イーサネットネットワークにおけるリンク制御方式の提案

渡辺　泰之†　　山崎　克之†

† 株式会社 KDDI 研究所
〒 356–8502 埼玉県上福岡市大原 2–1–15
E-mail: †{yasuyuki,yamazaki}@kddilabs.jp

あらまし　イーサネット技術の発展に伴って，その高速性・利用の簡便性等からイーサネットの適用領域が従来の LAN から MAN，WAN へと拡大しており，イーサネットベースの広域レイヤ 2 ネットワークの構築が進んでいる．ところが，イーサネットには能動的にリンクの状態を確認する機能，接続先デバイスの情報を収集する機能がないため，広域におけるレイヤ 2 ネットワークの運用管理が困難なものとなっている．本稿では，イーサネットレベルでリンク接続状況を伝達するためのプロトコル，およびそのプロトコルを利用したリンク制御方式を提案し，その詳細を説明する．また，本方式を PC UNIX 上へ実装し，イーサネットネットワークの運用管理の改善に有効であることを示す．
キーワード　イーサネット，運用管理，リンク制御

A Proposal of a Protocol and a Method for Ethernet Link Control

Yasuyuki WATANABE† and Katsuyuki YAMAZAKI†

† KDDI R&D Laboratories Inc.
2–1–15 Ohara, Kamifukuoka-shi, Saitama, 356-8502 Japan
E-mail: †{yasuyuki,yamazaki}@kddilabs.jp

Abstract　With the development of Ethernet technology such as Gigabit and 10 Gigabit Ethernet, Ethernet is getting widely used in not only LAN but also MAN or WAN environment due to its higher bandwidth, lower cost and easy-of-use characteristics. However, Ethernet does not provide the function of in-service measurement of link status as well as the information exchange of peer or neighbor devices, which make operation and management of an Ethernet network difficult especially for wide-area network. In this paper, we propose a layer 2 protocol which convey the information between Ethernet devices and a method for Ethernet link control using this protocol. We also have implemented the protocol on the PC UNIX platform. By showing some test results with the PC platforms, we have proven this method effective for improvement of operation and management of Ethernet networks.
Key words　Ethernet, Operation and Management, Link Control

1. はじめに

イーサネット技術の発展に伴って，その高速性や利用の簡便性等からイーサネットの適用領域が従来の LAN から MAN，WAN へと拡大している．長距離伝送が可能なギガビットイーサネットの普及や 10 ギガビットイーサネットの出現，あるいは WDM や SDH ベースのイーサネット多重化装置の利用によって，キャリアの提供するサービスも従来の専用線，ATM/フレームリレーからイーサネット接続サービスへと移行しつつあり，イーサネットベースの広域レイヤ 2 ネットワークの構築が進んでいる．ところが，イーサネットはもともと LAN の技術ということもあり，能動的にリンクの状態を確認する機能や接続先デバイスの情報を取得する機能がないため，広域におけるレイヤ 2 ネットワークの運用管理が困難なものとなっている [1] [2].

本稿では，まず 2. 項においてイーサネットベースのレイヤ 2 ネットワークの運用管理面での課題を整理するとともに，その解決に向けてイーサネット自身に必要な機能について述べる．次に 3. 項において，本稿で提案するイーサネットレベルでリンク接続状況を伝達するプロトコルである BNDP（Bridge Neighbor Discovery Protocol）の説明を行い，4. 項では BNDP を用いたリンク制御方式について述べる．5. 項では，BNDP を PC UNIX 上に実装して機能評価を実施した内容を紹介するとともに，6. 項において BNDP の仕様や機能に関する考察を行う．

