

NGN IPv6 ISP 接続
<トンネル方式>
NNI 仕様書

—6.0 版—

2010 年 12 月

NTT 東日本

NTT 西日本

(今後の検討状況により修正の可能性があります。)

当社網と直接接続事業者網間で使用するインタフェース仕様は次のとおりとします。

インタフェース種別	利用する I P	インタフェース仕様
1 0 0 0 B A S E - L X インタフェース	I P v 6	本 N N I 仕様書の「1 . 1 0 0 0 B A S E - L X インタフェースにて接続する場合」に示すとおりとします。
	I P v 4 / I P v 6	I P v 4 は技術的条件集別表 26、I P v 6 は本 N N I 仕様書の「1 . 1 0 0 0 B A S E - L X インタフェースにて接続する場合」に示すとおりとします。
1 0 G B A S E - L R インタフェース	I P v 6	本 N N I 仕様書の「2 . 1 0 G B A S E - L R インタフェースにて接続する場合」に示すとおりとします。
	I P v 4 / I P v 6	I P v 4 は技術的条件集別表 26.2、I P v 6 は本 N N I 仕様書の「2 . 1 0 G B A S E - L R インタフェースにて接続する場合」に示すとおりとします。

[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 RFC2461 (Neighbor Discovery for IP Version 6 (IPv6) 1998.12)

IETF RFC2463 (Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification)

IETF RFC2545 (Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing 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)

IETF RFC4443 (Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification 2006.3)

IETF RFC4760 (Multiprotocol Extensions for BGP-4 2007.1)

IETF RFC4818 (RADIUS Delegated-IPv6-Prefix Attribute 2007.4)

IETF RFC4861 (Neighbor Discovery for IP version 6 (IPv6) 2007.9)

IEEE std 802.3-2002 (IEEE Standard for Information technology--Telecommunications and informationexchange between systems--Local and metropolitan area networks--Specificrequirements--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 informationexchange between systems--Local and metropolitan area networks--Specificrequirements--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)

目 次

1．1000BASE-LXインタフェースにて接続する場合

1．1．インタフェース規定点	5
1．2．下位層（レイヤ1～2）仕様	5
1．2．1 物理層（レイヤ1）仕様	5
1．2．2 データリンク層（レイヤ2）仕様	5
1．2．2．1 論理的条件フレーム構成	5
1．2．2．2 物理アドレス解決方法	5
1．3．ネットワーク層（レイヤ3）仕様	5
1．3．1 IP	5
1．3．2 ICMP	5
1．3．3 ルーティング方式	5
1．4．上位層（レイヤ4以上）仕様	5
1．4．1 制御情報交換方式	5
1．4．1．1 RADIUSシーケンス	6
1．4．1．2 パケットフォーマット	7
1．4．2 エンド・ユーザへのIPアドレス割り当て方式	10
1．4．3 ダイナミックルーティングプロトコル	10
1．5．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	10

2．10GBASE-LRインタフェースにて接続する場合

2．1．インタフェース規定点	10
2．2．下位層（レイヤ1～2）仕様	10
2．2．1 物理層（レイヤ1）仕様	10
2．2．2 データリンク層（レイヤ2）仕様	10
2．2．2．1 論理的条件フレーム構成	10
2．2．2．2 物理アドレス解決方法	10
2．3．ネットワーク層（レイヤ3）仕様	11
2．3．1 IP	11
2．3．2 ICMP	11
2．3．3 ルーティング方式	11
2．4．上位層（レイヤ4以上）仕様	11
2．4．1 制御情報交換方式	11
2．4．1．1 RADIUSシーケンス	11
2．4．1．2 パケットフォーマット	12
2．4．2 エンド・ユーザへのIPアドレス割り当て方式	15
2．4．3 ダイナミックルーティングプロトコル	15
2．5．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	15

