本資料について

- 本資料は下記の論文をもとに作成しました
- 文章内容の正確さは保障できないため，
  正確な知識を求める方は原文を参照してください

- 発表日：2003年8月
- 論文名：エンドツーエンド型IPソフトハンドオーバ
- 著者：松岡　保静　吉村　健　大矢　智之
- 出展：電子情報通信学会論文誌　B　Vol. J86-B No.8

著者の所属

NTTドコモ　マルチメディア研究所

エンドツーエンド型
IPソフトハンドオーバ

- End-to-End IP Soft Handover

名城大学 理工学部 情報科学科 渡邊研究室

山崎浩司

題名に？

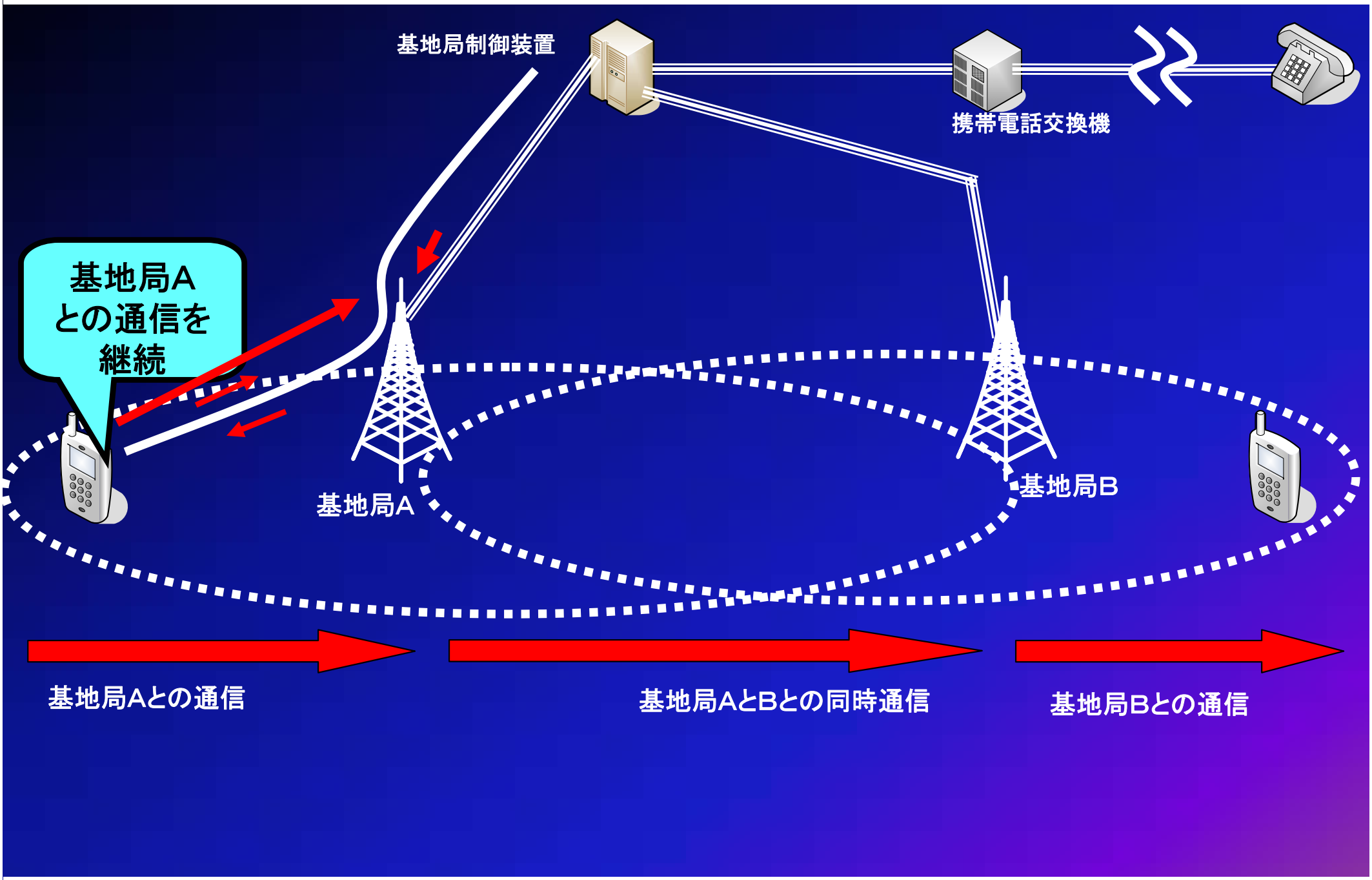
IPソフトハンドオーバ　－　IP

＝ ソフトハンドオーバ

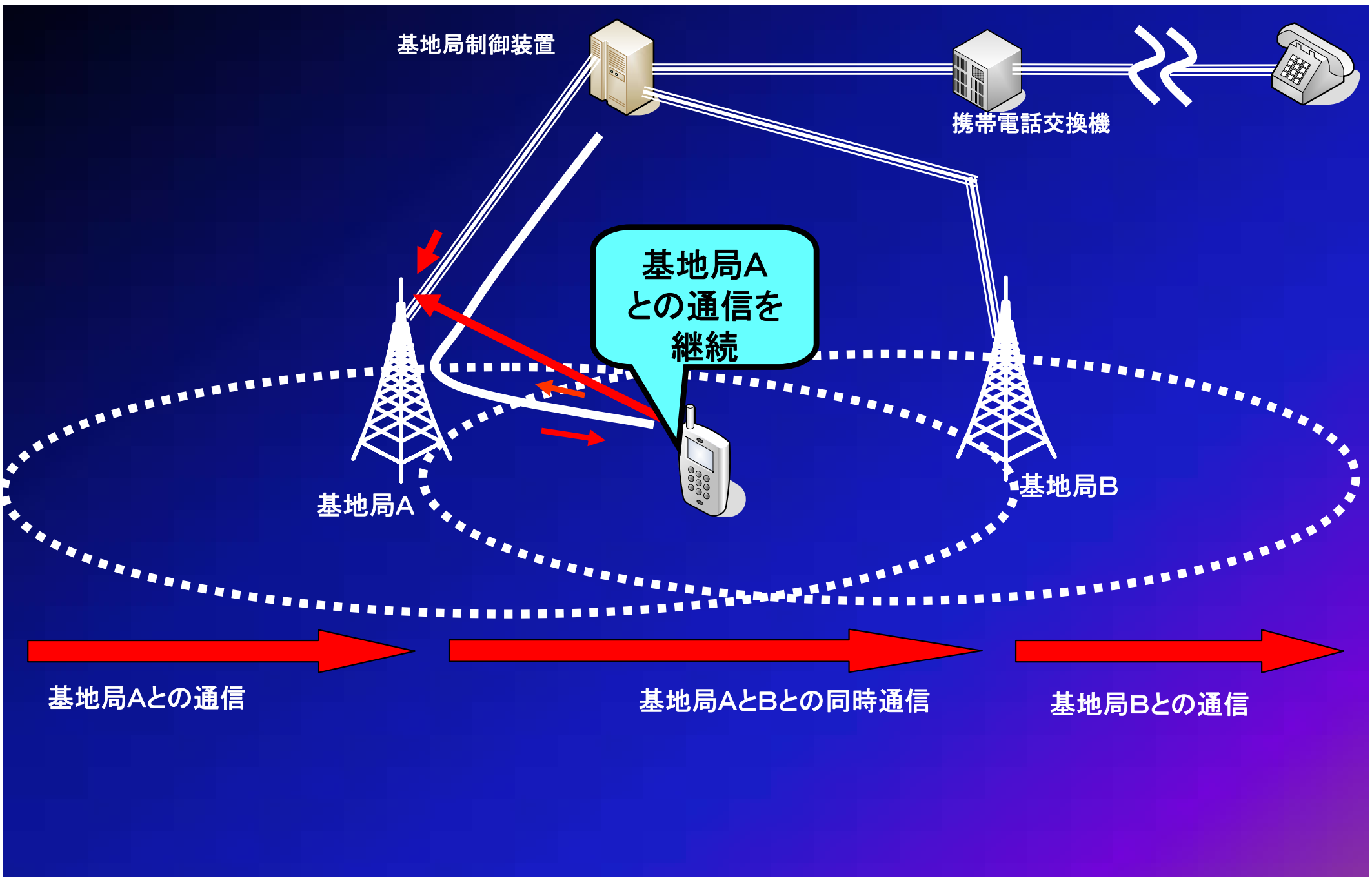
ソフトハンドオーバとは

- 携帯電話の技術
- 複数の基地局からの電波を同時に利用する
- ハンドオーバ時にいったん両方の基地局と接続し完全に受け渡してから元回線を切る事により通信の切断を防ぐ
- とぎれそのものが起こりにくい

