修 士 論 文

ホームネットワークの障害診断に関する研究

北陸先端科学技術大学院大学
情報科学研究科情報システム学専攻

相川　恵

2007年3月

修 士 論 文

ホームネットワークの障害診断に関する研究

指導教官　丹康雄 助教授

審査委員主査　丹康雄 助教授
審査委員　篠田陽一 教授
審査委員　敷田幹文 教授

北陸先端科学技術大学院大学
情報科学研究科情報システム学専攻

510001 相川　恵

提出年月: 2007 年 2 月

概 要

本研究では障害発生時のユーザサポートへの負担を減らすことと，ユーザへの負担をできる限り少なくすることを目的としたホームネットワーク障害診断システムの提案を行なう．

ホームネットワーク障害診断システムをユーザインタフェースとホームネットワークの障害を診断する機能を持ったホームネットワーク障害診断ツールと, ホームネットワークの情報を収集してホームネットワーク障害診断ツールに提供するホームネットワーク情報収集スキャナの 2 つの要素からなると定義し，これらをホームネットワークにどのように配置するかを検討した．

今回は DLNA(Digital Living Network Alliance) という家電・パソコン・モバイル機器などの間でデジタルコンテンツを家庭内で簡単に共有することを目的とした規格においてのユーザ視点の障害とシステム視点の障害を分類し対応付けた．DLNA ネットワークでの障害検出のために，デバイスに組み込む自己診断機能の提案と、DLNA ネットワークの情報の収集法について検討した．ブロードキャストフレームとマルチキャストフレームのパケットモニタリングによって，障害診断に用いるホームネットワーク情報の学習を基本としたネットワーク情報の収集法を提案している．

目 次

図 目 次

表 目 次

第1章　はじめに

1.1　ホームネットワークとは

ホームネットワークシステムとは宅内外のネットワークを介して家電を管理・制御することで，今までにない新しいサービスを提供可能にするものである．このようなシステムに対応した家電は情報家電と呼ばれこれらは従来の家電機器に比べネットワークへの参加機能，サービスの提供機能などを持ち合わせている．

ホームネットワークと情報家電が提供するサービスは，大きく 2 つの分野に分けられる．1 つは家庭内でのコンテンツ配信に関するものである．DVD レコーダ, 専用メディアサーバ，パソコンなどに蓄積されたコンテンツをホームネットワークを通じてテレビやパソコンなどのクライアント機器に出力するものである．コンテンツは時と場所，そして機器を問わずに楽しむことが求められており，実際の機器の開発もそれを実現する方向で進んでいる．もう 1 つは白物家電の緻密な制御を実現し，消費電力の削減，二酸化炭素排出の抑制などに役立てようとするものである．

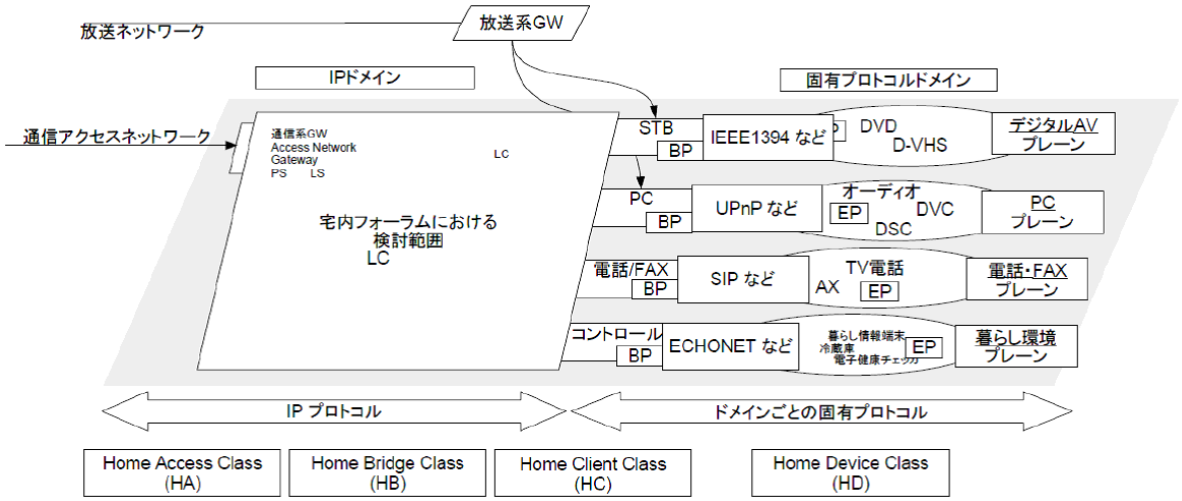

図 1.1: ホームネットワークアーキテクチャ(ITU-T J.190 で標準化されたリファレンスモデル)

1.2 各種ホームネットワーク規格

家庭ではオフィスのように計算機ネットワークの専門的な知識・技術を有する人材は期待できない．そのため，誰にでも簡単に情報家電を接続でき，かつ複雑な設定無しにその情報家電の持つサービスを利用できる必要がある．また, 情報家電はユーザにネットワークの物理的な存在を意識させずに既存の家電製品と同じような感覚で使えるものでなければならない．

また，一般の家庭には複数のメーカの製品が存在している．よって，ホームネットワークには異なるメーカの異なる製品でも相互に接続でき，サービスを提供できる仕組みが必要になる．これらのような環境を AV 機器や白物家電でも実現するために各メーカは協力して相互接続のための標準規格の策定に取り組んでいる．以下にいくつかの有力な団体が提供する標準仕様を挙げる．

1.2.1 UPnP

UPnP(Universal Plug and Play) はマイクロソフトを中心に設立された UPnP フォーラム [2] が策定する仕様である (図??)．対応機器としてはパソコン，ブロードバンドルータ，プリンタ，また情報家電では AV 系のデバイスとしてのメディアサーバなどの仕様に加えられている．UPnP はインターネットで利用されている既存技術，および既存技術を拡張した技術によって構成される点を大きな特徴としている．

1.2.2 ECHONET

ECHONET はエコーネットコンソーシアム [3] が白物家電への適用をスコープにおいて規格制定を行っているミドルウェアである．下位の階層には電灯線通信，小電力無線など既存の複数のメディアをカバーすることが特徴である．

1.2.3 IEEE1394

IEEE1394 は米 apple 社が開発を先導し，IEEE(Institute of Electrical and Electronics Engineers) によって標準化された，動画や音声を含む様々なデータを 1 つのシリアルバスによって転送することを狙いとして作られたマルチメディア伝送技術である．それと同時に，様々な AV 機器などを制御するための上位インタフェースとして AV/C コマンド，コンテンツ保護のためのコピープロテクション機構が用意されている．

1.2.4 DLNA

DLNA(Digital Living Network Alliance) [4] は，家電・パソコン・モバイル機器などの間でデジタルコンテンツを家庭内で簡単に共有することを目的とし，業界標準技術に基づいたオープンな相互接続互換性を構築するための技術的な設計ガイドラインを策定するために設立された非営利団体である．

1.3 研究の目的

ホームネットワークは基本的に管理者不在のネットワークであるという性質からネットワーク構築・管理が困難なことが問題となっている．特に，IP をベースとした接続規格を用いてホームネットワークに参加する機器は増加の傾向にあり，これらの機器においては導入時に IP アドレスや DNS サーバのアドレスなどの設定を必要とすることや, ある程度高速なネットワークを必要とするためホームネットワークの構築をさらに複雑なものにしている．結果としてこれらの機器を製造・販売する企業はユーザサポートに多くの人的資源を割くことになる．また機器の導入が困難であることはホームネットワークの普及を妨げる要因にもなる．今後ホームネットワークの管理を専門とする業者が現れることも予想されるが，実際にビジネスとして成立するまでには時間がかかるものと考えられる．

そこで，本研究では障害発生時のユーザサポートへの負担を減らすことを目的にホームネットワーク障害診断システムの提案を行い，システムの用いる障害診断手法，障害診断のためのネットワーク情報の収集法の検討を行なった．

第2章　ホームネットワーク障害診断システムの提案

ホームネットワークにおける障害の診断，検出を行いユーザによるホームネットワークの管理や障害の検出をサポートするホームネットワーク障害診断システムの提案を行なう．図 2.1 に提案システムのイメージを示す．

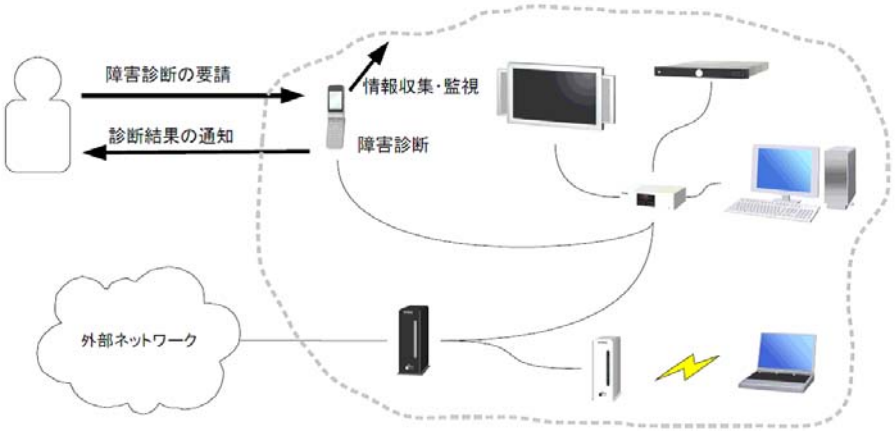

図 2.1: 提案システムのイメージ

2.1　ホームネットワーク障害診断システム

提案システムはホームネットワークで用いられる多種多様な規格で起こる障害を診断しユーザにそれを伝える．この提案システムは次の 2 つの要素からなる．

1．ホームネットワーク障害診断ツール
2．ホームネットワーク情報収集スキャナ

このホームネットワーク障害診断システムが実現することで，ユーザは障害診断ツールを使ってホームネットワークの障害監視を自動で行なうことができる．

2.1.1 ホームネットワーク障害診断ツール

ホームネットワーク障害診断ツールは，ホームネットワークの情報を基に障害診断を行なう機能を持つ．情報から各障害を検出するためのルールセットと，検出した障害をユーザに提示するための何らかのユーザーインタフェースを持つ．また，ユーザーから診断の要請を受けてホームネットワークの情報を基に障害診断を行なうモデルもある．そのためホームネットワーク障害診断ツールはユーザから診断の要請を受けるためのユーザインタフェースを持つ．

2.1.2 ホームネットワーク情報収集スキャナ

ホームネットワーク情報収集スキャナは，ホームネットワーク障害診断ツールの補助的な役割をこなす．スキャナはホームネットワークのあらゆる場所に配置される．ホームネットワーク障害診断ツールがホームネットワークの障害診断を行なう時には自分が配置された場所で自分が収集できる情報をできうる限り収集する．ツールから情報の要請を受けた時に，自身の情報をツールに送信する機能を持つ．

2.2 ツール、スキャナの配置

障害診断ツールと情報収集スキャナをどのようにネットワークに配置するかを検討する．現在ホームネットワークには様々な規格が入り乱れている．ひとつのスキャナですべての規格上で動作する機器の情報を収集するためには、そのスキャナがすべての規格に対応している必要がある．また、外からは絶対に見えない、その機器しかわからない情報は必ず存在する．これらのことから、スキャナはできるだけ多くの機器に組み込まれていたほうがよい．

ツールはこれらのスキャナと通信ができる場所にあればよいが、ツールとスキャナ間で断線などの障害が起こった場合にこれらが通信不可能になってはならない．そのためツールもできるだけ様々な場所に存在する必要がある．

