

Mobile IP

移動ノードからのインターネットアクセス

発表者

00J011 伊藤将志

Mobile IPの必要性

ノードが外部リンクに移動するためには・・・

解決すべき問題

特定のアドレス宛のパケットはそのネットワークプリフィクスへ到達可能なルータに転送されるので、存在すべきリンク上にノードが存在しなければパケットは配送できない

現在のインターネットの経路制御で考えられる3つの方法

- ホスト特定経路で解決
- 移動するごとにIPアドレスを変える
- リンク層で解決

Mobile IPの必要性

• ホスト特定経路で解決

- ・多くのホスト特定経路に変更が必要
- ・セキュリティに問題あり

• IPアドレスを変える方法

- ・コネクションまで新規で行わなければならない
- ・DNSサーバの問い合わせ、更新が多くなる
- ・セキュリティに問題あり

• リンク層での解決

- ・媒体間の可搬性のみ有効

Mobile IPの概要

- Mobile IPに必要な機器

- 移動ノード

- 通信を維持したまま、あらゆるリンクから別のリンクに接続を変更できるノード

- ホームエージェント

- 移動ノードのホームリンク上にインターフェースをもつルータ

- 外部エージェント

- 移動ノードの外部リンク上にあるルータ

- Mobile IPに必要なアドレス

- ホームアドレス

- 移動ノードに永続的に割り当てられたIPアドレス

- 気付アドレス

- 外部エージェント気付アドレス

- 外部エージェントのIPアドレスの任意の一つを割り当てる

- 共存気付アドレス

- 外部リンク上で外部エージェントを利用できない場合利用する

単純化したMobile IPの動作

1. ホームエージェントや外部エージェントはエージェント広告というメッセージを定期的にマルチキャストまたはブロードキャストする。
2. 移動ノードがエージェント広告を受け、自分がホームリンクにいるか外部リンクにいるか判別する。
3. 外部リンクに接続している移動ノードは気付アドレスを獲得。
4. 気付アドレスをホームエージェントに登録する。
5. ホームエージェントは移動ノードのホームアドレス宛の packets を引き寄せ、気付アドレスに向かってトンネルを張る。
6. 気付アドレスにおいてパケットはトンネルから取り出され、移動ノードに配送される。
7. 移動ノードが送ったパケットはトンネル経由はせず、宛先へ直接配送する。

トンネル経由の転送

送信者: 元々の送信者
宛先: 最終的な宛先



元のIPパケット

送信者: トンネル入り口
宛先: トンネル出口



カプセル化されたIPパケット

(外部ペイロード)

移動ノード



Mobile IPの主要3要素

エージェント探索

登録

外部リンクに接続した移動ノードが
送受信するパケットの経路制御

エージェント探索

エージェント探索における移動ノードの処理

- 現在、ホームリンクか外部リンクのいずれに接続中かの判断
- リンク間を移動したことの検出
- 外部リンク接続時の気付アドレスの取得

探索に使用する2つのメッセージ

- エージェント広告
- エージェント要請

エージェント探索

エージェント探索メッセージ形式

Vers=4	IHL	サービスタイプ	全長	
識別子			フラグ	フラグメントオフセット
Time to Live = 1	プロトコル = ICMP		ヘッダチェックサム	
送信元アドレス = 移動ノードのホームアドレス				
受信先アドレス = 255.255.255.255(ブロードキャスト)または224.0.0.2(マルチキャスト)				
タイプ = 10	コード = 0		チェックサム	
予約				

IP
ヘッダ

ICMP
ルータ要請

エージェント要請メッセージ

エージェント探索

エージェント探索メッセージ形式

Vers=4	IHL	サービスタイプ	全長							
識別子		フラグ	フラグメントオフセット							
Time toLive	プロトコル = ICMP		ヘッダチェックサム							
送信元アドレス = ホーム / 外部エージェントのアドレス										
受信先アドレス = 255.255.255.255 (ブロードキャスト) または 224.0.0.1 (マルチキャスト)										
タイプ = 9	コード		チェックサム							
アドレス総数	アドレスエントリ長		(この通知の)有効時間							
ルータアドレス[1]										
選択レベル[1]										
ルータアドレス[2]										
選択レベル[2]										
...										
タイプ = 16	長さ		シーケンス番号							
(最大)登録有効時間			R	B	H	F	M	G	V	予約
気付アドレス[1]										
気付アドレス[2]										
...										
タイプ = 19	長さ		プリフィックス長[1]			プリフィックス長[2]				
...										

