

(19) 日本国特許庁(JP)

## (12) 特 許 公 報(B2)

(11) 特許番号

特許第4732974号  
(P4732974)

(45) 発行日 平成23年7月27日(2011.7.27)

(24) 登録日 平成23年4月28日(2011.4.28)

(51) Int.Cl.

F 1

H04L 12/66 (2006.01)  
H04L 12/56 (2006.01)H04L 12/66  
H04L 12/56E  
B

請求項の数 9 (全 33 頁)

(21) 出願番号	特願2006-204406 (P2006-204406)
(22) 出願日	平成18年7月27日 (2006.7.27)
(65) 公開番号	特開2008-35037 (P2008-35037A)
(43) 公開日	平成20年2月14日 (2008.2.14)
審査請求日	平成21年3月25日 (2009.3.25)

(73) 特許権者	000005108 株式会社日立製作所 東京都千代田区丸の内一丁目6番6号
(74) 代理人	110000350 ポレール特許業務法人
(72) 発明者	鎌田 正典 神奈川県横浜市戸塚区戸塚町216番地 株式会社日立コミュニケーションテクノロジー キャリアネットワーク事業部内
(72) 発明者	宮田 裕章 神奈川県横浜市戸塚区戸塚町216番地 株式会社日立コミュニケーションテクノロジー キャリアネットワーク事業部内

最終頁に続く

(54) 【発明の名称】パケット転送制御方法およびパケット転送装置

## (57) 【特許請求の範囲】

## 【請求項 1】

ユーザ端末と通信するための複数のアクセス回線を収容したエッジ側パケット転送装置と、ISPドメイン名によって識別可能な複数のコア側パケット転送装置と、ISPドメイン名と対応してレイヤ2トンネリング制御情報を記憶している認証サーバとからなり、上記各コア側パケット転送装置が、それぞれに付随する少なくとも1つのゲートウェイ(GW)装置と接続され、各ISPに所属するユーザ端末とレイヤ3網との接続が上記GW装置によって制御されるようにした広域イーサネット網におけるパケット転送制御方法であって、

ユーザ端末からレイヤ3網への接続要求パケットを受信した上記エッジ側パケット転送装置が、上記認証サーバに、該接続要求パケットから抽出されたISPドメイン名とユーザ認証情報とを含むユーザ認証要求メッセージを送信し、

上記ユーザ認証要求メッセージを受信した上記認証サーバが、ユーザ認証に成功した時、上記エッジ側パケット転送装置に、該ユーザ認証要求メッセージが示すISPドメイン名と対応するレイヤ2トンネリング制御情報を含む応答メッセージを返送し、

上記応答メッセージを受信した上記エッジ側パケット転送装置が、上記接続要求パケットの送信元アドレスと該応答メッセージが示す上記レイヤ2トンネリング制御情報との対応関係を示す新たなテーブルエントリを第1のユーザ管理テーブルに登録し、上記接続要求パケットを該レイヤ2トンネリング制御情報に従ってカプセル化し、レイヤ2トンネリングパケットとして上記広域イーサネット網に送信し、

10

20

上記レイヤ2トンネリングパケットを受信したコア側パケット転送装置が、上記受信パケットから抽出されたレイヤ2トンネリング制御情報と上記接続要求パケットの送信元アドレスとの対応関係を示す新たなテーブルエントリを第2のユーザ管理テーブルに登録し、該受信パケットをデカプセル化して得られた接続要求パケットを付随するGW装置に転送することを特徴とするパケット転送制御方法。

#### 【請求項2】

前記コア側パケット転送装置が、前記GW装置からユーザ端末宛のパケットを受信した時、前記第2のユーザ管理テーブルから上記受信パケットの送信先アドレスと対応するテーブルエントリを検索し、該テーブルエントリが示すレイヤ2トンネリング制御情報に従って上記受信パケットをカプセル化して、レイヤ2トンネリングパケットとして前記広域イーサネット網に送信し、

上記レイヤ2トンネリングパケットを受信した前記エッジ側パケット転送装置が、上記レイヤ2トンネリングパケットをデカプセル化し、得られたパケットをその送信先アドレスと対応するユーザ端末に転送することを特徴とする請求項1に記載のパケット転送制御方法。

#### 【請求項3】

前記第2のユーザ管理テーブルに、前記GW装置から受信したパケットの送信先アドレスと対応するテーブルエントリが登録されていなかった場合に、前記コア側パケット転送装置が、上記受信パケットを廃棄することを特徴とする請求項2に記載のパケット転送制御方法。

#### 【請求項4】

前記エッジ側パケット転送装置が、前記ユーザ端末からレイヤ3網への接続要求パケット以外のパケットを受信した時、前記第1のユーザ管理テーブルから、上記受信パケットの送信元アドレスと対応するテーブルエントリを検索し、該テーブルエントリが示すレイヤ2トンネリング制御情報に従って該受信パケットをカプセル化し、レイヤ2トンネリングパケットとして前記広域イーサネット網に送信し、

上記レイヤ2トンネリングパケットを受信したコア側パケット転送装置が、上記受信パケットをデカプセル化し、得られたパケットを付随するGW装置に転送することを特徴とする請求項1～請求項3の何れかに記載のパケット転送制御方法。

#### 【請求項5】

前記第1のユーザ管理テーブルに、前記ユーザ端末から受信したパケットの送信元アドレスと対応するテーブルエントリが登録されていなかった場合に、前記エッジ側パケット転送装置が、上記受信パケットを廃棄することを特徴とする請求項4に記載のパケット転送制御方法。

#### 【請求項6】

前記エッジ側パケット転送装置が、前記第1のユーザ管理テーブルに登録される新たなテーブルエントリに、前記接続要求パケットを受信したアクセス回線を示すポート番号を記憶しておき、前記コア側パケット転送装置からレイヤ2トンネリングパケットを受信した時、該レイヤ2トンネリングパケットをデカプセル化して得られたパケットを上記テーブルエントリが示すポート番号をもつ特定のアクセス回線に転送することを特徴とする請求項2に記載のパケット転送制御方法。

#### 【請求項7】

前記第1、第2のユーザ管理テーブルの各テーブルエントリが、前記レイヤ2トンネリング制御情報として、トンネリングタイプと、トンネリングタイプに対応したカプセル化ヘッダ情報を記憶しており、

前記エッジ側パケット転送装置が、上記第1のユーザ管理テーブルから検索されたテーブルエントリが示すトンネリングタイプによって決まるカプセル化ヘッダ情報を適用して、前記各アクセス回線からの受信パケットをカプセル化し、

前記コア側パケット転送装置が、上記第2のユーザ管理テーブルから検索されたテーブルエントリが示すトンネリングタイプによって決まるカプセル化ヘッダ情報を適用して

10

20

30

40

50

、前記 G W 装置からの受信パケットをカプセル化することを特徴とする請求項 2 に記載のパケット転送制御方法。

**【請求項 8】**

前記コア側パケット転送装置の少なくとも 1 つが、サービス名によって識別される複数の G W 装置と接続され、前記広域イーサネット網から、パケットヘッダに I S P ドメイン名とサービス名とを含むレイヤ 2 トンネリングパケットを受信した時、受信パケットをデカプセル化して上記サービス名で特定される G W 装置に転送することを特徴とする請求項 1 ~ 請求項 7 の何れかに記載のパケット転送制御方法。

**【請求項 9】**

I S P ドメイン名によって識別可能な複数のコア側パケット転送装置と、I S P ドメイン名と対応してレイヤ 2 トンネリング制御情報を記憶している認証サーバとを含む広域イーサネット網に接続され、ユーザ端末と通信するための複数のアクセス回線を収容したパケット転送装置であって、10

上記何れかのアクセス回線から、ユーザ端末が送信したレイヤ 3 網への接続要求パケットを受信した時、上記認証サーバに、上記接続要求パケットから抽出された I S P ドメイン名とユーザ認証情報とを含むユーザ認証要求メッセージを送信し、上記認証サーバから、上記ユーザ認証要求メッセージが示す I S P ドメイン名と対応したレイヤ 2 トンネリング制御情報を含む応答メッセージを受信するための手段と、

上記接続要求パケットの送信元アドレスと上記応答メッセージから抽出された上記レイヤ 2 トンネリング制御情報との対応関係を示す新たなテーブルエントリをユーザ管理テーブルに記憶するための手段と、20

上記接続要求パケットを上記レイヤ 2 トンネリング制御情報に従ってカプセル化し、レイヤ 2 トンネリングパケットとして上記広域イーサネット網に送信するための手段と、

上記ユーザ端末からレイヤ 3 網への接続要求パケット以外のパケットを受信した時、上記ユーザ管理テーブルから、該受信パケットの送信元アドレスと対応するテーブルエントリを検索し、該テーブルエントリが示すレイヤ 2 トンネリング制御情報に従って上記受信パケットをカプセル化し、レイヤ 2 トンネリングパケットとして上記広域イーサネット網に送信するための手段と、

上記広域イーサネット網からレイヤ 2 トンネリングパケットを受信した時、上記レイヤ 2 トンネリングパケットをデカプセル化し、得られたパケットをその送信先アドレスと対応するユーザ端末に転送するための手段とを備えたことを特徴とするパケット転送装置。30

**【発明の詳細な説明】**

**【技術分野】**

**【0 0 0 1】**

本発明は、パケット転送制御方法およびパケット転送装置に関し、更に詳しくは、P P P o E パケットなど、ユーザ認証プロトコルをレイヤ 2 トンネリングで転送するレイヤ 2 仮想私設網 ( L 2 - V P N ) におけるパケット転送制御方法およびパケット転送装置に関する。

**【背景技術】**

**【0 0 0 2】**

A D S L ( Asymmetric Digital Subscriber Line ) 、 F T T H ( Fiber To The Home ) 、無線 L A N ( Local Area Network ) などの高速アクセス回線を利用した認証型の高速インターネット接続サービス ( 高速リモートアクセスサービス ) が普及し、コンテンツデータなど、大容量の情報をユーザ端末に効率的に転送できる通信環境が整ってきている。40

**【0 0 0 3】**

高速リモートアクセスサービスでは、通信事業者が管理するゲートウェイ装置：高速アクセス終端装置 ( B A S : Broadband Access Server ) によって、端末間の接続プロトコルである P P P o E ( Point to Point over Ethernet ) と P P P が終端される。 B A S は、ユーザ端末からインターネットへの接続要求を受信すると、インターネットサービスプロバイダ ( I S P : Internet Service Provider ) その他の接続サービス企業が管理する50

認証サーバ、例えば、Radius (Remote Authentication Dial-In User Service) サーバにユーザ認証を要求する。BASは、ユーザ認証に成功したユーザ端末について、ISP網との間のレイヤ3レベルでのパケット転送サービスを開始する。

#### 【0004】

従来、専用の高速アクセス回線をもたないISP（または接続サービス企業）は、通信事業者から、高速アクセス回線とBASとを含むレイヤ3のIP（Internet Protocol）中継網を借用している。ISPは、借用した中継網をIP-VPN（Virtual Private Network）として運用することにより、PPPoEおよびPPPを意識することなく、ユーザ認証とレイヤ3のみを意識した認証型高速インターネット接続サービスを提供することができる。

10

#### 【0005】

但し、IP-VPNを利用した高速リモートアクセスサービスでは、中継網におけるレイヤ3の通信プロトコルが制約となって、ISPが、ユーザが所望する接続サービスを提供できない可能性がある。例えば、ユーザが、IPv6や汎用コンピュータで使用される独自プロトコルを利用したい場合でも、中継網がIPv4プロトコルにしか適合できなければ、ユーザの要望には応えられない。

#### 【0006】

近年、通信事業者は、IP網を前提としたIP-VPNに代えて、ADSL、FTTH、無線LANなどの高速アクセス回線と、広域イーサネット網とを利用したL2-VPNサービスを提供している。L2-VPNでは、通信事業者が管理する広域イーサネット網（イーサネットは登録商標）に、例えば、IEEE 802.1ahに規定されたEthernet over Ethernet、またはIEEE802.1adに規定された拡張VLANなどのレイヤ2トンネリングを利用することによって、拠点Aと拠点B間をあたかも同一のブロードキャスト・ドメインのように見せることができる。

20

#### 【0007】

中継網が広域イーサネット網から構成された場合、専用の高速アクセス回線をもたないISP（または通信サービス企業）でも、中継網にBASを接続し、中継網上にL2-VPNを形成することにより、高速アクセス回線に接続されたユーザに対して、従来、ISDN等においてダイヤルアップで提供していたサービスと同等の接続サービスを提供することが可能となる。すなわち、BASを所有するISP（または通信サービス企業）に対して、通信事業者が広域イーサネット網をL2-VPNとして提供することによって、各ISPは、中継網上のL3通信プロトコルによる制約を受けることなく、自由度の高い通信サービスも提供が可能となる。

30

#### 【0008】

【非特許文献1】IEEE 802.1ah : Ethernet over Ethernet

【非特許文献2】IEEE 802.1ad : 拡張VLAN

#### 【発明の開示】

##### 【発明が解決しようとする課題】

#### 【0009】

従来、通信事業者は、ISPにIP-VPNを提供するとき、高速アクセス回線やBASなどの通信設備を複数のISPに共用させている。この場合、BASは、ユーザ情報を各ユーザの契約先ISPと対応付けて管理しておき、PPPプロトコルの認証フェーズにおいて、ユーザから受信した認証要求を該ユーザと対応するISPに動的に振分けるようにしている。

40

#### 【0010】

ISPに対して、IP-VPNに代えてL2-VPNが提供された場合、拠点Aと拠点Bとの間でレイヤ2トンネリングによるパケット転送を実現するためには、拠点A、Bとなるパケット転送装置に、例えば、Ethernet over Ethernetや拡張VLAN等、トンネリングタイプに応じたトンネリング制御情報（パケット転送制御パラメータ）を設定する必要がある。しかしながら、拠点A、拠点Bとなる各パケット転送装置に、レイヤ2トンネ

50

リング制御情報を予めスタティックに設定すると、パケット転送ルートが固定的に決定される。そのため、I P - V P Nで共有B A Sが行っていたように、受信パケットをユーザ対応のI S Pに動的に振分けることが困難となる。

#### 【0011】

本発明の目的は、ユーザ端末からI P網への接続要求が発行された時点で、広域イーサネット網にレイヤ2トンネリングに必要な制御情報を動的に設定し、ユーザ端末からの送信パケットをユーザが所属するI S Pに転送可能なパケット転送制御方法およびパケット転送装置を提供することにある。

#### 【課題を解決するための手段】

#### 【0012】

上記目的を達成するため、本発明によるパケット転送制御方法は、

ユーザ端末と通信するための複数のアクセス回線を収容したエッジ側パケット転送装置（E G W）と、I S Pドメイン名によって識別可能な複数のコア側パケット転送装置（C G W）と、I S Pドメイン名と対応してレイヤ2トンネリング制御情報を記憶している認証サーバとからなり、上記各コア側パケット転送装置が、それぞれに付随する少なくとも1つのゲートウェイ（G W）装置と接続され、各I S Pに所属するユーザ端末とレイヤ3網との接続が上記G W装置によって制御される広域イーサネット網において、

