2STiC

Future internet architectures: SCION

Joeri de Ruiter
SIDN Labs

Operator of the .nl TLD

- *Stichting Internet Domeinregistratie Nederland* (SIDN)
- Critical infrastructure services
  - Lookup IP address of a domain name (almost every interaction)
  - Registration of all .nl domain names
  - Manage fault-tolerant and distributed infrastructure

.nl = the Netherlands
17M inhabitants
6.1M domain names
3.4M DNSSEC-signed
2.5B DNS queries/day

SIDN Labs

- Goal: increase the trustworthiness of our society's internet infrastructure
  - Measure, prototype, evaluate mechanisms that increase the trustworthiness of the Internet and for new internet infrastructures that complement the Internet
  - Reinforce the Dutch, European, and global research and operational communities
- Daily work: help operational teams, write open source software, analyze vast amounts of data, run experiments, write academic papers and tech reports, work with universities

The internet

- Started as small scale experiment
  - Nowadays a basic infrastructure
- Not designed with current usage in mind
  - For example, in the area of security
- Reactive approach to issues
- New infrastructures can offer solutions to this
  - Address issues fundamentally and pro-actively

ZDNet

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

Russian telco hijacks internet traffic for Google, AWS, Cloudflare, and others

Rostelecom involved in BGP hijacking incident this week impacting more than 200 CDNs and cloud p

By Catalin Cimpanu for Zero Day | April 5, 2020 -- 21:53 GMT (22:53 BST) | Topic: Security

Earlier
larges
provic
Russia

The in

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BORDER GATEWAY PROTOCOL —

How 3ve's BGP hijackers eluded the Internet—and made $29M

3ve used addresses of unsuspecting owners—like the US Air Force.

DAN GOODIN - 12/21/2018, 6:30 PM

c|net

REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

YouTube blames Pakistan network for 2-hour outage

Company appears to confirm reports that Pakistan Telecom was responsible for routing traffic according to erroneous Internet Protocols.

Tech Culture

Updated, 9:40 p.m. to add YouTube's

Security, Stability and Transparency in inter-network Communication

Put Dutch and European internet communities in leading position of secure, stable and transparent inter-network communication

2STiC

amsix

ndix

NLNETLABS

SDN LABS

SURF

TU Delft

University of Amsterdam

University of Twente.

2STiC

2STiC

- New applications have new security, stability and transparency requirements
  - More interaction with physical space (e.g., transport, smart grids, drones, remote surgery)
- Open programmable network equipment is becoming commercially available
  - Eases adoption
- Experiment with and evaluate emerging internet architectures
  - For example: SCION, RINA and NDN