IP
ヘッダ

ICMP
ルータ
広告

移動性
エージェント
広告拡張

プリフィックス長
拡張
(オプション)

エージェント応答メッセージ

• 移動の検出

- 有効時間フィールドの指定時間内に同じ外部エージェントからエージェント広告がなければ移動。
- 外部エージェントから広告を記録しておき、次から広告を受信したときにネットワークプリフィックスを比べて判断する。

登録

移動ノードは接続点が別のリンクに移動したことを検出したら常に登録する。また、登録には有効時間があるので再登録も必要

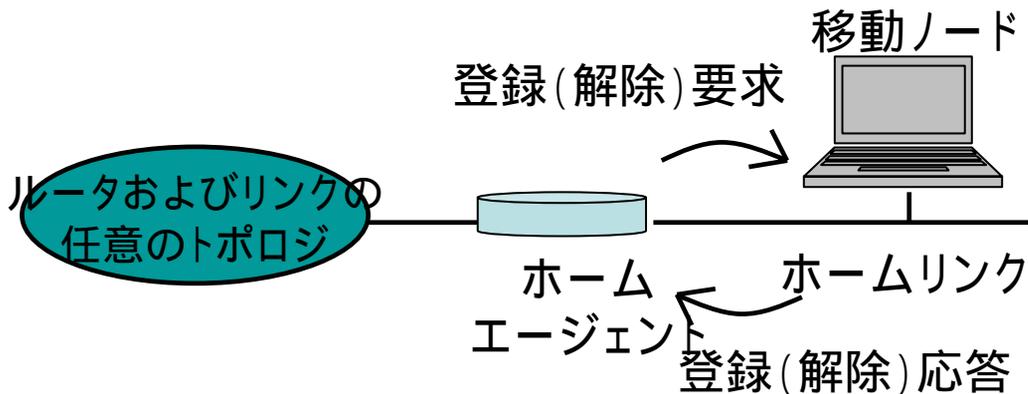
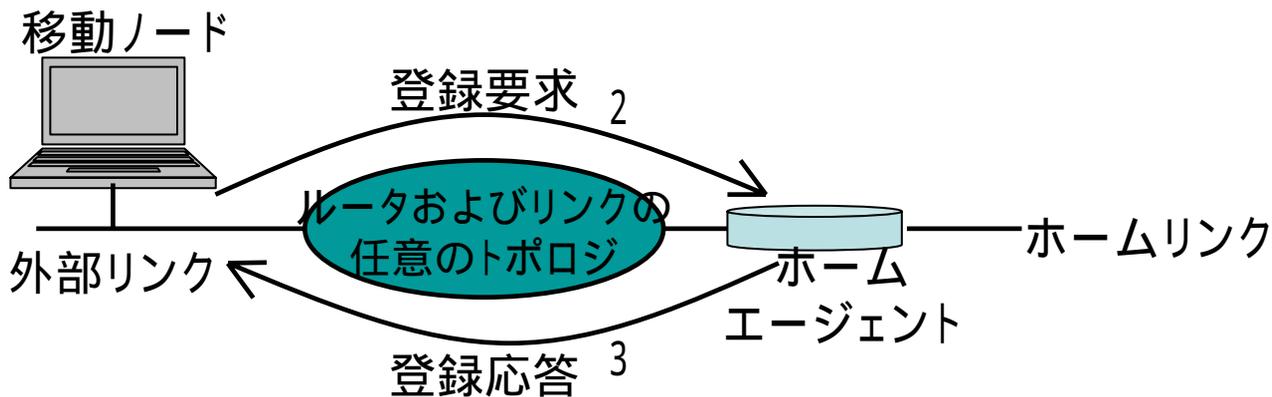
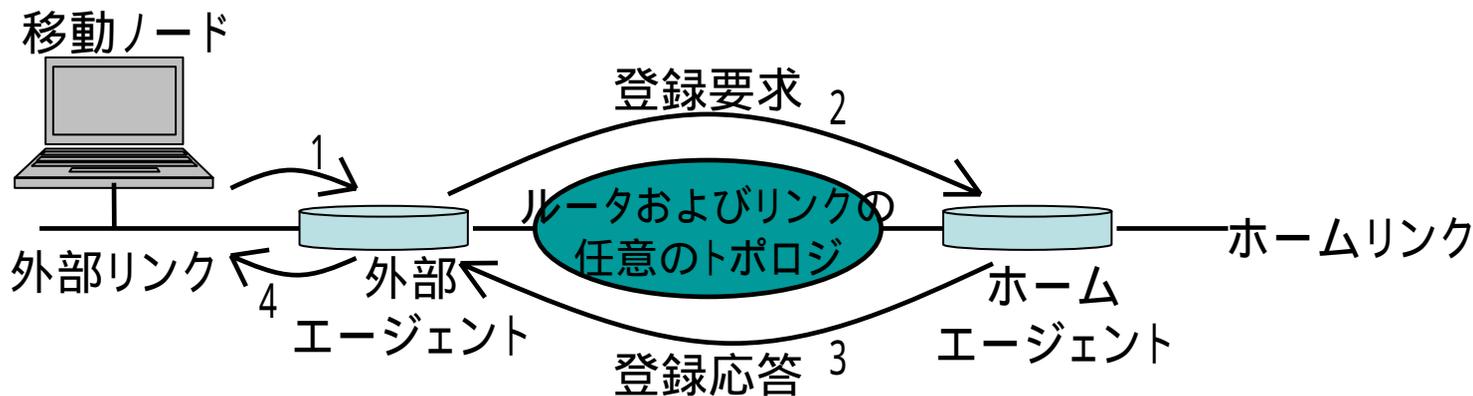
登録とは移動ノードによる以下の処理になる

