【公報種別】公表特許公報の訂正
【部門区分】第７部門第３区分
【発行日】平成17年8月4日(2005.8.4)

【公表番号】特表2005-513915(P2005-513915A)
【公表日】平成17年5月12日(2005.5.12)
【年通号数】公開・登録公報2005-018
【出願番号】特願2003-555749(P2003-555749)
【訂正要旨】【要約】中の半角スペースを誤って削除したため、下記のとおり全文を訂正する。
【国際特許分類第７版】
　Ｈ０４Ｌ　12/46
　Ｈ０４Ｌ　12/28
　Ｈ０４Ｌ　12/56
【ＦＩ】
　Ｈ０４Ｌ　12/46　　Ｖ
　Ｈ０４Ｌ　12/28　３００Ｚ
　Ｈ０４Ｌ　12/56　　Ｈ
【記】別紙のとおり

(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-513915
(P2005-513915A)
(43)公表日　平成17年5月12日(2005.5.12)

| (51)Int.Cl.[7] | F I | | テーマコード（参考） |
|---|---|---|---|
| H04L 12/46 | H04L 12/46 | V | 5K030 |
| H04L 12/28 | H04L 12/28 | 300Z | 5K033 |
| H04L 12/56 | H04L 12/56 | H | |

審査請求 有　予備審査請求 有　（全 19 頁）

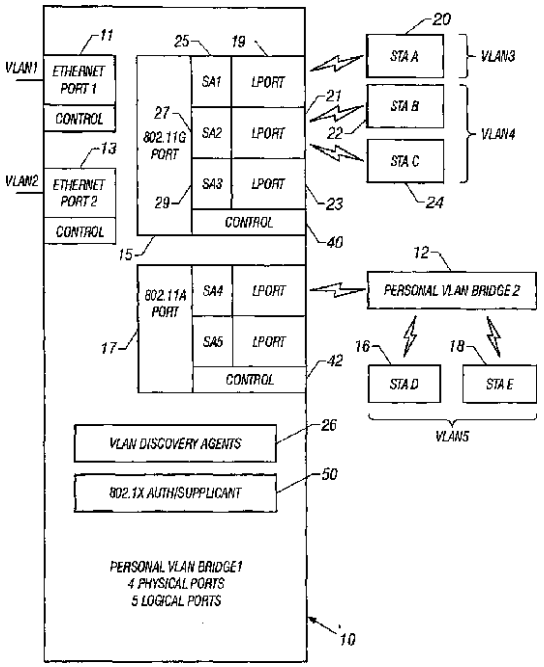
(21)出願番号　特願2003-555749 (P2003-555749)
(86)(22)出願日　平成14年2月1日 (2002.2.1)
(85)翻訳文提出日　平成16年6月16日 (2004.6.16)
(86)国際出願番号　PCT/US2002/002905
(87)国際公開番号　WO2003/055151
(87)国際公開日　平成15年7月3日 (2003.7.3)
(31)優先権主張番号　60/343,307
(32)優先日　平成13年12月20日 (2001.12.20)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　10/057,566
(32)優先日　平成14年1月25日 (2002.1.25)
(33)優先権主張国　米国 (US)

(71)出願人　504232022
クラナイト　システムズ　インク
ＣＲＡＮＩＴＥ　ＳＹＳＴＥＭＳ　ＩＮＣ．
アメリカ合衆国　９５１１９　カリフォルニア州　サンホセ　２番　フロアー　ヴィア　デル　オロ　６６２０
６６２０　Ｖｉａ　Ｄｅｌ　Ｏｒｏ，２ｎｄ　Ｆｌｏｏｒ，　Ｓａｎ　Ｊｏｓｅ，　ＣＡ　９５１１９　Ｕ．Ｓ．Ａ．
(74)代理人　100092048
弁理士　沢田　雅男

最終頁に続く

(54)【発明の名称】パーソナル仮想ブリッジ・ローカル・エリア・ネットワーク

(57)【要約】
【課題】当該ブリッジと関連している信頼できないSTAが同じブリッジと関連している別のSTA上でリンク層(OSI Layer 2)攻撃を開始するために使用されることが出来ないように、ブリッジと関連しているSTA間でトラフィックを分けるメカニズムを提供すること。
【解決手段】本明細書において、パーソナル仮想ブリッジ・ローカル・エリア・ネットワーク （パーソナルVLAN）と呼ばれる、ブリッジと関連しているSTA間でトラフィックを分けるメカニズムは、トラフィックを分けるためにVLANを使用することに基づく。IEEE 802.1Q-1998（仮想ブリッジ LAN）プロトコルは、LANセグメントを論理的に複数のVLANに分割する本発明によって拡張されるメカニズムを提供する。好ましい実施例において、VLANブリッジは、フレームが、属するVLANを供するそれらのポートのみに、ユニキャストおよびグループ・フレームを転送する。本発明の一実施例は、APの範囲内での使用に適しているメカニズムを提供するために標準VLANブリッジ・モデルを拡張する。好適な一実施例において、パーソナルVLANブリッジは、以下の方法の少なくとも何れ



【特許請求の範囲】
【請求項１】
アクセスポイントと関連している複数のステーション間でトラフィックを分ける装置であって、
LANセグメント、および、
当該LANセグメントを複数の仮想ブリッジ・ローカル・エリア・ネットワーク(VLAN)に論理的に分割するパーソナル仮想ブリッジ・ローカル・エリア・ネットワーク（パーソナル VLAN）を有する装置。
【請求項２】
当該パーソナル VLANが、更に、グループ・フレームが属する前記VLANを供するそれらのポートのみにユニキャストおよび前記フレームを転送するVLANブリッジを有する請求項1に記載の装置。
【請求項３】
当該パーソナル VLANが、更に、VLAN発見のためのプロトコルを有する請求項1に記載の装置。
【請求項４】
当該パーソナル VLANが、更に、ステーションが新しいVLANを供する新しいポートを作成すること、または認証プロトコルを介して既存のVLANを結合することを可能にする手段を有する請求項1に記載の装置。
【請求項５】
当該パーソナルVLANが、更に、パーソナル VLANブリッジが物理ポートごとに１つ以上の論理ポートを維持することができ、かつ任意の種類のポート間をブリッジする1つ以上の論理ポートを有する請求項1に記載の装置。
【請求項６】
当該パーソナルVLANが、更に、パーソナルVLANの場合、論理ポートが、多くて1つのVLANを供する、しかし、物理ポートごとに１つ以上の論理ポートが存在することが可能であるので、１つ以上のVLANが物理ポートに存在することが可能である、暗号VLAN分離のための手段を有する請求項1の装置。
【請求項７】
1つのVLANの範囲内のトラフィックが、暗号によって同じ物理ポート上の別のVLANから分離される請求項1に記載の装置。
【請求項８】
認証コードが、暗号化の別のレベルが、当該VLANのメンバに対して以外には、トラフィックを秘密に保ちながら、トラフィックが属するVLANを独自に識別する請求項1に記載の装置。
【請求項９】
当該パーソナルVLANが、更に、IEEE 802.1Q-1998（仮想ブリッジ LAN）プロトコルを有する拡張されたプロトコルを有する請求項1に記載の装置。
【請求項１０】
ルーターにわたるレイヤ2VLANサポートを提供するための手段を、更に有する請求項1に記載の装置。
【請求項１１】
パーソナルVLANが、STAが、前記STA自体がブリッジであるVLANを作成することを可能する時、スパニング・ツリー・アルゴリズムを実施するための手段を、更に有する請求項1に記載の装置。
【請求項１２】
アクセスポイントと関連している複数のステーション間でトラフィックを分ける方法であって、
複数の仮想ローカル・エリア・ネットワーク(VLAN)を有するディストリビューション・システム(distribution system)であって、当該アクセスポイントと関連するすべてのス

