

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6976411号

(P6976411)

(45) 発行日 令和3年12月8日 (2021. 12. 8)

(24) 登録日 令和3年11月11日 (2021. 11. 11)

(51) Int. Cl.

F I

HO 4 W 76/11 (2018. 01)

HO 4 W 76/11

HO 4 W 12/06 (2021. 01)

HO 4 W 12/06

HO 4 W 48/16 (2009. 01)

HO 4 W 48/16

HO 4 W 8/26 (2009. 01)

HO 4 W 8/26

HO 4 L 12/70 (2013. 01)

HO 4 L 12/70

A

請求項の数 23 (全 25 頁)

(21) 出願番号 特願2020-504757 (P2020-504757)
 (86) (22) 出願日 平成30年4月18日 (2018. 4. 18)
 (65) 公表番号 特表2020-517207 (P2020-517207A)
 (43) 公表日 令和2年6月11日 (2020. 6. 11)
 (86) 国際出願番号 PCT/CN2018/083565
 (87) 国際公開番号 W02018/192528
 (87) 国際公開日 平成30年10月25日 (2018. 10. 25)
 審査請求日 令和1年10月9日 (2019. 10. 9)
 (31) 優先権主張番号 201710253160.0
 (32) 優先日 平成29年4月18日 (2017. 4. 18)
 (33) 優先権主張国・地域又は機関
 中国 (CN)

(73) 特許権者 503433420
 華為技術有限公司
 HUAWEI TECHNOLOGIES
 CO., LTD.
 中華人民共和国 518129 広東省深
 ▲チェン▼市龍崗区坂田 華為總部▲ベン
 ▼公樓
 Huawei Administration Building, Bantian,
 Longgang District, Shenzhen, Guangdong
 518129, P. R. China
 (74) 代理人 100110364
 弁理士 実広 信哉

最終頁に続く

(54) 【発明の名称】 ネットワークアクセス方法および装置ならびにネットワークデバイス

(57) 【特許請求の範囲】

【請求項 1】

固定コアネットワークとモバイルコアネットワークにプロトコルの互換性がない場合におけるネットワークアクセス方法であって、前記方法が、アクセスゲートウェイによって実行され、

ユーザ端末からポイントツーポイントオーバーイーサネット (PPPoE) メッセージまたはインターネットプロトコルオーバーイーサネット (IPoE) メッセージを受信するステップと、

前記PPPoEメッセージまたは前記IPoEメッセージに含まれる前記ユーザ端末のアクセス情報を取得するステップと、

前記アクセス情報を非アクセス層 (NAS) メッセージにカプセル化するステップと、

前記NASメッセージを制御プレーン (CP) 機能エンティティに送信するステップと、

前記CP機能エンティティからネットワークインタフェース情報を受信し、前記ネットワークインタフェース情報を前記ユーザ端末に送信するステップであって、前記ネットワークインタフェース情報は、前記ユーザ端末が、ネットワークにアクセスするために使用される、ステップと

を含む、ネットワークアクセス方法。

【請求項 2】

前記アクセス情報が、ユーザ端末識別子、または固定ネットワークアクセスポイント識別子のうちの少なくとも1つを含み、

前記ユーザ端末識別子が、ユーザ端末永久識別子、ユーザ端末一時識別子、ユーザ端末メディアアクセス制御（MAC）アドレス、ユーザ端末ネットワークアクセス識別子（NAI）、ユーザ端末ユーザ名、またはエージェントリモート識別子のうちの少なくとも1つであり、

前記固定ネットワークアクセスポイント識別子が、回線識別子、物理的位置識別子、および論理識別子のうちの少なくとも1つである、

請求項1に記載のネットワークアクセス方法。

【請求項3】

前記アクセス情報をNASメッセージにカプセル化する前記ステップが、

NAS要求メッセージを生成し、前記アクセス情報を前記NAS要求メッセージに追加するステップであって、前記NAS要求メッセージが、登録要求メッセージまたはプロトコルデータユニット、PDU、セッション確立要求メッセージである、ステップと、

ユーザ端末初期化メッセージを送信し、前記NAS要求メッセージを前記ユーザ端末初期化メッセージに追加するステップ

を含む、請求項1または2に記載のネットワークアクセス方法。

【請求項4】

前記アクセス情報が、固定ネットワークアクセスポイント識別子を含む場合、前記NASメッセージをCP機能エンティティに送信する前記ステップの後、かつ前記CP機能エンティティからネットワークインタフェース情報を受信する前記ステップの前に、

前記CP機能エンティティによって、前記固定ネットワークアクセスポイント識別子を認証エンティティに送信するステップと、

前記固定ネットワークアクセスポイント識別子に基づいて前記認証エンティティによって実行された認証の結果を前記CP機能エンティティによって受信するステップと、

前記認証の前記結果が前記認証が成功したことであるときに前記CP機能エンティティによって前記ユーザ端末のための前記ネットワークインタフェース情報を構成するステップと

をさらに含む、請求項1または2に記載のネットワークアクセス方法。

【請求項5】

前記アクセス情報が固定ネットワークアクセスポイント識別子を含む場合、前記NASメッセージをCP機能エンティティに送信する前記ステップの後、かつ前記CP機能エンティティからネットワークインタフェース情報を受信する前記ステップの前に、前記方法が、特に、

前記CP機能エンティティが前記アクセス情報を認証エンティティに送信した後に、前記CP機能エンティティによって、前記固定ネットワークアクセスポイント識別子に基づいて前記認証エンティティによって送信された認証ベクトルを受信するステップと、

前記CP機能エンティティによって、前記認証ベクトルに基づいてchallenge値を生成し、前記challenge値を前記アクセスゲートウェイに送信するステップと、

前記アクセスゲートウェイによって、ユーザ名およびパスワードを取得するための要求を前記ユーザ端末に送信するステップであって、前記要求が、前記challenge値を含み、前記パスワードが、前記challenge値および初期パスワードに対してハッシュ演算を実行することにより前記ユーザ端末によって取得される、ステップと、

前記アクセスゲートウェイによって前記ユーザ名および前記パスワードを受信するステップと、

前記アクセスゲートウェイによって前記ユーザ名および前記パスワードを前記CP機能エンティティに送信するステップと、

前記CP機能エンティティによって前記ユーザ名および前記パスワードを前記認証エンティティに送信するステップであって、これにより、前記認証エンティティが、前記ユーザ名および前記パスワードに基づいて認証を実行する、ステップと

を含む、請求項1または2に記載のネットワークアクセス方法。

【請求項6】

前記CP機能エンティティによって前記ユーザ端末のための前記ネットワークインタフェース情報を構成する前記ステップが、

前記CP機能エンティティのセッション管理機能エンティティによって、インターネットプロトコル、IP、アドレスまたは動的ホスト構成プロトコル、DHCP、サーバアドレスのうちの少なくとも一方を前記ユーザ端末に割り当てるステップと、

前記CP機能エンティティのモビリティ機能エンティティによって、NAS返信メッセージを生成し、前記IPアドレスまたは前記DHCPサーバアドレスのうちの少なくとも一方を前記NAS返信メッセージに追加し、前記ネットワークインタフェース情報を取得するステップと

を含む、請求項4に記載のネットワークアクセス方法。

10

【請求項7】

前記NAS返信メッセージが、ロケーションエリア識別子を含み、前記ロケーションエリア識別子が、ヌル値、固定ネットワークエリア識別子、特別なロケーションエリア識別子、または回線識別子に設定される、

請求項6に記載のネットワークアクセス方法。

【請求項8】

前記CP機能エンティティによって送信されたネットワークインタフェース情報を受信し、前記ネットワークインタフェース情報を前記ユーザ端末に送信する前記ステップが、

前記ネットワークインタフェース情報内の少なくとも前記IPアドレスを読み取るステップと、

20

IP構成メッセージまたはネットワーク制御プロトコル、NCP、メッセージを使用して少なくとも前記IPアドレスを前記ユーザ端末に送信するステップと

を含む、請求項6に記載のネットワークアクセス方法。

【請求項9】

前記PPPoEメッセージが、PPPoEアクティブディスカバリ指示（PADI）メッセージ、PPPoEアクティブディスカバリ要求（PADR）メッセージ、リンク制御プロトコル（LCP）メッセージ、またはNCPメッセージを含み、

前記IPoEメッセージが、DHCPディスカバリメッセージまたはDHCP要求メッセージを含む、

請求項1に記載のネットワークアクセス方法。

30

【請求項10】

固定コアネットワークとモバイルコアネットワークにプロトコルの互換性がない場合に動作可能なネットワークアクセス装置であって、

ユーザ端末からポイントツーポイントオーバーサネット（PPPoE）メッセージまたはインターネットプロトコルオーバーサネット（IPoE）メッセージを受信し、前記PPPoEメッセージまたは前記IPoEメッセージに含まれる前記ユーザ端末のアクセス情報を取得するように構成された取得モジュールと、

前記アクセス情報を非アクセス層（NAS）メッセージにカプセル化するように構成されたカプセル化モジュールと、

前記NASメッセージを制御プレーン（CP）機能エンティティに送信するように構成された送信モジュールと、

40

前記CP機能エンティティによって送信されたネットワークインタフェース情報を受信し、前記ネットワークインタフェース情報を前記ユーザ端末に送信し、前記ネットワークインタフェース情報は、前記ユーザ端末が、ネットワークにアクセスするために使用される、ように構成された受信モジュールと

を備える、ネットワークアクセス装置。

【請求項11】

前記カプセル化モジュールが、生成ユニットおよび送信ユニットを備え、

前記生成ユニットが、NAS要求メッセージを生成し、前記アクセス情報を前記NAS要求メッセージに追加し、前記NAS要求メッセージが、登録要求メッセージまたはプロトコルデ

50

ータユニット（PDU）セッション確立要求メッセージである、ように構成されており、

前記送信ユニットが、ユーザ端末初期化メッセージを送信し、前記NAS要求メッセージを前記ユーザ端末初期化メッセージに追加するように構成されている、請求項10に記載のネットワークアクセス装置。

【請求項12】

固定コアネットワークとモバイルコアネットワークにプロトコルの互換性がない場合に動作可能な、プロセッサおよび通信インタフェースを備えるネットワークデバイスであって、

前記通信インタフェースが、ユーザ端末からポイントツーポイントオーバーサネット（PPPoE）メッセージまたはインターネットプロトコルオーバーサネット（IPoE）メッセージを受信するように構成されており、

前記プロセッサが、前記PPPoEメッセージまたは前記IPoEメッセージに含まれる前記ユーザ端末のアクセス情報を取得し、前記アクセス情報を非アクセス層（NAS）メッセージにカプセル化するように構成されており、