2. イーサネットネットワークにおける運用上の課題

イーサネットスイッチベースのネットワークを広域で構築する場合に，運用管理上問題となる項目を整理すると，以下のような項目が挙げられる．

- リンク接続状況の確認

イーサネットネットワークの運用管理上まず問題となるのは，イーサネットには隣接デバイス間のリンク接続状況を確認する手段がないことである．

2台のイーサネット機器を接続する場合，通常レイヤ2での接続性は隣接するデバイスとの間のリンクのアップ/ダウンにより判断する．これは2台の機器が1本のリンクで接続されている場合はよいが，イーサネットネットワークを広域に拡張する際によく用いられるように，機器間にメディアコンバータやブリッジ等が挿入される，あるいはL2TP（Layer Two Tunneling Protocol）やEoMPLS（Ethernet over MPLS）技術を利用したイーサネット接続サービス等を利用するような場合には，機器間が複数のリンクによって接続されることになるため，単一のリンクのアップ/ダウンにより必ずしも2台のイーサネット機器間の接続性が判断できない．

リンク間に挿入される機器によっては，リンク断を検知すると他のリンクへ障害情報を転送する機能を持つものもあるが，必ずしも全ての機器が対応しているわけではない．

- 接続先デバイスの設定情報の確認

次に問題となるのは，イーサネットには隣接デバイスの情報を収集する機能がないため，接続先のデバイスやポートの設定情報を確認できないことである．

そのため，物理的な接続構成を常に把握しておく必要があるが，広域でネットワークを構築する場合には，必ずしも接続構成がすぐに確認できる場所に機器があるとは限らないため，機器間で設定情報を確認する手段があれば有用である．

上記2つの課題に関しては，問題点は共通しており，イーサネットにおいて隣接デバイス間でリンク状況や設定情報を伝達するためのメカニズムがないことに起因していると考えられる．イーサネットスイッチ等には，レイヤ3（IP）のレベルで隣接デバイスとの情報交換を行うための機能が実装されている機器もあるが，IPの利用を前提としていたり，ベンダ独自機能であるため，マルチベンダで構成するレイヤ2ネットワークの管理には適切でない場合があり，やはりイーサネットレベルでの実現が必要と考えられる．

以上まとめると，イーサネットネットワークにおける運用管理の改善には，イーサネットの標準的な機能として，デバイス間のリンクの状態を能動的に確認する機能，および対向デバイスの情報を取得する機能が必要であり，本稿ではそのためのプロトコルとしてBNDP（Bridge Neighbor Discovery Protocol）を定義するとともに，BNDPを用いたリンク制御方式を提案する[3]．

3. BNDP

3.1 概要と特徴

BNDPは，イーサネットインタフェース間でポート情報の交換および接続性の確認を行うレイヤ2プロトコルであり，以下の特徴を持つ．

- 自身のデバイス識別子とポート識別子を含むフレームを定期的に送出する．
- フレームの宛先アドレスは，BNDP用に割り当てられたリンク制限付きマルチキャストアドレスとし，対向機器以遠には転送されないものとする．
- 受信側では，フレームに含まれるデバイス識別子とポート識別子により接続先を確認するとともに，一定時間内にフレームを受信しなかった場合に接続性が失われたと判断する．
- 対向デバイスが複数存在する場合にも対応する．すなわち，ポイント-ポイント構成に加えて，ポイント-マルチポイントの構成にも適用可能である．

BNDPの動作概要を図1に示す．まず，BNDPが有効化されたポートにおいては，自身のデバイス識別子とポート識別子を含むフレームを定期的（hellotime）に送出する．フレームの宛先アドレスは，STP（Spanning Tree Protocol）[4]におけるBPDU（Bridge Protocol Data Unit）の転送等にも用いられる予約済みマルチキャストアドレスとし，BNDP用に定義されたアドレスを利用する．このマルチキャストアドレスを宛先アドレスとして持つフレームは，ブリッジによって転送されないため，単一のリンクの範囲内でのみ有効となるが，BNDPを解釈しないブリッジにおいては透過的にフレームを通過させることが可能である．また，ユニキャストではなくマルチキャストアドレスを用いることにより，接続先デバイスのレイヤ2アドレスを事前に確認しなくてもフレームの送出が可能である．

フレームの受信側では，フレームに含まれるデバイス識別子とポート識別子により接続先デバイスを確認するとともに，最後にフレームを受信した瞬間からタイマーを作動させ，一定時間内（maxage）に次のフレームを受信しなかった場合には，対向デバイスとの接続性が失われたと判断することができる．