2STiC

SCION

SCION

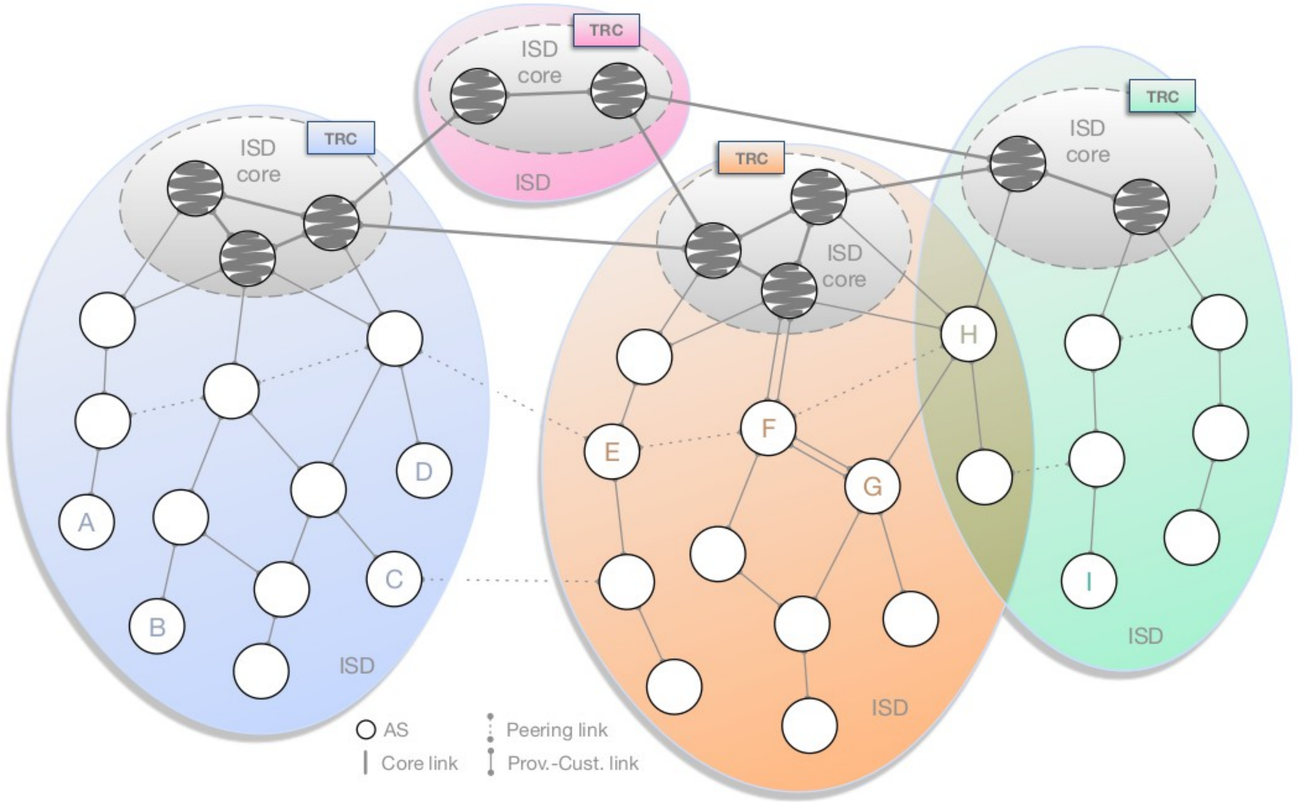
- Scalability, Control, and Isolation On Next-generation Networks
- New internet architecture
- Network Security Group, ETH Zurich
- Goal: improve security of inter-domain routing and isolation of compromise
- Scalability and security through Isolation Domains (ISDs)
  - Group of autonomous systems
  - E.g., per country or jurisdiction

SCION

- Security by design
  - Routes authenticated both in control and data plane
- Path-aware networking
  - Sender selects path
  - Enables, for example, geofencing
- Multi-path communication
  - Can be used, for example, for redundancy
- Existing application can still be used