テーションが、そのメンバとしてそれ自体および当該ディストリビューション・システムで新しいVLANを作成することができ、新しいVLANのクリエータが、当該新しいVLANを結合することを望むステーションを認証することができるディストリビューション・システムを提供するステップ、および、
信頼されるステーションおよび信頼できないステーション間でトラフィックを分離するステップを有する方法。
【請求項１３】
既存のVLANを発見するステップを、更に有する請求項12に記載の方法。
【請求項１４】
既存のVLANを結合するステップを、更に有する請求項12に記載の方法。
【請求項１５】
アクセスポイントと関連している複数のステーション間でトラフィックを分ける方法であって、
仮想ローカル・エリア・ネットワーク(VLAN)発見のためのプロトコルであって、ステーションが、新しいVLANを供する新しいポートを作成すること、または既存のVLANを結合することを可能にするプロトコルを提供するステップ、
物理ポートごとに１つ以上の論理ポートを維持するステップ、および、
1つのVLANの範囲内のトラフィックが、暗号によって同じ物理ポート上の別のVLANから分離される暗号VLAN分離を提供するステップとを有する方法。
【請求項１６】
トラフィックが属するVLANを、独自に識別する認証コードを提供するステップを、更に有する請求項15に記載の方法。
【請求項１７】
当該VLANのメンバに対して以外には、トラフィックを秘密に保つ暗号化メカニズムを提供するステップを、更に有する請求項16に記載の方法。
【請求項１８】
すべてのポートに、制御フレームおよび認証プロトコル・フレームを送受信するためのパーソナルVLAN制御チャネルを提供するステップを、更に有する請求項15に記載の方法。
【請求項１９】
アクセスポイントと関連している複数のステーション間でトラフィックを分けるシステムにおいて、仮想ローカル・エリア・ネットワーク(VLAN)発見のための装置であって、
LANセグメントを複数VLANに論理的に分割するためのパーソナルVLANブリッジ、および、
他のVLANを発見する、および／または当該VLANブリッジが供するVLANを発見することを可能にする、当該VLANブリッジと関連しているサーバおよびクライアントVLAN発見エージェントを有する装置。
【請求項２０】
発見フレームを伝送するための手段を、更に有する請求項19に記載の装置。
【請求項２１】
応答して、当該発見フレームのソースMACアドレスにVLANオファー・フレームを伝送するための手段を更に有し、当該オファー・フレームが、それらの中から選択するために使用することができるブリッジおよび情報によって供される少なくともいくつかの前記VLANを記述する請求項20に記載の装置。
【請求項２２】
新しいVLANを供するという要求を受信するための手段を、更に有する請求項19に記載の装置。
【請求項２３】
当該要求が、新しいVLANの仮想LAN ID (VID)を有する請求項22に記載の装置。
【請求項２４】
アクセスポイントと関連している複数のステーション間でトラフィックを分けるシステ

ムにおいて、新しい仮想ローカル・エリア・ネットワーク(VLAN)のためのサービスを要求する方法であって、
ブリッジが、物理ポートの制御チャネルによって、当該MACアドレスのホルダがリクエスタである、ソースMACアドレスで要求フレームを受信するステップ、
当該制御チャネルにより当該リクエスタに関する認証プロトコルを開始する当該要求フレームの受信を受信するステップ、
当該リクエスタを認証することができない、または、当該リクエスタが当該ブリッジからVLANサービスを要求するために許可されない場合、当該要求を破棄するステップ、
要求された仮想LAN ID (VID)を使用する際に、コンフリクトがない場合、新しい論理ポートを作成し、かつ当該新しい論理ポートをそれによって当該要求フレームが受信される物理ポートと関連させるステップ、
そうでない場合、当該ブリッジが、当該リクエスタとVIDを取り決めるステップ、および、
ポート状態情報を、当該論理ポートが、当該ポートにより全てのトラフィックに対して効果を有する、当該リクエスタと共有されるセキュリティ・アソシエーションを含むようにアップデートするステップを有する方法。
【請求項２５】
アクセスポイントと関連している複数のステーション間でトラフィックを分けるシステムにおいて、新しい仮想ローカル・エリア・ネットワーク(VLAN)を、ブリッジの物理ポートによって供される１つ以上の既存のVLANにリンクさせる方法であって、
制御チャネルによって結合-VLAN要求を送るステップ、
認証が失敗する場合、当該要求は、破棄される、当該要求を認証するステップ、
宛先VLANを有する物理ポートのセットによって供されるVLANに対するVIDのセットにおけるすべての仮想LAN ID (VID)のメンバセットにソースVLANを供する論理ポートを加えるステップ、および、
当該ソースVLANのメンバセットに物理ポートの当該セットのすべての物理的ポートを加えるステップ、および、
宛先VLANを有する物理ポートのセットによって供されるVLANに対するVIDの当該セットにおけるVIDに対する全てのタグ無しセットの和集合とることによって、当該ソースVLANのタグ無しセットを形成するステップであって、要求フレームがそのタグ・ヘッダに空VIDを含む場合、または、それがタグ無しの場合、当該ブリッジの論理ポートが、宛先VLANを有する物理ポートのセットによって供されるVLANに対するVIDのセットにおけるすべてのVIDのタグ無しセットに加えられるステップを有する方法。
【請求項２６】
アクセスポイントと関連している複数のステーション間でトラフィックを分けるシステムにおいて、論理ポートによって供されるパーソナル仮想ローカル・エリア・ネットワーク(VLAN)を結合するための方法であって、
ソースおよび宛先VLANが同じクリエータを有し、かつ当該クリエータが結合-VLAN要求を出す場合、当該要求が破棄されるステップ、
当該ソースおよび宛先VLANは、同一であり、かつ、当該クリエータは、要求を出さなかった場合、当該クリエータが、当該パーソナルVLANへのメンバシップに対する当該リクエスタを認証するステップ、および、
他の全てのケースにおいて、ブリッジが、最初に、当該リクエスタが当該ソースVLANの前記クリエータであることを確認する当該要求を認証するステップであって、認証が成功する場合、当該クリエータが、当該宛先VLANへのメンバーシップに対する当該リクエスタを認証し、かつ、当該リクエスタが、当該クリエータが当該宛先VLANの前記クリエータであることを確認するため、当該クリエータを認証するステップとを有する方法。
【請求項２７】
アクセスポイントと関連している複数のステーション間でトラフィックを分けるシステムにおいて、論理ポートによって供されるパーソナル仮想ローカル・エリア・ネットワー

