Operational Aspects of SCION

Samuel Hitz – hitz@anapaya.net

PANRG IETF 118 – November 2023

Agenda

- The SCION Internet Ecosystem
- Bootstrapping a SCION Isolation Domain
- How to become a SCION AS
- IP-in-SCION tunneling
- Using SCION today: Use Cases and productive deployments
- The long-term need for standardization

The SCION Internet Ecosystem

SCION Backbone

- Community of ISPs that deploy and interconnect SCION Routers
- Think of each SCION Router as a “waypoint” of a SCION end-to-end path
- Isolation Domains are “logical layers” – each ISP can be part of multiple ISDs

SCION Network Edge

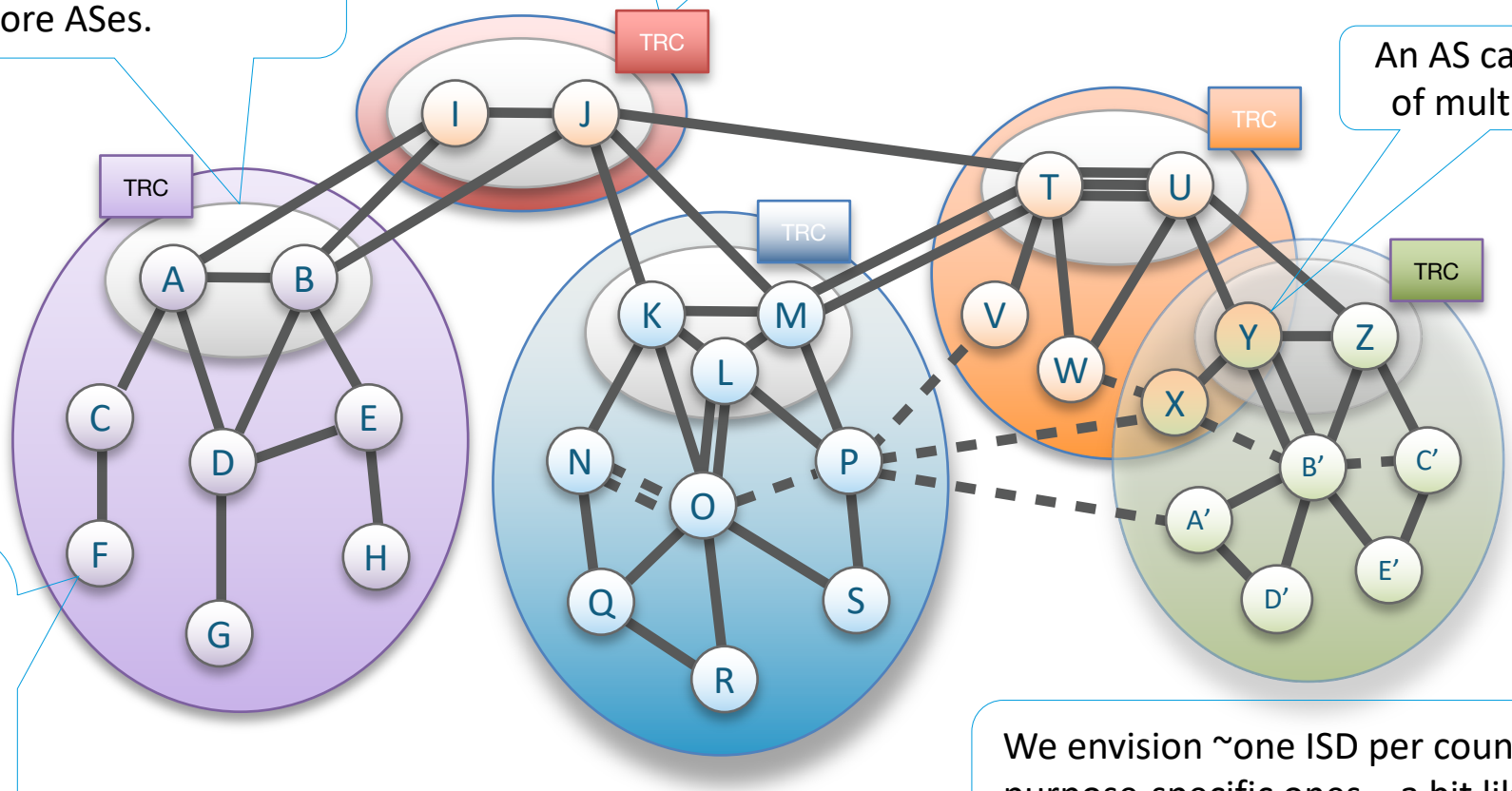
- SCION-IP Gateways provide SCION forwarding and IP-in-SCION tunneling functionality
- SCION-IP Gateways come in different flavors: physical (on-prem), virtual (cloud, uCPE), carrier-grade
- SCION-IP Gateways can choose paths based on requirements: Network performance metrics (latency, jitter, drop rate), Trust/ geographical jurisdiction

Recap: Isolation Domains

Each isolation domain defines a trust root configuration (TRC) and a routing hierarchy

Each ISD core that manages the ISD is made up of a set of core ASes.