ユーザ端末からレイヤ3網への接続要求パケットを受信した上記エッジ側パケット転送装置が、上記認証サーバに、該接続要求パケットから抽出されたI S Pドメイン名とユーザ認証情報とを含むユーザ認証要求メッセージを送信し、

上記ユーザ認証要求メッセージを受信した上記認証サーバが、ユーザ認証に成功した時、上記エッジ側パケット転送装置に、該ユーザ認証要求メッセージが示すI S Pドメイン名と対応するレイヤ2トンネリング制御情報を含む応答メッセージを返送し、

上記応答メッセージを受信した上記エッジ側パケット転送装置が、上記接続要求パケットの送信元アドレスと該応答メッセージが示す上記レイヤ2トンネリング制御情報との対応関係を示す新たなテーブルエントリを第1のユーザ管理テーブルに登録し、上記接続要求パケットを該レイヤ2トンネリング制御情報に従ってカプセル化し、レイヤ2トンネリングパケットとして上記広域イーサネット網に送信し、

上記レイヤ2トンネリングパケットを受信したコア側パケット転送装置が、上記受信パケットから抽出されたレイヤ2トンネリング制御情報と上記接続要求パケットの送信元アドレスとの対応関係を示す新たなテーブルエントリを第2のユーザ管理テーブルに登録し、該受信パケットをデカプセル化して得られた接続要求パケットを付随するG W装置に転送することを特徴とする。

#### 【0013】

更に詳述すると、本発明のパケット転送制御方法では、上記コア側パケット転送装置が、上記G W装置からユーザ端末宛のパケットを受信した時、上記第2のユーザ管理テーブルから上記受信パケットの送信先アドレスと対応するテーブルエントリを検索し、該テーブルエントリが示すレイヤ2トンネリング制御情報に従って上記受信パケットをカプセル化して、レイヤ2トンネリングパケットとして上記広域イーサネット網に送信し、上記レイヤ2トンネリングパケットを受信した上記エッジ側パケット転送装置が、上記レイヤ2トンネリングパケットをデカプセル化し、得られたパケットをその送信先アドレスと対応するユーザ端末に転送する。尚、上記第2のユーザ管理テーブルに、上記G W装置から受信したパケットの送信先アドレスと対応するテーブルエントリが登録されていなかった場合に、上記コア側パケット転送装置は、上記受信パケットを廃棄する。

#### 【0014】

本発明のパケット転送制御方法では、更に、上記エッジ側パケット転送装置が、上記ユーザ端末からレイヤ3網への接続要求パケット以外のパケットを受信した時、上記第1のユーザ管理テーブルから、上記受信パケットの送信元アドレスと対応するテーブルエントリを検索し、該テーブルエントリが示すレイヤ2トンネリング制御情報に従って該受信パケットをカプセル化し、レイヤ2トンネリングパケットとして前記広域イーサネット網に

10

20

30

40

50

送信し、上記レイヤ2トンネリングパケットを受信したコア側パケット転送装置が、上記受信パケットをデカプセル化し、得られたパケットを付随するG W装置に転送する。尚、上記第1のユーザ管理テーブルに、上記ユーザ端末から受信したパケットの送信元アドレスと対応するテーブルエントリが登録されていなかった場合に、上記エッジ側パケット転送装置は、上記受信パケットを廃棄する。

#### 【0015】

本発明の実施例では、上記第1、第2のユーザ管理テーブルの各テーブルエントリが、上記レイヤ2トンネリング制御情報として、トンネリングタイプと、トンネリングタイプに対応したカプセル化ヘッダ情報を記憶しており、上記エッジ側パケット転送装置が、上記第1のユーザ管理テーブルから検索されたテーブルエントリが示すトンネリングタイプによって決まるカプセル化ヘッダ情報を適用して、上記各アクセス回線からの受信パケットをカプセル化し、上記コア側パケット転送装置が、上記第2のユーザ管理テーブルから検索されたテーブルエントリが示すトンネリングタイプによって決まるカプセル化ヘッダ情報を適用して、上記B A Sからの受信パケットをカプセル化する。尚、上記第1、第2のユーザ管理テーブルのテーブルエントリは、通信終了要求パケットが発生した時点で削除される。

10

#### 【0016】

本発明の実施例では、上記コア側パケット転送装置の少なくとも1つが、サービス名によって識別される複数のG W装置と接続され、上記広域イーサネット網から、パケットヘッダにI S Pドメイン名とサービス名とを含むレイヤ2トンネリングパケットを受信した時、受信パケットをデカプセル化して上記サービス名で特定されるG W装置に転送することを特徴とする。

20

#### 【0017】

本発明によるパケット転送装置は、I S Pドメイン名によって識別可能な複数のコア側パケット転送装置と、I S Pドメイン名と対応してレイヤ2トンネリング制御情報を記憶している認証サーバとを含む広域イーサネット網に接続され、ユーザ端末と通信するための複数のアクセス回線を収容しており、

上記何れかのアクセス回線から、ユーザ端末が送信したレイヤ3網への接続要求パケットを受信した時、上記認証サーバに、上記接続要求パケットから抽出されたI S Pドメイン名とユーザ認証情報とを含むユーザ認証要求メッセージを送信し、上記認証サーバから、上記ユーザ認証要求メッセージが示すI S Pドメイン名と対応したレイヤ2トンネリング制御情報を含む応答メッセージを受信するための手段と、

30

上記接続要求パケットの送信元アドレスと上記応答メッセージから抽出された上記レイヤ2トンネリング制御情報との対応関係を示す新たなテーブルエントリをユーザ管理テーブルに記憶するための手段と、

上記接続要求パケットを上記レイヤ2トンネリング制御情報に従ってカプセル化し、レイヤ2トンネリングパケットとして上記広域イーサネット網に送信するための手段と、

上記ユーザ端末からレイヤ網への接続要求パケット以外のパケットを受信した時、上記ユーザ管理テーブルから、該受信パケットの送信元アドレスと対応するテーブルエントリを検索し、該テーブルエントリが示すレイヤ2トンネリング制御情報に従って上記受信パケットをカプセル化し、レイヤ2トンネリングパケットとして上記広域イーサネット網に送信するための手段と、

40

上記広域イーサネット網からレイヤ2トンネリングパケットを受信した時、上記レイヤ2トンネリングパケットをデカプセル化し、得られたパケットをその送信先アドレスと対応するユーザ端末に転送するための手段とを備えたことを特徴とする。

#### 【0018】

また、本発明によるパケット転送装置は、少なくとも1つのゲートウェイ(G W)装置と接続され、広域イーサネット網から受信したレイヤ2トンネリングパケットをデカプセル化して上記G W装置に転送し、上記G W装置から受信したパケットをレイヤ2トンネリングパケットに変換して上記広域イーサネット網に転送するパケット転送装置であって、

50

上記広域イーサネット網から、ユーザ端末が送信したレイヤ3網への接続要求パケットを含むレイヤ2トンネリングパケットを受信した時、該受信パケットから抽出されたレイヤ2トンネリング制御情報と上記接続要求パケットの送信元アドレスとの対応関係を示す新たなテーブルエントリをユーザ管理テーブルに登録するための手段と、

上記GW装置からパケットを受信した時、上記ユーザ管理テーブルから上記受信パケットの送信先アドレスと対応するテーブルエントリを検索し、該テーブルエントリが示すレイヤ2トンネリング制御情報に従って該受信パケットをカプセル化し、レイヤ2トンネリングパケットとして上記広域イーサネット網に送信するための手段とを備えたことを特徴とする。

#### 【発明の効果】

10

#### 【0019】

本発明によれば、L2-VPNによる高速リモートアクセスサービスにおいて、ユーザ端末からISP網への接続要求が発行された時点で、レイヤ2トンネリングに必要な制御情報を動的に設定して、ユーザ端末からの送信パケットをユーザが所属するISPに転送することが可能になる。

#### 【発明を実施するための最良の形態】

#### 【0020】

以下、本発明の実施例について、図面を参照して詳細に説明する。

図1は、ISPに対して、広域イーサネット網をL2-VPNとして提供可能な本発明による通信ネットワークの構成の1例を示す。

20

NW1は、複数のユーザ端末H(H1~Hx)およびP(P1~Pm)を複数のISP網NW2(NW2-1~NW2-n)のうちの1つに選択的に接続するための広域イーサネット網(L2-VPN網)を示す。

#### 【0021】

広域イーサネット網NW1は、それぞれユーザ端末側の複数のアクセス回線を収容するエッジ側の複数のパケット転送装置(レイヤ2ゲートウェイ:L2GW)10(10-1、10-2)と、それぞれISP網NW2(NW2-1~NW2-n)のブロードバンドアクセスサーバ(以下、BASと言う)40(40-1~40-n)と接続されたコア側の複数のパケット転送装置(レイヤ2ゲートウェイ:L2GW)20(20-1~20-3)と、ユーザ認証サーバであるRadiusサーバ31と、L2GW10(10-1、10-2)をL2GW20(20-1~20-3)に接続するための複数のレイヤ2スイッチ(以下、L2SWと言う)30(30-1~30-3)とからなっている。

30

#### 【0022】

以下の説明では、ユーザ端末側の各L2GW10を「EGW(Edge Gateway)」、ISP網側のL2GW20を「CGW(Core Gateway)」と呼ぶ。本発明では、EGW10とCGW20との間で、Ethernet over Ethernet、拡張VLANなどによるレイヤ2トンネリングを行うことによって、広域イーサネット網NW1上にISP対応の複数のL2-VPNを実現する。

#### 【0023】

各EGW10は、アクセス回線を介して各ユーザ端末(H1~Hx、P1~Pn)から受信したPPPoEパケットをEthernetヘッダでカプセル化し、レイヤ2トンネリングパケット形式でL2SW30に転送すると共に、L2SW30から受信したレイヤ2トンネリングパケットをデカプセル化し、宛先ユーザ端末が接続されたアクセス回線にPPPoEパケット形式で転送する。

40

#### 【0024】

一方、各CGW20は、L2SW30から受信したレイヤ2トンネリングパケットをデカプセル化して、ISP網NW2にPPPoeパケット形式で転送すると共に、ISP網NW2から受信したPPPoeパケットをEthernetヘッダでカプセル化し、レイヤ2トンネリングパケット形式でL2SW30に転送する。

#### 【0025】

50

図1に示した例では、各ISP網に所属するBAS40(40-1~40-n)は、各種の情報通信サービスを提供するインターネット網NW3、またはIP電話による音声通信サービスを提供するVoIP網NW4に接続されている。

ユーザ端末とEGW10との接続には、各種のアクセス回線形式が採用できる。

#### 【0026】

図示した例では、ユーザ端末H1~H3は、それぞれ個別のアクセス回線でEGW10-1に接続され、ユーザ端末P1~Pmは、受動光網PON(Passive Optical Network)を介してEGW10-1に接続されている。PONは、EGW10-1に接続された局側装置OLT(Optical Line terminal)51と、それぞれユーザ宅に配置される複数の加入者接続装置ONU(Optical Network Unit)52(52-1~52-m)とからなり、OLTに接続された光ファイバが、光カプラ(S.C:Star Coupler)53で複数の支線光ファイバに分岐され、各支線光ファイバにONUを接続した構造となっている。一方、EGW10-2には、個別アクセス回線を介してユーザ端末Hxが接続され、L2SW50を介してユーザ端末H4、H5が接続されている。  
10

各EGW10は、後述するユーザ管理テーブルによって、それぞれに収容されているユーザ端末毎にレイヤ2トンネリング制御情報を管理し、Radiusサーバ31を利用してユーザ認証を行う。

#### 【0027】

図2(A)は、図1のネットワークにおいて、EGW10とユーザ端末、CGW20とBAS40との間で送受信されるPPPoEパケットのフォーマットを示す。  
20

PPPoEパケットは、Ethernetヘッダ71と、PPPoEヘッダ72と、PPPパケットの主体となる可変長のPPPoEペイロード73とから構成される。

Ethernetヘッダ71は、送信元MACアドレス711と、宛先MACアドレス722と、後続ヘッダのプロトコルタイプ713と、その他のヘッダ項目からなる。

#### 【0028】

PPPoEヘッダ72は、バージョン721、タイプ722、コード723、セッションID724、ペイロード長725を含む。コード723は、ユーザ端末から接続要求パケット(PPPoEフェーズの開始パケット)として送信されるPADI(The PPPoE Active Discovery Initiation)パケット、PADIに対する応答パケットであるPADO(The PPPoE Active Discovery Offer)パケット、PPPセッションの開始要求パケットであるPADR(The PPPoE Active Discovery Request)パケット、PADRに対する応答パケットであるPADS(The PPPoE Active Discovery Session-Confirmation)パケット、PPP通信の終了要求パケットであるPADT(PPPoE Active Discovery Terminate)等、パケット種別を示す識別情報が設定される。  
30

#### 【0029】

また、PPPoEペイロード732には、TAG731が含まれる。TAG731は、図2(B)に示すように、TAGタイプ7311、TAG長7312、TAG VALUE7313からなる。TAGタイプ7311は、TAG VALUE7313の種別を示す。ユーザが、所望の通信サービスをサービス名によって指定する場合、TAGタイプ7311には値「0x0101」が設定され、TAG長7313でサービス名の長さを指定し、TAG VALUE7313にサービス名が記述される。  
40

#### 【0030】

例えば、ユーザがVoIP網NW4を利用したIP電話サービスを所望した場合、TAGタイプ7311に「0x0101」、TAG VALUE7313にVoIPサービスの識別名称、TAG長7312に上記サービス名称の長さが設定される。TAG VALUE7313に何も記述されていなければ、TAG長7312は「0」とみなされる。

#### 【0031】

TAG VALUE7313には、後述するように、サービス名と共に、ISPのドメイン名とパスワードを記述できる。また、サービス名を省略して、ISPのドメイン名とパスワードのみを記述することもできる。サービス名が指定されていなければ、CGW2  
50

0側では、通常のインターネット網NW3への接続サービスが実行される。

#### 【0032】

図3に、図1に示した広域イーサネット網におけるユーザ端末の接続先BASの選択動作の説明図を示す。

本発明では、広域イーサネット網(L2-VPN網)NW1を利用した接続サービスにおいて、ユーザ端末(H1~Hx、P1~Pm)から受信したPPPoEパケットをISP網NW2(NW2-1~NW2-n)にある複数のBAS40-1~40-nのうちの1つに動的に振分けるために、図2に示したPPPoEパケットのTAG VALUE7313に、サービス名(サービス識別子)の他に、接続先となるISPを示すドメイン名とパスワード情報を記述する。

10

#### 【0033】

PPPoeパケットの転送装置であるEGW10(10-1、10-2)とCGW20(20-1~20-3)は、ユーザ端末からIP網への接続要求パケット(PADIパケット)を受信すると、PADIパケットをTAG VALUE7313が示すドメイン名で特定されるISP網に振分ける。