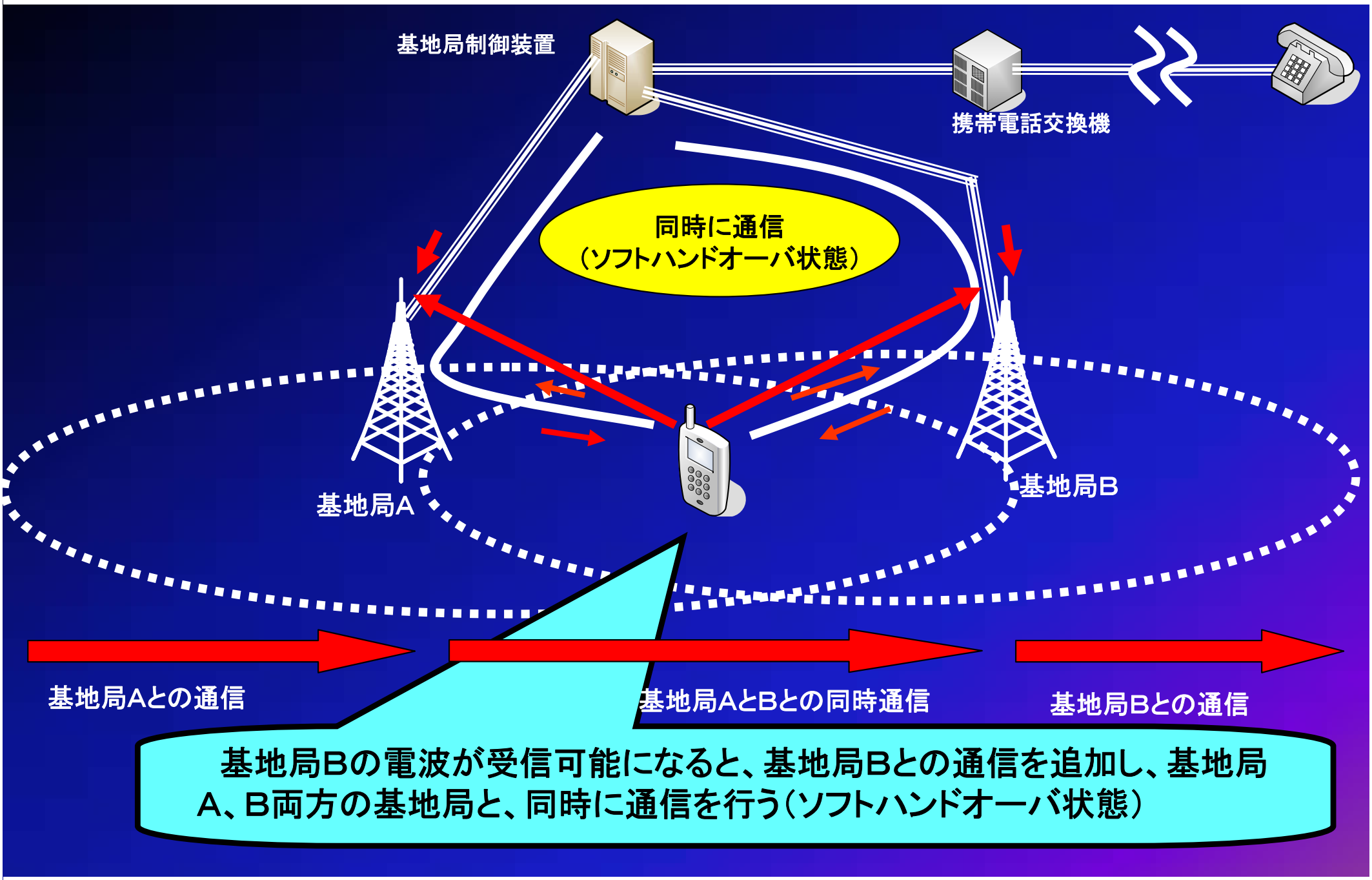
ソフトハンドオーバとは



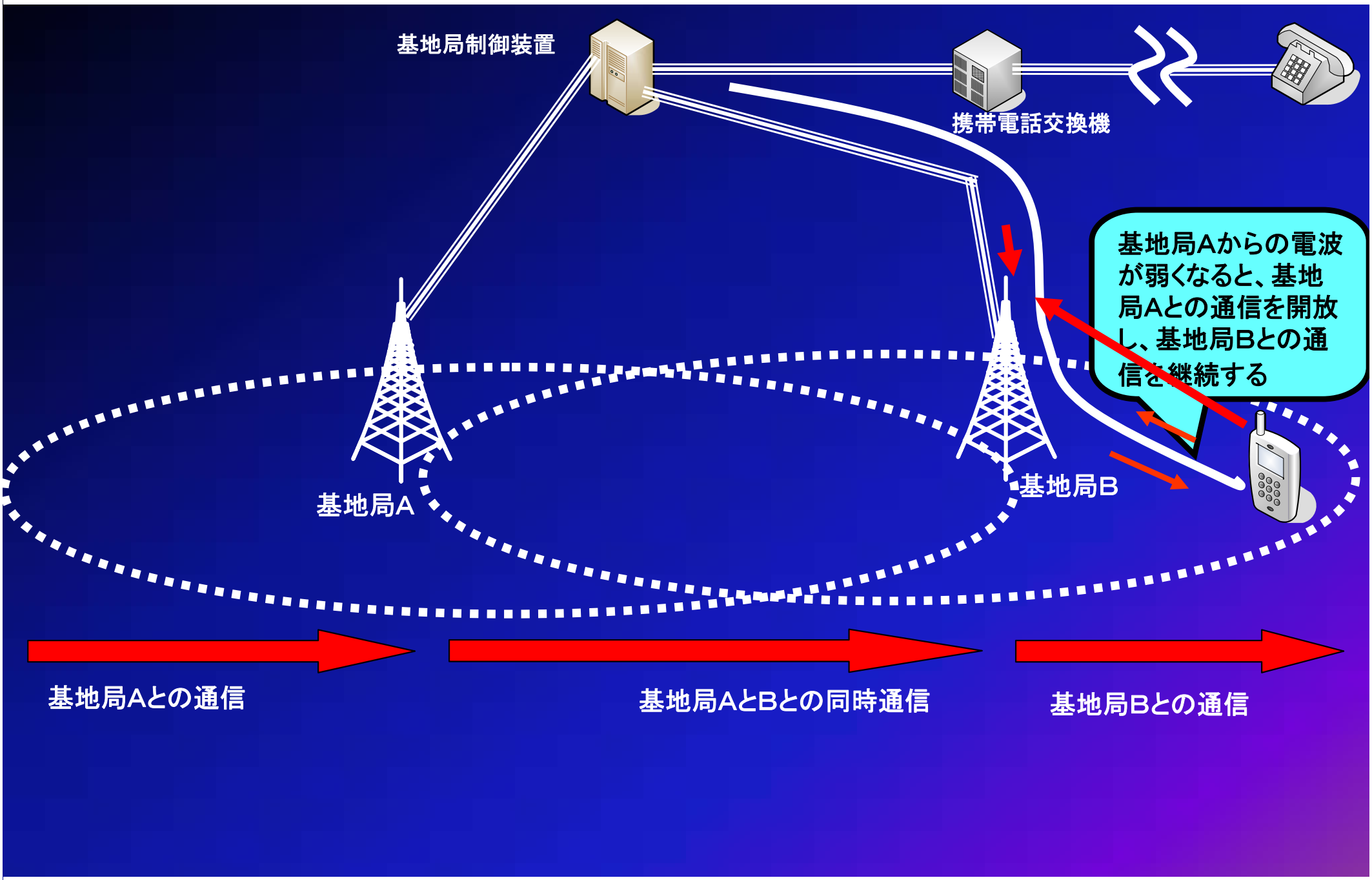
ソフトハンドオーバとは



ソフトハンドオーバとは



ソフトハンドオーバとは



IPソフトハンドオーバとは

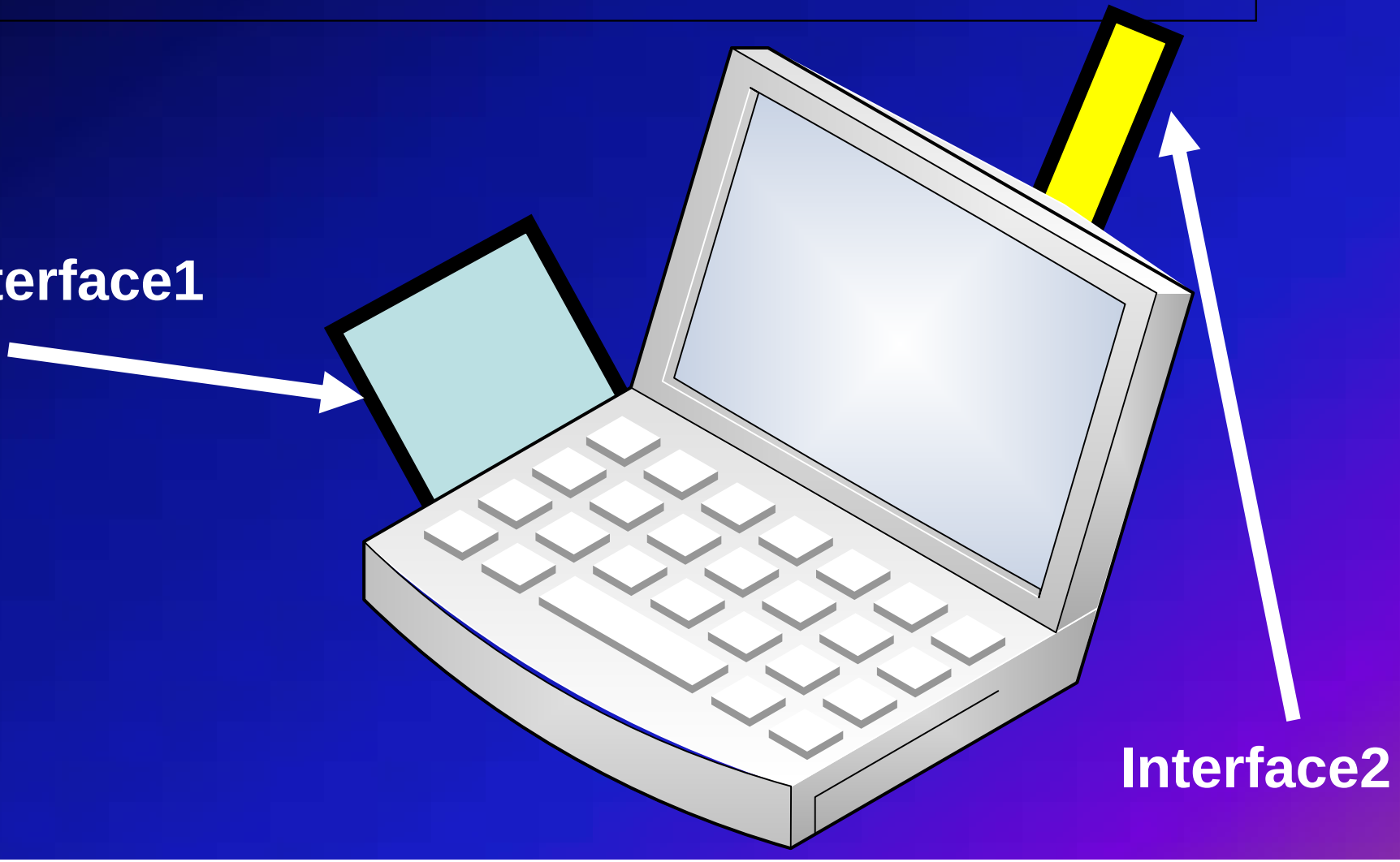
- 一時的に複数の経路にIPパケットを送信し、通信が途切れることなくハンドオーバを実現できる技術のこと