An AS can be part of multiple ISDs

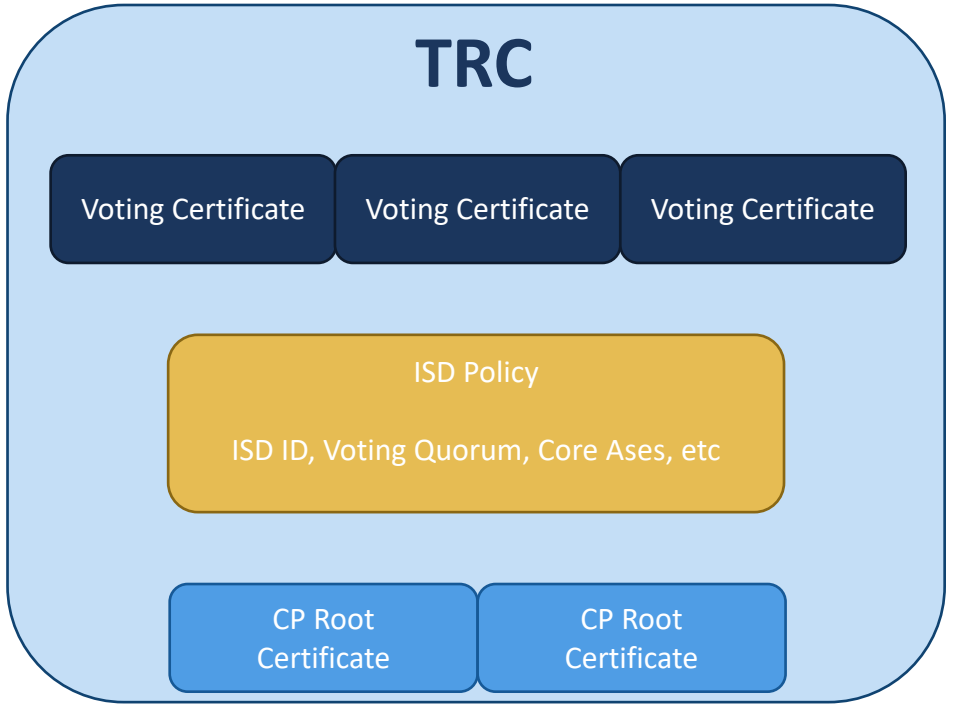


Each AS needs a certificate to be a member of an ISD. This enables access control and policy enforcement for ISDs.

We envision ~one ISD per country and a number of purpose-specific ones – a bit like top-level domains (ccTLDs, .com, .net, etc)