例えば、図3のユーザ端末H1が、TAG VALUE7313として「voip@isp1;pass1」を含むPADIパケットを送信した場合を想定する。ここで、「voip」はサービス名、「@isp1」はドメイン名、「pass1」はパスワード情報を示している。この場合、PADIパケットは、ドメイン名に従って、図3に太い実線で示すように、EGW10-1とL2SW30を経由してCGW20-1に転送される。CGW20-1は、上記PADIパケットを受信すると、これをドメイン名「voip」をもつISP網NW2-1に設置されたVoIP網(NW4)接続用のBAS40-1に振り分ける。

20

#### 【0034】

同様に、ユーザH3から送信されたTAG VALUE7313に「voip@isp4;pass4」を含むPADIパケットは、太い一点鎖線で示すように、EGW10-1とL2SW30を経由してCGW20-2に転送され、ドメイン名「isp4」をもつISP網NW2-4に設置されたVoIP網接続用のBAS40-4に転送される。

#### 【0035】

ユーザ端末H4から送信されたTAG VALUE7313に「@isp5;pass5」を含むPADIパケットは、サービス名が省略されているため、太い鎖線で示すように、EGW10-2とL2SW30を経由してCGW20-3に転送される。この場合、TAG VALUE7313でサービス名が省略されているため、PADIパケットは、ドメイン名「isp5」をもつISP網NW2-5に設置されたインターネット網(NW3)接続用のBAS40-5に振り分けられる。

30

#### 【0036】

図4は、EGW10(10-1、10-2)の1実施例を示すブロック構成図である。

EGW10は、それぞれポート番号をもつ複数の入出力回線インターフェース11(11-1~11-n)と、これらの入出力回線インターフェース11に接続されたルーティング部12と、ルーティング部12に接続された制御部13とからなる。90は、制御部13に接続された制御端末を示す。

40

#### 【0037】

制御部13は、ルーティング部12と共同して、プロトコル処理を実行する。

制御部13は、プロセッサ14と、メモリ15と、送信バッファ16Tおよび受信バッファ16Rとからなる。メモリ15には、プロセッサ14が実行するプログラムとして、ユーザ端末のインターネット接続/切断、PPPoeパケットのカプセル化、レイヤ2トунネリングパケットのデカプセル化を行うための通信処理ルーチン100と、Radiusサーバ31と通信するためのRadius通信処理ルーチンが格納されている。また、メモリ15には、後述するユーザ管理テーブル17とポート管理テーブル18が形成されている。

#### 【0038】

50

ルーティング部12は、回線インターフェース11-1~11-nからパケットを受信すると、PPPoEヘッダのパケット種別識別情報から、受信パケットが通信制御パケットかユーザパケットかを判定し、受信パケットが、前述したPADI等の通信制御パケットの場合、受信パケットを受信バッファ16Rに転送する。ルーティング部12は、回線インターフェース11-1~11-nから受信したユーザパケットと、プロセッサ14が送信バッファ16Tに出力した通信制御パケットについては、送信先MACアドレス711またはTAG731に従って、回線インターフェース11-1~11-nのうちの何れかに転送する。

#### 【0039】

図5A~図5Fは、EGW10-1の制御部13が備えるユーザ管理テーブル17の構成と時系列的な内容変化を示す。他のEGWも、これと同様の構成をもつユーザ管理テーブル17を備えている。10

ユーザ管理テーブル17は、ユーザ端末のMACアドレス（以下、ユーザMACアドレスと言う）と対応した複数のテーブルエントリ170（170-1、170-2、・・・）からなる。

#### 【0040】

各テーブルエントリ170は、ユーザMACアドレス171と、ユーザ端末とBAS40との間に定義されたVLANの識別子（VLAN ID）172と、EGW10-1とCGW20（20-1~20-3）との間に形成されたレイヤ2トンネリングの種類、例えば、Ethernet over Ethernet、拡張VLANなどを示すレイヤ2トンネリングタイプ173と、EGW10-1とCGW20（20-1~20-3）との間のVLANの識別子を示すS-VLAN ID174と、EGW10-1のMACアドレス175と、レイヤ2トンネリングで接続されたCGWのMACアドレス176と、MACアドレス171をもつユーザ端末を収容している回線インターフェースのポート番号（ユーザ側ポート番号）177と、VLANを中継する広域イーサネット網側の回線インターフェースのポート番号（L2-VPN側ポート番号）178を示す複数のフィールドからなる。20

#### 【0041】

プロセッサ14は、ユーザ端末からPADIパケット受信した時、例えば、図5Aのエントリ170-2が示すように、ユーザMACアドレス171と、VLAN ID172と、ユーザ側ポート番号177とを示す新たなテーブルエントリをユーザ管理テーブル17に追加する。受信したPADIパケットにVLAN IDが設定されていなかった場合、VLAN ID172には、ID未定義を示すコード「-」が設定される。30

#### 【0042】

レイヤ2トンネリングタイプ173、S-VLAN ID174、EGW MACアドレス175、CGW MACアドレス176には、後述するように、ユーザ認証を行なったRadiusサーバD1からアクセス許可メッセージAccess-Acceptを受信した時点で、受信メッセージ（Access-Accept）から抽出された値が設定される。

#### 【0043】

Access-Acceptメッセージが、VLAN識別子（S-VLAN ID）を示していない場合、例えば、トンネリングタイプがEthernet over Ethernetの場合は、S-VLAN ID174には、ID未定義を示すコード「-」が設定される。また、Access-Acceptメッセージが、EGW2のMACアドレスとCGWのMACアドレスを示していなかった場合、例えば、トンネリングタイプが拡張VLANの場合は、EGW MACアドレス175とCGW MACアドレス176には、アドレス未定義を示すコード「-」が設定される。40

L2-VPN側ポート番号178には、ポート管理テーブル18に登録されたドメイン名毎のポート番号の値が設定される。図5B~図5Fが示すユーザ管理テーブル17の時系列的な内容変化については、後で詳述する。

#### 【0044】

図6は、EGW10-1が備えるポート管理テーブル18の構成を示す。50

ポート管理テーブル18は、EGW10-1がアクセス可能なISP網NW2-1～NW2-nのドメイン181と対応して、L2-VPN側の回線インターフェース11のポート番号(L2-VPN側ポート番号)182を示す複数のエントリからなる。ポート管理テーブル18の各エントリは、ネットワーク管理者によって予め登録される。

#### 【0045】

図7は、CGW20(20-1～20-3)の構成を示す。

CGW20は、それぞれポート番号をもつ複数の入出力回線インターフェース21(21-1～21-n)と、これらの回線インターフェース21に接続されたルーティング部22と、ルーティング部22に接続された制御部23とからなる。91は、制御部22に接続された制御端末を示す。

10

#### 【0046】

制御部23は、ルーティング部22と共同して、プロトコル処理を実行する。制御部23は、プロセッサ24と、メモリ25と、送信バッファ26Tおよび受信バッファ26Rとからなる。

メモリ25には、プロセッサ24が実行するプログラムとして、ユーザ端末のインターネットへの接続/切断、PPPoeパケットとレイヤ2トンネリングパケットとを相互変換するための受信パケットのカプセル化/デカプセル化、PADIパケットのTAGVALEからのサービス名を特定などの処理を実行するための通信処理プログラム200が格納されている。また、メモリ25には、後述するユーザ管理テーブル27とポート管理テーブル28が形成される。

20

#### 【0047】

ルーティング部22は、回線インターフェース21-1～21-nからパケットを受信すると、PPPoeヘッダが示すパケット種別から、受信パケットが通信制御パケットか否かを判定し、受信パケットが、前述したPADI等の通信制御パケットの場合、受信パケットを受信バッファ26Rに転送する。ルーティング部22は、回線インターフェース21-1～21-nから受信したパケットユーザと、プロセッサ24が送信バッファ26Tに出力した通信制御パケットについては、送信元MACアドレス711またはTAG731に従って、回線インターフェース21-1～21-nの何れかに転送する。

#### 【0048】

図8(A)、(B)は、CGW20-1が備えるユーザ管理テーブル27-1、図9(A)、(B)は、CGW20-2が備えるユーザ管理テーブル27-2の構成を示す。

30

ユーザ管理テーブル27-1、27-2は、それぞれユーザ端末のMACアドレスと対応した複数のテーブルエントリ270(270-1、270-2、・・・)からなる。

#### 【0049】

各テーブルエントリ270は、ユーザ端末のMACアドレス(ユーザMACアドレス)271と、ユーザ端末とBAS40との間に定義されたVLANの識別子(VLANID)272と、CGW20(20-1または20-2)とEGW10(10-1または10-2)との間に形成されたレイヤ2トンネリングの種類、例えば、Ethernet over Ethernet、拡張VLANなどを示すレイヤ2トンネリングタイプ173と、CGW20とEGW10との間のVLANの識別子を示すS-VLAN ID274と、CGW20のMACアドレス275と、レイヤ2トンネリングで接続されたEGW10のMACアドレス276と、L2-VPN側ポート番号277と、ISP側ポート番号278とを示す複数のフィールドからなる。

40

#### 【0050】

CGW20-1(20-2)は、ユーザ端末からレイヤ2トンネリングパケット形式でPADIパケットを受信した時、ユーザMACアドレス271、VLAN ID:272、レイヤ2トンネリングタイプ273、S-VLAN ID:274、CGW MACアドレス275、EGW MACアドレス276、L2-VPN側ポート番号277を含む新たなテーブルエントリをユーザ管理テーブル27-1(27-2)に登録する。

#### 【0051】

50

受信したレイヤ2トンネリングパケットに、ユーザ端末とBAS間のVLAN ID、およびEGWとCGW間のVLAN ID(S-VLAN ID)が設定されていなかった場合、すなわち、受信パケットのトンネリングタイプがEthernet over Ethernetの場合、上記テーブルエントリのVLAN ID272とS-VLAN ID274には、ID未定義を示すコード「-」が設定される。

#### 【0052】

また、受信したレイヤ2トンネリングパケットに、CGWのMACアドレスおよびEGWのMACアドレスが設定されていなかった場合、すなわち、受信パケットのトンネリングタイプが拡張VLANの場合、CGW MACアドレス275とEGW MACアドレス276には、アドレス未定義を示すコード「-」が設定される。10

ISP側ポート番号278には、ポート管理テーブル28(28-1、28-2)から検索されたポート番号が設定される。尚、ユーザ管理テーブル27-1、27-2の更新については、後で詳述する。

#### 【0053】

図10に、CGW20-1が備えるポート管理テーブル28-1、図11にCGW20-2が備えるポート管理テーブル28-2の構成を示す。

ポート管理テーブル28-1(28-2)は、複数のテーブルエントリからなり、各エントリは、CGW20-1(20-2)に接続されるISP網のドメイン281と、ISP網側の回線インターフェース21(21-1~21-n)に付与されたISP側ポート番号282と、サービス名編集フラグ283との対応関係を示している。20

#### 【0054】

サービス名編集フラグ283は、L2-VPN網からPADIパケットを受信した時、受信パケットのTAG VALUE7313からドメイン名とパスワードを除外し、サービス名のみを含むTAG VALUEに編集してから、受信パケットをBASに転送するか、このようなサービス名の編集を実行することなく、受信パケットをBASに転送するかの区別を示す。ここでは、フラグ情報「1」は、サービス名編集の実行要を示し、フラグ情報「0」はサービス名編集の実行不要を示している。これらのテーブルエントリは、ネットワーク管理者によって、予めポート管理テーブル28-1、28-2に登録される。

#### 【0055】

図12は、Radiusサーバ31が備えるユーザ管理テーブル37の構成を示す。

ユーザ管理テーブル37の各エントリは、ISPのドメイン371と、パスワード372と、EGWとCGWとの間に適用すべきレイヤ2トンネリングのタイプ373と、EGWとCGWとの間のVLAN IDを示すS-VLAN ID374と、EGWのMACアドレス375と、CGWのMACアドレス376との対応関係を示している。30

#### 【実施例1】

#### 【0056】

次に、本発明の第1実施例として、EGW10-1とCGW20-1との間にEthernet over Ethernetのレイヤ2トンネリングを適用してL2-VPNを実現する場合のEGWとCGWの動作について、図13~図20を参照して説明する。40

#### 【0057】

図13は、図1に示した通信ネットワークにおいて、ユーザ端末H1がVoIP網NW4への接続要求パケットPADIを発行した場合の通信シーケンス図を示す。図14は、第1実施例におけるPADIパケットのフォーマットの変換過程、図15は、PAD0パケットのフォーマット変換過程、図16は、PADRパケットのフォーマット変換過程を示している。

#### 【0058】

また、図17は、EGW10-1が実行する上りパケット(ユーザ端末側からの受信パケット)の処理ルーチン110のフローチャート、図18は、EGW10-1が実行する下りパケット(L2-VPN網側からの受信パケット)の処理ルーチン130のフローチ50

ヤート、図19は、CGW20-1が実行する上りパケット(L2-VPN網側からの受信パケット)の処理ルーチン210のフローチャート、図207は、CGW20-1が実行する下りパケット(ISP網側からの受信パケット)の処理ルーチン230のフローチャートを示している。尚、EGW10-1が実行するパケット処理ルーチン110と130は、通信処理プログラム100の一部であり、CGW20-1が実行するパケット処理ルーチン210と230は、通信処理プログラム200の一部である。

#### 【0059】

ユーザ端末H1は、VoIP網NW4への接続を要求する場合、TAG VALUEで、サービス名「voip」を指定したPADIパケットをブロードキャストする(図13のSQ1-1)。上記PADIパケットは、図14にフォーマットF1-1で示すように、送信先MACアドレス(Mac DA)711にブロードキャストアドレス、送信元MACアドレス(Mac SA)712にユーザ端末H1のMACアドレスを含み、パケット種別コード723に「PADI」、TAG731に、TAG VALUEとして、「voip@isp1;pass1」を含む。ここで、「voip」、「@isp1」、「pass1」は、それぞれサービス名、ドメイン名、パスワードを示している。

#### 【0060】

EGW10-1は、上記PADIパケットを受信すると、図17に示す上りパケット処理ルーチン110を実行し、受信したPPPoeパケットが、PADIパケットか否かを判定する(ステップ111)。今回の受信パケットはPADIパケットであるため、EGW10-1は、ユーザ管理テーブル17に新たなテーブルエントリを追加登録する(112)。

#### 【0061】

上記テーブルエントリは、図5Aのエントリ170-2が示すように、ユーザMACアドレス171として、受信パケットの送信元MACアドレス「00.99.c0.61.72.00」、ユーザ側ポート番号177として、PADIパケットを受信した回線インタフェース11-iのポート番号(この例では「1」)を含む。レイヤ2トンネリングタイプがEthernet over Ethernetの場合、PADIパケットには、VLAN IDが付与されていない。従つて、上記テーブルエントリのVLAN ID172には、コード「-」が設定される。

#### 【0062】

EGW20-1は、この後、受信パケットからTAG VALUE7313:「voip@isp1;pass1」を抽出し(113)、このTAG VALUEから抽出されたドメイン名「isp1」とパスワード「pass1」とを含むユーザ認証要求メッセージ(Access-Request)をRadiusサーバ31に送信して(114、図13のSQ1-2)、Radiusサーバ31からの応答(認証結果)メッセージを待つ(115)。

