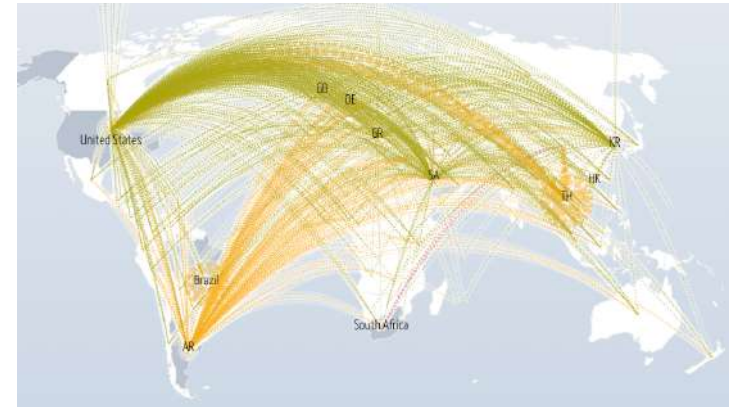


Experiencing a new Internet Architecture

Adrian Perrig, Network Security Group

The Internet is on Fire!

- Lack of sovereignty
- Frequent outages
 - <https://downdetector.com>
- Constant DDoS attacks
 - <https://www.digitalattackmap.com>
- Frequent routing attacks
 - <https://bgpstream.com>
- Lack of communication guarantees
- Expensive maintenance



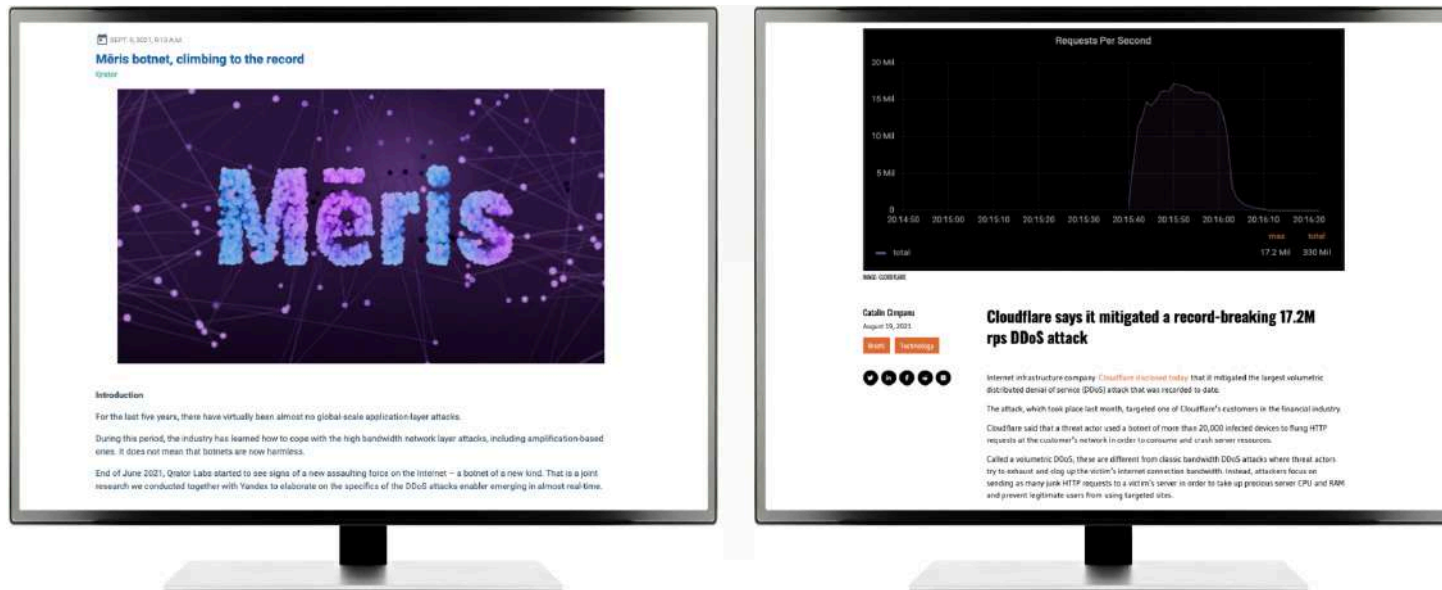
All map by and for BGStream

Event type	Country	ASN	Start time (UTC)	End time (UTC)	More info
Possible Hijack		Expected Origin AS: ZOHQ-EU, NL (AS 20911) Detected Origin AS: L3LT-3549, US (AS 3549)	2020-10-05 01:01:28		More detail
Possible Hijack		Expected Origin AS: ZOHQ-EU, NL (AS 20911) Detected Origin AS: L3LT-3549, US (AS 3549)	2020-10-05 01:01:28		More detail
Outage		SWIFTNETBROADBAND-AS SWIFTNET BROADBAND PRIVATE LIMITED, IN (AS 133113)	2020-10-05 22:18:00	2020-10-05 22:22:00	More detail
Outage		U-LAN-AS, RU (AS 48126)	2020-10-05 21:24:00		More detail
Outage		TPOGLASIE, PL (AS 38379)	2020-10-05 20:00:00	2020-10-05 20:52:00	More detail

Ransom DDoS Attacks on the Rise

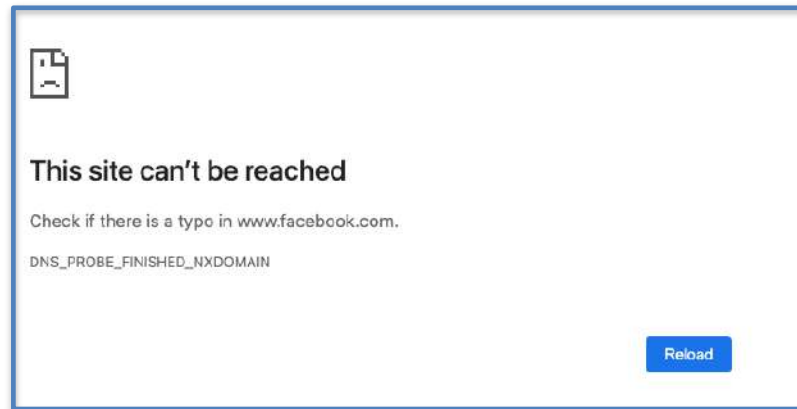
Network security attacks continue to be relevant:

- Ransom DDoS attacks on the Rise: recent Meris botnet capable to send over 300 Tbps!
- Routing attacks through BGP hijacking occur daily



Facebook Outage (4 Oct 2021)

- Over 6 hour global downtime of Facebook, Instagram, WhatsApp
- BGP management system detected an issue and withdrew routes to entire Facebook DNS infrastructure
- Circular dependencies resulted in cascading failures
 - Administrators could not reach data center any more and could not log in to fix the problem
 - Door locks used the Internet to verify credentials, so personnel could not enter building any more



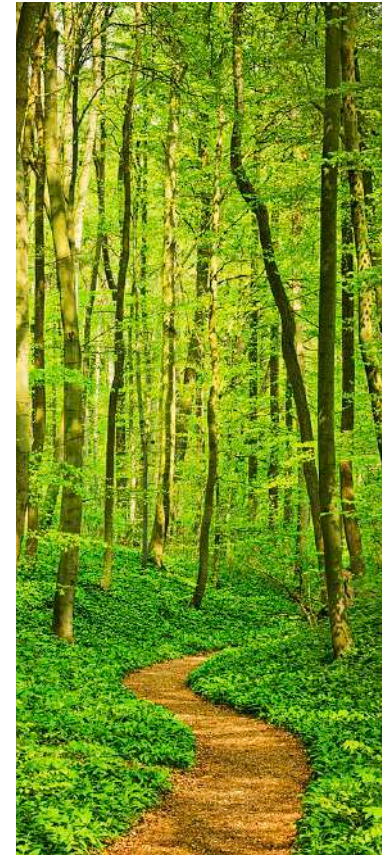
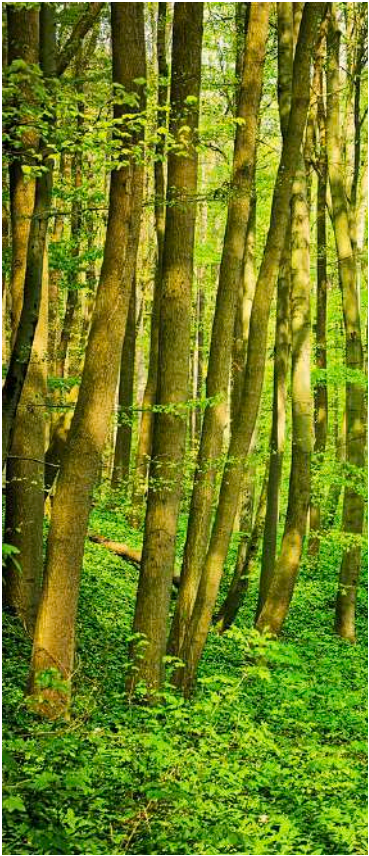
Inspirations for a New Beginning

- Many exciting next-generation Internet projects over the past 25 years
- General Future Internet Architectures (FIA)
 - XIA: enhance flexibility to accommodate future needs
 - MobilityFirst: empower rapid mobility
 - Nebula (ICING, SERVAL): support cloud computing
 - NIMROD: improved scale and flexibility
 - NewArch (FARA, NIRA, XCP)
 - RINA: clean API abstractions simplify architecture
- Content-centric FIAs: NDN, CCNx, PSIRP, SAIL / NETINF
- Routing security: BGPSEC, S-BGP, soBGP, psBGP, SPV, PGBGP, H-NPBR
- Path control: MIRO, Deflection, Path splicing, Pathlet, I3
- Inter-domain routing proposals: ChoiceNet, HLP, HAIR, RBF, AIP, POMO, ANA, ...
- Intra-domain / datacenter protocols: SDN, HALO, ...

