

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2010-50987

(P2010-50987A)

(43) 公開日 平成22年3月4日(2010.3.4)

(51) Int.Cl.		F I				テーマコード (参考)
HO 4W 28/24	(2009.01)	HO 4Q	7/00	2 8 5		5 K O 6 7
HO 4W 80/04	(2009.01)	HO 4Q	7/00	6 0 2		

審査請求 有 請求項の数 16 O L (全 50 頁)

(21) 出願番号	特願2009-229463 (P2009-229463)	(71) 出願人	501082716
(22) 出願日	平成21年10月1日 (2009.10.1)		ノキア オサケ ユキチュア
(62) 分割の表示	特願2000-568269 (P2000-568269)		フィンランド エフイーエンーO 2 1 5 O
	の分割		エスプー ケイララーデンティエ 4
原出願日	平成11年8月27日 (1999.8.27)	(74) 代理人	100059959
(31) 優先権主張番号	9818873.3		弁理士 中村 稔
(32) 優先日	平成10年8月28日 (1998.8.28)	(74) 代理人	100067013
(33) 優先権主張国	英国 (GB)		弁理士 大塚 文昭
(31) 優先権主張番号	9819175.2	(74) 代理人	100082005
(32) 優先日	平成10年9月1日 (1998.9.1)		弁理士 熊倉 禎男
(33) 優先権主張国	英国 (GB)	(74) 代理人	100084009
			弁理士 小川 信夫
(特許庁注：以下のものは登録商標)		(74) 代理人	100086771
1. GSM			弁理士 西島 孝喜

最終頁に続く

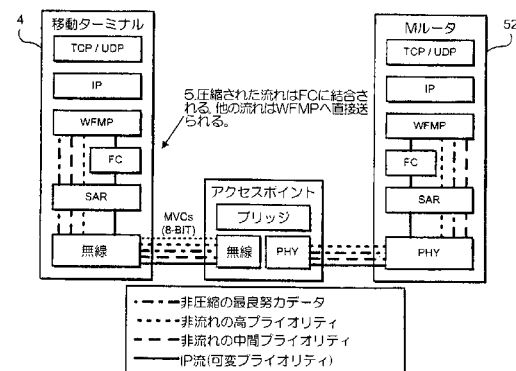
(54) 【発明の名称】 ワイヤレスネットワークのサービスクオリティをサポートする方法及びシステム

(57) 【要約】

【課題】無線ネットワークにおいて区別化サービス（サービスクオリティ）をサポートする機構が提供される。

【解決手段】エアインターフェイスを経てのデータパケット送信においてサービスクオリティをサポートする無線アクセスシステムが提供される。このシステムは、異なるサービスクオリティ特性を有する所定のデフォルト無線流の選択体と、この選択体から、エアインターフェイスを経て送信されるべきパケットに対して適当なサービスクオリティ特性を有する無線流を選択するための手段(4,52)とを備えている。

【選択図】図1 4



【特許請求の範囲】**【請求項 1】**

エアインターフェイスを経ての送信が無線流において行なわれるように無線ネットワークのパケットデータ送信のサービスクオリティをサポートする方法において、

異なるサービスクオリティ特性を有する所定のデフォルト無線流の選択体から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有する無線流を選択する段階を含むことを特徴とする方法。

【請求項 2】

上記無線流を選択する段階は、送信されるべきパケットに、異なるサービスクオリティ特性を表わす所定のデフォルト無線流識別子から選択された無線流識別子を与えることを含む請求項 1 に記載の方法。

10

【請求項 3】

パケットを、エアインターフェイスを経て送信するための識別されたデフォルト無線流へとマッピングする段階を更に含む請求項 2 に記載の方法。

【請求項 4】

ある無線サブネットワークから別の無線サブネットワークへのアクティブな接続を有する移動通信装置のハンドオーバーを検出し、そして

ハンドオーバーの検出に応答してアクティブな接続に対しデフォルト無線流の選択を遂行する、

という段階を更に含む請求項 1 ないし 3 のいずれかに記載の方法。

20

【請求項 5】

エアインターフェイスを経て送信されるべきパケットを監視して、IP 流を検出し、そして

検出された IP 流を、対応するサービスクオリティ特性を有する専用無線流へスイッチングする、

という段階を更に含む請求項 1 ないし 4 のいずれかに記載の方法。

【請求項 6】

検出された IP 流を専用無線流にスイッチングする上記段階は、

検出された IP 流のパケットに専用無線流の識別子を与え、そして

検出された IP 流のパケットを、エアインターフェイスを経て送信するための識別された専用無線流へとマッピングする、

という段階を含む請求項 5 に記載の方法。

30

【請求項 7】

エアインターフェイスを経てのデータパケット送信においてサービスクオリティをサポートするための無線アクセスシステムにおいて、

異なるサービスクオリティ特性を有する所定のデフォルト無線流の選択体と、

上記選択体から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有する無線流を選択する手段と、

を備えたことを特徴とする無線アクセスシステム。

【請求項 8】

上記無線流の選択手段は、送信されるべきパケットに、所定のデフォルト無線流に対応する識別子から選択された無線流識別子を与えるための手段を備えている請求項 7 に記載のシステム。

40

【請求項 9】

パケットを、エアインターフェイスを経て送信するための識別されたデフォルト無線流へとマッピングする手段を更に備えた請求項 8 に記載のシステム。

【請求項 10】

ある無線サブネットワークから別の無線サブネットワークへのアクティブな接続を有する移動通信装置のハンドオーバーを検出するための手段を更に備え、そして上記選択手段は、ハンドオーバーの検出に応答してアクティブな接続に対しデフォルト無線流を選択

50

する請求項 7 ないし 9 のいずれかに記載のシステム。

【請求項 11】

エアインターフェイスを経て送信されるべきパケットを監視して IP 流を検出する手段と、

検出された IP 流を、対応するサービスクオリティ特性を有する専用無線流へスイッチングする手段と、

を更に備えた請求項 7 ないし 10 のいずれかに記載のシステム。

【請求項 12】

上記スイッチング手段は、

検出された IP 流のパケットに専用無線流の識別子を与える手段と、

検出された IP 流のパケットを、エアインターフェイスを経て送信するための識別された専用無線流へとマッピングする手段と、

を備えた請求項 11 に記載のシステム。

【請求項 13】

エアインターフェイスを経てのデータパケット送信においてサービスクオリティをサポートするものであって、異なるサービスクオリティ特性を有する所定のデフォルト無線流の選択体を備えたシステムに使用するための通信装置において、

上記選択体から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有するデフォルト無線流を選択するように構成されたことを特徴とする装置。

【請求項 14】

上記装置は、移動通信装置又は移動ルータである請求項 13 に記載の装置。

【請求項 15】

請求項 7 ないし 12 のいずれかに記載のシステムに使用するための請求項 13 又は 14 に記載の装置。

【請求項 16】

エアインターフェイスを経ての送信がパケットスケジューリングに基づいて行なわれるように無線ネットワークのパケットデータ送信のサービスクオリティをサポートする方法において、

異なるサービスクオリティ特性を有するデフォルト無線スケジューリング待ち行列の選択体から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有する無線スケジューリング待ち行列を選択する段階を含むことを特徴とする方法。

【請求項 17】

上記無線スケジューリング待ち行列は、エアインターフェイスに集合されるか、或いは待ち行列又は接続特有の無線流識別子の助けによりエアインターフェイスにおいて別々に識別される請求項 16 に記載の方法。

【請求項 18】

エアインターフェイスを経てのデータパケット送信においてサービスクオリティをサポートするための無線アクセスシステムにおいて、

異なるサービスクオリティ特性を有するデフォルト無線スケジューリング待ち行列の選択体と、

上記選択体から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有する無線スケジューリング待ち行列を選択する手段と、
を備えたことを特徴とする無線アクセスシステム。

【請求項 19】

エアインターフェイスを経てのデータパケット送信においてサービスクオリティをサポートするものであって、異なるサービスクオリティ特性を有するデフォルト無線スケジューリング待ち行列の選択体を備えたシステムに使用するための通信装置において、

上記選択体から、エアインターフェイスを経て送信されるべきパケットに対して適切な

10

20

30

40

50

サービスクオリティ特性を有するデフォルト無線スケジューリング待ち行列を選択するように構成されたことを特徴とする装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、無線ネットワークのサービスクオリティをサポートするための構成に係る。より詳細には、本発明は、無線ネットワークのパケットデータ送信においてサービスクオリティをサポートする方法、システム及び通信装置に係る。

このような構成は、例えば、ワイヤレスインターネットプロトコル（IP）ネットワークに必要とされる。

10

【背景技術】

【0002】

「インターネット」という用語は、一般に、パーソナルコンピュータ（PC）のようなデータプロセッサから情報を検索できる場所の情報リソースを表現するのに使用される。データプロセッサは、モデムを介してテレコミュニケーションネットワークと通信する。この情報リソースは、世界的な規模で分散されており、テレコミュニケーションネットワークとも通信する多数の記憶位置を備えている。インターネットは、TCP（転送制御プロトコル）、UDP（ユーザデータグラムプロトコル）及びIP（インターネットプロトコル）のような幾つかのデータ通信規格及びプロトコルを定義することにより動作でき、これらは、インターネットの多数の部分間のデータ送信を制御するのに使用される。TCP及びUDPは、インターネットに送信されるデータのデータ送信エラーを防止し修正することで含まれ、そしてIPは、パケットアドレッシング及びルート指定に含まれる。インターネットプロトコルの現在指定されているバージョンは、IPv4及びIPv6である。IPv4はRFC791に規定され、そしてIPv6はRFC1883に規定されている。

20

【0003】

オープンデータシステムが益々普及してきているために、送信制御プロトコル/インターネットプロトコル（TCP/IP）の通信プロトコルが、一般に使用されるプロトコルとなっており、従って、種々のサイズ及び機種のコピュータが互いに通信することができる。ほとんど全てのオペレーティングシステムに対してTCP/IPのサポートを現在利用することができる。TCP/IPのネットワーク層プロトコルであるインターネットプロトコルIPは、ゲートウェイ即ちルータによりパケットをルート指定するのに使用される。ルート指定は、4バイトのIPアドレス及びルートテーブルによって行なわれる。インターネットプロトコルにより、TCP/IPを使用するコンピュータは、ルータネットワークのメッセージを世界の反対側へも転送することができる。

30

【0004】

インターネットワイスの急速な発展は、高いデータレート及びサービスクオリティ（QoS）をもつ広帯域ネットワークの強い要望を生じさせた。ビデオブロードキャスト配信及び他のマルチメディア配信サービスも急速に発展している。ユーザは、ワイヤレス環境においてもこれらのサービスにアクセスしようとしている。現在、固定のIPネットワークでは、IPパケットが最良努力（best effort）データトラフィックとして通常送信される。ネットワークが混雑している場合には、全てのデータ流が同じプライオリティで取り扱われ、これは、マルチメディアサービスに多大な影響を及ぼす。2つの主たる問題が生じる。即ち、第1に、現在のワイヤレスネットワークは、十分なQoS構成を与えない。そして第2に、既存のワイヤレスネットワークは、高いデータレート及びQoS要求をもつ多数の同時接続にサービスすることができない。顧客の高い要求を満足するために、新規なワイヤレス広帯域ネットワーク技術が要望されている。

40

【0005】

インターネット・エンジニアリング・タスク・フォース（IETF）は、インターネットアーキテクチャー及びインターネットのオペレーションの開発に関連した組織である。

50

彼等は、2つの異なるIPベースのQoS概念、即ちIPネットワークのリアルタイムアプリケーションをサポートするための標準的構成を与える一体化及び差別化サービスを定義している。一体化サービスは、指定プロトコル(RSVP、RFC2205)及び受け入れ制御を伴う抽象的流れモデルをベースとするものである。ネットワークは、各ネットワーク装置においてリアルタイム接続のためのリソースを静的に指定し、従って、最適な効率ではない。その結果、差別化サービスの概念が開発された。この概念は、IPヘッダの使用をベースとして、そのパケットに対して要求されたサービスクラスを指示する。その結果として、各IPパケットヘッダはQoS情報を搬送し、静的な指定は要求されない。IETFは、IPヘッダを使用してQoSを指示することを示唆するが、実際のパケット取り扱い機構は、標準化されそうもない。

10

【発明の概要】

【発明が解決しようとする課題】

【0006】

本発明は、QoSをサポートし、特に、エアインターフェイスにおける差別化サービスをサポートするワイヤレスIPネットワークアーキテクチャーを提供する。

【課題を解決するための手段】

【0007】

本発明の第1の特徴によれば、エアインターフェイスを経ての送信が無線流において行なわれるように無線ネットワークのパケットデータ送信のサービスクオリティをサポートする方法において、異なるサービスクオリティ特性を有する所定のデフォルト無線流の選択体から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有する無線流を選択する段階を含む方法が提供される。

20

【0008】

デフォルト無線流を設けることにより、無線ネットワークは差別化サービスをサポートすることができ、従って、ワイヤレス広帯域サービスに対する準備をすることができる。特に、IPネットワークの無線部分にデータのボトルネックが生じるのを防止する。

無線流の選択は、送信されるべきパケットに、異なるサービスクオリティ特性を表わす所定のデフォルト無線流識別子から選択された無線流識別子を与えることにより行うことができる。次いで、パケットは、エアインターフェイスを経て送信するための識別されたデフォルト無線流へとマッピングすることができる。

30

【0009】

好都合にも、本発明の方法は、ある無線サブネットワークから別の無線サブネットワークへのアクティブな接続を有する移動通信装置のハンドオーバーを検出し、そしてハンドオーバーの検出に応答してアクティブな接続に対しデフォルト無線流の選択を遂行する段階を含む。

これは、ドメイン間の移動を更に改善する。例えば、移動ターミナルが新たな無線サブネットワーク(例えば、新たな移動ルータのエリア)へと移動するときに、デフォルト無線流を使用してハンドオーバーの性能を改善することができる。新たなルータは、通常、ターミナル接続及び必要なQoSに関する情報を有していない。それ故、QoS流を前もって確立することはできない。ハンドオーバー中のパケット損失を減少するために、ターミナル及びネットワークは、既存の接続(古い流れ)をデフォルト無線流の1つへと一時的にスイッチすることができる。この解決策は、新たなルータがQoS(IP)流を検出しそして接続を個別の無線流へとスイッチするまで、ある接続に対して高いQoSを指定することができる。

40

【0010】

又、本発明の方法は、一体化サービスをサポートするのが好ましい。例えば、本発明の好ましい実施形態では、この方法は、エアインターフェイスを経て送信されるべきパケットを監視してIP流を検出し、そして検出されたIP流を、対応するサービスクオリティ特性を有する専用無線流へとスイッチングするという段階を更に含む。通常、デフォルト無線流が最初に選択され、次いで、その無線流が設定されると、IP流が個別の無線流

50

へ転送される。

検出されたIP流を専用無線流へスイッチングすることは、検出されたIP流のパケットに専用無線流の識別子を与え、そして検出されたIP流のパケットを、エアインターフェイスを経て送信するための識別された専用無線流へとマッピングすることにより行うことができる。

【0011】

上記方法を実施するシステム及び通信装置が提供される。

例えば、本発明の別の特徴によれば、エアインターフェイスを経てのデータパケット送信においてサービスクオリティをサポートするための無線アクセスシステムにおいて、異なるサービスクオリティ特性を有する所定のデフォルト無線流の選択体と、この選択体から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有する無線流を選択する手段とを備えた無線アクセスシステムが提供される。

10

上記無線流の選択手段は、送信されるべきパケットに、所定のデフォルト無線流に対応する識別子から選択された無線流識別子を与えるための手段と、パケットを、エアインターフェイスを経て送信するための識別されたデフォルト無線流へとマッピングするための手段とを任意に備えている。

【0012】

又、本発明のシステムは、ある無線サブネットワークから別の無線サブネットワークへのアクティブな接続を有する移動通信装置のハンドオーバーを検出するための手段を含むのが好ましい。この場合、選択手段は、ハンドオーバーの検出にตอบสนองしてアクティブな接続に対しデフォルト無線流を選択する。

20

好都合にも、本発明のシステムは、更に、エアインターフェイスを経て送信されるべきパケットを監視してIP流を検出する手段と、検出されたIP流を、対応するサービスクオリティ特性を有する専用無線流へスイッチングする手段とを備えている。このスイッチング手段は、検出されたIP流のパケットに専用無線流の識別子を与える手段と、検出されたIP流のパケットを、エアインターフェイスを経て送信するための識別された専用無線流へとマッピングする手段とを備えている。

【0013】

本発明の更に別の特徴によれば、エアインターフェイスを経てのデータパケット送信においてサービスクオリティをサポートするものであって、異なるサービスクオリティ特性を有する所定のデフォルト無線流の選択体を備えたシステムに使用するための通信装置において、上記選択体から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有するデフォルト無線流を選択するように構成された装置が提供される。この通信装置は、例えば、移動通信装置、アクセスポイントコントローラ又は移動ルータである。

30

【0014】

本発明の実施形態によれば、無線モデムは、無線ネットワークが差別化サービスをサポートし、従って、ワイヤレス広帯域サービスに対して準備できるようにする幾つかの異なるサービス形式を提供する。特に、これは、インターネットアクセスネットワークの無線部に時間厳密データのボトルネックが生じるのを防止する。無線QoSクラスの選択は、IP形式のサービスビット、即ちdiffsビットを定義し、そしてそれに対応する所定のデフォルト無線QoSクラスを選択することにより実行できる。次いで、パケットは、エアインターフェイスを経て送信するために、識別されたデフォルト無線待ち行列へとマップされる。

40

【0015】

エアインターフェイスを経ての送信は、例えば、無線流をベースとすることができ、本発明の方法は、異なるサービスクオリティ特性を有する所定のデフォルト無線流の選択体から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有する無線流を選択する段階を含む。或いは又、本発明のシステムは、異

50

なるスケジューリングプライオリティをもつ多数の無線レベルサービス待ち行列を使用することができる。

上述したように、本発明の方法は、ある無線サブネットワークから別の無線サブネットワークへのアクティブな接続を有する移動通信装置のハンドオーバーを検出し、そしてハンドオーバーの検出に応答してアクティブな接続に対しデフォルト無線流の選択を遂行する段階を含む。

【 0 0 1 6 】

これは、ドメイン間移動を更に改善する。本発明のこの実施形態では、新たなルータは、到来するパケットのIPヘッダを読み取ることにより必要なサービス形式を直ちに通知することができる。従って、リアルタイムデータを、最も高いサービスクラスの待ち行列に直接マップすることができ、これは、ハンドオーバー中のパケット損失を減少する。デフォルト無線流が使用される場合に、この解決策は、新たなルータがQoS(IP)流を検出しそして接続を個別の無線流へとスイッチするまで、ある接続に対して高いQoSを指定できるようにする。

この実施形態の方法は、一体化サービスもサポートするのが好ましい。例えば、この方法は、エアインターフェイスを経て送信されるべきパケットを監視してIP流を検出し、そして検出されたIP流を、対応するサービスクオリティ特性を有する専用無線サービス待ち行列へとスイッチングする段階を更に含む。

【 0 0 1 7 】

本発明の更に別の実施形態によれば、エアインターフェイスを経てのデータパケット送信においてサービスクオリティをサポートするための無線アクセスシステムであって、所定のデフォルト無線サービス待ち行列の選択体を備えた無線アクセスシステムが提供される。異なる待ち行列は、エアインターフェイスにおいて異なる仕方でスケジューリングされる。ある待ち行列に属するパケットは、特定の無線流識別子を使用することによりエアインターフェイスを経て送信されてもよいし、或いは異なるサービス待ち行列が異なる仕方でスケジューリングされるが、流れ特有の識別子をもたずに送信されてもよい。異なるサービスクオリティ特性を有する無線待ち行列は、ネットワークレベルに対応する無線サービスクラス、例えば、エアインターフェイスを経て送信されるべきパケットに対するIP、QoSクラスを上記選択体から選択するための手段を形成する。

