オーバーレイネットワークにおける一般ノードをサポートするCYPHONICアダプタの研究

研究者 後藤廉　　指導教員 内藤克浩

愛知工業大学 情報科学部 情報科学科
令和3年度 学士論文発表会
2022年 2月 14日 (月)

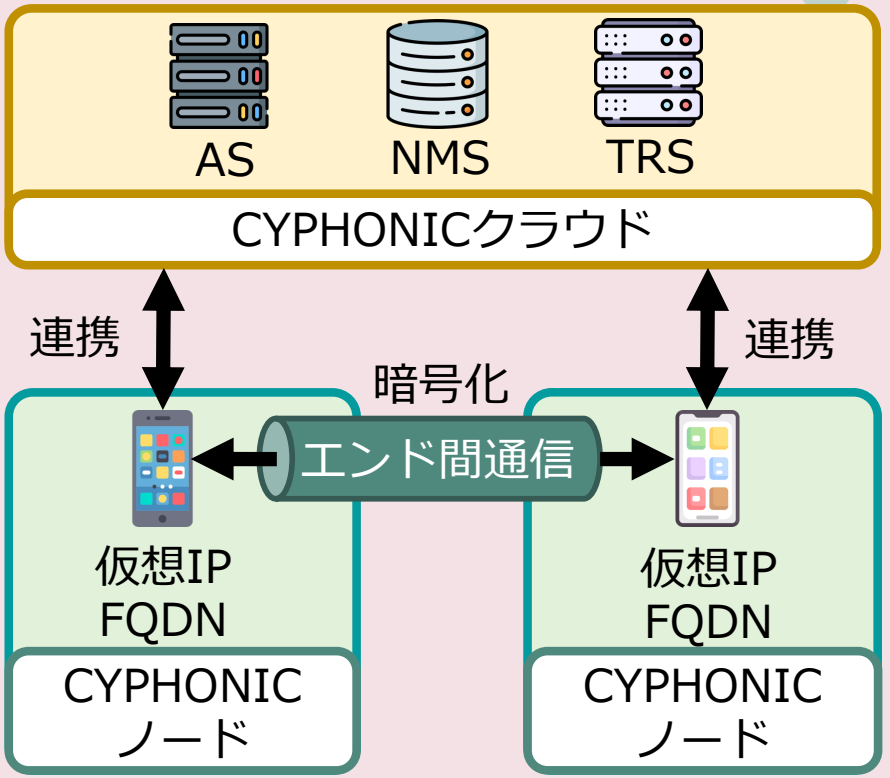
CYPHONIC 概要

セキュアなエンド間通信を
実現する通信フレームワーク

- 端末をクラウドで認証
- エンド間で直接通信
- 送受信データの暗号化

CYPHONICノードの処理

1. クラウドサービスと連携して
   相手ノードへの通信経路を取得
2. 暗号鍵を生成して相手ノードと
   交換することでトンネルを構築
3. 送受信データを暗号化して
   エンド間で直接通信



CYPHONIC Daemon

- シグナリングの実行
- DNSパケットの処理
- 仮想IPパケットの処理

AS: Authentication Service
TRS: Tunnel Relay Service
NMS: Node Management Service

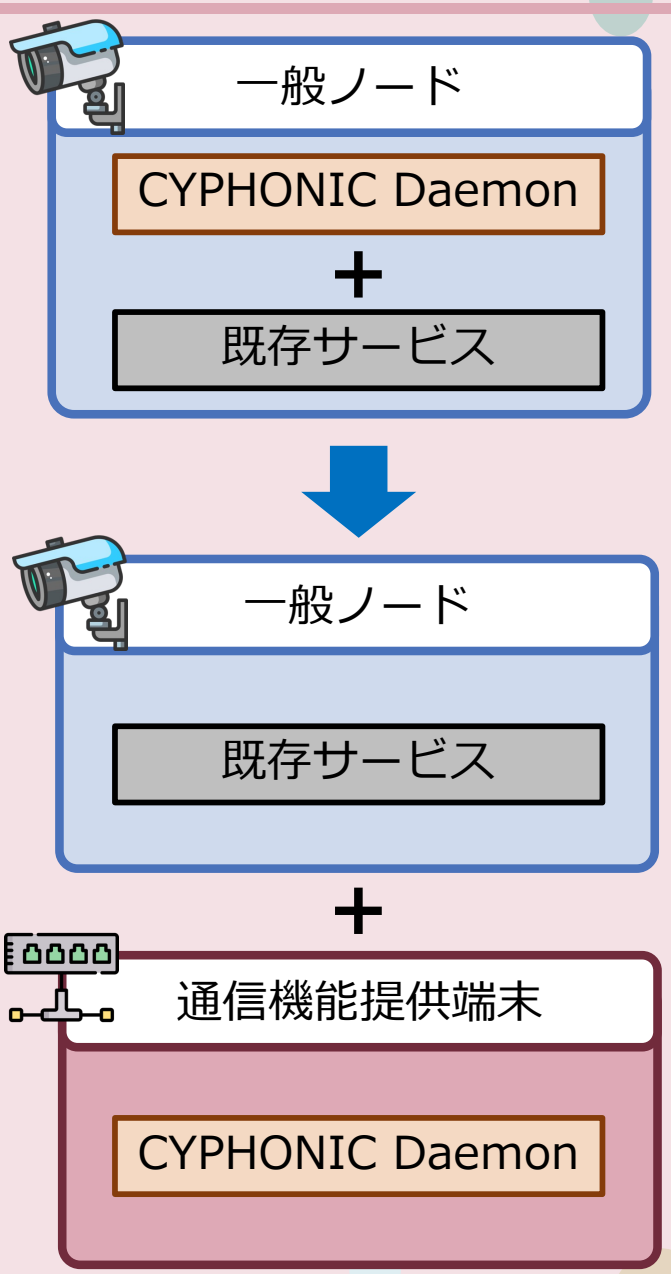
CYPHONIC 課題

端末に改良を加えることが
困難な端末が存在

IoT機器・組込み機器
マスクROMは工場出荷後に
プログラムの変更が極めて困難

特定のサービスを提供する専用サーバ
サービス安定性への影響を懸念して
追加プログラムの導入を避ける傾向

既存の端末やサービスに変更を
加えることなくCYPHONICの機能を
提供可能な仕組みが必要



研究目的

CYPHONICにおける通信処理を代行する
CYPHONICアダプタの提案

CYPHONIC通信機能
CYPHONIC Daemonの既存機能を活用

一般ノード管理機能
アダプタの機能として追加実装

CYPHONICアダプタ 機能概要

CYPHONIC通信機能（既存機能）

シグナリング機能
クラウドから通信に必要な情報を取得

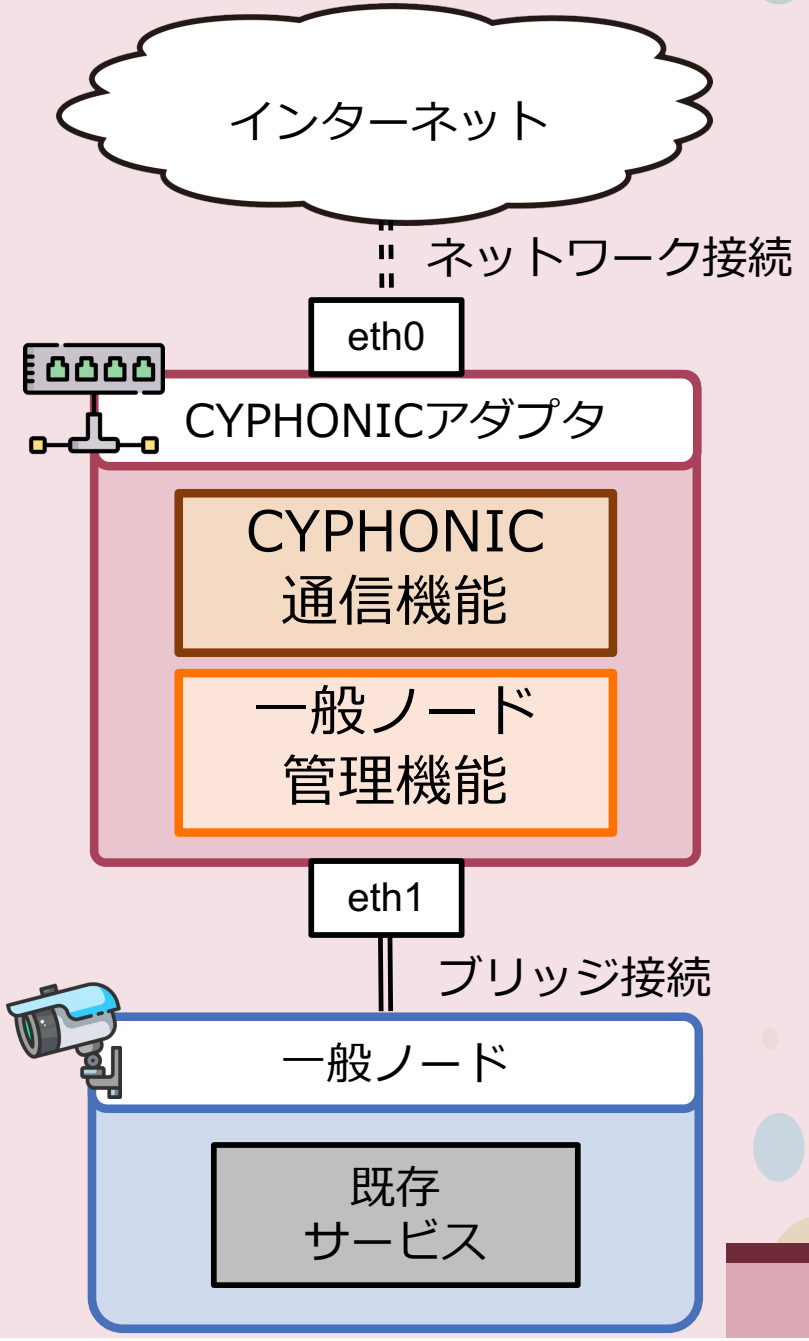
パケット処理機能
カプセル化処理および暗号化処理

一般ノード管理機能（追加機能）

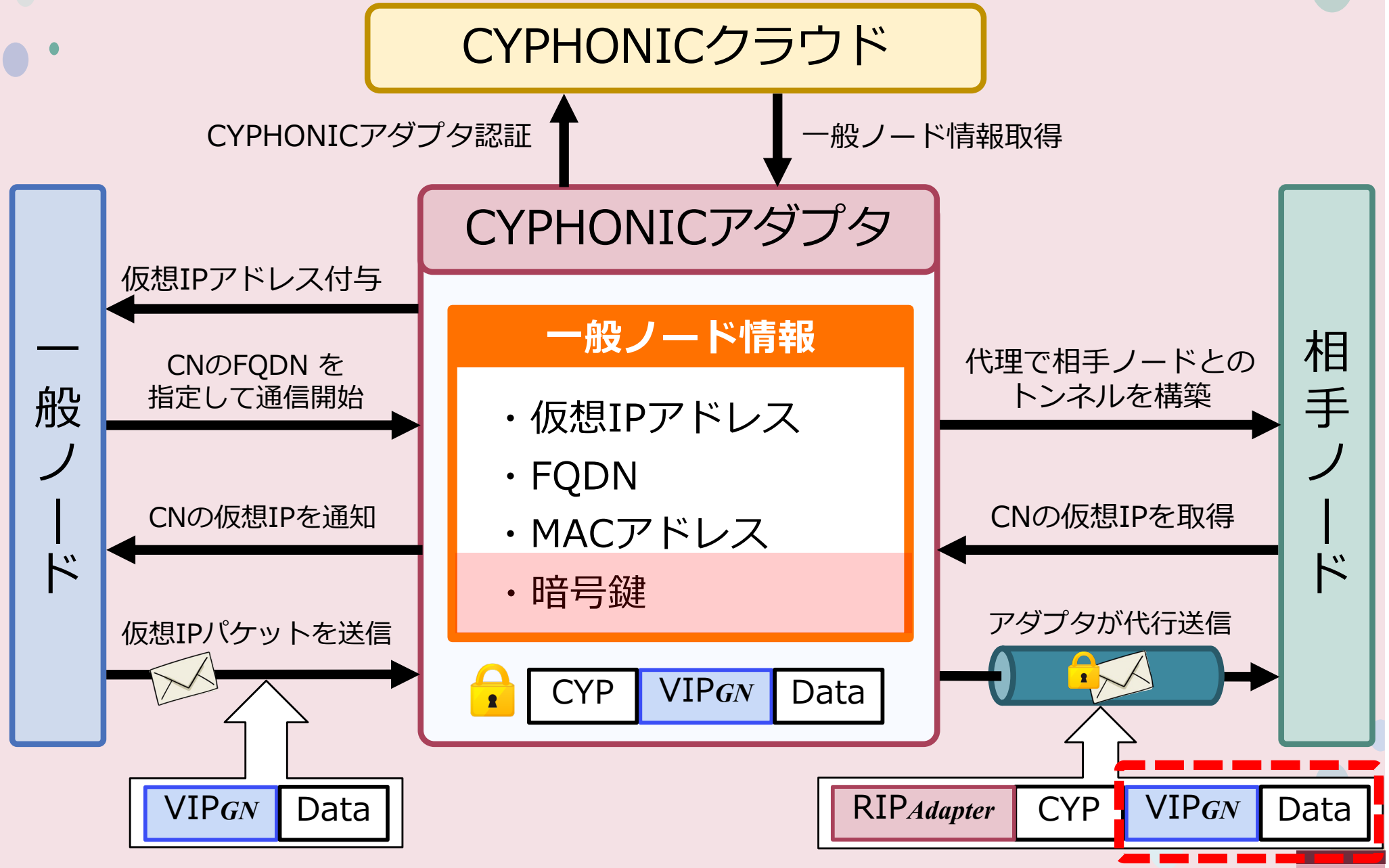
一般ノード情報管理機能
通信に必要な情報を管理
・仮想IPアドレス　・FQDN
・MACアドレス　　・暗号鍵

仮想IPアドレス割り当て機能
DHCPを使用したアドレス割り当て

仮想IPパケット取得機能
一般ノードから仮想IPパケットを取得



処理シーケンス



GN :General Node　CN：Correspondent Node　CYP：CYPHONIC

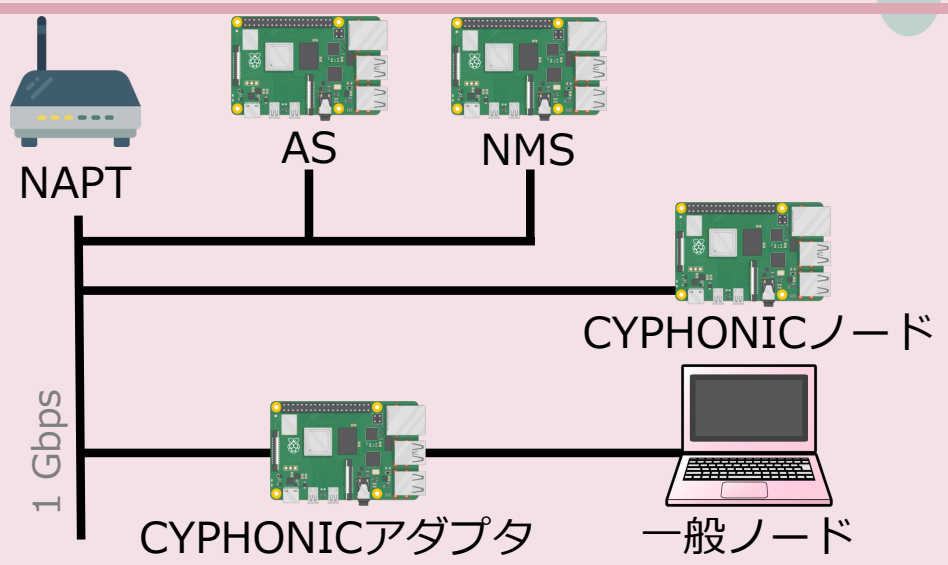
動作検証及び性能評価

動作検証

- 一般ノードに対して
  通信機能を提供可能か確認

性能評価

- 通信遅延時間の測定
  → ping を使用
- 通信スループットの測定
  → iperf を使用



クラウド / アダプタ / ノード	
Machine	Raspberry Pi 4 Model B
OS	Raspbian GNU/Linux 10.0
CPU	Quad Core 1.5GHz Broadcom BCM2711
Memory	4GB RAM