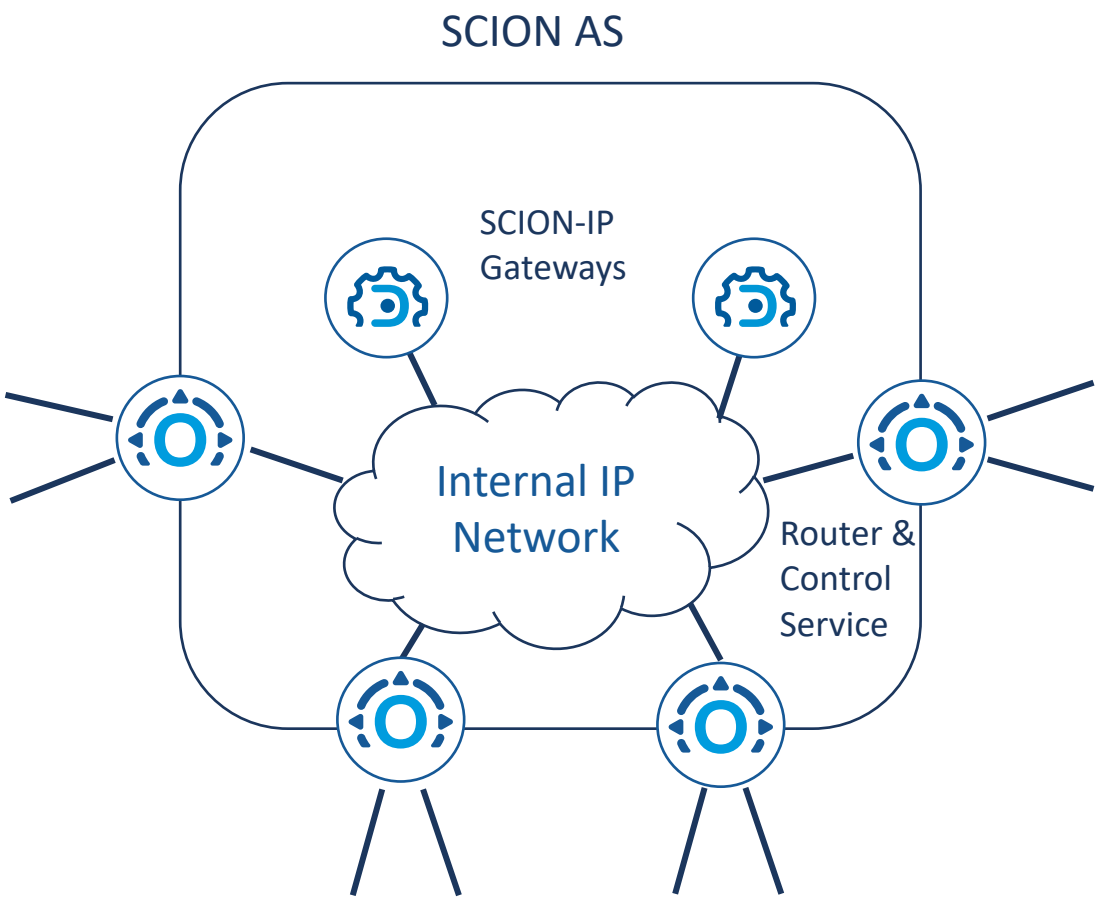
Bootstrapping a SCION Isolation Domain

- Step 1: Define Governance
  - Voting Members
  - Certificate Authorities
  - Core ASes
- Step 2: Get an ISD ID allocated
  - Currently, Anapaya assigns ISD IDs but there are plans to hand this over to the SCION Association
  - Future: Existing numbering authorities (IANA, RIRs)
- Step 3: Create the Trust Root Configuration
  - TRC Signing Ceremony https://docs.scion.org/en/latest/cryptography/trc-signing-ceremony-phases-base.html
- Creating and operating an ISD comes with certain overheads and the need for an ISD should be carefully considered



SCION AS Overview

- SCION Routers
  - Implement the SCION Control and Data Plane
  - Strategically deployed to peer with other SCION providers or aggregate customer ASes
  - Run on COTS x86 servers
- SCION-IP Gateways
  - Gateways that encapsulate IP traffic in SCION – IP-in-SCION tunneling
  - Provide means for all applications and hosts to use the SCION network
- Internal IP network used for local communication



How to become a SCION AS?

- Step 1: Install SCION Routers
  - SCION Routers are deployed at the borders of the network where they peer with SCION routers of other ISPs or downstream customers.
  - Internally, SCION routers needs to be connected via an IP underlay network.
- Step 2: Get a SCION ASN and SCION AS Certificate
  - SCION ASNs are different from BGP ASNs!
  - Current numbering practice reserves the BGP ASN space in the SCION ASN space, i.e., organization with a BGP ASN will get the same SCION ASN assigned.
  - One SCION AS Certificate per Isolation Domain the AS should be part of. These need to be deployed to the SCION routers.
- Step 3: Set up SCION peerings
  - Type of peerings depend on business relationship: peer, parent/child.
  - The SCION routers can now participate in the SCION control and dataplane.
- Optional: Install SCION-IP Gateways to provide internal IP hosts connectivity via the SCION Internet