【 0 0 1 8 】

この実施形態のシステムは、ある無線サブネットワークから別の無線サブネットワークへのアクティブな接続を有する移動通信装置のハンドオーバーを検出するための手段を備えている。この場合に、選択手段は、ハンドオーバーの検出に応答して、適切な無線QoSクラス、即ちアクティブな接続に対するスケジューリング待ち行列及び/又は無線流を選択する。

【 図面の簡単な説明 】

【 0 0 1 9 】

【 図 1 】 GRAN 基準モデルを示す図である。

【 図 2 】 一般的システムアーキテクチャーを示す図である。

【 図 3 】 ターゲット動作環境及び送信リンク態様を示す図である。

【 図 4 】 データ経路アーキテクチャーの外観図である。

【 図 5 】 送信リンク態様を示す図である。

【 図 6 】 イーサネット（登録商標）ベースのシステムアーキテクチャーを示す図である。

【 図 7 】 ATM のデータ平面を示す図である。

【 図 8 】 イーサネットのデータ平面を示す図である。

【 図 9 】 無線アクセスネットワーク識別子 (RAN_ID) の例示的構造を示す図である。

【 図 10 】 ATM 送信リンクが使用される場合のパケットカプセル化を示す図である。

【 図 11 】 イーサネット送信リンクの場合の流れマッピングを示す図である。

【 図 12 】 定められた流れ管理構成の概要を示す図である。

10

20

30

40

50

- 【図 1 3】 I P 及び無線流マルチプレクシング構成を示す図である。
- 【図 1 4】 I P 及び無線流マルチプレクシング構成を示す図である。
- 【図 1 5】 システムアーキテクチャ及びメインインターフェイスを示す図である。
- 【図 1 6】 異なる流れ形式の例を示す図である。
- 【図 1 7】 典型的な W F M P テーブルを示す図である。
- 【図 1 8】 ダウンリンクパケットに対する移動ルータ (M ルータ) W F M P ルート指定を示す図である。
- 【図 1 9】 アップリンクパケットに対する M ルータ W F M P ルート指定を示す図である。
- 【図 2 0】 2 つの移動ターミナル間の送信を示す図である。
- 【図 2 1】 アップリンクに対する移動ターミナル側の W F M P 動作を示す図である。
- 【図 2 2】 ダウンリンクに対する移動ターミナル側のルート指定を示す図である。
- 【図 2 3】 流れ圧縮 (F C) 構造を示す図である。
- 【図 2 4】 一体化サービスを示す図である。
- 【図 2 5】 区別化サービスを示す図である。
- 【図 2 6】 ポート情報を示す図である。
- 【図 2 7】 H . 3 2 3 を示す図である。
- 【図 2 8】 ワイヤレス Q o S 駆動の待ち行列及びエラー制御戦略を示す図である。
- 【発明を実施するための形態】

10

20

以下、添付図面を参照して、本発明の実施形態を一例として詳細に説明する。

狭帯域パケットデータサービス及び遅延感知の広帯域マルチメディアサービスの両方への効率的な移動アクセスを可能にする本発明の好ましい実施形態のワイヤレス I P ネットワークアーキテクチャについて説明する。先ず、ネットワーク構造、データ平面アーキテクチャ、並びに I P 流管理及びアーキテクチャを含むシステムアーキテクチャについて述べる。

最初に、主たる物理的ブロック、プロトコルフレーム及び主たる内部インターフェイスを定める一般的システムアーキテクチャを説明する。次いで、定められた機能的エンティティ及びプロトコルの機能及びインターワーキングについて説明する。

【 0 0 2 1 】

30

ネットワーク構造

理論的な基準モデル

システムアーキテクチャは、添付図面の図 1 に示した理論的な「一般的無線アクセスネットワーク (G R A N) 」基準モデルの概要に従う [E S 2 1]。広帯域無線アクセスネットワーク 1 (B R A N) は、無線アクセスネットワーク 2 (R A N) と、コアネットワークに從属するインターワーキング機能 (I W F) ブロックとを備えている。 R A N は、全ての無線從属部分を保持し、そして I W F は、 R A N を種々のコアネットワーク 3 及びターミナルエンティティ 4 にリンクする。以下の説明において、「好ましいシステム」という用語は、一般に、 R A N 及び必要な I W F をカバーする全 B R A N ネットワークを指すものとする。好ましいシステムは、 I P コアネットワークに接続される。

【 0 0 2 2 】

40

ネットワークエンティティ

図 2 に示す広帯域無線アクセスネットワークは、移動ターミナル 4 と、アクセスポイント 5 1、5 1' と、それらの間のエアインターフェイスと、移動度向上 I P ルータ 5 2 (M ルータ) とを有する無線アクセスネットワーク 2 で構成される。 B R A N は、インターネットバックボーン 2 1 及びホームエージェント 2 2 を含むコア I P ネットワークに接続される。

無線アクセスネットワーク 2 (R A N) は、無線リソース管理、ワイヤレス流の設定及び解除、ハンドオーバー並びにパケット圧縮のような全ての無線從属機能を実施する。この R A N は、移動ターミナル及びアクセスポイントを含む。移動ターミナル 4 は、ワイヤレスインターネットサービスにアクセスするためのユーザ通信装置であり、そしてインタ

50

ーネット及び無線アクセスネットワーク制御プロトコルのエンドポイントである。アクセスポイント51、51'は、無線リソース管理のような全ての無線従属制御機能を実施する。これは、無線リソース管理及び無線リンク制御機能を含む。GSMにおける対応ネットワーク要素は、ベーストランシーバステーション(BTS/TRX)及びベースステーションコントローラ(BSC)である。

【0023】

Mルータ52は、1つ以上のアクセスポイントにデータを送給するワイヤレスIPサブネットワークを形成する。或いは又、Mルータは、アクセスポイント51、51'に登録されたターミナルの移動及び位置管理を取り扱ってもよい。Mルータは、DHCP(動的ホスト構成プロトコル)のようなIP移動サービスを提供する。DHCPは、ターミナルに対してIPアドレスを割り当てるのに使用される。GSMネットワークにおける対応要素は、ゲートウェイGPRSサポートノード(GGSN)である。アクセスポイント51、51'と、同じIPサブネットワーク(同じMルータを使用する)に属するIPスタックを伴うターミナル4とが論理的リンクを形成する。

コアネットワーク3は、ホームエージェント22を備え、これは、関連ターミナル4のホームネットワーク内にあって、標準IPゲートウェイを経てアクセスされる。通常、ホームエージェント22は、ホームネットワークのMルータ52の一部として実施される。しかしながら、これは、個別のエンティティ(例えば、PCホスト)であってもよい。ホームエージェント22は、ユーザ認証情報及び勘定データベースを含むことができる。これは、GSMにおけるホーム位置レジスタ(HLR)に類似している。

【0024】

ターゲット環境

本発明のこの好ましいシステムは、専用及び公衆ネットワークに使用することができる。公衆ネットワークは、通常、インターネットサービスプロバイダー又はテレコムオペレータによって動作される。公衆ワイヤレスアクセスネットワークの共通の場所は、空港やホテルや駅等のホットスポットである。この場合に、公衆ネットワークオペレータは、勘定の目的でユーザを確実に認証できねばならない。更に、ネットワークは、IPレベルにおいてセキュリティを与えねばならない。

業務用ローカルエリアネットワーク(LAN)は、本発明のシステムにとって別の興味深いアプリケーションエリアを形成する。ここでは、システムは、既存の固定LANインフラストラクチャーに対するワイヤレス拡張を与える。典型的な会社のLANは、イーサネット配線をベースとする。それ故、このような実施においては、アクセスポイントがイーサネットを経てMルータ52に接続される。Mルータは、固定ターミナル及び移動ターミナル4の両方の働きをすることができる。添付図面の図3は、種々の送信リンク態様を示す。

【0025】

データ平面

OSIデータ層レベルにおけるシステムの一般的なアーキテクチャーについて説明する。

本発明の好ましい実施形態では、Mルータ52は全TCP/IPスタック機能を有する。これは、パケットをRANインターフェイスへ送給する標準的なIPルート指定を実行し、そして無線流制御及びターミナル管理機能のようなワイヤレス特有の制御機能を埋め込むことができる。到来するIPパケットは、本発明により、以下に詳細に述べるように、Mルータ52において分類することができる。Mルータ52は、到来するIPパケット流を、対応するアクセスポイントを経て、適当なQoS特性を用いる移動ターミナルへ中継する。ワイヤレス拡張は、無線流、ターミナルの移動及び位置の管理を制御する。Mルータ52は、特定の制御プロトコルを用いてアクセスポイントを制御することができる。アクセスポイント5は、IP流を無線流へとマルチプレクスする。アクセスポイントは、単純なLANブリッジであってもよいし、或いは完全なIPスタック機能を実施してもよい。後者の場合には、アクセスポイントは、IPパケットヘッダを読み取ることによりI

10

20

30

40

50

P パケット Q o S クラスを分類することができ、それ故、I P Q o S クラスを、以下に述べるように、対応する Q o S クラスをもつ対応する無線サービス待ち行列へとマッピングすることができる。アクセスポイント 5 は、I P パケットを、無線リンクパケットに適合するセグメントにセグメント化したり再組立したりする。セグメント化及び再組立 (S A R) ブロックは、移動ターミナル 4 と M ルータとの間のセグメント化を取り扱う。

【0026】

移動ターミナル 4 は、全ての標準的な T C P / I P エンティティ及びワイヤレス特有の制御サービスを含む。制御メッセージは、制御プロトコルを用いて M ルータ 5 2 とターミナル 4 との間で透過的に送信される。図 4 は、データ経路アーキテクチャーを示す。

送信リンク態様

システムは、アクセスポイントを移動ルータへ接続するための別々の物理的な送信リンクを与え、例えば、A T M 及びイーサネットを展開することができる。ここで、A T M は、制御シグナリングをもたない物理的リンクを指す。この場合に、A T M は、セグメント化及び再組立、並びに I P トラフィックに対する送信サービスしか与えない。公衆オペレータが所有する公衆テレコミュニケーションネットワークに対して A T M オプションが意図され、一方、上述したように、イーサネットは、専用ワイヤレス業務用 L A N に対する理想的な解決策を与える。図 5 は、これら 2 つの送信リンクオプションを示す。

【0027】

イーサネットの場合には、隣接アクセスポイントは、通常、ルータに接続された同じイーサネットセグメントに属する。同じイーサネットセグメント内のアクセスポイントは、同じ I P サブネットワークアドレスを有する。それ故、それらは、1 つの I P サブネットワーク (移動ドメインと称する) より成る。同じルータは、個別の I P ドメインに位置する固定ネットワーク要素を制御することができる。アクセスポイントを異なるルータポートにインストールし、そして異なる I P ネットワークアドレスをもつ多数の移動ドメインを形成することもできる。図 6 は、それにより形成されるアーキテクチャーを示す。

添付図面の図 7 は、A T M の場合のパケットカプセル化を示す。A T M リンクでは、M ルータのポートがアクセスポイントを独特に識別する。I P パケットは、M ルータと移動ターミナルとの間で A A L 5 フレームへとカプセル化される。A A L 5 層は、パケットを 4 8 ビット長さの A T M セルペイロードにセグメント化する。この場合、アクセスポイントは、A T M セルを M ルータへ透過的に通過させる。

【0028】

添付図面の図 8 は、イーサネットの場合のパケットカプセル化の一例を示す。イーサネットリンクにおいては、I E E E M A C アドレスを使用して、アクセスポイント及び M ルータポートが識別される。M ルータ及び移動ターミナルは、I P パケットをイーサネットフレーム内にカプセル化する。パケットは、イーサネット層へ通される前に、I P / イーサネット収斂層に通される。この収斂層は、I P パケットヘッダ及び要求された I P Q o S を照合し、そしてパケットをそれに対応する R A N 待ち行列へとマップする。I P パケットとイーサネットヘッダの間には専用の流れラベルが追加され、その概念は、公告されたフィンランド特許出願 F 1 9 8 0 1 9 1 号の要旨である。その内容は、参考としてここに取り上げる。収斂層は、I P パケットを無線アクセスネットワーク特有の R A N 識別子 (R A N _ I D) でマークする。A T M の場合には、R A N _ I D は、V P I / V C I 値に対応し、一方、イーサネットは、M ルータにより割り当てられたランダム識別子を使用する。この流れラベルは、A T M 仮想経路識別子に対応し、従って、I E T F 多プロトコルラベルスイッチング (M P L S) 概念に類似している。流れラベルは、イーサネットパケットを正しい無線流へとマルチプレクスするアクセスポイントにおいてデコードされる。無線流とイーサネットフレームとの間のマッピングは、収斂層において行なわれる。

【0029】

図 9 は、R A N _ I D の例示的構造と、本発明の実施形態による無線流へのマッピングとを示す。

10

20

30

40

50

A T M送信リンクを使用する場合には、流れマッピング及びR A N __ I D (V P I / V C I) の使用は平凡なものであり、図 1 0 は、この場合のパケットカプセル化を示す。

別のイーサネットベースの解決策は、アクセスポイントにおいてI P Q o S と無線Q o S との間のマッピングを直接実行することである。この場合に、無線流識別子は必要とされない。アクセスポイント及び移動ターミナルは、I P プロトコルスタックを実施し、従って、到来するI P パケットヘッダのサービスフィールドの形式を読み取ることができる。要求されたI P Q o S クラスに基づいて、アクセスポイント/移動ターミナルは、データパケットを、それに対応する無線サービス待ち行列へとマルチプレクスする。このモデルでは、種々の接続がエアインターフェイスにおいて区別されない。

【 0 0 3 0 】

I P 流管理の概要

インターネットプロトコルは、無接続パケットデータシステムを実施する。データはパケット内に保持され、そのヘッダは、正しい行先アドレスを指示する。この送信構成は、システムが種々の接続を分離できるようにするものではない。接続を検出する唯一の可能性は、M ルータ 5 2 / 移動ターミナル 4 内でI P トラフィックを監視し、そしてI P 流と称するI P パケット流を検出及び分類するよう試みることである。I P 流は、2つのホスト(アプリケーション)が互いの間でI P パケットを頻繁に(規則的に)送信する場合に確立される。流れ分類については、以下に詳細に説明する。ネットワークは、流れに対する幾つかのQ o S 特性を指定することができ、これは、I P ネットワークにおけるマルチメディアサービスの実施に必要とされるものである。

【 0 0 3 1 】

本発明の機構は、エアインターフェイスにおいてI P パケットのQ o S 特性を維持し、そして無線リンクにおいて異なるI P パケット(流)のプライオリティを決めることができる。この概念は、移動ターミナルとアクセスポイントとの間に形成される無線流を展開することができる。この場合に、特定の無線流識別子を使用することができる。別の機構は、I P 形式のサービスパラメータから異なる無線レベルスケジューリング待ち行列への直接的なマッピングを実行することである。後者の解決策は、I P 又は無線流を使用する必要がない。好ましい実施形態における特定の別の流れ管理の概要は、次の通りである。

【 0 0 3 2 】

M ルータ 5 2 は、到来するI P パケットのヘッダを監視し、そしてI P v 6 流れラベル及び/又は行先及びソースI P / I P v 6 アドレス及びポートを用いて既存のI P 流(即ち規則的なパケット流)を分類するよう試みる。M ルータは、それがI P 流を検出した場合に、その流れに属するパケットを特定のR A N __ I D (無線アクセスネットワーク識別子)でマークし始める。ルータは、各検出された流れに対して独特のR A N __ I D を割り当てる。R A N __ I D は、無線アクセスネットワークにおいてI P 流に属するパケットを分離するのに使用される。従って、R A N __ I D の使用は、R A N を横切ってI P 流がバックされるところの「仮想接続」を形成する(M T - M ルータ)。R A N __ I D は、A T M V P I / V C I 識別子に対応する。R A N 識別子を管理するためのワイヤレス流れ管理プロトコル(W F M P)が上記出願中の特許出願に開示されている(付録 1)。ターミナル 4 及びM ルータ 5 2 は、両方とも、ワイヤレスリンクを経てピア対ピアで通信するW F M P エンティティを有する。W F M P は、実際には、収斂層の機能を発揮する。M ルータW F M P は、流れを検出し、R A N __ I D を割り当て、そして移動ターミナルのW F M P に指定のI D 値を指定する。オーバーヘッドを最小にするために、R A N __ I D は、短い無線流識別子に圧縮することができる。

【 0 0 3 3 】

上述したように、無線リンクは、Q o S 及びスループットに関するボトルネックである。本発明は、この好ましい実施形態において、異なるサービス特性をもつ若干の無線スケジューリング待ち行列を備えたシステムを提供して広帯域サービスに対するワイヤレスサポートを改善することにより、この問題に対処する。無線サブシステムは、種々の無線待ち行列、即ち無線Q o S クラスを異なる仕方で行き扱う。無線サブシステムは、例えば、

10

20

30

40

50

到来するトラフィックに関して3つの別々のバッファ待ち行列、即ちリアルタイムトラフィックのための高プライオリティ待ち行列、非リアルタイムデータのための中間プライオリティ待ち行列、及び最良努力データのための低プライオリティ待ち行列を有することができる。2つの別の機構は、IPパケットのQoS要求を無線レベルQoS機能へとマッピングするのに使用でき、即ちIPパケットの直接的QoSマッピング又は無線流ベースのQoSマッピングである。

【0034】

直接的QoSマッピング

直接的QoSマッピング機構においては、アクセスポイント及び移動ターミナルは、エ
10
アインターフェイスを経て送信されるべきIPパケットのヘッダを分類する。この解決策では、全てのIPパケットが独立して処理される。アクセスポイント又は移動ターミナル、即ち無線リンクのエンドポイントは、無線リンクプロトコルの構造体内で送信されるべきIPパケットをカプセル化する。無線リンクサービス待ち行列は、オリジナルIPパケットのサービスフィールドの形式の値(diffs.ビット)に基づいて選択される。この値に基づいて、IPパケットは、それに対応するスケジューリング待ち行列、例えば、異なるサービス特性及び送信プライオリティを有するリアルタイム、中間プライオリティ又は最良努力データ待ち行列へとマッピングされる。

【0035】

無線流IPベースのQoSマッピング

上述したように、本発明のシステムは、直接的QoSマッピング又はIP流検出の考え
20
方を使用して、無線アクセスネットワークにおける接続を管理する。IP流マッピングの考え方は、最良努力IPトラフィックからIP流を分離して、流れを異なる仕方で処理できるようにすることである。異なる処理とは、検出された流れに異なるプライオリティ(QoSクラス)を与えることができ、そして検出された流れを圧縮して、無線リソースを節約できることを意味する。

流れベースのQoSマッピングに関する本発明は、異なるQoSクラスに対して固定チャ
30
ンネルを設けることにある。この実施形態では、各移動ターミナルは、最良努力トラフィックに対して1つと、中間プライオリティトラフィックに対して1つと、高プライオリティトラフィックに対して1つの、3つのデフォルト無線チャンネルを有する。全てのデフォルトチャンネルは、MルータWFMPモジュールで終わる(n対1関係)。デ
35
フォルトチャンネルに加えて、移動ターミナルは、検出された流れをもつことができる。図16は、異なる流れがネットワーク内でいかにルート指定されるかを示す。この図は、2つの移動ターミナルが2つのアクセスポイント(APインターフェイスしか示されていない)を経てMルータに接続される簡単なネットワークアーキテクチャーを示している。各MTは、3つの異なる無線レベルのQoS待ち行列を有する。Mルータ及び移動ターミナル側のオペレーションについて説明する。

