
# UNIVERSITY OF WEST ATTICA

## FACULTY OF ENGINEERING

## DEPARTMENT OF INFORMATICS AND COMPUTER ENGINEERING

**MASTER THESIS**

**SCION Architecture – A Study**

**Maria Souvalioti**

**(mngd21017)**

**Supervisor: Adonis Bogris, Professor**

**Athens, September 2024**

**Master Thesis**

# SCION Architecture – A Study

**Maria Souvalioti**

**mngd21017**

**Supervisor:**

**Adonis, Bogris, Professor**

Antonios Bogris
Digitally signed by Antonios Bogris
Date: 2024.09.19 21:39:37 +03'00'

**Examining Commitee:**

**Panagiotis Karkazis, Associate Professor**

PANAGIOTIS KARKAZIS
Digitally signed by PANAGIOTIS KARKAZIS
Date: 2024.09.19 14:08:38 +03'00'

**Ioanna Kantzavelou, Associate Professor**

IOANNA KANTZAVELOU
Digitally signed by IOANNA KANTZAVELOU
Date: 2024.09.19 14:03:03 +03'00'

**Date of Examination: 13/09/2024**

# ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη Μαρία Σουβαλίωτη του Φωτίου Σουβαλιώτη και της Νικολέττας Φωτοπούλου, με αριθμό μητρώου mngd21017 φοιτήτρια του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Βεβαιώνω ότι είμαι συγγραφέας αυτής της Διπλωματικής εργασίας και κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο/Η Δηλών/ούσα

# THANKS

This thesis was completed after persistent efforts, in such an interesting and cutting-edge subject as is SCION Architecture.

This effort was supported by:

- Adonis Bogris, Professor in the University of West Attica and my supervisor in this thesis.
- George Xilouris, manager of the Network Operations Center at the National Center for Scientific Research Demokritos where I am currently employed and supervisor.
- Ioannis Korovesis, tenure associate researcher at the National Center for Scientific Research Demokritos and former manager of the Network Operations Center.

I would like to thank all three of them for their support in this thesis.

I would also like to thank the following members of the SCION infrastructure team in SCIERA, the European RIR and Greece's NREN:

- David Hausheer, Professor at Otto von Guerick University in Magdeburd, Germany and core member of the SCION Education and Research Network, SCIERA.
- Marten Gartner, software developer and researcher at Otto von Guerick University in Magdeburd, Germany and also member of Prof. Hausheer's team in SCIERA.
- The implementation and networking team of Géant in France.
- The networking team of GRNET SA in Greece.

without whose help and efforts our SCION connection could never have happened.

Finally, I would like to thank my family for their continuous support in all my endeavors and their faith in me.

Thank you all from the bottom of my heart!

# Abstract

This thesis deals with the new network architecture based on the secure transfer of information that is developed in Europe, SCION Architecture. SCION architecture is aiming to replace the existing network infrastructure which is based on the Border Gateway Protocol (BGP) by offering secure and encrypted traffic for the data plane from a secured control plane using source routing and Public Key Infrastructure (PKI). At the same time, it introduces the new concept of Isolation Domains (ISDs), which are logical groups of Autonomous Systems (AS), offering the possibility of connecting to other ASes and inserting them into an Isolation Domain (ISD).

Through ISDs it is possible to trust the heterogeneity, the transparency in the security relationships between AS and the network paths that unite them. With SCION the routing process can be isolated from heterogeneous factors such as cyber-attacks, and the scalability of routing can be improved by separating it into two processes; one within the ISD itself and one between the cooperating ISDs.

In particular, the SCION architecture offers a secure connection to the Internet without affecting the existing BGP connections of customers that do not participate in the Secure Backbone that SCION creates. Using it can prevent attacks based on BGP's vulnerabilities such as BGP hijacking, which intercepts and then redirects normal BGP traffic to wrong geographic locations. Furthermore, SCION can significantly reduce, if not completely eliminate, Distributed Denial of Service (DDoS) attacks.

Our purpose is to study this new architecture in depth and to arrive at the creation of the first SCION Attachment Point node in Greece for the Academic and Research Network.

## ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία ασχολείται με την νέα δικτυακή αρχιτεκτονική με βάση την ασφαλή μεταφορά της πληροφορίας που αναπτύσσεται στην Ευρώπη, την SCION Architecture. Η αρχιτεκτονική SCION έχει σκοπό να αντικαταστήσει την υπάρχουσα δικτυακή υποδομή που βασίζεται στο Border Gateway Protocol (BGP) προσφέροντας ασφαλή και κρυπτογραφημένη κίνηση για το data plane από ένα secured control plane με χρήση source routing και PKI. Ταυτόχρονα συστήνει την νέα λογική των Isolation Domains (ISDs), τα οποία αποτελούν λογικά group αυτόνομονων συστημάτων (AS), προσφέροντας τη δυνατότητα σύνδεσης σε άλλα AS και την εισαγωγή τους στο ISD. Μέσω των ISDs είναι εφικτή η εμπιστοσύνη στην ετερογένεια, τη διαφάνεια στις σχέσεις ασφαλείας μεταξύ των AS και στα δικτυακά μονοπάτια που τους ενώνουν. Με το SCION μπορούμε να απομονώσουμε την διαδικασία δρομολόγησης από ετερογενείς παράγοντες όπως είναι οι κυβερνοεπιθέσεις, και να βελτιωθεί η επεκτασιμότητα της δρομολόγησης μέσω του διαχωρισμού της σε δύο διεργασίες· μία μέσα στο ίδιο το ISD και μια μεταξύ των συνεργαζόμενων ISDs.

Συγκεκριμένα, με την αρχιτεκτονική SCION προσφέρεται ασφαλής σύνδεση στο Διαδίκτυο χωρίς να επηρεάζονται οι υπάρχουσες BGP διασυνδέσεις πελατών που δεν συμμετέχουν στο Secure Backbone που δημιουργεί η SCION. Με τη χρήση της μπορούν να αποφευχθούν επιθέσεις και κενά ασφαλείας του BGP όπως είναι το BGP hijacking, που υποκλέπτει και ανακατευθύνει κανονική BGP κίνηση ενός peering σε λάθος τοποθεσίες, και σημαντική μείωση – αν όχι εξάλειψη – των Distributed Denial of Service (DDoS) attacks.

Σκοπός μας είναι να μελετήσουμε σε βάθος την νέα αυτή αρχιτεκτονική και να καταλήξουμε στη δημιουργία του πρώτου κόμβου SCION στην Ελλάδα για το Ακαδημαϊκό και Ερευνητικό Δίκτυο.

Scientific Area: Next Generation Networks, Cyber Security

Keywords: SCION, scion-architecture, SCION education, SCION-ED, SCIERA, network, next-generation networks, network architecture, NREN, cryptography, cybersecurity, PKI

# Table of Contents

# Table of Images

# Table of Figures

# Table of Tables

# ABBREVIATIONS

| | |
|---|---|
| 3GPP | Third Generation Partnership Project |
| 5G | Fifth Generation |
| 5G-AKA | 5G Authentication and Key Aggrement |
| AARC | Authentications and Authorisation Framework |
| ACL | Access Control List |
| AFRINIC | African Network Information Centre |
| AI | Artificial Intelligence |
| API | Application Programming Interface |
| APNIC | Asia Pacific Network Information Centre |
| APT | Advanced Persistent Threats |
| ARIN | American Registry for Internet Numbers |
| ARP | Address Resolution Protocol |
| AS | Autonomous System |
| ASN | Autonomous System Number |

| | |
|---|---|
| AWS | Amazon Web Services |
| BFD | Bidirectional Forwarding Detection |
| BGP | Border Gateway Protocol |
| BR | Border Router |
| BS | Beacon Service |
| CA | Certification Authority |
| CCPA | California Consumer Privacy Act |
| CDN | Content Delivery Network |
| CIDR | Classless Inter-Domain Routing |
| CP | Control Plane |
| CP-PKI | Control Plane Public Key Infrastructure |
| CRL | Certificate Revocation List |
| CS | Control Service |
| CUSUM | Adaptive Cumulative Sum |
| DAF | Distributed Application Facility |

| | |
|---|---|
| DANTE | Delivery of Advanced Network Technology to Europe |
| DAP | Distributed Application Process |
| DDoS | Distrubuted Denial of Service |
| DHCP | Dynamic Host Configuration Protocol |
| DIF | Distributed Inter-Process Communication |
| DL | Deep Learning |
| DNN | Deep Neural Networks |
| DNS | Domain Name Resolving |
| DoS | Denial of Service |
| DP | Data Plane |
| DPO | Data Protection Officer |
| DRKey | Dynamically Recreatable Key |
| DTL | Distruibuted Ledger Technologies |
| EC | European Commission |
| EIGRP | Enhanced Interior Gateway Routing Protocol |

| | |
|---|---|
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| EWMA | Exponentially Weighted Moving Average |
| FII | Framework for Internet Innovation |
| GDPR | General Data Policy Regulation |
| GR-IX | Greece's Internet Exchange point |
| GRNET | National Infrastructures for Research and Technology |
| HF | Hop Field |
| HIPAA | Health Insurance Portability and Accountability Act |
| HPCA | High-Performance Computing Act |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HyperText Transfer Protocol (Secure) |
| IANA | Internet Assigned Numbers Authority |
| ICMP | Internet Control Message Protocol |
| IDE | Integrated Development Environment |

| | |
|---|---|
| IDS | Intrusion Detection System |
| IHL | Internet Header Length |
| IHR | Internet Health Report |
| INF | INformation Field |
| IoT | Internet of things |
| IP | Internet Protocol |
| IPC | Inter-Process Communication |
| IPS | Intrusion Prevention System |
| IRR | Internet Routing Registry |
| ISD | ISolation Domain |
| ISG | Industry Specification Group |
| IS-IS | Intermediate System to Intermediate System |
| ISO | International Organization for Standardization |
| ISP | Internet Service Provider |
| ITU | International Telecommunication Union |

| | |
|---|---|
| K-NN | K Nearest Neighbour |
| LACNIC | Latin America and Caribbean Network Information Centre |
| LGPD | Law for General Protection of Data |
| LoRaWAN | Low Range Wide Area Network |
| LSA | Link-State Advertisement |
| LTE | Long Term Evolution |
| LTE-M/LTE-MTC | Long Term Evolution Machine Type Communication |
| M2M | Machine-to-Machine |
| MAC | Media Access Control |
| MIMO | Multiple Input Multiple Output |
| mIoT | Massive Internet of Things |
| MitM | Man in the Middle |
| ML | Machine Learning |
| mMTC | Massive Machine Type Communications |
| MPLS | MultiProtocol Label Switching |

| | |
|---|---|
| NFV | Network Function Virtualization |
| NIDS | Network Intrusion Detection System |
| NII | National Information Infrastructure |
| NIRA | New Internet Routing Architecture |
| NIST | National Institute of Standards and Technology |
| NR | New Radio |
| NREN | National Research and Education Network |
| NRO | Number Resource Organization |
| NSF | National Science Foundation |
| ONF | Open Networking Foundation |
| OS | Operational System |
| OSI | Open Systems Interconnection |
| OSPF | Open Shortest Path First |
| P2P | Point-to-Point |
| PCB | Path Control Beacon |

| | |
|---|---|
| PCFS | Packet-Carried Forwarding State |
| PDPA | Personal Data Protection Act |
| PIPEDA | Personal Information Protection and Electronic Documents Act |
| PKI | Public Key Infrastructure |
| PoP | Point of Presence |
| PS | Path Service |
| QoS | Quality of Service |
| RAT | Radio Access Technology |
| RFC | Request For Comments |
| RFID | Radio Frequency IDentification |
| RHINE | Robust and High-performance Internet Naming for End-to-end security |
| RINA | Recursive Inter-Network Architecture |
| RIP | Routing Information Protocol |
| RIPE NCC | Réseaux IP Européens Network Coordination Centre |
| RIR | Regional Internet Registry |

| | |
|---|---|
| RIS | Routing Information Service |
| ROA | Route Origination Authorization |
| ROV | Route Origination Validation |
| RPC | Remote Procedure Call |
| RPKI | Resource Public Key Infrastructure |
| RR | Resource Record |
| RTNTAD | Real-Time Network Traffic Attacks Detection |
| SBAS | Secure Backbone AS |
| SBR | SCION Border Router |
| SCIERA | SCION Education, Research and Academic Network |
| SCION | Scalable, Controlled and Isolated Next-Generation Networks |
| SCMP | SCION Control Message Protocol |
| SDN | Software Defined Networks |
| SD-SEC | Software Defined Security |
| SD-WAN | Software Defined Wide Area Network |

| | |
|---|---|
| SGRP | SCION Gateway Routing Protocol |
| SIAM | SCION-IP Address Mapping System |
| SIC | Swiss Interbank Clearing |
| SIG | SCION-IP Gateway |
| SLA | Service-Level Aggreement |
| SNB | Swiss National Bank |
| SNMP | Simple Network Monitoring Protocol |
| SoC | System on a Chip |
| SSFN | Secure Swiss Finance Network |
| SSHN | Secure Swiss Health Network |
| SSP | SCION Stream Protocol |
| TCP | Transmission Control Protocol |
| TERENA | Trans-European Research and Education Networking Association |
| TLS | Transport Layer Security |
| TOFU | Trust On First Use |

| | |
|---|---|
| TOMA | Trust oOn Multiple Announcements |
| ToS | Type of Service |
| TRC | Trust Root Configuration |
| TTL | Time to Live |
| UDP | User Datagram Protocol |
| VM | Virtual Machine |
| VNF | Virtual Network Functions |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |

# 1 Background

In this thesis we get acquainted and gain some hands-on experience with the up and coming new Internet architecture SCION, which stands for Scalable, Controlled and Isolated Next-Generation Networks. We will see how it works, how this new approach of the Internet for more secured and controlled communications is carried out, which security tools will be used to achieve our data's protection against BGP hijacking and DDoS attacks, how SCION is deployed and its inner mechanisms, and, finally, how an interested party (either an organization or a person) can become involved in this new technology and deploy their own SCION instance.

The 1st chapter of this thesis, consists of some basic concepts and their brief explanations, so advancing to following chapters will be smoother for the reader. This chapter could be skipped from an advanced user as it reiterates already known concepts.

The 2nd chapter, explains what is the current situation in Internet and network communications in general, expanding on some fundamental concepts, as well as describing emerging technologies, security concerns, and established regulations and policies.

The 3rd chapter, describes and analyses projects and initiatives similar to SCION in their views of the importance of rectifying and eliminating security risks that rise in network communications and differntiating the established networking protocols in accordance to modern technologies and know-how. Eventually, in this chapter a comparison is made between those projects and the reasons why SCION was chosen amongst them and its benefits are shown.

The 4th chapter, explains the SCION Architecture and model, its core components, and how established concepts change to accommodate SCION's aspects. It also describes security mechanisms that are implemented in SCION as core-components of the architecture Finally, it shows the different parts of a SCION host.

The 5th chapter, consists of the deployment methods used depending on who the interested party is, as there is a different approach if they are a country's NREN, an ISP or a security/network laboratory of a University, as was our own case.

The 6th chapter, is our own use case of the SCION architecture, which steps we took, how we implemented it, challenges we faced, quests we conquered, metrics we took from our adventure down the rabbit hole and all the fantastic things we found out. This chapter will be focused on the sub-project SCION Education, Research and Academic Network (SCIERA) and we aspire it to be a guide

for other interested Universities or Research Centers to follow when they will be in favour of joining forces.

## 1.1 Basic Concepts

Before proceeding with a detailed examination of the intricate workings and interconnections of networks, it is imperative to take a moment and gain a comprehensive understanding of the structure of communication systems and their core components, summarizing briefly their core components and operational mechanisms, including their core infrastructure and constituent entities [1][2][3].

In general, networks are defined by three core functions of network devices:

- Data plane
- Control Plane
- Management Plane

Depending on the headers of the incoming packets, they are going to either be instantly forwarded to their next-hop destination as soon as they reach a switch's data plane or move up to the control plane for further processing, resulting in the control plane updating the data plane's forwarding table.

The management plane is where the network administrator can monitor and configure the switch as they deem appropriate. By utilizing the management plane, network administrators can oversee and configure switches to maintain optimal network performance[4].

In a bigger scale, for example a research organization, edge devices, namely workstations, laptops, tablets and mobile devices, are connected to a lab's switch that is part of a network of interconnected switches, forming the Institute's network that converges to the primary aggregation switch of the building/s. In continuation, the Institute's primary aggregation switch connects to the main aggregation router-switch of the Organization, becoming the backbone of the Organization where all Institutes have a Point of Presence (PoP). Subsequently, the main aggregation router is connected to an Internet Service Provider (ISP) via a physical link, the link in most cases being a fiber optic connectivity channel.

In an even bigger scale, the ISP needs to be able to be connected at all times with the rest of ISPs to ensure continuous connectivity enabling seamless Internet access for their end-users. Besides the physical and network layer of things, they have to have implemented the appropriate routing protocols, i.e. BGP, to distinguish between the different ISPs, as well as they have to have utilized seamlessly the Domain Name Resolving service (DNS) for domain to IP resolution, and vice versa. That way

their clients, even when in their homes or on the way with their mobile devices, can have a consistent experience utilizing their edge devices as they see fit, without ever realizing the inner workings of the means of Internet network processes and protocols. As in that scale ISPs need to be able to be interconnected to another network between one another, they also need to be able to distinguish themselves between each other, by name, number as well as geophysically at all times. That need, amongst others, is the responsibility of the Regional Internet Registries (RIRs).

RIRs are responsible for managing the registry for their respective region of the world, assigning each ISP and end-user organization a respective number, as each one is considered to be an Autonomous System (AS), separate from one another, distinguished by its alpharuthmetic name, and its appointed public subnets. The Internet Assigned Numbers Authority (IANA) delegates Internet resources to the RIRs to use in their regions and the Number Resource Organization (NRO) is responsible, as an unincorporated organization, for the unification and connection of the five global RIRs under its umbrella.

Table 1.1 Regional Internet Registries and their respective regions

| **RIR entity** | **Region** |
|---|---|
| African Network Information Centre (AFRINIC) | Africa |
| American Registry for Internet Numbers (ARIN) | Antarctica, Canada, parts of the Caribbean, United States |
| Asia Pacific Network Information Centre (APNIC) | East Asia, Oceania, South Asia, Southeast Asia |
| Latin America and Caribbean Network Information Centre (LACNIC) | Latin America, and most of the Caribbean |
| Réseaux IP Européens Network Coordination Centre (RIPE NCC) | Europe, Central Asia, Russia, West Asia |

### 1.1.1 Data Plane

The Data Plane, also known as the Forwarding Plane, is a fundamental component of network devices, such as routers and switches, and its primary responsibility is to quickly and efficiently inspect the information contained within the packets' headers and forward them according to its local forwarding table, without any additional processing from the other two planes. When a data packet arrives to the network device, the Data Plane examines the packet's headers determining its destination and then

forwards the packet to the appropriate interface, which is found on the information within its local forwarding table, following the appointed protocols for the communication (OSPF, BGP, IS-IS etc).

The forwarding table is created, updated and maintained by the Control Plane which is, in contrast to the Data Plane, responsible for network-wide decision making, such as the implementation of network protocols, traffic engineering and general network management. The forwarding decisions on the Data Plane happen autonomously and efficiently without any interference from the Control Plane as long as the destination network location exists as an entry in the forwarding table. If a packet's destination is not found in the forwarding table, then Data Plane forwards the aforementioned packet to the Control Plane for further processing, which results in Control Plane investigating the paths that can be used for the packet to reach its destination, establishing the appropriate protocols and then updating the Data Plane's forwarding table, pushing the packet back to Data Plane for the forwarding.

In detail, when a packet arrives at a networking device and its destination is not found in the local forwarding table of the Data Plane, the device encounters what is known as a "routing table miss" or "forwarding table miss" event [5]. In such cases, the Data Plane cannot make an autonomous forwarding decision because it lacks the necessary information about how to route the packet. In traditional networking architectures, when a forwarding table miss occurs, the packet is typically forwarded to the Control Plane for further analysis and processing. The Control Plane investigates the paths that can be used for the packet to reach its destination by analyzing the network topology, which routes are available, and potentially applying routing protocols such as OSPF, BGP, or others to determine the best path. Based on its analysis, the Control Plane establishes the appropriate protocols necessary for routing the packet to its destination, a process that may involve exchanging routing information with neighboring devices, calculating optimal routes, and making routing decisions. Once the Control Plane has determined the appropriate path for the packet, it updates the Data Plane's forwarding table with the relevant forwarding information, thus ensuring that future packets destined for the same destination can be forwarded autonomously by the Data Plane without needing to involve the Control Plane again for similar packets. As the forwarding table is updated with the appropriate information, the Control Plane pushes the packet to the Data Plane for forwarding. As the Data Plane is equipped with the updated table it can continue and autonomously forward the packet along the established path to its destination. The process of routing table misses and the subsequent interaction between the two planes is crucial for ensuring that the packets can be successfully routed across the network, even to destinations not previously known [6].

### 1.1.2 Control Plane

The Control Plane, as stated, is, amongst other things, responsible for keeping Data Plane's forwarding table updated, so that the later can in turn handle independently as much volume of the network's traffic as swiftly as possible. Thus, saving the network device from needing additional processing power, ensuring the smooth operation of the network by reducing the probability of bottleneck or congestion. This helps prevent issues from appearing and obstructing the full utilization of a link, allowing network traffic flows sharing that link to achieve maximum data rates network-wide [7].

Control Plane has a pivotal role, overseeing the configuration of the Data Plane's packet forwarding behaviour of the incoming packets, akin to a communications' coordinator, and shaping the network topology. Within the Control Plane, decisions are made regarding data processing, management and routing. In the Control Plane, protocols and algorithms regarding the network, such as BGP, OSPF and IS-IS, network management, such as SNMP, and application layer, such as HTTP/S, TFTP, are stored and utilized to dictate and program the functionality of the Data Plane. These protocols are often employed in SDNs, creating virtual networks and enabling the segmentation of the network traffic, prioritization of data flows, and traffic isolation.

The conceptual separation and distinction between the two planes has helped in organizing the tasks, as Data Plane is responsible and optimized for speed, simplicity and regularity, whereas the Control Plane is optimized for customizing, policing and handling more demanding network requirements [8].

### 1.1.3 Management Plane

The Management Plane is where network administrators can monitor, operate and control network devices. Within the Management Plane reside management protocols, such as Telnet and SSH, and monitoring protocols, such as Simple Network Monitoring Protocol (SNMP).

The Management Plane is focused on configuring and monitoring network devices. At the same time it provides to the network administrator remote access to their network devices for management and it provides a local interface for remote console connections to them. Here is also where an administrator can manage the devices' Operational System (OS) updates and the required backups of the machine's state.

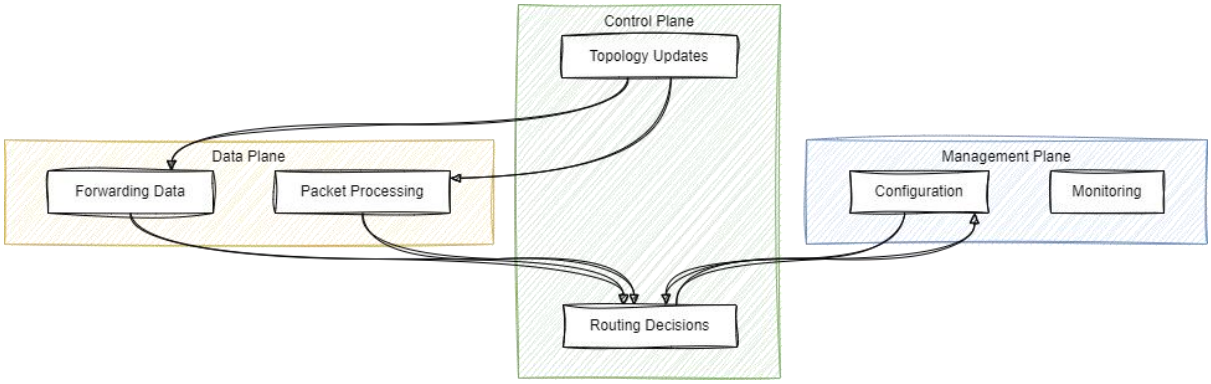


Figure 1.1 Data, Control, Management intercommunications

### 1. 1. 4 Routing

The routing process is the cornerstone of networks and what enables the communications between core and edge devices of all kinds. It refers to the process of determining the optimal path for data packets to traverse from source to destination across networks. Networking protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) are used by the underlying infrastructure to facilitate the routing process in conventional network architectures.

In traditional networks, routing is handled by routers where forwarding decisions are being made based on information on the routers' routing tables. The routing tables contain records for different networks and network topologies with information as metrics for which is the best path to reach a destination network, and are updated dynamically as network conditions change over time.

In Software Defined Networks (SDN), the control plane and data plane are separated and become distinct, in contrast with traditional network where the control and data plane reside within the routers. In SDN, as was previously shown, the control plane, responsible for making routing decisions, is appointed to a software based controller. This controller in turn is responsible for communicating with the forwarding devices, such as switches, through a standardized protocol, such as OpenFlow.

With SDN the routing process is optimized as SDN provides centralized control, programmability of the routing process, dynamic adaptation ensuring optimal adaptation, performance and reliability, as well as traffic engineering and simplified management. More specifically, centralized control of the network happens through the SDN controller that allows for easier management, optimized and more efficient routing decisions based on real-time traffic and network conditions. SDN gives to network administrators the flexibility and ability to programmatically define the networks under their administration and customize network policies and behaviours through software tools, which allows for more dynamic and adaptive routing strategies to be tailored according to an organization's specific

needs and requirements. Furthermore, as for dynamic adaptation provided by SDN architectures, SDN facilitates that need through the controller which can quickly respond to network failures, congestion or other events by rerouting the traffic and choosing another path for the data packets to reach their destination, thus ensuring optimal performance and reliability of the architecture. SDN also enables fine-grained control over traffic engineering as it allows network administrators to control network traffic and the path based on factors such as a path's latency, bandwidth or cost. This capability is especially beneficial for the optimization of network resources and the support of diverse application requirements. Lastly, by providing a simplified network control administration by abstracting the control plane into software, management tasks such as provisioning, configuration and monitoring become simplified in their operations and the operational overhead is reduced, thus enabling efficient management of large scale networks. Predominantly, those benefits are the reason SDN has become an attractive approach for building scalable, agile, and efficient networks and has already been implemented in many large and small scale networks.

### 1.1.5 Autonomous System

Autonomous Systems (AS) refer to collections of IP networks under the control of one or more entities, and are designated with a unique Autonomous System Number (ASN). These ASNs are registered and assigned by the appropriate geographically responsible RIR, responsible for its respective geographical region. Depending on the geolocation of the AS, one of the five RIRs, namely ARIN, RIPE NCC, APNIC, LACNIC and AFRINIC as shown previously in Table 1.1, has the responsibility of managing the AS under its jurisdiction. The RIR, upon request, registers any new AS, and maintains databases containing information about the region's allocated ASNs and their associated registration details. For reference, an excerpt of ASes with physical presence in the Greece's Internet Exhange point (GR-IX), under RIPE NCC's jurisdiction is shown below in Table 1.2, alongside the names with which they are commonly known, their AS name as well as their appointed ASN.

Table 1.2 Autonomous Systems with presence in GR-IX

| **Organization** | **AS Name** | **ASN** |
|---|---|---|
| Amazon | Amazon | 16509 |
| Greece Telecom | GREEKSTREAM-AS | 206652 |
| Greek Internet Exchange (GR-IX) | GR-IX-AS | 199399 |
| National Infrastructures for Research and Technology (GRNET) | GR-NET | 5408 |

| | | |
|---|---|---|
| Microsoft | Microsoft | 8075 |
| OTE | OTENET-GR | 6799 |
| Verizon | AS702 | 702 |
| Vodafone | HOL-GR | 3329 |
| WIND | WIND-AS | 25472 |

Network administrators can request an ASN directly from their respective RIR for the AS under their management. Once an AS is assigned its ASN and its routing information, it becomes part of the global routing infrastructure, and is propagated across the Internet through the BGP protocol for the interconnection and routing with the other ASes.

AS are autonomous entities within known public address space, and are defined by specific routing policies that dictate the way network traffic is handled. They are autonomous in their control and administration, allowing their administrators to utilize their preferred network protocols and policies within the AS, shaping the behaviour of their network with specific routing policies, traffic prioritization and traffic engineering. Each AS has it own border router, or in many cases a cluster of border routers for reasons of redundancy and load balancing, which connects them to the other AS to facilitate global connectivity. AS border routers exchange routing information with one another. They utilize exterior gateway protocols such as BGP, or BGP-4 [9] which is the most utilized across the globe, and establish connectivity agreements, such as peering and transit limits, to govern the protocols, bandwidth, policies and limits of the traffic exchanged between the AS.

