WAPL におけるハンドオーバの実現方式

山崎　浩司

インターネットをインフラとしたサービスの増加にともない，万博などの展示会，工事現場や，災害発生地区などで一時的に無線 LAN 環境を構築し，ネットワークサービスを提供したい，というニーズがある．無線 LAN 環境構築のためにはアクセスポイント(AP：Access Point)の整備が不可欠である．しかし，現在 AP 間は有線で接続されているのが一般的であり，AP の設置には多大なコストを要するのが現状である．そこで我々は，AP 間を無線化することで，この問題を解決する WAPL (Wireless Access Point Link)を提案している．本稿ではまず，WAPL で使用する AP の実装の報告を行う．次に，WAPL における端末の移動(ハンドオーバ)の方式を検討したので，報告する．

A Realization of Handover on WAPL

Koji Yamazaki

Recently, wireless LAN is used as a resource of broadband Internet service. We want to use this service area temporary. For example world science exposition, construction field, a disaster area, and so on. To expand its service area, we must establish access points. However, access points are connected by the cable now. Therefore, it takes large cost to set up access points. To solve this problem we study WAPL (Wireless Access Point Link). That concept is connecting access points by wireless. In this research, I report implementation of WAPL and its Handover.

１．はじめに

インターネットをインフラとしたサービスの増加，無線 LAN 機能を持つノート PC，PDA(Personal Data Assistance)のモバイル化，日用品化にともない，万博などの展示会，工事現場や，災害発生地区などで一時的に無線 LAN 環境を構築し，ネットワークサービスを提供したい，というニーズがある．無線 LAN 環境構築のためにはアクセスポイント(AP：Access Point)の整備が不可欠である．しかし，現在 AP 間は有線で接続されているのが一般的である．そのため，ネットワークレイアウトの拡張性，柔軟性が乏しく，計画的に AP を設置しなければならないという課題がある．この課題のため，AP の設置には多大な時間とコストを要するのが現状である．そこで現在，AP 間を無線リンクにより網の目状に接続するメッシュネットワークへの取り組みが，広く行われている．図 1 にメッシュネットワークのイメージ図を示す．

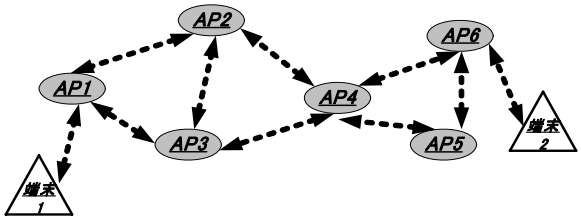


図 1．メッシュネットワークの例

AP 間を無線化することにより得られる利点として，AP 設置の容易性，ネットワークトポロジの柔軟な拡張性，そして，迂回経路を持つことによる通信の高信頼性，の三点が上げられる．これらの利点により，低コストで信頼性のある無線 LAN 環境を短時間で構築することが可能となる．我々は，メッシュネットワークを実現するための一方式として WAPL (Wireless Access Point Link)[1]-[6]を提案している．しかし，現在 WAPL では,WAPL 内での端末の移動(ハンドオーバ)が未検討項目である．そこで本稿では，WAPL のハンドオーバを検討したので報告する．

以下，2 章で従来研究，3 章で WAPL の紹介，

4 章において実装方式について報告し，5 章で WAPL におけるハンドオーバについて述べ，最後に 6 章でまとめを行う．

2. 従来研究

２．１　メッシュネットワーク

メッシュネットワークを提供する既存の技術例として， Tropos Networks 社[7]の Metro Mesh や，Mesh Networks 社[8]の MEA(Mesh Enable Architecture)，また新潟大学の M-WLAN (Multi-Hop Wireless LAN)[9]-[15]が上げられる．Metro Mesh は産能大学湘南キャンパスや米海兵隊岩国基地でインフラとして実際に使用されている．また， MEA は 2004 年に行われた ITS 世界会議のデモで使用された実績がある．いずれも独自の方式でメッシュネットワークを実現しており，詳細な実装方法は明らかにされていない．そのため，他ベンダ製品との相互接続は保障されていないのが現状である．そこで 2004 年 5 月から，802.11s タスク・グループ[16]によりメッシュネットワークの技術標準化が始まったが，標準候補が乱立しており，技術の標準化には時間を要すると考えられる．

２．２　Ｍ－ＷＬＡＮ

図 2 に M-WLAN の構成例を示す．この図は本稿における提案方式 WAPL にも適用できる概念図である．

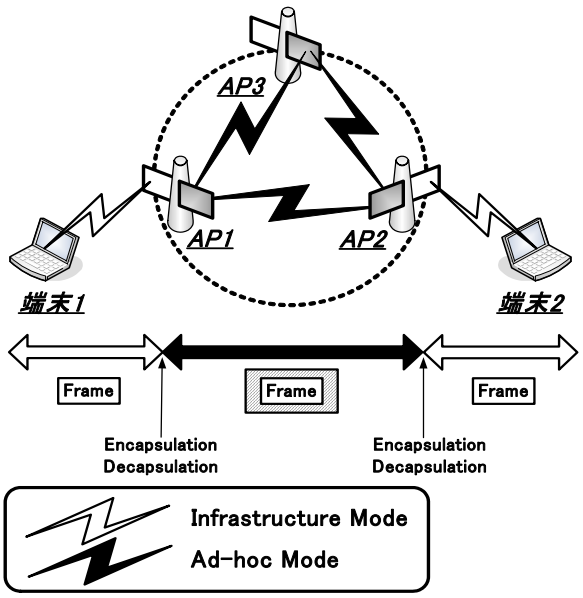


図 2．M-WLAN の構成例

M-WLAN で使用する AP は，無線インタフェースを二つ持つ．一つは配下の端末とインフラストラクチャモードで通信を行う．もう一つは AP どうしで，アドホックモードにより通信を行う．AP 間は，MANET WG (Mobile Ad-hoc Network Working Group) [17]で規定されたアドホックルーチングプロトコルを使用し，パケットをマルチホップでリレー式に転送する．

M-WLAN の実現方式としては，いくつか提案がなされているが，本稿では LAN エミュレーション方式について述べる．LAN エミュレーション方式とは，AP が配下端末から受信した Ethernet フレームを UDP パケットにカプセリングし，目的 AP へと転送する方式である．端末からのフレームをカプセル化するために，AP は宛先端末の MAC アドレスと，宛先端末がアソシエートしている AP のアドホック側の IP アドレスを対応づけた情報が必要である．そのため，AP は，無線レベルでアソシエーションされている端末の MAC アドレスを定期的に全 AP に対してフラッディングする．このフラッディングパケットを受け取った AP は，フラッディングパケットの生成元 IP アドレス(アドホック側の IP アドレス)と，端末の MAC アドレスを独自定義したテーブルに保持･更新する．この動作により，M-WLAN 内の全ての AP は，どの端末が，どの AP の配下に存在するかを把握することが可能となる．この方式は，定期的フラッディングを実現するために MANET WG で標準化されているルーチングプロトコルに改造を加える．よって，ネットワークに合わせた最適なルーチングプロトコルの選択ができない．また，定期的フラッディングを行なうので，システム内のトラヒックが懸念される．

3. WAPL

３．１　ＷＡＰＬの概要

上記課題を解決するため，我々は，WAPL(Wireless Access Point Link)を提案している．WAPL の設計方針として，AP 間通信に必要なルーチングテーブルは，MANET WG で議論されているアドホックルーチングプロトコルをそのまま使用する．これにより，ネットワークに合わせた最適なルーチングプロトコルの選択が可能となる．また，端末からの通信要求があった時点で，オンデマンドで必要なテーブルを作成することとした．この動作により制御トラヒックを大幅に減少することが可能となる．WAPL における AP を以後 WAP(Wireless Access Point)と呼ぶ．WAP は M-WLAN の AP と同様にインタフェースを二

つ持ち, 一つは配下端末とインフラストラクチャモードで通信を行い，もう一つは AP どうしで，アドホックモードにより通信を行う．また WAP 間はカプセル化/デカプセル化を用いて通信を行う． WAPL は，カプセル化を実現するために, 独自に定義したリンクテーブルを保持する. このテーブルは, 通信相手端末の MAC アドレスと, 端末がアソシエーションしている WAP のアドホック側インタフェースの IP アドレスを，対応づけて管理したもので，端末間の通信に先立ち必ず実行される ARP (Address Resolution Protocol)をトリガとして，必要に応じて生成される. WAPL では， WAP 間通信は MANET のルーチングテーブル，カプセル化に必要な情報はリンクテーブル, という二つのテーブルを使用する．これにより WAPL 内の端末数が増加しても，WAP 内のテーブル増加量は最小限におさえられ，WAP 間の制御トラヒックは変化しないという特徴を持つ．WAPL は Ethernet をエミュレートするため，端末は WAPL の存在を意識せず，通信を行うことが可能である．

３．２　リンクテーブルの生成

図 3 に，リンクテーブルが生成される手順を示す. まず, 端末 1, 端末 2 の保持する MAC アドレスを S1，S2，次に，WAP1，WAP2，WAP3 の保持するアドホック側の IP アドレスをそれぞれ W1，W2，W3 とする．端末 1 が端末 2 と通信を開始するとき，端末 1 は端末 2 の MAC アドレスを解決するために，ネットワークに対して必ず ARP Request が実行される．WAP1 は端末 1 からの ARP Request を受信すると，WAP のアドホック側のマルチキャストアドレスでカプセル化をして，他の全 WAP へフラッディングを行なう．WAP2，WAP3 は，ARP Request を受信すると，デカプセル化を行い, 配下のネットワークに転送すると同時に，端末 1 と WAP1 の関連を示すリンクテーブルを生成する． WAP2 は，配下に存在する端末 2 からの ARP Reply を受け取ると, 上記手順で生成したリンクテーブルを参照し，WAP1 の IP アドレスでカプセル化をして WAP1 へ転送する．上記パケットを受信した WAP1 は，デカプセル化を行ない端末 1 に転送すると同時に，端末 2 と WAP2 の関連を示すリンクテーブルを生成する．その後の端末 1 と端末 2 の通信は，生成されたリンクテーブルを参照して行なわれる．

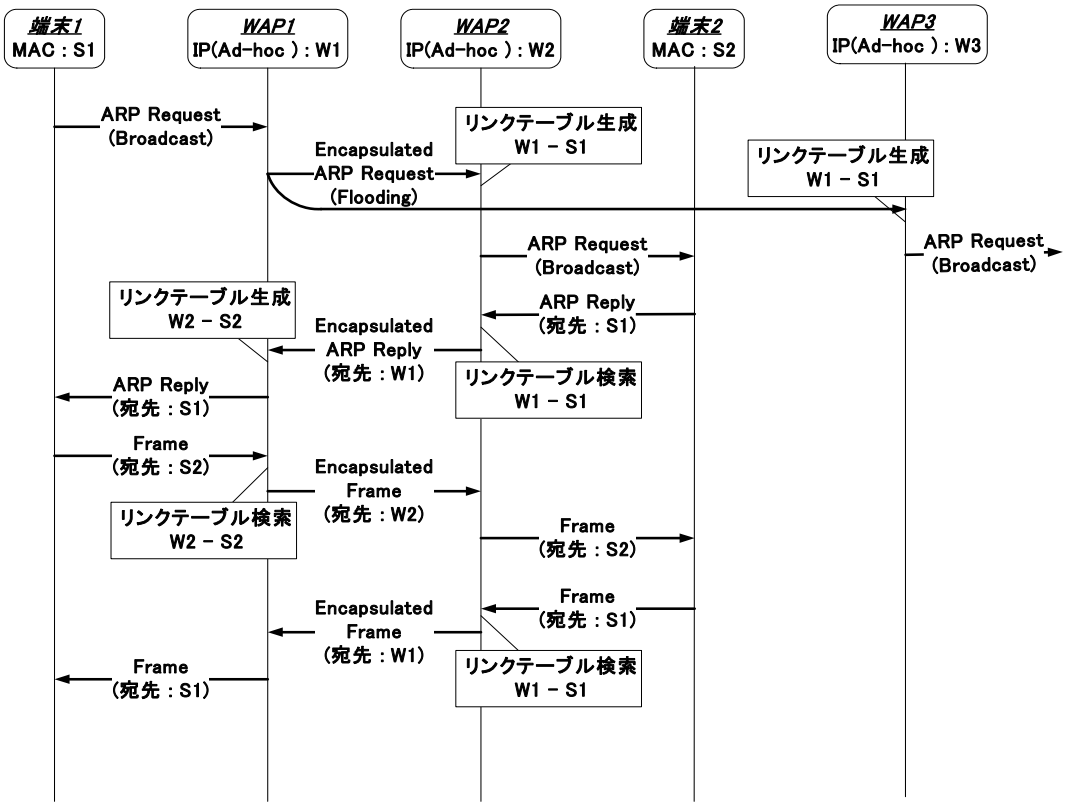


図 3. リンクテーブルの生成

4. WAP の実装

４．１　WAP の構成

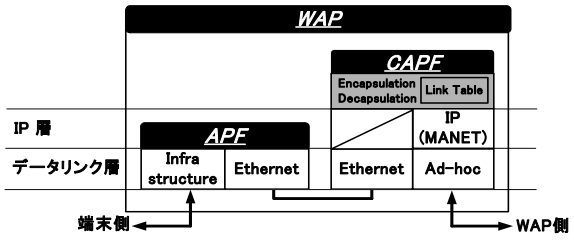


図 4. WAP の構成

図 4 に WAP の構成を示す．WAP は端末に対するインタフェースを提供する APF(Access Point Function)と，カプセル化機能を実行する CAPF(Capsulation Function)から構成される．APF は，端末側のインタフェースで，一般の AP と全く同じ機能を持つ．CAPF は Ethernet とアドホックモード通信を中継する機能であり，リンクテーブルを参照後，Ethernet フレームを IP ヘッダでカプセル化し, Ethernet をエミュレートする．今回の実装では APF には BUFFALO 社製の AP（WLA-G54）をそのまま利用した．CAPF は FreeBSD 5.4-RELEASE を搭載した PC（Epson endeavor NT350）に，カーネルを改造する形で実装を行なった. アドホック側のインタフェースは，PC に内蔵された無線インタフェースを利用した．CAPF 部の Ethernet 側のインタフェースは，AP から送られてくるフレームを全て処理するため, プロミスキャスモードに設定した．WAPL では，MANET のルーチングプロトコルには一切手を加えないので, 用途に合わせて最適なルーチングプロトコを選択することが可能である. 今回の実装では, ルーチングプロトコルにプロアクティブ型の OLSR[18]を採用し，WAP を使用した端末間の 2 ホップ通信が行えることを確認した.

４．２　ＣＡＰＦ詳細

図 5 に CAPF の実装概要を示す．CAPF は，FreeBSD の Ethernet のドライバに改造を加えることにより実現している．点線は，端末が送信した Ethernet フレームを，WAP が受信し，カプセル化後, アドホック側に送信するときの処理，実線は，WAP がアドホック側で，カプセル化された Ethernet フレームを受け取り, デカプセル化後, 端末側へ送信するときの処理を表す. 端末側から受け取った Ethernet フレームは, Ethernet のドライバの入力処理から，そのままアプリケーション層に実装された CAPF に渡される．CAPF は，リンクテーブルを参照後，宛先 WAP のアドホック側の IP アドレスを知り，IP 層に対して送信を指示する．アドホック側で受け取ったカプセル化処理された Ethernet フレームは, IP 層での処理の後, CAPF に渡される．CAPF は，デカプセル化処理を行い，Ethernet フレームを取り出す．このとき，フレームが ARP メッセージの場合，リンクテーブルへの登録処理が行われる．そして Ethernet フレームをデータリンク層の Ethernet のドライバの出力処理へと渡され, 端末側へ送信される.

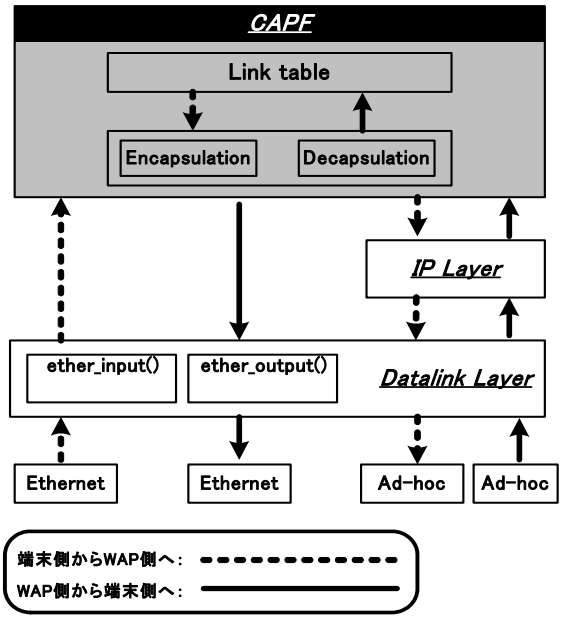


図 5. CAPF の実装概要

5. WAPL のハンドオーバ

WAP 間通信が Ethernet をエミュレートしている点を活かし，WAPL のハンドオーバについて検討した. 図 6 に検討に要した実験機器構成を示す．有線部分のパケットの解析には Ethereal（ Version 0.10.13 ），無線部分のパケットの解析には AirPacMon（Version1.00）を使用した．AP1 と AP2，DHCP サーバ(ゲートウェイ)は Ethernet で接続している．端末の IP アドレスは DHCP サーバから取得する. 端末 1 は AP1，端末 2 は AP2 とそれぞれインフラストラクチャモードによりアソシエーションされている.