【0036】

IP流ベースのマッピング機構においては、Mルータが流れを確立する。又、システム
40
は、移動ターミナルが、特定のIP流に対して所与のプライオリティを有する無線流(RAN_ID)を確立するように、Mルータに要求できるようにする。Mルータは、IP流を分類するときに、確立された無線流に対して対応するプライオリティクラスを指定する。IP流の形式及びトラフィック特性に基づいて判断がなされる。種々の無線流プライオリティがワイヤレス広帯域サービスを可能にする。

【0037】

検出されたIPレベル流のみが別々の無線流へスイッチングされる。他のIPパケット
50
は、最良努力データとしてエアインターフェイスを経て送信される。この実施形態の基準システムは、非流れパケットを送信するのに使用される固定(ハードコード化)の無線流識別子を定義するか、又はそれらの流れに対して流れ識別子を動的に指定することができる。基準システムは、各無線プライオリティ待ち行列に対して1つずつ、3つのマルチプレクスされた無線流をターミナルごとに与える。上述したように、これらの「デフォルト

ト」無線流は、本発明により、IPドメイン間移動及び差別化サービスに対するサポートを改善するために形成される。好ましい実施形態の構成においては、Mルータ52又はターミナル4は、単一IPパケットのプライオリティビットを見て、それに対応無線QoS（プライオリティ）と共に送信することができる。次いで、IP流が検出されるや否や、パケットを、あるQoS及びIPヘッダ圧縮を伴う個別の無線流にスイッチングすることができる。図12は、IP流に対して定められた流れ管理概念の概要を示す。検出されたIP流は、専用のRAN__IDラベルでマークされる（ATM VPI/VCIにおいて）。アクセスポイントは、RAM流-無線流マルチプレクシング、即ちRAN__IDとMVCとの間のマッピングを実行する。Mルータは、MTの位置を管理すると共に、移動ターミナルがアクセスポイント間のハンドオーバーを実行する場合にルートテーブルを更新する。個別無線流の使用に関する特別な効果は、IPヘッダ圧縮機構（図12のFCブロック）を適用できることである。

10

【0038】

IP流マルチプレクシング

図13及び14は、ダウンリンクトラフィックに対する流れ管理手順を示す。このプロセスは、次の通りである。

Mルータは、到来するトラフィックを連続的に監視する。IP流（あるホスト（ポート）間の）当たりのパケットの量がスレッシュホールド値（時間当たり）を越えたときには、WFMPは、RAN流を確立し、そしてそしてそれに新たなRAN__IDを割り当てる。次いで、その流れに属するパケットが、その割り当てられた流れ特有のRAN__IDを用いて、流れ圧縮（FC）によってアクセスポイントへ通される。本発明によれば、いずれの流れにも属さないIPパケットは、差別化を与えるために3つのデフォルトRAN__IDの1つでマークされる。

20

【0039】

FCエンティティは、検出された流れのIPヘッダを圧縮し、そしてそれにより得られたパケットにRAN__IDをコピーする。受信端では、ピアFCエンティティは、RAN__IDをデコードすることにより正しいソースを検出し、そして欠落IPヘッダを指定した後に、パケットを上位層に通することができる。検出されたIP流のみが圧縮される。

この実施形態では、アクセスポイント51、51'は、MVC（無線流）を正しいRAN__IDへとマッピングする変換テーブルを有する。Mルータ52は、アクセスポイント当たりのRAN__IDアドレススペースを割り当てる。次いで、パケットは、RAN__ID「流」と共にMルータへ送信される。次いで、パケットは、無線リンクへ送信される。デフォルトRAN__IDには、固定無線リンクプライオリティが指定される。この実施形態では、ユーザデータとして3つのデフォルト「パイプ」（RAN__ID）、即ちリアルタイム流、非リアルタイム流及び最良努力流が存在する。もちろん、要求に応じて、別の数のデフォルトチャンネルを使用することもできる。例えば、混雑がこのような問題になり難いある場合や、多数のQoS特性への更なる分離が必要となる他の環境においては、高いプライオリティ及び低いプライオリティの2つのチャンネルで充分である。各チャンネル即ちパイプは、予め構成されたRAN__IDを有する。非流れIPTrafficは、圧縮を伴わずにこれらの流れの中で送信される。

30

40

【0040】

アクセスポイント（層1及び層2）の無線は、RAN__ID当たり独特のMVC値を割り当てる。又、エアインターフェイスにおいて非圧縮トラフィックに対して3つのデフォルトMVC「パイプ」が存在する。デフォルトRAN__IDは、それに対応するハードコード化MVCへとマッピングされ、一方、圧縮されたIP流は、専用のMVC接続へとスイッチングされる。異なる流れは、エアインターフェイスにおいて、MVC及びターミナルワイヤレスMACアドレスを使用して分離される。

この実施形態の移動ターミナル4においては、その無線モデムが、受信したMVCをそれに対応するRAN__ID値に変換し、そしてパケットをSAR層へ通し、SAR層は、データを、RAN__ID情報を依然として維持するIPパケットへと再組立する。圧縮さ

50

れた流れは、次いで、FCへ通され、FCは、RAN_IDを識別すると共に、正しいIPヘッダ情報を追加する。デフォルトRAN_IDトラフィックは、WFMPへ直接通される。

【0041】

プロトコルアーキテクチャ

本発明の好ましい実施形態の詳細なシステムアーキテクチャが図15に示されている。主たる外部インターフェイスを以下のテーブルに示す。

テーブル1：外部制御インターフェイス

<u>IF#</u>	<u>インターフェイス</u>	<u>説明</u>	
1.	MMC-MMC	ターミナルとMルータとの間の移動管理メッセージ。移動管理メッセージは、新たなターミナルがネットワークに登録されるとき及びハンドオーバーの場合に使用される。	10
2.	WFMP-WFMP	流れ管理制御シグナリングメッセージ。これは、無線流を確立及び解除するためのものである。	20
3.	MCP-MCP	移動制御プロトコル(MCP)は、移動ターミナルとMルータとの間にWFMP及びMMCメッセージを送信するための信頼性の高いピア対ピアプロトコルを与える。MCPは、全てのワイヤレス特有のシグナリングに使用される。	30
4.	無線制御 メッセージ	無線制御メッセージは、無線リンク制御メッセージを送信するのに使用される。例えば、ターミナル関連及び無線流(MVCレベル)制御シグナリングがここに保持される。	40
5.	APCP インターフェイス	アクセスポイント制御プロトコル(APCP)は、アクセスポイントと移動ルータとの間で無線リンク制御及び無線リソース管理メッセージを送信するのに使用される。	

【0042】

外部制御インターフェイスは、移動ターミナル4と無線アクセスネットワーク(アクセ

スポイント 5 1、5 1'、M ルータ 5 2) との間、及び無線アクセスネットワーク 2 とコアネットワーク 3 との間 (A P - M ルータ) の論理的インターフェイスを定義する。異なる製造者からの装置で構成できる互換性のある標準システムを定義することが目標である場合には、外部インターフェイスを標準化しなければならない。

標準的なインターフェイスに加えて、システムは、以下のテーブルに示す多数の重要な内部制御インターフェイスも有する。

【 0 0 4 3 】

<u>I F #</u>	<u>インターフェイス</u>	<u>説明</u>
--------------	-----------------	-----------

40

8. ワイヤレスQoS ワイヤレス特有のQoSコントローラは、R
 コントローラーR SVPモジュールと対話して、リソース指定
 SVPインターフ を得ると共に、それらを無線リソース指定及
 ェイス び無線QoSに変換する。R SVPモジュ
 ールは、このインターフェイスを経てQoSマ
 ネージャーからあるQoSを要求する。 10
9. ワイヤレスQoS このインターフェイスは、ハンドオーバーの
 コントローラーM 場合に使用される。MMCモジュールは、Q
 MCインターフェ oSコントローラにハンドオーバーについて
 ェイス 通知し、そしてワイヤレス流を再確立するよ
 うにQoSコントローラに要求する。この確
 立要求は、次いで、WFMPエンティティへ 20
 送られる。

【0044】

システムアーキテクチャーは、本発明の好ましい実施形態特有の次の機能的ブロックを備えている。

QoS - ワイヤレスQoSコントローラ：このエンティティは、IPパケットに対して無線リンクQoSを割り当てる。QoSコントローラはH.323及びRSVPブロックへのインターフェイスを有し、これは、IP流に対して遅延、帯域巾といった明確なQoS要求を与えることができる。明確なQoSパラメータが得られない場合には、QoSマネージャーは、DSフィールド（区別化サービス）又はポート情報（標準アプリケーション）に基づいてQoSを指定する。WFMPは、流れを検出すると、Mルータ - QoSエンティティに、評価されたパケットスループットを通知し、この情報は、無線リンクQoSを割り当てるように展開することもできる。QoSコントローラは、割り当てられた無線リンクQoS値をWFMPエンティティへ送信し、このエンティティは、次いで、選択されたQoSを伴う無線流を確立する。又、QoSコントローラは、WFMPを経てQoS更新メッセージを送信することもできる。QoS更新メッセージを使用して、QoSコントローラは、既存の流れに対して無線QoS値を変更することができる。この機能は、H.323又はRSVPパラメータが接続中に変化する場合にも有用である。 30

【0045】

移動管理コントローラ（MMC）：MMCエンティティは、ターミナル移動管理の役目を果たす。Mルータ - MMCは、登録されたターミナル及びそれらの現在位置（アクセスポイント）の情報を含むデータベースを有する。ターミナルの登録中に、MMCは、ユーザを認証するのに使用できる。移動ターミナルMMCは、Mルータ - MMCにハンドオーバー要求メッセージを送信することによってハンドオーバーを開始し、Mルータ - MMCは、新たなアクセスポイントにおける無線リソースをチェックし、そして新たなアクセスポイントに新たな無線流を確立しそして古い無線流を解除するようにWFMPに要求する。 40

【0046】

ワイヤレス流れ管理プロトコル（WFMP）：WFMPエンティティは、無線流を管理する。これは、IPトラフィックを検出しそしてIP流を分類する。WFMPは、新たな 50

流れを検出すると、流れ情報をQoSコンとロータに通し、該コントローラは、その流れに対し正しい無線リンクプライオリティを指定する。次いで、WFMPは、割り当てられたプライオリティをもつ無線流を確立する。WFMPは、RAN_IDを割り当て、そしてアクセスポイントRAN_ID、即ち無線流テーブルを更新する。Mルータは、流れを分類して全ての既存流のデータベースを維持するマスターWFMPを備え、一方、移動ターミナルは、RAN_IDを正しい無線流へとマルチプレクスする簡単なWFMPエンティティのみを含む。MT-WFMPは、所与のプライオリティをもつ新たな無線流を確立するようにMルータ-WFMPに要求することができる。これは、例えば、MT-H.323が明確なQoSをもつ流れを要求する場合である。又、ルータ間ハンドオーバー手順は、この機構を使用して、ハンドオーバー後に、移動ターミナルと新たなMルータとの間の流れを迅速に設定することができる。

10

【0047】

移動制御プロトコル(MCP)：MCPプロトコルは、移動ターミナルとMルータとの間にWFMP及びMMCメッセージを送信する。MMCは、制御情報を送信するための信頼性の高い機構を形成する。MMCは、簡単な「Nだけ戻る(go-back-N)」形式の再送信プロトコルを実施する。制御メッセージの信頼性の高い送信を保証するために、TCP/IPを使用するのではなく、個別の下位層プロトコルが追加されている。TCP/IPは、制御メッセージを他のTCPトラフィックから分離することができない。それ故、例えば、ハンドオーバーの場合には、制御メッセージがユーザデータトラフィックと混合され、これは、ハンドオーバー手順に対する著しい遅延及び接続の再確立を生じさせる。MCPのユーザは、ユーザデータパケットの前に全ての制御トラフィックをプライオリティ決めすることができる。

20

【0048】

流れ圧縮(FC)ブロック：Mルータ及び移動ターミナルは、検出されたIP流を圧縮するFCエンティティを備えている。流れ圧縮は、分類されたIP流に対してのみ使用される。他のIPトラフィックは、圧縮されずに送信される。

無線リソースマネージャ(RRM)：各アクセスポイントは、特定のアクセスポイントの無線リソースを管理するRRMエンティティを有する。本発明のシステムでは、WFMPは、新たな流れが確立されるたびにRRMにリソース待ち行列を送信する。WFMPは、要求された無線流プライオリティ(QoSにより割り当てられた)及び推定された流率(WFMP評価)を送信する。この情報に基づいて、RRMは、接続が受け入れられるかどうかを判断する。RRMは、各アクセスポイントが無線リソースを動的に管理するための機構を形成する。RRMは、推定された流率を、要求された無線流の空き容量と比較する。十分な容量が得られない場合には、RRMは、低いQoSを使用するようにWFMPに提案することができる。WFMPは、要求されたQoSより低い戻りQoS値を得ると、接続の確立を停止するか又は低いQoSで続行することができる。IPの場合には、RRM容量計算は、主として、推定流率(Mルータ)に基づく。RSVP及びH.323シグナリングのみが明確なスループット及び遅延要求を与え、これは、RRMに直接マップすることができる。

30

【0049】

アクセスポイント制御プロトコル(APCP)：APCPプロトコルは、アクセスポイントとMルータとの間に制御メッセージを送信するための機構を形成する。APCPは、TCP/IPスタックの上部に配置することができ、これは、制御メッセージの信頼性ある送信を保証する。WFMPは、RRM待ち行列に対してAPCPを展開し、流れ制御情報を無線サブシステムに送信する。

40

システムの詳細な機能について以下に説明する。

IP流の管理

上述したように、本発明のシステムは、IP流を検出して無線アクセスネットワークの接続を管理するという考え方を使用する。この考え方は、IP流を最良努力IPトラフィックから分離して、流れを異なる仕方で「処理」できるようにする。異なる処理とは、検

50

出された流れに異なるプライオリティ（ＱoSクラス）を与えることができ、そして検出された流れを圧縮して、無線リソースを節約できることを意味する。

【0050】

本発明は、少なくとも2つの異なるＱoSクラスに対してデフォルトチャンネルを設けることにある。この実施形態では、各移動ターミナルは、最良努力トラフィックに対して1つと、中間プライオリティトラフィックに対して1つと、高プライオリティトラフィックに対して1つの、3つのデフォルト無線チャンネルを有する。全てのデフォルトチャンネルは、ＭルータWFMPモジュールで終わる（ n 対1関係）。デフォルトチャンネルに加えて、移動ターミナルは、検出された流れをもつことができる。検出された流れの他端がＩＰコアネットワークに位置する場合には、流れがＭルータ圧縮モジュールで終わる（全ての流れが圧縮される）。対応ノードが別の移動ターミナルである場合には、流れがＡＰインターフェイス間で直接的にスイッチングされる。図16は、異なる流れがネットワーク内でいかにルート指定されるかを示す。この図は、2つの移動ターミナルが2つのアクセスポイント（ＡＰインターフェイスしか示されていない）を経てＭルータに接続される簡単なネットワークアーキテクチャーを示す。各ＭＴは、デフォルトチャンネル（それらの3つ）と、ＩＰネットワークへの1つの流れと、移動ターミナル間でスイッチングされる1つの流れとを有する。

10

次いで、WFMP流れ管理機能について詳細に説明する。Ｍルータ側及び移動ターミナル側の両方の動作について説明する。

【0051】

20

流れ分類

WFMPは、流れを検出すると共に、ネットワークと移動ターミナル／無線接続との間にＩＰパケットをルート指定するという役割を果たす。流れ検出を取り扱う機能を「流れクラシファイア(classifier)」と称する。この流れクラシファイアは、ＩＰパケットが流れに属するときを判断し、そしてこの判断の後に、流れを無線接続に結合する。又、流れが終わるときを検出しそしてそれに対応する無線接続を解除することにも必要である。

【0052】

流れ分類は、WFMPがＩＰトラフィック及び特定のヘッダフィールドを監視して新たな流れを検出するように機能する。ＩＰ及び搬送プロトコルヘッダフィールドに基づいて、次の4つの異なる流れ形式を特定することができる。

30

- 1．流れラベルにより識別される流れ（形式1）
- 2．TCP／UDPポート番号により識別される流れ（形式2）
- 3．ソース及び行先ＩＰアドレス＋セキュリティパラメータインデックスにより識別される流れ（形式3）
- 4．ソース及び行先ＩＰアドレスにより識別される流れ（形式4）

【0053】

第1のオプションは、アプリケーションがＩＰv6流れラベルを使用して異なるＩＰセッションをマークできる場合に適用できる。このような進歩型アプリケーションが使用できずそしてTCP／UDPポート情報が使用できる場合には、流れ形式2が選択される。ＩＰ暗号化が使用される場合には、ポート情報が暗号化されるので、第2のオプションを適用することができない。このような場合には、セキュリティパラメータインデックス（SPI）がソース及び行先アドレスと共に使用され、考えられる流れが識別される。TCP／UDPポート情報、流れラベル又はSPIパラメータが使用できない場合には、唯一のオプションは、ソース及び行先ＩＰアドレスのみを探して、ホスト間で流れを分離することである（最初の2つのオプションは、ＩＰセッション／プロセス間で流れを分離する）。

40

【0054】

各流れ形式は、流れを識別するのに使用されたＩＰパケットヘッダから1組のフィールドを指定する。特定の流れを識別する1組のヘッダフィールドは、流れ識別子と称する。流れの形式に基づき、流れ識別子は、次のフィールドを含む。

50

- 形式 1 : ソースアドレス + 行先アドレス + 流れラベル
- 形式 2 : ソースアドレス + 行先アドレス + プロトコル (次のヘッダ) +
ソースポート + 行先ポート
- 形式 3 : ソースアドレス + 行先アドレス + セキュリティパラメータ
インデックス (S P I)
- 形式 4 : ソースアドレス + 行先アドレス

【 0 0 5 5 】

W F M P は、これら 4 つの流れ形式間を区別化することができ、そして流れ分類機構に基づいて、各流れ形式の流れに結合する。本発明のシステムに適用することのできる 3 つの異なる流れクラシファイア機構は、次の通りである。

- X / Y クラシファイア : これは、Y 秒間に X 個のパケット (同じ流れ識別子をもつ) があって、新たな流れを生じることを意味する。
- プロトコルクラシファイア : これは、全ての T C P パケットの流れに単に指定する。
- ポートクラシファイア : これは、搬送層ポート番号を使用して、どの流れを結合するか判断する。

X / Y クラシファイアは、流れ形式 1 及び 2 をサポートする唯一のものであるので、好ましい選択肢である。

【 0 0 5 6 】

流れ検出基準

X / Y クラシファイアに対する典型的な流れ検出基準は、以下の「テーブル 3 X / Y クラシファイアの推奨」に示されている。このテーブルは、異なる量の使用可能な流れスペースの関数における X 及び Y の値を示す (この場合、流れスペースとは、必要とされる無線接続の量を指す) 。予想性能は、流れに対してスイッチングされるパケットの部分を意味する。

明らかなように、値は、異なる環境において若干相違する。それ故、W F M P の実施において X 及び Y の値を容易に変更できねばならない。

【 0 0 5 7 】

10

20

テーブル3 X/Yクラシファイアの推奨

所要流れ

スペース	ゲートウェイ	大学/企業バックボーン	
1 K	クラシファイア: X=5/Y=15秒 流れ検出遅延: 30-120秒 予想性能: 85%	クラシファイア: X=40/Y=40秒 流れ検出遅延: 30-60秒 予想性能: 79%	10
2 K	クラシファイア: X=5/Y=60秒 流れ検出遅延: 30-120秒 予想性能: 90%	クラシファイア: X=10/Y=45秒 流れ検出遅延: 30-60秒 予想性能: 89%	
8 K	クラシファイア: X=2/Y=60秒 流れ検出遅延: 30-120秒 予想性能: 93%	クラシファイア: X=5/Y=60秒 流れ検出遅延: 30-60秒 予想性能: 92%	20
16 K	クラシファイア: X=2/Y=60秒 流れ検出遅延: 30-120秒 予想性能: 93%	クラシファイア: X=2/Y=60秒 流れ検出遅延: 30-60秒 予想性能: 95%	
32 K	クラシファイア: X=2/Y=60秒 流れ検出遅延: 30-120秒 予想性能: 93%	クラシファイア: X=2/Y=60秒 流れ検出遅延: 30-60秒 予想性能: 95%	30
∞	クラシファイア: 全パケット 流れ検出遅延: ∞ 予想性能: 99%	クラシファイア: 全パケット 流れ検出遅延: ∞ 予想性能: 98%	