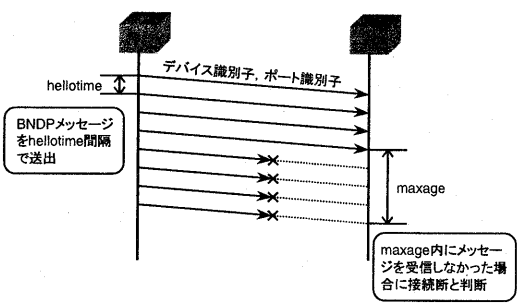

図1 BNDPの動作概要
Fig. 1 Overview of BNDP

No.	Device	Port	Aging
1	00:00:D1:EF:76:35	1	100

図 2　アドレステーブル
Fig. 2　Address table

3.2 状　　態

BNDP では以下の 4 つの状態を持つ.

（1） disabled

インタフェースが利用不可である状態.

（2） blocking

インタフェースが利用可能となった状態. BNDP メッセージの受信のみを行い，フレーム送信および BNDP メッセージ以外のフレーム受信は行わない.

（3） listening

BNDP メッセージの送受信のみを行う. BNDP メッセージは一定間隔（hellotime）で送信する. 一般フレームの送受信は行わない.

（4） forwarding

BNDP メッセージの送受信および一般フレームの送受信を行う. BNDP メッセージは一定間隔（hellotime）で送信する.

また，インタフェース毎に図 2 に示すようなアドレステーブルを 1 つ持ち，blocking，listening，forwarding 状態において BNDP メッセージを受信した場合，BNDP メッセージの内容に基づいてアドレステーブルに項目を追加するものとする.

- アドレステーブルにおいて，Device，Port はそれぞれ接続先のデバイス識別子，ポート識別子を，また Aging は BNDP メッセージを受信してからの経過時間（単位は ms）を表すものとする.
- すでにアドレステーブルに存在するデバイス識別子，ポート識別子を持つ BNDP メッセージを受信した場合は，その Aging のみが更新（リセット）される.
- 各項目の Aging は逐次更新され，一定時間（maxage）経過した場合，その項目はアドレステーブルから削除される. ここで maxage>hellotime とする.

3.3 状態遷移

BNDP では，図 3 に示す通り以下のような状態遷移を行う.

（1） disabled 状態において，インタフェースが利用可能となると blocking 状態へ移行する.

（2） blocking 状態において，以下のいずれかの場合に listening 状態へ移行する.

- BNDP メッセージを受信する.
- blocking 状態となってから一定時間（maxage）経過する.

（3） listening 状態において，一定時間（forward delay）経過の後に forwarding 状態へ移行する. ここで forward delay≧maxage とする.

（4） listening または forwarding 状態において，アドレステーブルの中身が空（すべての接続先デバイスが maxage 経過）になった場合，blocking 状態へ移行する.

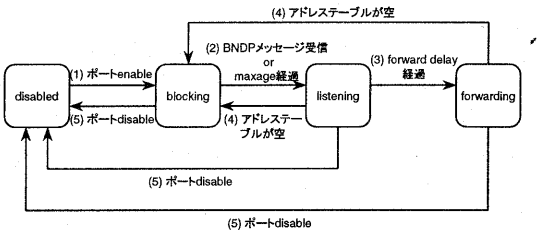

図 3　状態遷移
Fig. 3　State machine

（5） blocking，listening，forwarding 状態において，インタフェースが利用不可となると disabled 状態へ移行する.

3.4 BNDP メッセージフォーマット

BNDP におけるメッセージフォーマットを図 4（左）に示す. また，各フィールドの説明を以下に示す.

（1） プロトコル識別子

BNDP のプロトコル識別子. MAC フレームへの LLC カプセル化を行うプロトコルには STP（0x0000）や GARP（Generic Attribute Registration Protocol）[4]（0x0001）があるが，それらとは異なる値を持つものとする.

（2） プロトコルバージョン

BNDP のバージョン番号. 現状では 0x00 とする.

（3） デバイス識別子

各デバイスでユニークなデバイスの識別子. 例えば，各デバイスが具備するイーサネットインタフェースの 1 つを任意に選択し，その MAC アドレスを利用すること等が考えられる.