一般ノード	
OS	macOS BigSur Ver 11.5
CPU	Dual Core 2.20GHz Intel(R) Core i7-5650U
Memory	8GB RAM

結果

動作検証

一般ノードは提案するアダプタを用いて
CYPHONIC上で通信可能であることを確認

性能評価

■ 通信遅延

Round-trip time	3.272 ms

大きなオーバーヘッドが
発生しないことを確認

■ 通信性能

一般ノード ⇒ CYPHONICノード	
Throughput	49.8 Mbits/sec
Loss rate	0.22 %

CYPHONICノード ⇒ 一般ノード	
Throughput	49.5 Mbits/sec
Loss rate	0.46 %

50 Mbits/sec 程度の
処理性能を確認

複数人でフルHD通信が
可能な性能を発揮

まとめ

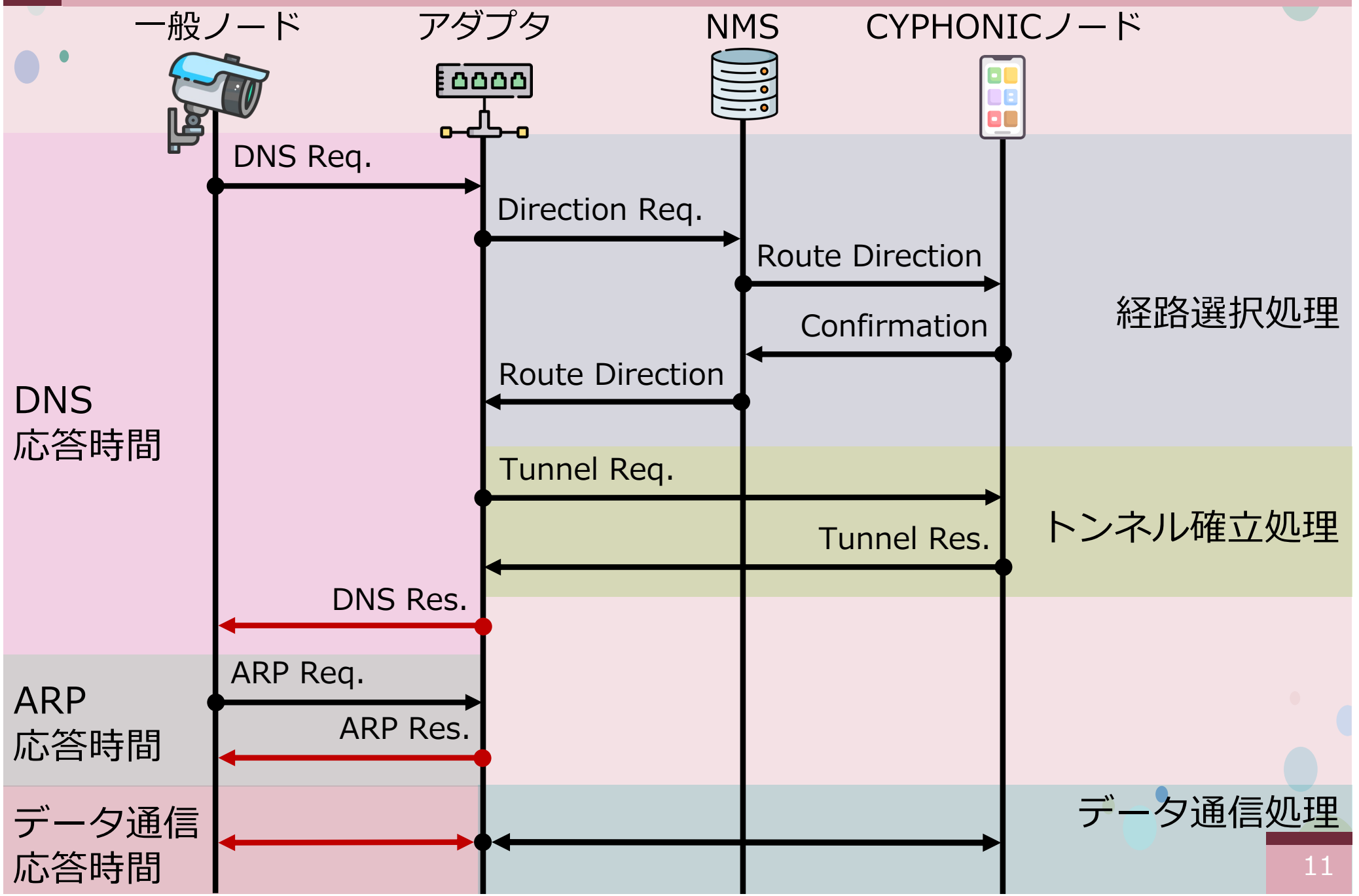
一般ノードをサポートする
CYPHONICアダプタを提案

CYPHONIC Daemonの通信機能を活用し
一般ノードの管理機能を追加実装することで
CYPHONICアダプタを実現

大きなオーバーヘッドを発生させることなく
通信機能の提供が可能であることを確認

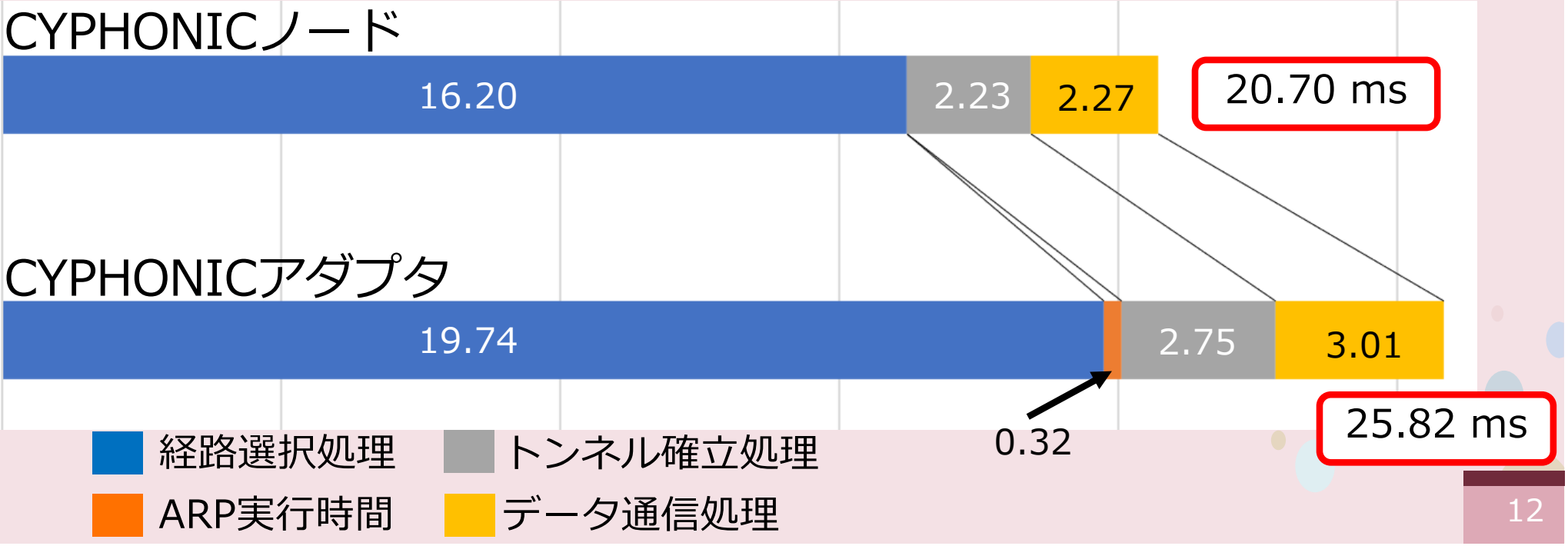
以下、予備スライド

評価対象の通信シグナリング



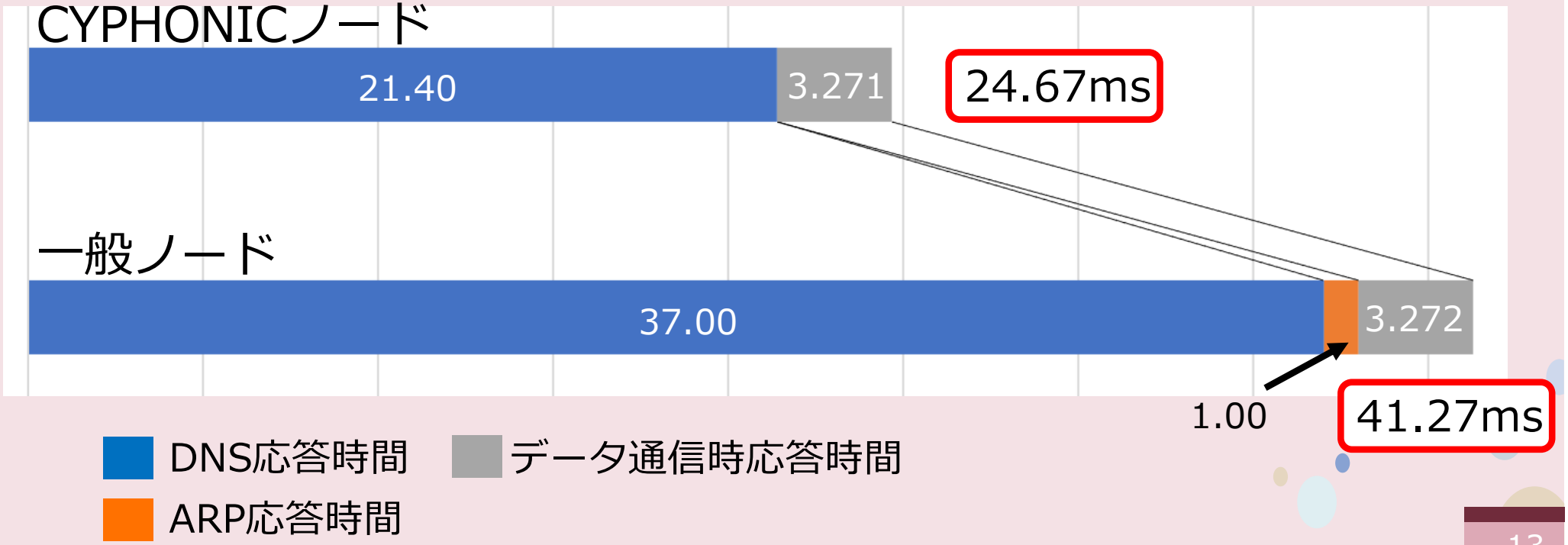
各処理に伴う実行時間の比較

	CYPHONICアダプタ	CYPHONICノード
経路選択処理	19.74 ms	16.20 ms
ARP実行処理	0.32 ms	
トンネル確立処理	2.75 ms	2.23 ms
データ通信処理	3.01 ms	2.27 ms
暗号化処理 (AES-128-CBC)	0.53 ms	0.49 ms
復号処理： (AES-128-CBC)	0.20 ms	0.12 ms



初回通信に伴う遅延時間の比較

	一般ノード	CYPHONICノード
DNS応答時間	37.00 ms	21.40 ms
ARP応答時間	1.00 ms	
データ通信時 応答時間	3.272 ms	3.271 ms



UDPスループット測定値

一般ノード ⇒ CYPHONICノード			
Traffic	Throughput	Jitter	Loss rate
10 Mbps	10.0 Mbits/sec	0.729 ms	0 %
20 Mbps	20.0 Mbits/sec	0.652 ms	0 %
30 Mbps	30.0 Mbits/sec	0.398 ms	0 %
40 Mbps	40.0 Mbits/sec	0.300 ms	0 %
50 Mbps	49.8 Mbits/sec	0.203 ms	0.22 %

CYPHONICノード ⇒ 一般ノード			
Traffic	Throughput	Jitter	Loss rate
10 Mbps	10.0 Mbits/sec	0.787 ms	0 %
20 Mbps	20.0 Mbits/sec	0.680 ms	0 %
30 Mbps	30.0 Mbits/sec	0.395 ms	0 %
40 Mbps	39.8 Mbits/sec	0.326 ms	0.28 %
50 Mbps	49.5 Mbits/sec	0.266 ms	0.46 %

UDPスループット測定値

CYPHONICノード ⇒ CYPHONICノード			
Traffic	Throughput	Jitter	Loss rate
10 Mbps	10.0 Mbits/sec	0.529 ms	0 %
20 Mbps	20.0 Mbits/sec	0.664 ms	0 %
30 Mbps	30.0 Mbits/sec	0.556 ms	0 %
40 Mbps	40.0 Mbits/sec	0.297 ms	0 %
50 Mbps	50.0 Mbits/sec	0.275 ms	0 %