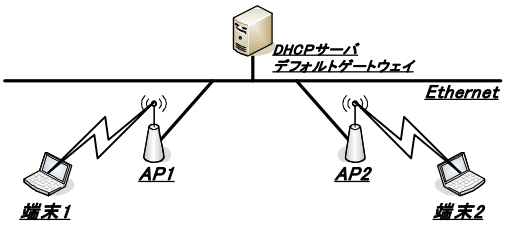


図 6. 実験機器構成

AP は BUFFALO 社製(WLA-G54)を使用し，端末は Windows XP を使用した．各 AP のチャネルと，ESSID（Extended Service Set Identification）は同一とした．ESSID とは，無線 LAN 環境で個々のネットワークの識別に使用する ID である. 端末 1 が端末 2 と通信中に，端末 1 が AP1 の電波範囲外へ物理的に移動を行ない，端末 1 が AP2 へ再参入後，端末 2 との通信が再開するまでのシーケンスを解析した結果を図 7 に示す.

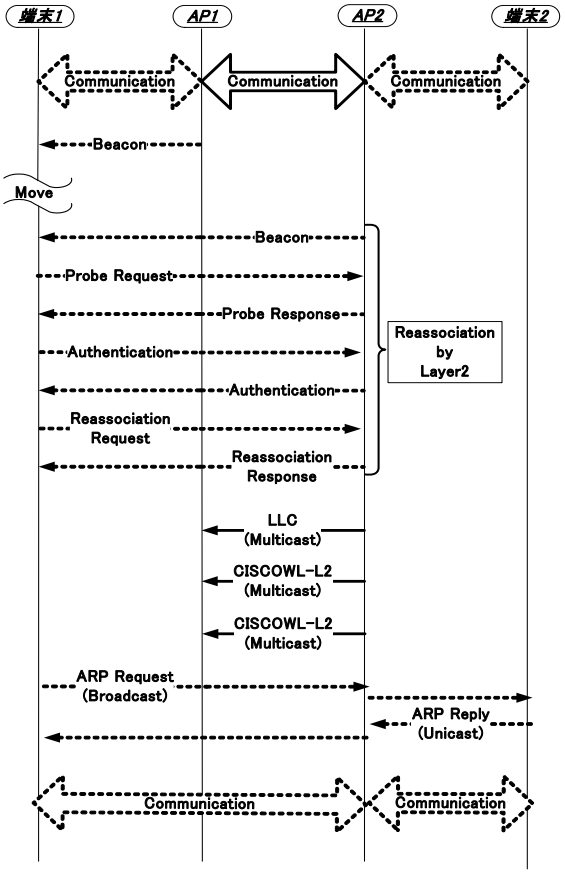


図 7. ハンドオーバのシーケンス

端末 1 が AP1 の電波範囲外へ移動すると，AP1 とのアソシエーションが切断される. このとき端末 1 の保持している ARP キャッシュは消去される．端末 1 はどの AP ともアソシエーションしていないので，接続可能な AP を探すためにスキャニングを行なう. そして，AP2 の存在をビーコンにより検知すると，プローブ要求フレームにより AP2 の存在を確認する．ブローブ要求を受けとった AP2 はプローブ応答フレームを返す．ブローブ応答フレームには AP2 とアソシエートするための設定情報が含まれている. この情報を用いて端末 1 は無線レイヤで，AP2 と認証，再参入を行う．再参入パケットの中には，端末 1 が以前 AP1 とアソシエートしていたという情報が含まれる．端末 1 と AP2 がアソシエーションを張ると，AP2 は端末 1 が再参入してきたことを他の AP へ伝えるために，LLC と CISCOWL-L2 というパケットがマルチキャストされる. CISCOWL-L2 の中には，端末 1 の MAC アドレスと AP2 の MAC アドレスの情報が含まれる．これらのパケットを受けとった AP1 は，端末 1 が配下に存在しているという情報を消去すると考えられる．ハンドオーバに使用されるパケットは，AP のベンダにより多少異なるが，BUFFALO の AP 同士であれば，上記パケットにより各 AP 内のテーブルが即座に書き換えられ，効率的なハンドオーバが実現される． その後，端末 1 は端末 2 のアドレス解決を行なうために ARP Request をネットワーク上に実行し，端末 2 のアドレス解決を行った後に，AP2 を介しての通信を再開する.

WAPL でのハンドオーバについて検討すると，端末は AP とのアソシエーションが切断されると，ARP キャッシュがクリアされる．よって，端末はハンドオーバ後に通信を開始するために必ず ARP を送信する．WAPL ではこの ARP を使用してカプセル化に必要なリンクテーブルの生成を通信開始時に行う. また CAPF の機能により自分とアソシエートしていない端末へのパケットは破棄される. よってハンドオーバ時に AP 間でやり取りされるパケットは，WAPL では不必要なトラヒックとなる．これらのパケットを WAP でブロックし，Ethernet を完全にエミュレートしないことにより，WAPL でのトラヒックの輻輳防止ができると考えられる． このようにして WAPL の環境下においてもハンドオーバを実現し，通信を継続することが可能である.

6. むすび

本稿では，WAP のアーキテクチャと実装方式，および WAPL 内でのハンドオーバの実現方式について検討した. 端末はハンドオーバ後にアドレス解決ために，必ず ARP を送信するので，WAPL ではこの動作を利用し，通信に

先立ちリンクテーブルを生成する. また, CAPF により自分とアソシエートしていない端末へのパケットは破棄されるので, ハンドオーバ時に AP 間でハンドオーバ時にやり取りされるパケットは，WAPL では不必要なトラヒックとなる. これらのパケットを WAP でブロックし, Ethernet を完全にエミュレートしないことにより，WAPL でのトラヒックの輻輳防止ができる．今後は，実機を用いた WAPL の性能評価を行う.

参考文献

[1] 市川祥平， 渡邊晃：アクセスポイントの無線化を実現する WAPL の方式, Dicomo2005，pp. 225-228 (2005-7).

[2] 竹山裕晃 ，渡邊晃：災害時における電子メールを利用した安否通信方法の検討, Dicomo2005，pp. 657-659 (2005-7).

[3] 小島崇広，市川祥平，渡邊晃：無線アクセスポイントリンク“WAPL”の立上げ方式，Dicomo2005，pp. 221-224 (2005-7).

[4] 大石泰大，増田真也，渡邊晃：WAPL を適用した車車間通信の実現，Dicomo2005, pp. 153-156 (2005-7).

[5] 加藤佳之, 大石泰大 増田真也 渡邊晃：WAPL とインターネットの接続に関する検討，電気関係学会東海支部連合大会 (2005-9).

[6] 山崎浩司, 小島崇広 市川祥平 渡邊晃：無線アクセスポイントリンク"WAPL"のアーキテクチャとハンドオーバーの検討, 電気関係学会東海支部連合大会 (2005-9).

[7] http://www.tropos.com/

[8] http://www.meshnetworks.com/

[9] k.Mase,et al. : "Wireless LAN with Wireless Multihop Backbone Network, "IEEE ICWLHN2001,pp349-358 (2001).

[10] 大和田泰伯, 間瀬憲一: WLAN における LAN エミュレータの実装と性能評価, 電気情報通信学会(2002-5).

[11] 大和田泰伯, 間瀬憲一：無線マルチホップ LAN の通信方式の検討とスループット評価，電気情報通信学会(2002-9).

[12] 大和田泰伯, 間瀬憲一：マルチホップ無線 LAN の通信プロトコルの検討と実装, 電気情報通信学会(2003-5).

[13] 大和田泰伯，照井宏康，間瀬憲一：無線マルチホップ LAN のアーキテクチャにおける検討, 電子情報通信学会(2004-11).

[14] 大和田泰伯，間瀬憲一 , et al :大規模アドホックネットワーク・テストベッドの構築電気情報通信学会 (2005-5).

[15] 大和田泰伯，照井宏康 , et al :マルチホップ無線 LAN の部分試作と評価：電気情報通信学会 (2005-9).

[16] http://www.ieee802.org/11/Reports /tgs_update.htm

[17] http://www.ietf.org/html.charters/ manet-charter.html

[18] T.Clausen P.jacquet : "Optimized LinkState Routing Protocol"(OLSR) RFC3626 (2003-10).

謝辞

本研究を行うにあたり，多大なるご指導，ご鞭撻を賜りました渡邊晃教授に心より感謝致します．また有益なご助言，ご検討頂きました渡邊研究室の学部生，学院生の皆様方に深く感謝いたします．特に学院生の皆様方には私からの度重なる質問や疑問に対し丁寧に答えて頂き，誠に感謝致します．

Appendix：ハンドオーバ報告書

名城大学　理工学部　情報科学科　渡邊研究室
山崎 浩司

※ この資料はハンドオーバの実験を行い，その結果を考察したものです．資料について不明な点，改良点がございましたら，山崎まで問い合わせください．

Email：　m0632032@ccmailg.meijo-u.ac.jp

目次

1. はじめに

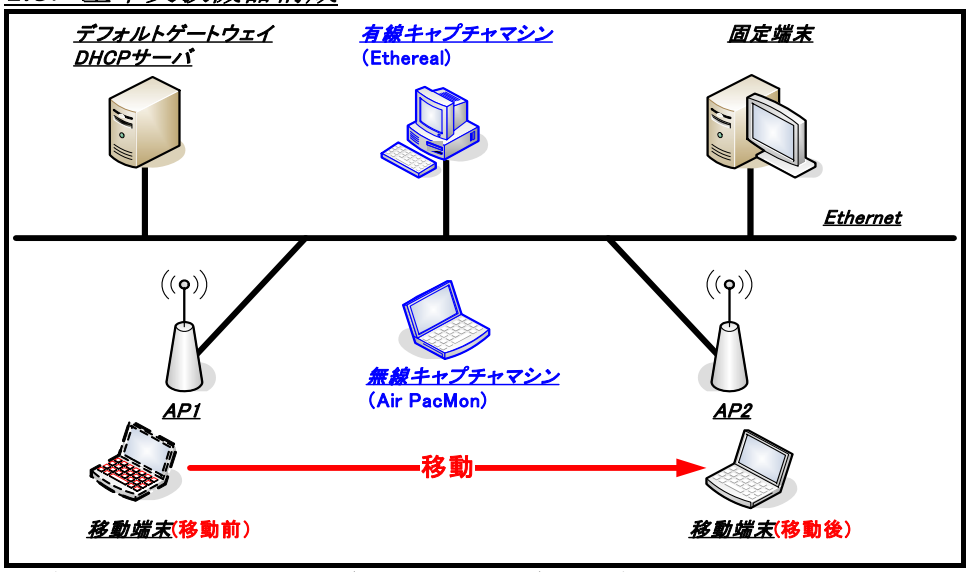
1.1. 実験の目的

・既存のハンドオーバ（アクセスポイント（Access Point：AP）の切り替え）を徹底的に調査.
・調査により，既存のハンドオーバの手順が，現在研究室で開発中のシステムに適用できるかを検討.

1.2. 資料概要

・移動端末が AP1 経由で，固定端末と通信をしているときに，AP1 から AP2 へハンドオーバ(移動端末が AP1 の電波範囲外に移動し，AP1 から離脱後，AP2 へ参入)後，固定端末との通信を再開するまでの間に有線，無線上にどのようなパケットが流れるのかを調査を行なった資料.
・実験後，得られた実験結果より考察を行い，ハンドオーバのシーケンス図を描いた資料.

1.3. 基本実験機器構成



・デフォルトゲートウェイ(DHCP サーバ)，有線キャプチャマシン，固定端末，AP1，AP2 は Ethernet で接続.
・移動端末は AP1，AP2 のどちらか一方に対して，インフラストラクチャモードで接続.
・無線キャプチャマシンは，移動端末，AP1，AP2 の電波をキャプチャできる範囲に置いた.
・移動端末，固定端末は DHCP サーバから IP アドレスを取得する.
・その他の機器には，あらかじめ IP アドレスを割り当てた.

1.4. 実験概要

・まず移動端末が固定端末と AP1 を介した ICMP メッセージのやり取りを行っている.
・このとき，移動端末を AP1 の電波圏外へ物理的に移動を行い，AP1 とのアソシエーションを切断させた後に，AP2 と再接続させた.（ハンドオーバ）
・AP1 から AP2 へハンドオーバしたときに流れるパケットを有線，無線上でそれぞれキャプチャを行なった.
・有線上に流れるパケットは Ethereal Version 0.10.13 (Ethereal 社) でキャプチャを行なった.
・無線上に流れるパケットは AirPacMon V1.00 (corega 社) でキャプチャを行なった.
・以後，機器構成として描いた図には，有線，無線上のキャプチャマシンを明記しないが，キャプチャマシンはあるものとする.

2. 実験内容

・実験は，各 5 回ずつ行った.

2.1. 実験 1

・テーマ　：BUFFALO 社製の AP を使用したハンドオーバ実験.
・目的　：既存に市販されている製品で，ハンドオーバ可能なのかを調査した.
・条件　：AP1，AP2 は，BUFFALO 社製のものを使用.
　：AP1，AP2 の ESSID*は同一に設定.

2.2. 実験 2

・テーマ　：実験 1 との比較実験.
　：ESSID の設定の違いによるハンドオーバ実験.
・目的　：ESSID の設定の違いにより，ハンドオーバ時の動作に変化があるのかを調査した.
・条件　：実験 1 の機器構成で ESSID のみを変更.
　：AP1，AP2 の ESSID はそれぞれ異なるものに設定.

2.3. 実験 3

・テーマ　：実験 1 との比較実験.
　：PLANEX 社製の AP を使用したハンドオーバ実験.
・目的　：AP を作成しているチップベンダの違いにより，シーケンスが変化するのかを調査した.
・条件　：実験 1 の機器構成で AP1，AP2 の機器のみを変更.
　：AP1，AP2 は，PLANEX 社製のものを使用.
　：この製品は IAPP**対応.

2.4. 実験 4

・テーマ　：実験 1 との比較実験.
　：単体の AP に対して再接続を行った実験.
・目的　：AP1→AP2 へとハンドオーバと，単体の AP1 に再接続するときの動作の違いを調査した.
・条件　：実験 1 の機器構成から，AP2 のみを取り外した.

*ESSID(Extended Service Set Identification)
・無線 LAN 環境で，個々のネットワークの識別に使う ID.
・AP と端末がインフラストラクチャモードで通信し合うには，この ID が一致することが条件.
・無線 LAN のネットワークを，論理的にグループ分けする役割を持つ.
・無線 AP や無線 LAN 端末で設定することができ，同じ ESSID を持つ装置間でのみ通信を行うことが可能.
・ESSID には，半角英数字の 32 文字までの任意の名前を付けることができる.

**IAPP(Inter Access Point Protocol)
・IEEE802.11f で定義された，AP 間通信プロトコル.
・異なるベンダ製の AP 間で，端末がアクセスポイントを切り替えられる機能をサポート.
・AP 間で，端末情報の交換を行うための手順を規定.

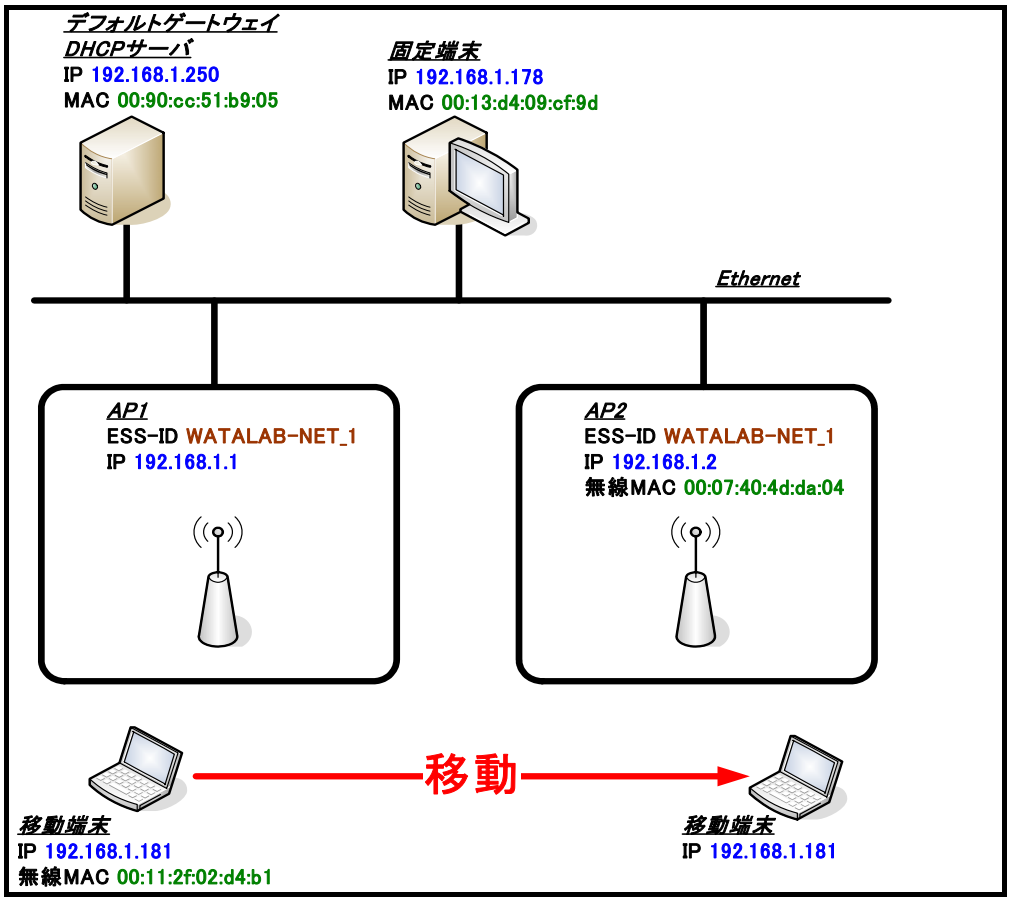
3. 機器構成，実験結果，考察，シーケンス図

3.1. 実験 1

・BUFFALO 製の AP を使用したハンドオーバ実験.