ク(VLAN)を結合する要求を認証するための方法であって、
クリエータによるリクエスタの認証のための制御チャネル有するパーソナルVLANブリッジを提供するステップ、
当該パーソナルVLANブリッジが当該クリエータおよび当該リクエスタ間で認証プロトコル・メッセージをリレーするために当該制御チャネルを使用するステップ、および、
当該クリエータが当該リクエスタを認証することができる場合、当該クリエータが、それが当該パーソナルVLANブリッジと共に保持するセキュリティ・アソシエーションを当該リクエスタとも共有するステップを有する方法。
【請求項２８】
論理ポートで入口フィルタリングを提供するステップを、更に有する請求項27に記載の方法。
【請求項２９】
当該セキュリティ・アソシエーションが、少なくとも2つのキー、暗号化のための1つのキー、および認証コードを計算するための別のキーを含み、
当該セキュリティ・アソシエーションが、VLANと関連し、
当該認証コードが、論理ポートで、全VLAN1のメンバに対してトラフィックを制限するために使用され、
暗号化が、メンバに対して以外には、トラフィックを秘密に保つために使用され、
当該セキュリティ・アソシエーションを有しているステーションだけが、VLANに属し、かつ、
当該セキュリティ・アソシエーションを有している全てのステーションが、同じブロードキャスト・ドメインに属する請求項27に記載の方法。
【請求項３０】
物理ポートが、それに関連している複数の論理ポートを有することによって1つ以上のVLANを供することが可能である請求項28に記載の方法。
【請求項３１】
受信されたフレームが空仮想LAN ID (VID)を伝える、またはタグ無しの場合(400)、そのソースMACアドレスを、論理ポートの先行のVLAN分類を判断するために使用するステップ、
当該フレームがVIDを伝える場合、当該VIDを、その代わりに、当該先行の分類として使用するステップ、
当該先行の分類を、認証コード・キーを与えているセキュリティ・アソシエーションのテーブルにインデックスを付けるために使用するステップ、
当該受信されたフレームが、認証時に当該パーソナルVLANブリッジおよび当該リクエスタの両方によって合意に達せられ、かつ当該セキュリティ・アソシエーションに記録された、メッセージ・ダイジェスト・アルゴリズムを使用して、フレーム・ペイロードに対して計算された認証コードを伝えるステップ、
当該パーソナルVLANブリッジが、認証コード・キーとして当該認証コードを使用し、当該受信されたフレームの当該ペイロードに対して、当該認証コードを再計算するステップ、
当該再計算された認証コードを当該受信されたコードを比較するステップ、
当該再計算された認証コードと当該受信されたコードが一致する場合、当該先行のVLAN分類が、最終的なVLAN分類になるステップ、
当該最終的な分類を任意の対応しているデータ要求プリミティブのVLAN分類パラメータの値として使用するステップ、
当該フレームを当該セキュリティ・アソシエーションを使用して解読するステップ、および、
当該解読されたフレームをフォワーディングおよびラーニングプロセスに提出するステップ、
そうでなければ、当該フレームを破棄するステップとを更に有する請求項27に記載の方

法。
【請求項３２】
VLANに属するフレームに対する伝送ポートが当該VLANのメンバセットにない場合、当該フレームが破棄される請求項27に記載の方法。
【請求項３３】
ブリッジと関連している複数のステーション(STA)間でトラフィックを分ける装置であって、トラフィックを分けるためにVLANを使用するパーソナル仮想ブリッジ・ローカル・エリア・ネットワーク（パーソナルVLAN）を有する装置。
【請求項３４】
当該パーソナルVLANが、更に、
LANセグメントを複数VLANに論理的に分割するための当該パーソナルVLANと関連している手段、および、
当該フレームが属するVLANを供するそれらのポートのみにユニキャストおよびグループ・フレームを転送する当該パーソナルVLANと関連するパーソナルVLANブリッジを有する請求項33に記載の装置。
【請求項３５】
当該パーソナルVLANブリッジが、
パーソナルVLANブリッジがVLAN発見のためのプロトコルを提供するVLAN発見方法、
パーソナルVLANブリッジが、ステーションが新しいVLANを供する新しいポートを作成すること、または認証プロトコルを介して既存のVLANを結合することを可能にするVLAN 拡張方法、
パーソナルVLANブリッジが、物理ポートごとに1つ以上の論理ポートを維持し、および任意の種類のポートの間でブリッジする論理ポート方法、および、
パーソナルVLANの場合、論理ポートが、多くて1つのVLANを供するが、物理ポートごとに１つ以上の論理ポートが存在することが可能であるので、１つ以上のVLANが物理ポートに存在することが可能である、暗号VLAN分離方法の少なくとも何れかで、標準VLANブリッジを拡張する請求項34に記載の装置。
【請求項３６】
1つのVLANの範囲内のトラフィックが、暗号によって同じ物理ポート上の別のVLANから分離される請求項35に記載の装置。
【請求項３７】
認証コードが、暗号化の別のレベルが、当該VLANのメンバに対して以外には、トラフィックを秘密に保ちながら、当該トラフィックが属するVLANを独自に識別する請求項35に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ローカル・エリア・ネットワークに関する。より詳細には、本発明は、パーソナル仮想ブリッジ・ローカル・エリア・ネットワークに関する。
【背景技術】
【０００２】
アクセスポイント(AP)は、１つ以上のステーション(STA)および1つのDS (distribution system)の間のリンク層ブリッジである。IEEE 802.11, 「無線LAN媒体アクセス制御および物理層仕様(Wireless LAN Medium Access Control and Physical Layer Specifications)」, ISO/IEC 8802-11: 1999 (E), ANSI/IEEE Std 802.11, 1999 Editionを参照されたい。DSの具体例は、LANセグメントまたはイントラネットである。APは、パケットが、通信を介して、ステーション(STA)からDSまで、あるいは、DSからSTAまでの何れかに伝送されることを可能にする。アクセスポイントは、したがって、少なくとも2つの物理ポートを有する。一方は、DSインタフェースであり、他方は、通信インタフェースである。複数のSTAは、各々自身の通信インタフェースを備え、APの単一の共有される通信インタフェ

ースを多重送信することによって、DSにパケットを送ることができる。通信インタフェースは、特定の周波数で動作し、および、STAは、媒体に相互排除アクセスを保証するMAC-PHYプロトコルにより、媒体を共有する。DSは、また、同じプロトコルを用いてSTAにパケットを送る。

【０００３】

APのSTAは、BSSID (Basic Service Set ID)を有する。それは、論理的に、802.11基本サービスセット(Basic Service Set)を分割するのに役立つ。APと関連するすべてのSTAは、APのBSSIDを共有する。APまたはSTAが属するBSSが、フレームのBSSIDに一致しない場合、APまたはSTAによって受信されるグループ・アドレス向けフレームは廃棄される。この意味で、BSSIDは、VID (Virtual LAN ID)としてふるまう。IEEE 802.1Q, IEEE Standards for Local and Metropolitan Area Networks：Virtual Bridged Local Area Networks, IEEE Std 802.1Q-1998を参照されたい。したがって、すべてのSTAは、同じAPと関連する結果として同じ仮想LAN (VLAN)のメンバである。

【０００４】

しかしながら、STAが互いを信頼しない場合、BSSのすべてのSTAは、同じVLANを共有すべきでない。それでも、公衆スペース展開において、一般的に、それらの間で信用がない場合、APと関連している全てのSTAは、同じVLANを共有しなければならない。これは、STAを、例えば、アドレス解決プロトコル(ARP)キャッシュ再マッピングのような、信頼できないSTAによって開始されるさまざまなリンク層攻撃に弱くする可能性がある。

【０００５】

例えば、当該ブリッジと関連している信頼できないSTAが同じブリッジと関連している別のSTA上でリンク層(OSI Layer 2)攻撃を開始するために使用されることが出来ないように、ブリッジと関連しているSTA間でトラフィックを分けるメカニズムを提供することは、有利であろう。

【０００６】

本発明は、例えば、当該ブリッジと関連している信頼できないSTAが同じブリッジと関連している別のSTA上でリンク層(OSI Layer 2)攻撃を開始するために使用されることが出来ないように、ブリッジと関連しているSTA間でトラフィックを分けるメカニズムを提供する。本発明は、トラフィックを分けるためにVLANを使用することに基づく。IEEE 802.1Q-1998（仮想ブリッジ LAN）プロトコルは、LANセグメントを論理的に複数VLANに分割する本発明によって拡張されるメカニズムを提供する。好ましい実施例の場合、VLANブリッジは、グループ・フレームが属するVLANを供するそれらのポートのみに、ユニキャストおよびグループ・フレームを転送する。本発明の一実施例は、APの範囲内での使用に適しているメカニズムを提供するために標準VLANブリッジ・モデルを拡張する。

【０００７】

APがDSにアタッチされると仮定する。APと関連するすべてのSTAは、そのメンバとしてそれ自体およびDSで新しいVLANを作成する機会を有するはずである。この方法で、それらが同じAPと関連する場合であっても、信頼されるSATと信頼できないSTA間でトラフィックを分離することが出来る。一般に、DSが複数VLANを有する場合、それらの任意のサブセットのメンバは、新しいVLANのメンバとなることが出来る。したがって、既存のVLANを発見する方法があるはずである。さらに、既存のVLANを結合するためのプロトコルが、あるはずである。VLANを作成することおよび既存のVLANを結合することは、どちらも認証を要求する動作である。IEEE Std 802.1Q-1998 VLANモデルは、これらの機能を提供しないので、このような目的のために不十分である。本発明の好ましい実施例は、本明細書において、パーソナル仮想ブリッジ・ローカル・エリア・ネットワーク （パーソナルVLAN）と呼ばれる、このような機能を提供するメカニズムを有する。