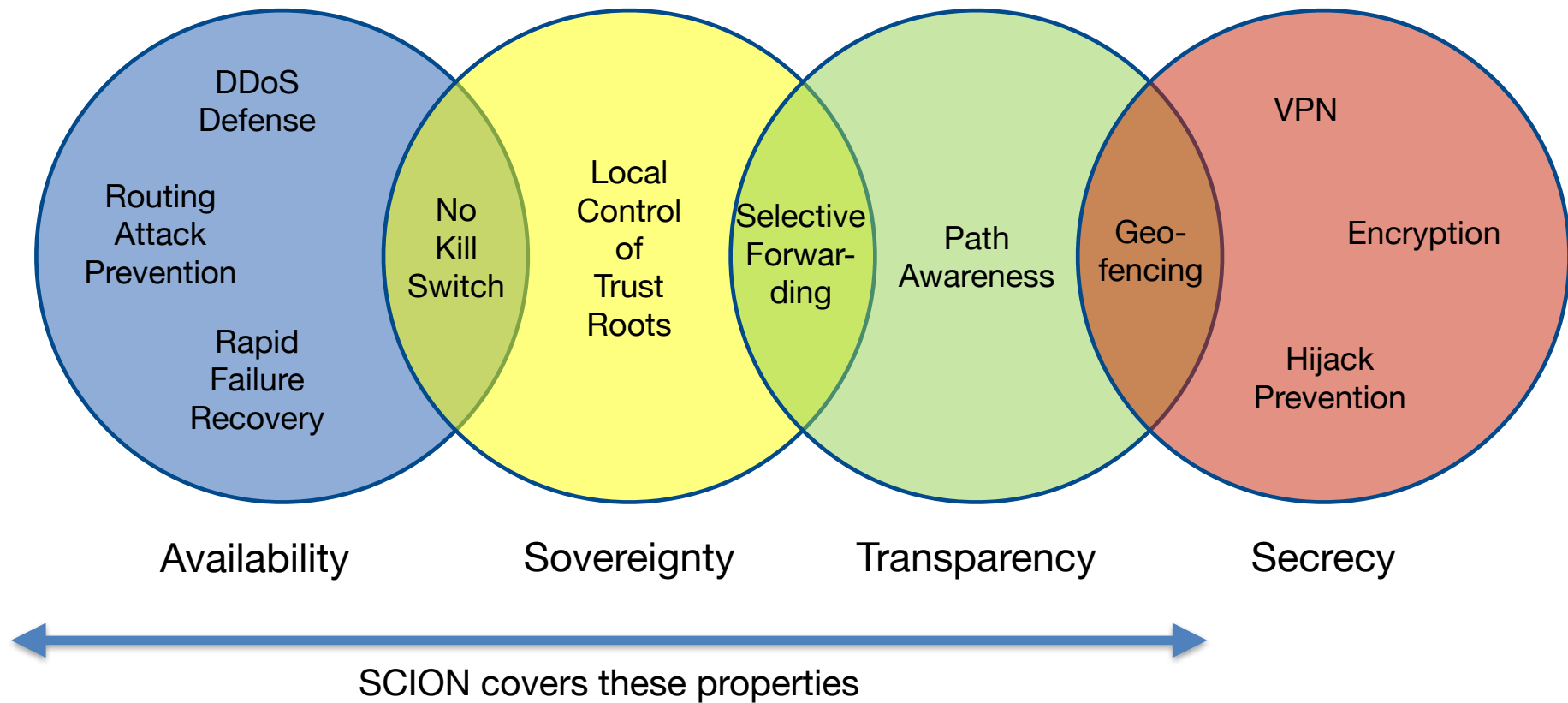
Discoveries on our Journey

- During our journey, we have encountered many interesting discoveries
- Several discoveries suggest new approaches for inter-domain networking

The real voyage of discovery consists not in seeking new landscapes, but in having new eyes. Marcel Proust

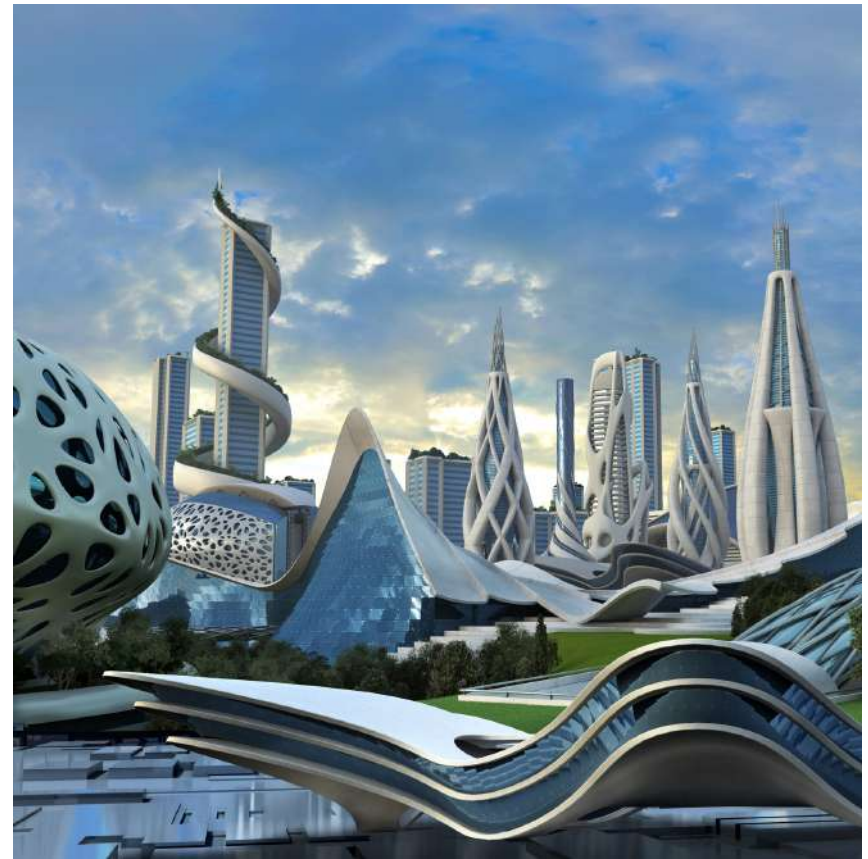


Important Properties: Availability, Sovereignty, Transparency, Secrecy



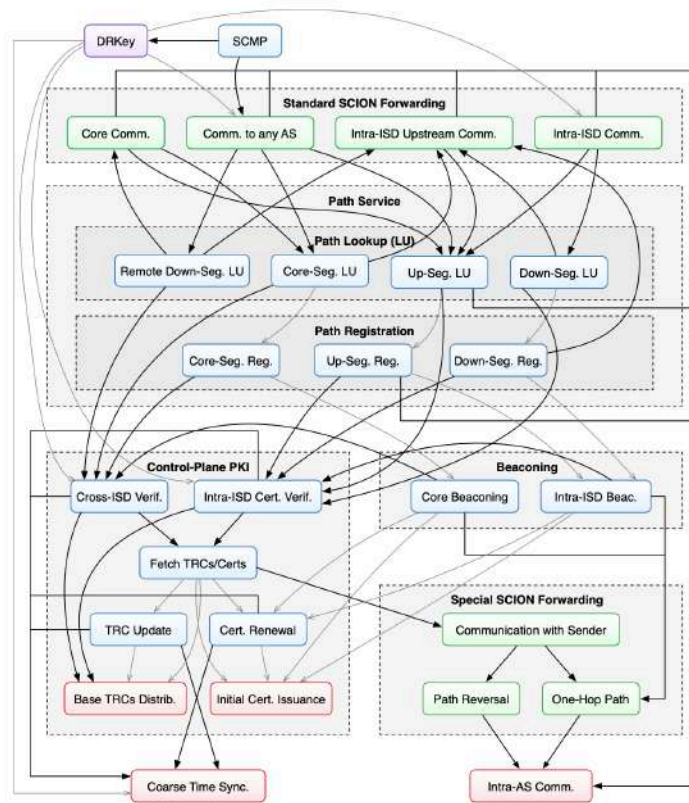
SCION Architecture Principles

- Stateless packet forwarding (no inconsistent forwarding state)
- “Instant convergence” routing
- Path-aware networking
- Multi-path communication
- Sovereignty and transparency for trust roots
- High security through design and formal verification



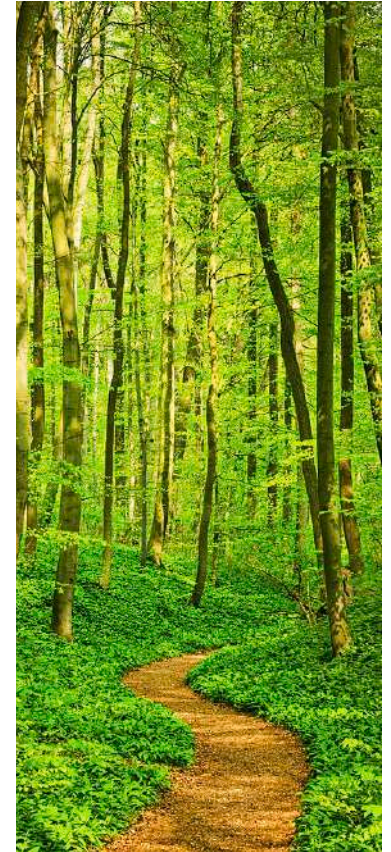
Dependency Analysis

- Absence of circular dependencies is important for reliability
- Design of SCION ensures no circular dependencies exist



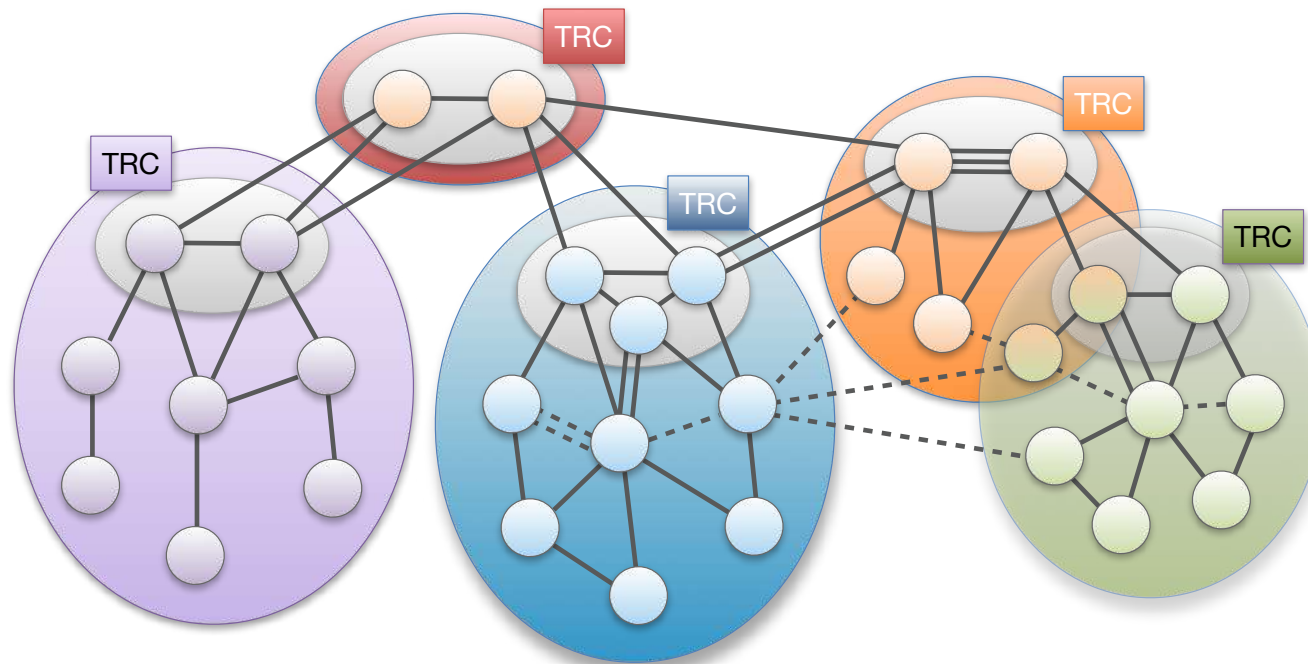
Insight: Formal Security Verification Necessary