- 携帯電話と違うこと
  →通信のためにインタフェースはIPアドレスを持つ

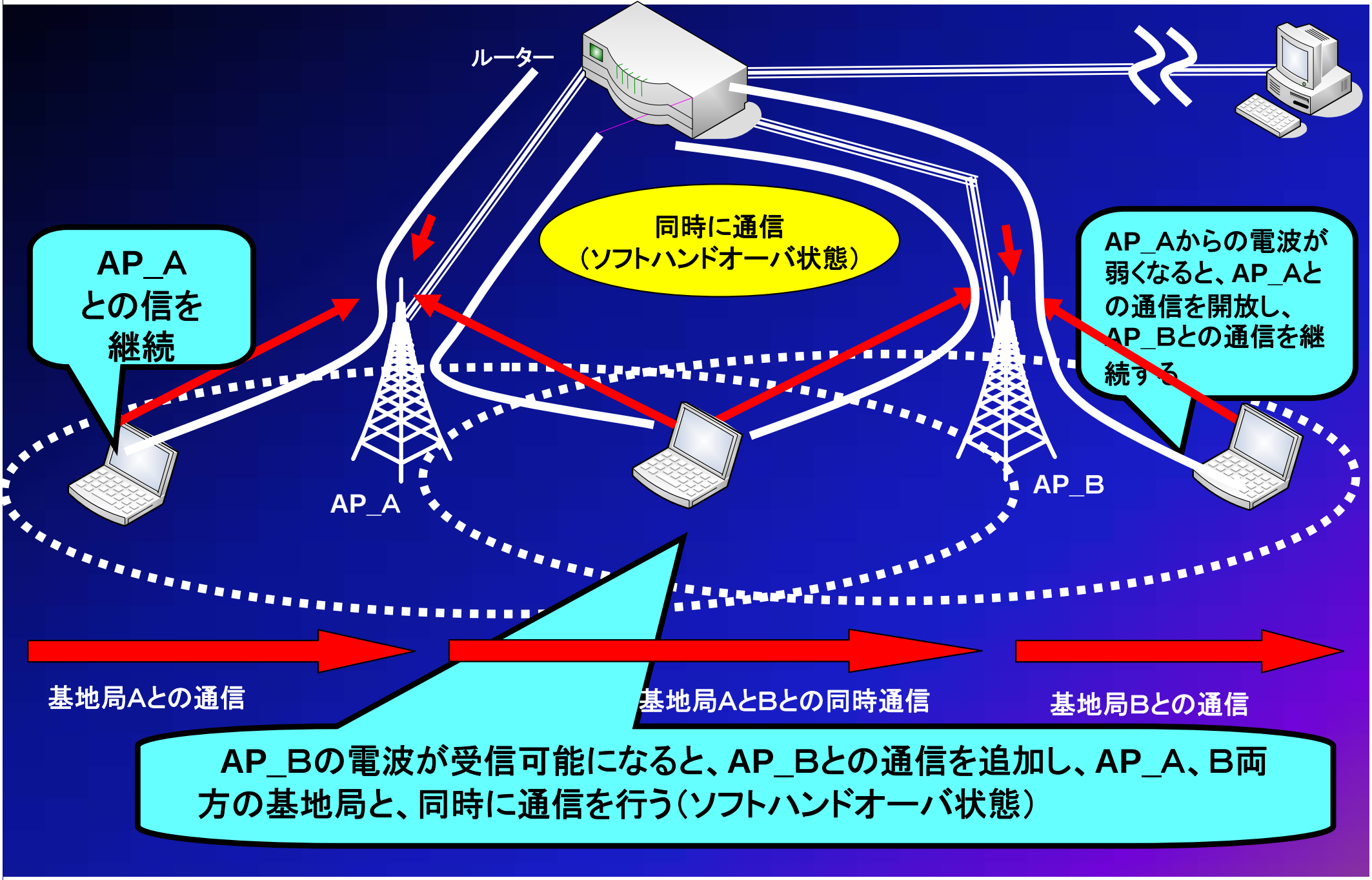
使用される端末

インタフェースを二つ搭載

それぞれのインタフェスにIPアドレスが割り当てられる



IPソフトハンドオーバとは



今回の発表

1.まえがき
2.関連研究
3.MMSP(Mobile Multimedia Streaming Protocol)の提案
4.MMSPの設計と実装
5.性能評価
6.むすび

・MMSPの肝となる部分の輪講を行う
・今回の発表で興味を持たれた方、疑問、質問、
資料の請求は山崎まで

初めに

- 現状のモバイルインターネットサービス
  - →電子メール
  - →Webコンテンツの伝送
- 今後期待されるサービス
  - →音声やビデオを伝送するMultimedia Streaming
  - →VoIP

初めに

リアルタイムアプリケーション実現への課題

- モバイル端末の通信中の移動
  →一時的に通信が途切れる

- 無線リンクでの干渉やノイズによるビットエラー
  →パケットロスの要因

提案方式

- MMSP(Mobile Multimedia Streaming Protocol)
- ハンドオーバの処理をトランスポート層のプロトコルをMMSPが行う
- UDPにMultihoming, FEC-Bicastingの機能を拡張したプロトコル

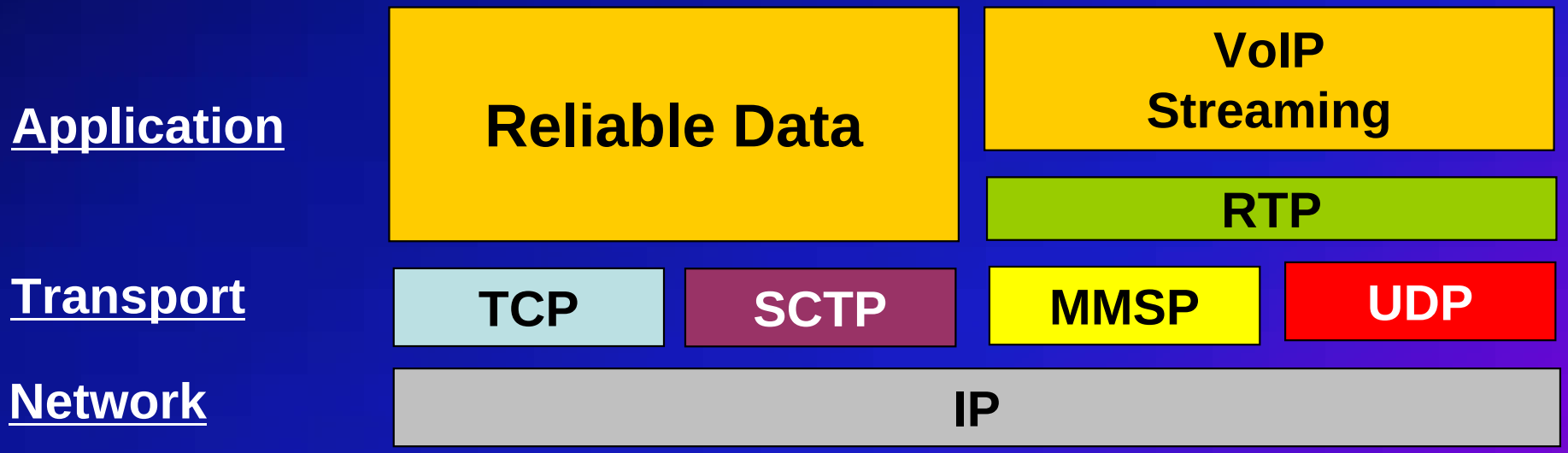
MMSPのプロトコルスタック

- A new transport layer protocol
  - →Multihoming
  - →Bicasting
  - →FEC (Forward Error Correction)

- Protocol Stack

RTP
Real time Protocol

SCTP
Streaming Control
Transmission Protocol
導入OS
BSD, Linux kernel
2.4/2.6, Solaris



MMSPの設計方針

- 既存のIPv4ネットワークや、今後普及するIPv6ネットワークに変更を必要とせず、端末の機能の拡張のみで実現可能

- 対象アプリケーション
  - →リアルタイム伝送を特徴とするアプリケーション
    - →VoIP
    - →Streaming

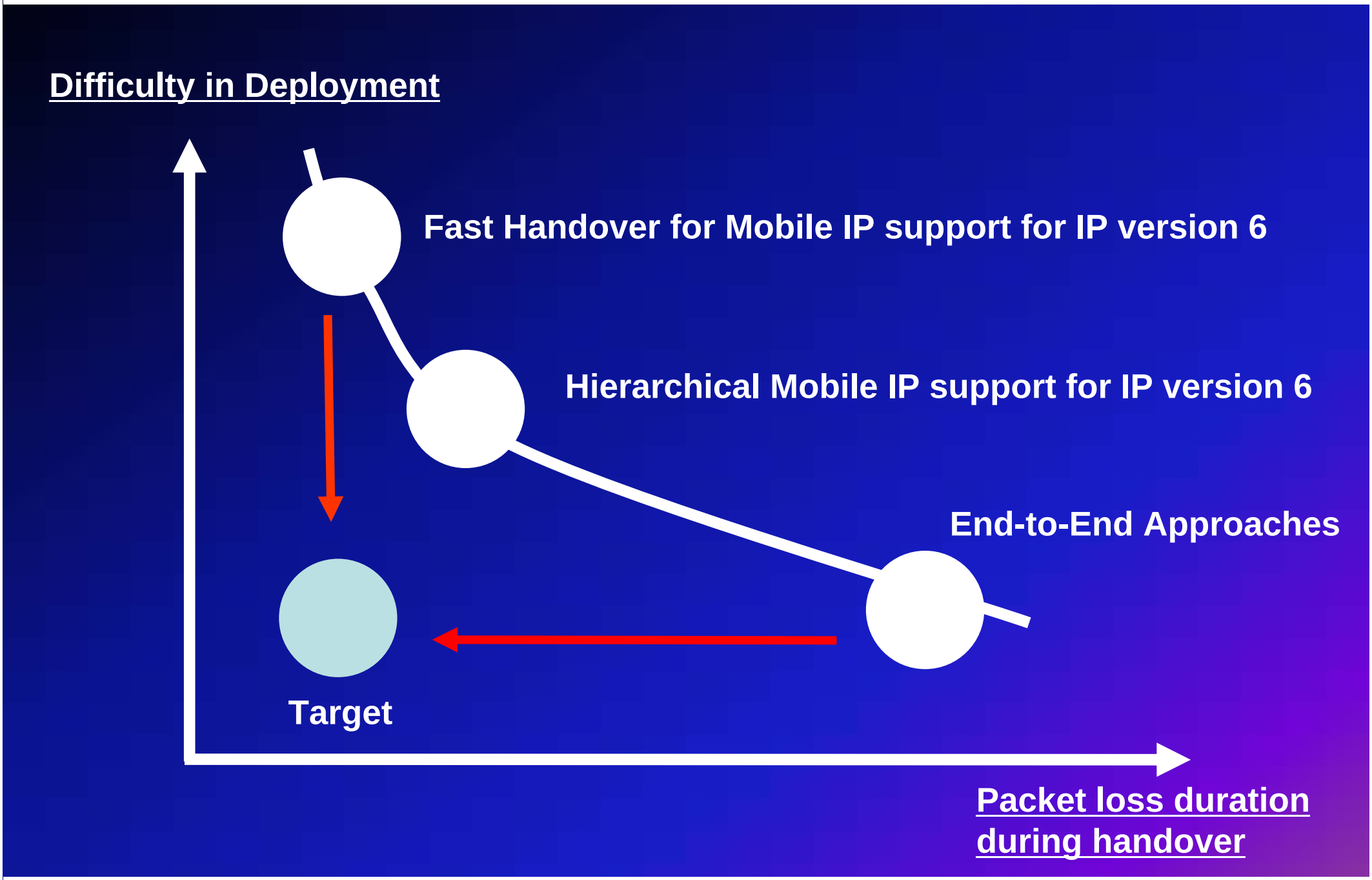
IPソフトハンドオーバ実現の為に必要な条件

- 機能仕様の為には、全ての端末はMMSPを実装する必要がある
- 移動のためのアドレスの変更
- セキュリティのため通信相手と鍵交換

関連研究

- Mobile IP
- 階層型Mobile IP
- Fast Handover
- トランスポート層でのアプローチ

既存方式のトレードオフ関係

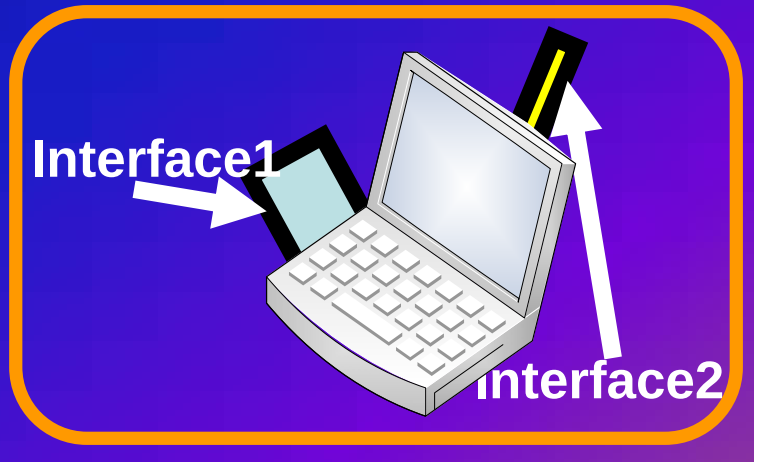


MMSP実現のために

- Multihoming
- FEC-Bicasting
- MMSPコネクションのセキュリティ

使用される端末

- それぞれのインタフェースにIPアドレスが割り当てられる
- DHCPやRA (Router Advertisement) によって
  別々のネットワークアドレスを割り当てられる
- パケットを送信する場合は、送信パケットの送信元ネットワーク
  アドレスと、宛先ネットワークアドレスを選択する必要がある
- TCPはコネクション設立時に
  この選択を行う



