Proposal of an extended CYPHONIC adapter supporting general nodes using virtual IPv6 addresses

Ren Goto[1)], Kazushige Matama[1)], Chihiro Nishiwaki[1)], Katsuhiro Naito[2)]

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

2022, October, 18
The 11th Global Conference on Consumer Electronics: GCCE 2022

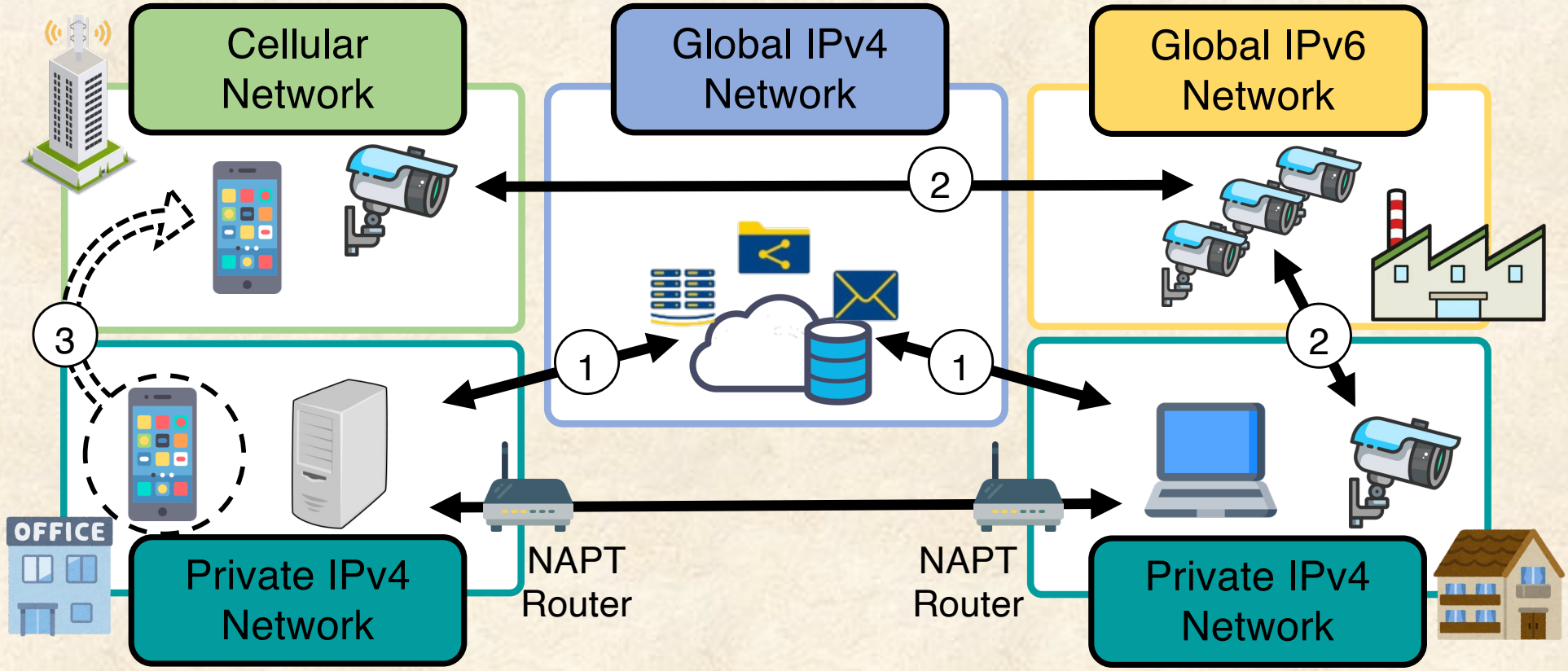
Presentation outline

- About network and security
- Concept of CYPHONIC
- Conventional systems and issues
- Objective
- Proposal system
- Performance evaluation
- Conclusions

Modern network usage patterns

Network usage has become increasingly diverse and complex.

1. Data management using external providers. (ex: Public cloud, IaaS)
2. Cooperative processing among several IoT devices.
3. Improved device mobility performance.



Devices will be distributed across multiple points,
each connected to a different network environment.

Zero-trust based Security approach and Issues

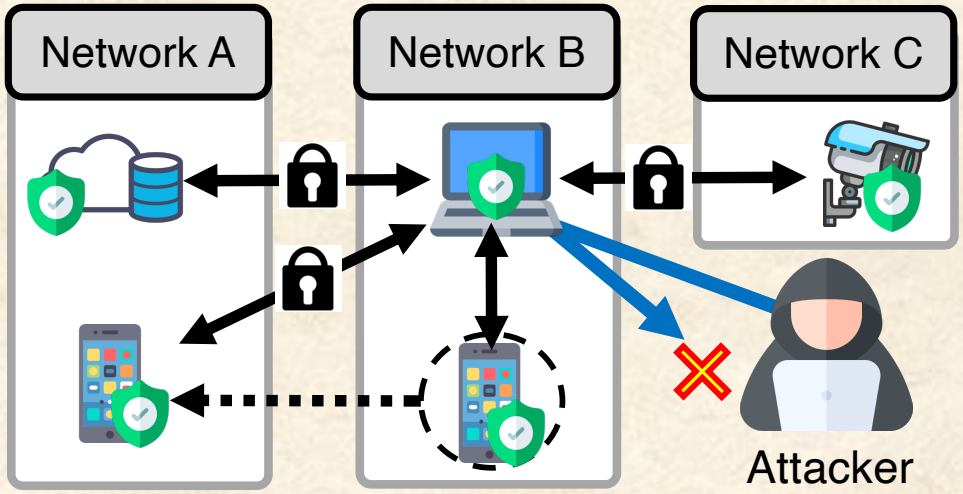
The zero-trust security model is suitable as a security measure to protect distributed, end-to-end connections between devices.

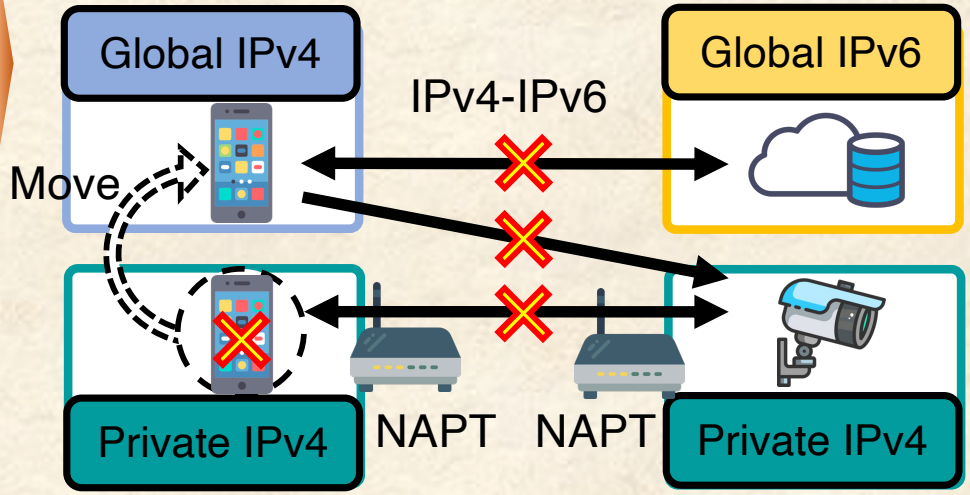
Security model

- ✓ Provides authenticated, authorized, and validated for all endpoints.
- ✓ Securely connect different networks.
- ✓ Encrypt communications between devices.

Network issues

- ✓ Differences between the NAPT mechanisms or IP versions make interconnection difficult.
- ✓ Device movement makes continuous protection difficult.





Zero-trust security requires cover a complex network environment and protect all devices and communications.

Concepts 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 secure end-to-end communication based on the zero-trust 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 (Security)

- CYPHONIC secures communication with digital certificates and encryption.

Conventional CYPHONIC systems

CYPHONIC provides an overlay network based on the virtual IP layer.

- A device will be equipped with a client program to communicate over our overlay network systems.
- The client program provides device authentication and overlay network communication functions.

CYPHONIC is difficult to use with the conventional devices (general nodes) due to difficulties in installing client programs.

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 avoided due to concerns about the system's reliability.

As a solution, we developed the CYPHONIC adapter.

- The CYPHONIC adapter is an adapter device that provides CYPHONIC communication functions to general nodes.

Issues of Conventional CYPHONIC adapter

The previous CYPHONIC adapter only supported virtual IPv4 addresses.

Conventional CYPHONIC adapter cannot handle the huge address space of IPv6.

- IPv4 addresses are feared to be exhausted.
- Some factory general-purpose devices communicates based on IPv6. (ex. 6LoWPAN)

Requires the CYPHONIC adapter supporting virtual IPv6 to provide IPv6-based communication to general nodes.

Objective

Proposal of the dual stack CYPHONIC adapter that extends the conventional CYPHONIC adapter to support both IPv4 and IPv6 versions of virtual IP addresses.

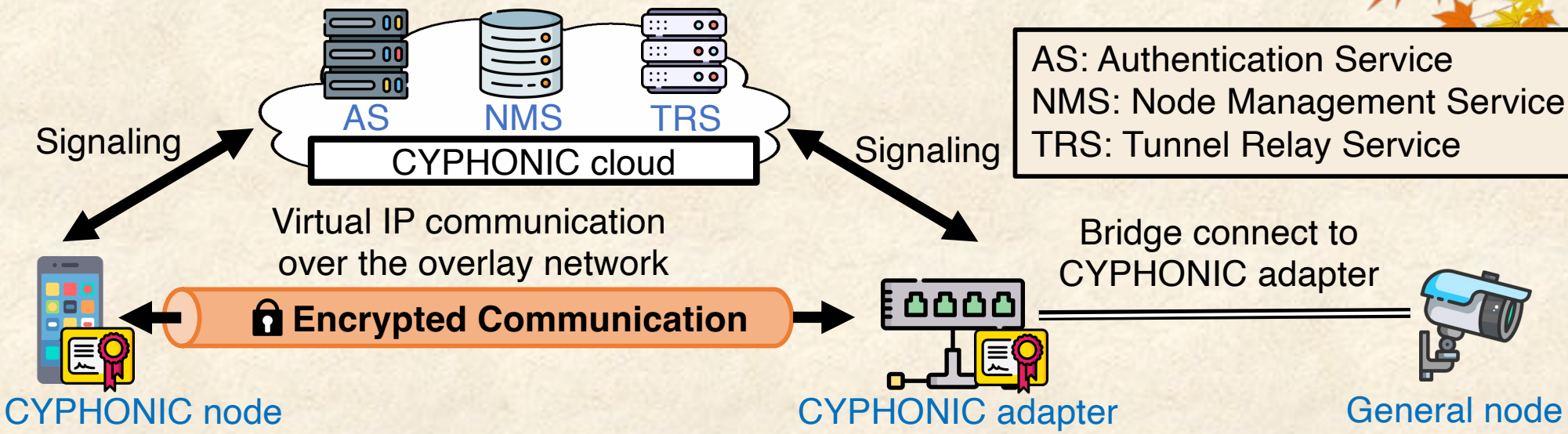
Supporting both IPv4 and IPv6 protocols in just one CYPHONIC adapter.

- Since CYPHONIC supports IPv4 and IPv6 networks to connect a network, new CYPHONIC adapter also works in IPv4 or IPv6 network environments.
- The type of virtual IP address can be easily selected according to the setting of the general node.

Configurating general nodes based on IPv6 mechanism.

- New CYPHONIC adapter can assign virtual IPv6 addresses to general nodes using the basic IPv6 protocols.

Components of CYPHONIC



CYPHONIC cloud (AS / NMS / TRS)

CYPHONIC's cloud services provides automatic authentication of all nodes, management of connected network information, and decides communication path, and relays communications between IPv4-IPv6 or NAPT-NAPT environments.

CYPHONIC node

Device with the CYPHONIC's client program.
Secure end-to-end communication over our overlay network using virtual IP addresses.
CYPHONIC nodes have a virtual IP address used for communication and an FQDN as an identifier.

CYPHONIC adapter

The CYPHONIC adapter is an adapter device that provides over our overlay network communication functions to general nodes that cannot install the CYPHONIC's client program.

Processing function in conventional CYPHONIC adapter

The CYPHONIC adapter has the adapter daemon that combines over our overlay network communication functions with general node management functions.

Signaling Module / Packet Handling Module

These modules provide various functions to communicate over our overlay network.

General Node Management Module

The general node management module manages information used by general nodes for communication.