2.3 システムの運用イメージ

ここでは提案システムの運用イメージについて述べる．運用イメージとして 2 つのケース考えられる．1 つはシステムが自動的にホームネットワークの情報を収集し障害検出した場合ユーザに提示するもので、これはシステムの定常動作になる．もうひとつのケースは、ユーザがサービスの利用時に不具合を発見しシステムに障害の発見を要求するものである．それぞれの流れを図 2.2 に示す．

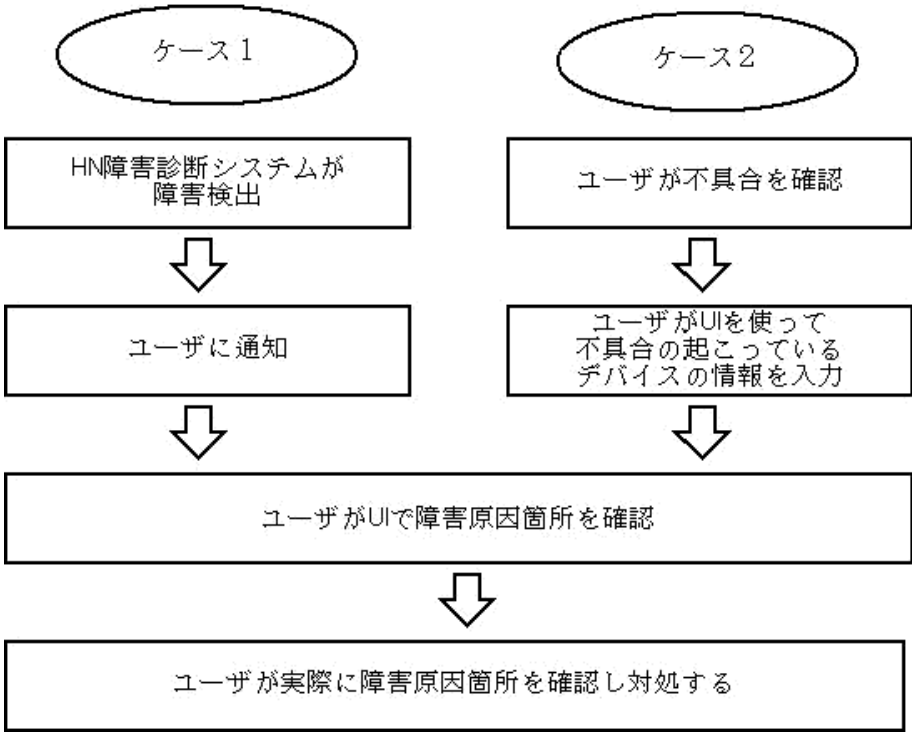

図 2.2: 運用イメージ

2.3.1 システムによる障害検出

システムが定常的にホームネットワークを監視し障害を検出した時に何らかの方法でもってユーザに伝える．

2.4 障害の検出

表 3.1 においてユーザ視点からの障害とシステム視点からの障害を対応付けたが，これらの障害をどのようにして検出するかについて検討する．ユーザによる障害の検出と，システムがホームネットワークの定期的な監視を行なうことで障害を検出するという 2 つの形態が考えられる．

2.4.1 システムによるホームネットワークの定期的な監視

ホームネットワークの定期的な監視を行なうデバイスもしくはそのような機能を既存の DLNA 機器に付随させる．定期的に情報を収集し，システム視点からの障害が発生していないか探す．もし障害を見つけた場合は何らかの方法でユーザに障害が発生していること，または障害の箇所を知らせる．

2.4.2　ユーザによる障害の検出

ユーザがホームネットワークのサービスを利用している時，もしくは利用しようとした時に，サービスが停止している，サービスが正常に動作しないといった状況に陥ることで，ユーザ自らが障害を検出する．

2.5　ツールに必要な機能

2.5.1　ネットワーク監視

ネットワークで何か異常な動作が起こっていないか、常に監視する必要がある．正常な動作と異常な動作を見分けるための

2.5.2　障害の検出

ネットワークで起こった障害を検出する機能が必要になる．
障害の検出のためにはルールセットが必要になる．

2.5.3　ユーザに障害を伝える

ユーザに障害の発生を伝えるには、様々な方法が考えられる．ユーザに分かりやすく障害を伝えるには、視覚的、聴覚的な伝達が好ましい．例えば、ホームネットワークの全ての機器にパトランプを仕掛け、ある機器で障害が発生した場合はその機器のパトランプを点灯させるといったものである．他に考えられるのは障害が発生したときにメールを送信するなどが挙げられる。

2.6　まとめ

ホームネットワークの各規格範囲内に配置されるスキャナと、スキャナの収集する情報からホームネットワークの障害を診断するホームネットワーク障害診断ツールからなるホームネットワークの障害診断システムを提案した。情報を収集するスキャナを様々な機器に組み込むことができれば、同じ規格内で動作する様々な機器情報の収集が可能になる。障害を診断するツールを分散配置することで、よりきめこまかな障害の診断が可能になる。

第3章　DLNAにおける障害診断

DLNA [4] は，家電・PC・モバイル機器などの間でデジタルコンテンツを簡単に共有するために策定された規格である．ここでは今回障害診断の対象としているDLNAと，DLNA内で機器発見として用いられているUPnP Device Architectureについて簡単に触れる．

3.1　DLNAとは

3.1.1　DLNAのフレームワーク

図3.1にDLNAのフレームワークを示す．

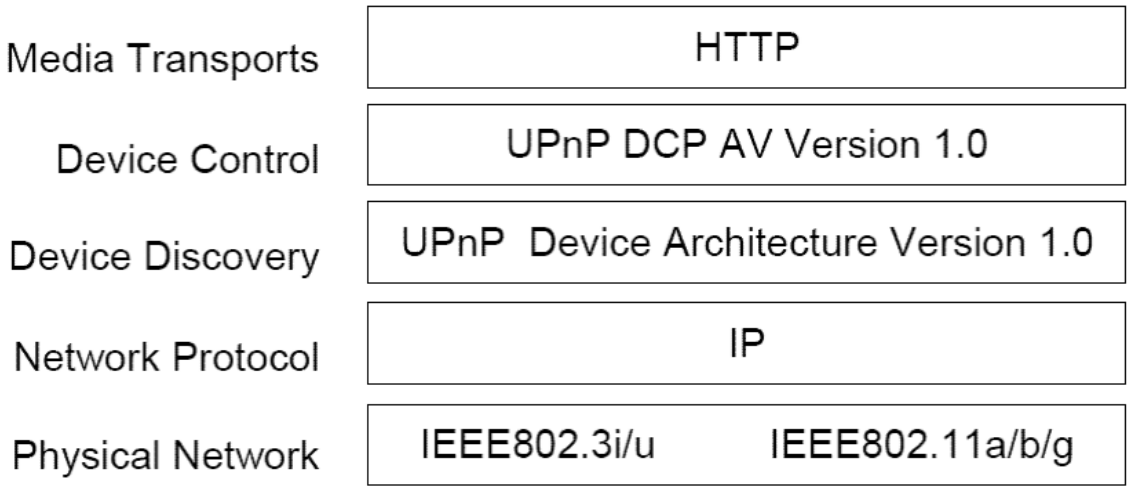

図3.1: DLNAのフレームワークに使用される標準技術

3.1.2　ユースケース

DLNAの設計ガイドライン策定プロセスでは，ホームネットワーク機器が家庭でどのように使用されるかというユースケースを最初に選定し，そのユースケースを実現するた

めの技術要求しようを確定して，最終的なガイドラインを策定する．ユースケースの中にはそれぞれの機器の役割を規定するデバイスクラスや，デジタル・コンテンツの種類を規定するメディアクラスなども含まれており，DLNA ガイドライン対応機器を開発するためには，これらのユースケースの検討が必要になる．

2004 年 6 月に策定された DLNA ガイドライン v1.0 ではデバイス，ユースケースとして 2 Box Pull 型のユースケースが選定された．このガイドラインは 2006 年 3 月に拡張され，モバイル・ハンドヘルド機器などの多種多様なデバイス，ユースケースが追加された．

2 Box Pull

デジタルメディアプレーヤー (DMP) とデジタルメディアサーバ (DMS) が 1 対 1 で接続されるユースケース．この DMP は操作画面やコンテンツ情報の表示，文字入力やポインティングといった UI 機能を持つ．ユーザの操作，コンテンツの再生はすべて DMP 側で行われ，サーバが意識されることはない．

2 Box Push

コントローラ (DMC) とコンテンツ再生機能を持つデジタルメディアレンダラー (DMR) が再生時に１対１で接続される．全ての操作は DMC で行われる．この場合の DMC は UI 機能およびコンテンツ配信機能を持ち，DMR は再生機能のみを持つ．

3 Box Control

DMC，DMS，DMR が接続される．この場合の DMC は UI 機能のみを持ち，実際の機器としては携帯ゲーム機，携帯電話，PDA，リモコンなどを想定している．

2 Box Printing

プリンターコントローラとプリンター (DMPr) がプリント時に接続される．この場合のプリンターコントローラは UI 機能とコンテンツ配信機能を持ち，実際の機器としてはデジタルカメラ，カメラ機能付き携帯電話などを想定している．

3 Box Printing

プリンターコントローラと DMS，DMPr が接続される．この場合の DPC は UI 機能のみを持つコントローラデバイスや DMR などへの実装が想定されている．

2 Box Uploading

アップローダとアップロード対応サーバが１対１で接続される．この場合のアップローダは携帯オーディオ，ビデオプレーヤ，デジタルカメラ，ビデオカメラなどを想定している．

2 Box Downloading

ダウンローダとダウンロード対応サーバが１対１で接続される．

3.2 UPnP

UPnP(Universal Plug and Play) は，家庭での情報家電およびパーソナル・コンピュータ (PC) の接続を容易にし機器の共有を行う仕組みである．UPnP はPnP をネットワーク全体に拡張し，ネットワーク・プリンタ，インターネットゲートウェイ，家電製品などのネットワーク・デバイスの検出と制御を容易に実現するものである．UPnP はマイクロソフトが制定した仕様に基づいて，IT，家電，通信関連などの業界の主要なサポート企業を中心に標準化を推進している．機器の種類やサービスを問わない共通のインタフェースの規格とするため，UPnP は既存の企画に基づいて設計されている．

図 3.2 に UPnP のプロトコルスタックを示す．UPnP は基本的な仕組みを定義している下位層にあたる UPnP Device ARchitecture と，上位層となる UPnP Device Contorol の各仕様がある．また，上位層として AV コンテンツの再生などを目的とした UPnP AV や，UPnP 対応ブロードバンドルータの挙動を定めた UPnP Internet Gateway Device などが有名だ得る．

3.2.1 UPnP ネットワークのコンポーネント

UPnP ネットワークは

1. デバイス
2. サービス
3. コントロールポイント

の三つの要素で構成されている．

- デバイス
  UPnP のデバイスはサービスコンテナとも呼び，デバイスがネストされたものである．
  図 3.3 に UPnP デバイスの構成例を挙げる．

図 3.2: UPnP Protocol Stack

- サービス
  UPnP デバイス内のサービスは，状態テーブル，コントロールサーバ，イベントサーバで構成される．状態テーブルは状態変数を通じてサービスの状態をモデル化し，状態が変更されると更新される．コントロールサーバは set_time などのアクション要求を受信して実行し，状態テーブルを更新してレスポンスを返す．サービス状態が変更されると，イベントサーバは関連サブスクライバにイベントを発行する．

- コントロールポイント
  UPnP ネットワーク内のコントロールポイントとは，他のデバイスを検出，制御可能なコントローラである．コントロールポイントはデバイスの検出後，以下の処理を行うことができる．

  デバイスディスクリプションを取得して，関連サービスのリストを取得する，興味あるサービスのサービスディスクリプションを取得する．サービスを制御するアクションを呼び出す．サービスのイベントソースをサブスクライブする．といった処理を行うことが出来る．