AS [10] have a crucial role in the Internet architecture as they provide and ensure the scalability and efficient management of the networks consisting the Internet. By dividing the global network into smaller, more manageable networks, AS facilitate the efficient administration and optimization of network resources. Network administrators can leverage AS to implement strategic traffic engineering solutions tailored to their respective requirements, thereby optimizing their managed networks by establishing the desired policies for optimization, balancing and prioritization and managing the resource allocation within the AS. Furthermore, AS provide policy enforcement within the AS by enabling the administrators to establish network policies that align with organizational security requirements, objectives and strategies. Thus, by offering and establishing logical boundaries for routing updates and containment procedures of routing information, AS contribute to the stability and resilience of the infrastructure.

### 1.1.6 NRENs

A National Research and Education Network (NREN) [11] is described as an entity that is specialized in high speed networks, dedicated to the network connectivity and support of the research, education and innovation fields of a nation. NRENs provide connectivity to national organizations, such as schools, universities, libraries, research centers and other academic and government organizations, and they offer advanced networking services.

Historically, on December 9, 1991, the High-Performance Computing Act (HPCA), or most commonly known as the "Gore Bill", is legislated by the American Congress and the federal government in the United States of America. HPCA led to the development and creation of the National Information Infrastructure (NII) and NREN, which came to expand on the already established academic and research networks, as well as ARPANET [12] and BITNET [13]. As it was stated in the contemporary media of the time, NREN was referred to as "a national superhighway for information", and was described as "a high-capacity, high-quality computer network that supports a broad set of applications and network services for the research and education community" [14]. After the legislation passed from the American Congress, the establishment of the entity NREN and the High-Performance Computing Act, led to the creation and funding of research programmes and collaborations that in turn created many significant technological developments and advancements. As the provided funding to general research, focused on large data transfer and collaborations in the scientific and medical fields [15], enabled, amongst others, the fields of computer science, computer engineering and computer visualization to be able to accelerate and procure breakthrough technologies and advancements that are still relevant, maintained, expanded and used today, such as high-speed fiber optic computer networks. Quickly the world was driven to the great "Internet boom" of the time, as the Internet became publicly available in 1991, firstly invented and developed in CERN by Tim Berners-Lee [16] in 1989, known as the World Wide Web initiative and was an approach to name the objects of the Internet [17]. In 1993, the expansion of the HPCA led to the National Science Foundation (NSF) being required to establish a program and interconnect all educational institutions, libraries and government organizations with one another and the Internet [18].

Since then, each country has one NREN responsible for the academic network, as it can be seen in Annex I Table 0.1. NRENs are known to be specialized Internet Service Providers, designed to meet unique requirements and the challenges of the research and education fields. In general, NRENs provide high-speed Internet connectivity to support data intensive research projects, large scale collaborations, many times between different Universities that are to different physical locations, and of course access to online contemporary educational material. An NREN offers a wide array of advanced networking tools and services, including secure data transfer, cloud computing, video

conferencing, and content delivery, always ensuring the reliable and resilient connectivity to the Academia via redundant network infrastructure, diverse routing paths, and disaster/recovery mechanisms to minimize disruption or downtime.

# 2 Current Situation

Despite more than five decades having passed since Internet became publicly available, the core Internet infrastructure continues to mostly rely on protocols and strategies that were invented and adopted a long time ago. The core blocks that define telecommunications, what they are, how they are being implemented and how they are used, were defined and standardized in the 1990s and since then design problems and vulnerabilities have come to plain sight by their exploitation from malicious actors.

To better study and understand the current situation in the Internet and the reasons researchers and academia try to move onto something more secure, one must have a good grasp on the following concepts:

- Fundamentals, such as the TCP/IP stack, infrastructure devices (routers, switches), key services (DNS, HTTP etc).
- Emerging technologies, such as Internet of Things (IoT) and proliferation of IoT devices, transition to IPv6, 5G networks, Edge Computing and Cloud Computing, the increasing adoption of Software Defined Networks (SDN) and Network Virtual Functions (NFV), and blockchain-based architectures.
- Security concerns, such as common security threats like BGP hijacking, Distributed Denial of Service (DDoS) attacks, DNS spoofing, and malware propagation, as well as security measures, such as encryption mechanisms (e.g. Transport Layer Security – TLS), authentication (e.g. DNSSEC), Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS).
- Regulations and policies, such as net neutrality, and data privacy regulations (i.e. GDPR).

As infrastructure network devices and their core functionalities have already been discussed, it is time for the fundamentals to be remembered, and the emerging technologies, security concerns, measures and mitigation techniques to be summarized, and regulations and policies to be mentioned about how they define the right usage of the network infrastructure and data traversing them. As the regulatory scope of network communications is not the core element of this thesis, only some important legislation and policies will be referred.

## 2.1 Fundamentals

### 2.1.1 TCP/IP stack

The Transmission Control Protocol and Internet Protocol, namely the TCP/IP stack, is the core component block of the Internet. First invented in the 1970s [19], it later became part of the “Protocol Wars” facing the International Organization for Standardization’s (ISO) Open Systems Interconnection (OSI) network architecture suite, and after 20 years it became the dominant protocol

suite and was rapidly adopted [20]. A comparison of the difference in layering between OSI and TCP/IP can be seen in Figure 2.1.

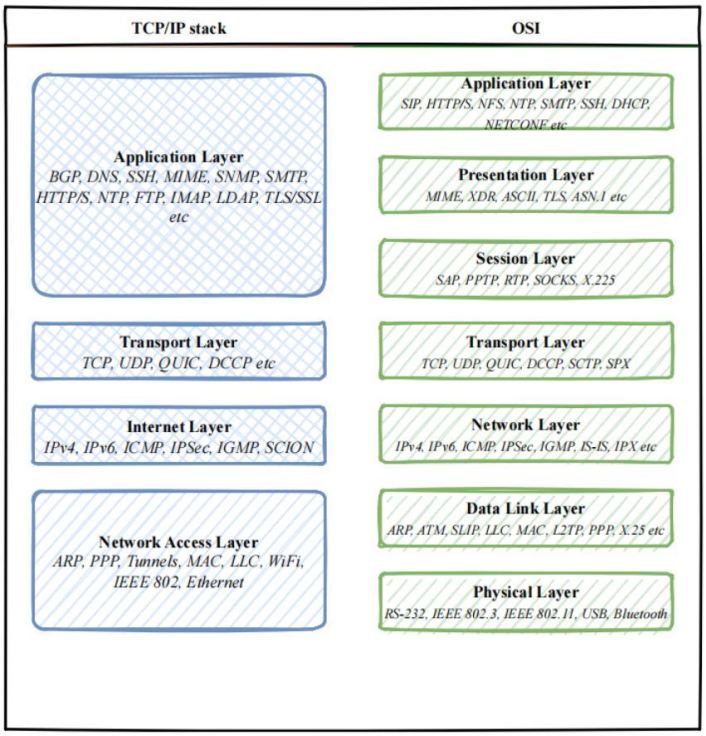


Figure 2.1 TCP/IP and OSI stacks layers comparison

By the adoption of the Internet stack, namely the TCP/IP stack, a characteristic architecture in the form of a conceptual framework was offered to research and academia, providing a division of operational scopes for the protocols that constitute the core functionalities of networks in the four distinct and abstract layers, namely Network Access (or Data Link or Link) Layer, Internet, Transport and Application Layers [21]. This framework helped in the standardization of protocols, algorithms and techniques. Each layer is responsible for performing specific functions in the chain of network communications and it provides the layer above a set of services, and obscures from view the details of how those services are implemented [22]. In that way, higher layers, i.e. the Application Layer, builds upon the services provided from the layer below, Transport Layer. For example, an HTTP application residing in the Application Layer is relying upon the Transport Layer for reliable data transfer by the use of TCP [23]. The Transport Layer in turn is dependant on the Network Layer so that data can be communicated and transferred between two endpoints using either IPv4 or IPv6, and by turn, the Network Layer relies upon the Link Layer for the physical transmission between connected source and destination network devices. As such, the Application Layer doesn't need to know how the data were transmitted to it, the Transport Layer doesn't need to know the specifics of how data was routed, and the Network Layer doesn't need to know details of the actual transmission

of the data packets across different physical media (copper, fibre optic etc.) that happens on the Link Layer.

The TCP/IP stack has become the global backbone modern network infrastructure, providing a robust, scalable and standardized framework and its success is evident in the widespread adoption of the model and its ability to support the evolving needs of the Internet infrastructure. It provides modularity and abstraction with its layered architecture, and simplifies network design and troubleshooting. With each layer of TCP/IP being responsible and focused on specific functions and relying upon the services provided by the layer below, the TCP/IP model facilitates efficient and reliable data communications across diverse environments.

### 2.1.2 IPv4 vs IPv6

IPv4 remains widely used, despite IPv6 adoption finally being increased as it has become more than apparent that IPv6 is the only sustainable addressing strategy based on the current tools at hand and the exhaustion of IPv4 addresses. The total amount of IPv6 addresses allocated and assigned in Europe can be seen in Figure 2.2 below, provided to the public by RIPE NCC [24] and from the RIPEstat [25] platform which uses measures taken from the Routing Information Service (RIS) project [26] that helps our understanding of global routing and the RIPE Atlas [27] infrastructure. In total, the number of IPv6 addresses in Europe that have been allocated to ASNs are approximately 174,257 and can be seen in the blue line in the graph, whereas the red line depicts IPv6 addresses assigned which are counted to 3 only units. The following measurements have been made by RIPE NCC which collects BGP routing data since 1999 by using the RIS project.

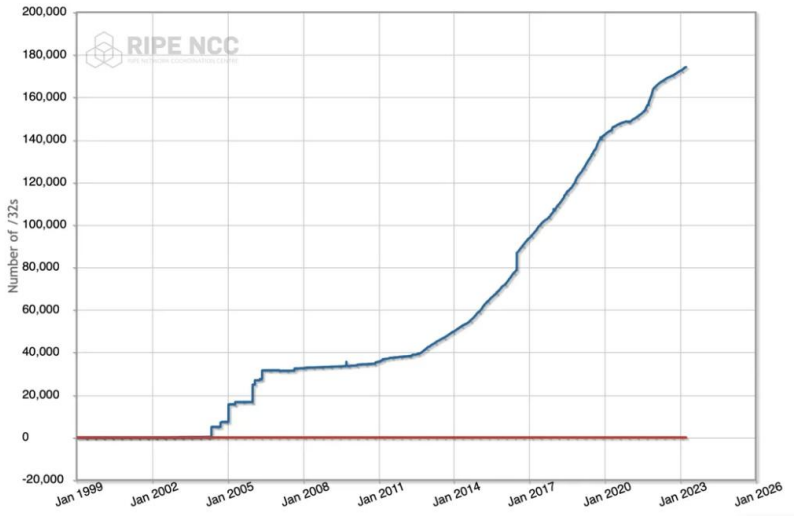


Figure 2.2 Amount of IPv6 addresses allocated and assigned by RIPE NCC [28]

Despite the serious BGP security vulnerabilities that continue to pose great risks to the seamless network connectivity and routing, BGP remains the primary networking protocol used between ASes used to exchange routing information between them, with vulnerabilities and attacks such as BGP-hijacking and BGP route leaks happening at an alarming rate each day and will be further investigated in the following subsection. In Image 2.1, the number of aggregated global BGP attacks in the time span of 18th May 2024 and 20 May 2024 can be seen, as was taken from the Internet Health Report (IHR) site.

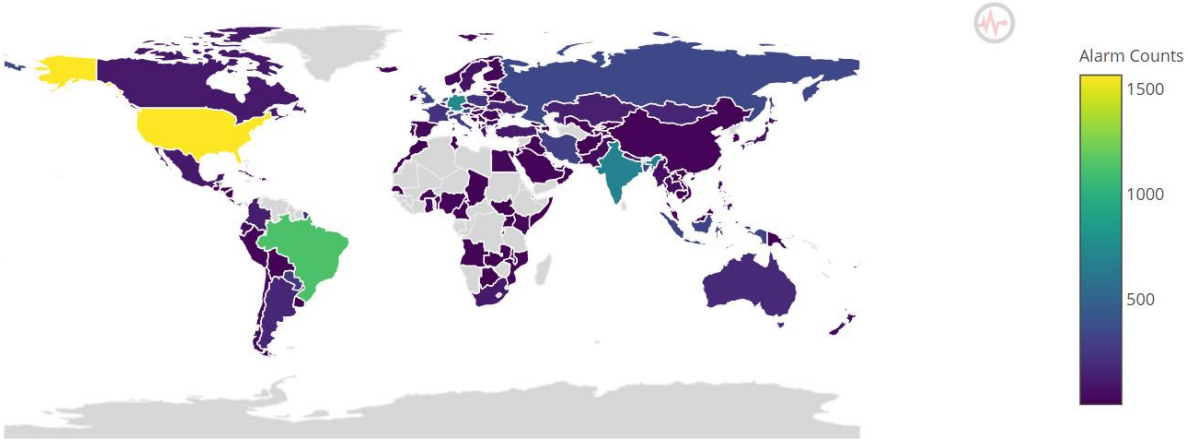


Image 2.1 Aggregated global BGP attacks for 2024-05-18 and 2024-05-20 [29]

Understanding the current state of the Internet involves recognizing the persistent reliance on IPv4. The transition from IPv4 to IPv6 is critical for the future of Internet scalability and sustainability, with IPv6 offering a vastly larger address space, necessary to accommodate the growing number of devices connected to the Internet.

## 2.2 Emerging Technologies

### 2.2.1 Internet of Things

The term “Internet of Things” is an ambiguous one but according to IEEE [30] refers to the network of interconnected physical objects called “things” which are embedded with sensors and software, enabling them to use their, usually limited, hardware in order to connect with other devices and systems on the Internet and exchange data.The objects can vary between smart thermostats and smart wearable watches, to smart cars and military drones. IoT was first mentioned by K. Ashton [31] in 1999 when he was researching the usage of Radio Frequency Identification (RFID) to improve on the supply chain management, making him a pioneer in the RFID field. IoT devices, usually retrieve and store data by the use of microcontrollers or Systems on a Chip (SoC) that have a whole computing system on the tiny surface of an electrical chip or an integrated circuit [32], and they offer services and applications, using Machine-to-Machine (M2M) communications, in order to close the gap

between the physical and digital world, and improve on the experience, efficiency and automation of tasks. IoT devices have become part of our everyday life as the technology supporting them has advanced, the necessary hardware has become smaller and the development of the appropriate low-power cost protocols (LoRaWAN, ZigBee, LTE-M, etc) have been developed and are continuously improving. The prominence, impact and extent IoT that allows any low cost devices [33] to be able to automate tasks at our convenience [34] has conquered the world, and has led and urged the appropriate research for the comparison of which low-cost protocol is better, i.e. Gloria et al. [35], but simultaneously IoT deployments are often found in exposed physical environments and are usually in insecure unencrypted networks [36] becoming a new security risk, a wealthy well of vast amounts of data that can be analysed to gain valuable insights for businesses and individuals that threat actors can target [37][38][39][40][41]. From this threat came into being multiple research projects on how to secure IoT infrastructures and IoT devices from attackers, in order to prevent malicious actors from collecting and transmitting sensitive personal data from the devices, or compromising and using them in botnet attacks. Research in the security aspect of IoT devices is ongoing. Just to name a few, such research includes Jurkut et al. [42] proposal for authentication and authorization, Zhang et al. [43] proposal to use a lightweight data integrity protection scheme in the form of a position random watermark generated by a one-way SHA-1 hash function, Raza et al. [44] development and proposal of an embedded IDS for IoT devices named SVELTE, and Jarjer et al. [45] proposal on the use of AI techniques such as ML and Deep Learning (DL).

### 2.2.2 5G Networks

5G Networks is the fifth generation of wireless communication technology, designed to enable high data speeds by operating on a wide range of frequencies, increased connectivity and reduced latency. The development of 5G started in 2010, driven by the need for the betterment of mobile broadband experiences and applications in IoT, and it became essential for implementing pervasive digital services and ensuring continuous connectivity. 3GPP in 2015 developed the New Radio Access Technology (RAT) for 5G Networks, namely 5G New Radio (NR), with Release 15 [46]. 5G NR's development drew to a conclusion in 2018, and then the Third Generation Partnership Project (3GPP) started delivering the first set of standards for 5G, with the first specifications being published in 2017. Soon after, commercial deployment started with widespread adoption rates and even bigger ones being expected in the next few years with increasing coverage and the introduction of more 5G-enabled devices. Key technological advancements in 5G include millimeter-wave frequencies, small cell deployments, massive Multiple Input Multiple Output (MIMO), beamforming and network slicing. These technologies facilitate faster data transmission, lower latency, and the ability to support a vast number of connected devices, which are essential for emerging applications, such as autonomous vehicles, smart cities and advanced IoT ecosystems [47].

Expanding on the cutting-edge technologies used in 5G networks, millimeter-wave frequencies are high-frequency bands (24 GHz and above) that can provide large bandwidths, enabling higher data rates compared to 4G with data rates up to 10Gbps, however they have limited range and require line-of-sight communication, necessitating dense network deployments [48]. Small cells are low-power base stations that cover small geographic areas, improving on the network capacity and coverage, especially in densely populated urban areas [49], which leads to Massive Internet of Things (mIoT) and Massive Machine Type Communications (mMTC). Massive MIMO is a multi-antennae wireless communication technology. It uses a large number of antennas at the base station to improve spectral efficiency and increase data throughput. Massive MIMO can handle multiple data streams simultaneously, thus enhancing overall network capacity [50]. Beamforming is an advanced signal processing technique used in wireless networks including 5G network, to direct radio waves to specific receivers, rather than broadcast them in all directions. It offers substantial improvements in signal quality, capacity and efficiency, by improving the signal's strength, reducing interference, and increasing data throughput. Beamforming is particularly useful for systems that use Massive MIMO to manage the complex interactions between the antennas and receivers, as it allows for spatial multiplexing, where multiple data streams are transmitted simultaneously over the same frequency channel but directed to different users, which significantly increases the network's capacity and spectral efficiency [51]. Network slicing [52] is a transformative concept in 5G networks that allows multiple virtual networks to be created on a shared physical infrastructure, by utilizing on SDN and NFV dynamic and efficient management of network resources. Each slice can be configured to meet specific requirements of different applications, services or customers, which enables operators to provide customized network services with varying levels of performance, security and reliability on the same physical network [53], thus enhancing service flexibility and efficiency [54] and enabling efficient resource allocation [55].

5G can provide high data speed rates, low latency, increased capacity, enhanced reliability, and energy efficiency. More specifically, 5G reduces latency to as low as 1 millisecond, which is crucial for real-time applications, and it increases the capacity of devices that can be connected per unit area, which is essential for IoT applications and infrastructure, enabling more robust connections with fewer drops and interruptions, as it is designed to be more energy efficient, which can be crucial for low-power IoT devices. On the other hand, 5G has high infrastructure costs, coverage limitations, compatibility issues, increased attack surface and protocol availability. As 5G networks enable applications ranging from ubiquitous broadband to autonomous vehicles, to fully autonomous transportation infrastructures and smart cities, there have been many research projects and many new ones on how to achieve secure and trustworthy 5G networks [56], by researching on efficient end-to-end security technologies that utilize Artificial Intelligence (AI) algorithms [57] , Machine Learning

(ML) [58][59][60] and Distributed Ledger Technologies (DTL) [61][62][63], involving developing AI-driven Software Defined Security (SD-SEC) solutions [64].

### 2.2.3 Edge and Cloud Computing

Edge Computing is the concept of the data processing occurring closer to the data source, at the network's periphery, rather than relying on centralized data centers, as was the case since not so long ago. The rise of Edge Computing is closely linked to the proliferation of Internet of Things (IoT) devices, which demand rapid and efficient data processing to function effectively. Seminal works such as by Shi et al. [65] have been instrumental in defining and advancing this field. Edge Computing offers numerous advantages, including decreased latency, improved bandwidth efficiency, real-time data processing, and enhanced reliability. By executing data processing tasks closer to the data source, latency is minimized, which is crucial for applications requiring immediate responses. The localization of the processing also ensures continuous uninterrupted operations, even if the connection to central cloud services is disrupted [66]. However, at the same time, Edge Computing has to deal with increased complexity in managing a distributed network of edge devices, scalability issues, higher initial deployment and maintenance costs, limited resources and energy consumption constraints at the edge nodes, particularly in remote or mobile environments [67]. Edge devices typically have limited processing power and storage capacity, making them less capable than centralized data centers. Furthermore, Edge Computing introduces a set of security risks, such as physical security threats to the edge devices, data integrity challenges, network vulnerabilities, and compliance issues. Edge devices can be physically compromised or stolen, making it difficult to ensure the integrity and authenticity of the data they process. Moreover, managing compliance across a vast and distributed array of edge devices adds another layer of complexity [68].

Cloud Computing involves delivering computing services, such as storage, processing power, and networking, over the Internet. This approach allows organizations to access the provided resources from providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform on-demand, eliminating the need to own and maintain physical infrastructure. Emerging in the mid-2000s from concepts like distributed computing and virtualization, Cloud Computing gained momentum as companies began offering scalable, cost-effective services. The influential paper by Armbrust et al. [69] significantly shaped the field's understanding and adoption. Cloud Computing provides scalability, cost efficiency, accessibility, robust disaster recovery solutions, and rapid deployment of applications and services. Organizations can scale resources up or down based on demand, reducing capital expenditure through a pay-as-you-go model. Additionally, cloud services offer ubiquitous access to applications and data, enabling remote work and collaboration, and support comprehensive disaster recovery strategies due to their distributed nature [70]. However, Cloud Computing also has

disadvantages, such as latency issues, where data must travel to and from remote data centers within the Cloud infrastructure of the vendor; reliance on stable internet connections; compliance challenges, as compliance with data protection regulations is often found to be complex and challenging to manage; resource limitations and high costs; and security risks, as centralized data storage can be vulnerable to cyber attacks, including data breaches, insider threats, account hijacking, and DoS attacks [71].

Hybrid Cloud-Edge Computing approaches can harness the strengths of both paradigms. Critical data can be processed at the edge for real-time needs, while less urgent data can be sent to the cloud for long-term storage and analysis. The deployment of 5G networks is expected to further bolster Edge Computing by offering faster, more reliable connectivity. Additionally, integrating AI and ML at the edge can facilitate more intelligent, autonomous decision-making processes in real time [72][73][74].

### 2.2.4 Software Defined Networks and Virtual Network Functions

Software Defined Networks (SDN) is an innovative network architecture that decouples the network control plane from the data plane, enabling centralized management of network resources and more agile network configurations. By abstracting the control functions from hardware, SDN allows network administrators to programmatically manage, control, and optimize network resources through software applications, resulting in more flexible and efficient network operations [75]. The concept of SDN emerged in the mid-2000s and was significantly advanced by the seminal work of the Open Networking Foundation (ONF) and initiatives like OpenFlow, which provided a standardized interface for the SDN control plane to communicate with network devices [76]. SDN offers several advantages, including improved network flexibility, easier management, rapid deployment of new services, and enhanced security. It allows for dynamic adjustment of network configurations in response to changing traffic patterns and business requirements, providing a more adaptive and responsive network infrastructure [77]. However, SDN also presents challenges such as the potential for single points of failure due to centralized control, security vulnerabilities in the SDN controller, and the need for substantial investments in new technologies and training for IT personnel [78].

Virtual Network Functions (VNF) refer to the virtualization of network services traditionally run on proprietary hardware, such as firewalls, load balancers, and routers. VNFs run on VMs or containers on standard servers, providing greater flexibility and cost efficiency compared to traditional hardware-based network functions. This shift is part of a broader movement towards Network Functions Virtualization (NFV), which aims to decouple network functions from dedicated hardware devices [79]. In the early 2010s, driven by the European Telecommunications Standards Institute (ETSI) NFV Industry Specification Group (ISG), laid down the foundational framework and standards for NFV

[80]. VNFs offer reduced capital and operational expenditures, faster deployment of network services, and improved scalability and elasticity, among other benefits. By leveraging standard IT virtualization technologies, VNFs allow network operators to quickly roll out new services and dynamically allocate resources based on demand [81]. However, VNFs also have performance overheads due to virtualization, interoperability issues between different vendors' solutions, and can be complex in their management [82].

The integration of SDN and NFV presents a powerful combination for modern network architecture, enabling more programmable, scalable, and efficient networks, that has become highly adopted. This integration supports advanced use cases such as network slicing in 5G, automated network management, and real-time service provisioning [83]. As technology evolves, the adoption of SDN and NFV is expected to grow even more, following the ongoing advancements in network virtualization, cloud computing, and AI-driven network management [84].

## 2. 3 Security Concerns

In continuation, we will mention some of the attacks that post serious threats to network infrastructure and the continuous deliverability of services, so that later on it will be clear what SCION is aiming at in terms of security in inter-connected ASes. We will briefly see how IoT devices are vulnerable and usually used to expand the field of an attack’s impact, as well as how vulnerabilities in routing protocols such as OSPF and Enhanced Interior Gateway Routing Protocol (EIGRP) are used from malicious actors, and some of the security concerns in 5G technology. As the reason we discuss the aforementioned cybersecurity vulnerabilities, risks, attacks and some of their contemporary mitigation techniques is in the scope of SCION and to set what is the background of technology nowadays to see how SCION comes in and solves these problems. We will not go into depth despite the severity and weight of these attacks. Nevertheless, the above attacks, as well as attacks such as phishing, DNS spoofing, e-mail spoofing, SQL injections, reverse engineering and many more constitute a very interesting and educational material that concerns us all and should be part of our early education in order to stay safe in the digital world. SCION aims to become a fortification between the sensitive and critical systems and the miscellaneous malicious attackers.

In general, malicious actors, ranging from individual hackers to sophisticated cybercrime organizations, exploit vulnerabilities and security risks inherent in systems. These risks arise from flaws within the code, misconfiguration in network infrastructure, firewalls and systems, or human error. By leveraging on a variety of tools and techniques these malicious actors capitalize on weaknesses and vulnerabilities in the systems in order to gain unauthorized access, steal sensitive data or disrupt the availability of services provided, using either malware, advanced persistent threats

(APT) or social engineering, with their motivations ranging from economical to political to egotistical. From exploiting on zero-day vulnerabilities, before security patches are available to the affected systems, to taking advantage of lax security protocols in organizations, the attackers operate with a mind in the maximization of their attack's impact in mind. As technology evolves rapidly and new vulnerabilities emerge with each new update, contemporary malicious actors have become extremely sophisticated, with a tool-set similar to that of the systems' defenders. This underscores the critical importance of proactive security measures and constant risk assessment in the face of evolving threats.

### 2.3.1 BGP hijacking

BGP hijacking, or prefix hijacking, is an attack where an AS and a network falsely, intentionally or mistakenly, originates a prefix that belongs to another AS without the latter's permission. Generally, BGP hijacking happens with malicious intent and is an illegitimate action taken to steal the network traffic from a popular network. For reference, in 17 August 2022, Amazon, namely AS 16509, lost for a period of three hours the control of their IP space as suddenly another AS, Quickhost.uk with ASN 209243, which itself may have been a victim of the original attackers, began to announce that AS209243 is the proper path to reach the subnet destination of 44.235.216.0/24 of Amazon. The affected Amazon subnet hosts cloud applications critical for the Celer Bridge cryptocurrency exchange. In the span of only three hours the attackers were able to drain 32 accounts of a total of $234,866.65, by posing as the legitimate application [85][86]. Likewise, similar BGP attacks happen regularly in the Internet to mislead legitimate popular network traffic to another destination with the intention to either be able to gain on the populace such traffic can bring them, attack their competitors, extort money or steal crypto currency. Several times, those attacks happen from the same malicious ASes, where the networks themselves act maliciously, repeatedly hijacking address spaces with intent, thus earning the designation of serial hijackers [87].

BGP hijacking is a persistent threat in network communications, and can also happen by a malicious actor purposefully injecting false records in the Internet Routing Registry (IRR) [88]. The IRR [89] is a set of distributed databases and used by networks to register routing information and validate messages received in BGP communications. Being first deployed in the 1990s, the IRR still remains the most widely registry used today, despite lacking strict validation standards for the creation or modification of records in the registry, as well as more recent and secure alternatives such as Resource Public Key Infrastructure (RPKI) [90] being available for implementation, enabling current research and development to shed light on the vulnerabilities and irregularities within the IRR system [91].

Some of the known mitigation methods for BGP hijacking attacks involve the implementation of digital certification of the source prefix enabling others to validate the association between a prefix and an autonomous system by the use of RPKI [92][93]. Another method is the utilization of tools for BGP monitoring connections for real-time detection and automatic mitigation for BGP hijacking, such as BGPmon and ARTEMIS [94]. Finally, network operators of ASes can apply strict network inbound and outbound filtering policies for their BGP announcements that can match on IP prefixes, AS paths, BGP communities, Time to Live (TTL) and other attributes [95].

### 2.3.2 Distributed Denial of Service

Distributed Denial of Service attacks or DDoS attacks are large scale attacks targeting large corporations and organizations, and they aim to overwhelm the systems, network or services provided by the organization with a flood of traffic, rendering the services unavailable to the legitimate users. Usually attackers target Web servers, DNS server, legacy servers and financial servers. Even when those servers are hosted in cloud infrastructure, the malicious actors exploit vulnerabilities found in the network systems hosting the Cloud services leading researchers in inventing new or enhancing already known security algorithms, as was the case with the study from C. Bayoli et al. [96] about implementing a Real-Time Network Traffic Attacks Detection (RTNTAD) algorithm that was designed and based upon the Adaptive Cumulative Sum (CUSUM), the Exponentially Weighted Moving Average (EWMA) and Naive Bayes security algorithms for detecting DDoS attacks in Cloud environments.

