Design and Basic Evaluation of Virtual IPv4 based CYPHONIC adapter

Ren Goto[1)], Taiki Yoshikawa[2)], Hijiri Komura[2)],
Kazushige Matama[1)], Chihiro Nishiwaki[2)], Katsuhiro Naito[1)]

[1)] Faculty of Information Science, Aichi Institute of Technology
[2)] Graduate School of Business Administration and Computer Science, Aichi Institute of Technology

2022, March, 8
The 13th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC 2022

Presentation outline

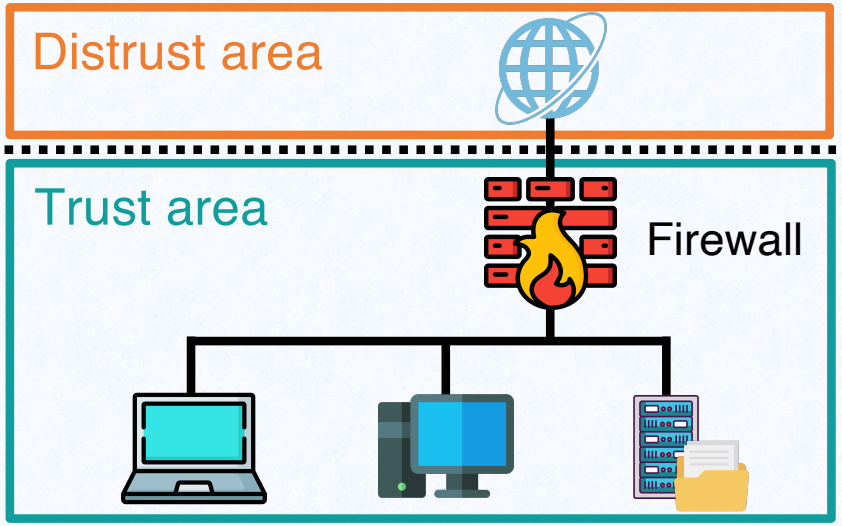
- About network and security
- Concept of CYPHONIC
- CYPHONIC issues
- Objective
- Proposed system
- Basic evaluation
- Conclusions

About Network and Security model

Perimeter security model

(Conventional security measures)

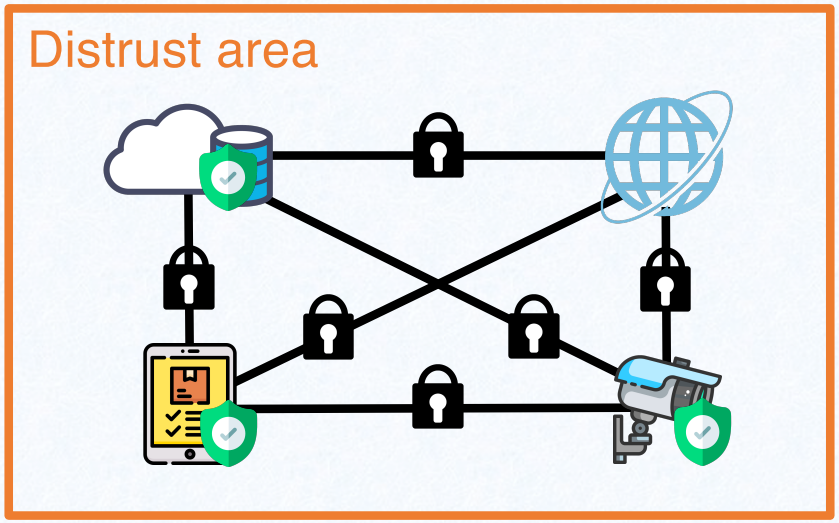
- Establishing a perimeter around the network to protect the internal network from distrusted areas.
- Setting up a Firewall or VPN with a static policy.



Zero-trust security model

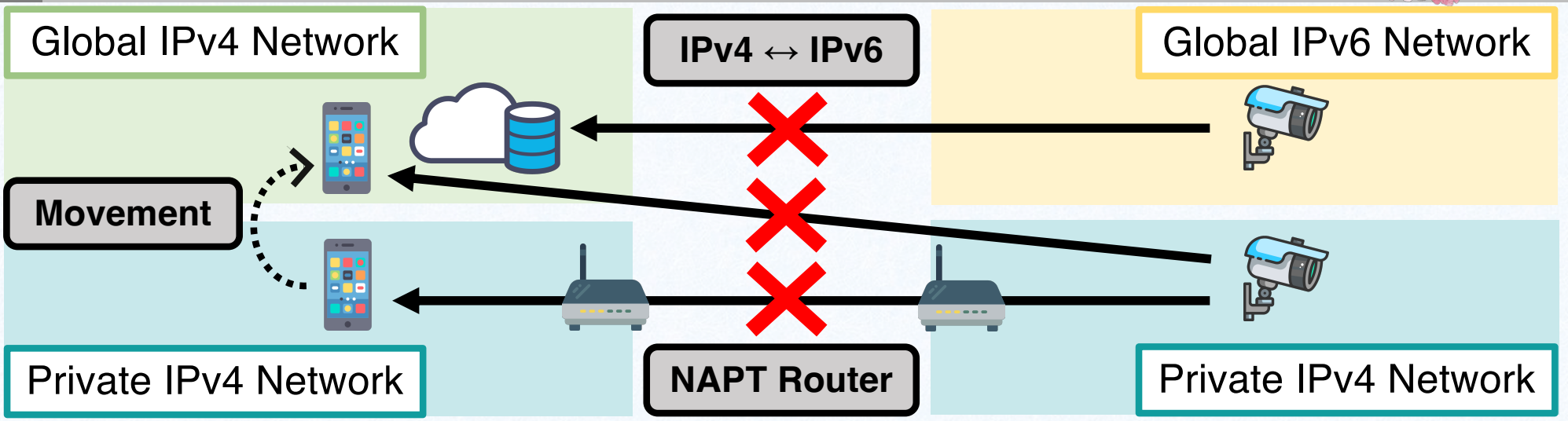
(Security measures required in the future)

- Protecting all devices, whether in or outside the organization's network.
- Authenticating the communication device and performs secure end-to-end communication.



In recent years, rapid spread of cloud services and IoT leads to a request for zero-trust security.

Requirement for Zero-trust security model



Zero-trust model requires direct connection between devices for secure end-to-end communication.

IoT service developers must be take security measures while ensuring network accessibility to fit the network environment in which the device resides.

Security is often a lower priority than the original service functionality, because safety and convenience are at odds in security measures.

Concept of CYPHONIC

CYber PHysical Overlay Network over Internet Communication
Communication framework for secure end-to-end communication

CYPHONIC offers a more packaged solution to realize their services on the zero-trust security model.

Supports inter-connectivity for IPv4 and IPv6 (Inter-connectivity)

- CYPHONIC guarantees independent connectivity from the network environment.
- CYPHONIC realizes IP address compatibility and connection between nodes behind NAPT routers via a relay server.

Supports seamless mobility (mobility / transparency)

- CYPHONIC can continue communication across different access networks.
- CYPHONIC hides the change of IP address by using the virtual IP addresses.

Supports secure authentication and communication (Secure)

- CYPHONIC secures communication with digital certificates and encryption.

Issues of Conventional CYPHONIC

The current CYPHONIC system requires a device to install the program for the CYPHONIC communication function.

CYPHONIC is not available for conventional devices (general nodes) due to the difficulty of the installation.

ex. IoT devices / Embedded devices

・Mask ROMs are very difficult to change programs after leaving the factory.

ex. Dedicated service servers

・The additional installation tends to be rejected due to concerns about the system's reliability.

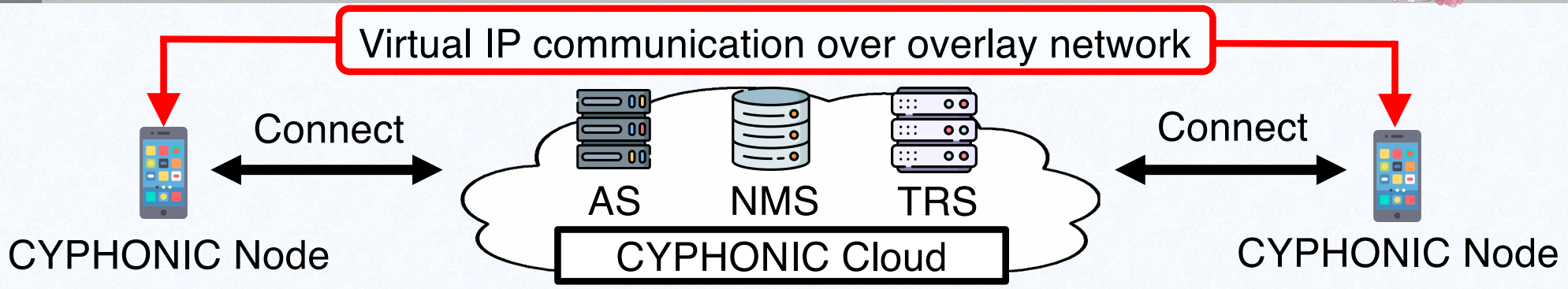
A new mechanism for CYPHONIC's communication capabilities without the installation is required.

Objective

Proposal of the virtual IPv4 based CYPHONIC adapter to perform processing for CYPHONIC communication instead of general nodes.

1. Equipping with the communication function of CYPHONIC.
   - ➡ Utilizing the conventional functions of the device program as a communication function.
2. Equipping functions to manage on connected general nodes.
   - ➡ Implementing additionally as the adapter's unique functions.

Components of CYPHONIC



CYPHONIC Node

Direct communication between CYPHONIC nodes using virtual IP.

Authentication Service (AS)

Automatic authentication of CYPHONIC node with digital certificate.

Node Management Service (NMS)

Management of network information of CYPHONIC node. Also, construction of virtual network communication path.

Tunnel Relay Service (TRS)

Relaying process for communications between IPv4-IPv6 and NAPT-NAPT environment.

Processing function in CYPHONIC node

CYPHPNIC Daemon provides the functionality needed to communicate over our overlay network.

Signaling Module

Signaling Module performs signaling to the cloud services to obtain a virtual IP address and an FQDN as the identifier of the device.