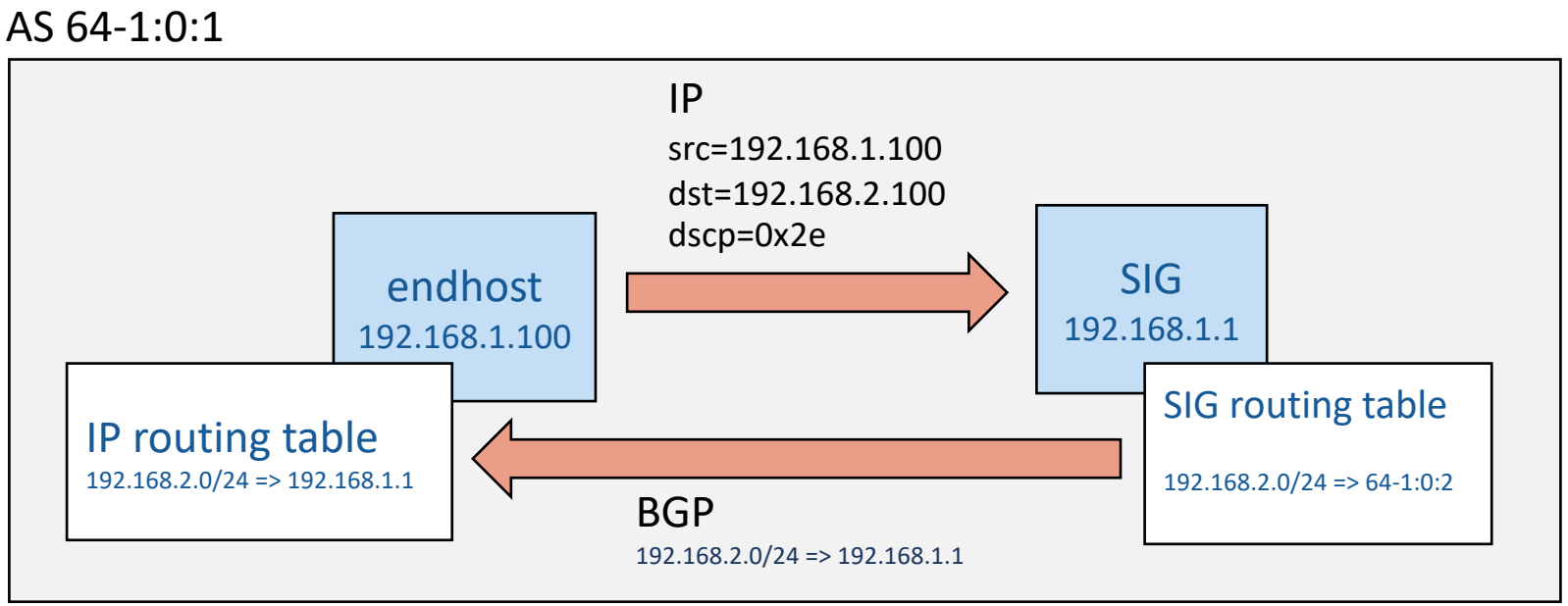
IP-in-SCION Tunneling

- Responsible for providing interoperability between IP and SCION
- The SCION-IP Gateway (SIG) encapsulates and routes IP traffic -> SCION tunnels
  - The SIG in the destination AS performs decapsulation

IP-in-SCION Tunneling - Example

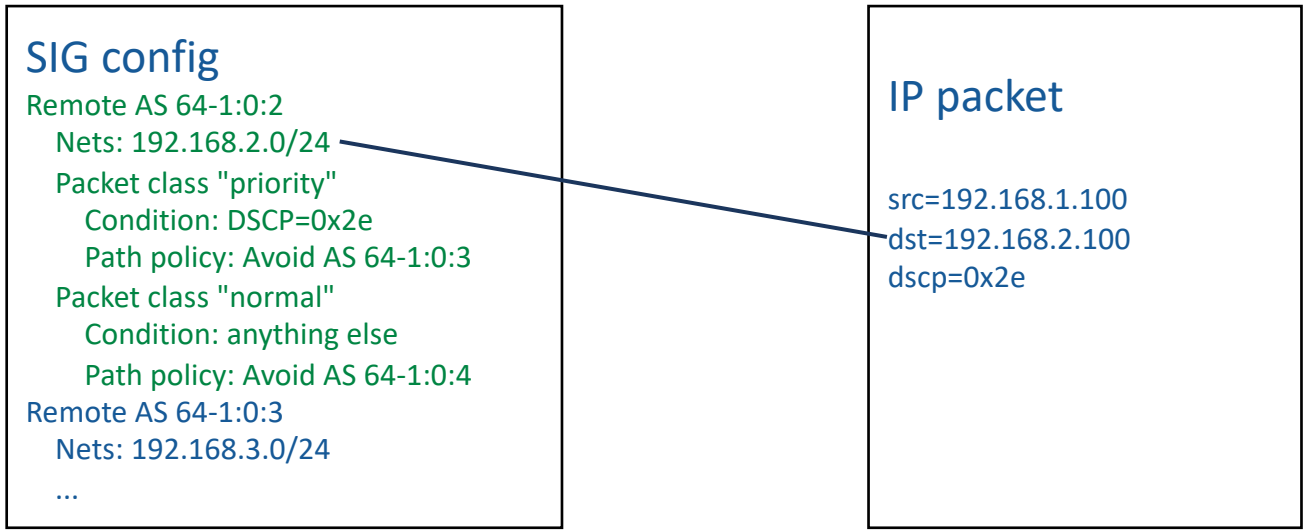
IP-in-SCION Tunneling - Example

- SIG builds internal routing table from announcements received.
- It distributes the routes to the local AS via BGP/OSPF.
- Endhost sends a packet.
- The packet is routed to the SIG.