There have been many mentionable studies from researchers, academia and corporate, to ensure the accurate detection of DDoS attacks in network systems. Namely, Soro et al. [97] studied how Artificial intelligence (AI) and Machine Learning (ML) can be used to develop and enhance security algorithms to monitor and detect attacks. Wang et al. [98] proposed an IDS solution that works upon the SDN and Cloud computing architectures of the defenders infrastructure and integrates a highly programmable Network Intrusion Detection System (NIDS) that can detect attacks and enable flexible control and reaction. Yin et al. [99] proposed an IDS approach that utilizes on deep learning and recurrent neural networks, and Zhang et al. [100] proposed a NIDS that utilizes NetFlow [101] for data captures, and is based on the random forest classification algorithm, adapting the algorithm to the Apache Spark [102] distributed processing system for real-time detection. Somasundaram and Meenakshi [103] proposed the usage of verification modules and elastic load balancers for the detection and mitigation of DDoS attacks, and Virupakshar et al. [104] proposed a system with an OpenStack [105] integrated firewall [106] enabling raw socket programming, utilizing algorithms such as Decision Tree, K Nearest Neighbour (K-NN), Naive Bayes and Deep Neural Networks (DNN).

For example, a common DDoS attack is when the threat actor targets the DNS resolving servers of an organization, using either DNS flooding or DNS amplification DDoS attacks. During either of those DNS DDoS attacks, the threat actor exploits on the core function of DNS servers which is that the DNS service, configured to be an open resolver, must answer the queries that reach it. In DNS amplification DDoS attacks, the malicious actor, taking advantage of that fact, launches a scalable attack where they enable, often geophysically, distributed botnet systems that have different or spoofed IP addresses, which cannot be summarized in one simple CIDR (Classless Inter-Domain Routing) and be blocked by adding a simple filtering policy on the organization's firewalls, to start asking the DNS server small queries that have large answers. By the bots having spoofed IP addresses the answers the DNS service provides reach the wrong target. In DNS amplification attacks the target is the holders of the spoofed IP addresses, as when the large answers the small but carefully crafted queries from the bots produced reach the spoofed IPs, in that way draining on network resources and eventually rendering the target unreachable and causing denial of service. By using an amount of bots in a botnet, the attacker can magnify their attack and stay obfuscated behind them, safe from detection.

In a DNS flood, the attacker enables bots, to have the magnitude the automated queries from the bots can offer, using them to open channels with the DNS servers, ask a query and instantly drop the connection before the server's answer reaches it. This tactic leaves open channels between the bot and the DNS server, that the DNS server cannot close by itself as it has to answer the query it received and then the channel can close, and it eventually overwhelms the targeted systems. Depending on the resources of the DNS server, how it is configured and the firewalls defending it,

The difference with a DNS flooding attack is that the threat actor's target is the organization serving DNS queries and its DNS servers, as it can be seen in Figure 2.3.

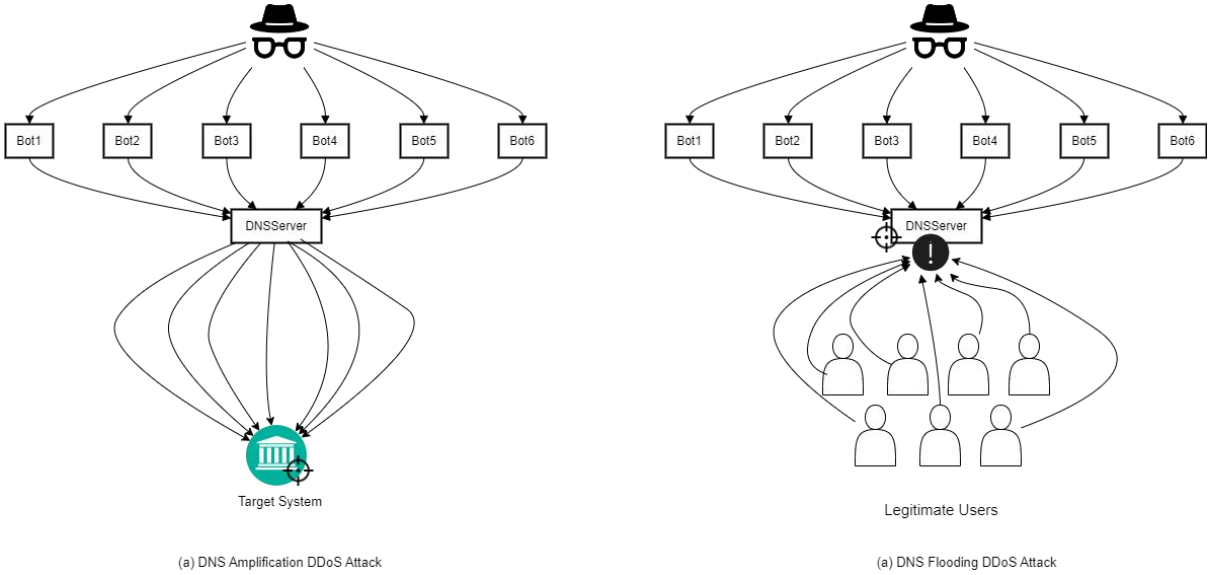


Figure 2.3 Comparison between (a) DNS amplification and (b) DNS flooding DDoS attack

### 2.3.3 IoT Vulnerabilities

The proliferation of IoT devices has introduced numerous security concerns and vulnerabilities that can be exploited by threat actors, posing significant risks to both individual users and large organizations and their infrastructures. These vulnerabilities stem from several factors, such as the inherent limitations of IoT devices, insufficient security measures, and the complexity of IoT ecosystems. The majority of IoT devices is structured with limited computational resources and minimal security features due to cost and power constraints. The hardware limitations of IoT devices make it challenging to implement robust security measures, thus IoT devices are left susceptible to various attacks, such as unauthorized access and data breaches [107]. As manufacturers often favour and prioritize functionality and their ability to be faster in introducing a new product in the market over security, we are left with devices that have hardcoded credentials, unpatched firmware and insecure communication protocols [108]. The IoT ecosystem being highly fragmented, with many different devices from different manufacturers, is often found lacking homogeneity and standardization, which complicates the implementation of comprehensive security frameworks, as the heterogeneous devices may very well be using different communication protocols and support different security standards from one another. The absence of universally accepted standards in IoT exacerbates interoperability issues, thus leading to security gaps that can be exploited by malicious actors [109]. As IoT devices frequently communicate over unsecured or poorly secured channels, they lack of encryption and have weak authentication mechanisms, which can expose sensitive data to eavesdropping and man-in-the-middle attacks. Additionally, many IoT devices use wireless

communication protocols, which are inherently vulnerable to interception and jamming [110]. Ensuring secure communications in a IoT infrastructure and data transfers between IoT devices and central systems, is crucial but is often overlooked in their implementations. Furthermore, another concern is that IoT devices are often left running on outdated firmware with known security flaws. As IoT have such an extended target group, with their consumers being from experienced IT technicians to ordinary people, the vast majority of the users lacks the technical expertise in order to keep their devices updated and patched. Even when updates are available, the process can be cumbersome and inconsistent across different devices. Unpatched vulnerabilities provide an easy target, leaving the devices open to attackers, as the devices can be easily compromised and potentially lead to breaches in larger networks [111]. IoT devices are often deployed in accessible and open locations, making them susceptible to physical tampering, where attackers can gain physical access and extract sensitive information, install malicious firmware, or disrupt their functionality. Ensuring the physical security of IoT devices is as important as securing their software components, yet it is frequently neglected [112]. The majority of IoT devices can create significant scalability and management challenges. Ensuring the security of a large and diverse fleet of devices requires substantial resources and advanced management tools. Network segmentation and access controls are critical to prevent unauthorized access and contain potential breaches, but implementing these measures at scale can be difficult and resource-intensive [113]. Lastly, as IoT devices often collect and transmit large volumes of personal and sensitive data, i.e. medical data, the data privacy and regulatory compliance is a significant challenge that must be conquered, especially with varying regulations across different regions. Data breaches can lead to severe legal and financial repercussions, making it essential to implement strong data protection measures [114].

### 2.3.4 Routing Protocol Vulnerabilities

Despite the advancements in network security, routing protocol vulnerabilities remain a significant concern. As previously stated, BGP is particularly susceptible to attacks due to its fundamental role in Internet's routing infrastructure, with ongoing efforts on enhancing the security of routing protocols through cryptographic techniques, improved protocol designs, and the adoption of secure routing standards like BGPsec [115][116]. Protocols such as OSPF and EIGRP are also widely adopted and play a crucial role in communications by determining the best path within large and complex networks, thus being targeted by malicious actors.

OSPF, being a widely used interior gateway protocol, standardized by the IETF as an open protocol, employing a link-state routing algorithm to calculate the shortest path for data packets [117], is susceptible to several types of attacks due to its reliance on trust among routers within the same area. The Link-State Advertisement (LSA) flooding attack, where the attacker floods the network with fake

LSAs, disrupting the OSPF database, overwhelming the OSPF routers, thus causing instability and routing loops [118] as the LSA attack causes the routers to consume excessive CPU resources and potentially crash [119]. Route injection is also a major issue, where the attackers inject incorrect routing information via malicious LSAs, redirecting network traffic through compromised or malicious routers [120], enabling man-in-the-middle (MitM) attacks and unauthorized data interception. OSPF is also vulnerable to hello packet spoofing attacks which disrupt the OSPF neighbour relationships, which can cause routers to falsely detect neighbours as down, leading to disrupted communication and network partitioning [121].

EIGRP is a Cisco proprietary interior gateway protocol, used for dynamic routing in large networks and it utilizes a hybrid routing approach combining the features of link-state and distance-vector protocols to optimize route calculation and minimize routing table updates [122]. Despite its robustness, EIGRP suffers from attacks such as unauthenticated route updates where routers may accept malicious routing information [123], routing table poisoning where an attacker injects false route information [124], and resource exhaustion attacks where continuous routing updates can deplete router processing resources, leading to degraded performance or outages [125].

### 2.3.5 5G Security

The enhanced capabilities 5G networks offer also introduce a range of security concerns that need to be addressed to ensure the reliability and safety of the network. In Table 2.1 a categorization of the security concerns as well as the reasons they arise is shown.

Table 2.1 5G security concerns

| **Category** | **Reason** | **What happens** |
|---|---|---|
| Increased Attack Surface | 5G supports massive number of connected devices including IoT devices. | The decentralized nature of 5G, with more edge devices and distributed architectures, further complicates the security landscape. [126] |
| Network Slicing Vulnerabilities | Multiple virtual networks running on the same physical infrastructure. | If one slice is compromised, it can potentially affect others, especially if isolation between slices is not properly maintained. [127] |
| Virtualization and Cloud Security | Heavily relying on virtualization technologies. | Vulnerabilities in SDN and NFV, such as hypervisor attacks, Virtual Machine (VM) escapes, and misconfigurations, affect 5G security. [128][129] |
| Supply Chain Risks | Complex and global 5G supply chains introduce risks related to | Vulnerabilities in the supply chain could be exploited by malicious |

| | | |
|---|---|---|
| | hardware and software integrity. | actors to insert compromised components, leading to potential backdoors and security breaches. [130][131] |
| Authentication and Encryption | Potential use of outdated cryptographic algorithms | The utilization of robust algorithms and ensuring end-to-end encryption is paramount. [129] |

To address the above concerns, the 5G standard utilizes enhanced security protocols, such as the 5G Authentication and Key Agreement (5G-AKA) which improves on the security mechanisms of 4G and 3G, and uses asymmetric randomized encryption to provide stronger mutual authentication between devices and network [129][132]. 5G implements a Zero Trust architecture, which assumes that threats could be present both inside and outside of the network, eventually helping in mitigating risks by employing Defense in Depth and tactics such as continuous verification of user identities, strict access controls, and continuous monitoring of the network traffic for anomalies as M2M IoT communications in 5G networks pose new threats [133][134]. To ensure that VNFs stay isolated from one another and secure NFV environments, techniques such as channel encryption by the use of Transport Layer Security (TLS) to protect data in transit, strong authentication mechanisms for the verification of the identity of users and systems, strong cryptographic hashes to ensure data integrity and unaltered software and configurations by implementing secure boot mechanisms to ensure that only trusted software is loaded, hardware-based security modules are also employed to ensure the integrity of VNFs and the underlying infrastructure. Furthermore, utilization of containerization, micro-segmentation, separation of VMs or containers help in the isolation and protection of VNFs, as well as the usage of automated tools to enforce configuration policies and regularly check for compliance [135]. For supply chain security, mitigation happens with the utilization of secure firmware updates, the implementation of tamper-evident technologies and the adoption of standards provided by organizations such as the National Institute of Standards and Technology's (NIST) guidelines on supply chain security [136]. Lastly, AI, Big Data and ML technologies are increasingly being used in 5G networks, as by their utilization helps in the analysis of large volumes of data to detect anomalies, and they can be used to predict potential security breaches, as well as automate responses to them, thus enhancing and providing an intelligent management of network security [137].

### 2.4 Regulations and Policies

Key regulations and policies governing data privacy and protection on the Internet, as well as standards and guidelines set by organizations such as NIST, have crucial importance in the digital environment we all live in. Foundational legal frameworks to regulate data privacy and protection

have been established globally in order to protect and ensure that personal data are handled responsibly and securely.

### 2.4.1 Net Neutrality

Net Neutrality is a fundamental principle of Internet governance that states that all data on the Internet should be treated equally by ISPs, without discriminations, differential charging based on user, content, website, platform or applications, and they must provide access to all content and applications regardless of the source, without favouring or blocking particular products or websites. [138]. The arguments for Net Neutrality are equality and fairness for equal access to information and services without undue discrimination; innovation by allowing new start-ups and services to compete on the same level as big corporations without being throttled or blocked by the ISP; and consumer protection by preventing ISPs from exploiting their control over Internet access to charge higher fees or to prioritize their own services over their competitors. At the same time, opponents argue that ISPs need the ability to manage their networks and charge for different levels of services to fund their expansion and maintenance, as an infrastructure investment, or they believe that allowing ISPs to offer premium services could lead to market efficiency, or they claim that Net Neutrality imposes heavy regulations that stifle innovation and adaptability. However, international treaties and cooperation can lead to more harmonized global standards. Net neutrality is a continuous and evolving issue, involving technology, politics and consumer rights, and understanding its implications helps in realising the broader regulatory environment and the needed balance between regulations, innovation, and access to information.

### 2.4.2 Data Privacy Regulations

The GDPR in the European Union (EU) was enacted in April 2016 and enforced from May 2018, and applies to all member states of the EU and any organization processing personal data of EU citizens, regardless of the organization's location. GDPR has set a high standard for data protection and has influenced regulations in other regions, as it ensures that individuals have rights to access, erase and transfer their data and organizations must obtain explicit consent from the individual before any processing of their data. GDPR also enforces organizations to appoint Data Protection Officers (DPOs) if they process any large amounts of sensitive data, and they must notify the authorities in case of data breaches within 72 hours. Non-compliance to GDPR policies can result in fines up to 4% of annual global turnover or 20€ millions, whichever is higher [139].

Similar to GDPR, is the California Consumer Privacy Act (CCPA) in California, USA. It was enacted in June 2018 and enforced from January 2020, and it applies to businesses that collect personal data from California residents and meet certain criteria, for example annual gross revenue over $25

millions. CCPA provides similar rights to Californians as GDPR does to Europeans, including the right to know, delete and opt-out of the sale of their personal data. According to CCPA, businesses must disclose what personal data they collect and how they are used, and their non-compliance can result in fines up to $7,500 per violation. CCPA has set a standard in the USA, and has set a precedent for state-level data privacy laws and many discussions about a federal privacy law have started [140].

Similar to GDPR and CCPA, are legislations and regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the US, the Personal Data Protection Act (PDPA) in Singapore, the Brazilian General Data Protection Law (LGPD) in Brazil, and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. These legislations provide the legal framework within which organizations must operate, ensuring that personal data is handled responsibly and securely, protecting the individual's rights.

# 3 Research Initiatives for a Secure Internet Architecture

As we have seen from the previous study, Internet while scalable and robust, has inherent security vulnerabilities and limitations. These issues necessitated the development of new, more secure Internet architectures through targeted research initiatives that aimed to address Internet's security flaws, to improve on resilience and reliability, to support emerging technologies like IoT and 5G, ensure privacy and adapt to regulatory changes.

## 3.1 New Internet Routing Architecture

The New Internet Routing Architecture (NIRA) is an initiative that aimed to give users the ability to choose the path their packets are going to take through the network, while simultaneously having control over the overall routes. NIRA supports "user choice without running a global link-state routing protocol", as is stated in X. Yang et al. (2007) NIRA proposal [141].

Key features of NIRA are path control, multiple path choice, traffic engineering and enhanced security. By depositing routing control to the end user, NIRA enables them to choose from multiple paths, thus providing redundancy and fault tolerance, allowing them to avoid congested or potentially insecure routes. By giving routing control to the end users, NIRA can also help in avoiding paths that go through compromised or malicious networks, reducing the risk of routing attacks like BGP hijacking. End hosts can optimize their path choices based on latency, bandwidth, and other performance metrics, and at the same time, NIRA architecture can adapt dynamically to changing network conditions, improving efficiency.

Despite its advantages, NIRA was not widely adopted as there had to be drastic infrastructure changes to the current network infrastructure and protocols, with the existing network technology heavily relying on established routing protocols like BGP, leading to high costs and significant changes to hardware, software and operational practices, Established ISPs and network operators resisted due to uncertainty on the technology, high costs and return on their investment. Finally, compatibility issues arose with complex interoperability with the current Internet architecture, as implementing NIRA requires coordination between multiple stakeholders, ISPs, network operators and end users which is very difficult to achieve, as well as the required effort to learn the new systems. So far, NIRA is mainly adopted in research settings and projects, remaining in Universities and Research Institutions, with minimal deployments in commercial operational networks.

## 3.2 Recursive InterNetwork Architecture

The Recursive InterNetwork Architecture (RINA) is a network architecture proposed in 2013 by Y. Wang et al. [142] as a novel network management architecture and solution to the current Internet architecture and its inherent security problems, as it treats networking as an Inter-Process Communication (IPC) only. RINA is a clean-slate network architecture that employs a single, recursive model to simplify network design and management. RINA provides layered architecture, by replacing the fixed layers of the traditional TCP/IP stack with multiple, repeating layers of IPC where each layer, or Distributed IPC Facility (DIF) in RINA, handles a specific scope of communication. DIFs are the fundamentals building blocks of RINA as they change the TCP/IP and OSI stacks by replacing the traditional layers with one single DIF that can be repeated as many times as the network architect requires. DIFs can be nested within each other, where each high-level DIF uses the services provided by lower-level DIFs to provide broad and complex communication capabilities according to the infrastructure's requirements [143]. DIFs naturally separate and handle miscellaneous issues in a coordinated and cooperative fashion to perform a certain function, i.e. network service management, orchestrating a set of application processes, thus creating a Distributed Application Facility (DAF). Each DAF has a group of processes responsible for the outcome of one function, with each process being a member of the DAF, namely a Distributed Application Process (DAP). The DIF is the organizing structure in RINA, a "layer", and a collection of IPC, whereas a DAF includes management functionalities but does not support IPC. RINA separates mechanisms and policies into different components of its architecture, enabling the optimal behaviour of a DIF to its best operational status, without the need for re-implementation of mechanisms each time there is a redefinition in its policies [144], thus making RINA more adaptive to real-time networking environments and their ever-changing conditions and specifications. More specifically, in RINA operations like data transfer, error detecting, flow and congestion controls, security and Quality-of-Service (QoS) are standardized in mechanisms, and their implementation happen via policies which can vary according to the environment's specifications and the DIF's requirements, thus enabling each DIF to implement specific policies for routing, security and resource management, making the architecture highly adaptable and flexible.

An example of a RINA network and the communication between two edge devices can be seen in Figure 3.1, with the different DIFs responsible for the different aspects of communications needed between two end hosts, and the intercommunications of the intra network of an ISP.

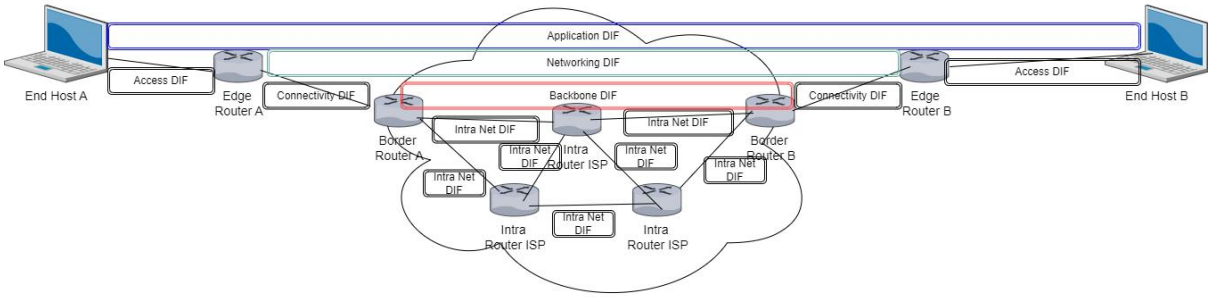


Figure 3.1 Communication between two edge devices through RINA enabled network

A simplified view of DIFs between three different devices, two end systems and a routerm, is depicted in Figure 3.2.

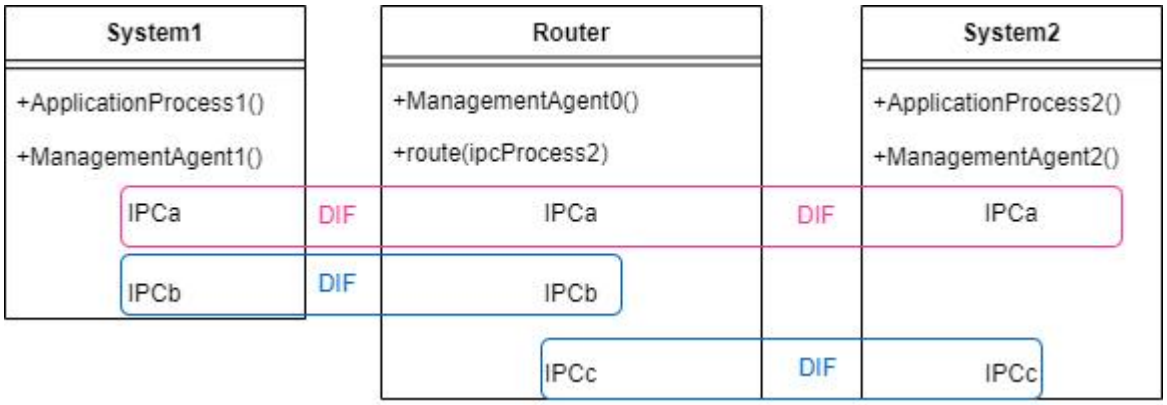


Figure 3.2 Intercommunications within a RINA network

DIFs can be loosely categorized in three different types based on their scope and function:

- The application process DIFs, where the DIFs manage the communication between application processes, similar to the Application Layer in TCP/IP.
- The network management DIFs, similar to the Network and Transport Layer in TCP/IP, where the DIFs manage the network resources and their allocation, including addressing, routing, and security.
- The network infrastructure DIFs, similar to the Physical and Data Link Layers, where the DIFs manage the basic communication functions necessary for the above DIFs to work.

The DIFs communicate and interact with each other via well-defined IPCs, which are managed through policies.

RINA integrates security and QoS in its model by having built-in security mechanisms for authentication, encryption, and data integrity, and enabling each DIF with its own set of specific security policies, and Access Control Lists (ACLs), as well as ensuring that network resources are efficiently managed and requirements are met. Moreover, RINA offers traffic engineering capabilities to control the flow and prioritization, with its recursive nature allowing for multiple communication paths, which can be chosen accordingly, thus providing resilience against routing attacks by choosing the more secure path. Finally, in case of a DDoS attack when a DIF becomes affected, it can be isolated from the rest and minimize the impact of the attack,

The RINA framework offers network operators and application programmers a transparent, minimal and dynamic Application Programming Interface (API), enabling them to programmatically manage and configure the various applications they want to be able to offer over their RINA network.

In conclusion, RINA provides a consistent, simplified network architecture, offering scalability, and uniformity with its recursive DIF model, as well as flexibility with its mechanisms and policies, and supports emerging applications, such as IoT[145] and 5G, with its flexible QoS management across DIFs and its efficiency in handling high-bandwidth applications.

Despite its advantages, the transformative architecture of RINA has not been widely adopted yet, as the transitioning requires fundamental changes in networking design principles, retraining of network professionals, and requires the development and deployment of a completely new architecture with the accompanying challenges and investments. Achieving widespread standardization, as essential as it is, is a slow and complex process, as the performance impact with the established networks, and interoperability issues with the existing Internet architecture and the established TCP/IP stack of implementing and transitioning to RINA must be ensured, as it will allow for a smooth and gradual transition. So far, RINA has seen adoption in academia, research, pilot projects and research initiatives, like PRISTINE (years active 2013-2016) and IRATI [143][146], and experimental deployments, but it still is in the early stages despite the significant progress that has been made in exploring and demonstrating RINA's potentials, the broader adoption still faces technical, economic and organizational challenges.

### 3. 3 **Pathlets**

Pathlets were proposed as an innovative approach to routing by P. B. Godfrey et al. in 2009 [147], and is a network architecture that views the Internet as smaller, more manageable segments, namely pathlets, which can be flexibly and dynamically combined to form bigger, end-to-end paths. It is a modular approach that aims to offer enhanced control, flexibility, adaptability, and resilience in

network routing. The modular nature of Pathlets allows for quick reconfiguration of paths to avoid compromised segments or for optimal performance.

Pathlets differ from the traditional networking architecture in the way that routing in Pathlets happens by dividing the fixed paths into smaller segments that can be recombined in various ways, offering more routing options. The key benefits of using Pathlets are enhanced control, flexibility, and resilience by allowing for the dynamic reconfiguration of routes, improved fault tolerance, and independent security management of each segment. The pathlets are managed independently from one another, with mechanisms in place to combine them dynamically based on the current network conditions and policies. Being independent, a pathlet can be secured from another that has become compromised, thus reducing widespread attacks, avoiding compromised segments and mitigating security threats. However, the management and optimization of Pathlets can be complex, as there is additional overhead associated with the segmentation management, and the integration of pathlets with the existing infrastructure. Nevertheless, experimental deployments have shown Pathlets potential in improving network performance and security, and concluded how Pathlets could be particularly beneficial in scenarios requiring high resilience and fault tolerance, such as disaster/recovery, high-performance computing, and military communications. Pathlets do not require a complete overhaul of the existing infrastructure and they work alongside the established protocols, such as BGP, source routing, and multipath proposals, as they are allowing for multiple policies. Research on Pathlets is still ongoing, with recent examples on how Pathlets can help in anomaly detection [148], and on expanding Pathlet potential and its resource management [149], as well as research on leveraging Pathlets for the design of a lightweight relationship anonymity protocol between end host and AS to be resilient against route injection and path altering attacks [150].

### 3.4 Scalability, Control, and Isolation on Next-Generation Networks

Scalability, Control, and Isolation on Next-Generation Networks, namely SCION [151] is a novel network architecture designed to provide scalability, control, security, and resilience to the contemporary Internet architecture. Key features of SCION, that are going to be discussed further in the continuation of this thesis, are:

- Path control and multipath communication, where end-users are allowed to control the paths their packets take through the network.
- Isolation Domains (ISDs), a new concept introduced in SCION where ASes and clusters of ASes are viewed independently, providing strong security and fault tolerance, enabling better trust management and security policies.
- Security by design, whereas SCION incorporates security features, such as cryptographic authentication of control messages, protection against BGP-hijacking, DDoS and routing attacks.

- Scalability, where the hierarchical design of ISDs, efficient path discovery and controls mechanisms ensure that SCION can support large networks.
- Fault tolerance, where the multipath communication and failover mechanisms make the SCION network more resilient to failures and attacks.

SCION introduces the new concept of ISDs, a logical cluster of ASes, that is the fundamental building block of SCION, where ASes and clusters of ASes are treated as independent entities. By isolating network connections of similar ASes to ISDs, SCION can achieve its targets of transparency, scalability, high availability, and heterogeneous trust support. As an AS can join an ISD by purchasing connectivity from a core AS, or by signing a Service-Level Agreement (SLA), the new AS accepts the core AS's Trust Root Configuration (TRC), which is the policy that governs the ISD and is negotiated by the ISD core, thus enhancing the trust between otherwise heterogeneous ASes. By joining an ISD, the AS members trust each other that their connections are secured from malicious traffic as all ASes under an ISD trust the TRC that governs their ISD. The TRC is responsible for defining the roots of trust within the AS that are going to be used to validate the bindings of names or addresses and public keys. This division in ISDs and the policies that govern them, enhances the security and fault tolerance between otherwise independent ASes, and offers better control by limiting the scope of routing information and reducing the impact of possible attacks, as disruptions are contained within a single ISD, preventing them from affecting the entire network of SCION. As each ISD operates autonomously, the overall resilience and scalability of the network is improved.