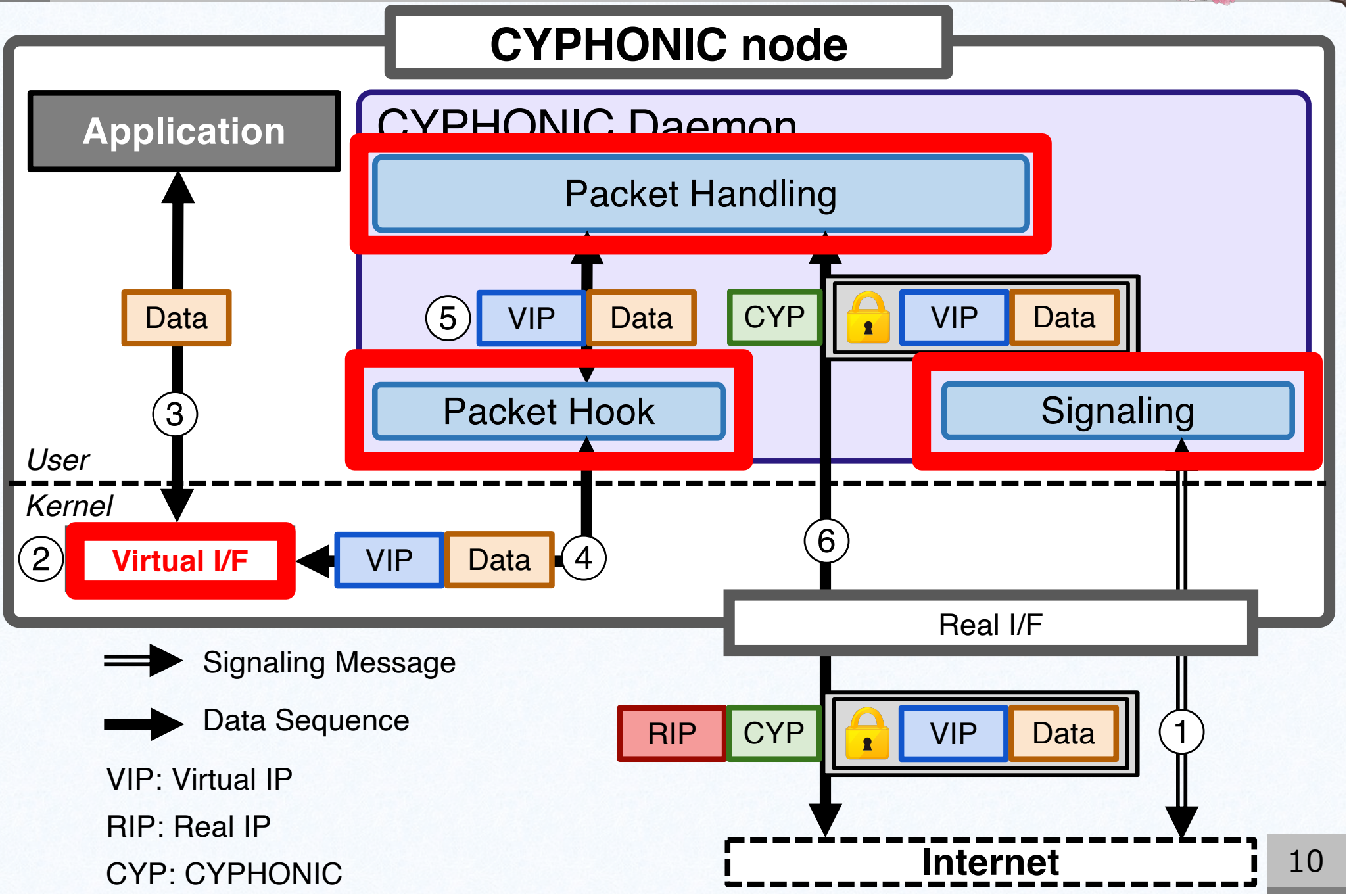
CYPHONIC Resolver Module

CYPHONIC Resolver Module generates a DNS response including a virtual IP address because FQDN is the identifier for each CYPHONIC node.

Packet Handling Module

Packet Handling Module encapsulates and encrypts virtual IP packet for communication over our overlay network.

System model of CYPHONIC node



Concept of CYPHONIC adapter

CYPHONIC adapter is implemented by extending the functionality of CYPHONIC Daemon.

CYPHONIC communication functions

CYPHONIC adapter performs communication to the peer node on behalf of the general node.

- Processing of virtual IP packets
- Transmission and reception data encryption
- Communication over the overlay network

General node management functions

CYPHONIC adapter manages the information required for communication.

- Virtual IP address of general node
- FQDN of general node
- Encryption key

Processing function in CYPHONIC adapter

CYPHONIC adapter has an Adapter Daemon that combines the conventional functionality of CYPHONIC Daemon with functionality of general node management.

Signaling Module / Packet Handling Module

Conventional module provides communication function.

General Node Management Module

General Node Management Module manages information used by general nodes for communication.

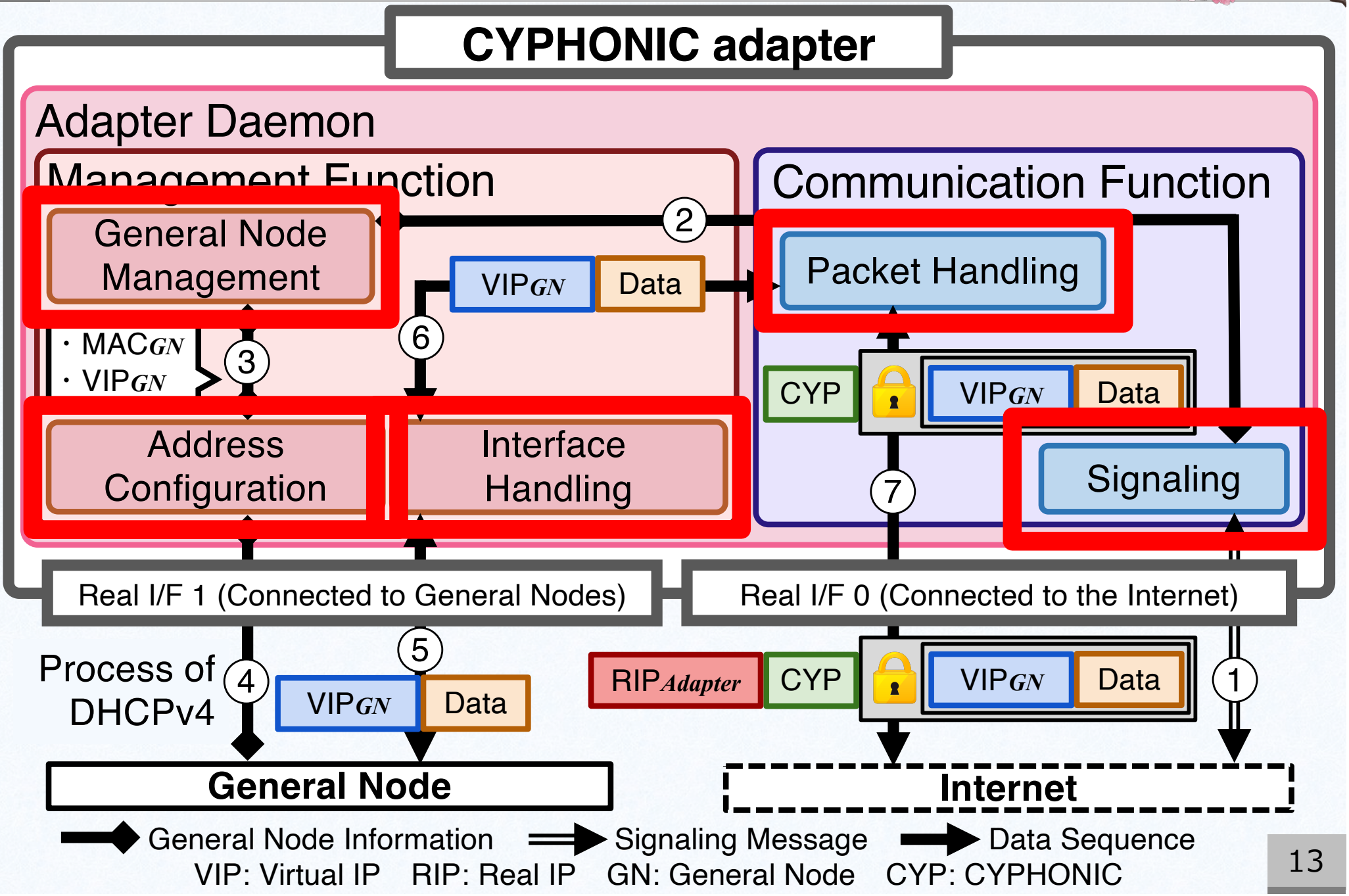
Address Configuration Module

Address Configuration Module assigns virtual IP address to general nodes. This paper assign a virtual IPv4 address, because the mainstream IP protocol is still IPv4.

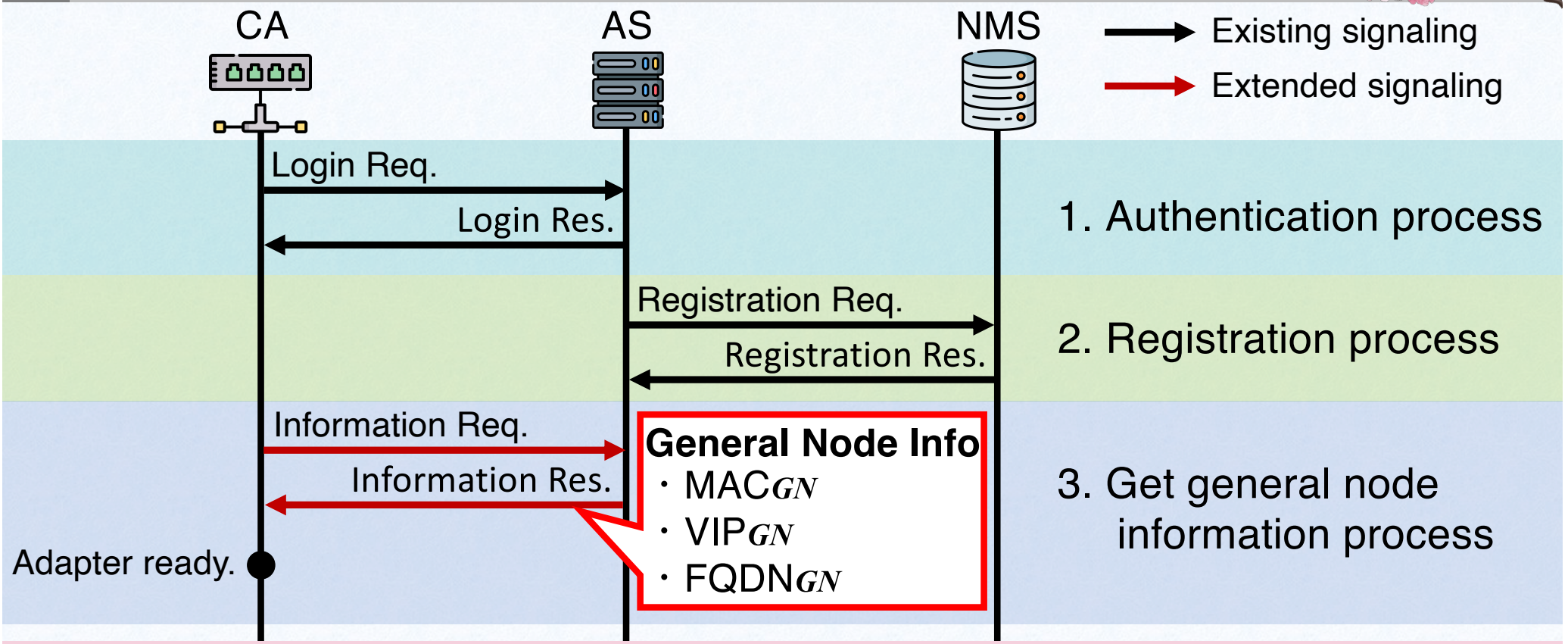
Interface Handling Module

Interface Handling Module hooks virtual IP packets from the general node.