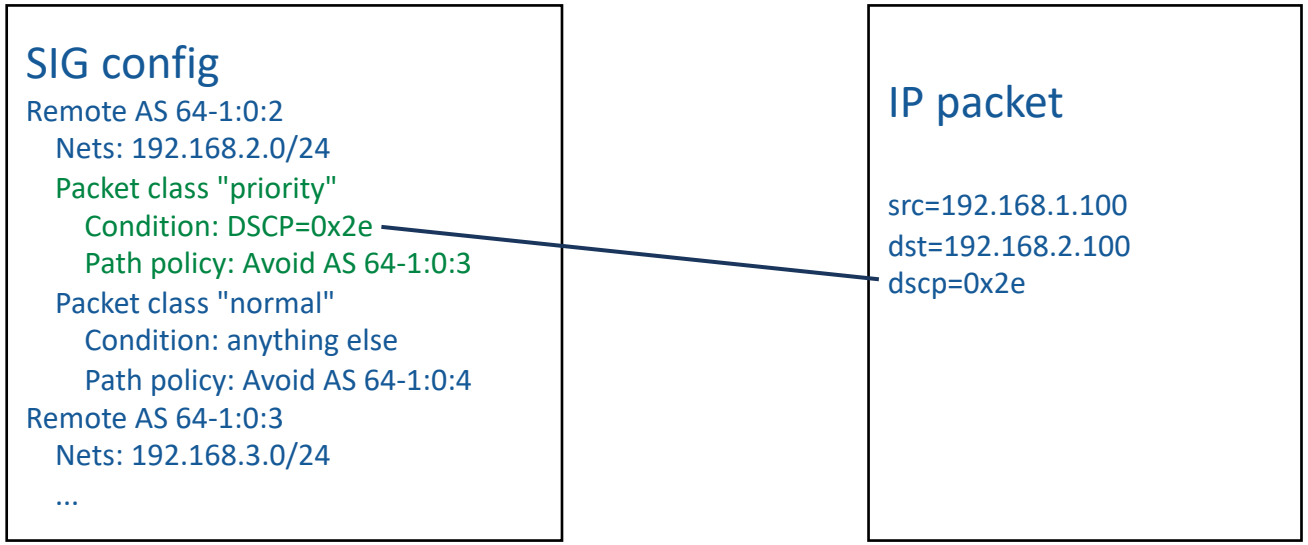
IP-in-SCION Tunneling - Example

- SIG looks at the destination IP address to find out which AS to send it to.
- Address 192.168.2.1 belongs to subnet 192.168.2.0/24.
- The packet should therefore go to AS 64-1:0:2.



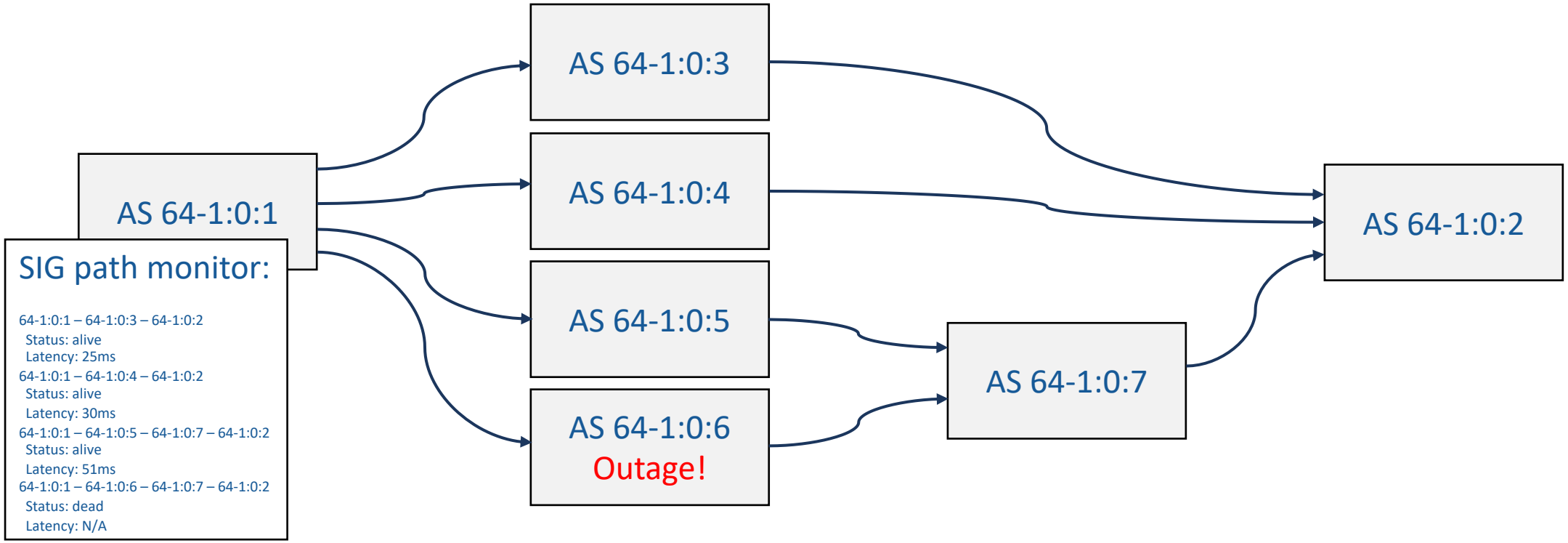
IP-in-SCION Tunneling - Example

- SIG checks which packet class the packet belongs to.
- The conditions are evaluated in order.
- This packet is in "priority" class.
- Each class has an associated path policy defining which SCION paths are permissible.



