技術的条件集別表　２６．２

ＩＰ通信網 ISP 接続用ルータ接続インタフェース仕様

(IPv4 トンネル方式-10GBASE インタフェース)

[参照規格一覧]

JIS C5973　(F04形単心光ファイバコネクタ　1998.5.20)

JIS C6835　(石英系シングルモード光ファイバ素線　1991)

IETF RFC791 (Internet Protocol　1981.9)

IETF RFC792 (Internet Control Message Protocol　1981.9)

IETF RFC826 (An Ethernet Address Resolution Protocol:Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware　1982.11)

IETF RFC894 (A Standard for the Transmission of IP Datagrams over Ethernet Networks　1984.4)

IETF RFC1771 (A Border Gateway Protocol 4 (BGP-4)　1995.3)

IETF RFC2548 (Microsoft Vendor-specific RADIUS Attributes　1999.3)

IETF RFC2865 (Remote Authentication Dial In User Service(RADIUS)　2000.6)

IETF RFC2866 (RADIUS Accounting　2000.6)

IETF RFC3576 (Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS) 2003.7)

IEEE std 802.3-2002 (IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications)

IEEE std 802.3ae-2002 (IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications--Amendment:Media Access Control (MAC) Parameters, Physical Layer and Management Parameters for 10 Gb/s Operation)

IEEE std 802.3ad-2000 (IEEE Standard for Information technology--Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements--Amendment to Carrier Sense Multiple Access with Collision Detection(CSMA/CD) Access Method and Physical Layer Specifications　1998 Edition)

1. インタフェース規定点

図１．１に、協定事業者との接続イメージを示す。当社と協定事業者とは、インタフェース点（以下「ＰＯＩ」という）で接続する。

ＰＯＩは、当社のＩＰ通信網終端装置と技術的条件集第２章第 26 節（形態 14）に規定する条件により接続する場合のインタフェース規定点である。

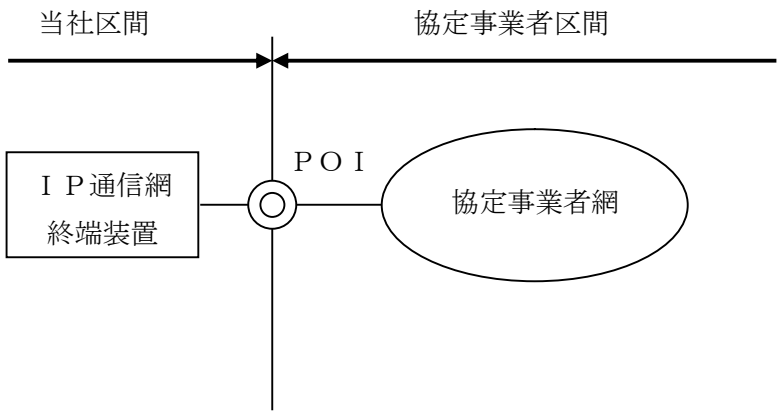


図１．１ 協定事業者との接続イメージ

２．　下位層（レイヤ１～２）仕様

２．１　物理層（レイヤ１）仕様

IEEE Std 802.3ae Clause49,51,52 準拠

コネクタ仕様　　JIS C5973/C5964-20 準拠

光ケーブル仕様　JIS C6835 SSM A-10/125 準拠

光ケーブル仕様　JIS C6835 SSM A-9.3/125 準拠

２．２　データリンク層（レイヤ２）仕様

IEEE Std 802.3ae Clause4 準拠

IEEE Std 802.3ad-2000 準拠

なお、IEEE Std 802.3ad-2000 はリンクアグリゲーションを使用する場合に準拠することとし、リンクアグリゲーションの使用は当社と協定事業者間で別途協議の上、決定することとする。