System model of CYPHONIC adapter

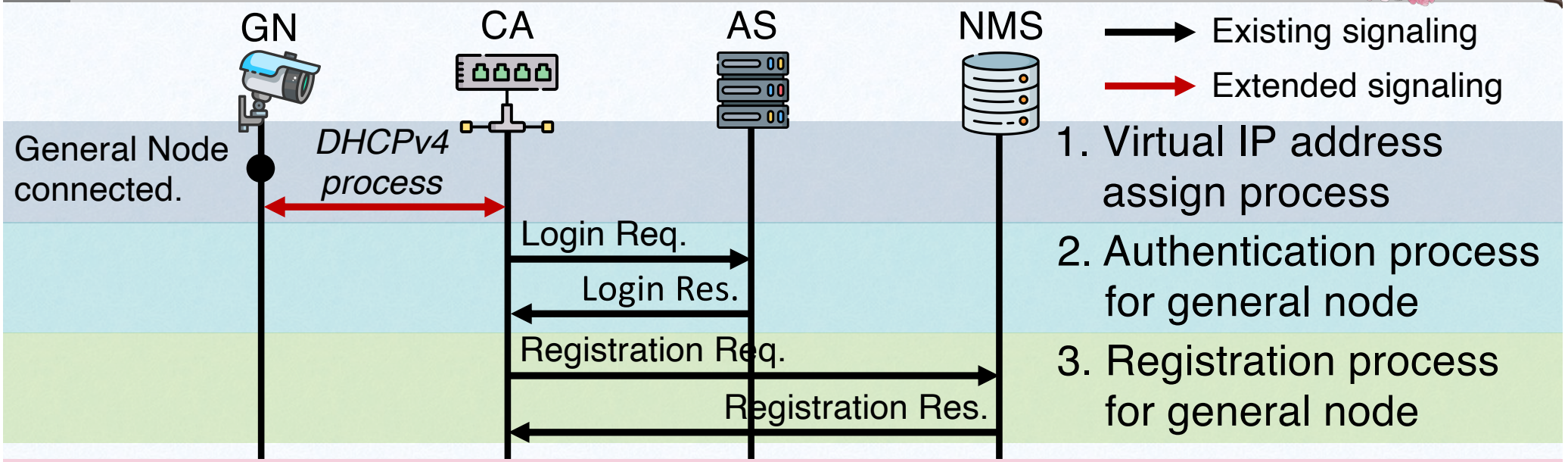


Sequence of Get General Node information



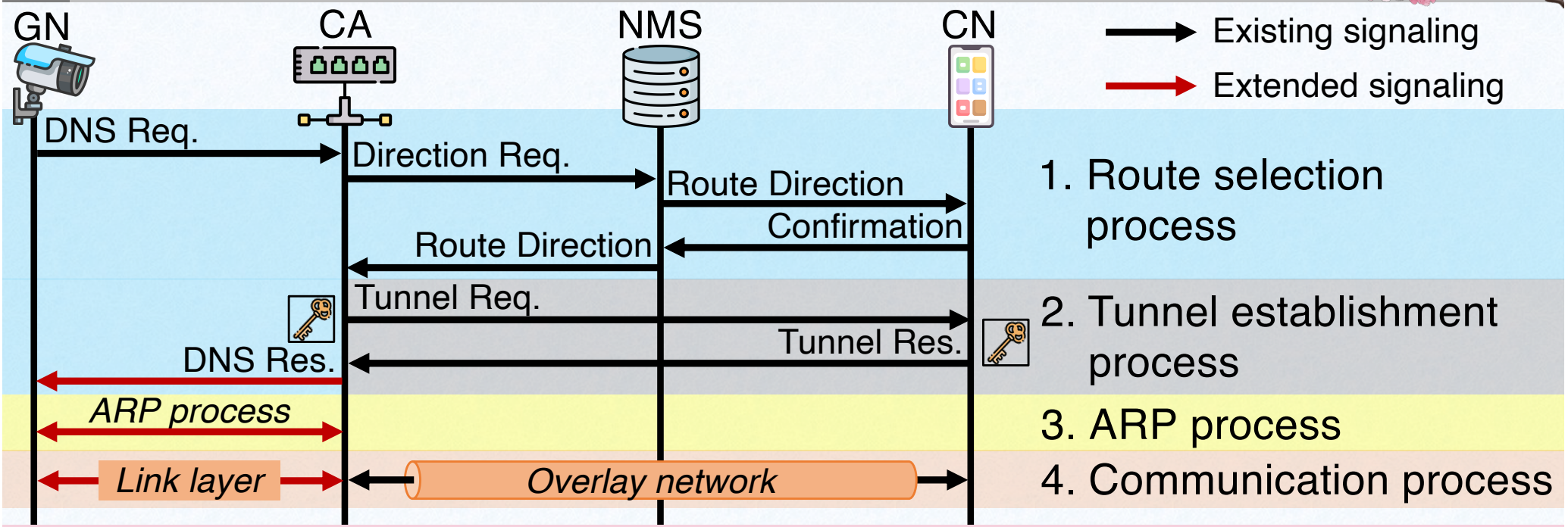
1. CYPHONIC adapter performs an authentication process to AS to gain its reliability.
2. CYPHONIC adapter registers network information to NMS.
3. CYPHONIC adapter gets general node information from AS.

Sequence of General Node configuration



1. CYPHONIC adapter assigns a virtual IPv4 address using the DHCPv4 mechanism when it detects the connection of the general node. Then, the general node can communicate by the virtual IPv4 addresses.
2. CYPHONIC adapter performs the authentication process to AS to authenticate general nodes.
3. CYPHONIC adapter registers network information of general nodes to NMS.

Sequence of Overlay network communication



1. CYPHONIC adapter determines the communication path to the desired FQDN by triggering a DNS query.
2. CYPHONIC adapter generates an encryption key and exchanges it with the peer node.
3. CYPHONIC adapter responds with adapter's MAC address, when an ARP request for virtual IP of the peer node is received.
4. Hooking virtual IP packets from general nodes and communicate over our overlay network.

Basic evaluation

Adapter processing time

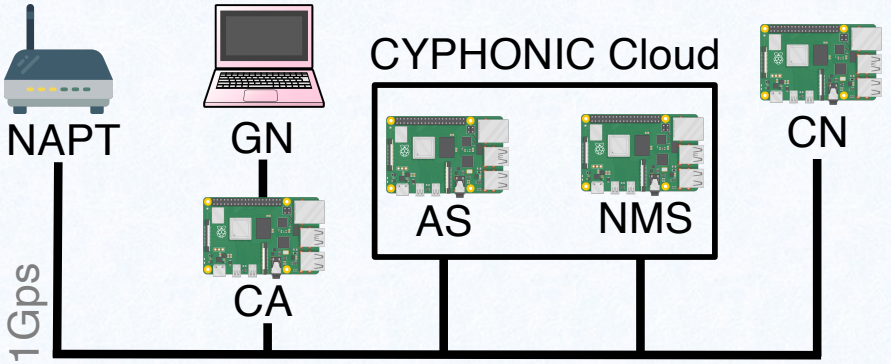
Measuring packet processing time and signaling processing time.

- Route selection processing time
- Tunnel establishment processing time
- ARP packet processing time

Communication delay time

Measuring the communication delay time of the general node.

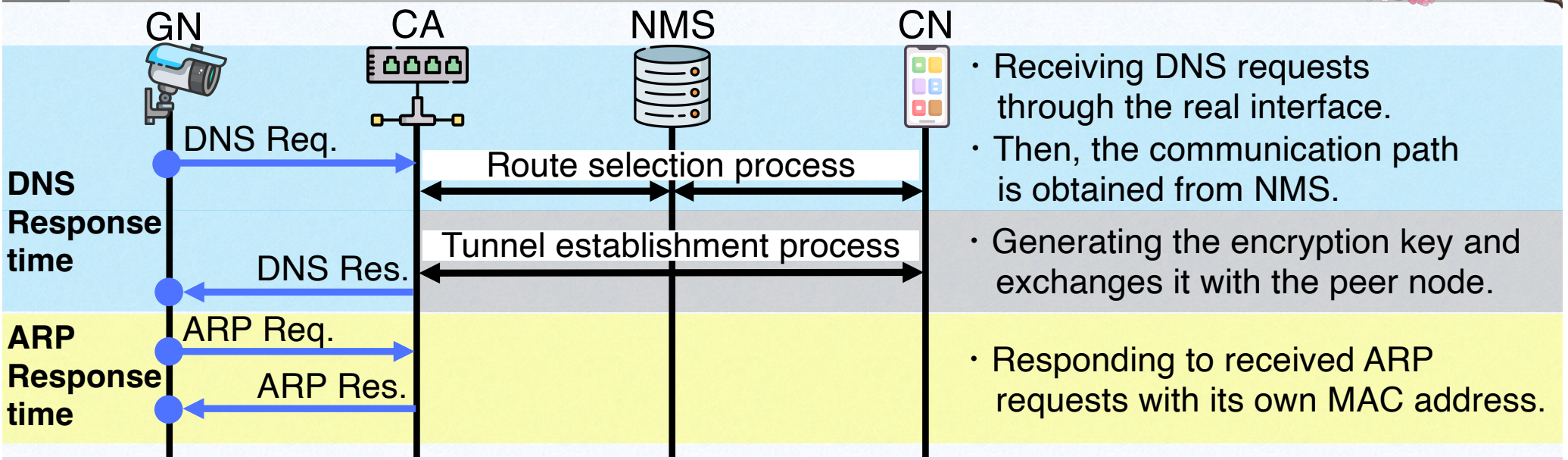
- DNS and ARP response time
- Round-trip time
- Communication throughput