3.2.2 UPnP Device Architecture

Addressing

個々の UPnP デバイスは自身が DHCP サーバで無い限り，DHCP クライアントの機能を持ち，ネットワークへの参加時に DHCP サーバを探さなければならない．もし自身が

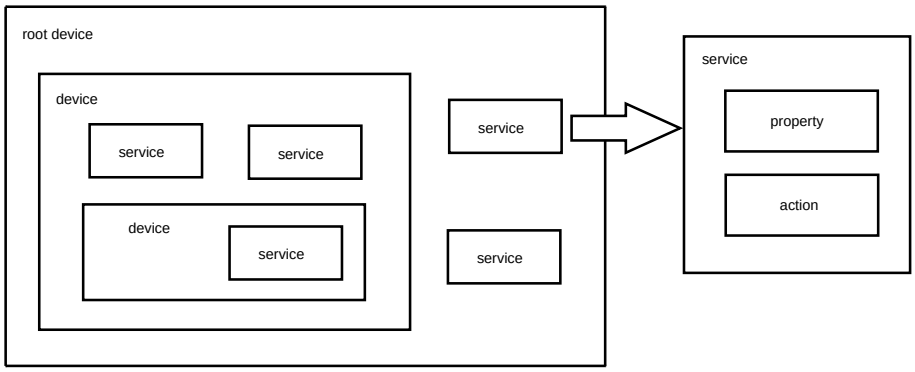

図 3.3: UPnP Device Architecture

DHCP サーバであった場合は UPnP デバイスに自身がプールしているアドレスを割り振る役になる．DHCP サーバが存在する場合，そのネットワークは管理されているということであり，デバイスは DHCP サーバに配布された IP アドレスを使用しなければならない．DHCP サーバの存在しない管理されていないネットワークにおいては，Auto-IP を用いてアドレスを自動取得する．

UPnP デバイスは DHCPDISCOVER メッセージを送信し DHCP サーバからの DHCPOFFER を待つ．DHCP クライアントが DHCPOFFER を待つ時間は処理系に依存する．DHCPOFFER を待ち時間中に受け取った場合はこのデバイスは割り当てられた動的アドレスを保持する．DHCPOFFER が一定時間中に送られてこなかった場合，デバイスは Auto-IP を使って IP アドレスを取得する．

UPnP デバイスは Auto-IP と DHCPDISCOVER によって IP アドレスをリクエストし，動的にアドレスを決定する機能を実装する．このアドレス割り当ての方法を用いたデバイスは管理されたネットワークと管理されていないネットワークの両方を容易に行き来することができる．

Auto-IP によって IP アドレスを自動的に取得する場合，デバイスは 169.254/16 の範囲からアドレスから自分の使用する IP アドレスをランダムに選択するアルゴリズムを使う．選択するアドレスは，すでに使われていないか調べるためのテストを行う必要がある．選択したアドレスが他のデバイスに使用されていた場合は他のアドレスを選び，同様にその新たに選択したアドレスをテストする (このリトライ数の定義を行う必要がある)．アドレス選択は衝突を回避するために無作為に行う必要がある (UPnP Device Architecture ではアドレスの選択にデバイスの MAC アドレスを Seed にした擬似ランダムパターン発生のアルゴリズムを推奨している)．

選択したアドレスが使用されていないかは，ARP probe を使う．ARP probe とは

```
Sender HwAddress : Device's MAC Address
Sender IPAddress : 0.0.0.0
Target HwAddress : 00:00:00:00:00:00
```

`Target IPAddress : Choosing IP Address`

の ARP リクエストを送信するものである．この ARP リクエストへの応答や，他の機器による同じ IP アドレスに対する ARP probe を発見した場合，デバイスは別のアドレスの使用を考慮しなければならない．自分が選択したアドレスが他の機器に使用されていなかった場合 (この ARP probe に対する返事がなかった場合) は 2 秒のインターバルを置いて 4 回ほど ARP prove の送信を繰り返すのが望ましい．

デバイスはリンクローカルなアドレスの設定に成功したら間に 2 秒ほど挟んで 2 度 gratuitous ARP を送信するべきである．この gratuitoue ARP は，以前に同じ IP アドレスを用いていたホストがいた場合，そのホストがネットワーク上の他ホストに残していった ARP キャッシュを更新することができる．

送信元または宛先が 169.254/16 の範囲に含まれる IP アドレスのパケットはフォワーディングのためにルータに送るべきではない．デバイスとコントロールポイントは，送信元アドレスが 169.254/16 の範囲内の場合は送信元が 1 つのリンク上に存在し，ダイレクトに届くと仮定する．よってこの 169.254/16 のアドレス範囲はサブネットに分割すべきではない．

Discovery

ネットワーク上の UPnP デバイスの検出を行う．ネットワークに参加したデバイスはマルチキャストパケットの送出を行い，コントロールポイントはそれを受け取り，デバイスを検出する．

検出フェーズにおいて，コントロールポイントはデバイスとサービスを検索し，デバイスはコントロールポイントに対して SSDP (Simple Service Discovery Protocol) によって存在を通知する．SSDP はマルチキャスト UDP 上の HTTP (HTTPMU)，およびユニキャスト UDP 上の HTTP (HTTPU) を利用する．デバイスはサービスを含んでいる．デバイスはタイプと，ユニークな識別子によって識別される．サービスはタイプによって識別される．ネットワーク上のデバイスまたはサービスを検索するために，コントロールポイントは HTTPM-SEARCH コマンドを 239.255.255.250:1900 に UDP で送信する．ネットワーク上の検出条件にマッチしたデバイスは，ユニキャストでディスクリプションの URL (3.3.2 節参照) を返信する．デバイスからの返信を受け取ったコントロールポイントは，ディスクリプションフェーズへと移行する．コントロールポイントが検索要求を出すとき，SSDP ヘッダには待機時間が含まれている．マッチしたデバイスは，返信するまでに 0 から待機時間までのランダムな時間待機する．コントロールポイントは待機時間が経過してもデバイスからの返信が無い場合には，デバイスが存在しないと判断する．

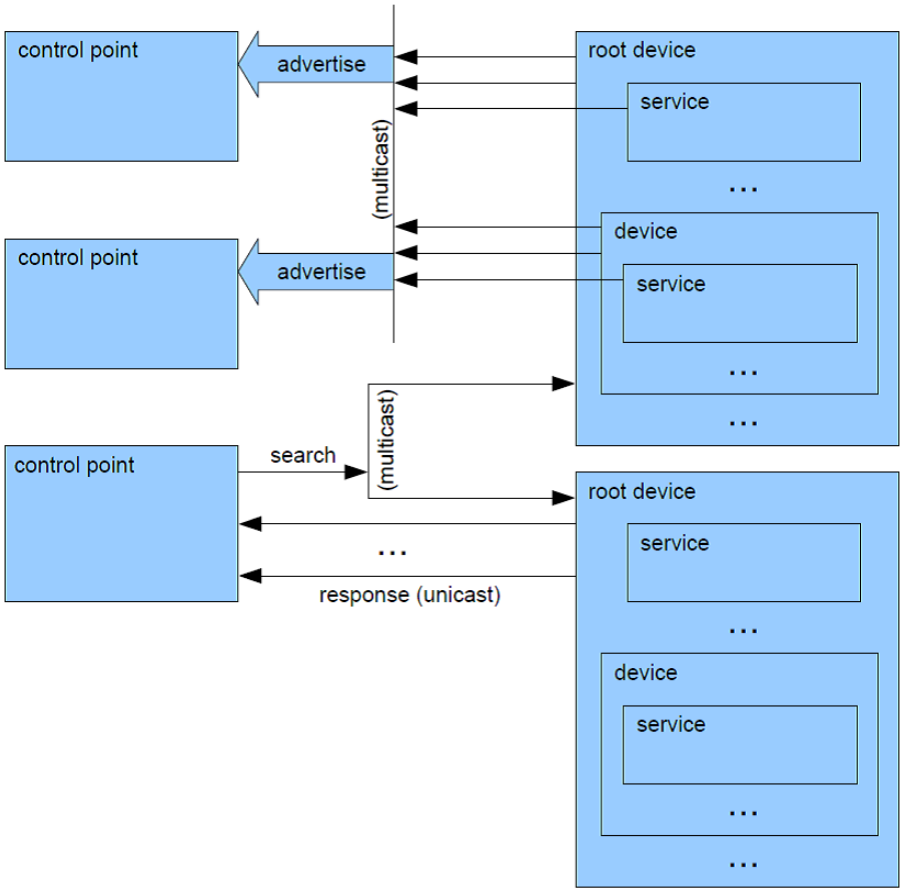

図 3.4: UPnP Discovery

Description

デバイスが提供できる機能や情報を記述した XML ファイルである．デバイス自身が持つサービスについて記述したデバイスディスクリプションと，各サービスが持つアクションなどについて記述したサービスディスクリプションの 2 種類がある．

コントロールポイントは制御したいサービスを検出すると，デバイスのディスクリプションを要求する．ディスクリプションはデバイスを記述した XML ドキュメントであり，以下の内容を含んでいる．

- 製造業者，バージョンなどの製品情報
- 埋め込まれているデバイス
- デバイスのサポートするサービス

ディスクリプションドキュメントのスキーマに関しては，割愛する．コントロールポイントは，ディスクリプションドキュメントを TCP 上の HTTP で要求する．このとき，コントロールポイントは標準的な HTTP の GET コマンドを使う (Web ページを取得する

のと同様)．サーバ側では，デバイスが標準的な HTTP サーバを動かしている．ディスクリプションドキュメントの要素には URL で記述されるものが多く，これらの要素も同様に HTTP/TCP によって取り出される．

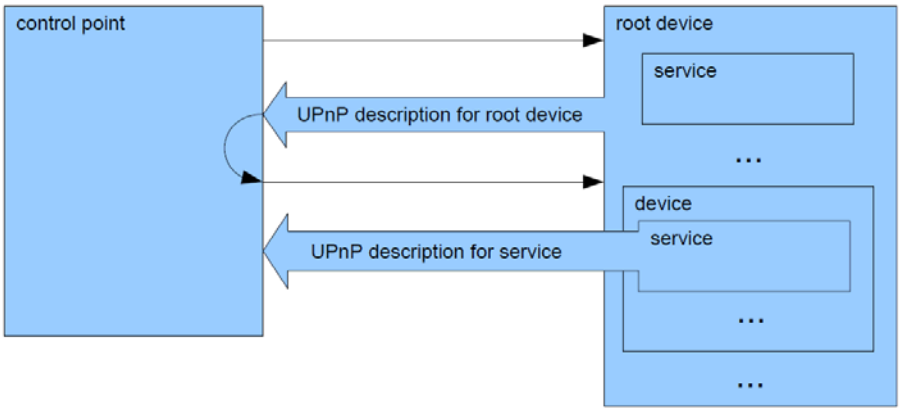

図 3.5: UPnP Description

Control

サービスの持つ機能を呼び出すアクションと，デバイスの状態変数を問い合わせるクエリがある．

デバイスを検出し，ディスクリプションドキュメントを取得すると，コントロールポイントはデバイスのサービスを制御することができる．サービスを制御する際，コントロールポイントは SOAP (Simple Object Access Protocol) を用いる．SOAP は HTTP の POST または M-POST コマンドを TCP 上で利用する．SOAP はサービスのアクションを XML で記述する．コントロールポイントはこの XML ドキュメントをディスクリプションドキュメントに示されたサービスの URL に送る．コントロールポイントはサービスの状態を取得設定することができる．

サーバ側では，コントロールサーバがコントロールリクエストを待っている．コントロールサーバは SOAP プロトコルを実装した HTTP ライクなサーバである．デバイスはサービスの組み合わせによって，複数のコントロールサーバを動かすことができる．

