ECCO
European Cybersecurity COmmunity

Security by Design through the Recursive InterNetwork Architecture

European Cybersecurity Competence Centre (ECCC) ECCO

Community Group on Human Factors

23 October 2024

ECCO
European Cybersecurity COmmunity

European Cybersecurity Competence Centre (ECCC) ECCO

Community Group on Human Factors

Kai Rannenberg / Narges Arastouei

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

Objectives

- Build a community of experts and "end users" for the WG domain by initiating work on a sequence of prioritized topics in the WG domain
- Support selected actions prioritised in the ECCC Strategic Agenda matching the WG domain, especially within
  - 1.1.4 Ensure the availability of easily accessible and user-friendly cybersecurity tools for SMEs
  - 1.2.3 Promote security and privacy 'by design'
  - 2.1.4 Promote security and privacy 'by design' approach in training and education

Methodology

- Start with actions related to one or several of the topics listed in the ECCO technical offer:
  - 5G applications, ICT in mobility, security of day-to-day tools like smartphones, web meeting systems and services, Internet access technologies, digital money.
- Deep dive on proposals for priorities for DEP or other appropriate support measures
- Build sub-groups as needed
- …

Matching: ECCC Strategic Agenda actions Topics from Technical Offer

Action/Topic	1.1.4 Ensure the availability of easily accessible and user-friendly cybersecurity tools for SMEs	1.2.3 Promote security and privacy 'by design'	2.1.4 Promote security and privacy 'by design' approach in training and education
5G applications			
ICT in mobility			
Security of day-to-day tools, e.g.			
Smartphones			
Web meeting systems and services			
Internet access technologies			
Digital money			
…			
…			

Work on topics within the matrix prioritized by the community of experts and "end users"

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

Activities and deliverables

- Identification of relevant achievements / best practices (e.g. developed in the ECCC pilots) to address the Strategic Agenda
  - 1st Webinar (March 8): **A Footprint of CyberSec4Europe: two prominent cybersecurity tools (Keynotes: Vashek Matyas et al, Masaryk University Brno, CZ)**
  - 2nd Webinar (May 22): **Security-by-design for SMEs exploiting trusted hardware (Keynote: Antonio Lioy, Politecnico di Torino, IT)**
  - 3rd Webinar (19 June): **Engaging Citizens and Civil Society in Cybersecurity (Dr. Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research)**
  - 4th Webinar (23 July): **LINDDUN GO, Lightweight & Gamified Privacy Threat Modeling (by Jonah Bellemans at the DistriNet Research Group of KU Leuven (Belgium)).**
  - 5th Webinar (16 September): **From Awareness to Action: Enhancing Parental Engagement in Online Privacy Protection (by Ann-Kristin Lieberknecht at Goethe University Frankfurt)**
- Today's webinar (23 October): **Security by Design through the Recursive InterNetwork Architecture [by Toktam Ramezanifarkhani, Associate Professor in Cyber security School of Economics, Innovation and Technology | Oslo, Kristiania University college & Peyman Teymoori, Associate Professor ,University of South-Eastern Norway (USN)]**

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

Activities and deliverables

- Recommendations for future specific priority "Joint Actions" (e.g. DEP projects) and other actions for the ECCC
  - Based on matching of goals with action types also considering the ECCC action plan
- Possible cooperation in immediate Joint Actions
  - Deep dive on specific topics: e.g. stemming from the needs of SMEs for easily accessible and user-friendly cybersecurity tools considering privacy
- Knowledge sharing events: presentations for EC, NCCs, ECCC
  - Webinars on the progress including refinement of the topics

ECCO
European Cybersecurity COmmunity

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

How to join the CG

- Email: community_humanfactors-owner@list.cyber-ecco.eu with your
  - Contact details
  - Affiliation and role therein
  - Area of expertise

Keynote & Speaker

• Security by Design through the Recursive InterNetwork Architecture

This webinar will focus on the growing importance of embedding security by design within modern network architectures. As cybersecurity challenges continue to evolve, there is a critical need for robust, scalable solutions that address vulnerabilities across diverse sectors. The session will highlight the potential of the Recursive InterNetwork Architecture (RINA) in mitigating such vulnerabilities, creating collaboration within the European cybersecurity community, and exploring pathways for future research and strategic initiatives in alignment with EU priorities.

• Keynote Speakers: Toktam Ramezanifarkhani & Peyman Teymoori

- **Toktam Ramezanifarkhani** received her MSc and PhD in information security and is an Associate Professor in Cyber Security at Kristiania University College and adjunct professor at University of Oslo, Department of Informatics. Her research interest is the wide area of Information Security including but not limited to Software and Language-Based Security, Network Security, Information Security Management, and Human Aspects of Information Security. She has been involved in several international and EU projects working with industrial and academic partners.
- **Peyman Teymoori** is an Associate Professor in Computer Science at the University of South-Eastern Norway (USN), with a Ph.D. in computer science, specializing in wireless ad hoc networks. Before joining USN, he was a Senior Research Fellow at the University of Oslo. His research focuses on the modeling, optimization, and performance evaluation of communication networks, including emerging technologies such as 5G/6G and the Internet of Things (IoT). He also explores Recursive InterNetwork Architecture (RINA) and network technologies that bridge theoretical and practical advancements in communication systems.

ECCO
European Cybersecurity COmmunity

ECCO Community-driven Knowledge Sharing Events

Disclaimer

- *These sessions are ECCOcommunity-driven and expert-led, reflecting the collective knowledge and contributions of the members of the ECCO Community Groups. They are designed as knowledge-sharing events to build/animate the cybersecurity Community Groups on key topics and share valuable insights among stakeholders.*
- *The information and opinions in this document are provided "as is" for general purposes only.*
- *Experts are encouraged to ensure their presentations are accurate and up-to-date.*
- *The views expressed in this webinar are purely those of the experts and may not, in any circumstances, be interpreted as stating an official position of the European Commission (EC), the European Cybersecurity Competence Centre (ECCC), the ECCO project, or any other EU institution, body or agency. The European Commission does not guarantee the accuracy of the information included in this webinar, nor does it accept any responsibility for any use thereof.*
- *References to specific commercial products, processes, or services do not imply endorsement or recommendation, and this webinar should not be used for advertising purposes.*

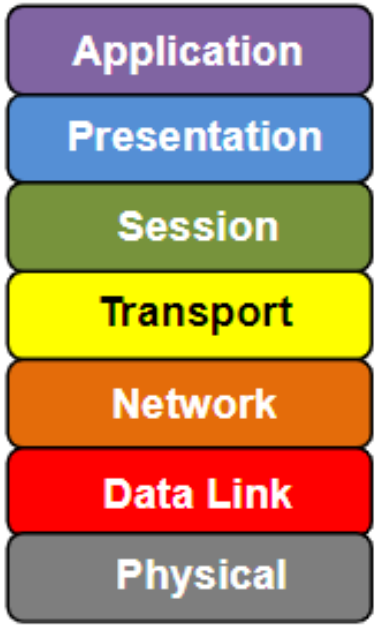
Security by Design through the Recursive InterNetwork Architecture

Toktam Ramezanifarkhani, *Kristiania University College (KUC)* &
Peyman Teymoori, *University of South-Eastern Norway (USN)*, 23 Oct 2024

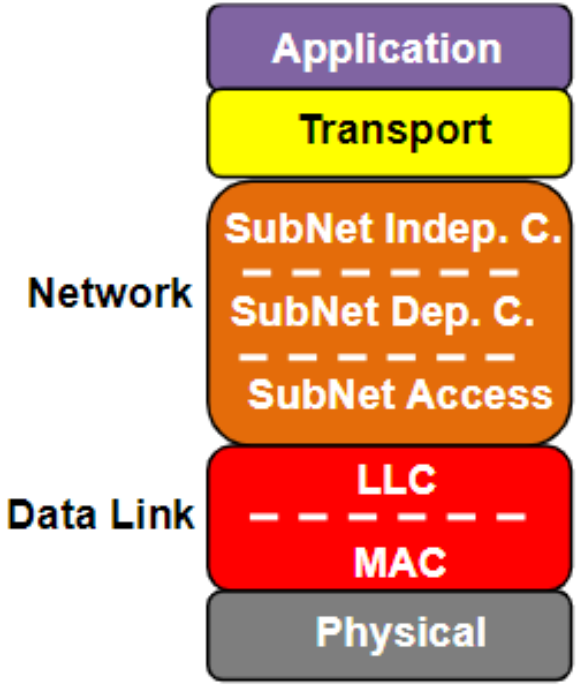
Overview

- OSI architecture model and TCP/IP
- IoT network stack
- Security challenges of current stacks
- Recursive InterNetwork Architecture (RINA)
- Future work

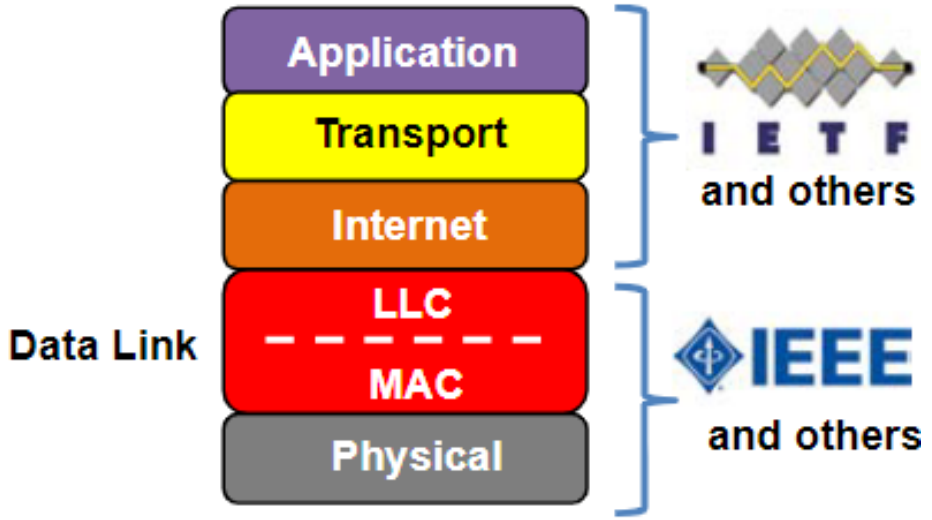
The OSI Model



OSI (Initial)