【0058】

TCP接続の確立は、常に、少なくとも3つの使用パケットを含み、そして流れ検出は、実際のデータパケットに基づいて行わねばならないので、Xに対して最小値6が適当であると考えられる（第3データパケットが流れ検出をトリガーする）。Yの値は、30秒となる。

流れ削除

流れは、ある一定秒数のインアクティビティの後に削除される。流れクラシファイアは、それが新たな流れを検出すると、流れインアクティビティタイマーをスタートさせる。このタイマーは、その流れに属するパケットを受け取るたびに再スタートされる。タイマーが時間切れすると、監視されたパケットのリストから流れ識別子が除去される。最終的に、WFMPは、RAN及び移動ターミナルの両方から流れを解除する。

【0059】

R S V P 指定された流れ

R S V Pを使用してネットワークからリソースを指定するときには、MルータのR S V Pモジュールは、移動特有のモジュールと通信して、無線アクセスネットワークからリソ

40

50

ースを指定する必要がある。RSVPモジュールは、QoSマネージャーへのインターフェイスを有し、そしてこのインターフェイスを経て、QoSマネージャーにワイヤレスリソースをチェックするよう求める。RSVP要求をQoSクラスへ変換した後に、QoSマネージャーは、APからの接続を指定するようにWFMPに要求する。この要求(WFMP内で流れ形式5により識別される)は、流れクラシファイアにおける流れ検出を自動的にトリガーする。

【0060】

流れ識別子は、フィルタスペック及びセッションパラメータにおいてRSVPにより与えられる。フィルタスペックは、ソースIPアドレス及びソースポート/流れラベル値より成る。セッションは、行先IPアドレス、プロトコルID及び行先ポート値を含む。フィルタスペック及びセッションパラメータにより搬送される情報は、WFMPへ与えられ、従って、これは、RSVP指定された流れに属する実際のデータパケットを識別することができる。この情報を使用して、WFMPは、特定のRSVP流に属するデータパケットを正しいRAN接続にルート指定することができる。RSVP-移動IPのアドレッシング問題が解決されると仮定する。この問題は、訪問先ネットワーク内の移動ターミナルがケア・オブ・アドレスにより識別されそしてRSVPがホームアドレスを使用する場合に生じる。このような場合には、RSVPにより与えられる流れ識別子が、データパケットにより搬送される識別子に一致しない。従って、REVP指定された流れに属するパケットは、識別もできないし、正しい無線流ヘルート指定することもできない。

【0061】

WFMP検出される流れと同様に、RSVP流は、流れクラシファイアにより監視される。監視は、流れを解除しなければならないときを検出するために必要とされる。別のオプションは、RSVPがQoSマネージャーモジュールに破壊(teardown)メッセージを送信することにより流れを明確に解除することである。次いで、QoSマネージャーは、APから流れを解除すべきことをWFMPに通知する。RFC2205は、次のことを言う。「古い指定を明確に破壊する必要はないが、アプリケーションが終了するや否や全てのエンドホストが破壊要求を送信することを推奨する。」この不確実さのために、RSVPシグナリングによるか又は時間切れにより(インアクティビティタイマーの時間経過後)流れを解除できねばならない。

【0062】

流れマッピング解決策における差別化サービスパケットの取り扱い

WFMPは、各IP流において要求されたIP形式のサービスビット(DCフィールド)を検出し、そしてこの流れに属するパケットを、DSフィールドに保持された値に基づいて処理することができねばならない。各DiffServパケットは別々に取り扱われ、そして更に、DiffServパケットに対して流れ検出/監視を行って、流れを検出する。

WFMPは、流れに属さないDiffServパケットを受信すると、DSフィールドの値を読み取り、そして正しいデフォルト流、例えば、(最良努力/中間プライオリティ/リアルタイムトラフィック)を選択する。WFMPは、DSフィールド値と、所定のRAN流、即ちデフォルト流との間をいかにマッピングするかの知識を有する。この知識は、QoSマネージャーモジュールとの相互作用を最小にするようにWFMPにおいて静的に構成され、即ちWFMPは、DiffServパケットを受け取るたびにQoSモジュールに相談する必要はない。

【0063】

Mルータ52における流れ管理

この好ましい実施形態では、Mルータは、流れを検出しそしてRAN流れ識別子を管理するという役割を果たす。又、これは、無線接続を形成及び除去するときに通る無線アクセスネットワークへの、そして新たな流れに対するQoSクラス及び帯域巾推定を検索するためのQoSマネージャーへのインターフェイスも有する。

WFMPは、流れ管理のための2つのテーブル、即ちアクティブ流テーブル(AFT)

及びデフォルト流テーブル (D F T) を使用する。テーブルの詳細な構造は、図 1 7 に示す。A F T は、全ての検出された流れを管理するのに使用され、一方、D F T は、各登録される移動ターミナルのエントリーを含む。デフォルト流テーブルは、非流れ及び D i f f S e r v パケットを移動ターミナルヘルト指定できるようにする。

【 0 0 6 4 】

アクティブ流テーブルは、各検出された流れに対するエントリーを有する。流れの形式に基づいて、正しい I P ヘッダ値が A F T に記憶される (流れ形式及びそれに対応するパラメータについては、第 0 章を参照) 。 I P ヘッダ値に加えて、R A N 流識別子 (R A N _ I D) 及び A P インターフェイス値が A F T に記憶される。考え方としては、流れ形式及びそれに対応する I P ヘッダ値が一致したときに、W F M P が R A N _ I D 及び A P _ i f 値をテーブルから読み取り、そしてパケットを正しい R A N 流に送り込むというものである。

10

【 0 0 6 5 】

デフォルト流テーブルは、非常に簡単なものであり、移動ターミナル識別子 (移動ターミナル I P アドレス) と、R A N _ I D 及び A P インターフェイス値しか含んでいない。各デフォルト流に対して 1 つの R A N _ I D 値があり、即ち B E トラフィックに対する R A N _ I D _ 1 と、中間プライオリティトラフィックに対する R A N _ I D _ 2 と、高プライオリティトラフィックに対する R A N _ I D _ 3 である。これらの値は、移動登録中に W F M P により選択される。到来する I P パケットに対して A F T からのエントリが見つからない場合には、パケットが D F T に対して比較される。行先又はソース I P アドレスが移動ターミナル識別子に一致すると、W F M P は、正しい R A N _ I D (R A N _ I D _ 1 がデフォルト選択である) と、A P インターフェイス値を D T F から読み取り、そしてパケットを正しい無線流に送り込む。非流れパケットが特定の取り扱いを要求する場合は、R A N _ I D _ 2 又は R A N _ I D _ 3 が選択される。

20

【 0 0 6 6 】

ダウンリンクにおける流れ管理

先ず、通常の I P ルート指定方法が適用され、そして到来する I P パケットが正しい I P アプリケーション / インターフェイスにルート指定される。I P パケットをルート指定するときには、次のルールに従わなければならない。

1 . パケットが M ルータ自体 (例えば、ピン (ping)) にアドレスされた場合には、それが通常のやり方で処理される。

30

2 . 個別の R S V P は、他の I P パケット (R S V P プロトコル番号 4 6 で識別された) からのパケットを制御する。

3 . 移動ターミナルにアドレスされたパケットは、W F M P プロセスへ送信される。

【 0 0 6 7 】

次に、W F M P の動作を詳細に説明する。

W F M P は、到来する I P パケットに対して正しい R A N 接続を選択する必要がある。パケットが流れに属さない場合には、W F M P は、正しい最良努力チャンネルのみを選択し、そしてパケットを S A R に送信する。パケットが、検出された流れに属する場合には、パケットが圧縮モジュールへ通され、このモジュールが、次いで、パケットを正しい R A N 接続へ送信する。図 1 8 は、W F M P のルート指定を明確に示す。

40

先ず、W F M P は、到来するパケットが搬送する流れ情報をチェックする。W F M P は、拡張ヘッダを含むパケットを通して進み、そして全ての当該情報をセーブする。基本的な I P v 6 ヘッダから、ソース及び行先 I P アドレスが流れラベル及びトラフィッククラス (D S フィールド) と共にセーブされる。I P パケットが、I P 暗号化が使用されていることを意味する E S P 拡張ヘッダ (カプセル化セキュリティペイロード) を搬送する場合には、セキュリティインデックスパラメータ (S P I) がセーブされる。パケットが E S P 拡張ヘッダを搬送せずそして T C P / I P ヘッダが見つかった場合には、W F M P がポート情報及びプロトコル識別子をセーブする。

【 0 0 6 8 】

50

流れ情報をセーブした後に、流れ検出の目的で流れクラシファイアが呼び出される。流れクラシファイアは、次の1つを検出する。

1. 流れが既に検出されており、従って、流れ情報のみが更新される。
2. 流れがまだ検出されておらず、流れ情報のみが更新される。
3. 流れ検出アルゴリズムが、この特定のバケットから始めて、新たな流れを形成することを決定する。

流れが検出されると、WFMPは、流れに対して新たなRAN流識別子を割り当てる。明確なQoS又はトラフィックパラメータが得られないので、WFMPは、欠落情報を得るためにQoSマネージャーと通信しなければならない。QoSクラス及び帯域巾推定を要求するときに、WFMPは、流れ識別子（流れ検出に使用される情報）及びTCP/UDPポート情報（もし得られれば）を、ある測定されたトラフィック特性と共に、QoSマネージャモジュールに与える。この情報を用いて、QoSマネージャーは、この流れに対してQoSクラス及び帯域巾推定を計算する。

【0069】

QoSマネージャーがQoSクラス及び推定された帯域巾を返送した後に、WFMPは、APからの接続を指定し、そして移動ターミナル及び圧縮モジュールに新たな流れを通知する。最終的に、WFMPは、アクティブ流テーブル（AFT）を更新する。

次いで、WFMPは、バケットを正しい無線接続にルート指定し始める。流れが検出された場合には、正しいRAN_IDをアクティブ流テーブル（AFT）から読み取ることができる。正しいRAN_IDは、流れ情報（流れ形式に基づく）及び流れ形式を、AFTにおける対応値と比較することにより見出される。これら全てのフィールドが一致したときには、WFMPがRAN_ID及びMルータインターフェイスをAFTから読み取り、そしてバケットを圧縮モジュールへ送信する。バケットを圧縮モジュールへ通すときには、RAN_IDも与えられなければならない。バケットを圧縮した後に、圧縮モジュールは、バケットを正しいRAN接続（WFMPにより与えられた）に送信する。

【0070】

AFTからのエントリーが見つからない場合には、バケットが流れに属しておらず、デフォルトチャンネルの1つにおいて送信される。正しいデフォルトチャンネルは、到来するバケットの行先IPアドレスをDFTにおける移動ターミナルのMT_id値と比較することによりデフォルト流テーブルから見出される。ネットワークに登録された各移動ターミナルは、DFTのエントリーを有する。IDが一致する（dst_addr = MT_id）と、流れクラシファイアは、対応するRAN_ID（特殊な処理が必要とされない場合にはRAN_ID_1）及びMルータインターフェイス値をDTFから読み取り、そしてバケットを正しいデフォルトチャンネルに送信する。行先IDがDFTにおけるいずれのMT_id値にも一致しない場合には、移動ターミナルがネットワークに登録されず、バケットは破棄される。

【0071】

アップリンクにおける流れ管理

無線アクセスネットワークからバケットが受信されると、それは、固定ホスト又は別の移動ターミナルのいずれかにアドレスされる。

RAN_IDにより、SAR層は、受信したIPバケットを正しいモジュールに通過させる。これは、自動的に行なわれる。というのは、各RAN接続とモジュールの1つ（SAR SAPで識別された）との間に1対1の関係があるからである。RAN接続が形成されると、結合が行なわれる。バケットが流れに属しそして行先がコアネットワーク内である場合には、バケットが、圧縮解除の目的で圧縮モジュールへ通される（図19参照）。バケットが非流れトラフィックである場合には、それがWFMPプロセスに直接通される。バケットがRSVPシグナリングである場合には、それがRSVPモジュール等に対して送信される。

【0072】

アップリンクWFMP処理は、ダウンリンク動作と若干異なり、即ちWFMPは、非流

10

20

30

40

50

れパケット、及び固定ホストにアドレスされた「流れ」パケットのみを受信する。それ故、WFMPルート指定は、ダウンリンクの場合に比較して非常に簡単である。

しかしながら、最初は、ダウンリンクオペレーションと同様であり、即ち流れ情報がセーブされ、そしてパケットが流れ検出の目的で流れクラシファイアへ通される。同じ3つのケースがここに適用される。即ち、(1)流れが既に検出された。(2)流れがまだ検出されていない。(3)新たな流れが検出される。新たな流れが検出される場合には、WFMPは、新たなRAN_IDを選択することが必要であり、そしてQoSマネージャーからQoSクラス及び帯域巾推定を要求する。次いで、WFMPは、圧縮モジュールに新たなIDを通知する。又、AP及び移動ターミナルも、新たなIDと、SARインターフェイスに追加される新たなサービスアクセスポイント(SAP)が通知されねばならない。移動ターミナルは、流れ情報を受信した後に、その流れに属する全てのパケットに対して新たなRAN_IDの使用を開始する。

10

【0073】

オプション(1)は、常に、対応ノードがIPネットワークに位置することを意味する。これは、移動対移動の流れがAPインターフェイス間で直接的にスイッチングされるからである。他方、オプション(2)及び(3)は、特定の注意を必要とする。

両方の場合に、WFMPは、移動対移動コールを検出し、そしてパケットを正しいデフォルトチャンネルに送給しなければならない。正しいデフォルトチャンネルは、行先IPアドレスをデフォルト流テーブルの値と比較することにより見出される。オプション(3)において、パケットは、先ず、デフォルトチャンネル(最良努力)を経て送信され、そしてその後にのみ、流れがスイッチングされる。行先がIPネットワークに位置する(DFTから見つからない)場合には、パケットがIP送給プロセスに送られ、該プロセスは、パケットを正しいネットワークインターフェイスへ送給する(通常のIPルート指定が適用される)。

20

【0074】

移動対移動トラフィック

スタートは、アップリンクオペレーションと同様であり、即ちSARが先ずパケットを、RAN_IDに基づいて正しいプロセスへ送給する。

非流れトラフィックの場合には、SARは、パケットをWFMPに送信する。パケットは、別の移動ターミナルにアドレスされるので、WFMPは、デフォルト流テーブルからエントリーを見出す。次いで、そのパケットを正しいデフォルトチャンネル(DFTから読み取られた)へ単に送給する。MT対MTの非流れパケットは、常に、WFMPを経てルート指定される。

30

【0075】

WFMPが新たな流れを検出しそして行先が別の移動ターミナルであるときには、WFMPは、2つの移動ターミナル間に接続を直接形成する。これは、WFMPが両APリンク(1つはMT1用、そしてもう1つはMT2用)に対して新たなRAN_IDを選択し、受信及び送信MTに新たなIDを通知し、そして新たな接続を両APに追加する。圧縮モジュールには通知されない。というのは、MT間で圧縮が直接使用されるからである。移動対移動のルート指定の場合が図20に示されている。

40

【0076】

先ず、受信側移動ターミナルに、新たなRAN_IDが通知される。このターミナルは、次いで、受信器が新たなRAN_IDを聴取していることを意味する確認を返送する。次いで、新たなRAN_IDが送信側移動ターミナルに与えられる。送信側移動ターミナルは、その流れに属するパケットを圧縮しなければならないと理解する。このターミナルは、新たなRAN_IDを使用してスタートし、そして圧縮機構を適用する。最終的に、受信側移動ターミナルは、全IPヘッダを保持する第1パケットを受信する。次いで、連続するパケットが圧縮されるので、ヘッダをセーブしなければならない。

【0077】

検出されたMT対MT流は、MルータのWFMPモジュールを経て送信されないので、

50

WFMPは、アクティブな流れを監視することができない。これは、流れを解除しなければならないときを検出できないことを意味する。それ故、受信側移動ターミナルは、トラフィックを制御し、そしてMルータのWFMPに流れをいつ解除すべきか通知する。考えられる監視場所は、MTのWFMP又はMTのFCモジュールである。任意の解決策は、SARブロックにおいてトラフィックを監視することである。SARブロックは、特定のRAN接続(RAN__IDで識別された)を経て進むトラフィックを測定することができ、そして一定時間のインアクティビティ(時間切れ)の後に、SARは、流れを解除すべきことをWFMPに通知する。

【0078】

移動ターミナルにおける流れ管理

移動ターミナル(MT)側の流れ管理は、Mルータ側より非常に簡単である。MTのWFMPは、流れを検出せず、MルータのWFMPにより指令されたときに新たな無線接続を用いてスタートする。

アップリンクにおける流れ管理

MTのWFMPは、IPパケットを正しいRAN接続に通すだけでよい。流れに属さないパケットは、デフォルトチャンネルの1つを経て送信され、流れに属するパケットは、AFTに基づいて正しい無線チャンネルに送信される(図21参照)。Mルータ側と同様に、WFMPは、先ず、流れ情報(識別された4つの同じ流れ形式)を更新し、そして正しいパラメータを使用してAFTを読み取る。流れ情報及び流れ形式がAFTエントリーの1つに対応する場合には、パケットが流れに属する。さもなくば、正しいデフォルト流がデフォルト流テーブルから読み取られる。

【0079】

ダウンリンクにおける流れ管理

ダウンリンクのケースも、極めて簡単である(図22参照)。WFMPは、RANチャンネル間でルート指定を行う必要がなく、受信したIPパケットをIP送給プロセスに通すだけでよく、該プロセスが最終的にパケットを正しいアプリケーションへ供給する。Mルータ側と同様に、SARは、到来するパケットを正しいMTプロセスに通すことによりルート指定を既に処理している。

MルータのWFMPは、移動対移動流を監視できない(流れは、MルータのAPインターフェイス間で直接的にスイッチングされ、従って、MルータのWFMPをバイパスする)ので、MTのWFMPは、到来する流れを監視しなければならない。これは、MTのWFMPが、流れが既に存在しないことに気付いたときに、RANから流れを解除すべきことをMルータのWFMPに通知しなければならないことを意味する。

【0080】

WFMPの流れ検出において上述したことに適用できる多数の異なる機構が存在する。例えば、Mルータにおいて最小の処理負荷が要求される場合には、次の考え方を使用できる。

最も簡単な機構は、IPv6流れラベル及びX/Yクラシファイアをベースとする。WFMPは、単に流れラベル値をチェックし、そしてそれが非ゼロである場合に、ソースIPアドレス及び流れラベルを流れ検出のために使用する。流れラベルがゼロの場合には、パケットが最良努力トラフィックとして処理され、そして流れクラシファイアは適用されない(=ゼロ流れラベルをもつパケットに対して検出される流れはない)。

【0081】

流れ圧縮機構

ヘッダ圧縮は、デガーマークによりIPヘッダ圧縮に関するインターネットドラフトに説明されたように、IPv6に対して実行される。IPデータグラムを、この文書に記載された圧縮可能な流れにグループ編成する方法は、実施されない。MルータのWFMPモジュールは、流れ圧縮(FC)モジュールに代わってIPデータグラムのグループ編成を実行すると仮定する。