3.1.1. 機器構成

・AP1，AP2 の ESSID 同一.
　　ESSID は，“WATALAB-NET_1” とした.
・アドレス空間：192.168.1.0 / 24



	OS	CPU	Memory
移動端末	WindowsXP	Intel(R)Pentium(R) 1.80GHz	504MB
固定端末	WindowsXP	Intel(R)Pentium(R) 1.70GHz	504MB
デフォルトゲートウェイ DHCP サーバ	FreeBSD	Intel(R)Celeron(R) 1.70GHz	511MB

	機器ベンダ	使用物理レイヤ	使用チャネル
AP1	BUFFALO Air Station WLA-G54	IEEE802.11b	8ch
AP2			

HUB	NetAgent 100BASE-TX 8 ポート Repeater 「IDS-HUB」

3.1.2. 実験結果

・2 種類の実験結果を得た.
・以後，得られた結果に基づき，A，B と，実験結果，考察，シーケンス図，を分けて描く.

3.1.2.A 実験結果

・A の実験結果は 5 回中 3 回得た.

・AirPacMon の実験結果

No	時間情報	通信レート	チャンネル	MACフレーム	BSSID	送信元ステーションアドレス	送信先ステーションアドレス
1239	38.505	1Mbps	8	データ	0090CC0F6B96	000874A01ED0	FFFFFFFFFFFF
1240	38.505	1Mbps	8	データ	0090CC0F77CC	000874A01ED0	FFFFFFFFFFFF
1241	38.745	1Mbps	8	プローブ要求	0007404DDA04	移動端末	AP2_BUFFALO_無線MAC
1242	38.745	1Mbps	8	ACK			
1243	38.745	1Mbps	8	プローブ応答	0007404DDA04	AP2_BUFFALO_無線MAC	移動端末
1244	38.745	1Mbps	8	ACK			
1245	38.745	1Mbps	8	認証	0007404DDA04	移動端末	AP2_BUFFALO_無線MAC
1246	38.745	1Mbps	8	ACK			
1247	38.745	1Mbps	8	認証	0007404DDA04	AP2_BUFFALO_無線MAC	移動端末
1248	38.745	1Mbps	8	ACK			
1249	38.745	1Mbps	8	参入要求	0007404DDA04	移動端末	AP2_BUFFALO_無線MAC
1250	38.745	1Mbps	8	ACK			
1251	38.755	1Mbps	8	参入確認	0007404DDA04	AP2_BUFFALO_無線MAC	移動端末
1252	38.755	1Mbps	8	ACK			

・Ethereal の実験結果

No.	Time	Source	Destination	Protocol	Info
51	27.509516	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
52	27.509849	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
53	33.011933	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
54	33.012298	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
55	37.047958	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	FC	[Malformed Packet]
56	38.508436	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
57	38.508805	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
58	38.977395	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.250? Tell 192.168.1.181
59	38.977456	00:90:cc:51:b9:05	00:11:2f:02:d4:b1	ARP	192.168.1.250 is at 00:90:cc:51:b9:05
60	38.979022	192.168.1.181	192.168.1.250	ICMP	Echo (ping) request
61	38.979091	192.168.1.250	192.168.1.181	ICMP	Echo (ping) reply
62	39.508737	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.178? Tell 192.168.1.181
63	39.508977	00:13:d4:09:cf:9d	00:11:2f:02:d4:b1	ARP	192.168.1.178 is at 00:13:d4:09:cf:9d
64	39.510833	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
65	39.511183	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
66	40.508349	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
67	40.508694	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply

※実験結果の時間軸について

・AirPacMon の実験結果の時間軸と，Ethereal の実験結果の時間軸のズレは，プラスマイナス 2 秒の範囲内にある.
・以後の AirPacMon のデータも同様.

・パケット No.55 の FC の中身

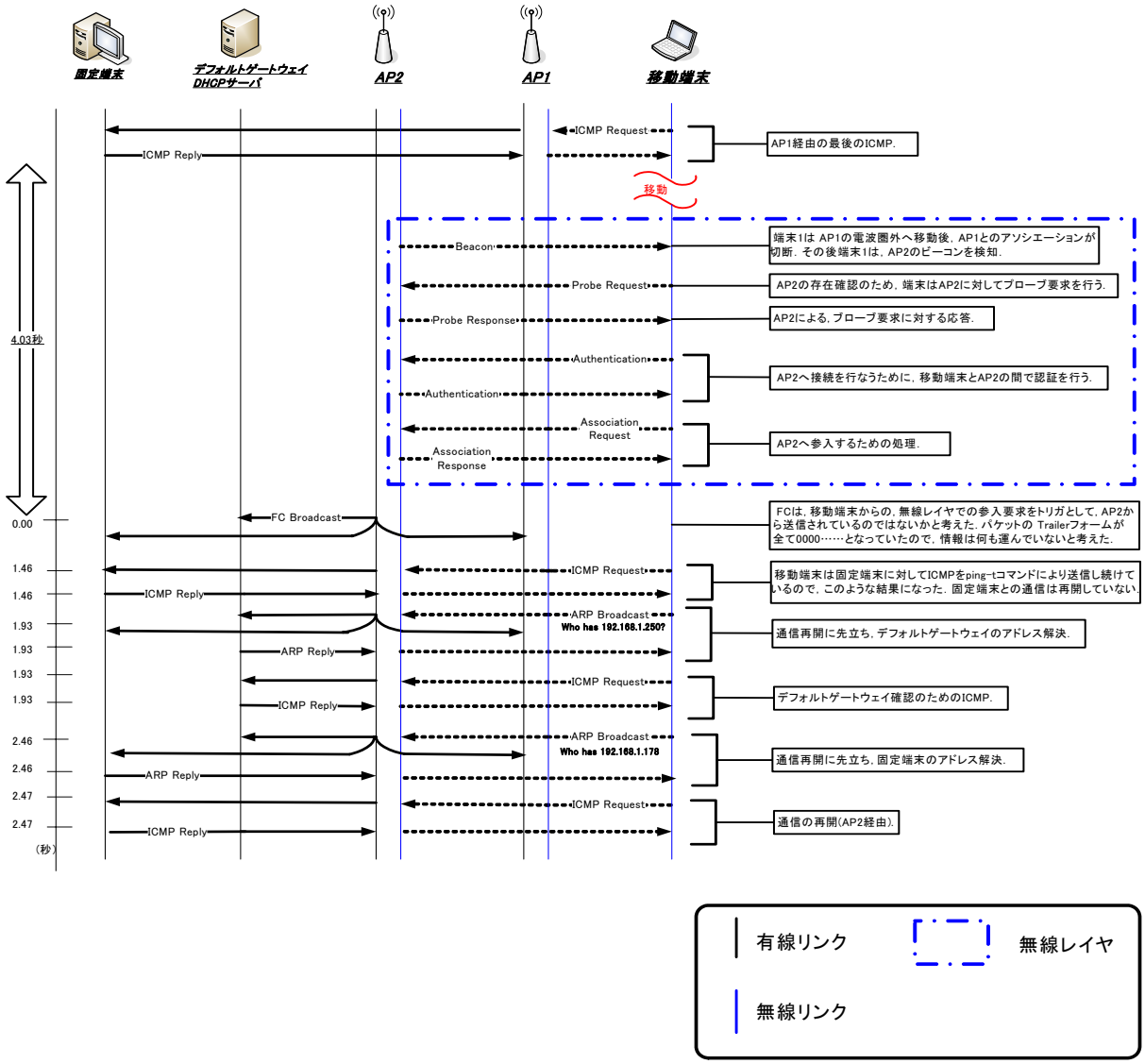
```
⊟ Frame 55 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Nov 23, 2005 16:09:36.388689000
    [Time delta from previous packet: 4.035660000 seconds]
    [Time since reference or first frame: 37.047958000 seconds]
    Frame Number: 55
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    [Protocols in frame: eth:mdshdr:fc]
⊟ Ethernet II, Src: 192.168.1.181 (00:11:2f:02:d4:b1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 192.168.1.181 (00:11:2f:02:d4:b1)
    Type: Unknown (0x0000)
    Trailer: 00000000000000000000000000000000000000000000000000...
⊟ MDS Header(Unknown(0)/Unknown(0))
  ⊟ MDS Header
      ...0 0000 0000 0000 = Packet Len: 0
      .... 0000 0000 00.. = Dst Index: 0x0000
      .... ..00 0000 0000 = Src Index: 0x0000
      .... 0000 0000 0000 = VSAN: 0
  ⊟ MDS Trailer
      EOF: Unknown (0)
      CRC: 0x00000000
  [Malformed Packet: FC]
```

```
0000  ff ff ff ff ff ff 00 11  2f 02 d4 b1 00 00 00 00   ........ /.......
0010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....
```

3.1.3.A 考察

No.	考察
53 54	移動端末が AP1 経由で固定端末に対して ICMP を送受信. この後、移動端末は AP1 の電波圏外へ物理的に移動を行い，AP1 から離脱する.
55	移動端末が，AP1 から離脱後 4.03 秒後にネットワーク上に FC がブロードキャスト. FC は，移動端末が AP1 から離脱したことをトリガとして出るのか，AP2 へ無線レイヤで参入したことをトリガとして出るのかは不明．今回は，移動端末が無線レイヤで AP2 へ参入した後に出るものと考えた. Ethereal の結果を見る限りでは，FC の送信元は移動端末となっているが，AirPacMon の結果に FC は現れなかった．よって FC は，無線レイヤで，移動端末から参入要求パケットを受け取ったことをトリガとして，AP2 が移動端末の MAC アドレスから送信しているように見せかけて，FC を送信しているのではないかと考えた. また，パケットの Trailer フォームが全て 0000……となっていたので，情報は何も運んでいないと考えた.
56 57	移動端末が AP2 経由で固定端末に対して，ICMP を送受信. 固定端末に対しての再接続動作は終了していないが，移動端末は固定端末に対して ICMP メッセージを ping -t コマンドにより送信し続けているので，このような結果を得たと考えた.
58 59	移動端末からの ARP. デフォルトゲートウェイのアドレス解決を行っている.
60 61	移動端末から，デフォルトゲートウェイへの ICMP. デフォルトゲートウェイの確認を行っている.
62 63	移動端末からの ARP. 固定端末のアドレス解決を行っている.
64 65	移動端末の固定端末に対しての再接続動作が終了. 移動端末は，AP2 を介して固定端末との通信を再開する.

3.1.4.A シーケンス図



※図の時間軸について

・縦軸の時間は，Ethereal の時間軸を参考に，移動端末がレイヤ 3 で AP2 に再接続を行い始めたときを 0 秒として記述した．

・実験結果の小数点二桁までを有効範囲として計算した．以後のシーケンス図の時間軸も同様．

3.1.2.B.　実験結果

・B の実験結果は 5 回中 2 回得た.

・AirPacMon の実験結果

No	時間情報	通信レート	チャンネル	MACフレーム	BSSID	送信元ステーションアドレス	送信先ステーションアドレス
2014	52.075	1Mbps	8	データ	0090CC0F77CC	000130121560	FFFFFFFFFFFF
2015	52.205	11Mbps	8	データ	000000000000	0090C7340A04	FFFFFFFFFFFF
2016	52.345	1Mbps	8	プローブ要求	0007404DDA04	移動端末	AP2_BUFFALO_無線MAC
2017	52.345	1Mbps	8	ACK			
2018	52.345	1Mbps	8	プローブ応答	0007404DDA04	AP2_BUFFALO_無線MAC	移動端末
2019	52.345	1Mbps	8	ACK			
2020	52.345	1Mbps	8	認証	0007404DDA04	移動端末	AP2_BUFFALO_無線MAC
2021	52.345	1Mbps	8	ACK			
2022	52.345	1Mbps	8	認証	0007404DDA04	AP2_BUFFALO_無線MAC	移動端末
2023	52.345	1Mbps	8	ACK			
2024	52.345	1Mbps	8	再参入要求	0007404DDA04	移動端末	AP2_BUFFALO_無線MAC
2025	52.345	1Mbps	8	ACK			
2026	52.355	1Mbps	8	再参入確認	0007404DDA04	AP2_BUFFALO_無線MAC	移動端末
2027	52.355	1Mbps	8	ACK			

・Ethereal の実験結果

No.	Time	Source	Destination	Protocol	Info
98	48.217610	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
99	48.217948	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
100	49.217808	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
101	49.217972	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
102	51.101089	00:11:2f:02:d4:b1	01:60:1d:00:01:00	LLC	U, func=UI; SNAP, OUI 0x00601D (Unknown), PID 0x0001
103	51.101208	00:11:2f:02:d4:b1	01:40:96:ff:ff:00	CISCOWL-	CISCOWL-L2
104	51.101323	00:07:40:4d:da:04	01:40:96:ff:ff:00	CISCOWL-	CISCOWL-L2
105	52.686386	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.250? Tell 192.168.1.181
106	52.686442	00:90:cc:51:b9:05	00:11:2f:02:d4:b1	ARP	192.168.1.250 is at 00:90:cc:51:b9:05
107	52.689541	192.168.1.181	192.168.1.250	ICMP	Echo (ping) request
108	52.689615	192.168.1.250	192.168.1.181	ICMP	Echo (ping) reply
109	54.717396	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.178? Tell 192.168.1.181
110	54.717652	00:13:d4:09:cf:9d	00:11:2f:02:d4:b1	ARP	192.168.1.178 is at 00:13:d4:09:cf:9d
111	54.725872	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
112	54.726258	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
113	55.717280	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
114	55.717629	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply

・パケット No.102 の LLC(Logical Link Control)の中身

```
⊟ Frame 102 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Nov 23, 2005 16:57:11.674342000
    [Time delta from previous packet: 1.883117000 seconds]
    [Time since reference or first frame: 51.101089000 seconds]
    Frame Number: 102
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    [Protocols in frame: eth:llc:data]
⊟ IEEE 802.3 Ethernet
    Destination: 01:60:1d:00:01:00 (01:60:1d:00:01:00)
    Source: 192.168.1.181 (00:11:2f:02:d4:b1)
    Length: 46
⊟ Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
  ⊟ Control field: U, func=UI (0x03)
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x03)
    Organization Code: Unknown (0x00601d)
    Protocol ID: 0x0001
  Data (38 bytes)
```

```
0000  01 60 1d 00 01 00 00 11  2f 02 d4 b1 00 2e aa aa   .`...... /.......
0010  03 00 60 1d 00 01 00 04  4c 75 63 65 6e 74 20 54   ..`..... Lucent T
0020  65 63 68 6e 6f 6c 6f 67  69 65 73 20 53 74 61 74   echnolog ies Stat
0030  69 6f 6e 20 41 6e 6e 6f  75 6e 63 65              ion Anno unce
```

・パケット No.103 の CISCOWL-L2 の中身

```
Frame 103 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Nov 23, 2005 16:57:11.674461000
    [Time delta from previous packet: 0.000119000 seconds]
    [Time since reference or first frame: 51.101208000 seconds]
    Frame Number: 103
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    [Protocols in frame: eth:llc:ciscowl]
IEEE 802.3 Ethernet
    Destination: 01:40:96:ff:ff:00 (01:40:96:ff:ff:00)
    Source: 192.168.1.181 (00:11:2f:02:d4:b1)
    Length: 42
    Trailer: 00000000
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
  Control field: U, func=UI (0x03)
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x03)
    Organization Code: Cisco Wireless (Aironet) L2 (0x004096)
    PID: CiscoWL (0x0000)
Cisco Wireless Layer 2
    Length: 34
    Type: 0x0202
    Dst MAC: 01:40:96:ff:ff:00 (01:40:96:ff:ff:00)
    Src MAC: 192.168.1.181 (00:11:2f:02:d4:b1)
    Some MAC: 192.168.1.181 (00:11:2f:02:d4:b1)
    Rest: 0007404DDA040007404DDA04
```

```
0000  01 40 96 ff ff 00 00 11  2f 02 d4 b1 00 2a aa aa   .@...... /....*..
0010  03 00 40 96 00 00 00 22  02 02 01 40 96 ff ff 00   ..@...." ...@....
0020  00 11 2f 02 d4 b1 00 11  2f 02 d4 b1 00 07 40 4d   ../..... /.....@M
0030  da 04 00 07 40 4d da 04  00 00 00 00               ....@M.. ....
```