- To achieve strong assurance for a large-scale distributed system, formal security verification is necessary
- Performing formal verification from the beginning avoids “difficult-to-verify” components
 - Many design aspects of SCION facilitate formal verification
- Collaboration with David Basin’s and Peter Müller’s teams in the VerifiedSCION project



Approach for Scalability: Isolation Domain (ISD)

- **Isolation Domain (ISD)**: grouping of Autonomous Systems (AS)
- **ISD core**: ASes that manage the ISD and provide global connectivity
- **Core AS**: AS that is part of ISD core



SCION Overview in One Slide



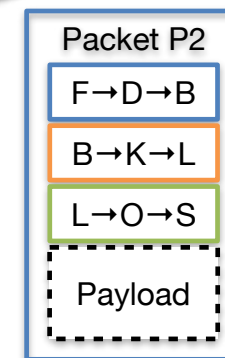
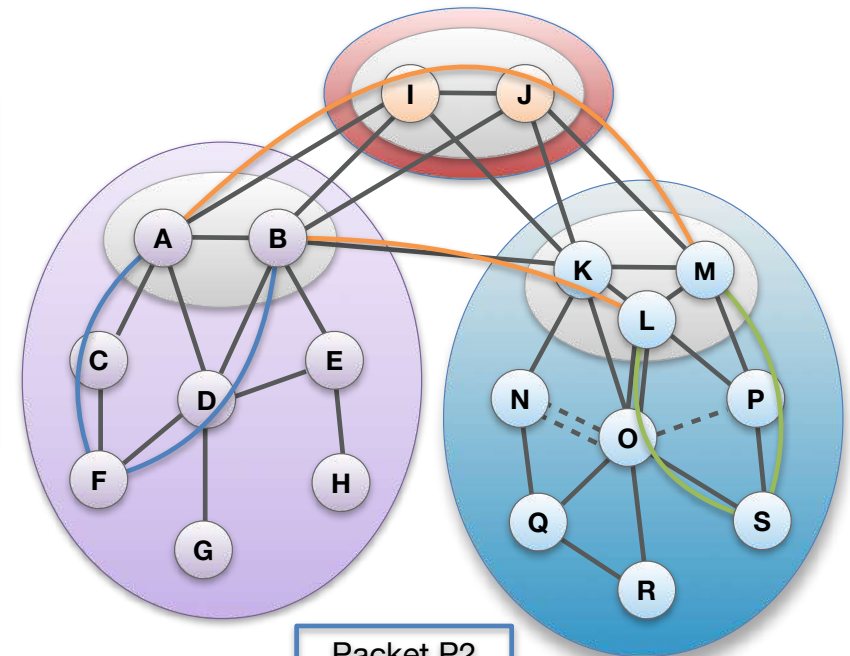
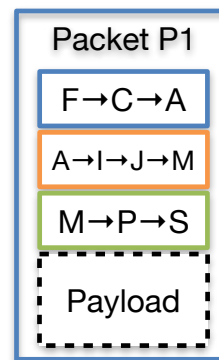
Path-based Network Architecture

Control Plane - Routing

- ❖ **Constructs** and **Disseminates** Path Segments

Data Plane - Packet forwarding

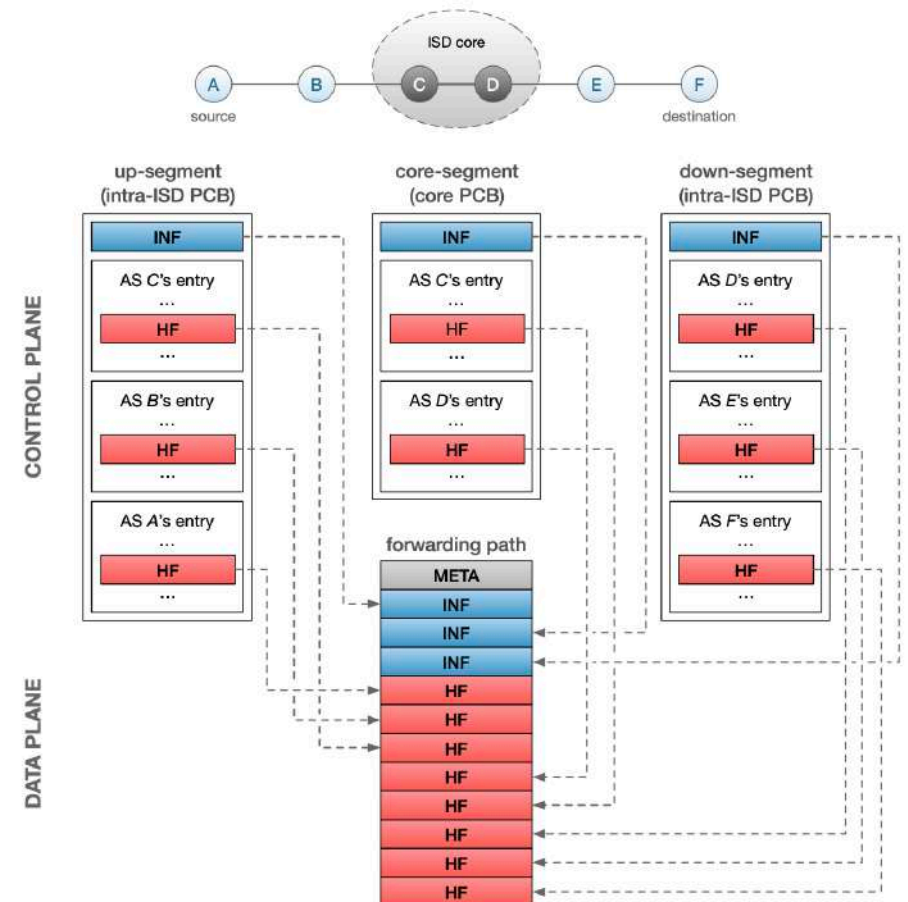
- ❖ **Combine** Path Segments to Path
- ❖ Packets contain Path
- ❖ Routers forward packets based on Path
 - ▶ Simple routers, stateless operation



SCION

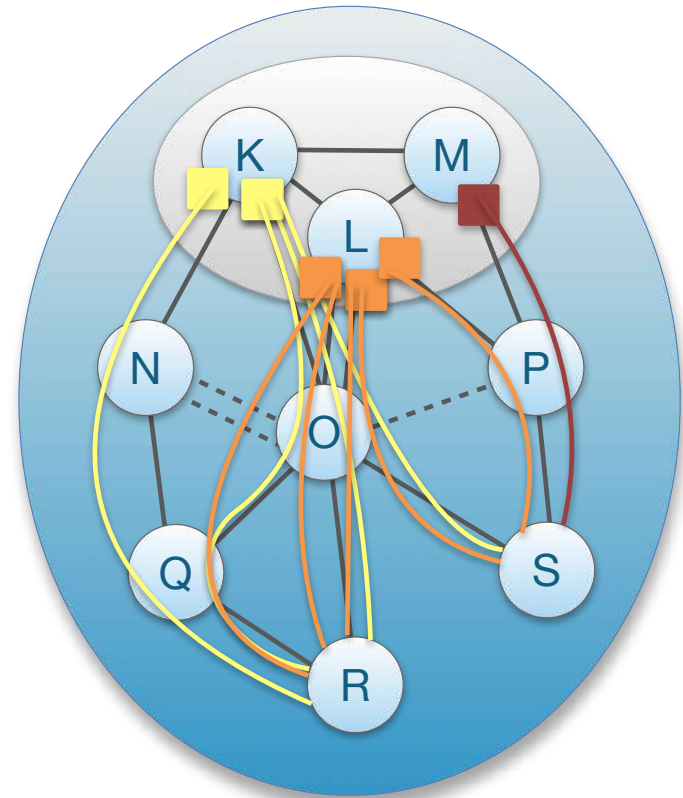
SCION Control and Data Plane

- Three main functions of the control plane
 1. Path exploration → path segments
 2. Path dissemination → senders requests segments
 3. Certificate dissemination/renewal
→ needed for segment verification
- Path segments contain forwarding and meta information. Meta information can include geographical location of routers, MTU, bandwidth, link latency...
- Senders extract the forwarding information from the path segments to form complete end-to-end paths
- Forwarding information is encoded in the packet header. Routers only verify the authenticity of the information
→ two AES operations replace longest-prefix match