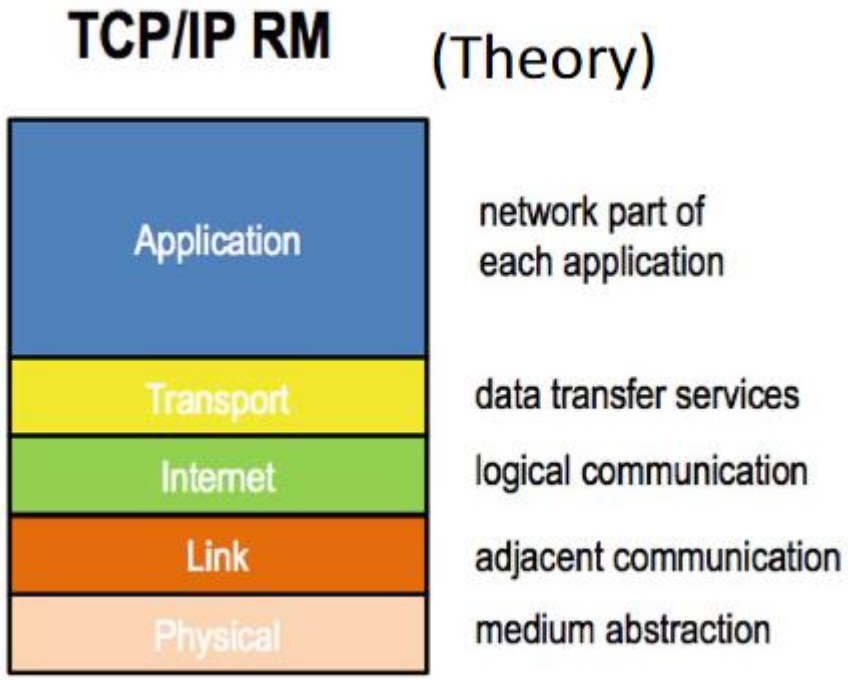


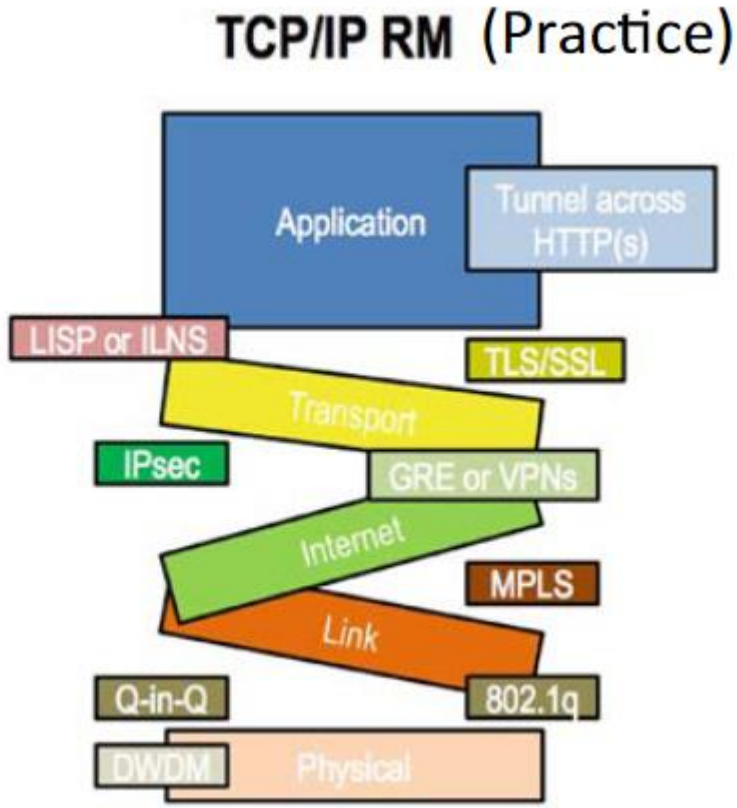
OSI (Final)



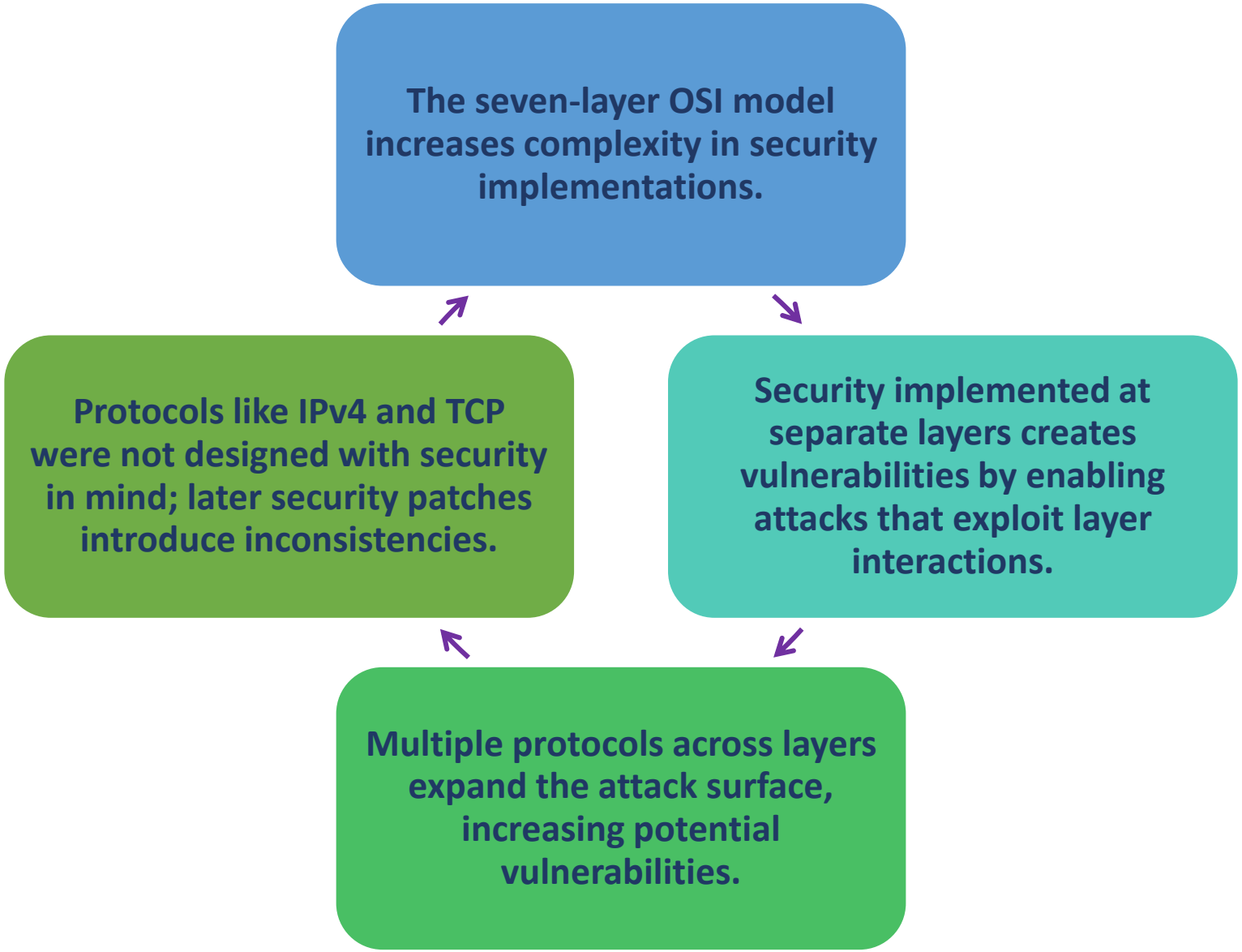
Internet (theory)

The OSI Model





Security Challenges in OSI

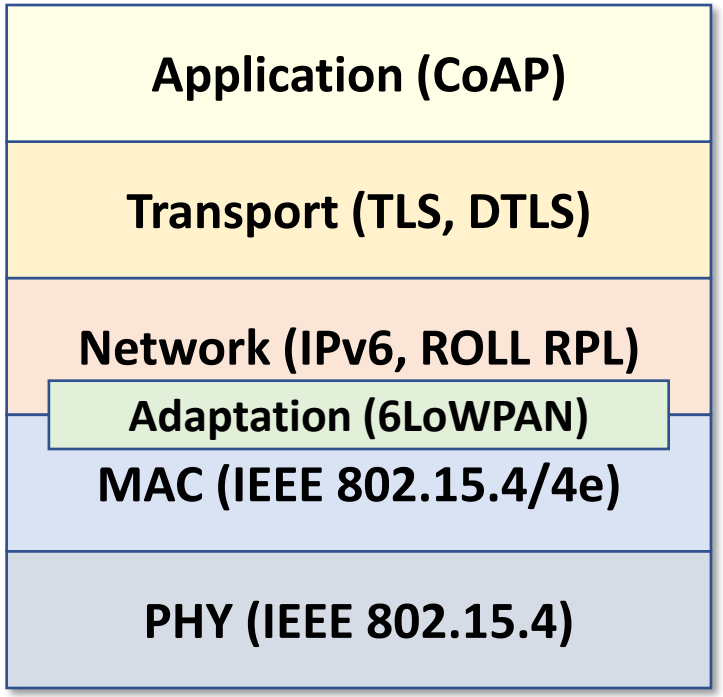


Internet of Things Network Stack

- A typical IoT network stack with common protocols

- **CoAP**: web transfer at the application layer over UDP (DTLS).
- **TLS and DTLS**: transport layer security using TCP and UDP,
- **RPL**: routing over 6LoWPAN,
- **6LoWPAN**: transmission of IPv6 over IEEE 802.15.4,
- **IEEE 802.15.4** as MAC/Physical layer

- **Resembles TCP/IP!**



IoT Challenges

Connected Devices Growth:

- The number of connected devices is projected to exceed 40 billion by 2040, with hyperconnectivity playing a critical role in daily life and global infrastructure.