1.1000BASE-LXインタフェースにて接続する場合

1.1. インタフェース規定点

図1.1に、接続事業者との接続イメージを示す。当社と接続事業者とは、インタフェース点（以下「POI」という）で接続する。

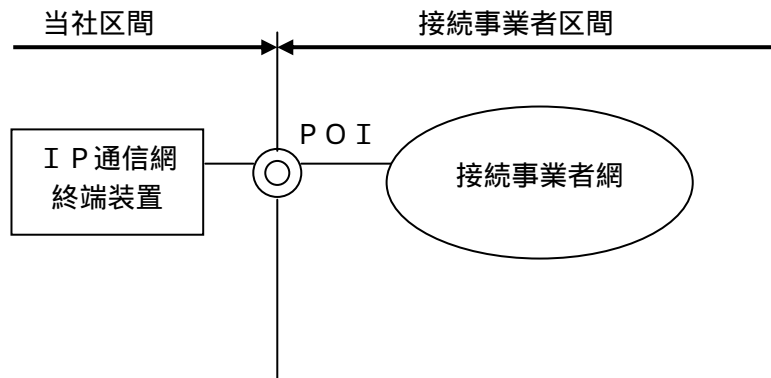


図1.1 接続事業者との接続イメージ

1.2. 下位層（レイヤ1～2）仕様

1.2.1 物理層（レイヤ1）仕様

IEEE Std 802.3 Clause38 準拠

コネクタ仕様 JIS C5973 準拠

光ケーブル仕様 JIS C6835 SSM A 準拠

1.2.2 データリンク層（レイヤ2）仕様

IEEE Std 802.3 Clause4 準拠

1.2.2.1 論理的条件フレーム構成

IEEE Std 802.3 Clause3 および IETF RFC894 準拠

1.2.2.2 物理アドレス解決方法

IPv4 IETF RFC826 準拠

IPv6 IETF RFC2461 準拠

IETF RFC4861 準拠

1.3. ネットワーク層（レイヤ3）仕様

1.3.1 IP

IPv4 IETF RFC791 準拠（RADIUSメッセージのネットワーク層として利用する）

IPv6 IETF RFC2463 準拠（マルチキャストアドレスは、リンクローカルスコープを除き、サポートしない）

1.3.2 ICMP

ICMPv4 IETF RFC792 準拠

ICMPv6 IETF RFC2463 準拠

IETF RFC4443 準拠

1.3.3 ルーティング方式

スタティックルーティングまたは1.4.3項に規定するダイナミックルーティング

1.4. 上位層（レイヤ4以上）仕様

1.4.1 制御情報交換方式

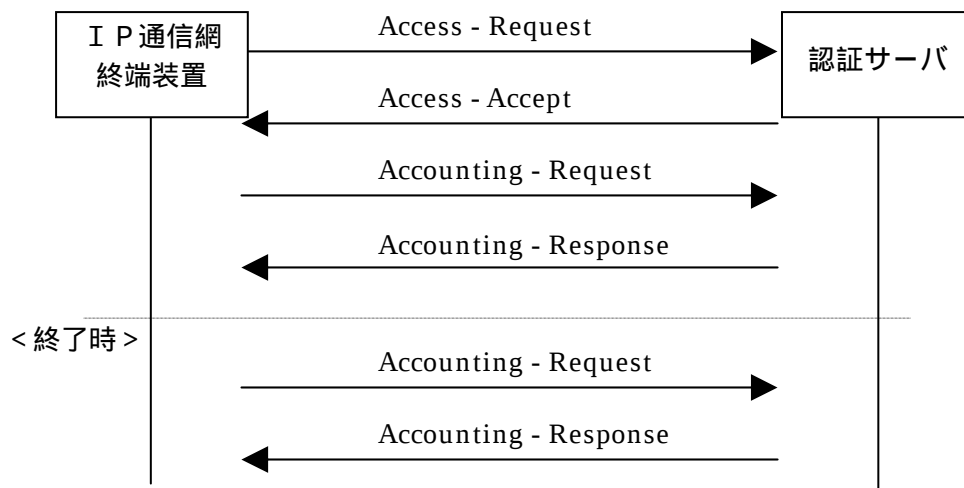
当社のIP通信網終端装置と接続事業者の認証サーバ間の制御情報交換はIETF RFC2865、IETF RFC2866、IETF RFC3576およびIETF RFC4818に準拠したRADIUSプロトコルに