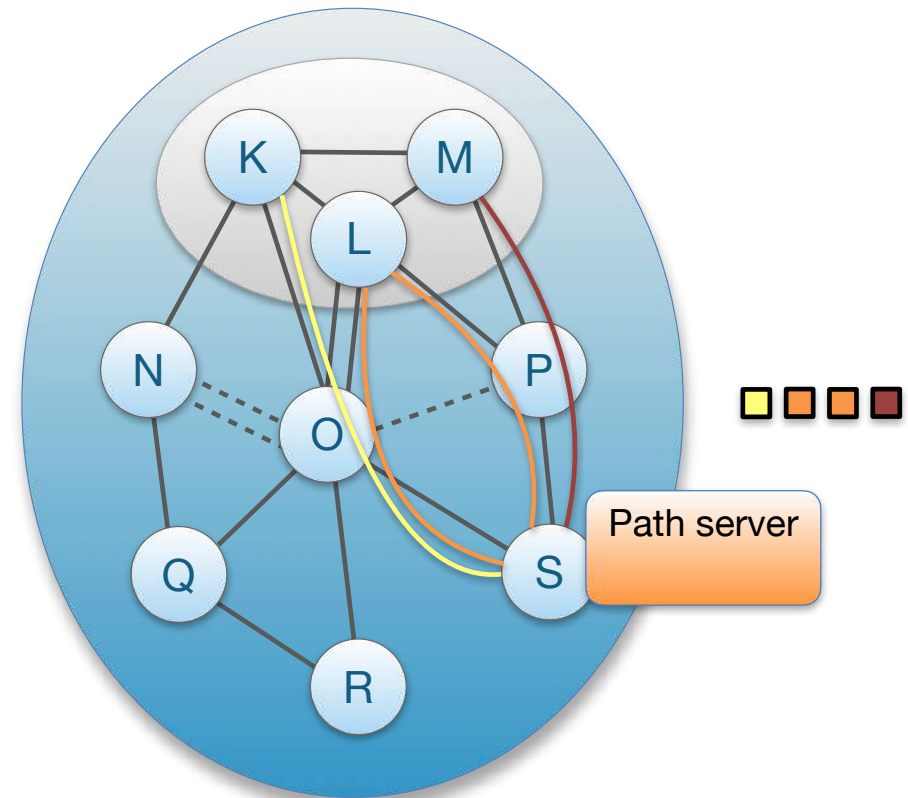
Intra-ISD Path Exploration: Beacons

- 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



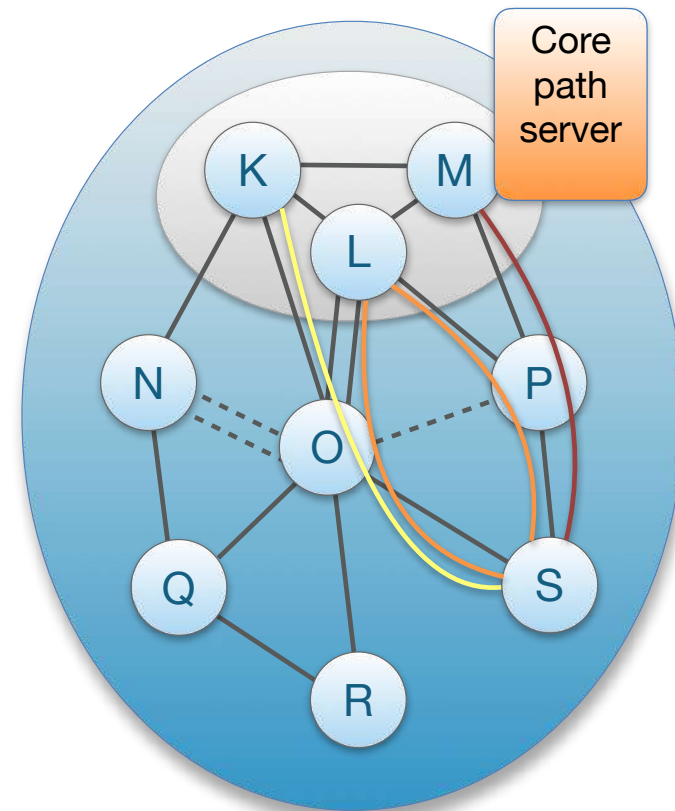
Up-Path Segment Registration

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



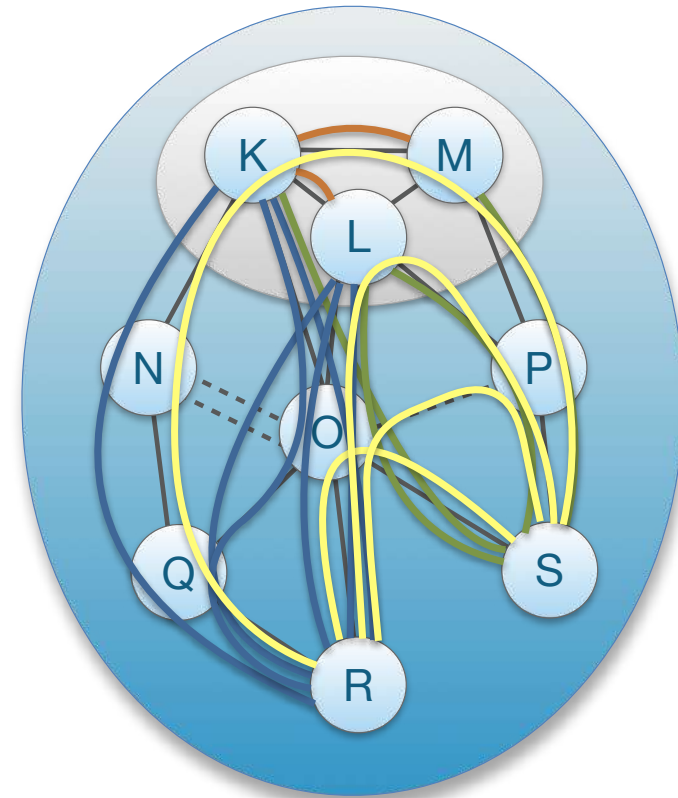
Down-Path Segment Registration

- 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



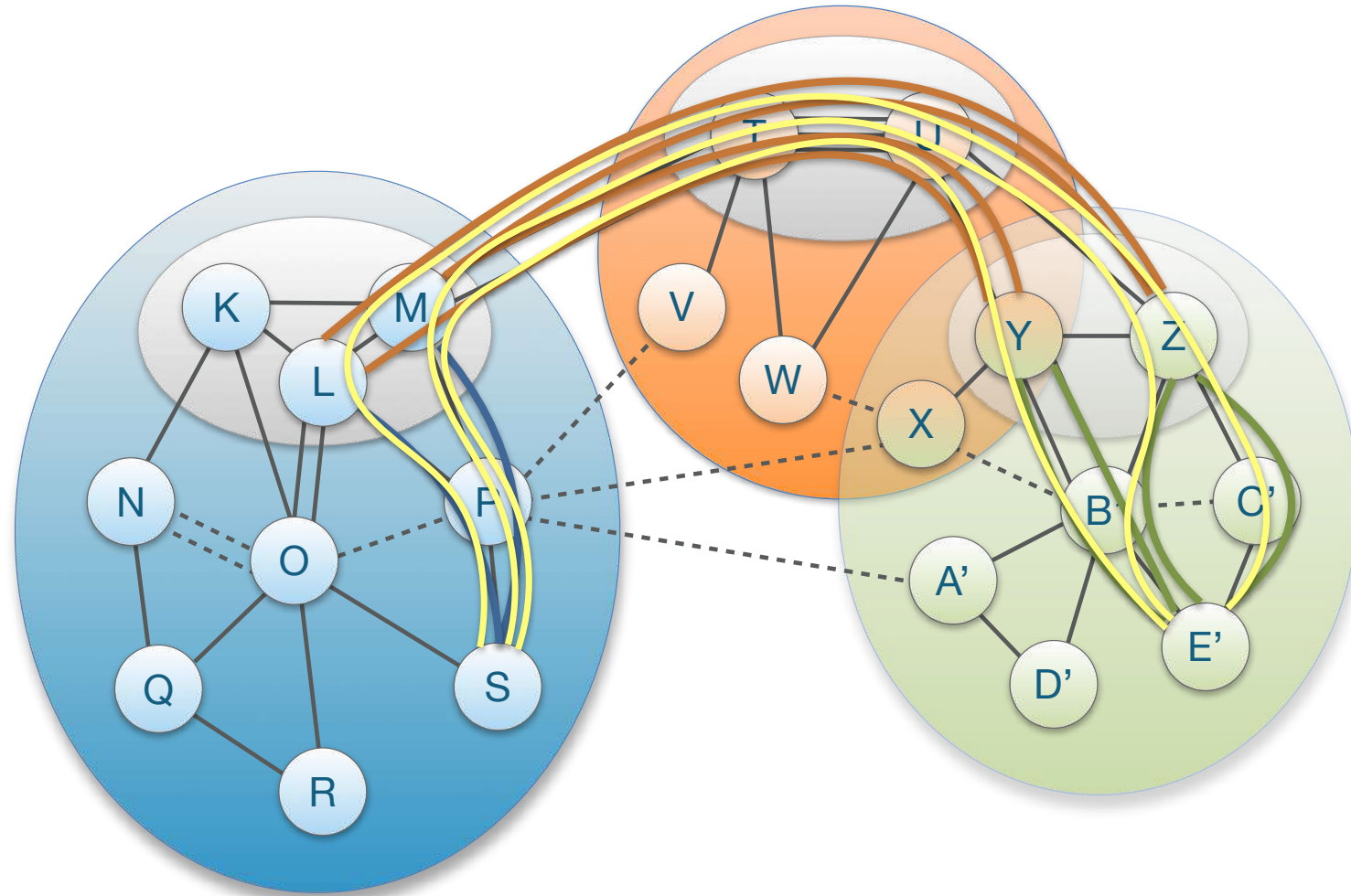
Communication within ISD

- Client obtains path segments
 - Up-path segments to local ISD core ASes (blue)
- Down-path segments to destination (green)
- Core-path segments as needed to connect up-path and down-path segments (orange)
- Client combines path segments to obtain end-to-end paths (yellow)



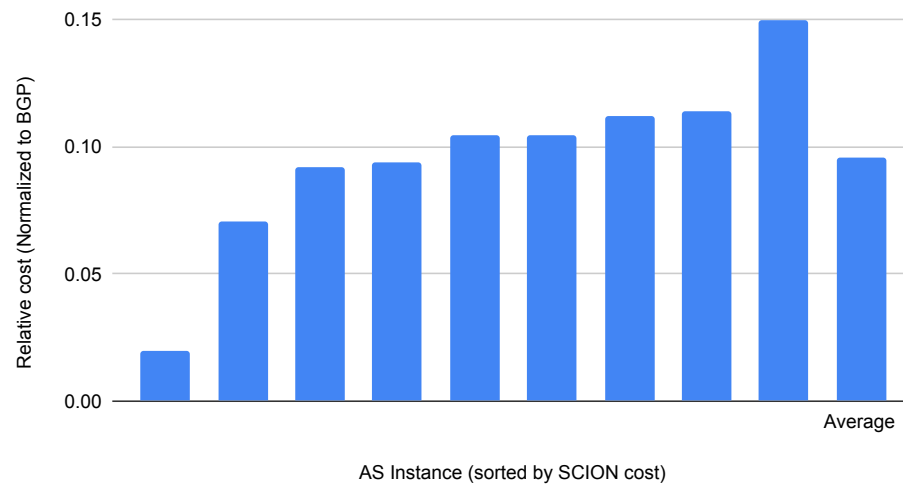
Communication to Remote ISD

- Host contacts local path server requesting $\langle \text{ISD}, \text{AS} \rangle$
- 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