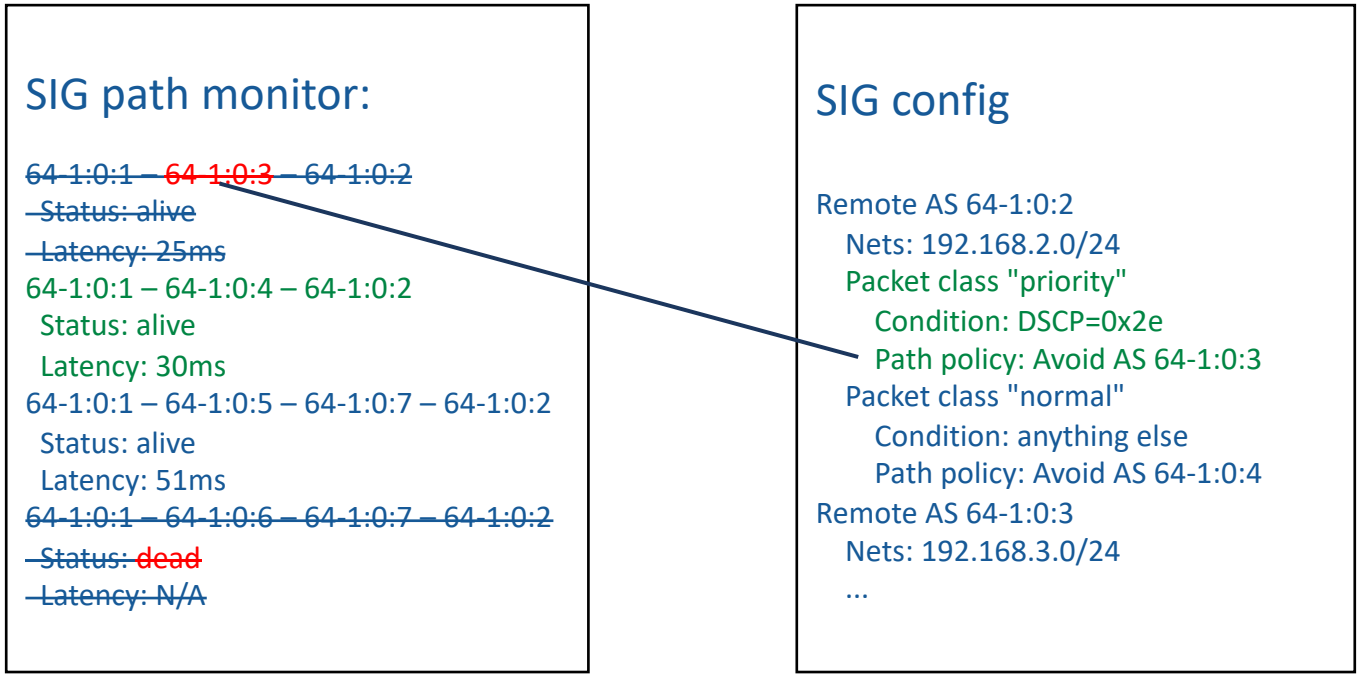
IP-in-SCION Tunneling - Example

- SIG monitors available SCION paths via periodic probes.
- It collects metrics about the health and performance characteristics, e.g., latency, jitter or drop rate.



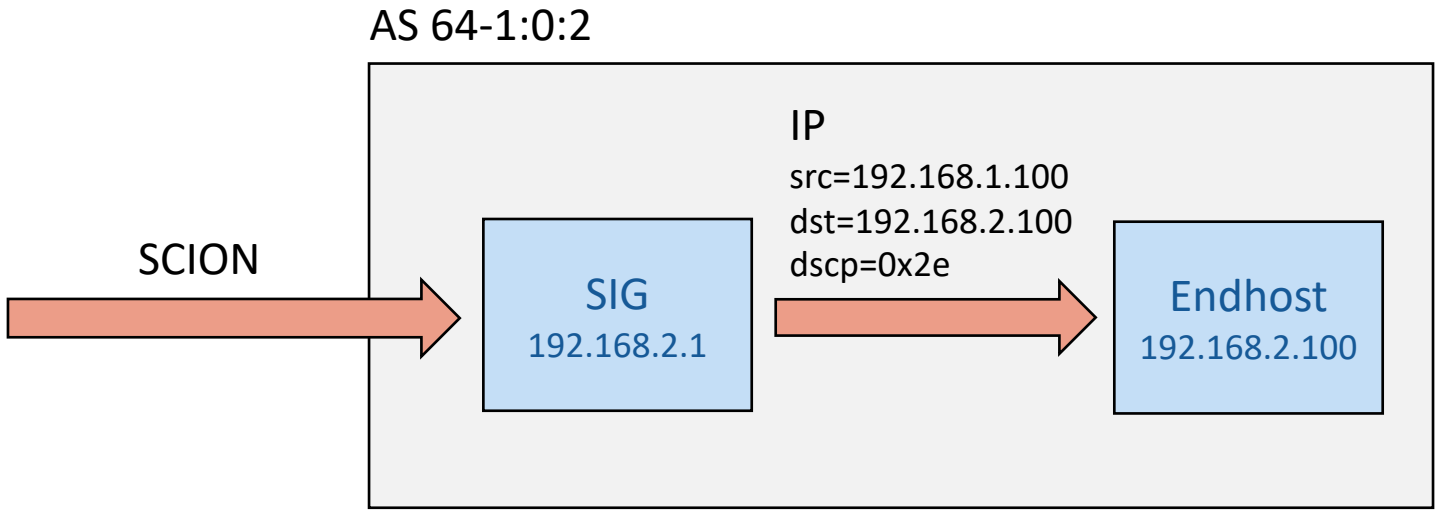
IP-in-SCION Tunneling - Example

- Avoid all dead paths.
- Avoid all paths that do not comply with the path policy.
- From remaining paths choose one with the lowest latency.
- And the winner is: 64-1:0:1 – 64-1:0:4 – 64-1:0:2