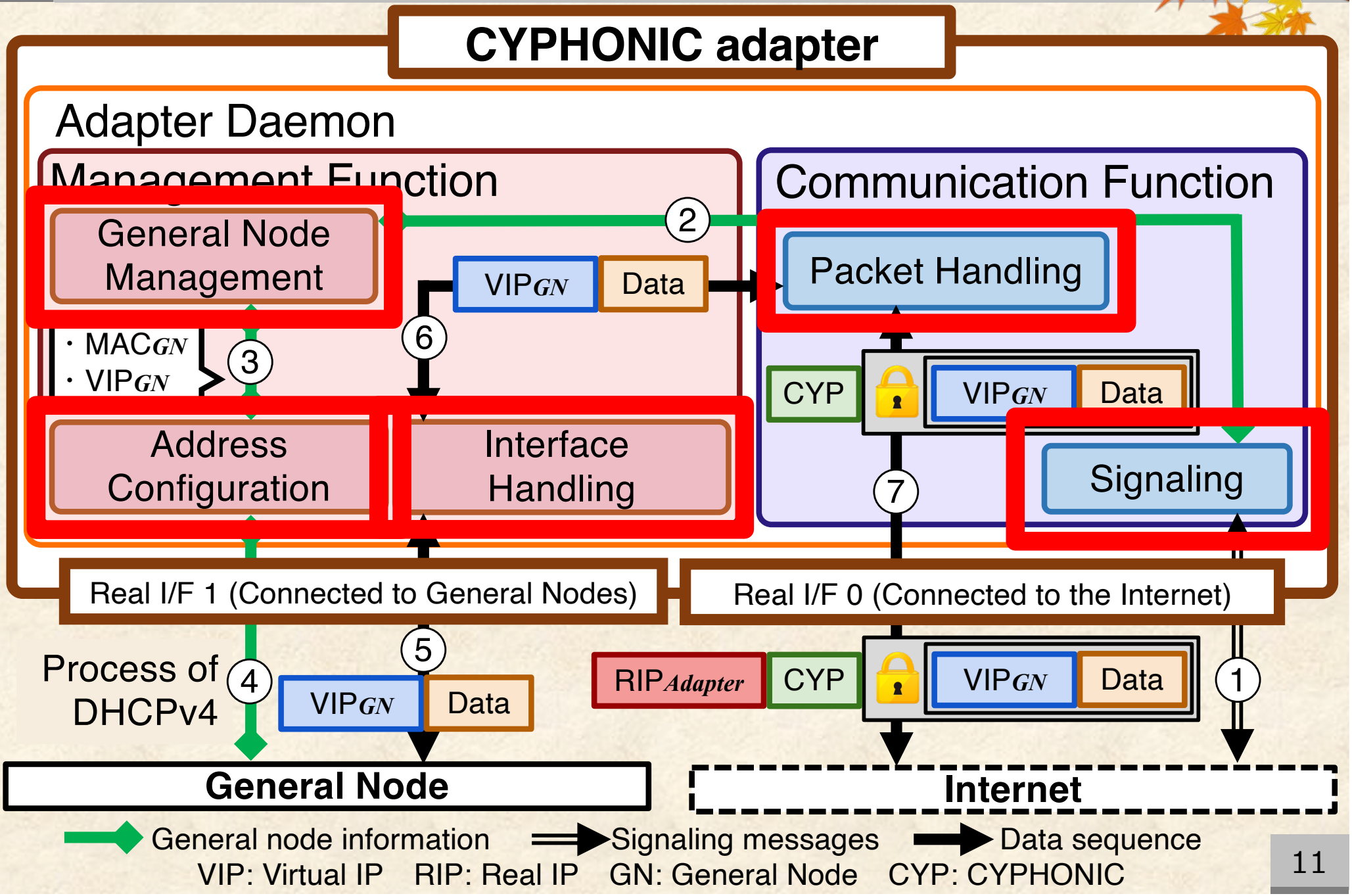
Address Configuration Module

The address configuration module assigns virtual IP address to general nodes.

Interface Handling Module

The interface handling module hooks virtual IP packets from a general node.

System model of conventional CYPHONIC adapter



Requirements for Proposed new CYPHONIC adapter

Functionality as an IPv6 router is required

General node' client mode instructions

The CYPHONIC adapter sends an advertisement message to use the DHCPv6 server and setting the general node to the stateful DHCPv6 mode.

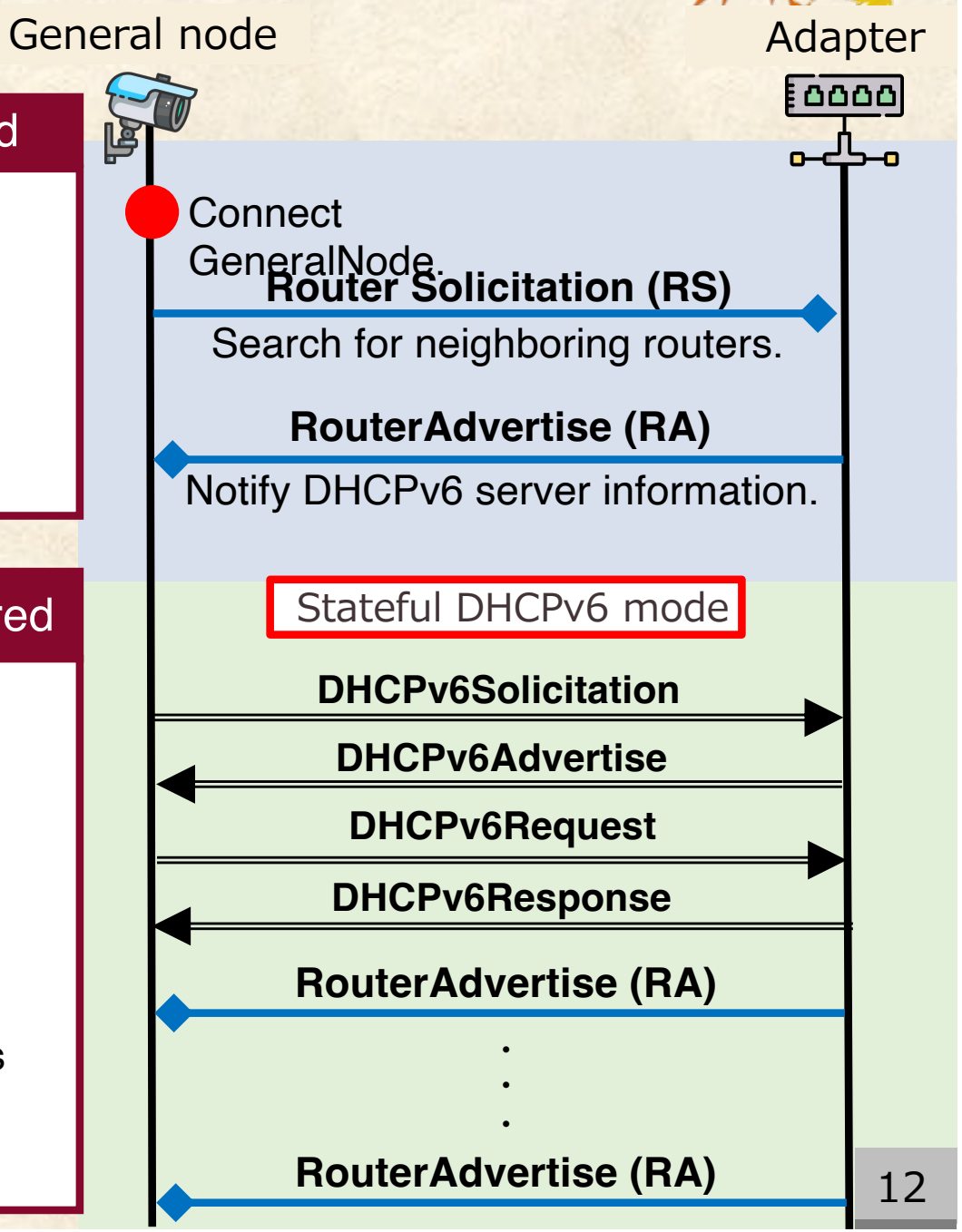
Functionality as a DHCPv6 server is required

Virtual IPv6 address assignment

The CYPHONIC adapter assigns the virtual IPv6 address used for communication as the real IP address.

DNS server information notification

The CYPHONIC adapter hooks DNS requests by periodically proxying router messages to general nodes.



Processing function in new CYPHONIC adapter

NDP: Neighbor Discovery Protocol

In addition to the conventional adapter daemon function, new CYPHONIC adapter includes NDP, DHCPv6 mechanism, and DNS server.

Host Configuration Module

When a general node uses IPv6, the CYPHONIC adapter performs address assignment by coordinating the address configuration module and router configuration module.

Router Configuration Module

- The router configuration module provides a function equivalent to an IPv6 router, which generates NDP messages and sends them to general nodes.
- NDP messages are sent as router messages configured with ICMPv6.

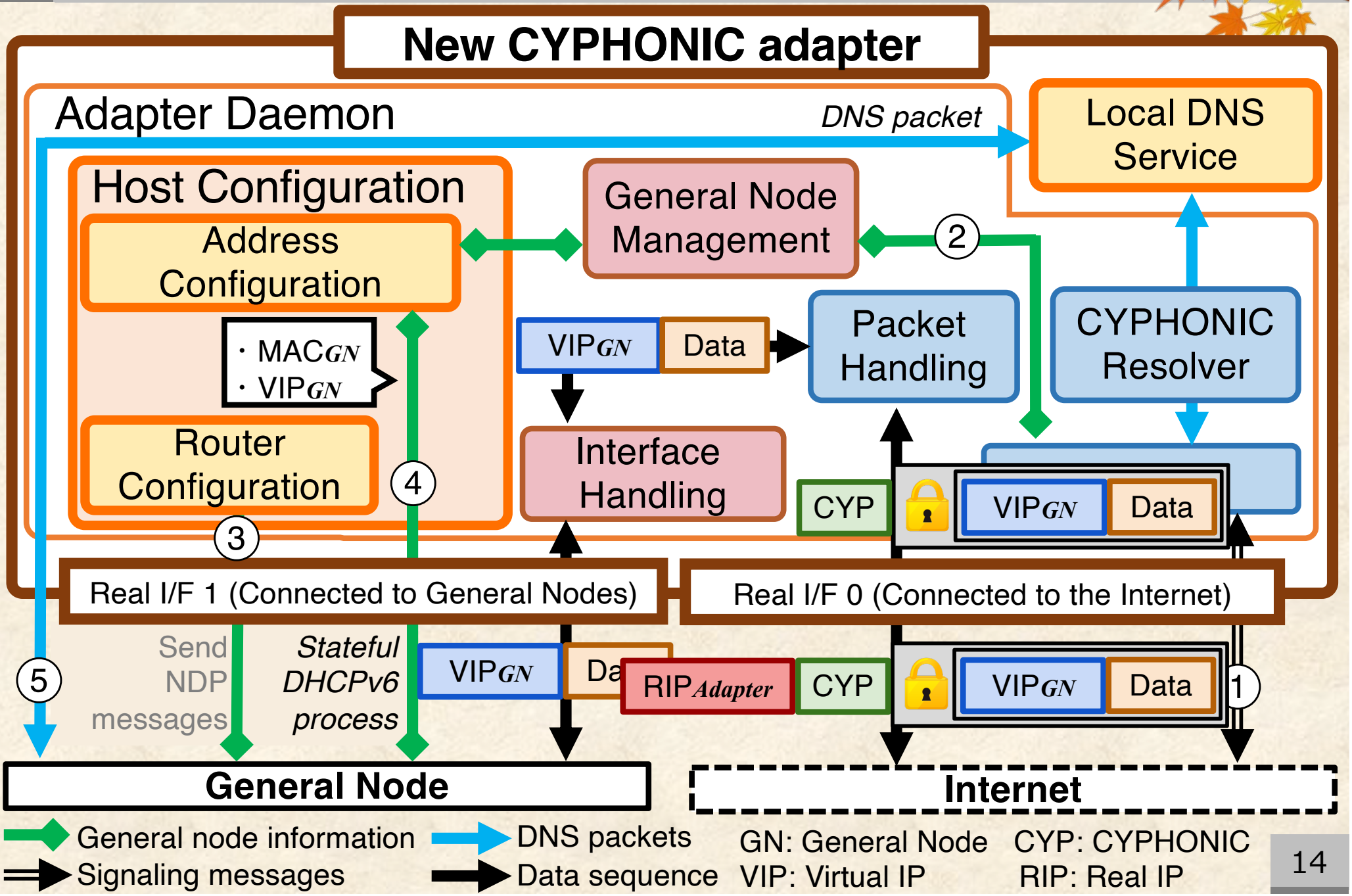
Address Configuration Module

- The address configuration module provides a stateful DHCPv6 mechanism based on the MAC address of the general node.
- The stateful DHCPv6 process explicitly provides all information, including the virtual IP address, default-gateway address, and DNS server address, to the connected general nodes.
- As a DNS server, it informs the “Local DNS Service” information.