Diversity of Services:

- Various domains such as smart cities, autonomous vehicles, and space technologies will rely on a wide range of configurations and services.

The Risk:

- The immense scale of connected devices poses significant challenges for maintaining security across billions of endpoints.

IoT Security Challenges: Network Stack

Heterogeneity and Interconnectivity:	• IoT environments consist of diverse devices with varying operating systems, protocols, and hardware, complicating seamless interconnectivity and compatibility.
Security Vulnerabilities Across Layers:	• Each IoT layer (e.g., perception, network, application) has unique vulnerabilities, such as inadequate authentication and encryption, especially at the network layer.
Protocol Overhead:	• Traditional protocols, like 6LoWPAN, lack inherent security mechanisms and have excessive overhead, leading to the need for lightweight alternatives.

IoT Security Challenges: Network Stack

Repeated Functionality in Layers/Protocols:

- Security functions often need to be implemented multiple times across different layers within a protocol, leading to redundancy.

Global, Public, and Large Address Space:

- The extensive size of public address spaces complicates adoption and increases security challenges, as identifying and managing target addresses becomes more difficult.

Security and Performance Enhancement Conflict:

- Performance improvements, such as those in CoAP gateways, can be negatively impacted by adding security features, especially at the transport layer.

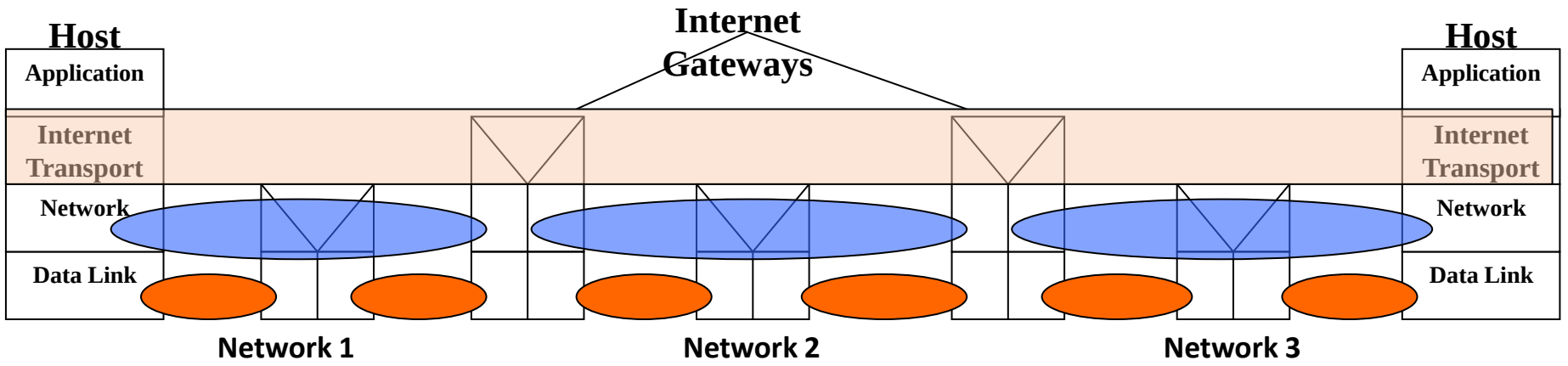
IoT Security Challenges: Network Stack

Attack Repetition:	Recent large-scale attacks like DDoS on IoT devices demonstrate how older attack methods are being revived with even greater impact.
Future Extensions:	Securing one IoT protocol or layer does not guarantee compatibility with other protocols or future extensions, such as mobility, multicast, or quality of service (QoS).
Domain Synergy:	The diversity of protocols and policies across different domains introduces new challenges in managing communication within cross-domain applications and heterogeneous environments.

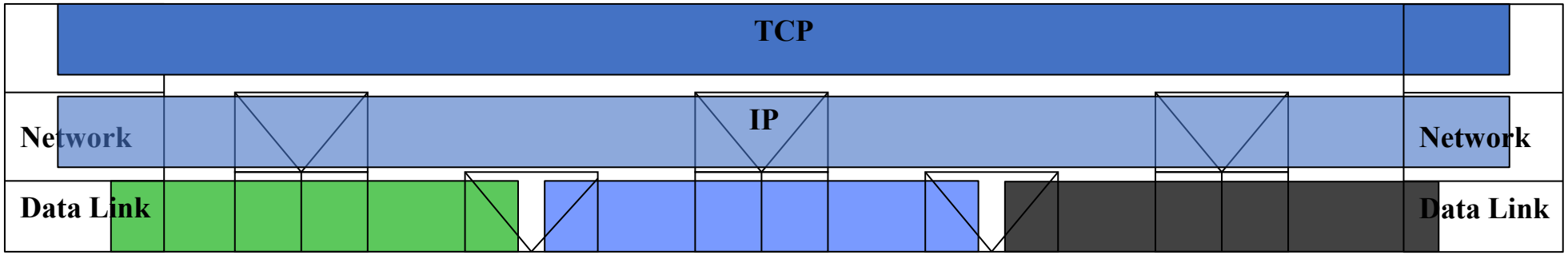
Recursive InterNetwork Architecture (**RINA**)

“The Internet Lost a Layer”

- INWG’s Internet Model in the 70’s:

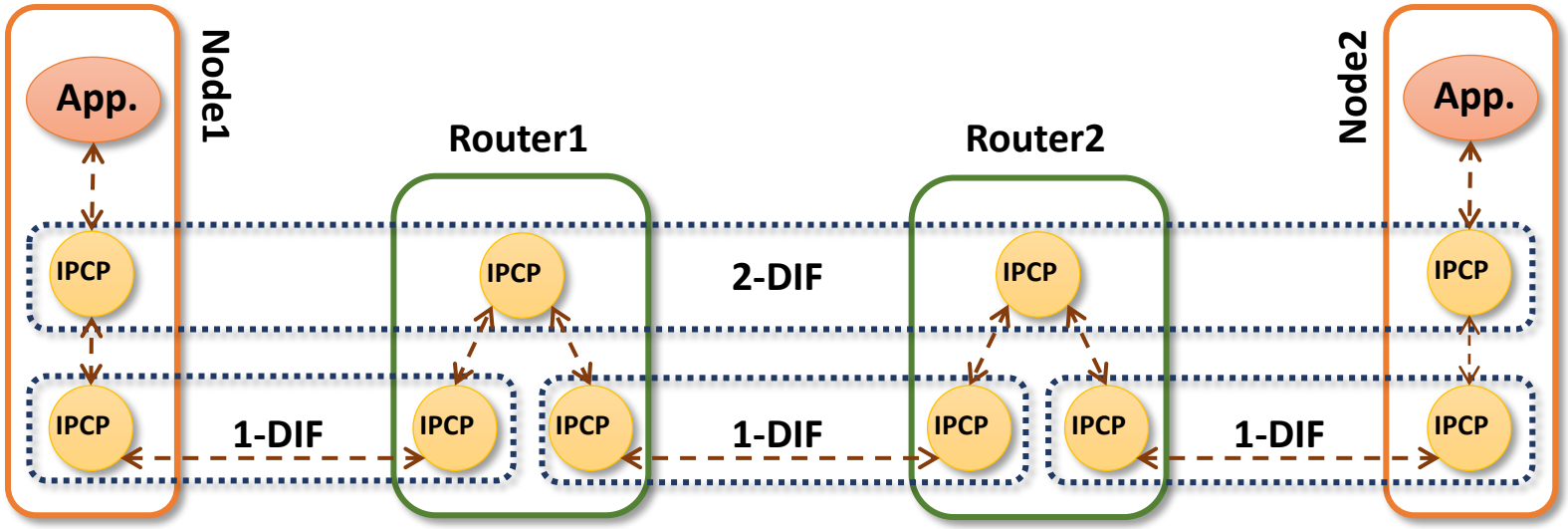


- Let’s look at today’s “Internet”: IP and TCP were split, but …



RINA Foundation

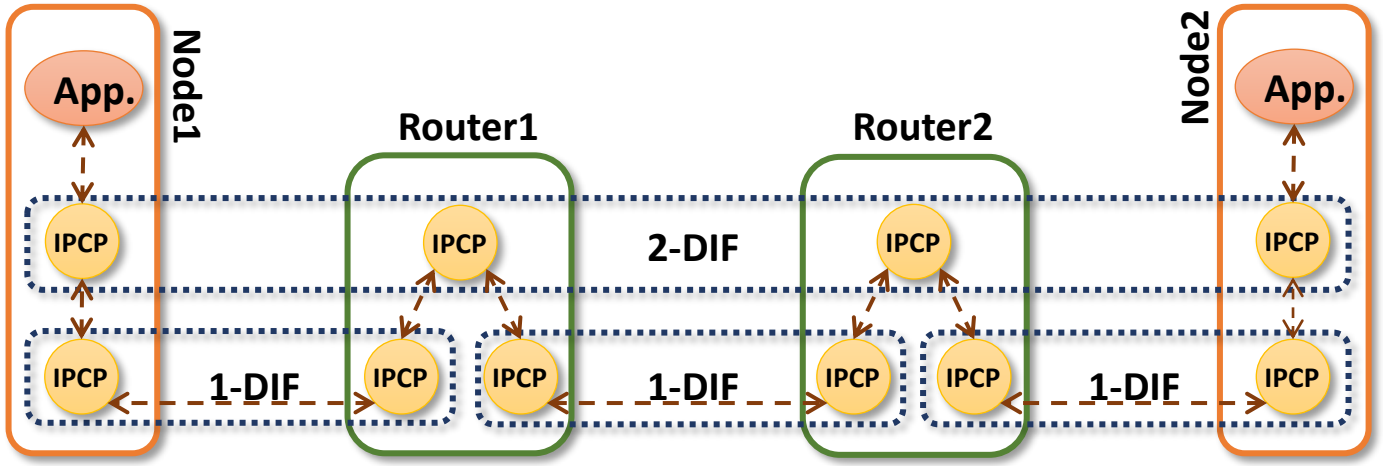
- Presented by John Day in "*Patterns in Network Architecture: A Return to Fundamentals*"
- Each layer is called Distributed IPC Facilities (DIF) consisting of fixed mechanisms, and can be programmed through policies on-the-fly; policies determine how mechanisms operate
- Employs a secured layer with basic IPC mechanisms (i.e., necessary functionalities)
- Through a common API, administrator is allowed to arrange/stack these layers as needed recursively.