TCPスループットにおける課題

CYPHONICノード間の通信

CYPHONICノード ⇔ CYPHONICノード	
Transfer	563 Mbytes
Throughput	78.7 Mbits/sec

既存のCYPHONICノードは
78 Mbits/sec 程度を処理可能

CYPHONICアダプタを介した通信

CYPHONICノード ⇒ 一般ノード	
Transfer	437 Mbytes
Throughput	74.2 Mbits/sec

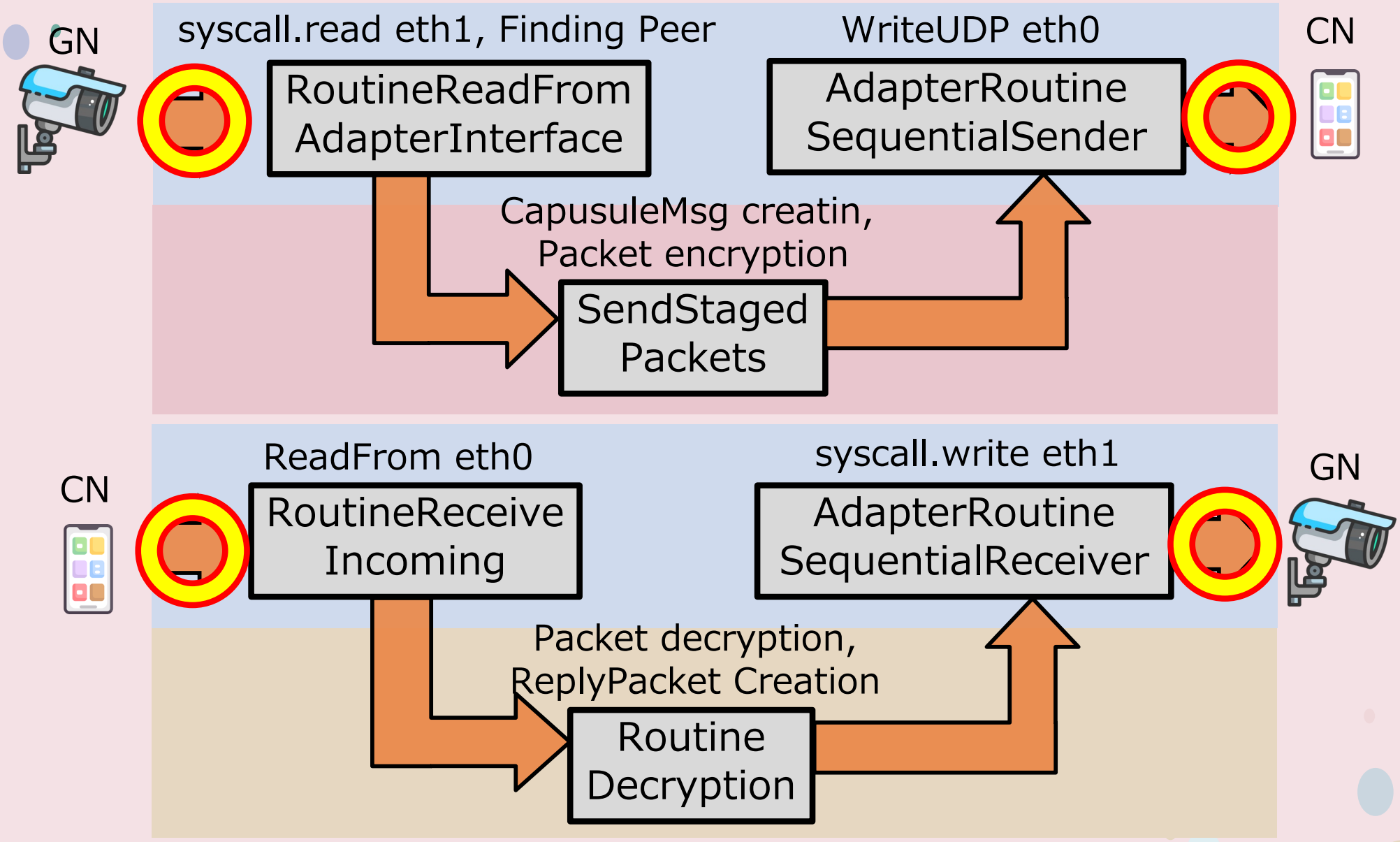
既存のCYPHONICノードと
同程度のトラフィックを処理可能

一般ノード ⇒ CYPHONICノード	
Transfer	6.01 Mbytes
Throughput	1.68 Mbits/sec

TCPスループットが極端に
低下することを確認

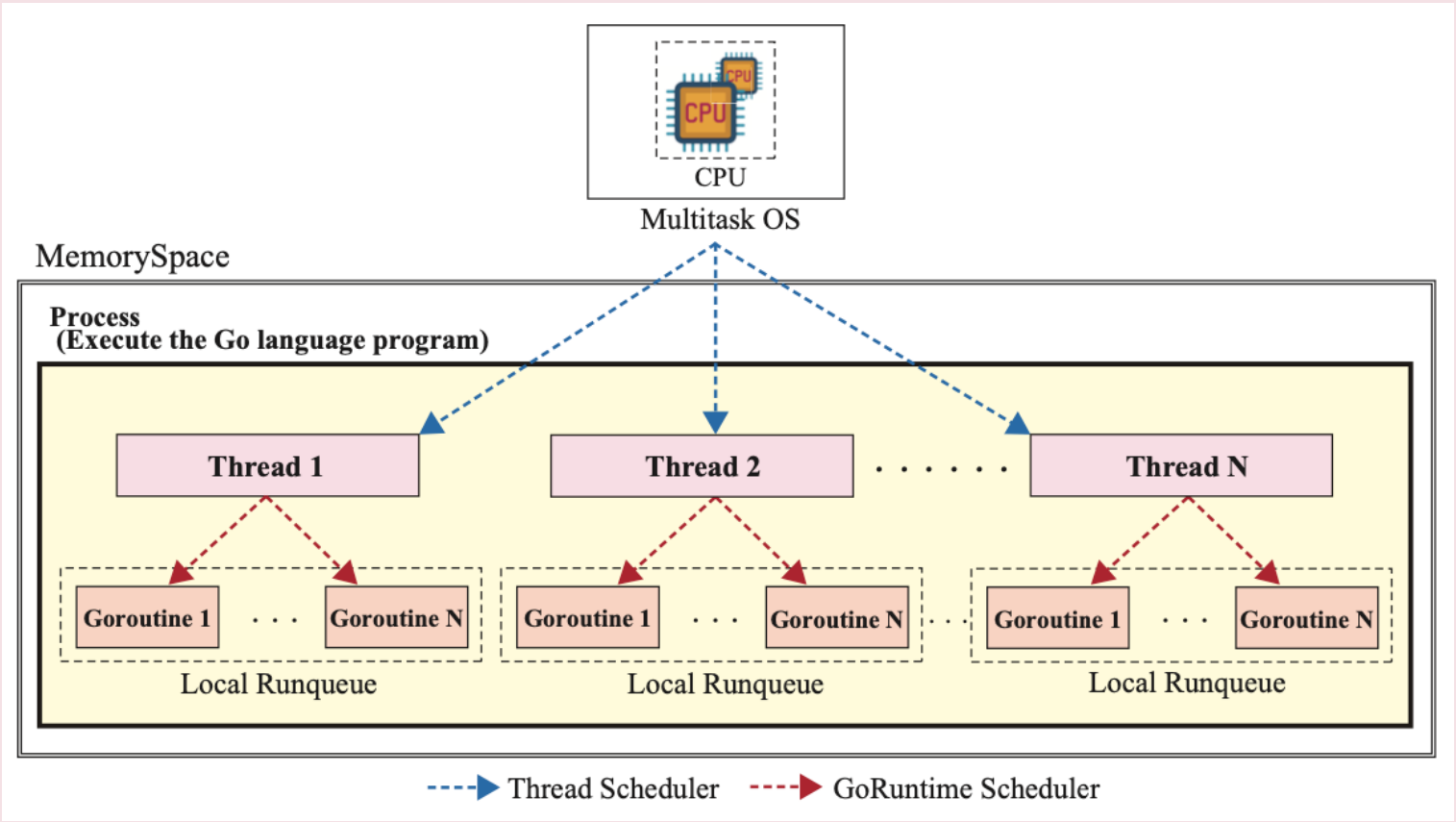
パケットの受信から処理までを単一スレッドで実行
（なお, 暗号化処理および復号処理はマルチスレッド化）

データ通信処理における関数呼び出し



暗号化・復号処理以外は単一スレッドで実行

Goroutine の処理モデル



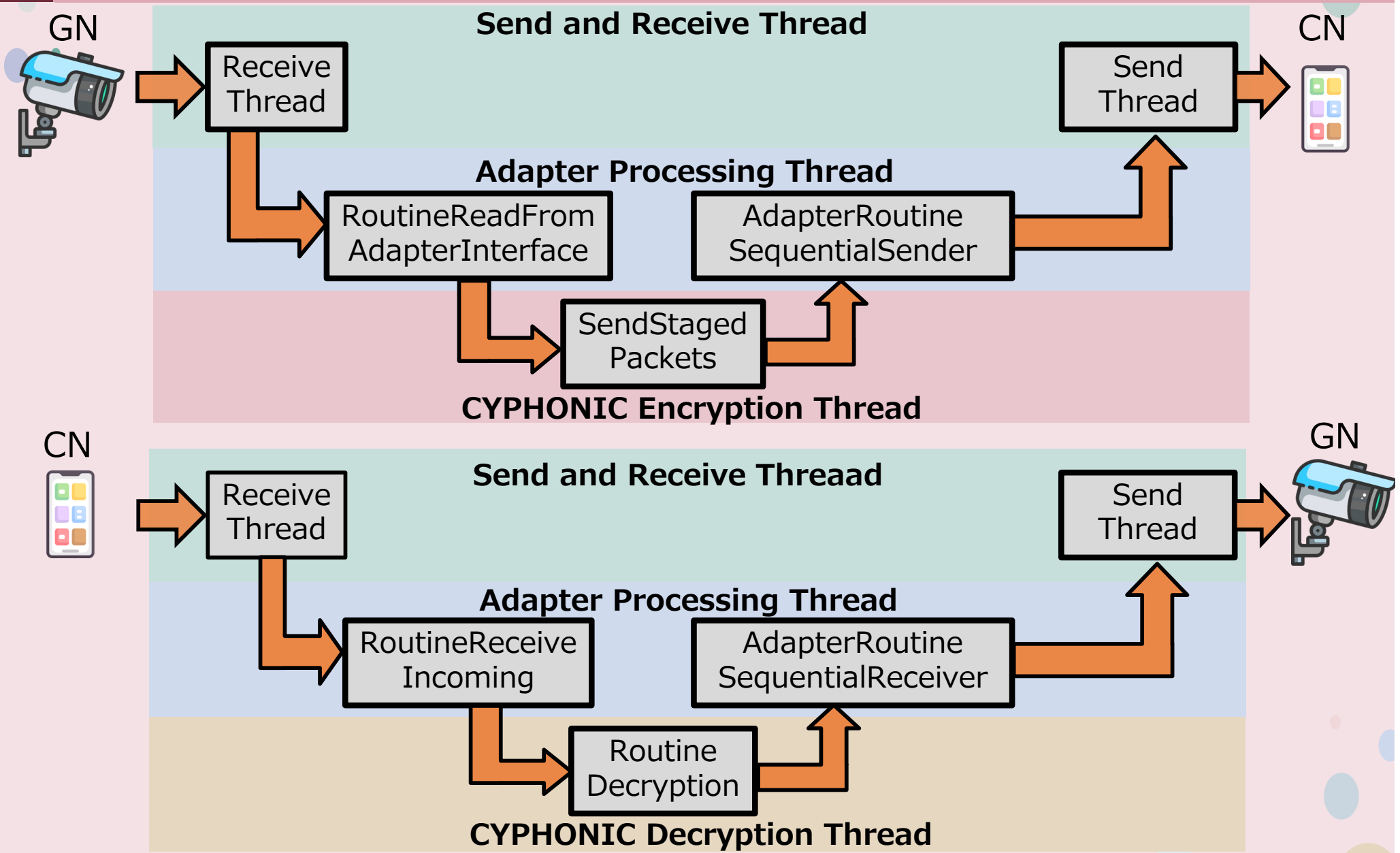
Hyper-threading Kernel（Threads）

- *M* 個 の物理コアに対して同時に *N* 個 の処理が可能な *M:N* スケジューラ

GoRuntime（Goroutines）

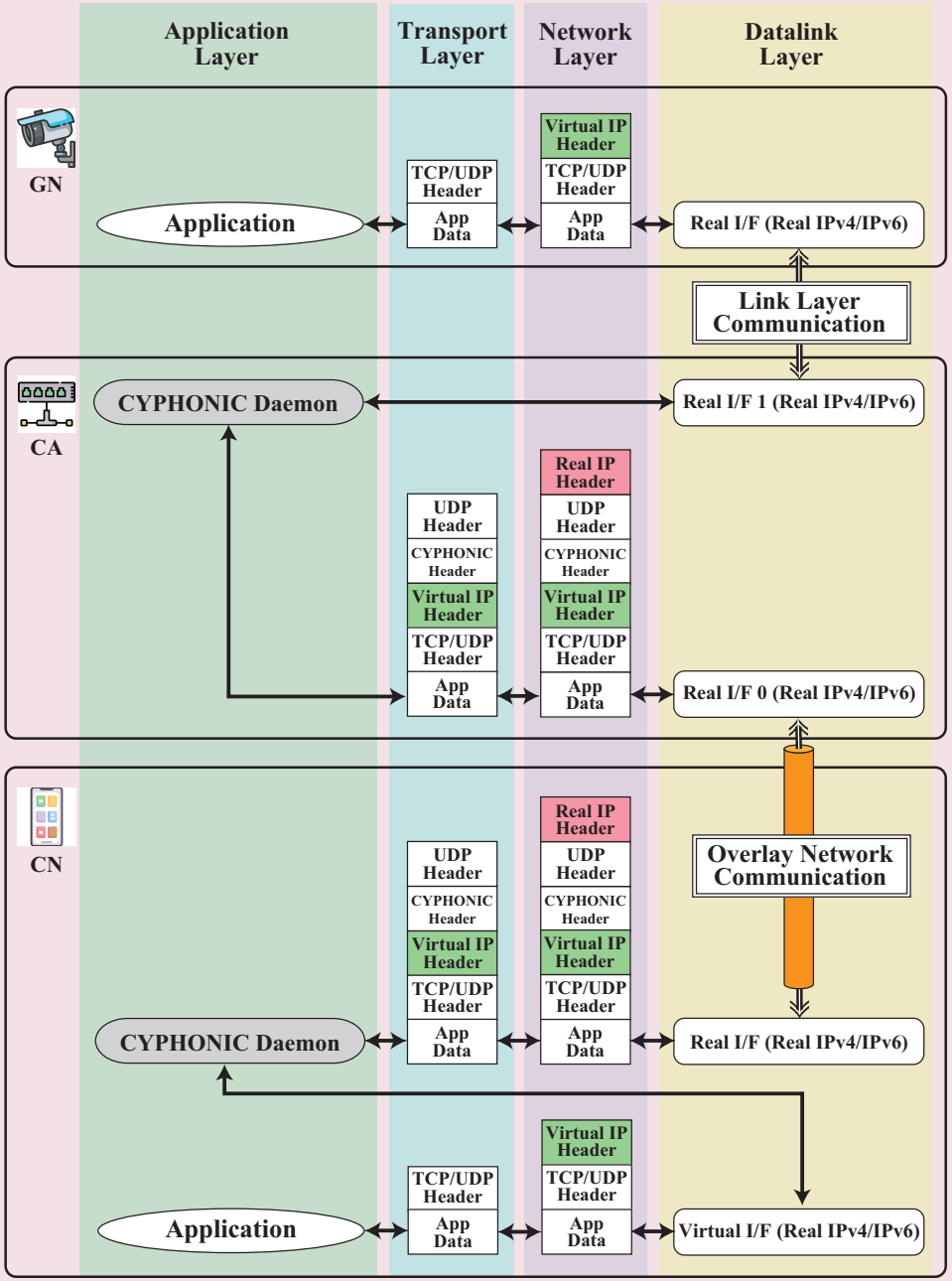
- *M* 個 の論理コアに対して同時に *N* 個 の処理が可能な *M:N* スケジューラ

スレッド分離による改善の検討



専用のスレッドを用いて受信キューに格納

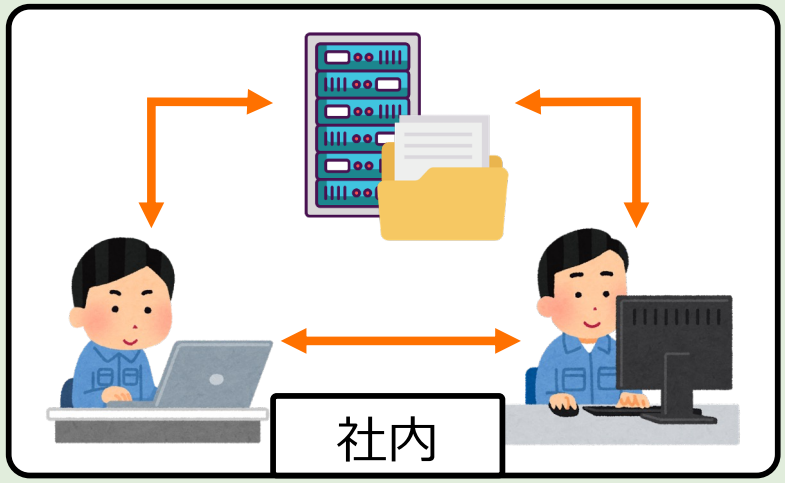
一般ノードのパケットフロー



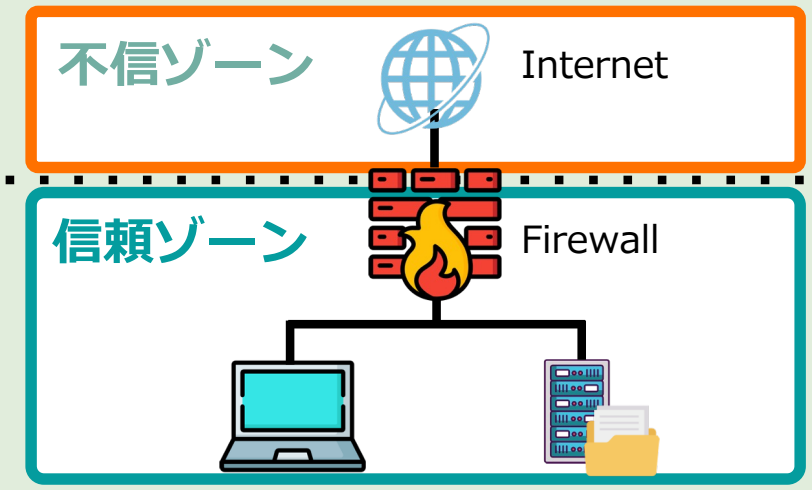
GN: General Node CA: CYPHONIC Adapter CN: Correspondent Node