・パケット No.104 の CISCOWL-L2 の中身

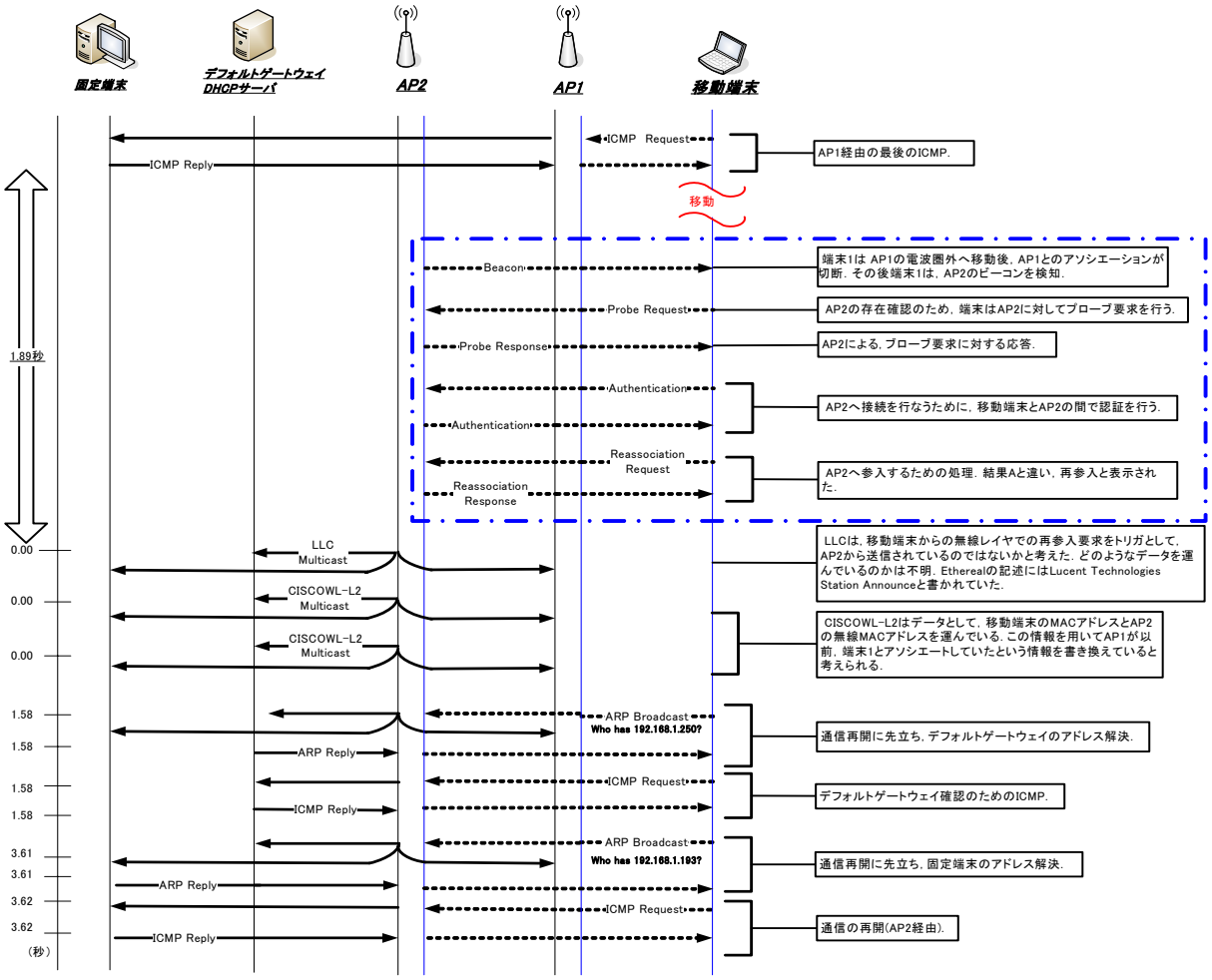
```
⊟ Frame 104 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Nov 23, 2005 16:57:11.674576000
    [Time delta from previous packet: 0.000115000 seconds]
    [Time since reference or first frame: 51.101323000 seconds]
    Frame Number: 104
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    [Protocols in frame: eth:llc:ciscowl]
⊟ IEEE 802.3 Ethernet
    Destination: 01:40:96:ff:ff:00 (01:40:96:ff:ff:00)
    Source: Melco_4d:da:04 (00:07:40:4d:da:04)
    Length: 42
    Trailer: 00000000
⊟ Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
  ⊟ Control field: U, func=UI (0x03)
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x03)
    Organization Code: Cisco Wireless (Aironet) L2 (0x004096)
    PID: CiscoWL (0x0000)
⊟ Cisco Wireless Layer 2
    Length: 34
    Type: 0x0202
    Dst MAC: 01:40:96:ff:ff:00 (01:40:96:ff:ff:00)
    Src MAC: Melco_4d:da:04 (00:07:40:4d:da:04)
    Some MAC: 192.168.1.181 (00:11:2f:02:d4:b1)
    Rest: 0007404DDA040007404DDA04

0000  01 40 96 ff ff 00 00 07  40 4d da 04 00 2a aa aa   .@...... @M...*..
0010  03 00 40 96 00 00 00 22  02 02 01 40 96 ff ff 00   ..@...." ...@....
0020  00 07 40 4d da 04 00 11  2f 02 d4 b1 00 07 40 4d   ..@M.... /.....@M
0030  da 04 00 07 40 4d da 04  00 00 00 00               ....@M.. ....
```

3.1.3.B 考察

No.	考察
100 101	移動端末が AP1 経由で固定端末に対して ICMP を送受信. この後、移動端末は AP1 の電波圏外へ物理的に移動を行い，AP1 から離脱する.
102	移動端末が，AP1 から離脱後 1.89 秒後にネットワーク上に LLC が送信. LLC は AP1 から離脱したことをトリガとして出るのか，AP2 へ無線レイヤで参入したことをトリガとして出るのかは不明. 今回は無線レイヤで AP2 へ参入した後に出るものと考えた. Ethereal の結果を見る限りでは，送信元が移動端末となっているが，AirPacMon の結果に LLC は現れなかった．よって，LLC は，移動端末からレイヤ 2 で再参入要求パケットを受け取ったことをトリガとして AP2 が，移動端末の MAC アドレスから送信しているように見せかけて，LLC を送信しているのではないかと考えた. パケットの中身を見たが，どのようなデータを運んでいるのかは不明．Ethereal の記述には Lucent Technologies Station Announce と書かれていた. パケットの宛先は MAC アドレス、01:60:1d:00:01:00．これはデータリンク層レベルでのマルチキャストアドレスを表す.
103	ネットワーク上に CISCOWL-L2 が送信. Cisco とはネットワーク機器ベンダ名で，実験に使用した AP はハンドオーバに，ベンダが独自に定義したパケットを使用していると考えた. Ethereal の結果を見る限りでは，送信元が移動端末となっているが，No102 のパケットと同様に AirPacMon で CISCOWL-L2 がキャプチャできなかった. よって, CISCOWL-L2 は 移動端末の MAC アドレスを知っている AP2 が，移動端末が送信した様に見せかけているのではないかと考えた. パケットの宛先は MAC アドレス、01:40:96:ff:ff:00．これはデータリンク層レベルでのマルチキャストアドレスを表す. データ部分を見てみると, 00 22　02 02 マルチキャストアドレス 移動端末の MAC アドレス　移動端末の MAC アドレス AP2 の無線 MAC アドレス　AP2 の無線 MAC アドレス　という情報を送信. この情報を用いて AP1 が以前, 端末 1 とアソシエートしていたという情報を消去していると考えられる.
104	AP2 が CISCOWL-L2 を送信. パケットの宛先はパケット No.103 と同様. データ部分を見てみると, 00 22　02 02 マルチキャストアドレス AP2 の無線 MAC アドレス　移動端末の MAC アドレス AP2 の無線 MAC アドレス　AP2 の無線 MAC アドレス　という情報を送信. この情報を用いて AP1 が以前, 端末 1 とアソシエートしていたという情報を消去していると考えられる.
105 106	考察 3.1.3.A のパケット No.58，59 と同様の情報のやり取り. 移動端末からの ARP. デフォルトゲートウェイのアドレス解決を行っている.
107 108	考察 3.1.3.A のパケット No.60，61 と同様. 移動端末から，デフォルトゲートウェイへの ICMP. デフォルトゲートウェイの確認を行っている.
109 110	考察 3.1.3.A のパケット No.62，63 と同様. 移動端末からの ARP. 固定端末のアドレス解決を行っている.
111 112	考察 3.1.3.A のパケット No.64，65 と同様. 移動端末の固定端末に対しての再接続動作が終了.

	移動端末は，AP2 を介して固定端末との通信を再開する．

3.1.4.B シーケンス図



3.1.5. シーケンス図 A と B の比較

・AirPacMon の結果を見る限りでは，
　　→レイヤ 2 で参入要求パケットを受け取った AP2 は FC を送信.
　　→レイヤ 2 で再参入要求パケットを受け取った AP2 は LLC 送信となる.
　　→他の部分の動作は実験結果 A，B とも同じ.

・本来のハンドオーバの動作は，再参入要求，応答パケットが観測できた実験結果 B の方であると考えれれる.

・参入要求パケットと再参入要求パケットの違いは，再参入要求フレームには以前，接続していたアクセスポイントの MAC アドレスが入るフィールドがあることである.

3.2. 実験 2

・実験 1 との比較実験.
ESSID の設定の違いによるハンドオーバ実験.
・実験 1 では AP1，AP2 は同一の ESSID を設定したが，実験 2 では ESSID が異なることによりハンドオーバの手順が変わるのではないかと考え実験を行った.

3.2.1. 機器構成

・実験 1 の機器構成からの変更点.
・AP2 の ESSID を変更.
・”WATALAB-NET_1”から”WATALAB-NET_2”とした.
・その他の条件は実験 1 と全て同様.

3.2.2. 実験結果

・AirPacMon の実験結果

No	時間情報	通信ﾚｰﾄ	ﾁｬﾝﾈﾙ	MACﾌﾚｰﾑ	BSSID	送信元ｽﾃｰｼｮﾝｱﾄﾞﾚｽ	送信先ｽﾃｰｼｮﾝｱﾄﾞﾚｽ
4071	113.594	1Mbps	8	ﾃﾞｰﾀ	0090CC0F6B96	0080920A5EFD	FFFFFFFFFFFF
4072	113.594	1Mbps	8	ﾃﾞｰﾀ	0090CC0F77CC	0080920A5EFD	FFFFFFFFFFFF
4073	113.694	1Mbps	8	ﾌﾟﾛｰﾌﾞ要求	0007404DDA04	移動端末	AP2_BUFFALO_無線MAC
4074	113.694	1Mbps	8	ACK			
4075	113.704	1Mbps	8	ﾌﾟﾛｰﾌﾞ応答	0007404DDA04	AP2_BUFFALO_無線MAC	移動端末
4076	113.704	1Mbps	8	ACK			
4077	113.704	1Mbps	8	認証	0007404DDA04	移動端末	AP2_BUFFALO_無線MAC
4078	113.704	1Mbps	8	ACK			
4079	113.704	1Mbps	8	認証	0007404DDA04	AP2_BUFFALO_無線MAC	移動端末
4080	113.704	1Mbps	8	ACK			
4081	113.704	1Mbps	8	参入要求	0007404DDA04	移動端末	AP2_BUFFALO_無線MAC
4082	113.704	1Mbps	8	ACK			
4083	113.704	1Mbps	8	参入確認	0007404DDA04	AP2_BUFFALO_無線MAC	移動端末
4084	113.704	1Mbps	8	ACK			

・Ethereal の実験結果

No.	Time	Source	Destination	Protocol	Info
109	91.120928	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
110	91.121297	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
111	96.622540	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
112	96.622916	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
113	112.270056	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	FC	[Malformed Packet]
114	112.279577	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x22b739ff
115	112.279929	192.168.1.250	192.168.1.181	ICMP	Echo (ping) request
116	112.290356	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x78df5c88
117	112.372465	192.168.1.250	192.168.1.181	DHCP	DHCP Offer - Transaction ID 0x22b739ff
118	116.370587	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x78df5c88
119	116.370962	192.168.1.250	192.168.1.181	DHCP	DHCP Offer - Transaction ID 0x78df5c88
120	116.378461	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x78df5c88
121	116.381422	192.168.1.250	192.168.1.181	DHCP	DHCP ACK - Transaction ID 0x78df5c88
122	116.384957	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
123	117.124722	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
124	117.125777	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
125	117.126142	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
126	118.120592	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
127	118.121618	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
128	118.121973	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
129	119.124499	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
130	119.124839	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
131	119.132803	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
132	119.136458	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.250? Tell 192.168.1.181
133	119.136512	00:90:cc:51:b9:05	00:11:2f:02:d4:b1	ARP	192.168.1.250 is at 00:90:cc:51:b9:05
134	119.137207	192.168.1.181	224.0.0.22	IGMP	V3 Membership Report
135	119.139912	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
136	119.140771	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
137	119.154764	192.168.1.181	255.255.255.255	DHCP	DHCP Inform - Transaction ID 0x649e15c8
138	119.198058	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
139	119.948591	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
140	120.119883	192.168.1.181	224.0.0.22	IGMP	V3 Membership Report
141	120.122428	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
142	120.122787	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
143	120.135099	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
144	120.698871	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
145	121.120579	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
146	121.120908	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
147	121.135460	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
148	121.448616	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
149	122.136035	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
150	122.229355	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
151	122.980089	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
152	123.135078	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
153	123.736665	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
154	124.154461	192.168.1.181	255.255.255.255	DHCP	DHCP Inform - Transaction ID 0x649e15c8
155	124.479842	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
156	125.152597	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
157	125.260472	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
158	125.265686	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
159	126.011598	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
160	126.013173	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
161	126.619746	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
162	126.620089	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
163	126.760364	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
164	126.760977	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
165	127.135346	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
166	127.510892	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
167	127.511483	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
168	127.619320	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
169	127.619637	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
170	128.292550	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
171	128.293269	192.168.1.181	192.168.1.255	BROWSER	Host Announcement WL-ENDEAVOR, Workstation, Server,
172	128.619720	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
173	128.620047	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
174	129.178125	192.168.1.3	255.255.255.255	UDP	Source port: 2061 Destination port: 10260
175	129.180673	192.168.1.3	192.168.1.255	NBDS	Direct_group datagram
176	129.619712	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
177	129.620041	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
178	129.792169	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
179	130.619672	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
180	130.620017	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
181	131.291916	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
182	131.619834	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
183	131.620148	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
184	132.155329	192.168.1.181	192.168.1.250	DNS	Standard query A wpad.exp.wata-lab.meijo-u.ac.jp
185	132.155731	192.168.1.250	192.168.1.181	DNS	Standard query response, No such name
186	132.156220	192.168.1.181	192.168.1.250	DNS	Standard query A wpad.exp.wata-lab.meijo-u.ac.jp
187	132.156612	192.168.1.250	192.168.1.181	DNS	Standard query response, No such name
188	132.158007	192.168.1.181	192.168.1.250	DNS	Standard query A wpad.exp.wata-lab.meijo-u.ac.jp
189	132.158384	192.168.1.250	192.168.1.181	DNS	Standard query response, No such name
190	132.158765	192.168.1.181	192.168.1.250	DNS	Standard query A wpad.exp.wata-lab.meijo-u.ac.jp
191	132.159153	192.168.1.250	192.168.1.181	DNS	Standard query response, No such name
192	132.160383	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
193	132.161932	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
194	132.619620	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
195	132.619949	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
196	132.791686	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
197	132.900618	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
198	132.901206	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
199	133.619599	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
200	133.619928	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
201	133.650573	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
202	133.651189	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
203	134.292026	192.168.1.181	192.168.1.255	BROWSER	Browser Election Request
204	134.620336	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
205	134.620667	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
206	135.291849	192.168.1.181	192.168.1.255	BROWSER	Browser Election Request
207	135.619546	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
208	135.619885	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
209	136.291818	192.168.1.181	192.168.1.255	BROWSER	Browser Election Request
210	136.619525	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
211	136.619856	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply

212	137.291802	192.168.1.181	192.168.1.255	BROWSER	Browser Election Request
213	137.619489	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
214	137.619807	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
215	138.291669	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
216	138.619594	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
217	138.619924	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
218	139.041562	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
219	139.619454	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
220	139.619804	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
221	139.791400	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
222	140.541529	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
223	140.618972	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
224	140.619298	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
225	141.322817	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
226	141.623184	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
227	141.623518	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
228	142.072741	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
229	142.619562	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
230	142.619890	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
231	142.825328	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
232	143.572698	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
233	143.618892	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
234	143.619205	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
235	144.354208	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
236	144.354816	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
237	144.355714	192.168.1.181	192.168.1.255	BROWSER	Domain/Workgroup Announcement WATANABE-LAB, NT
238	144.619335	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
239	144.619661	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
240	145.619317	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
241	145.619662	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply

・Ethereal の結果に対してフィルタの適用

→ESSID が違うネットワークに再接続するので，Windows のアプリケーションが，アソシエーションが切れたことを感知し，ハンドオーバ後に，Windows アプリケーションがコネクションを張るためにさまざまなパケットのやり取りをしていると考えた．今回の考察は，ハンドオーバに必要なパケットについて考察を行いたいので Ethereal の実験結果に以下のフィルタを適用．余分なパケットに対してフィルタを適用して排除した．

```
!( udp.port == 1900 || ip.dst == 224.0.0.22 || udp.port == 53 || udp.port == 137 || udp.port == 138 || udp.port == 10260)
```

・SSDP(Simple Service Discovery Protocol)

No.	Time	Source	Destination	Protocol	Info
131	119.132803	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
136	119.140771	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
149	122.136035	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
156	125.152597	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1

・IGMP(Internet Group Management Protocol)

No.	Time	Source	Destination	Protocol	Info
134	119.137207	192.168.1.181	224.0.0.22	IGMP	V3 Membership Report
140	120.119883	192.168.1.181	224.0.0.22	IGMP	V3 Membership Report

・DNS(Domain Name System)

No.	Time	Source	Destination	Protocol	Info
135	119.139912	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
143	120.135099	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
147	121.135460	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
152	123.135078	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
165	127.135346	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
184	132.155329	192.168.1.181	192.168.1.250	DNS	Standard query A wpad.exp.wata-lab.meijo-u.ac.jp
185	132.155731	192.168.1.250	192.168.1.181	DNS	Standard query response, No such name
186	132.156220	192.168.1.181	192.168.1.250	DNS	Standard query A wpad.exp.wata-lab.meijo-u.ac.jp
187	132.156612	192.168.1.250	192.168.1.181	DNS	Standard query response, No such name
188	132.158007	192.168.1.181	192.168.1.250	DNS	Standard query A wpad.exp.wata-lab.meijo-u.ac.jp
189	132.158384	192.168.1.250	192.168.1.181	DNS	Standard query response, No such name
190	132.158765	192.168.1.181	192.168.1.250	DNS	Standard query A wpad.exp.wata-lab.meijo-u.ac.jp
191	132.159153	192.168.1.250	192.168.1.181	DNS	Standard query response, No such name

・NBNS(NetBIOS Name Service)

No.	Time	Source	Destination	Protocol	Info
138	119.198058	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
139	119.948591	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
144	120.698871	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
148	121.448616	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
150	122.229355	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
151	122.980089	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
153	123.736665	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
155	124.479842	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
157	125.260472	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
158	125.265686	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
159	126.011598	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
160	126.013173	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
163	126.760364	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
164	126.760977	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
166	127.510892	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
167	127.511483	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
192	132.160383	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
193	132.161932	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
197	132.900618	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
198	132.901206	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
201	133.650573	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
202	133.651189	192.168.1.181	192.168.1.255	NBNS	Name query NB WPAD<00>
215	138.291669	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
218	139.041562	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
221	139.791400	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
222	140.541529	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
225	141.322817	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
228	142.072741	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
231	142.825328	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
232	143.572698	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>

・BROWSE

No.	Time	Source	Destination	Protocol	Info
170	128.292550	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
171	128.293269	192.168.1.181	192.168.1.255	BROWSE	Host Announcement WL-ENDEAVOR, Worksta
178	129.792169	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
181	131.291916	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
196	132.791686	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
203	134.292026	192.168.1.181	192.168.1.255	BROWSE	Browser Election Request
206	135.291849	192.168.1.181	192.168.1.255	BROWSE	Browser Election Request
209	136.291818	192.168.1.181	192.168.1.255	BROWSE	Browser Election Request
212	137.291802	192.168.1.181	192.168.1.255	BROWSE	Browser Election Request
235	144.354208	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
236	144.354816	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
237	144.355714	192.168.1.181	192.168.1.255	BROWSE	Domain/Workgroup Announcement WATANABE

・UDP

No.	Time	Source	Destination	Protocol	Info
174	129.178125	192.168.1.3	255.255.255.255	UDP	Source port: 2061 Destination port: 10260

・NBDS(NetBIOS Datagram Service)

No.	Time	Source	Destination	Protocol	Info
175	129.180673	192.168.1.3	192.168.1.255	NBDS	Direct_group datagram

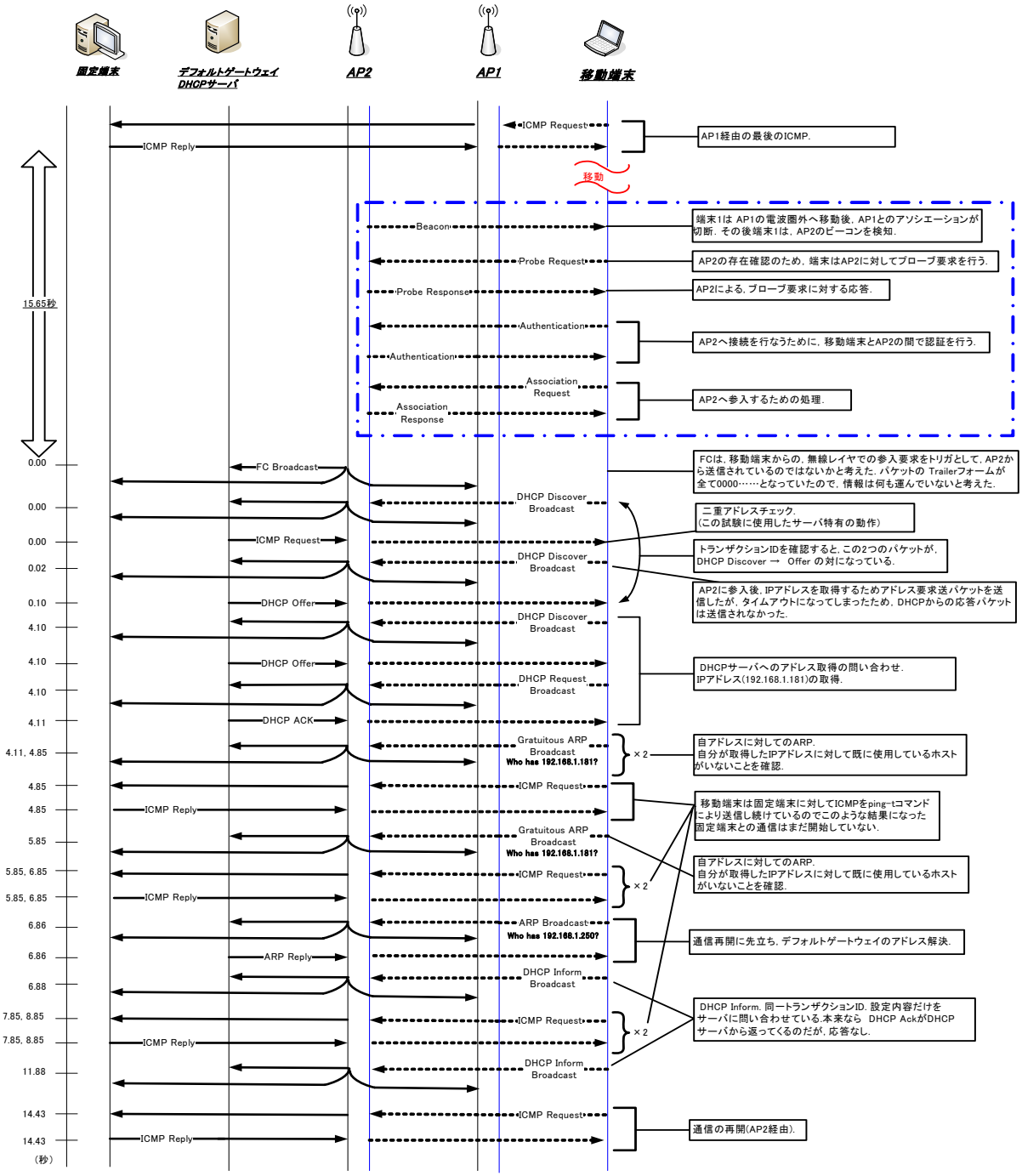
・フィルタ適用後の Ethereal のデータ

No.	Time	Source	Destination	Protocol	Info
109	91.120928	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
110	91.121297	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
111	96.622540	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
112	96.622916	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
113	112.270056	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	FC	[Malformed Packet]
114	112.279577	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x22b739ff
115	112.279929	192.168.1.250	192.168.1.181	ICMP	Echo (ping) request
116	112.290356	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x78df5c88
117	112.372465	192.168.1.250	192.168.1.181	DHCP	DHCP Offer - Transaction ID 0x22b739ff
118	116.370587	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x78df5c88
119	116.370962	192.168.1.250	192.168.1.181	DHCP	DHCP Offer - Transaction ID 0x78df5c88
120	116.378461	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x78df5c88
121	116.381422	192.168.1.250	192.168.1.181	DHCP	DHCP ACK - Transaction ID 0x78df5c88
122	116.384957	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
123	117.124722	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
124	117.125777	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
125	117.126142	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
126	118.120592	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
127	118.121618	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
128	118.121973	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
129	119.124499	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
130	119.124839	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
132	119.136458	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.250? Tell 192.168.1.181
133	119.136512	00:90:cc:51:b9:05	00:11:2f:02:d4:b1	ARP	192.168.1.250 is at 00:90:cc:51:b9:05
137	119.154764	192.168.1.181	255.255.255.255	DHCP	DHCP Inform - Transaction ID 0x649e15c8
141	120.122428	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
142	120.122787	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
145	121.120579	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
146	121.120908	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
154	124.154461	192.168.1.181	255.255.255.255	DHCP	DHCP Inform - Transaction ID 0x649e15c8
161	126.619746	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
162	126.620089	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
168	127.619320	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
169	127.619637	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply

3.2.3. 考察

No.	考察
111 112	移動端末が AP1 経由で固定端末に対して ICMP を送受信. この後、移動端末は AP1 の電波圏外へ物理的に移動を行い，AP1 から離脱する.
113	移動端末が，AP1 から離脱後 15.65 秒後にネットワーク上に FC が送信. 考察 3.1.3.A のパケット No.55 と同様.
114	移動端末からの DHCP Discover – Transaction ID 0x22b739ff
115	DHCP サーバからの二重アドレスチェック. 今回の実験で使用した DHCP サーバ特有の動作.
116	移動端末からの DHCP Discover – Transaction ID 0x78df5c88
117	パケット No.114 と同様の トランザクション ID. DHCP offer – Transaction ID 0x22b739ff のプロセス. この後、Transaction ID 0x22b739ff のプロセスは死亡
118 119 120 121	パケット No.116 と同様の トランザクション ID. Transaction ID 0x78df5c88 のプロセス. 移動端末が DHCP サーバから IP アドレスを取得するための一連の流れ. Discover → Offer → Request → Ack
122 123	移動端末が，自アドレスに対しての ARP を送信. 自分が取得した IP アドレスに対して,既に使用しているホストがいないことを確認している. 応答がないことにより，DHCP サーバから割り振られた IP アドレスが使用可能となる.
124 125	考察 3.1.3.A のパケット No.56，57 と同様. 移動端末が AP2 経由で固定端末に対して，ICMP を送受信. 固定端末に対しての再接続動作は終了していないが，移動端末は固定端末に対して ICMP メッセージを ping -t コマンドにより送信し続けているので,このような結果を得た.
126	パケット No.122，123 の考察と同様.
127 128 129 130	パケット No.124，125 の考察と同様.
132 133	考察 3.1.3.A のパケット No.58，59 と同様. 移動端末からの ARP. デフォルトゲートウェイのアドレス解決を行っている.
137	DHCP Inform – Transaction ID 0x649e15c8 設定内容をサーバに問い合わせている. 本来なら　DHCP Ack が DHCP サーバから返ってくるのだが，応答なし.
141 142 145 146	パケット No124，125 の考察と同様.
154	パケット No.137 の考察と同様. Transaction ID も同一
161 162	考察 3.1.3.A のパケット No.64，65 と同様. 移動端末の固定端末に対しての再接続動作が終了. 移動端末は，AP2 を介して固定端末との通信を再開する.

3.2.4. シーケンス図



3.2.5. 実験 1 のシーケンス図との比較

・AP 間の ESSID が異なる環境で，移動端末がハンドオーバを行うと，端末は異なるネットワークに参入したとみなし，ネットワークに参加するため DHCP の動作により，IP アドレスなどの再設定を行う.

・ESSID が異なる AP 間をハンドオーバすると，上記理由により通信の再開に時間がかかる.

ESSID 同一の場合　→平均 2.96 秒(実験結果 3.1.2.A ． + 実験結果 3.1.2.B. / 2 より).

ESSID 非同一の場合→14.43 秒.

3.3. 実験 3

・実験 1 との比較実験.
  ・PLANEX 社製の AP を使用したハンドオーバ実験.
    ・実験 1 で使用した AP の機器ベンダと違うベンダの製品を使用し，ベンダごとにハンドオーバの手順が違うのではないかを調査を行なった.

3.3.1. 機器構成

・実験 1 の機器構成からの変更点.
    ・AP の機器ベンダを変更.
・使用した AP の詳細

	機器ベンダ	*MAC_Address*
AP1	PLANEX GW-AP11SP	00:90:cc:5a17:fe
AP2		00:90:cc:9f:65:58

・その他の条件は実験 1 と全て同様.

3.3.2. 実験結果

・2 種類の実験結果を得た.
・以後，得られた結果に基づき，A，B と，実験結果，考察，シーケンス図，を分けて描く.

3.3.2.A 実験結果

・A の実験結果は 5 回中 3 回得た.

・Air-PacMon の実験結果
　→移動端末からの認証，参入要求が表示されていないのは，移動端末の電波が微弱なため，AirPacMon でキャプチャできなかったためと考えた.
・四角で囲ってある部分は，AP2 からマルチキャストされたデータ.
　→赤色の部分は，STP(Spanning Tree Protocol)と考えた.
　→青色の部分は，UDP と IAPP.

No	時間情報	通信レート	チャンネル	MACフレーム	BSSID	送信元ステーションアドレス	送信先ステーションアドレス
2018	49.632	11Mbps	8	ﾌﾟﾛｰﾌﾞ応答	0090CC9F6558	AP2_PLANEX_MAC	移動端末
2019	49.942	1Mbps	8	ﾌﾟﾛｰﾌﾞ要求	0090CC9F6558	移動端末	AP2_PLANEX_MAC
2020	49.942	1Mbps	8	ACK			
2021	49.942	11Mbps	8	ﾌﾟﾛｰﾌﾞ応答	0090CC9F6558	AP2_PLANEX_MAC	移動端末
2022	49.942	11Mbps	8	ACK			
2023	49.942	1Mbps	8	ACK			
2024	49.942	11Mbps	8	認証	0090CC9F6558	AP2_PLANEX_MAC	移動端末
2025	49.942	11Mbps	8	ACK			
2026	49.942	1Mbps	8	ACK			
2027	49.942	11Mbps	8	参入確認	0090CC9F6558	AP2_PLANEX_MAC	移動端末
2028	49.942	11Mbps	8	ACK			
2029	50.202	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	移動端末	AP2_PLANEX_MAC
2030	50.202	11Mbps	8	ACK			
2031	50.262	11Mbps	8	ﾃﾞｰﾀ	000000000000	0090C7340A04	FFFFFFFFFFFF
2032	50.433	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	AP2_PLANEX_MAC	0180C2000000
2033	51.434	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	AP2_PLANEX_MAC	0180C2000000
2034	52.436	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	AP2_PLANEX_MAC	0180C2000000
2035	53.237	11Mbps	8	CF-END+...	6B301DBAF338		
2036	53.237	11Mbps	8	ACK			
2037	53.237	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	固定端末	移動端末
2038	53.237	11Mbps	8	ACK			
2039	53.377	11Mbps	8	ﾃﾞｰﾀ	48F8CC9F6558	移動端末	AP2_PLANEX_MAC
2040	53.377	11Mbps	8	ACK			
2041	54.208	11Mbps	8	ACK			
2042	54.208	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	移動端末	FFFFFFFFFFFF
2043	54.208	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	NATFBOX	移動端末
2044	54.208	11Mbps	8	ACK			
2045	54.208	11Mbps	8	ACK			
2046	54.208	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	NATFBOX	移動端末
2047	54.208	11Mbps	8	ACK			
2048	54.238	11Mbps	8	ACK			
2049	54.238	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	移動端末	FFFFFFFFFFFF
2050	54.238	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	固定端末	移動端末
2051	54.238	11Mbps	8	ACK			
2052	54.238	11Mbps	8	ACK			
2053	54.238	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	固定端末	移動端末
2054	54.238	11Mbps	8	ACK			
2055	54.358	11Mbps	8	ACK			
2056	54.438	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	AP2_PLANEX_MAC	0180C2000000
2057	54.469	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	AP2_PLANEX_MAC	01005E0001B2
2058	54.739	11Mbps	8	ﾃﾞｰﾀ	0090CC9F6558	AP2_PLANEX_MAC	FFFFFFFFFFFF

・パケット No.2057，2058 の詳しい情報
　・このパケットが Ethereal の No.103，102 のパケットに対応する.