２．２．１　論理的条件フレーム構成

IEEE Std 802.3 Clause3 および IETF RFC894 準拠

２．２．２　物理アドレス解決方法

IETF RFC826 準拠

３．　ネットワーク層（レイヤ３）仕様

３．１　ＩＰ

IETF RFC791 準拠

３．２　ＩＣＭＰ

IETF RFC792 準拠

３．３　ルーティング方式

スタティックもしくは４．３に規定するダイナミックルーティング

４．　上位層（レイヤ４以上）仕様

４．１　制御情報交換方式

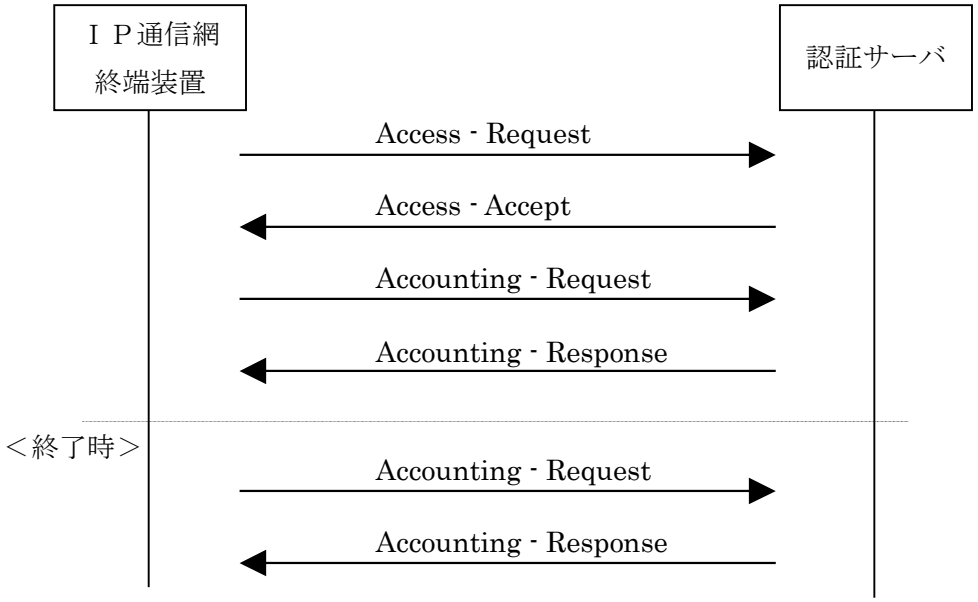
当社のＩＰ通信網終端装置と協定事業者の認証サーバ間の制御情報交換はＩＥＴＦ　ＲＦＣ２５４８、ＩＥＴＦ　ＲＦＣ２８６５、ＩＥＴＦ　ＲＦＣ２８６６およびＩＥＴＦ　ＲＦＣ３５７６準拠したＲＡＤＩＵＳプロトコルにより行う。このとき、ＩＥＴＦ　ＲＦＣ２５４８、ＩＥＴＦ　ＲＦＣ２８６５、ＩＥＴＦ　ＲＦＣ３５７６およびＩＥＴＦ　ＲＦＣ２８６６中で記述されているＲＡＤＩＵＳサーバおよびＲＡＤＩＵＳ課金サーバは協定事業者の認証サーバを、ＲＡＤＩＵＳクライアントについては当社のＩＰ通信網終端装置を、それぞれ示すものとする。