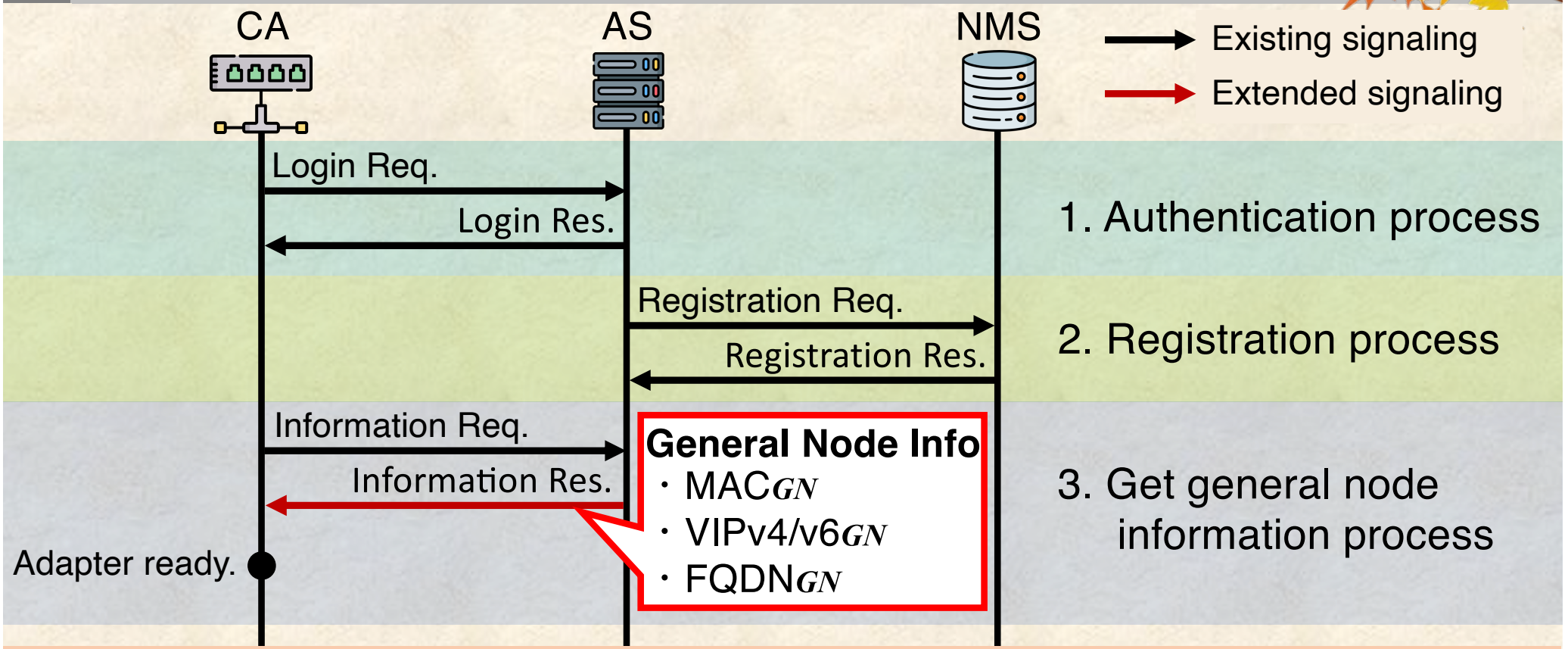
Local DNS Service

This component provides a DNS server to handle DNS requests from general nodes.

System model of New CYPHONIC adapter



Sequence of Get General Node information

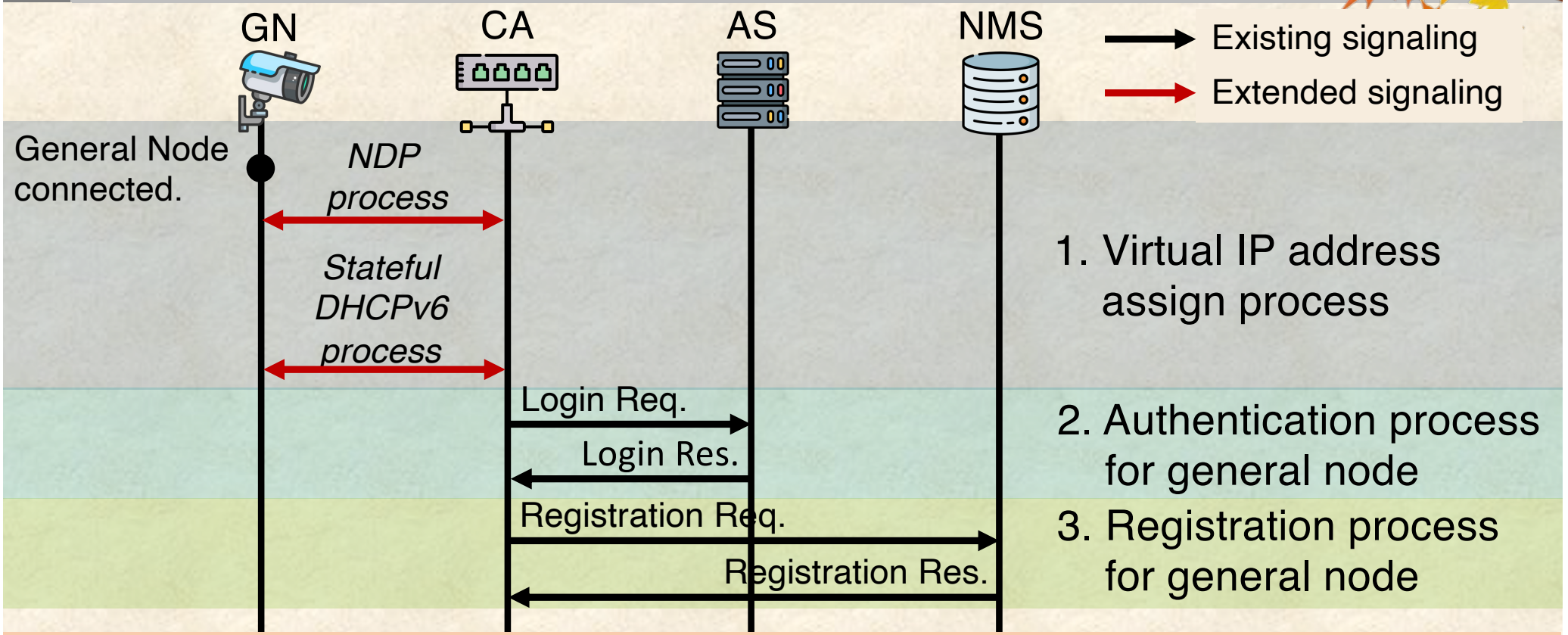


1. The CYPHONIC adapter has the root certificate in advance.
   Then, it performs an authentication process to AS to gain its reliability.

2. The CYPHONIC adapter registers network information to NMS.
   When a node starts communication, the NMS determines the communication path based on the registered information and instructs the node.

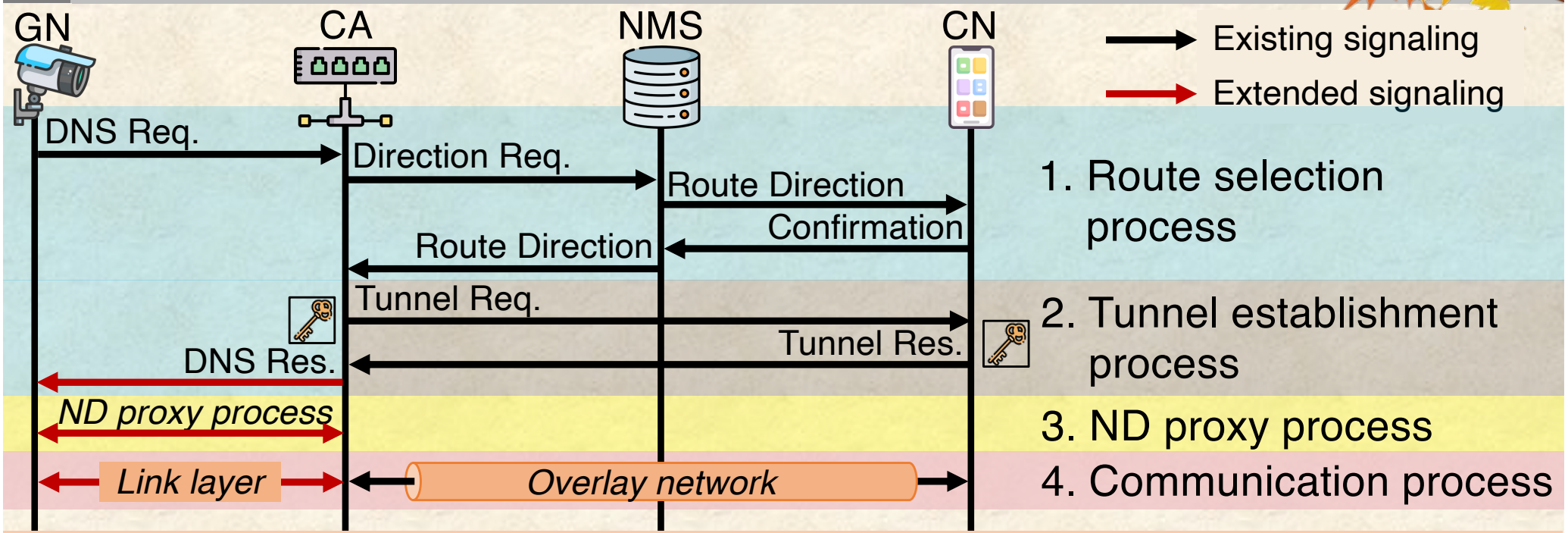
3. The CYPHONIC adapter gets general node information from AS.
   It manages general nodes based on information obtained from cloud services.

Sequence of General Node configuration



1. The CYPHONIC adapter sends RA messages to the general node and configures it as a Stateful DHCPv6 client.
   Then, the CYPHONIC adapter assigns a virtual IPv6 address using the stateful DHCPv6 mechanism when it detects the connection of the general node.
   As a result, the general node can communicate by the virtual IPv6 addresses.
2. The CYPHONIC adapter performs the authentication process to AS to authenticate general nodes.
3. The CYPHONIC adapter registers network information of general nodes to NMS.

Sequence of Overlay network communication



1. The CYPHONIC adapter periodically sends RA messages to hook DNS queries.
   It determines the communication path to the desired FQDN by triggering a DNS query.

2. The CYPHONIC adapter generates an encryption key and exchanges it with the peer node.
   The encryption keys exchanged with the peer node are also managed
   by the CYPHONIC adapter.

3. The CYPHONIC adapter responds with adapter's MAC address,
   when an Neighbor Solicitation (NS) messages for virtual IPv6 of the peer node is received.

4. The CYPHONIC adapter hooks up virtual IPv6 packets through link layer communication
   and forwards the packets it processes to our overlay network.

Performance evaluation

Adapter processing time

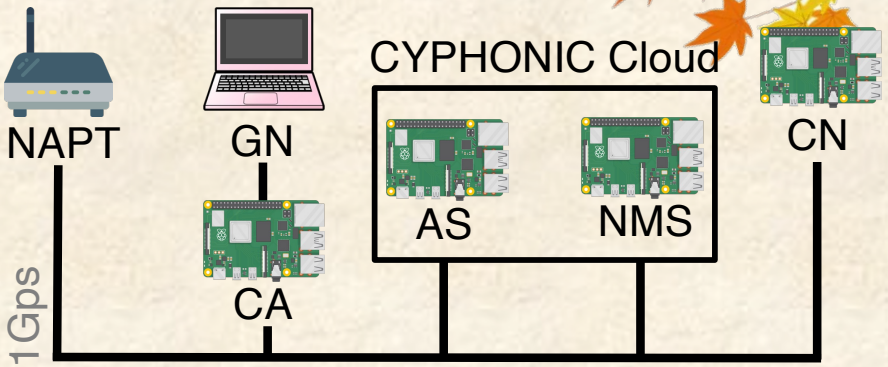
Measuring packet processing time and signaling processing time.

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

Communication delay time

Measuring the communication delay time of the general node.

