ユーザをエンドツーエンドでグルーピングする フレキシブルプライベートネットワーク FPN の提案

桑畑　成美[†*]，鈴木　秀和[†]，内藤　克浩[‡]，渡邊　晃[†] ([†] 名城大学，[‡] 愛知工業大学)

Proposal for Flexible Private Network by Making End to End User Groups

Narumi Kuwahat[†], Hidekazu Suzuki[†], Katsuhiro naito[‡], Akira Watanabe[‡] ([†]Meijo University, [‡]Aichi Instiure of Technology)

1　はじめに

モバイル端末の普及や無線インフラの普及により，確実に通信経路を確立する通信接続性や，通信中にネットワークが切り替わっても通信を継続することができる移動透過性が求められている．これらの課題を解決する技術として，NTMobile（Network Traversal with Mobility）が提案されている．しかしながら NTMobile は通信の制約を完全に除去することはできるが，エンドツーエンドの相手認証については今後の課題であった．そこで本稿では DC（Direction Coordinator）にユーザグループを定義することにより，エンドツーエンドの相手認証を可能にする方式を提案する．具体的には，業務サーバごとにアクセスを許可されたユーザを定義する．この定義はユーザが社外にいても有効で，かつ場所を移動しても定義を変える必要がない．

2　現状のネットワークの課題と NTMobile

インターネットにつながるネットワークのほとんどはプライベートアドレスである．しかしながら，このようなネットワークではインターネット側からプライベート空間への通信開始ができず，また異なるプライベート空間同士の直接通信ができない．通信中に移動すると IP アドレスが変化し通信が途切れる．さらに，IPv6 への移行が求められているが IPv4/IPv6 互換性がないため移行が進まず，両者が混在した環境となっている．

これらの問題を解決する技術の一つとして，NTMobile が提案されている．NTMobile はエンド端末（以下 NTM 端末）に NTMobile アプリケーションをインストールすることで，既存のユーザアプリケーションを変更することなく，通信接続性と移動透過性を可能とする技術である．NTMobile はインターネット上に，NTM 端末へ通信経路を指示する DC を設置する必要がある．DC と NTM 端末間は常に通信経路が確保されており，通信開始時に DC から NTM 端末に対して適切な指示を出すことにより，通信接続性と移動透過性を実現可能にしている．このように NTMobile によりネットワークの制約を除去できるが，エンド端末間の認証が定義されておらず，同じ NTM 端末同士で不正アクセスができる可能性があった．

3　フレキシブルプライベートネットワーク FPN の提案

<3・1>提案方式　Fig. 1 に，フレキシブルプライベートネットワーク（FPN;flexible Private Network）のネットワーク構成を示す．FPN はあらゆる環境で通信が可能な，エンドツーエンド VPN であることを示す新たな用語である．Fig. 1 では携帯網のスマートフォン，自宅 PC，企業内 PC に NTMobile がインストールされている．インストールすることにより NTM 端末ごとに NTMobile 特有の名前が与えられる．企業とインターネット間の FW には NTMobile の通信が可能となるよう，ポート番号の設定がされている．これにより NTM 端末同士は通信の制約が完全に除去された自由な通信をすることが可能となる．しかしセキュリティ上，自由に通信できては困る場合が多い．そこで DC に通信グループを設定し，経路の生成を制御する．NTMobile では DC が両エンドノードに対して返信経路を指示するため，DC に定義されたグループの情報をもとに同一グループのメンバーだけが通信を行うように制御することが可能である．Fig. 1 では，企業 A および企業 B が NTMobile を運用しており，グループとしてサーバ S1,S2,S3 にアクセスできる 3 グループが定義されている．NTM 端末やサーバには “（利用者名）.（所属名）.ntm.jp” のように名前が付けられている．グループの定義方法としては，業務サーバごとにアクセスが可能な NTM 端末を指定する．サーバ S1 には企業 A，企業 B の特定の社員がアクセス可能である．異なる企業に所属している場合でも，サーバごとにアクセス可能な社員の名前を直接記述することでアクセス制御が可能となる．また，サーバ S2,S3 にはそれぞれ企業 A，企業 B 内の社員がアクセス可能である．同じ企業に所属している場合，NTM 端末の名前に企業特有の共通部分があるため，ワイルドカードを用いることで簡単に定義することができる．

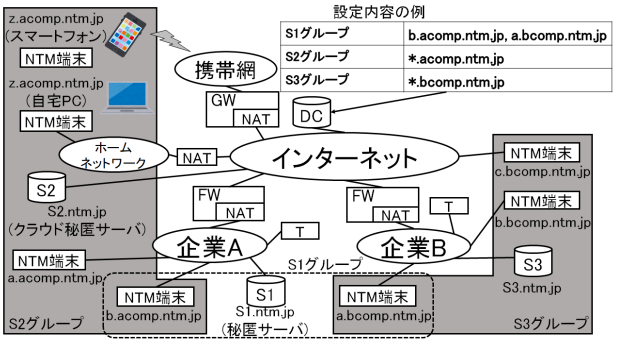


Fig. 1　フレキシブルネットワークの構成

4　まとめ

DC にアクセス可能なユーザグループのリストを持たせることにより,NTMobile を用いてフレキシブルプライベートネットワークを実現する方式を提案した．

文　献

[1] 上酔尾．他：IPv4/IPv6 混在環境で移動透過性を実現する NTMobile の実装と評価, 情報処理学会論文誌 Vol.54, No.10, pp.2288-2299, 2013

ユーザをエンドツーエンドで グルーピングする フレキシブルプライベートネットワーク FPN の提案

桑畑成美†, 鈴木秀和†, 内藤克浩‡, 渡邊晃†
†名城大学　理工学部　情報工学科
‡愛知工業大学　情報工学科

Watanabe Lab.

研究背景　～現状のネットワーク～

- インターネットの普及により様々な問題が発生している
  - NAT越え問題
    - インターネット側からプライベート側へ通信を開始できない
  - IPv4/IPv6の非互換性
    - 互換性がなく、通信が行えない
  - 移動透過性
    - 通信中にネットワークの切り替えが行えない
  - セキュリティ
    - 不正アクセス、盗聴の可能性

解決策：NTMobile (Network Traversal with Mobility)

