



**Remote Access Dial-In User Service
(RADIUS)
For Telstra IP Remote**

Information Document

Version 10, April 2004

Purpose

This document is provided to assist in the correct configuration of a service provider's RADIUS server for interworking with the Telstra IP Remote RADIUS Proxy.

This publication has been prepared and written by Telstra Corporation Limited (ABN 33 051 775 556), and is copyright. Other than for the purposes of and subject to the conditions prescribed under the Copyright Act, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission from the document controller. Product or company names are trademarks or registered trademarks of their respective holders.

Note for non-Telstra readers: The contents of this publication are subject to change without notice. All efforts have been made to ensure the accuracy of this publication. Notwithstanding, Telstra Corporation Limited does not assume responsibility for any errors nor for any consequences arising from any errors in this publication.

Table Of Contents

1	INTRODUCTION	3
2	WHY USE RADIUS?	3
3	USE OF RADIUS	3
3.1	THE RADIUS PROXY	4
3.2	RADIUS MESSAGING	4
3.3	RADIUS MESSAGING RETRIES	4
3.4	USER CONNECTION PROCESS	6
3.5	RADIUS MESSAGE SECURITY	8
3.6	SERVICE PROVIDER'S RADIUS TO RADIUS PROXY CONNECTION	8
4	STANDARDS	9
5	AUTHENTICATION / AUTHORISATION	9
5.1	AUTHENTICATION	9
5.2	AUTHORISATION	9
5.3	RADIUS AUTHENTICATION AND AUTHORISATION ATTRIBUTES	9
5.4	SERVICES	10
5.5	USER INFORMATION ON RADIUS SERVER	10
5.5.1	IP Remote network Interface Section	10
5.5.2	IP Address Allocation	11
5.5.2.1	Fixed IP Address Allocation	12
5.5.2.2	RADIUS Proxy Managed Pools	12
5.5.2.3	IP address selection from default pool or via Least Cost Routing	12
5.5.3	Framed IP Netmasks	13
5.5.4	User Passwords	13
5.5.5	Idle Limit	13
5.5.6	Maximum Session Length	14
5.5.7	DNS Entries	14
5.6	IPX	14
5.7	AUTHENTICATION METHODS	14
5.8	DATA RATES	15
6	ACCOUNTING	16
6.1	ACCOUNTING RECORDS	16
6.1.1	Start and Stop Time	16
6.1.2	Start Records	16
6.1.3	Stop Record	17
6.1.4	Session Duration	17
6.1.5	Called & Calling Station Id	17
6.1.6	Account Delay Time	17
6.1.7	Account Session Identifier	18
6.1.8	Disconnect Causes	18
6.1.8.1	Specific Disconnect Causes	18
6.1.9	Real Time Call Zone Advice	19
6.1.10	Global IP Remote	19
7	ACRONYMS	20
8	GLOSSARY	20
9	REFERENCES	20

1 Introduction

RADIUS is a protocol for handling authentication (verifying usernames and passwords), authorisation (control of services allowable) and accounting (reporting on session time and bytes transferred etc) for dial in users. Telstra uses the RADIUS protocol as it is an industry standard that is recognised as a flexible and secure method of administering dial in user connections.

This document describes the RADIUS interface between the network and the service provider's RADIUS server for the Telstra IP Remote product.

2 Why Use RADIUS?

There are a number of reasons to use RADIUS. They include:

1. Security
RADIUS provides security by ensuring that users are authenticated before allowing access to network services. All user passwords are encrypted before transmitting them. The use of a shared secret between the service provider's RADIUS server and the Telstra network provides secure message exchange.
2. Central Management
RADIUS provides a central way of managing user configuration details. Users can be provided with customised services or default values given.
3. Standardised
RADIUS is widely used by industry and is an Internet "standard" protocol. (See References.) Telstra supports many of the RADIUS attributes described in the documents.
4. Extensible
RADIUS has an open design and is able to easily support new user services, as they become available.
5. Reliable
Multiple RADIUS Servers can be installed to ensure high reliability.

* See Reference section for sources of more information on RADIUS.

3 Use of RADIUS

The Telstra network uses a RADIUS Proxy to support dial user authentication, authorisation and accounting by the service provider. The RADIUS Proxy provides a central and reliable point for the distribution of RADIUS messages to/from customers. Figure 3.1 gives an indication of Telstra network topology and the use of RADIUS.