No	時間情報	送信元ステーションアドレス	送信先ステーションアドレス	トランスポート層プロトコル	送信元ネットワークアドレス	送信先ネットワークアドレス	送信元サービス	送信先サービス
2052	54.238							
2053	54.238	固定端末	移動端末	ICMP (エコー応答)	192.168.1.178	192.168.1.181		
2054	54.238							
2055	54.358							
2056	54.438	AP2_PLANEX_MAC	0180C2000000					
2057	54.469	AP2_PLANEX_MAC	01005E0001B2	UDP	192.168.1.2	224.0.1.178	3517	3517
2058	54.738	AP2_PLANEX_MAC	FFFFFFFFFFFF	UDP	192.168.1.2	192.168.1.255	2313	2313

・Ethereal の実験結果

No.	Time	Source	Destination	Protocol	Info
76	38.066703	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
77	38.067082	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
78	39.079975	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
79	39.080308	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
80	39.194740	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
81	40.006998	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
82	40.007333	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
83	41.194783	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
84	43.194735	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
85	45.194750	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
86	47.194703	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
87	49.194714	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
88	49.194945	00:90:cc:9f:65:58	01:80:c2:00:00:00	STP	Topology Change Notification
89	50.194679	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. TC + Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
90	51.194820	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. TC + Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
91	51.998514	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
92	51.998896	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
93	52.967576	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.250? Tell 192.168.1.181
94	52.967640	00:90:cc:51:b9:05	00:11:2f:02:d4:b1	ARP	192.168.1.250 is at 00:90:cc:51:b9:05
95	52.970084	192.168.1.181	192.168.1.250	ICMP	Echo (ping) request
96	52.970135	192.168.1.250	192.168.1.181	ICMP	Echo (ping) reply
97	52.998000	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.178? Tell 192.168.1.181
98	52.998199	00:13:d4:09:cf:9d	00:11:2f:02:d4:b1	ARP	192.168.1.178 is at 00:13:d4:09:cf:9d
99	53.000625	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
100	53.000941	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
101	53.194710	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. TC + Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
102	53.220720	192.168.1.2	192.168.1.255	IAPP	Announce Request(0) (version=0)
103	53.225030	192.168.1.2	224.0.1.178	UDP	Source port: 3517 Destination port: 3517
104	53.225645	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	LLC	U, func=XID; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
105	53.998877	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
106	53.999213	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
107	54.998264	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
108	54.998619	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply

・パケット No.83 の STP(Spanning Tree Protocol)の中身

```
⊟ Frame 83 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Nov 23, 2005 20:23:11.255534000
    [Time delta from previous packet: 1.187450000 seconds]
    [Time since reference or first frame: 41.194783000 seconds]
    Frame Number: 83
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    [Protocols in frame: eth:llc:stp]
⊟ IEEE 802.3 Ethernet
    Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
    Source: PlanetCo_5a:17:fe (00:90:cc:5a:17:fe)
    Length: 38
    Trailer: A5A5A5A5A5A5A5A5
⊟ Logical-Link Control
    DSAP: Spanning Tree BPDU (0x42)
    IG Bit: Individual
    SSAP: Spanning Tree BPDU (0x42)
    CR Bit: Command
  ⊟ Control field: U, func=UI (0x03)
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x03)
⊟ Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: Spanning Tree (0)
    BPDU Type: Configuration (0x00)
  ⊟ BPDU flags: 0x00
      0... .... = Topology Change Acknowledgment: No
      .... ...0 = Topology Change: No
    Root Identifier: 32768 / 00:90:cc:5a:17:fe
    Root Path Cost: 0
    Bridge Identifier: 32768 / 00:90:cc:5a:17:fe
    Port identifier: 0x8002
    Message Age: 0
    Max Age: 20
    Hello Time: 2
    Forward Delay: 0

0000  01 80 c2 00 00 00 00 90  cc 5a 17 fe 00 26 42 42   ........ .Z...&BB
0010  03 00 00 00 00 00 80 00  00 90 cc 5a 17 fe 00 00   ........ ...Z....
0020  00 00 80 00 00 90 cc 5a  17 fe 80 02 00 00 14 00   .......Z ........
0030  02 00 00 00 a5 a5 a5 a5  a5 a5 a5 a5               ........ ....
```

・No.88 以前の STP は全てこの形式.

・パケット No.88 の STP(Spanning Tree Protocol)の中身

```
⊟ Frame 88 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Nov 23, 2005 20:23:19.255696000
    [Time delta from previous packet: 0.000231000 seconds]
    [Time since reference or first frame: 49.194945000 seconds]
    Frame Number: 88
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    [Protocols in frame: eth:llc:stp:data]
⊟ IEEE 802.3 Ethernet
    Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
    Source: PlanetCo_9f:65:58 (00:90:cc:9f:65:58)
    Length: 7
    Trailer: A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5A5...
⊟ Logical-Link Control
    DSAP: Spanning Tree BPDU (0x42)
    IG Bit: Individual
    SSAP: Spanning Tree BPDU (0x42)
    CR Bit: Command
  ⊟ Control field: U, func=UI (0x03)
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x03)
⊟ Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: Spanning Tree (0)
    BPDU Type: Topology Change Notification (0x80)
```

```
0000  01 80 c2 00 00 00 00 90  cc 9f 65 58 00 07 42 42   ........ ..eX..BB
0010  03 00 00 00 80 a5 a5 a5  a5 a5 a5 a5 a5 a5 a5 a5   ........ ........
0020  a5 a5 a5 a5 a5 a5 a5 a5  a5 a5 a5 a5 a5 a5 a5 a5   ........ ........
0030  a5 a5 a5 a5 a5 a5 a5 a5  a5 a5 a5 a5              ........ ....
```

・この STP を境に，STP のパケットフォーマットが変わる．

・パケット No.89 の STP(Spanning Tree Protocol)の中身

```
Frame 89 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Nov 23, 2005 20:23:20.255430000
    [Time delta from previous packet: 0.999734000 seconds]
    [Time since reference or first frame: 50.194679000 seconds]
    Frame Number: 89
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    [Protocols in frame: eth:llc:stp]
IEEE 802.3 Ethernet
    Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
    Source: PlanetCo_5a:17:fe (00:90:cc:5a:17:fe)
    Length: 38
    Trailer: A5A5A5A5A5A5A5A5
Logical-Link Control
    DSAP: Spanning Tree BPDU (0x42)
    IG Bit: Individual
    SSAP: Spanning Tree BPDU (0x42)
    CR Bit: Command
  Control field: U, func=UI (0x03)
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x03)
Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: Spanning Tree (0)
    BPDU Type: Configuration (0x00)
  BPDU flags: 0x81 (Topology Change Acknowledgment, Topology Change)
      1... .... = Topology Change Acknowledgment: Yes
      .... ...1 = Topology Change: Yes
    Root Identifier: 32768 / 00:90:cc:5a:17:fe
    Root Path Cost: 0
    Bridge Identifier: 32768 / 00:90:cc:5a:17:fe
    Port identifier: 0x8002
    Message Age: 0
    Max Age: 20
    Hello Time: 2
    Forward Delay: 0
```

```
0000  01 80 c2 00 00 00 00 90  cc 5a 17 fe 00 26 42 42   ........ .Z...&BB
0010  03 00 00 00 00 81 80 00  00 90 cc 5a 17 fe 00 00   ........ ...Z....
0020  00 00 80 00 00 90 cc 5a  17 fe 80 02 00 00 14 00   .......Z ........
0030  02 00 00 00 a5 a5 a5 a5  a5 a5 a5 a5               ........ ....
```

・赤色の部分のみがパケット No.83 の STP(Spanning Tree Protocol)と違う.
・このパケットフォーマットが 11 回続いた後に，No.83 のパケットフォーマットに戻った.

・パケット No.102 の IAPP(Inter Access Point Protocol)の中身

```
⊟ Frame 102 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Nov 23, 2005 20:23:23.281471000
    [Time delta from previous packet: 0.026010000 seconds]
    [Time since reference or first frame: 53.220720000 seconds]
    Frame Number: 102
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    [Protocols in frame: eth:ip:udp:iapp]
⊟ Ethernet II, Src: PlanetCo_9f:65:58 (00:90:cc:9f:65:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: PlanetCo_9f:65:58 (00:90:cc:9f:65:58)
    Type: IP (0x0800)
    Trailer: 2020
⊟ Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.255 (192.168.1.255)
    Version: 4
    Header length: 20 bytes
  ⊟ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..0. = ECN-Capable Transport (ECT): 0
      .... ...0 = ECN-CE: 0
    Total Length: 44
    Identification: 0x0000 (0)
  ⊟ Flags: 0x04 (Don't Fragment)
      0... = Reserved bit: Not set
      .1.. = Don't fragment: Set
      ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
  ⊟ Header checksum: 0xb66f [correct]
      [Good: True]
      [Bad : False]
    Source: 192.168.1.2 (192.168.1.2)
    Destination: 192.168.1.255 (192.168.1.255)
⊟ User Datagram Protocol, Src Port: 2313 (2313), Dst Port: 2313 (2313)
    Source port: 2313 (2313)
    Destination port: 2313 (2313)
    Length: 24
    Checksum: 0x5f85 [correct]
⊟ Inter-Access-Point Protocol
    Version: 0
    Type: Announce Request(0)
  ⊟ Protocol data units
      Network Name(0) Value: ""
      PHY Type(16) Value: Proprietary
```

```
0000  ff ff ff ff ff ff 00 90  cc 9f 65 58 08 00 45 00   ........ ..eX..E.
0010  00 2c 00 00 40 00 40 11  b6 6f c0 a8 01 02 c0 a8   .,..@.@. .o......
0020  01 ff 09 09 09 09 00 18  5f 85 00 00 00 00 00 10   ........ _.......
0030  06 00 00 11 2f 02 d4 b1  00 00 20 20               ..../... ..
```

・パケット No.103 の UDP の中身

```
Frame 103 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Nov 23, 2005 20:23:23.285781000
    [Time delta from previous packet: 0.004310000 seconds]
    [Time since reference or first frame: 53.225030000 seconds]
    Frame Number: 103
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: PlanetCo_9f:65:58 (00:90:cc:9f:65:58), Dst: 01:00:5e:00:01:b2 (01:00:5e:00:01:b2)
    Destination: 01:00:5e:00:01:b2 (01:00:5e:00:01:b2)
    Source: PlanetCo_9f:65:58 (00:90:cc:9f:65:58)
    Type: IP (0x0800)
    Trailer: 2020
Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 224.0.1.178 (224.0.1.178)
    Version: 4
    Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..0. = ECN-Capable Transport (ECT): 0
      .... ...0 = ECN-CE: 0
    Total Length: 44
    Identification: 0x0000 (0)
  Flags: 0x04 (Don't Fragment)
      0... = Reserved bit: Not set
      .1.. = Don't fragment: Set
      ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
  Header checksum: 0x9764 [correct]
      [Good: True]
      [Bad : False]
    Source: 192.168.1.2 (192.168.1.2)
    Destination: 224.0.1.178 (224.0.1.178)
User Datagram Protocol, Src Port: 3517 (3517), Dst Port: 3517 (3517)
    Source port: 3517 (3517)
    Destination port: 3517 (3517)
    Length: 24
    Checksum: 0x3712 [correct]
  Data (16 bytes)
```

```
0000  01 00 5e 00 01 b2 00 90  cc 9f 65 58 08 00 45 00   ..^..... ..eX..E.
0010  00 2c 00 00 40 00 40 11  97 64 c0 a8 01 02 e0 00   .,..@.@. .d......
0020  01 b2 0d bd 0d bd 00 18  37 12 00 00 00 00 00 10   ........ 7.......
0030  06 00 00 11 2f 02 d4 b1  00 00 20 20               ..../... ..
```

・パケット No.104 の LLC の中身

```
Frame 104 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Nov 23, 2005 20:23:23.286396000
    [Time delta from previous packet: 0.000615000 seconds]
    [Time since reference or first frame: 53.225645000 seconds]
    Frame Number: 104
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    [Protocols in frame: eth:llc:data]
IEEE 802.3 Ethernet
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 192.168.1.181 (00:11:2f:02:d4:b1)
    Length: 8
    Trailer: 2020202020202020202020202020202020202020202020...
Logical-Link Control
    DSAP: NULL LSAP (0x00)
    IG Bit: Individual
    SSAP: NULL LSAP (0x00)
    CR Bit: Command
  Control field: U, func=XID (0xAF)
      101. 11.. = Command: Exchange identification (0x2b)
      .... ..11 = Frame type: Unnumbered frame (0x03)
  Data (5 bytes)
```

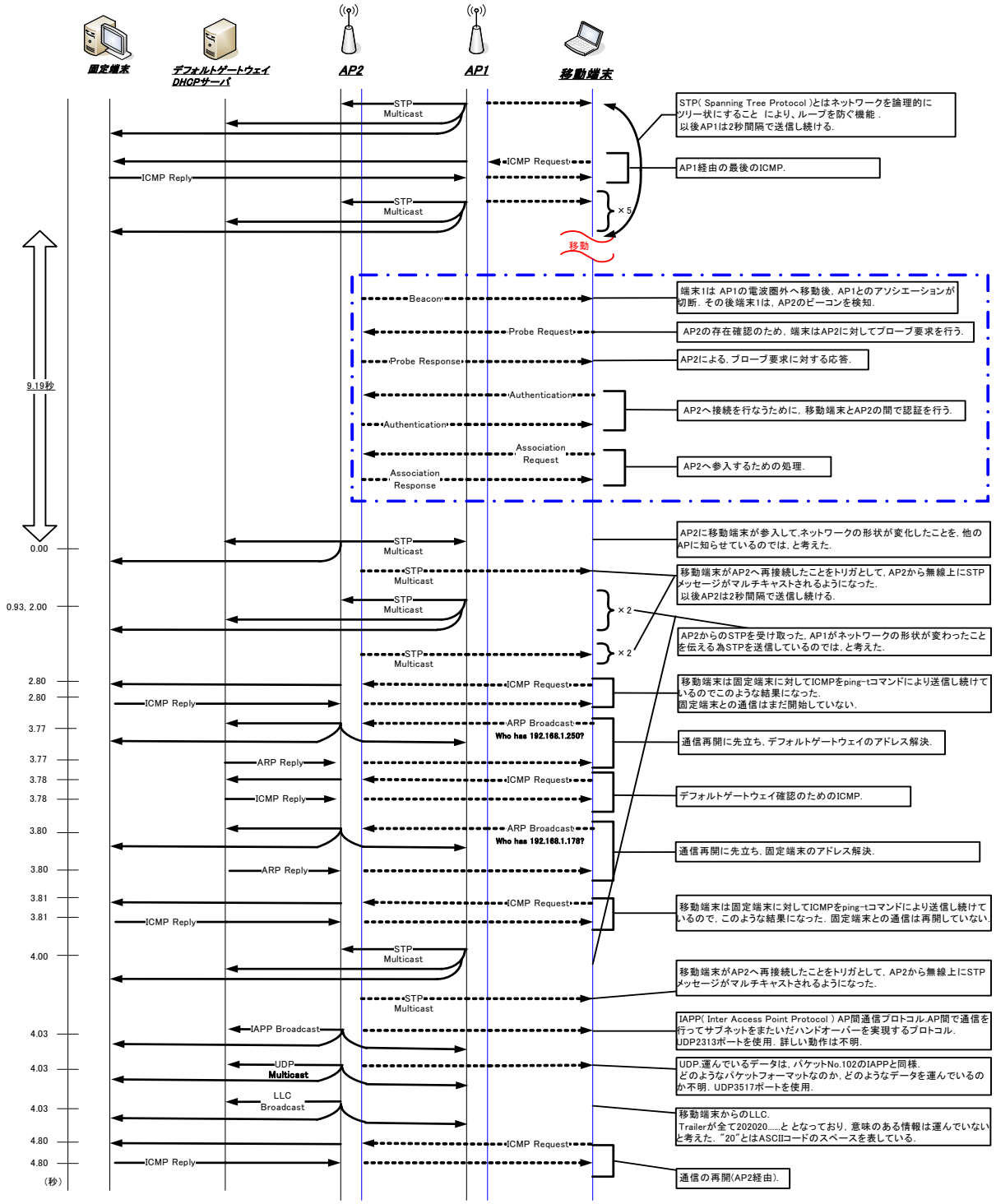
```
0000  ff ff ff ff ff ff 00 11  2f 02 d4 b1 00 08 00 00   ........ /.......
0010  af 81 01 02 20 20 20 20  20 20 20 20 20 20 20 20   ....
0020  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0030  20 20 20 20 20 20 20 20  20 20 20 20
```