前記通信インタフェースが、ネットワークインタフェース情報を前記ユーザ端末に送信し、前記ネットワークインタフェース情報は、前記ユーザ端末が、ネットワークにアクセスするために使用される、ようにさらに構成されている、ネットワークデバイス。

【請求項13】

前記プロセッサが前記アクセス情報を前記NASメッセージにカプセル化することが、以下のように実行され、すなわち、

前記プロセッサが、NAS要求メッセージを生成し、前記アクセス情報を前記NAS要求メッセージに追加し、ユーザ端末初期化メッセージを生成し、前記NAS要求メッセージを前記ユーザ端末初期化メッセージに追加するようにさらに構成されている、請求項12に記載のネットワークデバイス。

【請求項14】

前記アクセス情報を前記非アクセス層（NAS）メッセージにカプセル化した後、前記プロセッサが、

前記アクセス情報内のユーザ端末識別子および固定ネットワークアクセスポイント識別子のうちの少なくとも一方に基づいて認証を実行し、認証結果を取得し、前記認証結果が前記認証が成功したことでありときに前記ユーザ端末のための前記ネットワークインタフェース情報を構成するようにさらに構成されている、請求項12に記載のネットワークデバイス。

【請求項15】

前記アクセス情報内の前記固定ネットワークアクセスポイント識別子に基づいて認証を実行することは、

前記プロセッサが、前記固定ネットワークアクセスポイント識別子に基づいて認証ベクトルを検索し、前記認証ベクトルに基づいてchallenge値を生成し、

前記通信インタフェースが、前記challenge値を前記ユーザ端末に送信し、前記ユーザ端末によって送信されたユーザ名およびパスワードを受信し、

前記プロセッサが、前記ユーザ名、前記パスワード、および前記challenge値に基づいて認証を実行し、認証結果を取得する、ように実行される、請求項14に記載のネットワークデバイス。

【請求項16】

前記プロセッサが前記ユーザ端末のための前記ネットワークインタフェース情報を構成することが、

セッション管理機能エンティティを使用してインターネットプロトコルアドレスIPアドレスおよびホスト構成プロトコル（DHCP）サーバアドレスのうちの少なくとも一方を前記ユーザ端末に割り当て、モバイル機能エンティティを使用してNAS返信メッセージを生成し、前記IPアドレスおよび前記DHCPサーバアドレスのうちの少なくとも一方を前記NAS返信メッセージに追加し、前記ネットワークインタフェース情報を取得することとして実行

される、請求項14に記載のネットワークデバイス。

【請求項17】

前記通信インタフェースが前記ネットワークインタフェース情報を前記ユーザ端末に送信することが、特に、

前記通信インタフェースがIP構成メッセージまたはネットワーク制御プロトコル（NCP）メッセージを使用して前記IPアドレスおよび前記DHCPサーバアドレスのうちの少なくとも一方を前記ユーザ端末に送信することとして実行される、請求項12に記載のネットワークデバイス。

【請求項18】

固定コアネットワークとモバイルコアネットワークにプロトコルの互換性がない場合に動作可能な、アクセスゲートウェイおよび制御プレーン（CP）機能エンティティを備えるネットワークアクセスシステムであって、

前記アクセスゲートウェイが、ユーザ端末からポイントツーポイントオーバーサネット（PPPoE）メッセージまたはインターネットプロトコルオーバーサネット（IPoE）メッセージを受信し、前記PPPoEメッセージまたは前記IPoEメッセージに含まれる前記ユーザ端末のアクセス情報を取得し、前記アクセス情報を非アクセス層（NAS）メッセージにカプセル化し、前記NASメッセージを前記CP機能エンティティに送信するように構成されており、

前記CP機能エンティティが、前記NASメッセージを受信し、ネットワークインタフェース情報を前記アクセスゲートウェイに送信するように構成されており、

前記アクセスゲートウェイが、前記ネットワークインタフェース情報を受信し、前記ネットワークインタフェース情報を前記ユーザ端末に送信し、前記ネットワークインタフェース情報が、ネットワークにアクセスするために使用される、ように構成されている、

ネットワークアクセスシステム。

【請求項19】

前記アクセスゲートウェイが、

NAS要求メッセージを生成し、前記アクセス情報を前記NAS要求メッセージに追加し、前記NAS要求メッセージが、登録要求メッセージまたはプロトコルデータユニット（PDU）セッション確立要求メッセージであり、ユーザ端末初期化メッセージを送信し、前記NAS要求メッセージを前記ユーザ端末初期化メッセージに追加する

ように構成されている、請求項18に記載のネットワークアクセスシステム。

【請求項20】

前記アクセス情報が、固定ネットワークアクセスポイント識別子を含み、

前記CP機能エンティティが、前記アクセス情報内のユーザ端末識別子または固定ネットワークアクセスポイント識別子のうちの少なくとも一方に基づいて認証を実行し、認証結果を取得し、前記認証結果が前記認証が成功したことであるときに前記ユーザ端末のための前記ネットワークインタフェース情報を構成するようにさらに構成されている、請求項18に記載のネットワークアクセスシステム。

【請求項21】

前記CP機能エンティティが、

前記固定ネットワークアクセスポイント識別子に基づいて認証ベクトルを検索し、前記認証ベクトルに基づいてchallenge値を生成し、

前記challenge値を前記ユーザ端末に送信し、前記ユーザ端末からユーザ名およびパスワードを受信し、

前記ユーザ名、前記パスワード、および前記challenge値に基づいて認証を実行し、認証結果を取得する

ように構成されている、請求項20に記載のネットワークアクセスシステム。

【請求項22】

前記CP機能エンティティが、

セッション管理機能エンティティを使用してインターネットプロトコル（IP）アドレス

10

20

30

40

50

またはホスト構成プロトコル（DHCP）サーバアドレスのうちの少なくとも一方を前記ユーザ端末に割り当て、モバイル機能エンティティを使用してNAS返信メッセージを生成し、前記IPアドレスおよび前記DHCPサーバアドレスのうちの少なくとも一方を前記NAS返信メッセージに追加し、前記ネットワークインタフェース情報を取得するように構成されている、請求項20に記載のネットワークアクセスシステム。

【請求項23】

請求項1から4のいずれか一項に記載のネットワークアクセス方法をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【技術分野】

10

【0001】

本願は、2017年4月18日に中国国家知識産権局に提出された、「ネットワークアクセス方法および装置ならびにネットワークデバイス」という名称の中国特許出願第201710253160.0号の優先権を主張し、その全体は、参照によりここに組み込まれる。

【0002】

本願は、通信技術の分野に関し、具体的には、ネットワークアクセス方法および装置ならびにネットワークデバイスに関する。

【背景技術】

【0003】

現在、UE（User Equipment、ユーザ機器）の機能の改善により、UEは、ネットワーク動作を実行するために広く使用されている。UEがネットワーク動作を実行するために使用される前、通常、UEは、ネットワークにアクセスできるようにされなければならない。従来技術では、UEは、オペレータによって提供されるコアネットワークを介してネットワークにアクセスし得る。許可されていないUEがネットワークにアクセスするのを防止し、許可されたUEのセキュリティを確保するために、ネットワークアクセス認証機能が、コアネットワークに設定されている。UEによって送信されたアクセス情報が受信されると、通常、UEのアイデンティティが認証されるかどうかを検証するためにネットワークアクセス認証がUEにおいて実行される。認証が成功した後、UEがネットワークにアクセスできるようにするために、ネットワークポートがUEに割り当てられる。

20

【0004】

具体的には、コアネットワークは、特定のタイプのプロトコルスタックをサポートし、制御エンティティおよび認証エンティティが、コアネットワークに配置される。認証されるUEが、コアネットワークにアクセス情報を送信すると、コアネットワークの制御エンティティは、対応するプロトコルタイプに基づいてアクセス情報からパラメータを抽出し、後続の動作を実行する。例えば、固定されたネットワーク（簡単に固定ネットワークと呼ばれる）のコアネットワークは、PPPoE（Point to Point Protocol over Ethernet、ポイントツーポイント接続プロトコル）／IPoE（Internet Protocol over Ethernet、動的ホスト構成プロトコル）プロトコルスタックをサポートする。固定コアネットワークが、UEのアクセス情報を受信すると、固定コアネットワークに配置されたBNG（Broadband Network Gateway、ブロードバンドネットワークゲートウェイ）制御デバイスが、PPPoE／IPoEプロトコルタイプに基づいてアクセス情報からUE識別子および認証パラメータを抽出し、認証を実行するために、抽出された認証パラメータをAAA（Authentication, Authorization and Account、認証、許可、およびアカウント機能）デバイスに送信する。認証パラメータで認証を実行した後、AAAは、認証結果をBNGに送信する。認証が成功すると、BNGは、DHCP（Dynamic Host Configuration Protocol、動的ホスト構成プロトコル）サーバからIP（Internet Protocol、ネットワークプロトコル）アドレスを取得し、PPPoE／IPoEプロトコルタイプを使用してIPアドレスをUEに送信し、これにより、UEは、IPアドレスを使用してネットワークにアクセスする。

30

40

【0005】

もちろん、固定コアネットワークに加えて、従来技術では、UEは、モバイルネットワー

50

ク（簡単にモバイルと呼ばれる）のコアネットワークにもアクセスし得る。しかしながら、モバイルコアネットワークは、PPPoE/IPoEのプロトコルスタックをサポートしていない。したがって、固定コアネットワークおよびモバイルコアネットワークは相互に互換性があり得ない。オペレータが完全なサービスを提供する場合、固定コアネットワークおよびモバイルコアネットワークの両方が展開される必要がある。これは、大量のリソースおよび不都合なメンテナンスを必要とする。

【発明の概要】

【課題を解決するための手段】

【0006】

本願は、固定コアネットワークとモバイルコアネットワークの非互換性の問題を解決するためにネットワークアクセス方法および装置ならびにネットワークデバイスを提供する。

10

【0007】

第1の態様によれば、本願は、ネットワークアクセス方法を提供する。アクセスゲートウェイが、ユーザ端末によって送信されたメッセージを受信すると、アクセスゲートウェイは最初に、メッセージがPPPoEメッセージまたはIPoEメッセージとNASメッセージまたはEAPメッセージとのどちらであるかを判定するためにメッセージのタイプを判定し得る。メッセージがPPPoEメッセージまたはIPoEメッセージである場合、アクセスゲートウェイは、PPPoEメッセージまたはIPoEメッセージからユーザ端末のアクセス情報を読み取り、アクセス情報のタイプを変換するために、アクセス情報をNAS（Non-access stratum、非アクセス層）メッセージまたはEAP（Extensible Authentication Protocol、拡張可能認証プロトコル）メッセージにカプセル化し、次に、NASメッセージまたはEAPメッセージをCP（Control plane function、制御プレーン）機能エンティティに送信する。CPは、認証されたユーザ端末のためのネットワークインタフェース情報を構成し、ネットワークインタフェース情報をアクセスゲートウェイに送信する。次に、アクセスゲートウェイは、ネットワークインタフェース情報をユーザ端末に送信する。このようにして、ユーザ端末は、ネットワークインタフェース情報に基づいてネットワークにアクセスし得る。