ネットワークに入る各ターミナルには、最良努力(BE)チャンネルが指定される。こ

10

20

30

40

50

の B E チャンネルに送られるデータグラムは、個々のデータグラム間に類似性がないために圧縮されない。M ルータの W F M P モジュールは、それが新たな流れを識別すると、その流れに対して新たな無線チャンネルを設定し、そしてそのチャンネルを経て送信されるデータグラムが F C により圧縮される。

【 0 0 8 2 】

I P データグラムがアップリンク又はダウンリンクのいずれかに送信されるときには、それが存在する流れに属するかどうか調べるためのチェックがなされる。流れが存在する場合には、I P データグラムが F C モジュールに送られ、該モジュールは、ヘッダの圧縮を行い、そしてその圧縮された I P データグラムを、指定の無線チャンネルを経てその行先へ送信する。データグラムがいずれの流れにも属さない場合には、それが圧縮されずに B E チャンネルに送信される。新たな流れが検出されると、新たな無線チャンネルが割り当てられ、そして F C は、圧縮状態を設定しそして到来するデータグラムを無線流から F C へ向けるように通知される。流れが終わると、F C は、ブックキーピングの目的で指定されたメモリを割り当て解除するように通知される。

10

【 0 0 8 3 】

ヘッダの圧縮解除は、圧縮よりも若干簡単である。データが B E チャンネルから受け取られると、それが W F M P へ直接供給される。無線チャンネルが流れに属する場合には、受信したデータが F C へ送られ、F C は、I P データグラムを圧縮解除しそしてそれを W F M P へ転送する。流れが終わると、F C は、ブックキーピングの目的で指定されたメモリを割り当て解除するように通知される。

20

ヘッダ圧縮が各非 B E チャンネルごとに行われても、M ルータ及びその F C を通ることなく 2 つのターミナル間に直接的なポイント対ポイント流（カット・スルー）を使用することができる。

【 0 0 8 4 】

デガーマークで提案されたドラフトによれば、パケットは、T C P パケットに対して 1 つと、非 T C P パケットに対して 1 つの、2 つの異なる分類に区分化される。各分類のパケットは、更に、I P アドレス、ポート番号等や、M ルータにおいて W F M P ソフトウェアモジュールで既に実行されたタスクに基づくパケット流に分割される。T C P パケットと非 T C P パケットとの間のこの区分化は、コンテキスト識別子（C I D）と共に、圧縮及び圧縮解除されたパケットのどれが同じパケット流に属するかを独特に識別する。圧縮は、変化するヘッダフィールドのみを送信することにより行なわれるか、或いは T C P の場合には、以前のデータグラムからの変化を送信することによって行なわれる。上記ドラフトは、どのヘッダフィールドを推測できるか（例えば、パケット長さ）、どれが一定であるか、そしてどのヘッダフィールドが以前と同様に又は以前とは異なるように送信されねばならないかを検討するものである。

30

【 0 0 8 5 】

通常の I P v 6（/ v 4）パケットに加えて、4 つの新たなパケット形式が定義される。

全ヘッダパケットは、圧縮可能な流れに属する非圧縮パケットを指示する。これは、コンテキスト識別子（C I D）と、パケットヘッダに存在する長さフィールドへとコード化される非 T C P パケットの世代とを含む。

40

圧縮された非 T C P パケットは、C I D と、世代と、以前の全ヘッダパケットから変化したフィールドとを含み、これは、世代値により識別される。

【 0 0 8 6 】

第 3 の形式は、「圧縮された T C P ヘッダを伴い、C I D と、どんなフィールドが変化したかを識別するフラグオクテットと、以前の値からの差としてエンコードされた変化したフィールドとを含むパケットを指示する」圧縮された T C P パケット、即ち以前のパケットである。このパケットには、T C P チェック和も含まれる。

第 4 の形式は、以前のパケットからの差として送信されるヘッダフィールドがそのまま送信されること以外は圧縮された T C P パケットに類似したあっしゅくされた T C P ノー

50

デルタ(delta)パケットである。この形式のパケットは、受信器により発生されるヘッダ要求に応答して送信されるだけである。

【0087】

これらの新たなパケット形式は、特殊な形式値をリンク層レベルに送信するか又は圧縮されたパケットの前に付加的なバイトを追加することにより指示される。又、パケットの長さは、リンク層により与えられると仮定する。

圧縮は、適当なCID値を選択しそして全ヘッダをデコンプレッサへ送信することによりスタートされる。全ヘッダは、時間又はパケットの上限に到達するまで指数関数的に増加する周期で送信される。TCPパケットエラーからできるだけ迅速に回復するために、デコンプレッサは、1組のTCP CIDに対して全ヘッダを要求する。この要求は、正しく圧縮解除しないであろうCIDのリストと共にコンテキスト状態パケットとして送信され、これは、コンプレッサとデコンプレッサとの間で同期が失われることを意味する。コンプレッサは、要求された各CIDに対して新たなTCPノードルタパケットで応答する。

【0088】

QoS管理

QoSは、IPネットワークにおける新たなトレンドである。以前は、QoSは、ATMにより実現されていたが、ネットワークからQoSを要求するIPアプリケーション(ユーザ)の量が増加するにつれて、ネットワークデザイナーがIPネットワークのQoSに注意を払うようになった。

本発明のシステムは、顧客及びコアネットワークのQoS機構の利点を取り入れるように設計される。通常、一体化サービスをベースとする機構は、ネットワークの最後のホップにおけるQoS機構のように見える。区別化サービスをベースとする機構は、コアネットワーク機構のように見える。両機構は、本発明のシステムを開発する際に考慮された。又、パケットを他のものから分離するための別の機構も導入されている。

【0089】

一般的QoS管理概念

実際に、QoSとは、低い優先順位クラスを犠牲にして高い優先順位サービスクラスにネットワークリソースを与えるようにデータサービスのクラスを区別化することを意味する。又、QoSとは、ネットワークリソースの割り当てを特定データ流[QoS]の特性に一致させるよう試みることを意味する。

QoSは、異なる情報に基づいてデータ流を区別化することによって実施できる。即ち、IPv6流れID+ソースアドレス+行先アドレス、ポート情報+ソースアドレス+行先アドレス、プライオリティビット+ソースアドレス+行先アドレス、RSVP指定、又はH.323。

【0090】

これらの流れは、互いに異なるやり方で処理することができ、そしてQoSは、各流れのQoSパラメータに基づいてこれらの流れをマルチプレクスすることにより実施できる。これらのパラメータは、明確な値(ピークセルレート、帯域巾要求等)であるか、又は単に好ましいサービスクラスの情報である。これは、QoSパラメータをいかに決定するかの機構に依存する。

流れに属するパケットは、適当な無線待ち行列に入れられる。本発明の好ましい実施形態では、最良努力、制御型負荷及び保証型サービスの3つの異なる待ち行列がある。これらの流れは、互いに異なるプライオリティを得、そして待ち行列内のスケジューリングも行なわれる。

【0091】

QoSマネージャー(QoSエンティティ)

QoSマネージャーの主たるタスクは、固定ネットワークのQoSパラメータを無線QoSにマッピングしそして無線リソースマネージャーと通信することである。実際には、これは、明確なQoS値を無線プライオリティ待ち行列にマッピングすることを意味する

。QoS マネージャーは、流れの幾つかの統計値を知りそしてそれを使用可能な無線帯域中に割り振りしなければならない。この情報で、QoS マネージャーは、異なる流れのプライオリティを決めることができる。

QoS マネージャーは、RSVP、H.323 及びWFMP エンティティへのインターフェイスを有する（図15を参照して上述したように）。これらのインターフェイス及び主たる信号を以下のテーブルに示す。

【0092】

テーブル4：QoS マネージャーインターフェイス

インターフェイス		信号
M-ROUTER_QoS	→ M-	RESV_FLOW_conf
ROUTER_RSVP		RESV_FLOW_req
MT_QoS	→ H.323	SETUP_conf, CLOSE_conf, UPDATE_conf
H.323	→ MT_QoS	SETUP_req, CLOSE_req, UPDATE_req
M-ROUTER_QoS	→ M-	RESERVE_FLOW_req
ROUTER_WFMP		RESERVW_FLOW_conf
M-ROUTER_WFMP	→ M-	
ROUTER_QoS		RR_STATUS_enquiry
M-ROUTER_QoS	→ M-	UPDATE_req
ROUTER_WFMP		UPDATE_conf

10

20

【0093】

M ルータのQoS マネージャーは、移動ターミナルのQoS マネージャーよりも多くの機能を有する。というのは、M ルータでは流れの確立が行なわれるからである。移動ターミナルのQoS マネージャーの最も重要な機能は、H.323 シグナリング及びハンドオーバーを助成することである。

アクティブ流テーブル

アクティブ流テーブルは、データ流に関する全ての情報が記憶される場所である。このテーブルは、WFMP 及びQoS マネージャーに対してアクセスできるものである。上述したように、アクティブ流テーブルは、図17に例示されている。提案されたアクティブ流テーブルに加えて、QoS 情報も、流れがシグナリングされるか又はWFMP により検出だけされるかを示す指示と共にこのテーブルに含まれねばならない。

30

【0094】

接続に対してQoS 情報を得る方法

RSVP (図24)

RSVP は、特定のデータ流に対して帯域巾及び所望のQoS を指定するよう試みるリソース指定プロトコルである。このシステムは、本発明のシステムでは容易にサポートされる。というのは、流れがWFMP によって検出され、そして流れを無線リンクにおいて互いに異なるやり方で処理できるからである。RSVP は、制御メッセージを使用して、中間ネットワーク要素において指定をマークする。これらの制御メッセージは、アプリケーションデータから分離される。これらのメッセージは、プロトコル番号に基づいて他のデータから分離され、そしてWFMP プロセスの前にRSVP へ向けられる。

40

【0095】

RSVP を使用するときには、次の2つの異なる筋書きが存在する。

1. WFMP は、既に流れを検出し、そして流れに対して専用のチャンネルを形成しており、その後、RSVP エンティティがその特定の流れに対して指定要求を得る。

2. RSVP エンティティは、WFMP が流れを検出する前に指定要求を得る。この後者の場合には、RSVP は、WFMP をトリガーしなければならない。これは、QoS マネージャーを介して行うことができる。

図24は、本発明のシステムにおいてRSVP 指定がいかに取り扱われるかを示す。この特定の図は、MT が受信者でありそして送信者がネットワークのどこかにいる状態（ダウンリンクのケース）を示す。

50

【 0 0 9 6 】

R S V Pメッセージ (P A T H / R E S V) は、プロトコル番号 4 6 を使用し、これは、指定メッセージを最良努力トラフィックからいかに分離できるかである。これらメッセージは、それを取り扱う R S V P エンティティへ供給される。R S V P エンティティは Q o S マネージャーと話をし、Q o S マネージャーは、適当な Q o S 値をもつ流れを確立するよう W F M P に求める。W F M P は、R R M からリソースを求め、そして Q o S マネージャーはこれについて心配しない。

移動 I P ルータにおいては、R S V P エンティティは、2 つの役割を果たし、即ち通常の R S V P デーモン (Daemon) のように働くが、ワイヤレス特有のオペレーションも行う。通常の R S V P デーモンは、移動ルータ自身の容量をチェックし、そして I P レベルにおいて R S V P メッセージを転送 / 操作する。ワイヤレス R S V P デーモンは、W F M P と通信し、そしてあるパラメータをもつ流れを確立するようにそれに求める。

10

【 0 0 9 7 】

R S V P の R E S V メッセージは、周期的に送信されるリフレッシュメッセージと称することもできる。これらメッセージは、新たな流れをトリガーしてはならず、既存のものをリフレッシュするだけである。これは、M ルータ - W F M P において次のように行なわれる。

1 . R E S V リフレッシュメッセージは、Q o S マネージャーをトリガーし、R E S E R V E _ _ F L O W _ _ r e q を W F M P に送信する。

2 . W F M P は、アクティブ流テーブルから、その特定のデータ流に対してシグナリングされた流れを既に有しているかどうかチェックする。アクティブ流テーブルには、流れが R S V P によりシグナリングされるか又は何らかの他のベースで (トラフィック量のよう) に検出されるかの指示がなければならない。

20

3 . 流れが既に存在する場合には、W F M P は、確認メッセージを送信するだけで、他の動作は行なわない。

【 0 0 9 8 】

区別化サービス

区別化サービスとは、一般に、各 I P ヘッダにおけるプライオリティビットの展開を意味する。W F M P は、プライオリティをもつ I P パケットの流れを検出した場合に、Q o S マネージャーにそれらビットについて通知しなければならない。Q o S マネージャーは、ビットを理解し、そして必要な無線 Q o S へのマッピングを行う機能を備えている。その特定の流れに対し接続テーブルへパラメータがマークされる。

30

パラメータが明確な Q o S 要求へといかにマッピングされるかは、ネットワーク側において展開される区別化サービスに依存する。プライオリティビットの式が準備できたときには、それに関連してパラメータが明確なプライオリティクラスへとマッピングされる。プライオリティビットの標準化は、依然、進行中であり、将来的にプライオリティビットを展開する異なる方法が出現するであろう。テーブル 5 及び 6 は、本発明の好ましい実施形態においてビットがプライオリティクラスへいかにマップされるかを例示する。

【 0 0 9 9 】

テーブル 5 : ビットパターンの例

40

<u>ビット</u>	<u>指示</u>
ビット 0 - 2	0 0 0 = ドロッププレフェレンス 1、0 0 1 = D P 2、 ・ ・ 1 1 1 = D P 8
ビット 3	0 = 通常遅延、1 = 低遅延
ビット 4	0 = 通常スループット、1 = 高スループット
ビット 5	0 = 通常信頼性、1 = 高信頼性
ビット 6 - 7	将来の使用のために指定

テーブル 6 : Q o S クラスへのプライオリティビットのマッピング例

<u>プライオリティビット</u>	<u>Q o S クラス (テーブル 8 参照)</u>
-------------------	--------------------------------

50

???001??

クラス3、BE

???101??

クラス2、制御型負荷

???110??

クラス1、保証型負荷

【0100】

WFMPが、プライオリティビットを含むパケットを検出するが、そのトラフィック流からの流れ（1秒当たり十分なパケットがない）を検出できない場合には、WFMPは、これらのパケットを正しいプライオリティ待ち行列に入れる。換言すれば、WFMPは、パケットが時々しかない場合には、QoSマネージャーから何も求めない。即ち、WFMPとQoSマネージャーとの間でインテリジェンスが分割され、従って、QoSマネージャーは過剰に展開される状態にならない。

10

良く知られたポート

多数の「良く知られた」TCP/UDPポートがあり、これは、トラフィックがあるリアルタイム特徴を必要とすることを指示するか、又はトラフィックの量が著しく高い又は低いことを指示してもよい。この種のポートは、例えば、ftpポート又はtelnetポートであり、これらは、両方とも、非常に異なる特性を有する。ftpは、相当の帯域巾を必要とするが、リアルタイム要求にはあまり厳密でない。逆に、telnetは、著しい帯域巾を必要としないが、大きな遅延によって影響されてはならない。この情報は、データ流に対して正しい無線リンク待ち行列を選択するときに展開することができる。好ましいシステムでは、流れが既に検出された後にポート情報の利点を取り入れるように関連される。これは、ポート情報自体がWFMPをトリガーして新たな流れを通知するのではなく、流れが検出された後に、ポート情報を展開できることを意味する。IPSEC又は他の何らかのプロトコルがポート情報を隠す場合には、それを展開することができない。

20

【0101】

図26は、WFMPが流れを検出し、そしてポート番号が、QoSマネージャーにより識別されたアプリケーションに属する状態を示す。

テーブル7は、異なるやり方で処理できる幾つかの共通のポートを示す。これらポートのリストは、一例に過ぎず、そして特定のサービスを得るポートを変更することができる。

。

テーブル 7 : ポート (例)

形式	ポート番号	説明	考えられる QoS	
			クラス (テーブル 8 参照)	
fpt-data	20/tcp	ファイル転送 [Default Data]	クラス 3	
fpt-control	21/tcp	ファイル転送 [Control]	クラス 3	10
telnet	23/tcp	テルネット	クラス 2	
http	80/tcp	ワールドワイド ウェブ HTTP	クラス 2	
snmp	161/tcp	SNMP	クラス 3	
ipx	213/tcp	I P X		20
dhcpv6-client	546/tcp	D H C P v 6 クライアント	クラス 2	
dhcpv6	547/tcp	D H C P v 6 サーバー	クラス 2	
vat	3456/tcp	V A T デフォルト データ	クラス 1	30
Vat-contol	3457/tcp	V A T デフォルト 制御	クラス 1	

【 0 1 0 2 】

ネットワークアドミニストレータは、どんな顧客会社の要望があるかに基づいて分類を構成することが望ましいので、特殊な取り扱いを得るポートを構成するのが好ましい。ある会社は、他の会社よりマルチメディアアプリケーションを非常に積極的に利用する。又、ある会社は、ほとんどの帯域巾を得なければならない彼等自身の特定のアプリケーションを利用する (例えば、銀行)。この特殊な処理は、例えば、QoS マネージャーが、容易に更新され得る個別の機能的エンティティである場合に考えられる。

40

H . 3 2 3

本発明のシステムでは、H . 3 2 3 は、2 つの異なるやり方で展開することができる。
1) H . 3 2 3 アプリケーションは、QoS マネージャーを経て接続を信号する。又は 2) H . 3 2 3 は、R S V P (図 2 7) を使用することによって接続を信号する。両方の場合に、接続を更新する機構がなければならない。

【 0 1 0 3 】

H . 3 2 3 コールシグナリング手順は、コール設定からコール終了までの 5 つの段階で形成される。考えられる全てのケースを伴うコール設定手順は、複雑であり、以下に簡単に述べる。

50

先ず、SETUP（設定）メッセージが発呼側エンドポイントから他の当事者へ送信され、他の当事者は、CONNECT（接続）メッセージで応答する。次いで、両当事者は、H.245 TERMINAL-CAPABILITY-SET（ターミナル能力設定）メッセージを送信することによりシステム能力情報を交換する。第3段階の間に、種々の情報流に対する論理的チャンネルがH.245を用いてオープンされる。これらの流れは、H.225.0に規定された信頼性の低いプロトコルを経て搬送される。H.245における論理的チャンネル設定で送信されるデータ通信が、信頼性の高いプロトコル（H.225.0）を用いて搬送される。セッションの間に、能力、受信モード等を変更する手順は、H.245に規定されている。

【0104】

接続に必要な帯域巾は、選択された音声コーデックをコーデックに必要なビットレートにマップするテーブルによりターミナル間で使用するものとして合意された能力から決定することができる。映像コーデックの場合は、使用可能な映像コーデック当たりの能力設定メッセージに最大許容ビットレートが含まれる。

最終的に、コールは、いずれかの当事者により、H.245制御チャンネルにおけるEND-SESSION-COMMAND（セッション終了コマンド）で終了される。他の当事者は、RELEASE-COMplete（解除完了）メッセージで応答する。

【0105】

H.323プロトコルスタックからQoSマネージャーへのインターフェイスは、H.323に伴う上記機能を容易にするために3つの機能を必要とする。当事者に関する情報（ソース及び行先アドレス）と共に必要な帯域巾を、コール設定段階の後に、QoSマネージャーに通さねばならない。当事者間の必要帯域巾がコール中に変化する場合には、そのことも、新たな帯域巾を示す更新要求と、この接続に対する識別情報と共にQoSマネージャーへ信号しなければならず、これにより、QoSマネージャーは、どの接続の帯域巾を変更しなければならぬかを識別することができる。最終的に、コールが終了した後に、この接続が終了したことをQoSマネージャーに信号することにより帯域巾を解除しなければならない。

【0106】

RAN QoS 機能

QoSベースの無線アクセスネットワークは、需要に応じた帯域巾、クラスに基づく待ち行列構成、及び信頼性を与えることができねばならない。ワイヤレス無線リンクでは、媒体への異なるサービスのマルチプレクシングが、通常、4つのQoS事項、即ち帯域巾、遅延、ジッタ及び信頼性の考慮を必要とする。