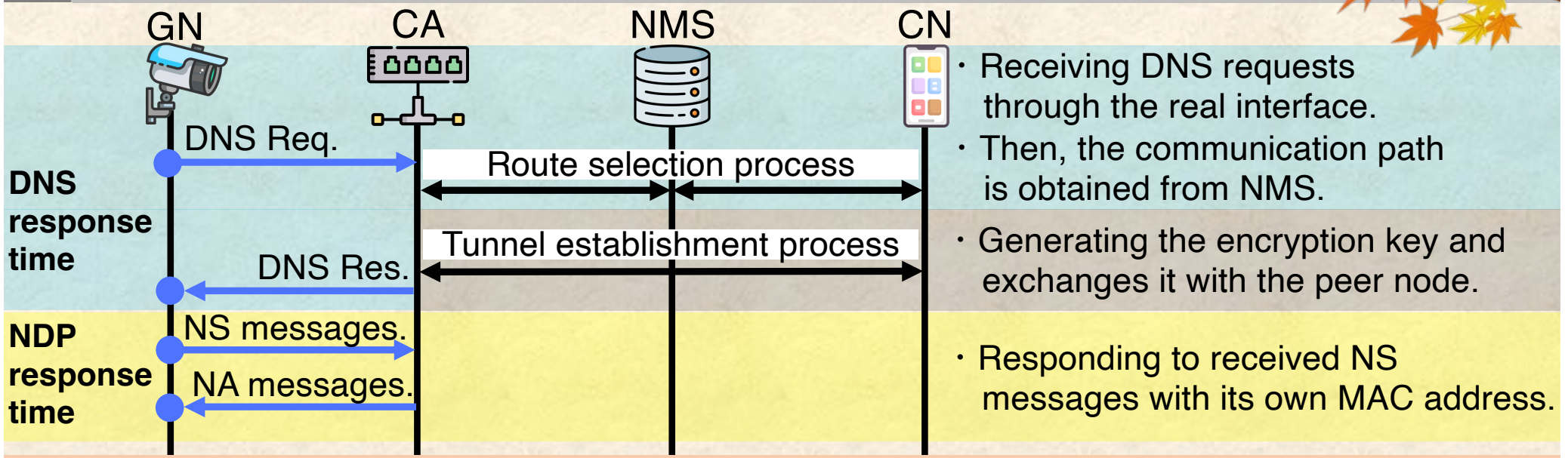
- DNS and NS message response time
- Round-trip time
- Communication throughput



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

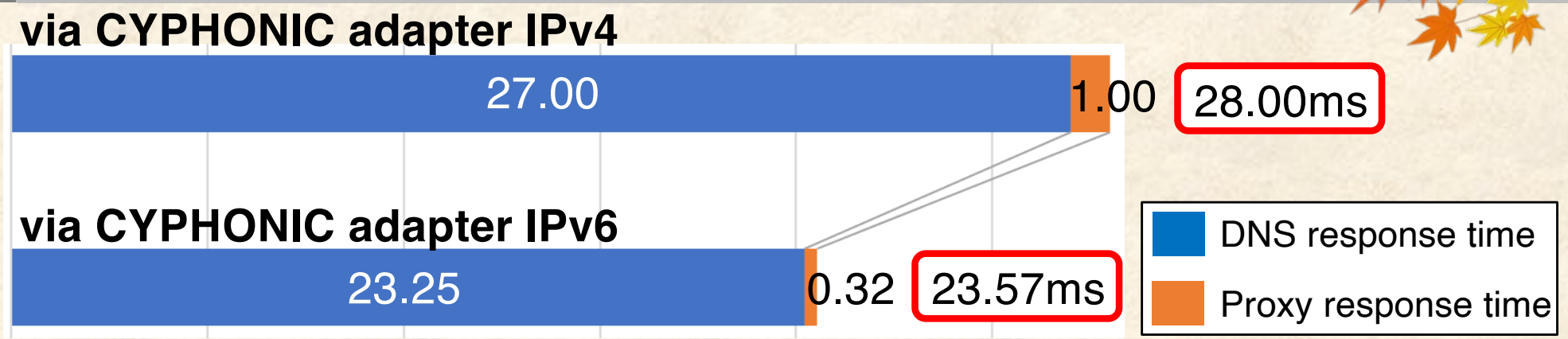
Process to be evaluated



Measure the delay time of initial communication

- The general node sends a DNS request to CYPHONIC adapter, when it initiates communication.
- The general node receives a DNS response and forwards it to the application.
- The application on the general node sends an NS messages to the peer node virtual IP address.
  Then, the CYPHONIC adapter responds by generating Neighbor Advertisement (NA) messages as a proxy.
- General node receives NA messages from CYPHONIC adapter.

Delay time of Initial communication



Adapter processing time		
	CYPHONIC adapter v6	CYPHONIC adapter v4
Route selection process time	14.21ms	19.74ms
Tunnel establishment process time	2.38ms	2.75ms
NDP/ARP process time	0.14ms	0.32ms

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

➡ In the proposed system, DNS query processing is separated from the adapter daemon to enable faster processing.

Results of Communication performance

Network Quality: Proposed systems (via CYPHONIC adapter IPv6)	
UDP Throughput	29.8 Mbits/sec
Jitter	0.42 ms
TCP Throughput	32.6 Mbits/sec
Round-trip time	3.45 ms

Network Quality: Conventional systems (via CYPHONIC adapter IPv4)	
UDP Throughput	29.7 Mbits/sec
Jitter	0.40 ms
TCP Throughput	33.3 Mbits/sec
Round-trip time	3.47 ms

Round-trip time

The proposed system showed equivalent measurement results to the conventional IPv4 version of the CYPHONIC adapter.

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

Communication throughput

Measurements showed that both TCP and UDP traffic achieved 30 Mbps with low jitter.

- For example, HD quality video streaming requires 5Mbps.
- The proposed system has good throughput performance required for high throughput applications such as streaming.

Conclusions

We proposed extended CYPHONIC adapter for general nodes with virtual IPv6 addresses

Supporting both IPv4 and IPv6 protocols in just one CYPHONIC adapter.

- Since CYPHONIC supports IPv4 and IPv6 networks to connect a network, new CYPHONIC adapter also works in IPv4 or IPv6 network environments.
- The type of virtual IP address can be easily selected according to the setting of the general node.

Configurating general nodes based on IPv6 mechanism.

- New CYPHONIC adapter can assign virtual IPv6 addresses to general nodes using IPv6 protocols.

The proposed system is capable of providing comparable performance compared to conventional systems.
And, with this proposal, general nodes can use both IPv4 and IPv6 versions with CYPHONIC.

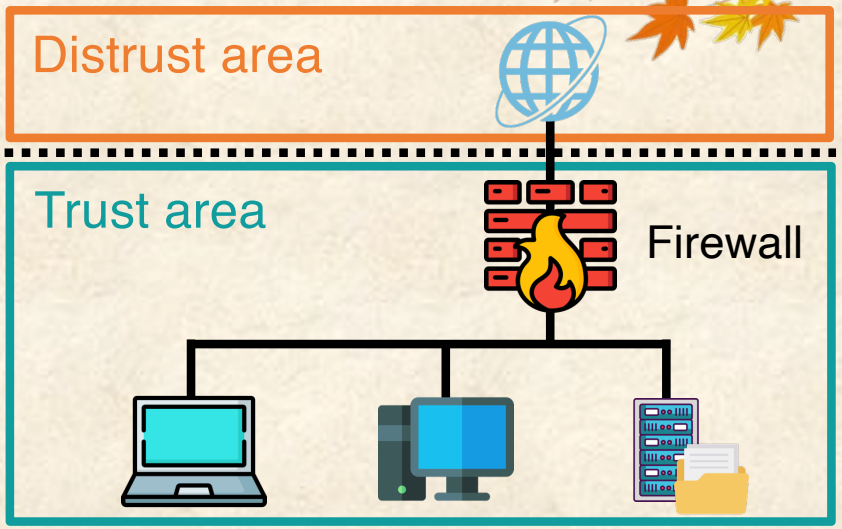
Question & Answer

About Network and Security model

Perimeter security model

(Conventional security measures)

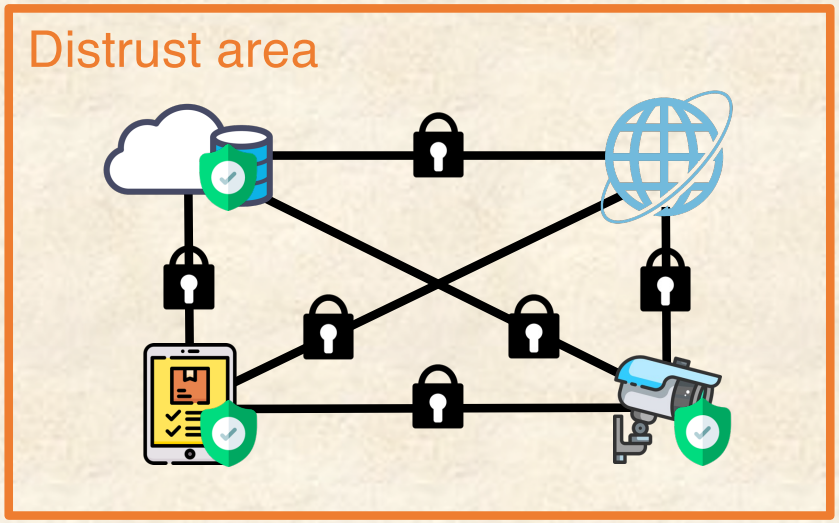
- Establishing a perimeter around the network to protect the internal network from distrusted areas.
- Setting up a Firewall or VPN with a static policy.



Zero-trust security model

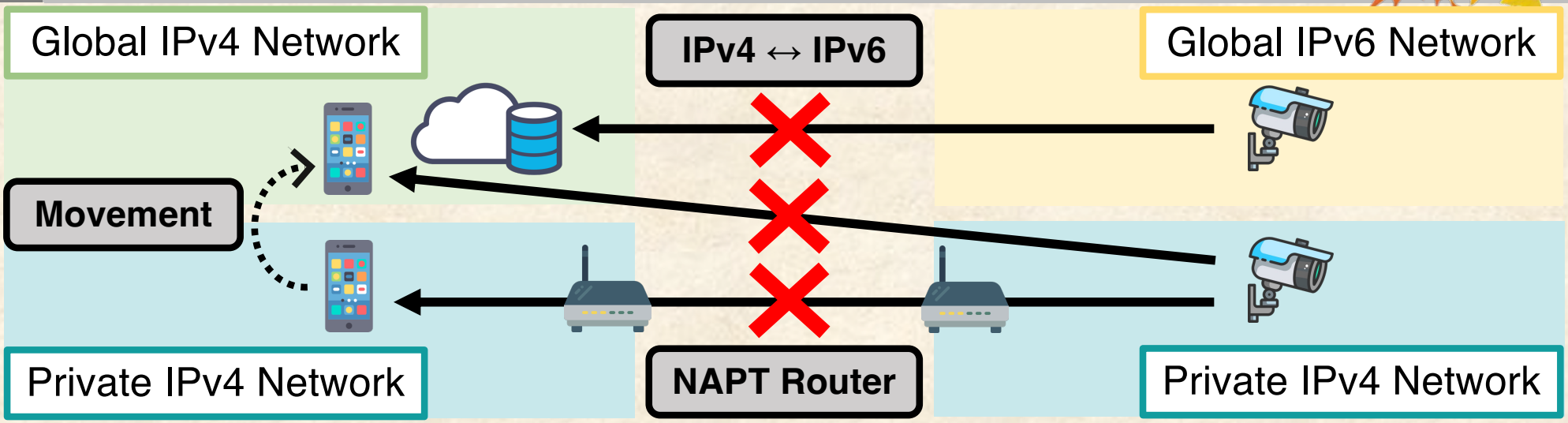
(Security measures required in the future)

- 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.