20

【0008】

このことから分かるように、この実施態様によれば、アクセスゲートウェイは、受信されたメッセージのタイプを判定し、メッセージを、ネットワークデバイスの別のネットワーク要素によって識別され得るタイプに変換し得、これにより、ユーザ端末は、ネットワークにアクセスする。言い換えれば、この解決策では、異なるプロトコルスタックタイプは相互に互換性があり得、このため、ユーザ端末は、ネットワークにアクセスするときに制限されない。したがって、完全なサービスは、ただ1つのコアネットワークを展開することによって提供され得る。これは、リソースを節約するだけでなく、ネットワークのメンテナンスも容易にする。

30

【0009】

第1の態様に関連して、第1の態様の第1の可能な実施態様では、アクセス情報は、セッション識別子、ユーザ端末識別子、および固定ネットワークアクセスポイント識別子のうちの少なくとも1つを含む。セッション識別子は、アクセスゲートウェイによってユーザ端末に割り当てられる。ユーザ端末識別子は、ユーザ端末永久識別子、ユーザ端末一時識別子、ユーザ端末物理MAC（Media Access Control、物理アドレス）アドレス、ユーザ端末ネットワークアクセス識別子NAI（Network Access Identifier、ネットワークアクセス識別子）、ユーザ端末ユーザ名、およびエージェントリモート識別子（Agent Remote ID）のうちの少なくとも1つである。固定ネットワークアクセスポイント識別子は、回線識別子（circuit ID）、物理的位置識別子、および論理識別子のうちの少なくとも1つである。

40

【0010】

この実施態様によれば、様々な形式のアクセス情報のタイプが識別および変換され得、このため、この解決策はより広く適用可能であり、機能がより完全になる。

50

【0011】

第1の態様に関連して、第1の態様の第2の可能な実施態様では、アクセスゲートウェイがアクセス情報をNASメッセージにカプセル化することは、アクセスゲートウェイがNAS要求メッセージを生成し、アクセス情報をNAS要求メッセージに追加することを含む。次に、アクセスゲートウェイは、ユーザ端末初期化メッセージを送信し、NAS要求メッセージをユーザ端末初期化メッセージに追加する。

【0012】

さらに、アクセス情報が、3つのタイプのメッセージ、すなわち、セッション識別子、ユーザ端末識別子、および固定ネットワークアクセスポイント識別子を含む場合、アクセスゲートウェイがアクセス情報をNASメッセージにカプセル化することは、アクセスゲートウェイがユーザ端末初期化メッセージを送信し、アクセス情報内の固定ネットワークアクセスポイント識別子およびセッション識別子のうちの少なくとも一方をユーザ端末初期化メッセージに追加することを含む。アクセスゲートウェイは、NAS要求メッセージを生成し、アクセス情報内のユーザ端末識別子をNAS要求メッセージに追加し、NAS要求メッセージをユーザ端末初期化メッセージに追加する。

10

【0013】

NAS要求メッセージは、登録要求メッセージまたはPDU (Protocol Data Unit、プロトコルデータユニット) セッション確立要求メッセージであり得る。

【0014】

第1の態様に関連して、第1の態様の第3の可能な実施態様では、アクセスゲートウェイがアクセス情報をEAPメッセージにカプセル化することは、アクセスゲートウェイがEAPメッセージを生成し、アクセス情報をEAPメッセージに追加することを含む。次に、アクセスゲートウェイは、登録要求メッセージを生成し、EAPメッセージを登録要求メッセージに追加する。さらに、アクセスゲートウェイは、ユーザ端末初期化メッセージを送信し、登録要求メッセージをユーザ端末初期化メッセージに追加する。

20

【0015】

このことから分かるように、この実施態様によれば、アクセスゲートウェイは、アクセス情報の特定の内容に基づいてアクセス情報を異なるタイプのメッセージに変換し得、変換は柔軟に実行され得、このため、この解決策は、より柔軟に実行され得、より広く適用可能である。

30

【0016】

第1の態様に関連して、第1の態様の第4の可能な実施態様では、アクセスゲートウェイによって送信されたNASメッセージまたはEAPメッセージを受信した後、CPは最初に、NASメッセージまたはEAPメッセージからアクセス情報を読み取り得る。アクセス情報が、ユーザ端末識別子および固定ネットワークアクセスポイント識別子のうちの少なくとも一方を含む場合、CPは、固定ネットワークアクセスポイント識別子およびユーザ端末識別子のうちの少なくとも一方に基づいて認証を実行するように認証エンティティをトリガするために、固定ネットワークアクセスポイント識別子およびユーザ端末識別子のうちの少なくとも一方を認証エンティティに送信する。認証を完了した後、認証エンティティは、認証の結果をCPに送信する。

40

【0017】

第1の態様に関連して、第1の態様の第5の可能な実施態様では、アクセス情報が固定ネットワークアクセスポイント識別子を含む場合、CPは最初に、固定ネットワークアクセスポイント識別子を認証エンティティに送信し、固定ネットワークアクセスポイント識別子に応答して認証エンティティによって送信された認証ベクトルを受信し得る。次に、CPは、認証ベクトルに基づいてchallenge値を生成し、ユーザ端末のユーザ名およびパスワードを取得するための要求にchallenge値を追加し、この要求をアクセスゲートウェイに送信する。ユーザ端末によって送信されたユーザ名およびパスワードを受信した後、アクセスゲートウェイは、ユーザ名およびパスワードをCPに送信する。CPは、認証情報としてユーザ名およびパスワードを認証エンティティに送信する。

50

【0018】

このことから分かるように、この実施態様によれば、固定ネットワークアクセスポイント識別子は、認証のためのパラメータとしてさらに使用され得る。さらに、アクセスゲートウェイがchallenge値を割り当てる従来技術と比較して、この実施態様では、CPがchallenge値を生成し、このため、アクセスゲートウェイのデータ処理量が低減され得、その結果、アクセスゲートウェイの動作が簡素化される。

【0019】

第1の態様に関連して、第1の態様の第6の可能な実施態様では、CPが認証エンティティによって送信された認証成功メッセージを受信した後、CPのSMF (Session Management Function、セッション管理機能) エンティティは、ユーザ端末のためにIPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方を構成し得る。さらに、IPアドレスおよび／またはDHCPサーバアドレスを構成した後、CPのAMF (Core Access and Mobility Management Function、モバイル機能) エンティティは、NAS返信メッセージを生成し、IPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方をNAS返信メッセージに追加し、ネットワークインタフェース情報を取得する。

10

【0020】

第1の態様に関連して、第1の態様の第7の可能な実施態様では、NAS返信メッセージは、ロケーションエリア識別子を含み、ロケーションエリア識別子は、ヌル値、固定ネットワークエリア識別子、特別なロケーションエリア識別子、または回線識別子に設定されることに留意されたい。具体的には、ロケーションエリア識別子は、要求に基づいて設定され得る。

20

【0021】

この実施態様では、CPは、ユーザ端末の特徴に基づいて、ユーザ端末に適したネットワークインタフェース情報を構成し得、ネットワークインタフェース情報の異なる内容に基づいて異なるプロトコルメッセージパラメータをさらに設定し得、これにより、CPの機能はより完全になる。

【0022】

第1の態様に関連して、第1の態様の第8の可能な実施態様では、ユーザ端末によって送信されるメッセージは、PPPoEメッセージまたはIPoEメッセージであるため、ユーザ端末は、PPPoE/IPoEプロトコルスタックをサポートする。したがって、アクセスゲートウェイが、CPによって送信されたネットワークインタフェース情報を受信すると、アクセスゲートウェイは、ネットワークインタフェース情報内のIPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方を読み取り、次に、PPPoE手順においてIP構成メッセージまたはNCP (Network Control protocols、ネットワーク制御プロトコル) メッセージを使用してIPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方をユーザ端末に送信するか、またはDHCP手順においてIP構成メッセージを使用してIPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方をユーザ端末に送信し得る。

30

【0023】

この解決策から分かるように、アクセスゲートウェイは、ユーザ端末によって送信されるメッセージを、ネットワークデバイスの別の機能ネットワーク要素によって識別され得るメッセージタイプに変換するだけでなく、別の機能ネットワーク要素によって送信されるメッセージを、ユーザ端末によって識別され得るメッセージタイプにも変換し得、これにより、異なるプロトコルスタックタイプは、ネットワークデバイスにおいて相互に互換性があり得るようになる。

40

【0024】

第1の態様に関連して、第1の態様の第9の可能な実施態様では、PPPoEメッセージは、PADI (PPPoE Active Discovery Indication、PPPoEアクティブディスカバリ指示) メッセージ、PADR (PPPoE Active Discovery request、PPPoEアクティブディスカバリ要求) メッセージ、LCP (Link control protocol、リンク制御プロトコル) メッセージ、またはNCPメッセージであり得る。IPoEメッセージは、DHCPディスカバリメッセージまたはDHCP要求

50

メッセージであり得る。

【0025】

第2の態様によれば、本発明の一実施形態は、ネットワークアクセス装置をさらに提供する。この装置は、第1の態様および第1の態様の実施態様のうちのいずれか1つの方法ステップを実行するように構成されたモジュールおよびユニットを含む。具体的には、本発明のこの実施形態に関してここでは詳細は再度説明されない。

【0026】

第3の態様によれば、本発明の一実施形態は、ネットワークデバイスをさらに提供する。ネットワークデバイスは、第1の態様および第1の態様の実施態様のうちのいずれか1つの方法ステップを実行するように構成されたプロセッサおよび通信インタフェースを含む。具体的には、本発明のこの実施形態に関してここでは詳細は再度説明されない。

【0027】

第4の態様によれば、本発明の一実施形態は、命令を含むコンピュータプログラム製品をさらに提供する。命令がコンピュータ上で実行されると、コンピュータは、第1の態様の方法を実行できるようにされる。

【0028】

第5の態様によれば、本発明の一実施形態は、コンピュータ記憶媒体をさらに提供する。コンピュータ記憶媒体は、プログラムを記憶し得る。プログラムが実行されると、本願で提供されているネットワークアクセス方法の実施形態の一部または全部のステップが実行され得る。