なお、４．１．１（３）項および（４）項に示すシーケンスの利用については、当社と協定事業者間で別途協議の上、決定することとする。

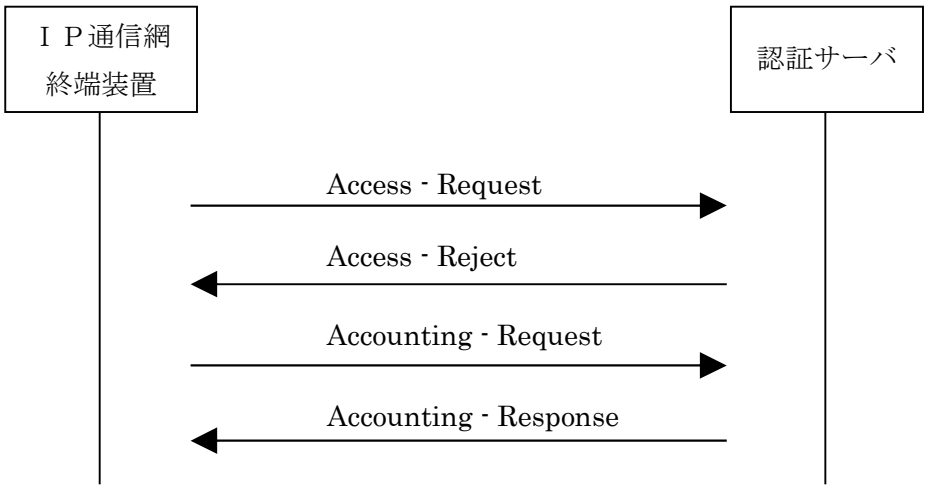
４．１．１　ＲＡＤＩＵＳシーケンス

当社のＩＰ通信網終端装置と協定事業者の認証サーバ間のシーケンスは以下のとおり。

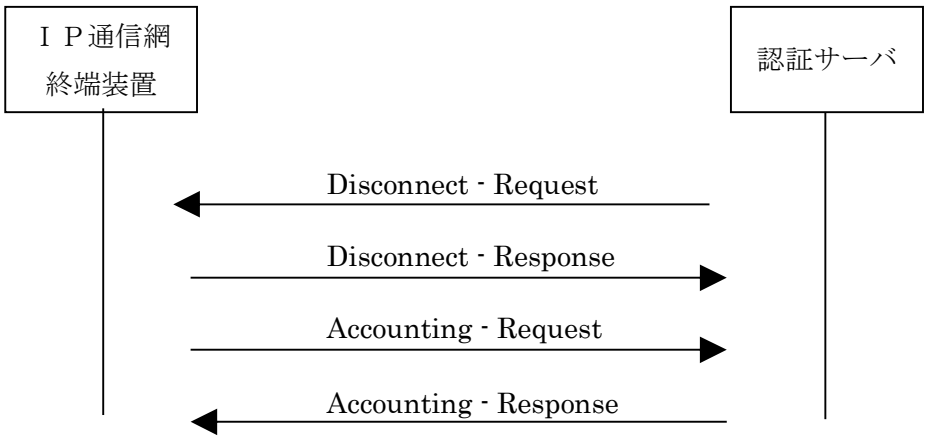
（１）正常時のシーケンス



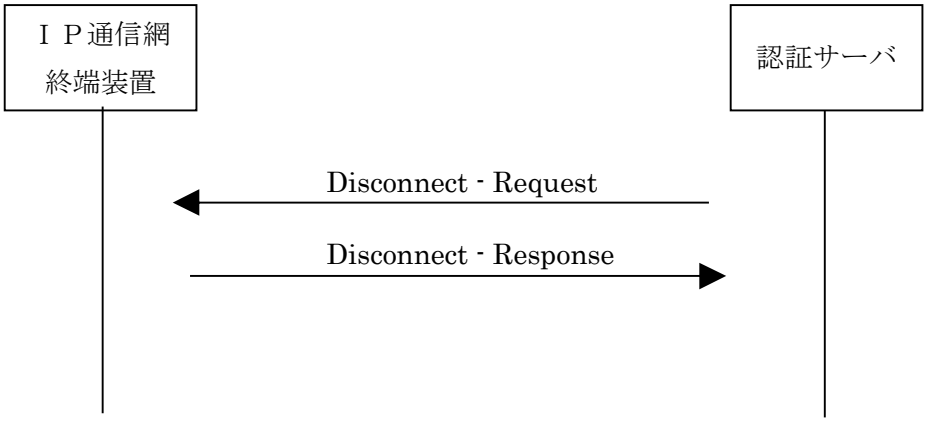
（２）誤ユーザ名、もしくは、誤パスワード時のシーケンス



（3）セッション解除成功時のシーケンス



（4）セッション解除失敗時のシーケンス

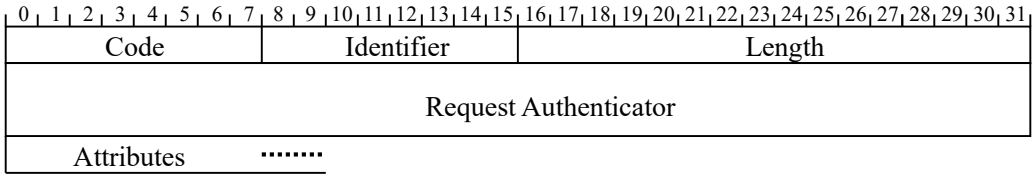


４．１．２ パケットフォーマット

当社のＩＰ通信網終端装置と協定事業者の認証サーバ間で用いる制御情報パケットのフォーマットを以下に示す。なお、図中の各フィールドは左から右への順で送られる。

（１）アクセス要求（Access-Request）

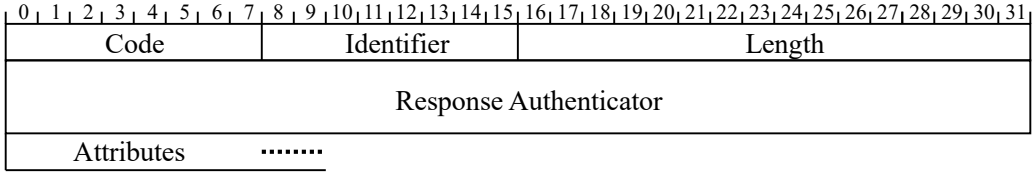
エンド・ユーザの協定事業者網への接続の可否を決定するために使われる情報を、当社のＩＰ通信網終端装置から協定事業者の認証サーバへ送出するパケット。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	1	1
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	１６	
Attributes	属性	可変	（属性情報）

（２）アクセス応答（Access-Accept）

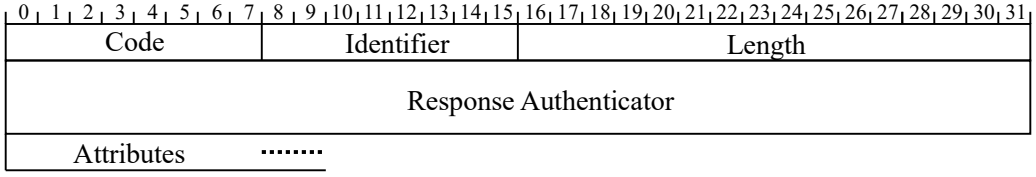