Processing function in CYPHONIC node

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

Signaling Module

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

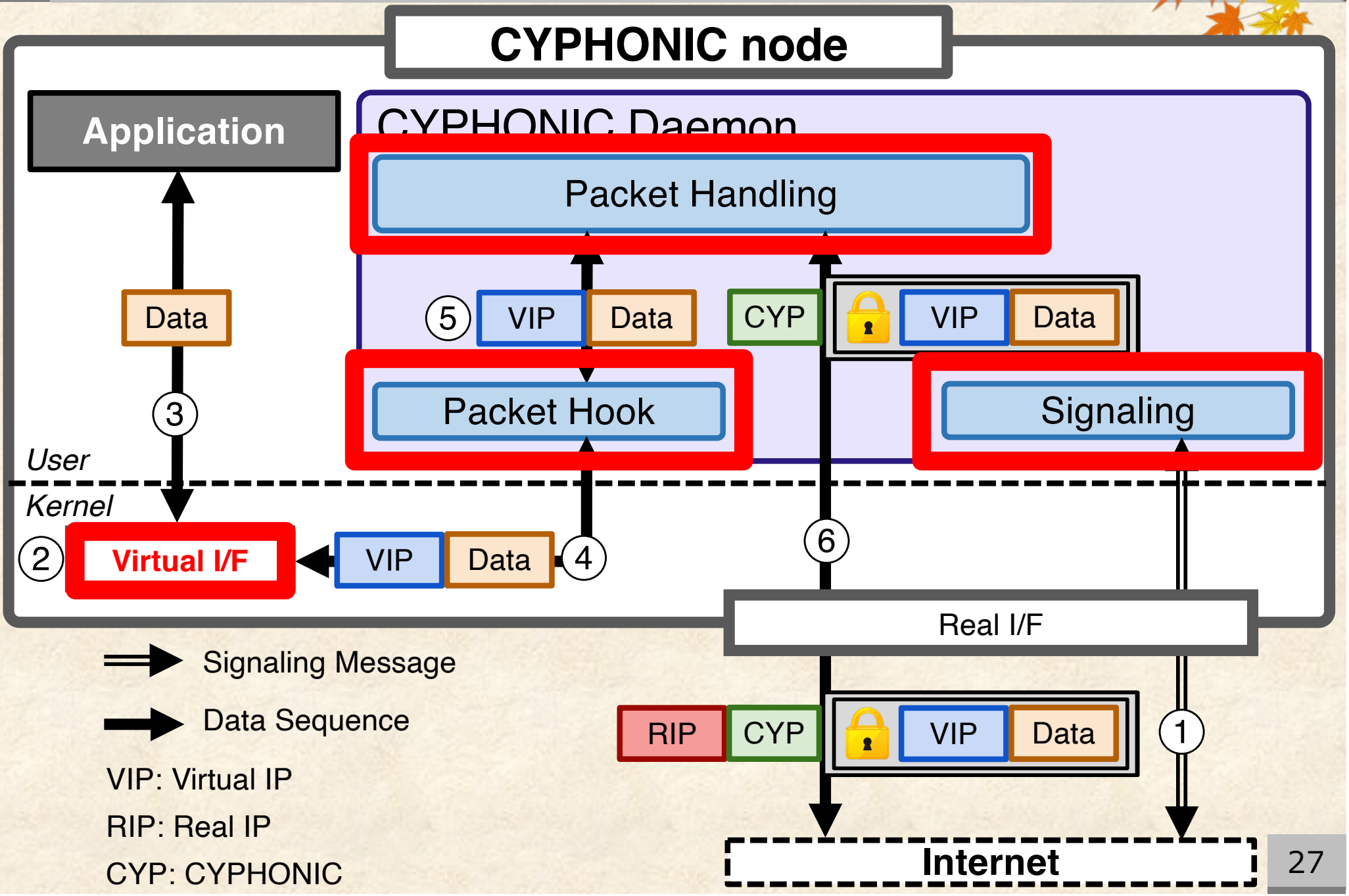
CYPHONIC Resolver Module

The CYPHONIC resolver module generates DNS responses containing virtual IP addresses.

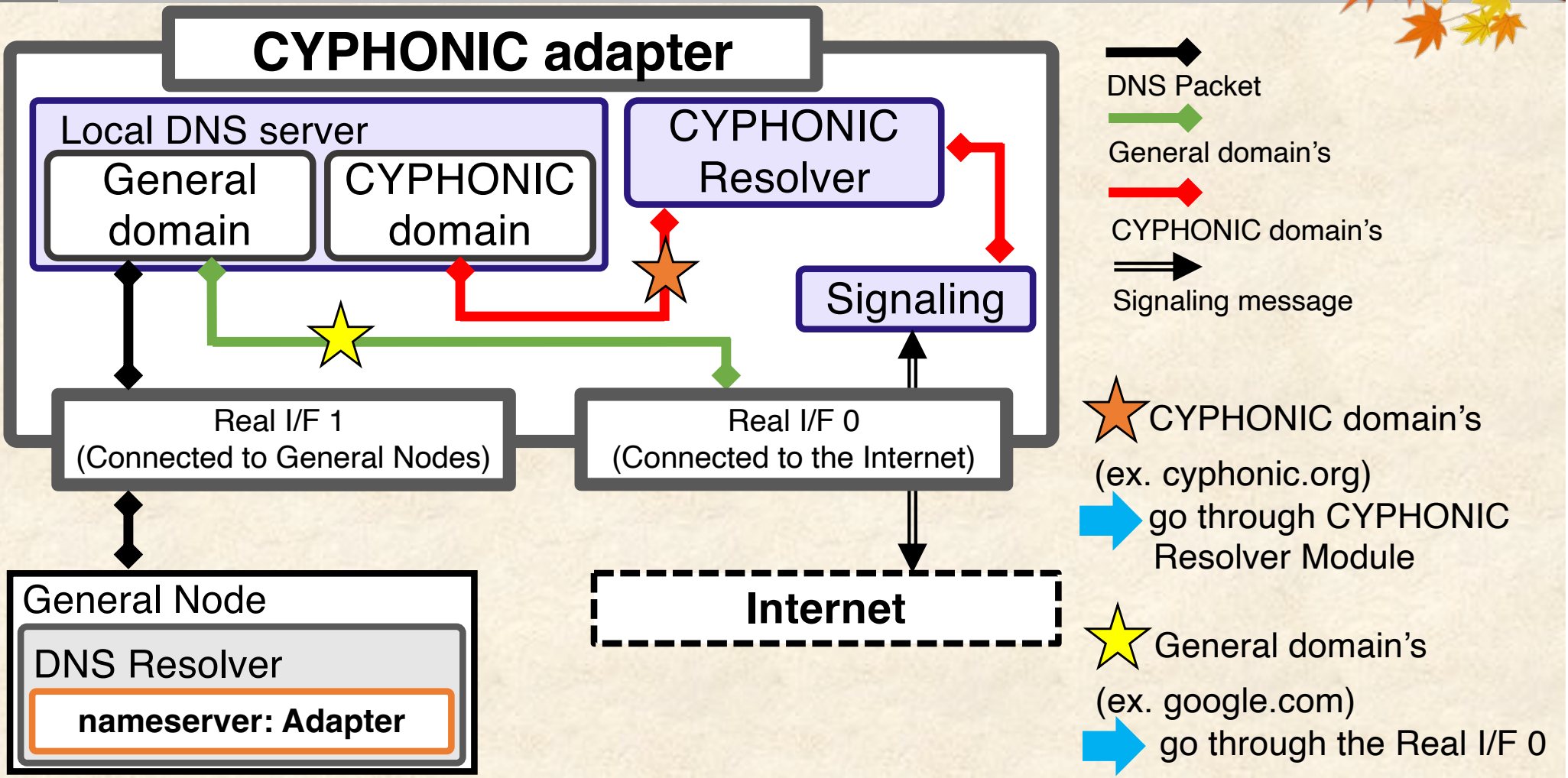
Packet Handling Module

The packet handling module encapsulates/decapsulates and encrypts/decrypts virtual IP packets for communication over our overlay network.