Eventing

イベントに対して，特定の状態変数を指定してイベント購読要求を行うと，その状態変数の値が変化するたびに，イベントが通知される．

コントロールポイントはデバイスを検出し，ディスクリプションドキュメントを取得すると，デバイスの提供するサービスの状態を監視することができる．コントロールポイ

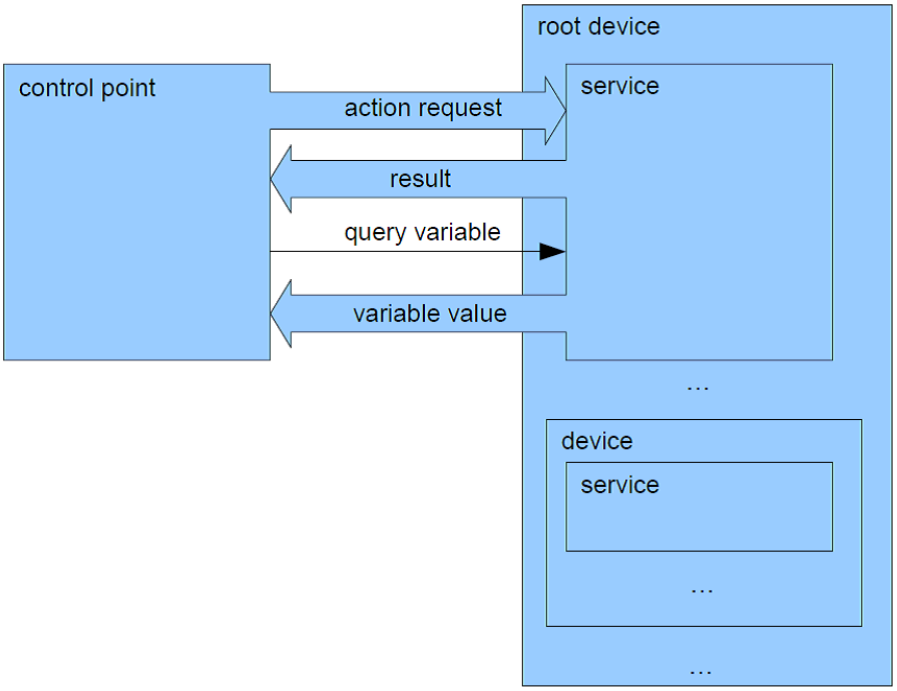

図 3.6: UPnP Control

ントは，監視したいサービスのディスクリプションドキュメントに示されたイベント通知サービスの URL をサブスクライブする．コントロールポイントへのイベントの通知は，サービスの状態が変更されるたびに行われ，これはコントロールポイント自身がサービスの状態を変更した場合も同様である．

サブスクライブとアンサブスクライブの要求は，イベント通知サービスの URL に対して HTTP/TCP によって行われる．コントロールポイントは，サブスクライブ中のイベント通知先 URL を指定する．イベント通知は，この URL に対して HTTP/TCP によって行われる．イベント通知は XML ドキュメントを含んでおり，サービスの状態変数が変更される等の，イベントの内容を記述する．

サーバ側では，イベントサーバがサブスクライブとアンサブスクライブの要求を待っている．イベントサーバは GENA (General Event Notification Architecture Protocol) を実装した HTTP ライクなサーバである．デバイスはサービスの組み合わせによって，複数のイベントサーバを動かすことができる．

Presentation

ウェブブラウザなどから，デバイスの状態の確認や制御ができる．

デバイスはプレゼンテーション用の URL を公開することができる．コントロールポイントは，この URL から HTML をダウンロードして，ユーザに対してデバイスの状態を表

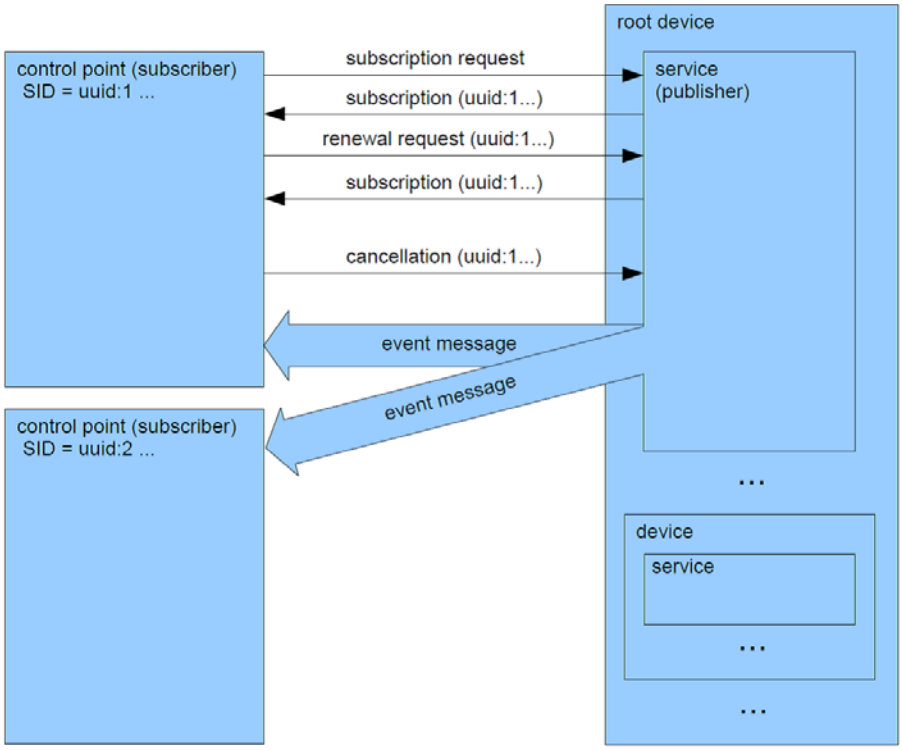

図 3.7: UPnP Eventing

示したり，ページの機能によってはデバイスを制御するインターフェースを表示することもできる．プレゼンテーションドキュメントを取得するためのプロトコルは，ディスクリプションドキュメントを取得するのと同様にHTTP/TCP である．コントロールポイントは，プレゼンテーションドキュメントを取得するために，ディスクリプションドキュメントに示されたプレゼンテーション URL を使う．すべてのデバイスがプレゼンテーションドキュメントを持っているわけではない．またすべてのコントロールポイントが，フレームや，Java アプレットのような複雑な HTML オブジェクトを表示できるわけでもない．

3.3 DLNA ネットワークにおける障害の分類

ネットワークシステムは階層構造になっており，層によって動作しているシステムが異なる．そして，下の層で起こった障害は上の層に連鎖するため，実際にどの層で障害が発生しているのかを判断するのは難しい．DLNA 対応機器やソフトウェアにはコンテンツの公開設定，また DiXiM などの WindowsOS などにインストールして使用するものではマシンに元から存在するファイヤーウォール機能によって UPnP で用いられるポート 1900 番を閉じられており，しばらく待たないとコンテンツのリストが取得できないといった現象が起こる．

ユーザからは詳しいシステムの障害原因を知ることができない．例えばDMS に入っている高画質な動画のコンテンツを DMR で再生するときに，DMS-DMR 間に実効帯域幅を制限する何かの要因があったとする．この時そのボトルネックとなる場所でパケットロスが発生しているのだが，ユーザにはこれは画像の乱れというようにしか知覚できない．もうひとつ，DiXiM で登録したコンテンツを発見できないという障害に対するトラブルシューティングの例を挙げる．DiXiM は，コンテンツが発見できないという障害の原因として考えられるのは，サーバが起動していない，公開の操作をしていない，公開フォルダが空である，公開フォルダに含まれるコンテンツのフォーマットが対応していない，同名の異なるフォルダを公開している，公開拒否の操作をしている，LAN 接続されていない，切断されている，ルータで接続許可されていないといったものが考えられると述べている．

ここでは障害が発生したレイヤを切り分けるために，ユーザ視点の障害とシステム視点の障害を分類した．そして，この二つの視点から見た障害を対応付けることで，ユーザが障害を発見した場合と，システムが障害を発見した場合で，あらかじめどのレイヤで障害が起こったのかを切り分けやすくする．

3.3.1 ユーザ視点からの障害

機器が発見できない

クライアントからコンテンツを配信してもらいたいサーバを発見できないことがある．この状態はシステム視点から見ると，物理・データリンク障害，アドレシング障害，ルーティング障害，機器発見・制御障害などが含まれる．

コンテンツを発見できない

クライアントから見て，サーバに置いてあるはずのコンテンツが見えないという状況である．これはクライアントに対して公開の操作をしていない，または公開拒否の操作をしているといった原因が考えられる．

コンテンツを再生できない

コンテンツは見えているが再生が出来ないといった障害．DLNA ではサポートするコンテンツのフォーマットを定義しているが，ベンダーによってその実装は様々である．ある機器では再生できるがある機器では再生できないといった場合，コンテンツを再生できないクライアントではそのコンテンツを再生するためのコーデックを持っていないということが考えられる．もうひとつは，そのファイル自体が何らかの原因で破損しているといったことが考えられる．

映像が乱れる

コンテンツのスムーズな再生ができないといった障害．ビデオを再生する際にコマ落ちする場合は大きく分けて 2 つの理由が考えられる．ひとつは，ホームネットワーク経由でビデオコンテンツ再生を行なう場合で，ネットワーク帯域が不足している場合にはコマ落ちが発生する恐れがある．802.11b 無線 LAN や 10Base-T でネットワークを構築している場合にはこの現象が発生しやすい．802.11a/g や 100Base-TX 接続であっても，同時に複数のコンテンツを配信・再生するなどして発生したクロストラフィックの影響を受けたとも考えられる．

もうひとつは，コンテンツ配信側または再生する側の処理能力が，コンテンツに対して不足している場合に起こる．高いビットレートで圧縮されていたり，高解像度の画面サイズのビデオコンテンツにおいて発生することがある．

3.3.2 システム視点からの障害

物理・データリンク障害

物理層になんらかの問題が発生して起こる障害．機器間を接続するケーブルの選択で，クロスとストレートを間違えた場合，Auto MDI/MDI-X 機能を持たないハブやスイッチの場合にデータリンク層での接続ができなくなる．この場合はスイッチやデバイスの LAN ケーブルを差し込むポートをランプを確認する．

デバイスのネットワークインタフェースになんらかの問題が生じて，データリンク的な通信ができなくなっている場合も考えられる．また機器自体の故障，電源が入っていない，電源が故障している場合もこれに含まれる

アドレシング障害

アドレシングに何らかの問題が発生して起こる障害．データリンク層では通信ができるがネットワーク層では通信ができないといった状況を指す．

例として，異なるネットワークアドレスを配信する DHCP サーバがブロードキャストフレームが届く範囲内に複数存在していた場合などがある．例えばこのホームネットワーク上に 2 台の DHCP サーバと 6 台の IP で通信をする DLNA デバイスが存在していたとする．6 台の DLNA デバイスはそれぞれ DHCP クライアントとして動作し，DHCPDISCOVER によって IP アドレスを求めてきた．ここで DHCP サーバが同じネットワークアドレスを配信すればよいが，そうでない場合，あるホスト群は 192.168/16 のネットワークアドレスを，もうひとつのホスト群は 10/8 のネットワークアドレスを基にした IP アドレスをふられたとする．そうすると，この機器同士は自分と同じネットワークアドレスを振られた，自分と同じ群に属するデバイスとしか IP 的な通信が行なえなくなる．もしもマルチホームでかつ IP forwarding の機能を持つデバイスがいた場合や，IP aliasing によって二

つのネットワークに属するようなデバイスがいた場合は，これらの 2 つの群が群を超えて通信をすることは可能になるかもしれないが，そのようなことはほぼ無いといってよい．