帯域巾は、QoS駆動サービスの第1要件であり、即ち要求されたトラフィックパラメータをサポートできるようにするための第1要件である。ワイヤレスリンクでは、主たる目的は、TCP/IPトラフィックに対しサービス特有のQoSを維持しながら効率的にチャンネルを利用することである。これは、APスケジューラが、無線流を確立すべきところの接続の所要平均及び/又はピーク帯域巾を知らねばならないことを意味する。このようにして、スケジューラは、需要に応じて帯域巾を満足させそして統計学的なマルチプレクシングを実行するよう保証できる。

【0107】

遅延及びジッタは、主としてワイヤレスリンクを経てのトラフィックスケジューリングによって影響される。ここに示す解決策では、流れに基づく接続が別々に待ち行列に入れられ（各接続に対する待ち行列）、そして接続が3つの異なる遅延クラス待ち行列にグループ分けされる。パケットを正しい待ち行列に入れることができるために、スケジューラ（又は待ち行列機能）は、到来するパケットの流れID及び遅延クラスを知る必要がある。又、遅延及びジッタ要求を考慮して、送信されるべきパケットを選択するために、スケジューラは、a) RAN層におけるパケットの最大許容遅延を知り、そしてb) 各パケットの時間スタンプを保持しなければならない。

【0108】

ワイヤレスリンクに対する信頼性は、例えば、コード化及び／又はデータ再送信により通常与えられるエラー制御を必要とする。コード化は、エラー検出及び修正の両方に使用され、これは、適用データにわたり一定のオーバーヘッドを課する。ＡＲＱ（自動再送信要求）は、崩壊したパケットのみに適用され、これは、パケット損失の確率があまり高くなく且つ再送信の遅延が受け入れられる限り実現可能である。スケジューラは、無線流（接続）ベースでのＡＲＱ使用に関する情報（例えば、ＡＲＱなし、限定ＡＲＱ、ＡＲＱ）を必要とする。ＦＥＣの使用は固定され、全てのパケットに使用することができる。

【 0 1 0 9 】

テーブル 8 は、本発明の好ましい実施形態により、ＴＣＰ／ＩＰ ＱｏＳから無線アクセスネットワーク特有のＱｏＳへマッピングする一例を示す。最初の 2 つの欄は、無線アクセス待ち行列及びエラー制御を示し、一方、欄 3 ないし 5 は異なるＴＣＰ／ＩＰレベルのＱｏＳ概念を示す。

テーブル 8：無線アクセスＱｏＳへのネットワークＱｏＳマッピングの例

遅延 クラス	無線アクセ スＱｏＳ	送信プロ トコル	一体化 サービス	区別化 サービス
第 1 クラス	ARQ+FEC なし	-	保証型負荷	低遅延 / 高 ドロップ
第 2 クラス	限定された ARQ+FEC	UDP/RTP流	制御型負荷	中間遅延 / 中間ドロップ
第 3 クラス	ARQ+FEC	TCP流 / 流れ なし	最良努力	高遅延 / 低 ドロップ

【 0 1 1 0 】

無線リンクは、種々の待ち行列に属するパケット（無線ＱｏＳクラス又は遅延クラスとも称する）を異なるやり方でスケジューリングして、種々の遅延要求を満足する。

無線流に関連した 1 つの実施形態では、Ｍルータは、無線アクセスネットワークの中央インテリジェンスポイントとして機能して、流れを検出し、流れを分類し、そしてネットワークのＱｏＳ概念を無線ＱｏＳ能力へとマッピングする。別の実施形態では、直接的なＱｏＳマッピングが使用される。この解決策では、アクセスポイントがＩＰパケットを処理し、各ヘッダのＱｏＳビットをチェックし、そしてＩＰパケットをそれに対応する無線スケジューリング待ち行列へとマッピングする。

【 0 1 1 1 】

待ち行列形成（図 2 8 参照）：好ましい実施形態において、プライオリティクラス 1 及び 2 に対する待ち行列形成の戦略は、各無線流がそれ自身の待ち行列を有するように無線流に基づいて行なわれる。流れＩＤに基づき、正しいプライオリティクラスを選択できると共に、パケットが入れられる待ち行列を選択することができる。この解決策が必要となる理由は、スケジューラが接続及びそれらのＱｏＳ要求を区別化できねばならないからである。最良努力データ（プライオリティクラス 3）の場合には、流れを識別することもできる。

遅延及びジッタ：これらは、エラー保護機構及びワイヤレスリンクに対するトラフィックスケジューリングによって主として影響される。もう 1 つの待ち行列を追加すると、インターネット音声に対して与えることのできるサービスクオリティを改善し、サービス区別化能力を高めることが分かった。

【 0 1 1 2 】

スケジューラ

ワイヤレス環境は、スケジューリングアルゴリズムの性能に特殊なストレスも課する。これは、接続のＱｏＳ及びトラフィック特性が分かる効率的なスケジューリングアルゴリズムを必要とする。

このスケジューリングアルゴリズムは、帯域限定されたワイヤレスチャンネルにわたりパケットの流れを制御する上で重要な役割を果たす。コール受け入れ制御（ＣＡＣ）及びリソース割り当てと一緒に使用すると、このスケジューリングアルゴリズムは、異なるト

ラフィック形式に対して異なる Q o S 要求を満足するよう保証することができる。受け入れ制御及びリソース割り当ては、接続が確立されるときに動作して、新たな無線流 / 接続がチャンネルにアクセスできるかどうか判断する。スケジューリングは、各 M A C フレームへのパケットの選択について判断を行う。スケジューリングアルゴリズムは、次の特性を与えることに向けられねばならない [G a r r e t t 9 6]。

【 0 1 1 3 】

- 接続のトラフィック特性を維持する。
- Q o S 要求を満足する。遅延及びロスに関連した Q o S パラメータは、トラフィック契約に基づいて維持することが重要である。
- 統計学的なマルチプレクス利得。スケジューリングは、スムーズでなければならぬいか、又は可変ビットレートの接続がバッファの占有率（混雑状態）に及ぼす作用を考慮しなければならない。
- アイドル接続に割り当てられた又は割り当てられていない帯域巾を利用する。アプリケーション（例えば、WWWブラウザ）は、常にセルを送信するものではなく、サイレントなものであるから、割り当てられないリソースをこれらの周期中に使用しなければならない。
- 宣言された真のトラフィック一貫性。ソースが予想以上のトラフィックを発生し、従って、トラフィック契約を破る場合には、スケジューラが、例えば、接続のプライオリティを「ドロップ」しなければならない。

10

【 0 1 1 4 】

好ましい実施形態の待ち行列構成では、スケジューラは、例えば、次のように機能することができる。

先ず、スケジューラは、3つのプライオリティクラスに基づいてパケットのプライオリティを決める。クラス1は最も高いプライオリティを有し、そしてクラス3は最も低いプライオリティを有する。スケジューラは、クラス1の待ち行列に保留中のパケットの割り当てを開始する。プライオリティクラス内では、パケット / 流れ間のプライオリティ決めは、遅延要求に基づいて行うことができ、即ち残された「寿命」が最も少ないパケット等を選択する。これと並列に、割り当てられたものよりも帯域巾を消費しない流れが、より高いプライオリティを有する。これは、「トークンバケット(Token Bucket)」のようなトラフィックポリシング機能を使用することにより考慮することができる。プライオリティ

クラス1の全てのパケットが割り当てられ、そしてM S Cフレームにまだ余裕があるときには、スケジューラは、クラス1のケースと同様に、プライオリティクラス2の待ち行列からパケットの割り当てを開始する。全てのクラス2パケットが割り当てられた後に、スケジューラは、クラス3パケットを空きスロットに割り当てる。クラス3待ち行列は、F I F O（先入れ先出し）として機能する。スケジューリングは、全てのパケットが割り当てられるか、又はM A C タイムフレームがいっぱいになったときに終了する。

20

30

【 0 1 1 5 】

移動管理

ターミナルの登録及び認証

ターミナルは、電源オンされたときにI Pレベル登録プロセスを実行する。これは、I Pレベルハンドオーバーの初期部分でもある。このプロセスは、ターミナルのホームネットワークおよび外部ネットワークにおいて同じである。

このプロセスは、リンクレベル登録プロセスの後に実行される。リンクレベル手順は、既にターミナルを認証しそしてネットワークへのそのアクセスを受け入れている。又、リンクレベルエンティティは、ターミナルを、全ノード及び懇請ノードマルチキャストグループのメンバーにしている。懇請ノードマルチキャストアドレスは、リンクレベル登録メッセージと共に与えられるE U I - 6 4 識別子から計算される。

40

【 0 1 1 6 】

これらのマルチキャストグループは、ターミナルが現在アタッチされているリンクに対してローカルである。これは、ターミナル及びMルータの両方が、このターミナルがこれ

50

らのマルチキャストグループに属することを知っていることを意味する。M ルータは、これらのグループにアドレスされたパケットをこのターミナルにルート指定すべきことを知り、そしてターミナルは、これらパケットを受け取って処理することができる。このため、ターミナルは、そのリンクローカルIPアドレスを発生した後にIPレベル登録プロセスの始めにリンクレベルマルチキャストメンバーシッププロトコルを使用してこれらグループに明確に加わることをしない。

【0117】

リンクレベルがその登録手順を実行したときに、リンクレベルは、上位レベルエンティティにその準備ができたことを通知する。これが電源オン状態である場合には、ターミナルのネットワークインターフェイスがイネーブル状態となる。この場合に、ターミナルは、リンクレベルにより与えられた情報からそのリンクローカルIPアドレスを発生する（インターフェイスのEUI-64フォーマット化MAC識別子）。通常、ホストは、アドレスが最終的に指定される前に複写アドレス検出手順を実行することによりこのアドレスを有効とする。しかしながら、MAC識別子は、リンクレベル登録手順の間に既に有効とされており、従って、リンクローカルIPアドレスがその同じ独特の識別子から発生されるときにこの照合を再び実行する必要はない。ターミナルは、リンクローカルIPアドレスをネットワークインターフェイスに指定する。

【0118】

電源オン状態及びIPレベルハンドオーバーの場合の両方に次の動作が実行される。ホストは、通常、リンクレベル機構を使用して、ここで、全ノード及び懇請ノードマルチキャストグループに加わる。上述した理由で、このタスクは、この環境においてはこの点で実行されない。というのは、このタスクは、リンクレベル登録手順の間に暗黙的に実行されているからである。

ネットワークインターフェイスに有効なリンクローカルIPアドレスが指定されると、ターミナルは、ルータ発見動作を遂行して、そのデフォルトルータを見つけると共に、おそらく、そのサイトローカル及びグローバルIPアドレスに対するネットワークプレフィックスを得る。M ルータは、ターミナルの懇請にアドバタイズメントで応答し、そしてターミナルにM ルータのリンクレベルアドレス及びそのIPアドレスに関する情報を与える。ターミナルは、そのアドレスを指すようにそのデフォルトルータを更新する。ルータ発見プロセスは、ホームネットワークのプレフィックスが番号付けし直されているかもしれないので、ホームネットワークにおいて必要な事象であることに注意されたい。

【0119】

ルータは、このリンクに対するそのサイトローカル及びグローバルIPアドレスプレフィックスをアドバタイズメントにおいて広告する。このような場合には、ターミナルは、そのサイトローカル及びグローバルIPアドレスをこれらプレフィックスに基づいて発生する。この場合も、ターミナルは、複写アドレス検出手順によりアドレスの独特さを照合する必要はない。というのは、アドレスのネットワークインターフェイス特有のサフィックスが、リンクレベル登録プロセス中に独特であることが既に証明されている。又、この場合に、ターミナルは、おそらく、これらアドレスの懇請ノードグループに加わる必要はない。というのは、これらグループは、潜在的に、このネットワークインターフェイスのリンクローカルアドレスに対する懇請ノードグループと同じだからである。

【0120】

又、ルータアドバタイズメントのビットは、DHCPv6のようなステートフル(stateful)・コンフィギュレーション機構によりそのサイトローカル及びグローバルなIPアドレスの収集をターミナルが要求されるように設定されてもよい。この場合には、ターミナルは、リンクを経て全てのコンフィギュレーションサーバーグループに懇請を送って、ターミナルにサービスしようとするサーバーを見つける。この環境では、サーバーは、M ルータ内にある。サーバーは、ターミナルがサーバーのIPアドレスを知るようにアドバタイズメントで応答する。ターミナルは、コンフィギュレーション要求をこのアドレスに送信し、そして要求したアドレスをサーバーの応答において受け取る。コンフィギュレ

10

20

30

40

50

ーションサーバーは、おそらく、ターミナルに代わってこれらアドレスの懇請ノードグループにターミナルを追加する。さもなくば、ターミナルは、これらのグループに加わるために一般的リンクレベル及びIPレベルマルチキャストグループメンバーシップ手順を開始しなければならない。いずれにせよ、ターミナルは、インターフェイスから到来してこれら懇請ノードグループにアドレスされたバケットを受信できねばならない。アドレスは、複写アドレス検出手順により照合される必要がなく、Mルータ内のコンフィギュレーションサーバー及び他のエンティティは、ターミナルのインターフェイスに対してどのアドレスが有効であるか知ることが予想される。ターミナルは、そのサイトローカル及びグローバルIPアドレスをインターフェイスに指定する。

【0121】

10

ステートフル・コンフィギュレーション機構は、DHCP懇請及びDHCP広告メッセージを無視することにより更に最適化することができる。それらは、ステートフル・コンフィギュレーションサーバーがMルータに配置され、そのアドレスがルータ発見プロセスから既に分かっていると仮定する場合には必要とされない。これは、ステートフル・コンフィギュレーション機構からの非標準偏差となり、提案されたIPレベル認証方法では着手できない。

アドレッシング構成

IPレベルアドレスは、標準的なアドレスコンフィギュレーション方法に基づいて構成される。IPアドレスのネットワークインターフェイス特有の部分は、そのインターフェイスのリンクレベルMAC識別子から形成される。この識別子は、EUI-64フォーマットである。この識別子は、リンクレベル登録プロセス中に照合され、そして同じサブネットにアタッチされた全てのターミナル間で独特であることが証明される。照合が失敗すると、ターミナルは、ネットワークを使用することができない。

20

【0122】

ターミナル特有のネットワークインターフェイスのリンクローカルIPアドレスは、静的な良く知られたプレフィックス及びネットワークインターフェイス識別子から発生される。リンクローカルアドレスは、複写アドレス検出プロセスにより照合されない。

ネットワークインターフェイスのサイトローカルIPアドレスは、ルータアドバタイズメントで受信されたサイトローカルプレフィックスと、ネットワークインターフェイス識別子とから形成される。サイトローカルプレフィックスは、サイトエリア内のこのサブネットを独特に識別する。又、サイトローカルアドレスは、ステートフル・コンフィギュレーションサーバーからも収集される。両方の場合に、発生された又は受信されたアドレスは、有効であると仮定され、複写アドレス検出は実行されない。

30

【0123】

ネットワークインターフェイスのグローバルIPアドレスは、ルータ発見プロセスにより与えられたグローバルプレフィックスと、ネットワークインターフェイス識別子から発生される。又、グローバルアドレスは、ステートフル・コンフィギュレーションサーバーからも受け取られる。グローバルアドレスは、複写アドレス検出プロセスでは照合されない。

ターミナルのアドレス割り当てプロセス（ステートレス又はステートフル）に使用されるMルータの情報は、本発明の範囲外の方法で管理される。又、ターミナルは、一度に1つのリンクのみにアタッチされ、従って、一度に1つのMルータのみがアクセスされると仮定する。アドレッシング構成は、複写アドレス検出が実行されないという点で標準的な手順とは相違する。

40

【0124】

位置管理（RAN+IP）

ターミナルが別のサブネットに移動したときには、リンクレベルが登録手順を実行する。IPレベルは、上述したように（ターミナル登録及び認証）、リンクレベルによりこれについて通知され、その後、IPレベルは、その同じセクションで述べたようにそれ自身の登録手順を実行する。IPレベルの移動は、サブネットワークが変化するたびに指示が

50

下位層から受信されるという点で、標準とは相違する。

潜在的なサブネットワーク変化は、リンクレベルによりIPレベルに指示されるが、ターミナルが別のサブネットワークへ移動したという最終的な事実は、ルータアドバタイズメントから収集したサイトローカル及びグローバルアドレスプレフィックスから推論されるか、又はステートフル・コンフィギュレーションサーバーから受信したサイトローカル及びグローバルアドレスから推論される。これらの新たなプレフィックスは、移動の前にこのネットワークインターフェイスに対してアクティブであった古いプレフィックスと比較される。プレフィックスが相違する場合には、IP移動手順をアクチベートしなければならない。

【0125】

10

ターミナルは、それがホームネットワークから離れているときに、ターミナル発信パケットに特殊なヘッダ拡張を使用する。このヘッダ拡張は、ホームアドレスオプションと称される。ホームアドレスオプションは、ターミナルネットワークインターフェイスのホームアドレスを含む。このオプションは、ターミナルがその新たなグローバルアドレスをパケットのソースアドレスフィールドに使用できるようにし、従って、パケットは、経路に沿ってファイアウォールを容易に貫通することができる。ホームアドレスオプションは、受信パケットのソースアドレスをホームアドレスオプションのアドレスと交換するように受信ノードによって取り扱われる。このように、ターミナルのアクティブなアドレスが変化するときでも、進行中のセッションが妨げられることはない。

【0126】

20

ターミナルは、バインディング更新をルータに送信することによりその新たなグローバルIPアドレスを以前のデフォルトルータに通知する。メッセージはIPSEC AHヘッダで認証される。以前のルータは更新を確認する。以前のルータは、ターミナルの以前のグローバルアドレスに対する代理となる。これは、以前のルータが、ターミナルの古いグローバルアドレスに向けられた全てのパケットを捕獲し、そしてその各々を新たなパケットへとカプセル化しそしてそれをターミナルの新たなグローバルアドレスへ送信する。又、以前のルータは、バインディング更新が終了するまで、そのエリアにおける他のターミナルに対してターミナルの古いアドレスを割り当てできないようにする。バインディング更新が終了すると、以前のルータは、もはや、ターミナルの古いグローバルアドレスに対する代理として働かない。

30

【0127】

又、ターミナルは、そのホームネットワークのルータにターミナルの新たなグローバルIPアドレスを通知する。これは、上記と同じバインディング更新 + AH / バインディング確認 + AHトランザクションによって実行される。ホームルータは、ここで、以前のケースにおける以前のルータのように働く。唯一の相違は、ターミナルがバインディング更新を規則的にホームルータへ送信し、従って、バインディング更新が決して終了しないことである。

又、ターミナルは、それが最近通信した全ての対応するノードに、その新たな位置を通知する。この場合もバインディング更新 + AHメッセージを使用する。それに対応するノードは、ターミナルのホームアドレスに向けられた各パケットにルート指定ヘッダが追加されるようにそのデータ構造を更新する。ルート指定ヘッダは、ターミナルのインターフェイスの新たなグローバルアドレスを含む。これは、パケットを先ずターミナルの新たな位置へルート指定させる。ここで、ルート指定ヘッダが除去され、そしてパケットは、ターミナルインターフェイスのホームアドレスに到達したかのように見える。ホームアドレスは、依然、ターミナルインターフェイスの有効アドレスであるから、パケットは、ターミナルがそのホームネットワークにあるかのように受信して処理することができる。