研究目的 ～NTMobileの課題～

- エンド端末間の認証がない
  - サーバへ不正アクセスの可能性
  - サーバ利用者の管理

解決策： DCに通信グループを定義

提案方式

- グループリストを定義
  - リストにより経路の生成を制御
  - ワイルドカードにより定義を簡単化

- DCがリストを所持
  - NTM端末では通信開始時にDCから経路を指示される
  - 経路確立が許可されているかリストで判断

FPN（flexible Private Network）

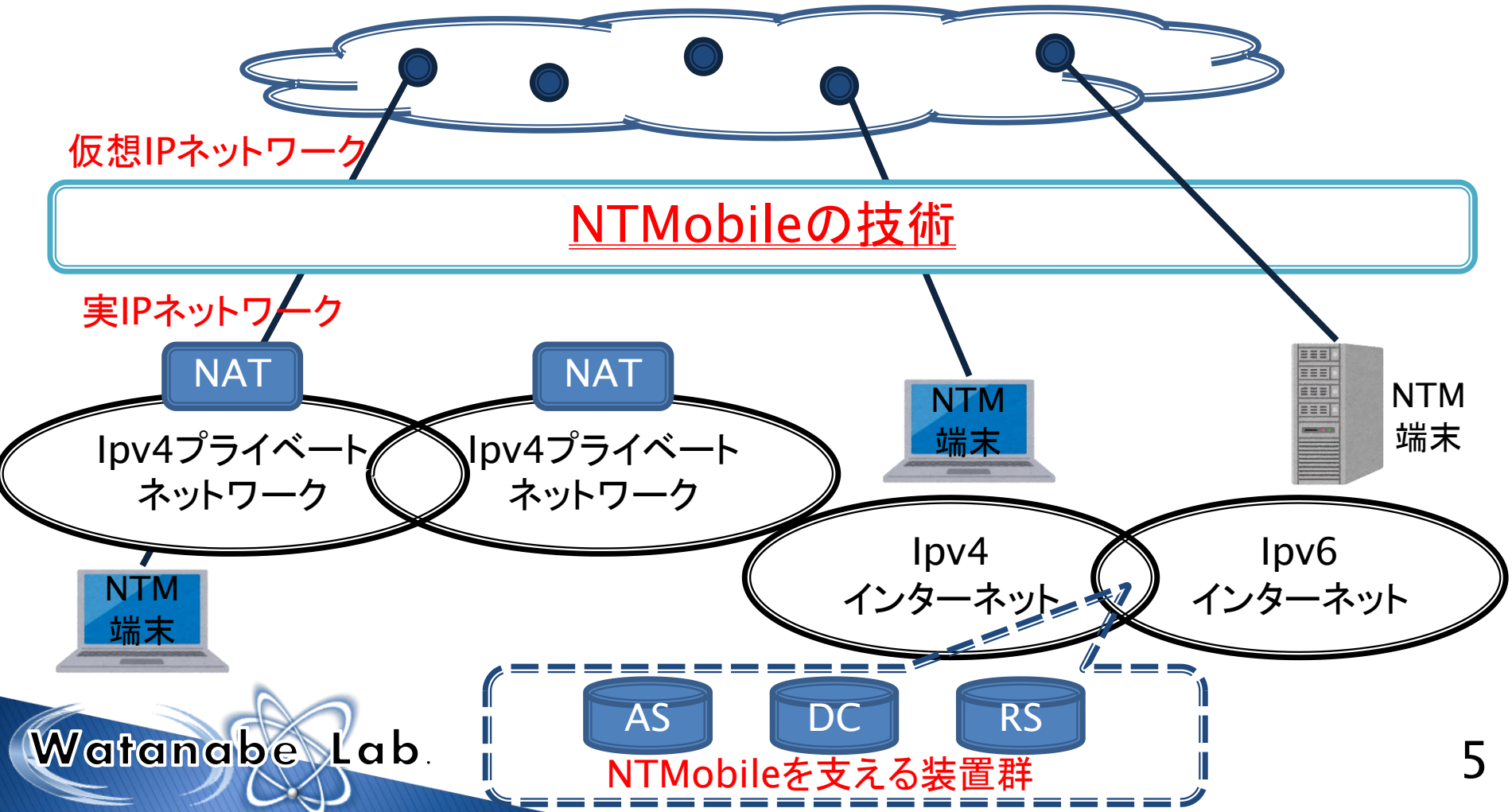
  - あらゆる環境で通信可能なエンドツーエンドVPN

NTMobileの構成

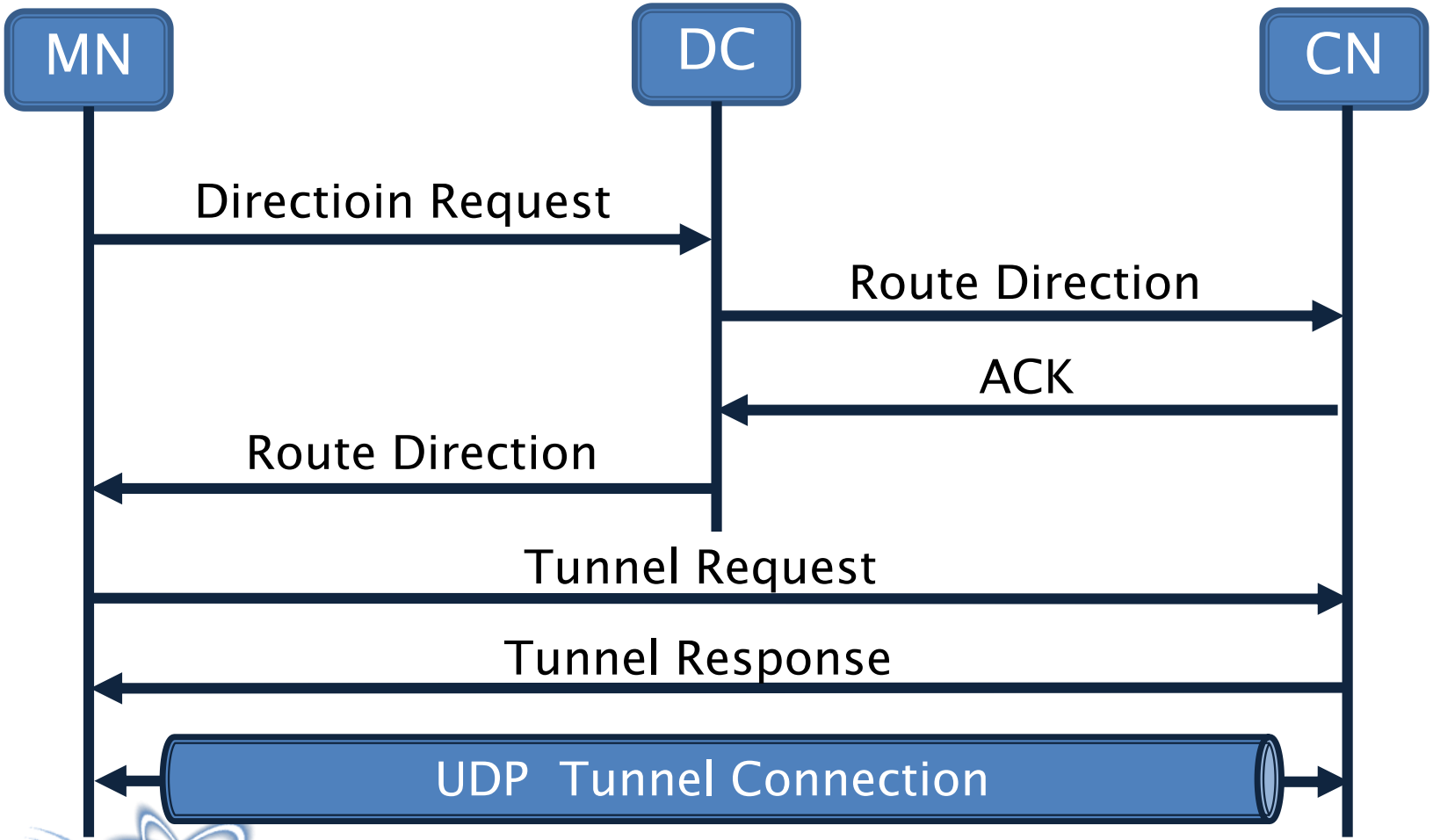
- NTM端末
  - NTMobileアプリをインストールした端末
- DC(Direction Coordinator)
  - 通信経路の指示
  - NTM端末の仮想IPアドレスの管理
- RS(Relay Server)
  - 通信の中継
    - 両NTM端末がいずれもNAT配下にある場合に利用