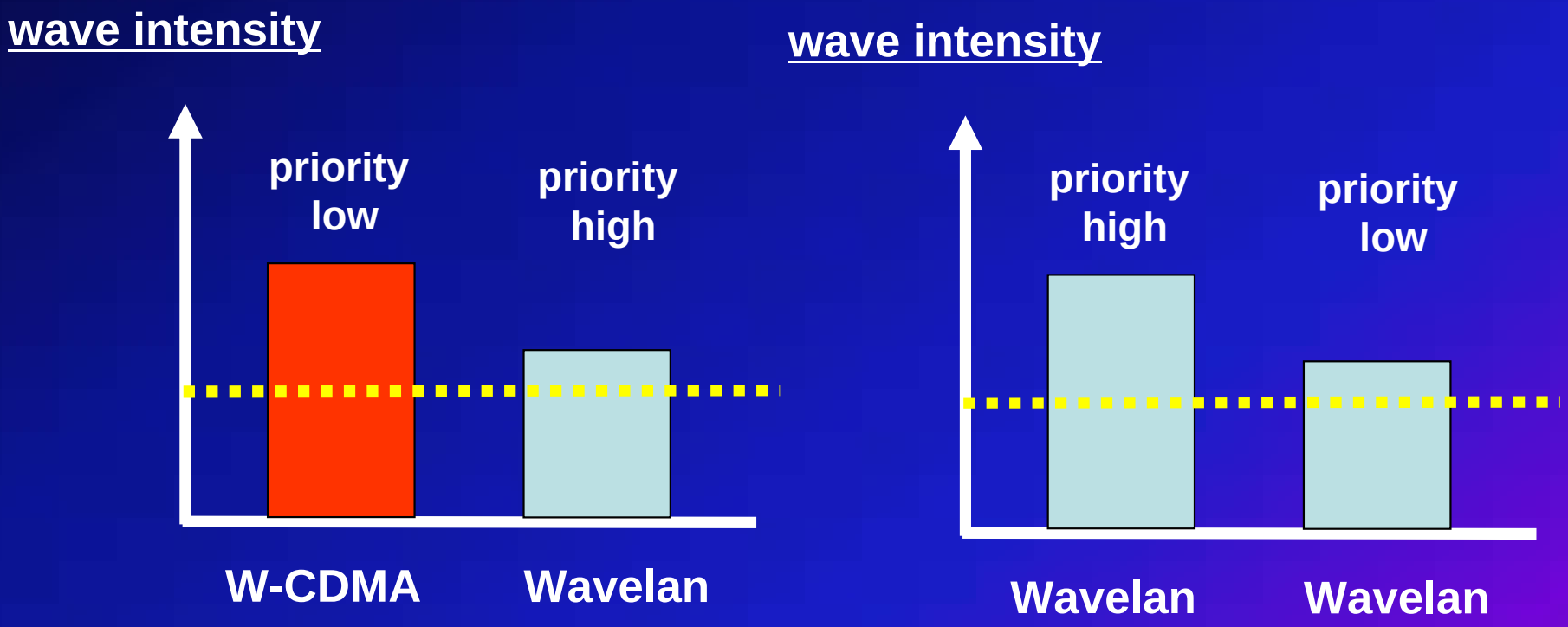
Multihoming

- 複数の通信インタフェースを利用して通信する技術
- MMSPでは、それぞれのインタフェースが、
  ネットワークアドレスに優先レベルを設定する
- 優先レベルは無線リンクの状態に応じて動的に変更
- 送信端末は複数の宛先ネットワークアドレスの中から
  最も高い優先度を持つネットワークアドレスに対して
  パケットを送信する

Multihoming

Address Priority

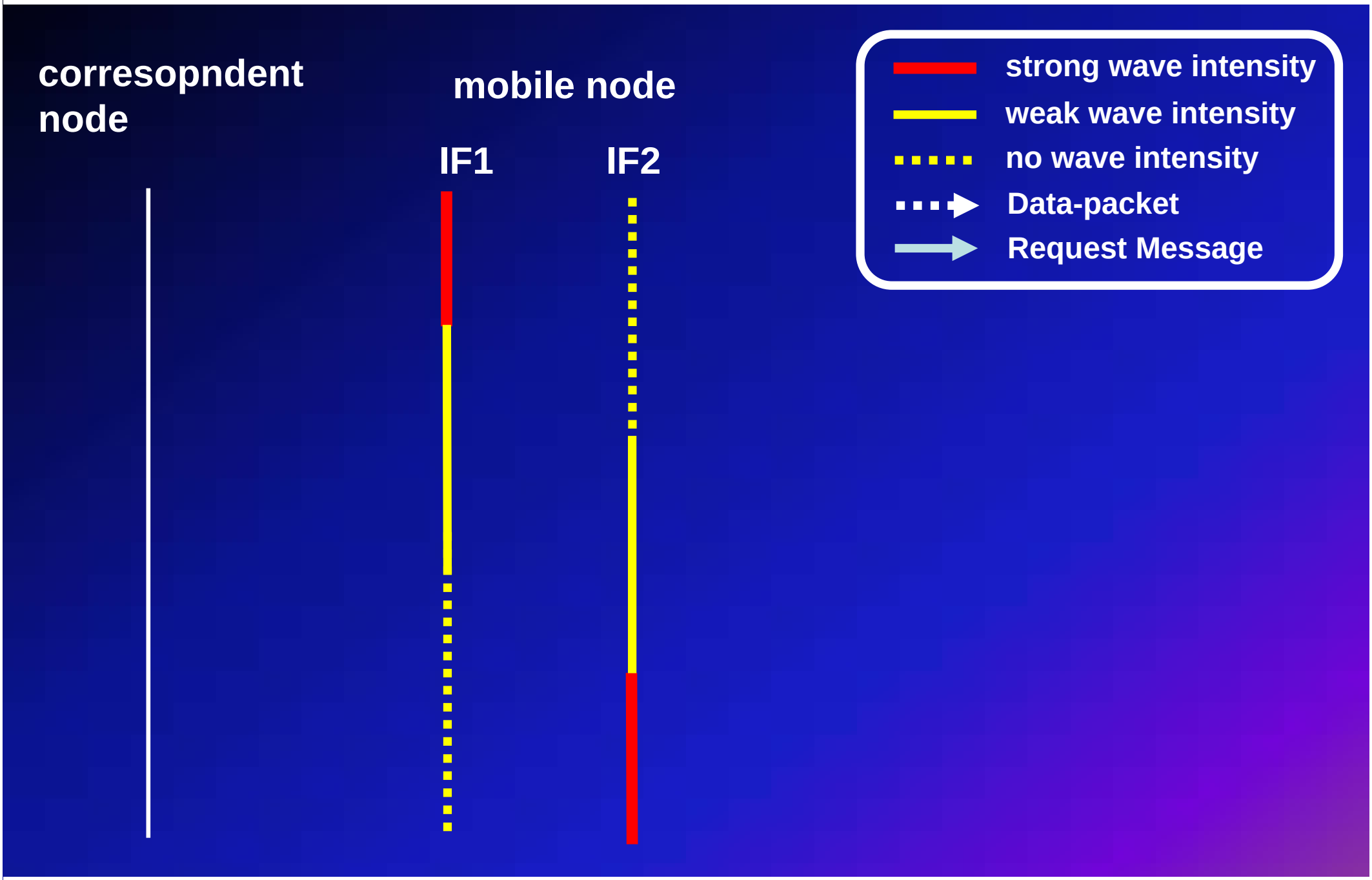
- Dynamically change base on layer 2 information



