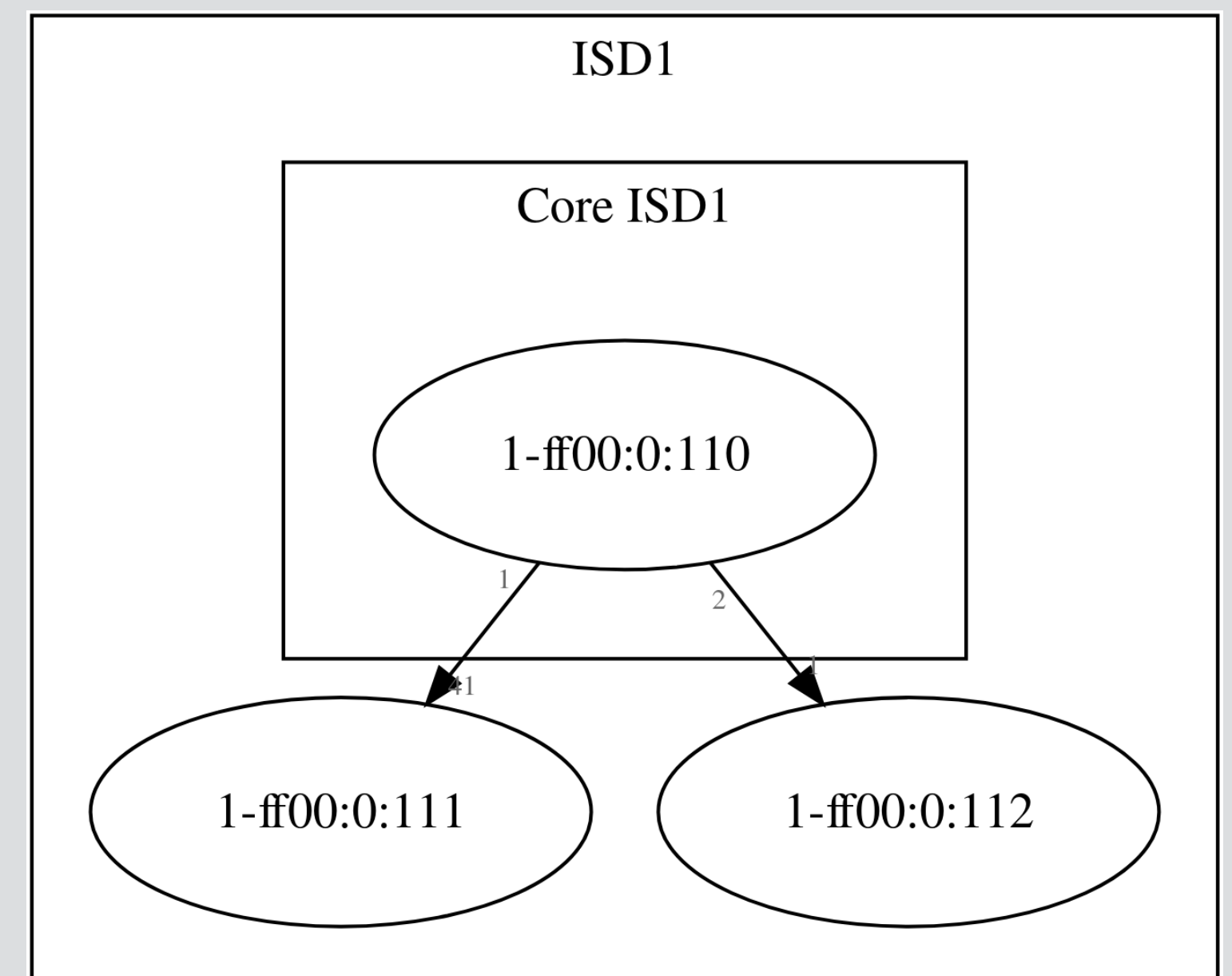
```
$ ./scion.sh topology -c your_topology.topo
$ ./scion.sh topodot your_topology.topo



$ ./scion.sh run
$ scion ping 1-ff00:0:110,0.0.0.0 --sciond 127.0.0.29:30255
88 bytes from 1-ff00:0:110,0.0.0.0: scmp_seq=0 time=0.770ms
```


ISD1

Core ISD1

1-ff00:0:110

1-ff00:0:111   1-ff00:0:112

ETH *zürich*   SCiON

Getting started – Testing

- Other options for **testing**

  - Use SEED network emulator

  - SCIONLab: A world wide testbed (overlay network)

- Production network

  - Some **ISPs** and AWS offer SCION access

  - In a University with SCION access: SCIERA

- Debugging

  - Scion `ping`, `traceroute`, `showpaths`, ...

  - Monitor traffic with wireshark SCION plugin

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

`scion.next_hdr == 17 && scion_udp.src_port == 42199`

No.	Time	Source	Destination	Protocol	Length	Info
983	2.116922765	127.0.0.1	127.0.0.41	UDP	189	42199 → 31024 Len=147 SCION 1-ff00:0:1111,[127.0.0.1] -> 1-ff00:0:112,[::1] UDP 42199 -> 44444 27
984	2.117090308	127.0.0.11	127.0.0.10	UDP	189	50000 → 50000 Len=147 SCION 1-ff00:0:1111,[127.0.0.1] -> 1-ff00:0:112,[::1] UDP 42199 -> 44444 27
985	2.117193746	127.0.0.34	127.0.0.33	UDP	189	31018 → 31016 Len=147 SCION 1-ff00:0:1111,[127.0.0.1] -> 1-ff00:0:112,[::1] UDP 42199 -> 44444 27
986	2.117276476	127.0.0.7	127.0.0.6	UDP	189	50000 → 50000 Len=147 SCION 1-ff00:0:1111,[127.0.0.1] -> 1-ff00:0:112,[::1] UDP 42199 -> 44444 27
987	2.117376515	127.0.0.26	127.0.0.27	UDP	189	31004 → 31006 Len=147 SCION 1-ff00:0:1111,[127.0.0.1] -> 1-ff00:0:112,[::1] UDP 42199 -> 44444 27
988	2.117502578	127.0.0.8	127.0.0.9	UDP	189	50000 → 50000 Len=147 SCION 1-ff00:0:1111,[127.0.0.1] -> 1-ff00:0:112,[::1] UDP 42199 -> 44444 27

Want to contribute?

- Create **your own projects**

  - Language libraries/bindings: C, C++, C#, Swift, ...

  - Support for embedded & mobile devices

  - Network protocols (E.g. Java: TCP, HTTP1/2, …)

- Add SCION support to **other projects**:

  - web proxies, http servers

  - chat & video conferencing

  - gaming, ...

Getting started – Getting Help

slack

scionproto workspace

matrix

#dev:matrix.scion.org

stackoverflow

tag questions with scion

ETH zürich

SCiON