【０００８】

好ましい実施例において、パーソナルVLANブリッジは、以下の方法の少なくとも何れかで標準VLANブリッジを拡張する。

・VLAN発見：パーソナルVLANは、（以下に記載される）VLAN発見のため

のプロトコルを提供する。
・VLAN 拡張／作成：パーソナルVLANブリッジは、ステーションが、新しいVLANを供する新しいポートを作成すること、または既存のVLANを結合すること、または認証プロトコルを介して既存のVLANを結合することを可能にする。
・論理ポート：パーソナルVLANブリッジは、物理ポートごとに1つ以上の論理ポートを維持することができる。それは、任意の種類のポート間をブリッジする。VLANのメンバセットは、論理および物理ポートの観点から定義される。すべての論理ポートは、ブリッジによって制御される寿命を有する。
・暗号VLAN分離：パーソナルVLANにおいて、論理ポートは、多くて1つのVLANを供する。しかしながら、物理ポートごとに1つ以上の論理ポートが存在することが可能であるので、1つ以上のVLANが物理ポートに存在することが可能である。1つのVLANの範囲内のトラフィックは、暗号によって同じ物理ポート上の別のVLANから分離される。認証コードは、暗号化の別のレベルが、VLANのメンバに対して以外には、トラフィックを秘密に保ちながら、トラフィックが属するVLANを独自に識別する。
・ルーターにわたるレイヤ2 VLANサポート：例えば、新しいAPと関連することによって、STAが移動することができ、かつ、異なるブリッジでのネットワークに再びアッタチすることができる場合、STAは、それがすでに属しているVLANのブリッジに知らせることができる。そのVLANは、別のブリッジでの１つ以上の論理または物理ポートとそのVLANをリンクさせるそのブリッジでのステーション、例えば、それ自体によって作成されたかもしれない。新しいブリッジが異なるサブネット上に置かれた場合でさえ、STAは、レイヤ2でVLANにおけるそのメンバシップを維持することができる。モバイルIPがルーターにわたるステーション用のサブネット・メンバシップを保持することを意図するので、この機能はモバイルIP機能を包含する。サブネットは、VLANに対応することが出来るが、しかし、一般には、対応しない。
・スパニング・ツリー・メンテナンス：パーソナルVLANブリッジは、STAが、STA自体がブリッジであるVLANを作成することを可能にする。メンバシップが付与されるときに、スパニング・ツリー・アルゴリズムは、ブリッジの中のサイクルを除去する。パーソナルVLANを結合するプロセスは、新しいブリッジがVLANを結合した後でスパニング・ツリーを再建することを不必要にする制約をVLANトポロジに強制する。

【０００９】

【非特許文献１】IEEE 802.11, 「無線LAN媒体アクセス制御および物理層仕様(Wireless LAN Medium Access Control and Physical Layer Specifications)」, ISO/IEC 8802-11: 1999(E), ANSI/IEEE Std 802.11, 1999 Edition.

【非特許文献２】IEEE 802.1Q, IEEE Standards for Local and Metropolitan Area Networks：Virtual Bridged Local Area Networks, IEEE Std 802.1Q-1998.

【非特許文献３】Service Location Protocol v2, IETF, RFC 2608

【発明の開示】

【発明が解決しようとする課題】

【００１０】

本発明の好ましい本実施例は、例えば、当該ブリッジと関連している信頼できないSTAが同じブリッジと関連している別のSTA上でリンク層(OSI Layer 2)攻撃を開始するために使用されることが出来ないように、ブリッジと関連しているSTA間でトラフィックを分けるメカニズムを提供する。当業者は、本明細書において開示される本発明が、有線および無線ネットワークを含み、これらに限定されない広範囲にわたるシステムおよびネットワークに適用可能であることを認めるであろう。

【課題を解決するための手段】

【００１１】
パーソナルVLANブリッジ・モデル
本発明は、トラフィックを分けるためにVLANを使用することに基づく。IEEE 802.1Q-1998（仮想ブリッジ LAN）プロトコルは、LANセグメントを論理的に複数のVLANに分割する本発明によって拡張されるメカニズムを提供する。好ましい実施例において、VLANブリッジは、フレームが、属するVLANを供するそれらのポートのみに、ユニキャストおよびグループ・フレームを転送する。本発明の一実施例は、APの範囲内での使用に適しているメカニズムを提供するために標準VLANブリッジ・モデルを拡張する。
【００１２】
APがDSにアタッチされると仮定する。APと関連するすべてのSTAは、そのメンバとしてそれ自体およびDSで新しいVLANを作成する機会を有するはずである。この方法で、それらが同じAPと関連する場合であっても、信頼されるSATと信頼できないSTA間でトラフィックを分離することが出来る。一般に、DSが複数のVLANを有する場合、それらの任意のサブセットのメンバは新しいVLANのメンバとなることが出来る。したがって、既存のVLANを発見する方法があるはずである。さらに、既存のVLANを結合するためのプロトコルが、あるはずである。VLANを作成することおよび既存のVLANを結合することは、どちらも認証を要求する動作である。IEEE Std 802.1Q-1998 VLANモデルは、これらの機能を提供しないので、このような目的のために不十分である。本発明の好ましい実施例は、本明細書において、パーソナル仮想ブリッジ・ローカル・エリア・ネットワーク （パーソナルVLAN）と呼ばれる、このような機能を提供するメカニズムを有する。
【発明を実施するための最良の形態】
【００１３】
本発明の好ましい本実施例が、図1～3と関連して本明細書において議論される。図1～3に示される構成が、具体例だけのために提供され、本発明が実施される構成を制限するものでないことは、当業者によって認められるであろう。
【００１４】
図1は、2つのブリッジ10、12を示すブロック略線図である。パーソナルVLANブリッジ 1 (10)は4つの物理ポート11、13、15、17を有し、そのうちの2つ11、13は、有線のイーサネット(Ethernet)である。有線のポートは、それぞれVLAN1およびVLAN2を供する。他の2つのポート15、17は、無線イーサネットポートである。これらのポートの一方のポート15は、高速の(54Mbps)802.11g標準に適合し、かつ、他方のポート17は、802.11a標準に適合する。802.11gのポートと関連している3つの論理ポート19、21、23 がある。各論理ポートは、それ自身のセキュリティ・アソシエーション25、27、29を有し、セキュリティ・アソシエーションは、別々のVLANを構成するためにある数のエンド・ステーション20、22、24によって共有される。
【００１５】
図2で図示されるように、ステーションA 20は、SA1 25をブリッジ1 10と共有する。他のいかなるステーションも、SA1を共有しない、したがって、STA Aは、一意的なVLAN、すなわち、ルートがブリッジ1であるスパニング・ツリーによって表現されるVLAN3に属する。
【００１６】
一方、ステーションBおよびC 22、24 は、SA2 27をブリッジ1と共有する（図2を参照）ので、VLAN4に属する。このVLANは、STA AまたはSTA Bの一方によって作成された。次に、他方のステーションは、クリエータによって認証された後にそれを結合した。これは、パーソナルVLAN（下記参照）を結合するケースを示す。VLAN4は、また、ルートとしてブリッジ1を有するスパニング・ツリーによって表現される。
【００１７】
ステーションD 16およびステーションE 18は、VLAN5に属する。しかしながら、他のステーションとは異なり、それらは、セキュリティ・アソシエーションをブリッジ1と共有しない、しかし、逆に、パーソナルVLANブリッジ2 12（図3を参照）と共有する。ブリッ