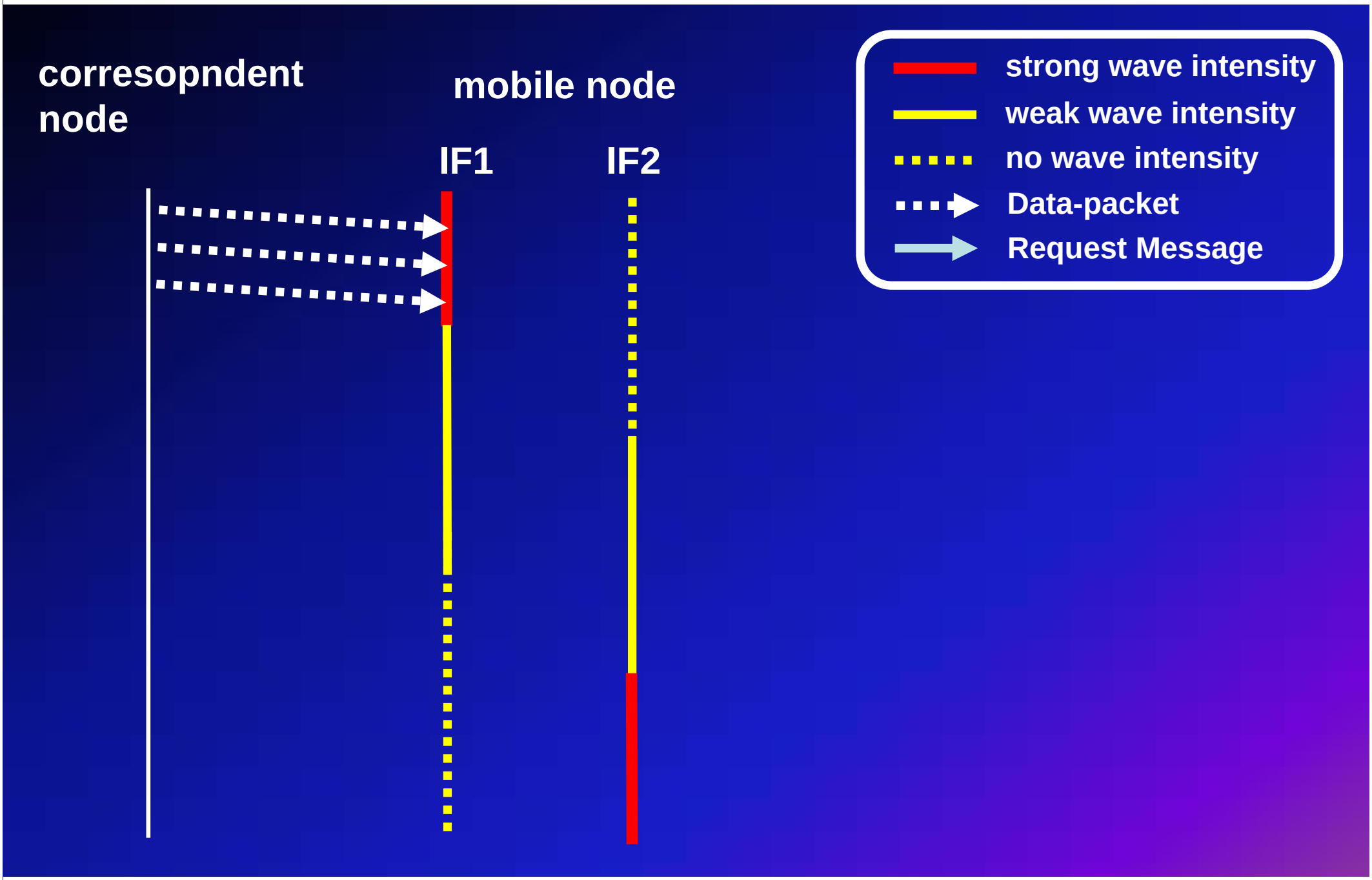
Bicasting

・同じ位の電波強度の無線LANアクセスポイントが二つ存在する場合に、データをコピーした上で、二つのアクセスポイントから同じパケットを流すこと

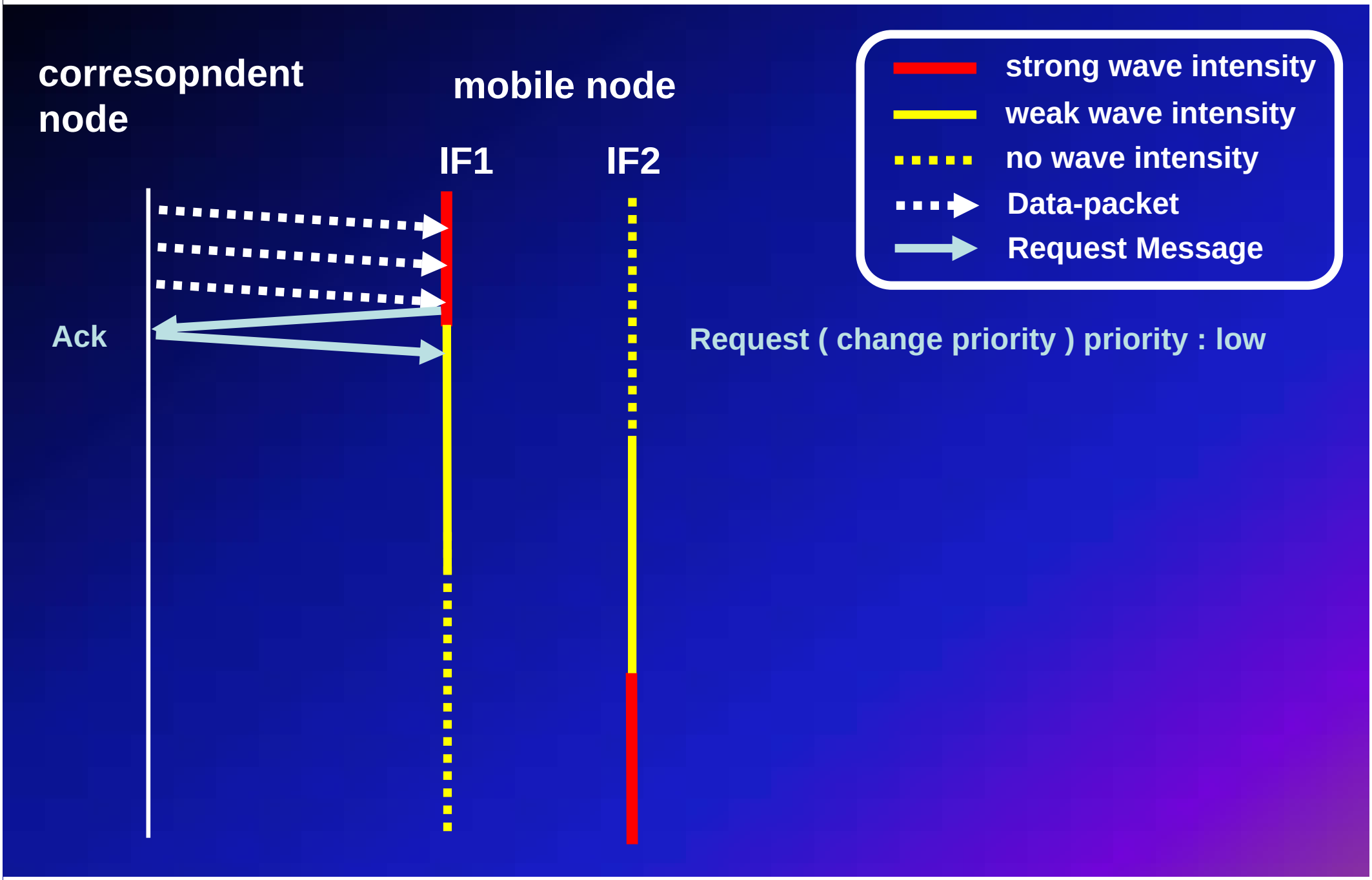
Bicasting


corresopndent node
mobile node
IF1
IF2
strong wave intensity
weak wave intensity
no wave intensity
Data-packet
Request Message

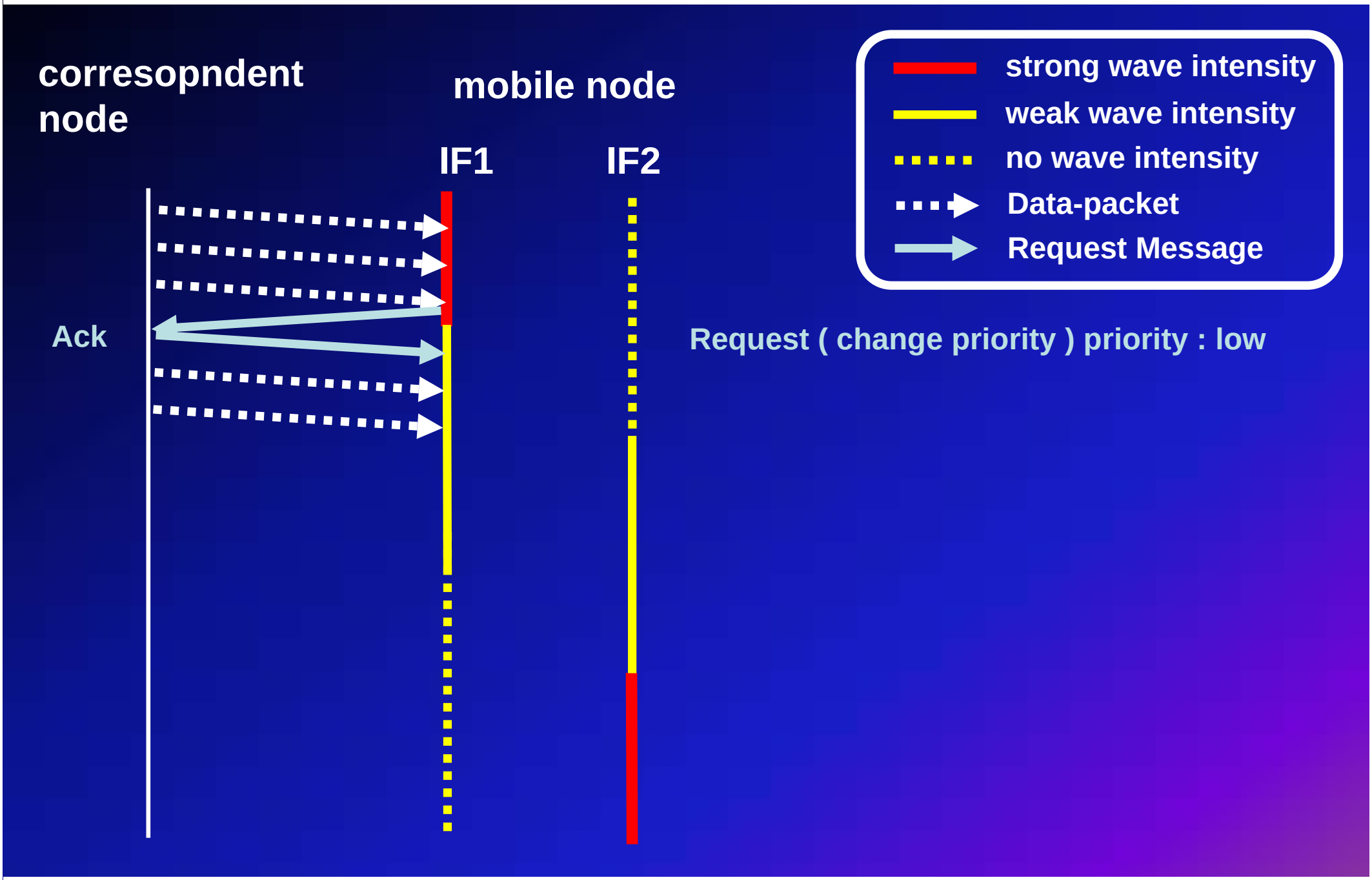
Bicasting


corresopndent node
mobile node
IF1
IF2
strong wave intensity
weak wave intensity
no wave intensity
Data-packet
Request Message