3.3.3.A 考察

No.	考察
81 82	移動端末が AP1 経由で固定端末に対して ICMP を送受信. この後、移動端末は AP1 の電波圏外へ物理的に移動を行い，AP1 から離脱する.
83	STP(Spanning Tree Protocol) ネットワークの冗長化に伴う「ブロードキャストストリーム」を防ぐために定期的に送信されるパケット．IEEE802.1d として標準化されている. 送信元の MAC アドレスを見ると，00:90:cc:5a:17:fe と表示されている. この MAC アドレスは AP1 のものである. 2 秒間に一回の割合で AP1 から送信されている. パケットの宛先は MAC アドレス、01:80:c2:00:00:00．これはデータリンク層レベルでのマルチキャストアドレスを表す.以下の STP の宛先アドレスも同様.
84	パケット No.83 の考察と同様.
85	パケット No.83 の考察と同様.
86	パケット No.83 の考察と同様.
87	パケット No.83 の考察と同様.
88	移動端末が AP1 から離脱後，9.19 秒後にネットワーク上に STP が送信. 送信元の MAC アドレスを見ると，00:90:cc:9f:65:58 と表示されている. この MAC アドレスは AP2 のものである. AP2 から有線上に送信された STP はこれのみだった. このパケットを境に，無線上に AP2 から STP がマルチキャストされる.(AirPacMon の結果参照) 有線上の STP が運ぶ情報は Topology Change Notification と表示された. 移動端末が AP2 参入して,ネットワークの形状が変化したことを，他の機器に知らせているのではないかと考えた. また，パケットの Trailer フォームが全て A5A5A5……となっており，意味のある情報を運んでいないと考えた.
89	AP1 からの STP. No.88 の Topology Change Notification を受け取ったことをトリガとして,No.83 の STP が運ぶデータが変化した. No.83 の STP と変化した部分は Topology Change：NO から Topology Change：Yes となり，ネットワークの形状が変わったことをマルチキャストしている. 2 秒間に一回の割合で AP1 から送信されている. 11 回同じメッセージを送信した後に，Topology Change：NO に戻り No.83 と同様の情報を送信するようになった.
90	パケット No.89 の考察と同様
91 92	考察 3.1.3.A のパケット No.56，57 と同様. 移動端末が AP2 経由で固定端末に対して，ICMP を送受信. 固定端末に対しての再接続動作は終了していないが，移動端末は固定端末に対して ICMP メッセージを ping -t コマンドにより送信し続けているので, このような結果を得たと考えた.
93 94	考察 3.1.3.A のパケット No.58，59 と同様. 移動端末からの ARP. デフォルトゲートウェイのアドレス解決を行っている.
95 96	考察 3.1.3.A のパケット No.60，61 と同様. 移動端末から，デフォルトゲートウェイへの ICMP. 移動端末がデフォルトゲートウェイの確認を行っている.
97 98	考察 3.1.3.A のパケット No.62，63 と同様. 移動端末からの ARP. 固定端末のアドレス解決を行っている.

99 100	パケット No.91，92 の考察と同様.
101	パケット No.89 の考察と同様.
102	AP2 からの IAPP(Inter Access Point Protocol) どのようなパケットフォーマットなのか，どのようなデータを運んでいるのか不明.
103	AP2 からの UDP 運んでいるデータは，パケット No.102 の IAPP と同様. どのようなパケットフォーマットなのか，どのようなデータを運んでいるのか不明. 補足情報 AirPacMon の実験結果では, パケット No.104 の UDP パケットの方が, パケット No.103 の IAPP よりも先にキャプチャされた. 原因は不明だが，今回は Ethereal の結果にもとづき，考察，シーケンス図を描く.
104	移動端末からの LLC. LLC は 実験 3.1.2.B でも見たが，実験 3.1.2.B の LLC とは運んでいるデータが異なる. Ethereal の結果を見る限りでは送信元が移動端末となっているが， AirPacMon の結果に LLC は現れなかった．よって，LLC は， AP2 が，移動端末の MAC アドレスから送信しているように見せかけて，LLC を送信しているのではないかと考えた. また，パケットの Trailer フォームが全て 202020……となっており，意味のある情報を運んでいないと考えた.”20”とは ASCII コードのスペースを表している.
105 106	考察 3.1.3.A のパケット No.64，65 と同様. 移動端末の固定端末に対しての再接続動作が終了. 移動端末は，AP2 を介して固定端末との通信を再開する.

3.3.4.A.　シーケンス図


固定端末
デフォルトゲートウェイ
DHCPサーバ
AP2
AP1
移動端末
STP
Multicast
STP(Spanning Tree Protocol)とはネットワークを論理的にツリー状にすること により、ループを防ぐ機能 .
以後AP1は2秒間隔で送信し続ける.
ICMP Request
ICMP Reply
AP1経由の最後のICMP.
× 5
移動
9.19秒
端末1は AP1の電波圏外へ移動後, AP1とのアソシエーションが切断. その後端末1は, AP2のビーコンを検知.
Beacon
Probe Request
AP2の存在確認のため, 端末はAP2に対してプローブ要求を行う.
Probe Response
AP2による, プローブ要求に対する応答.
Authentication
AP2へ接続を行なうために, 移動端末とAP2の間で認証を行う.
Association Request
Association Response
AP2へ参入するための処理.
0.00
AP2に移動端末が参入して,ネットワークの形状が変化したことを, 他のAPに知らせているのでは, と考えた.
移動端末がAP2へ再接続したことをトリガとして, AP2から無線上にSTPメッセージがマルチキャストされるようになった.
以後AP2は2秒間隔で送信し続ける.
0.93, 2.00
× 2
AP2からのSTPを受け取った, AP1がネットワークの形状が変わったことを伝える為STPを送信しているのでは, と考えた.
2.80
2.80
移動端末は固定端末に対してICMPをping -tコマンドにより送信し続けているのでこのような結果になった.
固定端末との通信はまだ開始していない.
3.77
ARP Broadcast
Who has 192.168.1.250?
通信再開に先立ち, デフォルトゲートウェイのアドレス解決.
3.77
ARP Reply
3.78
3.78
デフォルトゲートウェイ確認のためのICMP.
3.80
Who has 192.168.1.178?
通信再開に先立ち, 固定端末のアドレス解決.
3.80
3.81
3.81
移動端末は固定端末に対してICMPをping -tコマンドにより送信し続けているので, このような結果になった. 固定端末との通信は再開していない
4.00
移動端末がAP2へ再接続したことをトリガとして, AP2から無線上にSTPメッセージがマルチキャストされるようになった.
IAPP
Broadcast
IAPP(Inter Access Point Protocol) AP間通信プロトコル.AP間で通信を行ってサブネットをまたいだハンドオーバーを実現するプロトコル.
UDP2313ポートを使用. 詳しい動作は不明.
4.03
UDP
Multicast
UDP.運んでいるデータは, パケットNo.102のIAPPと同様.
どのようなパケットフォーマットなのか, どのようなデータを運んでいるのか不明. UDP3517ポートを使用.
4.03
LLC
Broadcast
4.03
移動端末からのLLC.
Trailerが全て202020.....と となっており, 意味のある情報は運んでいないと考えた. "20"とはASCIIコードのスペースを表している.
4.80
4.80
通信の再開(AP2経由).
（秒）

3.3.2.B 実験結果

・B の実験結果は 5 回中 2 回得た.

・Air-PacMon の実験結果

No	時間情報	通信レート	チャンネル	MACフレーム	BSSID	送信元ステーションアドレス	送信先ステーションアドレス
574	44.684	11Mbps	8	データ	0090CC9F6558	AP2_PLANEX_MAC	0180C2000000
575	44.945	1Mbps	8	プローブ要求	0090CC9F6558	移動端末	AP2_PLANEX_MAC
576	44.945	1Mbps	8	ACK			
577	44.945	11Mbps	8	プローブ応答	0090CC9F6558	AP2_PLANEX_MAC	移動端末
578	44.945	11Mbps	8	ACK			
579	44.945	1Mbps	8	認証	0090CC9F6558	移動端末	AP2_PLANEX_MAC
580	44.945	1Mbps	8	ACK			
581	44.945	11Mbps	8	認証	0090CC9F6558	AP2_PLANEX_MAC	移動端末
582	44.945	11Mbps	8	ACK			
583	44.945	1Mbps	8	参入要求	0090CC9F6558	移動端末	AP2_PLANEX_MAC
584	44.945	1Mbps	8	ACK			
585	44.945	11Mbps	8	参入確認	0090CC9F6558	AP2_PLANEX_MAC	移動端末
586	44.945	11Mbps	8	ACK			
587	45.125	11Mbps	8	データ	0039BB1C6558	移動端末	AP2_PLANEX_MAC

・Ethereal の実験結果

No.	Time	Source	Destination	Protocol	Info
118	26.483633	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
119	26.483979	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
120	27.330723	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
121	27.524265	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
122	27.524597	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
123	29.330625	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
124	31.330637	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
125	33.330592	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
126	35.330611	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
127	37.330561	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
128	39.330574	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
129	39.333922	00:90:cc:9f:65:58	01:80:c2:00:00:00	STP	Topology Change Notification
130	40.330540	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. TC + Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
131	41.330677	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. TC + Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
132	43.330554	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. TC + Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
133	44.496132	192.168.1.2	192.168.1.255	IAPP	Announce Request(0) (version=0)
134	44.500364	192.168.1.2	224.0.1.178	UDP	Source port: 3517 Destination port: 3517
135	44.500966	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	LLC	U, func=XID; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
136	44.639328	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
137	44.639646	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
138	45.330526	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. TC + Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
139	45.639096	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
140	45.639438	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
141	46.639000	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
142	46.639356	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
143	47.330517	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. TC + Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
144	47.639630	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
145	47.639938	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
146	48.107908	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.1.250? Tell 192.168.1.181
147	48.107968	00:90:cc:51:b9:05	00:11:2f:02:d4:b1	ARP	192.168.1.250 is at 00:90:cc:51:b9:05
148	48.110688	192.168.1.181	192.168.1.250	ICMP	Echo (ping) request
149	48.110756	192.168.1.250	192.168.1.181	ICMP	Echo (ping) reply
150	48.639086	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.1.178? Tell 192.168.1.181
151	48.639327	00:13:d4:09:cf:9d	00:11:2f:02:d4:b1	ARP	192.168.1.178 is at 00:13:d4:09:cf:9d
152	48.641476	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
153	48.641820	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
154	49.330466	00:90:cc:5a:17:fe	01:80:c2:00:00:00	STP	Conf. TC + Root = 32768/00:90:cc:5a:17:fe Cost = 0 Port = 0x8002
155	49.639028	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
156	49.639381	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
157	50.638810	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
158	50.639152	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply

3.3.3.B.考察

・パケットフォーマットは全て実験結果 3.3.2.A の Ethereal のものと同様.
・違う点は IAAP，UDP ,LLC の 3 つのパケットが，実験結果 3.3.2.A のパケット No.90 の STP の上に現れている点のみである.
・パケット一つ一つについての考察，シーケンス図は省略.

3.3.5. 実験 1 のシーケンス図との比較

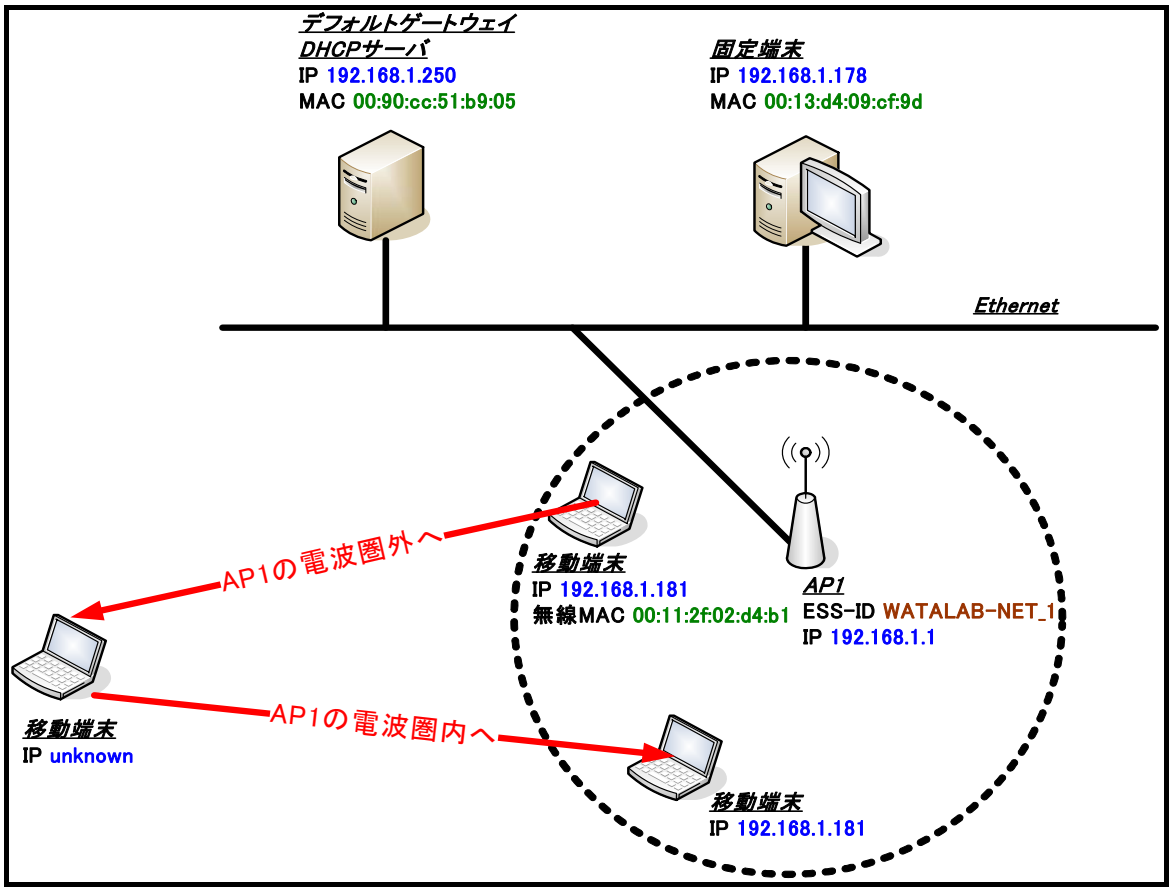
・この実験に使用した機器は STP(Spanning Tree Protocol)を利用して，ネットワークを論理的にツリー状にし，ネットワークのループを防いでいる．このプロトコルにより，AP はネットワークの形状を理解する.
・IAPP，UDP，LLC の 3 つのパケットはハンドオーバ時に現れるパケットだが，これらの仕組みが，よく分からない.
・レイヤ 2 での動作を見ても，ESSID が同一の場合は実験 1 では，再参入要求→再参入応答，参入要求→参入応答と二種類あったが，実験 3 の場合,参入要求→参入応答と一種類しかない.
・詳しいハンドオーバ動作の解明には至らなかったが，チップベンダの違いにより，ハンドオーバのシーケンスが変化することが今回の実験で分かった.

3.4. 実験 4

・実験 1 との比較実験.
　・単体の AP に対して再接続を行った実験.

3.4.1. 機器構成

・実験 1 の機器構成からの変更点.
　　・実験 1 の機器構成から AP2 のみを取り外した.
　　・その他の条件は実験 1 と全て同様.