#### 【0063】

Radiusサーバ31は、Access-Requestを受信すると、ユーザ管理テーブル37からドメイン名「isp1」をもつテーブルエントリ370-1を検索し、該テーブルエントリが示すパスワード372とAccess-Requestが示すパスワード「pass1」とを照合する。

#### 【0064】

パスワードが正常であった場合、Radiusサーバ31は、EGW19-1に、Access-Requestに対する応答メッセージとして、ユーザ認証成功を示すアクセス許可メッセージ(Access-Accept)を送信する(SQ1-3)。上記Access-Acceptは、ユーザ管理テーブル37のテーブルエントリ370-1に登録されているレイヤ2トンネリングタイプ373:「Ethernet over Ethernet」と、CGW MACアドレス376:「00.99.c0.44.2.1.00」と、EGW MACアドレス375:「00.99.c0.36.11.00」とを含む。尚、Access-Requestが示すパスワードが、テーブルエントリ370-1に登録されたパスワード372と一致しなかった場合、Radiusサーバ31は、認証失敗を示す応答メッセージを返送する。

#### 【0065】

10

20

30

40

50

E G W 1 0 - 1 は、 R a d i u s サーバ D 1 からの応答メッセージを受信すると、認証結果を判定する(116)。もし、認証に失敗していた場合、E G W 1 0 - 1 は、ユーザ管理テーブルから上記新エントリを削除し、要求元ユーザ端末 H 1 に、P P P 通信の終了要求パケット(P A D T)を送信して(117)、このルーチンを終了する。

#### 【 0 0 6 6 】

R a d i u s サーバ D 1 からの応答メッセージがAccess-Acceptの場合、E G W 1 0 - 1 は、受信したAccess-Acceptが示すレイヤ2トンネリングタイプ:「Ethernet over Ethernet」、E G W M A C アドレス:「00.99.c0.36.11.00」、C G W M A C アドレス:「00.99.c0.44.21.00」をユーザ管理テーブルに登録する(118)。この時点で、テーブルエントリ 1 7 0 - 2 は、図 5 B に示した状態となる。レイヤ2トンネリングタイプが「Ethernet over Ethernet」の場合、Access-Acceptには、E G W と C G W との間のV L A N I D の値が含まれないため、テーブルエントリ 1 7 0 - 2 のS - V L A N I D 1 7 4 には、コード「-」が設定される。  
10

#### 【 0 0 6 7 】

E G W 1 0 - 1 は、次に、P A D I パケットのT A G V A L U E 7 3 1 3 からドメイン名「isp1」を抽出し、ポート管理テーブル 1 8 から、上記ドメイン名「isp1」と対応するL 2 - V P N 側ポート番号 1 8 2 の値「5」を検索し(119)、検索されたポート番号「5」をユーザ管理テーブル 1 7 にL 2 - V P N 側ポート番号 1 7 8 として登録する(120)。これによって、ユーザ管理テーブル 1 7 のエントリ 1 7 0 - 2 は、図 5 C に示した状態となる。  
20

#### 【 0 0 6 8 】

この後、E G W 1 0 - 1 は、ユーザ管理テーブル 1 7 のテーブルエントリ 1 7 0 - 2 のレイヤ2トンネリングタイプ 1 7 3 を判定する(122)。この例では、レイヤ2トンネリングタイプ 1 7 3 は、「Ethernet over Ethernet」となっている。そこで、E G W 1 0 - 1 は、図 1 4 にフォーマット F 1 - 2 で示すように、カプセル化ヘッダ 7 4 のS - M a c D A 7 4 1 と S - M a c S A 7 4 2 として、上記テーブルエントリ 1 7 0 - 2 が示すC G W M A C アドレス 1 7 6 と E G W M A C アドレス 1 7 5 を適用して、P A D I パケットをカプセル化する(123、図 1 3 のS Q 1 - 4)。

#### 【 0 0 6 9 】

E G W 1 0 - 1 は、ユーザ管理テーブル 1 7 のエントリ 1 7 0 - 2 が示すL 2 - V P N 側ポート番号 1 7 8 の値「5」をメモリ 2 5 のワークエリアに一時的に保持し(125)、上記カプセル化されたパケットの種別を判定する(126)。今回のように、カプセル化パケット(レイヤ2トンネリングパケット)がP A D I パケットの場合、E G W 1 0 - 1 は、カプセル化パケットをポート番号「5」をもつ回線インターフェースから広域イーサネット網(L 2 - V P N )に送信して(128、図 1 3 のS Q 1 - 5)、このルーチンを終了する。  
30

#### 【 0 0 7 0 】

尚、カプセル化パケットが、P A D T パケットの場合、E G W 1 0 - 1 は、ユーザ管理テーブル 1 7 から、ユーザM A C アドレス 1 7 1 が上記P A D T パケットの送信先M A C アドレスまたは送信元M A C アドレスに一致するテーブルエントリを削除(127)した後、上記カプセル化パケットのL 2 - V P N への送信(128)を実行する。  
40

#### 【 0 0 7 1 】

上記カプセル化されたP A D I パケット(レイヤ2トンネリングパケット)は、L 2 S W 3 0 - 1 で受信される。L 2 S W : 3 0 - 1 は、E G W 1 0 - 1 からレイヤ2トンネリングパケットを受信すると、送信先M A C アドレス「00.99.c0.44.21.00」に従って、上記受信パケットをC G W 2 0 - 1 に転送する(図 1 3 のS Q 1 - 6)。

#### 【 0 0 7 2 】

C G W 2 0 - 1 は、上記レイヤ2トンネリングパケットを受信すると、図 1 9 に示す上りパケット処理ルーチン 2 1 0 を実行し、受信パケットのトンネリングタイプを判定する(211)。今回は、受信パケットのトンネリングタイプは、「Ethernet over Ethernet  
50

」となっているため、CGW20-1は、受信したレイヤ2トンネリングパケットから、カプセル化ヘッダ74を除去し(デカプセル化:212、図13のSQ1-7)、受信パケットの種別を判定する(214)。

受信パケットが、PADIパケットの場合、CGW20-1は、ユーザ管理テーブル27に、受信したPADIパケットの送信元MACアドレスをユーザMACアドレス271とする新たなテーブルエントリを追加する。

#### 【0073】

図8(A)のテーブルエントリ270-2は、この時点でユーザ管理テーブル27に新たに追加されたエントリの内容を示している。ユーザMACアドレス271には、ユーザ端末H1のMACアドレス「00.99.c0.61.72.00」、レイヤ2トンネリングタイプ273には、受信パケットのトンネリングタイプである「Ethernet over Ethernet」を示すコードが設定される。CGW MACアドレス275とEGW MACアドレス276には、カプセル化ヘッダ74のS-MacDA741とS-MacSA742が示す「00.99.c0.44.21.00」と「00.99.c0.36.11.00」が設定され、L2-VPN側のポート番号277には、上記レイヤ2トンネリングパケットを受信した回線インターフェースのポート番号「2」が設定される。  
10

#### 【0074】

トンネリングタイプが「Ethernet over Ethernet」のレイヤ2トンネリングパケットには、ユーザ端末とBASとの間のVLAN IDと、EGWとCGWとの間のVLAN ID(「S-VLAN ID」)が設定されていないため、テーブルエントリ270-2のVLAN ID272とS-VLAN ID274にはコード「-」が設定される。  
20

#### 【0075】

CGW20-1は、次に、図10に示したポート管理テーブル28-1から、PADIパケットのTAG VALUEが示すドメイン名「isp1」と対応するISP側ポート番号282とサービス名編集フラグ283を検索し(216)、検索されたISP側ポート番号の値(この例では「5」)をユーザ管理テーブル27-1にISP側ポート番号278として登録する(217)。この結果、テーブルエントリ270-2は、図8(B)に示した状態となる。

#### 【0076】

CGW20-1は、検索されたサービス名編集フラグ283の値から、サービス名編集の要否を判定する(218)。ポート管理テーブル28-1では、ドメイン名「isp1」と対応するテーブルエントリ280-11で、サービス名編集フラグ283が「1」に設定されている。そこで、CGW20-1は、PADIパケットのTAG VALUEが示す「voip@isp1;pass1」を解析して、TAG VALUEからドメイン名「isp1」とパスワード情報「pass1」を除外して、図14にフォーマットF1-3で示すように、受信パケット(PADIパケット)をTAG VALUEとしてサービス名「voip」のみを含む送信パケットに変換する(219、図13のSQ1-8)。  
30

#### 【0077】

この後、CGW20-1は、ユーザ管理テーブル27-1から、上記送信パケットの送信元MACアドレスと対応するISP側ポート番号278の値「5」を検索し(220)、送信パケットをISP側ポート番号「5」をもつ回線インターフェース21-5からISP網に送信して(224、図13のSQ1-9)、このルーティングを終了する。  
40

#### 【0078】

CGW20-1がISP網に送信したPADIパケットは、BAS40-1によって受信される。BAS40-1は、上記PADIパケットを受信すると、応答パケットとしてPADOパケットをCGW20-1に返送する(図13のSQ1-10)。PADOパケットは、図15にフォーマットF2-1で示すように、送信先MACアドレス711にユーザ端末H1のMACアドレスを含み、送信元MACアドレス712にBAS40-1のMACアドレスを含む。

#### 【0079】

C GW20 - 1は、ISP網側からパケットを受信すると、図20に示す下りパケット処理ルーチン230を実行し、ユーザ管理テーブル27 - 1から、ユーザMACアドレス271が受信パケットの送信先MACアドレス711に該当するテーブルエントリを検索する(231)。検索の結果(232)、送信先MACアドレスに対応するテーブルエントリがユーザ管理テーブル27 - 1に未登録と判定され場合、C GW20 - 1は、受信パケットを廃棄して(233)、このルーチンを終了する。

#### 【0080】

今回の例では、ユーザ管理テーブル27 - 1から、受信パケット(PAD0)の送信先MACアドレス「00.99.c0.61.72.00」と対応するテーブルエントリ270 - 2が検索される。そこで、C GW20 - 1は、検索されたテーブルエントリ270 - 2のレイヤ2トンネリングタイプ273を判定する(234)。トンネリングタイプが「Ethernet over Ethernet」の場合、C GW20 - 1は、上記テーブルエントリが示すC GW MACアドレス275とEGW MACアドレス276をカプセル化ヘッダ74に適用して、受信パケットをカプセル化する(235、図13のSQ1 - 11)。上記カプセル化によって、受信パケット(PAD0)は、図15にフォーマットF2 - 2で示すように、S-MacDA741としてEGW110 - 1のMACアドレス「00.99.c0.36.11.00」、S-MacSA742としてC GW20 - 1のMACアドレス「00.99.c0.44.21.00」をもつ送信パケット(レイヤ2トンネリングパケット)に変換される。

#### 【0081】

C GW20 - 1は、次に、送信パケットがPPP通信の終了要求を示すPADTパケットか否かを判定する(237)。今回のように、送信パケットがPAD0パケットの場合は、C GW20 - 1は、ユーザ管理テーブル27 - 1のテーブルエントリ270 - 2が示すL2 - VPN側ポート番号278と対応する回線インターフェースから、上記送信パケットを送信し(239、図13のSQ1 - 12)、このルーチンを終了する。これによって、PAD0パケットは、PAD1パケットとは逆のルートでL2SW30 - 1に転送される。

尚、送信パケットがPADTパケットの場合、C GW20 - 1は、ユーザ管理テーブル27 - 1から、上記検索されたテーブルエントリを削除(238)した後、ステップ239を実行する。

#### 【0082】

L2SW30 - 1は、C GWからレイヤ2トンネリングパケットを受信すると、カプセル化ヘッダの送信先MACアドレス741(この例では「00.99.c0.36.11.00」)に従つて、受信パケットをEGW110 - 1に転送する(図13のSQ1 - 13)。

#### 【0083】

EGW110 - 1は、L2 - VPN側から上記レイヤ2トンネリングパケットを受信すると、図18に示す下りパケット処理ルーチン130を実行し、受信パケットのトンネリングタイプを判定する(131)。この例では、トンネリングタイプが「Ethernet over Ethernet」となっているため、EGW110 - 1は、受信パケットからカプセル化ヘッダ74を除去(デカプセル化)する(132、図13のSQ1 - 14)。これによって、図15に示すように、フォーマットF2 - 2のL2トンネリングパケットが、フォーマットF2 - 3のPPPoEパケットに変換される。

#### 【0084】

EGW110 - 1は、ユーザ管理テーブル17から、ユーザMACアドレス171が、デカプセル化された受信パケットの送信先MACアドレス711に該当するテーブルエントリを検索する(134)。EGW110 - 1は、検索結果を判定し(135)、ユーザ管理テーブル17に送信先MACアドレス711と対応するテーブルエントリが見つからなければ、受信パケットを廃棄して(140)、このルーチンを終了する。

#### 【0085】

今回は、受信パケットの送信先MACアドレス「00.99.c0.61.72.00」と対応するテーブルエントリ170 - 2がユーザ管理テーブル17から検索される。この場合、EGW1

10

20

30

40

50

0 - 1 は、テーブルエントリ 170 - 2 が示すユーザ側ポート番号 177 の値「1」をワークメモリに記憶（136）した後、受信パケットの種別を判定する（137）。受信パケットが、PPP通信の終了要求パケット（PADT）でなければ、EGW10 - 1 は、受信パケットをユーザ側ポート番号「1」をもつ回線インターフェース 11 - 1 から送出して（139）、このルーチンを終了する。これによって、BAS40 - 1 から返送されたPADOパケットが、PADIパケットの送信元ユーザ端末H1に転送される（図13のSQ1 - 15）。

尚、受信パケットがPADTパケットの場合、EGW10 - 1 は、上記検索されたテーブルエントリ 170 - 2 をユーザ管理テーブル 17 から削除（138）した後、ステップ 139 を実行する。  
10

#### 【0086】

ユーザ端末H1は、PADOパケットを受信すると、PPPセッションの開始要求パケットであるPADRを送信する（図13のSQ1 - 16）。PADRパケットは、図16にフォーマットF3 - 1で示すように、Ethernetヘッダの送信先MACアドレス711が、BAS40 - 1 のMACアドレス「00.99.c0.93.19.00」を示している。

#### 【0087】

EGW10 - 1 は、上記PADRパケットを受信すると、図17に示す上りパケット処理ルーチン 110 を実行し、受信パケットの種類を判定する（111）。今回は、PADRパケットを受信しているため、EGW10 - 1 は、ユーザMACアドレス171が、受信パケットの送信元MACアドレス712（「00.99.c0.61.72.00」）に該当するテーブルエントリがユーザ管理テーブル 17 に登録済みか否かを判定する（121）。目的のテーブルエントリがユーザ管理テーブル 17 に登録されていなければ、EGW10 - 1 は、受信パケットを廃棄して（129）、このルーチンを終了する。  
20

#### 【0088】

今回は、送信元MACアドレス「00.99.c0.61.72.00」と対応するテーブルエントリ 170 - 2 がユーザ管理テーブル 17 に登録済みとなっているため、EGW10 - 1 は、上記テーブルエントリ 170 - 2 のレイヤ2トンネリングタイプ 173 を判定する（122）。この例では、テーブルエントリ 170 - 2 のレイヤ2トンネリングタイプ 173 は、「Ethernet over Ethernet」となっている。そこで、EGW10 - 1 は、図16にフォーマットF3 - 2で示すように、S-MacDA741とS-MacSA742に、ユーザ管理テーブルのエントリ 170 - 2 が示すCGW MACアドレス 176 と EGW MACアドレス 175 を含むカプセル化ヘッダ 74 を適用して、PADRパケットをカプセル化し（123、図13のSQ1 - 17）、レイヤ2トンネリングパケットに変換する。  
30