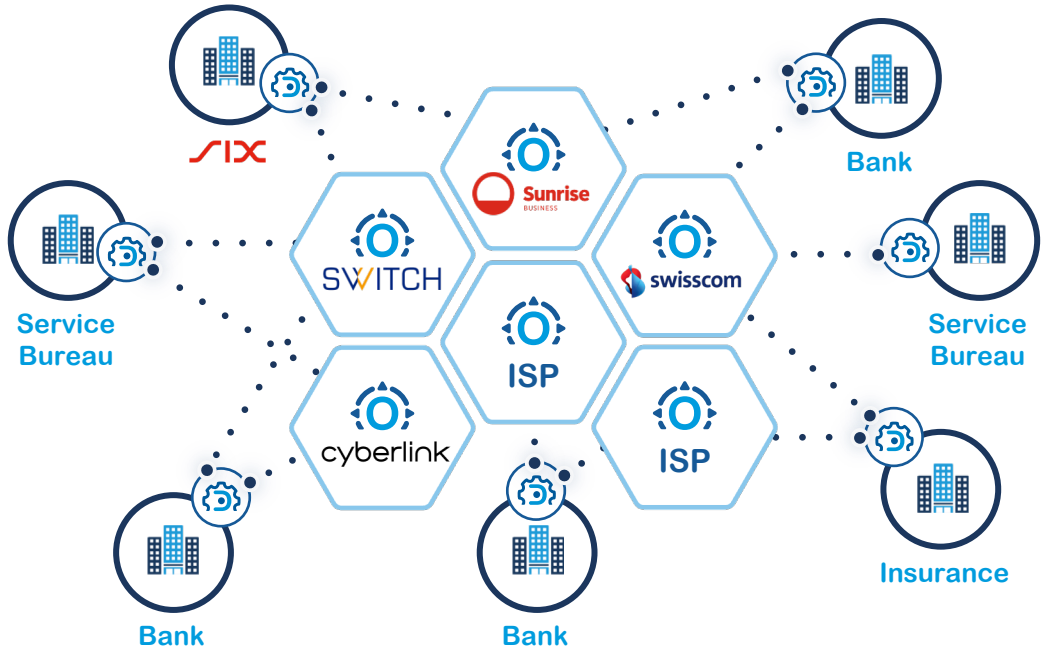
IP-in-SCION Tunneling - Example

- In the destination AS, the SIG extracts the IP packet from the SIG frame.
- It sends it to the local network.
- Finally, via standard IP routing, the packet arrives at its destination.



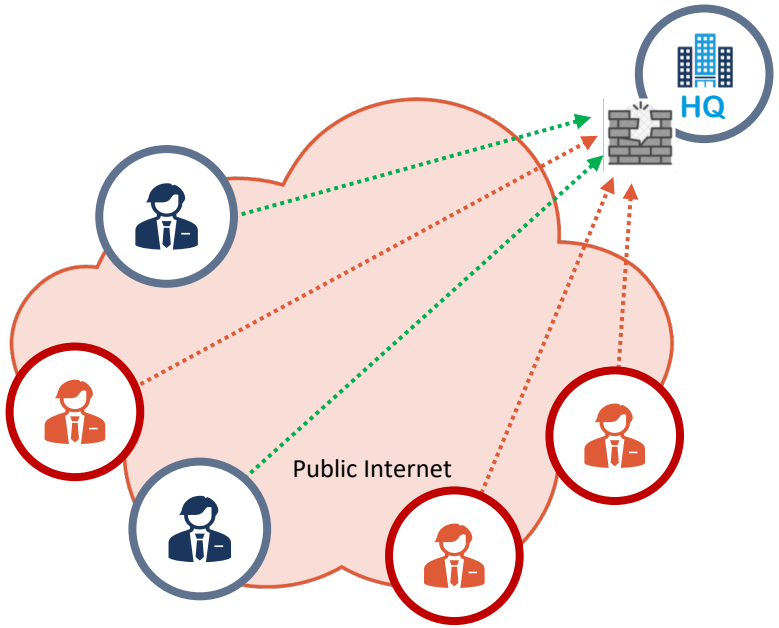
Use Case: Multi-provider/multi-organization ecosystems

- Multitude of SCION NSPs form the SCION backbone for the ecosystem.
- Each member connects to one or multiple NSPs.
- IP-in-SCION tunneling is used to enable existing applications to communicate via the SCION network.
- Can be built on top of existing ISDs or as a separate ISD
  - Reuse of existing ISD infrastructure is simpler and quicker.
  - Separate ISD enables custom governance and separate roots of trust.
- Features and Benefits:
  - High availability and resilience: multi-provider backbone and instant path fail-over.
  - Flexibility: One access to reach everyone in the ecosystem.
  - Control: traffic control for end-user and access control for ISD governance.