NTMobileの概要

- NTMobileが構築する仮想IPネットワーク



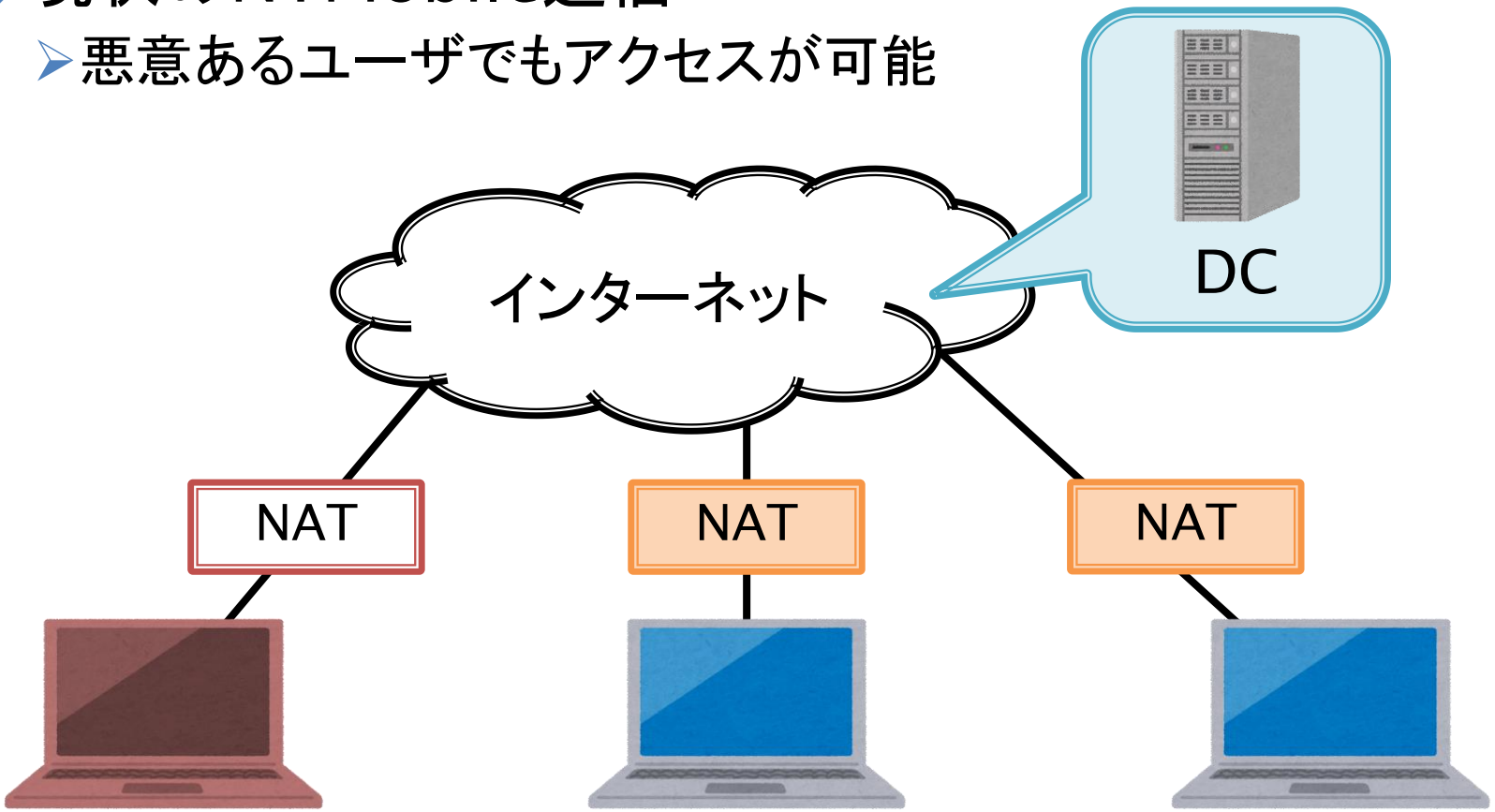
現状のシーケンス



※MN,CNはNTM端末

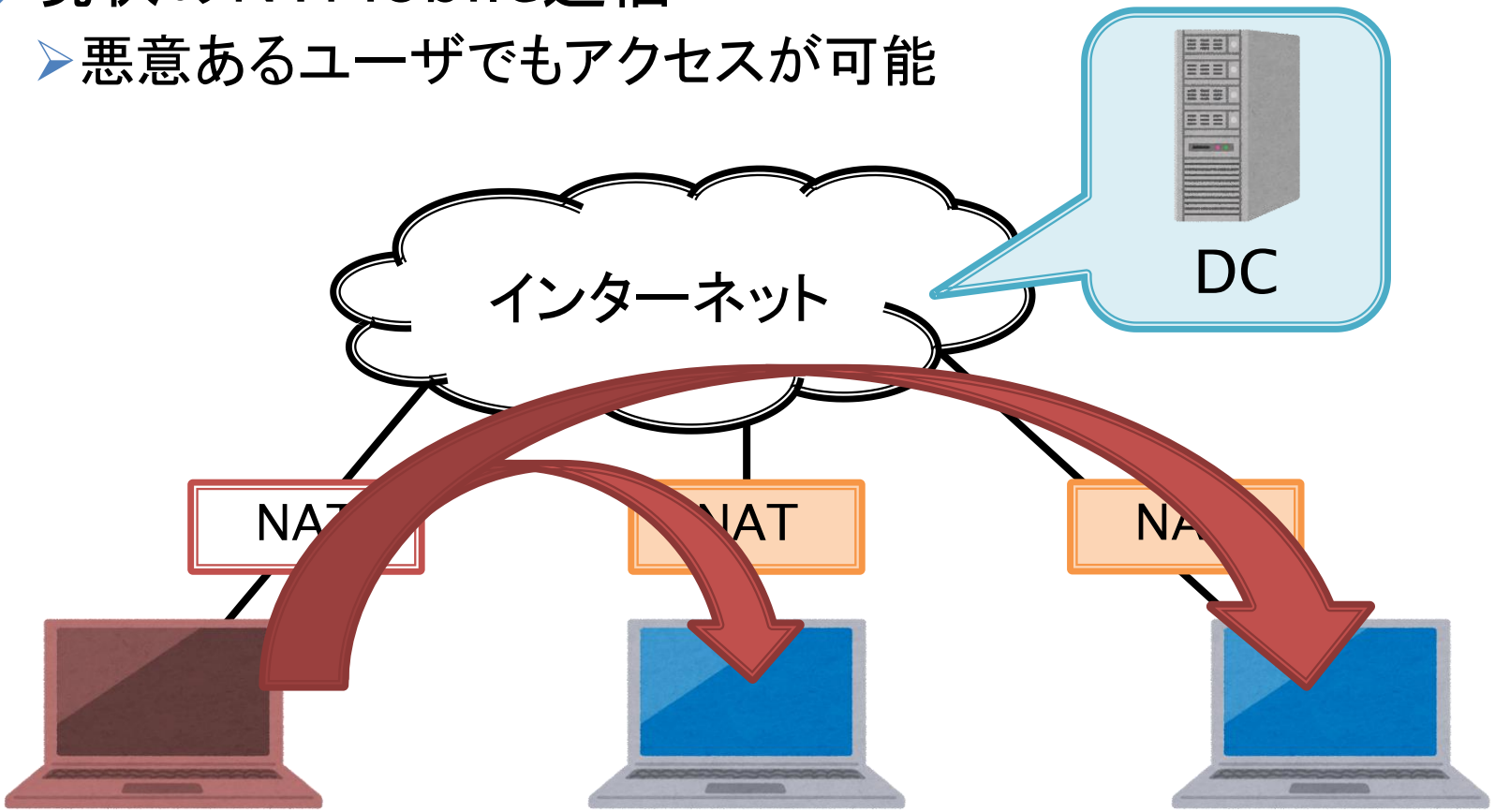
現状の通信

- 現状のNTMobile通信
  - 悪意あるユーザでもアクセスが可能