Raspberry Pi 4 Model B (CYPHONIC Cloud, Adapter, Node)	
OS	Raspbian GNU/Linux 10.0
CPU	Quad Core 1.5GHz Broadcom BCM2711
Memory	4GB

MacBook Air 2017 (General Node)	
OS	macOS Monterey Ver 12.2
CPU	Dual Core 2.20GHz Intel(R) Core i7-5650U
Memory	8GB

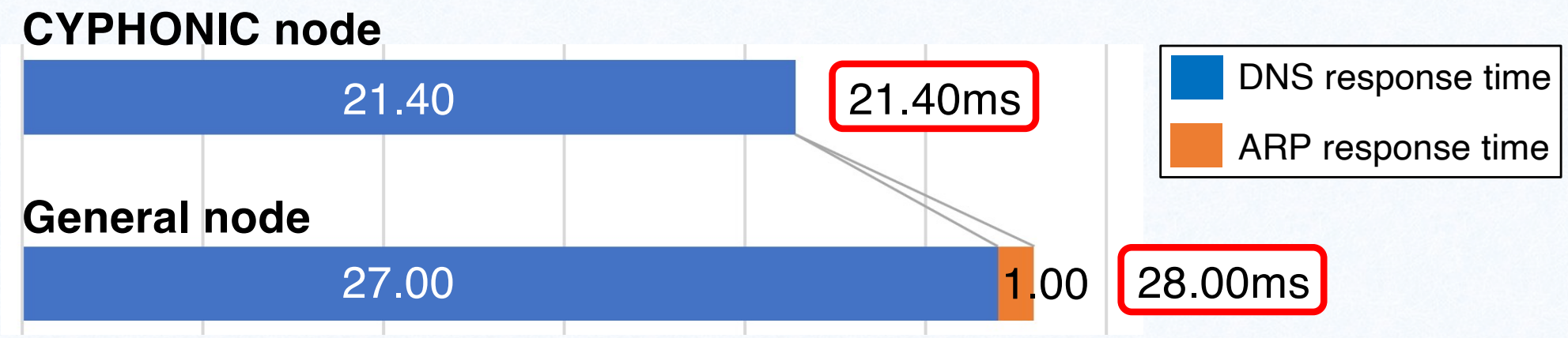
Process to be evaluated



Measure the delay time of initial communication

- General node sends a DNS request to CYPHONIC adapter, when it initiates communication.
- General node receives a DNS response and forwards it to the application.
- The application on the general node sends an ARP request to the peer node virtual IP address.
- General node receives ARP response from CYPHONIC adapter.

Delay time of Initial communication



Adapter processing time		
	CYPHONIC adapter	CYPHONIC node
Route selection process time	19.74ms	16.20ms
Tunnel establishment process time	2.75ms	2.23ms
ARP process time	0.32ms	

The route selection process includes communication delay between the adapter and the general node and transferring time for the answer section from the data link layer to the application layer.

Results of Communication performance

Network Quality (General node via CYPHONIC adapter)	
UDP Throughput	30.0 Mbits/sec
Jitter	0.459 ms
TCP Throughput	37.3 Mbits/sec
Round-trip time	3.594 ms

Network Quality (CYPHONIC node)	
UDP Throughput	30.0 Mbits/sec
Jitter	0.450 ms
TCP Throughput	44.4 Mbits/sec
Round-trip time	2.523 ms

Round-trip time

RTT of the general node is slightly lower than that of the CYPHONIC node.

- Measuring values do not have a significant effect on communication.
- Providing communication capabilities to the general node without incurring significant overhead.

Communication throughput

CYPHONIC adapter performs throughputs of about 30 Mbps or higher for UDP and TCP communications.

- Typically, when HD quality requires a throughput of 5 Mbps.
- It is enough for acceptable performance for streaming services.

Conclusions

Proposal of the virtual IPv4 based CYPHONIC adapter to perform processing for CYPHONIC communication instead of general nodes.

1. Equipping with the communication function of CYPHONIC.
   - ➡ Utilizing the conventional functions of the device program as a communication function.
2. Equipping functions to manage on connected general nodes.
   - ➡ Implementing additionally as the adapter's unique functions.

Proposed system can provide communication capabilities to general nodes without incurring significant overhead

Question & Answer

UDP throughput of General Node

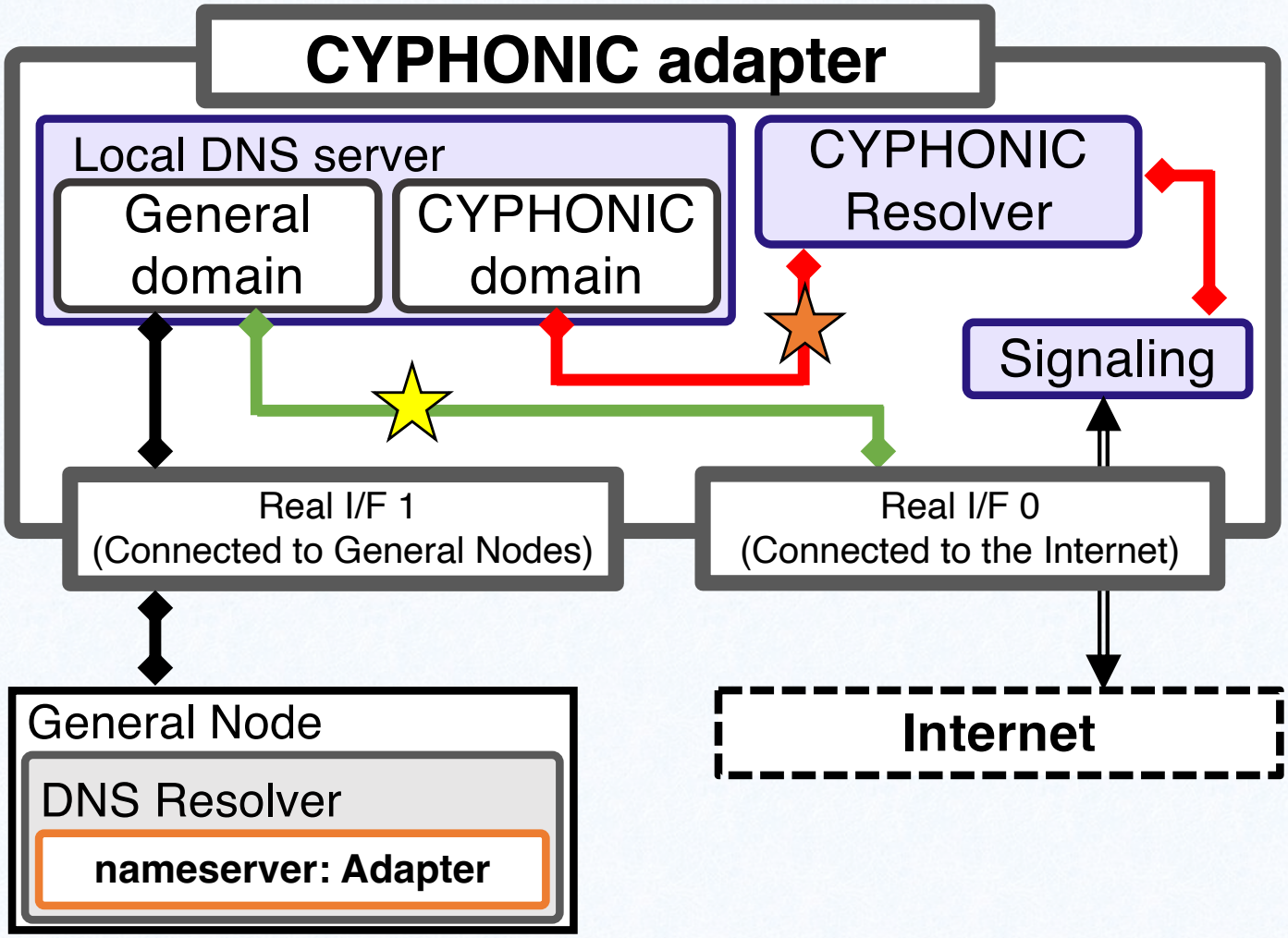
General Node ⇒ CYPHONIC Node			
Traffic	Throughput	Jitter	Loss rate
10Mbps	10.0Mbps	0.547ms	0%
20Mbps	20.0Mbps	0.531ms	0%
30Mbps	30.0Mbps	0.459ms	0%
40Mbps	39.6Mbps	0.250ms	0.93%
50Mbps	47.7Mbps	0.173ms	1.27%

CYPHONIC Node ⇒ General Node			
Traffic	Throughput	Jitter	Loss rate
10Mbps	10.0Mbps	0.787ms	0%
20Mbps	20.0Mbps	0.680ms	0%
30Mbps	30.0Mbps	0.395ms	0%
40Mbps	39.8Mbps	0.326ms	0.28%
50Mbps	49.5Mbps	0.266ms	0.46%

UDP throughput of CYPHONIC Node

CYPHONIC Node ⇒ CYPHONIC Node			
Traffic	Throughput	Jitter	Loss rate
10Mbps	10.0Mbps	0.524ms	0%
20Mbps	20.0Mbps	0.520ms	0%
30Mbps	30.0Mbps	0.450ms	0.%
40Mbps	40.0Mbps	0.385ms	0.013%
50Mbps	49.9Mbps	0.246ms	0.056%