- ・外部エージェントへ経路制御サービスを要求
- ・ホームエージェントへ気付アドレスを通知
- ・期限切れになりそうな登録を更新
- ・ホームリンクに戻った場合、登録を解除

結合

登録する際にホームエージェントでは気付アドレスと移動ノードのホームアドレスの対応表を作る

登録



Vers=4	IHL	サービスタイプ	全長		
識別子		フラグ	フラグメント		
Time to Live	プロトコル=UDP		ヘッダチェックサム		
送信元アドレス					
受信先アドレス					
送信元ポート			受信先ポート=434		
長さ			チェックサム		
タイプ=1	S	B	D	M	G V rsv
有効時間					
移動ノードのホームアドレス					
ホームエージェントアドレス					
気付アドレス					
識別子					
オプションの拡張...					
タイプ=32	長さ		セキュリティパラメータ...		
インデックス(SPI)					
認証子(デフォルトはKeyed MD5)					
オプション拡張...					

IP
ヘッダ

UDPヘッダ

登録応答の
固定長部

移動ホーム
認証拡張

登録要求メッセージ

タイプ = 3	コード	有効時間
移動ノードのホームアドレス		
ホームエージェントアドレス		
識別子		

登録応答の
固定長部

登録応答メッセージ

登録処理

移動ノードはどのように登録処理するか？

いつ移動ノードは登録すべきか？

- ・リンク間を移動した時
- ・外部エージェントが再起動した時
- ・有効期限が切れた時

送信の仕方

場合によって受信先MACアドレス取得の方法を変える。

- ・外部エージェント気付アドレスで登録する場合
エージェント広告のMACアドレスを記録しておく
- ・共存気付アドレスで登録する場合
気付アドレスを使ってARPを流して取得
- ・ホームリンクで登録を解除する場合
ホームアドレスを使ってARPを流して取得

外部エージェントの登録要求処理

登録要求を受信すると一連の有効性検査をして失敗するとコードフィールドに拒否理由の番号をつけ返信する。

拒否理由

- ・移動ノードが外部エージェントで認識できない
- ・有効時間が長い
- ・サポートしていないトンネル形式
- ・資源を提供する余裕がない

これらの条件を満たしたとき外部エージェントはホームエージェントの中継する。このとき後のため特定の情報を記録しておく。

記録するもの

- ・リンク層送信元アドレス
- ・IPアドレス
- ・UDP送信ポート
- ・ホームエージェントアドレスフィールド
- ・識別子フィールド
- ・要求中の有効フィールド