#### 【0089】

EGW10 - 1 は、ユーザ管理テーブル 17 のエントリ 170 - 2 が示すL2 - VPN 側ポート番号 178 の値「5」をメモリ 25 のワークエリアに一時的に保持し（125）、上記レイヤ2トンネリングパケット（送信パケット）の種別を判定する（126）。今回のように、送信パケットがPADRパケットの場合、EGW10 - 1 は、送信パケットをポート番号「5」をもつ入出力回線インターフェースから広域イーサネット網（L2 - VPN）に送信して（128、図13のSQ1 - 18）、このルーチンを終了する。  
40

#### 【0090】

上記カプセル化されたPADRパケット（レイヤ2トンネリングパケット）は、L2SW30 - 1 を介してCGW20 - 1 に転送される。

CGW20 - 1 は、上記PADRパケットを含むレイヤ2トンネリングパケットを受信すると、図19に示す上りパケット処理ルーチン 210 を実行して、受信パケットのトンネリングタイプを判定する（211）。今回は、トンネリングタイプが「Ethernet over Ethernet」となっているため、CGW20 - 1 は、受信したレイヤ2トンネリングパケットからカプセル化ヘッダ 74 を除去し（デカプセル化：212、図13のSQ1 - 19）、受信パケットを図16のフォーマットF3 - 3 に変換した後、パケット種別を判定する（214）。  
50

## 【0091】

受信パケットが P A D R パケットの場合、 C G W 2 0 - 1 は、ユーザ管理テーブル 2 7 - 1 に、ユーザ M A C アドレス 2 7 1 が受信パケットの送信元 M A C アドレス 7 1 2 (「00.99.c0.61.72.00」) に該当するテーブルエントリが登録済みか否かを判定する (2 2 1)。目的のテーブルエントリがユーザ管理テーブル 2 7 - 1 になければ、 C G W 2 0 - 1 は、受信パケットを廃棄して (2 2 5)、このルーチンを終了する。

## 【0092】

今回の例では、ユーザ管理テーブル 2 7 - 1 から、受信パケット (P A D R) の送信元 M A C アドレス 「00.99.c0.61.72.00」 と対応するテーブルエントリ 2 7 0 - 2 が検索される。そこで、 C G W 2 0 - 1 は、送信すべきパケットの種別を判定する (2 2 2)。今回のように、 P A D R パケットの場合、 C G W 2 0 - 1 は、上記送信パケットを I S P 側ポート番号 「5」 をもつ回線インタフェース 2 1 - 5 から I S P 網に送信して (2 2 4、図 1 3 の S Q 1 - 2 0)、このルーチンを終了する。尚、送信パケットが P A D T パケットの場合、 C G W 2 0 - 1 は、ユーザ管理テーブル 2 7 - 1 から上記検索エントリを削除 (2 2 3) した後、ステップ 2 2 4 を実行する。

## 【0093】

上記 P A D R パケットは、その送信先 M A C アドレスで指定されている B A S 4 0 - 1 によって受信される。B A S 4 0 - 1 は、 P A D R パケットを受信すると、その送信元であるユーザ端末 H 1 宛に、 P A D R パケットに対する応答パケットである P A D S パケットを返信する (図 1 3 の S Q 1 - 2 1)。P A D S パケットは、前述した P A D O と同様、図 1 5 に F 2 - 1 で示したフォーマットとなっている。

## 【0094】

C G W 2 0 - 1 は、上記 P A D S パケットを受信すると、図 2 0 に示した下りパケット処理ルーチン 2 3 0 を実行し、ユーザ管理テーブル 2 7 - 1 から、ユーザ M A C アドレス 2 7 1 が受信パケットの送信先 M A C アドレスに該当するテーブルエントリを検索する (2 3 1)。

今回の例では、ユーザ管理テーブル 2 7 - 1 から、受信パケット (P A D S) の送信先 M A C アドレス 「00.99.c0.61.72.00」 と対応するテーブルエントリ 2 7 0 - 2 が検索される。そこで、 C G W 2 0 - 1 は、検索されたテーブルエントリ 2 7 0 - 2 のレイヤ 2 トунネリングタイプ 2 7 3 を判定し (2 3 4)、トунネリングタイプが 「Ethernet over Ethernet」 となっているため、上記テーブルエントリが示す C G W M A C アドレス 2 7 5 と E G W M A C アドレス 2 7 6 をカプセル化ヘッダ 7 4 に適用して、受信パケットをカプセル化する (2 3 5、図 1 3 の S Q 1 - 2 2)。

## 【0095】

上記カプセル化によって、受信パケット (P A D S) は、図 1 5 にフォーマット F 2 - 2 で示すように、 S - M a c D A 7 4 1 として E G W 1 1 0 - 1 の M A C アドレス 「00.99.c0.36.11.00」、 S - M a c S A 7 4 2 として C G W 2 0 - 1 の M A C アドレス 「00.99.c0.44.21.00」 をもつレイヤ 2 トунネリングパケット (送信パケット) に変換される。

## 【0096】

C G W 2 0 - 1 は、送信パケットが P P P 通信の終了要求を示す P A D T パケットか否かを判定する (2 3 7)。今回のように、送信パケットが P A D S パケットの場合は、 C G W 2 0 - 1 は、ユーザ管理テーブル 2 7 - 1 のテーブルエントリ 2 7 0 - 2 が示す L 2 - V P N 側ポート番号 2 7 8 と対応する回線インタフェースから、上記送信パケットを送信して (2 3 9、図 1 3 の S Q 1 - 1 2)、このルーチンを終了する。これによって、 P A D S パケットは、 P A D R パケットとは逆のルートで、 L 2 S W 3 0 - 1 に転送され、 L 2 S W 3 0 - 1 によって、 E G W 1 0 - 1 に転送される。

## 【0097】

E G W 1 0 - 1 は、上記 P A D O パケットを受信すると、図 1 8 に示す下りパケット処理ルーチン 1 3 0 を実行し、受信パケットのトунネリングタイプを判定する (1 3 1)。今回は、トунネリングタイプが 「Ethernet over Ethernet」 となっているため、 E G W 1

0 - 1 は、受信パケットからカプセル化ヘッダ 7 4 を除去する (132、図13のSQ1 - 24)。これによって、図15に示すように、フォーマットF2 - 2 の受信パケットが、フォーマットF2 - 3 のパケットに変換される。

#### 【0098】

E GW10 - 1 は、ユーザ管理テーブル17から、ユーザMACアドレス171が、デカプセル化された受信パケットの送信先MACアドレス711に該当するテーブルエントリを検索する (134)。今回は、受信パケットの送信先MACアドレス「00.99.c0.61.72.00」と対応するテーブルエントリ170 - 2 がユーザ管理テーブル17から検索される。この場合、E GW10 - 1 は、テーブルエントリ170 - 2 が示すユーザ側ポート番号177の値「1」をワークメモリに記憶 (136) した後、受信パケットの種別を判定する (137)。受信パケットがPADTパケットでないため、E GW10 - 1 は、受信パケットをユーザ側ポート番号「1」をもつ回線インターフェース11 - 1 から送出して (139)、このルーチンを終了する。これによって、BAS40 - 1 から返送されたPADSパケットが、PADRパケットの送信元ユーザ端末H1に転送される (図13のSQ1 - 25)。  
10

#### 【0099】

E GW10 - 1 は、ユーザ側 (またはL2 - VPN側) からユーザパケットを受信すると、上述したパケット処理ルーチン110 (または130) に従って、受信パケットをカプセル化 (またはデカプセル化) し、L2 - VPN網 (またはアクセス網) に転送する。同様に、CGW2 - 0 - 1 も、L2 - VPN側 (またはISP側) からユーザパケットを受信した場合、上述したパケット処理ルーチン210 (または230) に従って、受信パケットをデカプセル化 (またはカプセル化) し、ISP網 (またはL2 - VPN網) に転送する。  
20

#### 【0100】

E GW10 - 1 (またはCGW20 - 1) は、ユーザ側またはISP側からPPP通信の終了要求パケットであるPADTパケットを受信した場合、受信したPADTパケットを対向装置であるCGW20 - 1 (またはE GW10 - 1) に転送すると共に、自装置のユーザ管理テーブル17 (または27 - 1) から、PADTパケットの送信元MACアドレスまたは送信先MACアドレスと対応するテーブルエントリを削除する (127、138、223、238)。  
30

#### 【実施例2】

#### 【0101】

次に、本発明の第2実施例として、EGWとCGWとの間で、S-VLAN IDを使用した拡張VLAN型のレイヤ2トンネリングを行う場合について説明する。

前提となるシステム構成と各種のテーブルは、第1実施例と同様である。

#### 【0102】

図21は、図1に示した通信ネットワークにおいて、ユーザ端末H3がVoIP網NW4への接続要求パケットPADIを発行した場合の通信シーケンスを示す。また、図22は、第2実施例におけるPADIパケットのフォーマットの変換過程、図23は、PADOパケットのフォーマット変換過程、図24は、PADRパケットのフォーマット変換過程を示している。  
40

#### 【0103】

ユーザH3が、VoIP網への接続を要求する場合、図22にフォーマットF4 - 1で示すように、VLAN\_ID714としてID値「1」を含み、TAG\_VALUE7313に、サービス名、ドメイン名、パスワードを示す「voip@isp4;pass4」を含むPADIパケットをブロードキャストする (図21のSQ2 - 1)。

E GW10 - 1 は、上記PADIパケットを受信すると、図17に示す上りパケット処理ルーチン110を実行し、受信したPPPoEパケットの種別を判定する (111)。受信パケットがPADIパケットであるため、E GW10 - 1 は、ユーザ管理テーブル17に新たなテーブルエントリを追加登録する (112)。  
50

**【0104】**

上記テーブルエントリは、図5Dにエントリ170-3で示すように、ユーザMACアドレス171として、受信したPADIパケットが示す送信元MACアドレス「00.99.c0.55.34.00」、ユーザ側ポート番号177として、上記PADIパケットを受信した回線インターフェース11-iのポート番号（この例では、「3」）を含み、VLAN ID172に、受信パケットが指定したID値「1」を含む。

**【0105】**

EGW10-1は、この後、受信パケットからTAG VALUE7313：「voip@isp4;pass4」を抽出し（112）、TAG VALUEから抽出したドメイン名「isp4」とパスワード「pass4」とを含むユーザ認証要求メッセージ（Access-Request）をRadiusサーバ31に送信し（114、図21のSQ2-2）、Radiusサーバ31からの応答を待つ（115）。

**【0106】**

Radius31は、第1実施例と同様のユーザ認証を行う。今回は、ユーザ管理テーブル37から検索されたドメイン名「isp4」をもつテーブルエントリ370-2が、レイヤ2トンネリングタイプ373で「拡張VLAN」、S-VLAN ID374でID値「2」を指定している。パスワードが正常であった場合、Radius31は、EGW10-1に返送するアクセス許可メッセージ（Access-Accept）（図21のSQ2-3）で、レイヤ2トンネリングタイプが「拡張VLAN」であり、S-VLAN IDの値が「2」であることを示す。

**【0107】**

EGW10-1は、Radiusサーバ31から応答パケット（Access-Accept）を受信すると、認証結果を判定する（116）。応答パケットがAccess-Acceptの場合、EGW10-1は、受信したAccess-Acceptが示すレイヤ2トンネリングタイプ：「拡張VLAN」と、S-VLAN ID」の値「2」をユーザ管理テーブルのテーブルエントリ170-3に登録する（118）。レイヤ2トンネリングタイプが拡張VLANの場合、Access-Acceptでは、EGW MACアドレスとCGW MACアドレスが指定されないため、テーブルエントリ170-3のEGW MACアドレス175とCGW MACアドレス176にはコード「-」が設定される。この時点で、テーブルエントリ170-3は、図5Eに示した状態となる。

**【0108】**

次に、EGW10-1は、PADIパケットのTAG VALUE7313からドメイン名「isp4」を抽出し、ポート管理テーブル18から、上記ドメイン名「isp4」と対応するL2-VPN側ポート番号182に値「6」を検索し（119）、検索されたポート番号「6」をユーザ管理テーブル17にL2-VPN側ポート番号178として登録する（120）。これによって、テーブルエントリ170-3は、図5Fに示した状態となる。

**【0109】**

この後、EGW10-1は、テーブルエントリ170-3のレイヤ2トンネリングタイプ173を判定する（122）。今回は、トンネリングタイプが拡張VLANとなっているため、EGW10-1は、図22にフォーマットF4-2で示すように、S-VLAN ID715を含むカプセル化ヘッダ（Ethernetヘッダ）74で受信パケットをカプセル化し、レイヤ2トンネリングパケットに変換する（124）。

**【0110】**

EGW10-1は、ユーザ管理テーブル17のエントリ170-3が示すL2-VPN側ポート番号178の値「6」をメモリ25のワークエリアに一時的に保持し（125）、上記レイヤ2トンネリングパケット（送信パケット）の種別を判定する（126）。今回のように、レイヤ2トンネリングパケットがPADIパケットの場合、EGW10-1は、送信パケットをポート番号「6」をもつ入出力回線インターフェースから広域イーサネット網（L2-VPN）に送信して（128、図21のSQ2-5）、このルーチンを終了する。

10

20

30

40

50

**【0111】**

上記 PADI パケットは、L2SW30-2 によって、CGW20-2 に転送される。CGW20-2 は、上記レイヤ2トンネリングパケットを受信すると、図19に示す上りパケット処理ルーチン210を実行し、受信パケットのトンネリングタイプを判定する(211)。

**【0112】**

今回は、受信パケットのトンネリングタイプが拡張VLANであるため、CGW20-2 は、受信パケットのヘッダからS-VLAN ID715を除去し(213、図21のSQ2-7)、上記S-VLAN ID715の値「2」を記憶した状態で、受信パケットの種別を判定する(214)。今回は、受信パケットがPADI パケットであるため、CGW20-2 は、ユーザ管理テーブル27-2に、受信したPADI パケットの送信元MACアドレスをユーザMACアドレス271とする新たなテーブルエントリを追加する(215)。

10

**【0113】**

図9(A)の270-22は、この時点でのユーザ管理テーブル27-2に追加されたテーブルエントリの内容を示している。ユーザMACアドレス271には、PADI パケットの送信元MACアドレスが示すユーザ端末H3のMACアドレス「00.99.c0.55.34.00」、VLAN ID272には、受信パケットが示すVLAN ID714の値「1」、レイヤ2トンネリングタイプ273には、拡張VLANを示すコードが設定される。また、S-VLAN ID274には、受信パケットが示していたS-VLAN ID715の値「2」が設定され、L2-VPN側ポート番号277には、上記レイヤ2トンネリングパケットを受信した回線インタフェースのポート番号、この例では「3」が設定される。今回は、レイヤ2トンネリングパケットでCGW MACアドレスとEGW MACアドレスが指定されていないため、CGW MACアドレス275とEGW MACアドレス276にはコード「-」が設定される。