ジ2は、ツリーが拡張され、ブリッジ1を新しいルートとするまで、VLAN5に対するスパニング・ツリーのルートである。

【００１８】

一実施例において、パーソナルVLANブリッジは、以下の方法の少なくとも何れかで、標準VLANブリッジを拡張する。

・VLAN発見：パーソナルVLANは、（以下に記載される）VLAN発見のためのプロトコルを提供する。

・VLAN 拡張／作成：パーソナルVLANブリッジは、ステーションが新しいVLANを供する新しいポートを作成すること、または既存のVLANを結合すること、または認証プロトコルを介して既存のVLANを結合することを可能にする。

・論理ポート：パーソナルVLANブリッジは、物理ポートごとに1つ以上の論理ポートを維持することができる。それは、任意の種類のポートの間でブリッジする。VLANのメンバセットは、論理および物理ポートの観点から定義される。すべての論理ポートは、ブリッジによって制御される寿命を有する。

・暗号VLAN分離：パーソナルVLANにおいて、論理ポートは、多くて1つのVLANを供する。しかしながら、物理ポートごとに1つ以上の論理ポートが存在することが可能であるので、1つ以上のVLANが物理ポートに存在することが可能である。1つのVLANの範囲内のトラフィックは、暗号によって同じ物理ポート上の別のVLANから分離される。認証コードは、暗号化の別のレベルが、VLANのメンバに対して以外には、トラフィックを秘密に保ちながら、トラフィックが属するVLANを独自に識別する。

・ルーターにわたるレイヤ2 VLANサポート：例えば、新しいAPと関連することによって、STAが移動することができ、かつ、異なるブリッジでのネットワークに再びアタッチすることができる場合、STAは、それがすでに属しているVLANのブリッジに知らせることができる。そのVLANは、別のブリッジでの１つ以上の論理または物理ポートとそのVLANをリンクさせるそのブリッジでのステーション、例えば、それ自体によって作成されたかもしれない。新しいブリッジが異なるサブネット上に置かれた場合でさえ、STAは、レイヤ2でVLANにおけるそのメンバシップを維持することができる。モバイルIPがルーターにわたるステーション用のサブネット・メンバシップを保持することを意図するので、この機能はモバイルIP機能を包含する。サブネットは、VLANに対応することが出来るが、一般には、それは、対応しない。

・スパニング・ツリー・メンテナンス：パーソナルVLANブリッジは、STAが、STA自体がブリッジであるVLANを作成することを可能にする。メンバシップが付与されるときに、スパニング・ツリー・アルゴリズムは、ブリッジの中のサイクルを除去する。パーソナルVLANを結合するプロセスは、新しいブリッジがVLANを結合した後でスパニング・ツリーを再建することを不必要にする制約をVLANトポロジに強制する。

【００１９】

本好適なパーソナルVLANブリッジ・モデルは、IEEE Std 802.1Q-1998, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, pp. 28に記載されているように、メンバ／タグ無しセットを判断し、フレームにタグを付けるためのそのルールによって、およびリレーしているMACフレームと関係している構成要素によって、VLANモデルに対応する。パーソナルVLANブリッジにおけるこれらの構成要素に対する拡張は、以下に記述される。

【００２０】

パーソナルVLAN制御チャネル

すべての物理ポートは、制御フレームおよび認証プロトコル・フレームを送受信するためのパーソナルVLAN制御チャネル40、42を有する。チャンネルは、セキュリティ・アソシ

エーションを備えておらずおよびフレーム・フィールド、例えばエンコードされたイーサネット・タイプ(Ethernet Type)によって識別される。認証フレームは、様々な認証プロトコルを扱うことができるEAPoL（IEEE 802.1X, IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001を参照）のようなフォーマットを使用して、カプセル化されることが好ましい。

【００２１】

VLAN発見

パーソナルVLANブリッジは、サーバおよびクライアントVLAN発見エージェント26および28、30をそれぞれ、実行する。クライアント・エージェントが情報要求を出す間、サーバ・エージェントは、情報要求に応じる。このようなエージェントの具体例は、Service Location Protocol v2, IETF, RFC 2608のクライアントおよびサーバ・エージェントである。したがって、パーソナルVLANは、他のVLANを発見することができ、および／または、それが供するVLANが発見されることを可能にする。発見（図4参照）は、VLAN発見(VLAN-DISCOVER)フレームの、伝送を意味する。応答して、VLANオファー(VLAN-OFFER)フレームは、発見フレームのソースMACアドレスに送られる。

【００２２】

オファー・フレームは、それらの中から選択するために使用することができるブリッジおよび情報によって供される全てのまたはいくつかのVLANを記述する。クライアントが送った発見フレームに応答して、クライアントによって受信される1つ以上のオファー・フレームが存在する可能性がある。VLANオファー・フレームの伝送は、応答側の間で衝突を最小化するためにランダムに選ばれたある期間だけ遅れる。

【００２３】

新しいVLANの提供

パーソナルVLANブリッジは、新しいVLANを供するという要求を受信することができる。要求は、新しいVLANのVIDを含む。リクエスタが許可され、要求が新しく、および、それを制御チャネルにより認証することができない限り、要求は承諾されない。ブリッジで新しいVLANを供することは、そのブリッジを名前付きVLANに対するスパニング・ツリーのルートとすることを要求する。新しいVLANに対するサービスを要求することは、次のステップから成る。

・ブリッジは、物理ポートの制御チャネルによりソースMACアドレスで要求フレームを受信する。そのMACアドレスのホルダは、リクエスタである(100)。
・要求フレームの受信は、制御チャネルによりリクエスタに関する認証プロトコルを開始する(102)。
・リクエスタを認証することができない、または、リクエスタがブリッジからVLANサービスを要求するために許可されない場合(104)、要求は破棄される(106)。
・要求されたVIDを使用する際に、コンフリクトがない場合(105)、新しい論理ポートは、作成され、かつそれによって要求フレームが受信される物理ポートと関連する(108)。これは、ブリッジがVLANを供するために使用する論理ポートである。そうでなければ、ブリッジは、リクエスタとVIDを取り決める(110)。VLANのフィルタ・ルールは、リクエスタのためのポリシーによって判断される。
・ポート状態情報は、論理ポートが、そのポートにより全てのトラフィックに対して効力を有する、リクエスタと共有されるセキュリティ・アソシエーション(SA)を含むようにアップデートされる(112)。SAのホルダだけは、論理ポート状態を変更することができる。

【００２４】

これらのステップ終了後、新しい論理ポートが、新しいVLANを供するために存在する、しかし、このVLANは、特定のVLANを結合するための要求がなされるまで、ブリッジによって供される他のいかなるVLANにも、リンクしない。この時まで、新しいVLANは、ブリッジ

で実施不可能である。

【００２５】

VLANの結合

ブリッジによって供される新しいVLANは、有効なブリッジの物理ポートによって供される１つ以上の既存のVLANを拡張しなければならない。言い換えると、それは、１つ以上の既存のVLANにリンクしなければならない。ブリッジで論理ポートによって供されるVLANをブリッジの物理ポートによって供される１つ以上のVLANにリンクさせることは、制御チャネルによって送られる結合-VLAN要求で実行される。要求は、物理ポートによって供されるVLANをブリッジしない。むしろ、それらは別々のままである、それでも、新しいVLANは同時にその全部を拡張する。

【００２６】

結合-VLAN要求は、本明細書においてソースVLANと呼ばれるブリッジの論理ポートP'によって供されるVLANのVID V'および物理ポートのセットPによって供される本明細書において宛先VLANと呼ばれるVLANに対するVIDのセットVを含む。要求は、V'をVのすべてのVLAN IDにリンクさせることを意図し、または、言い換えると、リクエスタがVのすべてのVLANを結合することを可能にすることを意図する。リクエスタは、すでにVを作成した。