On path control and transparency, SCION offers the ability to senders and receivers of choosing and controlling the paths their data will take through the network. Unlike traditional network architectures, SCION provides multipath options, thus enabling its users to choose their routes based on performance metrics, such as latency and bandwidth, reliability, or security preferences, allowing for improved performance and reliability. This transparency enhances the overall user experience by ensuring more efficient and predictable data transmissions.

As security is viewed and treated as a foundational part of SCION, various security features are incorporated within SCION to protect against common network threats. Within others, SCION includes the cryptographic authentication of control messages so they are authenticated, thus ensuring their integrity and preventing their tampering, the secure verification of the authenticity of routing information to protect against BGP-hijacking attacks, and the implementation of robust security mechanisms to ensure the uninterruptedly continuation of network services, thus mitigating the impact of DDoS and routing attacks.

Furthermore, the hierarchical design of ISDs, along with efficient path discovery and control mechanisms, ensure the support of large and complex networks. As ISDs enable scalable routing by

the limitation of the scope of routing information within each domain, the overhead associated with global routing tables is reduced, and the network is allowed to grow without compromising the ISD's performance. The efficient path discovery processes further improves on the scalability by the quick identification of optimal paths.

The fault-tolerant design of SCION with multipath communication and failover mechanisms significantly heightens the network's resilience to failures and attacks, making SCION a robust and reliable network architecture capable of withstanding network disruptions. Even if some paths become unavailable, SCION ensures the continuous connectivity by offering more path choices for the data transmissions, as the failover mechanisms enabled in SCION automatically reroute traffic to an alternative path in case of the primary's failure, thus minimizing downtime and maintaining service availability.

In general, SCION offers improved performance with low latency and high bandwidth, as bandwidth usage is optimized by enabling more efficient routing and data handling, and the path selection mechanisms and direct inter-domain communications reduce latency. Moreover, in SCION, network administrators are able to define and enforce custom routing and policies within their own ISDs, establishing the connections and increased security they deem necessary. SCION is by design adaptable to various network environments and requirements, making it suitable for a wide range of applications and networks. Integration with existing networks and infrastructure are allowed by SCION's modular design, which in addition can support the integration with new protocols and technologies, ensuring the architecture's long-term viability. SCION is being actively supported by ongoing research and development initiatives, being continuously improved and addressing emerging challenges. At the same time though, one could be thoughtful of deploying SCION due to a possible management overhead, increased complexity, or simple resistance to change, being afraid of possible interoperability issues and initial costs. A comparison of advantages and disadvantages in deploying and implementing SCION can be studied at Table 3.1.

Table 3.1 Advantages and disadvantages of deploying and using SCION

| **Aspect** | **Advantages** | **Disadvantages** |
|---|---|---|
| Security | ● Cryptographic authentication of control messages<br>● Protection against BGP-Hijacking attacks<br>● Resilience to DDoS attacks<br>● Resilience to routing attacks | ● Dependency on cryptographic algorithms/techniques that may have vulnerabilities<br>● Potential introduction of new attack vectors |
| Path Control | ● User controlled path selection<br>● Multiple path options | ● Increased complexity in path management |

| Aspect | Advantages | Disadvantages |
|---|---|---|
| Performance | ● Low latency due to efficient path selection<br>● High bandwidth efficiency | ● Possible latency due to additional security measures<br>● Possible overhead from cryptographic operations and control messages |
| Scalability | ● Hierarchical design reducing global routing table complexity<br>● Efficient path discovery mechanisms<br>● Efficient control mechanisms | ● Managing large number of ISDs<br>● Careful management of ISDs' scalability |
| Fault Tolerance | ● Multipath communication for continuous connectivity<br>● Failover mechanisms for automatic traffic rerouting | ● Increased complexity in implementing failover mechanisms |
| Control and Isolation | ● ISDs<br>● Trust management<br>● Security policies | ● Potential administrative overhead with ISD management |
| Flexibility | ● Customizable routing and security policies<br>● Adaptable to miscellaneous network environments | ● Changes to existing infrastructure required |
| Design | ● Modular design allowing for integrations with new technologies<br>● On-going research and development | ● Initial deployment and training costs<br>● Resistance to change from existing infrastructure |
| Deployment | ● Offering test-beds to interested users and entities to test SCION (i.e. SCIONlab)<br>● Available for deployment both on ISPs with large and complex network infrastructure and end-users with COTS hardware | ● Potential interoperability issues with existing network protocols and systems |

### 3.4.1 The role of Géant

Géant is the pan-European data network for the research and education communities, offering robust and high-speed internet connectivity with speeds up to 1Tbps, extensive coverage as the Géant network connects over 50 million users in more than 10,000 institutions, including links to other research network facilities worldwide, using advanced technologies such as dark fiber infrastructure for dedicated scientific needs. Moreover it offers advanced services to universities, research institutes, and NRENs across Europe, such as cloud services, including data storage and processing, security

services, collaboration tools, and network services. Géant is aiming to support and advance research, education, and innovation, as well as ensure the communities' access to the most advanced network services and technologies, while facilitating global collaborations and scientific advancements.

Géant is actively involved in various EU projects, as their objectives align in advancing technology in the fields of networking, security, and collaboration, and it is either managing the projects in partnership with the European Commission (EC) in order to interconnect national research institutes with NRENs by procuring, designing, deploying, and managing large-scale international networks, or it participates in the research programmes to build new services in the field of trust and identity. Some notable projects include:

- GN5-IC1 [152] which is a sister project to GN5 and GN5-1, which aims to extend and secure Géant's global reach by upgrading intercontinental connectivity infrastructure,
- such as developing an interoperable Authentications and Authorisation Framework (AARC) [153],
- characterising the requirements for research and education in access and identity management (REFEDS) [154], and
- managing the development and expansion of eduGAIN [155].

Géant is working continuously on innovative projects to enhance the their targets in network, security, and services, very often collaborating with regional and global research networks.

In the case of Géant, SCION is an innovative project which its targets align with Géant's regarding communication security and continuous provision of networking and services, and could offer secure and reliable high-performance connectivity for the collaborative research projects across Europe, ensuring the data integrity and confidentiality, as well as greatly improve the reliability and performance of educational platforms and virtual classrooms, greatly improving the learning experience for a multitude of students in Europe. Moreover SCION's low latency and high bandwidth capabilities can heighten the performance of HPC applications running in Géant. Data-intensive tasks in many projects in the fields of particle physics and climate research, could benefit from SCION's efficient and secure data transmission.

Since November 24, 2022 Géant offers SCION connectivity for research institutions and universities. Interested parties, such as NRENs and associated universities, are shown how they can deploy SCION in their infrastructure to study path-aware networking, and QoS through bandwidth allocation, among other topics [156].

### 3.4.2 SCION in SWITCH

SWITCH [157], the NREN of Switzerland, established in 1987 by the Swiss Confederation, is responsible for the enabling, maintaining, and promoting secure connectivity and robust services to the public sector, research, and education institutions in Switzerland. Along with its providing services of LAN IP Access, Point-to-Point (P2P) connections, and Eduroam to professors, researchers, employees, and students, SWITCH already offers access services to the SCION LAN network [158], promoting security, reliability, and control in the academia's communications.

SWITCH has supported the development of SCION since 2015 at ETH Zürich, as it has evaluated the work done in SCION worthy of promoting and developing, seeing the potential of such a novel architecture and the steps already taken.

# 4 Why SCION?

When considering Next-Generation Network Architectures, factors such as provided security, flexibility, scalability, redundancy, resilience, robustness, user control, integration with IoT, 5G and existing infrastructure are crucial. SCION stands out, and that was our main consideration in choosing SCION for a deep study, and investment in resources and time. From the previously studied next-generation architectures, the differences in security focus is shown in Table 4.1 below, showcasing each architecture's approach regarding their core concepts, the provided control of their users to path selection, the layering model used and if it was altered from the traditional TCP/IP stack, core security aspects, level of resilience, and integration with emerging technologies.

Table 4.1 NIRA, RINA, Pathlets and SCION differences and approaches to security

| Aspects / Project | Core Concept | User Control | Layering Model | Security Focus | Resilience | Emerging Technologies |
|---|---|---|---|---|---|---|
| **NIRA** | User controlled routing paths | High | Traditional with user choice | Path control and flexibility | Multiple path options | Moderate |
| **RINA** | Recursive inter-process communication layers | Medium | Recursive IPC layers (DIFs) | Integrated security in all layers | Consistent security across layers | Adaptable to new technologies |
| **Pathlets** | Segment-based routing | High | Segment-based | Control over path segments | Fault tolerance with segments | Moderate |
| **SCION** | Network segmentation through ISDs | Medium | Segmented (ISDs) with hierarchical control | Cryptographic protection, and path transparency | Multipath communication, and compartmentalization | Integration with cryptographic protocols, scalable architecture |

A comparative table was constructed in order to summarize the adoption ratews of each next-generation network architecture, the key challenges they face or have faced, and the current use cases that are showcasing each project's potential. Table 4.2, and especially the current use cases column, is what urged us to follow SCION more closely and stay updated on its progress, aiming to study and understand the reasons behind its higher adoption rates. It is

evident that, despite the other architectures presented, and many others with similar core principles that were not covered here due to the scope of this document, SCION has an advantage that other before lacked. This is especially evident with its adoption in commercial applications, the Swiss Finance Network, and the present plans of its integration into Switzerland's critical infrastructure sectors.

Table 4.2 Comparison between next-generation network architectures of NIRA, RINA, Pathlets, and SCION

| **Project** | **Adoption Rates** | **Key Challenges** | **Current Use Cases** |
|---|---|---|---|
| NIRA | Low | • Infrastructure overhaul<br>• Compatibility issues<br>• Economic barriers | • Academic research<br>• Experimental projects |
| RINA | Low | • Paradigm shift<br>• Implementation complexity<br>• Standardization | • Academic research<br>• Pilot projects |
| Pathlets | Low | • Routing complexity<br>• Deployment barriers<br>• Scalability | • Research prototypes<br>• Academic studies |
| SCION | Growing | • Early-stage deployment<br>• Infrastructure integration<br>• Standardization | • Pilot deployments<br>• SCIONLab [159]<br>• Secure Swiss Finance Network (SSFN) via SIX, Switzerland's finance telecommunications provider [160]<br>• Commercial applications through Anapaya [161]<br>• Swiss critical infrastructure sectors (i.e. Health, power, telecommunications) [162]<br>• Anapaya EDGE provided by Amazon in the AWS Marketplace [163][164]<br>• Deployment in Geant offering SCION access connectivity to research institutions and universities [165]<br>• Deployment in Switzerland's NREN SWITCH [166]<br>• Deployment in several Swiss ISPs [167][168][169] |

SCION seems to have garnered significant attention, particularly in enhancing security and reliability, and is steadily moved beyond the close-knit cycles of academia, being incorporated and integrated

into commercial applications and critical infrastructure. It seems that for now it is mostly contained in Switzerland, but the results and efficiency of its deployment have already drawn the eye of big stakeholders like Amazon, and Cyberlink. In the continuation, we will delve into the new concepts introduced in the SCION protocol, the underlying architecture of SCION, how security is a built-in attribute of SCION's design, and how everything comes together in a SCION host.

## 4.1 The SCION Model and its Components

The SCION architecture model [170] introduces several novel concepts which are key components of the architecture to ensure multipathing, security between trusted domains, scalability, and efficiency. Isolation Domains, Beaconing, Trust Root Configurations (TRCs), and Path Control Beacons (PCBs), each component has a vital role in the model's overall offered functionality and security, and we are going to expand on those concepts in the following pages.

### 4.1.1 Isolation Domains

ISDs, as stated before, are autonomous regions within the SCION network that independently from a central authority can manage the security, routing policies and trust relationships that govern them from one another. Each ISD has several ASes members, which are divided into core ASes and non-core ASes, with the core ASes having a leadership role in the ISD, as they are being responsible for the path discovery, the propagation of learned paths, the routing processes within their ISD, and for propagating PCBs to other core and non-core ASes, thus facilitating the establishment of secure routes. Both core and non-core ASes within an ISD are operating under a common administrative domain, establishing a hierarchy within the ISD, which enables the scalable growth of the network without compromising the ISDs security mechanisms. Core ASes, non-core, and the processes of inter- and intra-routing are going to be explained in the continuation.

The segmentation of the overall network into multiple ISDs, and the independent growth of each ISD, enables SCION to scale more efficiently. The autonomy of ISDs allows for localized control and implementation of policies. Another advantage of the ISD component is is the containment of potential failures, misconfigurations and attacks within a limited segment, instead of the expansion and propagation of disruptions to other networks.

In general, ISDs allow for trust heterogeneity, as each ISD chooses their own roots of trust and provide for transparency in their trust relationships, as we will see later on in the chapter.

### 4.1.2 AS roles within SCION

All ASes within an ISD have a task of signing and verifying control messages within the ISD, but some ASes have additional roles and responsibilities. ASes are categorized into core ASes, non-core ASes, Certification Authorities (CAs), voting ASes, and authoritative ASes. In particular:

- Core ASes

  Core ASes have a leadership role in the ISD, as they are responsible for critical functions within the ISD, such as leading the path discovery and routing processes within their ISD, the propagation of PCBs to other ASes, both core and non-core, the establishment of secure routes, and the enforcement of security policies through TRCs. Core ASes are linked to other core ASes via core links either within the same ISD or to another, as shown in Figure 4.1, and each ISD explicitly states what its core ASes are in the TRC.

- Non-Core ASes

  Non-core ASes are simple ASes with no additional functions in the ISD besides handling their local routing and their communication and connectivity within the ISD. Unlike core ASes, non-core ASes do not participate in inter-ISD routing, and they are not responsible for managing the trust relationships and policies governing the ISD. They use path information that they received in PCBs provided by the core ASes, they rely on the trust framework and policies established by the core ASes through the TRCs, and they comply with the security policies and routing guidelines set by the core ASes.

- Certification Authorities

  CAs have the responsibility of issuing AS certificates to themselves (self-signed) and other ASes.

- Voting ASes

  Voting ASes are specific ASes within an ISD that hold the private keys required to sign TRCs and TRCs updates.

- Authoritative ASes

  Authoritative ASes are the ones that hold the latest TRCs of the ISD, and they are responsible for the beginning of the announcement of the TRC update.

### 4. 1. 3 Links

Between ISDs and within them, there are three types of links:

- The core links, that connect two core ASes, either from different ISDs, i.e. ISD-1 and ISD-2, or within the same ISD. Core links purpose is within business connections when the connections are offered in the type of provider-consumer or peering relationships.
- The parent-child links, that create the hierarchy within an ISD. Typically, parent-child links have a relationship of provider-consumer.
- The peering links, that connect ASes that have a peering relationship. Peering links can be established between any two ASes, either core or non-core, and they can cross ISD boundaries, connecting two ASes from different ISDs.

An overview of such links can be viewed in Figure 4.1 below, where core links are depicted with dashed, blue lines, parent-child links with dashed black lines and arrow heads on either end, and peering links are drawn with black lines and arrows on either end.

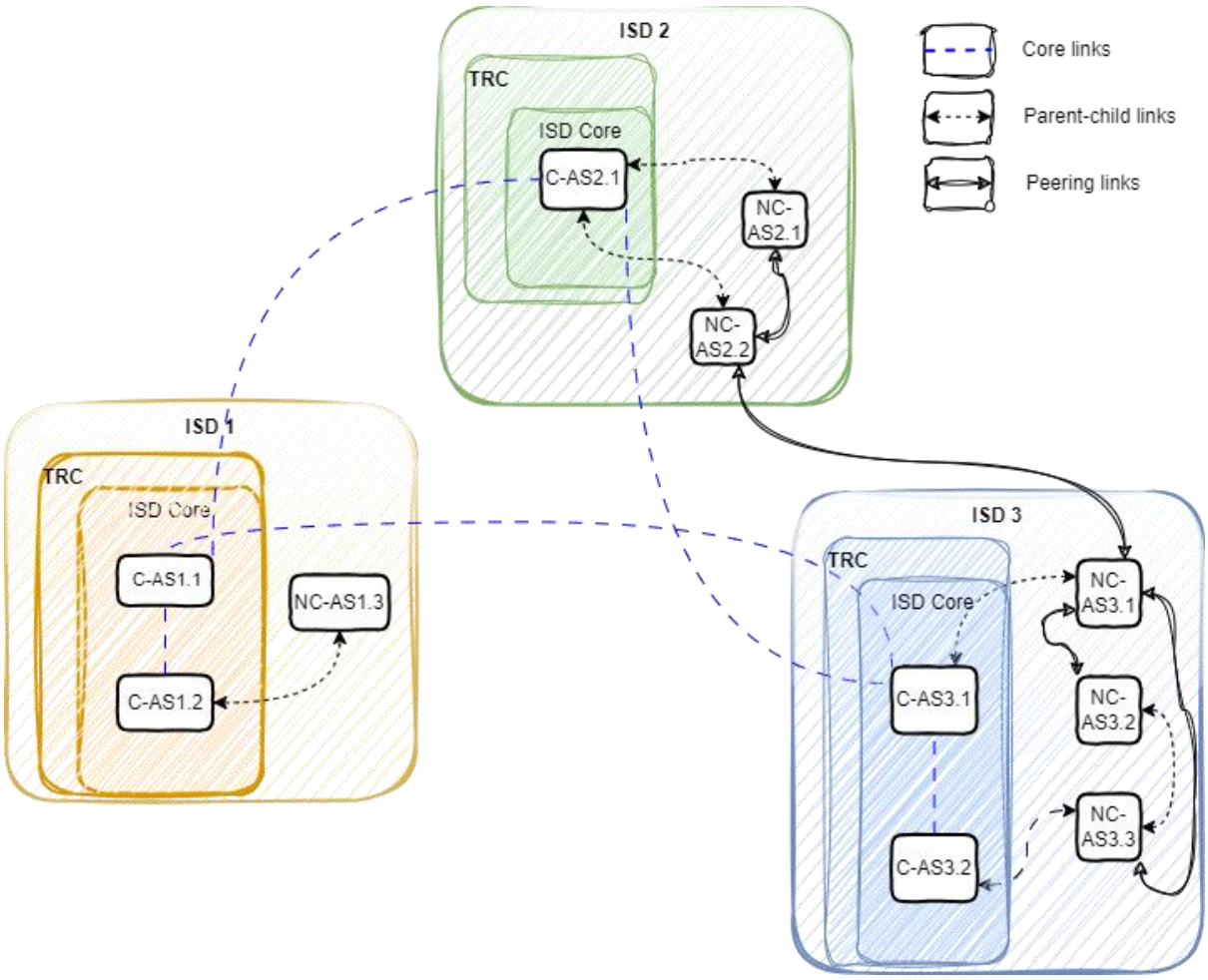


Figure 4.1 Overview of links between ASes in 3 different ISDs

### 4.1.4 Beaconing and Path Control Beacons

Beaconing is the process of path exploration, where an AS discovers paths for other ASes. Each AS's control service is responsible for the beaconing process, which occurs in regular intervals and can generate, retrieve, and propagate Path-segment Construction Beacons (PCBs) to construct path segments. The PCBs contain information about the topology and authentication used, and can include metadata to further help in path management and selection. The beaconing process is further divided into two routing processes that run on two different levels; the inter-ISD and intra-ISD. The inter-ISD, or core beaconing process, is a periodic process responsible for the construction of path segments between core ASes, regardless of their ISD. During core beaconing, PCBs are either initiated in the core AS or propagated to be received from the core AS's neighbours, and they travel through policy-compliant paths as a means to discover all the possible paths between any pair of ASes. The intra-ISD beaconing is the process responsible for the creation of path segments from core ASes to non-core ASes.

There are three types of path segments an AS can learn in SCION:

- an up-segment, a segment from a non-core to the core AS,
- a down-segment, a segment from the core to a non-core AS, and
- a core-segment, which is a path segment between two core ASes.

Path segments are bidirectional, so up-segments and down-segments are invertible.

PCBs are created in the core AS's control service and sent to the non-core child ASes, where the control service of the child AS receives them and then forwards them to their own child AS. The procedure concludes when the PCB reaches an AS that has no child of their own. In that way, the ASes of an ISD receive the path segments needed to reach the core AS of the ISD, making all possible paths known. As a PCB travels through the network of an ISD, it gathers cryptographically protected path and forwarding information from each AS it traverses. At each AS, metadata and information about the AS's ingress and egress interfaces with specific and unique IDs are added to the PCB, with the IDs uniquely identifying the connections to the neighbouring ASes. These IDs need to be unique only in the same ISD, and are irrelevant to other ISDs' ingress and egress interface IDs, thus enabling the autonomous governance of each ISD from one another, as no coordination between them is needed for the configuration of the IDs. Each AS is able to independently set the policies best suited to it to determine which PCBs are going to be propagated, the time of the propagation, and to which neighbours. The selection process is based on several properties about the paths, such as the length of the path, and PCB, such as the PCB's age or remaining TTL. Then, when the selection is complete,

the control service of the AS can determine the quality of each candidate PCB based on their path and PCB properties and conclude which one is the best to be used for the beaconing and eventual construction of the end-to-end paths.

Furthermore, SCION supports shortcuts and peering links, where shortcuts are simple paths containing an up-path and a down-path only, with a non-core AS common to both segments, and peering links which are used to be added to an up or down-path segment and eventually resemble an operation similar to how the traditional Internet works.

### 4.1.5 Control Plane Public Key Infrastructure and Trust Root Configuration

The Control Plane Public Key Infrastructure (CP-PKI) is the PKI upon which SCION's control plane relies for the authentication of messages, and which is organized in the level of the ISD. CP-PKI is a set of policies, roles and processes that are used for the management of TRCs and certificates, which bind the name and public key explicitly as well as sign the public key, thus proving the ownership of the corresponding private key.

TRCs are cryptographic structures within SCION that establish and manage the trust within and between ISDs. TRCs are essential for ensuring the authenticity, integrity, and security within an ISD and in extend the communications across the SCION network. Key functions of TRCs include the authentication of an ISD's borders and the entities within the ISD (core and non-core ASes), the verification of the ISD's members' identities and permissions, the integrity of path information by providing cryptographic verification, and the verification of the integrity of the data transmitted. TRCs also manage and distribute cryptographic keys used to sign and verify messages within SCION, and they allow for the dynamic update of trust relationships and cryptographic keys, thus enabling an adaptable network environment that is resilient to threats and changes. TRCs are responsible for the ISD policies, that specify the TRC's usage, validity period, and updates, and their enforcement for the intra-routing, as well as for the policies that characterize the inter-routing communications, thus maintaining consistent and secure trust across SCION. In addition to the establishment of trust and enforcement of policies, TRCs are the entities that are responsible for the verification of the paths' authenticity and integrity during the path discovery process, for the path segments that are advertised by PCBs, and for the validation of the paths, ensuring that all path segments are secure and trusted.

Trust roots and policies are encoded in the TRC, which in turn has a version number, a list of public keys that serve as trust roots, and the policies governing the amount of signatures needed for performing different actions. In that way, all authentication is initiated and managed by the TRC. The signed root certificates of the TRC are used to sign the CA certificates, which in turn are used to sign each AS's certificate within the ISD. TRC updates occur either periodically as a means to re-issue the

TRC and maintain the entities and policies listed within the TRC unchanged, where in this case they are called regular TRC updates, or as means to modify critical details of the TRC, such as updating the list of core ASes of the ISD, where they are called sensitive TRC updates.

The TRC is a crucial and fundamental component of the ISD and the ISD's CP-PKI. The base TRC entity serves as the ISD's trust anchor and is thus inherently trust by all ASes within the ISD. The base TRC is signed by voting ASes, and then it gets distributed across the ISD. All ASes within the ISD must be pre-loaded with the currently valid base TRC of the ISD.

## 4.2 SCION Router Architecture

The underlying architecture of a SCION enabled router showcases the changes made in the already established concepts of data plane, control plane, and routing, and how a packet header evolves to accommodate the differences SCION proposes in networking communications.

### 4.2.1 Data Plane

As we've seen, the data plane in traditional networking is responsible only for the quick forwarding of the packets it receives to the next destination. In SCION the way packets are transmitted, routed, and authenticated had to be rethought and eventually changed the data plane accordingly to accommodate security mechanisms, path transparency, and path selection, as the data plane is seen as the appropriate plane to establish such mechanisms. SCION uses path-specific forwarding, where each packet contains a list of forwarding instructions for each hop, and only the border router at the packet's destination needs to examine the packet's header to forward it to the right local host [170].

Addressing various limitations of the traditional data plane, associated with the TCP/IP stack, SCION designs a data plane able to incorporate explicit path control. This fundamental change of data plane's approach to path control and packet forwarding, allows users to define the exact paths their data will take through the network. With the theory behind this approach being grounded on path-aware networking, path information is being embedded within the packet's header, source-controlled routing is enabled, and the end systems are able to select paths based on their desired criteria, such as latency, bandwidth, and/or security [170].

As it will be shown in chapter 4.2.3 and Figure 4.3, packets in SCION carry detailed information, including a sequence of forwarding instructions, specifying the exact sequence of ASes and the interfaces the packet must traverse. By embedding the path within the packet's header, the reliance on intermediate routers is reduced, and the ability to make independent forwarding decisions is

minimized, thus the risk of route hijacking is diminished, improving on path predictability and transparency.

Cryptographic path validation is performed in SCION's data plane, with each segment of the path being authenticated using cryptographic methods that will be discussed in chapter 4.3.4,ensuring that the path information cannot be tampered with by malicious actors. With this approach, unauthorized modifications to the routing paths, a commonality in BGP-based routing systems, is prevented, thus enhancing the security of the data plane. The cryptographic validation of the paths, not only secures the path information, but also ensures the integrity and authenticity of the data being transmitted, in that way providing end-to-end security of the path [171].

With multipath communication in the data plane, SCION allows data to be transmitted simultaneously over multiple paths, improving on fault tolerance, load balancing, and network utilization, which is crucial in scenarios where high availability of services and reliability of the network are critical, i.e. in financial transactions. With multipath enabled, the communication is secured that even if a path fails for whatever reason, the data can still reach their destination via alternative routes, maintaining the continuity of the transmission.

With the theoretical model of SCION introducing the concept of ISDs, SCION's data plane also includes the use of ISDs. The segmentation ISDs achieve by compartmentalizing the network into smaller, more manageable segments, the overall security and scalability of the network is heightened, as ISDs limit the impact of security breaches to domains and simplify the management of routing information.

The comparative analysis of SCION and traditional TCP/IP networks reveals several advantages of the SCION data plane. Traditional networks, with their destination-based routing and reliance on BGP, are prone to various attacks and inefficiencies. SCION's explicit path control, cryptographic validation, and multipath capabilities address these vulnerabilities, providing a more robust and resilient networking environment.

### 4.2.2 Control Plane

In the SCION architecture, the control plane is reconstructed to be more secure and efficient in its routing, using ISDs and Beaconing. As it has already been stated previously, ISDs segment the network into independently managed units. Each ISD operates under its own TRC which governs the cryptographic keys and security policies within that ISD. The cryptographic authentication of each path segment and control message ensures their authenticity and integrity, preventing unauthorized modification of routing entries, a common vulnerability in BGP-based environments. This approach

limits the impact of a potential compromise to a single ISD, and improves on the scalability by reducing the complexity of global routing tables.

Beaconing is a key process happening in the control plane. It is an asynchronous process responsible for the creation and dissemination of path segments within the ISD. It involves the transmission from ISD core routers to edge routers of PCBs which contain authenticated path information that the routers use to build and maintain their routing infrastructure, ensuring fault tolerance and load balancing. Beaconing allows core ASes to learn paths to other ASes through inter-domain beaconing, whereas intra-domain beaconing enables non-core ASes to learn the paths to the core ASes, thus enabling the communication between non-core ASes and the ISD core ASes.

Except from path exploration, registration, and lookup happening in the control plane in SCION, the control plane is also enabled with functions for secure path withdrawal and control messages [170], to secure that link failures will be automatically resolved and handled by the network itself. Link failures in SCION can go unnoticed by the end user, as the construction of a new path can happen promptly by a three-part process which utilizes beaconing every few seconds, the SCION control message protocol (SCMP), and the default multipath communication at the SCION end-hosts.

The control plane in SCION is enabled with hierarchical path construction, where within each ISD the paths are constructed by starting from the core and extending to the edges. This approach simplifies path management and reduces the overhead created by having to keep up with and maintain large routing tables, thus enhancing the overall efficiency of path discovery and maintenance [175]. Furthermore, with multipathing in the control plane the reliability and performance of the network is enhanced, providing redundancy and enabling load balancing, as with SCION same traffic coming from a source and travelling to a destination can be configured to simultaneously traverse two different paths, a notion impossible in BGP [176].

### 4.2.3 SCION Header

As seen in Figure 4.3 [20], the classic IP packet header does not contain any information on the path it will take to traverse from its source to the destination, and only the information of the sender and the receiver's IP addresses are recorded. A traditional packet header has the following fields:

- Version, which is 4 bits in length, and indicates the version of the IP protocol used, and can be 4 to indicate IPv4 or 6 to indicate IPv6.
- Internet Header Length (IHL), with a size of 4 bits it indicates the length of the IP header. The smallest value it can hold is 5.
- Type of Service (ToS), 8 bits of size specifies the QoS desired and priority.