セキュリティモデルの変化

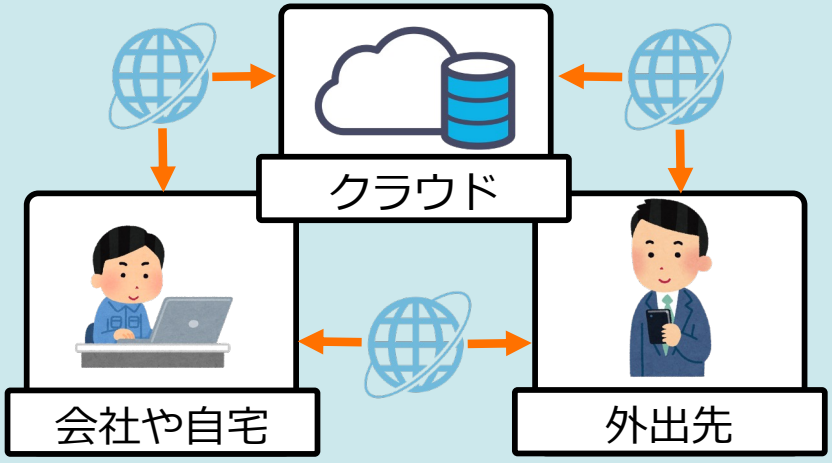
従来の利用形態



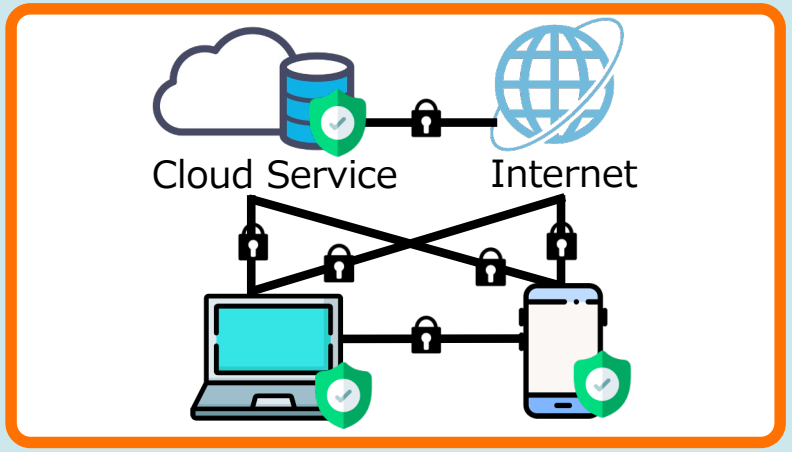
境界型モデル



今後の利用形態

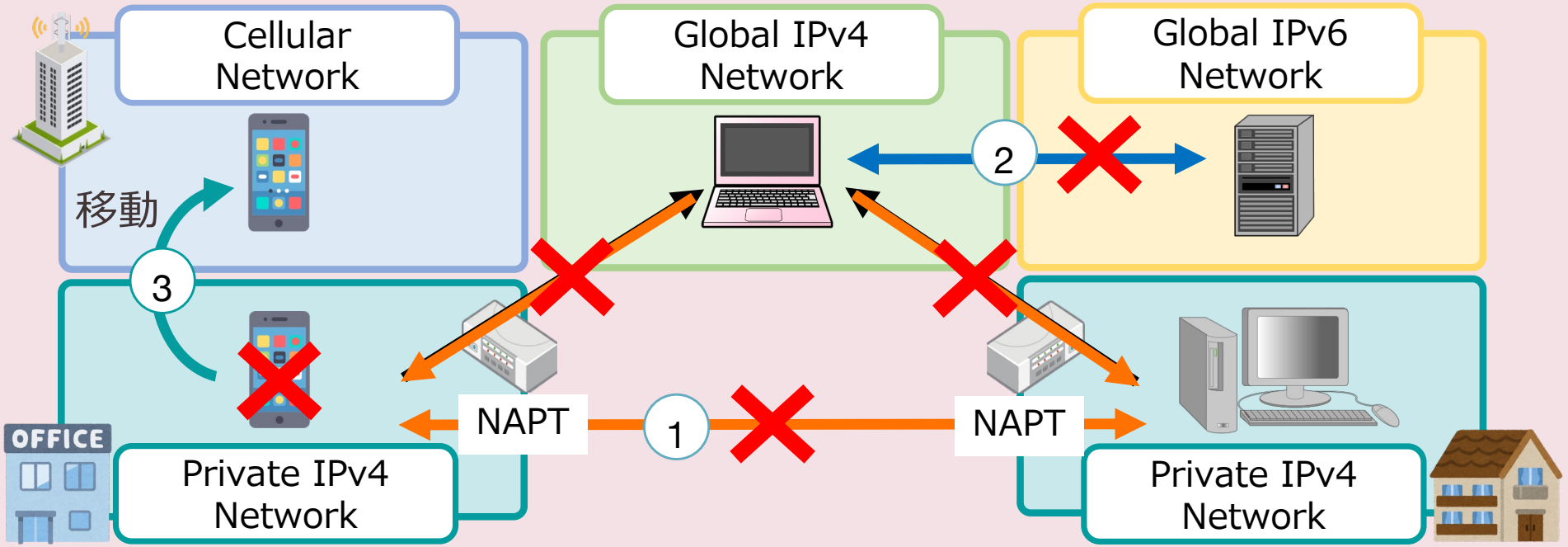


ゼロトラストモデル



インターネット利用形態の多様化に伴い
セキュリティモデルも変化

エンド間通信に伴う課題



IPv4アドレス枯渇対策のためNAPTとIPv6を導入

課題１：NAPTによる通信の遮断

課題２：IPv4とIPv6の非互換性

IPは端末の移動について考慮されていない

課題３：ネットワーク移動による通信切断

エンド間での直接通信を実現する技術が必要

既存技術と課題

	通信接続性	移動透過性
	NAPTやIPバージョンの差異依らず通信接続可能	ネットワーク移動時も通信継続可能
Hole Punching / STUN	●	X
ICE	●	X
Mobile IP	X	●
DSMIPv6	X	●

- 既存技術にはそれぞれ課題が存在
- 概念実証の評価やセキュア通信に関する検討が不十分

端末間でのセキュアなエンド間通信を実現するために
通信接続性と移動透過性を確保する技術が必要

CYPHONIC

CYber PHysical Overlay Network over Internet Communication

セキュアなエンド間接続を実現する
オーバーレイネットワークプロトコル

■ 端末間でのセキュアな通信を実現

・サービス利用端末の認証と送受信データの暗号化
・端末間でのエンドツーエンド通信を提供

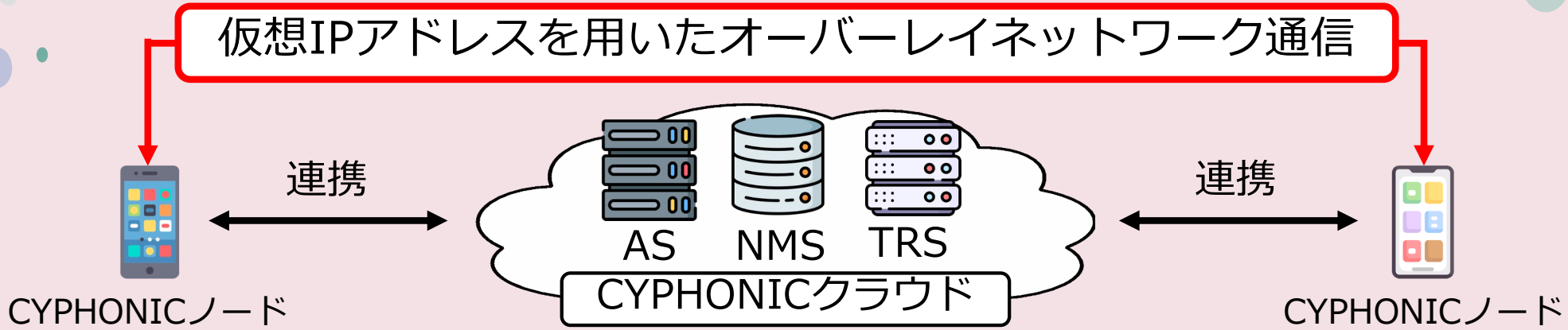
■ 通信接続性を実現

・NAPTの配下に存在する端末への通信を提供
・IPバージョンの互換性を提供

■ 移動透過性を実現

・端末の移動時も継続した通信を提供
・仮想IPアドレスによる通信で実ネットワークの影響を隠蔽

CYPHONICの構成要素



CYPHONICノード

・CYPHONICを用いた通信を行う端末
・クラウドサービスと連携することで相手端末と直接通信

Authentication Service (AS)

・CYPHONICノ ードを認証
・CYPHONICノードの識別子としてFQDNを付与

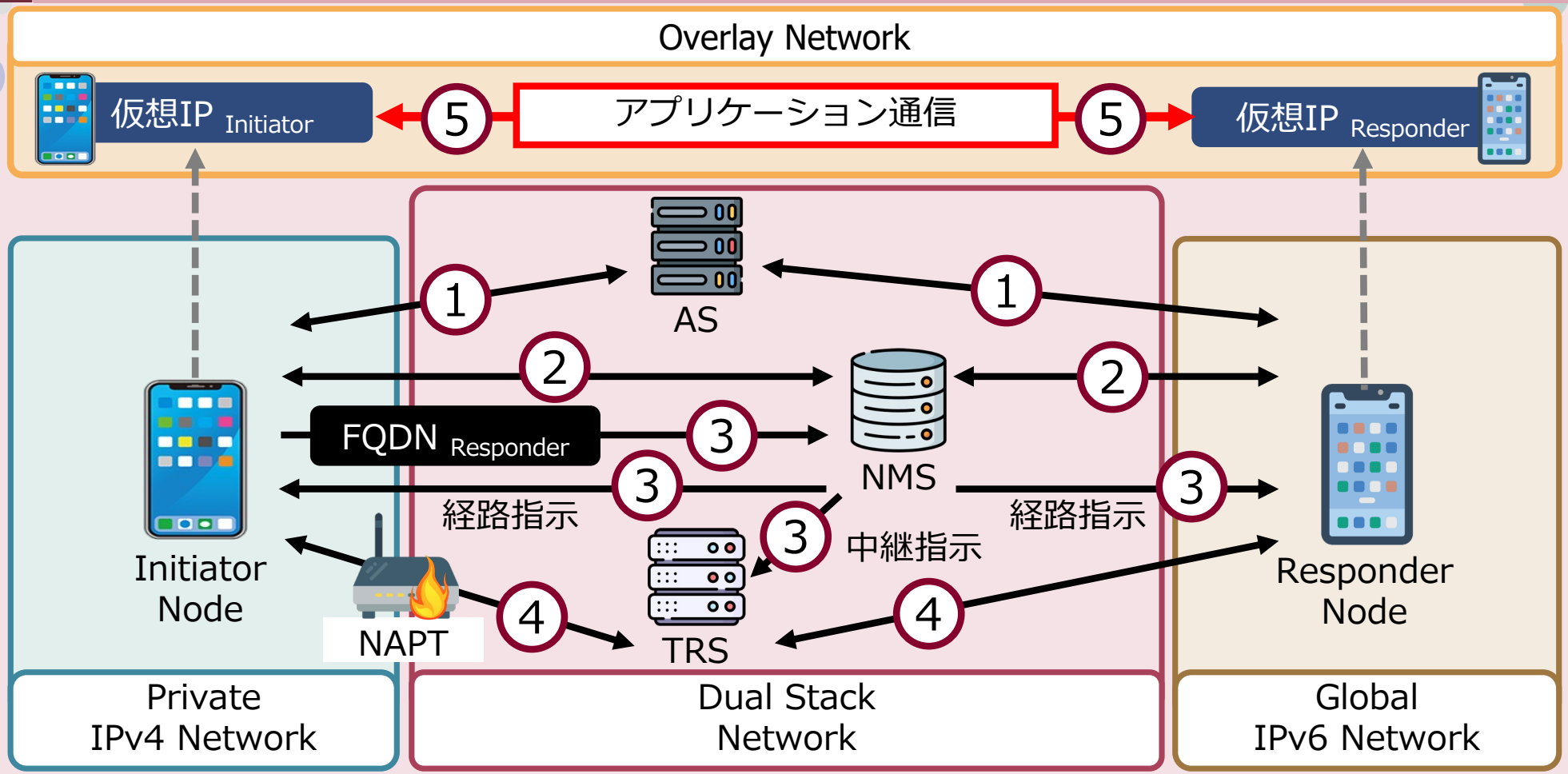
Node Management Service (NMS)

・CYPHONICノードのネットワーク情報管理と通信経路の指示
・CYPHONICノードが通信に用いる仮想IPアドレスを付与

Tunnel Relay Service (TRS)

・NAPTを跨いだ通信とIPv4/IPv6間の通信を中継

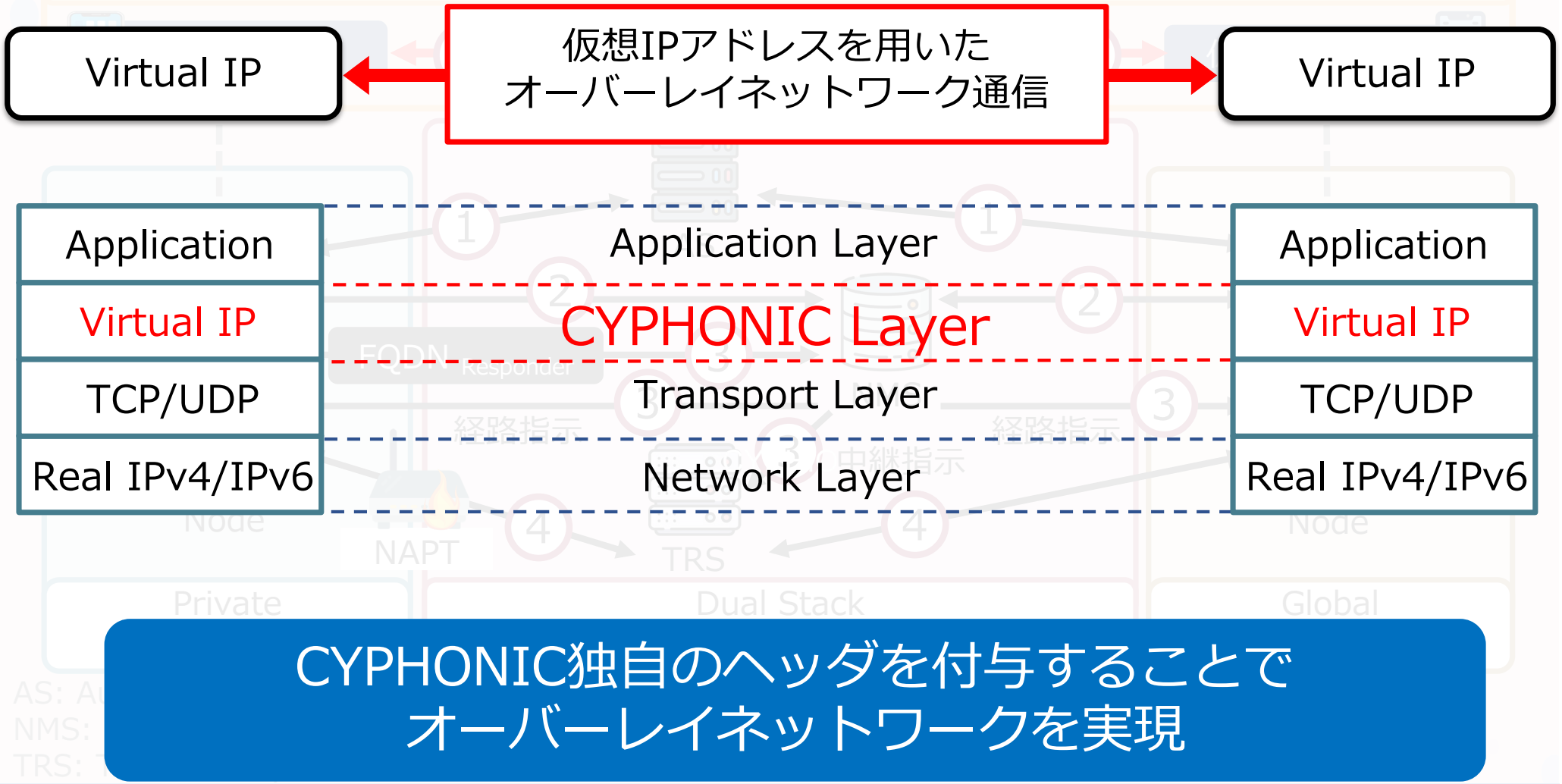
CYPHONIC 全体概要



AS: Authentication Service
NMS: Node Management Service
TRS: Tunnel Relay Service
NAPT: Network Address Port Translation
FQDN: Fully Qualified Domain Name

1. 認証処理：端末の認証
2. 位置情報登録処理：ネットワーク情報登録
3. 経路選択処理：通信経路決定
4. トンネル確立処理：エンド間トンネル構築
5. データ通信処理：オーバーレイネットワーク上の通信