20

**【0114】**

CGW20-2 は、次に、図11に示したポート管理テーブル28-2から、PADI パケットのTAG VALUEが示すドメイン名「isp4」と対応するISP側ポート番号282とサービス名編集フラグ283を検索し(216)、検索されたISP側ポート番号の値(この例では「8」)をユーザ管理テーブルのテーブルエントリ270-22にISP側ポート番号278として登録する(217)。この結果、テーブルエントリ270-22は、図9(B)に示した状態となる。

30

**【0115】**

CGW20-1 は、検索されたサービス名編集フラグ283の値から、サービス名編集の要否を判定する(218)。ポート管理テーブル28-2では、メイン名「isp4」と対応するテーブルエントリ280-22で、サービス名編集フラグ283が「1」に設定されているため、CGW20-2 は、PADI パケットのTAG VALUEが示す「voip@isp4;pass4」を解析して、TAG VALUEからドメイン名「isp4」とパスワード情報「pass4」を除外して、図14にフォーマットF4-3で示すように、受信パケット(PADI パケット)をTAG VALUEとしてサービス名「voip」を含む送信パケットに変換する(219、図21のSQ2-8)。

40

**【0116】**

この後、CGW20-2 は、ユーザ管理テーブル27-2から、上記送信パケットの送信元MACアドレスと対応するISP側ポート番号278の値「8」を検索し(220)、送信パケットをISP側ポート番号「8」をもつ回線インタフェース21-8からISP網に送信して(224、図21のSQ2-9)、このルーチンを終了する。

**【0117】**

上記PADI パケットは、BAS40-4 によって受信される。BAS40-4 は、受信したPADI パケットに応答してPADO パケットを送信する(図21のSQ2-10)。上記PADO パケットは、図23にフォーマットF5-1で示すように、送信先MA

50

Cアドレス711として、PADIパケットの送信元であるユーザ端末H3のMACアドレス「00.99.c0.55.34.00」、送信元MACアドレス712として、BAS40-4のMACアドレス「00.99.c0.26.24.00」を含み、VLAN ID714として、PADIパケットと同じID値「1」を含んでいる。

#### 【0118】

CGW20-2は、上記PAD0パケットを受信すると、図20に示す下りパケット処理ルーチン230を実行し、ユーザ管理テーブル27-2から、ユーザMACアドレス271が受信パケットの送信先MACアドレスに該当するテーブルエントリを検索する(231)。今回の例では、ユーザ管理テーブル27-2から、ユーザMACアドレス271が「00.99.c0.55.34.00」のテーブルエントリ270-22が検索される。そこで、CGW20-2は、検索されたテーブルエントリ270-22のレイヤ2トンネリングタイプ273を判定する(234)。この場合、トンネリングタイプは、拡張VLANとなっているため、CGW20-2は、テーブルエントリ270-22のS-VLAN ID274の値「2」を適用して、PAD0パケットをカプセル化する(236、図21のQ2-11)。ここでカプセル化は、図23にフォーマットF5-2で示すように、PAD0パケットをEthernetヘッダにS-VLAN ID717を追加した形のレイヤ2トンネリングパケット(送信パケット)に変換することを意味している。

#### 【0119】

CGW20-2は、上記送信パケットの種別を判定し(237)、送信パケットがPADTパケットでなければ、ユーザ管理テーブル27-2から検索されたテーブルエントリ270-22が示すL2-VPN側ポート番号278(「3」と対応する回線インターフェースから、上記送信パケットを送信して(239、図21のSQ2-12)、このルーチンを終了する。これによって、PAD0パケットは、PADIパケットとは逆ルートで、L2SW30-2に転送される。

#### 【0120】

L2SW30-2は、CGW20-2からレイヤ2トンネリングパケットを受信すると、S-VLAN IDに従って、受信パケットをEGW10-1に転送する(図21のSQ2-13)。

#### 【0121】

EGW10-1は、上記レイヤ2トンネリングパケットを受信すると、図18に示す下りパケット処理ルーチン130を実行し、受信パケットのトンネリングタイプを判定する(131)。今回は、トンネリングタイプが拡張VLANとなっているため、EGW10-1は、受信パケットからS-VLAN ID715を除去(デカプセル化)する(133、図21のSQ2-14)。上記デカプセル化によって、レイヤ2トンネリングパケットは、図23にフォーマットF5-3で示すPPP0Eパケットに変換される。

#### 【0122】

EGW20-1は、この後、ユーザ管理テーブル17から、ユーザMACアドレス171が、上記送信パケットの送信先MACアドレス711に該当するテーブルエントリを検索し(134)、検索結果を判定する(135)。今回は、ユーザ管理テーブル17から、テーブルエントリ170-3が検索されるため、EGW10-1は、ユーザ側ポート番号177が示すポート番号「3」をワークメモリに記憶(136)した後、送信パケットの種別を判定する(137)。送信パケットがPADTパケットでなければ、EGW10-1は、送信パケットをポート番号「3」をもつ回線インターフェースから送出して(139、図21のSQ2-15)、このルーチンを終了する。これによって、PAD0パケットは、PADIパケットの送信元ユーザ端末H3に転送されることになる。

#### 【0123】

ユーザ端末H3は、PAD0パケットを受信すると、PPPセッションの開始要求パケットであるPADRパケットを送信する(図21のSQ2-16)。上記PADRパケットは、図24にフォーマットF6-1で示すように、Ethernetヘッダの宛先MACアドレス711がBAS40-4のMACとなっており、VLAN ID714にPADIパケ

10

20

30

40

50

ットと同一の値「1」を含んできる。

#### 【0124】

E GW10-1は、上記PADRパケットを受信すると、図17に示す上りパケット処理ルーチン110を実行し、受信パケットの種別を判定する(111)。今回は、受信パケットがPADTパケットでないため、E GW10-1は、ユーザ管理テーブル17に、ユーザMACアドレス171が受信パケットの送信元MACアドレス712に該当するテーブルエントリが登録済みか否かを判定する(121)。

#### 【0125】

受信パケットの送信元MACアドレス「00.99.c0.55.34.00」と対応するテーブルエントリ170-3がユーザ管理テーブル17に既に登録済みとなっているため、E GW10-1は、上記テーブルエントリ170-3のレイヤ2トンネリングタイプ173を判定する(122)。今回は、レイヤ2トンネリングタイプが拡張VLANとなっているため、E GW10-1は、上記テーブルエントリ170-3のS-VLAN ID174が示すID値「2」を適用して、受信パケットをカプセル化し(124、図21のSQ2-17)、レイヤ2トンネリングパケット(送信パケット)に変換する。ここでカプセル化は、図24にフォーマットF6-2で示すように、EthernetヘッダにS-VLAN ID715を追加することを意味している。

#### 【0126】

E GW10-1は、この後、ユーザ管理テーブル17のエントリ170-3が示すL2-VPN側ポート番号178の値「6」をメモリ25のワークエリアに一時的に保持し(125)、上記レイヤ2トンネリングパケットの種別を判定する(126)。今回のように、レイヤ2トンネリングパケット(送信パケット)がPADRパケットの場合、E GW10-1は、送信パケットをポート番号「6」をもつ回線インタフェースから広域イーサネット網(L2-VPN)に送信して(128、図21のSQ21-18)、このルーチンを終了する。上記レイヤ2トンネリングパケット(PADR)は、L2SW30-2を介してCGW20-2に転送される。

#### 【0127】

CGW20-2は、上記レイヤ2トンネリングパケットを受信すると、図19に示す上りパケット処理ルーチン210を実行し、受信パケットのトンネリングタイプを判定する(211)。今回は、受信パケットのトンネリングタイプが拡張VLANとなっているため、CGW20-2は、受信パケットからS-VLAN ID715を除去(デカプセル化)し(213)、受信パケットを図23のフォーマットF6-3をもつ送信パケット(PPPoeパケット)に変換した後、パケットの種別を判定する(214)。

#### 【0128】

送信パケットがPADRパケットの場合、CGW20-2は、ユーザ管理テーブル27-2から、ユーザMACアドレス271が受信パケットの送信元MACアドレス712に該当するテーブルエントリを検索する(221)。検索の結果、送信元MACアドレス「00.99.c0.55.34.00」に該当するテーブルエントリ270-22が見つかると、CGW20-2は、送信パケットがPADTパケットか否かを判定する(223)。今回は、送信パケットがPADRパケットであるため、CGW20-2は、テーブルエントリ270-22のISP側ポート番号278が示すポート番号「8」をもつ回線インタフェースから送信パケットを送出して(224、図21のSQ2-21)、このルーチンを終了する。

#### 【0129】

上記パケット(PADR)は、BAS40-4で受信される。BAS40-4は、PADRパケットを受信すると、PADRパケットに対する応答パケットとしてPADSパケットを返送する(図21のSQ2-21)。PADSパケットは図23にフォーマットF5-1で示すように、送信先MACアドレス711が、ユーザ端末H3のMACアドレス「00.99.c0.55.34.00」となっている。

#### 【0130】

CGW20-2は、BAS40-4からPADSパケットを受信すると、図20に示す下

10

20

30

40

50

リパケット処理ルーチン 230 を実行し、ユーザ管理テーブル 27-2 から、ユーザ MAC アドレス 271 が受信パケットの送信先 MAC アドレス 712 と一致するテーブルエントリを検索する(231)。今回は、送信先 MAC アドレス「00.99.c0.55.34.00」に該当するテーブルエントリ 270-22 が検索されるため、CGW20-2 は、PAD0 パケットの受信時と同様、テーブルエントリ 270-22 のレイヤ2トンネリングタイプ 273 を判定し(234)、テーブルエントリ 270-22 のS-VLAN ID 274 の値「2」を適用して、PADS パケットをカプセル化し(236、図21のQ2-22)、図23 にフォーマット F5-2 で示すレイヤ2トンネリングパケットに変換する。

#### 【0131】

CGW20-2 は、上記レイヤ2トンネリングパケットをテーブルエントリ 270-2 2 が示す L2-VPN 側ポート番号 278(「3」) と対応する回線インターフェースから送信して(239)、このルーチンを終了する。これによって、PADS パケットは、PADR パケットとは逆ルートで、L2SW30-2 に転送され、L2SW30-2 によって EGW10-1 に転送される(図21のSQ2-23)。

#### 【0132】

EGW10-1 は、上記 PADS を受信すると、図18 に示す下りパケット処理ルーチン 130 を実行する。PAD0 パケットの受信時と同様、EGW10-1 は、受信パケットのトンネリングタイプを判定し(131)、受信パケットから S-VLAN ID 715 を除去(デカプセル化)し(133、図21のSQ2-24)、ユーザ管理テーブル 17 からテーブルエントリ 170-3 を検索し(134)、図23 のフォーマット F5-3 をもつ送信パケットをポート番号「3」をもつ回線インターフェースから送出して(139、図21のSQ2-25)、このルーチンを終了する。これによって、PADS パケットは、PADR パケットの送信元ユーザ端末 H3 に転送されることになる。

#### 【0133】

EGW10-1(CGW20-2) は、ユーザ側または ISP 側から PPP 通信の終了要求パケットである PADT パケットを受信した場合、受信した PADT パケットを対向装置である CGW20-2(EGW10-1) に転送すると共に、自装置のユーザ管理テーブル 17(27-2) から、PADT パケットの送信元 MAC アドレスまたは送信先 MAC アドレスと対応するテーブルエントリを削除する。

#### 【0134】

上述した実施例では、EGW と CGW が、PPPoE プロトコルにおける接続要求パケットである PADI パケットの受信時に、ユーザ管理テーブルに新たなテーブルエントリを追加することによって、EGW と CGW の間に L2-VPN を設定しているが、ネットワークに、例えば、IEEE802.1X を適用した場合、EAP-Response / ID 通知パケットの受信時に、ユーザ管理テーブルに新たなテーブルエントリを追加することによって、EGW と CGW の間に L2-VPN を設定することが可能となる。

#### 【0135】

また、以上の実施例では、L2-VPN におけるレイヤ2トンネリングのタイプが、Ethernet over Ethernet と拡張 VLAN の場合について説明したが、本発明は、例えば、L2TPv3 や Ethernet over IP など、他のレイヤ2トンネリングタイプにも適用可能である。

#### 【図面の簡単な説明】

#### 【0136】

【図1】本発明が適用される通信ネットワークの構成例を示す図。

【図2】(A) は PPPoE パケットのフォーマット、(B) は T A G 731 の詳細を示す図。

【図3】図1の通信ネットワークにおけるユーザ端末の接続先 B A S の選択動作を説明するための図。

【図4】図1に示した EGW10(10-1, 10-2) の 1 実施例を示す構成図。

【図5A】EGW10-1 が備えるユーザ管理テーブルの構成を示す図。

10

20

30

40

50

【図 5 B】E GW10 - 1が備えるユーザ管理テーブルの内容変化を示す図。

【図 5 C】E GW10 - 1が備えるユーザ管理テーブルの内容変化を示す図。

【図 5 D】E GW10 - 1が備えるユーザ管理テーブルの内容変化を示す図。

【図 5 E】E GW10 - 1が備えるユーザ管理テーブルの内容変化を示す図。

【図 5 F】E GW10 - 1が備えるユーザ管理テーブルの内容変化を示す図。

【図 6】E GW10 - 1が備えるポート管理テーブルの構成を示す図。

【図 7】図1に示したCGW20(20 - 1 ~ 20 - 3)の1実施例を示す構成図。

【図 8】CGW20 - 1が備えるユーザ管理テーブル27 - 1の構成と内容変化を説明するための図。

【図 9】CGW20 - 1が備えるユーザ管理テーブル27 - 1の構成と内容変化を説明するための図。 10

【0137】

【図 10】CGW20 - 1が備えるポート管理テーブル28 - 1の構成を示す図。

【図 11】CGW20 - 2が備えるポート管理テーブル28 - 2の構成を示す図。

【図 12】Radiusサーバ31が備えるユーザ管理テーブル37の構成を示す図。

【図 13】本発明の第1実施例を示す通信シーケンス図。

【図 14】第1実施例におけるPADIパケットのフォーマット変換過程を示す図。

【図 15】第1実施例におけるPADOパケットのフォーマット変換過程を示す図。

【図 16】第1実施例におけるPADRパケットのフォーマット変換過程を示す図。

【図 17】EGWが実行する上りパケット処理ルーチン110の1実施例を示すフローチャート。 20

【図 18】EGWが実行する下りパケット処理ルーチン130の1実施例を示すフローチャート。

【図 19】CGWが実行する上りパケット処理ルーチン210の1実施例を示すフローチャート。

【図 20】CGWが実行する下りパケット処理ルーチン230の1実施例を示すフローチャート。

【図 21】本発明の第2実施例を示す通信シーケンス図。

【図 22】第2実施例におけるPADIパケットのフォーマット変換過程を示す図。

【図 23】第2実施例におけるPADOパケットのフォーマット変換過程を示す図。 30

【図 24】第2実施例におけるPADRパケットのフォーマット変換過程を示す図。

【符号の説明】

【0138】

H1 ~ Hx、P1、P2 : ユーザ端末、10 : ユーザ側L2GW(EGW)、

20 : ISP側L2GW(CGW)、30、50 : L2SW、31 : Radiusサーバ

、40 : プロードバンドアクセスマシン(BAS)、NW1 : L2 - VPN、

NW2 : ISP網、NW3 : インターネット網、NW4 : VoIP網、

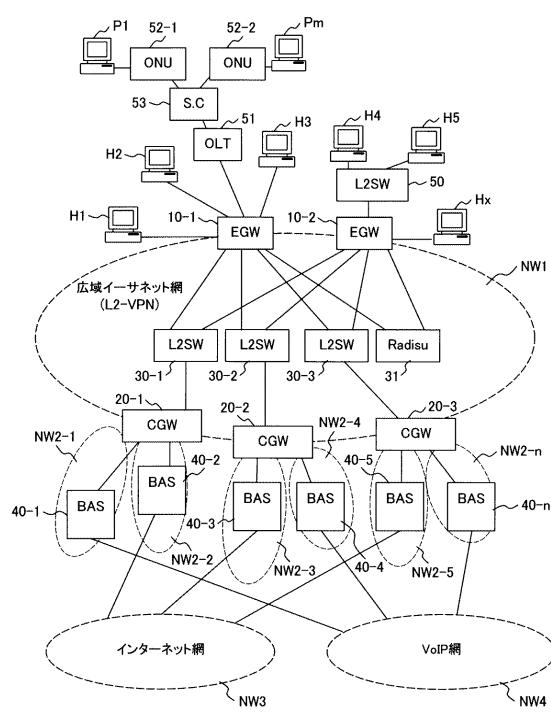
11、21 : 回線インターフェース、12、22 : ルーティング部、13、23 : 制御部、