（4） ポート識別子

BNDP フレームを送出するインタフェースの識別子. 同一デバイス上のポートについてはユニークな識別子が割り当てられるものとする.

（5） maxage

maxage タイマー. 1/256 秒単位で指定し，デフォルト値は

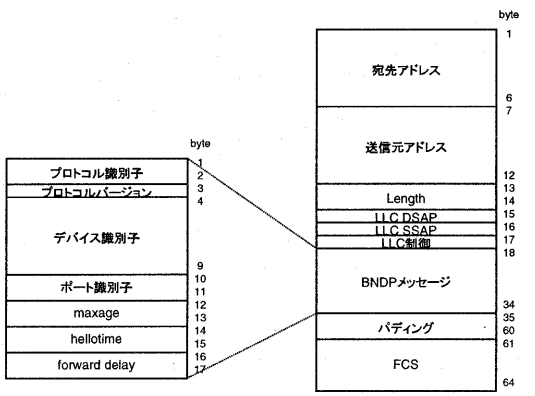

図 4　フレームフォーマット
Fig. 4　Frame format

2秒とする．

（6） hellotime

hellotime タイマー．1/256 秒単位で指定し，デフォルト値は1秒とする．

（7） forward delay

forward delay タイマー．1/256 秒単位で指定し，デフォルト値は2秒とする．

3.5 フレームフォーマット

BNDP メッセージは，図4（右）に示すように MAC フレームへ LLC カプセル化される．各フィールドの説明を以下に示す．

（1） 宛先アドレス

マルチキャストアドレスとして予約されている 01-80-C2-00-00-00〜0F の中から，未使用のアドレスを BNDP 用として利用する．

（2） 送信元アドレス

BNDP メッセージフレームを送信するインタフェースの MAC アドレスとする．

（3） Length

LLC DSAP フィールドから BNDP メッセージフィールドまでの長さであり，20 バイト（=0x14）となる．

（4） LLC DSAP，LLC SSAP，LLC 制御

LLC DSAP/SSAP には，IEEE802.1 での使用のために割り当てられている値（0x42）を用い，LLC 制御としてはコネクションレス型のデータ交換を表す値（0x03）をとる．

（5） BNDP メッセージ

上記に示す BNDP メッセージが入る．

（6） パディング

フレーム長を 64 バイトとするためのパディングとし，26 バイトを 0x00 で埋める．

（7） FCS

フレームチェックシーケンス．

4. BNDP を用いたリンク制御

イーサネットインタフェース間で BNDP を動作させることにより，各インタフェースではアドレステーブルにより接続先のデバイスおよびリンク状況の確認を行うことできる．アドレステーブルには，複数のデバイスを登録することができるため，同時に複数の接続先の管理を行うことが可能である．

また，forwarding 状態をインタフェースアップ，それ以外の状態ではインタフェースダウンと認識させることにより，BNDP のタイマー設定値に応じた間隔でのリンク制御を実現することができる．具体的には，図5のような構成において考えてみると，デバイス A，B がブリッジ C によって接続されているものとする．A，B において BNDP が動作していない状態では，例えばリンク2がダウンしたとしてもリンク1がダウンするわけではないため，デバイス A は B との接続性が失われたことを検出できない．一方，BNDP を動作させた場合には，リンク2がダウンすることによって，B から送出される BNDP メッセージが A に到達できなくなり，A では maxage 経過後に（接続先が B 以外になければ）ポートが blocking 状態に移行しインタフェースダウンとなる．

図5 構成例1
Fig. 5 Network example 1

図6 構成例2
Fig. 6 Network example 2

同様に図6のような構成においては，デバイス A，B がブリッジ C，D によって接続されているとすると，通常リンク2がダウンした場合に，デバイス A，B はそれを検出することができない．このような状況は，デバイス A，B 間をキャリア等が提供するイーサネット接続サービスを利用して接続し，キャリアのネットワーク内で障害が起こった場合に想定されるが，C，D の管理はキャリア側の管轄となるため，やはり A，B 間でリンク接続状況を確認する手段が必要とされる．A，B で BNDP を動作させれば，リンク2がダウンした場合でも，それぞれ maxage 経過後には接続断を検出してインタフェースをダウンさせることが可能である．