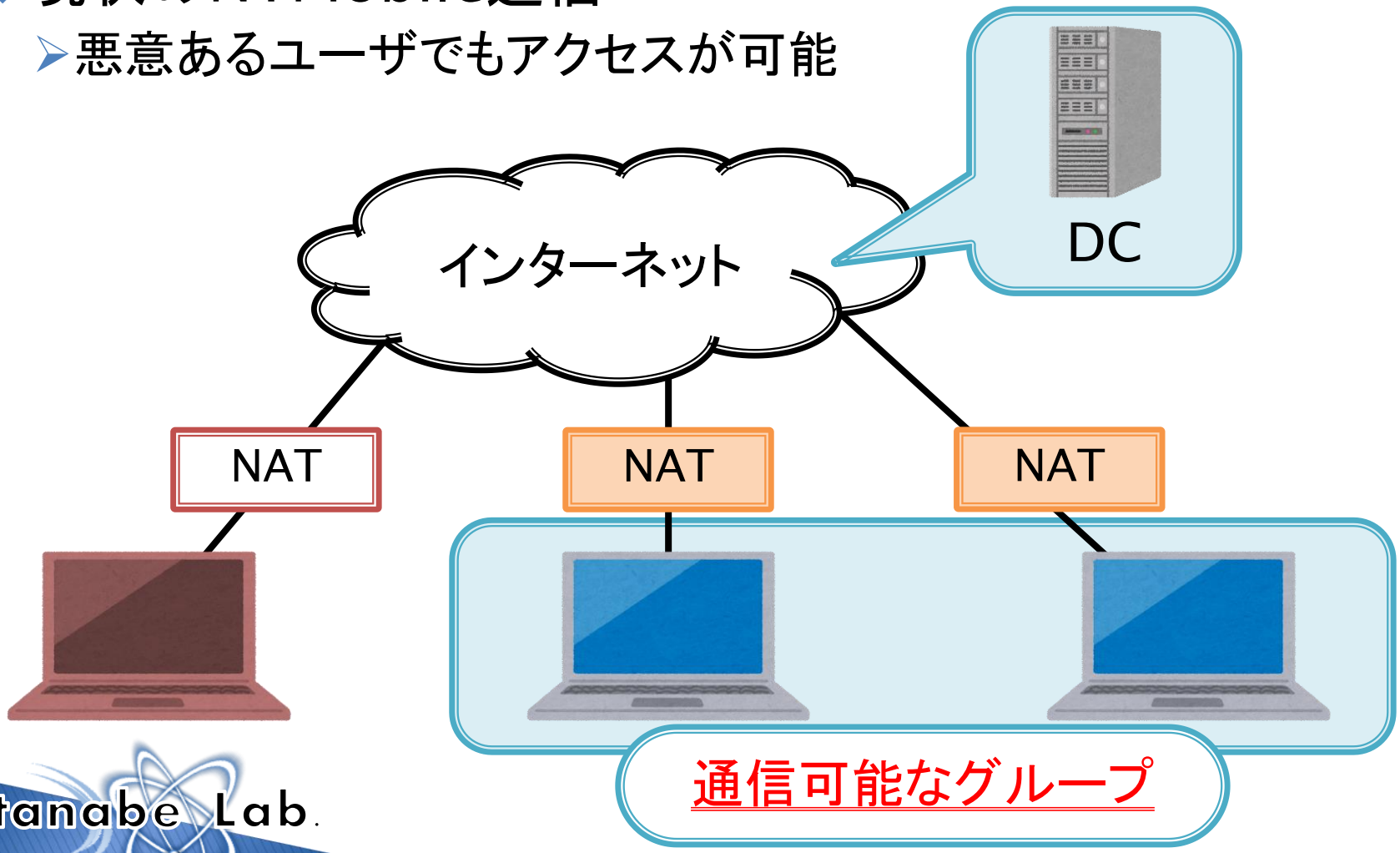
現状の通信

- 現状のNTMobile通信
  - 悪意あるユーザでもアクセスが可能



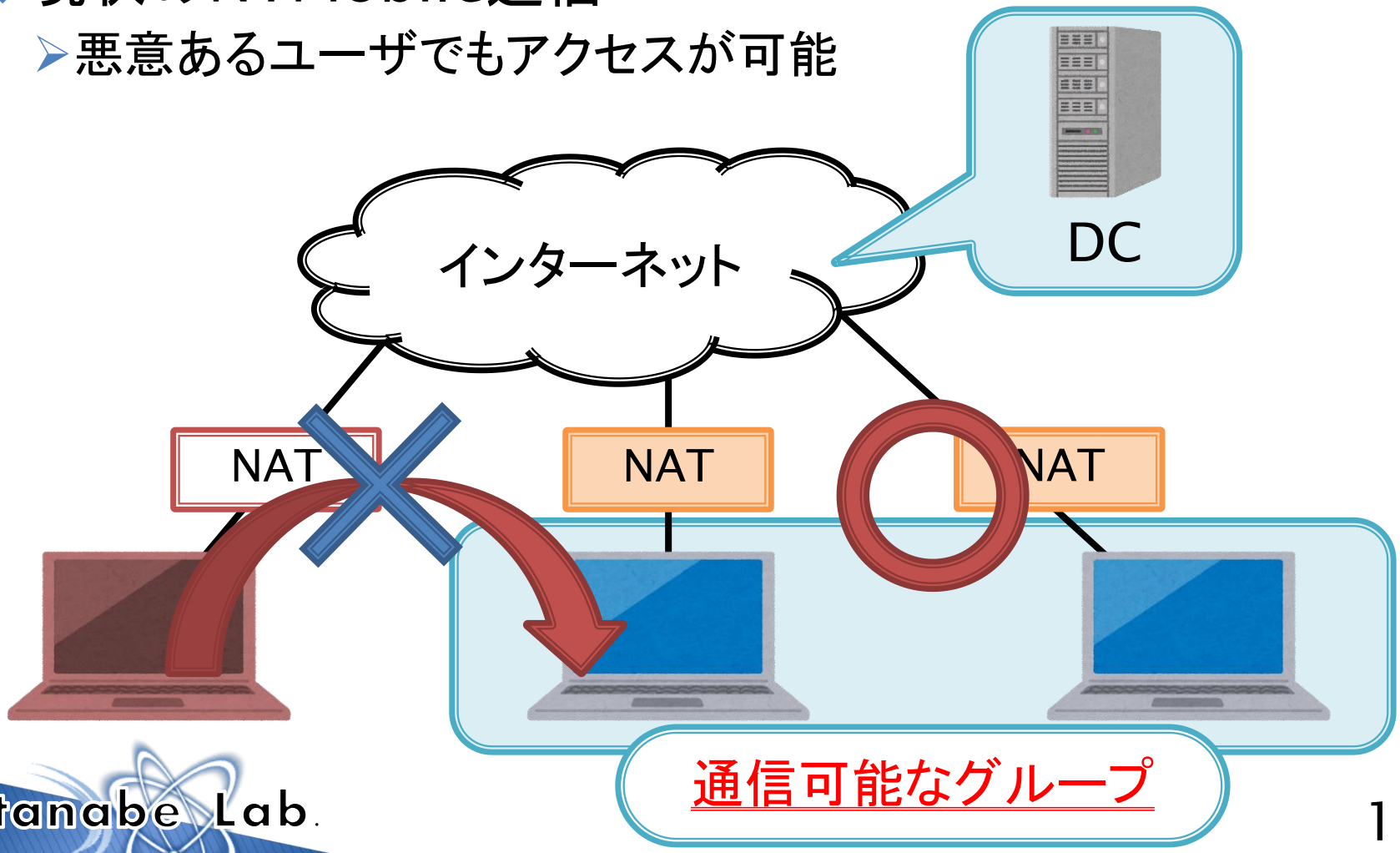
現状の通信

- 現状のNTMobile通信
  - 悪意あるユーザでもアクセスが可能

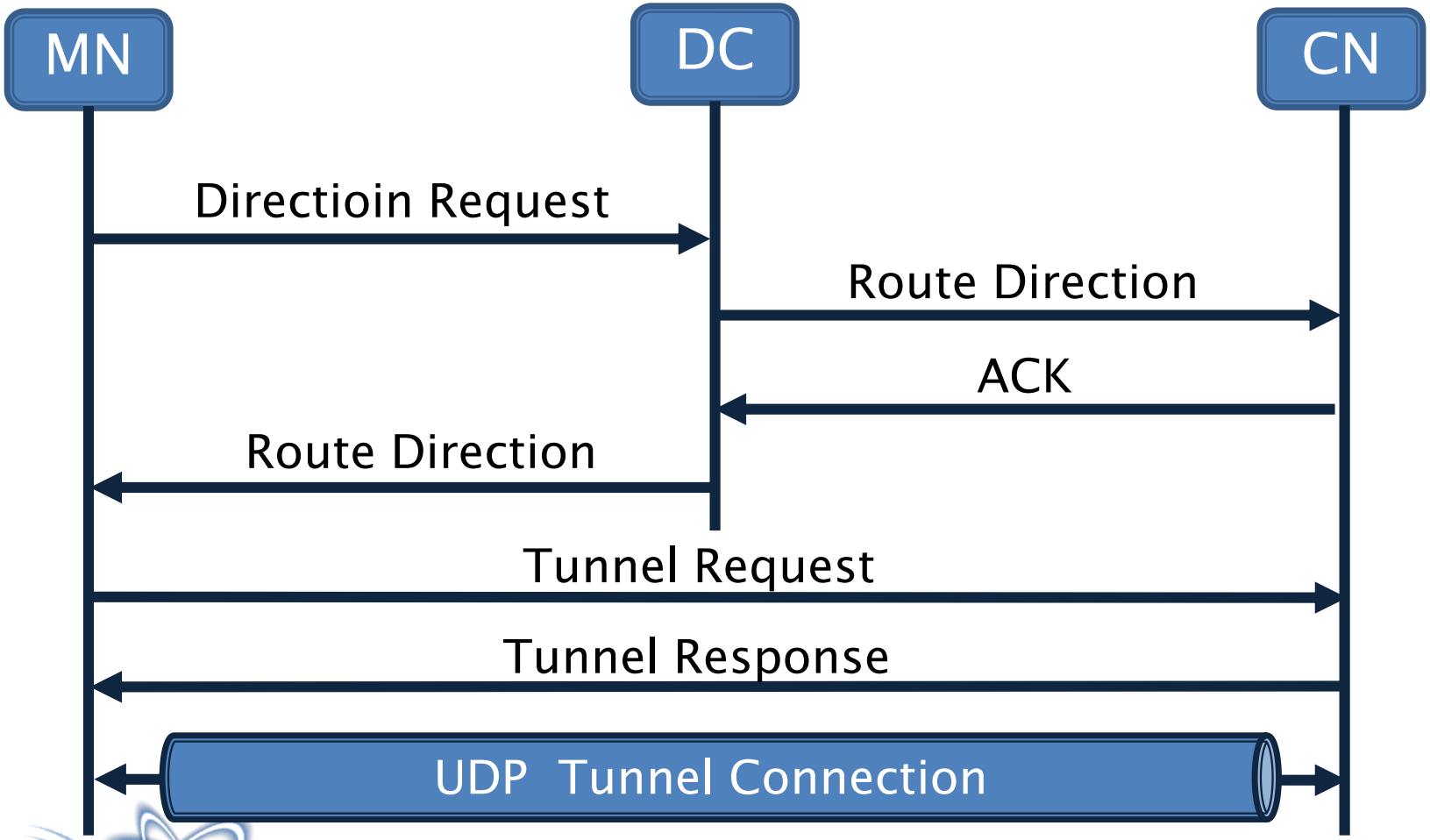


現状の通信