Isolation domains

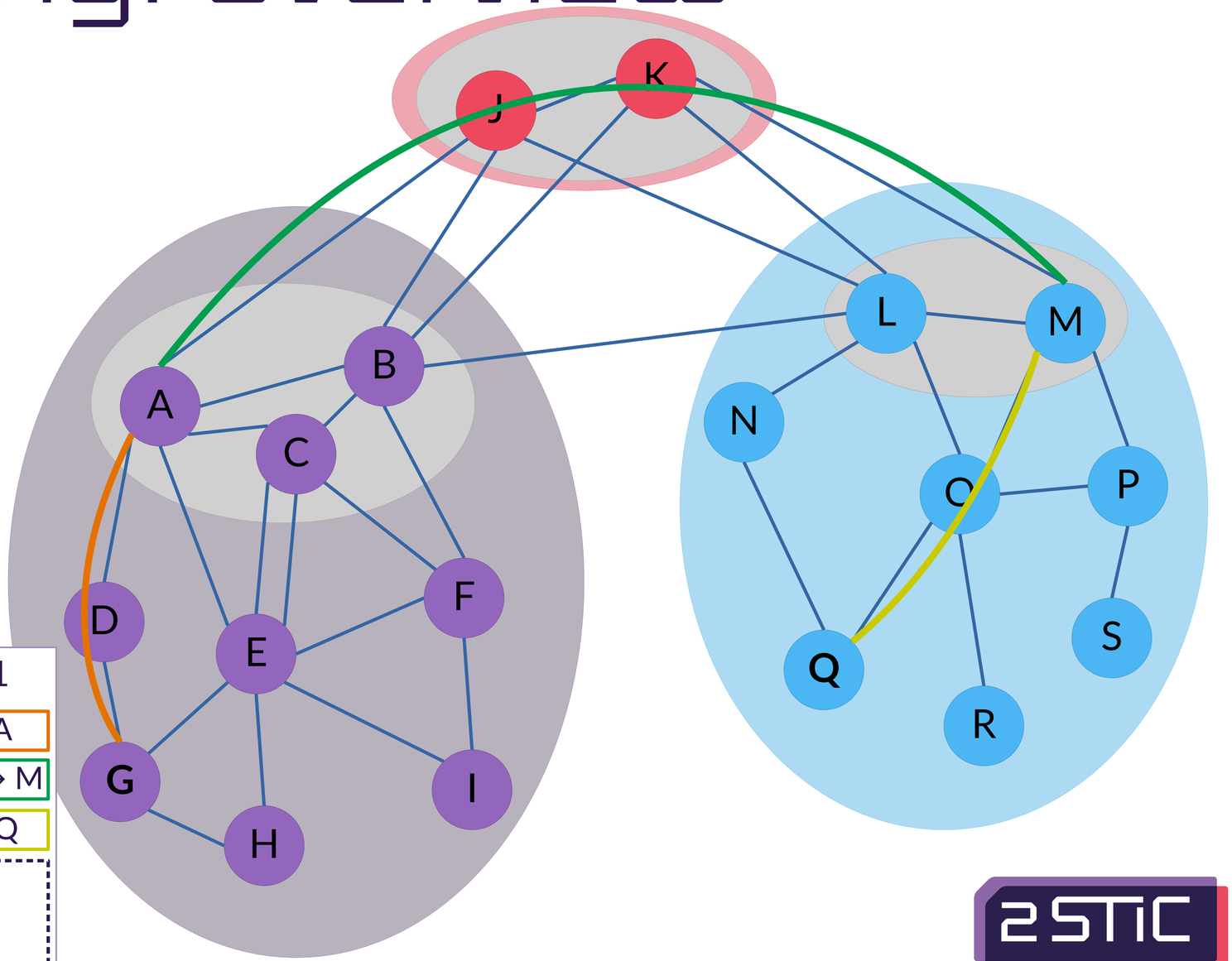
- Group of autonomous systems
  - E.g., per country or jurisdiction
- ISD core: ASes managing the ISD
- Core AS: AS part of the ISD core
- PKI organised per ISD
- Hierarchical control plane
  - Inter-ISD control plane
  - Intra-ISD control plane



Source: The SCION Internet Architecture: An Internet Architecture for the 21st Century, Barrera et al., 2017

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)