- Total Length, 16 bits of size, which specifies the total length of the packet, including its header and data, and it ranges from 20 to 65,535 bytes.

- Identification, with a size of 16 bits, it is a unique, identifying value to each packet, set by the sender in order to help in the reassembling the fragments of the original packet to their correct order.

- Flags, with a size of 3 bits, this field help in the control of a packet's fragmentation. It has three possible values; 0 for reserved, DF for Don't Fragment, and MF for More Fragments.

- Fragment Offset, which with a size of 13 bits indicates the relevant position of a fragment in the original packet. It is measured in 8 bytes.

- Time to Live (TTL), which has a size of 8 bits and it the field responsible for determining the packet's lifespan by decrementing at each router it passes. When a packet's TTL reaches zero and is still in transmit, the packet is discarded.

- Protocol, with 8 bits in size, it indicates the next level protocol used in the data portion of the packet and the value it takes is according with the assigned numbers described in RFC 790 [172][173]. For example, the protocol value could be 6 if the next level protocol is TCP, 17 for UDP, or 88 for IGRP [174].

- Header Checksum, 16 bits of size, provides error-checking for the header to ensure the data's integrity.

- Source Address, 32 bits, is populated with the IP of the sender.

- Destination Address, 32 bits in size also, indicates the IP address of the receiver.

- Options, up to 320 bits in size, it is an optional and variable field for additional features, such as security, route tracing, timestamps, or other features. The presence of Options extends the header beyond it standard 20 bytes.

- Padding, it is also an optional field, its size depending on the presence of the Options field. Padding field is only populated accordingly to the Options field to ensure that the packet header will end on a 32-bit boundary. Padding bytes are added to align the total header length to a multiple of 4 bytes.

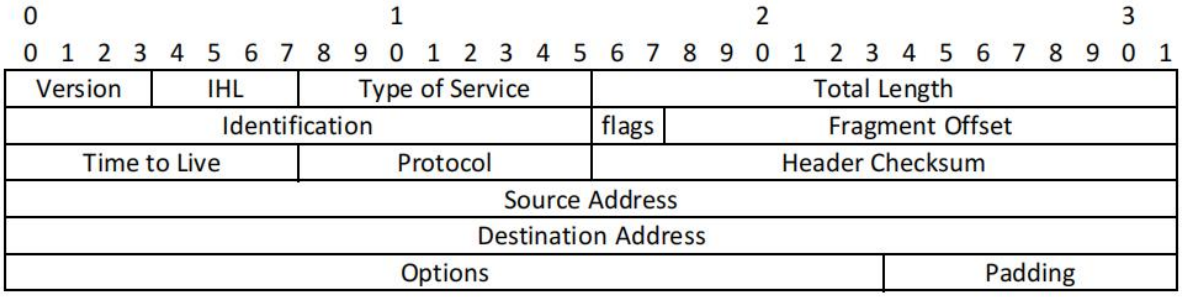


Figure 4.2 TCP/IP IPv4 packet header format

The changes that were made to the traditional format of the IP packet header to accommodate SCION, eventually becoming the SCION header, so that the packet can traverse a SCION network can be seen in Figure 4.4 below.

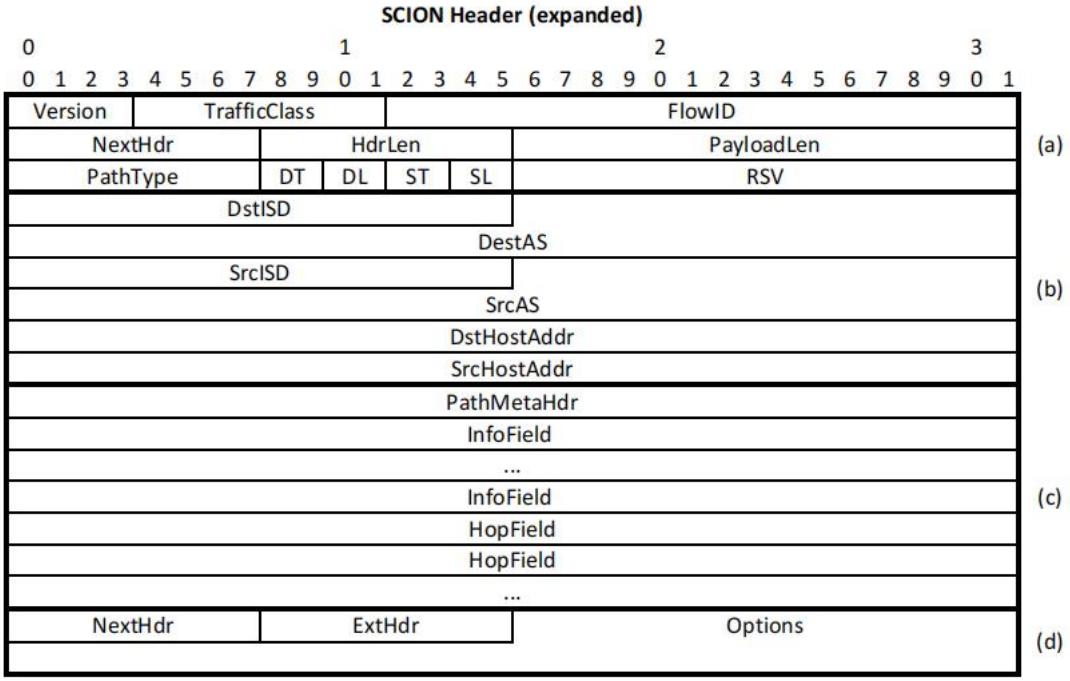


Figure 4.3 SCION header containing (a) the common header, (b) the address header, (c) the path header, and (d) an optional expansion header

The SCION header consists of 4 segments:

(a) The common header, which contains important information such as the version of SCION used (currently only 0 is available), traffic class, the flow identification, the encoding of the first header after the SCION header, the lengths of the header and the payload, the type of the SCION path which are shown in Table 4.3, as well as fields to define the endpoint address type and length for the source and destination endpoints.

(b) The address header, which contains information about the ISD, AS and the endpoints of both source and destination, and which supports variable lengths and types, and can be set accordingly with the flags used in the common header.

(c) The path header, which contains the full AS forwarding path, with its format specified in the PathType field in the common header, as it will be shown in the continuation where the different fields are going to be briefly explained.

(d) And finally an optional extension header that contains a variable number of options to be used between hops or between endpoints. [177] [178]

In particular, the SCION header contains the below information:

- Version, the indicator of the version of the SCION header, currently the only supported version is 0.
- TrafficClass, which is the value of the Traffic Class in bits as they are specified in RFC 2474 and RFC 3168.
- FlowID, which is a mandatory field and is used to label sequences of the packets to indicate that they must be treated as a single flow by the source.
- NextHdr, which encodes the type of the first header after the SCION header.
- HdrLen, indicator of the length of the SCION header.
- PayloadLen, which is the length of the payload in bytes.
- PathType, which specifies the type of the SCION path and can be up to 256 different types. The proposed SCION path types are shown in Table 4.3 and are the Empty type, SCION, OneHopPath, EPIC, and COLIBRI.
- DT/DL/ST/SL, which encode the host type and host length for the destination and source host addresses.
- RSV, which is a field reserved for future use.
- DstISD, the identifier for the destination ISD.
- DestAS, the identifier for the destination AS.
- SrcISD, the identifier for the source ISD.
- SrcAS, the identifier for the source AS.
- DstHostAddr, which is the destination host's address, its type and length are given with DT and DL.
- SrcHostAddr, which is the source host's address, its type and length are given with ST and SL.
- PathMetaHdr, which is a 4 byte field that contains information about the SCION path.
- InfoField, which contains information such as a flag to indicate if the forwarding path is built as a peering path, flag to indicate that the hope fields are arranged as they were constructed during the process of beaconing, timestamps, etc.
- HopField, which includes information such as the expiration time of the hop field, the ingress and egress interface IDs, and a Message Authentication Code (MAC).

Table 4.3 Possible values of PathType field

| **Value** | **Path Type** |
|---|---|
| 0 | Empty path |
| 1 | SCION path |

| Value | Path Type |
|---|---|
| 2 | One-hop path |
| 3 | EPIC path [179] |
| 4 | COLIBRI path [180] |

### 4.2.4 Routing in SCION

In SCION routing and forwarding of the packets to the appropriate destinations becomes excitingly more efficient, as routing tables and matches of longest prefix are absent in the architecture, enabling a router to simply access the NextHop field of the packet's header. SCION uses two types of routing; inter-domain and intra-domain routing. Both types of routing utilize PCBs for the exploration of the network. The routing process in SCION happens as PCBs are initiated in the core ASes, and the beaconing process begins as they are being propagated to the network by being disseminated within the ISD as a policy constrained multipath flood to explore the internal paths of the ISD, or among core ASes to explore the core paths which potentially span across different ISDs. As PCBs accumulate cryptographically protected path information, they also gather forwarding information in the form of hop fields (HF) and metadata about the links and the traversed ASes. The hop fields are subsequently used by the end hosts to create end-to-end forwarding paths. In that way, packets contain AS-level path information making the need for border routers to keep inter-domain routing tables obsolete, and in SCION is referred to as packet-carried forwarding state (PCFS).

Important steps during the acquisition process of the forwarding paths, are as follows:

- Path exploration, where ASes discover the paths connecting them with other ASes.
- Path registration, which allows ASes to change some PCBs into path segments and register them into their path infrastructure, thus making them available to other ASes too.
- Path resolution, which allows end hosts to create end-to-end paths to a destination. Path resolution, also consists of two steps:
  - The path lookup step, which is when the end host obtain the path segments, and
  - the path combination step, which is when the path segments are combined into a forwarding path.

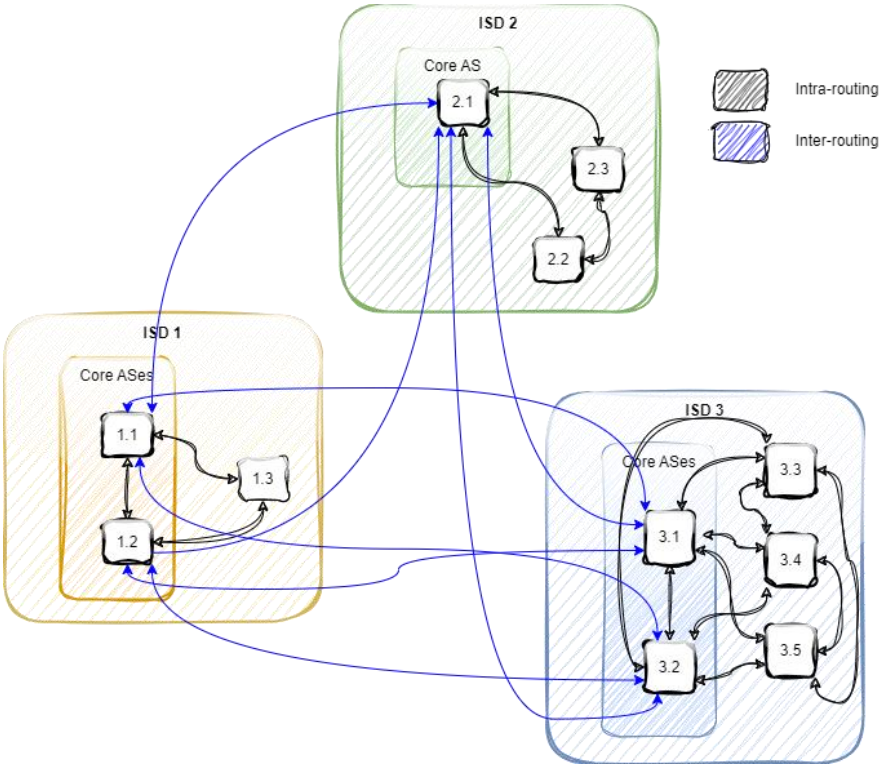


Figure 4.4 Simplified view of ISDs, their inter-routing (blue) and intra-routing (black)

## 4.3 Security

Security is a fundamental part of SCION and one of the main reasons of its creation. In the continuation authentication mechanisms, the usage of certificates in the TRC, PKIs in the control plane, name resolution and in the end hosts, as well as cryptographic algorithms used are going to be studied.

### 4.3.1 Authentication Mechanisms

Authentication is integral to SCION networks, ensuring data integrity, authenticity and trust across the network. SCION employs a variety of authentication mechanisms to achieve those targets, such as hierarchical PKI for the authentication of path segments, where each AS has its own unique pair of private and public keys and they use their private key to sign control messages and path segments, while the public key is distributed for utilization by the others for verification of the signatures. This process ensures that path segments are authenticated at each step, preventing tampering. It also employs end-to-end and hop-by-hop authentication, dynamic certificate revocation, and secure control messaging, ensuring that only legitimate entities can participate and that data integrity is maintained throughout the communication process. End-to-end authentication processes, where the received data

packets are authenticated that they have not been tampered with during their transit. This is achieved with the utilization of cryptographic tokens and Message Authentication Codes (MACs), which are generated by the usage of shared symmetric keys between neighbouring ASes, ensuring that each hop in the network path can verify the authenticity of the data received, thus maintaining a secure and trusted environment. The certificate revocation mechanisms to manage the validity of AS certificates allow all ASes to verify the current status of certificates and prevent compromised entities from participating. If a key is compromised or trust is lost, certificates can be rapidly revoked and added to a Certificate Revocation List (CRL), which is then distributed across the network. Moreover, SCION Control Messages (SCMP) are authenticated to secure control plane communications. These messages are used for critical functions such as path establishment and maintenance, and their authentication prevents spoofing and ensures message integrity, protecting the network from malicious disruptions.

### 4.3.2 Certificates

Certificates and TRCs in SCION are crucial for the authentication of ASes and the trust relationships and policies across the network. Each AS is issued a certificate that contains its public key, identity information, and other relevant data. These certificates are part of a hierarchical PKI, which establishes a chain of trust within the network. When an AS sends a message or signs a path segment, other ASes can verify its authenticity by checking the certificate against this hierarchy.

TRC files are used in SCION to manage and distribute trust information across the network. TRCs contain the root certificates and policy information that define the trust relationships within a specific ISD. They are periodically updated and distributed to all ASes in the ISD to ensure that each AS has the latest trust information. Verification of TRCs is crucial for maintaining the network's security, as it allows ASes to confirm the validity of the root certificates and the trust policies in place. When an AS receives a new TRC, it checks the signatures and the version number to ensure that the TRC is legitimate and has not been tampered with.

### 4.3.3 PKI

The hierarchical PKI system is designed to manage cryptographic keys and certificates across various levels of the network architecture, ensuring that all entities can reliably verify each other's identities and the integrity of the data they exchange. PKIs exist in the Control Plane, in name resolution and the end entity. In the control plane, they authenticate path segments and control messages, ensuring the integrity and authenticity of network paths. In name resolution, they secure the mappings between names and addresses, and for end entities, they provide robust authentication, preventing unauthorized access and ensuring secure communications. The hierarchical structure of SCION's PKI system

ensures the scalability, as well as the efficient certificate management, and a reliable chain of trust across the entire network.

In particular, as the control plane in SCION is responsible for the establishment, maintenance, and management of network paths, PKIs play a critical role in the authentication of path segments and control messages. Each AS in SCION has a unique key pair, and when an AS signs a path segment, this signature is verified by the receiving AS, thus ensuring the path's integrity and authenticity as only legitimate ASes can contribute to the path setup process. The hierarchical nature of the PKI ensures scalability and trustworthiness, as each AS can verify signatures based on a chain of trust extending back to a root certificate authority.

In name resolution SCION relies on secure and trustworthy mapping between human-readable names and network addresses. PKIs ensure the integrity and authenticity of this mapping process. When a name resolution request is made, the response, which includes the resolved address, is signed by the authoritative entity. This signature is verified using the corresponding public key, ensuring that the response has not been tampered with and is from a legitimate source. The hierarchical PKI structure allows for the delegation of authority, where higher-level authorities can delegate name resolution responsibilities to lower-level entities, each securely authenticated and verified within the PKI framework. This process ensures that end-users can trust the name resolution responses they receive, critical for the reliability of services that depend on accurate and secure name-to-address mappings.

For end entity authentication, PKIs in SCION provide a robust mechanism for ensuring that only authorized devices and users can access network resources. End entities, such as user devices and servers, are issued certificates that include their public keys and identity information. These certificates are signed by a trusted CA within the SCION PKI hierarchy, so when an end entity attempts to communicate or access a resource, its certificate is presented and verified by the receiving party. This verification process involves checking the certificate's signature, validity period, and revocation status. Here, the hierarchical PKI structure allows for efficient management of the certificates, including the ability to revoke them swiftly if an end-entity is compromised.

### 4.3.4 Cryptographic Algorithms

SCION uses cryptography for authentication and not encryption. In that way, vulnerabilities or malicious usage of a cryptographic algorithm used for the authentication does not directly leak data or compromise the trust of previously shared protected data. When efficiency is not the primary focus of a protocol, multiple cryptographic algorithms can be used at the same time to authenticate data. In that way, if in the chain of cryptographic algorithms used, one still remains secure while the others have

been compromised, the AS certificates and control plane messages still remain protected and secured [170].

SCION uses both symmetric and asymmetric cryptography. Symmetric cryptography is used to generate and extract keys, and enable fast authentication of data, whereas asymmetric cryptography is used in digital signatures for the certification of the binding between a key and a name or identifier, for the authentication of information contained within control plane messages, or for the key establishment to security protocols such as TLS.

## 4.4 Parts of a SCION Host

A SCION host consists of several components, such as the SCION Dispatcher, SCION Daemon, TCP/SCION, and SCION Stream Protocol (SSP). Each component has a unique role in the overall functionality and performance of the SCION network. In general, each component is contributing to the host's functionality and performance within the SCION network. The SCION Dispatcher manages packet flow and ensures that data reaches the correct endpoint within the host, while the SCION Daemon handles control plane operations, path discovery, and routing table management, ensuring secure and efficient path selection. TCP/SCION adapts the traditional TCP protocol to leverage SCION's path-aware capabilities, providing reliable and secure communication, and SSP offers a modern transport layer solution, utilizing multiple paths for enhanced performance, security, and reliability.

### 4.4.1 SCION Dispatcher

The central component of the SCION host is the Dispatcher, which is a single process that handles all SCION packets on the designated UDP port. It receives incoming packets and delivers them to the appropriate SCION applications, that have already registered their desired ports to receive or send traffic. The Dispatcher maintains a table of all registrations used for lookups.

The SCION Dispatcher acts as a central communication hub within the SCION host, with its primary function being to manage incoming and outgoing packets between the host and the SCION network. When a packet arrives, the SCION Dispatcher determines the appropriate process or application to forward the packet to, based on the destination address and port. It handles the demultiplexing of packets, ensuring that data reaches the correct endpoint. The Dispatcher also plays a crucial role in encapsulating and decapsulating packets, adding or removing SCION-specific headers as necessary. This component is vital for maintaining the flow of data within the host and ensuring seamless integration with the SCION network infrastructure.

In addition, the Dispatcher also handles some SCMP tasks, such as when an SCMP packet is received for a local application, then the Dispatcher will check on the registration table on information to deliver it, and when an SCMP packet is received for a local host, then the Dispatcher will process the packet, deliver it, and if needed reply to the sender.

### 4.4.2 SCION Daemon

The SCION Daemon is responsible for managing the control plane operations of a SCION host. It handles tasks such as path discovery, path verification, and routing table updates. The Daemon communicates with other SCION Daemons across the network to exchange control messages and maintain an up-to-date view of the network topology. It ensures that the host can find and verify valid paths to destination addresses, leveraging SCION's path-aware networking capabilities. The SCION Daemon also manages the security aspects of path selection, ensuring that only authenticated and authorized paths are used for data transmission.

The Daemon is a background process that runs on the end hosts of a SCION network, handling control messages and offering an API to interact with the SCION control plane. The daemon is responsible for the services of path lookup, topology information, and extensions. In particular, it provides path lookup functionality for the end hosts, topology information of the local AS including the addresses of the border routers and on running servers, and extensions such as COLIBRI and EPIC.

### 4.4.3 TCP/SCION

TCP/SCION is an adaptation of the traditional Transmission Control Protocol (TCP) designed to operate over the SCION network. It provides reliable, connection-oriented communication between hosts, leveraging SCION's enhanced path control and security features. TCP/SCION ensures that data packets are delivered in order, without loss or duplication, and that network congestion is managed effectively. By integrating with SCION's path-aware capabilities, TCP/SCION can take advantage of multiple paths for data transmission, improving redundancy and fault tolerance. This multi-path capability allows TCP/SCION to dynamically distribute traffic across different paths, improving redundancy, load balancing, and fault tolerance. In the event of path failure or congestion, TCP/SCION can seamlessly switch to alternative paths without interrupting the connection, ensuring continuous and reliable data flow. This protocol adaptation maintains compatibility with existing TCP-based applications while enhancing their performance and security within the SCION environment. Additionally, TCP/SCION enhances security by incorporating SCION's authentication mechanisms, as each path segment used by TCP/SCION is authenticated, ensuring that the data packets follow verified routes and unauthorized entities are prevented from intercepting or tampering

with the data. This is particularly important for maintaining data integrity and confidentiality in scenarios where security is paramount. Furthermore, TCP/SCION maintains compatibility with existing TCP-based applications, allowing them to benefit from SCION's advanced features without requiring significant modifications. Performance-wise, TCP/SCION offers improved congestion management and data throughput. By leveraging multiple paths and SCION's efficient routing, TCP/SCION can optimize data flow, reduce latency, and enhance overall network performance. These improvements are particularly beneficial in high-demand environments such as data centers, cloud services, and real-time applications where network efficiency and reliability are critical.

### 4. 4. 4 SCION Stream Protocol – SSP

The SCION Stream Protocol (SSP) is a transport layer protocol specifically designed for the SCION network. SSP is built to address the limitations of traditional transport protocols like TCP and UDP, particularly in terms of security, reliability, and efficiency. One of the core features of SSP is its ability to utilize multiple paths for data transmission, allowing for better load balancing and fault tolerance. SSP provides secure and reliable stream-oriented communication, ensuring that data integrity and confidentiality are maintained throughout the transmission process. The protocol supports features such as congestion control, flow control, and retransmission of lost packets, making it a robust solution for modern network communication needs. SSP's integration with SCION's path-aware architecture enables it to dynamically adapt to network conditions and optimize performance. This multi-path capability enables SSP to dynamically balance load and improve fault tolerance by distributing traffic across various available paths. If one path experiences congestion or failure, SSP can seamlessly switch to an alternative path, maintaining uninterrupted data flow and enhancing overall reliability. Security is a core component of SSP, as it incorporates cryptographic mechanisms to ensure data integrity and confidentiality. Each data packet transmitted via SSP is authenticated and encrypted, preventing unauthorized access and tampering. This high level of security is particularly beneficial for sensitive applications that require strong data protection. Moreover, SSP's use of multiple paths for data transmission improves performance and mitigates the risk of single points of failure or targeted attacks, further enhancing the security posture of the communication. Performance-wise, SSP is designed to optimize network efficiency by minimizing latency and maximizing throughput, as it includes advanced congestion control and flow control mechanisms that can adapt to real-time network conditions, ensuring smooth and efficient data transfer, making SSP particularly suitable for high-performance applications, such as real-time video streaming, online gaming, and large-scale data transfers, where consistent and high-speed communication is critical

# 5 Deployment Approaches

Deployment approaches in SCION focus on integrating its advanced network architecture within existing and new network infrastructures. SCION offers a flexible and modular design, allowing it to be deployed incrementally or comprehensively, depending on organizational needs and resources. This adaptability is crucial for facilitating the transition from traditional Internet architectures to the SCION framework.

There are several strategies for deploying SCION, each catering to different network environments and operational requirements. These strategies include partial deployment within existing ISPs and enterprise networks, full deployment in greenfield environments, and hybrid approaches that leverage both SCION and legacy protocols. Additionally, SCION can be deployed using virtualised environments and SDN technologies to enhance scalability and manageability. Partial deployment approaches enable organizations to gradually adopt SCION, integrating its security and path control features into specific segments of their network without a complete overhaul. This can involve deploying SCION routers and border gateways alongside existing infrastructure, allowing seamless interoperability between SCION and traditional IP networks. Full deployment approaches, on the other hand, involve building an entirely new network infrastructure based on SCION principles, which is particularly suitable for new network projects or large-scale upgrades. Hybrid deployment approaches combine elements of both partial and full deployments, enabling organizations to leverage SCION's benefits while maintaining compatibility with existing systems, which can involve using SCION for critical applications requiring high security and performance, while continuing to use traditional protocols for other services. Virtualization and SDN based deployment approaches provide additional flexibility and scalability, allowing SCION to be implemented in dynamic and programmable network environments, which in turn enable rapid provisioning and management of SCION infrastructure, facilitating efficient resource allocation and network optimization.

The diverse deployment approaches available for SCION cater to a wide range of network environments and organizational needs, ensuring that the transition to SCION architecture can be tailored to specific requirements and constraints.

## 5.1 SCION IP Gateway & SCION Gateway Routing Protocol

The SCION-IP Gateway (SIG) enables interoperability between traditional IP end hosts and SCION enabled ones to benefit from the SCION network. Every SCION AS that wants to provide traditional IP connectivity between SCION and IP hosts, deploys a SIG service. Providing proper interoperability requires traditional IP connectivity to be transparently supported, meaning that traffic routing must be

fully supported between two legacy IP hosts, one in a regular non-SCION AS and one in a SCION AS, as well as for traffic between two regular IP hosts that reside in SCION ASes. In that way, the same rules in routing apply regarding public and private IP ranges, as hosts in SCION ASes that wish to be reachable by legacy hosts in other ASes must have public IP addresses. The SIG service is responsible for handling the routing, encapsulation and decaplsulation of IP traffic within the AS and between SCION ASes.

The SCION Gateway Routing Protocol (SGRP) enables SIGs to discover and announce IP prefixes directly from remote SIGs, as each SIG is configured with a prefix policy than contains the IP prefixes that were announced or learned. In that case, SIGs can use a dynamic routing protocol as BGP to learn or advertise the prefixes.

## 5.2 ISP

The deployment of SCION within an ISP's core network involves several critical steps taking into consideration the criticality of an ISP's infrastructure. When integrating SCION into an ISP's core network, the process typically begins with the establishment of SCION border routers (SBRs) at key network junctions. These routers facilitate the communication between SCION and legacy IP networks, ensuring compatibility and the smoothness of the transition, and they can be standard COTS servers. The ISP must also deploy SCION control plane servers (CS) and path servers (PS) that manage the routing and forwarding tables within the SCION architecture. These servers are responsible for path computation, ensuring that data packets follow the most efficient and secure routes through the network. The deployment process involves significant coordination with other ISPs and SCION-enabled networks to establish inter-domain links. ISPs also need to update their network management and monitoring systems to support SCION's architecture, ensuring real-time visibility and control over the network. Deploying SCION within an ISP's core network necessitates thorough testing and validation to ensure all components function seamlessly. The transition plan might include running SCION in parallel with existing protocols to minimize disruptions, and even then partially SCION-enabled ISPs should be able communicate with others without a problem. By implementing and leveraging SCION's path-aware networking, advanced routing and security features, ISPs gain granular control over traffic flows, which enhances performance and mitigates the risks of network attacks such as hijacking or DDoS attacks, and they can offer enhanced service quality, reliability, and security to their customers, addressing many of the inherent weaknesses of the traditional internet infrastructure.

It is important that existing internal IP or MPLS connections within the ISP can be reused within SCION for the communication within the AS, and if dedicated links are or become unavailable queuing disciplines on internal switches can provide separation of the IP and SCION traffic.

### 5.3 Customer Deployment

A customer can use SCION either natively or as transparent IP-to-SCION conversion [170]. In the first case, the customer can benefit from the full range of SCION as SCION becomes available to their applications and the applications become SCION-aware. In the latter, SIG is being utilized as a fast approach. A customer's SCION network deployment can either constitute an independent SCION AS or it can leverage the provider's AS, which has the advantage of not owning and maintaining an AS and its infrastructure. The required certificates for the SCION AS are issued by the core ASes and AS numbers are assigned either in accordance with their previous AS number or they are freshly allocated from a 48-bit space of SCION's AS numbers.

### 5.4 End domain

An end entity can easily deploy SCION, as they are seen as an integral part for the broad adoption of SCION. In that way, end hosts within an AS that already has adopted SCION as a network and security solution, can easily bootstrap the automated process of becoming a SCION-enabled end host. Bootstrapping resources can be signed, so that the authenticity of the retrieved resources are trusted. The process of bootstrapping an end host is simply done by installing the appropriate bootstrap package found in the AS's local central bootstrapping server, by enabling an external orchestrator (i.e. systemd) to manage the bootstrap process and start the SCION Daemon once the process is finished successfully. The bootstrapping server is a simple web server that serves bootstrapping configuration files to the end hosts within the network.