また，図6のような状況において，ネットワークの可用性を確保するために冗長ルートを用意して STP によりループの解消を行っている場合を考えると，障害時には通常 STP の BPDU の到達性をみるため一定時間経過してから STP の状態遷移が開始されるが，BNDP を利用して障害検出時にインタフェースをダウンできれば，すぐに STP の状態遷移が開始されるため，STP におけるネットワーク再構成に要する時間を短縮することが可能となる．

次に図7のように，デバイス A，B，C が BNDP を解釈しないブリッジ D によって接続されるポイント-マルチポイントの構成を考えてみると，各デバイスが送信する BNDP メッセージはマルチキャストによって他の全てのデバイスまで到達し，各インタフェースのアドレステーブルにはそれぞれ2つのデバイス/ポートが登録されることになる．この状況でリンク2がダウンしたとすると，デバイス B からの BNDP メッセージがデバイス A，C に届かなくなり，それぞれの maxage 経過後に

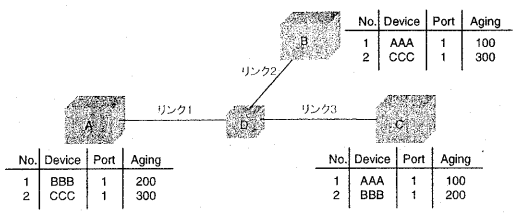

図7 構成例3
Fig. 7 Network example 3

表 1　PC プラットフォームの仕様
Table 1　Specification of PC platform

OS	NetBSD 1.6
CPU	Intel Pentium 4 2.5GHz
メモリ	512M byte
NIC	FE x 4 ポート（Adaptec ANA-64044LV）

アドレステーブルから B の項目が削除され，B との接続性が失われたことを検出できるが，アドレステーブルは空ではないためデバイス A，C のインタフェースの状態には影響しない．その後例えばリンク 3 がダウンすることにより，デバイス A のアドレステーブルが空となり，そのインタフェースは使用不可状態となる．このように BNDP を用いると，ポイント–マルチポイントの環境においても，対向機器との接続状況に応じたリンク制御が可能となる．

5. 実装評価

5.1 PC UNIX 上への実装

これまでに説明した BNDP を PC UNIX 上に実装して，簡単な評価を実施したのでその結果を報告する．

実装した PC プラットフォームの仕様を表 1 に，また機能上の特徴を以下に示す．

（1） BNDP は疑似インタフェースとして実装し，それに実インタフェースを対応付けて使用する．

（2） 各タイマーの精度は，NetBSD の仕様により 10ms 程度である．

（3） NetBSD のブリッジ機能との連携が可能である．

（4） BNDP 用の MIB を拡張 MIB として定義し，BNDP の情報を SNMP により操作可能である．

5.2 コマンド出力イメージ

図 8 の構成において，デバイス A，B の疑似インタフェースの状態を示すコマンドの出力イメージを図 9 に示す．

`bnd0` とは，作成された BNDP の疑似インタフェースであり，この例では実インタフェースとして `sf0` が割り当てられていることがわかる．このように BNDP 疑似インタフェース毎に，インタフェースの状態，タイマー設定値，割り当てられた実インタフェース，およびアドレステーブルによって接続先デバイスに関する情報を確認することができる．

5.3 タイマー精度の検証

本実装におけるタイマー値の精度を以下のような方法で検証を行った．図 10 の構成において，デバイス A，B をブリッジ C によって接続し，A，B 間で BNDP を動作させるものとする．また，ブリッジ C には端末 D を接続する．ブリッジ C が BNDP を解釈しないとすると，デバイス A，B から送出される BNDP メッセージはブリッジ C において透過的に転送され，端末 D では両者を受信することができる．

この状態でリンク 2 をダウンさせると，デバイス B からの BNDP メッセージの送信は停止され，デバイス A では maxage 経過後に blocking 状態へ移行し BNDP メッセージの送信が停止される．よって，端末 D において，デバイス B から送信される最後のメッセージ以降に受信するデバイス A からのメッセージをカウントすることによって，厳密ではないが maxage タイマーの精度を検証することができる．