3.4.2. 実験結果

・Air-PacMon の実験結果

No	時間情報	通信レート	チャンネル	MACフレーム	BSSID	送信元ステーションアドレス	送信先ステーションアドレス
2278	77.432	1Mbps	8	プローブ要求	0007404DD356	移動端末	AP1_BUFFALO_無線MAC
2279	77.432	1Mbps	8	ACK			
2280	77.432	1Mbps	8	プローブ応答	0007404DD356	AP1_BUFFALO_無線MAC	移動端末
2281	77.432	1Mbps	8	プローブ応答	0007404DD356	AP1_BUFFALO_無線MAC	移動端末
2282	77.442	1Mbps	8	プローブ応答	0007404DD356	AP1_BUFFALO_無線MAC	移動端末
2283	77.442	1Mbps	8	ACK			
2284	77.442	1Mbps	8	プローブ応答	0007404DD356	AP1_BUFFALO_無線MAC	移動端末
2285	77.442	1Mbps	8	認証	0007404DD356	移動端末	AP1_BUFFALO_無線MAC
2286	77.442	1Mbps	8	ACK			
2287	77.442	1Mbps	8	プローブ応答	0007404DD356	AP1_BUFFALO_無線MAC	移動端末
2288	77.442	1Mbps	8	ACK			
2289	77.442	1Mbps	8	認証	0007404DD356	AP1_BUFFALO_無線MAC	移動端末
2290	77.442	1Mbps	8	ACK			
2291	77.442	1Mbps	8	参入要求	0007404DD356	移動端末	AP1_BUFFALO_無線MAC
2292	77.442	1Mbps	8	ACK			
2293	77.442	1Mbps	8	参入確認	0007404DD356	AP1_BUFFALO_無線MAC	移動端末
2294	77.452	1Mbps	8	ACK			

・Ethereal の実験結果

No.	Time	Source	Destination	Protocol	Info
73	42.609088	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
74	42.609472	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
75	48.112469	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
76	48.112857	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
77	75.838141	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	FC	[Malformed Packet]
78	77.584912	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x553ff0d6
79	77.585310	192.168.1.250	192.168.1.181	ICMP	Echo (ping) request
80	77.742542	192.168.1.250	192.168.1.181	DHCP	DHCP Offer - Transaction ID 0x553ff0d6
81	77.764811	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x553ff0d6
82	77.767369	192.168.1.250	192.168.1.181	DHCP	DHCP ACK - Transaction ID 0x553ff0d6
83	77.831854	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
84	78.607956	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
85	78.610974	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.178? Tell 192.168.1.181
86	78.611232	00:13:d4:09:cf:9d	00:11:2f:02:d4:b1	ARP	192.168.1.178 is at 00:13:d4:09:cf:9d
87	78.622734	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
88	78.623104	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
89	79.607921	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
90	79.608969	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
91	79.609330	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
92	80.611691	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
93	80.612050	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
94	80.632774	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
95	80.637563	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.250? Tell 192.168.1.181
96	80.637619	00:90:cc:51:b9:05	00:11:2f:02:d4:b1	ARP	192.168.1.250 is at 00:90:cc:51:b9:05
97	80.645575	192.168.1.181	224.0.0.22	IGMP	V3 Membership Report
98	80.647114	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
99	80.651544	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
100	80.686019	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
101	81.436618	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
102	81.607978	192.168.1.181	224.0.0.22	IGMP	V3 Membership Report
103	81.626190	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
104	81.626521	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
105	81.627723	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
106	82.186564	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
107	82.608054	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
108	82.608389	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
109	82.622819	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
110	82.936551	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
111	83.607926	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
112	83.608270	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
113	83.641312	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
114	83.717097	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
115	84.467895	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
116	84.607938	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
117	84.608216	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
118	84.622798	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
119	85.217735	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
120	85.607866	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
121	85.608204	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
122	85.967731	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
123	86.607547	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
124	86.607892	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
125	86.654498	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
126	86.748507	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
127	86.749088	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
128	87.498968	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
129	87.500556	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
130	88.248941	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
131	88.250514	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
132	88.623415	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
133	88.999003	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
134	89.000580	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
135	89.781115	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
136	89.782753	192.168.1.181	192.168.1.255	BROWSER	Host Announcement WL-ENDEAVOR, Workstation,
137	91.279447	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
138	92.107002	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
139	92.107364	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
140	92.782576	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
141	93.107662	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
142	93.107995	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
143	94.107640	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
144	94.107977	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
145	94.280055	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
146	95.107637	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
147	95.107996	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
148	95.781527	192.168.1.181	192.168.1.255	BROWSER	Browser Election Request
149	96.107682	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
150	96.108012	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
151	96.781977	192.168.1.181	192.168.1.255	BROWSER	Browser Election Request
152	97.107545	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
153	97.107881	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
154	97.783918	192.168.1.181	192.168.1.255	BROWSER	Browser Election Request
155	98.107587	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
156	98.107911	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
157	98.723541	192.168.1.3	255.255.255.255	UDP	Source port: 2096 Destination port: 10260
158	98.726023	192.168.1.3	192.168.1.255	NBDS	Direct_group datagram
159	98.779270	192.168.1.181	192.168.1.255	BROWSER	Browser Election Request
160	99.106823	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
161	99.107151	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
162	99.780134	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
163	100.107575	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
164	100.107907	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
165	100.532968	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
166	101.106861	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
167	101.107186	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
168	101.280475	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
169	102.028875	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
170	102.106712	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request

171	102.107062	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
172	102.810214	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
173	103.106732	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
174	103.107062	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
175	103.560093	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
176	104.106774	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
177	104.107101	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
178	104.310129	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
179	105.060161	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
180	105.106652	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
181	105.106999	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
182	105.841481	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
183	105.842098	192.168.1.181	192.168.1.255	BROWSER	Request Announcement WL-ENDEAVOR
184	105.842782	192.168.1.181	192.168.1.255	BROWSER	Domain/Workgroup Announcement WATANABE-LAB, NT
185	106.106617	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
186	106.106948	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
187	107.106725	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
188	107.107061	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply

・Ethereal の結果に対してフィルタの適用（実験 2 と全く同様のフィルタを適用)

→Ethereal の結果を見ると，パケット No.75，76 の ICMP メッセージを最後に，27.72 秒間 AP1 の電波範囲外で待機した後に，移動端末は再接続動作を始めた．そのため実験結果 3.2.2 と同様に，ハンドオーバ後に，Windows アプリケーションがコネクションを張るためにさまざまなパケットのやり取りをしていると考えた．今回の考察は，ハンドオーバに必要なパケットについて考察を行いたいので，Ethereal の実験結果に以下のフィルタを適用．余分なパケットに対してフィルタを適用して排除した．

```
!( udp.port == 1900 || ip.dst == 224.0.0.22 || udp.port == 53 || udp.port == 137 || udp.port == 138 || udp.port == 10260)
```

・SSDP(Simple Service Discovery Protocol)

No.	Time	Source	Destination	Protocol	Info
94	80.632774	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
99	80.651544	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
113	83.641312	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
125	86.654498	192.168.1.181	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1

・IGMP(Internet Group Management Protocol)

No.	Time	Source	Destination	Protocol	Info
97	80.645575	192.168.1.181	224.0.0.22	IGMP	V3 Membership Report
102	81.607978	192.168.1.181	224.0.0.22	IGMP	V3 Membership Report

・DNS(Domain Name System)

No.	Time	Source	Destination	Protocol	Info
98	80.647114	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
105	81.627723	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
109	82.622819	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
118	84.622798	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com
132	88.623415	192.168.1.181	192.168.1.250	DNS	Standard query A time.windows.com

・NBNS(NetBIOS Name Service)

No.	Time	Source	Destination	Protocol	Info
100	80.686019	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
101	81.436618	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
106	82.186564	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
110	82.936551	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<00>
114	83.717097	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
115	84.467895	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
119	85.217735	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
122	85.967731	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<00>
126	86.748507	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
127	86.749088	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
128	87.498968	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
129	87.500556	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
130	88.248941	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
131	88.250514	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
133	88.999003	192.168.1.181	192.168.1.255	NBNS	Registration NB WL-ENDEAVOR<20>
134	89.000580	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1e>
162	99.780134	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
165	100.532968	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
168	101.280475	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
169	102.028875	192.168.1.181	192.168.1.255	NBNS	Registration NB WATANABE-LAB<1d>
172	102.810214	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
175	103.560093	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
178	104.310129	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>
179	105.060161	192.168.1.181	192.168.1.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><01>

・BROWSE

No.	Time	Source	Destination	Protocol	Info
135	89.781115	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
136	89.782753	192.168.1.181	192.168.1.255	BROWSE	Host Announcement WL-ENDEAVOR, Workstat
137	91.279447	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
140	92.782576	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
145	94.280055	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
148	95.781527	192.168.1.181	192.168.1.255	BROWSE	Browser Election Request
151	96.781977	192.168.1.181	192.168.1.255	BROWSE	Browser Election Request
154	97.783918	192.168.1.181	192.168.1.255	BROWSE	Browser Election Request
159	98.779270	192.168.1.181	192.168.1.255	BROWSE	Browser Election Request
182	105.841481	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
183	105.842098	192.168.1.181	192.168.1.255	BROWSE	Request Announcement WL-ENDEAVOR
184	105.842782	192.168.1.181	192.168.1.255	BROWSE	Domain/Workgroup Announcement WATANABE-

・UDP

No.	Time	Source	Destination	Protocol	Info
157	98.723541	192.168.1.3	255.255.255.255	UDP	Source port: 2096 Destination port: 10260

・NBDS(NetBIOS Datagram Service)

No.	Time	Source	Destination	Protocol	Info
158	98.726023	192.168.1.3	192.168.1.255	NBDS	Direct_group datagram

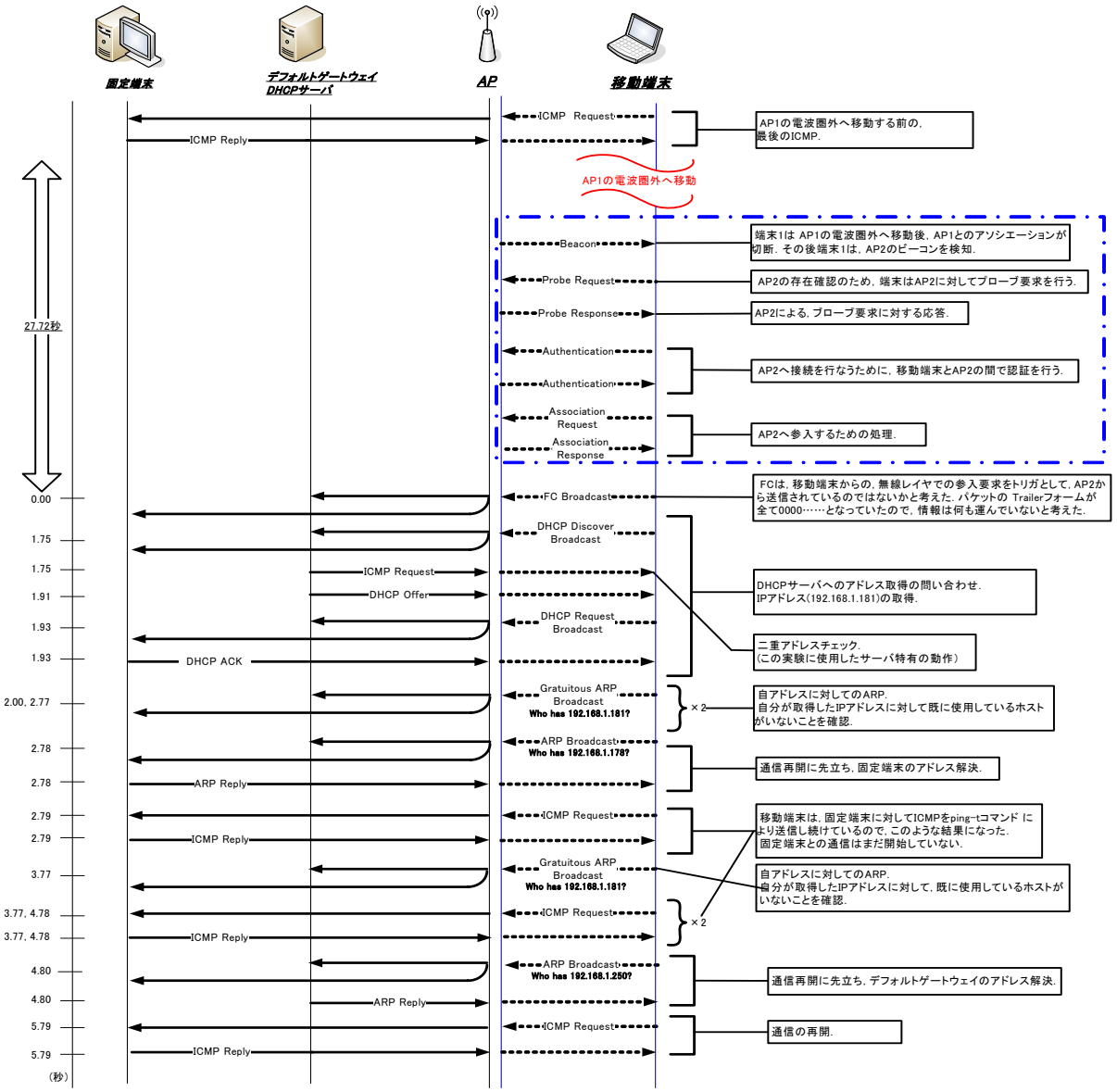
・フィルタ適用後の Ethereal のデータ

No.	Time	Source	Destination	Protocol	Info
63	30.999968	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
64	31.000326	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
67	31.999842	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
68	32.000158	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
69	34.068174	192.168.1.178	192.168.1.250	DHCP	DHCP Request - Transaction ID 0xa988f573
70	34.070748	192.168.1.250	192.168.1.178	DHCP	DHCP ACK - Transaction ID 0xa988f573
71	37.109099	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
72	37.109497	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
73	42.609088	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
74	42.609472	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
75	48.112469	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
76	48.112857	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
77	75.838141	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	FC	[Malformed Packet]
78	77.584912	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x553ff0d6
79	77.585310	192.168.1.250	192.168.1.181	ICMP	Echo (ping) request
80	77.742542	192.168.1.250	192.168.1.181	DHCP	DHCP Offer - Transaction ID 0x553ff0d6
81	77.764811	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x553ff0d6
82	77.767369	192.168.1.250	192.168.1.181	DHCP	DHCP ACK - Transaction ID 0x553ff0d6
83	77.831854	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
84	78.607956	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
85	78.610974	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.178? Tell 192.168.1.181
86	78.611232	00:13:d4:09:cf:9d	00:11:2f:02:d4:b1	ARP	192.168.1.178 is at 00:13:d4:09:cf:9d
87	78.622734	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
88	78.623104	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
89	79.607921	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.181? Gratuitous ARP
90	79.608969	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
91	79.609330	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
92	80.611691	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
93	80.612050	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
95	80.637563	00:11:2f:02:d4:b1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.250? Tell 192.168.1.181
96	80.637619	00:90:cc:51:b9:05	00:11:2f:02:d4:b1	ARP	192.168.1.250 is at 00:90:cc:51:b9:05
103	81.626190	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
104	81.626521	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply
107	82.608054	192.168.1.181	192.168.1.178	ICMP	Echo (ping) request
108	82.608389	192.168.1.178	192.168.1.181	ICMP	Echo (ping) reply

3.4.3. 考察

No.	考察
75 76	移動端末が AP1 経由で固定端末に対して ICMP を送受信. この後、移動端末は AP1 の電波圏外へ物理的に移動を行い，AP1 から離脱する.
77	移動端末が，AP1 の電波範囲内へ移動. ネットワーク上に FC が送信される. 考察 3.1.3.A のパケット No.55 と同様.
78	移動端末からの DHCP Discover – Transaction ID 0x553ff0d6
79	DHCP サーバからの二重アドレスチェック. 今回の実験で使用した DHCP サーバ特有の動作.
80 81 82	パケット No.78 の Transaction ID 0x553ff0d6 のプロセス パケット No.78 の DHCP Discover を受けて，Offer → Request → Ack，と移動端末が DHCP サーバから IP アドレスを取得するための一連の流れ.
83 84	移動端末が，自アドレスに対しての ARP を送信. 自分が取得した IP アドレスに対して既に使用しているホストがいないことを確認している. 応答がないことにより，DHCP サーバから割り振られた IP アドレスが使用可能となる.
85 86	考察 3.1.3.A のパケット No.62，63 と同様. 移動端末からの ARP. 固定端末のアドレス解決を行っている.
87 88	考察 3.1.3.A のパケット No.56，57 と同様. 移動端末が AP2 経由で固定端末に対して，ICMP を送受信. 固定端末に対しての再接続動作は終了していないが，移動端末は固定端末に対して ICMP メッセージを ping -t コマンドにより送信し続けているので, このような結果を得た.
89	パケット No.83，84 の考察と同様
90 91 92 93	パケット No.87，88 の考察と同様
95 96	考察 3.1.3.A のパケット No.58，59 と同様. 移動端末からの ARP. デフォルトゲートウェイのアドレス解決を行っている.
103 104	考察 3.1.3.A のパケット No.64，65 と同様. 移動端末の固定端末に対しての再接続動作が終了. 移動端末は，AP2 を介して固定端末との通信を再開する.

3.4.4. シーケンス図



3.4.5. 実験 1 のシーケンス図との比較

・新規参入動作は完全にアソシエーションが切れてから，再接続を行なっているので，DHCP によりアドレスを再設定する必要がある．

・また，端末はアプリケーションレベルでもコネクションが切れたということを検知するので，再接続時には，端末のアプリケーションがコネクションを張りなおすために様々なパケットがネットワーク上に送信される．

4. まとめ

・OS を WindowsXP としたとき，既存の AP で AP 間のハンドオーバは可能.
・有線上に現れるハンドオーバ用のパケットは，無線レイヤで，端末が AP とやり取りするパケットによって決まる.
・AP 間で同一の ESSID を使用している場合のハンドオーバは, 同一 LAN 内での移動とみなし，IP アドレスは変化しない.
・同一ネットワーク内なら，AP 間の ESSID は同じものを使用したほうが，ハンドオーバにかかる時間が短縮される．これは，AP 間の ESSID が異なる環境で，移動端末がハンドオーバを行うと，Windows は，異なるネットワークに参入したとみなし，ネットワークに参加するため DHCP の動作により，IP アドレスなどの再設定を行うためである.
・ハンドオーバのシーケンスは AP のベンダごとに違う.
・ハンドオーバの動作はベンダごとに独自に定義していると考えられる.そのため，不明なパケットが多い.
・端末は AP とのアソシエーションが切断されると，端末の保持している ARP キャッシュがクリアされる．そのため，通信を再開するために再接続時に端末から必ず ARP が送信される.

5. 参考文献

・802.11 無線ネットワーク管理
Mattbew S. GAST 著
水野 忠則，渡辺 尚，石原 進，峰野 博史 訳
オライリー・ジャパン 発行
2003 年 9 月 24 日　初版第一刷発行

・改訂版 802.11 高速無線 LAN 教科書
守倉 正博，久保田 周治 監修
インプレス 発行
2005 年 1 月 1 日　初版第一刷発行