System model of CYPHONIC node

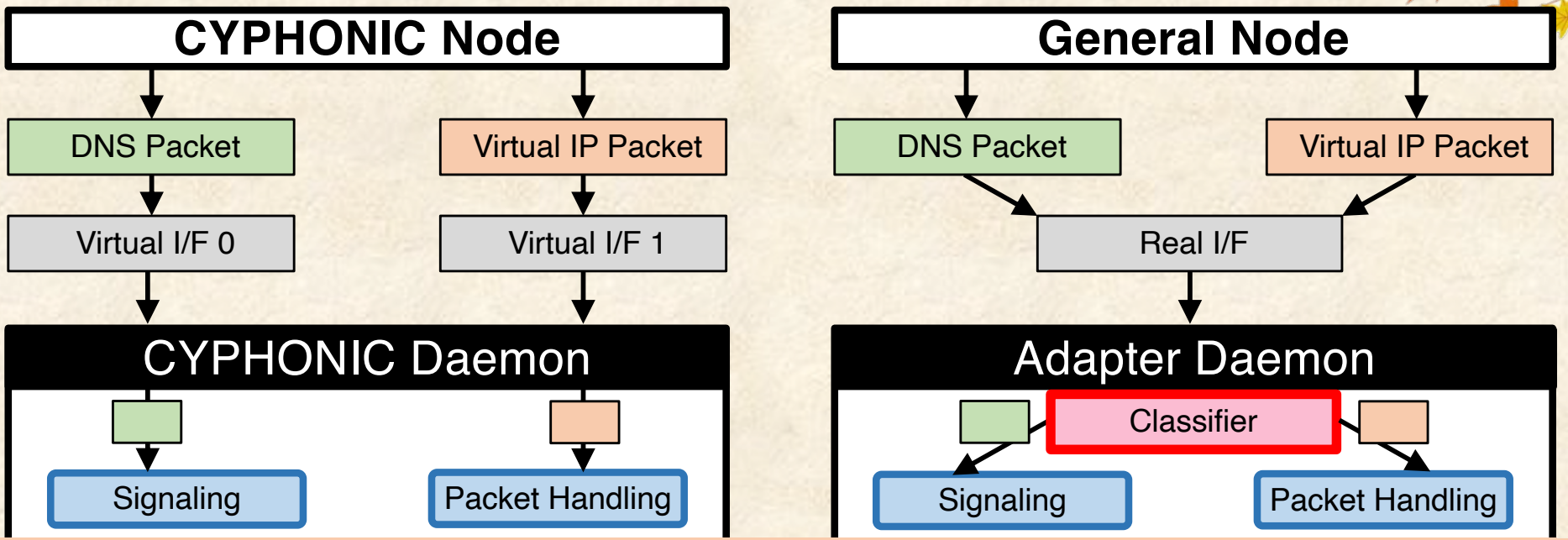


Process of DNS packets



- 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



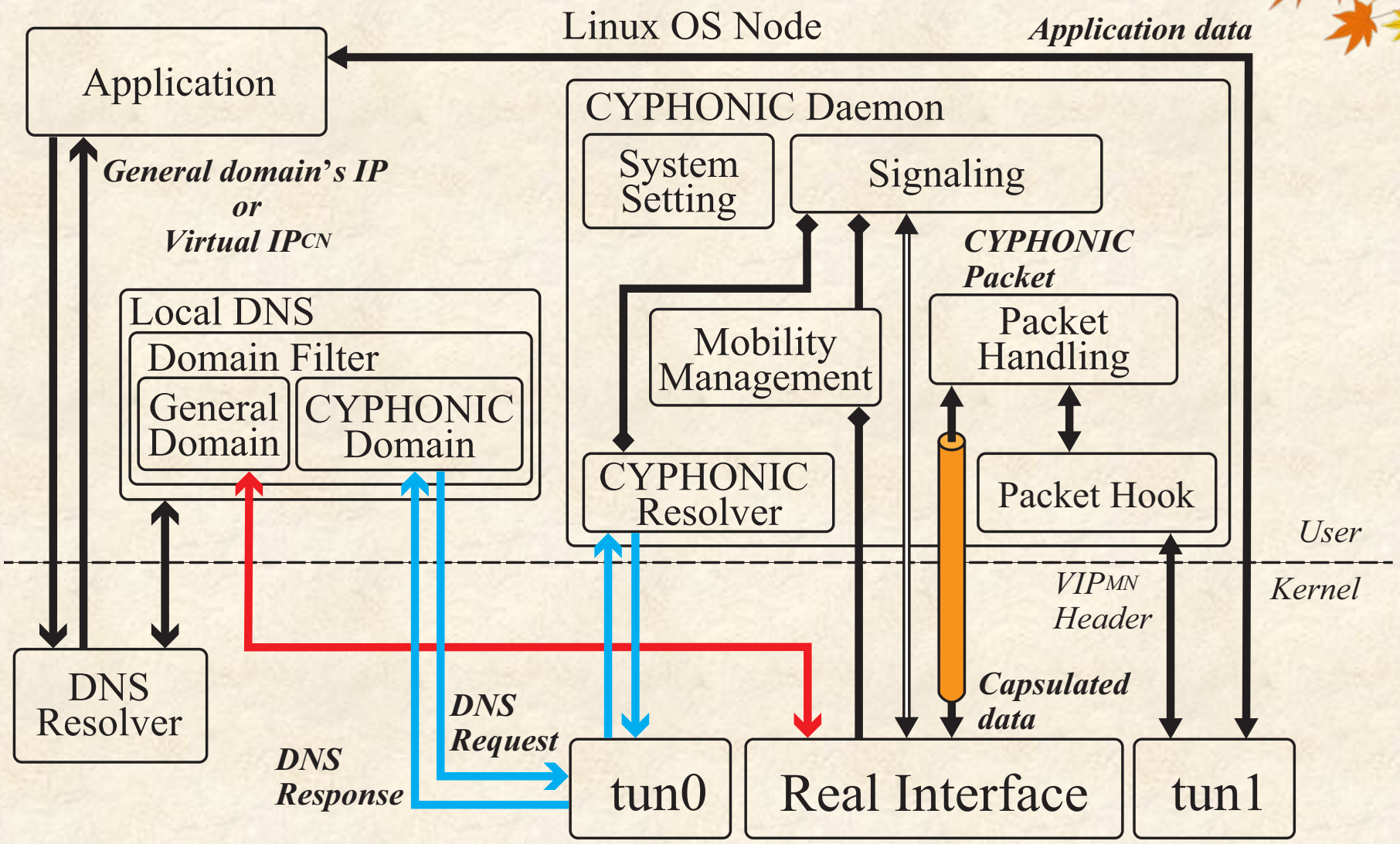
CYPHONIC node

- 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

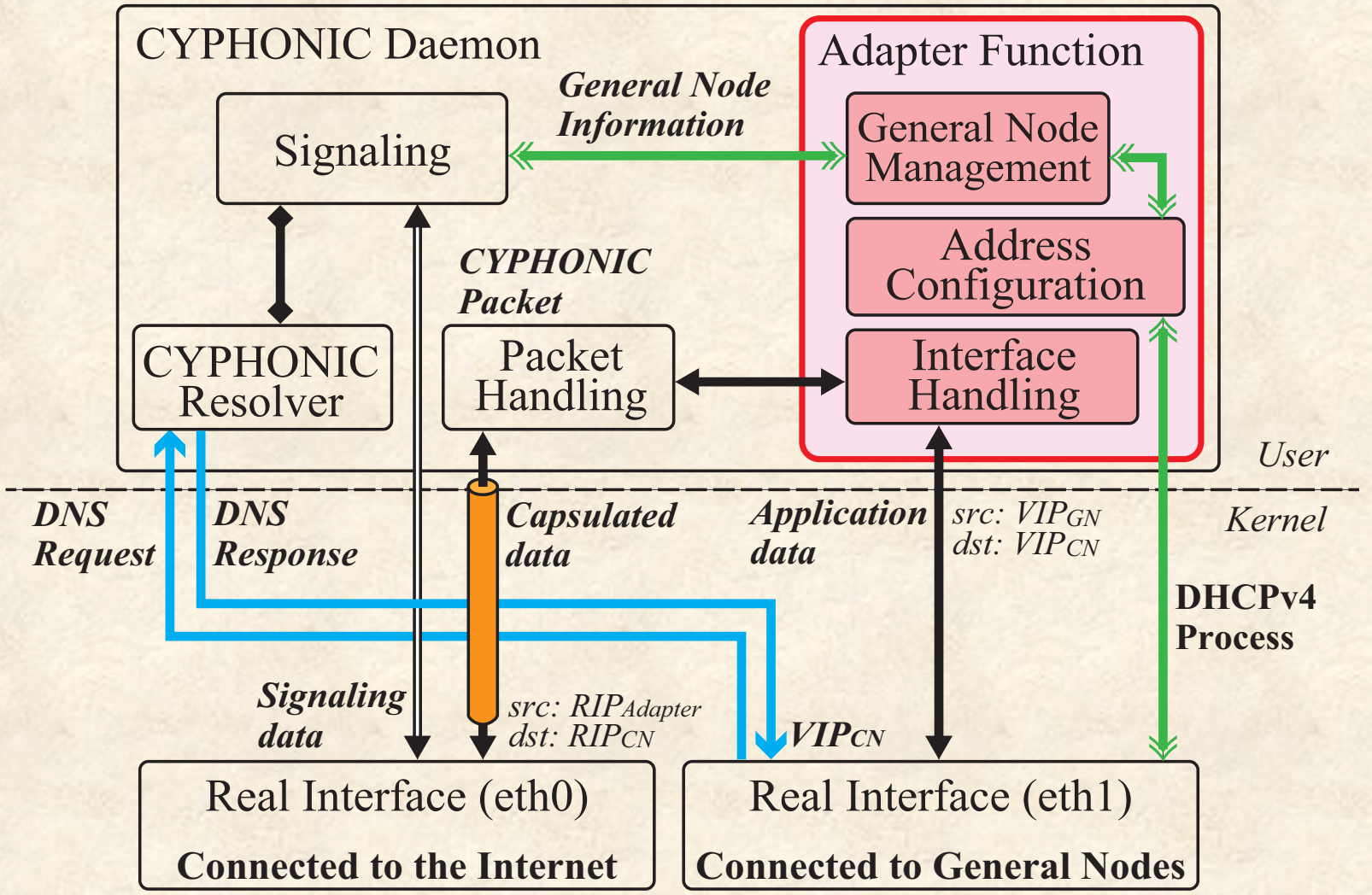
Signaling Message

DNS Packets

Data Sequence

Informations

System model of conventional CYPHONIC adapter



GN: General Node CN: Correspondent Node

RIP: Real IP VIP: Virtual IP

CYPHONIC domain's DNS Packets

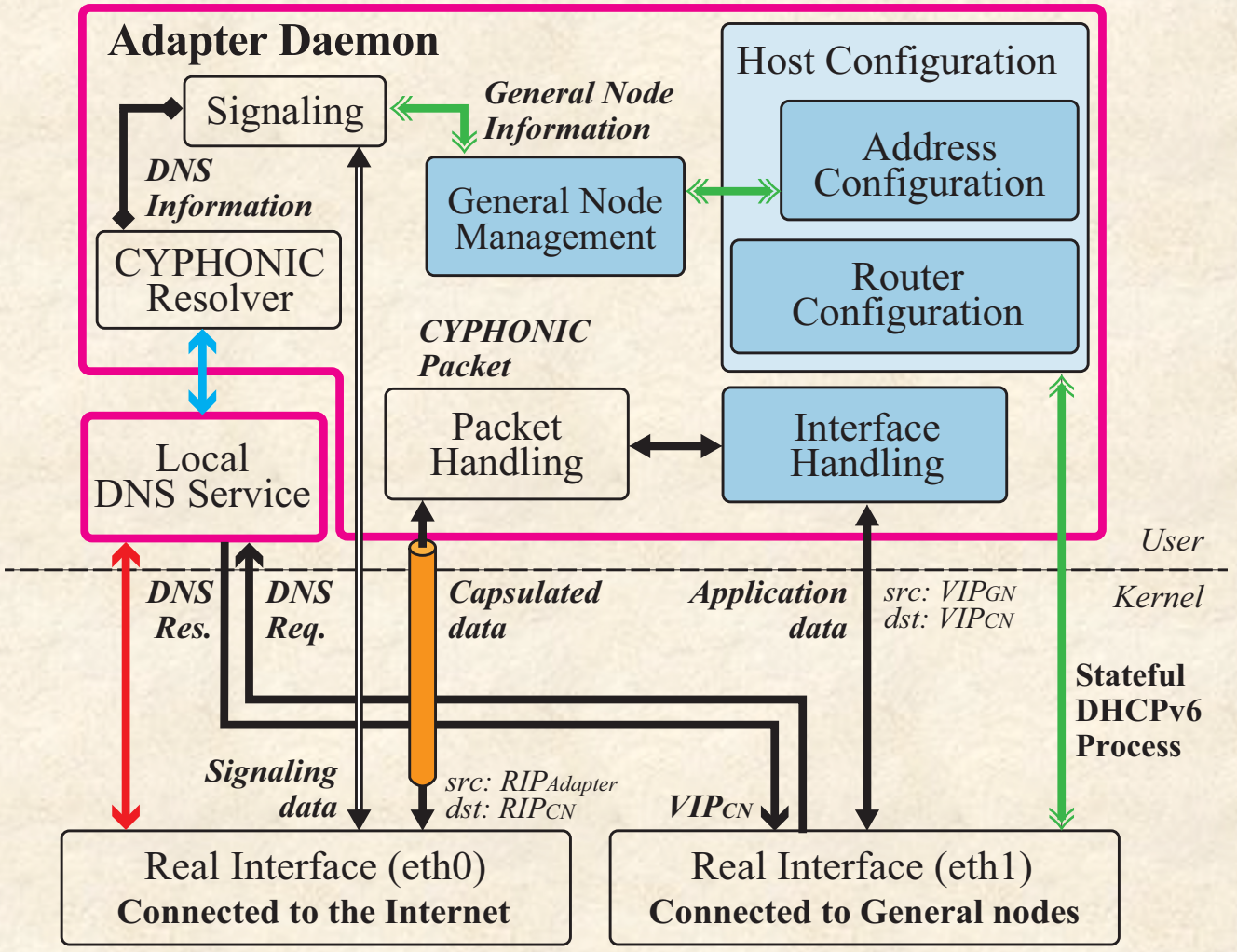
General Node Configuration

Informations

Signaling Message

Data Sequence

System model of New CYPHONIC adapter



GN: General Node CN: Correspondent Node

RIP: Real IP VIP: Virtual IP

CYPHONIC domain's DNS Packets **General domain's DNS Packets**

General Node Configuration **DNS Packets** **Data Sequence**

Signaling Message **Informations**

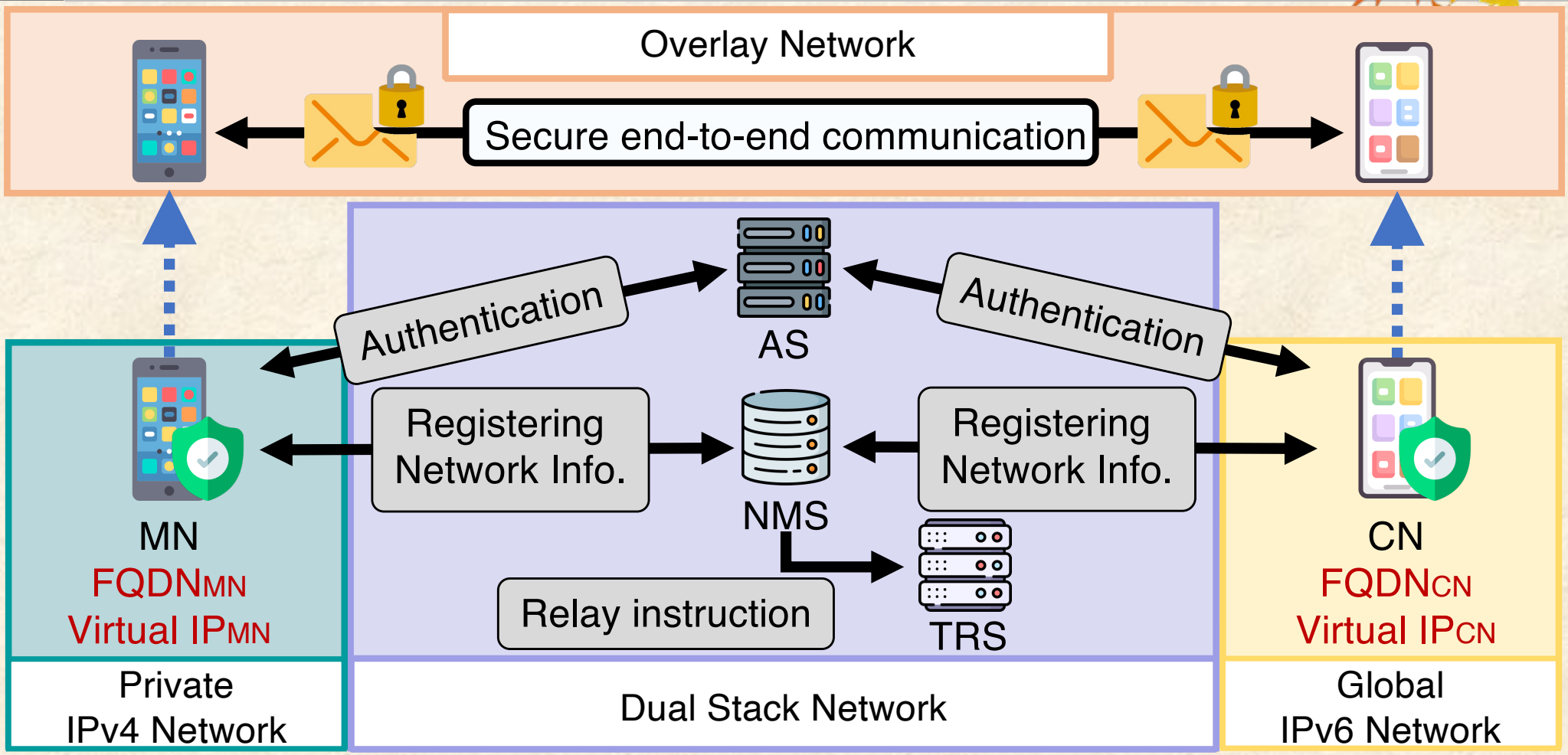
Issues of Conventional Technology

	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.