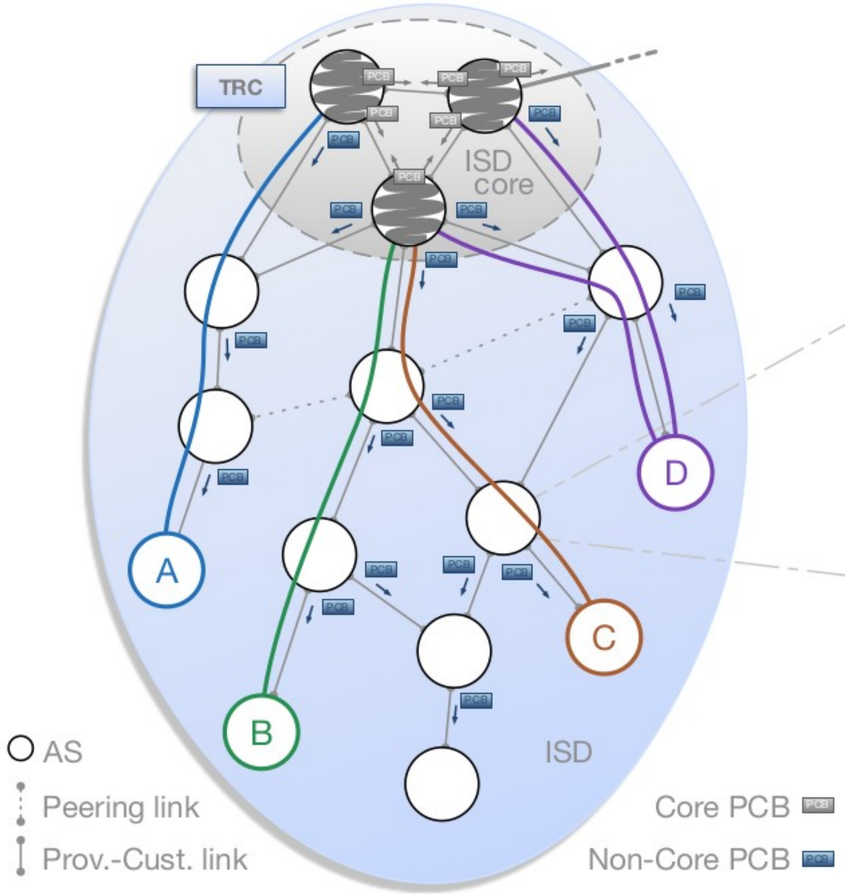


Control plane: path exploration

- Inter-ISD
  - Performed by core ASes
  - Flooding similar as with BGP
  - Less ASes involved (only core)
- Intra-ISD
  - Downstream multi-path flooding

Intra-ISD path exploration

- Path Construction Beacons (PCBs) sent downstream using multi-path flooding
  - Initialised by core ASes
  - Extended and forwarded by receiving ASes
  - Add incoming and outgoing interface and optional peerings
- Eventually all nodes know how ISD core can be reached
- Path registration
  - Preferred down-segments (path from core to AS) with path server in the core
  - Preferred up-segments registered with local path server in AS



Source: The SCION Internet Architecture: An Internet Architecture for the 21st Century, Barrera et al., 2017