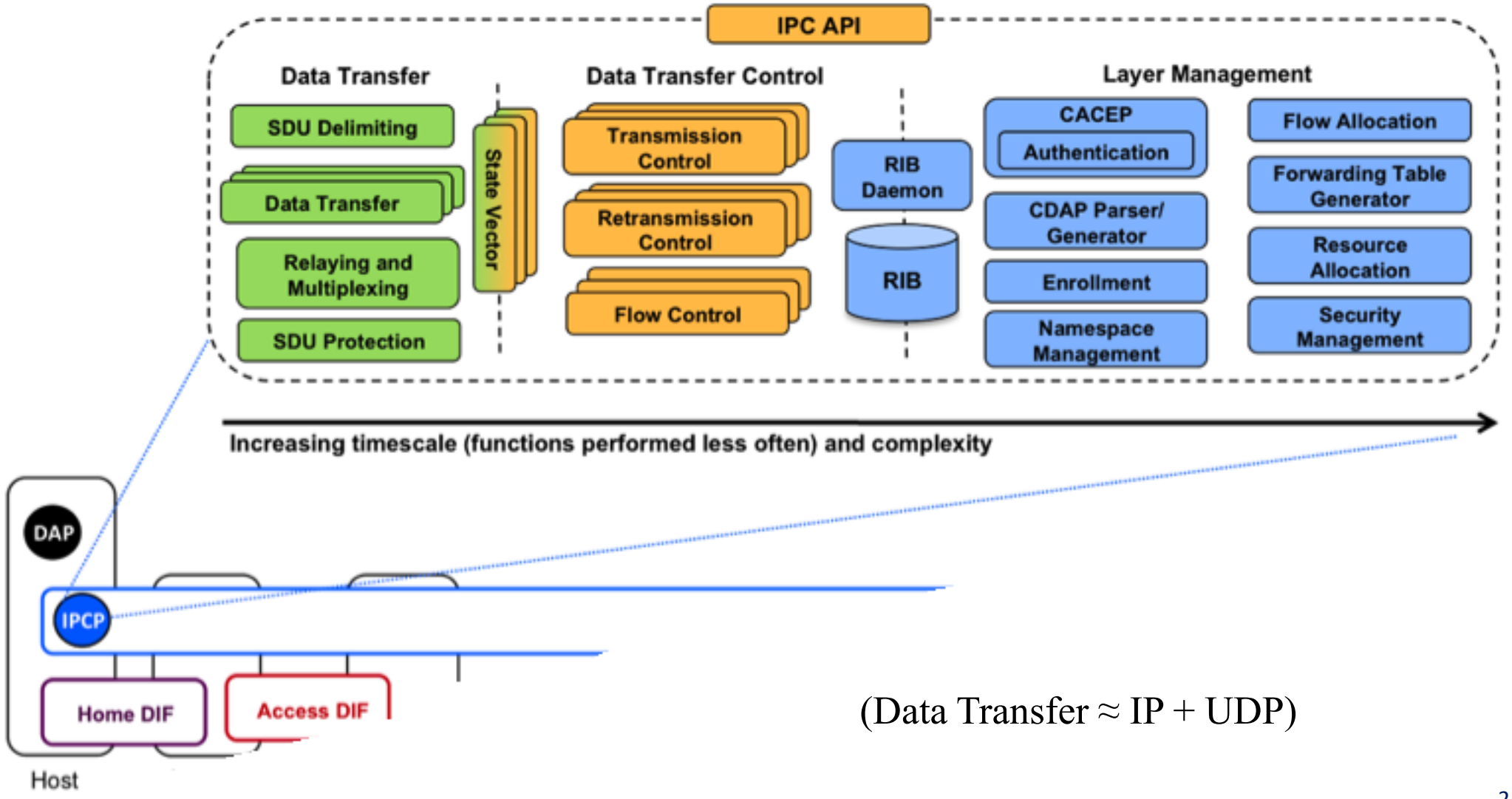
A sample RINA topology with two end-nodes and two routers. Every IPCP has the same internal structure.

IPC in RINA

- Adopts the foundation of networking:
  - *"Networking is Inter-Process Communication (IPC)"*. Robert Metcalfe, 1972
- What is IPC?
  - a mechanism for establishing a connection between processes, running on two computers or on a single multitasking computer, to allow data to flow between those processes.
- RINA's view on IPC:
  - "both the *transport* and *internetworking* tasks together constitute an IPC service to application processes",
  - "we need to repeat such an IPC service over different regions/scopes."