Process of DNS packets



DNS Packet

General domain's

CYPHONIC domain's

Signaling message

CYPHONIC domain's

(ex. cyphonic.org)

go through CYPHONIC Resolver Module

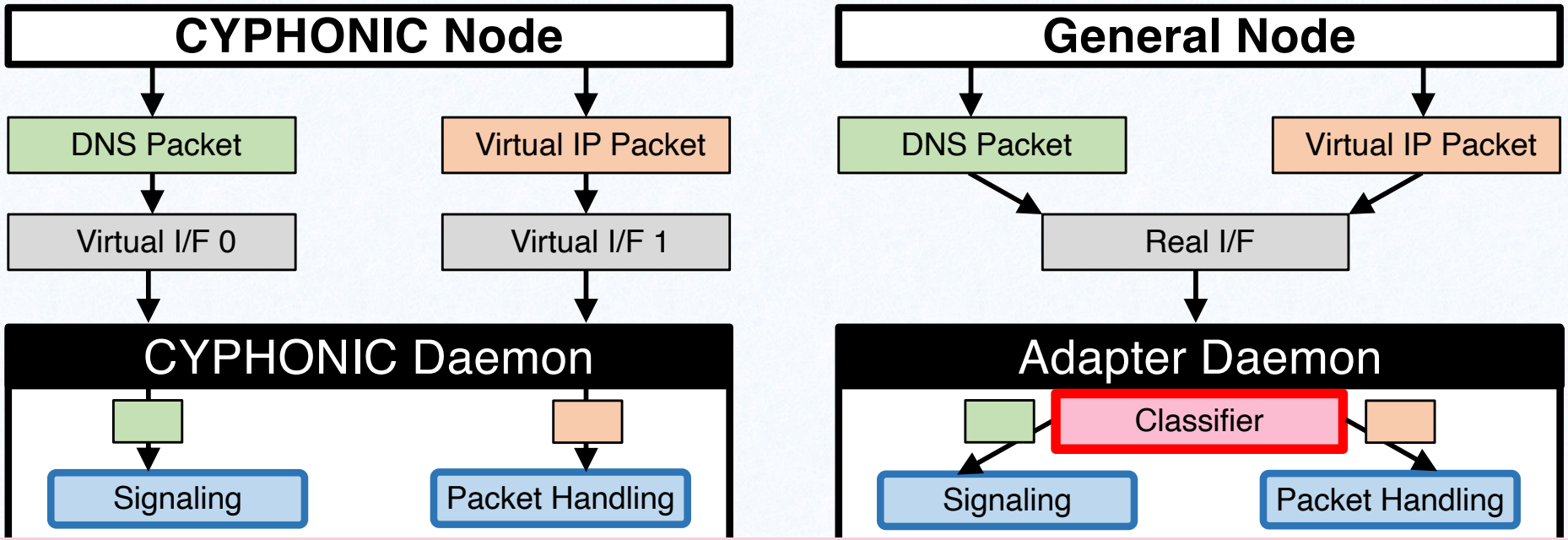
General domain's

(ex. google.com)

go through the Real I/F 0

- The address of the CYPHONIC adapter is registered in the DNS server address of the general node.
- First, Filtering domains using Local DNS Server.
- Then, Obtaining the FQDN of the peer node from the DNS request.
- Finally, Obtaining virtual IP address by Signaling Module and generates the DNS response packet.

Difference in Processing methods



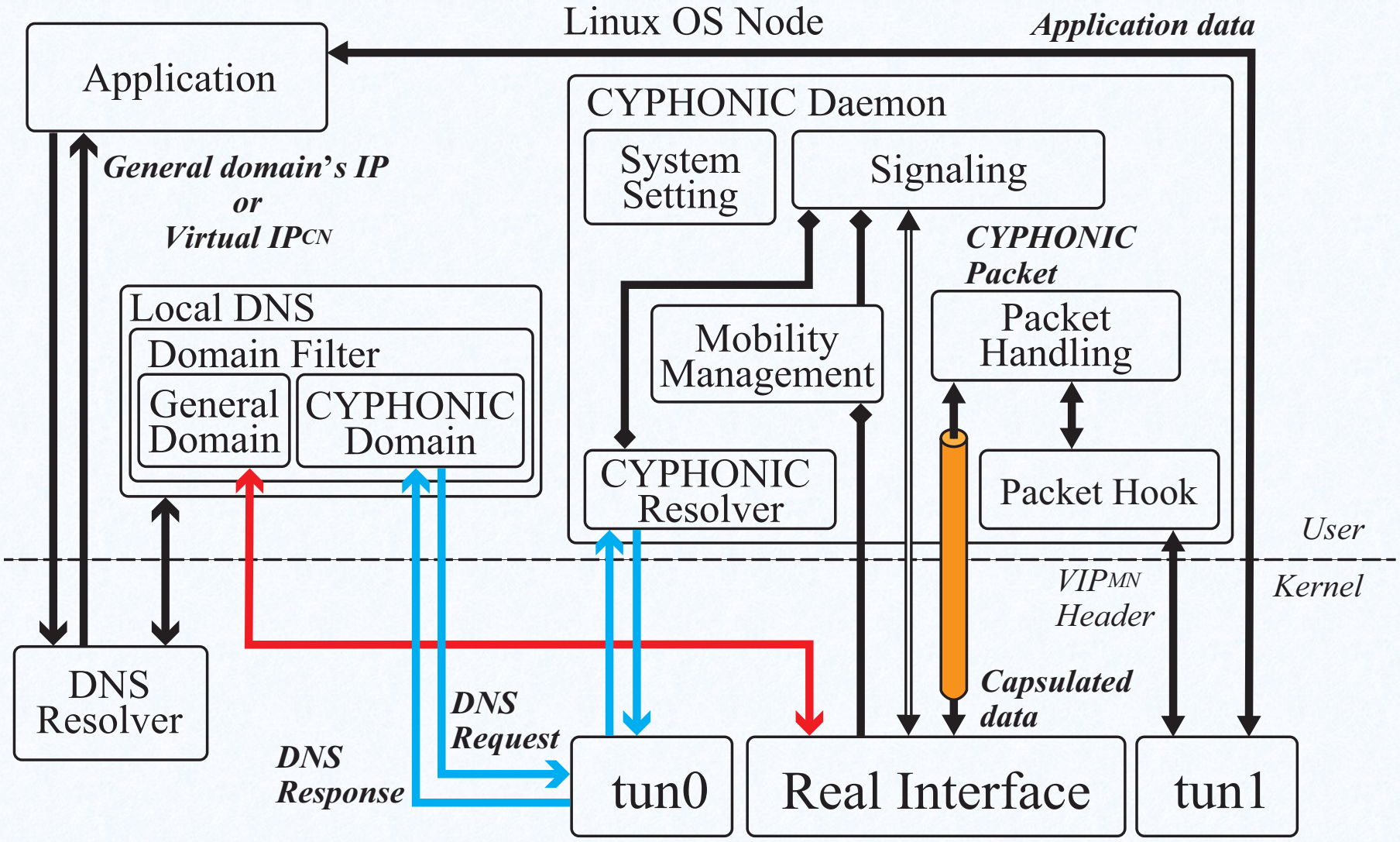
CYPHONIC node

- DNS packets and virtual IP packets are processed by different virtual interfaces.
- Processing function to DNS packets and virtual IP packets perform in parallel.

CYPHONIC adapter

- Receiving any in-coming packets through only one interface.
- CYPHONIC adapter must determine packet type.