このように，ブロードキャストフレームが届くネットワーク内で異なるネットワークが存在し，本来機器間で行いたい通信を行なえないような状況に陥った場合をアドレシング障害とする．機器 A と機器間 B では通信ができるが，機器 A と機器 B は通信ができないといった状況や，リンクアップしており，サーバも立ち上がっているのに通信ができない場合はこの障害を疑うべきである．

また，同じ IP アドレスを持った複数のデバイスが存在している場合，IP duplicate のエラーが起きる．

ルーティング障害

経路制御に何らかの問題が発生して起こる障害を指す．機器に設定したデフォルトゲートウェイの IP アドレスを間違っていて外部と通信できない，ゲートウェイに何らかの故障が生じて外との通信ができない場合などにこの障害が起こっているとする．

機器発見・制御障害

DLNA の機器発見･制御に何らかの問題が発生して起こる障害．アドレシングに問題がないが，UPnP デバイスとして発見できない場合をこの障害とする．UPnP Device Discovery で使用する 1900 番ポートを閉じられていた場合など，機器発見にしばらく時間がかかったり，発見できなかったりする場合がある．このような場合もこの障害に分類する．

メディア管理・制御障害

DLNA のメディア管理･制御に何らかの問題が発生して起こる障害．あるメディアサーバ上で特定の MAC アドレス，IP アドレスに対してコンテンツの公開を拒否するような設定をされていたりした場合がこの障害になる．

メディアフォーマット障害

クライアントがコンテンツに対応したコーデックを持たない場合に発生する．

QoS 障害

実効帯域幅が不足して起こる障害．ユーザからは再生している動画の映像が乱れたり，コマ落ちが見られたりといった様子に見える．これはコンテンツ配信サーバ，クライアントの接続が間に無線 LAN を挟んでいたり，間のスイッチにおけるクロストラフィックの影響を受けたりしていることが考えられる．

3.3.3 各障害の対応付け

ユーザ視点からの障害とシステム視点からの障害を対応付けると次のようになる.

表 3.1: 各障害の対応付け

ユーザ視点からの障害	システム視点からの障害	障害の原因
映像が乱れる	QoS 障害	CPU パワーの不足 帯域幅の不足 間線での異常
コンテンツを再生できない	メディアフォーマット障害	コーデックがない メディアが壊れている
コンテンツを発見できない	メディア管理・制御障害	コンテンツ保護設定
機器が発見できない	機器発見・制御障害	ポートが閉じられている サーバが立ち上がっていない
	ルーティング障害	サブネットマスクの設定ミス デフォルトゲートウェイの設定
	アドレシング障害	IP duplicate 不正な DHCP サーバ
	物理・データリンク障害	間線が切断されている ケーブリング（クロス or ストレート） 電源障害

第4章　デバイスへ組み込む自己診断機能の提案

DLNA デバイスが形成するネットワークで発生する障害の多くは、ネットワークの知識の無いユーザが間違った設定のデバイスをネットワークに参加させてしまい、システム視点からは『物理・データリンク障害』『アドレシング障害』『ルーティング障害』と認識でき、ユーザからは『機器が発見できない』というようしか見えないという障害がほとんどである。

手動で IP アドレス、サブネットマスクなどを設定した場合、ネットワークの知識を持たないユーザは知らず知らずのうちに間違った設定をしている場合がある。また、ケーブルが LAN ポートにささっていない、ケーブルはささっているがクロスケーブルであるため通信できないといった場合も考えられる。このような外部との連絡が取れないような障害を特定するには、デバイス自身が自身の状態を診断することで可能になる。

RDZ-D97A は「接続診断」というものを持っており，これを選択すると RDZ-D97A は現在自身に設定されている項目に対して診断を行なう．この機能は実験機材として用いた機器の中では RDZ-D97A のみが持っていた．しかし，この診断機能は大変簡略されている．

RDZ-D97A の診断項目にもういくつかの項目を加えることで，よりきめ細かな自己診断ができると考える．DLNA デバイスに自己診断機能を組み込むことで、ユーザがデバイスに対して間違った設定を行うことを防ぐことができ、DLNA デバイス同士での接続でのトラブルの発生を抑えることができる。

ここでは、ユーザによる間違った設定の例を挙げる。次にそれらのユーザの間違った設定を検出するために、DLNA デバイスが行なうべき診断について述べる。

4.1　間違った設定の例

4.1.1　IP duplicate の例

プロバイダと契約しており、プロバイダからある 1 つの静的 IP アドレスをもらっている家庭を考える。その家には IP アドレスが IP デバイス同士が通信するために必要なもので、同じセグメント内で同一の IP アドレスを設定してはならないという知識を持たないユーザしかいなかった。その家のユーザはプロバイダからもらった IP アドレス、サブ

ネットマスクの値を、家庭内にある全てのIPネットワークに対応した製品にまったく同じ値で入力した。

このような場合に当然ホームネットワーク内ではIP duplicateが発生する。複数のDLNAデバイスであるMedia Serverがマルチキャスト239.255.255.250:1900宛てにNOTIFYメッセージを送信するが、Media Serverにコンテンツを配信してもらうべきMedia Rendererも、自分と同じIPアドレスを持つMedia ServerにIPレベルで話しかけることはできない。本来ならばMedia RendereはMedia ServerによるNOTIFYメッセージを受信したら即座にNOTIFYメッセージ中のLOCATIONにあるデバイスのディスクリプションを取得しにいくが、同じIPアドレスを設定されたためにIPレベル以上のメッセージ交換が行なえなくなってしまったために、これが不可能になった。

ユーザからは『Media RendererからMedia Serverが見えない』という障害が発生したようにしか見えない。

4.1.2 不正なDHCPサーバの例

DHCPサーバ機能が実装されたLAN側に4ポートの口を持ったブロードバンドルータAと4台のDLNAデバイスを用いて形成されているホームネットワークがあったとする。どのDLNAデバイスもブロードバンドルータAのDHCPサーバから動的にIPアドレスを割り振られ、何の問題も無く通信ができていた。新しくもう1台のDLNAデバイスをこのホームネットワークに参加させることになったが、ブロードバンドルータAにはもう空いているポートがない。その家には昔使っていたブロードバンドルータBを発見したので、スイッチ代わりに使うことにした。その日から、その家のホームネットワークでは、デバイスAからはデバイスBが見えるが、デバイスCからはデバイスBが見えない、といった障害が起こるようになった。

この障害はブロードバンドルータBがDHCPサーバ機能を持っており、そのDHCPサーバはネットワークアドレスに10.10/16のIPアドレスを、元々使っていたブロードバンドルータAはネットワークアドレス192.168/16のIPアドレスを配布していたために起こっていた。

4.1.3 サブネットマスクの設定ミス

手動でデバイスAのIPアドレスの設定を行ったときに、IPアドレス192.168.0.15、サブネットマスク255.255.255.0、デフォルトゲートウェイ192.168.0.254という値を入力するはずが、IPアドレス192.168.0.15、サブネットマスク192.168.0.15、デフォルトゲートウェイ192.168.0.254というように、IPアドレスとサブネットマスクの値をまったく同じものに設定してしまった。

この場合、ユーザ視点での『機器が見つからない』という障害が発生する。デバイスAは239.255.255.250:1900に向けてNOTIFY ssdp:aliveのメッセージを送り、それを見た他

のデバイスがデバイス A の 192.168.0.15:30000 宛てにデバイス A のディスクリプションを要求するが、デバイス A からは自分以外のデバイスは（デフォルトゲートウェイでさえも）皆異なるネットワークに属するデバイスなので、ディスクリプションの要求に応えることができなかったためである。

4.2 自己診断項目

DLNA デバイスで行なう自己診断の項目を列挙した。それぞれ何の診断を行うか、どのようにして行うかを述べている。

4.2.1 リンクアップ・ダウンの診断

デバイスは、自身のネットワークインタフェースの状態を確かめてリンクダウンしていないか診断する。もしもケーブルが接続されていない、ケーブルの種類が間違っている、接続先のデバイス（スイッチ等）の電源が OFF になっている、自身のネットワークインタフェースが故障しているなどの理由でリンクダウンしていた場合は、ユーザにそれを伝える。

4.2.2 IP duplicate の診断

入力された IP アドレスが既に他の機器で使われていないかを診断する。診断内容は入力された IP アドレスを Target IP Address に指定した ARP Request を送り、ARP Reply が返ってこないか一定時間待つというものである。もし ARP Reply が帰ってきた場合、その IP アドレスはすでに使用されているとみなし、ユーザに違うアドレスの入力を求める。

考慮すべき事項

本来 IP duplicate の診断には gratuitous ARP が用いられるべきだが、gratuitous ARP は全ての機器に実装されているわけではなく、gratuitous ARP メッセージを無視する機器が存在する。

WindowsXP は自身のネットワークインタフェースの INIT 時には gratuitous ARP を送信して IP duplicate の確認をしているが、他のホストが出してきた gratuitous ARP は無視している．本研究でブロードバンドルータとして使用した Airport は，gratuitous ARP の送信も行わなかった。また、自身と同じ IP アドレスに対する gratuitous ARP が送信されてきても、それに対して ARP Reply を返さないことを確認した．推測であるが、Airport は Sender IPAddr が 0.0.0.0 の ARP Request を無視している．

このように gratuitous ARP の実装は機器依存であるため、IP duplicate の診断のために送信する ARP Request は gratuitous ARP ではない普通の ARP Request のほうがよい。

4.2.3　不正なサブネットマスクの診断

この診断では不正なサブネットマスクが設定されていないかを確認する。通常サブネットマスクは 192.168/16 といった書き方をするように，事前にビットパターン 1 の列が続き 0 がきた場合にはそこから下はホスト用に割り当てられるため全て 0 になるはずである．不正なサブネットマスクとは、このビットパターン 1 の列の後にきた 0 よりも後ろに、再び 1 がくるようなパターンのサブネットマスクを指す。

もし，ユーザが手動で IP アドレス，サブネットマスクの設定を行ったときに，正しくは IP アドレス 192.168.1.25，サブネットマスク 255.255.255.0，デフォルトゲートウェイ 192.168.1.254 と入力するところを，IP アドレスとサブネットマスクに同じ 192.168.1.25 という値を入力したとする。このときサブネットマスクは 11000000 10101000 ... といったような、不正なサブネットマスクである。デバイスはこのようなサブネットマスクが入力されていた場合に何らかのアクションを起こす。

4.2.4　複数台の DHCP サーバの検索

ローカルエリアネットワーク内に複数台の DHCP サーバがいないか、もし複数台いた場合はそれらが異なるネットワークアドレスを持った IP アドレスを配布していないかを診断する。デバイスは DHCPDISCOVER メッセージをブロードキャスト宛てに配信し、DHCP サーバからの DHCPOFFER を待つ。もし複数の DHCPOFFER が来た場合はその中の『client IP Address』とサブネットマスクを確認する。

もし異なるネットワークアドレスを持った IP アドレスを配布する複数台の DHCP サーバが存在した場合、デバイスは『ローカルエリアネットワーク内にはこのような複数台の DHCP サーバがいます。』とユーザに提示する。この後はユーザにどちらの DHCP サーバに IP アドレスをリクエストするかを選ばせる、といった動作が必要かと思われる。

4.2.5　デフォルトゲートウェイの診断

デバイスに設定されるデフォルトゲートウェイの IP アドレスは、デバイスと同じネットワークアドレスを持っていなければならない。もしデバイスのネットワークアドレスとデフォルトゲートウェイのネットワークアドレスが異なっていた場合はデフォルトゲートウェイのアドレス、またはデバイスの IP アドレス、またはサブネットマスクの再入力を求める。