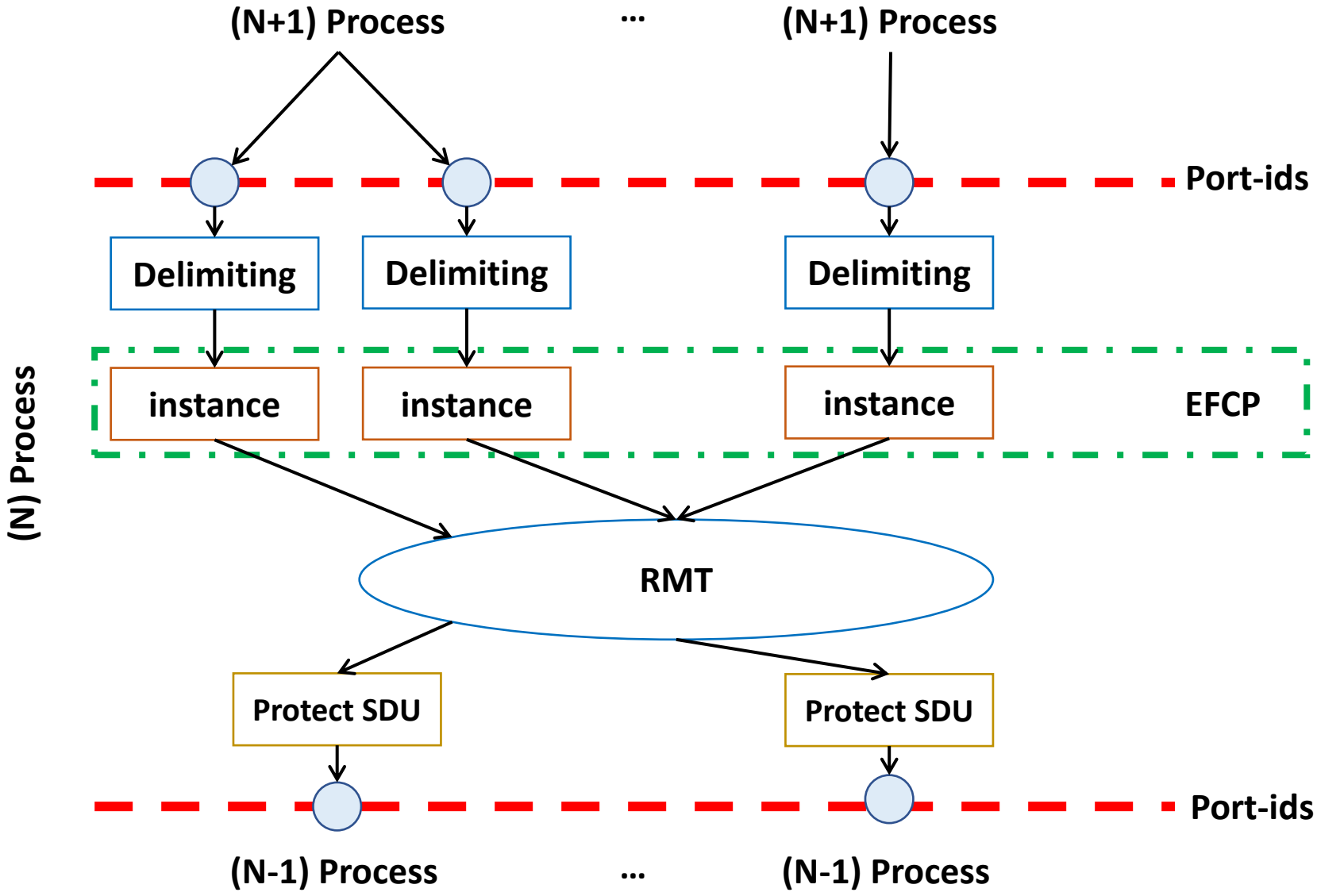


How an IPCP Looks Like



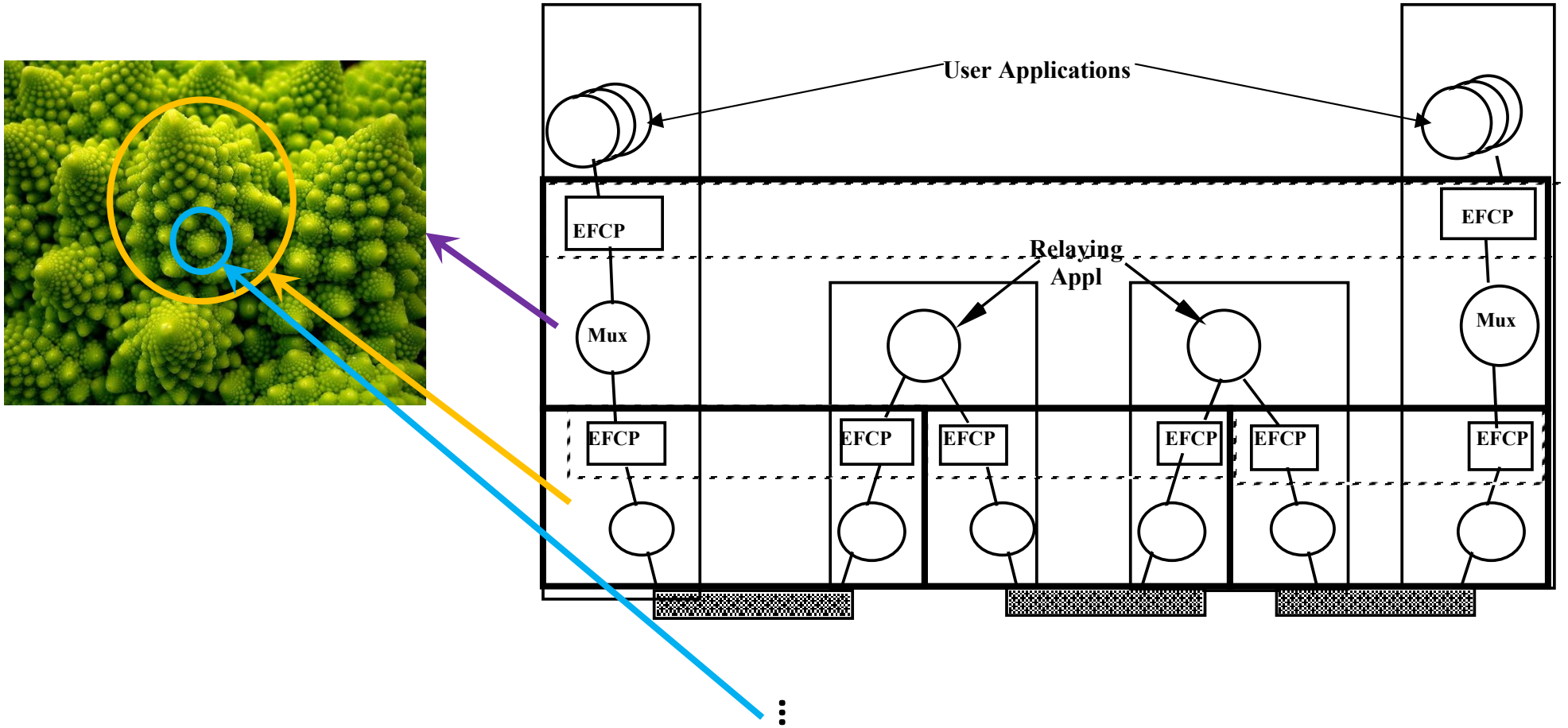
(Data Transfer ≈ IP + UDP)

IPC Process (IPCP)



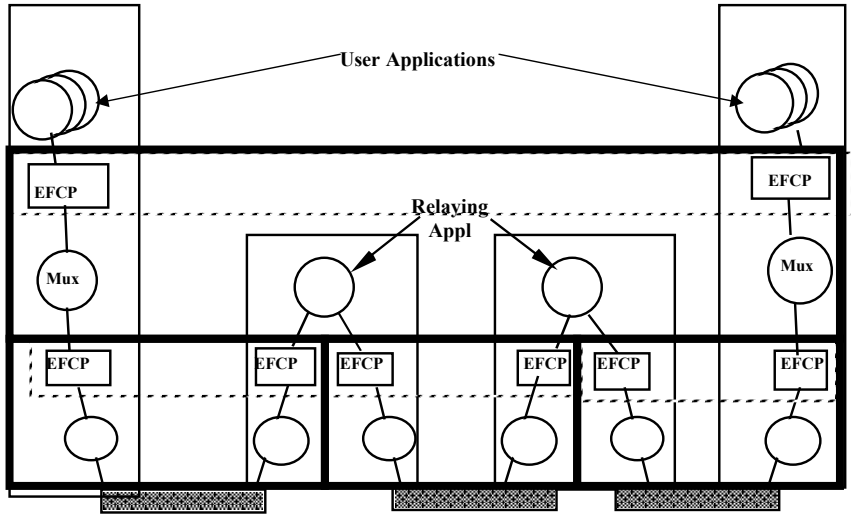
The IPC Model

In RINA, layers are fractals!



The Implications*

- Networking is IPC *and only IPC*.
- All layers have the same functions, but different scope.
- Not all instances of layers may need all functions, but don't need more.
- A Layer is a Distributed Application that provides and manages IPC.
  - A Distributed IPC Facility (DIF)

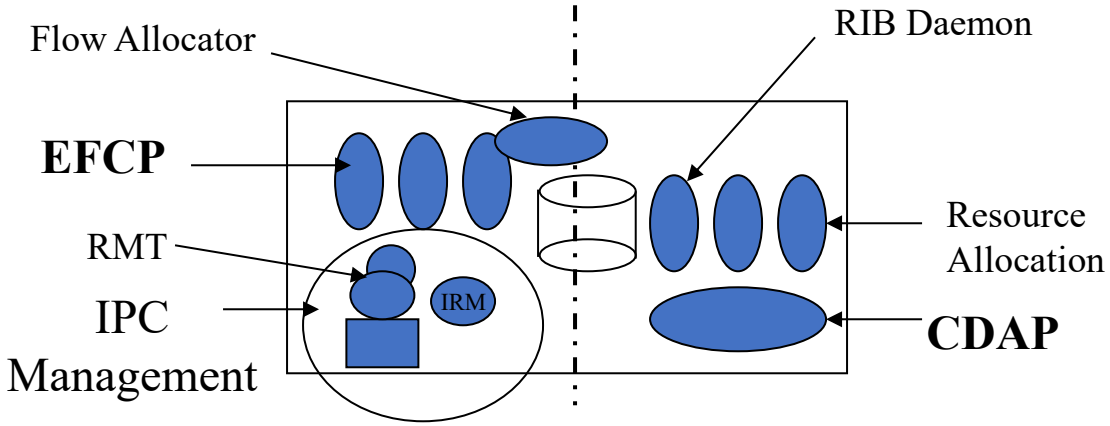


- This yields a theory and an architecture that is simple, elegant, and scales indefinitely.
- This is a distributed computing model, not a Telecom or Data comm model.
  - the Internet (and all the diagrams today) emphasize boxes, when they should be emphasizing layers, as a Distributed Application that does IPC.

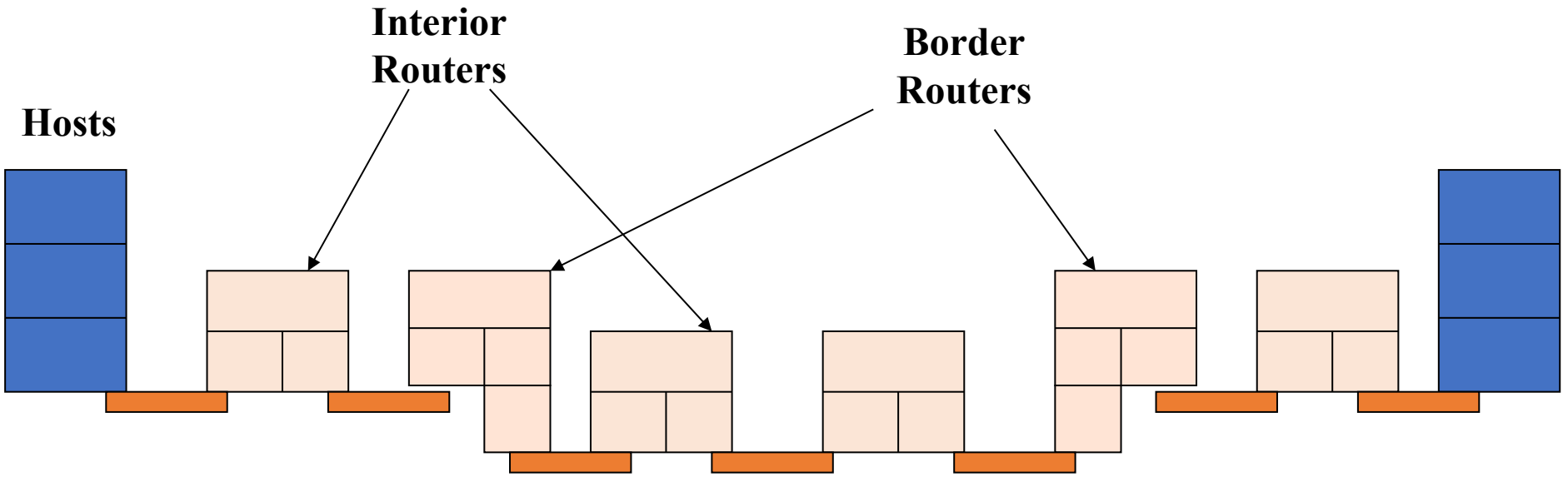
* John Day, Ibrahim Matta, and Karim Mattar. "Networking is IPC: a guiding principle to a better internet," *In Proceedings of the 2008 ACM CoNEXT Conference (CoNEXT '08)*. Association for Computing Machinery, New York, NY, USA, Article 67, 1–6. https://doi.org/10.1145/1544012.1544079.

What are the Protocols?