The bootstrapping process consists of the following steps:

- The bootstrap daemon probes the local network for hints about a discovery server address using the available discovery mechanisms (i.e., DHCP, DNS, and mDNS).
- Wait for hints from the discoverers.
- Once a hint gets received, the bootstrapper tries to download the topology of the AS and some TRCs from the discovery server, at least the TRC of the ISD the AS is in.
    - On success, the bootstrapper prepares the SCION Daemon files and exits successfully, and the SCION Daemon is automatically started by the orchestrator.
    - On failure, wait for hints from the discoverers.

## 5.5 SCIONLab

SCIONLab [181] is a globally distributed network offering a research and testbed environment of SCION to foster research and development, so that users and interested parties can easily be up and running with a working SCION environment in order to connect and run tests before deciding whether to deploy SCION in their networks. There are two types of SCIONLab ASes, infrastructure ASes, which are the core ASes of SCIONLab, and user ASes, that are created and managed by the end users, and run on user-provided infrastructure. All SCIONLab ASes run SCION control services—including a beacon service, a certificate service, a path service, and a COLIBRI service.

The life cycle of a user AS begins when the user creates an account on the Coordinator at https://www.scionlab.org. After selecting an attachment point, the Coordinator provides the AS configuration, which includes the necessary certificates for operation. Once the user deploys their AS, it begins receiving PCBs from the attachment point's AS and registers its down-paths in the core path service. From this point forward, the user AS is reachable by other SCIONLAB ASes.

## 5.6 SCION Education, Research and Academic Network – SCIERA

The SCION Education, Research and Academic Network (SCIERA) [182] is a target implementation of SCION that has the goal to interconnect universities, national research institutes, and NREN and to enable them to provide native SCION connectivity to their personnel and students in an overlay-free and productive network, as a way to encourage and advance research and education. SCIERA is presently established across three primary regions; Europe, North America, and Asia. Each region has a core AS and connects multiple research and education entities that run their SCION enabled ASes as shown in Figure 5.1. Each participating research entity runs its own AS, which is linked to the regional core-AS. This decentralized structure ensures that each entity maintains control over its own network while benefiting from the broader SCIERA connectivity. SCIERA is also connected to the production SCION network offered by Anapaya [161] through ISD 64, which extends SCIERA's reach and capabilities.

As SCIERA is the entity that facilitates research collaboration, so various research and education entities can be connected to the SCION network for synergies across different institutions and geographical locations. In our studies into SCION, SCIERA seemed like the perfect match for what we intended to do with this thesis, which was to study the SCION architecture in depth and research its capabilities. As SCIERA was our chosen environment of implementation, we will delve deeeper into its inner working in Chapter 6.

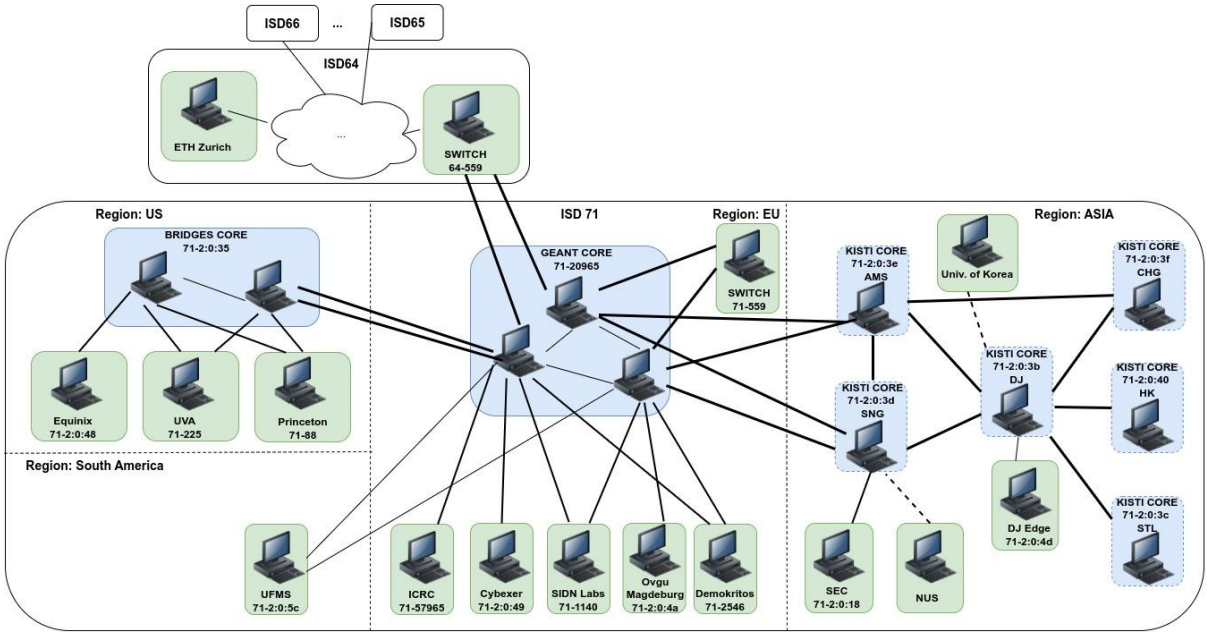


Figure 5.1 SCIERA network topology ASes

## 5.7 Use Cases

The use of ISDs and SCION networks is supported by practical implementations, such as in the deployment of SCION within the Swiss financial sector, where ISDs help manage the complex trust relationships between different financial institutions and ensure secure data exchanges [160]. The Secure Swiss Finance Network (SSFN) has become the new gateway for the Swiss Interbank Clearing (SIC) since November 2021, when the Swiss National Bank (SNB) and the financial infrastructure provider SIX have launched SSFN along with the collaboration of the telecommunication companies Sunrise, Swisscomm, SWITCH, and Anapaya Systems. SSFN is scheduled to completely replace the previous network Finance IPNet by the end of September 2024. By the utilization of SCION network and architecture, SSFN leverages greater resilience against cyber attacks, and offers high-level connectivity and network stability, thus strengthening the overall resilience of the Financial Center Switzerland. The SNB has been a sponsor to the R&D phase of SCION and continues to be, and rightfully so if the frameworks results are to be counted.

The major use case of SSFN, as well as the introduction of the software Anapaya EDGE to the AWS Marketplace, has opened the path for more sensitive and critical infrastructures to take interest and invest time and effort into becoming SCION enabled entities. Through the collaboration with AWS, reference architectures and user guides for customers have been provided, making the overall effort of establishing SCION connectivity streamlined and easily implemented via virtual appliances.

In the same spirit as SSFN, the Secure Swiss Health Network (SSHN) comes to ensure the resilience and and network stability of critical applications and environments within the health public sector of Switzerland. Through geofencing and path optimization techniques, SSHN can meet the strict requirements and high standards of the health industry, and operate as a standalone ISD with its unique set of TRCs, leveraging to their full extend SCION's attributes. By running critical medical devices and applications over SSHN, a private, secure and trusted network is created to be used by healthcare professionals, hospitals, government agencies, service providers, and laboratories, offering great protection against DDoS attacks and route attack, all the while protecting sensitive data.

Along with the major use cases of SSFN and SSHN, SCION and Anapaya have application in the fortification of IoT services and environments, as well as web services companies and remote services (i.e. VPN and VPN vulnerabilities). The large range of application of SCION shows the great potential in the protocol and its merits, as well as it separates it from other similar initiatives. From the comparisons made previously, none of the other next-generation innovative projects have known such high adoption rates, and especially escaping the close confines of universities and academia fleeing to the industry sector.

# 6 Implementation

The implementation of SCION involves a series of steps that include setting up a SCION-enabled router, establishing the SCION AS, and integrating with the existing network infrastructure. This process requires a comprehensive understanding of both SCION's architectural principles and the specific needs of the deploying entities, that have been analysed previously. Nevertheless, in the resources stated in the Bibliography section of this thesis, one can find much more information about the different entities and part of SCION, as we seem to have touched only the tip of the iceberg.

In the continuation, the practical implementation of SCION into the existing network infrastructure of the Network Operations Center of the National Center for Scientific Research Demokritos will be recorded.

## 6.1 Hardware

The hardware used for this implementation was a Supermicro X10SDV-TLN4F motherboard, equipped with two 10GbE network interfaces and an Intel® Xeon® Octa-core D-1541 processor. Details about the specifications and characteristics of the motherboard can be found on https://www.supermicro.com/en/products/motherboard/X10SDV-TLN4F.

The server was already equipped with a Samsung SSD 870 EVO drive of 256GB storage, and that was chosen to stay on board, but smaller storage devices can also be used. The recommended sizes for new Debian or Ubuntu installations are enough for the deployment of a SCION router, as SCION will be installed as a package over the operating system of our choice.

## 6.2 Installation and Configuration

Firstly, the initial contact with the appropriate entity has to be established, i.e. with the implementation tean of Géant for Europe, BRIDGES for the USA, or KISTI for Asia, so the physical link between the new location and one of the Points-of-Presence (PoPs) of SCION can be established, for example by using a dedicated VLAN carrying the SCION network. At the moment, SCIERA has three PoPs, each located respectively to Frankfurt, Paris and Geneva.

In our case, as we are located in Europe, we contacted Géant, which in turn contacted our respective NREN, GRNET to carry the appropriate VLANs, one connecting us with the PoP in Paris and one to Paris. The VLAN tag was discussed between the three entities of Géant, GRNET and Demokritos, as to coordinate and find one that was not in use already. As the National Center for Scientific Research Demokritos already has an ASN assigned by RIPE, our AS was named 71-2546, 71 because it is the

SCION assigned number for the Global SCION Education Network, and 2546 as it is Demokritos' ASN in RIPE [183].

The installation process of SCION is pretty straight-forward, as it only requires a Debian-esk system so that the appropriate packages can be installed. Currently, Ubuntu is recommended to be used to run SCION, and its packages can be found in the official repositories of the distribution.

The installation of SCION is as simple as running the following commands in the terminal of the server:

```
sudo apt-get install apt-transport-https ca-certificates

echo "deb [trusted=yes] https://packages.netsec.inf.ethz.ch/debian all main" | sudo tee /etc/apt/sources.list.d/scionlab.list

sudo apt-get update

sudo apt-get install scionlab
```

Because we wanted to participate in SCIERA, after the installation of the package, we contacted the developing team of SCIERA, and we received a compressed file containing the dedicated configuration for our host, which we executed in the system by running the below command. The host1.tar.gz is a compressed file containing configuration files that describe the topology of the SCION node we set up and who the parent ISD is, others that set up the SCION daemon, SCION dispatcher, and the control services, and files that establish the beacon policies, and of course the TRCs needed for our node to become a trusted part of the SCIERA infrastrucure.

```
sudo bash install.sh host1.tar.gz
```

The execution of the above command leads to the installation of the proper SCION configuration, the start of all SCION services, and the addition of the host to the SCIERA network.

To check the connectivity of our AS with the rest of the SCION network, and that we have retrieved the paths correctly from the beaconing service, we run the following command which shows the paths we have received from the beacons and can be used to reach our parent, ISD 71-20965 (Otto von Guericke University):

```
scion showpaths 71-20965
```

```
Available paths to 71-20965

2 Hops:

[0] Hops: [71-2546 1>10 71-20965] MTU: 8952 NextHop: 127.0.0.1:30001 Status: alive LocalIP: 127.0.0.1

[1] Hops: [71-2546 2>11 71-20965] MTU: 8952 NextHop: 127.0.0.1:30001 Status: alive LocalIP: 127.0.0.1
```

To check the operations and status of the SCION connectivity and the SCION services, we are provided with the below command line tools. To check on the SCION service status, we execute the command:

```
sudo systemctl list-dependencies scionlab.target
```

To check on the border router's log, we can execute the following command, to check on the correct completion of the bidirectional-forwarding detection (BFD) handshake, and the state of the interfaces:

```
sudo journalctl -u scion-border-router@br-1.service
```

Alternatively we can view the same results by executing:

```
curl -sfS localhost:30401/metrics | grep router_interface_up
```

To check on the control service's logs and that beacons are registered in the our system, we execute:

```
sudo journalctl -u scion-control-service@cs-1.service
```

Or, alternatively:

```
curl -sfS localhost:30454/metrics | grep control_beaconing_received_beacons_total
```

We can view the paths the node has received for each neighbours, shown in Figure 5.1, and which are available to our AS by executing the following command. The SCION ASes and ISDs in the SCION/SCIERA network can be viewed in the knowledge base of Anapaya [183].

```
scion showpaths 71-2:0:35

scion showpaths 71-20965
```

Alternatively we can view the same results by executing:

```
curl -sfS localhost:30401/metrics | grep router_interface_up
```

Examples of the above commands in the running system are shown in Figures 6.1 through 6.4. Information on how the topology is configured on the router, can be seen in the provided JSON file in Annex II.

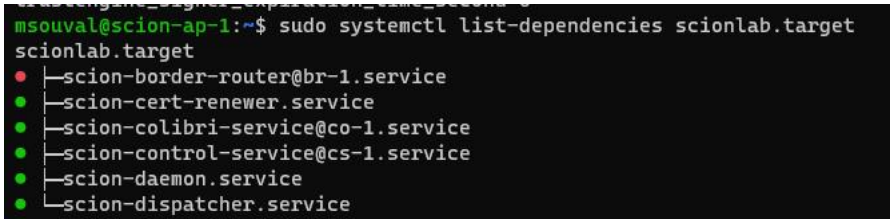


Figure 6.1 SCION Border Router status down

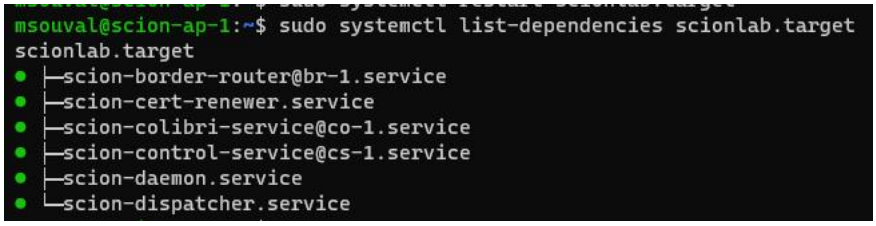


Figure 6.2 SCION services status up

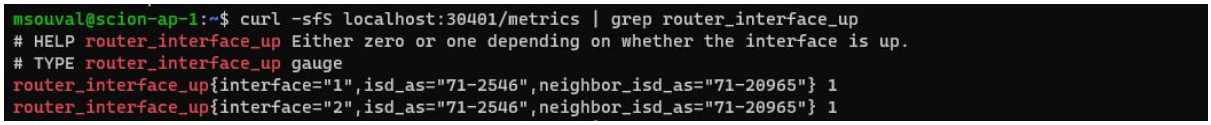


Figure 6.3 Information on the router's interface, showing the ISD number of the host and its neighbour

```
msouval@scion-ap-1:~$ scion ping 71-2546,127.0.0.1
Resolved local address:
  127.0.0.1
Using path:
  Hops: [] MTU: 8952 NextHop: <nil>

PING 71-2546,127.0.0.1:0 pld=0B scion_pkt=44B
52 bytes from 71-2546,127.0.0.1: scmp_seq=0 time=472µs
52 bytes from 71-2546,127.0.0.1: scmp_seq=1 time=468µs
52 bytes from 71-2546,127.0.0.1: scmp_seq=2 time=582µs
52 bytes from 71-2546,127.0.0.1: scmp_seq=3 time=467µs
52 bytes from 71-2546,127.0.0.1: scmp_seq=4 time=622µs
52 bytes from 71-2546,127.0.0.1: scmp_seq=5 time=501µs
^C
--- 71-2546,127.0.0.1 statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5.09279s
```

Figure 6.4 Executing scion ping to the localhost with µs latency

## 6.3 Monitoring

After setting up the SCION node, we can set up a monitoring server that can give metrics about the node's performance. The SCIERA developing team provides its users with the appropriate files and instructions on how to set up the monitoring server. It is recommended that the monitoring server is independent from the node, an entirely different machine (virtual or physical). In this chapter, "server" is used to describe the monitoring server, and "client" is used to describe the SCION node, thus characterizing the relationship between the two.

SCIERA provides two pairs of files, one pair to be installed on the client or clients to export metrics, and one to be installed on the monitoring server to gather the metrics from its clients, in case we have more than one SCION nodes in our infrastructure. By executing and installing these files on a client or server, a new directory named /etc/monitoring is created and populated with the necessary scripts.

After the installation of the monitoring files on either side, on the client the IP needs to be set as a value to the appropriate variables in the script of the client. On the server there are some additional steps to be taken in order to install and configure the docker packages and then install, run and configure Grafana, Prometheus, Alertmanager and Traefic Proxy containers. Editing accordingly the appropriate YAML files of the services as well as the Docker Compose file, we can pass the needed values for the web access to the services, create the appropriate admin users, hash their passwords, establish alerting for the SCION connectivity, and secure the services with TLS. Starting our monitoring instance by navigating to the monitoring directory and bringing up the containers with the docker compose command as show in the Figure 6.5 below, we can get a first view on the SCION server and its connectivity.

```
cd /etc/monitoring

docker-compose up -d
```

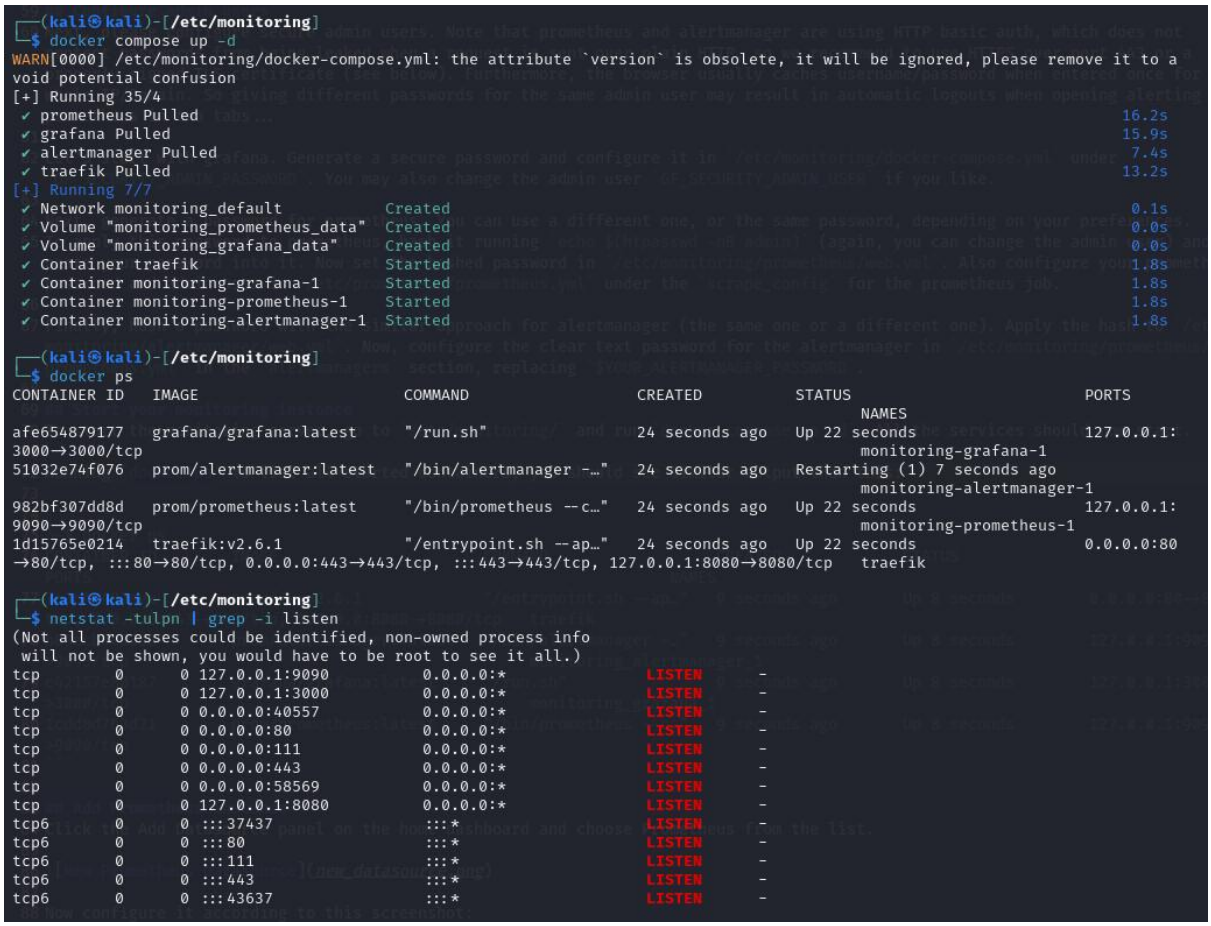


Figure 6.5 Pulling and starting container images, and checking open ports of monitoring server

Checking on the services exposed ports, we can view the initial dashboards, as shown in Figure 6.6 through 6.7.

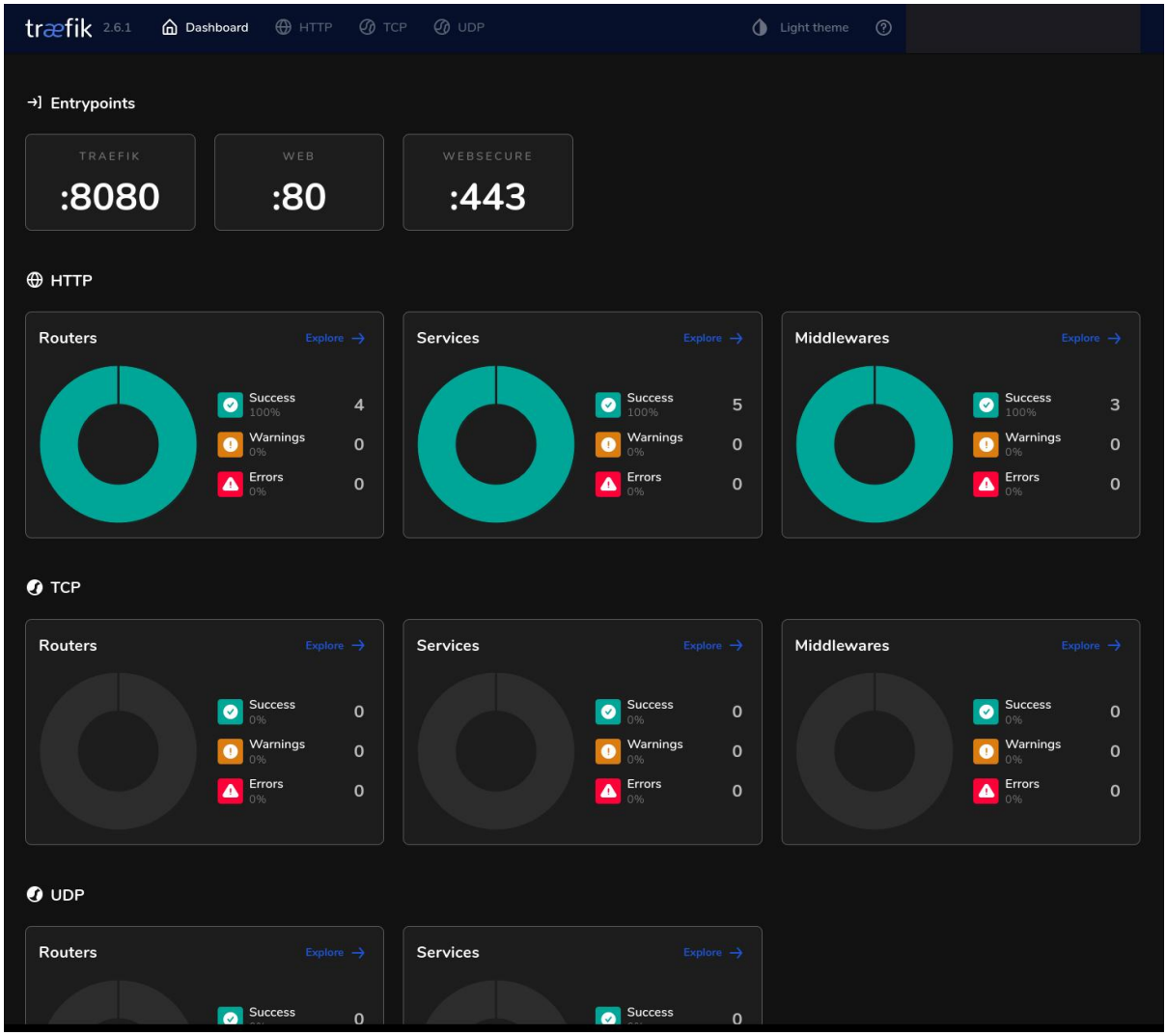


Figure 6.6 Trafic dashboard

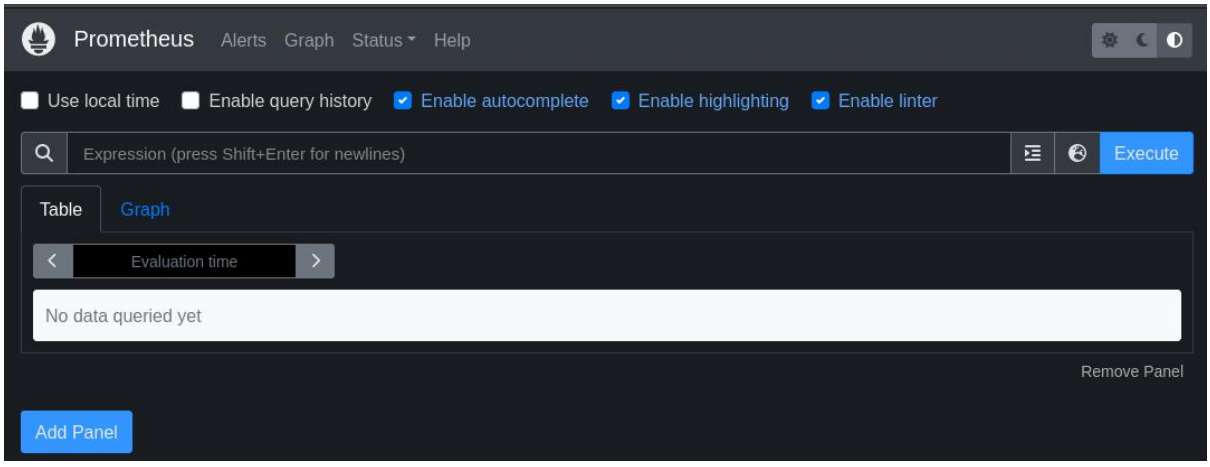


Figure 6.7 Prometheus dashboard

Now we can login with the credentials we provided in the docker-compose.yml file, and set up the final information of client we want to monitor.

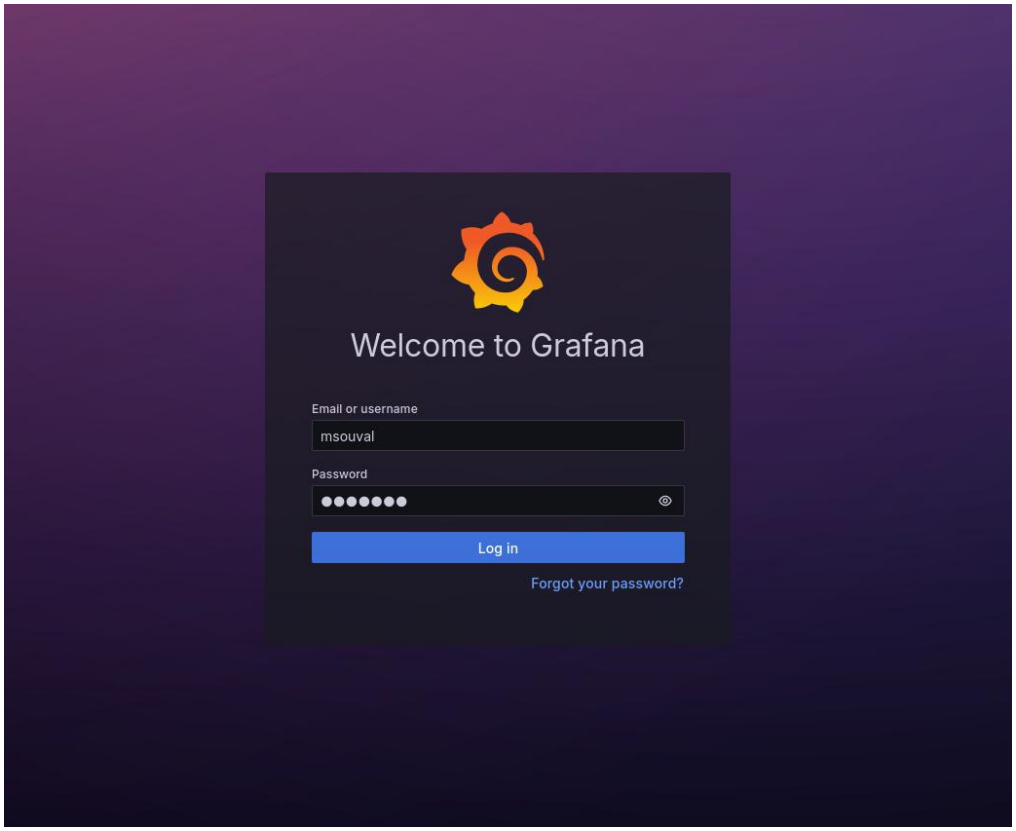


Figure 6.8 Grafana login page

To add the SCION node we want monitored, we just need to add a new data source in Grafana. By creating a new data source, Grafana automatically creates a data source ID, that we will use later on to create the dashboard.