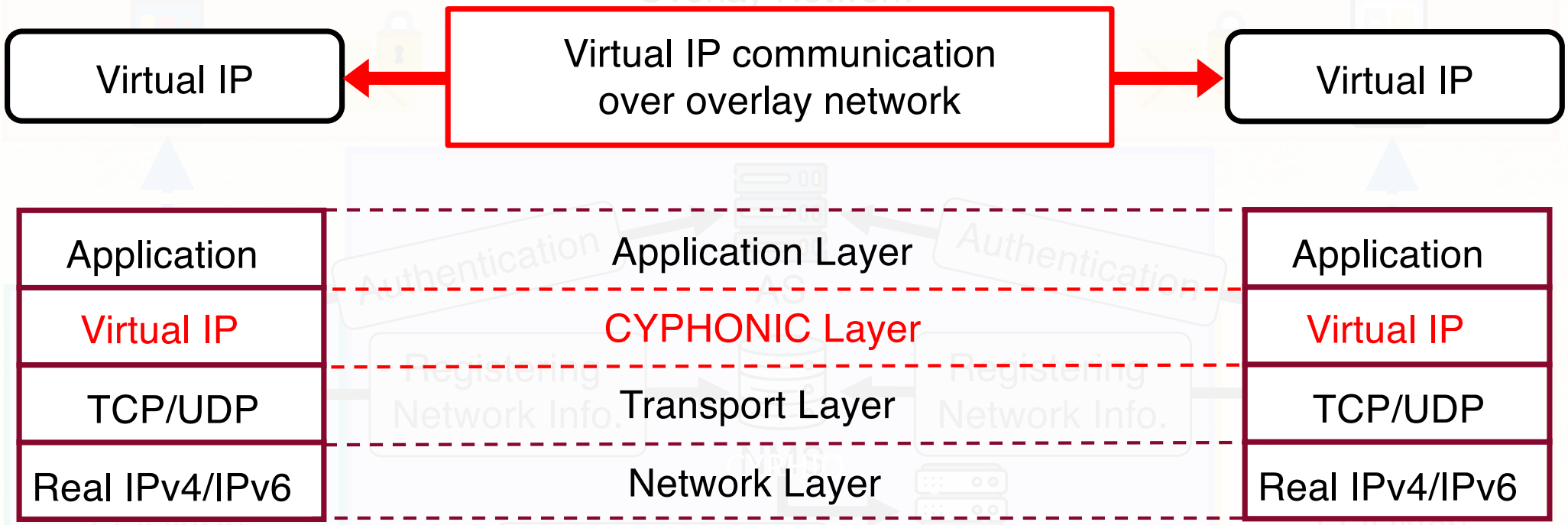
Overview of CYPHONIC



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.

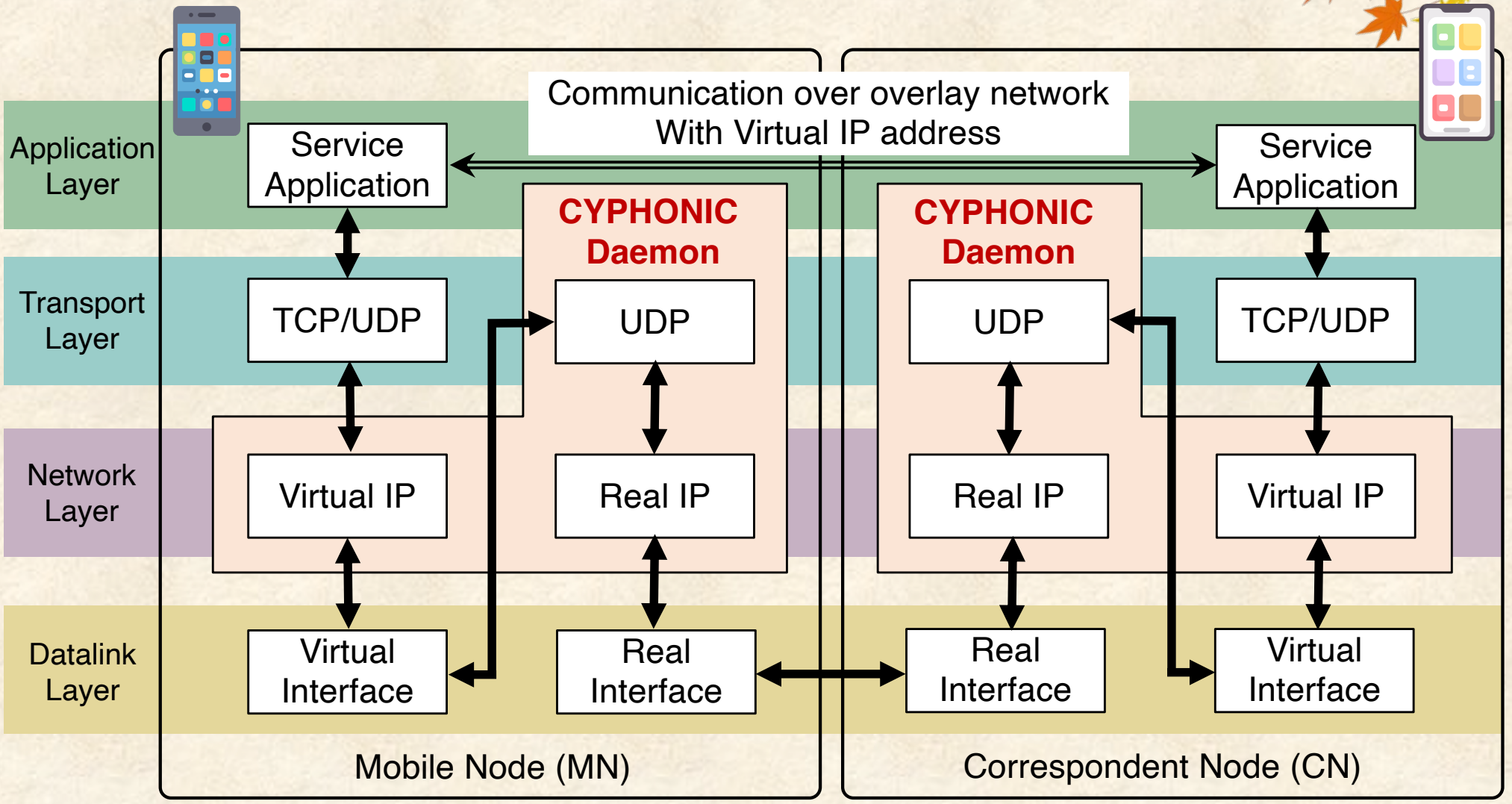
Overview of CYPHONIC



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

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

PDU flow in CYPHONIC



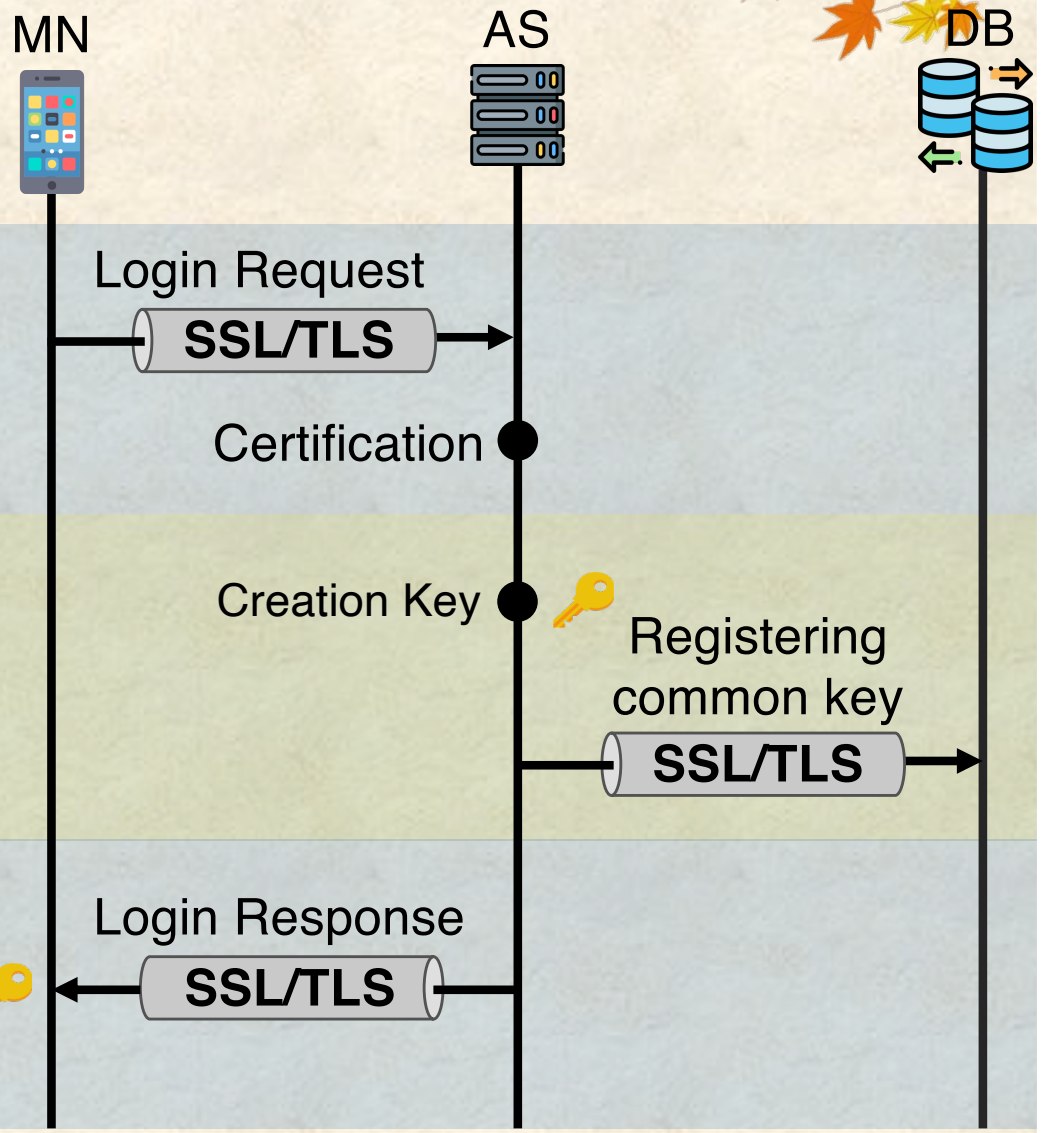
CYPHONIC Daemon gets virtual IP packets from the virtual interface, encapsulates all packets with UDP and sends it from the real interface.

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.