System model of CYPHONIC node



MN: Mobile Node CN: Correspondent Node

RIP: Real IP VIP: Virtual IP

General domain's DNS Packets

CYPHONIC domain's DNS Packets

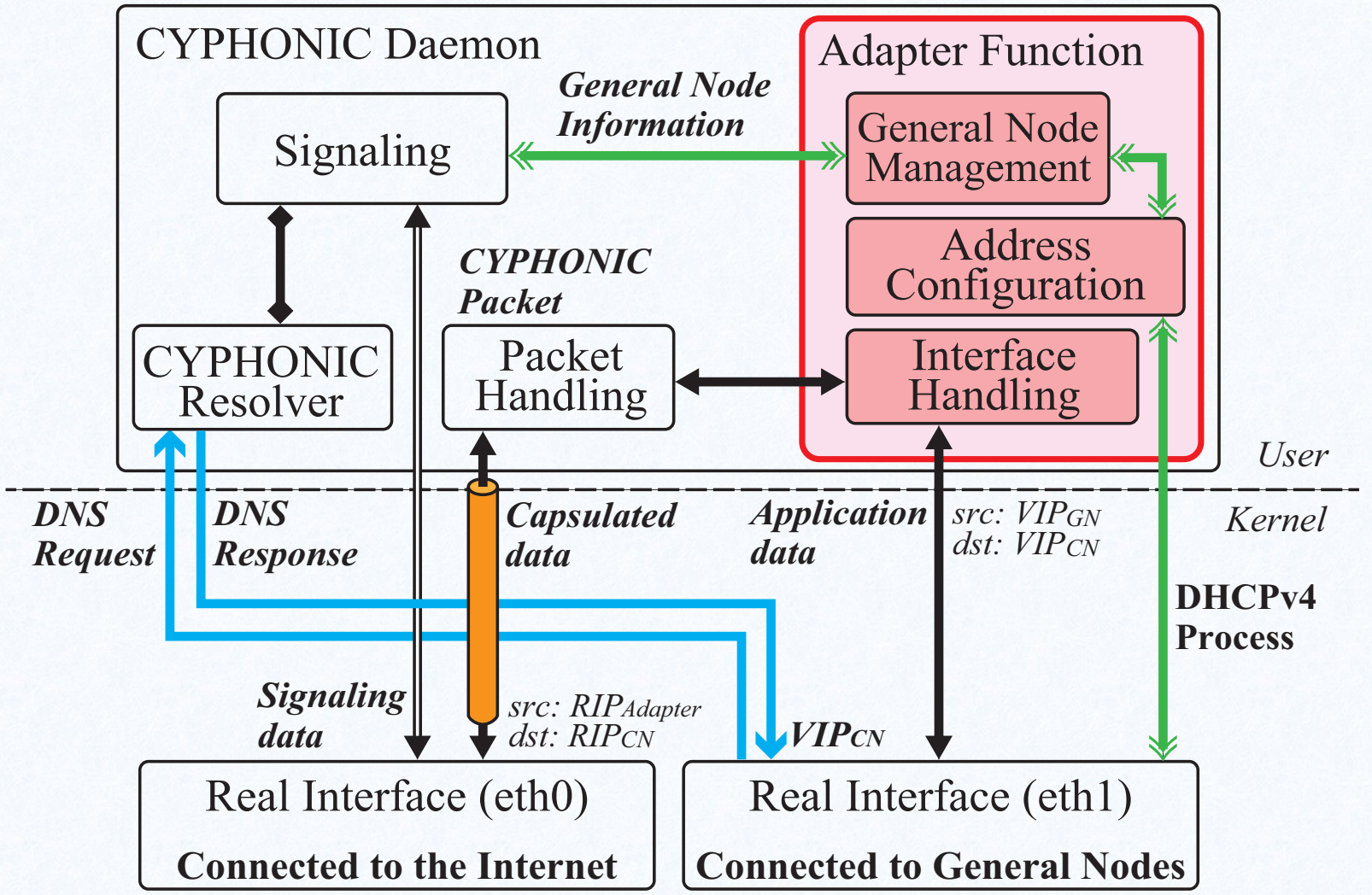
Signaling Message

DNS Packets

Data Sequence

Informations

System model of CYPHONIC adapter



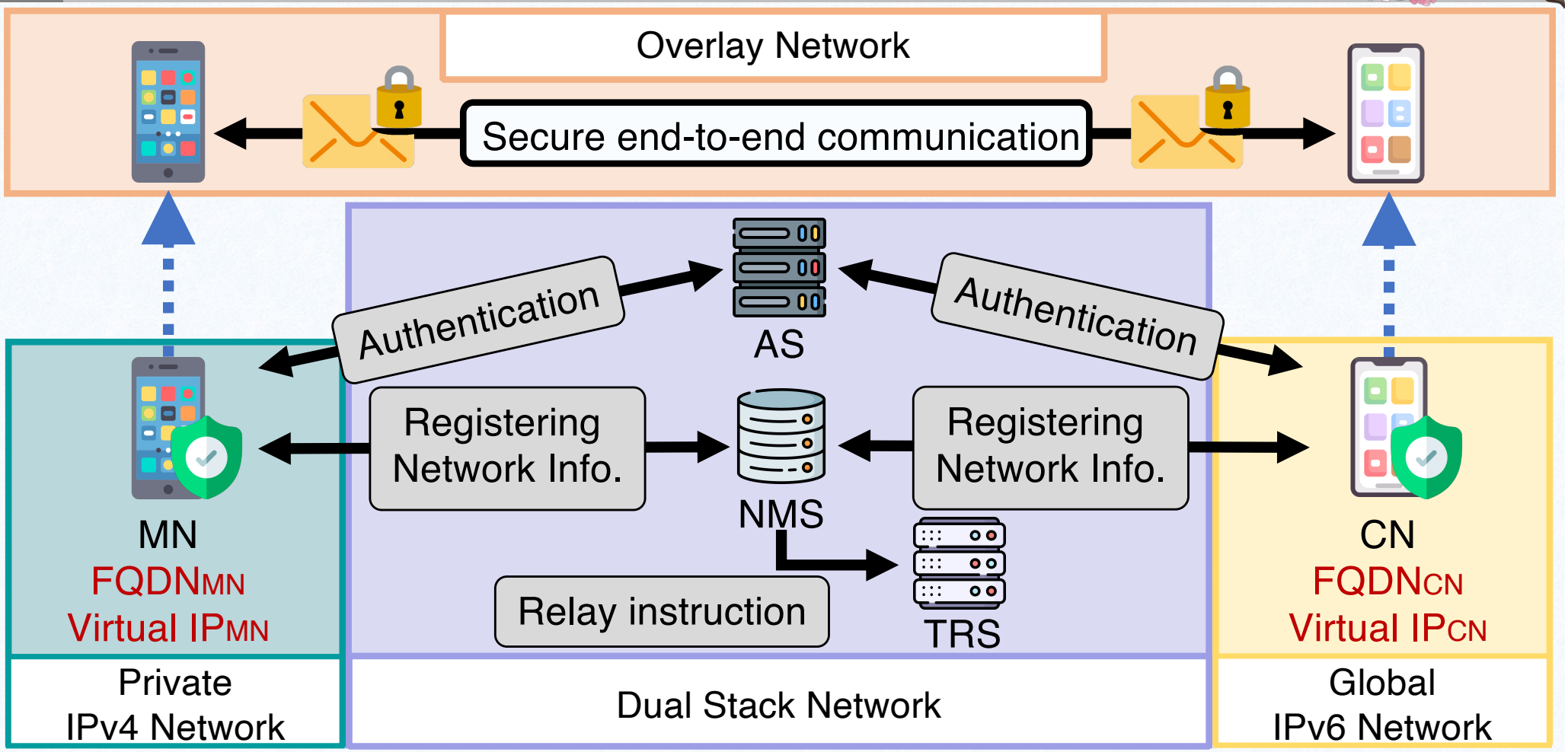
Issues of Conventional Technology

	Inter-connectivity	Mobility / Transparency
	• Communication block due to NAPT Router. • Incompatibility between IPv4 and IPv6.	• Disconnection due to network movement.
STUN	●	X
ICE	●	X
Mobile IPv4	X	●
DSMIPv6	X	●
CYPHONIC	●	●

There is no technology that can solve inter-connectivity and mobility / transparency at the same time.

➡ Practical implementation supporting inter-connectivity and mobility / transparency is required to realize a service for IoT devices.

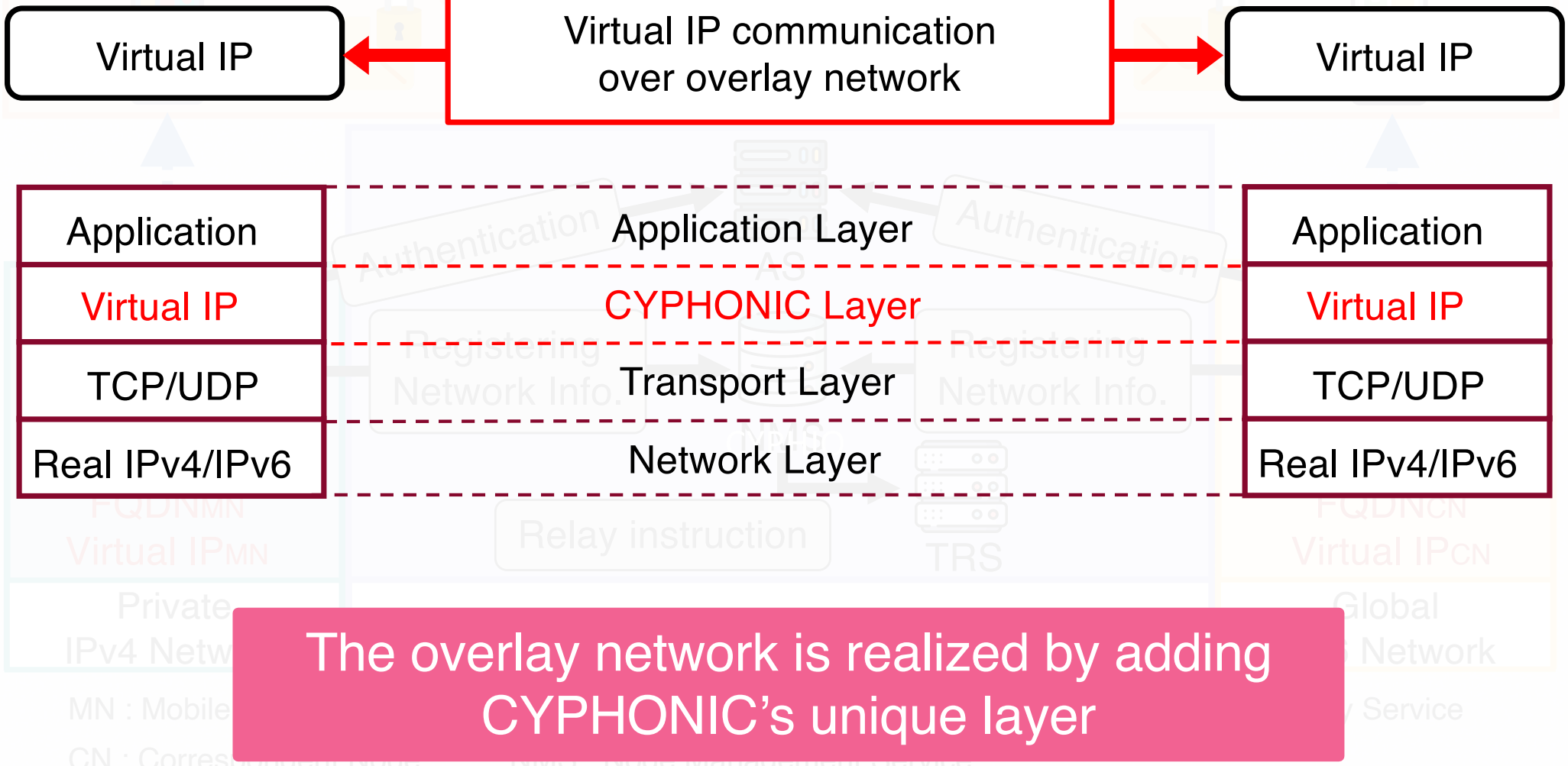
Overview of CYPHONIC



MN : Mobile Node
CN : Correspondent Node
AS : Authentication Service
NMS : Node Management Service
TRS : Tunnel Relay Service

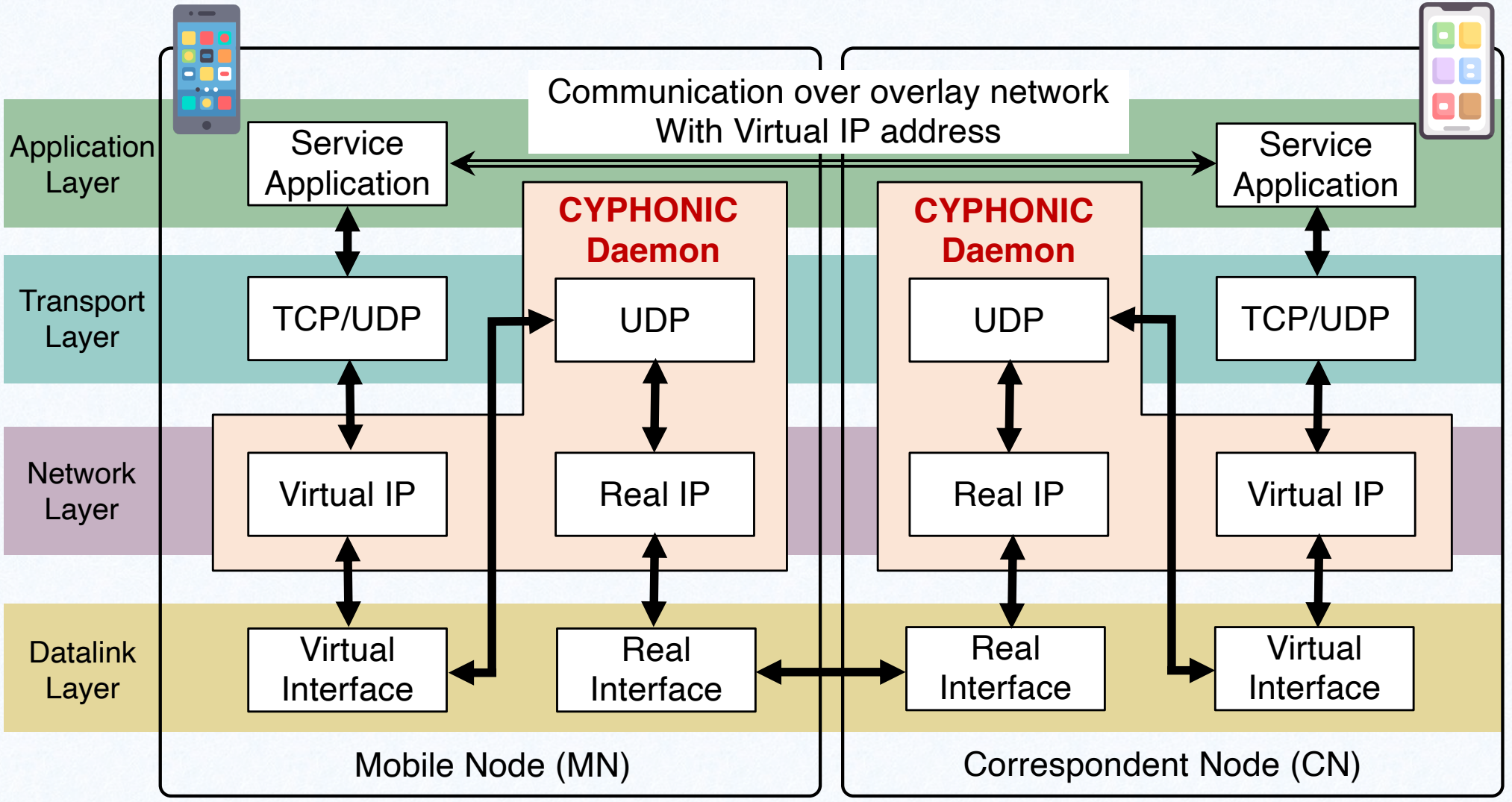
Secure end-to-end communication over our overlay network using virtual IP addresses.