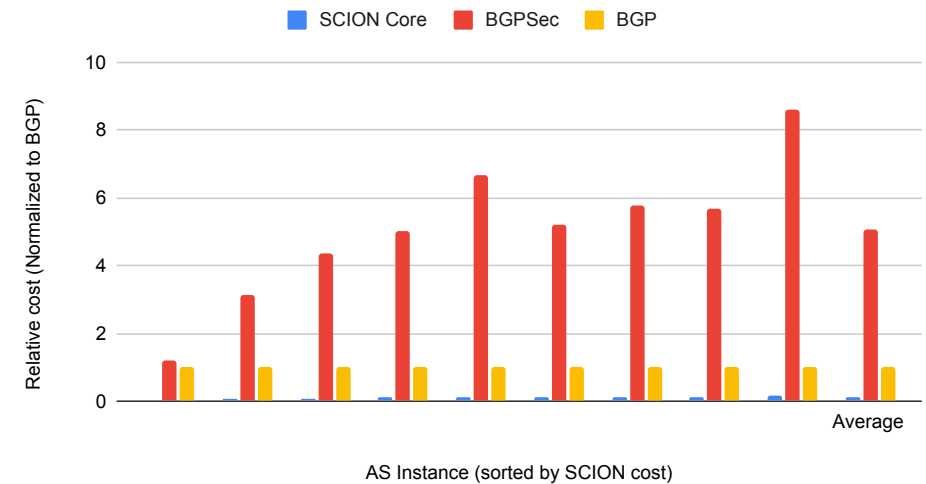


Scalability of SCION Core Beaconsing

SCION Core

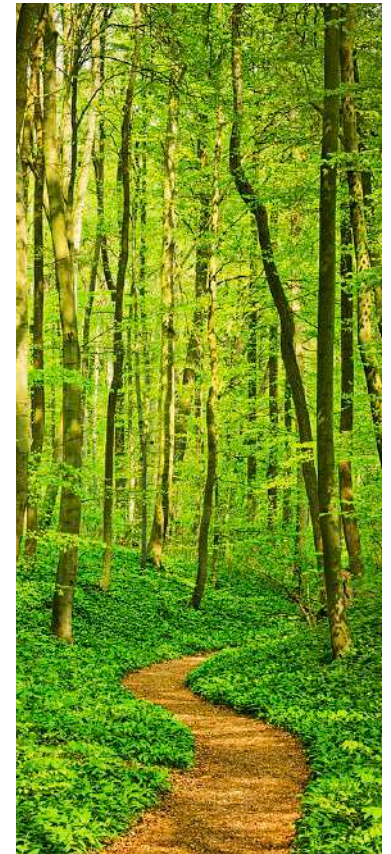


SCION Core, BGPsec and BGP



Scalability Study Results

- On a per-path basis, SCION overhead about 200 times lower than BGP, and about 1000 times lower than BGPsec
- Time-to-connectivity in SCION is over 3 orders of magnitude faster than BGP
 - The iterative convergence approach in BGP takes minutes to converge with fully updated forwarding tables (in case of small changes), sometimes even hours in case of large-scale outages



SCION Drawbacks

Initial Latency Inflation

- ❖ Additional latency to obtain paths
- ✓ BUT amortized by caching & path reuse

Bandwidth Overhead

- ❖ Due to paths in the packets
- ❖ About 80 additional bytes
- ✓ Enables path control, simpler data plane, etc

Increased Complexity in Key Mgmt.

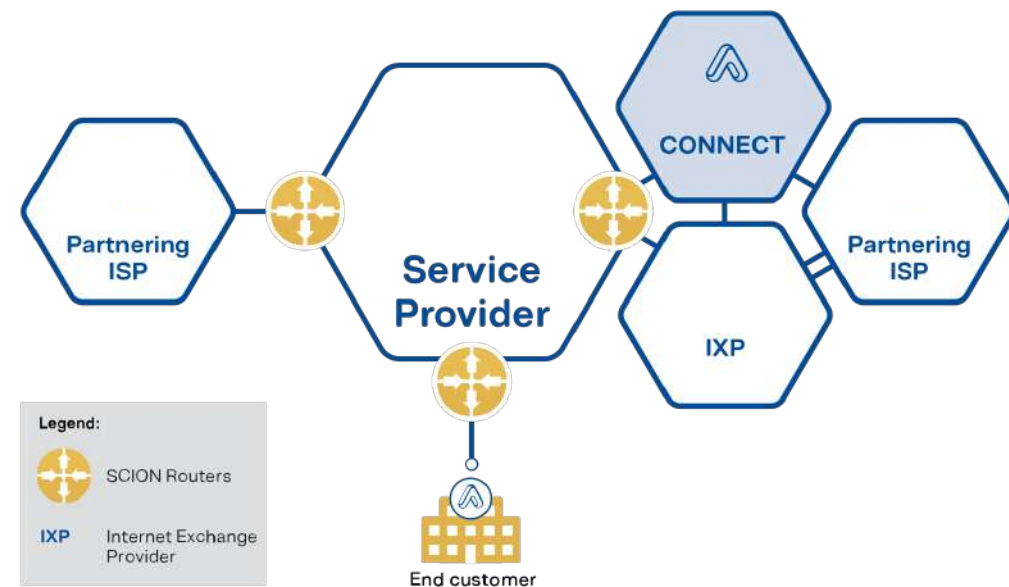
- ❖ New certificates (e.g., TRC Certificates)
- ✓ High security design

Initial Set-up Cost

- ❖ Training network operators
- ❖ Installing new infrastructures
- ✓ Offers methods to facilitate deployment

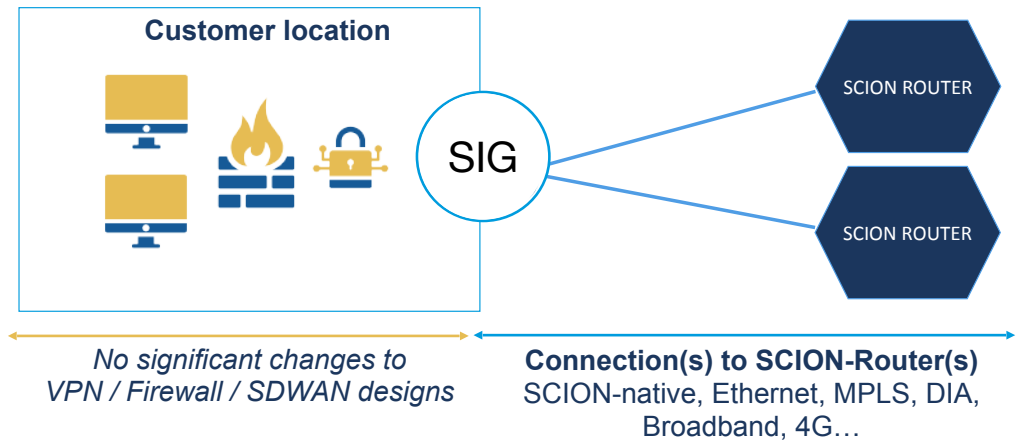
How to Deploy SCION: ISP

- CORE Routers are set up at the borders of an ISP
 - to peer with other SCION-enabled networks
 - to collect customer accesses
- No change to the internal network infrastructure of an ISP needed!



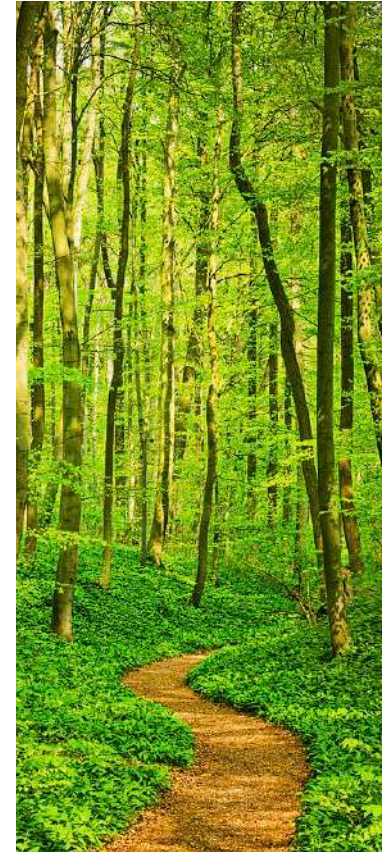
How to Deploy SCION: End Domain

- SCION IP Gateway (SIG) enables seamless integration of SCION capabilities in end-domain networks
- No upgrades of end hosts or applications needed




Insight: Incremental Deployment Possible

- Incremental deployment of a new Internet architecture is possible, operating side-by-side with BGP
- For ISPs, new architecture can be deployed with minimal effort
- For end domains, SCION-IP Gateway (SIG) offers immediate benefits without updating any end hosts
- Important: no reliance on BGP for inter-domain operation (“BGP-free”)
 - Overlay / insecure underlay should be avoided not to inherit vulnerabilities
- Re-use of intra-domain network architecture for local communication



SCION Production Network

- Led by Anapaya Systems  ANAPAYA
- **BGP-free global communication**
 - Fault independent from BGP protocol
- Deployment with international ISPs
 - Goal: First **global public secure** communication network
- Construction of SCION network backbone at select locations to bootstrap adoption
- Current deployment
 - ISPs: Swisscom, Sunrise, SWITCH, + others joining soon
 - IXPs: SwissIX offers SCION peering, + others joining soon
 - Bank deployment: 4 major Swiss banks, some in production use



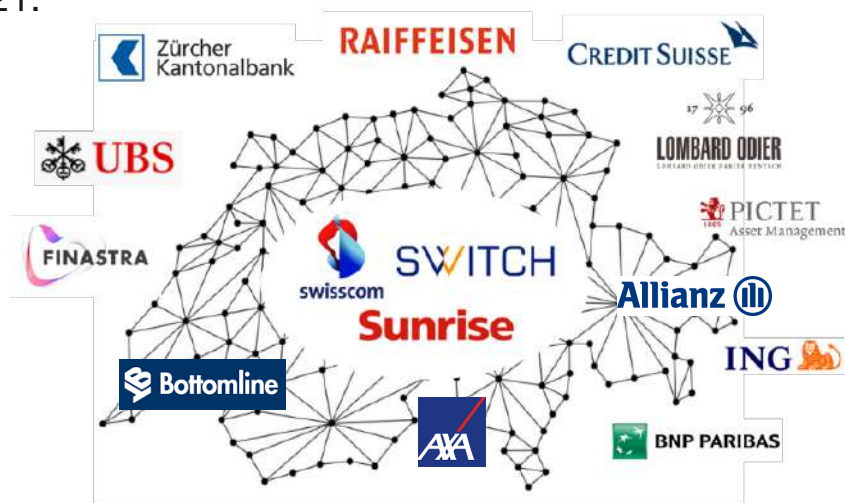
Secure Swiss Finance Network (SSFN)

The Swiss Interbanking Clearing system in numbers:

- 321 participants, including 280 banks, 14 insurance companies and 12 securities firms
- 2.9 million transaction representing 178 billion CHF per day

SSFN: Secure Swiss Finance Network

The new secure, reliable, community-based and sovereign network announced in July 2021:




SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIONALE SVIZZERA
SWISS NATIONAL BANK

SIX

Logos are illustrative

 **Andrea M. Maechler** · 1st
Member of the Governing Board...
1mo · 🌐

A great initiative, which will allow us to build a secure, more cost efficient and resilient «any-to-any» communication network for the Swiss RTGS and other critical financial markets infrastructures in Switzerland. We look forward to finalizing the pilot project with Anapaya Systems and SIX.

 **Anapaya Systems**
409 followers
1mo · 🌐

Anapaya is truly honoured to participate in the modernization of the Swiss interbank network!