ホームページエージェントの登録処理要求

受信すると外部エージェントと同様の有効性検査をする、無効なら拒否理由を示すコードを移動ノードの送信し、条件を満たすなら、結合エントリを書き換える。

結合エントリとは

移動ノードのホームアドレスと現在の気付アドレスを対応させた表の各エントリ

最後に登録が成功したことを伝える登録応答を送信する。

登録要求フィールド			結果
気付アドレス	有効時間	Sビット	
ホームアドレスと異なるアドレス	> 0	0	移動ノードの既存の全結合を指定された新規の気付アドレスに置き換える
ホームアドレスと異なるアドレス	> 0	1	指定された気付アドレスのための結合を作成し、移動ノードのための既存の結合はすべて変更せずにおく
ホームアドレスと異なるアドレス	0	1	指定された気付アドレスのための移動ノード結合を削除し、既存の結合はすべて変更せずにおく
移動のーどのホームアドレス	0	任意の値	移動ノードのすべての結合を削除する
移動ノードのホームアドレス	> 0	任意の値	移動ノードは破損しているため、その移動ノードの製造元を呼ぶ

外部エージェントの登録応答処理

ホームエージェントからの登録応答の一連の有効性を検査し、無効ならコードフィールドに理由を示した登録応答を作成し、移動ノードに送信する。