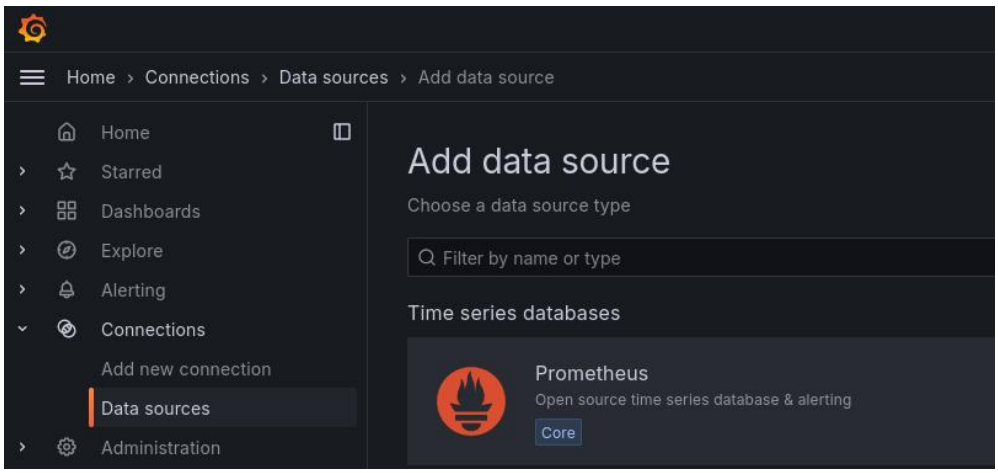


Figure 6.9 Adding data source in grafana

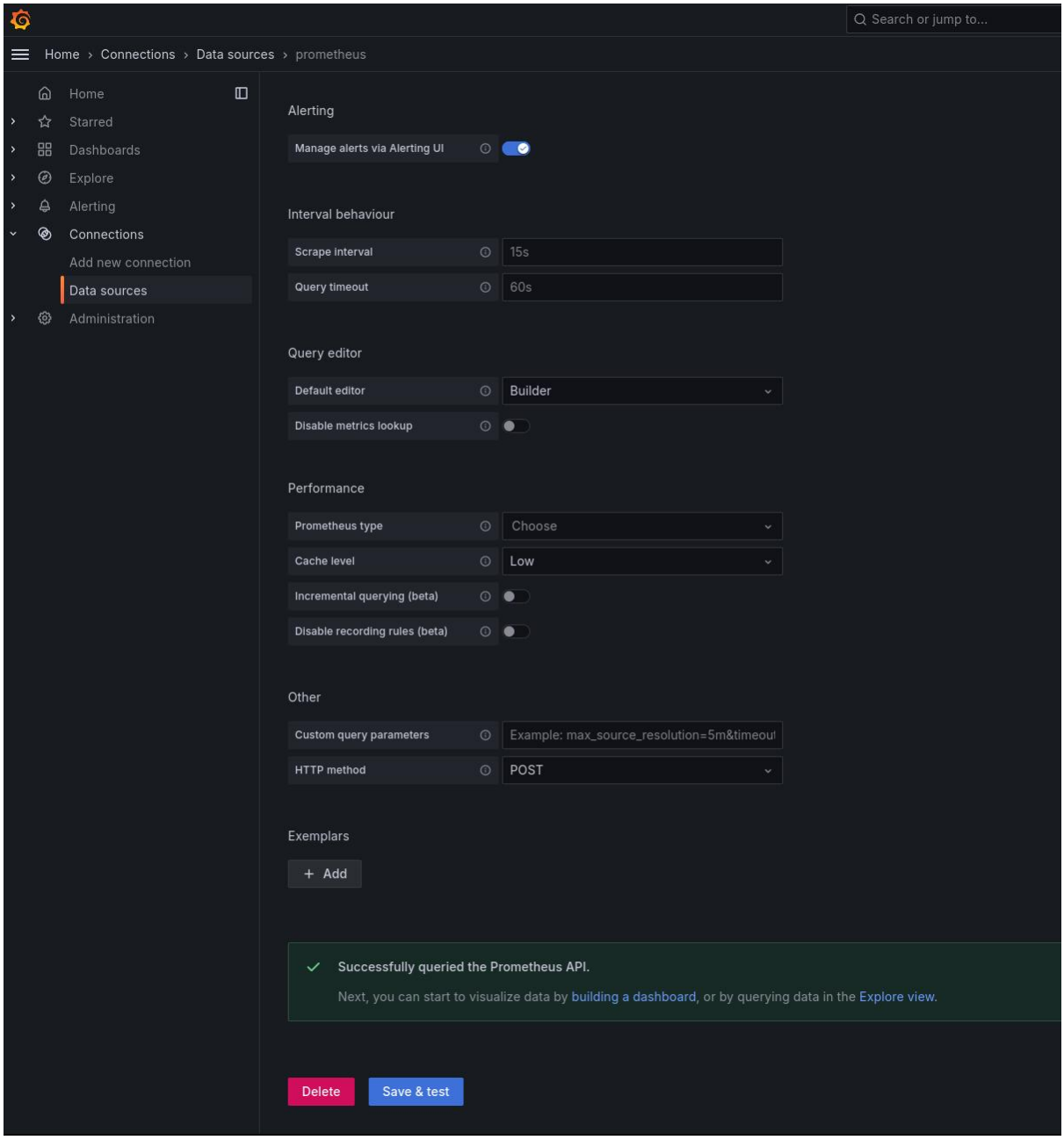


Figure 6.10 Adding new data source details

Finally, we can create a new dashboard by choosing to import a file. We edit the provided file from SCIERA and pass the value of the data source ID we created earlier. We load and save the dashboard. By navigating to the grafana dashboards, we can now be shown the metrics and status of the client SCION node, as shown in Figure 6.11

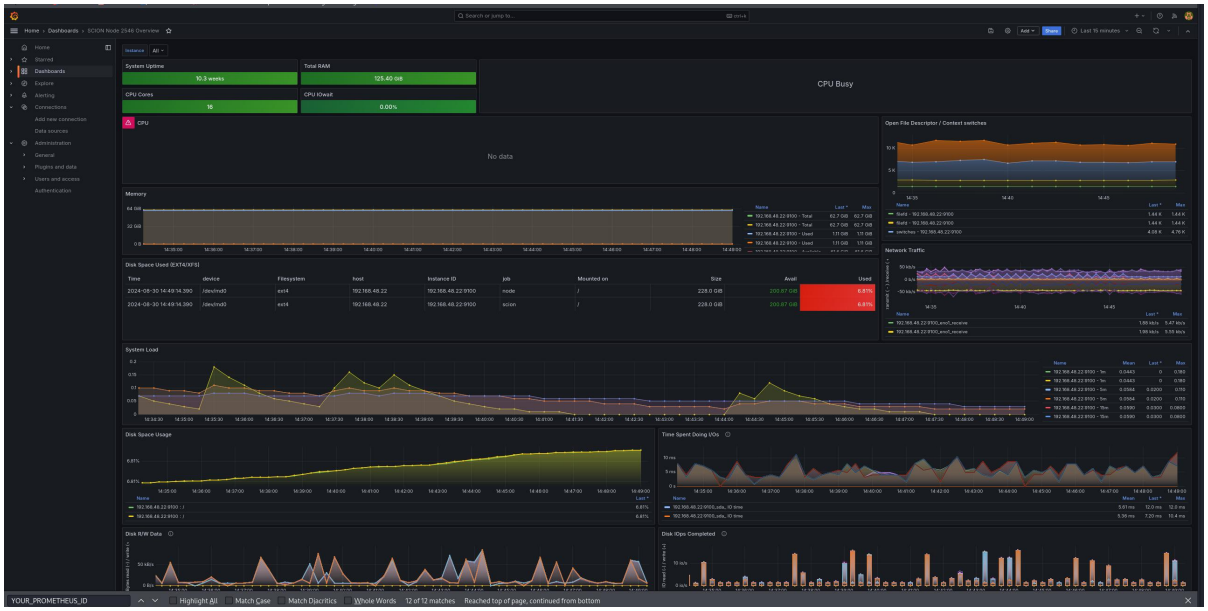


Figure 6.11 SCION node status

# 7 Conclusions

From the research in the SCION architecture topic, it is shown that hrough the years that SCION is active, it has showcased its potential and capabilities to great extends. The fact that sensitive infrastructures such as the Swiss Banking System and Healthcare System, as well as the Energy sector, have shown such great interest, and have invested both in money, but also in time and training, shows the great potential of SCION, its adoption, and it makes clear that SCION is here to stay. The time needed to study, understand and adopt the new architecture and its concepts of ISDs, beaconing, RPKI, and the rest, does not seem to be exceedingly long, so in our point of view it could be integrated in the existing IP infrastructure of an organization without much ado, offering to the network operators time to trinket with a demo SCION enabled router before implementing SCION's path-aware networking and multipath communication, security and resiliency into their production infrastructure, offering their users secure connectivity, devoid of common security problems, such as DoS and MitM attacks, and BGP-hijacking.

Looking ahead, the next steps in SCION's development already involve further research into optimizing its performance, aiming at high-traffic environments, enhancing the environments' security measures, and offering innovative solutions. As more people, especially engineers and network architects and operators, become curious about the architecture and begin experimentining with SCION, it is our belief that SCION's rates of adoption will be greatly increased in the next couple of years.

Additionally, the phased integration of SCION into existing networks, supported by the global collaboration with research and industry partners, and the provision of SCION to be readily available to end users for installation and usage, is what could give the final push and be that crucial detail for its widespread adoption. In our view, the bootstrapping of end host devices seamlessly and in bulk, with not much input or knowledge from the end user is what keeps SCION within the confines of bigger infrastructures and knowledgeable crowds. By addressing these challenges and leveraging its advanced features, SCION has the potential to significantly improve the security and performance of next-generation networks and enhance peoples' everyday experiences in their digital lives.

As for the future, SCION keeps moving forward with a fast pace, and we are enthusiastic to follow its progress and evolution. SCION networks can secure previously open and vulnerable networks, such as 5G and IoT infrastructures, and secure private and sensitive networks end-to-end. We wish to be

able to follow the next steps ahead and maybe become a small part of the development and expansion of such an interesting network, by providing SCION enabled paths, systems and applications.

# Annex I – European NRENs

Table 0.1 European National Research and Education Networks

| Abbreviation | Name | Nation/Region | ASN | URL | Comments | Created on |
|---|---|---|---|---|---|---|
| EARN [1] | European Academic and Research Network | Europe | | https://earn-history.net/ | Merged with RARE on October 20, 1994, which later became TERENA | 1983 |
| GÉANT | GÉANT Project | Europe | 21320 | https://geant.org | Develops and maintains the GÉANT backbone network on behalf of European NRENs. Formerly DANTE (circa 1993) and TERENA (circa 1986). | 2015 |
| CEENet | Central and Eastern European Research Networking Association | Central and Eastern Europe | | | Responsible for the co-ordination of the establishment and operation of data networks in research networks in Central and Eastern Europe and in adjacent countries | 1994 |
| Eumedconnect | Eumedconnect3 | South Mediterranean Backbone | | https://eumedconnect3.net/ | Founded under the Euro-Mediterranean Information Society (EUMEDIS) programme and managed by GÉANT | 2004 |
| ANA | Academic Network of Albania | Albania | 57961 | https://www.rash.al/en/ | Known as RASH since 2011 | 2007 |
| ASNET-AM | Academic Scientific Research Computer Network of Armenia | Armenia | 47623 | https://asnet.am/ | Under Institute for Informatics and Automation Problems of National Academy of Sciences of the Republic of Armenia | 1994 |
| ACOnet | Austrian Academic Computer Network | Austria | 1853 | http://www.aco.net/ | | 1986 |
| AzScienceNet | Azerbaijan Science Network | Azerbaijan | 29584 | https://azsciencenet.az/en/ | | 1991 |

[1] Francois Fluckiger, “The European Researchers’ Network”, CERN, La Recherche, Issue number 328, February 2000, “Special Internet, l’Avenir du Web”

| Abbreviation | Name | Nation/Region | ASN | URL | Comments | Created on |
|---|---|---|---|---|---|---|
| BASNET | Network of the National Academy of Sciences of Belarus | Belarus | 21274 | https://www.basnet.by/ | State Scientific Enterprise 'United Institute of Informatics Problems of National Academy of Sciences of Belarus' (UIIP NASB) | 2002 |
| Belnet | Belgian Network | Belgium | 2611 | https://www.belnet.be/ | | 1993 |
| BREN | Bulgarian Research and Education Network Association | Bulgaria | 6802 | http://www.bren.bg/ | | 2004 |
| CESNET | CESNET z.s.p.o. | Czechia | 2852 | https://www.cesnet.cz/ | | 1996 |
| CARNET | Croatian Academic and Research Network | Croatia | 2108 | http://www.carnet.hr/ | | 1991 |
| CYNET | Cyprus Research and Academic Network | Cyprus | 211779 | https://cynet.ac.cy/ | | 2017 |
| SURF | SURFnet | Dutch, Netherlands | 1103 | http://www.surf.nl/en | | 2002 |
| EENet | Estonian Education and Research Network | Esthonia | 3221 | http://www.eenet.ee/EENet/EENet_en | Also known as EENet of HTM | 2002 |
| RENATER | RENATER/GIP RENATER | France | 2200 | https://www.renater.fr/en/accueil-english/ | | 1993 |
| DFN | Deutsches Forschungsnetz | Germany | 680 | https://www.dfn.de/ | | 1984 |
| GRENA | Georgian Research and Educational Networking Association | Georgia | 20545 | https://grena.ge/ | | 1999 |
| GRNET | Greek Research and Technology Network | Greece | 5408 | https://grnet.gr/ | | 1998 |
| KIFU/NIIF | Hungarian Governmental Agency for ICT | Hungarian | 1955 | https://kifu.gov.hu/en/main-page/ | KIFU is the convergance of NIIF and HUNGARNET | 2004 |

| Abbreviation | Name | Nation/Region | ASN | URL | Comments | Created on |
|---|---|---|---|---|---|---|
| | Development | | | | (founded on 2016) | |
| HEAnet | HEAnet | Ireland | 1213 | https://www.heanet.ie/ | The National Education and Research Network of Ireland | 1983 |
| GARR | Consurtium GARR | Italy | 137 | http://www.garr.it/ | The Italian Academic and Research Network | 2001 |
| KazRENA | KazRENA – Kazakhstan Research and Education Network Association | Kazakhstan | 41419 | http://kazrena.kz/ | Association of Users of Scientific and Educational Computer Network of Kazakhstan | 2001 |
| SigmaNet | SigmaNet | Latvia | 29345 | https://sigmanet.lv/ | The Academic Network Laboratory of the University of Latvia Institute of Mathematics and Computer Science and the Latvian NREN. Since 1992 as LATNET, renamed as SigmaNet in 2008 | 1992 |
| LITNET | LITNET | Lithuania | 2847 | http://www.litnet.lt/ | | 1991 |
| RESTENA | Fondation RESTENA | Luxembourg | 2602 | https://www.restena.lu/ | | 2000 |
| MARNET | Macedonian Academic Research Network Skopje | The Former Yugoslav Republic of Macedonia | 44224 | https://marnet.mk/ | | 2010 |
| RičerkaNet | RICERKANET | Malta | 12046 | https://ricerka.net.mt/ | National Research and Educational Network (NREN) for the Maltese Islands | 2009 |
| RENAM | RENAM | Republic of Moldova | 9199 | https://renam.md/ | | 1999 |
| MREN | Montenegrin Research and Education Network | Montenegro | 40981 | https://mren.ucg.ac.me/organization.php | For technical management and monitoring of the NREN, the Information Technology Center of the University of Montenegro is responsible | 2006 |
| PIONIER | Poznan Supercomputing and Networking Center | Poland | 8501 | https://www.pionier.net.pl/ | | 2003 |

| Abbreviation | Name | Nation/Region | ASN | URL | Comments | Created on |
|---|---|---|---|---|---|---|
| FCCN | Fundacao para a Computacao Cientifica Nacional | Portugal | 1930 | http://www.fccn.pt/ | | 1987 |
| RoEduNet | RoEduNet | Romania | 2614 | https://www.roedu.net/ | Romanian Education Network | 1990 |
| RUNNet | Russian UNiversity Network | Russia | 3267 | https://niks.su/ | Federal State Institution "Federal Scientific Research Institute for System Analysis of the Russian Academy of Sciences" | 2002 |
| AMRES | Akademska Mreza Republike Srbije | Serbia | 13092 | https://www.amres.ac.rs/en/amres/amres-infrastructure | | 2010 |
| ARNES | Academic and Research Network of Slovenia | Slovenia | 2107 | https://www.arnes.si/en/ | | 2014 |
| SANET | Slovak Academic Network | Slovakia | 2607 | http://www.sanet.sk/ | | 2001 |
| RedIRIS | RedIRIS/Red.es | Spain | 766 | http://www.rediris.es/ | Interconexión de los Recursos InformáticoS de las universidades y centros de investigación | 1988 |
| SWITCH | SWITCH | Switzerland | 559 | http://www.switch.ch/ | | 1987 |
| ULAKBIM | Turkish Academic Network and Information Center | Turkey | 8517 | https://ulakbim.tubitak.gov.tr/ | ULAKNET/ TUBITAK ULAKBIM | 1996 |
| URAN | User Association of Ukrainian Research & Academic Network "URAN" | Ukraine | 12687 | http://www.uran.ua/ | | 1996 |
| Jisc | Joint Information Systems Committee | United Kingdom | 786 | https://www.jisc.ac.uk/janet | JANET is the research and education network provided by JISC | 1993 |
| KREN | KREN | Kosovo | 211080 | https://kren-ks.eu/ | Ministry of Economy of Republic of Kosovo | 2019 |

# ANNEX II – Topology JSON file


```
{
 "attributes": [],
 "border_routers": {
  "br-1": {
   "interfaces": {
    "1": {
     "isd_as": "71-20965",
     "link_to": "PARENT",
     "mtu": 8952,
     "underlay": {
      "public": "[fe80::9f2:1630%eno3]:50000",
      "remote": "[fe80::51e5:1630]:50000"
     }
    },
    "2": {
     "isd_as": "71-20965",
     "link_to": "PARENT",
     "mtu": 8952,
     "underlay": {
      "public": "[fe80::9f2:1640%eno4]:50000",
      "remote": "[fe80::51e5:1640]:50000"
     }
    }
   },
   "internal_addr": "127.0.0.1:30001"
  }
 },
 "colibri_service": {
```

```
    "co-1": {
      "addr": "127.0.0.1:30257"
    }
  },
  "control_service": {
    "cs-1": {
      "addr": "127.0.0.1:30254"
    }
  },
  "discovery_service": {
    "ds-1": {
      "addr": "127.0.0.1:30254"
    }
  },
  "isd_as": "71-2546",
  "mtu": 8952
}
```

# Bibliography

[1] J. F. Kurose and K. W. Ross, Computer networking: a top-down approach, Seventh edition. Boston: Pearson, 2017.

[2] A. S. Tanenbaum and D. Wetherall, Computer networks, 5. ed. Boston Amsterdam: Prentice Hall, 2011.

[3] W. Stallings, Data and computer communications, Tenth edition. Boston: Pearson, 2014.

[4] L. Peterson and B. Davie, 'Computer Networks: A Systems Approach'.

[5] F. Hu, Q. Hao, and K. Bao, 'A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation', IEEE Commun. Surv. Tutorials, vol. 16, no. 4, pp. 2181–2206, 2014, doi: 10.1109/COMST.2014.2326417.

[6] N. McKeown et al., 'OpenFlow: enabling innovation in campus networks', SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, Mar. 2008, doi: 10.1145/1355734.1355746.

[7] J. Y. Le Boudec, "Rate adaptation, Congestion Control and Fairness: A Tutorial", Ecole Polytechnique Fédérale de Lausanne, 2021

[8] L. Yang, R. Dantu, T. Anderson, and R. Gopal, 'Forwarding and Control Element Separation (ForCES) Framework', RFC Editor, RFC3746, Apr. 2004. doi: 10.17487/rfc3746.

[9] Y. Rekhter, T. Li, and S. Hares, 'A Border Gateway Protocol 4 (BGP-4)', RFC Editor, RFC4271, Jan. 2006. Accessed: Jun. 23, 2024. [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc4271.txt.pdf

[10] J. Hawkinson and T. Bates, 'Guidelines for creation, selection, and registration of an Autonomous System (AS)', RFC Editor, RFC1930, Mar. 1996. doi: 10.17487/rfc1930

[11] A. P. Bishop, 'The National Research and Education Network (NREN): Update 1991. ERIC Digest', ERIC Clearinghouse on Information Resources, Syracuse University, 030 Huntington Hall, Syracuse, NY 13244-2340 (free while supply lasts)., Dec. 1991. Accessed: May 17, 2024. [Online]. Available: https://eric.ed.gov/?id=ED340390

[12] 'ARPANET, Internet', LivingInternet. Accessed: Jun. 23, 2024. [Online]. Available: https://www.livinginternet.com/i/ii_arpanet.htm

M. Hauben, R. Hauben, 'Netizens: on the history and impact of usenet and the internet', Chapter 7, pp 66-70. Washington: IEEE computer, 1997.

[13] 'BITNET'. Accessed: Jun. 23, 2024. [Online]. Available: https://bit.net/

[14] 'Information Superhighway Envisioned-Legislation Pending to Establish National Computer Network'. Accessed: Jun. 23, 2024. [Online]. Available: https://web.archive.org/web/20061001232135/http://www.nal.usda.gov/pgdic/Probe/v1n1_2/info.html

[15] Duncan Greaves, "NREN Capability Maturity",

[16] Berners-Lee, T.; Cailliau, R.; Groff, J.-F.; Pollermann, B. (1992). "World-Wide Web: The Information Universe". Electron. Netw. Res. Appl. Policy. 2: 52–58. doi:10.1108/eb047254

[17] T. Berners-Lee, 'Universal Resource Identifiers in WWW: A Unifying Syntax for the Expression of Names and Addresses of Objects on the Network as used in the World-Wide Web', Internet Engineering Task Force, Request for Comments RFC 1630, Mar. 1994. doi: 10.17487/RFC1630.

[18] 'H.R. 1757--High Performance Computing and High Speed Networking Applications Act of 1993'. Congress of the U.S., Washington, DC, p. 582, May 27, 1993. Accessed: May 27, 2024. [Online]. Available: https://eric.ed.gov/?q=H.R.+1757&id=ED365282

[19] V. Cerf and R. Kahn, "A Protocol for Packet Network Intercommunication," in IEEE Transactions on Communications, vol. 22, no. 5, pp. 637-648, May 1974, doi: 10.1109/TCOM.1974.1092259

[20] Information Sciences Institute and University of Southern California, 'RFC 791, "Internet Protocol", IETF'. IETF, Sep. 1981. Accessed: May 27, 2024. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc791

[21] A. S. Tanenbaum, D. J. Wetherall, "Computer Networks", 5th Edition, Pearson, 2011

[22] D. D. Clark, "The Design Pilosophy of the DARPA Internet Protocols", ACM SIGCOMM Computer Communication Review, 1988

[23] Information Sciences Institute and University of Southern California, 'RFC 793, "Transmission Control Protocol", IETF'. IETF, Sep. 1981. Accessed: May 27, 2024. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc793

[24] [1] ‘About Us’, RIPE Network Coordination Center. Accessed: Jun. 23, 2024. [Online]. Available: https://www.ripe.net/about-us/

[25] ‘RIPEstat’. Accessed: Jun. 23, 2024. [Online]. Available: https://stat.ripe.net/

[26] ‘Routing Information Service (RIS)’, RIPE Network Coordination Center. Accessed: Jun. 23, 2024. [Online]. Available: https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/

[27] ‘RIPE Atlas – RIPE Network Coordination Centre’. Accessed: Jun. 23, 2024. [Online]. Available: https://atlas.ripe.net/

[28] ‘Amount of IPv6 Addresses Allocated and Assigned’, RIPE Network Coordination Center. Accessed: Jun. 23, 2024. [Online]. Available: https://www.ripe.net/analyse/statistics/amount-of-ipv6-addresses-allocated-and-assigned/

[29] ‘Internet Health Report | Monitoring networks health’, Internet Health Report. Accessed: May 20, 2024. [Online]. Available: https://ihr.iijlab.net/ihr/

[30] R. Minerva, A. Biru, D. Rotondi, "Towards a definition of the internet of things (IoT)", IEEE Internet Initiative, 2015.

[31] ‘That “Internet of Things” Thing – RFID JOURNAL’. Accessed: Jun. 23, 2024. [Online]. Available: https://www.rfidjournal.com/that-internet-of-things-thing

[32] C. Doukas, Building internet of things with the Arduino: V1.1 [Arduino V.10 ready! ; covers: communication with wired and wireless networks, android communication, cloud communication and more!]. S.l.: CreateSpace, 2012.

[33] P. Kocovic, R. Behringer, M. Ramachandran, and R. Mihajlovic, Eds., Emerging Trends and Applications of the Internet of Things: in Advances in Wireless Technologies and Telecommunication. IGI Global, 2017. doi: 10.4018/978-1-5225-2437-3.

[34] M. A. Ghosh, ‘Intelligent appliances controller using Raspberry Pi’, IEEE, 2016, doi: 10.1109/IEMCON.2016.7746253.

[35] A. Gloria, F. Cercas, and N. Souto, ‘Comparison of Communication Protocols for Low Cost Internet of Things Devices’, doi: 10.23919/SEEDA-CECNSM.2017.8088226.

[36] M. Mowbray and H. Labs, ‘HP Internet of Things Research Study’, 2015. Accessed: May 23, 2024. [Online]. Available: http://conference2015.chistera.eu/sites/conference2015.chistera.eu/files/CHIST-ERA%20Conference%202015%20-%20Mowbray.pdf [Online: last accessed May 2024]

[37] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, ‘Security of the Internet of Things: perspectives and challenges’, Wireless Networks, vol. 20, no. 8, pp. 2481–2501, Nov. 2014, doi: 10.1007/s11276-014-0761-7.

[38] F. Alaba, M. Othman, I. Hashem and F. Alotaibi, “Internet of Things security: A survey”, Journal of Network and Computer Applications, 88, pp.10-28, 2017.

[39] H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," in IT Professional, vol. 19, no. 5, pp. 27-33, 2017. doi: 10.1109/MITP.2017.3680960

[40] Jurcut, A.D., Coffey, T., Dojen, R., “On the Prevention and Detection of Replay Attacks using a Logic-based Verification Tool”, In: Computer Networks, Series: Communications in Computer and Information Science, Springer International Publishing Switzerland, Volume 431, ISBN: 978-3-319-07940-0, pp. 128-137, June , 2014, DOI: 10.1007/978-3-319-07941-7_13

[41] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 32-37, DOI: 10.1109/I-SMAC.2017.8058363.

[42] A. D. Jurcut, P. Ranaweera, and L. Xu, ‘Introduction to IoT Security’, in Wiley 5G Ref, 1st ed., R. Tafazolli, C. Wang, and P. Chatzimisios, Eds., Wiley, 2019, pp. 1–39. doi: 10.1002/9781119471509.w5GRef260.

[43] G. Zhang, L. Kou, L. Zhang, C. Liu, Q. Da, and J. Sun, ‘A New Digital Watermarking Method for Data Integrity Protection in the Perception Layer of IoT’, Security and Communication Networks, vol. 2017, pp. 1–12, 2017, doi: 10.1155/2017/3126010.

[44] S. Raza, L. Wallgren, and T. Voigt, “Svelte: Real-time intrusion detection in the internet of things,” Ad Hoc Netw., vol. 11, no. 8, p. 2661–2674, nov 2013. [Online]. Available: https://doi.org/10.1016/j.adhoc.2013.04.014

[45] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, ‘Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions’, 2022, doi: 10.20944/preprints202203.0087.v1.

[46] “Release 15”, 3GPP. Accessed: Jun. 02, 2024. [Online]. Available: https://www.3gpp.org/specifications-technologies/releases/release-15

[47] I. F. Akyildiz, S. Nie, S. C. Lin, and M. Chandrasekaran, "5G roadmap: 10 key enabling technologies," Computer Networks, vol. 106, pp. 17-48, Sep. 2016.

[48] T. S. Rappaport et al., "Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!," IEEE Access, vol. 1, pp. 335-349, 2013.

[49] M. Simsek, M. Bennis, and Ö. B. Akan, "5G Enabled Tactile Internet," IEEE Journal on Selected Areas in Communications, vol. 34, no. 3, pp. 460-473, Mar. 2016.

[50] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," IEEE Communications Magazine, vol. 52, no. 2, pp. 186-195, Feb. 2014.

[51] E. Björnson, E. G. Larsson, and T. L. Marzetta, ‘Massive MIMO: ten myths and one critical question’, IEEE Commun. Mag., vol. 54, no. 2, pp. 114–123, Feb. 2016, doi: 10.1109/MCOM.2016.7402270.