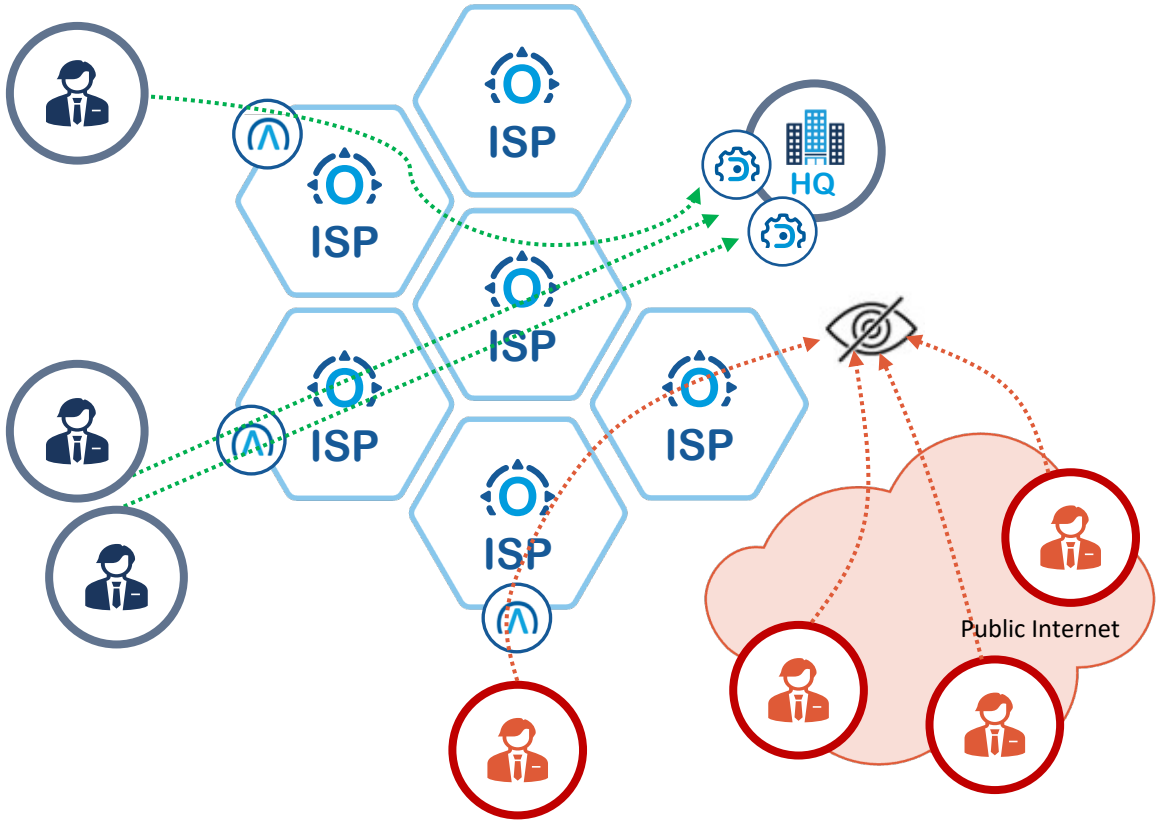


Use Case: Reducing Attack Surface of Mission Critical Services

Service is exposed to the public Internet



Service is only visible in the SCION Internet



Reduce attack surface of mission critical services by exposing it in the SCION Internet and controlling from where it is reachable.

Suitable for services that only need limited (not global) exposure.

Productive SCION Deployment Today: Some Numbers

- 7 Isolation Domains
  - 4 geographical, 3 industry-specific
- 106 SCION Ases
  - 11 of which are network service providers
- 1 IXP (SwissIX) offering a dedicated SCION peering mesh
- (Almost) 100% SCION coverage in Switzerland
  - 5 ISPs that offer SCION accesses
  - Every endhost can reach destinations in the SCION Internet through carrier-grade SCION EDGE Gateways
- Global SCION reach is limited but growing
  - SCION PoPs from international ISPs are available in UK, France, Germany, Luxembourg, US east and west coast, Singapore, Hong Kong, and South Korea.

The Long-term Need for Standardization

- The SCION ecosystem is still small but growing
  - Standardization at the IETF further supports the growth of the ecosystem and the acceptance of the technology
- SCION is being used for mission critical deployments today
  - Standardization at the IETF can ensure that the SCION protocol evolves to a robust and future-proof protocol
- SCION needs more independent implementations and it needs to be supported natively on the application-level
  - Standardization at the IETF can ensure interoperability of implementations and applications
- SCION needs to be interoperable with the existing Internet infrastructure
  - Standardization at the IETF almost certainly guarantees interoperability
- We are still far away from a standard, but we believe that further work at the IETF/IRTF is crucial to work towards this long-term goal

Thank you!

Samuel Hitz, CTO & co-founder

hitz@anapaya.net

www.anapaya.net

Anapaya Systems AG
Hardturmstrasse 253
CH-8005 Zürich