- 現状のNTMobile通信
  - 悪意あるユーザでもアクセスが可能

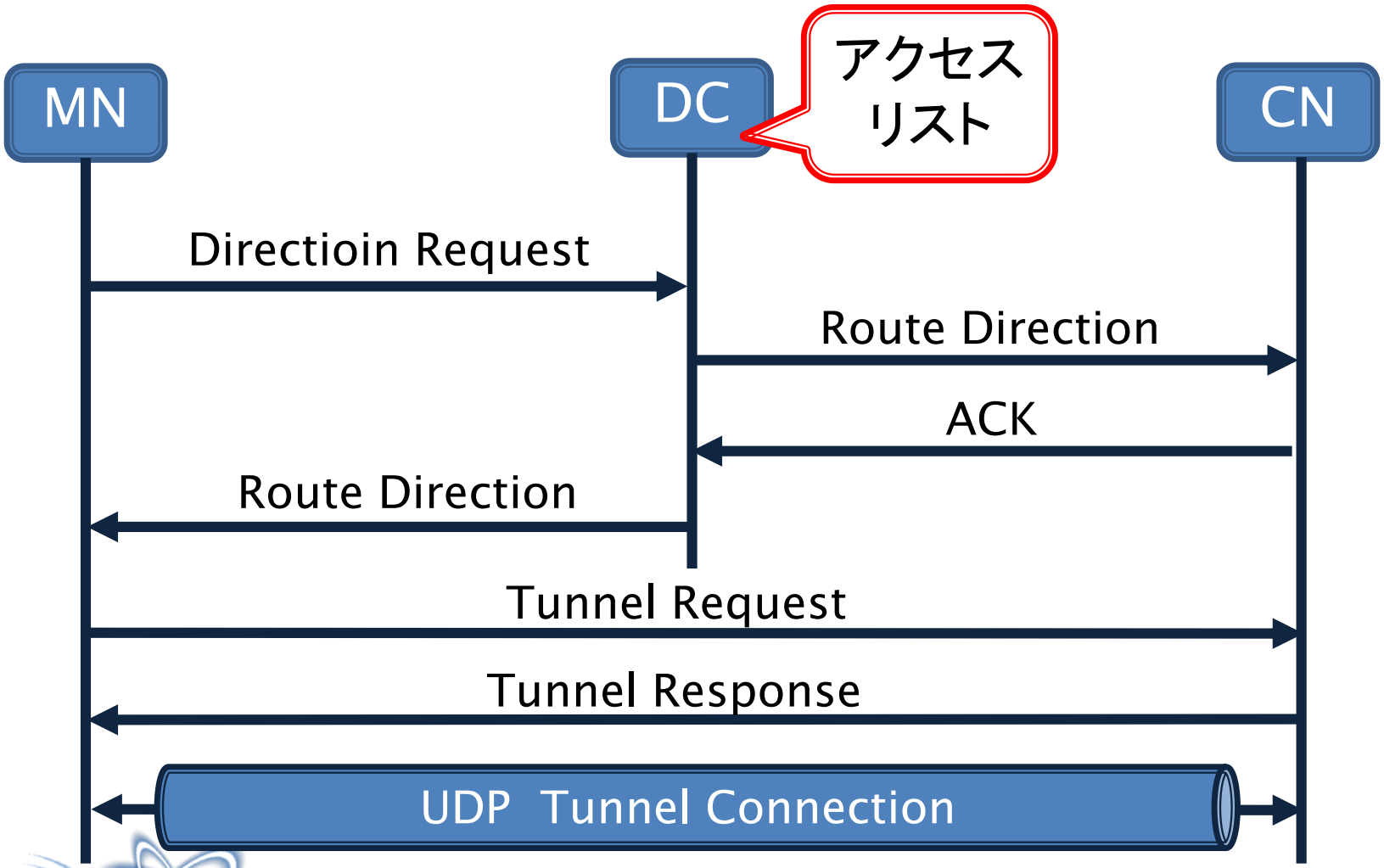


提案方式のシーケンス(1/3)



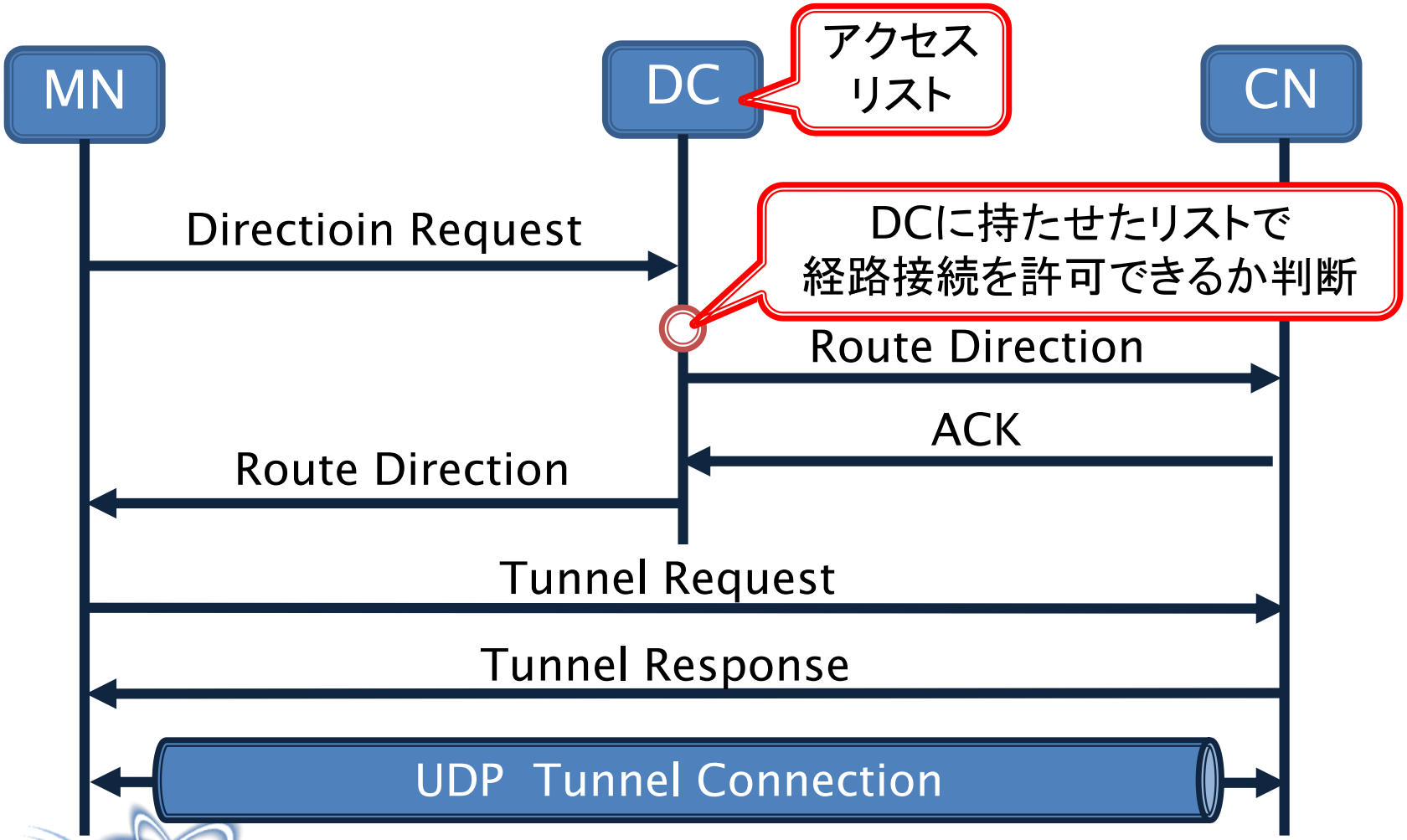
※MN,CNはNTM端末

提案方式のシーケンス(2/3)



※MN,CNはNTM端末

提案方式のシーケンス(3/3)