【００２７】

ブリッジは、次のステップをとる(図6を参照)。

・最初に、要求が認証される(200)。これは、ブリッジがV'を供するよう依頼されたとき、確立されたV'と関連するSAに関して行われる。他のアプローチが、適切に使用されることが可能であるにもかかわらず、簡単なチャレンジ-応答戦略が、好ましい実施例において使用される。認証が失敗する場合、要求は破棄される。

・論理ポートP'は、VのすべてのVIDのメンバセットに加えられる(202)、および、Pのすべての物理ポートは、V'のメンバセットに加えられる(204)。V'のタグ無しセットは、VのVIDに対する全てのタグ無しセットの和集合をとることによって形成される(206)。要求フレームがそのタグ・ヘッダにおいて空VIDを含む場合、または、それがタグ無しの場合、P'は、VのすべてのVIDのタグ無しセットに加えられる(208)。

【００２８】

新しいVLANを供しかつそれを他のVLANにリンクさせる要求は、1つの要求に組み込ませることができる。したがって、1つのVLANを作成しかつ別のものを結合することは、1つの認証プロセス、具体的には、新しいVLANを供するために要求されたプロセスにより実行させることができる。

【００２９】

パーソナルVLANの結合

パーソナルVLAN、すなわち論理ポートによって供されるものを結合することは、特別な処理を要求する。パーソナルVLANブリッジは、それがその物理ポートと異なったポートを作成しないので、論理ポートによって供されるVLANをリンクさせるために許可されない。この場合、論理ポートのクリエータは、相互に同意するプロトコル(mutually-agreed upon protocol)、例えば、チャレンジ・レスポンス(challenge-response)によりリクエスタを認証する。その宛先VLANセットが論理ポートによって供される単一のVLANから成る、ブリッジが結合-VLAN要求を受信する時(298)、このインター・ステーション認証（図7参照）は、起動する。

【００３０】

3つのケースがある。

・ソースおよび宛先VLANは、同じクリエータを有し、かつ、クリエータは、結合-VLAN要求を出した(300)。この場合、要求は破棄される(302)。そうでなければ、サイクルはブリッジされたVLANに結果としてなり得たであろう。

・ソースおよび宛先VLANは、同一であり、かつ、クリエータは、要求を出さ

なかった(304)。この場合、クリエータは、パーソナルVLANへのメンバシップに対してリクエスタを認証する(306)。
・他の全てのケースにおいて(308)、ブリッジは、最初に、リクエスタがソースVLANのクリエータであることを確認する要求を認証する（VLANを結合するためのステップ1が物理ポートだけによって供されたときと同じ― 上記参照）(310)。認証が成功する場合(312)、クリエータは、宛先VLANへのメンバシップに対してリクエスタを認証する(314)。

【００３１】

パーソナルVLANを結合する場合、宛先VLANセットは、正確に1つのVLAN、すなわち、ソースVLANに限定されることが好ましい。それは、次のような方法で限定される。その理由は、限定されない場合には、要求が、それが所有していないVLANを他のVLAN （行うことが許可されていない何か）にブリッジするためにステーションによる試行を反映するであろうと言うことである。VLANのオーナーは、新しいVLANを結合することができ、かつ、その結果、全てのそのメンバステーションは、また、新しいVLANのメンバになる。

【００３２】

クリエータによるリクエスタの認証は、ブリッジおよびそれぞれの認証／サプリカントモジュール50、52、54の制御チャネルによって容易にされる。ブリッジは、クリエータとリクエスタの間で認証プロトコル・メッセージをリレーするためにチャンネルを使用する。制御チャネルおよびリレーしているメッセージの管理は、例えば、IEEE 802.1X, IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control IEEE Std 802.1X-2001を使用して実施させることができる。802.1Xモデルにおいて、リクエスタは、サプリカントであり、およびクリエータは認証者である。クリエータがリクエスタを認証することができる場合、それは、それがブリッジと共に保持するSAをリクエスタとも共有する。ブリッジは、それがクリエータと共に保持するSAをリクエスタと共有するべきか否かを決めることは、ブリッジの責任でない。これは、クリエータの責任である。多くの方法が、共有を達成するためにある。1つの方法は、SAをリクエスタのステーションで引き出すことができるであろうTLS v1.0 (Transport-Layer Security)プレ・マスタシークレット(pre-master secret)を暗号化するリクエスタの公開鍵を使用することである。

【００３３】

論理ポートの入口フィルタリング

セキュリティ・アソシエーションは、少なくとも2つのキーを含み、一方は、暗号化のためのもの、および他方は、認証コードを計算するためのものであり、本明細書でMIC(Message Integrity Code)と呼ばれる。SAは、独自に、VLANと関連している。暗号化が、メンバに対して以外には、トラフィックを秘密に保ちながら、認証コードは、論理ポートで、全VLANのメンバに対して、トラフィックを制限するために使用される。SAを有しているステーションだけは、VLANに属する。各SAに対して単一ブロードキャスト・ドメインが、ある。SAを有している全てのステーションは、同じブロードキャスト・ドメインに属する。したがって、別々の暗号化キーは、ブロードキャストのために必要とされない。

【００３４】

物理ポートは、それと関連している複数の論理ポートを有することによって1つ以上のVLANを供することが可能である（図1参照）。したがって、このようなポートで受信されるフレームがVIDを伝えない場合、そのVLAN分類は、ポート・ベースの分類の範囲を超えてルールを使用しなければならない。IEEE 802.1Q, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks IEEE Std 802.1Q-1998, D.2.2を参照されたい。そうでなければ、どのVIDをポートによって供されるVLANの中から割り当てるべきかをこのステージで知る方法が、ない。それによってフレームが受信される論理ポートを識別することは、必要である。

【００３５】

以下の説明と関連して図8を参照されたい。受信されたフレームが空VIDを伝えるかまた

はタグ無しの場合(400)、そのソースMACアドレスは、先行のVLAN分類を判断するために使用される(402)。これは、論理ポートのPVIDである。フレームがVIDを伝える場合、VIDは、その代わりに、先行の分類として使用される(404)。先行の分類は、MICキーを与えているセキュリティ・アソシエーションのテーブルにインデックスを付けるために使用される(406)。受信されたフレームは、認証時にブリッジおよびリクエスタの両方によって合意に達せられかつSAに記録された、メッセージ・ダイジェスト・アルゴリズム、例えば、HMAC-MD5を使用して、フレーム・ペイロードに対して計算されたMICを伝える。パーソナルVLANブリッジは、そのMICキーを使用し、受信されたフレームのペイロードに対して、MICを再計算する(408)、そして次に、それを受信されたMICと比較する(410)。それらが一致する場合(412)、先行のVLAN分類は、最終的なVLAN分類になる(414)。最終的な分類は、任意の対応しているデータ要求プリミティブのVLAN分類パラメータの値として使用される(416)。フレームは、次に、SAを使用し、解読され、そして、次に、 IEEE802.1Q フォワーディングおよびラーニングプロセス(Forwarding and Learning Processes)に提出される(418)。そうでなければ、フレームは破棄される。

【００３６】

論理ポートでの出口フィルタリング

VLANブリッジ・モデルにおいて、あるVLANに属するフレームに対する伝送ポートがVLANのメンバセットにない場合、フレームは破棄される。同じルールは、全ての論理伝送ポートに適用される。

【００３７】

本明細書において、本発明は、好ましい実施例と関連して説明されたが、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明細書で説明した応用例の代わりに他の応用例を使用できることを、容易に認めるであろう。従って、添付の特許請求の範囲しか本発明を限定さしない。

【図面の簡単な説明】

【００３８】

【図１】本発明によるパーソナルVLANネットワークにおける2つのブリッジを示すブロック略線図である。

【図２】ステーションAがSA1をブリッジ1と共有する一実施例を示すブロック略線図である。

【図３】ステーションDおよびEは、VLAN5に属し、しかしながら、他のステーションとは異なり、それらはセキュリティ・アソシエーションをブリッジ1と共有しない、しかし、逆に、パーソナルVLANブリッジ2と共有する実施例を示すブロック略線図である。