Overview of CYPHONIC



The overlay network is realized by adding CYPHONIC's unique layer

PDU flow in CYPHONIC



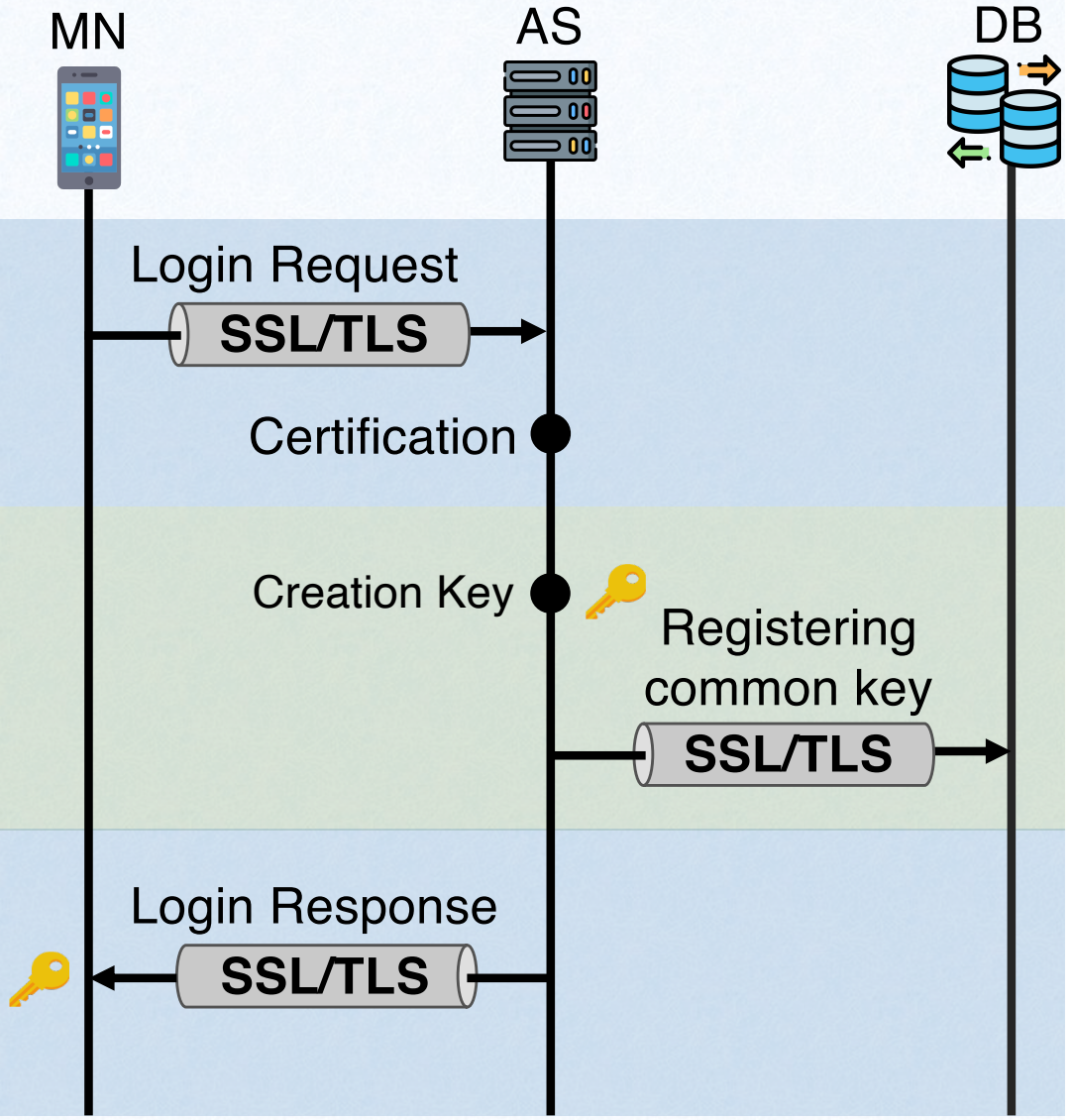
CYPHONIC Daemon gets virtual IP packets from the virtual interface, encapsulates all packets with UDP and sends it from the real interface.

Authentication process

First, authenticating MN.
(ID&password, Digital certificate, SSO)

Then, generating the common key to be used in communication between MN and NMS and store it in the DB.

Finally, sending the common key used for communication between MN and NMS.

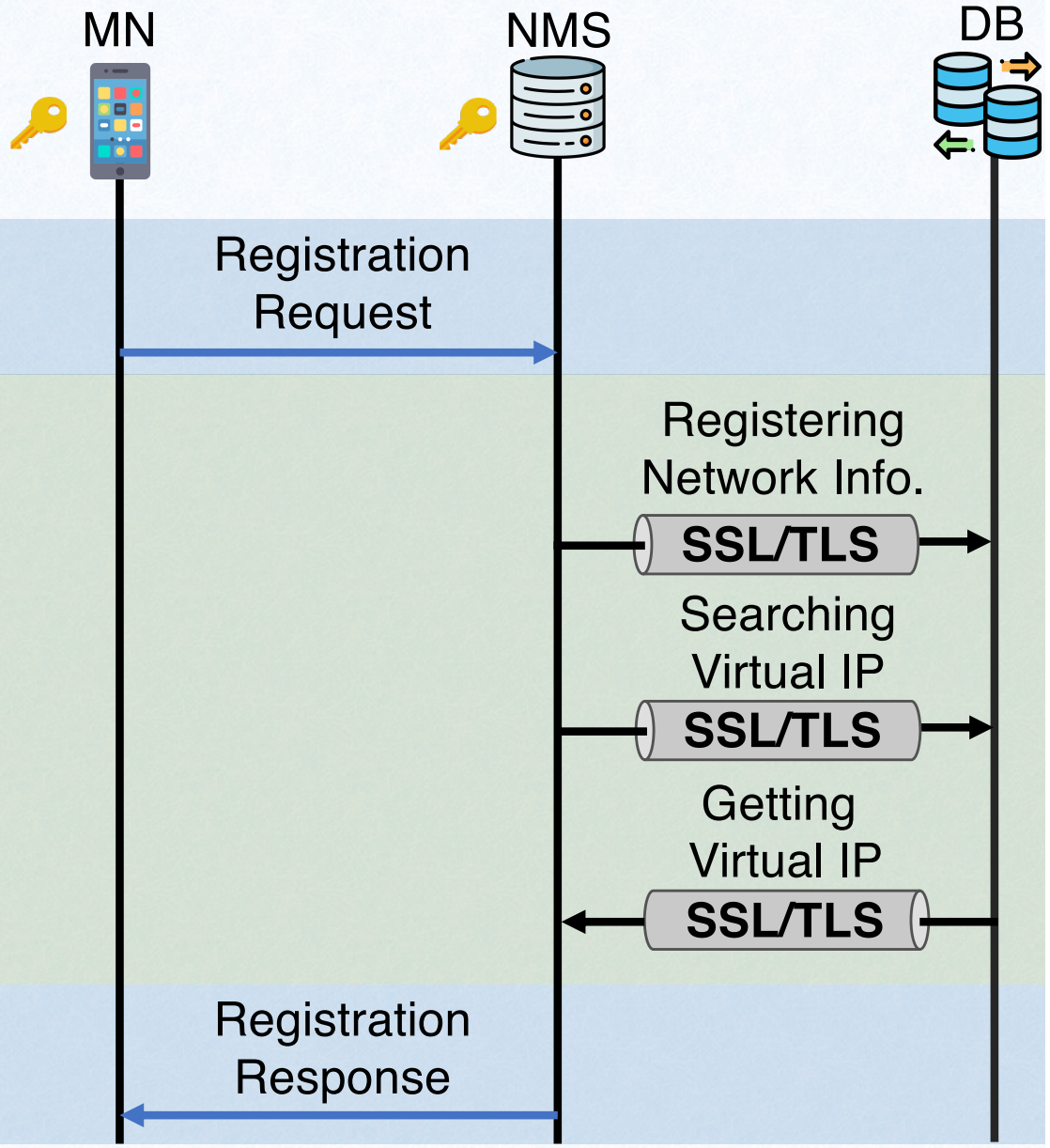


Registration process

First, sending MN network information to NMS.

Then, getting the MN's virtual IP address from the DB, after registering the MN's network information.

Finally, returning the virtual IP address to MN.