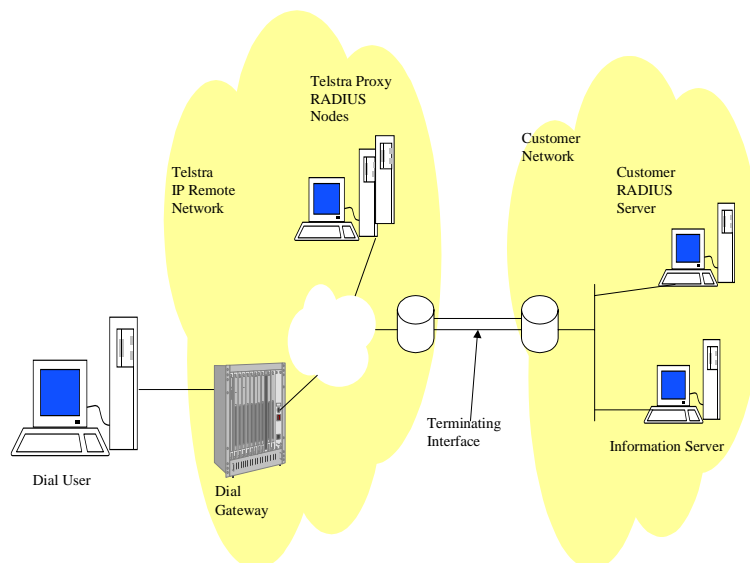


Figure 3.1 Telstra network topology and the use of RADIUS

3.1 The RADIUS Proxy

The RADIUS Proxy forwards RADIUS messages from the Dial Gateways to the appropriate service provider RADIUS server. As far as the service provider's RADIUS server is concerned the RADIUS Proxy looks like a Dial Gateway.

There is more than one RADIUS Proxy Node to ensure reliability and availability of the network. Service provider's can choose to have up to three RADIUS servers to handle their Authentication / Authorisation and up to three to handle Accounting.

3.2 RADIUS Messaging

RADIUS utilises a protocol from the IP protocol suite called UDP (User Datagram Protocol) to transfer messages. In order to ensure reliability, RADIUS software provides error checking and retransmissions for all messages.

In order to know which process is meant to receive a message, computers use "Port numbers" embedded inside the IP packets. The RADIUS systems utilise the following ports for messages:

Message Category	UDP Port
Authentication	1645 or 1812
Accounting	1646 or 1813

Table 3.2.1 RADIUS UDP Ports

The preferred UDP ports can be specified at service application time. The default UDP ports used by the IP Remote service are 1645 and 1646.

The method used by the Telstra Proxy system to track RADIUS messages is to issue them with a *source* UDP port value greater than 1024, never re-using a port while a message is outstanding with that service provider. The default behaviour of a commercial RADIUS server tends to be that it *listens* to UDP ports 1645/1812 & 1646/1813, and *reply* back to whatever source UDP port originated the RADIUS message.

Within the two categories there are message types identified by number.

Message Category	Type of Message	Number	Use	Message Direction Telstra RADIUS Proxy < > Customer RADIUS Server
Authentication	Access-Request	1	Initial request for connection	Proxy → Server
	Access-Accept	2	Accept user connection	Proxy ← Server
	Access-Reject	3	Reject user connection	Proxy ← Server
	Access-Challenge	11	Challenge user to provide more information.	Proxy ← Server
Accounting	Request – Start	4	Record issued at the start of a user session.	Proxy → Server
	Request – Stop	4	Record issues at the completion of a user session.	Proxy → Server
	Acknowledge	5	RADIUS server acknowledges receipt of Start or Stop record.	Proxy ← Server

Table 3.2.2 RADIUS Message Type and Numbers

3.3 RADIUS Messaging Retries

RADIUS Authentication and Account messages will be sent from the RADIUS Proxy to the service provider's RADIUS server a predefined number of times. The number of attempts to each of the service provider's RADIUS servers will depend on the number of servers that the service provider has nominated. The tables below list the number of authentication and accounting messages that will be sent depending on the number of RADIUS servers configured for the service provider.

Authentication message retries

Number of RADIUS Servers	1	2	3
No. of Retries	2	1	0
Number of attempts per server	3	2	1
Total attempts per service	3	4	3

Table 3.3.1 Authentication message retries

The interval between each attempt is 7 seconds. The service provider's RADIUS server should respond to an authentication message within 3 seconds.