ユーザに対して、サービスを始めるために必要となる情報を提供するパケットで、協定事業者の認証サーバから当社のＩＰ通信網終端装置へ送られる。Access-Request の属性が受け入れられた時に、協定事業者の認証サーバはコードフィールドに「２」を入れて送出する。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	1	2
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	１６	
Attributes	属性	可変	（属性情報）

（３）アクセス拒否（Access-Reject）

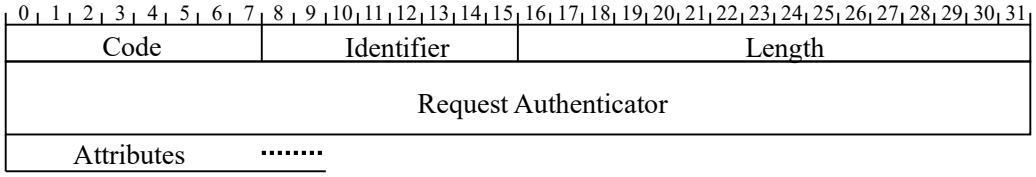
Access-Request の属性が受け入れられない時に、協定事業者の認証サーバはコードフィールドに「３」を入れて送出する。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	1	3
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	１６	
Attributes	属性	可変	（属性情報）

（4）アカウント要求（Accounting-Request）

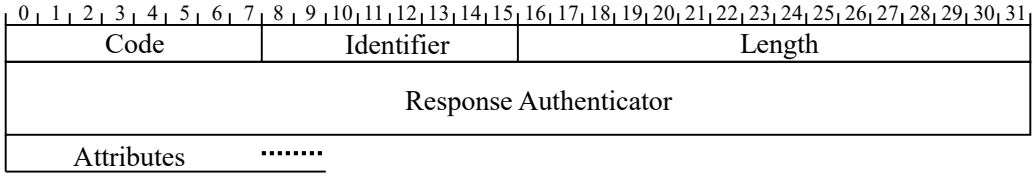
当社のＩＰ通信網終端装置から協定事業者の認証サーバに送られるパケットで、ユーザに提供されるサービスに対するアカウンティング情報を含んでいる。当社のＩＰ通信網終端装置はコードフィールドに「４」を入れて送出する。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	1	4
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	１６	
Attributes	属性	可変	（属性情報）