- Only two:
  - A data transfer protocol, **EFCP**, based on delta-t with mechanism and policy separated. This provides both unreliable and reliable flows.
    - separating mechanism and policy
  - The common application protocol based on **CDAP**:
    - Transition from an IPC Model to a Programming Model
    - 6 Fundamental Operations on Objects.
    - Assembler for Distributed Applications



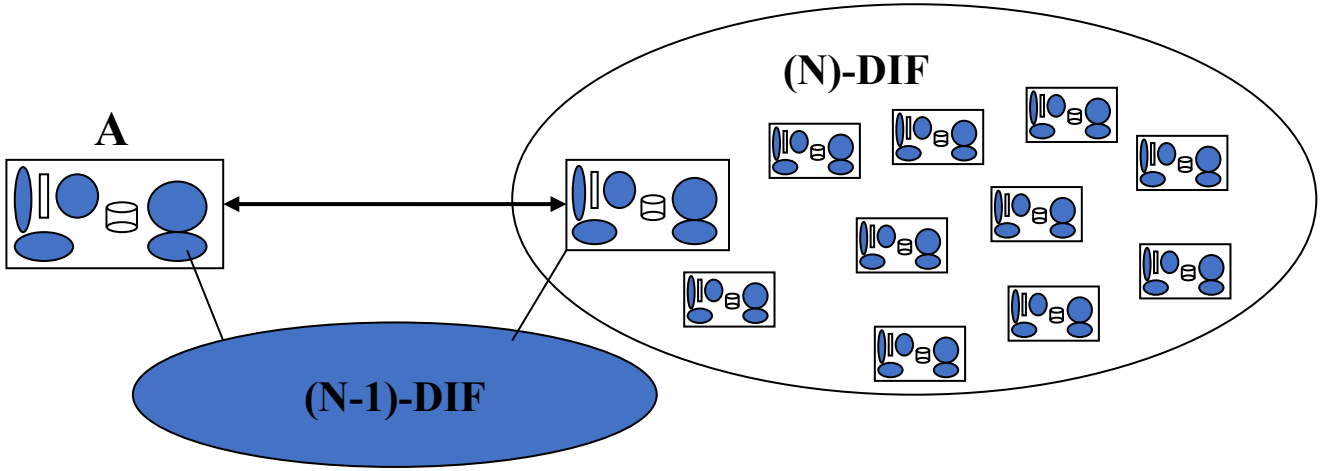
Only Three Kinds of Systems



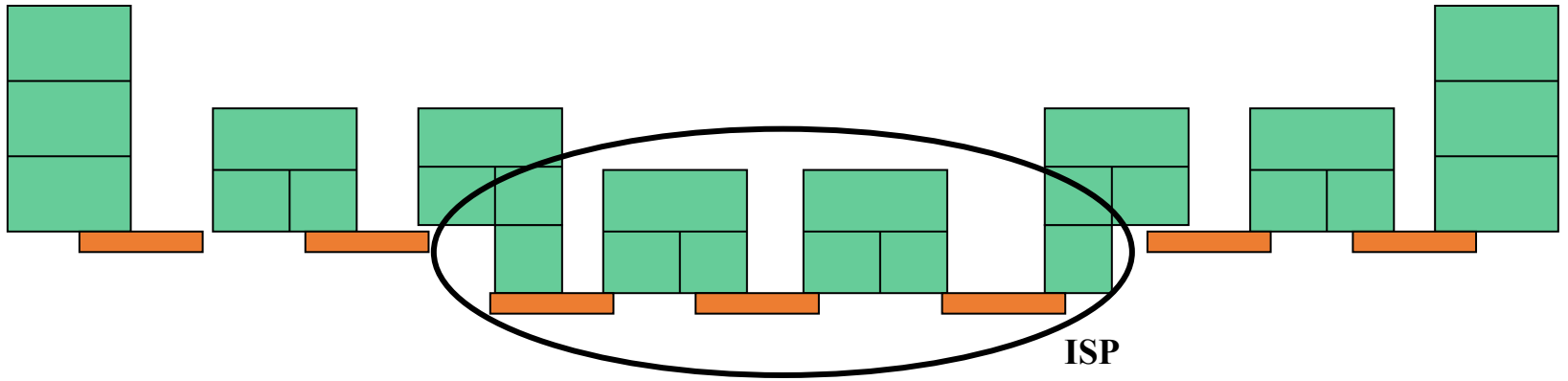
- Middleboxes? No middleboxes!
- NATs: again, no!
- Firewalls: well, no!
- Hosts may have more layers, depending on what they do.

How Does It Work?

- Enrollment or Joining a Layer:
  - Authenticating that A is a valid member of the (N)-DIF
  - Initializing it with the current information on the DIF
  - Assigning it a synonym to facilitate finding IPC Processes in the DIF, i.e., an address



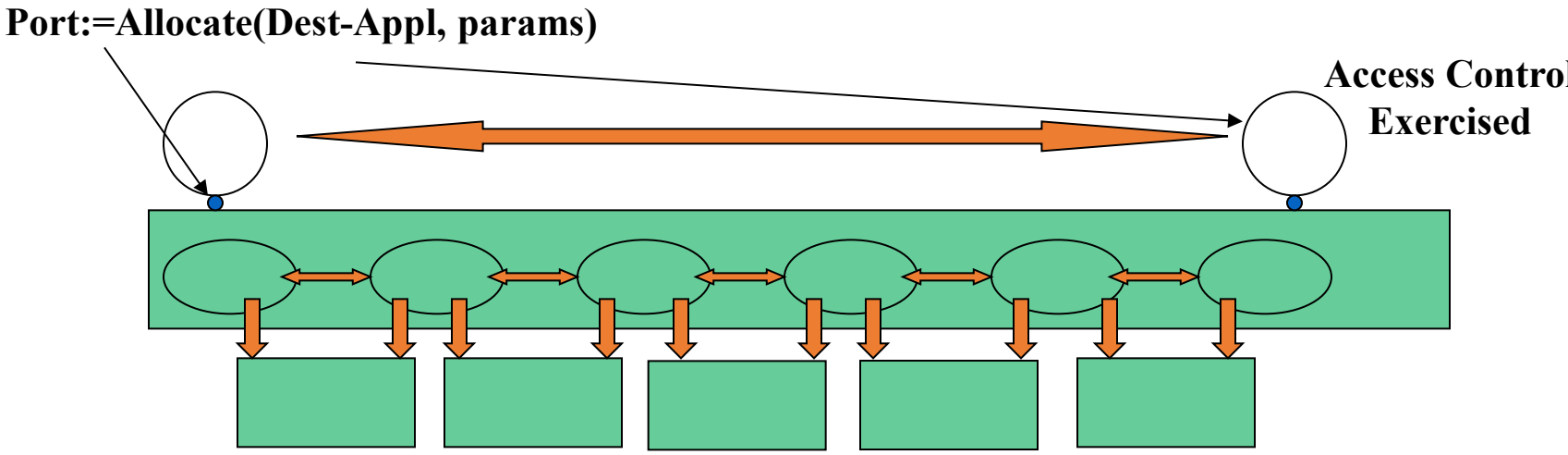
How Does It Work? Security



Hosts and ISPs do not share DIFs.
(ISP may have more layers)

- Security by isolation.
- Hosts can not address any element of the ISP.

How Does It Work? Security



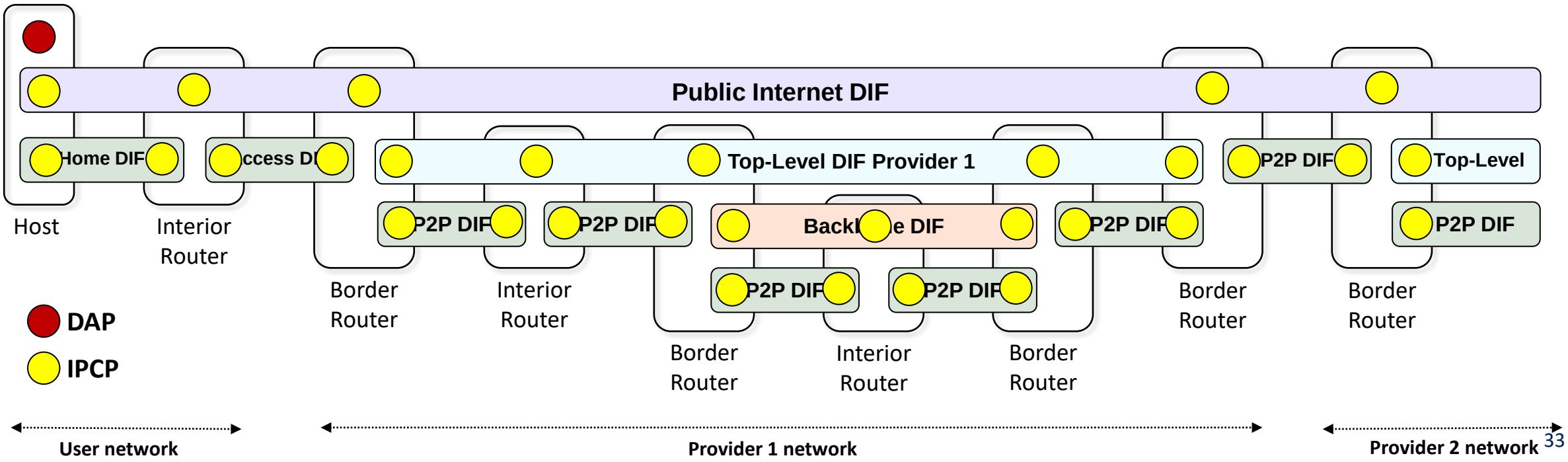
- A DIF is a securable container.
  - The DIF is the firewall!
- RINA security is considerably less complex than the current Internet security
  - Only doing a rough estimate counting protocols and mechanisms*

* J. Small (Boston University). "Patterns in Network Security: An analysis of architectural complexity in securing Recursive Inter-Network Architecture Networks". Master Thesis, 2012.