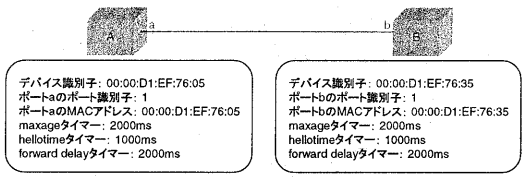

図 8　構成例 4
Fig. 8　Network example 4

```
デバイスA:
# bndconfig bnd0
bnd0:   <FORWARDING  uptime = 00:00:10>  device: 00.00.d1.ef.76.05  port=1
        Configuration:
          maxage 2000  hellotime 1000  fwddelay 2000
        Interface:
          sf0  mac 00.00.d1.ef.76.05
        Address table:
          device              port  maxage  hellotime  fwddelay mac
          00.00.d1.ef.76.35   1     2000    1000       2000     00.00.d1.ef.76.35
#
デバイスB:
# bndconfig bnd0
bnd0:   <FORWARDING  uptime = 00:00:10>  device: 00.00.d1.ef.76.35  port=1
        Configuration:
          maxage 2000  hellotime 1000  fwddelay 2000
        Interface:
          sf0  mac 00.00.d1.ef.76.35
        Address table:
          device              port  maxage  hellotime  fwddelay mac
          00.00.d1.ef.76.05   1     2000    1000       2000     00.00.d1.ef.76.05
#
```

図 9　コマンド出力例
Fig. 9　Example of command output

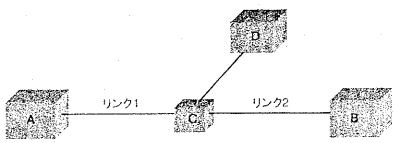

図 10　タイマー精度の検証
Fig. 10　Verification of timer precision

検証の結果，hellotime として仕様上の最小値である 10ms，maxage として 100ms を設定した場合でも動作上問題ないことが確認できた．

5.4 ブリッジ機能との連携

本実装においては，NetBSD のブリッジ機能との連携が可能であり，PC プラットフォームにイーサネット NIC を複数装着することにより，BNDP 対応のブリッジとして動作させることができる．STP の動作も可能であり，4. 項で説明した通り，冗長ルートを用意して STP にてループの解消を行っている場合に，BNDP を併用することにより，障害時のネットワーク再構成に要する時間が短縮できることを確認した．

具体的には，STP では定期的に BPDU を送受することによってネットワークの正常性を確認しているが，受信側では一定期間 BPDU を受信しないとネットワーク構成に変更が生じたと判断し，インタフェースの状態遷移を開始する．この期間は標準値として 20 秒という比較的長い値が設定されているが，

BNDP によってリンク断を検出してインタフェースをダウンさせることによって，この期間を待たずに STP のネットワーク再構成を開始させることが可能となる．

6. 考　　察

6.1 リンク状態の検出間隔

BNDP では 3 種類のタイマーを利用しており，それらの設定値に応じてリンク状態の検出間隔を変化させることが可能である．具体的には，検出間隔を決めてその値を maxage として設定する．maxage を決定したら，後は hellotime をその値よりも小さく，forward delay はその値以上の適当な数値を設定すればよい．各タイマー値は，仕様上は ms 単位での指定が可能であり，短く設定すればそれだけ検出間隔を短くすることが可能であるが，BNDP メッセージによるトラヒックは増加し，インタフェースの負担となることに注意しなければならない．また，一般トラヒックの影響により BNDP メッセージの受信間隔にゆらぎが発生し，リンク断の誤検出を招く可能性もあることから，ネットワーク環境や利用状況を考慮した上でタイマー値を決定することが必要となる．