4.3　まとめ

DLNA デバイスへ組み込む自己診断機能の提案を行なった。この自己診断機能をできるだけ多くの DLNA デバイスに組み込むことで、DLNA で発生する障害を減らすことが

できる。

診断項目として、

- リンクアップ・ダウンの診断
- IP duplicate の診断
- 不正なサブネットマスクの診断
- 複数台の DHCP サーバの検索、デフォルトゲートウェイの診断

の 4 項目を挙げ、それぞれの診断手法を述べた。

第5章　DLNAネットワーク診断機能

前章では、DLNAデバイスに組み込む自己診断機能の提案を行なった。本章ではDLNAネットワークの診断を行なう機能とその手法について検討する。

既存のネットワーク管理手法に欠かせない、障害監視・検出のツール群と、SNMPというネットワーク監視プロトコル、そしてネットワーク管理を自動で行なう機能を持つNetwork Management Serverについて、それらの機能と、動作について簡単に述べた。これらの既存のネットワーク管理の手法をホームネットワーク障害診断に適用できるかを検討した。

その結果、DLNAネットワークの診断はパケットのモニタリングと試験パケットの送信が適していると考え、DLNAネットワークで流れてくるブロードキャスト・マルチキャストフレームでどのような情報が収集できるか、どのような試験パケットを送信すればより効率よくネットワークの情報が収集できるかをまとめた。

5.1　既存のネットワーク管理手法

5.1.1　障害監視・検出のツール

障害の発生を最小限にするためには、障害が発生する前にその兆候を検出するための監視が必要になる。常日頃からネットワークの健康状態を知っておくことによって、ネットワーク拡張の予測を立てたり、外部からの攻撃を見つけられるという長所もある。以下では障害の監視・発見によく用いられるツールとその概要を述べる。

MRTG

MRTG(Multi Router Traffic Grapher)はルータのトラフィックや、サーバのディスク容量などをグラフ化して表示するツールである。類似品としてRRD Toolというものもあり、こちらはツールを組み合わせてより細かな監視を行なうことができる。

ping

pingはICMP ECHOパケットを利用してターゲットホストまでのRTTの参考値を得るツールである。パケットが回線を伝わる時間や、インタフェースでパケットを送受信す

るための時間が含まれるため、RTT の目安にしかならない。

traceroute

UDP パケットの TTL を変化させ、帰りとなる ICMP パケットによって経路を確認するツール。パケットは行きと帰りで同じルートを通るとは限らないため注意が必要になる。traceroute で確認できるのは「行き」の経路のみである。

telnet

サーバのサービスが稼動しているかを確認できる。

TTCP

2 つのホスト間で TCP パケットをバースト的に送出して、ホスト間のパケットロスや伝送時間を計測するツール。ネットワークにかなりの負担をかける。

Pathchar

大量の ICMP パケットを送出し、そのジッターを計測することで、ターゲットホストまでの回線残容量を測定する。ネットワークにかなりの負荷をかける。

BGPView

BGP-4 の経路監視を行なうツール。

その他

awk や perl といったスクリプト言語を使って、細かい監視ツールを有機的に結びつけて利用することで、きめ細かく、かつ利用しやすい管理ツールを構築できる。

5.1.2 SNMP

Simple Network Management Protocol(SNMP) は、IP ネットワーク上の機器を管理するインターネット標準プロトコルである。ルータ、スイッチ、サーバ、プリンタ、UPS といった多種多様な機器が SNMP に対応している。SNMP を用いることで遠隔地のルータやサーバ、その他のネットワーク機器の状態を把握すること、問題が起きたときに報告を送らせる、その他の操作を自動で行わせることが可能になる。

SNMP はマネージャとエージェント間のデータ転送プロトコルとして UDP を用いる。

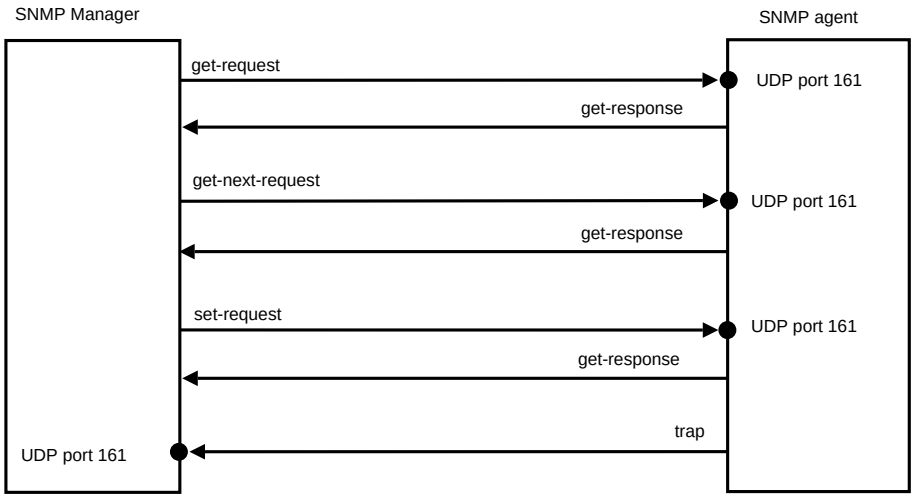

図 5.1: 5 種類の SNMP オペレータ

MIB

SNMP ベースのシステム上のマネージャとエージェント間で交換されるデータは、管理情報ベース (MIB: Management Ingormation Base) を使う。MIB はハードウェアとソフトウェアの構成要素に関する情報を交換する際の標準的な定義のセットである。各 MIB には管理可能な要素を定義する構造と、形式を指定するオブジェクトのグループが含まれている。

MIB-I

MIB-I は、TCP/IP ネットワーク上のデバイスの監視と制御に必要とされる情報ベースを正確に説明し定義する最初の標準である。MIB-I に含まれるオブジェクトは、設定制御と障害監視に不可欠である。ほかのすべての MIB は、MIB-I に基づいて構築され、MIB-I の定義を含んでいる。

MIB-II

MIB-II では、MIB で定義するオブジェクトのセットを拡大することで、MIB-I で定義された情報を拡張している。MIB-II に拡張されたオブジェクトのタイプには、さまざまな転送媒体タイプを処理するオブジェクト、および SNMP を使ってネットワーク管理自体を制御し、監視するオブジェクトが含まれている。

5.1.3 ネットワーク管理ツール

主なネットワーク管理ツール

ネットワーク管理を行うツールはさまざまなベンダーから製品として売りに出されている。ここではHP OpenView [6], DAIKIN COMTEC PNDDA [7] の2つのネットワーク管理ツールを挙げ、その特徴と動作について説明をする。

HP OpenView NNM HP OpenView Network Node Manager(NNM) はHP社のライセンス商品である。SNMPv1, SNMPv2、TCP/IP、IPX/DMI、UDP、ICMP、ARP/RARPのプロトコルを使って、ネットワーク上の管理対象デバイスとの通信チャネルを維持する。

NNM はSNMP を主要なプロトコルとして使用している。NNM は ARPA ファミリー、バークレーファミリー、NFS ファミリーなど、他の下位レベルのプロトコル・ファミリーも用いる。これらのプロトコルはファイル転送、電子メール、リモート・ログインなどの機能で使う。NNM はネットワークのマップを表示し、マップのシンボルは色の変化で障害の状況を示す。重要な情報の収集は基本的なSNMP サービスを用いて行う。

NNM はネットワーク上のデバイスを自動検出し、デバイスと他のデバイスとの接続関係も自動検出する。検出した情報はNNM のオブジェクトデータベースとトポロジデータベースに保存される。NNM はこれらのデータベースからデフォルトマップを描き、イベント・トラッキングシステムを設定する。

PNDDA PNDDA は物理ネットワークを自動表示するネットワーク統合管理アプライアンスである。

PNDDA が管理の対象とするのはSNMP エージェント機能を搭載した機器、Ping 応答機能を持った機器である。SNMP エージェント機能を持つ機器にはSNMP ポーリングを行い管理情報を収集し、非SNMP 機器にはPing を使用してデバイスへの到達性を確認する。障害診断には機器のSNMP トラップを用いるので管理側のイベントフィルタの設定は不要となっている。PNDDA も HTML+JAVA を用いてユーザインタフェースを提供しているため、実際の機器の管理はリモートからWeb ブラウザで行うことができる。

PNDDA の導入手順について簡単に述べる。PNDDA にあるLAN ポートにケーブルを接続し、管理するネットワークにPNDDA を参加させる。PNDDA 自身のIP アドレス、サブネットマスク、デフォルトゲートウェイの設定をキーボードから行う。最後にWeb ブラウザを使用して監視範囲を指定する。これでPNDDA の導入作業は終了する。この設定が終わればPNDDA は自動的に監視範囲のネットワークのインベントリー収集-監視を開始する。

表5.1 にPNDDA が管理の対象とする機器とその管理に用いるプロトコルを示す。

表 5.1: PNDDA の管理対象機器と機器の管理に用いるプロトコル

機器	使用するプロトコル
スイッチングハブ	SNMP+Ping
ハブ	SNMP エージェント搭載機器
サーバ、プリンタ	Ping
PC(Win, Mac 機)	Ping

管理可能デバイス数は 100〜15,000 デバイスとなっている。複数台の PNDDA を集中監視する機能を用いれば 15000 デバイス以上でも一元管理が可能になる。

初期検出プロセス

初期検出プロセスでは、どのネットワークに対してデバイスの検索を行なうかが問題になる。このネットワークの選び方は、自分が足を生やしているネットワークで検索を行なうというものと、ユーザにどのネットワークを検索するのかといった情報が書かれている Seed ファイルを手動で作成してもらう、マップ中のシンボルを手操作で選択することで管理対象に設定するなどがある。

NNM は DHCP でデバイスを検索するセグメントを決めることができる。DHCP サーバ Polling Option を ON にすると DHCP サーバから配布されたネットワークアドレスを初期検出の範囲にあてる。

NMS はいずれかの方法で取得した初期検出範囲にデバイスが存在しないかを確認する。このデバイスの検索は自分と同じ LAN 内にいる IP アドレスに対して ICMP Echo Request または ARP Request を発行することで行なう。それぞれの Request に対する Reply が来た場合そのデバイスを検出したとし、自身が持つネットワークトポロジデータベース等に加える。

NMS は snmpwalk を発行し、検出されたデバイスからインタフェース情報や ARP Table 等の新たな情報が引き出そうと試みる。デバイスの ARP table を取得できた場合、table のリストにあるデバイスを初期検出のプロセスに追加する。デバイスがトポロジデータベースに追加されると、それらのデバイスに対し新たに Echo Request などを行う。返事がきたらトポロジデータベースに加える。そしてさらにそのデバイスに snmpwalk 要求を発行するといったようにして NMS は管理ドメインを拡大する。

NNM は初期検出プロセスが完了した後にデフォルトマップを見て、初期マップが正しく抜けがないかどうかを確かめる必要がある。これは初期マップ検出プロセスではネットワーク設定上の問題を見つけることがあるためだとしている。この問題とは、適切な通信を行わない SNMP エージェント、不適切なサブネット・マスク、DNS 設定、コミュニティ名の不一致、所有していないネットワークセグメントへの予期しない接続といったも

のである。
　この初期検出に関するトラブルは、多くの場合

・ GET 用および SET 用コミュニティ名が public でない
・ DNS 名解決の矛盾
・ IP アドレスの重複
・ 不正なサブネット・マスク
・ 特定のデバイス上の SNMP エージェント設定の不具合