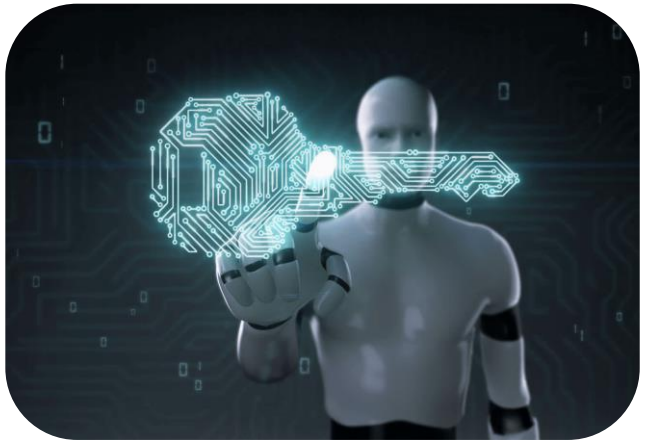
Security Implications

- Secure Distributed IPC Facilities (DIFs)
- Hidden Addresses
- Decoupled Synchronization and Port Allocation
- Port-Independent Communication
- Authentication
- Access Control

- Soft-State Connection Management
- Connection Management Independent Authentication
- Variable Address Space
- Multi-Layer Security
- Communication Through a Common DIF
- Insiders Resistance

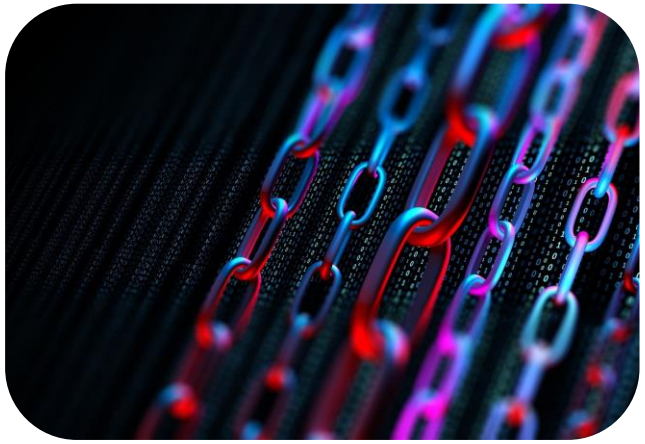


RINA for Emerging Technologies



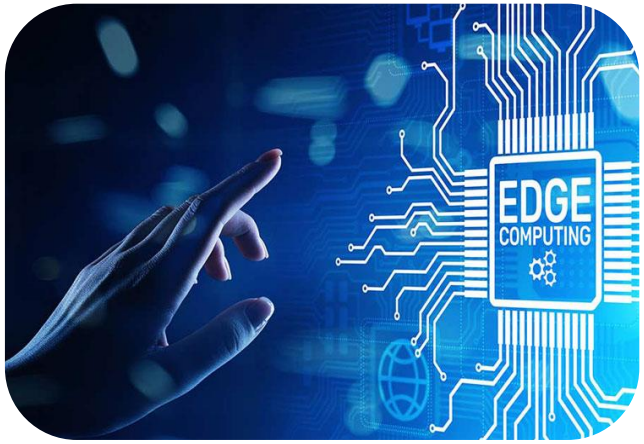
AI-Driven Security:

- **Challenge**: Integration of AI/ML in IoT networks introduces new attack vectors
- **RINA Solution**: RINA's multi-layer security approach (ML) creates multiple barriers against adversarial attacks.



Blockchain for IoT:

- **Challenge**: Scalability and energy consumption issues in resource-constrained environments
- **RINA Solution**: Efficient layering and customizable DIFs can improve blockchain integration



Edge Computing:

- **Challenge**: Decentralized security controls and data protection at network edge
- **RINA Solution**: Multi-layer security approach and secure DIFs can protect edge computations

RINA for Emerging Technologies

Massive IoT:

- **Challenge**: Secure management of billions of endpoints
- **RINA Solution**: Scalable addressing scheme and efficient security policies

Cognitive IoT:

- **Challenge**: Ensuring integrity of autonomous decision-making processes
- **RINA Solution**: Layered security and programmable DIFs protect cognitive functions

RINA: Promoting Security by Design

Design Principles:	Multi-Layer Security,
	Policy-Driven Security,
	Isolation and Minimal Exposure.
Education and Training:	RINA's principles can be used to teach security-by-design concepts, promoting a more intuitive understanding of network security.
Future Research:	While RINA is a network architecture, its recursion and security-by-design principles can inspire similar approaches in other areas of cybersecurity.

Thank you!

toktam.ramezanifarkhani@kristiania.no
peyman.teymoori@usn.no

References

[1] J. Day, "How in the Heck do you lose a layer!?," 2011 International Conference on the Network of the Future, 2011, pp. 135-143, doi: 10.1109/NOF.2011.6126673.

[2] John Day, Ibrahim Matta, and Karim Mattar. “Networking is IPC: a guiding principle to a better internet,” In Proceedings of the 2008 ACM CoNEXT Conference (CoNEXT '08). ACM, New York, NY, USA, Article 67, 1–6. https://doi.org/10.1145/1544012.1544079.

[3] John Day, “How in the Hell Do You Lose a Layer?!!”, Invited talk, Oslo, Oct 2019.

[4] John, Day, Patterns in network architecture: a return to fundamentals, Pearson, ISBN: 9780132252423, 2007.

[5] J. Day et al., "Bounding the router table size in an ISP network using RINA," 2011 International Conference on the Network of the Future, 2011, pp. 57-61, doi: 10.1109/NOF.2011.6126683.

[6] J. Small (Boston University). "Patterns in Network Security: An analysis of architectural complexity in securing Recursive Inter-Network Architecture Networks". Master Thesis, 2012.

[7] Ishakian, Vatche, et al. "On supporting mobility and multihoming in recursive internet architectures." Computer Communications 35.13 (2012): 1561-1573.

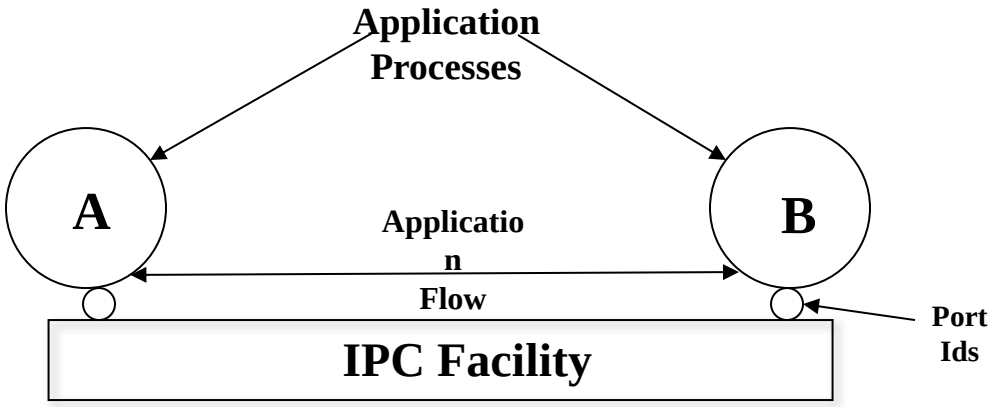
[8] Handley, Mark. "Why the Internet only just works." BT Technology Journal 24.3 (2006): 119-129.

[9] ETSI, “Next Generation Protocols (NGP); An example of a non-IP network protocol architecture based on RINA design principles”, ETSI GR NGP 009 V1.1.1, 2019. [online:] https://www.etsi.org/deliver/etsi_gr/NGP/001_099/009/01.01.01_60/gr_ngp009v010101p.pdf

[10] Ramezanifarkhani, Toktam, and Peyman Teymoori. "Securing the Internet of Things with recursive InterNetwork architecture (RINA)." *2018 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2018.

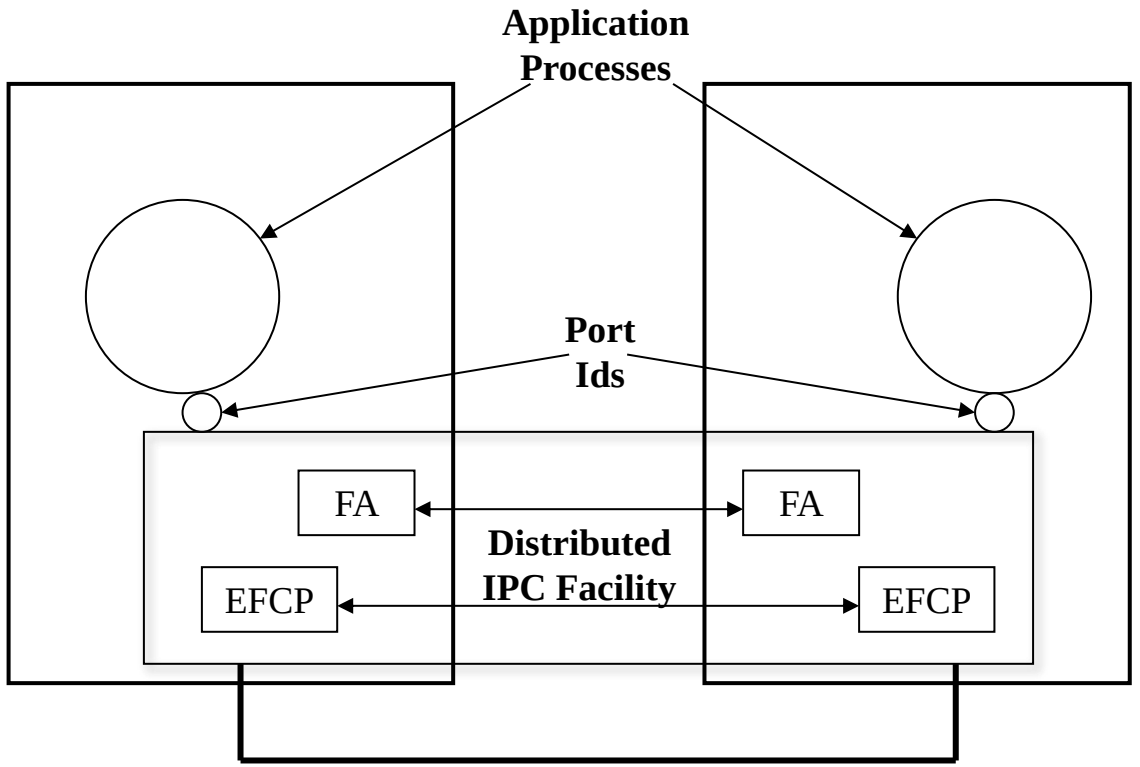
Starting with the Basics

- Two applications communicating in the same system:
- This establishes the API.
- The Application should not be able to distinguish a slow correspondent from operating over the network.