【図４】本発明によるパーソナルVLAN発見を示すブロック略線図である。

【図５】本発明による新しいVLANに対するサービスの要求を示す流れ線図である。

【図６】本発明によるブリッジで物理ポートによって供される１つ以上のVLANに対するブリッジの論理ポートによって供されるVLANのリンクを示す流れ線図である。

【図７】本発明によるブリッジが、その宛先VLANセットが論理ポートによって供される単一のVLANから成る結合-VLAN要求を受信する時、起動されるインター・ステーション認証を示す流れ線図である。

【図８】本発明による論理ポートにフィルターをかけている入口を示している流れ線図である。

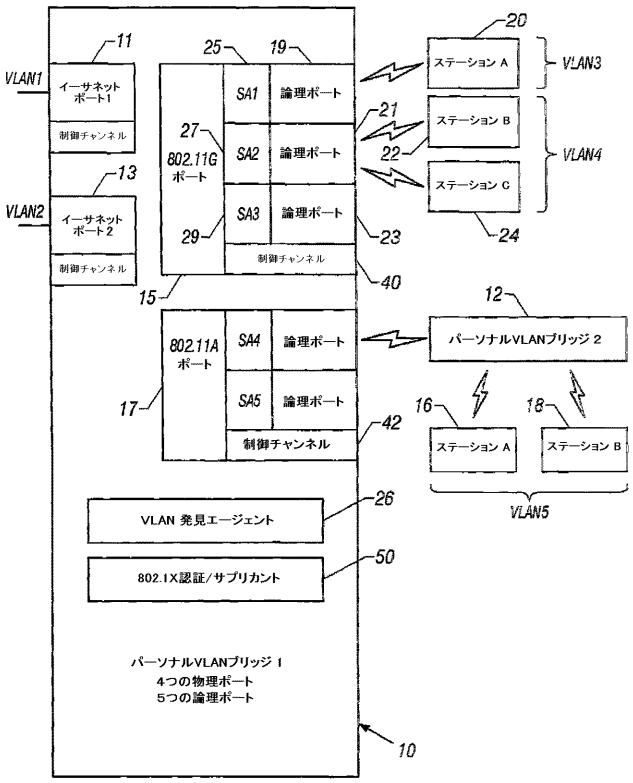
【符号の説明】

【００３９】

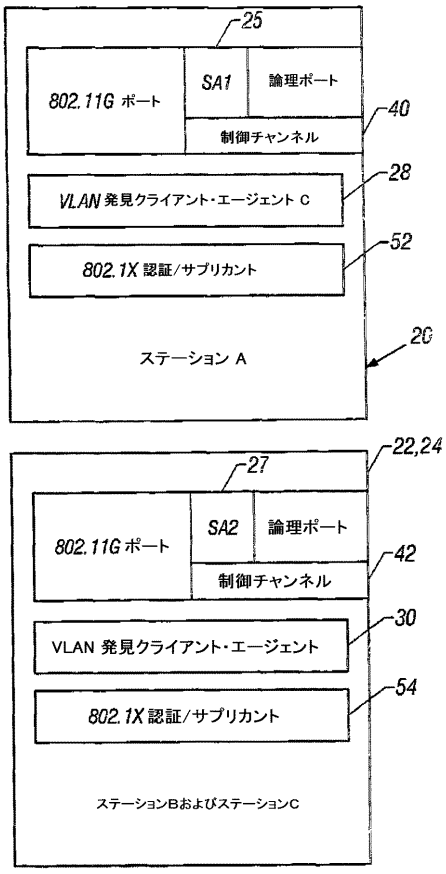
10、12　パーソナルVLANブリッジ
11、13、15、17　物理ポート
25、27、29　セキュリティ・アソシエーション
19、21、23　論理ポート
20、22、24　エンド・ステーション
16、18　ステーション

40、42　制御チャンネル
26　VLAN発見エージェント
50　認証／サプリカントモジュール

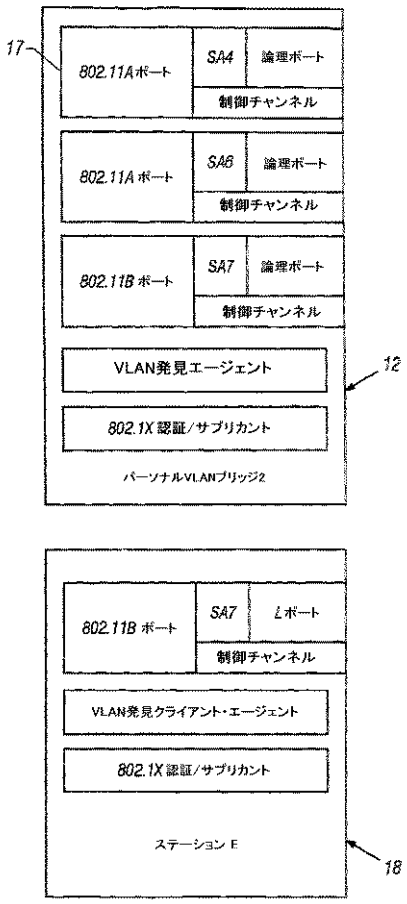
【図１】



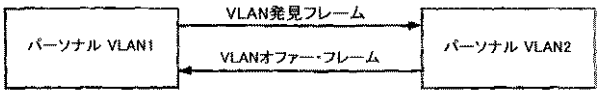

【図２】



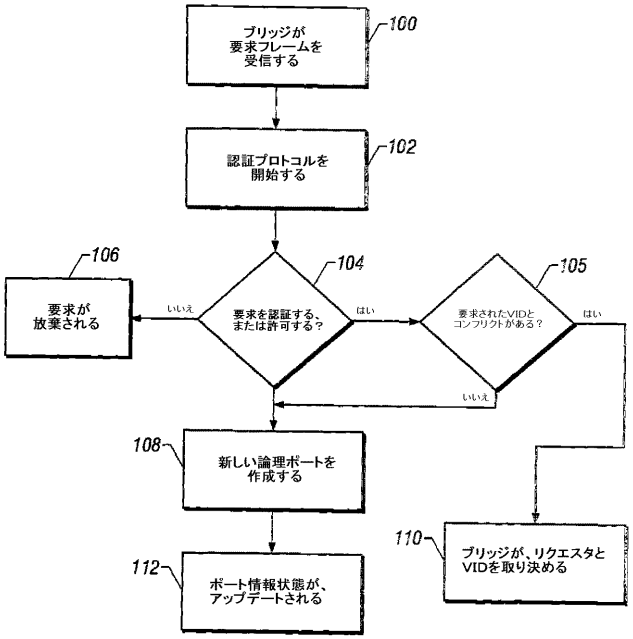
【図３】


17
802.11Aポート
SA4
論理ポート
制御チャンネル
802.11A ポート
SA6
論理ポート
制御チャンネル
802.11B ポート
SA7
論理ポート
制御チャンネル
VLAN発見エージェント
802.1X 認証/サプリカント
パーソナルVLANブリッジ2
12
802.11B ポート
SA7
Lポート
制御チャンネル
VLAN発見クライアント・エージェント
802.1X 認証/サプリカント
ステーション E
18