拒否理由

- ・形式が不正
- ・未知の拡張を含む
- ・外部エージェントとホームエージェント間の認証に失敗

登録応答が有効なら自分のリンクを訪れている移動ノードのリストを更新し、登録応答を移動ノードに中継する。

ここでついにトンネルの入り口と出口が完成する

移動ノードの登録応答処理

登録応答を受信すると一連の有効検査を行う。有効であるなら登録がホームエージェント、外部エージェントに受け入れられたか調べる

拒否理由

- ・有効時間が許可される値より大きい
- ・識別子フィールドが不正

登録拒否された場合

拒否された理由を正して登録要求の再送を試みる

登録受諾された場合

現在のリンクに合うように経路表を訂正し、通信を始め、登録要求の再送を止める

登録

移動ノードがホームエージェントのアドレスを知る方法

- 一般

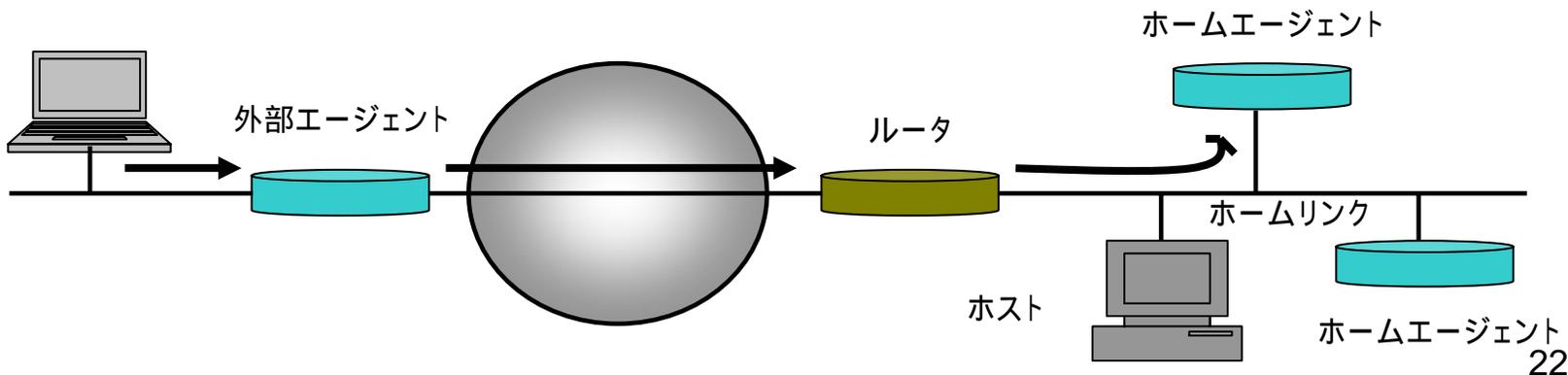
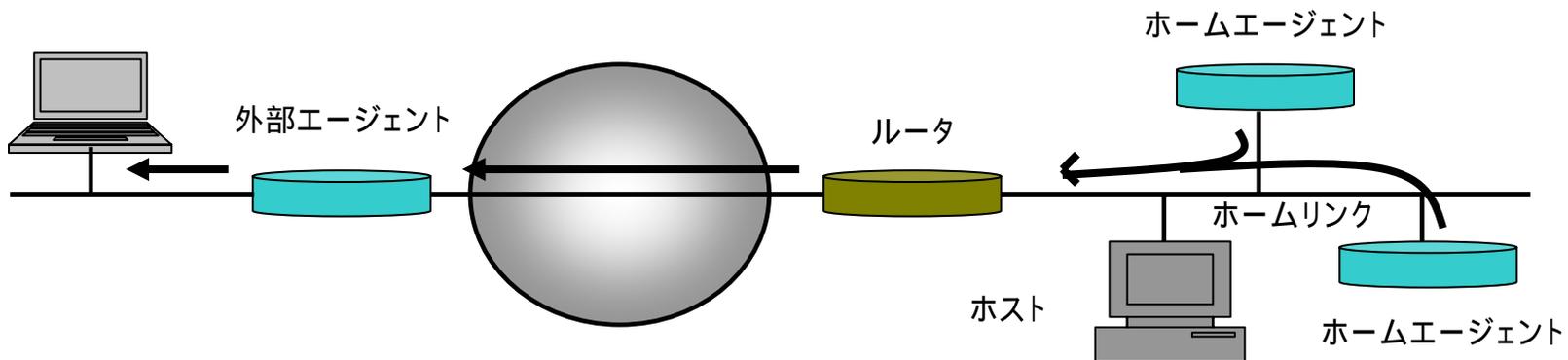
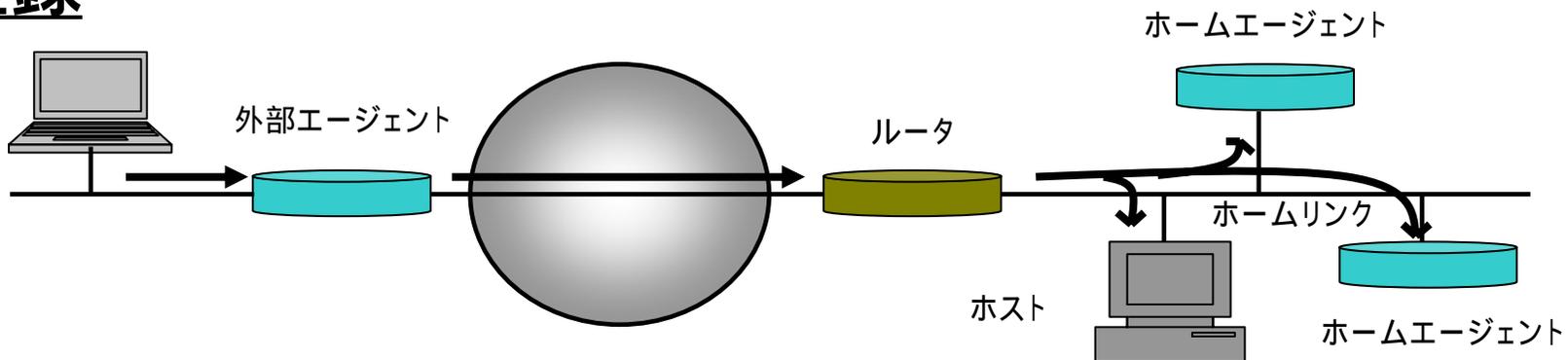
移動ノードにホームアドレスと同時にホームエージェントアドレスやホームアドレスのネットワークプレフィクス、DNSサーバアドレスなどを設定する