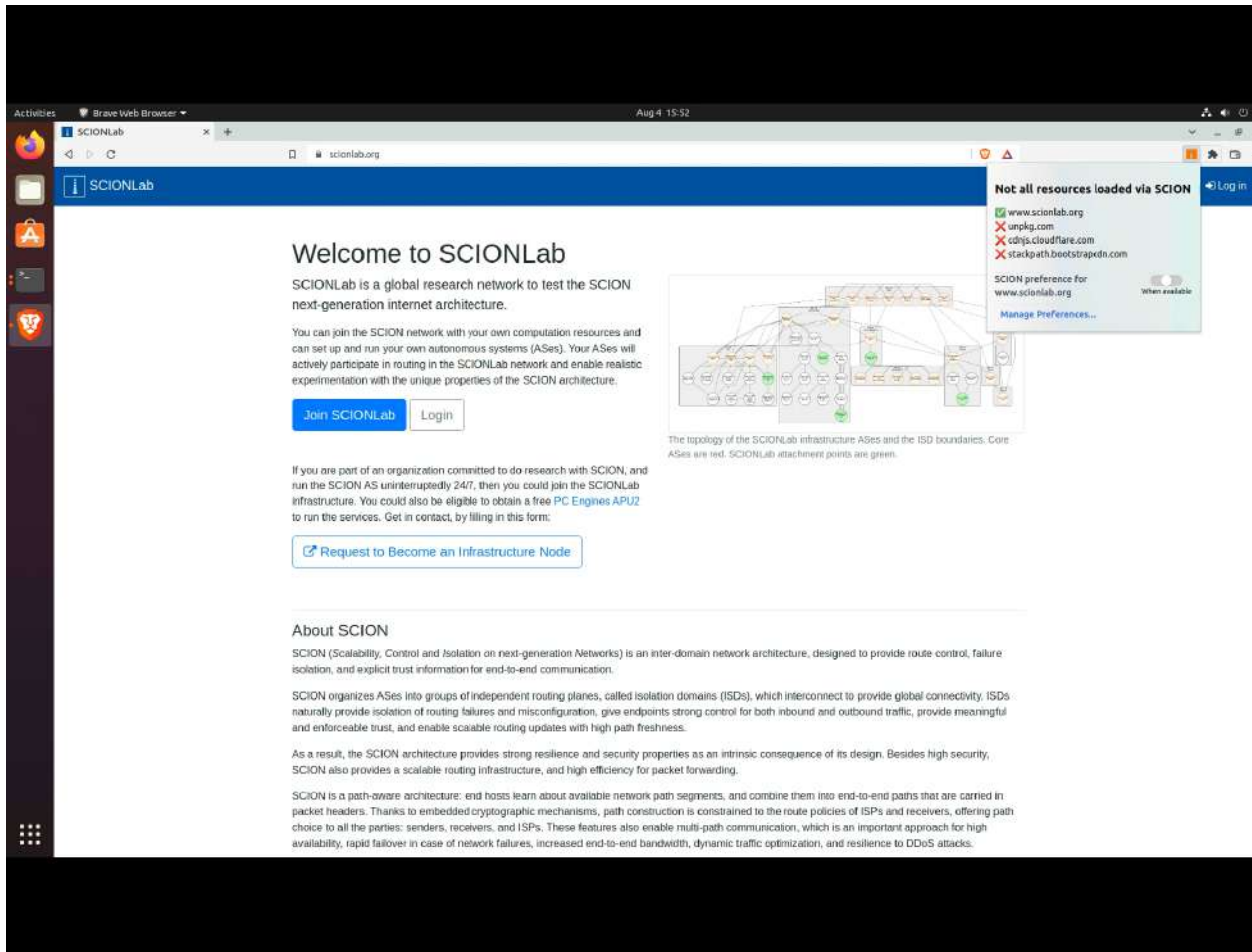
Technologies to Drive Deployment

- Changes required: change required, no change required
- SCION-IP Gateway (SIG) deployed at local AS
 - ISP (src, dst), Leaf AS (src, dst), OS (src, dst), App (src, dst)
- Secure home office: Carrier-Grade SIG deployed at ISP
 - ISP (src, dst), Leaf AS (src, dst), OS (src, dst), App (src, dst)
- In-application deployment will take advantage of SCION if present in local AS
 - ISP (src, dst), Leaf AS (src, dst), OS (src, dst), App (src, dst)
- “Happy eyeballs” standard with SCION support
 - ISP (src, dst), Leaf AS (src, dst), OS (src, dst), App (src, dst)
- Secure Backbone AS (SBAS) approach
 - ISP (src, dst), Leaf AS (src, dst), OS (src, dst), App (src, dst)



- Collaboration with Brave browser team to build native SCION communication into browser
- Without OS support, SCION-enabled browser can directly fetch web pages over the SCION network if host is within SCION-enabled network
- Compelling advantages
 - Download speed optimization
 - Specific optimizations possible: low carbon footprint paths, low delay, high bandwidth, low jitter, low loss, ...
- 60M enabled devices would help spur SCION adoption

brave Demo



Activities Brave Web Browser Aug 4 15:52

SCIONLab

Not all resources loaded via SCION

- www.scionlab.org
- unpkg.com
- cdnjs.cloudflare.com
- stackpath.bootstrapcdn.com

SCION preference for www.scionlab.org

When available

Manage Preferences...

Welcome to SCIONLab

SCIONLab is a global research network to test the SCION next-generation internet architecture.

You can join the SCION network with your own computation resources and can set up and run your own autonomous systems (ASes). Your ASes will actively participate in routing in the SCIONLab network and enable realistic experimentation with the unique properties of the SCION architecture.

[Join SCIONLab](#) [Login](#)

If you are part of an organization committed to do research with SCION, and run the SCION AS uninterruptedly 24/7, then you could join the SCIONLab infrastructure. You could also be eligible to obtain a free PC Engines APU2 to run the services. Get in contact, by filling in this form:

[Request to Become an Infrastructure Node](#)

About SCION

SCION (Scalability, Control and Isolation on next-generation Networks) is an inter-domain network architecture, designed to provide route control, failure isolation, and explicit trust information for end-to-end communication.

SCION organizes ASes into groups of independent routing planes, called isolation domains (ISDs), which interconnect to provide global connectivity. ISDs naturally provide isolation of routing failures and misconfiguration, give endpoints strong control for both inbound and outbound traffic, provide meaningful and enforceable trust, and enable scalable routing updates with high path freshness.

As a result, the SCION architecture provides strong resilience and security properties as an intrinsic consequence of its design. Besides high security, SCION also provides a scalable routing infrastructure, and high efficiency for packet forwarding.

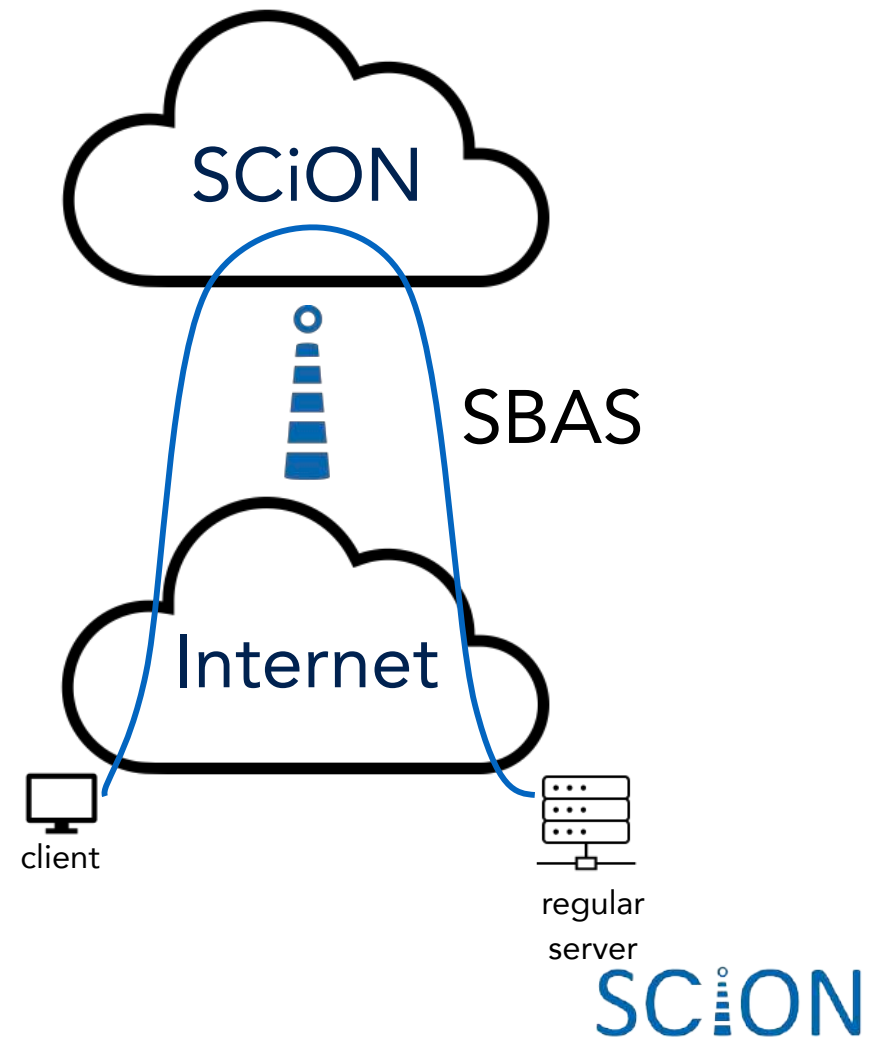
SCION is a path-aware architecture: end hosts learn about available network path segments, and combine them into end-to-end paths that are carried in packet headers. Thanks to embedded cryptographic mechanisms, path construction is constrained to the route policies of ISPs and receivers, offering path choice to all the parties: senders, receivers, and ISPs. These features also enable multi-path communication, which is an important approach for high availability, rapid failover in case of network failures, increased end-to-end bandwidth, dynamic traffic optimization, and resilience to DDoS attacks.