　のようなネットワーク設定の誤りが原因で生じると NNM は述べ、それらに対するトラブルシューティングのサンプルを用意している。

初期検出後の監視

　検出したデバイスの稼動状況の監視や、デバイス間のネットワークトラフィックの監視などを行なう。ポーリング間隔の設定や閾値の設定をデバイス毎に行うことができる。稼動が確認できなかったり、ある特定の値が設定した閾値を超えた場合、障害を検出したと設定できる。障害を検出した時にどのような動作をするかもデバイス毎に設定できるものが多い。障害通知方法の設定では、ログの取得、ビープ音を鳴らす、メールを送信する、電話をかける、UNIX コマンドの実行、set コマンドの送信、アラームウィンドウの自動オープンなどがある。

5.1.4　既存の手法の問題

　既存の障害監視・発見のツールは利用に IP アドレスの入力を必要としたり、何かしらの設定を行ったりとネットワークの知識を必要とするうえに、DLNA 対応の家電しかホームネットワークに存在しない家庭の場合はこれらのツールを使うことができない。
　既存のネットワーク管理ソフトウェアは、管理する IP ネットワークの範囲をユーザにあらかじめ指定させたり、ネットワーク検出プロセスでの間違いをユーザに発見させるといったところがあるため、ネットワークの知識の無いユーザには敷居の高いものになっている。
　ほとんどの製品が SNMP を用いて障害の管理を行なっていることも問題である。SNMP はネットワーク管理においては欠かせない技術であるがホームネットワーク機器で SNMP を実装している機器はほとんどない。SNMP に対応した一般家庭向けのブロードバンドルータや小型の L2 スイッチは比較的安価なものが出回っているが、これらの SNMP 対応の製品が一般家庭に完全に普及してはいない。
　SNMP 対応の L2 スイッチをホームネットワークの中央に配置できれば、既存のネットワーク管理手法で機器構成管理、障害管理などがある程度容易になる。しかし、そのため

にはL2スイッチにIPアドレスを割り当てる作業が必要になる。このような作業はユーザへの負担になると考えられ、結果SNMP対応のL2スイッチの導入は難しいといえる。

これらのような理由から、既存の障害監視・発見のツールやネットワーク管理ソフトウェア・アプライアンスをホームネットワークの障害管理にそのまま使用するのは難しいといえる。

5.2 パケットモニタリングによる情報の収集

既存のネットワーク管理ソフトウェア・アプライアンスでは，主なプロトコルにSNMPを用いていると述べた．しかし，最近SNMPを実装した機器が安価に手に入るようにはなってきたものの，全ての機器にエージェントの機能を持たせるのは不可能である．また，SNMPにはUDPであるためにIP層での通信が成り立たないと，メッセージの交換ができなくなる．

ホームネットワークは比較的小規模なネットワークであるため，複数セグメントにまたがってネットワークの管理を行なうような従来の手法全てを実装する必要はない．

このような小さいネットワークであれば、ブロードキャスト・マルチキャストフレームに着目することで情報が収集できると考え、パケットモニタリングによるネットワーク情報の収集を検討する。

次のブロードキャスト・マルチキャストフレームからの学習ではDLNAで流れてくるブロードキャストフレーム，マルチキャストフレームからどのような情報が得られるかを述べた．このブロードキャスト・マルチキャストフレームの学習に試験パケットの送信を付け加えた手法についても検討する．

5.2.1 ブロードキャスト・マルチキャストフレームからの学習

DLNAネットワークでネットワークモニタリングを行なうことで、どのような情報が収集できるかを述べた。DLNAネットワークを流れるブロードキャストメッセージは以下のものが想定される．

- IPアドレス解決のために送信されるARP Requstメッセージ
- 動的なIPアドレスの割り当てを行なうDHCPメッセージ
- DLNAデバイスのdiscoverに用いられるSSDPメッセージ

これらのメッセージからどのような情報が収集できるかをまとめた。

ARP Request

ARP RequestはIPアドレスとMACアドレスのアドレス解決をするために送信するパケットである．ブロードキャストフレームとして流されるため，同じセグメントに属する

デバイスで，データリンク層での通信が行なえる状態ならばパケットモニタリングで確認できる．ARP Request はブロードキャストであるうえに，送信元の IP アドレスと MAC アドレスの組を取得でき，リクエスト内容からそのリクエスト送信者のサブネットマスクの予測までできる非常に有用なパケットである．

リクエスト送信元デバイスの IP アドレスと MAC アドレス ARP Request を収集することで，そのネットワークセグメント内にどのようなデバイスが存在するかが分かる．ARP Request はブロードキャストフレームであるため，ルータを超えない．ARP Request に対する ARP Reply はユニキャストであるために間に L2 スイッチが挟まっている状態では他のデバイスへの ARP Reply は見ることができない．

ARP Request には Ruquest 送信元の IP アドレス・MAC アドレス情報が含まれているため，ARP Request の収集をすることでそのセグメント内にいるデバイスの IP アドレス・MAC アドレスのマッピングされた情報が取得できる．ARP Request は同じネットワークセグメント内にいるデバイスと IP 通信をする時には必ず送信される．

リクエスト送信元デバイスのサブネットマスク ARP Request から，Request 送信元のサブネットマスクが推定できる．ARP Request は同じネットワークセグメントに属する（と Sender が思っている）IP アドレスを持つデバイスの MAC アドレスを解決するために用いられる．そのため ARP Request の Sender 情報と Target 情報から，Sender が Target の IP アドレスを同じネットワークセグメントと認識するようなサブネットマスクを Sender が持っていることが分かる．

サブネットマスクは次のように推測する．ある Sender が 2 つの IP アドレスについて ARP Request を出していたとする．

Sender IP アドレス	192.168.3.115	11000000	10101000	00000011	01110011
Target IP アドレス 1	192.168.3.25	11000000	10101000	00000011	00011001
Target IP アドレス 2	192.168.3.231	11000000	10101000	00000011	11100111

Sender IP アドレスのビットと，Target IP アドレスのビットをこれらの情報から Sender のサブネットマスクは 255.255.255.0 という 24 ビットのマスクではないかと推測できる．この推測の後に新たに Sender が 192.18.2.2 を Target とした ARP Request を出した場合，テーブルに次のように書き加えられる．

Sender IP アドレス	192.168.3.115	11000000	10101000	00000011	01110011
Target IP アドレス 1	192.168.3.25	11000000	10101000	00000011	00011001
Target IP アドレス 2	192.168.3.231	11000000	10101000	00000011	11100111
Target IP アドレス 3	192.168.2.2	11000000	10101000	00000010	00000010

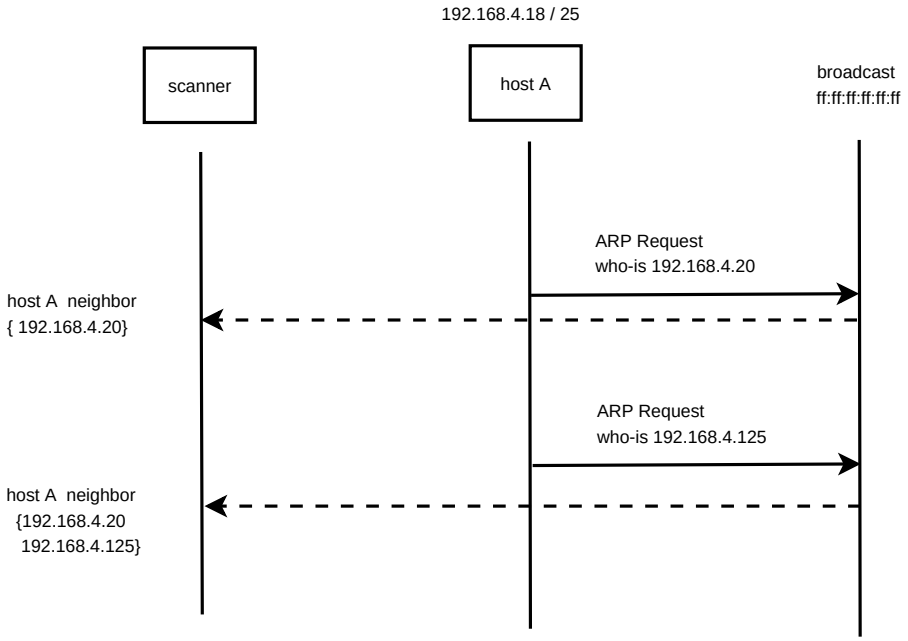

図 5.2: ARP request によるサブネットマスクの推定

この新たに追加された Target IP アドレス 3 から，Target IP アドレスのネットマスクは 255.255.254.0 の 23 ビット長のマスクであると推測できる．

このように、ARP Request は有用なパケットである。ARP Request からは、Sender IP アドレスを持ったデバイスが、リンクローカルエリアネットワーク内に存在することがわかる。ARP Request の Sender IP アドレスと Target IP アドレスの組は、Sender のサブネットマスクを推測するための手がかりになる。

DHCP メッセージ

DHCP メッセージは、DLNA デバイスが

もしもそのネットワークが DHCP サーバによって IP アドレスを割り当てを管理されていた場合，DHCPDISCOVER メッセージを送信することでこのネットワークのアドレスとネットマスクを知ることが出来る．これは DHCP サーバがいた場合であり，もしも DHCP サーバが発見できなかった場合はそのネットワークは管理されていないネットワークであるとし，3.2 の Addressing で定められる通り 169.254/16 のアドレスがそのネットワークのアドレスであると考える．

新規参入ノードの確認 初期状態の DHCP クライアントはに DHCPDISCOVER メッセージをブロードキャストし，DHCP サーバの発見と IP アドレスやその他の設定項目の要

求をする．図 5.3 に DHCP クライアントの状態遷移図を示す。INIT または REBOOT 時には DHCPDISCOVER を発し、DHCP サーバからの OFFER を待つ。

DHCP サーバの情報を取得 DHCPDISCOVER や DHCPREQEUST メッセージに対する DHCP サーバからの応答である DHCP OFFER もクライアントの IP アドレスが定まっていない場合は宛先 IP アドレス 0.0.0.0 のブロードキャスト宛てに送信される．そのため、どのような DHCP サーバがそのネットワークでアドレスを配布しているかを知ることができる。

もしもネットワークアドレスの異なる IP アドレスや、長さの異なるサブネットマスクを配布するような複数台の DHCP サーバがいた場合、ネットワークのモニタリングで発見することができる。

同一セグメント内の他のホストへの手がかり DHCP サーバが配布するネットワークアドレスは、同一のネットワーク上にいるかもしれない他のデバイスへの手がかりとなる。

SSDP メッセージ

239.255.255.250:1900 宛てに流れるパケットを監視することで UPnP デバイスやサービスが流す Advertisement を発見できる．この 239:255:255:250:1900 宛てに流されるメッセージには DLNA デバイスの Discovery に用いられる SSDP メッセージが含まれる．

SSDP メッセージは Advertisement と Search の 2 種類がある．Advertisement は ssdp:alive と ssdp:byebye の 2 種類がある。ssdp:alive は DLNA の MediaServer などが自身と自身の持つサービスを広告するために定期的に流してくる。ssdp:byebye は逆にデバイスがマルチキャストグループから離れることを意味しており、デバイスやサービスが自身を終了させるときに流すメッセージである。

M-SEARCH メッセージ M-SEARCH メッセージは、DLNA の Media Renderer などがコンテンツを提供してくれる Media Server をなどを探すときに用いられる。

NOTIFY メッセージ 図 5.4 は DiXiM Media Server の NOTIFY メッセージである．この NOTIFY メッセージには様々な情報が含まれている．まず LOCATION 部には DiXiM Media Server の Description の場所が書かれている．SERVER 部には OS の Version と UPnP のバージョン、そして製品のバージョンが記されている。USN にはデバイスを識別するための uuid が含まれている。

このように 239.255.255.250:1900 のマルチキャストフレームをリッスンすることで DLNA(UPnP) デバイスの情報が得られる。NOTIFY メッセージで広告されている LOCATION に対して GET 要求を行なうことでその DLNA デバイスのディスクリプションを得ることもできる。