[52] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network Slicing in 5G: Survey and Challenges," IEEE Communications Magazine, vol. 55, no. 5, pp. 94-100, May 2017.

[53] P. Cabaj, A. Kotulski, K. Mazurczyk, and M. Smolarczyk, "Software-Defined Networking and Security: A Survey," IEEE Communications Surveys & Tutorials, vol. 18, no. 4, pp. 3027-3058, Fourth Quarter 2016.

[54] D. M. Gutierrez-Estevez, S. Khatibi, S. Ayaz, P. Ahokangas, and I. A. Stoica, "5G Network Slicing for Digital Twin Implementation: A Case Study on Remote Airport Tower," IEEE Access, vol. 8, pp. 219645-219657, 2020.

[55] X. Zhou, R. Li, T. Chen, and H. Zhang, "Network slicing as a service: enabling enterprises' own software-defined cellular networks," IEEE Communications Magazine, vol. 54, no. 7, pp. 146-153, Jul. 2016.

[56] X. Zhang, J. Fei, H. Jiang, and X. Huang, ‘Research on Power 5G Business Security Architecture and Protection Technologies’, in 2021 6th International Conference on Power and Renewable Energy (ICPRE), Shanghai, China: IEEE, Sep. 2021, pp. 913–917. doi: 10.1109/ICPRE52634.2021.9635437.

[57] J. Lee, H. Kim, C. Park, Y. Kim, and J.-G. Park, ‘AI-based Network Security Enhancement for 5G Industrial Internet of Things Environments’, in 2022 13th International Conference on Information

and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of: IEEE, Oct. 2022, pp. 971–975. doi: 10.1109/ICTC55196.2022.9952490.

[58] F. Lopez-Pires and B. Baran, 'Machine Learning Opportunities In Cloud Computing Data Center Management for 5G Services', in 2018 ITU Kaleidoscope: Machine Learning for a 5G Future (ITU K), Santa Fe: IEEE, Nov. 2018, pp. 1–6. doi: 10.23919/ITU-WT.2018.8597920.

[59] S. Sarkar and A. Debnath, 'Machine Learning for 5G and Beyond: Applications and Future Directions', in 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India: IEEE, Aug. 2021, pp. 1688–1693. doi: 10.1109/ICESC51422.2021.9532728.

[60] G. S. Chavhan, A. Rautkar, J. Prithviraj, R. Agrawal, N. Chavhan, and C. Dhule, 'Machine Learning For 5G Security Using Random Forest', in 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), Faridabad, India: IEEE, Nov. 2023, pp. 544–549. doi: 10.1109/ICAICCIT60255.2023.10466178.

[61] S. B. M. Baskaran, T. Faisal, C. Wang, D. R. Lopez, J. Ordonez-Lucena, and I. Arribas, 'The Role of DLT for Beyond 5G Systems and Services: A Vision', IEEE Comm. Stand. Mag., vol. 7, no. 1, pp. 32–38, Mar. 2023, doi: 10.1109/MCOMSTD.0004.2200053.

[62] F. Miatton, 'Blockchain at the Edge: The Nexus of Capturing New Value in 5G', in 2020 International Conference on Technology and Entrepreneurship – Virtual (ICTE-V), San Jose, CA, USA: IEEE, Apr. 2020, pp. 1–6. doi: 10.1109/ICTE-V50708.2020.9113786.

[63] A. Fernandez-Fernandez et al., 'Multi-Party Collaboration in 5G Networks via DLT-Enabled Marketplaces: A Pragmatic Approach', in 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal: IEEE, Jun. 2021, pp. 550–555. doi: 10.1109/EuCNC/6GSummit51104.2021.9482487.

[64] 'INSPIRE-5Gplus'. Accessed: May 29, 2024. [Online]. Available: https://www.inspire-5gplus.eu/

[65] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198.

[66] M. Satyanarayanan, "The Emergence of Edge Computing," IEEE Computer, vol. 50, no. 1, pp. 30-39, Jan. 2017, doi: 10.1109/MC.2017.9.

[67] R. Roman, J. Lopez, and M. Mambo, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," Future Generation Computer Systems, vol. 78, pp. 680-698, Jan. 2018, doi: 10.1016/j.future.2016.11.009.

[68] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile Edge Computing—A Key Technology Towards 5G," ETSI White Paper, no. 11, pp. 1-16, Sep. 2015. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

[69] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," EECS Department, University of California, Berkeley, Technical Report No. UCB/EECS-2009-28, Feb. 2009. [Online]. Available: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[70] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Special Publication 800-145, Sep. 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[71] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," in Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 2009, pp. 199-212, doi: 10.1145/1653662.1653673.

[72] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches," Wireless Communications and Mobile Computing, vol. 13, no. 18, pp. 1587-1611, Dec. 2013, doi: 10.1002/wcm.1203.

[73] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.

[74] X. Li, F. Zhao, and X. Xu, "Future Internet: The Internet of Things," China Communications, vol. 12, no. 11, pp. 1-10, Nov. 2015, doi: 10.1109/CC.2015.7407393.

[75] A. N. Toosi, R. K. Thulasiram, and R. Buyya, "Resource Provisioning for Heterogeneous Workloads in Software Defined Networks," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 467-480, July 2017, doi: 10.1109/TCC.2015.2471262.

[76] N. McKeown et al., "OpenFlow: Enabling Innovation in Campus Networks," ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69-74, Apr. 2008, doi: 10.1145/1355734.1355746.

[77] M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, "Software Defined Networking: State of the Art and Research Challenges," Computer Networks, vol. 72, pp. 74-98, Oct. 2014, doi: 10.1016/j.comnet.2014.07.004.

[78] M. P. Fernández, "Comparing OpenFlow Controller Paradigms Scalability: Reactive and Proactive," IEEE Latin America Transactions, vol. 10, no. 2, pp. 1586-1591, Apr. 2012, doi: 10.1109/TLA.2012.6148971.

[79] W. Cerroni, F. Callegati, and G. D. Battista, "Efficient Deployment of Virtual Network Functions," in Handbook of Fiber Optic Data Communication: A Practical Guide to Optical Networking, 4th ed. London, U.K.: Academic Press, 2013, pp. 667-691

[80] ETSI Industry Specification Group, "Network Functions Virtualisation (NFV); Architectural Framework," ETSI GS NFV 002, 2013, [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_nfv002v010101p.pdf

[81] R. Mijumbi, J. Serrat, J. L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network Function Virtualization: State-of-the-Art and Research Challenges," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 236-262, First Quarter 2016, doi: 10.1109/COMST.2015.2477041.

[82] A. Mestres, J. R. Espinosa, D. Meyer, S. Jouet, P. Barlet-Ros, and E. Alarcón, "Understanding the Network and Service Management Implications of Virtualization and Software-Defined Networking," IEEE Communications Magazine, vol. 54, no. 1, pp. 62-69, Jan. 2016, doi: 10.1109/MCOM.2016.7378437.

[83] M. Chiosi et al., "Network Functions Virtualization: An Introduction, Benefits, Enablers, Challenges & Call for Action," ETSI, Oct. 2012. [Online]. Available: https://portal.etsi.org/nfv/nfv_white_paper.pdf

[84] L. A. Grieco, M. B. Alaya, T. Monteil, M. Drira, "Architecting the Future Internet of Things (IoT): A Standpoint from the Post-Cloud Era," Springer Series on Internet of Things, 2014. [Online]. Available: https://link.springer.com/book/10.1007/978-3-319-04223-7

[85] SlowMist, ‘Truth Behind the Celer Network cBridge cross-chain bridge incident: BGP hijacking’, Coinmonks. Accessed: Jun. 23, 2024. [Online]. Available: https://medium.com/coinmonks/truth-behind-the-celer-network-cbridge-cross-chain-bridge-incident-bgp-hijacking-52556227e940

[86] ‘Celer Bridge incident analysis’. Accessed: Jun. 23, 2024. [Online]. Available: https://www.coinbase.com/blog/celer-bridge-incident-analysis

[87] C. Testart, P. Richter, A. King, A. Dainotti, D. Clark, “Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table”, “In Proceedings of the Internet Measurement Conference”, 2019, IMC '19, Association for Computing Machinery, New York, pp. 420–434, https://doi.org/10.1145/3355369.3355581

[88] B. Du, K. Izhikevich, S. Rao, G. Akiwate, C. Testart, A.C. Snoeren, K.C. Claffy, “IRRegularities in the Internet Routing Registry”, IMC '23: Proceedings of the 2023 ACM on Internet Measurement Conference, October 2023, Pages 104–110, https://doi.org/10.1145/3618257.3624843

[89] ‘IRR | Home’. Accessed: Jun. 23, 2024. [Online]. Available: https://irr.net/

[90] R. Bush, R. Austein, “The Resource Public Key Infrastructure (RPKI) to Router Protocol”, Version 1, RFC 8210, IETF, Sep 2017

[91] B. Du, K, Izhikevich, S. Rao, G. Akiwate, C. Testart, A. C. Snoeren, kc claffy, “IRRegularities in the Internet Routing Registry”, 2023, Proceedings of the 2023 ACM on Internet Measurement Conference (IMC '23), Association for Computing Machinery, New York, NY, USA, 104–110, retrieved from https://doi.org/10.1145/3618257.3624843

[92] M. Lepinski and S. Kent, ‘An Infrastructure to Support Secure Internet Routing’, Internet Engineering Task Force, Request for Comments RFC 6480, Feb. 2012. doi: 10.17487/RFC6480.

[93] Internet Society, ‘Mitigating prefix hijacks with RPKI (Part 2)’, MANRS. Accessed: May 26, 2024. [Online]. Available: https://manrs.org/2020/09/mitigating-prefix-hijacks-with-rpki-part-2/

[94] ‘FORTH-ICS-INSPIRE/artemis’. INSPIRE Group @FORTH-ICS, May 03, 2024. Accessed: May 26, 2024. [Online]. Available: https://github.com/FORTH-ICS-INSPIRE/artemis

[95] J. Durand, I. Pepelnjak, and G. Döring, ‘BGP Operations and Security’, Internet Engineering Task Force, Request for Comments RFC 7454, Feb. 2015. doi: 10.17487/RFC7454.

[96] C. Baloyi, D. P. Du Plessis, T. E. Mathonsi, and T. M. Tshilongamulenzhe, ‘Implementation of an Enhanced Security Algorithm for Detecting Distributed Denial of Services Attacks in Cloud

Computing', in 2022 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA: IEEE, Dec. 2022, pp. 953–957. doi: 10.1109/CSCI58124.2022.00170.

[97] F. Soro, T. Favale, D. Giordano, L. Vassio, Z. Ben Houidi, and I. Drago, 'The New Abnormal: Network Anomalies in the AI Era', in Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning, IEEE, 2021, pp. 261–288. doi: 10.1002/9781119675525.ch11.

[98] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, 'DDoS attack protection in the era of cloud computing and Software-Defined Networking', Computer Networks, vol. 81, pp. 308–319, Apr. 2015, doi: 10.1016/j.comnet.2015.02.026.

[99] C. Yin, Y. Zhu, J. Fei, and X. He, 'A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks', IEEE Access, vol. 5, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[100] H. Zhang, S. Dai, Y. Li, and W. Zhang, 'Real-time Distributed-Random-Forest-Based Network Intrusion Detection System Using Apache Spark', in 2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC), Orlando, FL, USA: IEEE, Nov. 2018, pp. 1–7. doi: 10.1109/PCCC.2018.8711068.

[101] RFC 3954, 'Cisco Systems NetFlow Services Export Version 9', IETF, 2004. Accessed: May 27, 2024. [Online]. Available: https://www.ietf.org/rfc/rfc3954.txt

[102] 'Apache Spark™ – Unified Engine for large-scale data analytics'. Accessed: May 27, 2024. [Online]. Available: https://spark.apache.org/

[103] A. Somasundaram and D. V. S. Meenakshi, 'DDOS Mitigation In Cloud Computing Environment By Dynamic Resource Scaling With Elastic Load Balancing', no. 11, 2021.

[104] K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D. G. Narayan, 'Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud', Procedia Computer Science, vol. 167, pp. 2297–2307, 2020, doi: 10.1016/j.procs.2020.03.282.

[105] 'Open Source Cloud Computing Infrastructure', OpenStack. Accessed: May 27, 2024. [Online]. Available: https://www.openstack.org/

[106] 'OpenStack Docs: Firewall-as-a-Service (FWaaS)'. Accessed: May 27, 2024. [Online]. Available: https://docs.openstack.org/neutron/pike/admin/fwaas.html

[107] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, Applications and Research Challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497-1516, Sep. 2012, doi: 10.1016/j.adhoc.2012.02.016.

[108] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security (CIS), Leshan, China, 2013, pp. 663-667, doi: 10.1109/CIS.2013.145.

[109] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

[110] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," in Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), Hangzhou, China, 2012, pp. 648-651, doi: 10.1109/ICCSEE.2012.373.

[111] A. Mohanty, D. Othman, A. Biswas, and K. Ramamohanarao, "IoT Security Vulnerability: A Case Study of a Web Camera," in Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2019, pp. 1044-1050, doi: 10.1109/UEMCON47517.2019.8993008.

[112] J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312, Third Quarter 2015, doi: 10.1109/COMST.2015.2388550.

[113] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146-164, Jan. 2015, doi: 10.1016/j.comnet.2014.11.008.

[114] P. Kumar and H. Zeadally, "Security and Privacy Issues in Healthcare: IoT Applications," in Security and Privacy in Smart Healthcare: The IoT Era, M. Gaur and V. Srivastava, Eds. Cham, Switzerland: Springer, 2020, pp. 1-36, doi: 10.1007/978-3-030-60385-5_1.

[115] S. Kent, C. Lynn, J. Mikkelson, and K. Seo, "Secure Border Gateway Protocol (Secure-BGP)," IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, pp. 582-592, Apr. 2000.

[116] A. Herzberg and H. Shulman, "Retrofitting Security into BGP," ACM SIGCOMM Computer Communication Review, vol. 44, no. 4, pp. 35-42, Oct. 2014.

[117] J. Moy, "OSPF Version 2," RFC 2328, Apr. 1998.

[118] R. Coltun, D. Ferguson, J. Moy, and A. Lindem, "OSPF for IPv6," RFC 5340, July 2008.

[119] S. Murphy, "OSPF protocol analysis," IETF RFC 1139, Jan. 1990.

[120] M. J. Behringer, "Link-state routing protocols vulnerabilities and solutions," ACM Transactions on Information and System Security (TISSEC), vol. 11, no. 3, pp. 1-32, July 2008.

[121] S. Murphy, M. Badger, "Digital signature protection of the OSPF routing protocol," in Proc. Symposium on Network and Distributed System Security (NDSS), 1996, pp. 93-102.

[122] D. S. Meyers and D. L. Mills, "Advanced Distance Vector Routing: The Enhanced Interior Gateway Routing Protocol," IEEE Commun. Mag., vol. 32, no. 5, pp. 60-66, May 1994.

[123] C. White and D. Masceri, "A study of EIGRP authentication vulnerabilities," J. Netw. Comput. Appl., vol. 36, no. 2, pp. 677-687, Mar. 2013.

[124] S. Kent, C. Lynn, J. Mikkelson, and K. Seo, "Secure Border Gateway Protocol (Secure-BGP)," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 582-592, Apr. 2000.

[125] P. Ferguson and G. Huston, "What is a VPN," Internet Protocol J., vol. 1, no. 1, pp. 2-16, Mar. 1998.

[126] E. Bertino and N. Islam, ‘Botnets and Internet of Things Security’, Computer, vol. 50, no. 2, pp. 76–79, Feb. 2017, doi: 10.1109/MC.2017.62.

[127] A. Kaloxylos, ‘A Survey and an Analysis of Network Slicing in 5G Networks’, IEEE Comm. Stand. Mag., vol. 2, no. 1, pp. 60–65, Mar. 2018, doi: 10.1109/MCOMSTD.2018.1700072

[128] A. Osseiran, J. F. Monserrat, P. Marsch, "5G Mobile and Wireless Communications Technology," Cambridge University Press, 2016.

[129] N. M. M. K. Chowdhury, M. R. Rahman, and R. Boutaba, ‘Virtual Network Embedding with Coordinated Node and Link Mapping’, in IEEE INFOCOM 2009, Rio de Janeiro, Brazil: IEEE, Apr. 2009, pp. 783–791. doi: 10.1109/INFCOM.2009.5061987.

[130] S. Qose, R. Zoltán, ‘Supply Chain in the Context of 5G Technology Security and Legal Aspects’, in 2024 IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics (SAMI), Stará Lesná, Slovakia: IEEE, Jan. 2024, pp. 000143–000148. doi: 10.1109/SAMI60510.2024.10432844.

[131] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon, 'Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations', National Institute of Standards and Technology, Oct. 2021. doi: 10.6028/NIST.SP.800-161r1-draft2.

[132] A. Koutsos, 'The 5G-AKA Authentication Protocol Privacy', in 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden: IEEE, Jun. 2019, pp. 464–479. doi: 10.1109/EuroSP.2019.00041.

[133] T. Sajid, 'Securing 5G Cloud Native NFV Architecture with Zero Trust Security', in 2023 IEEE Future Networks World Forum (FNWF), Baltimore, MD, USA: IEEE, Nov. 2023, pp. 1–5. doi: 10.1109/FNWF58287.2023.10520441.

[134] K. Singh, B. Kumar, R. Saxena, and V. Lohani, 'A Defense in Depth with Zero Trust Architecture for Securing 5G Networks', in 2023 31st Telecommunications Forum (TELFOR), Belgrade, Serbia: IEEE, Nov. 2023, pp. 1–4. doi: 10.1109/TELFOR59449.2023.10372633.

[135] S. Pearson and G. Yee, Eds., Privacy and Security for Cloud Computing. in Computer Communications and Networks. London: Springer London, 2013. doi: 10.1007/978-1-4471-4189-1.

[136] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon, 'Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations', National Institute of Standards and Technology, Oct. 2021. doi: 10.6028/NIST.SP.800-161r1-draft2.

[137] M. Li, M. Huo, X. Cheng, and L. Xu, 'Research and Application of AI in 5G Network Operation and Maintenance', in 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Exeter, United Kingdom: IEEE, Dec. 2020, pp. 1420–1425. doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00212.

[138] T. Wu, 'NETWORK NEUTRALITY, BROADBAND DISCRIMINATION', vol. 2.

[139] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). 2016. Accessed: Jun. 05, 2024. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/2016-05-04/eng

[140] 'Bill Text – AB-375 Privacy: personal information: businesses.' Accessed: Jun. 05, 2024. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[141] X. Yang, D. Clark, and A. W. Berger, 'NIRA: A New Inter-Domain Routing Architecture', IEEE/ACM Trans. Networking, vol. 15, no. 4, pp. 775–788, Aug. 2007, doi: 10.1109/TNET.2007.893888.

[142] Y. Wang, F. Esposito, I. Matta, and J. Day, 'RINA: An Architecture for Policy-Based Dynamic Service Management', Computer Science Department, Boston University, Boston, USA, BUCS-TR-2013-014, Nov. 2013. Accessed: Jun. 06, 2024. [Online]. Available: https://csr.bu.edu/rina/papers/BUCS-TR-2013-014.pdf

[143] Vrijders, S., Staessens, D., Colle, D., Salvestrini, F., Grasa, E., Tarzan, M., and Bergesio, L. (2014). Prototyping the recursive internet architecture: The IRATI project approach. IEEE Network, 28(2), 20–25. https://doi.org/10.1109/MNET.2014.6786609

[144] S. Vrijders, D. Staessens, D. Colle, F. Salvestrini, V. Maffione, L. Bergesio, M. Tarzan-Lorente, B. Gaston, and E. Grasa, 'Experimental evaluation of a Recursive InterNetwork Architecture prototype', in 2014 IEEE Global Communications Conference, Austin, TX, USA: IEEE, Dec. 2014, pp. 2017–2022. doi: 10.1109/GLOCOM.2014.7037104.

[145] [1] D. Sarabia-Jácome, S. Giménez-Antón, A. Liatifis, E. Grasa, M. Catalán, and D. Pliatsios, 'Progressive Adoption of RINA in IoT Networks: Enhancing Scalability and Network Management via SDN Integration', Applied Sciences, vol. 14, no. 6, p. 2300, Mar. 2024, doi: 10.3390/app14062300.

[146] 'IRATI'. Accessed: Jun. 09, 2024. [Online]. Available: https://irati.github.io/stack/

[147] P. B. Godfrey, I. Ganichev, S. Shenker, and I. Stoica, 'Pathlet routing', in Proceedings of the ACM SIGCOMM 2009 conference on Data communication, Barcelona Spain: ACM, Aug. 2009, pp. 111–122. doi: 10.1145/1592568.1592583.

[148] M. Kiermeier, M. Werner, C. Linnhoff-Popien, H. Sauer, and J. Wieghardt, 'Anomaly detection in self-organizing industrial systems using pathlets', in 2017 IEEE International Conference on Industrial Technology (ICIT), Toronto, ON: IEEE, Mar. 2017, pp. 1226–1231. doi: 10.1109/ICIT.2017.7915538.

[149] L. Luo, H. Yu, S. Luo, Z. Ye, X. Du, and M. Guizani, 'Scalable explicit path control in software-defined networks', Journal of Network and Computer Applications, vol. 141, pp. 86–103, Sep. 2019, doi: 10.1016/j.jnca.2019.05.014.

[150] Y. Yoshinaka, J. Takemasa, Y. Koizumi, and T. Hasegawa, 'Design and analysis of lightweight anonymity protocol for host- and AS-level anonymity', Computer Networks, vol. 222, p. 109559, Feb. 2023, doi: 10.1016/j.comnet.2023.109559.

[151] X. Zhang, H.-C. Hsiao, G. Hasker, H. Chan, A. Perrig, and D. G. Andersen, 'SCION: Scalability, Control, and Isolation on Next-Generation Networks', in 2011 IEEE Symposium on Security and Privacy, Oakland, CA, USA: IEEE, May 2011, pp. 212–227. doi: 10.1109/SP.2011.45.

[152] 'GN5-IC1 – GÉANT Intercontinental Connectivity – GÉANT Network'. Accessed: Jun. 23, 2024. [Online]. Available: https://network.geant.org/gn5-ic1/

[153] 'AARC I Authentication and Authorisation for Research and Collaboration – Interoperability, sustainability, integration and compatibility: AARC – a set of turn-key solutions bringing research collaborations closer together.' Accessed: Jun. 23, 2024. [Online]. Available: https://aarc-community.org/

[154] 'REFEDS – The Voice of Research and Education Identity Federations'. Accessed: Jun. 23, 2024. [Online]. Available: https://refeds.org/

[155] 'eduGAIN – enabling worldwide access'. Accessed: Jun. 23, 2024. [Online]. Available: https://edugain.org/

[156] 'Infoshare: SCION Access for Universities and Research Institutes – 24 Nov 2022 | GÉANT CONNECT Online', GÉANT CONNECT Online | The leading collaboration on e-infrastructure and services for research and education. Accessed: Jun. 23, 2024. [Online]. Available: https://connect.geant.org/2022/11/18/infoshare-scion-access-for-universities-and-research-institutes-24-nov-2022

[157] 'Switch', Switch. Accessed: Jun. 23, 2024. [Online]. Available: https://www.switch.ch/en

[158] 'Switch LAN SCION Access', Switch. Accessed: Jun. 23, 2024. [Online]. Available: https://www.switch.ch/en/network/scion-access

[159] 'SCIONLab'. Accessed: Jun. 24, 2024. [Online]. Available: https://www.scionlab.org/

[160] ‘Secure Swiss Finance Network (SSFN)’, SIX. Accessed: Jun. 24, 2024. [Online]. Available: https://www.six-group.com/en/products-services/banking-services/ssfn.html

[161] ‘Anapaya | Secure, resilient, and controlled connectivity with SCION’. Accessed: Jun. 24, 2024. [Online]. Available: https://www.anapaya.net

[162] ‘Anapaya, AWS and InterCloud to Expand SCION network access for Swiss Critical Infrastructure Sectors’. Accessed: Jun. 24, 2024. [Online]. Available: https://www.anapaya.net/news/anapaya-aws-and-intercloud-to-expand-scion-network-access-for-swiss-critical-infrastructure-sectors

[163] ‘Empowering Regulated Customers: Connecting SCION Networks to AWS Environments | AWS in Switzerland and Austria (Alps)’. Accessed: Jun. 24, 2024. [Online]. Available: https://aws.amazon.com/blogs/alps/connecting-scion-networks-to-aws-environments/

[164] ‘InterCloud partners with Anapaya Systems to enable secure cloud connectivity via the SCION Internet’. Accessed: Jun. 24, 2024. [Online]. Available: https://www.anapaya.net/news/intercloud-partners-with-anapaya-systems-to-enable-secure-cloud-connectivity-via-the-scion-internet

[165] ‘Infoshare: SCION Access for Universities and Research Institutes – 24 Nov 2022 | GÉANT CONNECT Online’, GÉANT CONNECT Online | The leading collaboration on e-infrastructure and services for research and education. Accessed: Jun. 23, 2024. [Online]. Available: https://connect.geant.org/2022/11/18/infoshare-scion-access-for-universities-and-research-institutes-24-nov-2022

[166] ‘Switch LAN SCION Access’, Switch. Accessed: Jun. 23, 2024. [Online]. Available: https://www.switch.ch/en/network/scion-access

[167] ‘SCION for secure data transmission’. Accessed: Jun. 24, 2024. [Online]. Available: https://www.swisscom.ch/en/business/enterprise/offer/wireline/scion.html

[168] ‘Sunrise UPC enters partnership with Anapaya Systems and now offers SCION solutions for secure connectivity’. Accessed: Jun. 24, 2024. [Online]. Available: https://www.anapaya.net/news/sunrise-upc-enters-partnership-with-anapaya-systems-and-now-offers-scion-solutions-for-secure-connectivity

[169] ‘New era of data security’. Accessed: Jun. 24, 2024. [Online]. Available: https://aequitec.ch/en/articles/20240417-SSFN

[170] A. Perrig, P. Szalachowski, R. M. Reischuk, and L. Chuat, 'SCION: A Secure Internet Architecture. in Information Security and Cryptography', Springer International Publishing, 2017, doi: 10.1007/978-3-319-67080-5.

[171] D. Barrera, L. Chuat, A. Perrig, R. M. Reischuk, and P. Szalachowski, 'The SCION internet architecture', Commun. ACM, vol. 60, no. 6, pp. 56–65, May 2017, doi: 10.1145/3085591.

[172] J. Postel, 'Assigned Numbers', Internet Engineering Task Force, Request for Comments RFC 790, Sep. 1981. Accessed: Jun. 24, 2024. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc790

[173] J. Reynolds and J. Postel, 'Assigned Numbers', Internet Engineering Task Force, Request for Comments RFC 1340, Jul. 1992. doi: 10.17487/RFC1340.

[174] J. Reynolds and J. Postel, 'Assigned Numbers', Internet Engineering Task Force, Request for Comments RFC 1700, Oct. 1994. Accessed: Jun. 24, 2024. [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc1700.txt.pdf

[175] 'Anapaya | Secure, resilient, and controlled connectivity with SCION'. Accessed: Jun. 26, 2024. [Online]. Available: https://www.anapaya.net/

[176] Anapaya, 'SCION Technology: Transformation and Optimization of your Connectivity Whitepaper'. Accessed: Jun. 27, 2024. [Online]. Available: https://content.anapaya.net/swisscom-intercloud-anapaya_white_paper

[177] N. Rustignoli and C. de Kater, 'SCION Components Analysis', Internet Engineering Task Force, Active Internet Draft, Sep. 2023. Accessed: Jun. 30, 2024. [Online]. Available: https://www.ietf.org/archive/id/draft-rustignoli-panrg-scion-components-03.txt

[178] C. de Kater, N. Rustignoli, and S. Hitz, 'SCION Data Plane', Internet Engineering Task Force, Active Internet Draft, Mar. 2024. Accessed: Jun. 30, 2024. [Online]. Available: https://www.ietf.org/archive/id/draft-dekater-scion-dataplane-01.txt

[179] 'EPIC for Hidden Paths — SCION documentation'. Accessed: Jul. 01, 2024. [Online]. Available: https://docs.scion.org/en/latest/dev/design/EPIC.html

[180] 'COLIBRI Service Design — SCION documentation'. Accessed: Jul. 01, 2024. [Online]. Available: https://docs.scion.org/en/latest/dev/design/ColibriService.html

[181] J. Kwon et al., ‘SCIONLAB: A Next-Generation Internet Testbed’, in 2020 IEEE 28th International Conference on Network Protocols (ICNP), Madrid, Spain: IEEE, Oct. 2020, pp. 1–12. doi: 10.1109/ICNP49622.2020.9259355.

[182] ‘SCION Education, Research and Academic Network — SCIERA 0.1 documentation’. Accessed: Jul. 05, 2024. [Online]. Available: https://sciera.readthedocs.io/en/latest/

[183] ‘ISD and AS Assignments — Anapaya Knowledge Base documentation’. Accessed: Jul. 05, 2024. [Online]. Available: https://docs.anapaya.net/en/latest/resources/isd-as-assignments/#europe