※MN,CNはNTM端末

NTM端末名の定義

- NTM端末に固有の名前を与える

NTM端末名：（利用者名）.（所属名）.ntm.jp

NTMサーバ名：（サーバ名）.ntm.jp

■ 定義の例

NTM端末名：a.acomp.ntm.jp
NTMサーバ名：S1.ntm.jp

NTM端末名の定義

- NTM端末に固有の名前を与える

NTM端末名：（利用者名）.（所属名）.ntm.jp

NTMサーバ名：（サーバ名）.ntm.jp

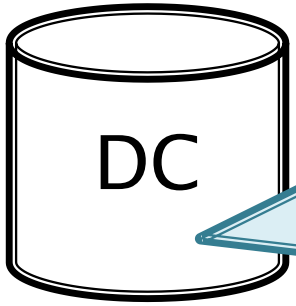
同じ企業，課など
所属が同じ場合は同じ

■ 定義の例

NTM端末名：a.acomp.ntm.jp
NTMサーバ名：S1.ntm.jp

認証方法

- DCがグループリストを所持
  - 接続要求時に経路確立が許可されているか判断
    - 許可されている時：シグナリングを継続
    - 許可されていない時：シグナリングを破棄



グループ名	利用者名
S1	b.acomp.ntm.jp,a.bcomp.ntm.jp
S2	＊.acomp.ntm.jp
S3	＊.bcomp.ntm.jp

グルーピング方法

- グルーピング方法としてサーバ主体，ユーザ主体の方法が考えられる
- 今回はサーバ主体で検討

■ サーバ主体の場合

グループ名	利用者名
S1	b.acomp.ntm.jp,a.bcomp.ntm.jp
S2	＊.acomp.ntm.jp

■ ユーザ主体の場合

グループ名	利用者名
b.acomp.ntm.jp	b.acomp.ntm.jp,a.bcomp.ntm.jp
a.bcomp.ntm.jp	＊.acomp.ntm.jp

リストの定義方法①

① 直接指定（例：S1）

- 利用者のNTM端末名を直接指定
- 所属が異なる場合にも、同じサーバへアクセスが可能

グループ名	利用者名
S1	b.acomp.ntm.jp,a.bcomp.ntm.jp
S2	＊.acomp.ntm.jp
S3	＊.bcomp.ntm.jp

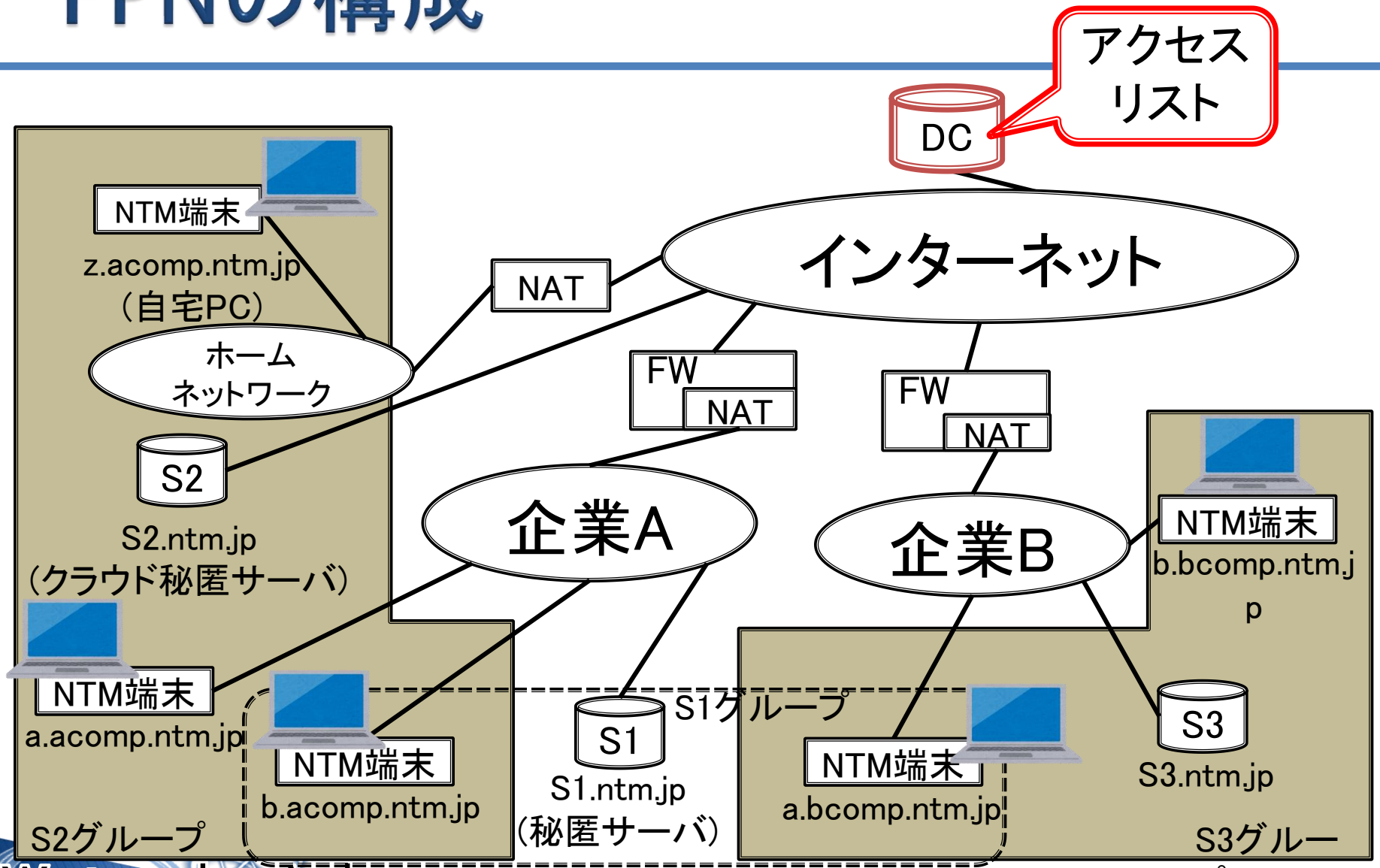
リストの定義方法②

② ワイルドカードを利用（例：S2,S3）

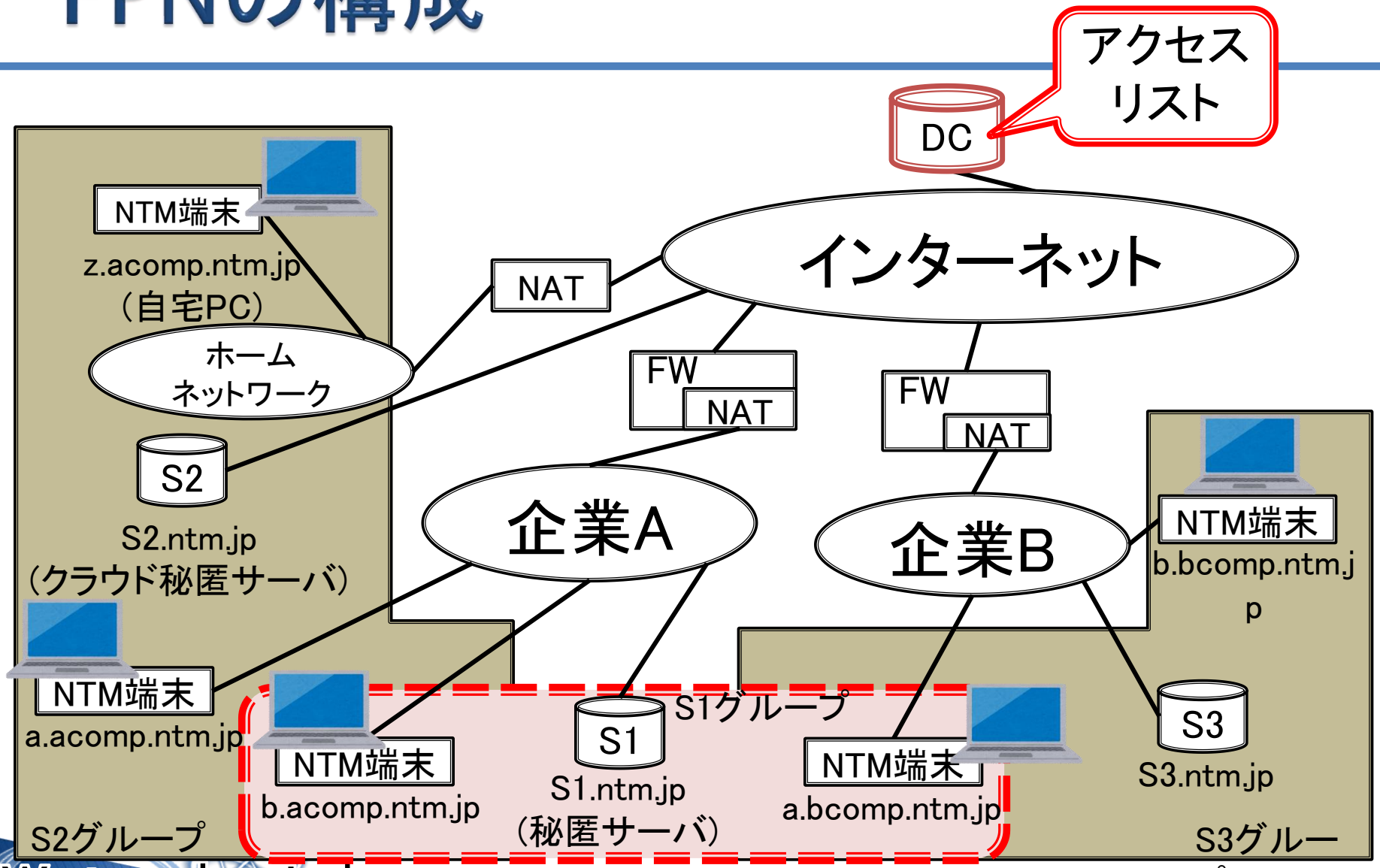
- 利用者名にワイルドカードを利用し、複数指定
- 所属名により簡単に複数人を指定可能