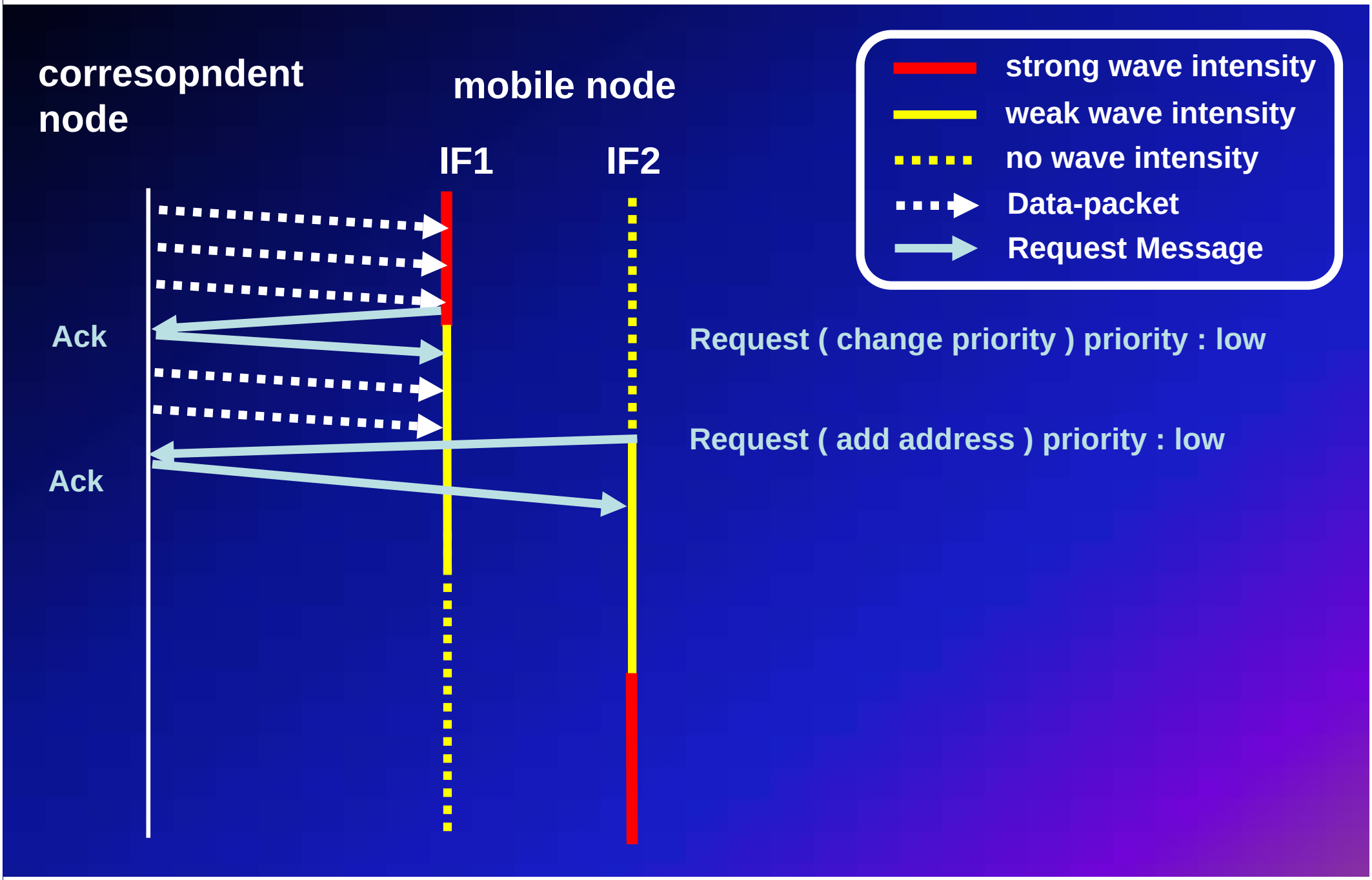
Bicasting


corresopndent node
mobile node
IF1
IF2
Ack
strong wave intensity
weak wave intensity
no wave intensity
Data-packet
Request Message
Request (change priority) priority : low

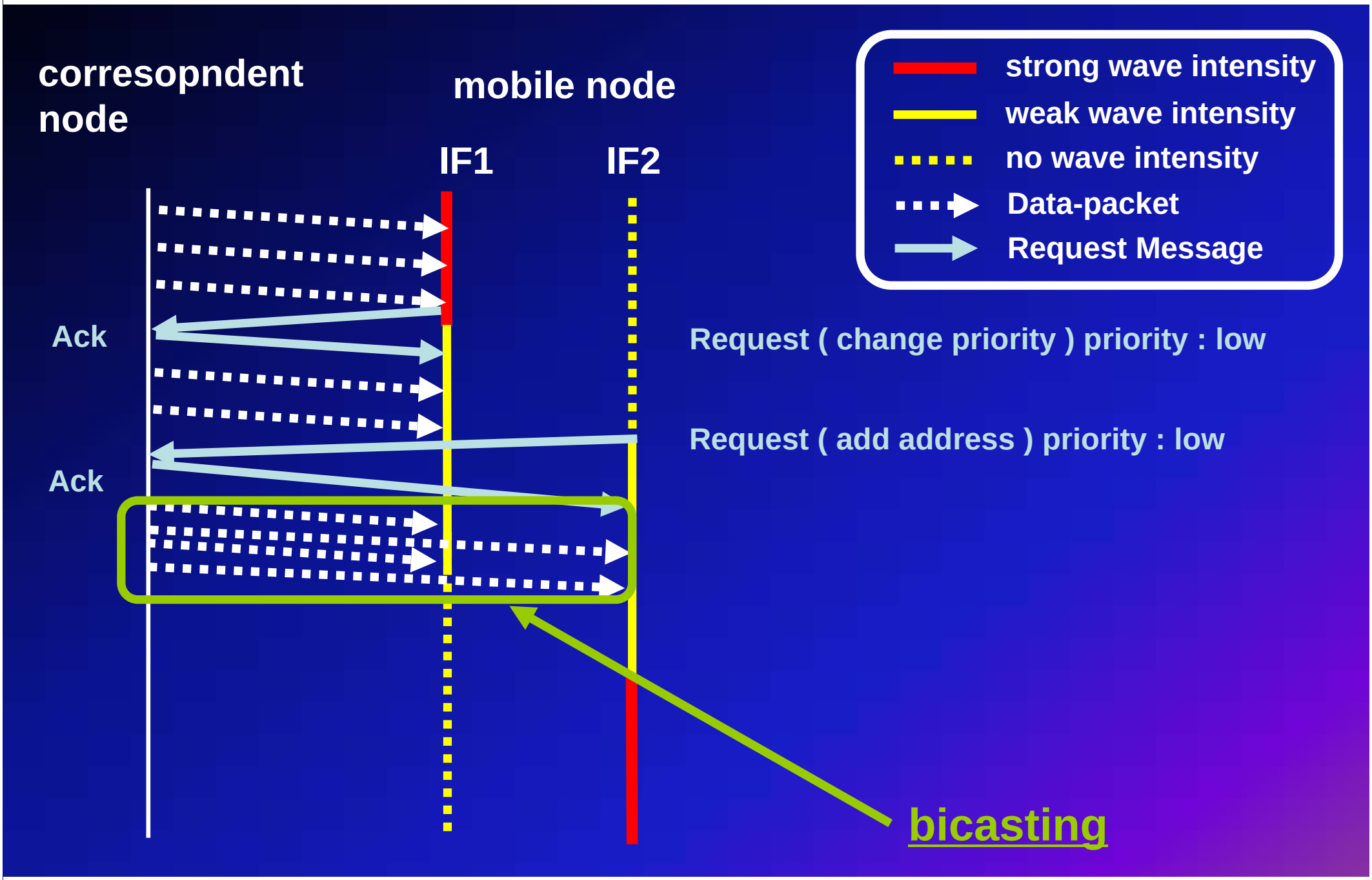
Bicasting


corresopndent node
mobile node
IF1
IF2
Ack
strong wave intensity
weak wave intensity
no wave intensity
Data-packet
Request Message
Request (change priority) priority : low

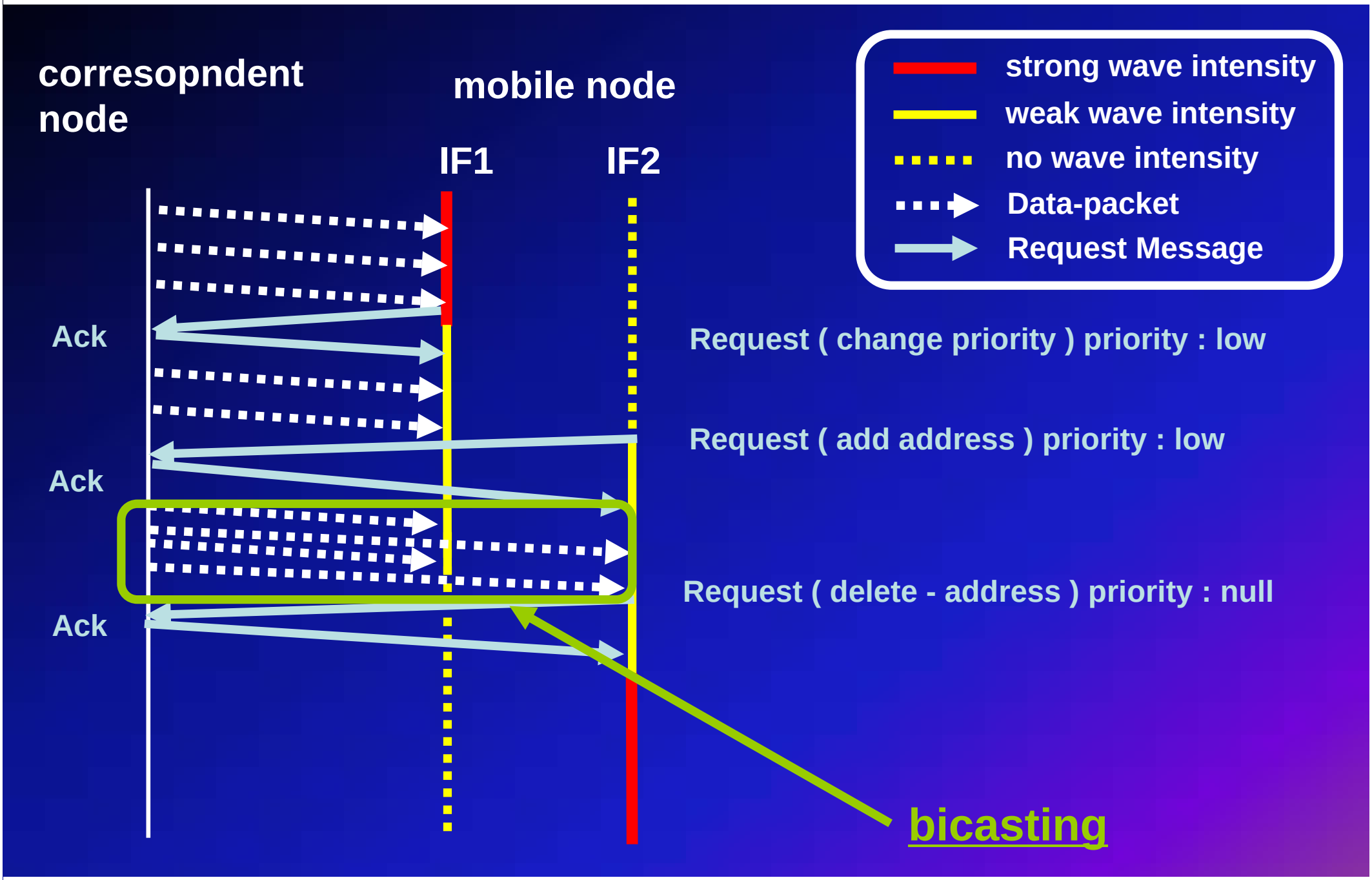
Bicasting


corresopndent node
mobile node
IF1
IF2
Ack
Ack
strong wave intensity
weak wave intensity
no wave intensity
Data-packet
Request Message
Request (change priority) priority : low
Request (add address) priority : low