17、27 : ユーザ管理テーブル、18、29 : ポート管理テーブル、

90、91 : 制御端末。 40

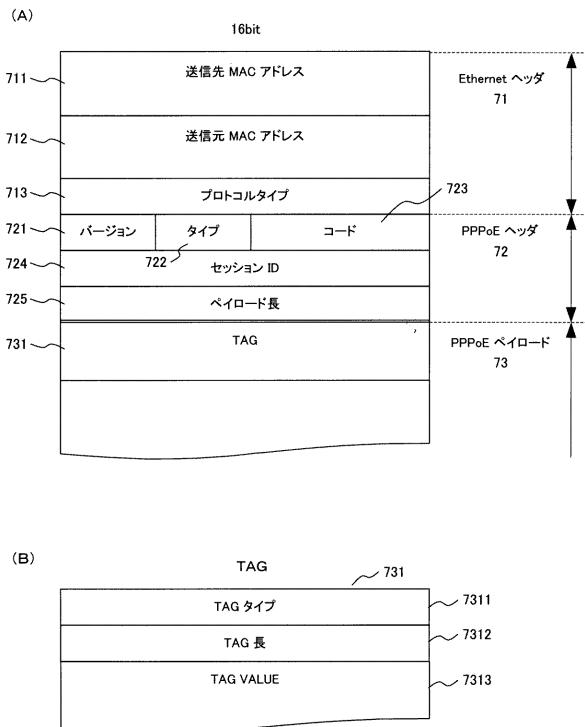
【図1】

図1



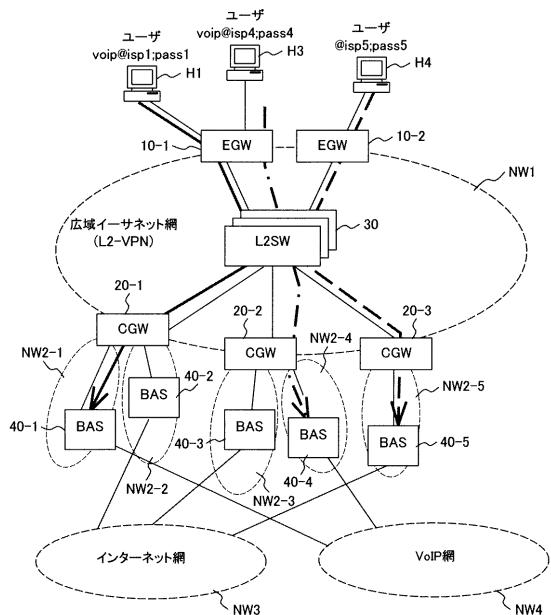
【図2】

図2



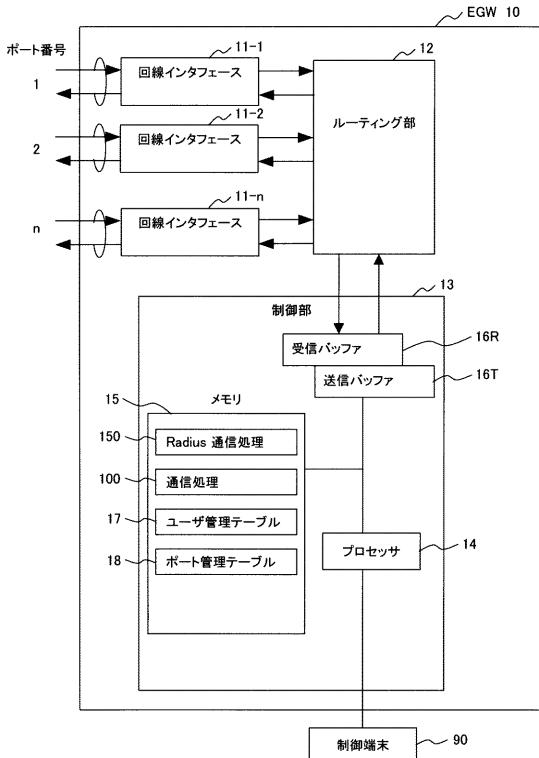
【図3】

図3



【図4】

図4



【図 5 A】

図 5 A

ユーザ管理テーブル 17								
ユーザ MAC アドレス	VLAN ID	レイヤ2 トンネリング タイプ	S-VLAN ID	EGW MAC アドレス	CGW MAC アドレス	ユーザ側 ポート番号	L2-VPN 側 ポート番号	
00.99.c0.58.66.00	—	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.33.84.00	4	8	～170-1
00.99.c0.61.72.00	—					1		～170-2
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図 5 B】

図 5 B

ユーザ MAC アドレス	VLAN ID	レイヤ2 トンネリング タイプ	S-VLAN ID	EGW MAC アドレス	CGW MAC アドレス	ユーザ側 ポート番号	L2-VPN 側 ポート番号	
00.99.c0.58.66.00	—	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.33.84.00	4	8	～170-1
00.99.c0.61.72.00	—	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.44.21.00	1		～170-2
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図 5 C】

図 5 C

ユーザ MAC アドレス	VLAN ID	レイヤ2 トンネリング タイプ	S-VLAN ID	EGW MAC アドレス	CGW MAC アドレス	ユーザ側 ポート番号	L2-VPN 側 ポート番号	
00.99.c0.58.66.00	—	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.33.84.00	4	8	～170-1
00.99.c0.61.72.00	—	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.44.21.00	1	5	～170-2
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図 5 D】

図 5 D

ユーザ MAC アドレス	VLAN ID	レイヤ2 トンネリング タイプ	S-VLAN ID	EGW MAC アドレス	CGW MAC アドレス	ユーザ側 ポート番号	L2-VPN 側 ポート番号	
00.99.c0.58.66.00	—	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.33.84.00	4	8	～170-1
00.99.c0.61.72.00	—	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.44.21.00	1	5	～170-2
00.99.c0.55.34.00	1	拡張 VLAN	2	—	—	3		～170-3

【図 5 E】

図 5 E

ユーザ MAC アドレス	VLAN ID	レイヤ2 トンネリング タイプ	S-VLAN ID	EGW MAC アドレス	CGW MAC アドレス	ユーザ側 ポート番号	L2-VPN 側 ポート番号	
00.99.c0.58.66.00	—	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.33.84.00	4	8	～170-1
00.99.c0.61.72.00	—	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.44.21.00	1	5	～170-2
00.99.c0.55.34.00	1	拡張 VLAN	2	—	—	3		～170-3
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図 5 F】

図 5 F

ユーザ MAC アドレス	VLAN ID	レイヤ2 トンネリング タイプ	S-VLAN ID	EGW MAC アドレス	CGW MAC アドレス	ユーザ側 ポート番号	L2-VPN 側 ポート番号	
00.99.c0.58.66.00	—	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.33.84.00	4	8	～170-1
00.99.c0.61.72.00	—	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.44.21.00	1	5	～170-2
00.99.c0.55.34.00	1	拡張 VLAN	2	—	—	3	6	～170-3
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図 6】

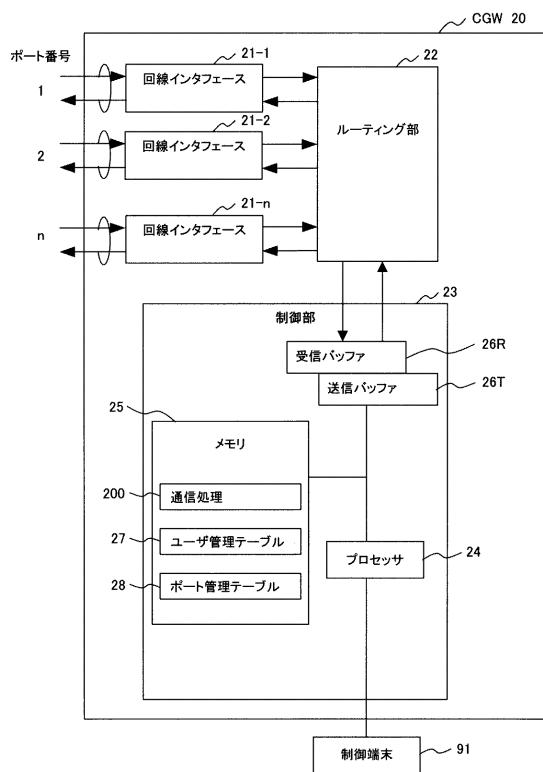
図 6

ポート管理テーブル 18

ドメイン	L2-VPN 側 ポート番号
ISP1	5
ISP4	6
ISP5	8
⋮	⋮

【図7】

図 7



【図8】

図 8

ユーザ管理テーブル 27-1

ユーザ MAC アドレス	VLAN ID	レイヤ2 トンネリング タイプ	S-VLAN ID	CGW MAC アドレス	EGW MAC アドレス	L2-VPN 側 ポート番号	ISP 側 ポート番号	271	272	273	274	275	276	277	278
00.99.c0.30.58.00	6	拡張 VLAN	8	—	—	4	10	270-11	270-11	270-11	270-11	270-11	270-11	270-11	270-11
00.99.c0.61.72.00	—	Ethernet Over Ethernet	—	00.99.c0.44.21.00	00.99.c0.36.11.00	2	—	270-12	270-12	270-12	270-12	270-12	270-12	270-12	270-12
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

ユーザ MAC アドレス	VLAN ID	レイヤ2 トンネリング タイプ	S-VLAN ID	CGW MAC アドレス	EGW MAC アドレス	L2-VPN 側 ポート番号	ISP 側 ポート番号	271	272	273	274	275	276	277	278
00.99.c0.30.58.00	6	拡張 VLAN	8	—	—	4	10	270-11	270-11	270-11	270-11	270-11	270-11	270-11	270-11
00.99.c0.61.72.00	—	Ethernet Over Ethernet	—	00.99.c0.44.21.00	00.99.c0.36.11.00	2	5	270-12	270-12	270-12	270-12	270-12	270-12	270-12	270-12
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図9】

図 9

ユーザ管理テーブル 27-2

ユーザ MAC アドレス	VLAN ID	レイヤ2 トンネリング タイプ	S-VLAN ID	CGW MAC アドレス	EGW MAC アドレス	L2-VPN 側 ポート番号	ISP 側 ポート番号	271	272	273	274	275	276	277	278
00.99.c0.29.80.00	—	Ethernet Over Ethernet	—	00.99.c0.81.63.00	00.99.c0.12.64.00	6	12	270-21	270-21	270-21	270-21	270-21	270-21	270-21	270-21
00.99.c0.55.34.00	1	拡張 VLAN	2	—	—	3	—	270-22	270-22	270-22	270-22	270-22	270-22	270-22	270-22
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図10】

図 10

ポート管理テーブル 28-1

ドメイン	ISP 側 ポート番号	サービス名編集 フラグ	281	282	283
ISP1	5	1	280-11	280-11	280-11
ISP4	8	1	280-12	280-12	280-12
ISP5	10	0	280-13	280-13	280-13
⋮	⋮	⋮	⋮	⋮	⋮

【図11】

図 11

ポート管理テーブル 28-2

ドメイン	ISP 側 ポート番号	サービス名編集 フラグ	281	282	283
ISP2	12	1	280-21	280-21	280-21
ISP4	8	1	280-22	280-22	280-22
ISP5	4	0	280-23	280-23	280-23
⋮	⋮	⋮	⋮	⋮	⋮

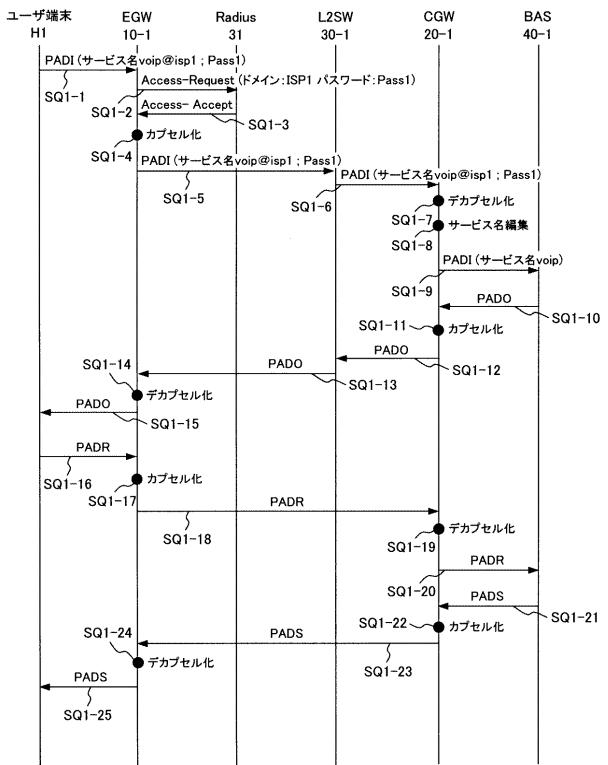
【図12】

図12

ユーザ管理テーブル 37					
ドメイン	パスワード	レイヤ2 トンネリング タイプ	S-VLAN ID	EGW MAC アドレス	CGW MAC アドレス
ISP1	Pass1	Ethernet Over Ethernet	—	00.99.c0.36.11.00	00.99.c0.44.21.00
ISP4	Pass4	拡張 VLAN	2	—	—
ISP5	Pass5	Ethernet Over Ethernet	—	00.99.c0.12.64.00	00.99.c0.33.84.00
⋮	⋮	⋮	⋮	⋮	⋮