- 動的

登録の過程で動的にホームエージェントアドレスを発見する

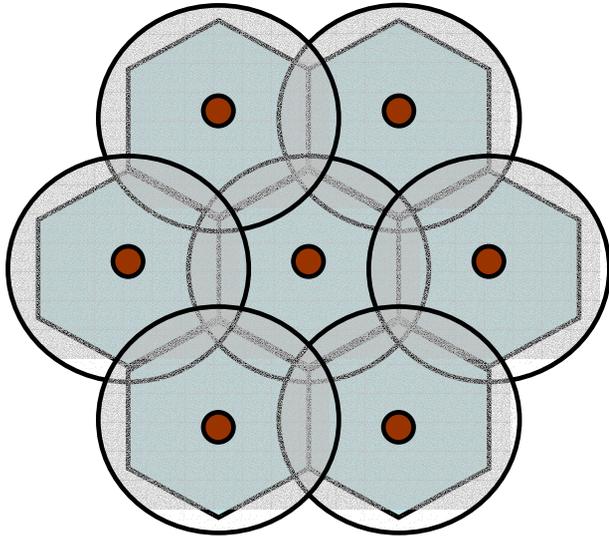
1. 移動ノードは登録要求のホームエージェントアドレスフィールドにホームリンク向けのブロードキャストアドレスを書き込む。
2. 外部エージェント利用の登録の場合、外部エージェントは登録要求を指定のブロードキャストアドレスに中継。外部エージェントなしの登録の場合は、登録要求パケットのIP受信アドレスをホームリンクのブロードキャストアドレスとする。
3. ホームリンク上の全ホームエージェントが登録要求を受信するが、その中でサービスを提供できるものは一度拒否し、ホームエージェントのユニキャストアドレスを含む登録応答を返信する。
4. 移動ノードは、これらの登録応答を集め、ユニキャストアドレスを知り、再度登録要求をする。

登録



登録

移動ノードが無線セルをあちこち頻繁に移った場合



セルの形は時間によって変化してしまうのでノードが動かないとしても頻繁にリンク間を移動し登録を行わなければならない

2つの解決法

・リンク層

ブリッジでセルを大きなリンクに統合

・同時結合

Mobile IPの同時結合、複数の気付アドレスを登録

移動ノードが送受信する パケットの経路制御

2つの場合

移動ノードがホームにいる場合

移動ノードが外部リンク上にいる場合

移動ノードがホームにいる場合

固定のノードと同じで、受信する場合、送信する場合共に特別な経路制御規則はない。

移動ノードがホームでの経路情報を保存しておく実装もあり、ホームに戻ったとき素早く経路情報を復元できる。

パケット経路制御

移動ノードが外部リンク上にいる場合

- 経路制御の要約 -

1. ホームエージェントは移動ノードのホームアドレスと同じネットワークプリフィクスへの到達性を広告
2. 移動ノードへのパケットはホームエージェントへ経路制御される
3. ホームエージェントは移動ノードへのパケットを捕捉し、気付アドレスにトンネル経由で転送
4. 気付アドレスでは元のパケットをトンネルから取り出し、移動ノードへ転送

外部エージェント
気付アドレスを
持つ移動ノード

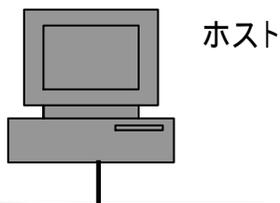
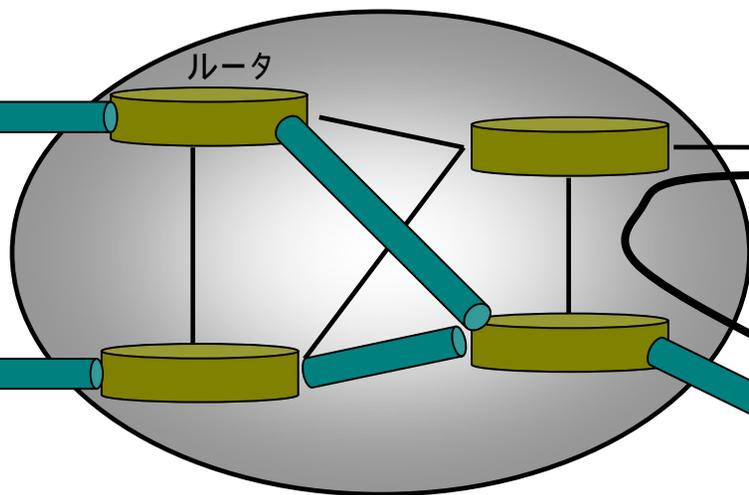