40

【0128】

ルータ内でのIPサブネットワーク間ハンドオーバー

これは、異なるIPドメインに属するルータポート間でターミナルが移動するケースを意味する。ここで、移動IPは、新たなアドレスを割り当てるが、RANに流れを維持す

50

ることができる。I P レベルにおいて、この種のハンドオーバーは、上記のケースと全く同じに実行される。

D H C P v 6

ホストがグローバル I P v 6 アドレスを収集しようとし、そして M ビットがセットされたルータアドバタイズメントを受信したときには、ホストは、ステートフル・アドレス・オートコンフィギュレーション、即ち D H C P v 6 の原理に従わねばならない。

【 0 1 2 9 】

ステートフル・アドレス・オートコンフィギュレーションは、ホスト即ちクライアントが D H C P 懇請メッセージを全ての D H C P エージェントマルチキャストアドレスに送信する状態でスタートし、サイトの D H C P サーバーの 1 つを見つける。D H C P サーバーは、サーバーの I P アドレスを含むユニキャスト D H C P アドバタイズメントメッセージで応答する。その後、クライアントは、D H C P 要求をサーバーへ送信して、ネットワークのパラメータを得る。サーバーは、可変量のパラメータがクライアントに供給される D H C P 応答で応答する。クライアントは、D H C P 解除メッセージをサーバーへ送信することにより D H C P セッションを終了し、サーバーは、次いで、D H C O 応答を送信することにより解除を確認する。又、サーバーは、あるパラメータが変化する場合に、D H C P 再コンフィギュレーションメッセージを送信することによりクライアントに通知する。

【 0 1 3 0 】

アドバタイズ、要求、応答、解除及び再コンフィギュレーションの D H C P メッセージは、全てユニキャストメッセージであり、そしてその後に、クライアントとサーバーとの間に付加的なパラメータを搬送する可変量の拡張が続く。クライアントの I P アドレス及び D N S エントリをコンフィギュレーションするのに加えて、上記拡張は、時間ゾーンに関する情報、T C P パラメータ及び他のネットワーク情報を含む。又、D H C P メッセージを認証することもできる。

サーバー及びクライアントは、同じリンクに存在する必要がなく、D H C P 応答サーバーをそれらの間に挿入して、1 つの D H C P サーバーのみでサービスされる大きなドメインを形成することもできる。

【 0 1 3 1 】

D H C P サーバーは、クライアントキー選択拡張をそのアドバタイズメントメッセージにアタッチして、クライアントがそれ自身をサーバーに対して認証するときにどのセキュリティパラメータインデックス (S P I) 値を使用すべきか指示することができる。認証は、クライアントサーバー認証拡張をいずれかの D H C P メッセージに追加することにより達成される。D H C P 認証拡張の目的は、クライアントが始めからサーバーをサーチするに十分な大きさのアドレス範囲を有しておらず、即ち D H C P 中継が使用され、それ故、通常の I P S E C 手順を適用できない場合に、認証を与えることである。現在のドラフトは、認証に使用されるキーを、D H C P 登録手順の前に、クライアント及びサーバーの両方が知らねばならないと仮定している。

【 0 1 3 2 】

サブネットにおける D H C P v 6

D H C P を使用してグローバルな I P v 6 アドレスを形成するときには、M ルータ及び D H C P サーバーが別々のエンティティである場合に M ルータが新たに形成されるグローバルな I P v 6 アドレスを知らない可能性が高い。D H C P サーバーは、正しいネットワークプレフィックスを伴う I P v 6 アドレスをターミナルに与え、これは、M ルータが、このアドレスに向けられた I P v 6 データグラムを直ちに又は後で受信することを意味する。正しい V P I / V C I 接続を経て正しいターミナルにデータグラムを送信するために、M ルータは、隣接発見プロトコル [N a r t e n 9 8] に基づいてアドレス分析を行なわねばならない。M ルータは、マルチキャスト隣接懇請をリンクに単に送信し、そして当該 I P v 6 アドレスを得たターミナルにより応答として送られる隣接アドバタイズメントにおいてリンク層アドレスを受け取る。その後、M ルータは、正しい接続を経てデータグラムを送信し、そしてグローバルな I P v 6 アドレスをそのルックアップテーブルに追

10

20

30

40

50

加する。

【 0 1 3 3 】

移動 I P v 6 と R S V P との相互オペレーション

移動 I P v 6 において、外部リンクに訪問している移動ターミナル (M T) は、そのホームアドレス (H A) を使用するか、又はいずれかのケア・オブ・アドレス (C o A s) を使用してアドレスすることができる。更に、対応ノード (C N) がパケットを M T の H A (又はストール C o A) へ向ける場合には、パケットがホームエージェント (又は以前に訪問したリンクのルータ) を通して M T へトンネル送信される。

M T をアドレスする種々のモードは、R S V P ([R F C 2 2 0 5] 、 [R F C 2 2 0 9]) がネットワークリソース指定に使用される移動 I P v 6 環境において相互オペレーションの問題を生じる。次のときには、アドレッシングモードを考慮しなければならない。

- R S V P メッセージをコンポーズして送信する。
- ネットワークノードにおいて指定状態を設定する。
- トラフィック制御を実施するときにパケットを分類する。
- 出て行くインターフェイスを見つけそしてルート変更が通知された状態にするためにルート指定プロセスを調べる。

【 0 1 3 4 】

R S V P メッセージにおいてアドレッシング情報を搬送し、そしてネットワークノードに指定状態を維持するために、次の 2 つのオプションを示すことができる。

1) M T は、常に、R S V P メッセージにおけるそのホームアドレスで識別される。

この単純な解決策は、送信者アプリケーション (H A により M T を知るだけである) により発信された R S V P P A T H メッセージが受信器への途中で変更されないという考え方から生じる。これは、M T に対する少なくとも 2 つのアドレス即ち H A 及び C o A を包含するために全てのノードにおける R S V P 状態を改善する必要があることを意味する。これは、アドレスバインディングをノードに通知しなければならないことを意味する。H A は、R E S V メッセージに対して一致する経路状態を見出すよう試みるときに R S V P セッションを識別するのに必要とされる。一方、C o A は、パケット分類 (もしあれば) 及びルート指定プロセスを調べるのに使用される。

【 0 1 3 5 】

この解決策は、R S V P に気付く全てのルータに対する変更を必要とする。又、現行の仕様書の表現に違反し、これは、P A T H メッセージの行先 I P アドレスがセッションの D e s t A d d r e s s ([R F C 2 2 0 5] p . 3 6) と同じでなければならないことを必要とする。

2) M T は、M T がホームにいないときに R S V P メッセージの C o A により識別される。

アプリケーショントラフィックの転送に関する限り、移動 I P v 6 では、M T へパケットをトンネル送信するホームエージェントの場合を除き、中間ルータが H A と C o A との間のバインディングに気付く必要はない。R S V P オペレーションにも同じ原理を適用できる。これは、ルータにおいて、R S V P セッションの全寿命期間にわたり R S V P 指定状態を維持する必要があるという観察により容易にされる。むしろ、M T がローミングするときには、実際の H A を知ることなく各新たな C o A ごとにデータ経路に沿って新たな経路状態を構築することができる。この解決策は、エンドシステムに変更を必要とするだけであるから更に拡張可能であるが、中間ルータにおける R S V P 処理は、現在の R S V P R F C に規定された通りのままである。

【 0 1 3 6 】

スムーズなローミングを達成するために、M T 及び C N には多数のメッセージ処理拡張及び改善が必要とされる。これらは、H A と C o A との間の I P アドレスマッピングに、I P v 6 アドレスコンフィギュレーション機構及びバインディングキャッシュ管理のサポートを合体させる。

上記のオプション 2) は、多数のコアネットワークルータを有する動作ネットワークにおいてより実現可能であると思われる。しかしながら、本発明のシステムでは、標準的な R S V P 特性からの逸脱が固定ネットワークノードにおいて予想し得ない。それ故、オプション 1) は、C o A と H A との間のパインディングを知っている M T 及び M ルータが、M T と C N との間の経路上にある R S V P に気付くノードだけであるという仮定で使用されねばならない。

【 0 1 3 7 】

要約

好ましい実施形態で説明した完全なシステムは、時間に厳密なデータをもつ I P パケットが高プライオリティの無線スケジューリング待ち行列へとマッピングされそして非リアルタイムトラフィックが低プライオリティ待ち行列に指定されるような I P v 6 又は I P v 4 ネットワークアーキテクチャーをベースとする。上述した機構は、ユーザ / アプリケーションが、異なるネットワークレベル、ここでは、無線リンク上の種々の接続形式に対する I P Q o S パラメータを指定できるようにする。上述した無線リンク Q o S 管理は、一体化及び区別化の両サービスをベースとする I P Q o S 機構をサポートする。

しかしながら、当業者に明らかなように、このシステムの全ての要素が本発明にとって重要というのではなく、ある特徴は全く必要とされないし、一方、他の特徴は、単なる例示に過ぎず、従って、変更可能である。

【 0 1 3 8 】

本発明は、区別化サービスをサポートするシステムを提供することにある。即ち、異なる遅延及び無線 Q o S 特性を伴う複数の無線スケジューリング待ち行列又は無線流を有するシステムを提供することにある。上述した解決策は、ネットワークのオペレータ及び / 又は製造者が固定 I P (D S フィールド) と無線 Q o S との間のマッピングを特定ネットワークの所望の流れポリシーに基づいて規定できるようにする。例えば、流れクラス基準 (例えば、流れを検出するのにいかに多くの同様のパケットが必要とされるか) を動的に構成するし、そして区別化ビットをデフォルト待ち行列へいかにマッピングするか規定する自分自身のポリシーを指定することができる。

【 0 1 3 9 】

好ましい実施形態では、システムは、3つの無線スケジューリング待ち行列、即ち特別クラストラフィックに対する高プライオリティサービス待ち行列、保証型クラストラフィックに対する中間プライオリティサービス待ち行列、及び最良努力クラストラフィックに対する低プライオリティサービス待ち行列を有し、そして各プライオリティ待ち行列は、これら Q o S を定義する種々の無線スケジューリングパラメータを有する。しかし、デフォルトチャンネルの数は、ネットワーク要件に依存し、3より多くても少なくともよいことが明らかである。

上述したように、区別化サービスは、一般に、各 I P ヘッダにおけるプライオリティビットの展開を意味する。好ましい実施形態では、テーブル 1 及び 2 は、I P v 6 ヘッダに使用できるプライオリティクラスビットマッピングを示す。プライオリティビットの標準化はまだ実施されていないが、この概念を異なるヘッダ (例えば、I P v 4 に規定されたヘッダの T O S オクテット又は将来の規格で規定されるもの) にいかに適応させるかは、当業者に明らかであろう。

【 0 1 4 0 】

又、好ましい実施形態では、ネットワークエンティティ (M ルータ 5 2 / アクセスポイント 5 1 / 移動ターミナル 4) は、サービスフィールドの I P 形式を処理し、そして異なるパケットをデフォルト無線待ち行列の 1 つに分類する。パケットは、I P サービスマッピングがルータにおいて実行される場合に流れ特有の R A N 識別子でマークされる。次いで、移動ターミナル / アクセスポイントは、R A N 識別子をデコードし、そしてパケットを対応する無線流へとマッピングする。或いは又、アクセスポイントは、I P パケットヘッダから無線待ち行列への直接的な Q o S マッピングを実行することもできる。しかしながら、これらの機能の性能は、これらの要素に限定されない。例えば、マッピングは、

アクセスポイントコントローラにおいて実行することもできるし、又はそれがIPパケットハンドラーに含まれる場合には単一のアクセスポイントで実行することもできる。

【0141】

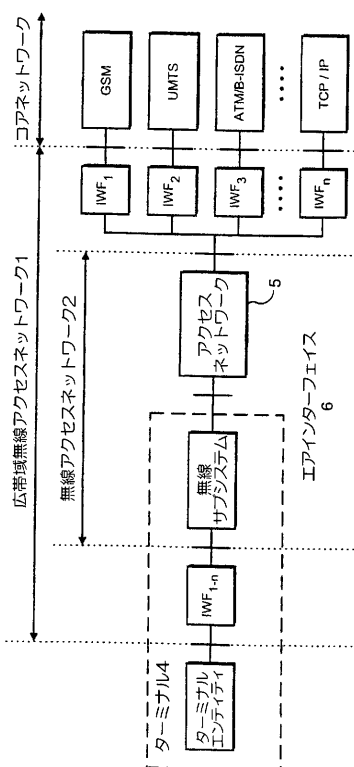
更に、IP流を検出するために好ましい実施形態に使用される流れ分類は、本発明にとって重要ではない。IP流の検出が必要とされる場合には、他の種々の基準を使用することができる。例えば、検出基準パラメータであるパケット/秒の値を変更することにより流れクラシファイアを動的に構成することができる。

本発明は、請求の範囲に記載した発明に係るか、本発明が向けられた問題のいずれか又は全部を軽減するかに関わらず、以上に開示した新規な特徴、又はそれら特徴の組合せを明確に包含し、或いはそれを一般化したものを包含する。

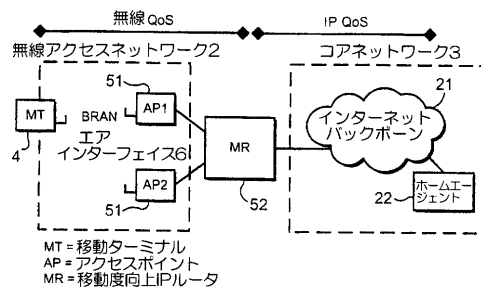
以上の説明から、本発明の範囲内で種々の変更がなされ得ることが当業者に明らかである。