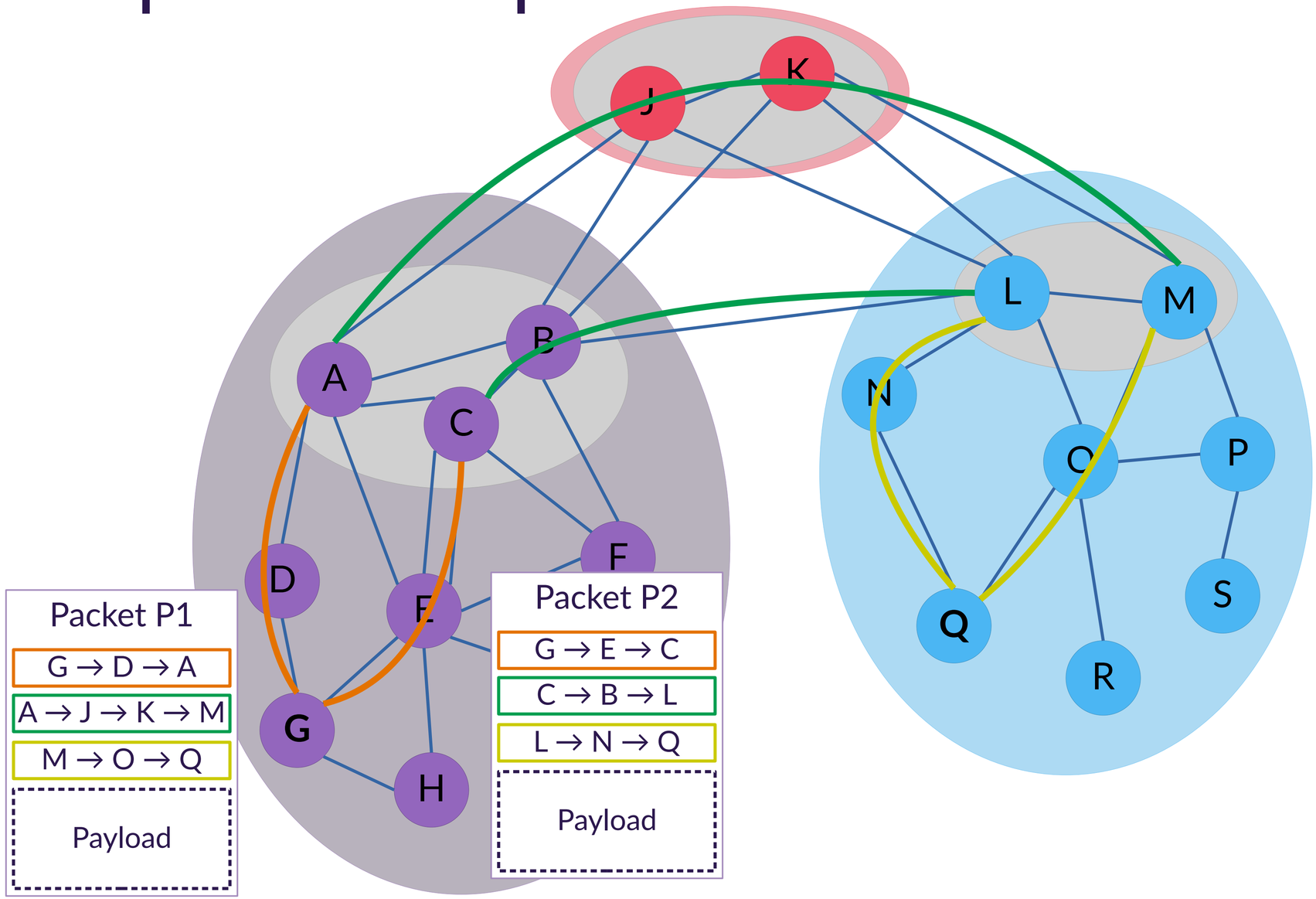
Path Construction Beacons

- Path Construction Beacons are signed by every AS along the path
  - Authenticated path
- Hop fields included that can be used to later select paths
  - Contain forwarding information
  - Contain cryptographic MAC computed using hop field key
  - Only processed locally

Data plane: path lookup

- Path construction performed by end hosts
- Request route to (ISD, AS) from local path server
- Local path server replies with
  - Up-path segments to local ISD core
  - Down-path segments in remote ISD from core to destination AS
  - Core-path segments needed to connect up-path and down-path segments
- End hosts pick and combine segments to determine path

Data plane: path combination



Data plane: path combination

- Possible paths determined by
  - Up-stream AS, by deciding which PCBs to forward to where
  - Core AS, by offering path segments to path server in local AS
  - Local AS, by registering down-path segments with ISD core
  - Local AS, by offering path segments to clients
  - Clients, by combining path segments offered by local path server

Routing summary

- Path information included in packet headers
  - Corresponding hop fields included
  - No forwarding information necessary at routers
  - Packet-carried forwarding state (PCFS)
- Sender selects the path
  - Possible to use multiple paths
  - Fast failover
- Recipient address no longer used to route between autonomous systems
  - Only used by the destination AS
  - Local delivery is responsibility of destination AS

Security

- Path information authenticated in control plane and data plane
- Control plane
  - Beacons authenticated using digital signatures
  - No route hijacks
- Data plane
  - User selects path
  - Hop fields ensure only authorised paths possible