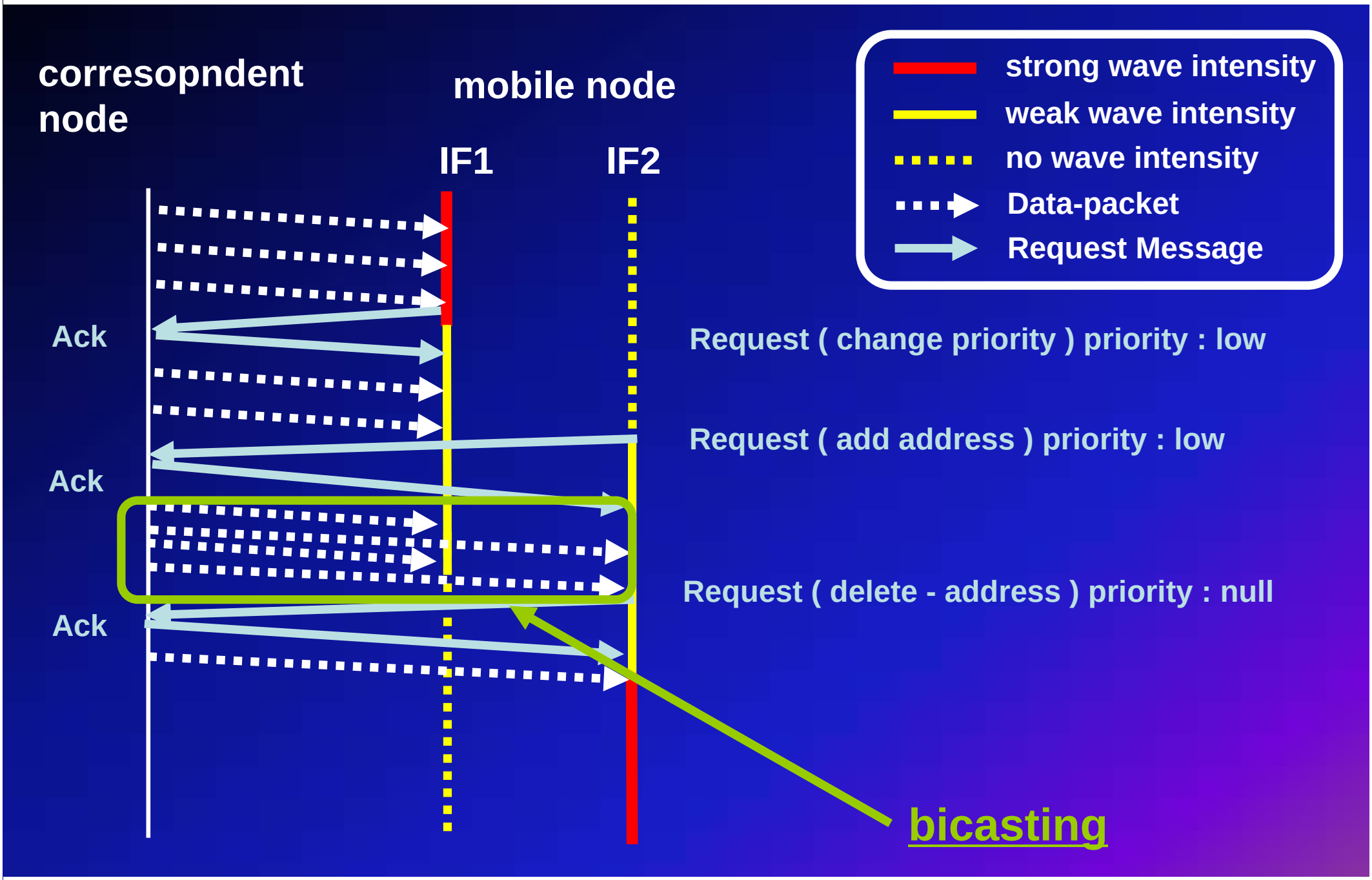
Bicasting


corresopndent node
mobile node
IF1
IF2
strong wave intensity
weak wave intensity
no wave intensity
Data-packet
Request Message
Ack
Ack
Request (change priority) priority : low
Request (add address) priority : low
bicasting

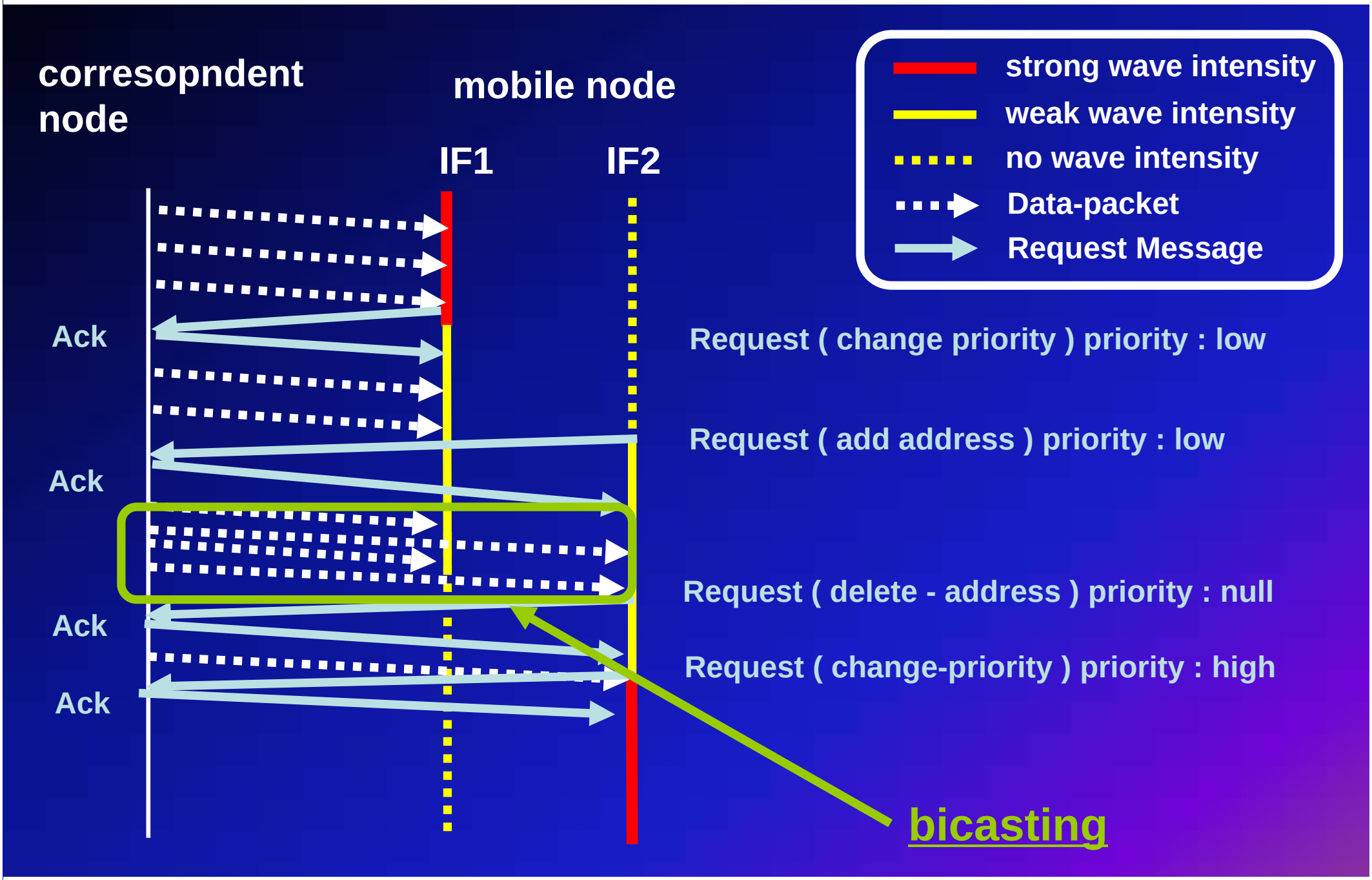
Bicasting


corresopndent node
mobile node
IF1
IF2
strong wave intensity
weak wave intensity
no wave intensity
Data-packet
Request Message
Ack
Ack
Ack
Request (change priority) priority : low
Request (add address) priority : low
Request (delete - address) priority : null
bicasting

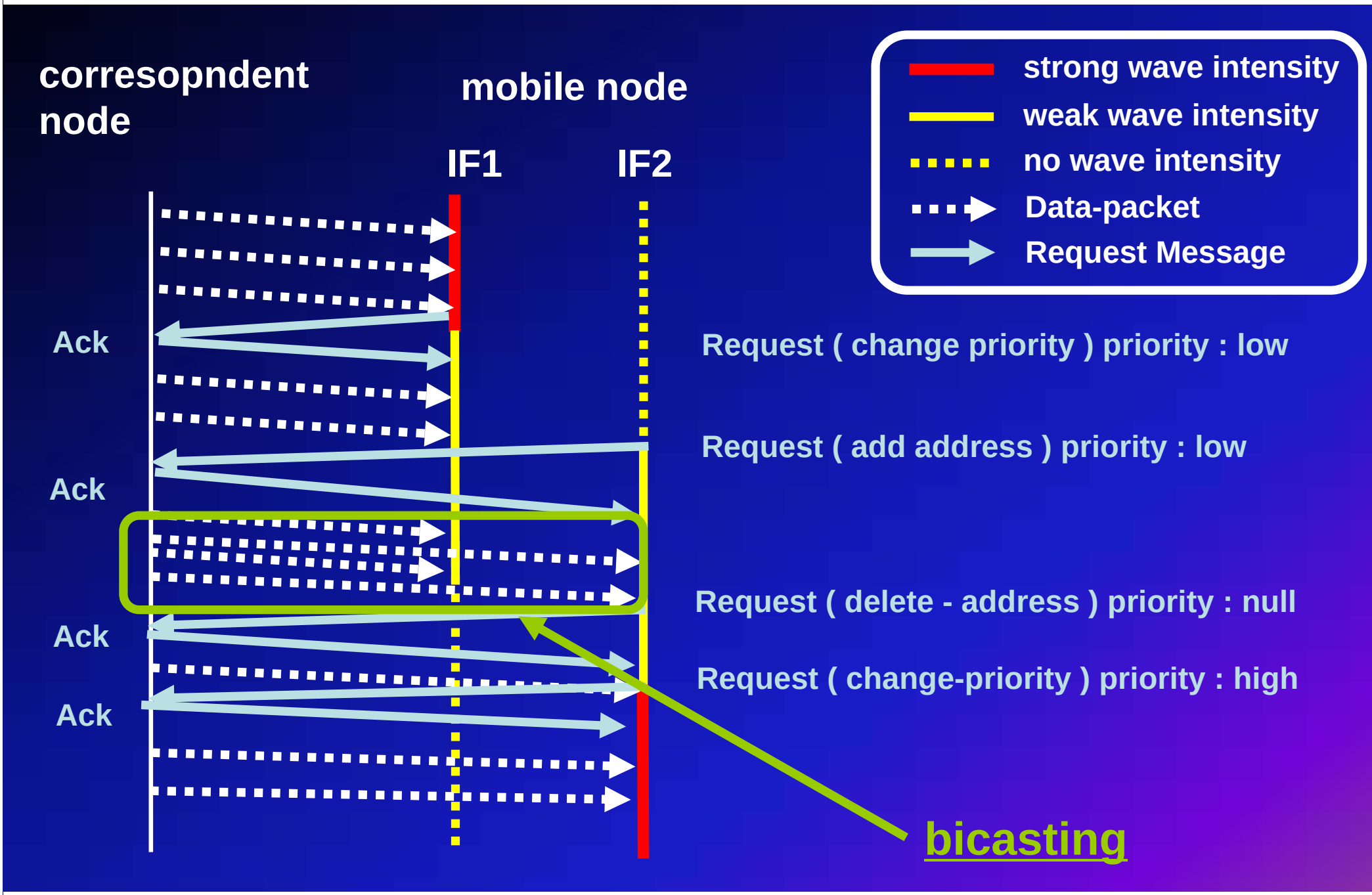
Bicasting


corresopndent node
mobile node
IF1
IF2
strong wave intensity
weak wave intensity
no wave intensity
Data-packet
Request Message
Ack
Ack
Ack
Request (change priority) priority : low
Request (add address) priority : low
Request (delete - address) priority : null
bicasting