【0029】

固定コアネットワークとモバイルコアネットワークの非互換性という従来技術の問題を解決するために、本願におけるネットワークアクセス方法および装置ならびにネットワークデバイスによれば、ユーザ端末によって送信されたメッセージを受信した後、アクセスゲートウェイは、メッセージがPPPoEメッセージとIPoEメッセージとのどちらであるかを判定し得る。メッセージがPPPoEメッセージまたはIPoEメッセージである場合、アクセスゲートウェイは、メッセージからユーザ端末のアクセス情報を抽出し、次に、抽出されたアクセス情報を、CPによって識別され得るNASメッセージまたはEAPメッセージにカプセル化し、NASメッセージまたはEAPメッセージをCPに送信する。NASメッセージまたはEAPメッセージを受信した後、CPは、NASメッセージまたはEAPメッセージ内のアクセス情報に基づいて、認証を実行するように認証エンティティをトリガする。さらに、認証エンティティがユーザ端末を認証した後、CPは、ネットワークインタフェース情報をアクセスゲートウェイに送信する。さらに、アクセスゲートウェイは、ネットワークインタフェース情報をユーザ端末に送信し、これにより、ユーザ端末は、ネットワークにアクセスする。この解決策から分かるように、ネットワークデバイスによってサポートされるプロトコルスタックが、ユーザ端末によってサポートされるプロトコルスタックと互換性がない場合、ネットワークデバイスのアクセスゲートウェイは、ユーザ端末によって送信されるメッセージを識別し得、このメッセージ内の情報を、ネットワークデバイスの別のネットワーク要素によって識別され得るメッセージタイプに変換し得、このため、ユーザ端末は、ネットワークにアクセスするときにプロトコルスタックによって制限されない。したがって、完全なサービスは、ただ1つのコアネットワークを展開することによって提供され得る。これは、リソースを節約するだけでなく、ネットワークのメンテナンスも容易にする。

【0030】

本願の技術的解決策をより明確に説明するために、以下、実施形態を説明するために必要とされる添付の図面について簡単に説明する。明らかに、当業者は、創造的な努力なしにこれらの添付の図面から他の図面を導き出し得る。

【図面の簡単な説明】

【0031】

【図1】本願によるネットワークシステムアーキテクチャの図である。

【図2】本願によるネットワークアクセス方法の情報交換の概略図である。

【図3】本願によるネットワークアクセス方法の第1の実施態様の情報交換の概略図である。

【図4】本願によるネットワークアクセス方法の第2の実施態様の情報交換の概略図である。

【図5】本願によるネットワークアクセス方法の第3の実施態様の情報交換の概略図である。

【図6】本願によるネットワークアクセス装置の概略構成図である。

【図7】本願によるネットワークデバイスの概略構成図である。

【発明を実施するための形態】

【0032】

以下、添付の図面を参照して本願について説明する。

【0033】

モバイルコアネットワークおよび固定コアネットワークは、異なるプロトコルスタックをサポートし、異なるプロトコルスタックの特徴に基づくため、モバイルコアネットワークの機能ネットワーク要素は、固定コアネットワークのそれとは異なり、これらの機能ネットワーク要素は、異なって配置されることに留意されたい。したがって、モバイルコアネットワークの機能アーキテクチャは、固定コアネットワークのそれとは異なり、これはさらに、モバイルコアネットワークと固定コアネットワークの非互換性につながっている。これを考慮して、問題を解決するために、本願の技術的解決策が提供される。

【0034】

図1は、本願によるネットワークシステムアーキテクチャの図である。ネットワークシステムアーキテクチャは、アクセスゲートウェイ、CP、およびAUSF (Authentication Server Function、認証エンティティ) などの機能ネットワーク要素を含む。アクセスゲートウェイは、ngPDG (Next Generation packet data gateway、次世代アクセスゲートウェイ) またはAGF (Access Gateway Function、アクセスゲートウェイ) であり、non-3GPPインターワーキング機能 (N3IWF: non-3GPP Interworking Function) を使用してネットワークにメッセージを送信する際にユーザ端末をサポートし、ユーザ端末によって送信されたメッセージを受信した後にメッセージをCPに送信し得る。CPは、AMFおよびSMFを含み、AMFは、ユーザ端末によるアクセス時の登録手順およびユーザ端末の位置の管理を担当し、SMFは、ユーザ端末に対してサービスを開始するときに対応するセッション接続を確立

【0035】

前述のネットワークシステムアーキテクチャおよび機能ネットワーク要素に基づく図2を参照すると、図2は、本願によるネットワークアクセス方法の情報交換の概略図である。本願で提供されるネットワークアクセス方法において、2つのプロトコルスタックは、相互に互換性があり得、このため、ユーザ端末は、ネットワークにアクセスするときにプロトコルスタックによって制限されない。具体的には、この方法は、以下の内容を含む。

【0036】

本願の方法は、ネットワークデバイスに適用され、ネットワークデバイスは、アクセスゲートウェイおよびCPを含む。ステップ1: アクセスゲートウェイは、ユーザ端末によって送信されたPPPoE/IPoEメッセージを受信し、PPPoE/IPoEメッセージに対応する、ユーザ端末のアクセス情報を取得する。ステップ2: アクセスゲートウェイは、アクセス情報をNAS/EAPメッセージにカプセル化し、NAS/EAPメッセージをCPに送信する。ステップ3: CPは、アクセス情報に基づいて、認証を実行するようにAUSFをトリガする。ステップ4: CPは、AUSFによって送信された認証成功メッセージを受信する。ステップ5: CPは、ユーザ端末のためのネットワークインタフェース情報を構成し、ネットワークインタフェース情報をアクセスゲートウェイに送信する。ステップ6: アクセスゲートウェイは、ネットワークインタフェース情報のインタフェースデータをユーザ端末に送信する。ステップ

7: ユーザ端末は、インタフェースデータに基づいてネットワークにアクセスする。

【0037】

具体的には、ユーザ端末によってネットワークデバイスに送信されるメッセージは、PPPoEメッセージもしくはIPoEメッセージ（説明を簡単にするために、PPPoEメッセージまたはIPoEメッセージは本願ではPPPoE/IPoEメッセージとして説明されている）であってもよく、またはNASメッセージもしくはEAPメッセージ（説明を簡単にするために、NASメッセージまたはEAPメッセージは本願ではNAS/EAPメッセージとして説明されている）であってもよく、異なるプロトコルタイプのメッセージに対応して、本願におけるネットワークデバイスに対応するアクセスプロセスは様々である。したがって、アクセスゲートウェイがメッセージを受信すると、メッセージがPPPoE/IPoEメッセージとNAS/EAPメッセージとのどちらであるかを判定するために、アクセスゲートウェイは最初に、メッセージのデータパケットヘッダのタイプ識別子を読み取ることによってメッセージのタイプを判定し得る。メッセージがNAS/EAPメッセージである場合、ネットワークデバイスの他のすべての機能ネットワーク要素は、メッセージを識別し得、アクセスゲートウェイは、メッセージをCPに直接送信し得、CPは、後続のアクセスプロセスを実行する。具体的には、ユーザ端末によって送信されたメッセージが、NAS/EAPメッセージである場合、ネットワークデバイスの各機能ネットワーク要素の処理プロセスは、当業者によって知られているプロセスである。本願においてここでは詳細は再度説明されない。ユーザ端末によって送信されたメッセージが、PPPoE/IPoEメッセージである場合、ネットワークデバイスの別の機能ネットワーク要素は、メッセージを識別し得ない。このため、ユーザ端末によってネットワークにアクセスする動作はさらに実行され得ない。したがって、アクセスゲートウェイは、ステップ1および後続の動作をさらに実行し、これにより、ユーザ端末は、ネットワークにアクセスし得る。

【0038】

この実施形態では、アクセス情報は、セッション識別子、ユーザ端末識別子、および固定ネットワークアクセスポイント識別子のうちの少なくとも1つを含み得ることに留意されたい。セッション識別子は、アクセスゲートウェイによってユーザ端末に割り当てられる。例えば、本願の任意選択の例では、アクセスゲートウェイは、一意のセッション識別子Session-IDをユーザ端末に予め割り当てる。ユーザ端末識別子は、ユーザ端末永久識別子またはユーザ端末一時識別子、ユーザ端末MACアドレスまたはユーザ端末NAI、ユーザ端末ユーザ名、およびエージェントリモート識別子のうちの少なくとも1つである。固定ネットワークアクセスポイント識別子は、回線識別子、物理的位置識別子、および論理識別子のうちの少なくとも1つである。これに基づいて、この実施形態では、アクセスゲートウェイがアクセス情報を取得することは、PPPoE/IPoEメッセージに含まれるユーザ端末のセッション識別子および／またはPPPoE/IPoEメッセージに含まれるユーザ端末識別子を抽出することを特に含み得る。もちろん、ユーザ端末のセッション識別子および／またはユーザ端末識別子を取得することに基づいて、以下、すなわち、PPPoE/IPoEメッセージのソースを識別し、ユーザ端末の固定ネットワークアクセスポイント識別子を判定することがさらに含められ得る。

【0039】

アクセス情報の内容に含まれる複数の異なる形式に基づいて、アクセスゲートウェイがアクセス情報をNAS/EAPメッセージにカプセル化するプロセスは、いくつかの実施態様を含み得る。さらに、アクセス情報に基づいてCPが認証を実行するようにAUSFをトリガするプロセスもまた、複数の異なる実施態様を含み得る。以下、2つの実行プロセス、すなわち、異なる内容形式のアクセス情報に対応する、カプセル化によってNAS/EAPメッセージを取得するプロセスおよびAUSFによって認証を実行するプロセスをそれぞれ説明する。

【0040】

具体的には、一実施形態では、アクセスゲートウェイがアクセス情報をNASメッセージにカプセル化することは、アクセスゲートウェイがNAS要求メッセージを生成し、アクセス情報をNAS要求メッセージに追加することを含む。次に、アクセスゲートウェイは、ユ

ーザ端末初期化メッセージを送信し、NAS要求メッセージをユーザ端末初期化メッセージに追加する。

【0041】

この解決策では、アクセスゲートウェイおよびCPがN2インタフェースを介してデータ通信を実行することに留意されたい。したがって、ユーザ端末初期化メッセージを生成した後、アクセスゲートウェイは、同様にN2インタフェースを介してユーザ端末初期化メッセージをCPに送信する。したがって、本願の説明中に、アクセスゲートウェイがユーザ端末初期化メッセージを生成して送信するプロセスは、以下として、すなわち、アクセスゲートウェイがユーザ端末初期化メッセージを送信し、ユーザ端末初期化メッセージにN2メッセージと名付け得ることとして説明され得る。