外部エージェント



共存気付アドレスを
持つ移動ノード

ルータ



ホスト

元の packets

ホームエージェント

ホームエージェントがパケットを捕捉する方法

移動ノードの到達性を広告

ホームリンクに接続していないインタフェースからホームエージェントに到達するのでIP経路の中で自然と捕捉する。

不要ARPと代理ARP

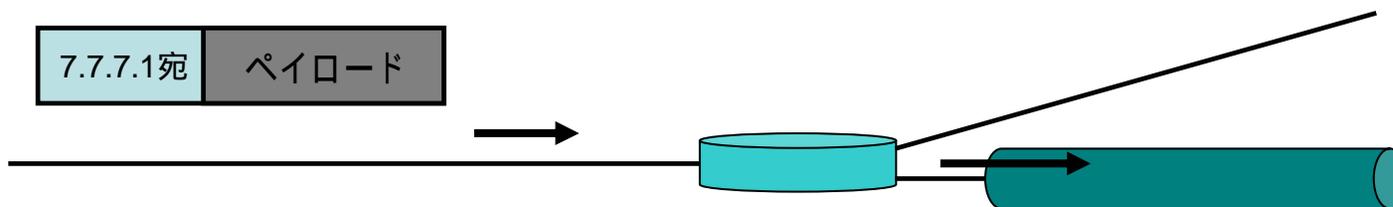
ホームリンクに接続されたホストから移動ノードに送信するとき、ARP要求をブロードキャストするが移動ノードは外部リンクにいるのでホームエージェントが代わりにMACアドレスを応答する。

最近ホームリンクに移動ノードが存在した時はキャッシュに移動ノードのMACアドレスが他のノードに残っている場合が多いので、ホームエージェントが移動ノードの結合を持たない場合、不要ARPを送信してキャッシュを書き換える。

移動ノードがホームリンクに戻ってきた時は移動ノードが不要ARPを送信しキャッシュを更新する。

仮想インターフェースによる経路情報の統合

トンネルを経路情報に統合するトリックとして仮想インターフェースがある。仮想インターフェースは状況に応じて、トンネル経由の転送のためのカプセル化およびカプセル開放を処理する。