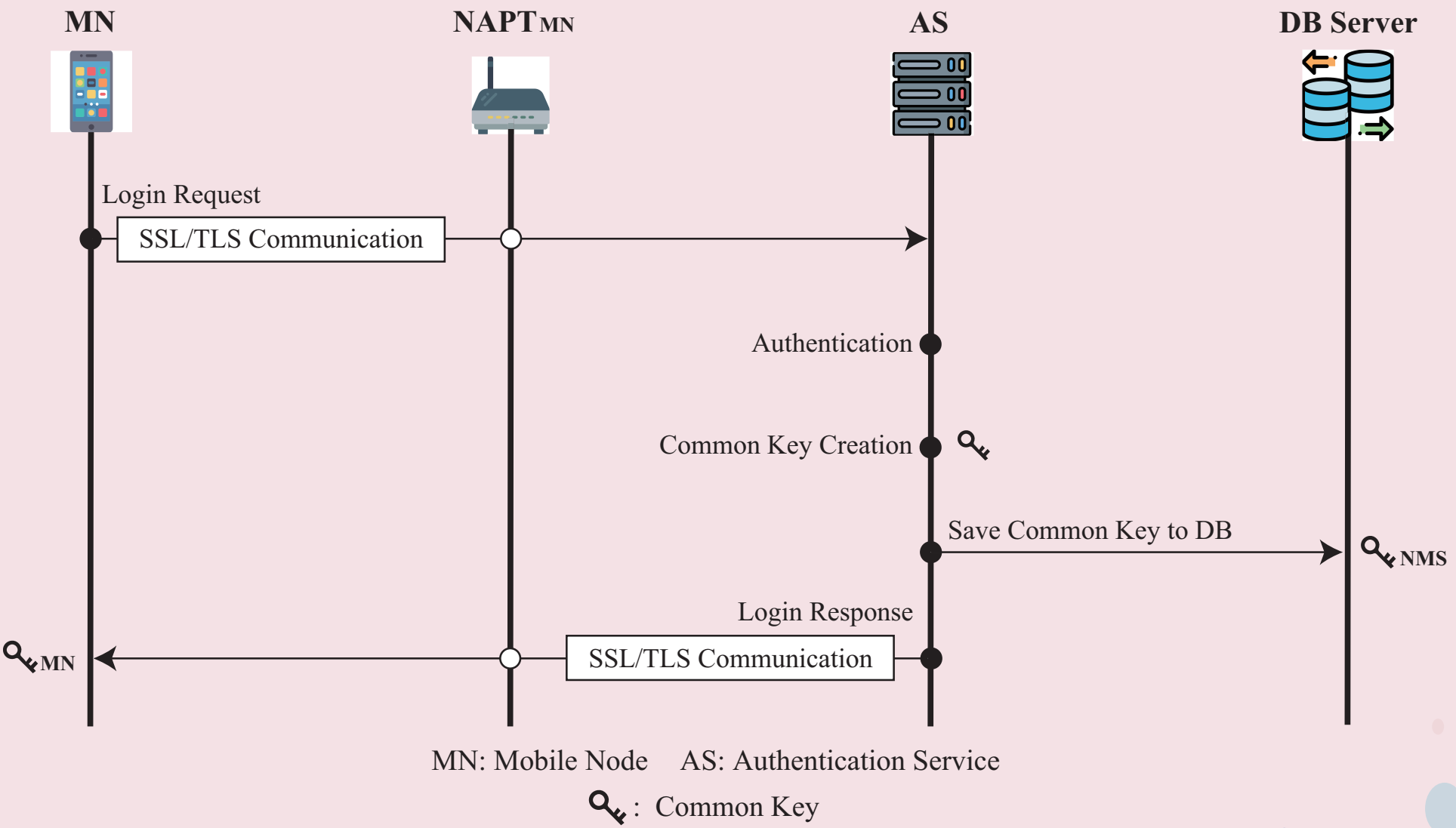
CYPHONIC 全体概要



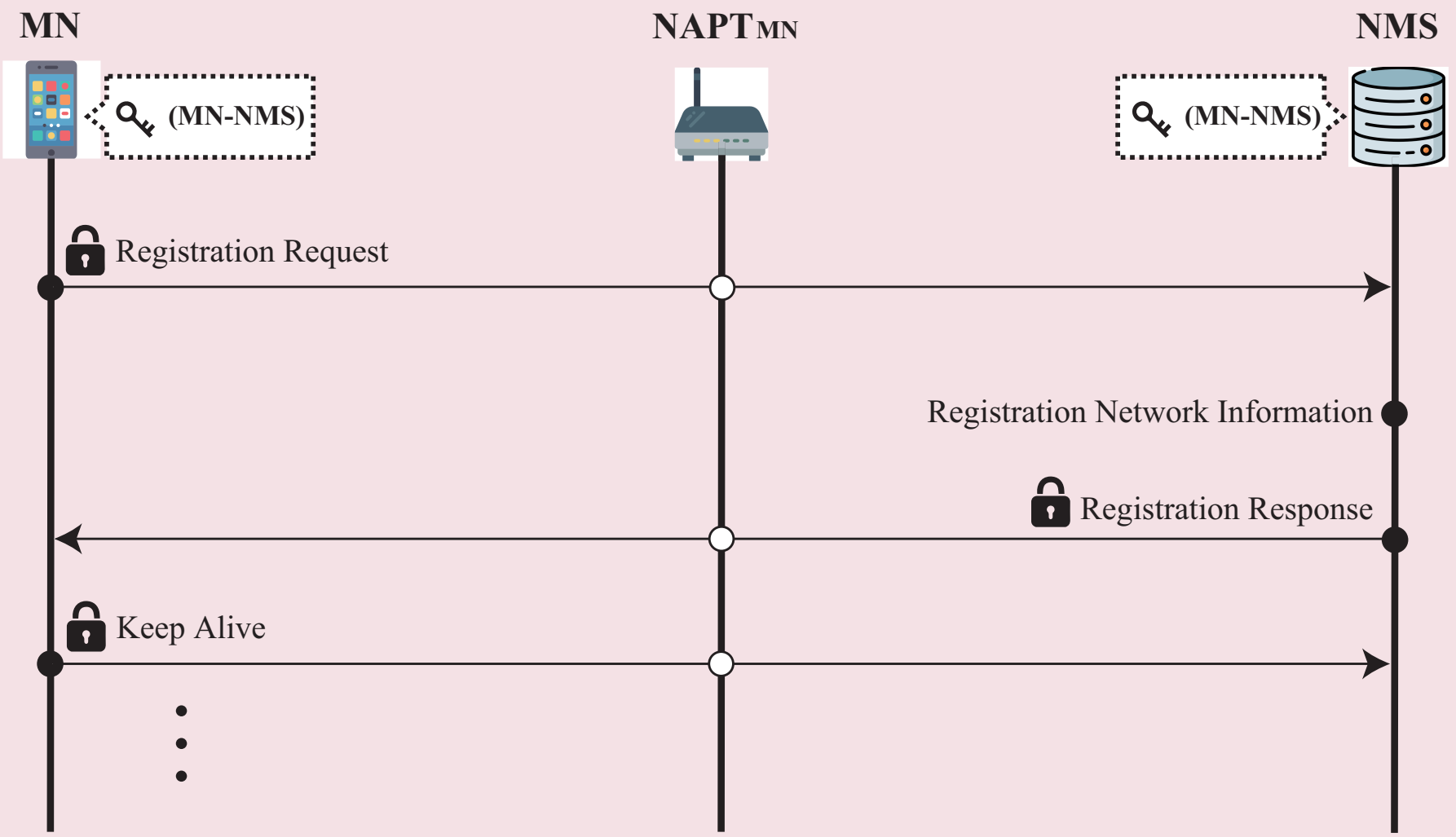
CYPHONIC独自のヘッダを付与することで
オーバーレイネットワークを実現

1. 認証処理：端末の認証　2. 位置情報登録処理：ネットワーク情報登録
3. 経路選択処理：通信経路決定　4. トンネル確立処理：エンド間トンネル構築
5. データ通信処理：オーバーレイネットワーク上の通信

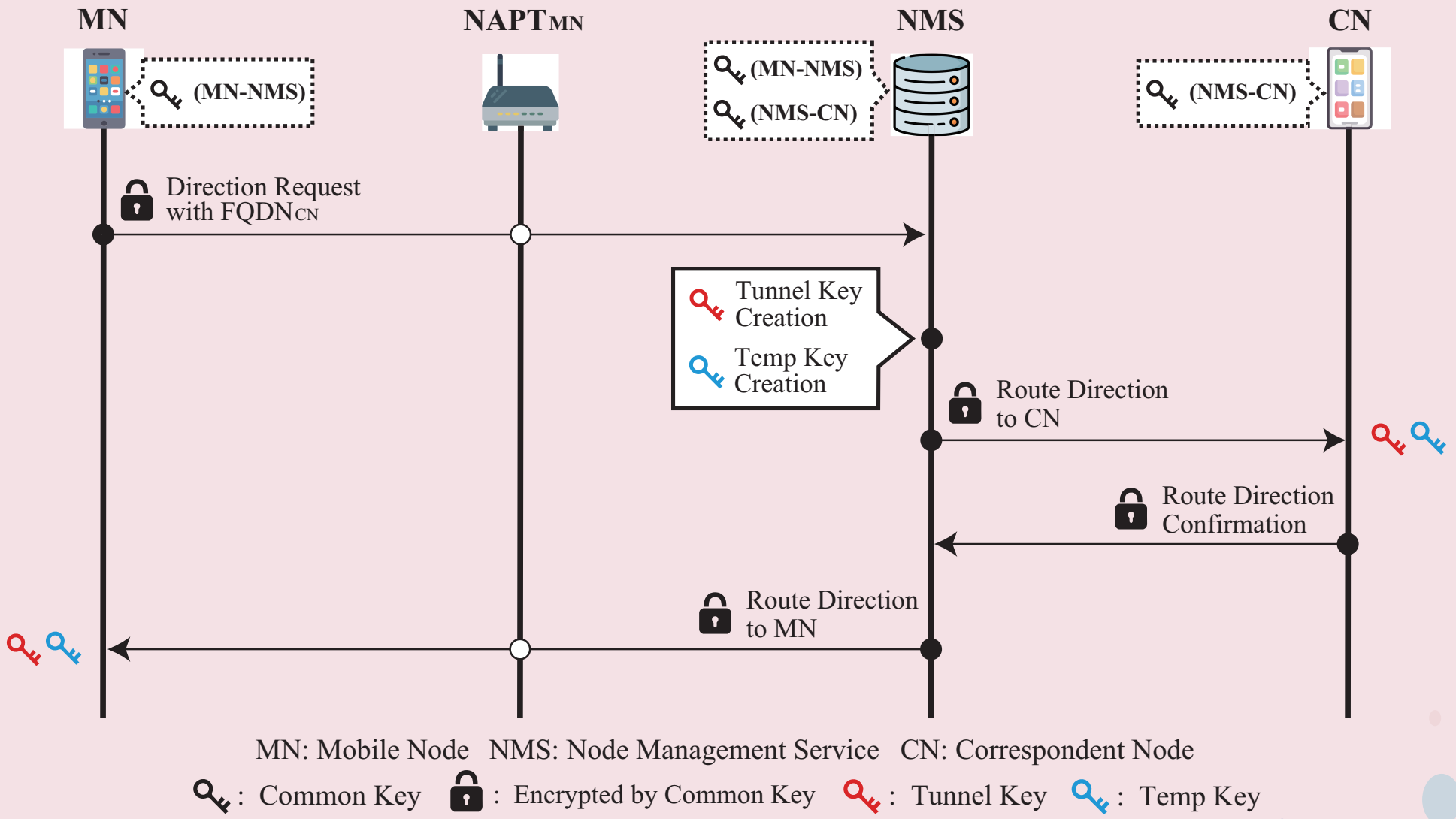
認証処理


MN
NAPT MN
AS
DB Server
Login Request
SSL/TLS Communication
Authentication
Common Key Creation
Save Common Key to DB
NMS
Login Response
SSL/TLS Communication
MN
MN: Mobile Node AS: Authentication Service
: Common Key

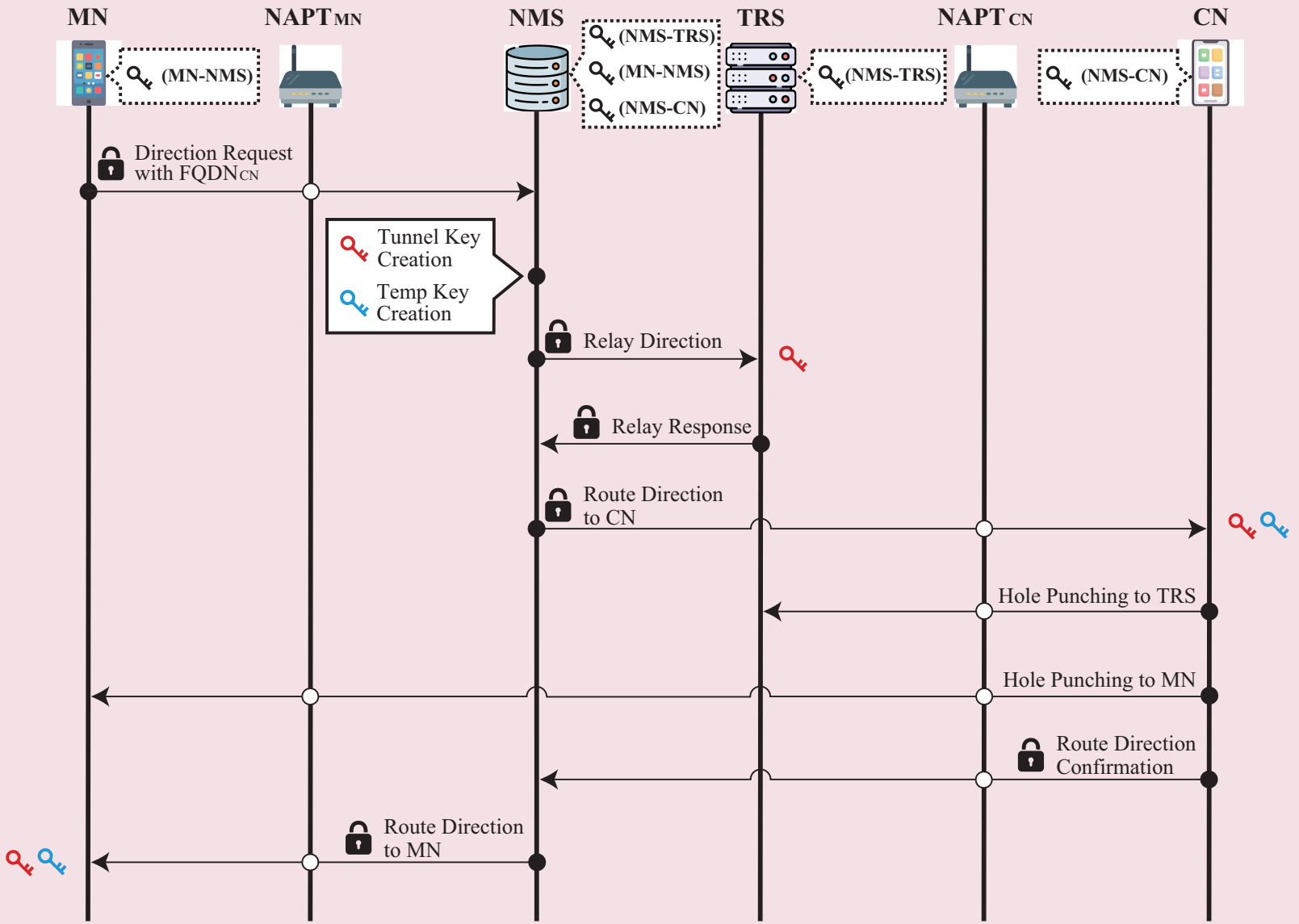
位置情報登録処理


MN
NAPT MN
NMS
(MN-NMS)
(MN-NMS)
Registration Request
Registration Network Information
Registration Response
Keep Alive
MN: Mobile Node NMS: Node Management Service
: Common Key : Encrypted by Common Key