10

【0042】

別の実施形態では、アクセス情報が、3つのタイプのメッセージ、すなわち、セッション識別子、ユーザ端末識別子、および固定ネットワークアクセスポイント識別子を含む場合、アクセスゲートウェイがアクセス情報をNASメッセージにカプセル化することは、アクセスゲートウェイがN2メッセージを送信し、アクセス情報内の固定ネットワークアクセスポイント識別子およびセッション識別子のうちの少なくとも一方をN2メッセージに追加することを含む。アクセスゲートウェイは、NAS要求メッセージを生成し、アクセス情報内のユーザ端末識別子をNAS要求メッセージに追加し、NAS要求メッセージをN2メッセージに追加する。

【0043】

20

NAS要求メッセージは、登録要求メッセージまたはPDUセッション確立要求メッセージであり得る。

【0044】

別の実施形態では、アクセスゲートウェイがアクセス情報をEAPメッセージにカプセル化することは、アクセスゲートウェイがEAPメッセージを生成し、アクセス情報をEAPメッセージに追加することを含む。次に、アクセスゲートウェイは、登録要求メッセージを生成し、EAPメッセージを登録要求メッセージに追加する。さらに、アクセスゲートウェイは、N2メッセージを送信し、登録要求メッセージをN2メッセージに追加する。

【0045】

例えば、この解決策の任意選択の例では、アクセス情報は、ユーザのMACアドレスである。ngPDGは、MACアドレスに基づいてNAIを生成し得る。次に、ngPDGは、NAIをEAPメッセージに追加し、EAPメッセージを登録要求メッセージに追加し、登録要求メッセージをN2メッセージにさらに追加する。

30

【0046】

さらに、この解決策では、PPPoEメッセージが、PADIメッセージ、PADRメッセージ、LCPメッセージ、またはNCPメッセージであり得ることに留意されたい。IPoEメッセージは、DHCPディスカバリメッセージまたはDHCP要求メッセージであり得る。この解決策の前述の実行プロセスは、様々な形式のPPPoEメッセージまたはIPoEメッセージに適用可能である。詳細については、前述の説明を参照することとし、この解決策では、特定の形式のメッセージのそれぞれは1つずつ説明されない。

40

【0047】

このことから分かるように、本願の技術的解決策では、アクセスゲートウェイは、メッセージのデータパケットヘッダ内のメッセージタイプ識別子に基づいて、ユーザ端末によって送信されたメッセージのプロトコルタイプを判定し得る。さらに、ネットワークデバイスの別の機能ネットワーク要素が、メッセージのプロトコルスタックをサポートしていない場合、それでもアクセスゲートウェイは、メッセージのタイプを変換し得、このため、ネットワークデバイスは、異なるプロトコルタイプのメッセージに基づいてアクセス動作を実行し得、このため、ユーザ端末は、ネットワークにアクセスするときにプロトコルスタックによって制限されない。

【0048】

50

前述の説明に基づいて、アクセスゲートウェイによって送信されたNAS/EAPメッセージを受信した後、CPは最初に、NAS/EAPメッセージからアクセス情報を読み取り得る。アクセス情報が、ユーザ端末識別子および固定ネットワークアクセスポイント識別子のうちの少なくとも一方を含む場合、CPは、固定ネットワークアクセスポイント識別子およびユーザ端末識別子のうちの少なくとも一方に基づいて認証を実行するようにAUSFをトリガするために、固定ネットワークアクセスポイント識別子およびユーザ端末識別子のうちの少なくとも一方をAUSFに送信する。認証を完了した後、AUSFは、認証の結果をCPに送信する。

【0049】

具体的には、本願の任意選択の実施形態では、アクセス情報の内容が、ユーザ端末識別子のみ、例えばSession-IDおよび／またはNAIのみである場合、CPは、ユーザ端末のユーザ名およびパスワードならびにchallenge値を取得するための要求をアクセスゲートウェイに送信し得る。アクセスゲートウェイは、この要求に応答してユーザ端末からユーザ端末のユーザ名およびパスワードを取得し、ユーザ名と、パスワードと、アクセスゲートウェイによって事前に生成されるchallenge値とをCPに送信し得る。CPは、認証情報としてユーザ名、パスワード、およびchallenge値をAUSFに対して使用し得る。

【0050】

別の任意選択の実施態様では、アクセス情報の内容が、Session-IDおよび／またはNAIならびに固定ネットワークアクセスポイント識別子である場合、CPは最初に、固定ネットワークアクセスポイント識別子をAUSFに送信し、固定ネットワークアクセスポイント識別子に応答してAUSFによって送信される認証ベクトルを受信し得る。次に、CPは、認証ベクトルに基づいてchallenge値を生成し、ユーザ端末のユーザ名およびパスワードを取得するための要求にchallenge値を追加し、この要求をアクセスゲートウェイに送信する。ユーザ端末によって送信されたユーザ名およびパスワードを受信した後、アクセスゲートウェイは、ユーザ名およびパスワードをCPに送信する。CPは、認証情報としてユーザ名およびパスワードをAUSFに送信する。

【0051】

この実施形態では、challenge値は、CPによって生成されるが、challenge値は、認証ベクトルのパラメータであってもよいことに留意されたい。この場合、固定ネットワークアクセスポイント識別子に応答して認証ベクトルを生成した後、AUSFは、認証ベクトルからchallenge値を直接取得し得る。この実施態様のシナリオでは、AUSFが、challenge値を既に獲得しているため、CPは、ユーザ名およびパスワードをAUSFに送信するときにchallenge値を伝える必要がない。もちろん、別の実施態様のシナリオにおいて、challenge値が、認証ベクトルから直接取得されず、CPによって生成される場合、CPは、ユーザ名およびパスワードをAUSFに送信するときにchallenge値も送信しなければならない。具体的には、本発明のこの実施形態に関してここでは詳細は説明されない。

【0052】

さらに、第3の任意選択の実施態様では、アクセス情報の内容が、NAIおよび固定ネットワークアクセスポイント識別子を含む場合、CPは、認証情報としてNAIおよび固定ネットワークアクセスポイント識別子をAUSFに直接送信し得る。

【0053】

固定コアネットワーク機能アーキテクチャでは、BNGの機能が、ユーザ端末との情報交換および認証制御を実行することを含むことが、従来技術から分かる。このため、固定コアネットワーク機能アーキテクチャは、本願のネットワークの機能アーキテクチャと互換性があり得ない。本願では、アクセスゲートウェイが、ユーザ端末との情報交換を実行し、CPが、認証制御を実行し、このため、固定コアネットワーク機能アーキテクチャおよび本願のネットワークデバイスの機能アーキテクチャは相互に互換性があり得、これにより、本願のネットワークデバイスの機能は改善され得、ネットワークデバイスは、異なるプロトコルスタックをサポートするユーザ端末にアクセスし得ることが、前述の説明から分かる。

【0054】

前述の説明に対応して、CPが、AUSFによって送信された認証成功メッセージを受信すると、CPのSMFは、対応するユーザ端末のためのIPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方を構成し得る。さらに、IPアドレスおよび／またはDHCPサーバアドレスを構成した後、CPのモバイル機能エンティティAMFは、NAS返信メッセージを生成し、IPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方をNAS返信メッセージに追加し、ネットワークインタフェース情報を取得する。

【0055】

NAS返信メッセージは、ロケーションエリア識別子を含み、ロケーションエリア識別子は、CPによってユーザ端末に割り当てられたロケーションエリア識別子であることに留意されたい。この解決策では、ユーザ端末は、固定ネットワーク端末であり、CPは、ロケーションエリア識別子をユーザ端末に割り当てる必要はない。したがって、この実施形態では、ロケーションエリア識別子は、ヌル値に設定されてもよい。代替的に、固定ネットワークエリア識別子、特別なロケーションエリア識別子、または回線識別子が、ユーザ端末に割り当てられてもよく、具体的には、設定は、要求に基づいて実行されてもよい。本願においてここでは詳細は再度説明されない。

10

【0056】

ユーザ端末によって送信されるメッセージがPPPoE/IPoEメッセージであることから、ユーザ端末は、PPPoE/IPoEプロトコルスタックをサポートしていることに留意されたい。したがって、アクセスゲートウェイが、CPによって送信されたネットワークインタフェース情報を受信すると、アクセスゲートウェイは、ネットワークインタフェース情報内のIPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方を読み取り、次に、PPPoE手順においてIP構成メッセージまたはNCPメッセージを使用してIPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方をユーザ端末に送信するか、またはDHCP手順においてIP構成メッセージを使用してIPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方をユーザ端末に送信し得る。

20

【0057】

さらに、別の実施態様のシナリオでは、アクセスゲートウェイは、ユーザ端末が固定ネットワーク端末であることを識別し得る。したがって、アクセスゲートウェイは、ユーザ端末に対して認証を直接実行し、認証が成功した後、ユーザ端末の認証成功情報およびアクセス情報をNAS/EAPメッセージにカプセル化し、NAS/EAPメッセージをCPに送信し得る。CPは、ユーザ端末のためのネットワークインタフェース情報を直接構成し、ネットワークインタフェース情報をアクセスゲートウェイに送信し得る。この実施態様のシナリオにおいて、認証プロセス以外の実行プロセスの詳細については、前述の説明を参照されたい。本願においてここでは詳細は再度説明されない。

30

【0058】

結論として、本願のネットワークアクセス方法によれば、異なるプロトコルスタックタイプは相互に互換性があり得、固定コアネットワークの機能は、固定コアネットワークの機能ネットワーク要素の機能を分散化することによって互換性があり得、このため、ユーザ端末は、ネットワークにアクセスするときに制限されない。したがって、完全なサービスは、ただ1つのコアネットワークを展開することによって提供され得る。これは、リソースを節約するだけでなく、ネットワークのメンテナンスも容易にする。

40

【0059】

この解決策は、前述の実施形態の簡単な説明の観点から詳述されている。当業者がこの解決策をより明確かつより詳細に知らせるために、以下、ユーザ端末によって送信されるPPPoEメッセージおよびIPoEメッセージにそれぞれ対応する例を参照してこの解決策を詳述する。

【0060】

図3は、本願によるネットワークアクセス方法の第1の実施態様の情報交換の概略図である。図3に示されている実施形態では、ユーザ端末は、PPPoEアクセス手順を開始し、アクセスゲートウェイはngPDGである。具体的には：ステップS21：ユーザ端末は、PADIメッセ

