

技術的条件集別表 26.2

I P 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「P O I」という）で接続する。

P O Iは、当社の I P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。

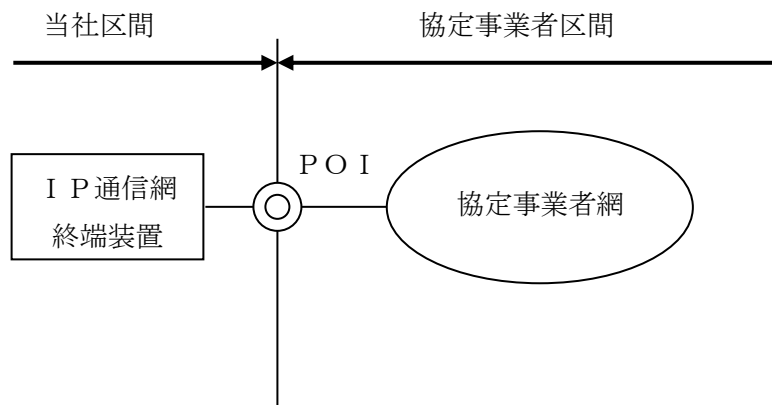


図1. 1 協定事業者との接続イメージ

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

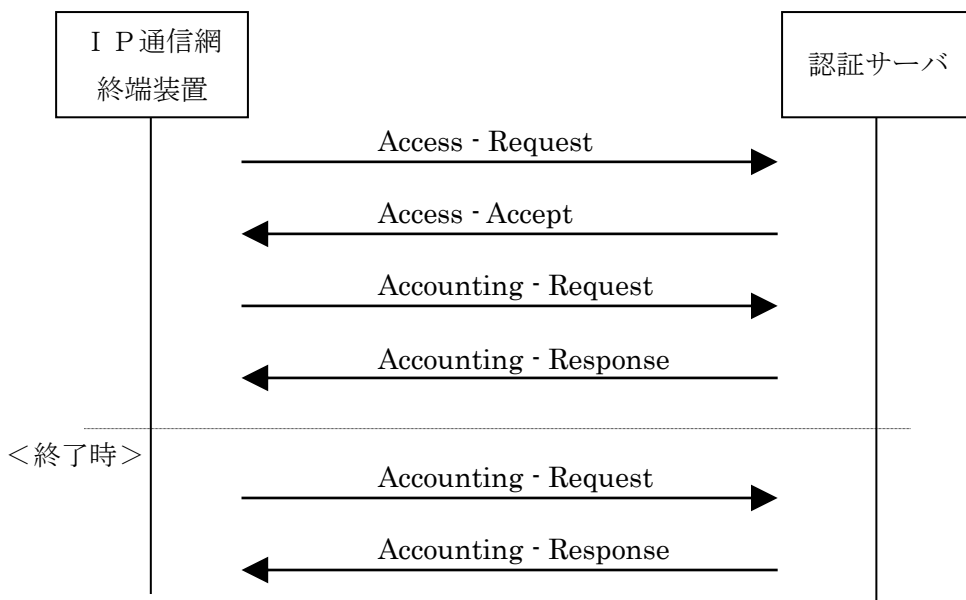
当社のIP通信網終端装置と協定事業者の認証サーバ間の制御情報交換はIETF RFC2548、IETF RFC2865、IETF RFC2866およびIETF RFC3576準拠したRADIUSプロトコルにより行う。このとき、IETF RFC2548、IETF RFC2865、IETF RFC3576およびIETF RFC2866中で記述されているRADIUSサーバおよびRADIUS課金サーバは協定事業者の認証サーバを、RADIUSクライアントについては当社のIP通信網終端装置を、それぞれ示すものとする。