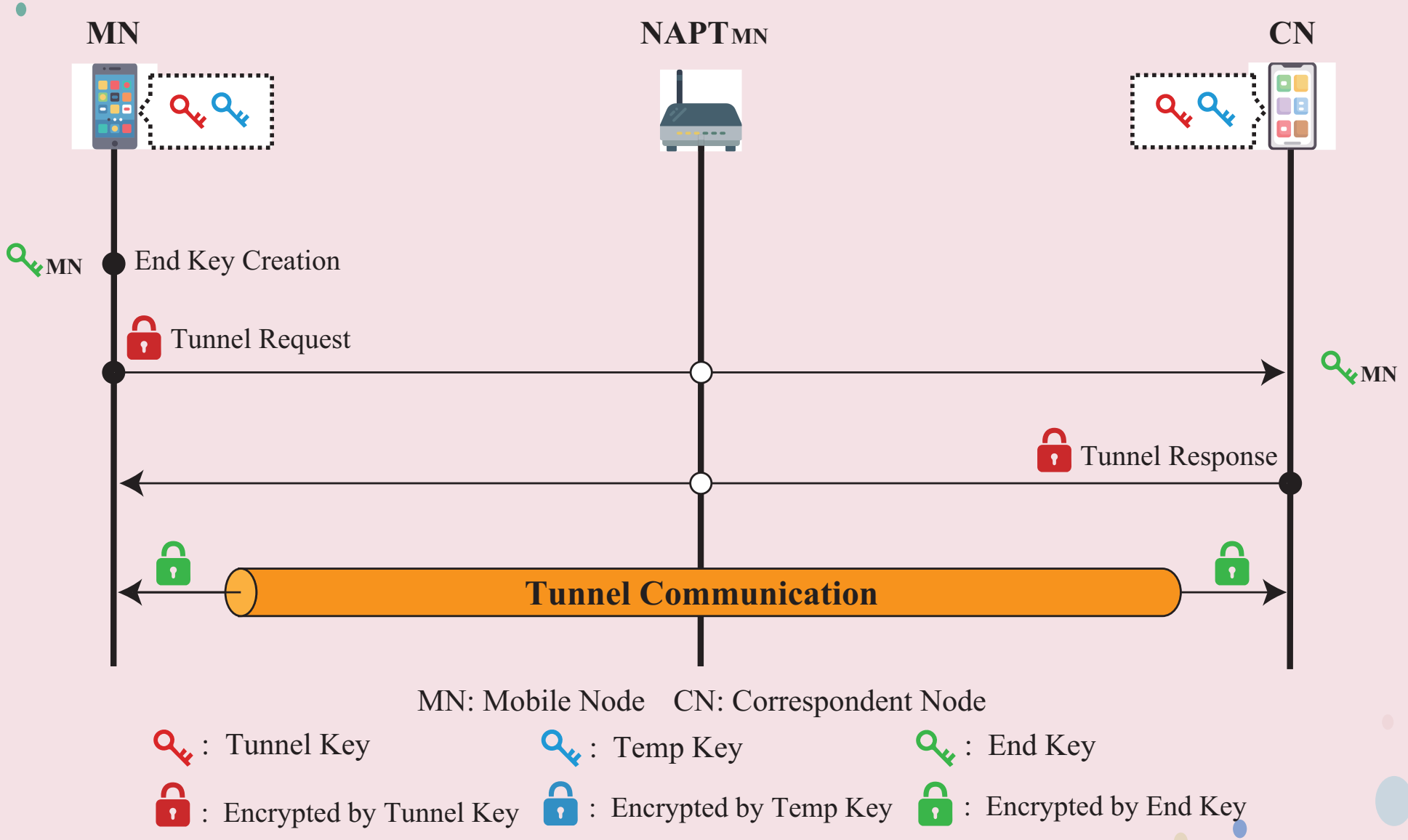
経路選択処理


MN
NAPT MN
NMS
CN
(MN-NMS)
(MN-NMS)
(NMS-CN)
(NMS-CN)
Direction Request with FQDN CN
Tunnel Key Creation
Temp Key Creation
Route Direction to CN
Route Direction Confirmation
Route Direction to MN
MN: Mobile Node NMS: Node Management Service CN: Correspondent Node
: Common Key : Encrypted by Common Key : Tunnel Key : Temp Key

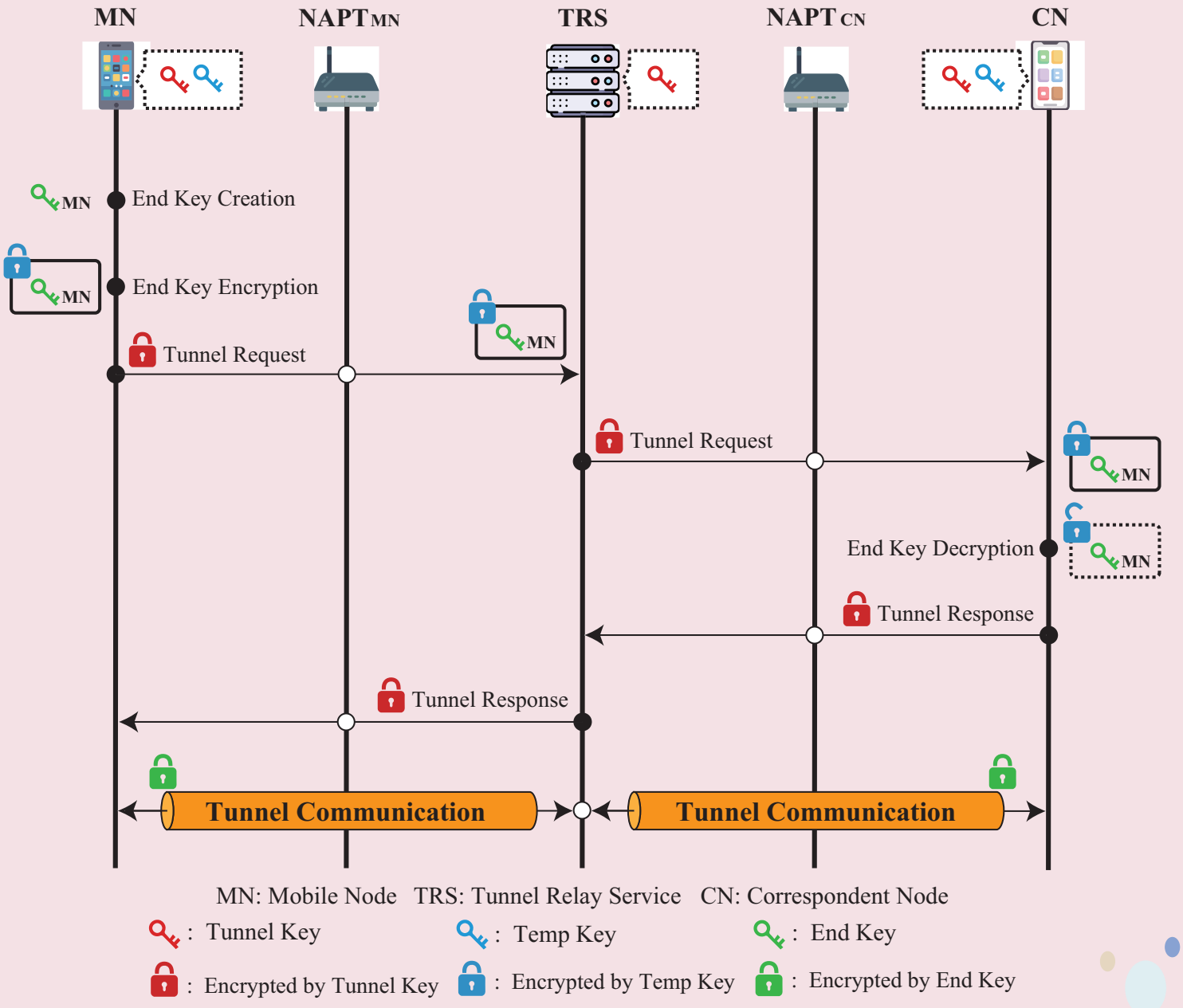
経路選択処理（TRS経由）



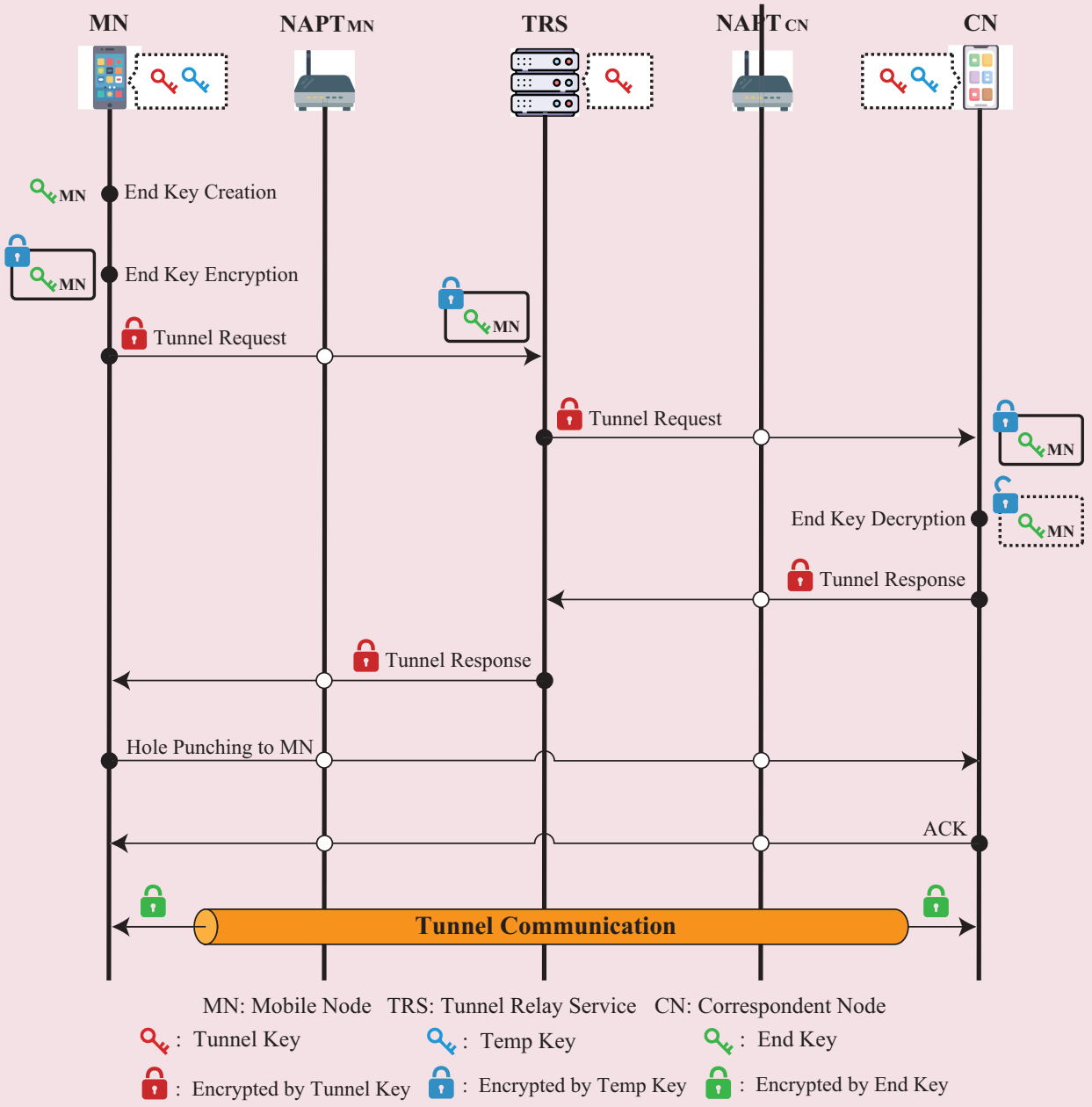
トンネル確立処理


MN
NAPT MN
CN
MN
End Key Creation
Tunnel Request
MN
Tunnel Response
Tunnel Communication
MN: Mobile Node CN: Correspondent Node
: Tunnel Key
: Temp Key
: End Key
: Encrypted by Tunnel Key
: Encrypted by Temp Key
: Encrypted by End Key