より行う。このとき、I E T F R F C 2 8 6 5、I E T F R F C 2 8 6 6、I E T F R F C 3 5 7 6およびI E T F R F C 4 8 1 8の中で記述されているR A D I U SサーバおよびR A D I U S課金サーバは接続事業者の認証サーバを、R A D I U Sクライアントについては当社のI P通信網終端装置を、それぞれ示すものとする。
なお、1 . 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、当社と接続事業者間で別途協議の上、決定することとする。

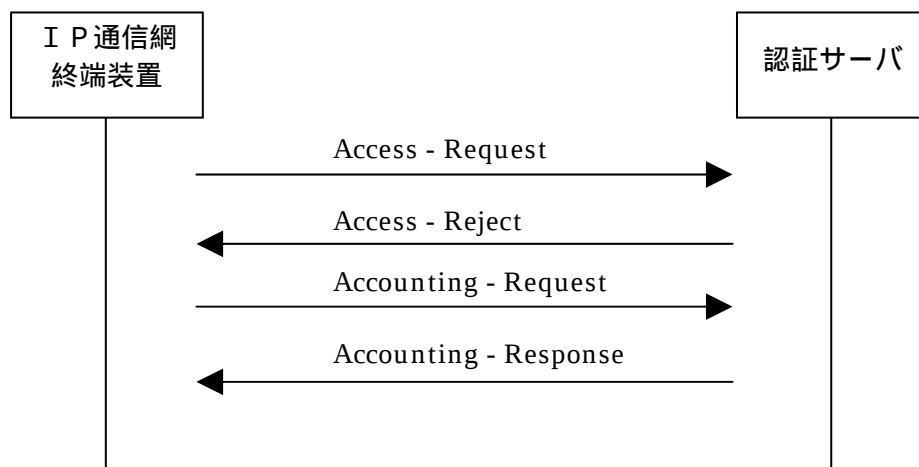
1 . 4 . 1 . 1 R A D I U Sシーケンス

当社のI P通信網終端装置と接続事業者の認証サーバ間のシーケンスは以下のとおり。

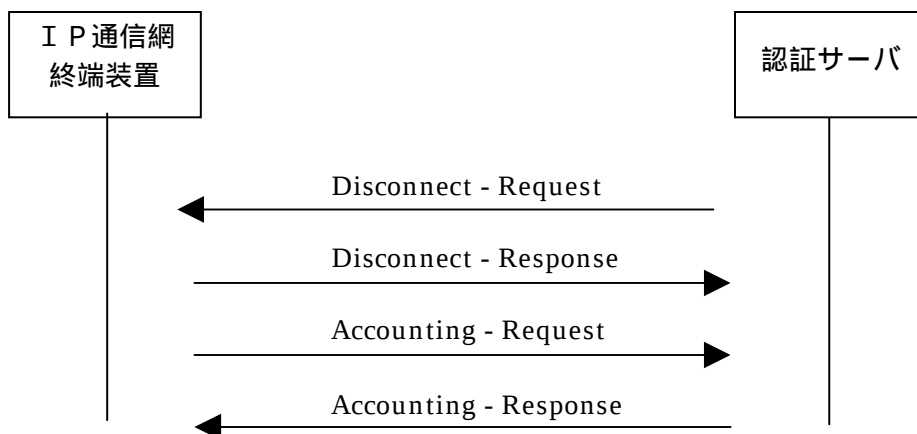
(1) 正常時のシーケンス



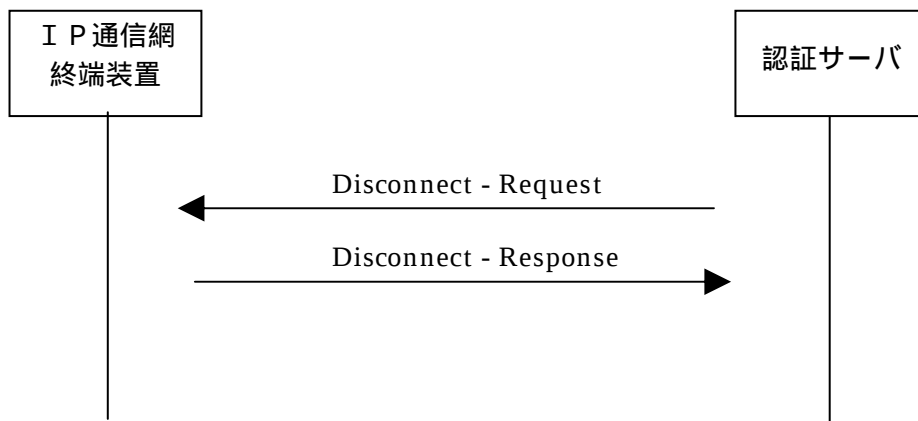
(2) 誤ユーザ名、もしくは、誤パスワード時のシーケンス



(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



1 . 4 . 1 . 2 パケットフォーマット

当社の I P 通信網端末装置と接続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。

フィールド名		フィールド長	値
Code	コード	1 オクテット	1 : Access-Request 2 : Access-Accept 3 : Access-Reject 4 : Accounting-Request 5 : Accounting-Response
Identifier	識別子	1 オクテット	
Length	パケット長	2 オクテット	
Authenticator	認証符号	16 オクテット	(属性情報)
Attributes	属性	可変長	

(1) アクセス要求 (Access-Request)

エンド・ユーザの接続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 通信網端末装置から接続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、接続事業者の認証サーバから当社の I P 通信網端末装置へ送られる。Access-Request の属性が受け入れられた時に、接続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、接続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	フィールド名	フィールド長(octet)	値
Code	コード	1	3
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	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接続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	フィールド名	フィールド長(octet)	値
Code	コード	1	4
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	1 6	
Attributes	属性	可変	(属性情報)

(5) アカウント応答 (Accounting-Response)

接続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、接続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	フィールド名	フィールド長(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)

接続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。接続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	16	
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接続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	16	
Attributes	属性	可変	(属性情報)

1.4.2 エンド・ユーザへのIPアドレス割り当て方式

エンド・ユーザにダイナミックに割り当てるIPv6 プレフィックスは、接続事業者の認証サーバでプールすることとし、接続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Delegated-IPv6-Prefix にユーザへ割り当てるIPv6 プレフィックスを設定する。

1.4.3 ダイナミックルーティングプロトコル

BGP-4+ IETF RFC2545 準拠

IETF RFC4760 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、当社と接続事業者間で別途協議の上、決定することとする。

1.5 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、当社と接続事業者間で別途協議の上、決定することとする。