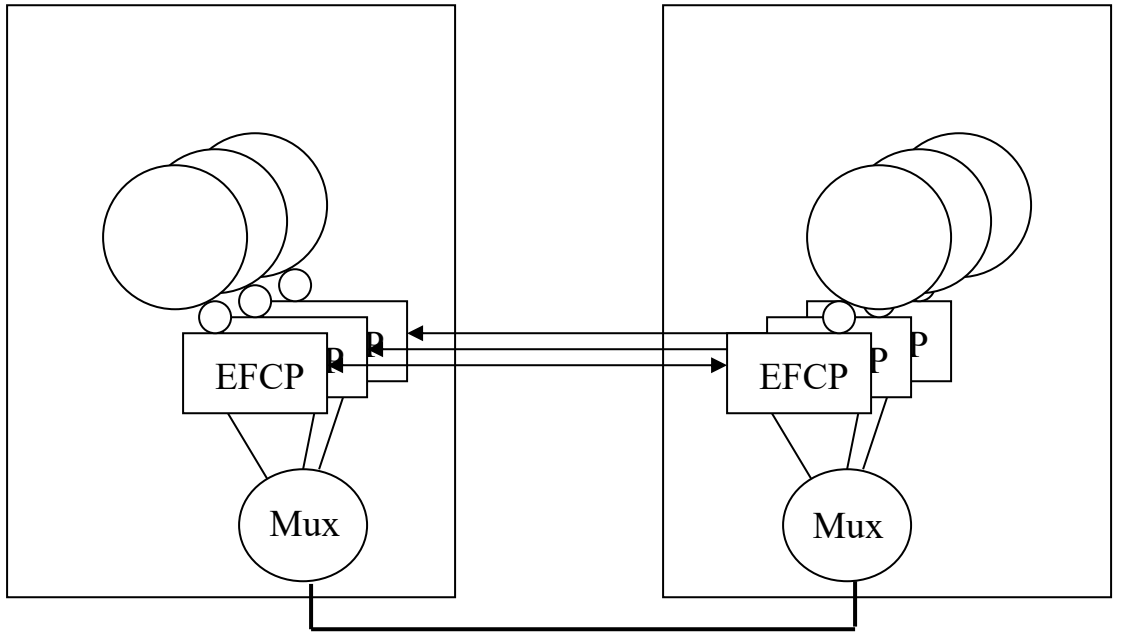
Extending to Two Nodes

- Management: the first capability needed to find the other application.
- Then, some sort of error and flow control protocol to transfer information between the two systems.



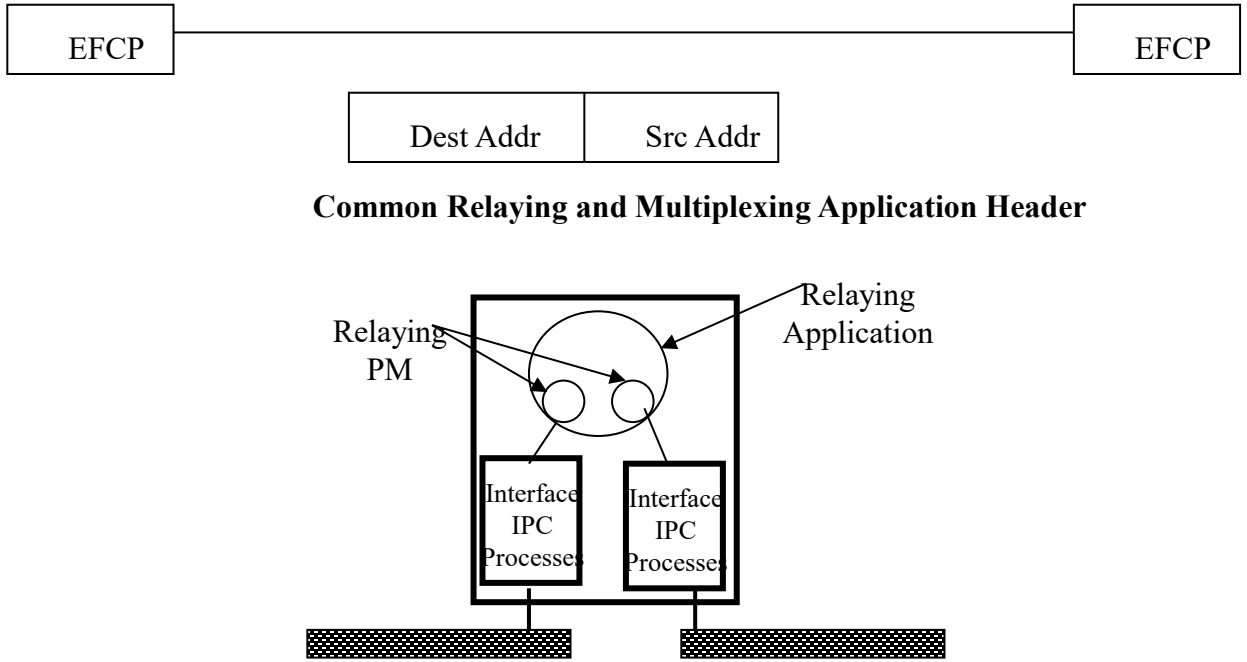
Communication Between Two Systems

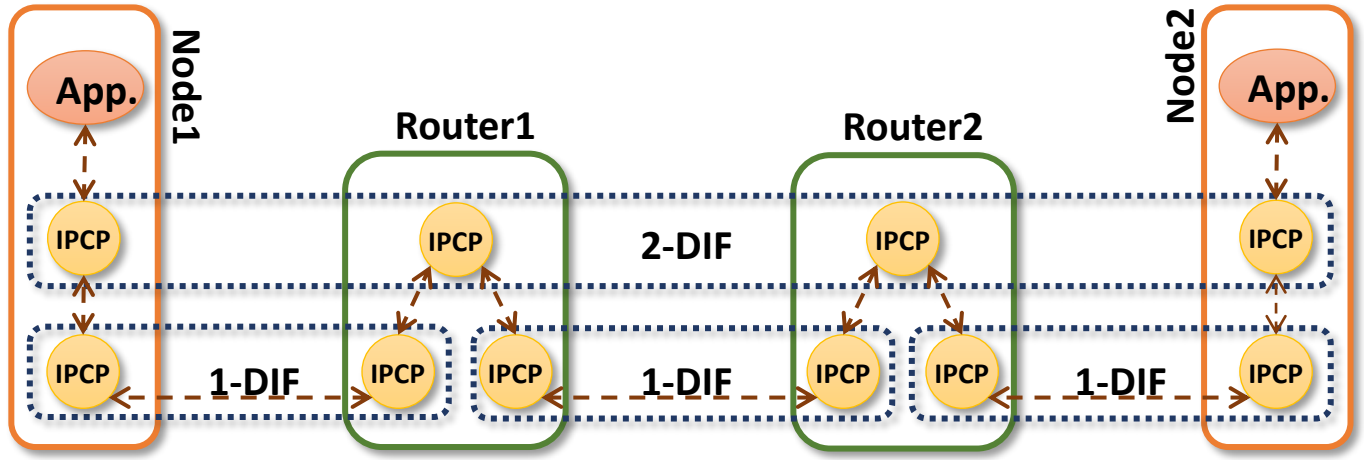
- Requires two new capabilities:
  - The ability in EFCP to distinguish one flow from another. Typically uses the port-ids of the source and destination,
  - To manage multiple users of a single resource.



Communicating with N Systems

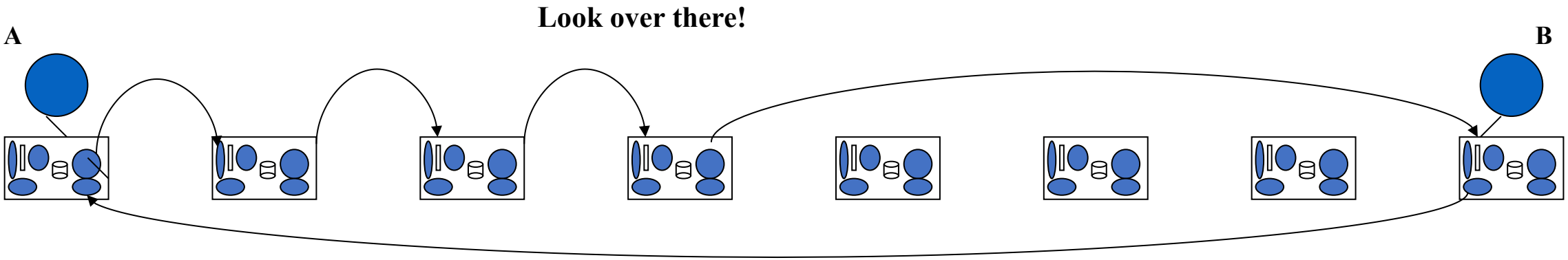
- Relaying systems over a wider scope requires carrying addresses.
- Will have to have an EFCP operating over the relays to ensure the requested QoS reliability parameters.





How Does It Work?

Establishing Communication:



- A asks IPC to allocate comm resources to B
- Determine that B is not local to A use search rules to find B
- Keep looking until we find it.
- Go see if it is there and whether we have access.
- Then tell A the result.