10

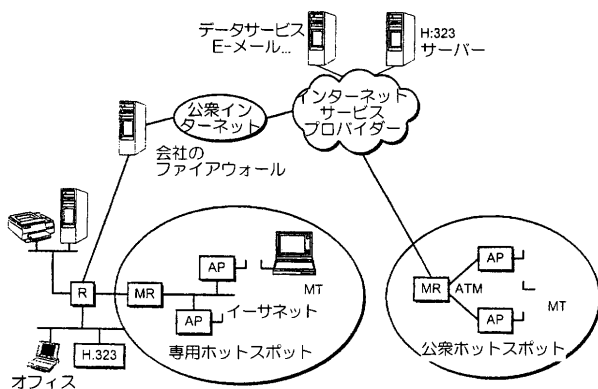
【図1】



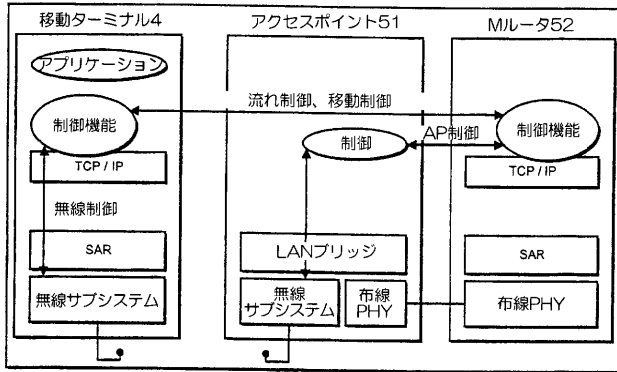
【図2】



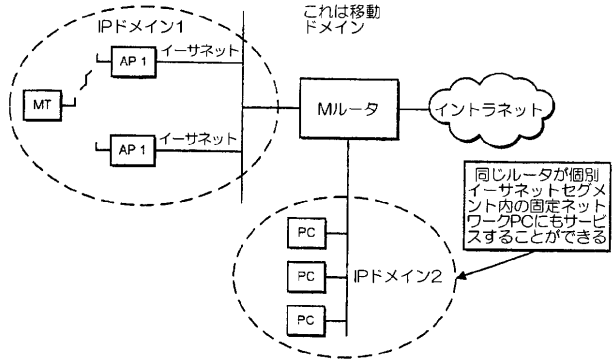
【図3】



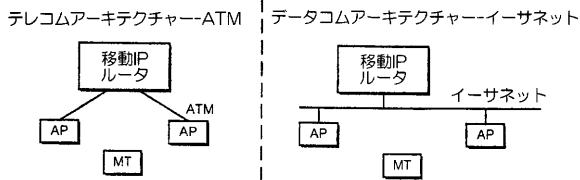
【図4】



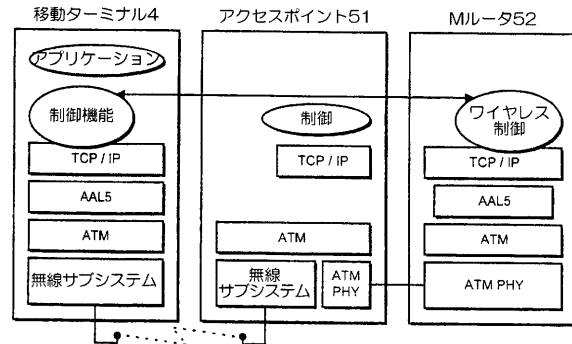
【図6】



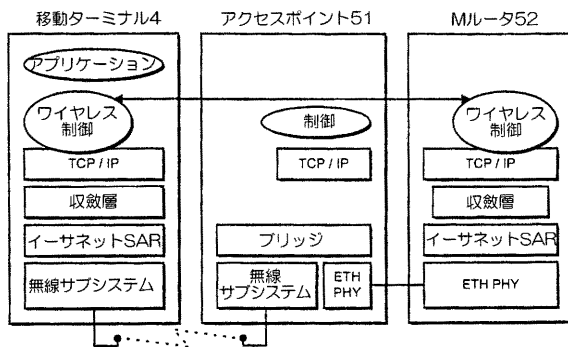
【図5】



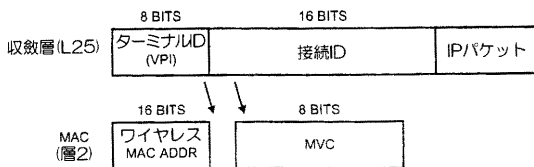
【図7】



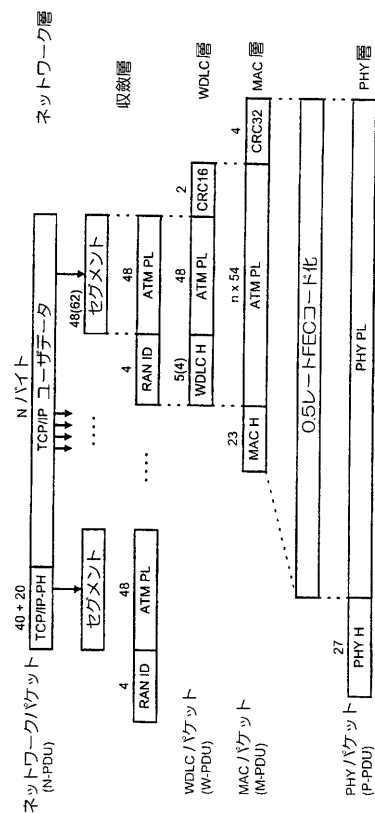
【図8】



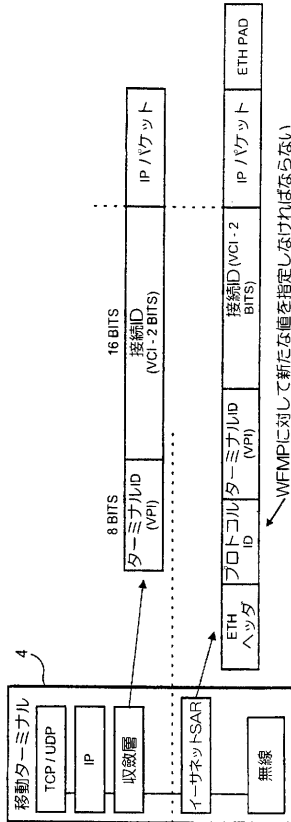
【図9】



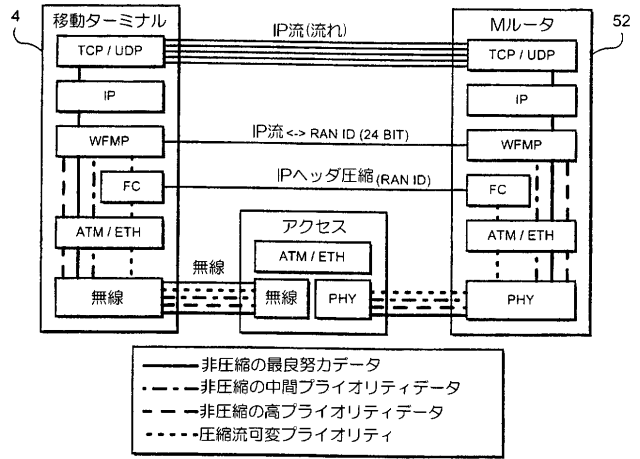
【図10】



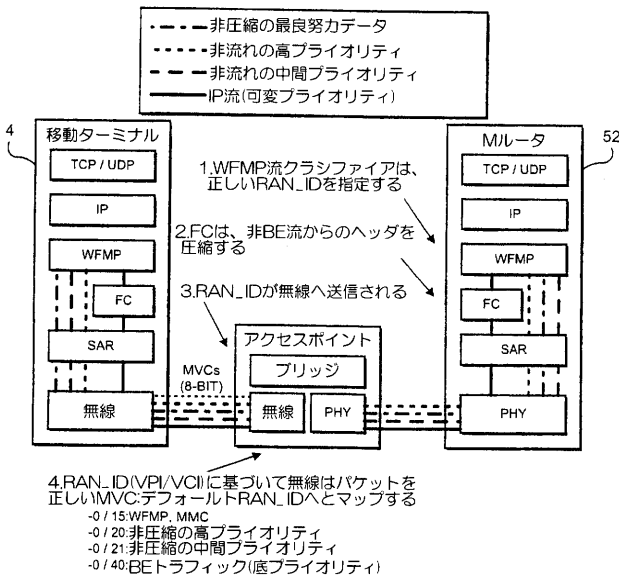
【図 1 1】



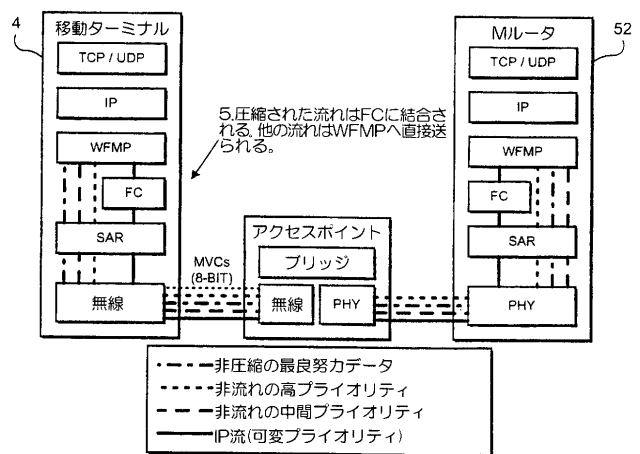
【図 1 2】



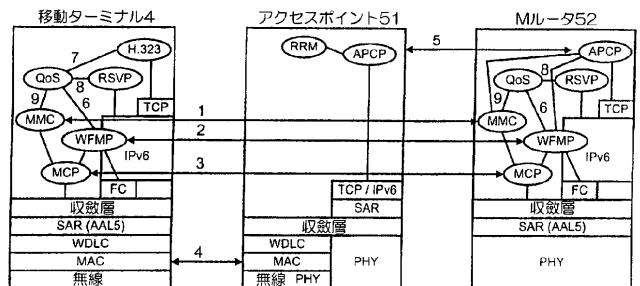
【図 1 3】



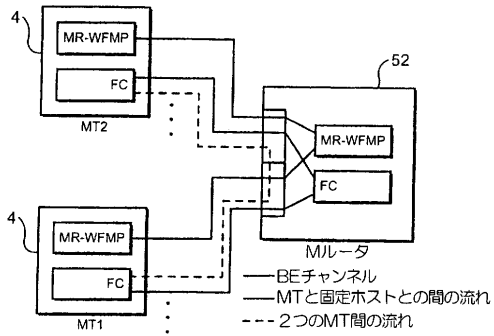
【図 1 4】



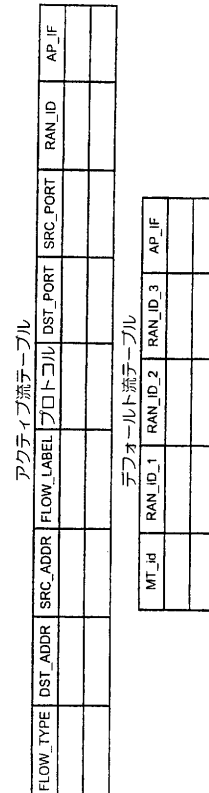
【図 1 5】



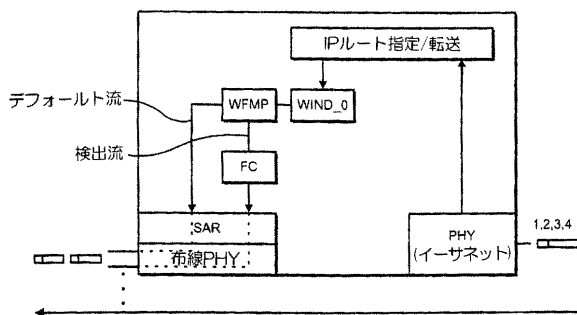
【 図 1 6 】



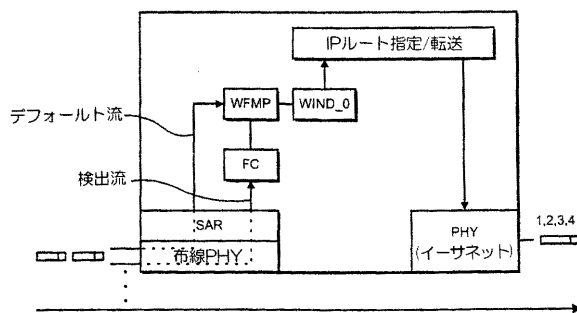
【 図 1 7 】



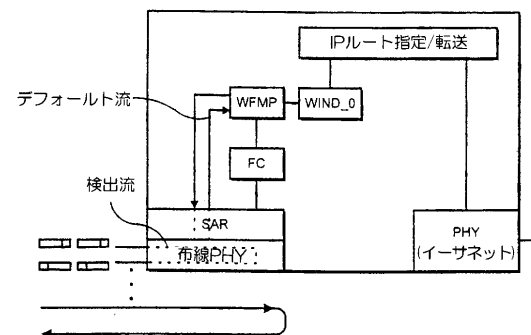
【 図 1 8 】



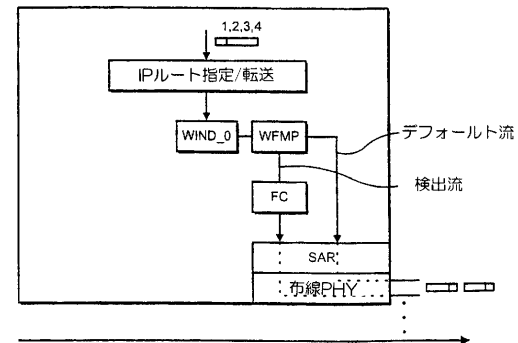
【 図 1 9 】



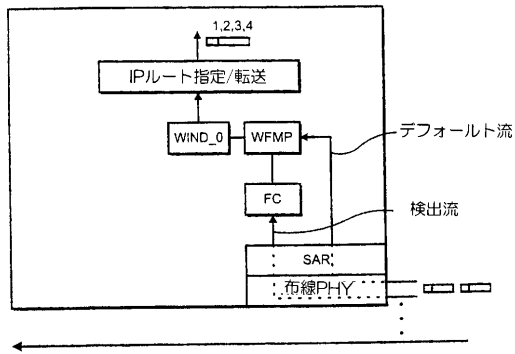
【 図 2 0 】



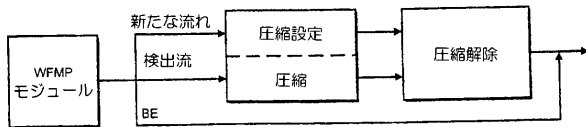
【 図 2 1 】



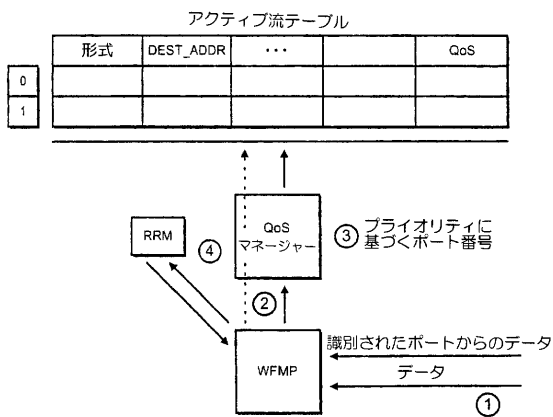
【図 2 2】



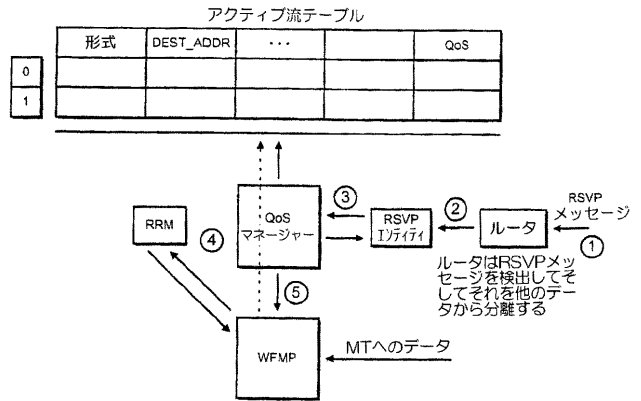
【図 2 3】



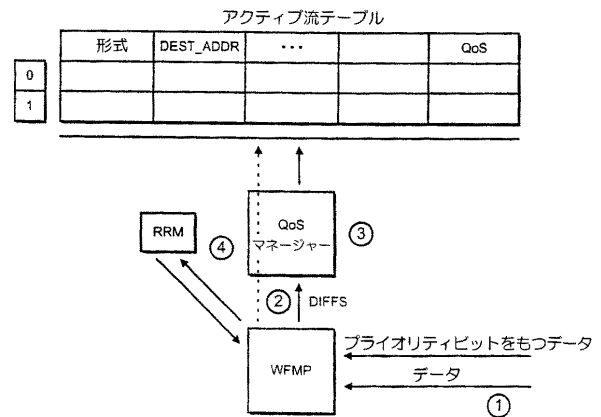
【図 2 6】



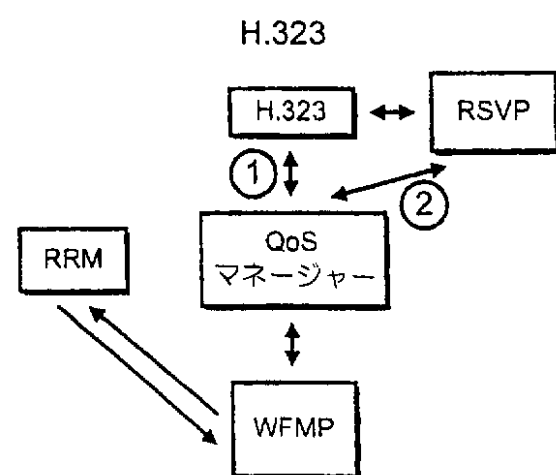
【図 2 4】



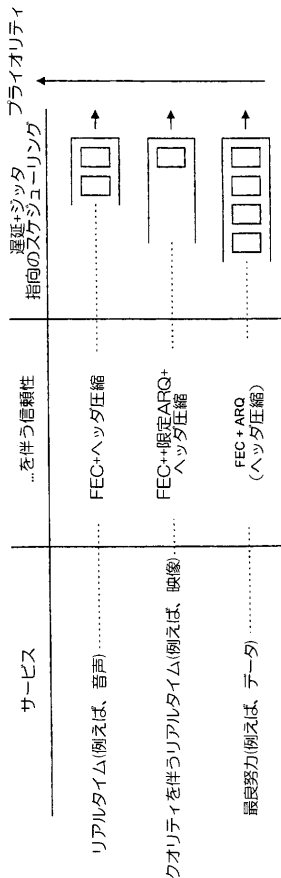
【図 2 5】



【図 2 7】



【図 28】



【手続補正書】

【提出日】平成21年10月2日(2009.10.2)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

少なくとも一つのアクセスポイント(51、51')及び移動ターミナル(4)を含む無線ネットワークの packets データ送信のサービスクオリティをサポートする方法であって、上記少なくとも一つのアクセスポイントと移動ターミナルとの間のエアインターフェースを経ての送信が無線流において行なわれ、上記無線ネットワークに移動度向上ルータ(52)が接続され、少なくとも一つの移動ターミナル(4)または当該ルータ(52)が流れ管理エンティティ(WFMP)を含むことにより、無線ネットワークの packets データ送信のサービスクオリティをサポートする方法において、

送信者(4、52)の上記流れ管理エンティティ(WFMP)において、異なるサービスクオリティ特性を有する移動ターミナルとそのアクセスポイントとの間の所定のデフォルト無線流の選択体(AFT、DFT)を形成する段階と、

上記選択体(AFT、DFT)から、エアインターフェースを経て送信されるべき packets に対して適切なサービスクオリティ特性を有する無線流を選択する段階を含むことを特徴とする方法。

【請求項2】

上記無線流を選択する段階は、送信されるべき packets に、異なるサービスクオリティ特性を表わす所定のデフォルト無線流識別子から選択された無線流識別子を与えること

を含む請求項 1 に記載の方法。

【請求項 3】

パケットを、エアインターフェイスを経て送信するための識別されたデフォルト無線流へとマッピングする段階を更に含む請求項 2 に記載の方法。

【請求項 4】

ある無線サブネットワークから別の無線サブネットワークへのアクティブな接続を有する移動通信装置のハンドオーバーを検出し、そして

ハンドオーバーの検出に応答してアクティブな接続に対しデフォルト無線流の選択を遂行する、という段階を更に含む請求項 1 ないし 3 のいずれかに記載の方法。

【請求項 5】

エアインターフェイスを経て送信されるべきパケットを監視して、IP 流を検出し、そして

検出された IP 流を、対応するサービスクオリティ特性を有する専用無線流へスイッチングする、という段階を更に含む請求項 1 ないし 3 のいずれかに記載の方法。

【請求項 6】

検出された IP 流を専用無線流にスイッチングする上記段階は、

検出された IP 流のパケットに専用無線流の識別子を与え、そして

検出された IP 流のパケットを、エアインターフェイスを経て送信するための識別された専用無線流へとマッピングする、という段階を含む請求項 5 に記載の方法。

【請求項 7】

エアインターフェイスを経てのデータパケット送信においてサービスクオリティをサポートするための無線アクセスシステムであって、少なくとも一つのアクセスポイント（51、51'）、移動ターミナル（4）、及び移動度向上ルータ（52）を含む無線アクセスシステムにおいて、

少なくとも一つの上記移動ターミナルまたは移動度向上ルータ（52）は、流れ管理エンティティ（WFMP）を含み、

上記流れ管理エンティティ（WFMP）は、異なるサービスクオリティ特性を有する移動ターミナルとそのアクセスポイントとの間の所定のデフォルト無線流の選択体（AFT、DFT）を形成し、

上記流れ管理エンティティ（WFMP）は、上記選択体（AFT、DFT）から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有する無線流を選択することを特徴とする無線アクセスシステム。

【請求項 8】

上記流れ管理エンティティ（WFMP）は、送信されるべきパケットに、所定のデフォルト無線流に対応する識別子から選択された無線流識別子（RAN ID）を与える請求項 7 に記載のシステム。

【請求項 9】

上記流れ管理エンティティ（WFMP）は、パケットを、エアインターフェイスを経て送信するための識別されたデフォルト無線流へとマッピングする請求項 8 に記載のシステム。

【請求項 10】

ある無線サブネットワークから別の無線サブネットワークへのアクティブな接続を有する移動通信装置のハンドオーバーを検出するための移動管理コントローラ（MMC）エンティティを更に備え、そして上記流れ管理エンティティ（WFMP）は、ハンドオーバーの検出に応答してアクティブな接続に対しデフォルト無線流を選択する請求項 7 ないし 9 のいずれかに記載のシステム。

【請求項 11】

上記流れ管理エンティティ（WFMP）は流れクラシファイアを更に備え、該流れクラシファイアは、

エアインターフェイスを経て送信されるべきパケットを監視して IP 流を検出し、

検出されたＩＰ流を、対応するサービスクオリティ特性を有する専用無線流へスイッチングする請求項 ７ ないし ９ のいずれかに記載のシステム。

【請求項 １ ２】

上記流れクラシファイアは、

検出されたＩＰ流のパケットに専用無線流の識別子を与え、

検出されたＩＰ流のパケットを、エアインターフェイスを経て送信するための識別された専用無線流へとマッピングする請求項 １ １ に記載のシステム。

【請求項 １ ３】

エアインターフェイスを経てのデータパケット送信においてサービスクオリティをサポートするものであって、異なるサービスクオリティ特性を有する所定のデフォルト無線流の選択体（ＡＦＴ、ＤＦＴ）を備えたシステムに使用するための装置であって、

上記選択体（ＡＦＴ、ＤＦＴ）から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有する移動ターミナルとそのアクセスポイントとの間のデフォルト無線流を選択する流れ管理エンティティ（ＷＦＭＰ）を含むことを特徴とする装置（４、５２）。

【請求項 １ ４】

上記装置は、移動通信装置（４）又は移動ルータ（５２）である請求項 １ ３ に記載の装置。

【請求項 １ ５】

請求項 ７ に記載のシステムに使用するための請求項 １ ３ 又は １ ４ に記載の装置。

【請求項 １ ６】

少なくとも一つのアクセスポイント（５１、５１'）及び移動ターミナル（４）を含む無線ネットワークのパケットデータ送信のサービスクオリティをサポートするためのシステムであって、上記少なくとも一つのアクセスポイントと移動ターミナルとの間のエアインターフェイスを経ての送信が無線流において行なわれ、上記無線ネットワークに移動度向上ルータ（５２）が接続され、少なくとも一つの移動ターミナル（４）または当該ルータ（５２）が流れ管理エンティティ（ＷＦＭＰ）を含むシステムにおける移動ターミナル（４）または当該ルータ（５２）に、

異なるサービスクオリティ特性を有する移動ターミナルとそのアクセスポイントとの間の所定のデフォルト無線流の選択体（ＡＦＴ、ＤＦＴ）を形成し、

上記選択体（ＡＦＴ、ＤＦＴ）から、エアインターフェイスを経て送信されるべきパケットに対して適切なサービスクオリティ特性を有する無線流を選択する手順を実行させることを特徴とするプログラムを記憶するコンピュータ読み取り可能な記憶媒体。

フロントページの続き

(74)代理人 100084663

弁理士 箱田 篤

(72)発明者 ミッコネン ヨウニ

フィンランド エフイーエン - 3 3 8 2 0 タムペレ カーボンクヤ 3 アー 4

(72)発明者 ソデルンド トム

フィンランド エフイーエン - 0 0 2 0 0 ヘルシンキ イエルデニニット 8 アー 1 8

(72)発明者 アラ ローリラ ユハ

フィンランド エフイーエン - 3 3 2 1 0 タムペレ ムスタンラーデンカテュ 1 0 アー 5

(72)発明者 イモネン ユッカ

アメリカ合衆国 マサチューセッツ州 0 1 8 0 3 バーリントン バーリントン ウッズ ドラ
イブ 3 スウィート 2 5 0 ノキア リサーチ センター

F ターム(参考) 5K067 AA21 BB04 BB21 CC08 DD11 DD17 EE02 EE10 EE16 FF02

HH22 HH23