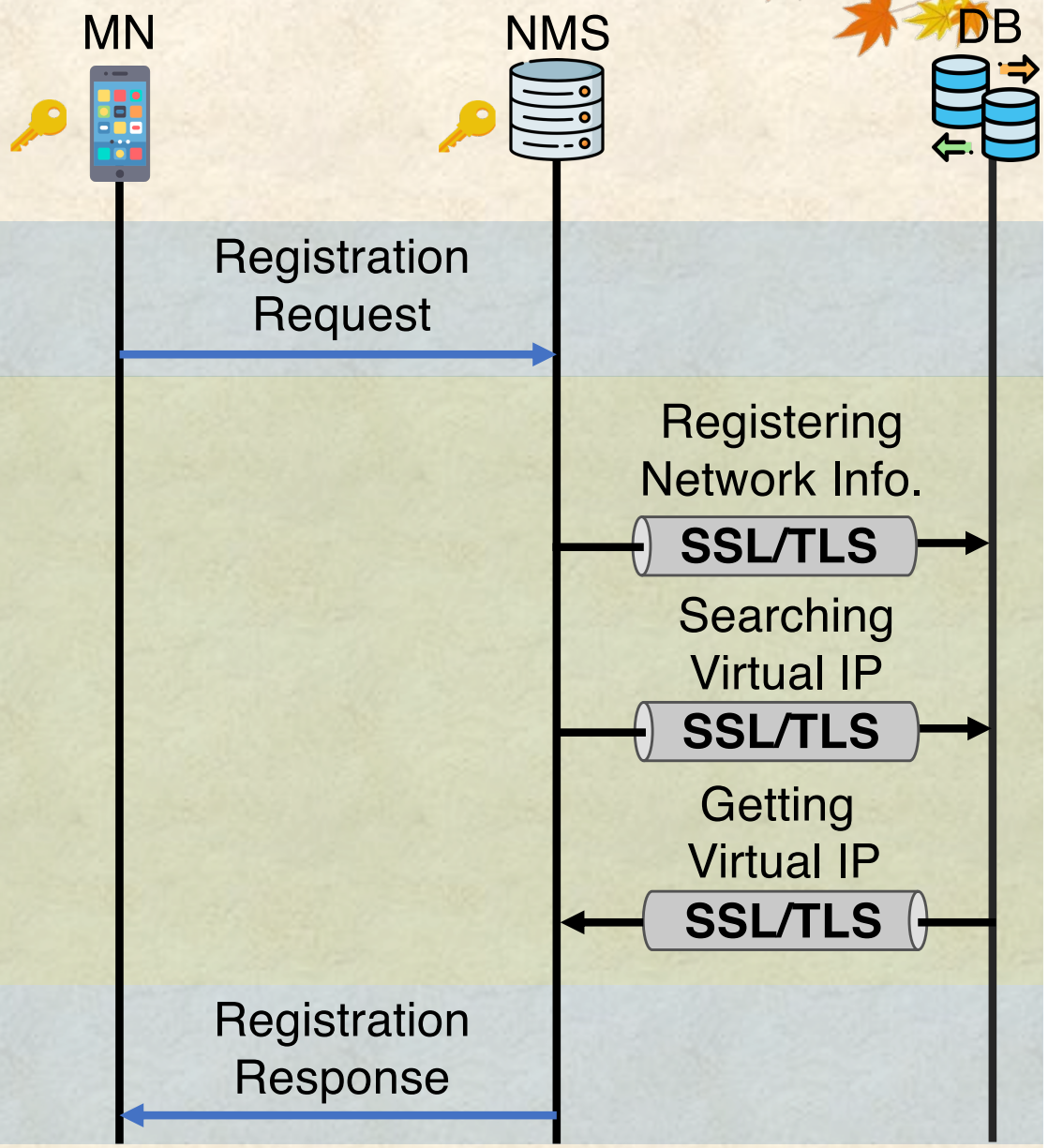


Registration process

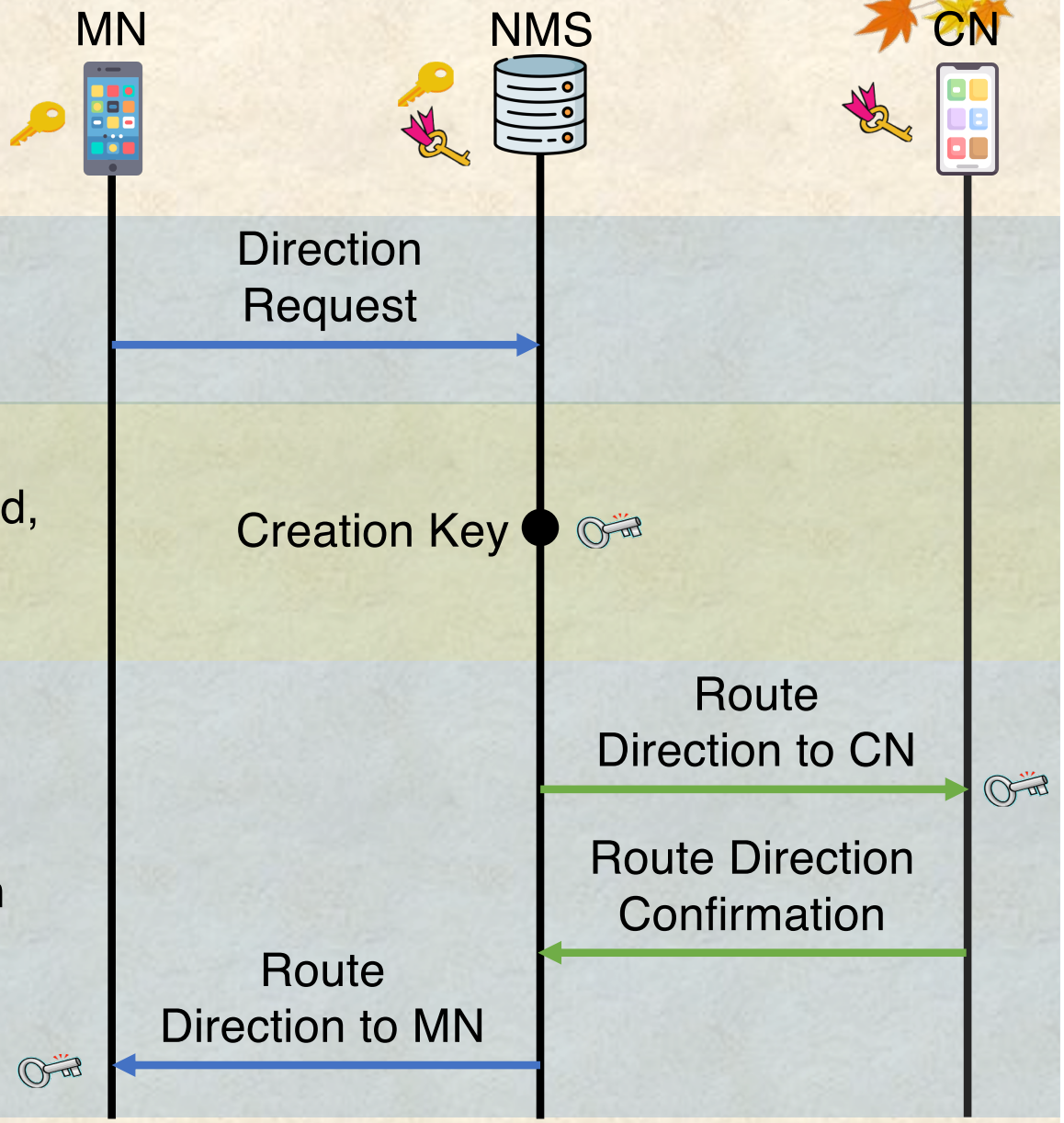
First, sending MN network information to NMS.

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.

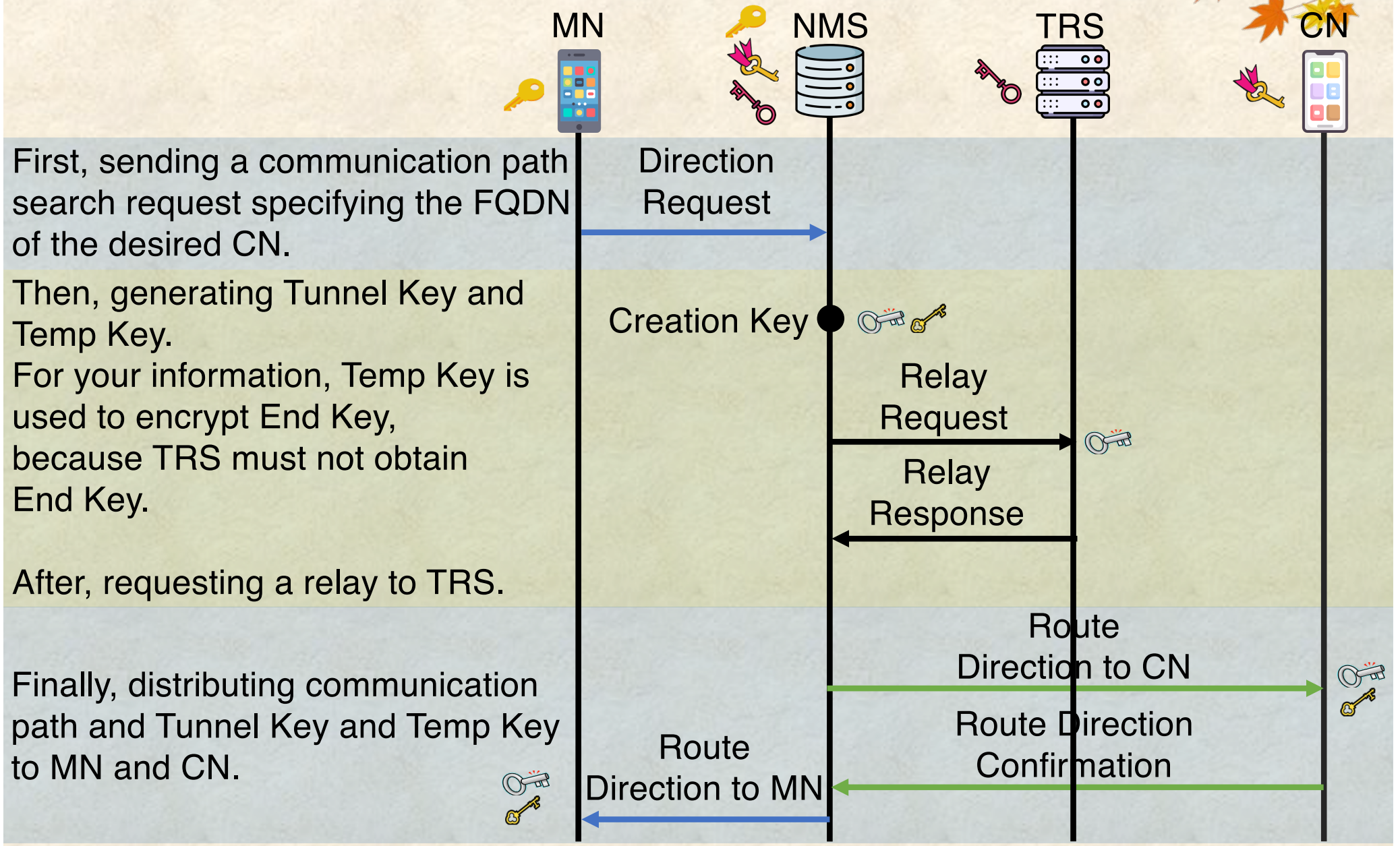
Then, generating Tunnel Key.
For your information, Tunnel Key is used, when both nodes exchange End Key for encrypting sent and received data.

After, distributing communication path and Tunnel Key to CN.

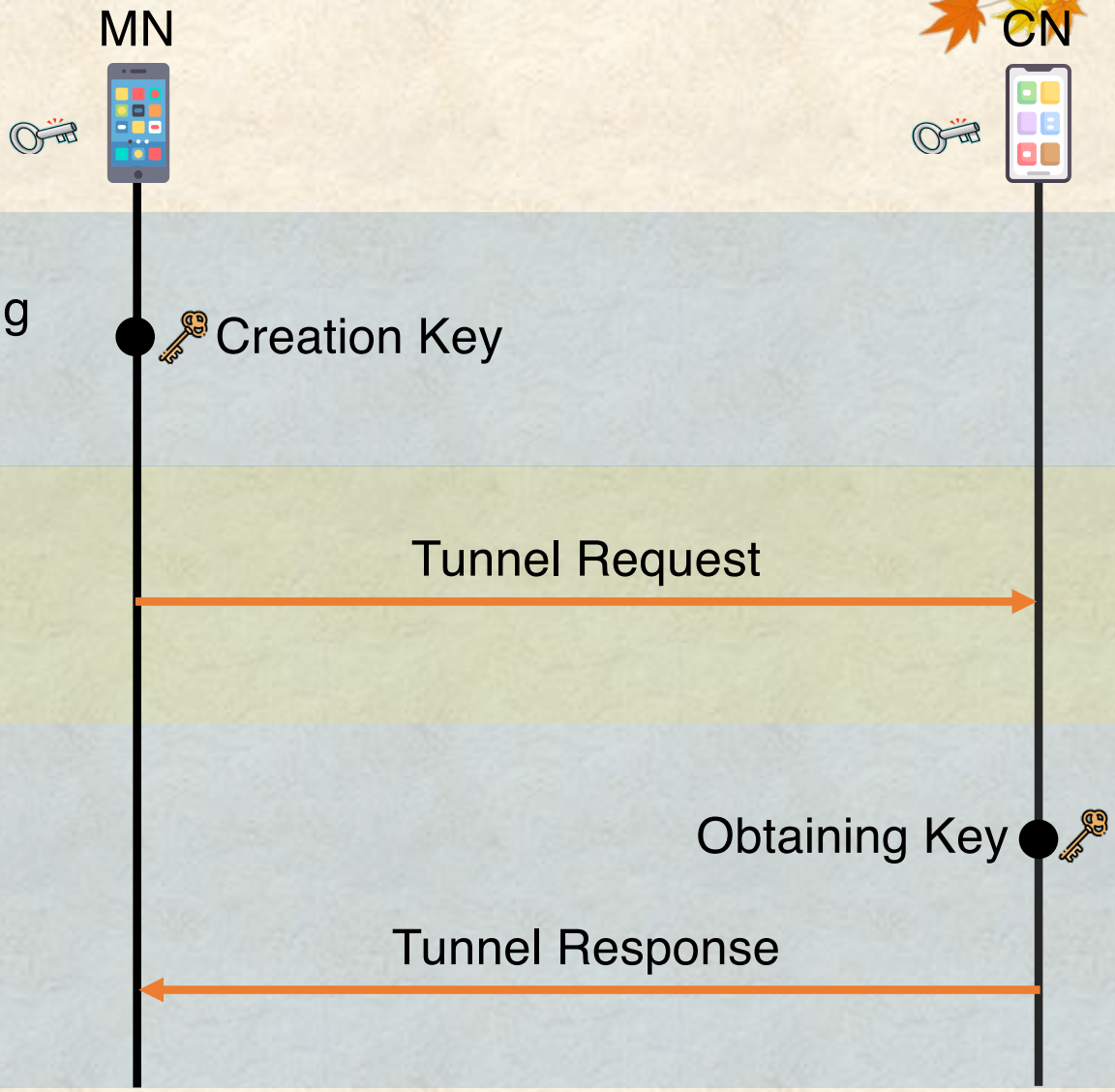
Finally, distributing communication path and Tunnel Key to MN, when NMS received a confirmation response from the CN.

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

Route selection process (via TRS)



Tunnel establishment process



Tunnel establishment process (via TRS)