まとめ

DLNA ネットワークを流れるブロードキャスト、マルチキャストフレームをモニタリングすることで、どのような情報が得られるかを述べた。ARP Request からはデバイスの存在の確認と、Sender と Target IP アドレスの組から Sender のサブネットマスクをある程度推測することができる。

DHCPDISCOVER メッセージからはホームネットワークに新規に参入するデバイスを発見することができる。DHCPOFFER からは DHCP サーバの配布するネットワークアドレスやサブネットマスクなどの情報がわかる。

SSDP メッセージからは DLNA デバイスの存在が確認できる。

5.3 試験パケットの送信による情報の収集

パケットモニタリングのみでデバイスの発見を行なうのは時間がかかりすぎたり、何のパケットも流さないデバイスがもしいた場合、そのようなデバイスをパケットモニタリングは発見するのは不可能である。

ここでは試験パケットの送信による情報の収集について述べる。使用するメッセージは

- `ARP Request` メッセージ
- `DHCPDISCOVER` メッセージ
- `SSDP NOTIFY` メッセージ
- `SSDP M-SEARCH` メッセージ

の 4 つである。

5.3.1 ARP Request メッセージ

ARP Request の送信で IP Duplicate の発見ができる。ARP Request の Target IP Address を、0.0.0.0 から 255.255.255.255 までのすべての IP アドレスに対して送信すれば、すべての IP アドレスと MAC アドレスの組を得ることができる。しかし、これを行なうと膨大な時間とネットワークの帯域をロスすることになる。試験的に 255 ノードへの ARP Request を行なってみた。全二重の 100baseTX で 255 個の ARP Request を送信するのに大体 6 秒から 8 秒かかった。0.0.0.0 から 0.0.255.255 までのノードを発見するためには 8 秒の 255 倍で 2040 秒かかる見込みになる。0.255.255.255. まで走査するならばさらに 255 倍で 520200 秒で約 144 時間の見込みになり、時間的にもあまり現実的ではない。

5.3.2 DHCPDISCOVER メッセージ

DHCPDISCOVER メッセージを発することで、同じリンクローカルなネットワークに存在する DHCP サーバに対して IP アドレスの要求を行うことができる。

5.3.3 SSDP M-SEARCH メッセージ

M-SEARCH メッセージの例を図 5.5 に示す。ST の部分が Search Target 部である。ここで探したいデバイスやサービスを指定すればよい。

5.3.4 DHCPDISCOVER + ARP Request

DHCPDISCOVER と ARP Request を組み合わせることで効率よくノードの探索が行なえる。4.1.2 節のような状況の場合、DHCPDISCOVER を送信すると 2 台の DHCP サーバからそれぞれ OFFER がくる。OFFER の内容を見て ARP Request を送信すれば、ノードを発見できる確率が高い。

5.3.5 考察

試験パケットの送信とパケットモニタリングを組み合わせる場合は、試験パケットであると見分けが付くようにするべきである。でなければ、他デバイスがパケットモニタリングによる学習を行なっていた場合などに精度を下げる原因になってしまう。実験では ARP メッセージの padding の部分に文字列を追加することで、この ARP メッセージが試験パケットであると示している。試験パケットであった場合はそのパケットを無視するようにすればよい。

試験パケットの送信から ARP Request が作られることがある。

5.4 まとめ

パケットモニタリングでの学習で、DLNA ネットワークに存在するデバイスを発見することが可能になった。また、IP 的に unreqchable な状態にあるデバイスの発見も可能になった。SSDP M-SEARCH メッセージから ARP Request が生成されることもある。この手法を上手く使えば相手のサブネットマスクを特定することができる。

これらの手法を用いることで DLNA ネットワークの情報を収集するホームネットワーク障害診断スキャナを生成することが可能になる。

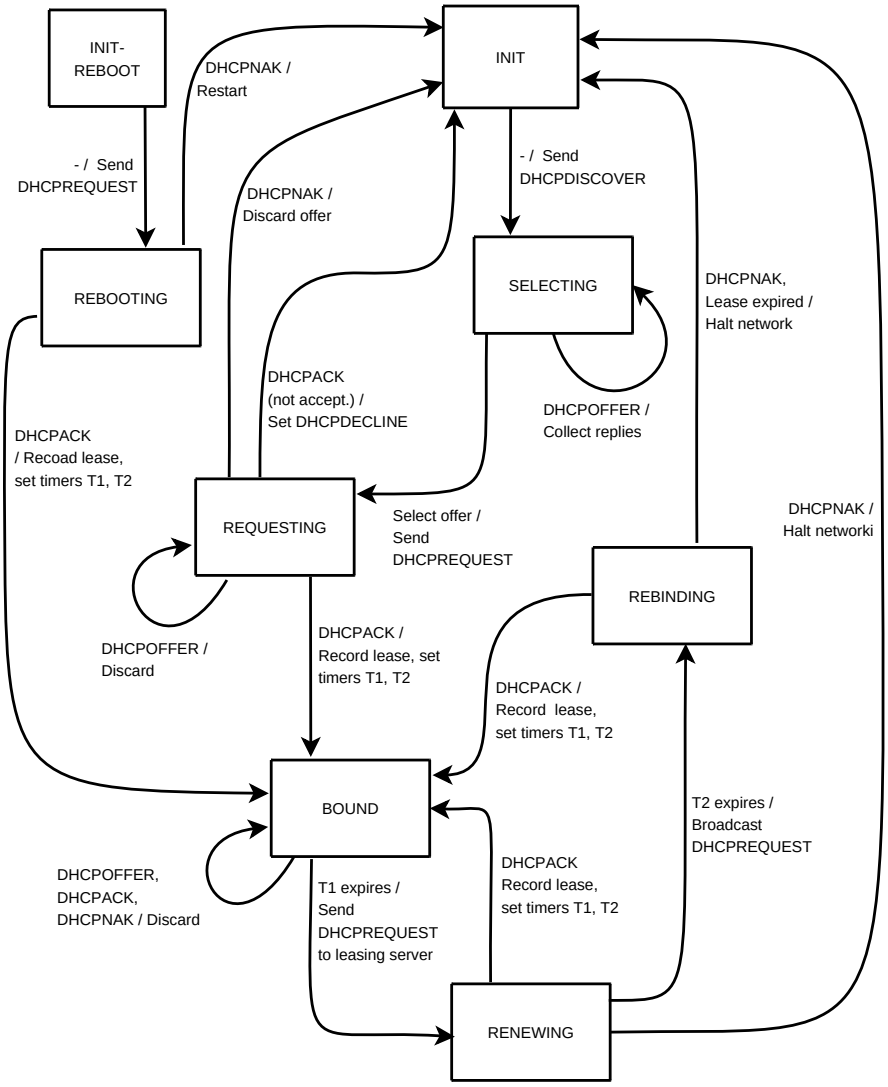

図 5.3: DHCP Client の状態遷移図

NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
CHACHE-CONTROL: max-age = 1800
LOCATION: http://192.168.0.12:30000
NT: upnp:rootdevice
NTS: ssdp:alive
SERVER: Windows/5.1 UPnP/1.0 DigiOn DiXiM UPnP/1.0
USN: uuid:e68818b5-82d0-64fa-3a61-684e61c5f1db::upnp:rootdevice

図 5.4: DiXiM Media Server の NOTIFY(ssdp:alive)

M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MX: 1
ST: usr:schemas-upnp-org:device:MediaServer:1

図 5.5: SSDP M-SEARCH メッセージの例

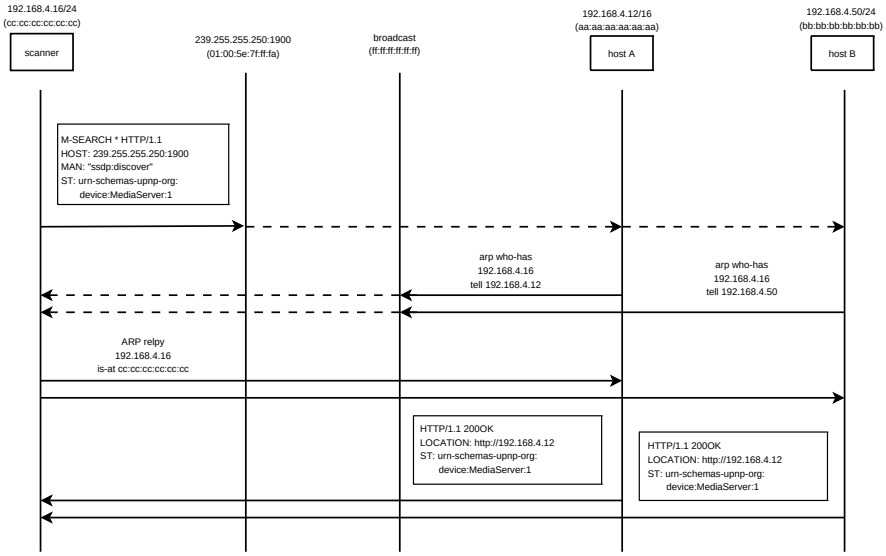

図 5.6: SSDP M-SEARCH から発生する ARP Request

第6章　まとめ

本研究では，様々な規格からなるホームネットワーク規格全体の障害診断を行なうために、障害診断とユーザインタフェースを備えるツール、ホームネットワークの情報を収集するホームネットワーク情報収集スキャナからなる、ホームネットワーク障害診断システムを提案した。

DLNA 機器の障害診断について，デバイスに組み込む自己診断機能の提案した。そしてホームネットワーク情報の収集法として，パケットモニタリングによる学習と試験パケットの送信を加えた手法を提案した.

6.1　今後の課題

今後の課題として DLNA ネットワークにおけるホームネットワーク障害診断ツールと情報収集スキャナの詳細な設計と実装、また DLNA の障害について実効帯域幅の障害をどのように検出するかが今後の課題である。

DLNA ネットワークのツールとスキャナを完成させた後、DLNA 以外の接続規格の障害診断手法を検討し、ホームネットワーク障害診断システムの完成を目指す。

謝辞

本研究をまとめるにあたり、常に暖かくご指導くださった丹康雄助教授に深く感謝致します。

参考文献

[1] 丹康雄監修 宅内情報通信・放送高度化フォーラム編 (2004), ホームネットワークと情報家電, オーム社.

[2] UPnP^{TM} Forum, on-line http://www.upnp.org/.

[3] ECHONET コンソーシアム, http://www.echonet.gr.jp/.

[4] Digital Living Network Alliance, http://www.dlna.org/en/consumer/home

[5] UPnP^{TM} Forum, UPnP Device Architecture, UPnP Forunm, 2000.

[6] 日本ヒューレット・パッカード社, HP OpenView, http://h50146.www5.hp.com/products/software/management/openview/index.html

[7] ダイキン工業株式会社, PNDDA, http://www.comtec.daikin.co.jp/IM/prd/pndda/.

[8] Douglas R.Mauro, Kevin J.Schmidt, 入門SNMP, オライリー・ジャパン, 2002.

[9] Ramesh Govindan and Hongsuda Tangmunarunkit, “ Heirustics for Internet Map Doscovery ”, In IEEE INFOCOM 2000, pp.1371-1380, Tel Aviv, Israel, Mar 2000. IEEE

[10] Erik T. Ray, 入門XML 第2版, オライリー・ジャパン, 2004.

[11] W リチャード・スティーブンス, 詳解 TCP/IP Vol,1, 株式会社ピアソン・エデュケーション.

[12] R.Siamwalla, R.Sharma, S. Keshav, “ Discovering Internet Topology ”.

[13] V. Jacobson, “ Congestion Avoidance and Control ”. In Proc. of the ACM SIGCOMM'88 Conference, Aug 1988.

[14] arpwatch, on-line available at http://www.securityfocus.com/tools/142.

[15] Wireshark, http://wireshark.org/.