Accounting message retries

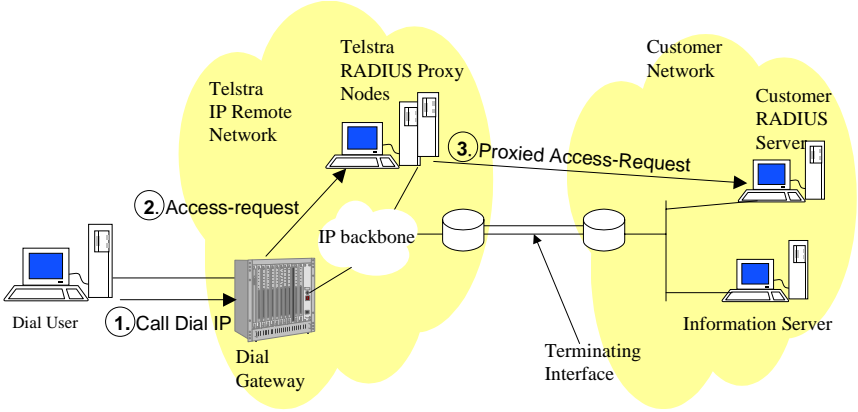
Number of RADIUS Servers	1	2	3
No. of Retries	3	2	1
Number of attempts per server	4	3	2
Total attempts per service	4	6	6

Table 3.3.2 Accounting message retries

The interval between each attempt is 7 seconds. The service provider's RADIUS server should respond to an accounting message within 6 seconds.

3.4 User Connection Process

This section explains the main steps involved in the user connection process and where the RADIUS messages described earlier are involved.

Step	Description	Network Event
1	<p>Call initiated from CPE. Username and password entered into appropriate fields. A call is placed to a service provider's allocated Telstra telephone number in the range 019830nnnn.</p>	 <p>The diagram illustrates the network architecture for the user connection process. It shows a 'Dial User' on the left who initiates a call (1) to a 'Dial Gateway' located within the 'Telstra IP Remote Network'. The gateway then sends an 'Access-request' (2) to 'Telstra RADIUS Proxy Nodes' also within the Telstra network. These proxy nodes forward a 'Proxied Access-Request' (3) to a 'Customer RADIUS Server' located in the 'Customer Network'. The Customer Network also contains an 'Information Server' and a 'Terminating Interface' which is connected to the 'IP backbone' that links the two networks.</p>
2	<p>A Dial Gateway in the Telstra network receives the call and forwards an Access-Request message to the RADIUS Proxy. The message contains the user name and password entered and some other call parameters.</p>	
3	<p>The RADIUS proxy then forwards the request to the correct Service provider's RADIUS.</p>	

<p>4</p>	<p>The Service provider's RADIUS server receives the Access-Request message. The user name and password is checked for validity. If valid then an Access-Accept message is generated by the Service provider's RADIUS. It contains the type of session allowed and other parameters such as IP pool number and session timeout</p>	<p>The diagram illustrates the network architecture for step 4. On the right, the 'Customer Network' contains a 'Customer RADIUS Server' and an 'Information Server'. An arrow labeled '4. Access-Accept' points from the Customer RADIUS Server to 'Telstra RADIUS Proxy Nodes' in the 'Telstra IP Remote Network'. The Telstra network is connected to an 'IP backbone' via a 'Terminating Interface'. From the IP backbone, a red arrow labeled '5. Virtual path' points to a 'Dial Gateway' in the 'Telstra IP Remote Network'. Finally, an arrow labeled '5. Proxied Access-Accept' points from the Dial Gateway to a 'Dial User' on the left.</p>
<p>5</p>	<p>The RADIUS Proxy receives the Access-Accept message and allocates an IP address out of an IP Pool (see section 5.5.2). The Access-Accept message is forwarded to the Dial Gateway, which then sets up a virtual path to the Telstra Interface that is connected to the service provider's edge router. The session is now established.</p>	

6	<p>A RADIUS start record is generated by the dial gateway and forwarded via the RADIUS Proxy to the Service provider's RADIUS server</p>	
7	<p>When the user's session is completed a RADIUS stop record is generated and forwarded via proxy to the Service Provider's RADIUS server. This message contains call duration and Advice of Charge. This message is also used by Telstra to bill the service provider</p>	

3.5 RADIUS Message Security

The RADIUS standard incorporates a number of features to ensure security of the RADIUS messages.