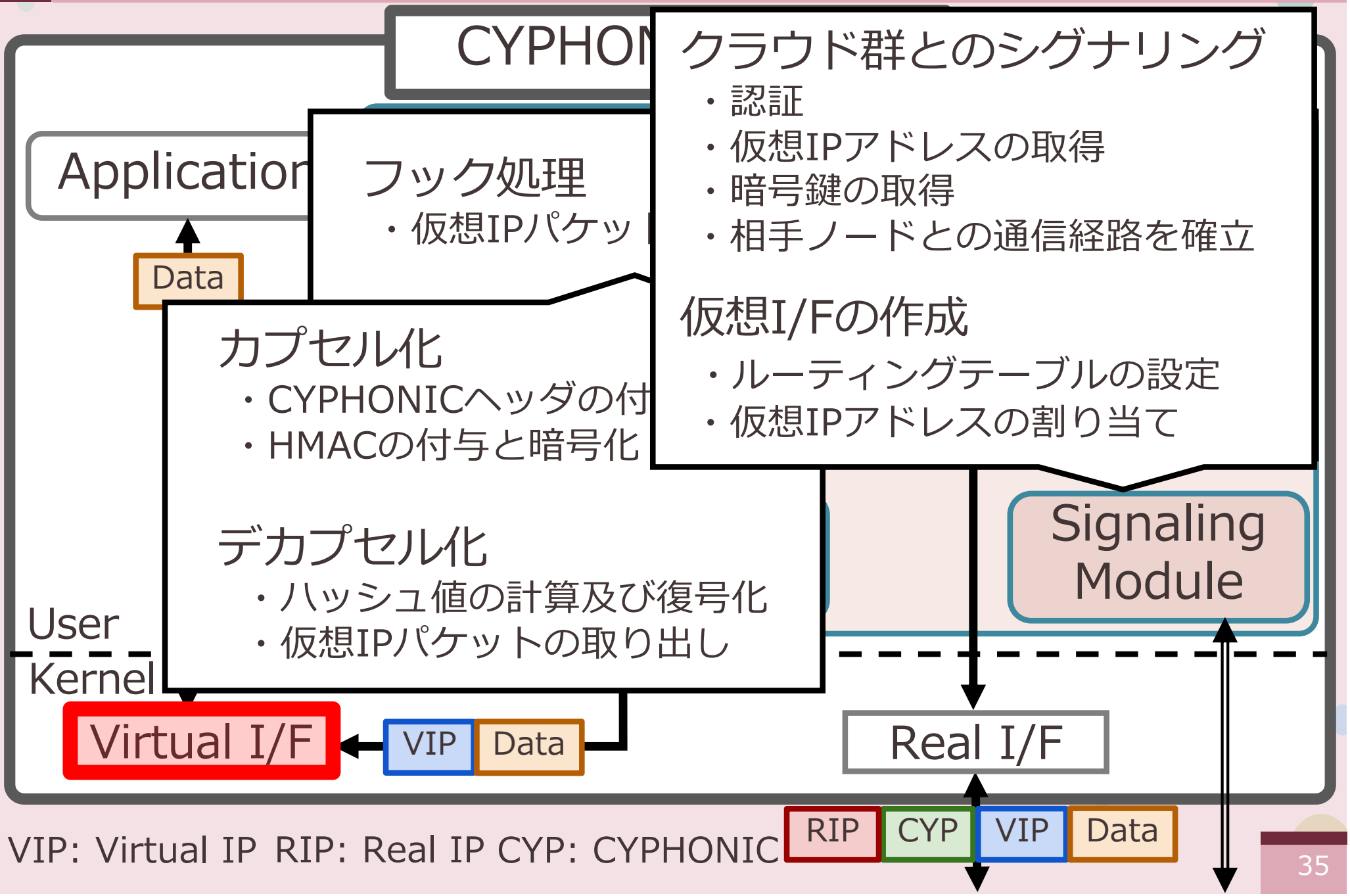
トンネル確立処理（TRS経由）



経路最適化処理

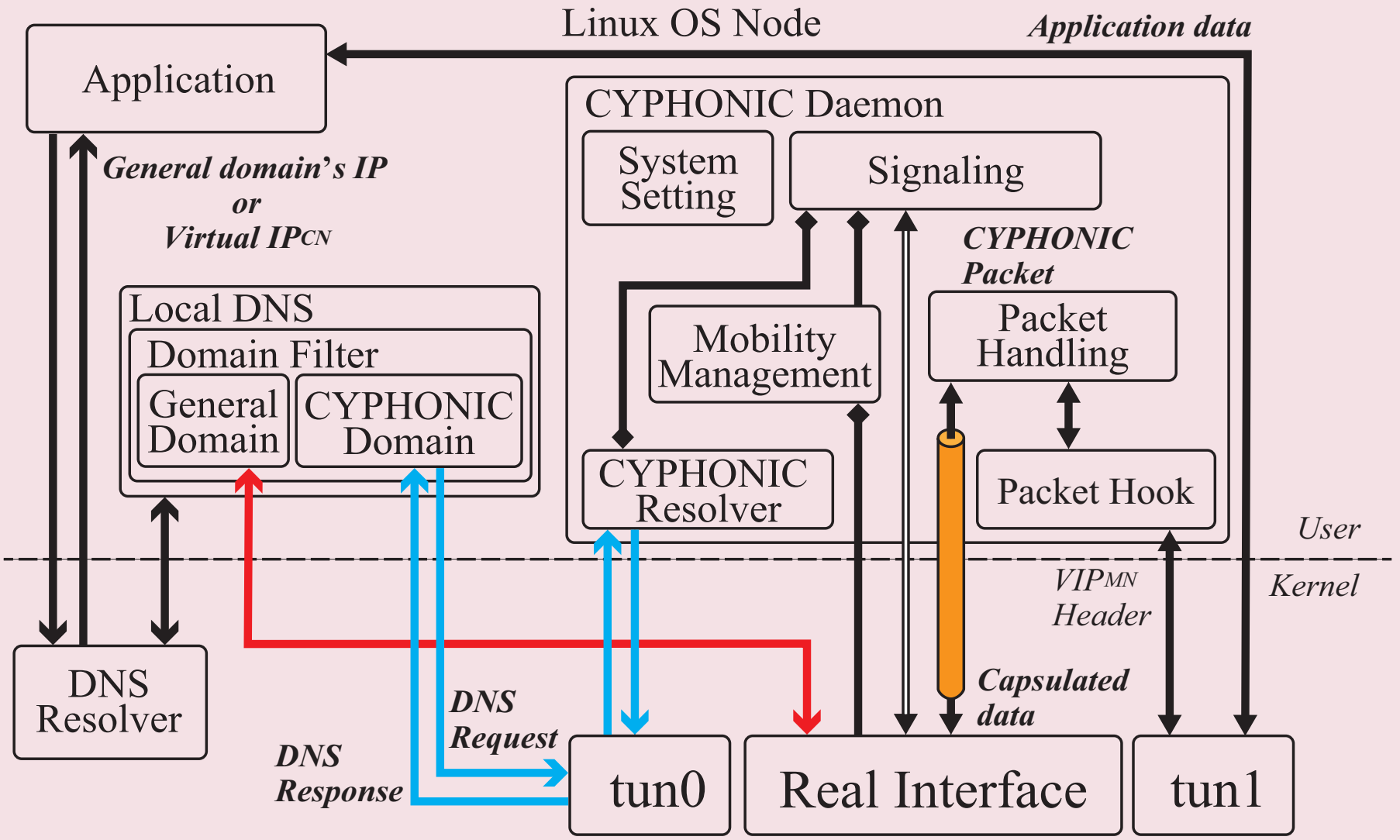

MN
NAPT MN
TRS
NAPT CN
CN
MN
End Key Creation
MN
End Key Encryption
MN
Tunnel Request
MN
Tunnel Request
MN
MN
End Key Decryption
Tunnel Response
Tunnel Response
Hole Punching to MN
ACK
Tunnel Communication
MN: Mobile Node TRS: Tunnel Relay Service CN: Correspondent Node
: Tunnel Key
: Temp Key
: End Key
: Encrypted by Tunnel Key
: Encrypted by Temp Key
: Encrypted by End Key

CYPHONICノード システムモデル



VIP: Virtual IP RIP: Real IP CYP: CYPHONIC

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

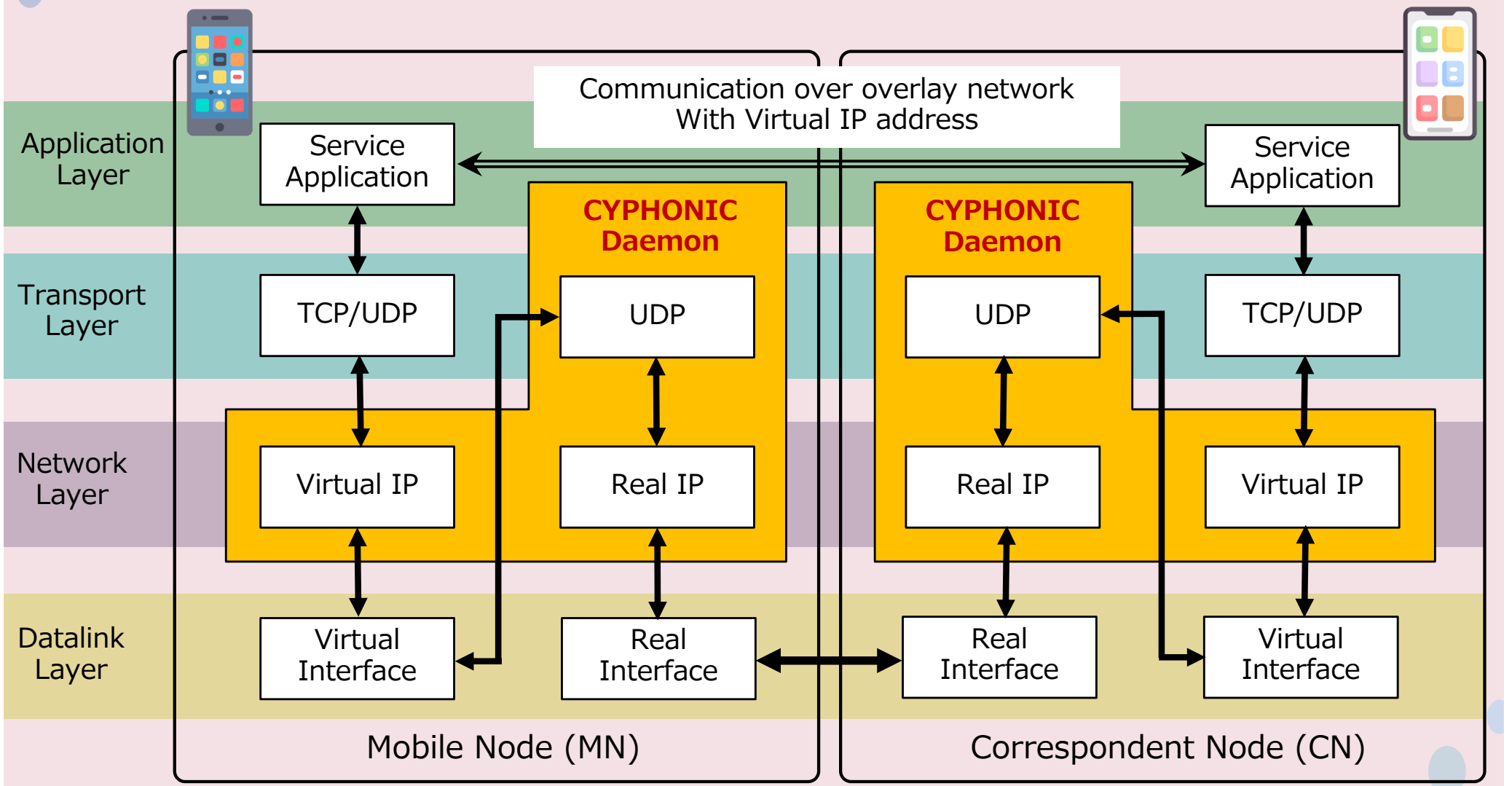
Signaling Message

DNS Packets

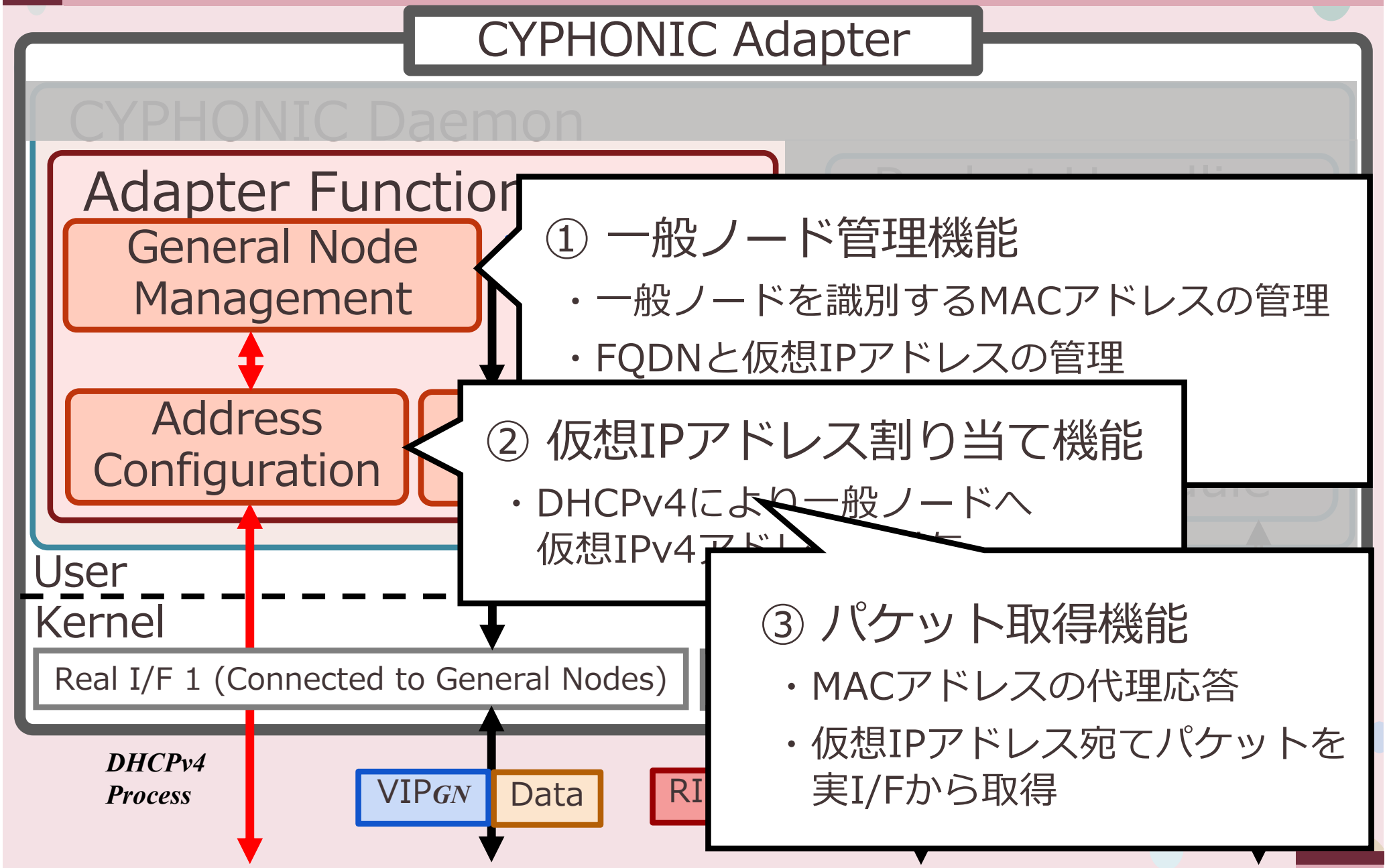
Data Sequence

Informations

CYPHONICにおけるカプセル化フロー

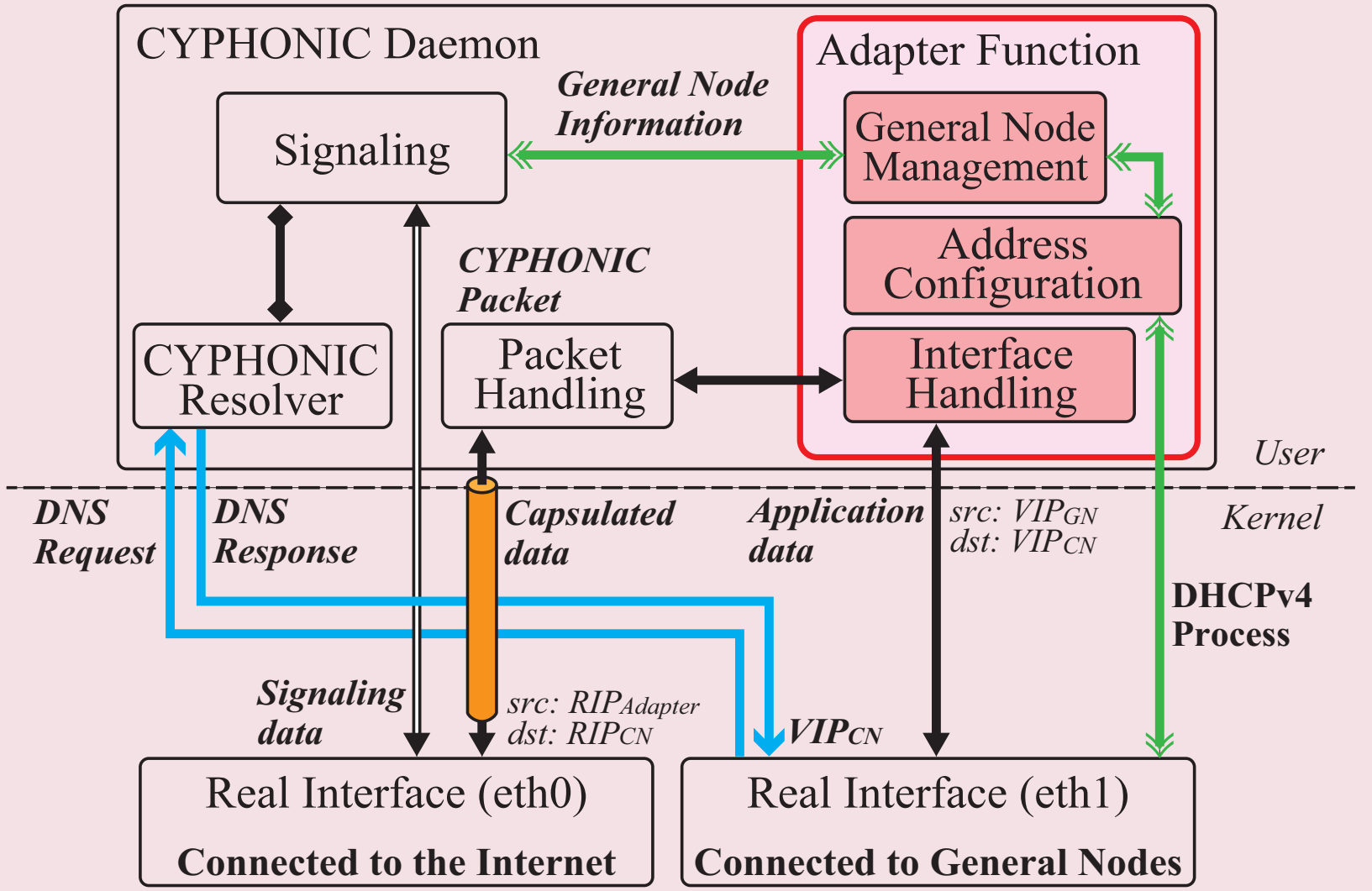


CYPHONICアダプタ システムモデル

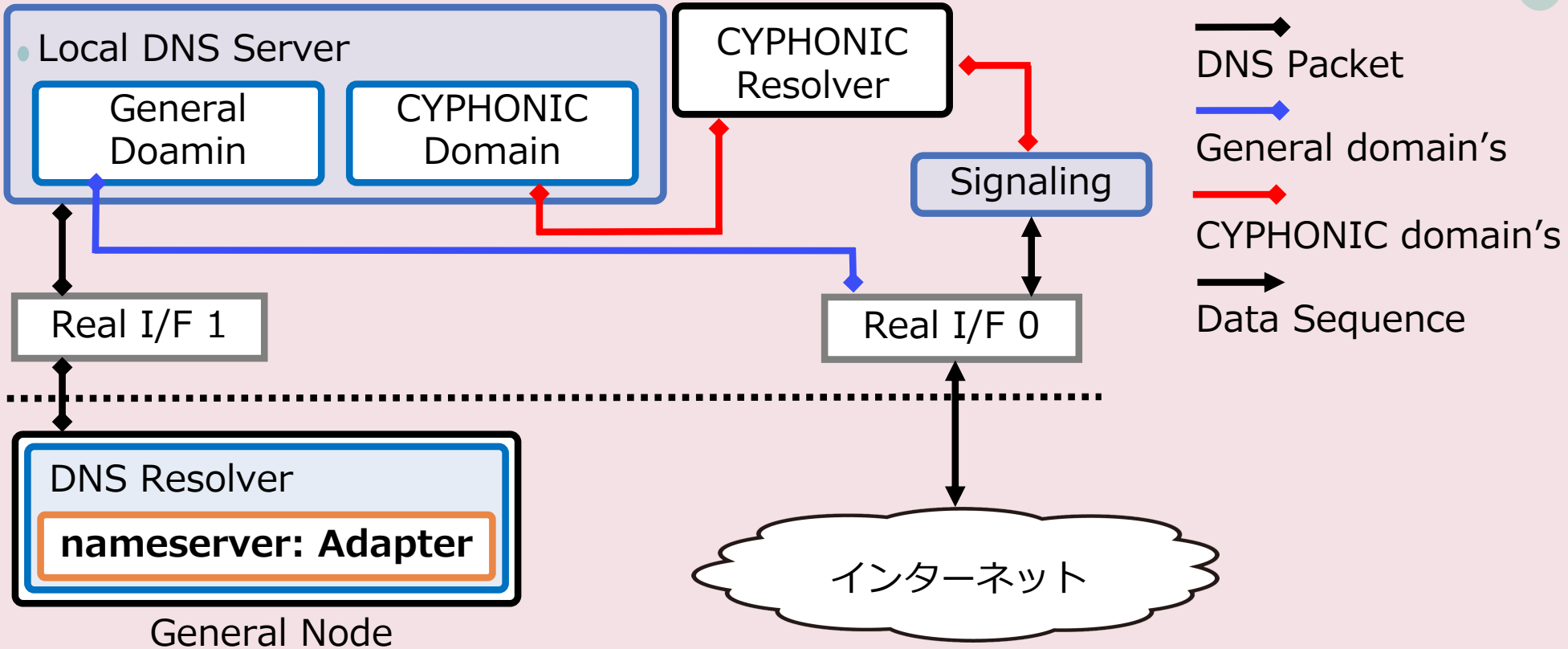


VIP: Virtual IP　RIP: Real IP　GN: General Node　CYP: CYPHONIC

System model of CYPHONIC Adapter



DNSパケットの処理



1. Real I/F 1 を介してDNSクエリを受信
2. Local DNSでドメインをフィルタリング
   - ・一般ドメイン　　：Real I/F 0 からネットワークへ送信
   - ・CYPHONICドメイン　：CYPHONIC Resolver Moduleへ転送
3. DNSリクエストから相手ノードのFQDNを取得
4. Signaling Moduleにより仮想IPアドレスを取得