（5）アカウント応答（Accounting-Response）

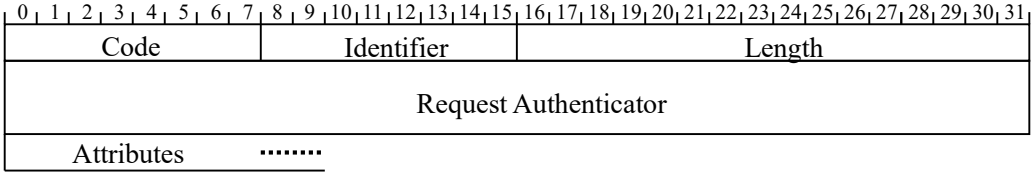
協定事業者の認証サーバから当社のＩＰ通信網終端装置に送られるパケットで、Accounting-Request が正しく受け取られ、記録されたことを示す。このとき、協定事業者の認証サーバはコードフィールドに「５」を入れて送出する。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	1	5
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	１６	
Attributes	属性	可変	（属性情報）

（６）切断要求(Disconnect-Request)

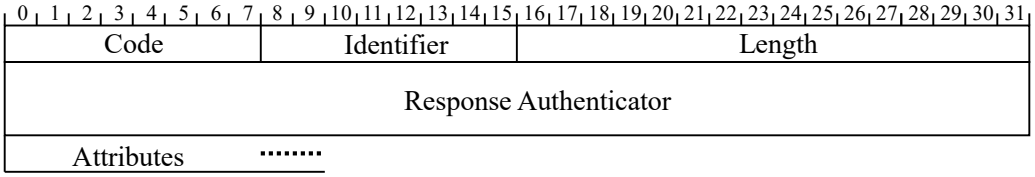
協定事業者の認証サーバから当社のＩＰ通信網終端装置に送られるパケットで、切断するセッションを特定する情報を含んでいる。協定事業者の認証サーバはコードフィールドに「４０」を入れて送出する。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	１	４０
Identifier	識別子	１	
Length	パケット長	２	
Authenticator	認証者	１６	
Attributes	属性	可変	（属性情報）

（７）切断応答（Disconnect-Response）

当社のＩＰ通信網終端装置から協定事業者の認証サーバに送られるパケットで、ACK の場合は Disconnect-Request が正しく受け取られ、セッションが切断されたことを示し、NAK の場合には Disconnect-Request が受け入れられなかったことを示す。当社のＩＰ通信網終端装置はコードフィールドに、ACK の場合には「４１」を、NAK の場合には「４２」を入れて送出する。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	１	４１(ACK) ４２(NAK)
Identifier	識別子	１	
Length	パケット長	２	
Authenticator	認証者	１６	
Attributes	属性	可変	（属性情報）

４．２ エンド・ユーザへのＩＰアドレス割り当て方式

エンド・ユーザへのＩＰアドレス割り当て方式には、以下に述べる２方式がある。

（１）協定事業者の認証サーバでのアドレス・プール

エンド･ユーザにダイナミックに割り当てるＩＰアドレスを協定事業者の認証サーバでプールする場合、協定事業者の認証サーバから当社のＩＰ通信網終端装置に転送する Access-Accept パケットの中に設定される Attribute のうち Framed-IP-Address にユーザへ割り当てる IP アドレスを設定する。

（２）ＩＰ通信網終端装置でのアドレス・プール

エンド・ユーザにダイナミックに割り当てるＩＰアドレスを当社のＩＰ通信網終端装置でプールする場合、協定事業者の認証サーバから当社のＩＰ通信網終端装置へ転送する Access-Accept パケットの中に設定される Attribute のうち Framed-IP-Address に 255.255.255.254 を設定する。

４．３ ダイナミックルーティングプロトコル

BGP-4　IETF RFC1771 準拠

なお、ダイナミックルーティングプロトコルの設定内容等の細目については、当社と直接協定事業者間で別途協議の上、決定することとする。

５．ＩＰ通信網終端装置へ同時に接続可能なＰＰＰセッション数の上限値について

ＩＰ通信網終端装置へ同時に接続可能なＰＰＰセッション数の上限値については、当社と協定事業者間で別途協議の上、決定することとする。

注）ＮＴＴ東日本の技術条件集のみに記載している事項は、波線二重下線を付して記載しています。
ＮＴＴ西日本の技術条件集のみに記載している事項は、二重下線を付して記載しています。