50

ージをngPDGに送信する。ステップS22：ngPDGは、ユーザ端末の要求に応答するために、PPoEアクティブディスカバリオファパドメッセージをユーザ端末に送信する。ステップS23：ユーザ端末は、ngPDGのPAD0メッセージを選択した後、PPPoEアクティブディスカバリ要求PADRメッセージをngPDGに送信する。ステップS24：ユーザ端末によって送信されたPADRメッセージを受信した後、一意のPPPoEセッション識別子Session-IDをユーザ端末に割り当てる。ステップS25：ngPDGは、アクティブディスカバリセッション確認PADSメッセージをユーザ端末に送信し、その場合、PADSメッセージは、Session-IDを含む。ステップS26：ngPDGは、challenge値を生成し、challenge値をユーザ端末に送信する。ステップS27：ユーザ端末は、HASH化されたパスワードchallenge-passwordを生成するために、challenge値および初期パスワードに対してMD5アルゴリズムを実行する。

10

【0061】

前述のステップは、ユーザ端末およびngPDGが相互にPPPoEセッションを実行するプロセスであることに留意されたい。このプロセスの情報プロトコルは、PPPoEプロトコルスタックをサポートする。このプロセスは、当業者に知られているプロセスであるため、本願では詳細を再度説明されない。

【0062】

ステップS21に基づいて、ngPDGは、PADIメッセージのデータパケットヘッダのタイプ識別子を使用して、ユーザ端末によって送信されたメッセージがPPPoEメッセージであることを既に判定し得る。したがって：ステップS28：ngPDGは、ユーザ端末のSession-IDを読み取り、N2 IDをSession-IDに設定し、Session-IDをN2メッセージに追加し、N2メッ

20

【0063】

もちろん、前述の説明は、実施態様にすぎない。この実施形態では、代替的に、Session-IDは、NASメッセージに追加されてもよい。代替的に、ngPDGは、ユーザ端末のMACアドレスを読み取り、NAI=MAC@domain nameを生成し、その場合、ドメイン識別子domain nameは、固定ネットワークオペレータPLMN情報であり得る。次に、NAIは、EAP-Responseメッセージに追加される。もちろん、本願のこの実施形態では、ngPDGは、Session-IDまたはNAIに対応するNAS/EAPメッセージをCPに送信し得る。

【0064】

さらに、本願のこの実施形態では、Session-IDまたはMACアドレスが、ユーザ端末のデバイス識別子として機能し、ngPDGが、NASメッセージにおいて、要求タイプを初期接続に設定し、また、PDNタイプをIPv4アドレスおよびIPv6アドレスに設定するか、構成に基づいてPDNタイプをonly IPv4またはonly IPv6アドレスに設定することに留意されたい。

30

【0065】

ステップS29：CPは、Session-IDおよび／またはMACアドレスを読み取って記憶し、EAP-Requestメッセージを運ぶN2メッセージをngPDGに送信する。EAP-Requestメッセージは、ユーザ端末のユーザ名およびchallenge-passwordを取得するための要求に関する情報を含み得ることに留意されたい。ステップS210：要求情報に回答して、ngPDGは、ユーザ端末からユーザ名およびchallenge-passwordを取得し、ユーザ名、challenge値、およびchallenge-passwordをEAPメッセージに追加し、EAPメッセージをCPに送信

40

【0066】

ユーザ端末のユーザ名およびchallenge-passwordなどの情報は、比較的高いセキュリティレベルを有する。したがって、この実施形態では、ngPDGがユーザ名およびchallenge-passwordをCPに送信する前に、CPは、ngPDGへの安全なチャネルを確立し得、これにより、ngPDGは、セキュアチャネルを介してユーザ名およびchallenge-passwordをCPに送信する。セキュアチャネルは、TLSセキュアチャネルであり得るが、これに限定されない。

【0067】

ステップS211：CPは、EAPメッセージからユーザ名、challenge-password、およびchallenge値を抽出し、認証を実行するようにAUSFをトリガするためにユーザ名、challenge-

50

password、およびchallenge値をAUSFに送信する。

【0068】

具体的には、AUSFは、ユーザ名に基づいてサブスクリプションデータを検索し、演算結果を取得するために、サブスクリプションデータ内のユーザ名に対応するパスワードおよび受信されたchallenge値に対してHASH演算を実行し、次に、演算結果と受信されたchallenge-passwordとを比較し得、演算結果が受信されたchallenge-passwordと同じである場合、ユーザ認証は成功しており、そうでない場合、ユーザ認証は失敗している。

【0069】

ステップS212：AUSFによって実行された認証が成功した後、AUSFは、認証成功通知情報をCPに送信し、その場合、通知情報は、ユーザサブスクリプションデータを含む。ステップS213：CPは、IPアドレスをユーザ端末に割り当て、割り当てられたIPアドレスをN2メッセージに追加し、N2メッセージをngPDGに送信する。この実施形態では、IPアドレスは、NASメッセージに追加され得る。具体的には、NASメッセージ内のロケーションエリア識別子が、ヌル値に設定され得る。ステップS214：ngPDGは、認証成功通知情報をユーザ端末に送信する。ステップS215：ユーザ端末は、ngPDGへのNCPネゴシエーションを開始し、IPアドレスを取得し、IPアドレスに基づいてネットワークにアクセスする。

【0070】

この解決策では、ngPDGとユーザ端末との間の相互作用に関する情報は、PPPoEプロトコルスタックをサポートし、ngPDGとCPとの間の相互作用に関する情報は、NAS/EAPメッセージをサポートし、言い換えれば、ngPDGは、PPPoEプロトコルスタックおよびNAS/EAPプロトコルスタックメッセージを識別して双方向に変換し得、このため、2つのプロトコルスタックは、ネットワークデバイスにおいて相互に互換性があり得ることが、この実施形態の説明から分かる。

【0071】

もちろん、図3に示されている実施形態は、この解決策の任意選択の実施態様である。本願の技術的解決策は、これに限定されない。

【0072】

図4は、本願によるネットワークアクセス方法の第2の実施態様の情報交換の概略図である。図4に示されている実施形態では、ユーザ端末はまた、特に以下の手順を含むPPPoEアクセス手順を開始する。

【0073】

ステップS31からステップS35は、ユーザ端末およびngPDGがPPPoEセッションを実行するプロセスであり、図3に示されている実施形態のステップS21からステップS25と同じである。詳細については、図3に示されている実施形態の説明を参照されたい。本願においてここでは詳細は再度説明されない。

【0074】

ステップS36：ngPDGは、ユーザ端末のSession-IDまたはMACアドレスを読み取り、PPPoE接続リソースを識別し、固定ネットワークアクセスポイント識別子を判定する。この実施形態では、固定ネットワークアクセスポイント識別子は、回線識別子である。ステップS37：ngPDGは、Session-IDまたはMACアドレスおよび回線識別子をNAS/EAPメッセージにカプセル化し、NAS/EAPメッセージをCPに送信する。ステップS38：CPは、Session-IDまたはMACアドレスおよび回線識別子を読み取って記憶し、回線識別子をAUSFに送信する。ステップS39：AUSFは、回線識別子に基づいて、回線に対応する認証ベクトルを取得し、認証ベクトルをCPに送信する。ステップS310：CPは、認証ベクトルに基づいてchallenge値を生成する。ステップS311：CPは、ngPDGへのセキュアチャネルを確立する。ステップS312：CPは、セキュアチャネルを介してEAP-RequestメッセージをngPDGに送信する。この実施形態では、EAP-Requestメッセージは、challenge値を含む。ステップS313：ngPDGは、challenge値と、ユーザ名およびchallenge-passwordを取得するための要求とをユーザ端末に送信する。

【0075】

ステップS314からステップS320の動作プロセスは、図3に示されている実施形態のステップS210からステップS215のプロセスと同様である。この実施形態に関してここでは詳細は説明されない。

【0076】

この実施形態では、challenge値は、認証ベクトル内の乱数であってもよいことに留意されたい。したがって、ステップS39において、認証ベクトルを生成した後、AUSFは、challenge値として認証ベクトル内の乱数を直接読み取り得る。したがって、この実施形態では、AUSFは、challenge値を既に獲得している。さらに、この実施形態と図3に示されている実施形態との違いは、以下の通りであり、すなわち、CPがユーザ名およびchallenge-passwordをAUSFに送信するときにchallenge値が運ばれないことである。詳細については、図4のステップS316の説明を参照されたい。この実施形態に関してここでは詳細は説明されない。

10

【0077】

さらに、この実施形態では、challenge値は、CPによって生成される。したがって、ngPDGは、ユーザ名およびchallenge-passwordのみをCPに送信する。さらに、CPが、割り当てられたIPアドレスをNASメッセージに追加するとき、CPは、NASメッセージ内のロケーションエリア識別子をヌル値または回線識別子に設定し得る。

【0078】

図3に示されている実施形態に基づいて、ngPDGは、ユーザ端末とPPPoEセッションを実行するように構成され、さらに、2つのプロトコル間の変換を実行する必要がある、これにより、ngPDGの比較的大きなデータ処理量および比較的複雑な動作がもたらされる。これに基づいて、この実施形態では、CPが、challenge値を生成し、これにより、ngPDGのデータ処理量は低減され得、ngPDGの動作は簡素化され得る。

20

【0079】

前述の2つの実施形態は、PPPoEプロトコルスタックを例として使用した本願の説明である。当業者がこの解決策をより完全に理解できるようにするために、以下、IPoEプロトコルスタックを例として使用して本願の動作プロセスを説明する。

【0080】

図5は、本願によるネットワークアクセス方法の第3の実施態様の情報交換の概略図である。この実施形態では、ユーザ端末は、IPoEアクセス手順を開始する。具体的には：ステップS41：ユーザ端末は、ngPDGへのレイヤ2接続を確立し、DHCPディスカバリメッセージをngPDGに送信する。ステップS42：ngPDGは、DHCPディスカバリメッセージからユーザ端末のMACアドレスを取得し、IPoE接続ソースを識別し、ユーザ端末の固定ネットワークアクセスポイント識別子を判定する。この実施態様では、固定ネットワークアクセスポイント識別子は、回線識別子であり得る。ステップS43：ngPDGは、MACアドレスおよび回線識別子をNAS/EAPメッセージにカプセル化し、NAS/EAPメッセージをCPに送信する。

30

【0081】

この実施形態では、ngPDGはまた、予め割り当てられたSession-IDをCPに送信し得ることに留意されたい。さらに、IPoEプロトコルスタックをサポートするユーザ端末は、DHCPサーバに基づいてIPアドレスを自動的に取得する。したがって、IPアドレスが取得される時間は遅延される。したがって、この実施形態では、NASメッセージの生成中に、IPアドレス遅延取得指示が設定される。

40

【0082】

ステップS44：CPは、MACアドレスおよび回線識別子を抽出して記憶し、認証を実行するようにAUSFをトリガするためにMACアドレスおよび回線識別子をAUSFに送信する。