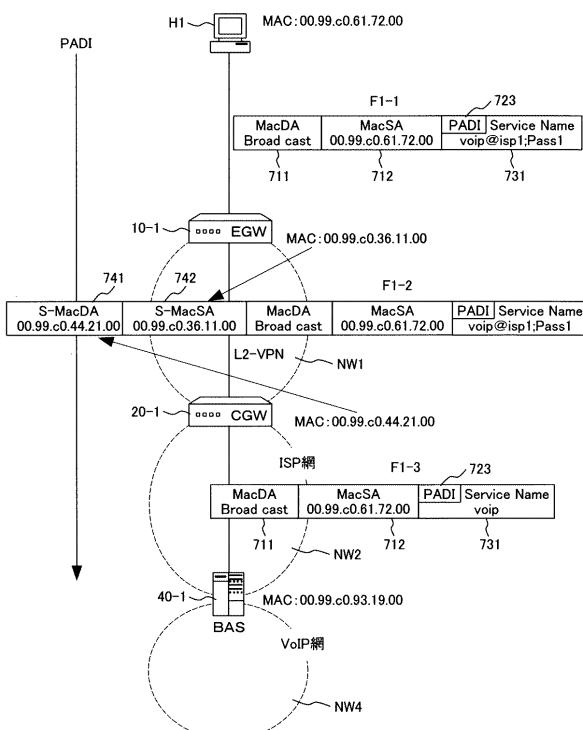
【図13】

図13



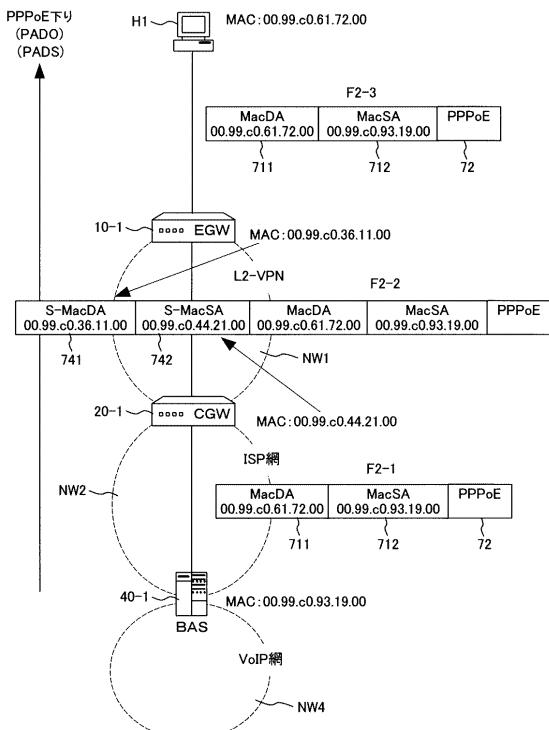
【図14】

図14



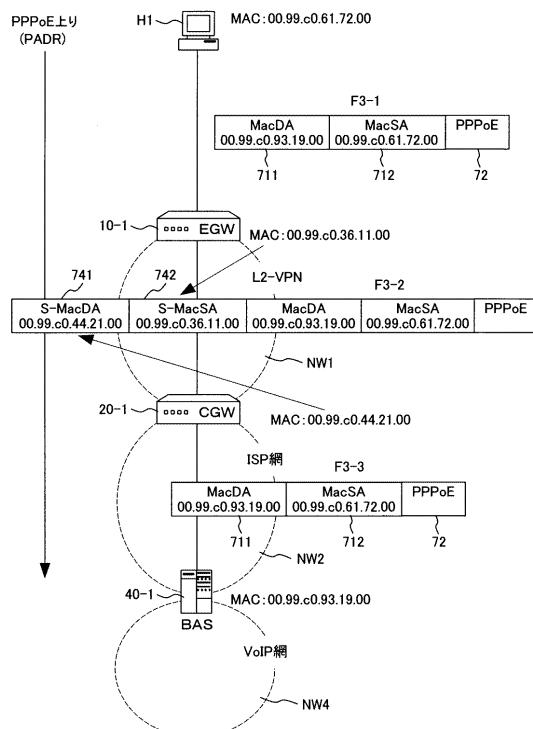
【図15】

図15



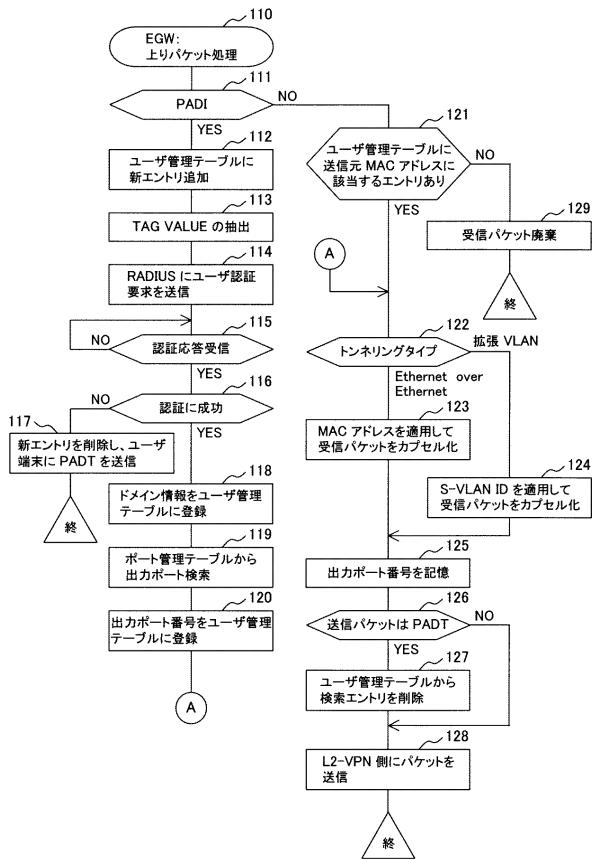
【図 16】

図 16



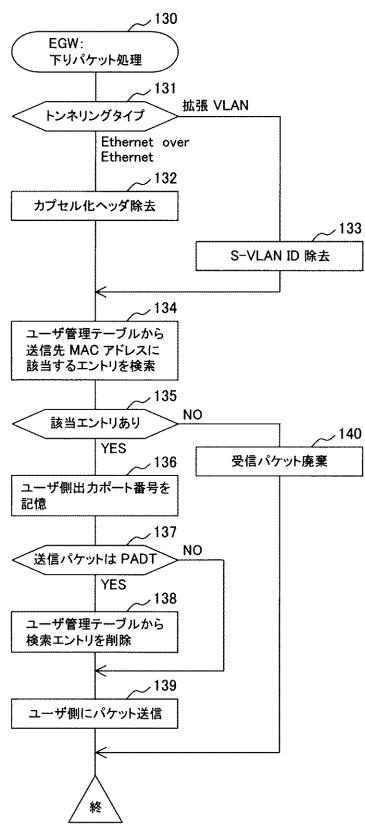
【図 17】

図 17



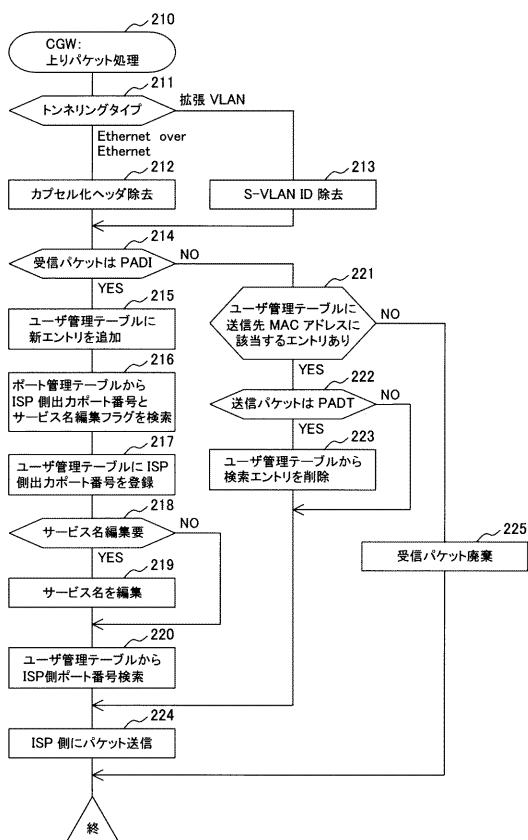
【図 18】

図 18



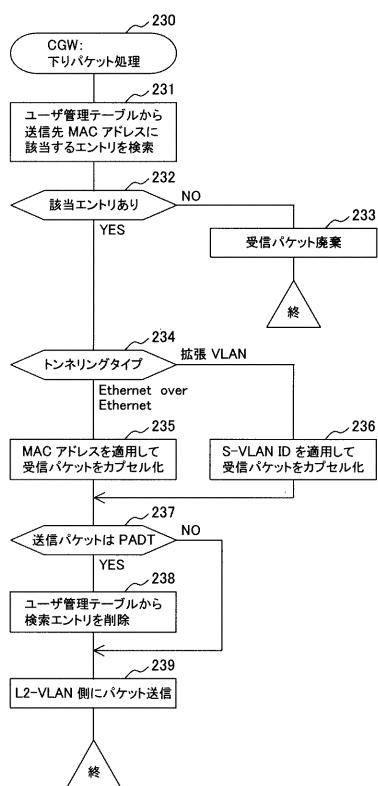
【図 19】

図 19



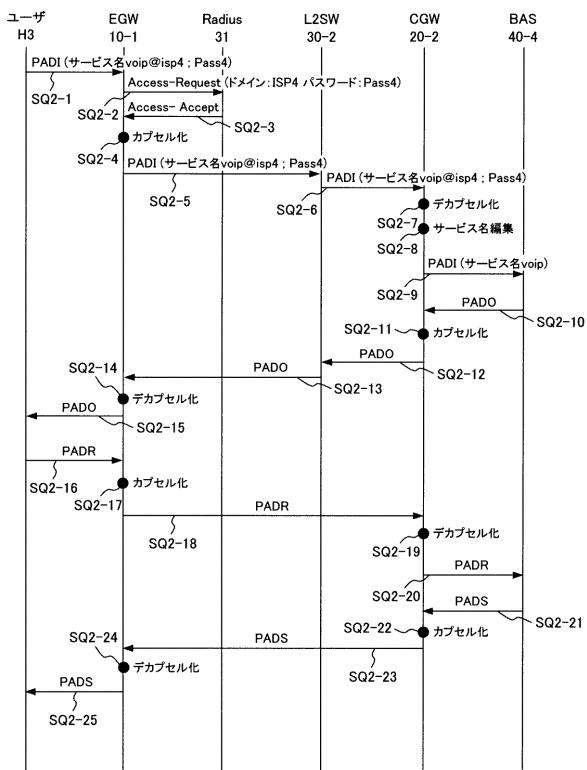
【図 20】

図 20



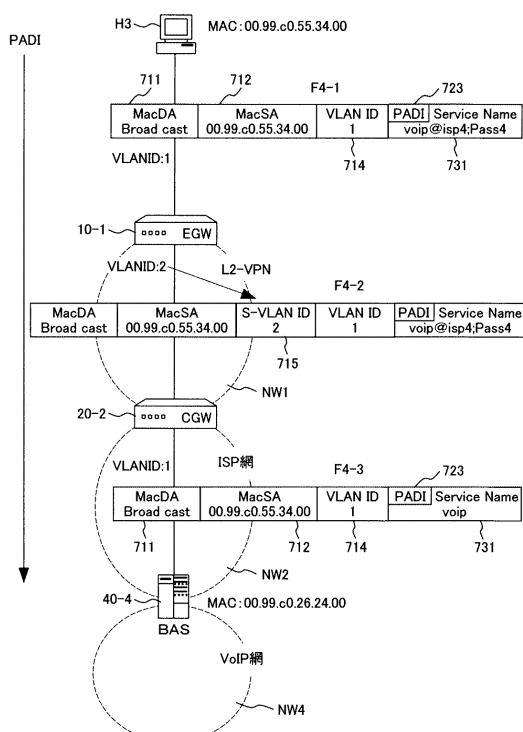
【図 21】

図 21



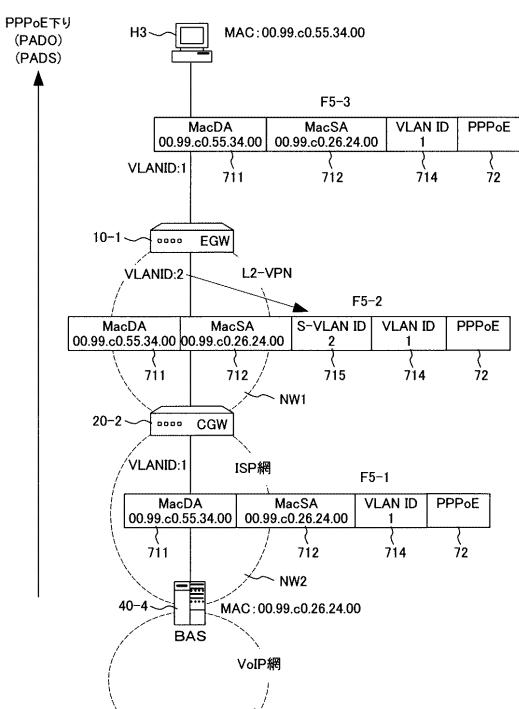
【図 22】

図 22



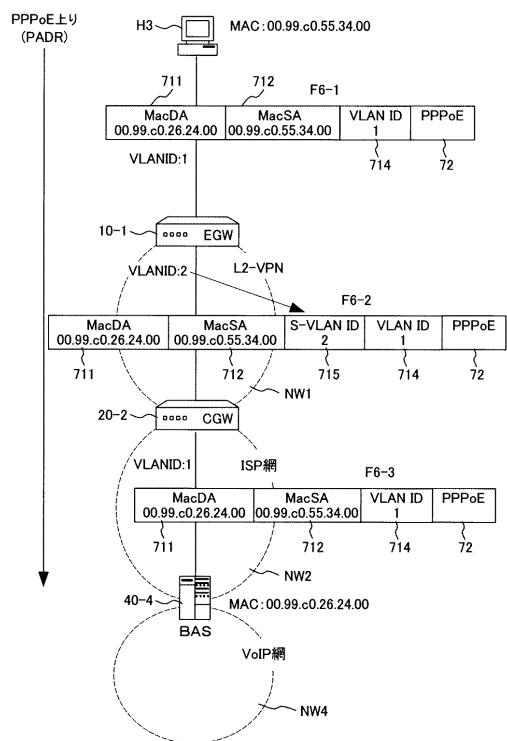
【図 23】

図 23



## 【図 2 4】

図 2 4



---

フロントページの続き

(72)発明者 高橋正

神奈川県横浜市戸塚区戸塚町216番地 株式会社日立コミュニケーションテクノロジー キャリ  
アネットワーク事業部内

審査官 保田亨介

(56)参考文献 特開2003-143236(JP,A)

特開2003-198580(JP,A)

特開2006-270273(JP,A)

特開2002-354015(JP,A)

特開2004-187282(JP,A)

(58)調査した分野(Int.Cl., DB名)

H04L 12/00-66