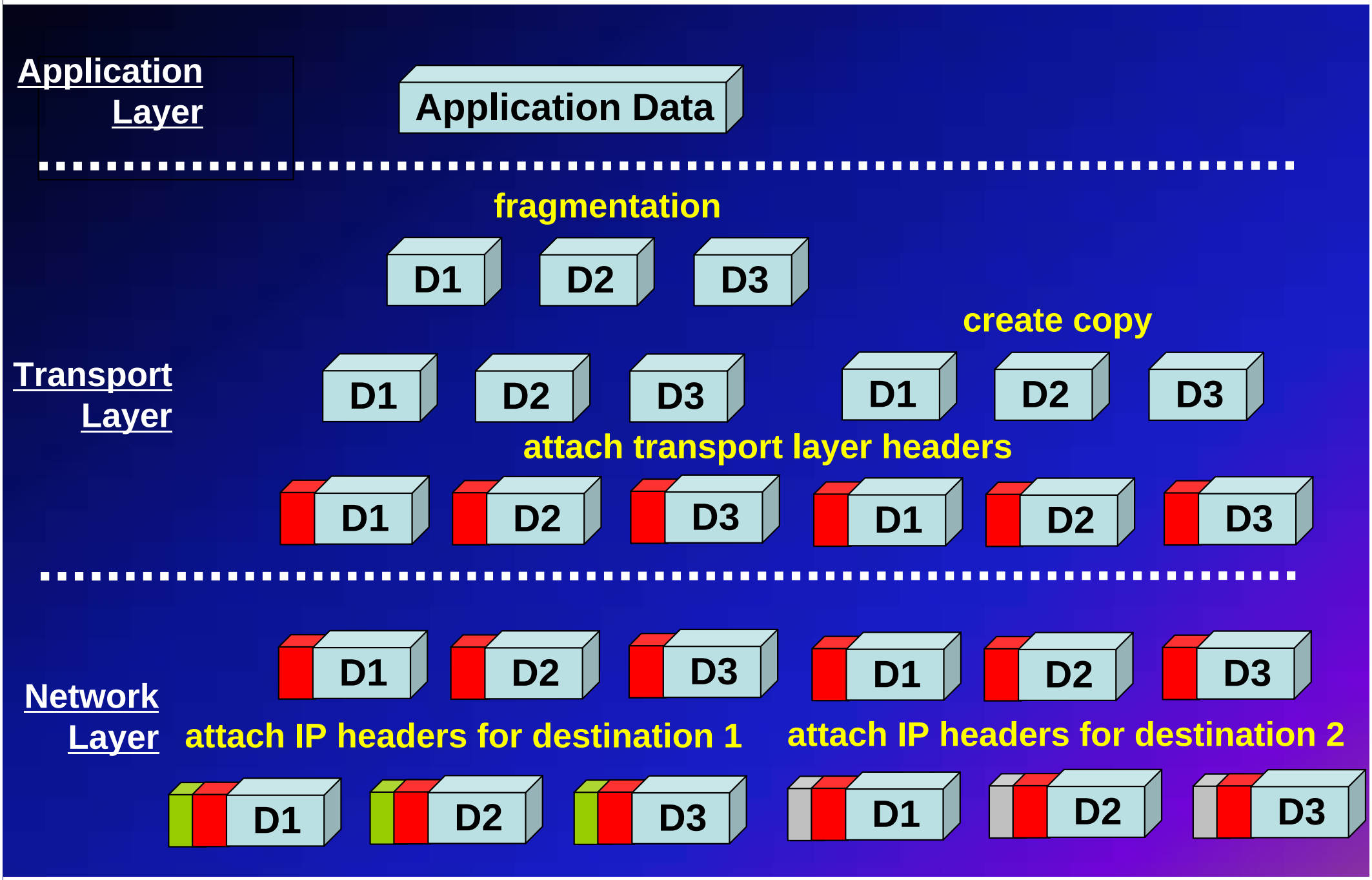
Bicasting


corresopndent node
mobile node
IF1
IF2
strong wave intensity
weak wave intensity
no wave intensity
Data-packet
Request Message
Ack
Ack
Ack
Ack
Request (change priority) priority : low
Request (add address) priority : low
Request (delete - address) priority : null
Request (change-priority) priority : high
bicasting

Bicasting


corresopndent node
mobile node
IF1
IF2
Ack
Ack
Ack
Ack
strong wave intensity
weak wave intensity
no wave intensity
Data-packet
Request Message
Request (change priority) priority : low
Request (add address) priority : low
Request (delete - address) priority : null
Request (change-priority) priority : high
bicasting

Bicasting


Application Layer
Application Data
fragmentation
D1
D2
D3
create copy
Transport Layer
D1
D2
D3
D1
D2
D3
attach transport layer headers
D1
D2
D3
D1
D2
D3
Network Layer
D1
D2
D3
D1
D2
D3
attach IP headers for destination 1
attach IP headers for destination 2
D1
D2
D3
D1
D2
D3

Bicastingの問題点

- 受信側ではフラグメンテーション化されたデータが3つともそろわなければならない
- 同じパケットを複数の経路で送信するのは、エラー耐性の観点から考えると効率が良くない
- 同一のパケットが両方の経路で消失すると、そのパケットは復元不可能

FEC-Bicasting

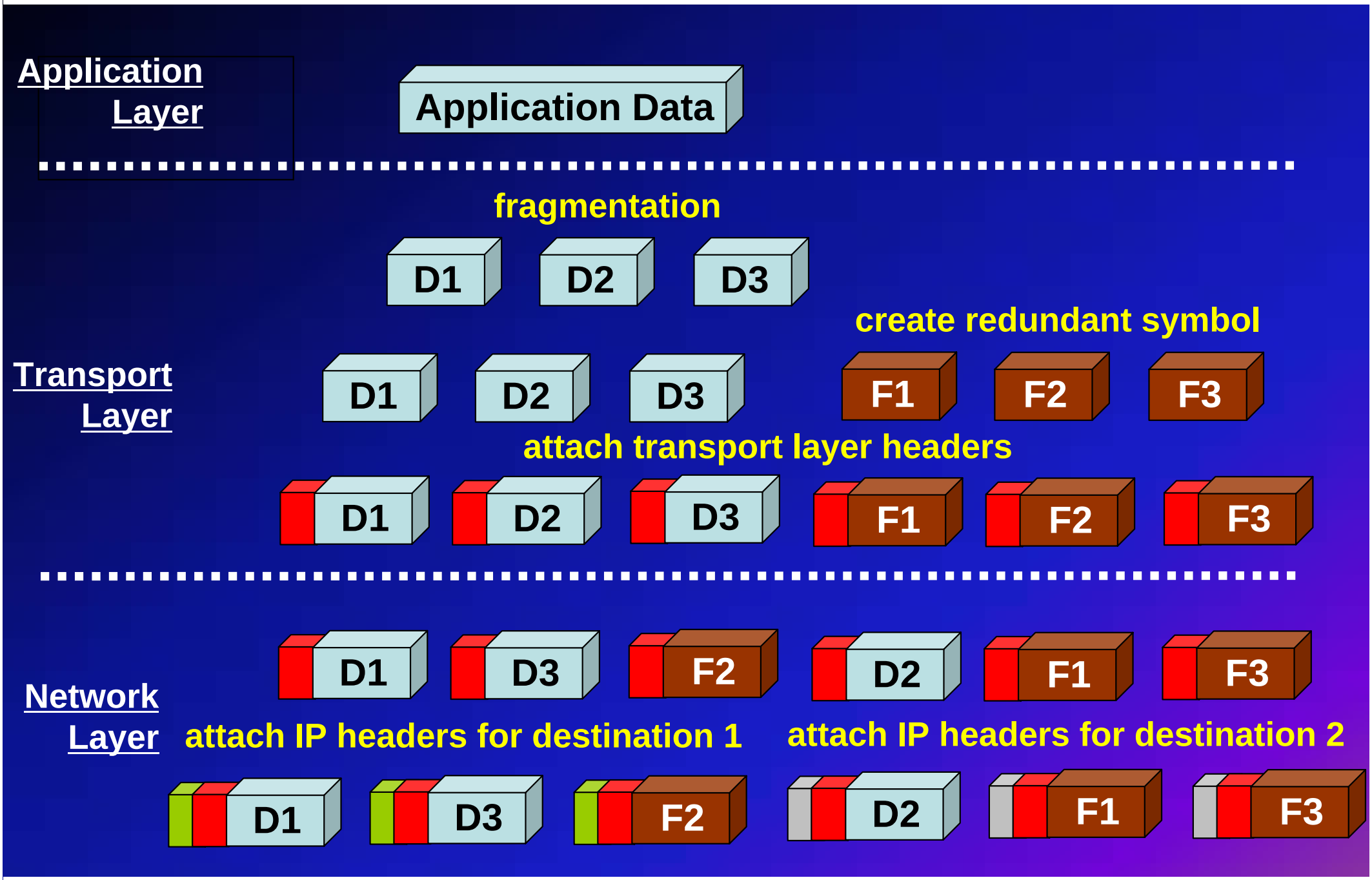
・エラー耐性の強い、効率の良い通信方式

・高度な数学を使用

※FEC（ Forward Error Correction ）

→データの廃棄や、誤りを検出した時にそのデータを再送することなく、転送すべきデータに付加した冗長データを用いて復元する技術

FEC-Bicasting



FEC-Bicasting

Bicasting →1通り

FEC-Bicasting → ${}_6C_3 = 6 \times 5 \times 4 / 3 \times 2 \times 1$

= 20通り

Security

- モバイル端末が通信相手にIPアドレスの追加、削除、優先レベルの変更、を要求するメッセージは容易に偽造できる。
- reply攻撃、man-in-the-middle攻撃への対策が必要
- 端末同士の認証が必要
- IPsecを用いることにより通信端末同士の認証可能

Security

- IPsecのSA(Security Association)はIPアドレスベースで管理
- IPアドレスが変更する度に、SAを更新するのは処理の負荷
- MMSPでは独自に通信の奪取を防止するためのセキュリティ機構を有する

Security

- 通信端末同士は、通信開始時にDiffie-Hellman鍵交換方式によって、共有鍵を生成
- モバイル端末から、通信相手への要求メッセージには、HMAC(Hash-based Message Authentication Code)によって署名を付加する
- HMACには、Diffie-Hellman 鍵交換で生成した共有鍵を使用する

Replay攻撃

- 不正侵入手段の一つ
- パスワードや暗号鍵などを盗聴しそのまま再利用することでそのユーザに成りすます方法
- パスワードが暗号化されていても、暗号化された後のデータをそのまま使用
- 受け取った相手は正しいパスワードを正しく暗号化していると思い過ごす

Replay攻撃に対しての対策

対策

- 要求メッセージにシーケンス番号を付加
- 一度ネットワークに送信したメッセージを再利用される事を防ぐ

Man-in-the-middle 攻撃

- 暗号通信を盗聴したり介入したりする手法の一つ
- 通信を行う二者の間に割り込み、両者が交換する公開情報を自分のものとすりかえることにより、気づかれること無く盗聴したり、通信内容に介入したりする方法

Man-in-the-middle 攻撃に対しての対策

・MMSPの機能自体では対応不可能

対策

・通信端末間であらかじめ秘密共有鍵を設定

・相手の公開鍵の設定

・認証局 (CA : Certificate Authority)などの公開鍵の正当性を証明する第三者が必要

まとめ

MMSP

- IPソフトハンドオーバを実現するための
  プロトコル

- UDPの拡張
  →Multihoming
  →FEC-Bicasting