【0083】

この実施形態では、AUSFは、回線識別子に基づいてユーザサブスクリプションデータを検索し、受信されたMACアドレスとサブスクリプションデータ内のMACアドレスとのマッチングを実行する。マッチングが成功した場合、認証は成功しており、そうでない場合、認証は失敗している。

50

【0084】

認証が成功した後：ステップS45：AUSFは、ユーザサブスクリプションデータをCPに送信する。ステップS46：CPは、DHCPサーバアドレスをユーザ端末に割り当て、NASメッセージまたはN2メッセージを使用してDHCPサーバアドレスをngPDGに送信する。ステップS47：ngPDGは、DHCP offerメッセージをユーザ端末に送信し、その場合、DHCP offerメッセージは、CPによって割り当てられたDHCPサーバアドレスを運ぶ。

【0085】

この実施形態では、CPは、代替的に、DHCPサーバアドレスをユーザ端末に割り当てなくてもよいことに留意されたい。この場合、この実施態様のシナリオでは、CPは、認証成功通知情報のみをngPDGに送信し、ngPDGは、DHCPサーバアドレスをユーザ端末に割り当てる。

10

【0086】

ステップS48：ユーザ端末は、DHCPサーバアドレスにアクセスし、DHCPサーバからIPアドレスを取得し、IPアドレスに基づいてネットワークにアクセスする。

【0087】

この実施形態では、ステップS46を実行するときに、CPは、代替的に、IPアドレスをユーザ端末に割り当て、後続の手順でIPアドレスおよびDHCPサーバアドレスと一緒にユーザ端末に送信してもよく、これにより、ユーザ端末は、CPによって割り当てられたIPアドレスに基づいてネットワークにアクセスし、ユーザ端末が、後続のネットワーク動作プロセスで別のIPアドレスを取得する必要があるとき、ユーザ端末は、DHCPサーバアドレスにアクセスすることによって別のIPアドレスを取得し得ることに留意されたい。

20

【0088】

さらに、この実施形態では、CPはまた、challenge値を生成し、NASメッセージを使用してchallenge値をngPDGに送信し、これにより、ユーザ端末は、challenge値に基づいてchallenge-passwordを生成する。具体的には、詳細については、図4に示されている実施形態のステップS38からステップS312を実行するプロセスを参照されたい。この実施形態に関してここでは詳細は説明されない。

【0089】

もちろん、前述の説明は、本願のいくつかの任意選択の実施態様にすぎず、本願の技術的解決策に対する制限を構成しないことが分かる。前述の実施態様では、アクセスゲートウェイは、代替的に、AGFに置き換えられてもよく、アクセス情報は、代替的に、別の適切なメッセージに置き換えられてもよい。具体的には、本願においてここでは詳細は再度説明されない。

30

【0090】

結論として、本願で提供されるネットワークアクセス方法によれば、ネットワークデバイスによってサポートされるプロトコルスタックが、ユーザ端末によってサポートされるプロトコルスタックと互換性がない場合、ネットワークデバイスのngPDGは、ユーザ端末によって送信されるメッセージを識別し得、このメッセージ内の情報を、ネットワークデバイスの別のネットワーク要素によって識別され得るメッセージタイプに変換し得、このため、ユーザ端末は、ネットワークにアクセスするときにプロトコルスタックによって制限されない。したがって、完全なサービスは、ただ1つのコアネットワークを展開することによって提供され得る。これは、リソースを節約するだけでなく、ネットワークのメンテナンスも容易にする。

40

【0091】

前述のネットワークアクセス方法に対応して、本願は、ネットワークアクセス装置をさらに提供する。図6は、本願によるネットワークアクセス装置の概略構成図である。この装置は、図2から図5に示されているネットワークアクセス方法を実行するように構成される。この装置は、取得モジュール61、カプセル化モジュール62、送信モジュール63、および受信モジュール64を含む。取得モジュール61は、ユーザ端末によって送信されたポイントツーポイント接続プロトコルPPPoEメッセージまたは動的ホスト構成プロトコルIPoEメ

50

ッセージが受信されたときに、PPPoEメッセージまたはIPoEメッセージに含まれるユーザ端末のアクセス情報を取得するように構成される。カプセル化モジュール62は、アクセス情報を非アクセス層NASメッセージまたは拡張可能認証プロトコルEAPメッセージにカプセル化するように構成される。送信モジュール63は、NASメッセージまたはEAPメッセージを制御プレーン機能エンティティCPに送信するように構成される。受信モジュール64は、CPによって送信されたネットワークインタフェース情報を受信し、ネットワークインタフェース情報をユーザ端末に送信し、これにより、ユーザ端末が、ネットワークにアクセスする、ように構成される。

【0092】

特定の実施形態では、カプセル化モジュール62は、生成ユニットおよび送信ユニットを含む。生成ユニットは、NAS要求メッセージを生成し、アクセス情報をNAS要求メッセージに追加し、NAS要求メッセージが、登録要求メッセージまたはプロトコルデータユニットPDUセッション確立要求メッセージである、ように構成される。送信ユニットは、ユーザ端末初期化メッセージを送信し、NAS要求メッセージをユーザ端末初期化メッセージに追加するように構成される。さらに、この実施形態では、送信ユニットは、ユーザ端末初期化メッセージを送信し、アクセス情報内の固定ネットワークアクセスポイント識別子およびセッション識別子のうちの少なくとも一方をユーザ端末初期化メッセージに追加するようにさらに構成され、生成ユニットは、NAS要求メッセージを生成し、アクセス情報内のユーザ端末識別子をNAS要求メッセージに追加し、NAS要求メッセージをユーザ端末初期化メッセージに追加するようにさらに構成される。

【0093】

別の実施形態では、生成ユニットは、EAPメッセージを生成し、アクセス情報をEAPメッセージに追加し、登録要求メッセージを生成し、EAPメッセージを登録要求メッセージに追加するようにさらに構成され、送信ユニットは、ユーザ端末初期化メッセージを送信し、登録要求をユーザ端末初期化メッセージに追加するようにさらに構成される。

【0094】

さらに、この装置は、構成モジュールをさらに含む。この実施形態では、送信モジュール63は、アクセス情報がユーザ端末識別子および固定ネットワークアクセスポイント識別子のうちの少なくとも一方を含むときに、固定ネットワークアクセスポイント識別子およびユーザ端末識別子のうちの少なくとも一方を認証エンティティに送信するようにさらに構成される。受信モジュール64は、固定ネットワークアクセスポイント識別子およびユーザ端末識別子のうちの少なくとも一方に基づいて認証エンティティによって実行された認証の結果を受信するようにさらに構成される。構成モジュールは、認証の結果が認証が成功したことであるときに、ユーザ端末のためのネットワークインタフェース情報を構成するように構成される。

【0095】

受信モジュール64は、送信モジュール63がアクセス情報を認証エンティティに送信した後に、固定ネットワークアクセスポイント識別子に基づいて認証エンティティによって送信された認証ベクトルを受信するように特に構成される。送信モジュール63は、認証ベクトルに基づいてchallenge値を生成し、challenge値をアクセスゲートウェイに送信し、ユーザ名およびパスワードを取得するための要求をユーザ端末に送信し、この要求が、challenge値を含み、このパスワードが、challenge値および初期パスワードに対してハッシュ演算を実行することによりユーザ端末によって取得される、ようにさらに構成される。受信モジュール64は、ユーザ名およびパスワードを受信するようにさらに構成される。送信モジュール63は、ユーザ名およびパスワードをCPに送信し、認証エンティティに送信されるユーザ名およびパスワードを送信し、これにより、認証エンティティが、ユーザ名およびパスワードに基づいて認証を実行する、ようにさらに構成される。

【0096】

さらに、構成モジュールは、インターネットプロトコルアドレスIPアドレスおよびホスト構成プロトコルDHCPサーバアドレスのうちの少なくとも一方をユーザ端末に割り当て、

NAS返信メッセージを生成し、IPアドレスおよびDHCPサーバのうちの少なくとも一方をNAS返信メッセージに追加し、ネットワークインタフェース情報を取得するように特に構成される。

【0097】

別の実施形態では、送信モジュール63は、ネットワークインタフェース情報内のIPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方を読み取り、IP構成メッセージまたはネットワーク制御プロトコルNCPメッセージを使用してIPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方をユーザ端末に送信するように特に構成される。

【0098】

さらに、本願は、ネットワークデバイスをさらに提供する。図7は、本願によるネットワークデバイスの概略構成図である。このデバイスは、図2から図5に示されているネットワークアクセス方法を実行するように構成される。このデバイスは、プロセッサ11および通信インタフェース12を含む。通信インタフェース12は、ユーザ端末によって送信されたPPPoEメッセージまたはIPoEメッセージを受信するように構成される。プロセッサ11は、PPPoEメッセージまたはIPoEメッセージに含まれるユーザ端末のアクセス情報を取得し、アクセス情報をNASメッセージまたはEAPメッセージにカプセル化するように構成される。通信インタフェース12は、ネットワークインタフェース情報をユーザ端末に送信し、これにより、ユーザ端末が、ネットワークにアクセスする、ように構成される。

【0099】

プロセッサ11がアクセス情報をNASメッセージにカプセル化することは、以下のように実行され、すなわち、プロセッサ11が、NAS要求メッセージを生成し、アクセス情報をNAS要求メッセージに追加し、ユーザ端末初期化メッセージを生成し、NAS要求メッセージをユーザ端末初期化メッセージに追加するか、またはユーザ端末初期化メッセージを生成し、アクセス情報内の固定ネットワークアクセスポイント識別子およびセッション識別子のうちの少なくとも一方をユーザ端末初期化メッセージに追加し、NAS要求メッセージを生成し、アクセス情報内のユーザ端末識別子をNAS要求メッセージに追加し、NAS要求メッセージをユーザ端末初期化メッセージに追加する。NAS要求メッセージは、登録要求メッセージまたはプロトコルデータユニットPDUセッション確立要求メッセージである。

【0100】

プロセッサ11がアクセス情報をEAPメッセージにカプセル化することは、以下のように実行され、すなわち、プロセッサ11が、EAPメッセージを生成し、アクセス情報をEAPメッセージに追加し、次に登録要求メッセージを生成し、EAPメッセージを登録要求メッセージに追加し、次にユーザ端末初期化メッセージを生成し、登録要求をユーザ端末初期化メッセージに追加する。