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。

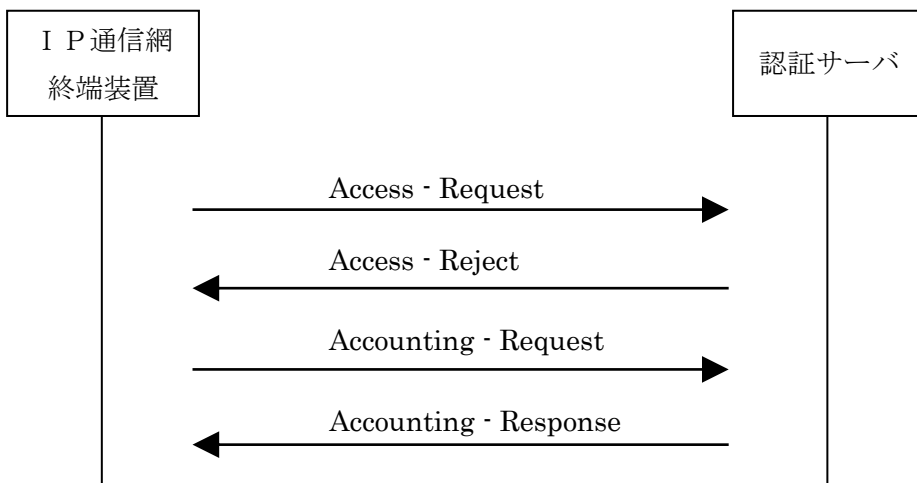
4. 1. 1 RADIUSシーケンス

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。

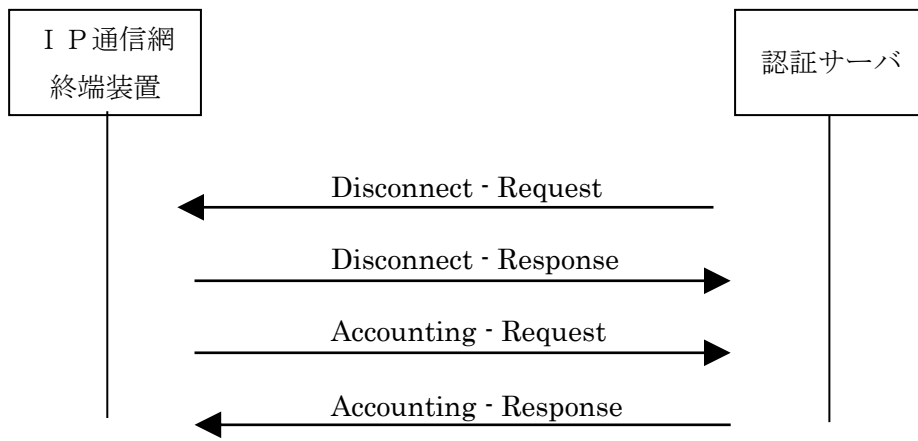
（1）正常時のシーケンス



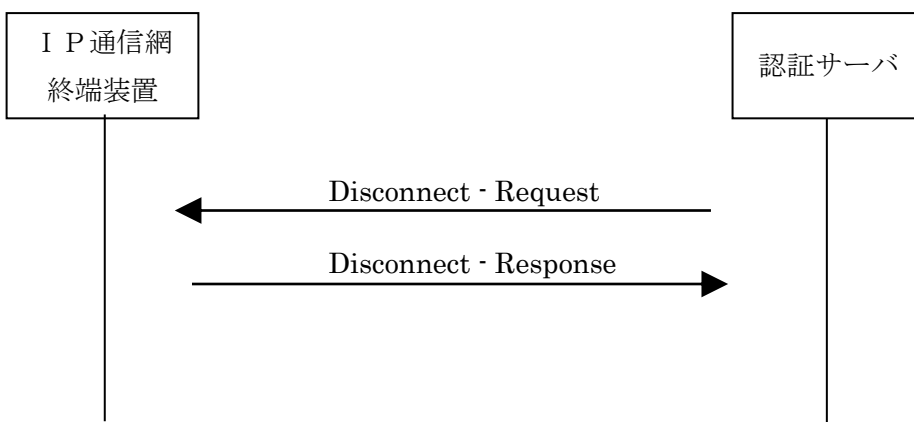
（2）誤ユーザ名、もしくは、誤パスワード時のシーケンス



(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 I P 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 I P 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。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Code			Identifier													Length															
Request Authenticator																															
Attributes																															

フィールド名	フィールド名	フィールド長 (octet)	値
Code	コード	1	1
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	1 6	
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 I P 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。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Code			Identifier													Length															
Response Authenticator																															
Attributes																															

フィールド名	フィールド名	フィールド長 (octet)	値
Code	コード	1	2
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	1 6	
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。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Code			Identifier													Length															
Response Authenticator																															
Attributes																															

フィールド名	フィールド長 (octet)	値
Code	コード	1
Identifier	識別子	1
Length	パケット長	2
Authenticator	認証者	1 6
Attributes	属性	可変 (属性情報)

(4) アカウント要求 (Accounting-Request)

当社の I P 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トリング情報を含んでいる。当社の I P 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。

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	Code	Identifier	Length
Request Authenticator			
Attributes			

フィールド名	フィールド長 (octet)	値
Code	コード	1
Identifier	識別子	1
Length	パケット長	2
Authenticator	認証者	1 6
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 I P 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。

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	Code	Identifier	Length
Response Authenticator			
Attributes			

フィールド名	フィールド長 (octet)	値
Code	コード	1
Identifier	識別子	1
Length	パケット長	2
Authenticator	認証者	1 6
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 I P 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「4 0」を入れて送出する。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Code				Identifier				Length																							
Request Authenticator																															
Attributes																														

フィールド名	フィールド名	フィールド長 (octet)	値
Code	コード	1	4 0
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	1 6	
Attributes	属性	可変	(属性情報)

(7) 切断応答 (Disconnect-Response)

当社の I P 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 I P 通信網終端装置はコードフィールドに、ACK の場合には「4 1」を、NAK の場合には「4 2」を入れて送出する。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Code				Identifier				Length																							
Response Authenticator																															
Attributes																														

フィールド名	フィールド名	フィールド長 (octet)	値
Code	コード	1	4 1 (ACK) 4 2 (NAK)
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	1 6	
Attributes	属性	可変	(属性情報)

4. 2 エンド・ユーザへの I P アドレス割り当て方式

エンド・ユーザへの I P 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 I P 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 I P 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) I P 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 I P アドレスを当社の I P 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 I P 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. I P 通信網終端装置へ同時に接続可能な P P P セッション数の上限値について

I P 通信網終端装置へ同時に接続可能な P P P 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) N T T 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。
N T T 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。