グループ名	利用者名
S1	b.acomp.ntm.jp,a.bcomp.ntm.jp
S2	＊.acomp.ntm.jp
S3	＊.bcomp.ntm.jp

FPNの構成


アクセス
リスト
DC
インターネット
NAT
NTM端末
z.acomp.ntm.jp
（自宅PC）
ホーム
ネットワーク
S2
S2.ntm.jp
（クラウド秘匿サーバ）
FW
NAT
FW
NAT
企業A
企業B
NTM端末
b.bcomp.ntm.j
p
NTM端末
a.acomp.ntm.jp
NTM端末
b.acomp.ntm.jp
S1グループ
S1
S1.ntm.jp
（秘匿サーバ）
NTM端末
a.bcomp.ntm.jp
S3
S3.ntm.jp
S2グループ
S3グループ

FPNの構成


アクセス
リスト
DC
インターネット
NAT
NTM端末
z.acomp.ntm.jp
（自宅PC）
ホーム
ネットワーク
S2
S2.ntm.jp
（クラウド秘匿サーバ）
FW
NAT
FW
NAT
企業A
企業B
NTM端末
b.bcomp.ntm.j
p
NTM端末
a.acomp.ntm.jp
NTM端末
b.acomp.ntm.jp
S1
S1.ntm.jp
（秘匿サーバ）
S1グループ
NTM端末
a.bcomp.ntm.jp
S3
S3.ntm.jp
S2グループ
S3グループ

まとめ

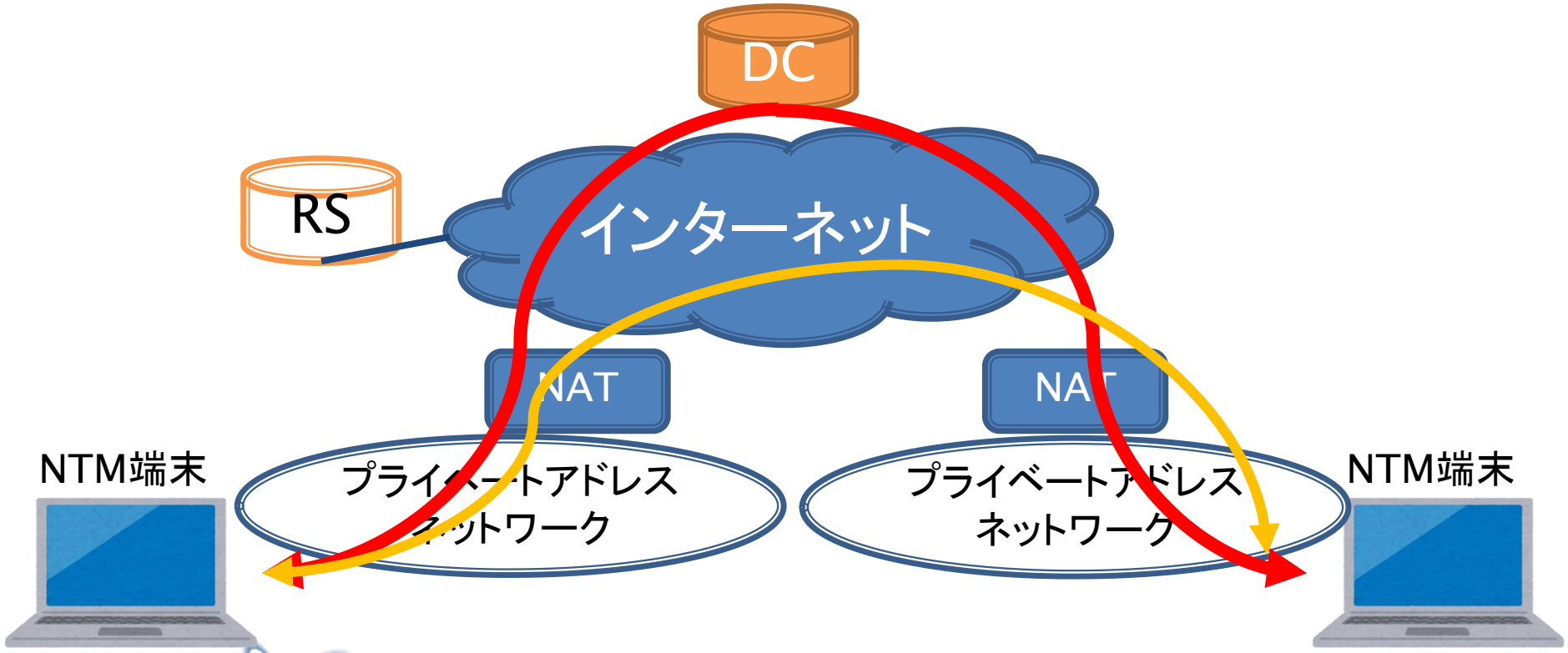
- NTMobileにおいて端末間の認証を検討
  - DCにアクセス可能なグループリストを持たせる
    - DCで経路を指示する際、リストで可能か判断
  - リストの定義
    - 所属が異なる場合や特定少数の場合、直接指定
    - 所属が同じ場合ワイルドカードで指定可
- 今後の予定
  - 実装及び性能評価