【0101】

さらに、アクセス情報を非アクセス層NASメッセージまたは拡張可能認証プロトコルEAPメッセージにカプセル化した後、プロセッサ11は、アクセス情報内のユーザ端末識別子および固定ネットワークアクセスポイント識別子のうちの少なくとも一方に基づいて認証を実行し、認証結果を取得し、認証結果が認証が成功したことであるときにユーザ端末のためのネットワークインタフェース情報を構成するようにさらに構成される。アクセス情報内の固定ネットワークアクセスポイント識別子に基づいて認証を実行することは、特に、以下のように実行され、すなわち、プロセッサ11が、固定ネットワークアクセスポイント識別子に基づいて認証ベクトルを検索し、認証ベクトルに基づいてchallenge値を生成する。通信インタフェース12は、challenge値をユーザ端末に送信し、ユーザ端末によって送信されたユーザ名およびパスワードを受信する。プロセッサ11は、ユーザ名、パスワード、およびchallenge値に基づいて認証を実行し、認証結果を取得する。

【0102】

別の実施形態では、プロセッサ11がユーザ端末のためのネットワークインタフェース情報を構成することは、SMFを使用してインターネットプロトコルアドレスIPアドレスおよびホスト構成プロトコルDHCPサーバアドレスのうちの少なくとも一方をユーザ端末に割り

10

20

30

40

50

当て、AMFを使用してNAS返信メッセージを生成し、IPアドレスおよびDHCPサーバのうちの少なくとも一方をNAS返信メッセージに追加し、ネットワークインタフェース情報を取得することとして実行される。

【0103】

通信インタフェース12がネットワークインタフェース情報をユーザ端末に送信することは、特に、通信インタフェースがIP構成メッセージまたはネットワーク制御プロトコルNCPメッセージを使用してIPアドレスおよびDHCPサーバアドレスのうちの少なくとも一方をユーザ端末に送信することとして実行される。

【0104】

さらに、当業者は、本発明の実施形態が、方法、装置（デバイス）、またはコンピュータプログラム製品として提供され得ることを理解すべきである。したがって、本発明は、ハードウェアのみの実施形態、ソフトウェアのみの実施形態、またはソフトウェアとハードウェアとの組み合わせを有する実施形態の形態を使用し得る。さらに、本発明は、コンピュータ使用可能プログラムコードを含む1つ以上のコンピュータ使用可能記憶媒体（ディスクメモリ、CD-ROM、および光メモリなどを含むが、これらに限定されない）で実施されるコンピュータプログラム製品の形態を使用し得る。

10

【0105】

本発明は、本発明の実施形態による方法、装置（デバイス）、およびコンピュータプログラム製品の情報交換図を参照して説明されている。情報交換図の各手順および情報交換図の手順の組み合わせは、コンピュータプログラム命令を使用して実施され得ることを理解されたい。これらのコンピュータプログラム命令は、マシンを作るために汎用コンピュータ、専用コンピュータ、組み込みプロセッサ、または任意の他のプログラマブルデータ処理デバイスのプロセッサに提供されてもよく、これにより、コンピュータまたは任意の他のプログラマブルデータ処理デバイスのプロセッサによって実行される命令は、フローチャートの1つ以上のプロセスにおける特定の機能を実施するための装置を作る。

20

【0106】

これらのコンピュータプログラム命令は、代替的に、特定の方法で動作するようにコンピュータまたは任意の他のプログラマブルデータ処理デバイスに命令し得るコンピュータ可読メモリに記憶されてもよく、これにより、コンピュータ可読メモリに記憶された命令は、命令装置を含む人工物を作る。命令装置は、フローチャートの1つ以上のプロセスの指定された機能を実施する。

30

【0107】

これらのコンピュータプログラム命令は、一連の動作およびステップがコンピュータまたは別のプログラマブルデバイス上で実行されるようにコンピュータまたは別のプログラマブルデータ処理デバイスにさらにロードされ、その結果、コンピュータ実施処理を生成し得る。したがって、コンピュータまたは別のプログラマブルデバイス上で実行される命令は、フローチャートの1つ以上のプロセスにおける特定の機能を実施するためのステップを提供する。

【0108】

これに対応して、本発明の一実施形態は、コンピュータ記憶媒体をさらに提供する。コンピュータ記憶媒体は、プログラムを記憶し得る。プログラムが実行されると、図1から図5に示されているネットワークアクセス方法の実施形態の一部または全部のステップが実行され得る。具体的には、本発明のこの実施形態に関してここでは詳細は説明されない。

40

【0109】

本発明のいくつかの好ましい実施形態が説明されたが、当業者は、基本的な発明概念を習得したら、これらの実施形態に対して変更および修正を行い得る。したがって、以下の特許請求の範囲は、本発明の範囲内に入る好ましい実施形態ならびにあらゆる変更例および修正例を包含すると解釈されることを意図されている。

【0110】

50

明らかに、当業者は、本発明の精神および範囲から逸脱することなく、本発明に対して様々な修正および変形を行い得る。本発明は、以下の特許請求の範囲およびその均等な技術によって規定される保護範囲内に入るならば、これらの修正例および変形例を包含することを意図されている。

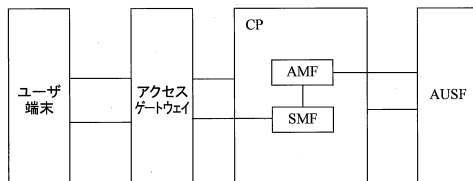
【符号の説明】

【0111】

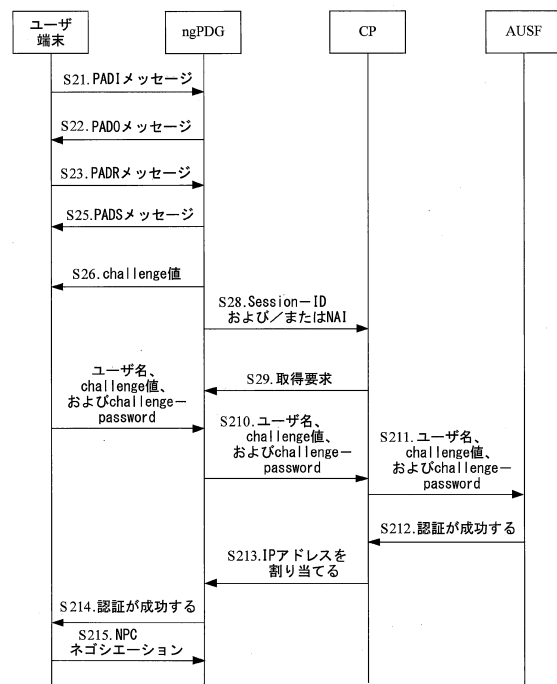
- 11 プロセッサ
- 12 通信インタフェース
- 61 取得モジュール
- 62 カプセル化モジュール
- 63 送信モジュール
- 64 受信モジュール

10

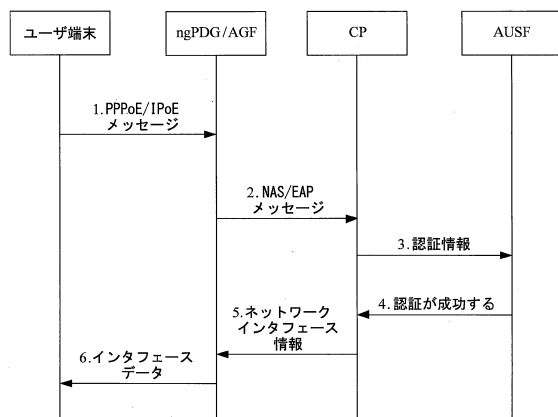
【図1】



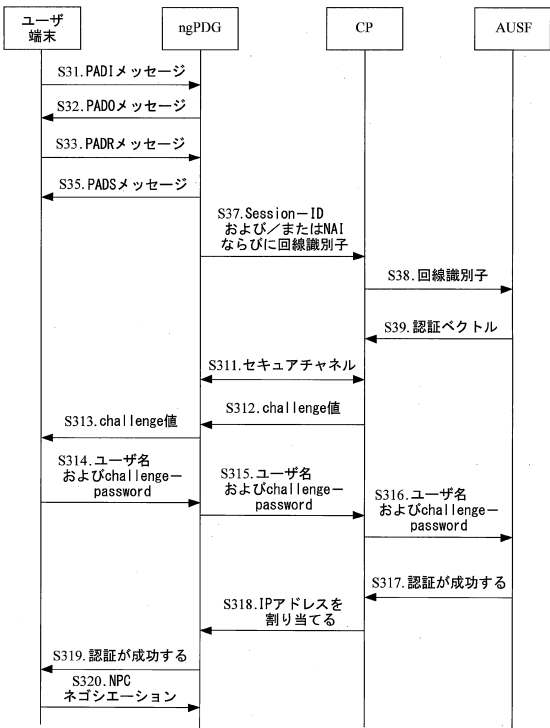
【図3】



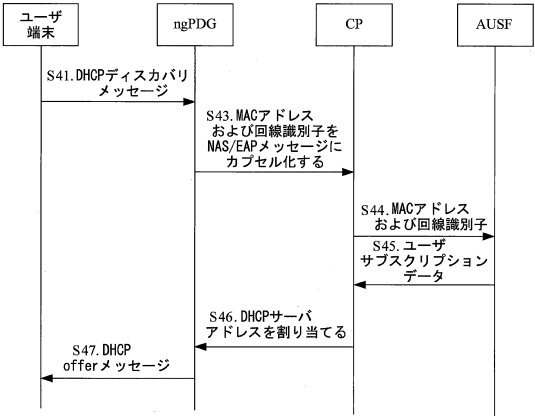
【図2】



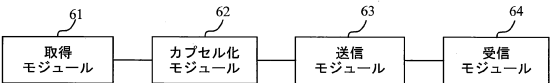
【図 4】



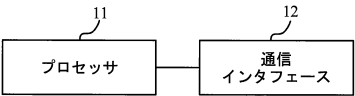
【図 5】



【図 6】



【図 7】



フロントページの続き

(74)代理人 100140534

弁理士 木内 敬二

(72)発明者 于 游洋

中華人民共和国 518129 広東省深▲チェン▼市龍崗区坂田 華為總部▲ベン▼公楼

(72)発明者 李 ▲華▼

中華人民共和国 518129 広東省深▲チェン▼市龍崗区坂田 華為總部▲ベン▼公楼

審査官 吉村 真治▲郎▼

(56)参考文献 特表2005-524341 (JP, A)

特開2014-212463 (JP, A)

米国特許出願公開第2015/0282226 (US, A1)

特開2014-155038 (JP, A)

特開2014-238664 (JP, A)

3GPP, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System; Stage 2 (Release 15), 3GPP TS 23.502 V0.2.0, 2017年02月24日, pages 24-37, 44-50, https://www.3gpp.org/ftp//Specs/archive/23_series/23.502/23502-020.zip

(58)調査した分野(Int.Cl., DB名)

H04B 7/24-7/26

H04W 4/00-99/00

H04L 12/70

3GPP TSG RAN WG1-4

SA WG1-4

CT WG1、4