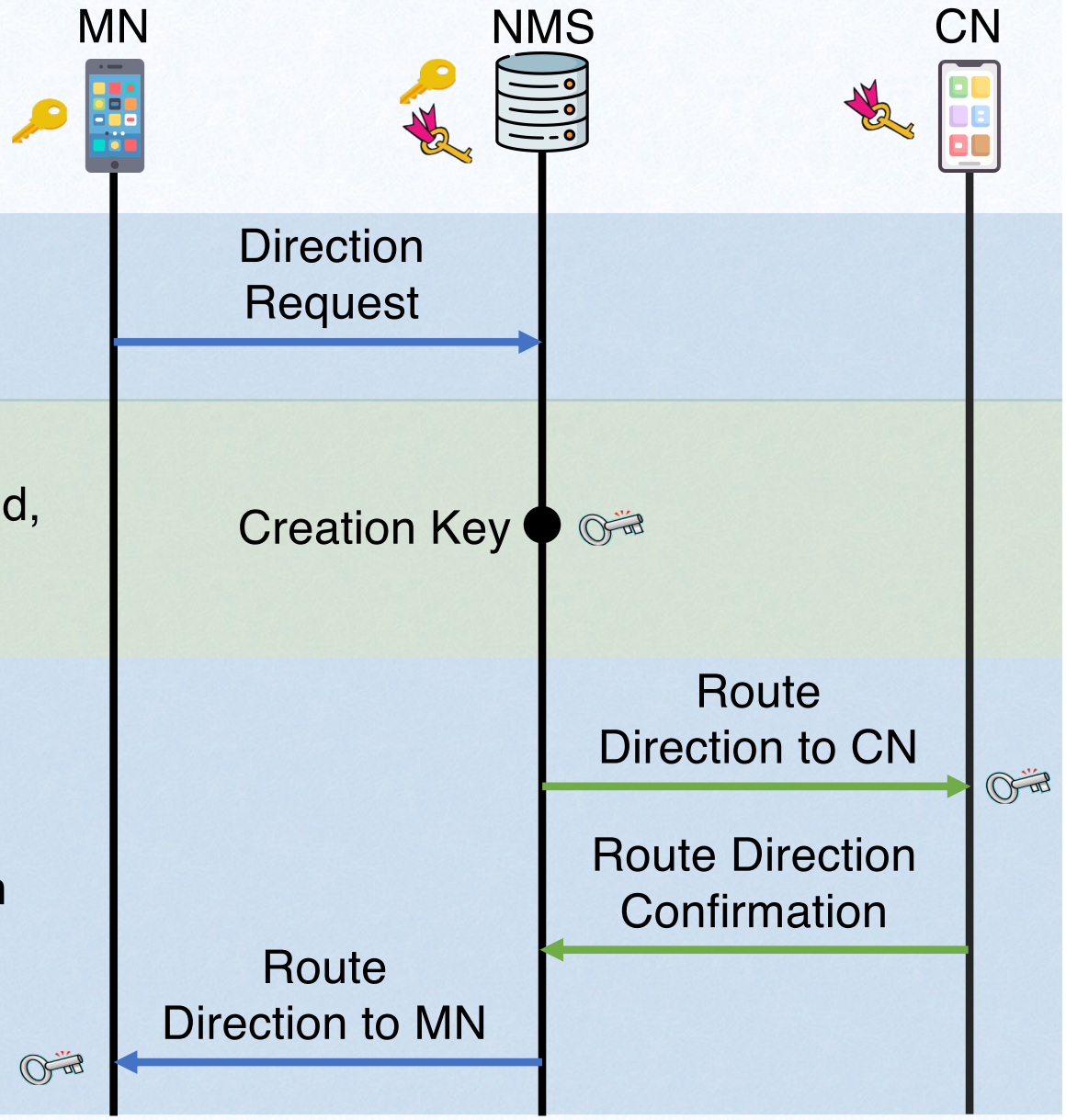
Route selection process

First, sending a communication path search request specifying the FQDN of the desired CN.

Then, generating Tunnel Key.
For your information, Tunnel Key is used, when both nodes exchange End Key for encrypting sent and received data.

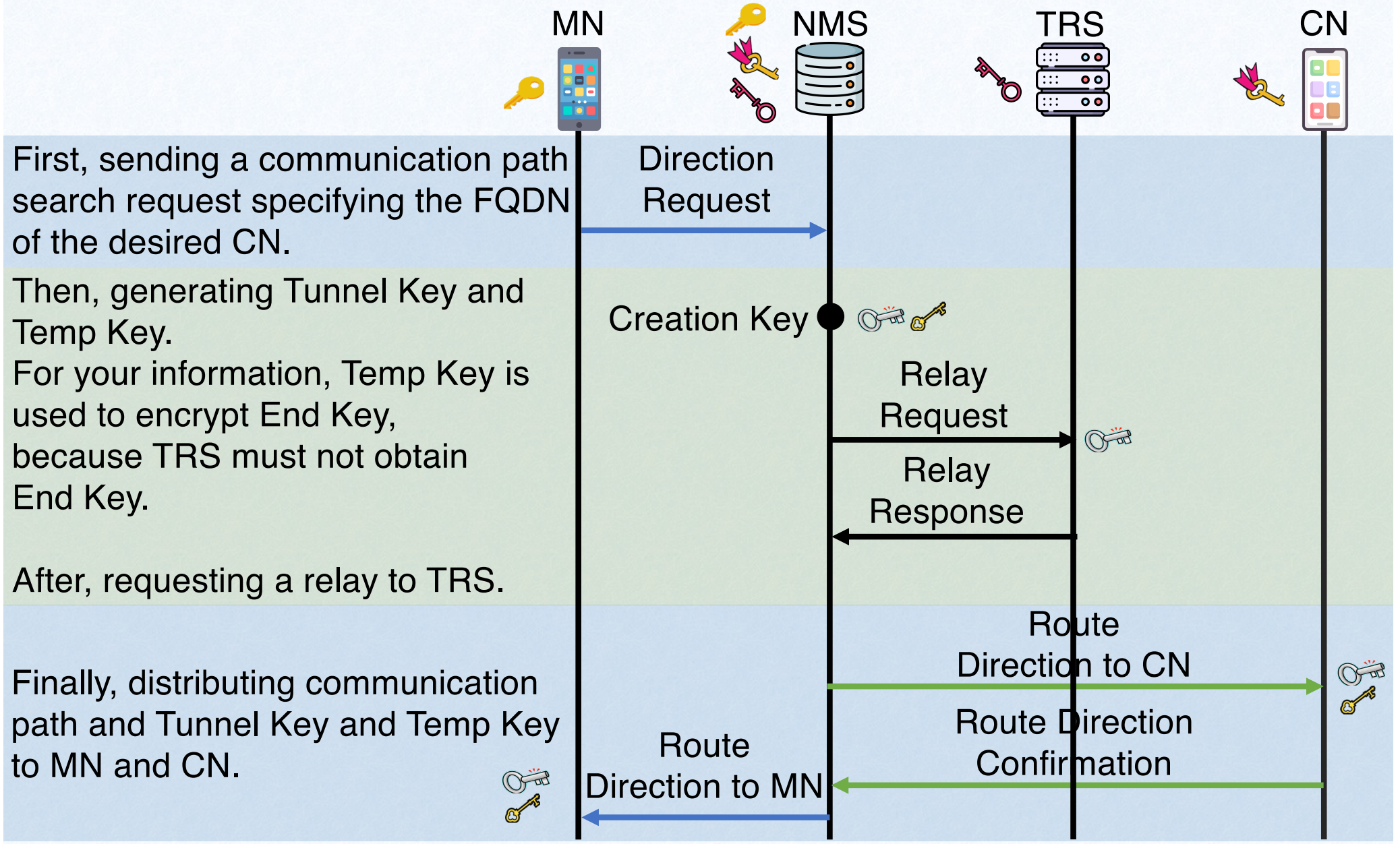
After, distributing communication path and Tunnel Key to CN.

Finally, distributing communication path and Tunnel Key to MN, when NMS received a confirmation response from the CN.

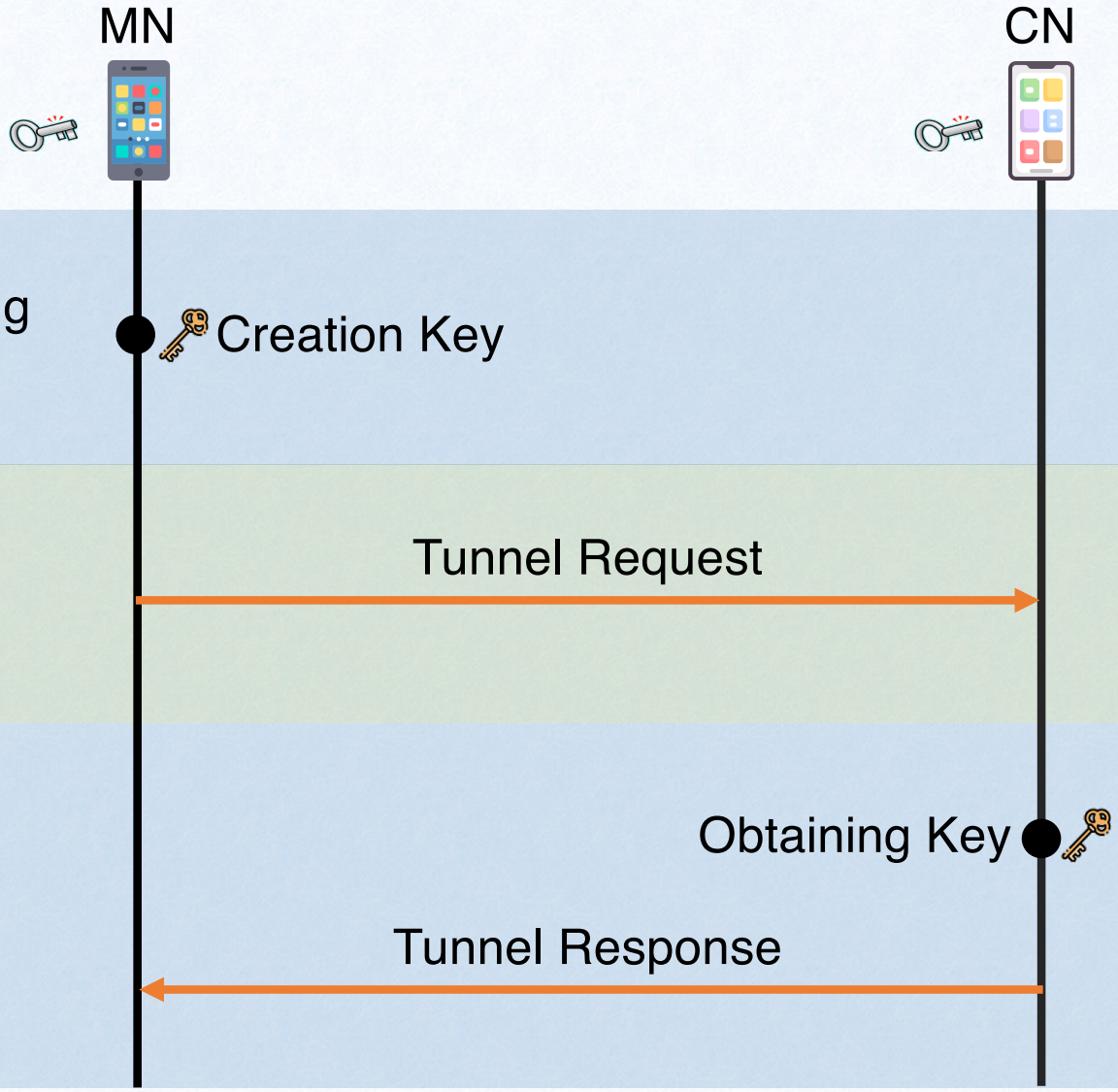


→ : Encrypted by (MN-NMS) → : Encrypted by (NMS-CN)

Route selection process (via TRS)



Tunnel establishment process



Tunnel establishment process (via TRS)