Secure Backbone AS (SBAS) Project

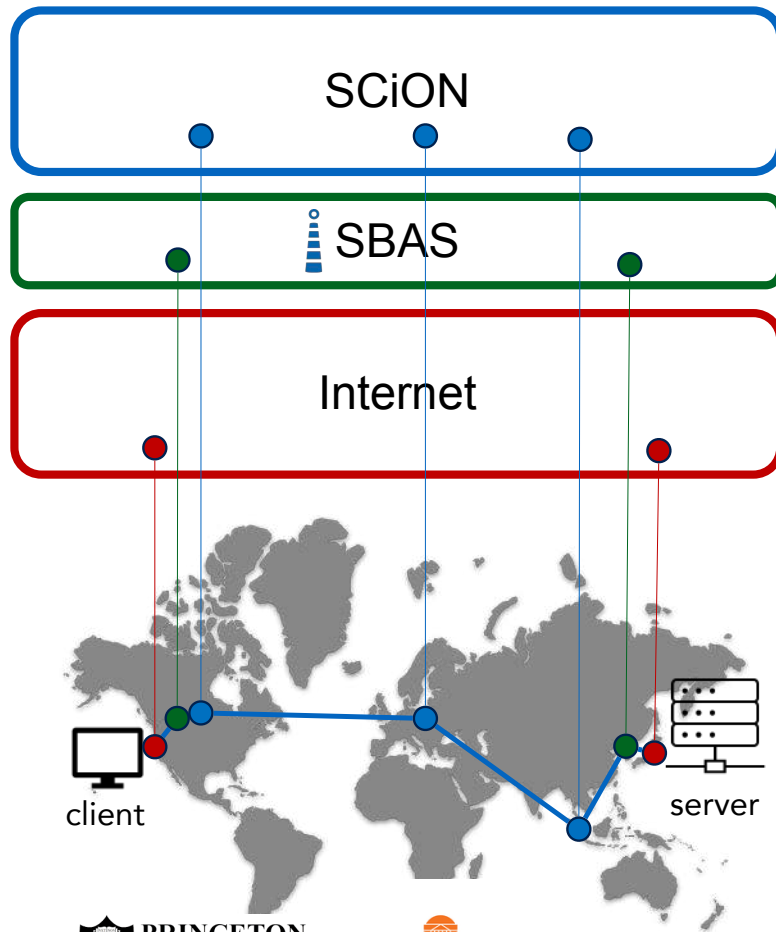
SBAS optimizes **regular** Internet traffic, using the SCiON backbone

- Optimizing latency, CO₂, security
- Transparent to Internet hosts
- Promising system to get traffic onto the SCiON network

Key point: no upgrade to source or destination!



Secure Backbone AS (SBAS) Project



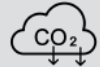
Hijack-resilient enterprise network

For security-conscious enterprise customers



Green Internet

Improved carbon efficiency for private customers



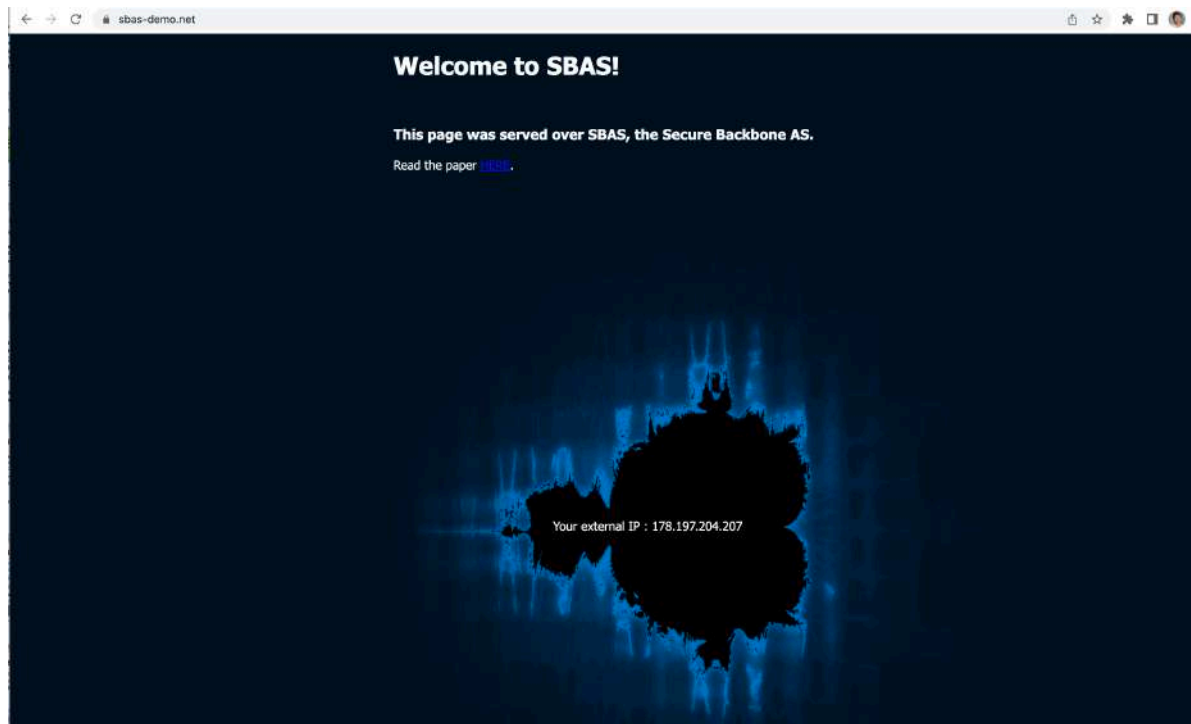
Gaming Internet

A latency-optimized home connection for private customers



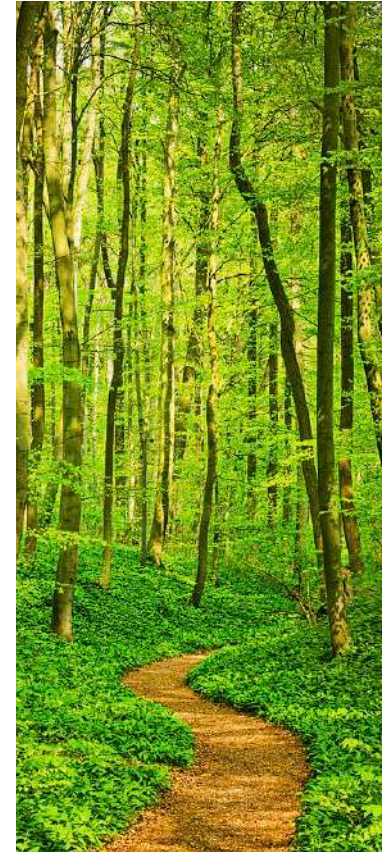
SBAS Demo is Live

- <https://www.sbas-demo.net>
- <https://sbas.netsec.ethz.ch>



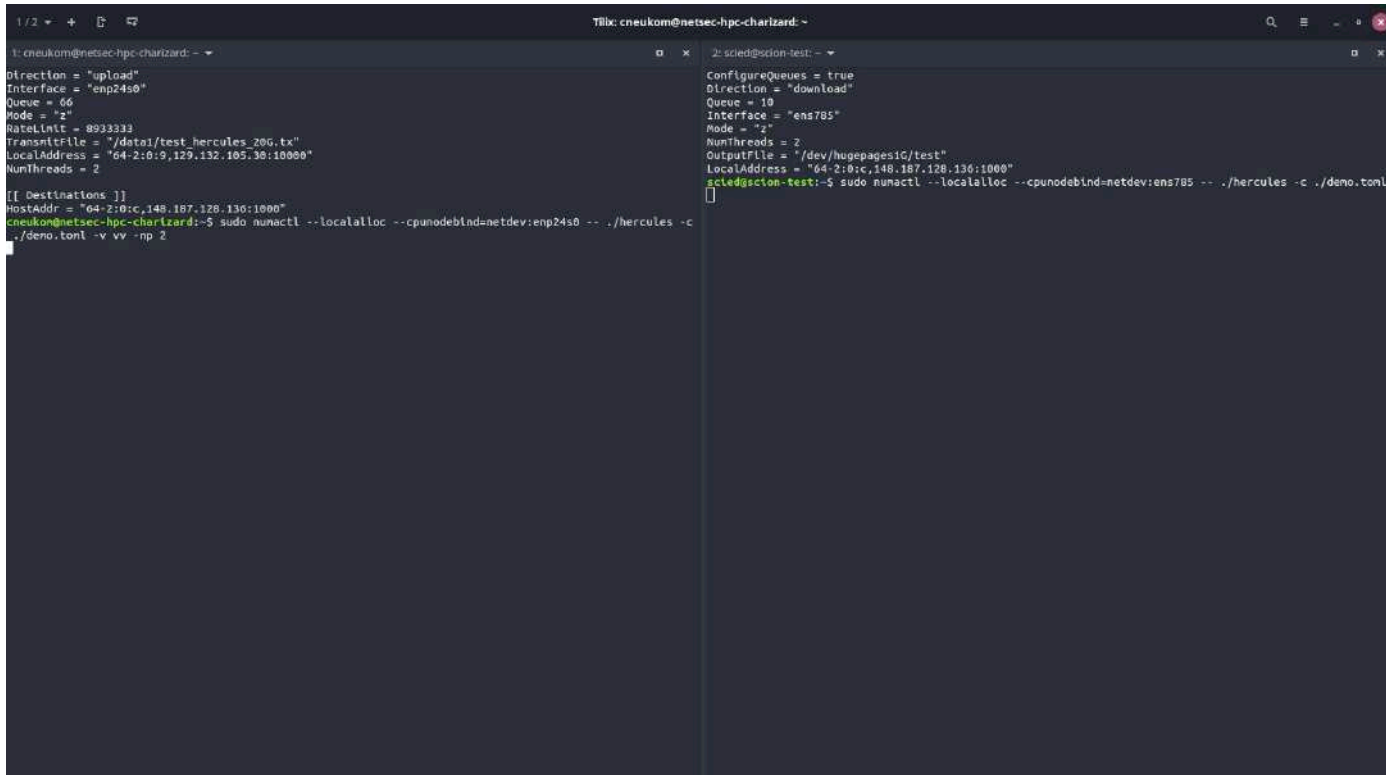
Insight: Incremental Deployment Possible

- Incremental deployment of a new Internet architecture is possible, operating side-by-side with BGP
- For ISPs, new architecture can be deployed with minimal effort
- For end domains, SCION-IP Gateway (SIG) offers immediate benefits without updating any end hosts
- Important: no reliance on BGP for inter-domain operation (“BGP-free”)
 - Overlay / insecure underlay should be avoided not to inherit vulnerabilities
- Re-use of intra-domain network architecture for local communication