IP経路制御ソフトウェア

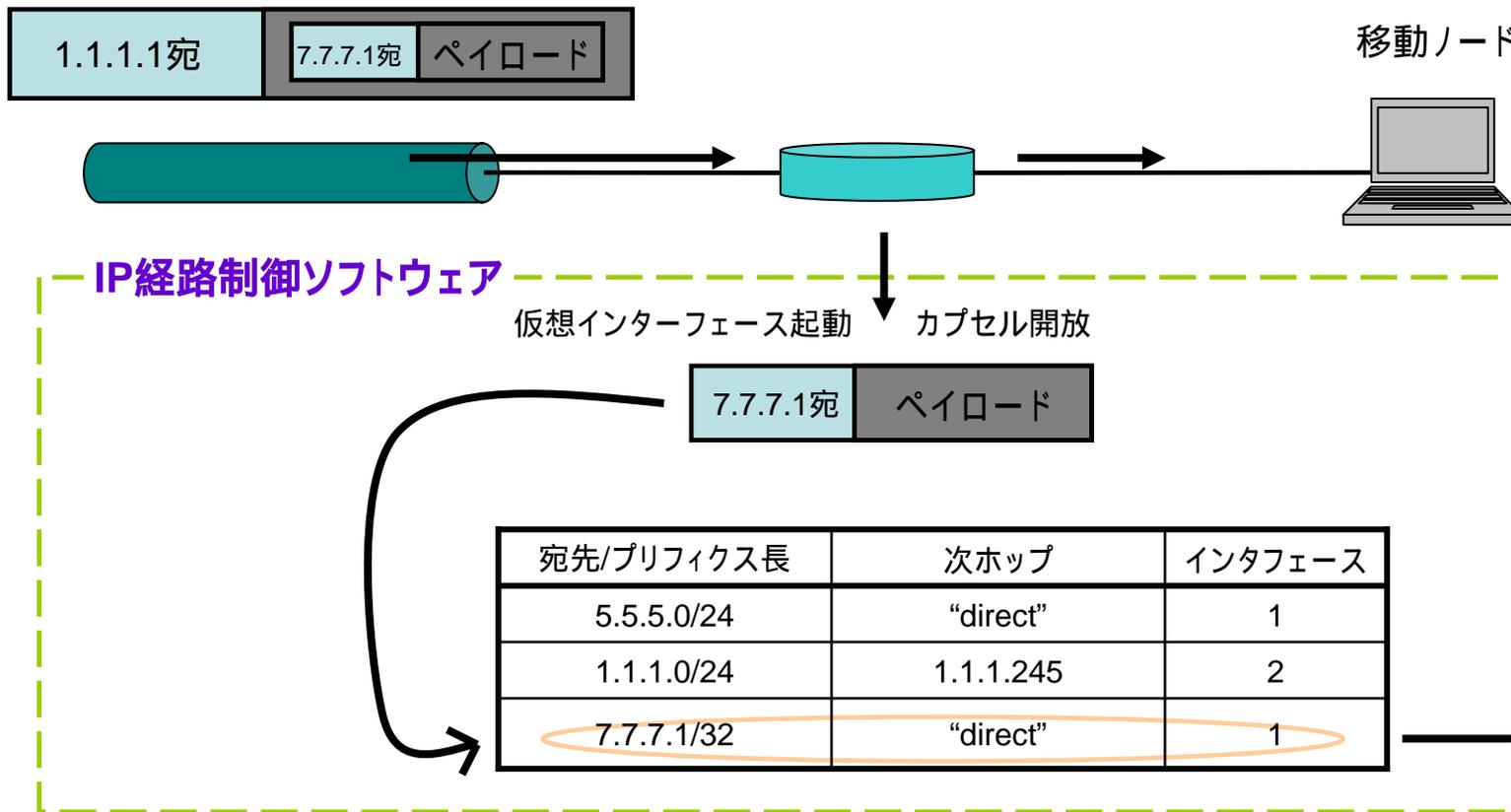
もう一度経路を選択する

宛先/プリフィクス長	次ホップ	インターフェース
7.7.7.0/24	"direct"	1
デフォルト/0	6.6.6.245	2
7.7.7.1/32	1.1.1.1	1

IPパケットをカプセル化

仮想インターフェース起動





IP経路制御ソフトウェアはコードフィールドを読みIP-in-IPカプセル化と判断し、仮想インターフェースのソフトウェアにパケットを渡す。

移動ノードのパケット送信法

ホームリンク上

固定ノードと同じ

外部リンク上

・外部エージェント経由の登録

ルータ選択のための2つの方法

1. エージェント広告で取得する外部エージェント自身
2. ICMPルータ広告に記載されているルータ

・外部エージェントなしで登録

ルータ選択のための2つの方法

1. ICMPルータ広告からのルータアドレス入手
2. DHCP, PPP, IPCPなどから入手

パケット経路制御

ブロードキャスト・マルチキャストは可能か？

ブロードキャスト

受信について

登録要求のBビットを恩にしておく

- ・共存気付アドレスで受信 Dビットオン
ユニキャストで受信する場合と同じ方法
- ・外部気付アドレスで受信 Dビット0

ホームエージェントがそのまま移動ノードへ送信するとカプセル開放したときに受信先がブロードキャストになってしまう。

2重にカプセル化する(ネストカプセル化)

1. ブロードキャストをカプセル化

送信元: ホームエージェント

受信先: 移動ノード

2. もう1度カプセル化

送信元: ホームエージェント

受信先: 気付アドレス

送信について

1. 外部リンクに向けてリンク特定ブロードキャスト
移動ノードは単にパケットをリンク層ブロードキャストアドレスで送信する。
2. ホームリンクに向けてリンク特定ブロードキャスト
移動ノードはパケットをトンネル経由でホームエージェントへ転送する。このとき
送信元: 移動ノードのホームアドレス
受信先: ホームエージェント
となる
3. プリフィクス特定ブロードキャストの場合
2と同じ方法

マルチキャスト

受信について

マルチキャストパケットはIP送信元アドレスのネットワークブリフィクスと、IPマルチキャストの送信元リンクのネットワークブリフィクスが同じでなければならない。

外部リンクでマルチキャストを送信

- ・ホームエージェントへトンネル経由で送信
- ・気付アドレスを使用する

外部リンクでマルチキャストを受信する

- ・ICMPパケットをホームエージェント(マルチキャストルータ)にトンネル経由で転送
- ・外部リンクに直接IGMPパケット送信

おわり