2.10 GBASE-LRインタフェースにて接続する場合

2.1. インタフェース規定点

図2.1に、接続事業者との接続イメージを示す。当社と接続事業者とは、インタフェース点（以下「POI」という）で接続する。

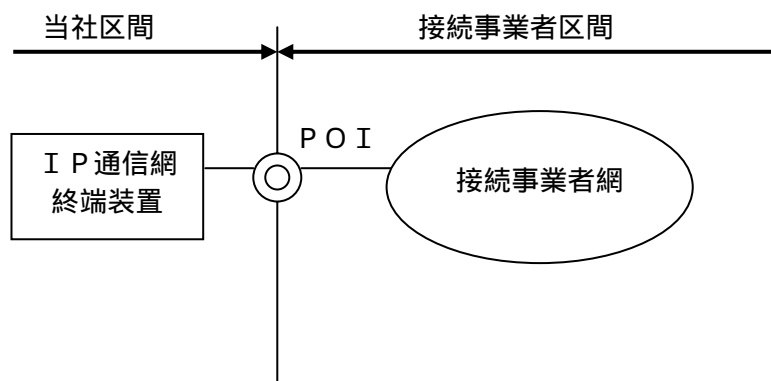


図2.1 接続事業者との接続イメージ

2.2. 下位層（レイヤ1～2）仕様

2.2.1 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 準拠

光ケーブル仕様 JIS C6835 SSM A 準拠

2.2.2 データリンク層（レイヤ2）仕様

IEEE Std 802.3ae Clause4 準拠

2.2.2.1 論理的条件フレーム構成

IEEE Std 802.3 Clause3 および IETF RFC894 準拠

2.2.2.2 物理アドレス解決方法

IPv4 IETF RFC826 準拠

IPv6 IETF RFC2461 準拠

2.3. ネットワーク層（レイヤ3）仕様

2.3.1. IP

IPv4 IETF RFC791 準拠（RADIUSメッセージのネットワーク層として利用する）

IPv6 IETF RFC2463 準拠（マルチキャストアドレスは、リンクローカルスコープを除き、サポートしない）

2.3.2. ICMP

ICMPv4 IETF RFC792 準拠

ICMPv6 IETF RFC2463 準拠

2.3.3. ルーティング方式

2.4.3項に規定するダイナミックルーティング

2.4. 上位層（レイヤ4以上）仕様

2.4.1. 制御情報交換方式

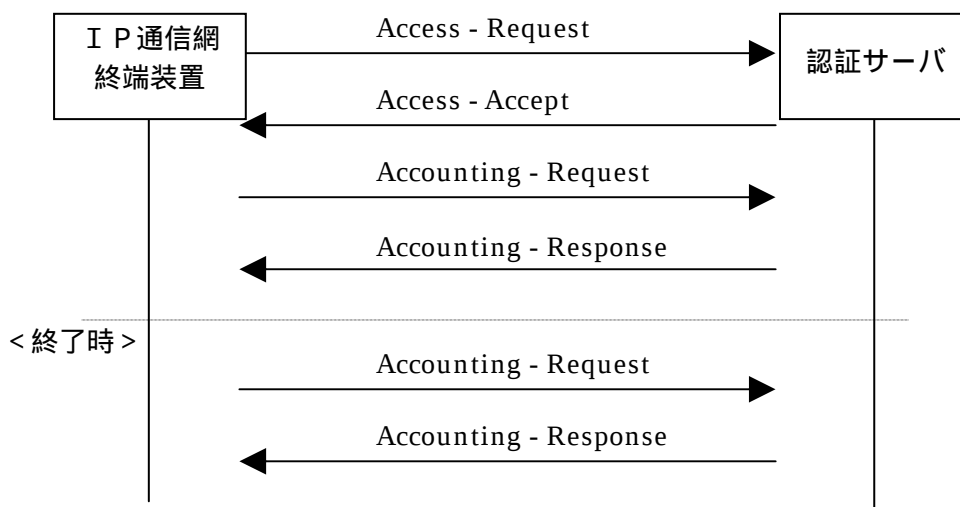
当社のIP通信網終端装置と接続事業者の認証サーバ間の制御情報交換はIETF RFC2865、IETF RFC2866、IETF RFC3576およびIETF RFC4818に準拠したRADIUSプロトコルにより行う。このとき、IETF RFC2865、IETF RFC2866、IETF RFC3576およびIETF RFC4818の中で記述されているRADIUSサーバおよびRADIUS課金サーバは接続事業者の認証サーバを、RADIUSクライアントについては当社のIP通信網終端装置を、それぞれ示すものとする。