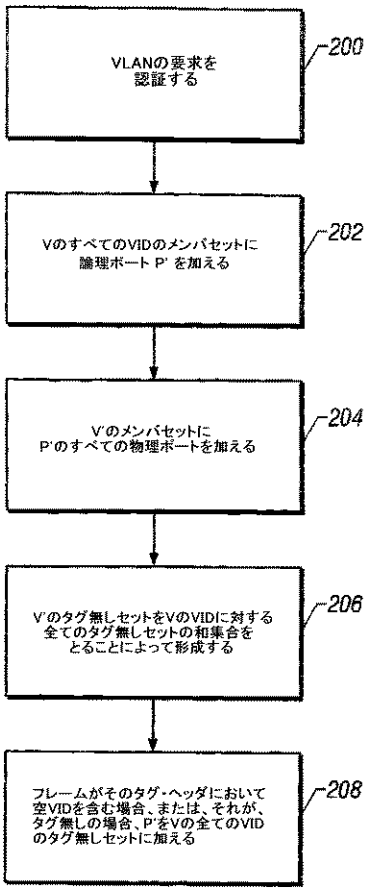
【図４】


パーソナル VLAN1
VLAN発見フレーム
VLANオファー・フレーム
パーソナル VLAN2

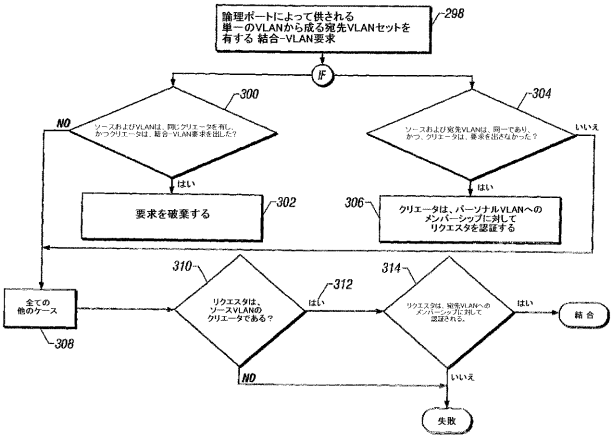
【図５】


ブリッジが
要求フレームを
受信する
100
認証プロトコルを
開始する
102
106
要求が
放棄される
いいえ
要求を認証する、
または許可する？
104
はい
要求されたVIDと
コンフリクトがある？
105
はい
いいえ
108
新しい論理ポートを
作成する
110
ブリッジが、リクエスタと
VIDを取り決める
112
ポート情報状態が、
アップデートされる

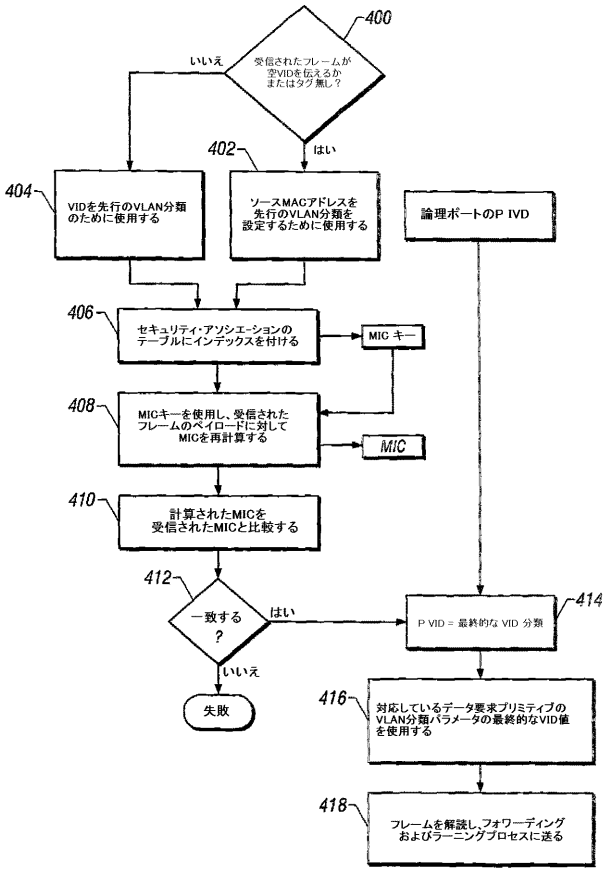
【図６】


VLANの要求を
認証する
200
VのすべてのVIDのメンバセットに
論理ポート P' を加える
202
V'のメンバセットに
P'のすべての物理ポートを加える
204
V'のタグ無しセットをVのVIDに対する
全てのタグ無しセットの和集合を
とることによって形成する
206
フレームがそのタグ・ヘッダにおいて
空VIDを含む場合、または、それが、
タグ無しの場合、P'をVの全てのVID
のタグ無しセットに加える
208

【図７】


論理ポートによって供される
単一のVLANから成る宛先VLANセットを
有する 結合-VLAN要求
298
IF
300
NO
はい
304
いいえ
はい
要求を破棄する
302
306
クリエータは、パーソナルVLANへの
メンバーシップに対して
リクエスタを認証する
310
全ての
他のケース
308
リクエスタは、
ソースVLANの
クリエータである？
312
はい
314
はい
結合
NO
いいえ
失敗

【図８】


400
受信されたフレームが
空VIDを伝えるか
またはタグ無し？
いいえ
はい
402
404
VIDを先行のVLAN分類
のために使用する
ソースMACアドレスを
先行のVLAN分類を
設定するために使用する
論理ポートのP IVD
406
セキュリティ・アソシエーションの
テーブルにインデックスを付ける
MIC キー
408
MICキーを使用し、受信された
フレームのペイロードに対して
MICを再計算する
MIC
410
計算されたMICを
受信されたMICと比較する
412
一致する
？
はい
414
P VID = 最終的な VID 分類
いいえ
失敗
416
対応しているデータ要求プリミティブの
VLAN分類パラメータの最終的なVID値
を使用する
418
フレームを解読し、フォワーディング
およびラーニングプロセスに送る

【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/02905

**A. CLASSIFICATION OF SUBJECT MATTER**
IPC(7) : H04L 12/28
US CL : 370/256, 397, 395.3, 395.31, 395.52, 399, 401, 409
According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 370/256, 397, 395.3, 395.31, 395.52, 399, 401, 409

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST Database

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 6,317,438 B1 (TREBES, Jr.) 13 November 2001(13.11.2001), see the entire document. | 1-12 |
| Y | US 6,304,575 B1 (CARROLL et al) 16 October 2001 (16.10.2001), see the entire document. | 1-12 |
| Y | U 6,032,194 A (GAI et al.) 29 February 2000 (29.02.2000), see the entire document. | 12-25 |
| Y | US 6,085,238 A (YUASA et al) 04 July 2000 (04.07.2000), see the entire document. | 12-25 |
| A | US 6,311,276 B1 (CONNERY et al) 30 October 2001 (30.10.2001), see the entire document. | 12-25 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 29 April 2002 (29.04.2002) | 23 MAY 2002 |
| Name and mailing address of the ISA/US<br>Commissioner of Patents and Trademarks<br>Box PCT<br>Washington, D.C. 20231<br>Facsimile No. (703)305-3230 | Authorized officer<br>Toan Nguyen<br>Telephone No. 703-305-9600 |

Form PCT/ISA/210 (second sheet) (July 1998)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CR,CU,CZ,DE,DK,DM,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,NO,NZ,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW

（特許庁注：以下のものは登録商標）
ＥＴＨＥＲＮＥＴ
イーサネット

(72)発明者 ボルパノ デニス マイケル
アメリカ合衆国 ９３９０８ カリフォルニア州 サリーナズ シュガーミル ロード １７５５５

Ｆターム(参考) 5K030 GA15 HA08 HC14 HD03 JL01
5K033 CB06 DA05 DA17 DB10 DB18 EC04

【要約の続き】
かで、標準VLANブリッジを拡張する。パーソナルVLANブリッジがVLAN発見のためのプロトコルを提供するVLAN発見方法、パーソナルVLANブリッジは、ステーションが新しいVLANを供する新しいポートを作成すること、または認証プロトコルを介して既存のVLANを結合することを可能にするVLAN 拡張方法、パーソナルVLANブリッジが、物理ポートごとに1つ以上の論理ポートを維持し、および任意の種類のポートの間でブリッジする論理ポート方法、および、暗号VLAN分離方法。