6.2 MAC フレームへのカプセル化

BNDP メッセージの MAC フレームへのカプセル化手法については，本稿では STP における BPDU の場合と同様に LLC カプセル化による手法を採用したが，hellotime タイマーの最小値が 200ms 程度で十分であれば，リンク集約化の際に用いる LACP（Link Aggregation Control Protocol）[5] 等と同様にスロープロトコルとして定義することも考えられる．スロープロトコルでは，処理能力の低いプロセッサ上でも実装可能なように，送信レートは毎秒 5 フレーム以下と制限されており，実際にイーサネット機器に実装する際には実装負担の軽減が期待できる．

6.3 隣接デバイスからの情報取得

BNDP が動作するデバイスにおいては，自身のインタフェースの情報を BNDP メッセージによって広報することによって，接続先デバイスとの間で設定情報を共有することが可能である．ただし現在の仕様では，広報できる情報は，デバイス識別子，ポート識別子，BNDP のタイマー値に限られているため，接続構成程度の最小限の情報しか共有できない．さらに，インタフェース仕様や VLAN 設定情報，デバイスにおける対応プロトコル等の情報を共有できれば，運用管理上有用であると考えられる．

イーサネットの仕様を既定している IEEE 802 委員会においては，IEEE 802.1 ワーキンググループにおいて IEEE 802.1AB として LLDP（Link Layer Discovery Protocol）の検討が進められている [6]．LLDP のコンセプトは，BNDP とよく似ているが，リンク制御を考慮した動作は想定されておらず，隣接デバイスからの情報収集を主目的としたものであり，収集可能な情報としてはデバイスやポートの識別子だけではなく，MAC アドレスや VLAN 識別子，インタフェース種別，対応プロトコルといったより多くの項目が定義されている．

よって，隣接デバイスからの情報収集目的には LLDP を用い，BNDP は主にリンク制御用に利用するという方法も考えられるが，LLDP は，メカニズムとしてレイヤ 2 マルチキャストアドレスを利用した一方向プロトコルである点や，デバイス識別子とポート識別子により隣接デバイスを認識する点が類似しており，共通している部分も多いため，両者をマージする方向で検討を進めることも一案と考えられる．

7. おわりに

本稿では，イーサネットネットワークの運用管理性の向上を目的として，イーサネットインタフェース間でポート情報の交換および接続性の確認を行うプロトコルである BNDP を定義し，また BNDP を用いたリンク制御方式の提案を行った．

本方式では，デバイス間で能動的にリンク情報を交換することによって接続性の確認を行うため，従来運用管理が難しかった，接続先デバイスとの間に監視対象とはならない機器が挿入されるような環境において特に有効である．さらに，BNDP をレイヤ 2 プロトコルとして定義することによって，他のレイヤ 2 プロトコルとの連携が可能となり，例えば STP と組み合わせることによりネットワーク再構成に要する時間を短縮できる場合があることを示した．

本稿ではまた，本方式を PC UNIX 上に実装して開発した BNDP 対応ブリッジに関して，その内容と機能評価結果について簡単に紹介した．KDDI 研究所では，研究所の所在地である埼玉県上福岡市と新宿，大手町を結ぶ MAN 環境を構築しており，各拠点との接続は光ファイバを利用したギガビットイーサネット/WDM による接続となっている．今後は，WDM 区間の監視を目的として，各拠点に開発した BNDP 対応ブリッジを実験的に導入し，実環境での機能検証，性能評価を実施する予定である．

文　　献

[1] 渡辺，堀田，山崎，“イーサネットスイッチによる広域レイヤ 2 ネットワークの管理方式の検討，” 電子情報通信学会ソサイエティ大会 B-14-2，2001.

[2] 渡辺，堀田，山崎，“管理サーバによるレイヤ 2 ネットワーク制御方式に関する一考察，” 電子情報通信学会総合大会 B-14-35，2002.

[3] 渡辺，堀田，山崎，“イーサネットレベルでのリンク情報伝達プロトコル及びリンク制御方式の提案，” 電子情報通信学会総合大会 B-14-19，2003.

[4] “Part 3: Media Access Contorl (MAC) Bridges，” IEEE 802.1D，1998 Edition.

[5] “Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications，” IEEE Std 802.3，2002 Edition.

[6] “Station and Media Access Control Connectivity Discovery，” IEEE 802.1AB Draft 3，2003.