なお、1.4.1.1（3）項および（4）項に示すシーケンスの利用については、当社と接続事業者間で別途協議の上、決定することとする。

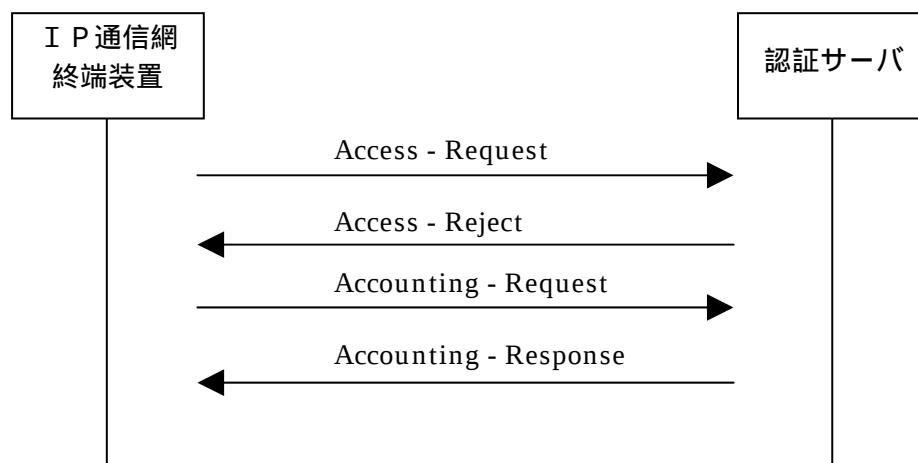
2.4.1.1. RADIUSシーケンス

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

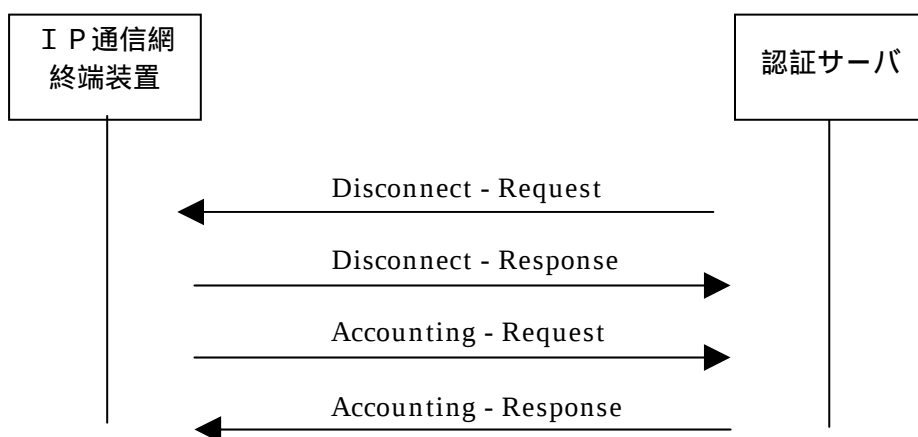
（1）正常時のシーケンス



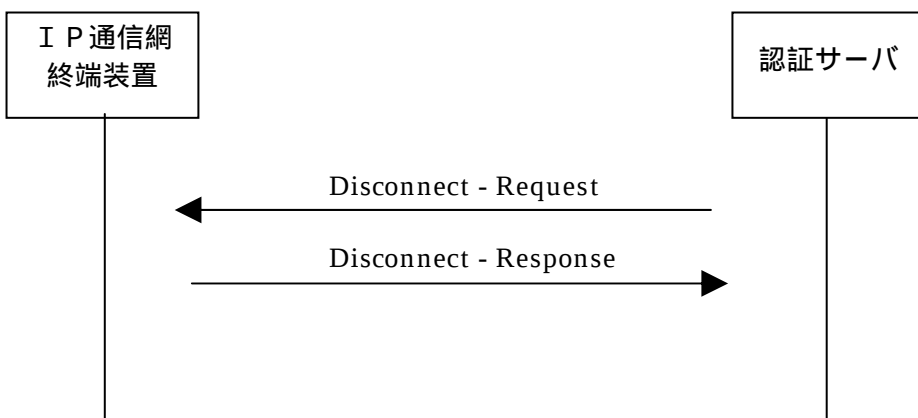
（2）誤ユーザ名、もしくは、誤パスワード時のシーケンス



(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



2 . 4 . 1 . 2 パケットフォーマット

当社の I P 通信網端末装置と接続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。

フィールド名		フィールド長	値
Code	コード	1 オクテット	1 : Access-Request 2 : Access-Accept 3 : Access-Reject 4 : Accounting-Request 5 : Accounting-Response
Identifier	識別子	1 オクテット	
Length	パケット長	2 オクテット	
Authenticator	認証符号	16 オクテット	(属性情報)
Attributes	属性	可変長	

(1) アクセス要求 (Access-Request)

エンド・ユーザの接続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接続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、接続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、接続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、接続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	3
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接続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	4
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)

接続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、接続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	5
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)

接続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。接続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接続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)

2 . 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・ユーザにダイナミックに割り当てる I P v 6 プレフィックスは、接続事業者の認証サーバでプールすることとし、接続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 Delegated-IPv6-Prefix にユーザへ割り当てる I P v 6 プレフィックスを設定する。

2 . 4 . 3 ダイナミックルーティングプロトコル

BGP-4+ IETF RFC2545 準拠

IETF RFC4760 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、当社と接続事業者間で別途協議の上、決定することとする。

2 . 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、当社と接続事業者間で別途協議の上、決定することとする。

注) N T T 東日本のみの事項は、波線二重下線を付して記載しています。

N T T 西日本のみの事項は、二重下線を付して記載しています。