以下補足資料

NTMobileの概要

① NAT越えの実現

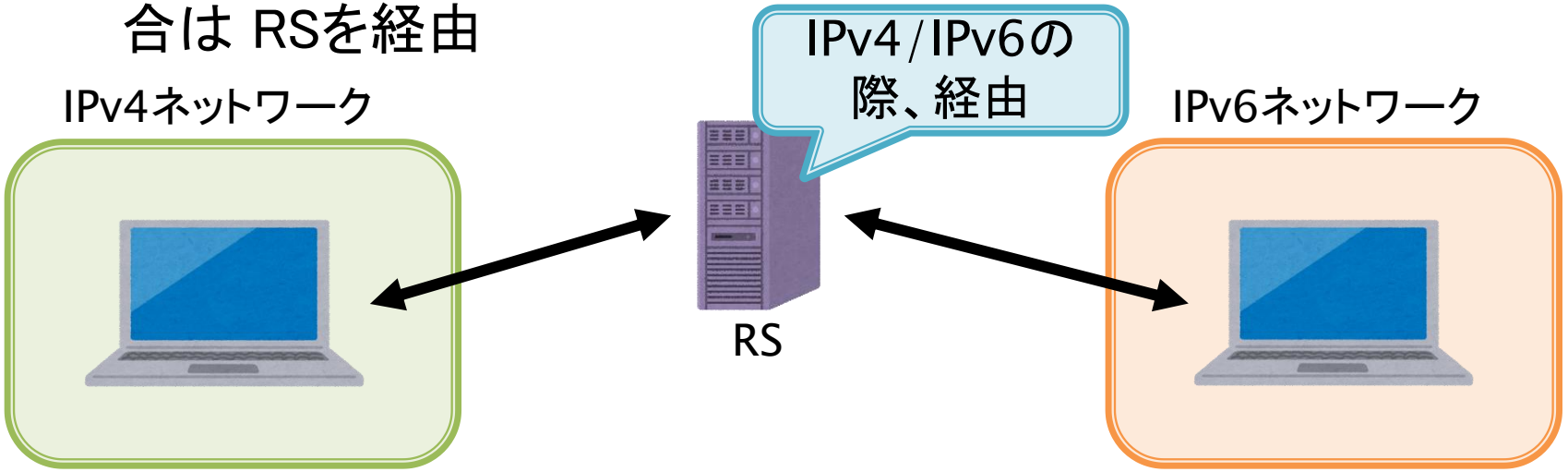
➢DCがNTM端末に最適な経路を指示



NTMobileの概要

② IPv4/IPv6の通信を実現

- DCにより経路指示
- 両NTM端末が異なるNAT配下、もしくはIPv4/IPv6通信の場合は RSを経由



実IPv4アドレス	カプセル化	
	仮想IPアドレス	データ

実IPv6アドレス	カプセル化	
	仮想IPアドレス	データ

NTMobileの概要

③ 移動透過性の実現

- 実IPアドレスでパケットをカプセル化
  - 移動しても仮想IPアドレス

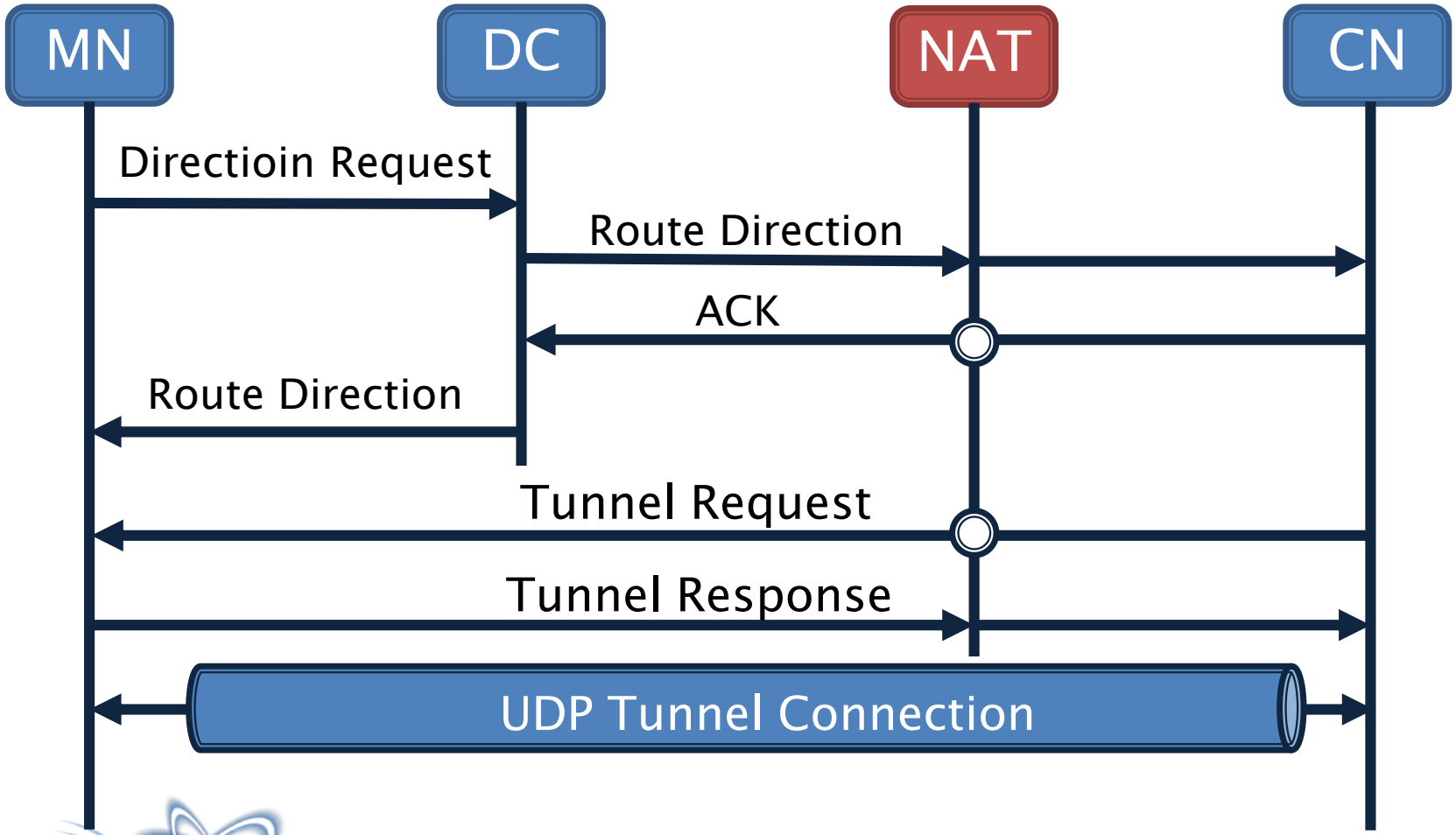
◆ 一般的なパケット

実IPアドレス	データ

◆ NTMobileのパケット

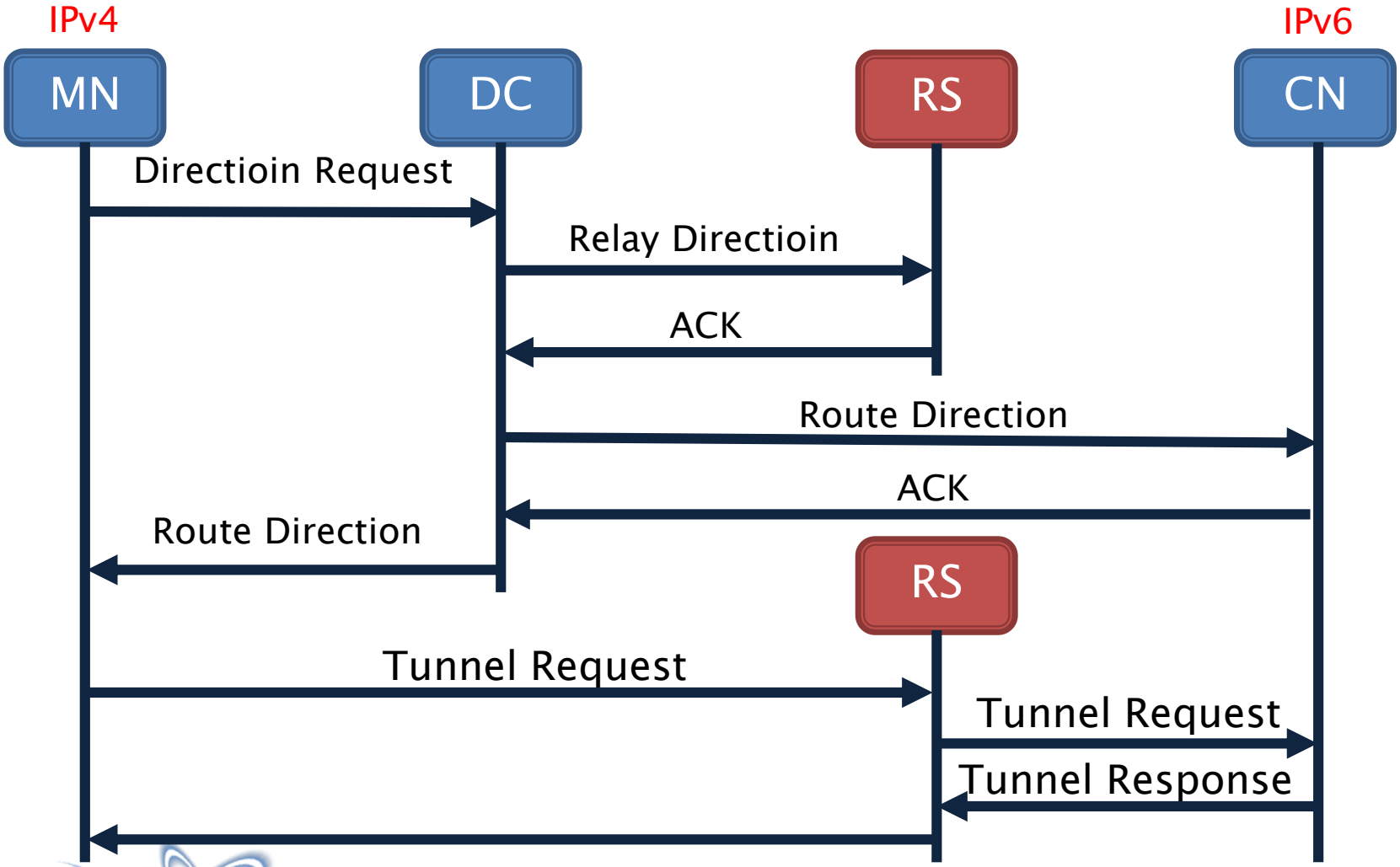
実 IPアドレス	カプセル化	
	仮想IPアドレス	データ

現状のシーケンス(NAT ver.)



※MN,CNはNTM端末

現状のシーケンス(RS ver.)



※MN,CNはNTM端末