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

Reliability and QoS

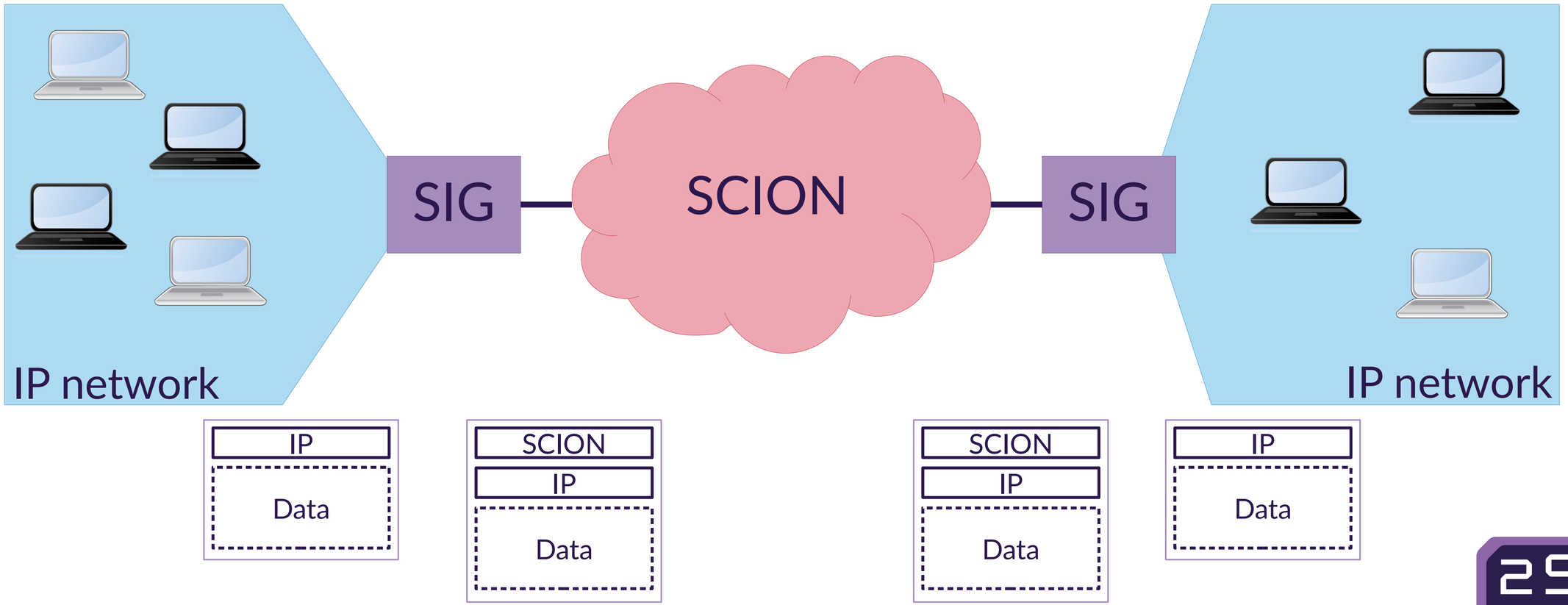
- Redundancy through use of multi-path communication
- Fast failover in case of link failure
  - No waiting for convergence
- Possible to add latency information to beacons
  - Path selection based on latency
- COLIBRI extension
  - Minimum bandwidth reservation

Deployment

- Open source implementation available
  https://github.com/scionproto/scion
- International testbed SCIONLab
  https://www.scionlab.org/
- Production network managed by spin-off Anapaya
- In use at banks, government and hospitals

Deployment

- Can be combined with existing applications using SCION-IP Gateway



SCION recap

- Security by design
  - Routes authenticated both in control and data plane
  - For example, no route hijacks and no address spoofing
- Path-aware networking
  - Control over path that network traffic takes
- Improved reliability and QoS
  - Multi-path communication
  - Bandwidth reservation
- Existing application can still be used
  - SCION-IP gateway

SCION at SIDN Labs

- BGP-free connection to SCIONLab
- Video conferencing demo

  https://www.sidnlabs.nl/en/news-and-blogs/a-practical-demo-of-scion-a-new-internet-architecture
- SCION in P4
  - Run SCION on programmable networking hardware
  - Sharing experiences with SCION team
  - Will be released as open source

Thanks for your attention!

info@2stic.nl

www.2stic.nl
www.sidnlabs.nl