Demo: Sending 20Gbytes ETH to CSCS

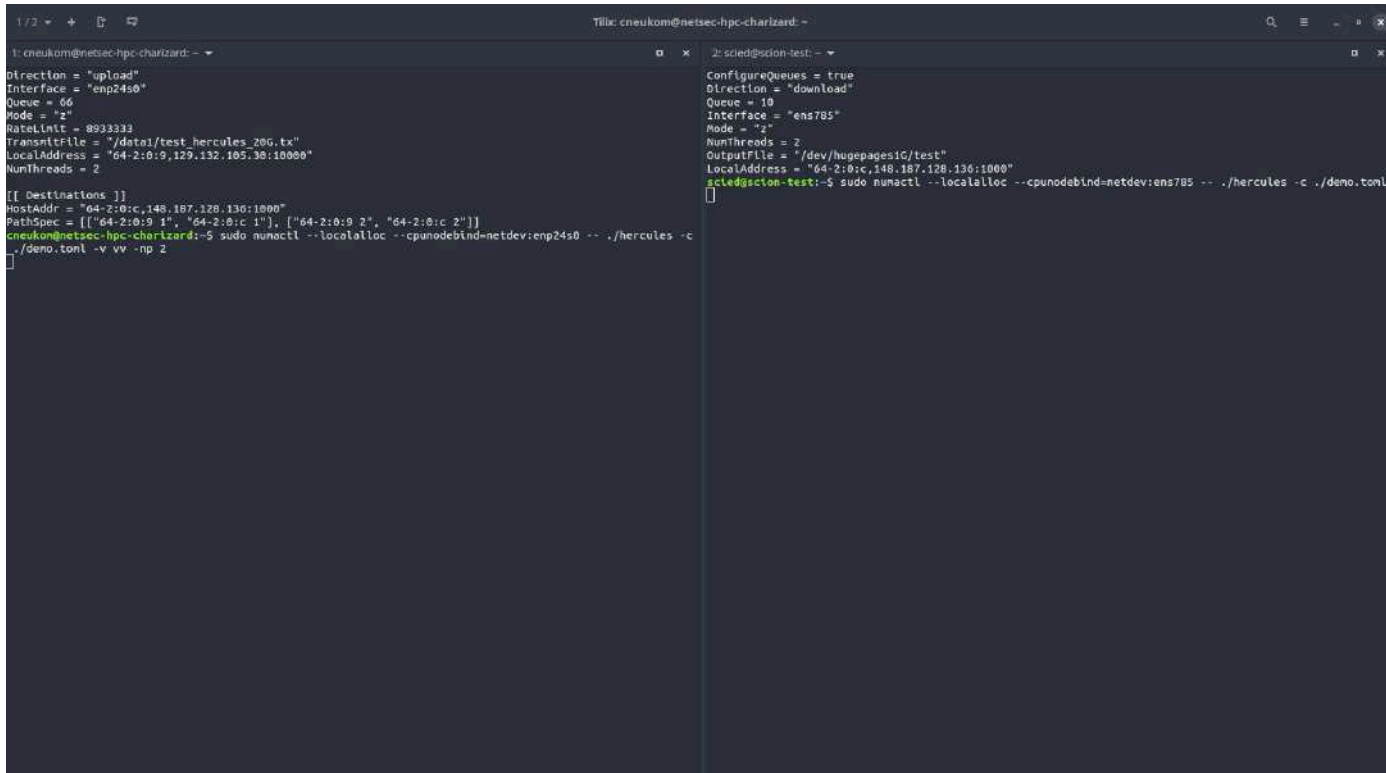
- Single path metrics
 - Duration: 14.6 s
 - Avg: 11 Gbps
 - Max: 16.4 Gbps



```
1: cneukom@netsec-hpc-charizard: ~  
Direction = "upload"  
Interface = "enp24s0"  
Queue = 66  
Mode = "z"  
RateLimit = 8933333  
TransmitFile = "/data/test_hercules_20G.tx"  
LocalAddress = "64-2:0:9,129.132.105.38:10000"  
NumThreads = 2  
[[ Destinations ]]  
HostAddr = "64-2:0:c,148.187.128.136:1000"  
cneukom@netsec-hpc-charizard:~$ sudo numactl --localalloc --cpunodebind=netdev:enp24s0 -- ./hercules -c  
./demo.toml -v vv -np 2  
2: scied@scion-test: ~  
ConfigureQueues = true  
Direction = "download"  
Queue = 10  
Interface = "ens785"  
Mode = "z"  
NumThreads = 2  
OutputFile = "/dev/hugepages1G/test"  
LocalAddress = "64-2:0:c,148.187.128.136:1000"  
scied@scion-test:~$ sudo numactl --localalloc --cpunodebind=netdev:ens785 -- ./hercules -c ./demo.toml
```


Demo: Sending 20Gbytes ETH to CSCS

- 2-paths used, as both ETH and CSCS have 2 SCION connections to SWITCH
 - Duration: 8.1 s
 - Avg: 20 Gbps
 - Max: 30 Gbps



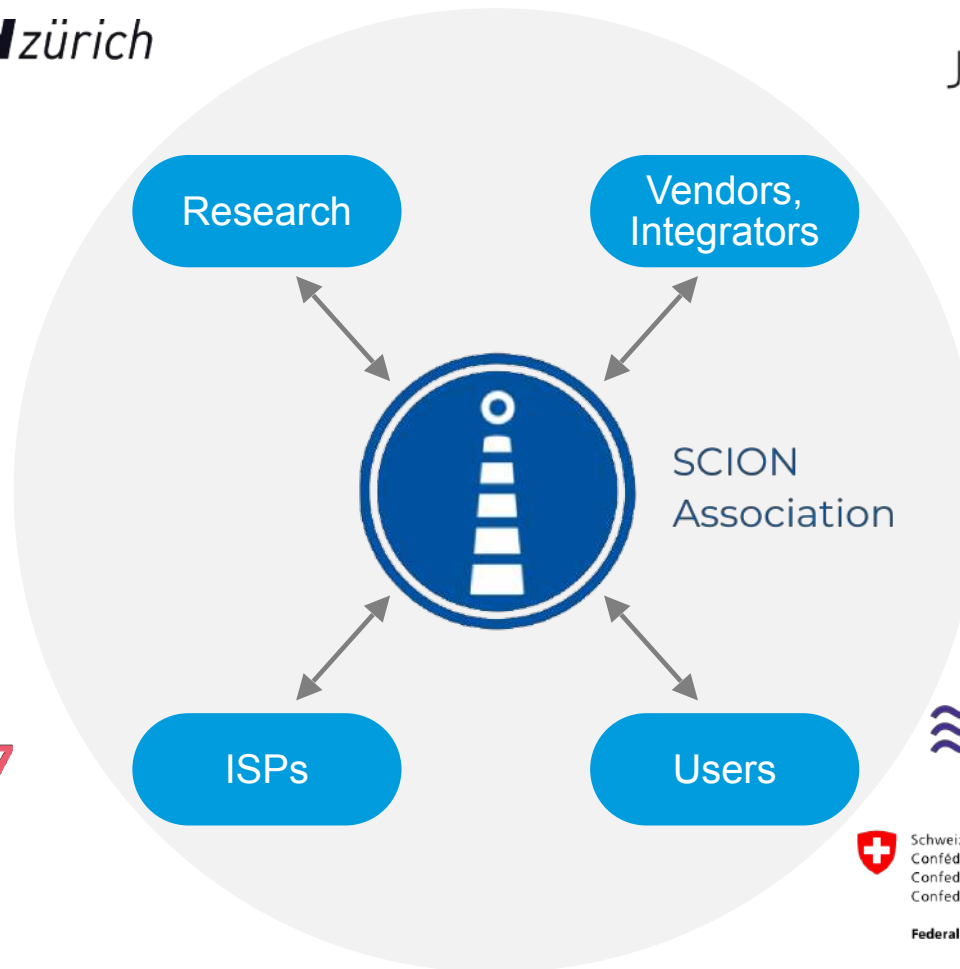
The image shows two terminal windows side-by-side. The left window is titled '1: cneukom@netsec-hpc-charizard: ~' and displays SCION configuration for an 'upload' direction. It specifies interface 'enp24s0', queue 66, mode 'z', and a transmit file '/data1/test_hercules_20G.tx'. It also shows a local address and a list of destinations. The right window is titled '2: scied@scion-test: ~' and shows configuration for a 'download' direction. It specifies interface 'ens785', queue 10, mode 'z', and an output file '/dev/hugepages1G/test'. It also shows a local address and a list of destinations. Both windows show the execution of 'sudo nupactl --localalloc --cpunodebind-netdev:enp24s0 -- ./hercules -c ./demo.toml'.

```
1: cneukom@netsec-hpc-charizard: ~
Direction = "upload"
Interface = "enp24s0"
Queue = 66
Mode = "z"
RateLimit = 8933333
TransmitFile = "/data1/test_hercules_20G.tx"
LocalAddress = "64-2:0:9,129,132,105,38:10000"
NumThreads = 2

[[ Destinations ]]
HostAddr = "64-2:0:c,148,187,128,136:1000"
PathSpec = [{"64-2:0:9 1", "64-2:0:c 1"}, {"64-2:0:9 2", "64-2:0:c 2"}]
cneukom@netsec-hpc-charizard:~$ sudo nupactl --localalloc --cpunodebind-netdev:enp24s0 -- ./hercules -c
./demo.toml -v vv -np 2

2: scied@scion-test: ~
ConfigureQueues = true
Direction = "download"
Queue = 10
Interface = "ens785"
Mode = "z"
NumThreads = 2
OutputFile = "/dev/hugepages1G/test"
LocalAddress = "64-2:0:c,148,187,128,136:1000"
scied@scion-test:~$ sudo nupactl --localalloc --cpunodebind-netdev:ens785 -- ./hercules -c ./demo.toml
```

SCION Association



ETH zürich



EPFL



SWITCH

proximus

Sunrise



Init7



aspo

ETH zürich



ICRC



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK



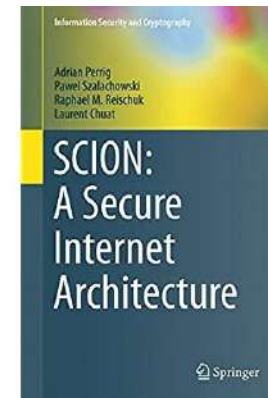
SCION Association

SCION Extensions

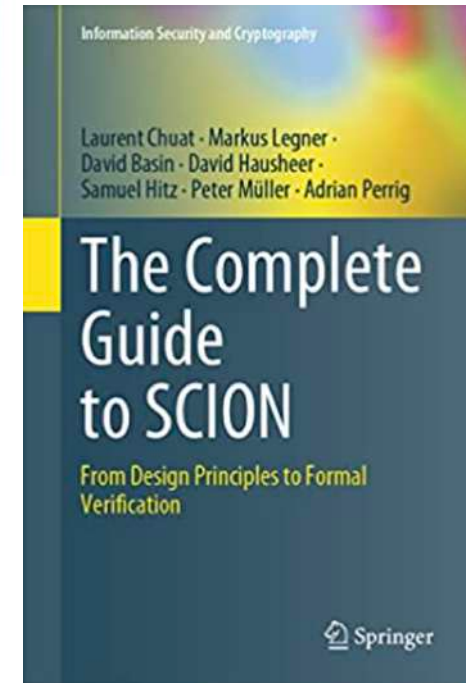


Online Resources

- <https://www.scion-architecture.net>
 - Book, papers, videos, tutorials
- <https://www.scionlab.org>
 - SCIONLab testbed infrastructure
- <https://www.anapaya.net>
 - SCION commercialization
- <https://github.com/scionproto/scion>
 - Source code
- SCION Association: <https://www.scion.org>



2017



2022

SCION Summary

- SCION: Next-generation Internet **you can use today!**
- **High-performance**
 - Path-aware network enables application-specific optimizations to provide **enhanced efficiency**
 - Multi-path communication enables simultaneous use of multiple paths, increasing available bandwidth
- **Secure, high assurance, high availability**
 - Per-packet authentication verification possible on routers
 - Formal verification of protocols and code
 - Immune against routing attacks, e.g., BGP prefix hijacking

SCION Team