認証処理および登録処理

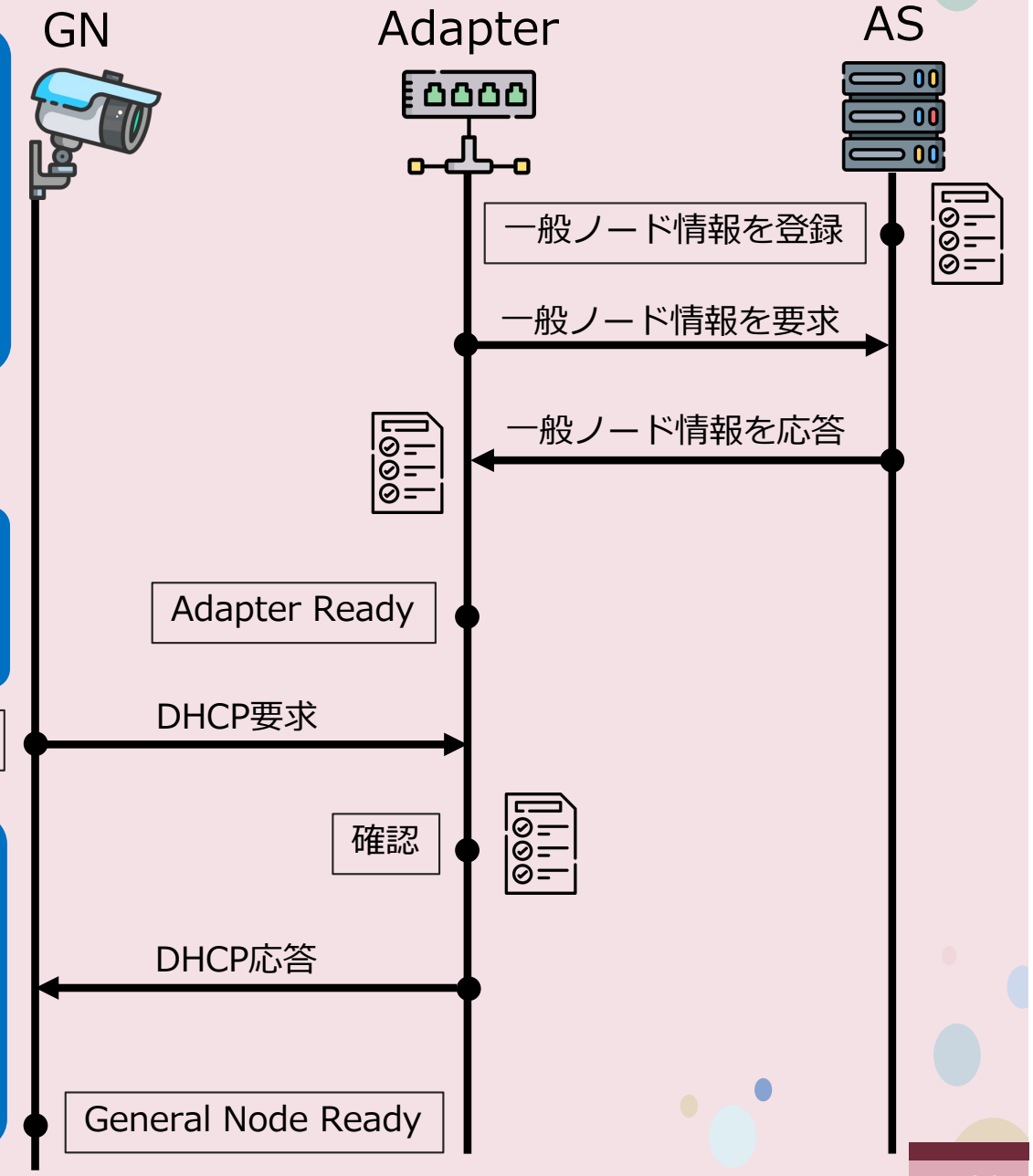
一般ノードの情報を
クラウドサービスに登録

・仮想IPアドレス
・FQDN
・MACアドレス

CYPHONICアダプタが
起動時に一般ノード情報を取得

管理している一般ノードの情報に
基づいて仮想IPアドレスを付与

→ クラウドサービスに登録された
端末のみが通信が可能



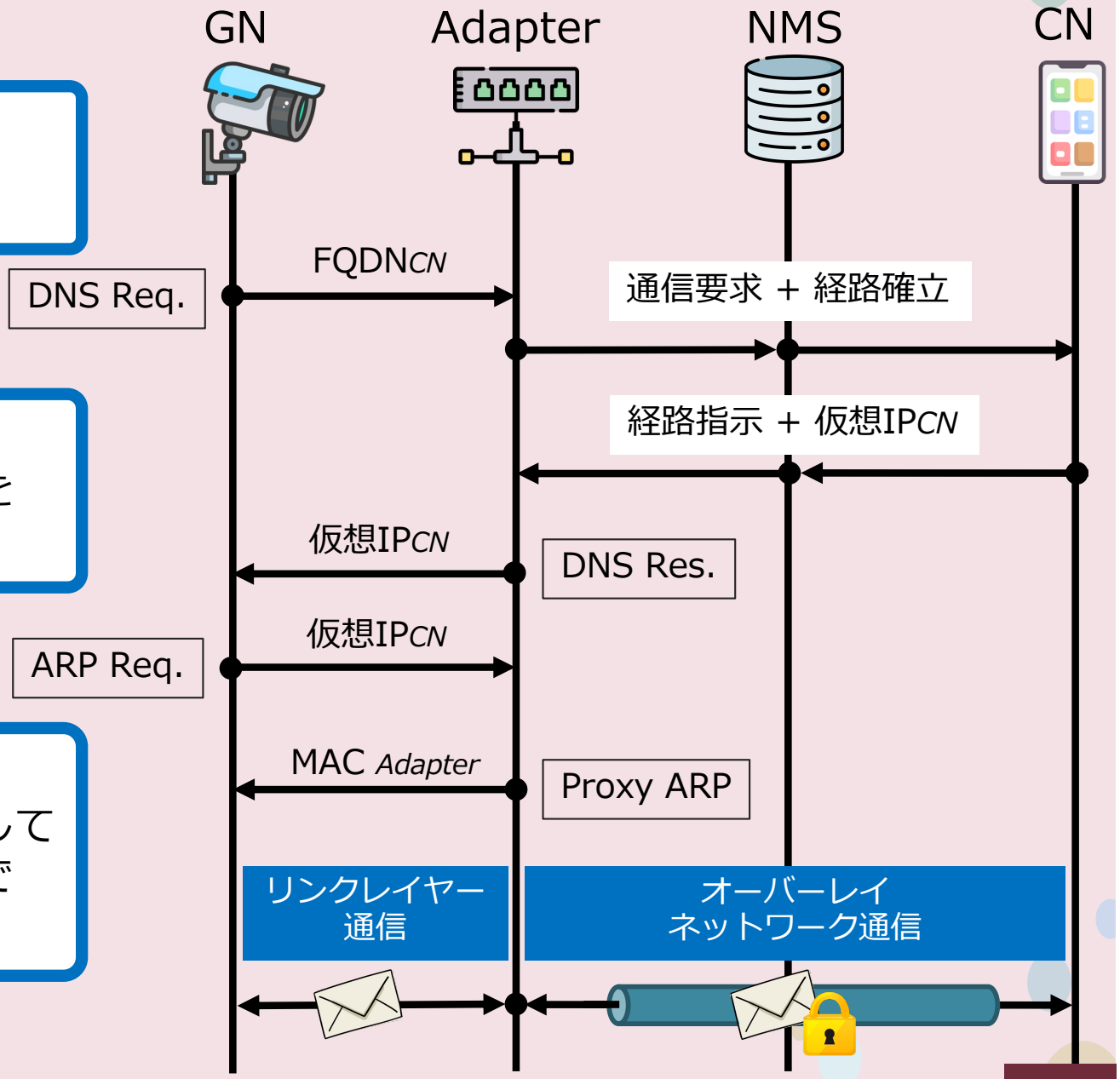
GN：General Node　AS：Authentication Service

通信処理

DNSリクエストを受信して
NMSに通信開始要求を送信

DNSレスポンスを生成して
相手ノードの仮想IPアドレスを
一般ノードへ通知

リンクレイヤー通信によって
一般ノードからパケットを取得して
オーバーレイネットワーク上で
相手ノードと通信

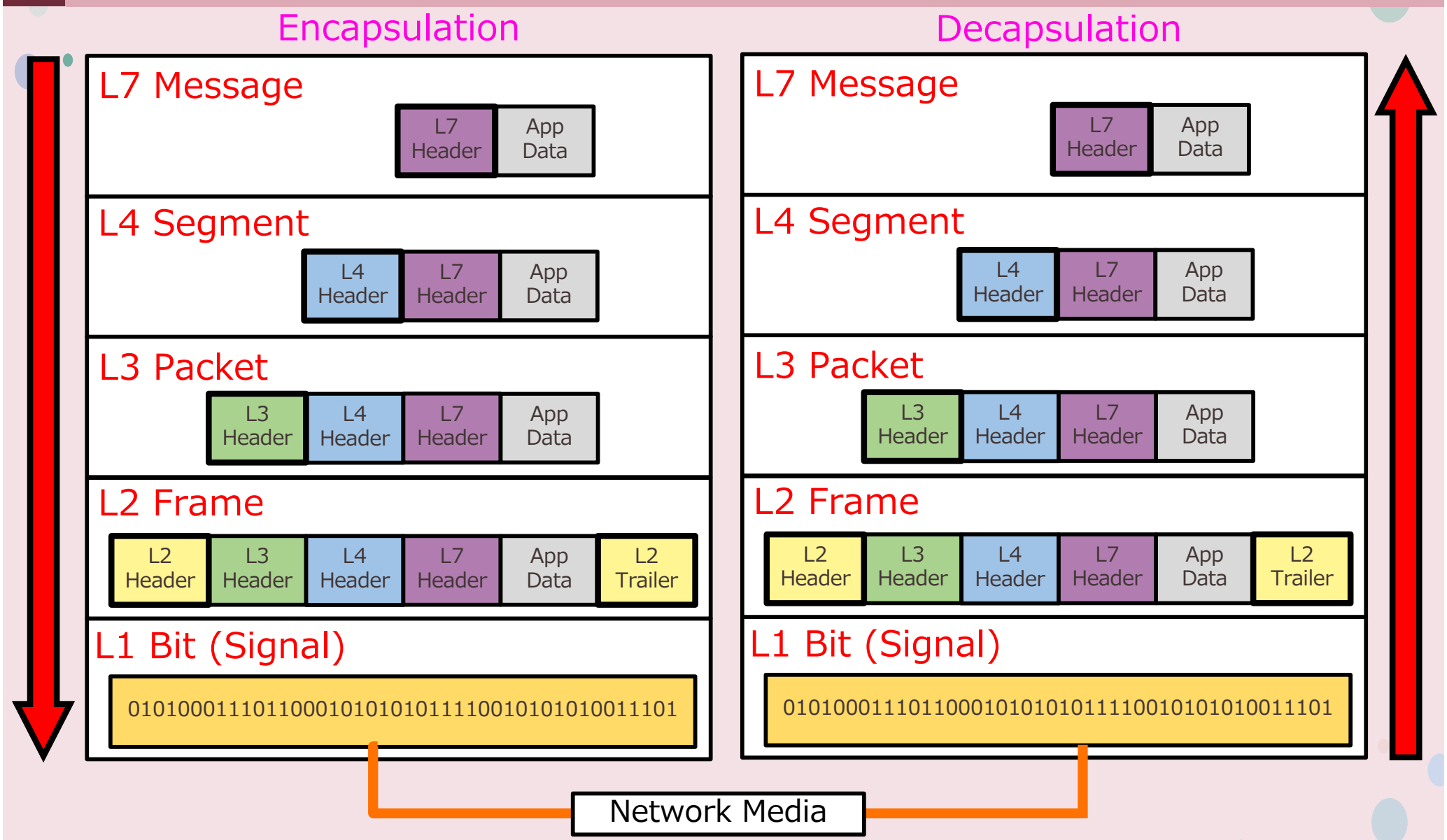


GN：General Node　NMS：Node Management Service　CN：Correspondent Node

TCP/IP プロトコルスイート

L7 (Application)	アプリケーション, ユーザインターフェースなどによりデータを扱う
L4 (Transport)	データ伝送に伴うエラー訂正, 再送制御などのフロー情報を管理 **信頼性のないIPをサポートし, 宛先まで確実な送受信を実現する**
L3 (Network)	複数のネットワーク間でデータ伝送を行う
L2 (Datalink)	直接接続されたネットワーク内で正確なデータ伝送を行う
L1 (Physical)	L2フレームをビット列, 電圧の高低などの信号情報に変換して伝送媒体に伝送

カプセル化・デカプセル化



各レイヤでPDU (Protocol Data Unit) を付加して送受信

【付録】研究業績

Ren Goto, Taiki Yoshikawa, Hijiri Komura, Kazushige Matama, Chihiro Nishiwaki, and Katsuhiro Naito.

"Design and Basic Evaluation of Virtual IPv4-based CYPHONIC adapter"

The 13th IIIS International Multi-conference on Complexity, Informatics and Cybernetics (IMCIC), March 2022.

DOI: N/A (Accepted)

Taiki Yoshikawa, Hijiri Komura, **Ren Goto**, Kazushige Matama, Chihiro Nishiwaki, and Katsuhiro Naito.

"Demonstration of video conferencing tool with overlay network protocol"

The 19th IEEE Consumer Communications & Networking Conference (CCNC), January 2022.

DOI: 10.1109/CCNC49033.2022.9700703.

Taiki Yoshikawa, Hijiri Komura, Chihiro Nishiwaki, **Ren Goto**, Kazushige Matama, and Katsuhiro Naito.

"Evaluation of new CYPHONIC: Overlay network protocol based on Go language"

The 40th IEEE International Conference on Consumer Electronics (ICCE), January 2022.

DOI: 10.1109/ICCE53296.2022.9730323.

【付録】研究業績

後藤 廉, 吉川 大貴, 小村 聖, 眞玉 和茂, 内藤 克浩

"【2021年度学生奨励賞】仮想 IPv4 アドレスを想定した CYPHONIC アダプタの設計と基礎評価"

Information Processing Society of Japan (IPSJ) - 第33回コンシューマ・デバイス&システム研究会 (CDS), January 2022.

J-GLOBAL ID: 202202291942447619, Reference number: 22A0421754

西脇 千紘, 吉川 大貴, 小村 聖, **後藤 廉**, 眞玉 和茂, 内藤 克浩

"iOS におけるアプリケーション内独自プロトコル実装に関する一検討"

Institute of Electronics, Information and Communication Engineers (IEICE) - 令和三年度 電気・電子・情報関係学会 東海支部連合大会, September 2021.

J-GLOBAL ID: 202202266081463947, Reference number: 22A0608290