The RADIUS Proxy and the service provider's RADIUS are configured with a shared secret so they can identify each other as being valid. Each RADIUS message header sent between them is encrypted and decrypted using this secret. If the two servers do not have the same shared secret then they can not decrypt or use the messages being sent. If an incorrect shared secret is configured then the packet will appear at the other end as having a bad authenticator, which makes it an invalid packet.

The RADIUS security features were designed to prevent RADIUS messages being intercepted and misused even if they were transmitted over a public network. The Telstra network provides an extra level of security as the RADIUS messages travel directly from the Telstra network to the Service provider's network via a secure link, usually a frame relay or ATM link.

3.6 Service Provider's RADIUS to RADIUS Proxy Connection

A Frame-Relay or ATM virtual circuit is configured between the service provider's router and the Telstra network for traffic to the RADIUS Proxy. During service commissioning an IP address for the proxies will be given and the service provider will need to add a route to them from their network. A separate virtual circuit is configured for the carriage of dial up user traffic. The separation of user traffic and RADIUS messages enables security, capacity and traffic priority to be implemented.

4 Standards

RADIUS has become an industry standard for authenticating dial in users. The majority of vendors supplying dial access equipment support RADIUS. RADIUS servers are available for many server platforms, including Sun Solaris, Windows NT and Linux.

A working group of the Internet standards body, the IETF, has produced an official version of the RADIUS protocol. The Protocol has been documented and published as two Internet standards documents known as RFCs. The current standards are:

RADIUS Specification: RFC-2865 - Remote Authentication Dial In User Service (RADIUS)

RADIUS Specification: RFC-2866 - RADIUS Accounting

The extended attributes referred to within these documents are from the Ascend dictionary.

5 Authentication / Authorisation

This section provides more detail on how the service provider can exert control of users connecting to their network using IP Remote.

5.1 Authentication

Authenticating a user is the process of making sure that a user enters the correct user name and password, so should be who they say they are. After the user enters a user name and password, the RADIUS server verifies these are valid. The RADIUS server can also make use of additional authentication methods such as PIN numbers and one time passwords.

When a user dials in, an authentication request is passed via the RADIUS Proxy to the RADIUS server.

The authentication request contains a user name and password. If the user name and password are valid then the RADIUS server returns an access accept. A user is allocated configuration information to enable a specified service to be established.

5.2 Authorisation

Authorisation sets the parameters for the users session. Most RADIUS service templates can be established to define the parameters of all users or the authorisation parameters can be defined on a per user basis. Parameters include session idle time out and maximum session length etc.

5.3 RADIUS Authentication and Authorisation Attributes

RADIUS Access-Accept packets contain the details used in establishing each session. These session details are communicated via authentication and authorisation attributes. The following list of Authentication and Authorisation attributes will be accepted in the Access Accept packet from the service providers RADIUS:

Attribute number	Attribute Name	Values
6	Service-Type	Framed
7	Framed-Protocol	PPP, SLIP
8	Framed-Address	See section 5.5.2
9	Framed-Netmask	See section 5.5.3
18	Reply-Message	See RFC 2865
23	Framed-IPX-Network	See section 5.6
24	State	See RFC 2865
27	Session-Timeout	See section 5.5.6
28	Idle-Timeout	See section 5.5.5
125	Ascend-Maximum-Call-Duration	See section 5.5.6
135	Ascend-Client-Primary-DNS	See Section 5.5.7
136	Ascend-Client-Secondary-DNS	See Section 5.5.7
137	Ascend-Client-Assign-DNS	See Section 5.5.7
182	Ascend-IPX-Node-Addr	See section 5.6
216	Ascend-IPX-Peer-Mode	See section 5.6
229	Ascend-Route-IPX	See section 5.6
244	Ascend-Idle-Limit	See section 5.5.5

Table 5.3.1 Accepted Authentication and Authorisation Attributes

Any attribute not explicitly described should not be included in RADIUS Access - Accept messages sent to the IP Remote RADIUS proxy.

5.4 Services

The type of service a user is given will determine how information is communicated between the user and the network.

PPP enables users to simultaneously run a number of applications with each making use of the one serial network connection. A user could run their web browser, a mail program and a news reader all at the same time. Each application could access the network as needed.

The Internet protocols (TCP/IP) run on top of PPP. PPP is just the way that TCP/IP is able to operate across a serial line such as a telephone or ISDN line. PPP is a replacement for SLIP (Serial Line Internet Protocol). PPP has more advanced features and should be used in preference.

5.5 User Information on RADIUS server

The user information needed for authentication can be stored in a flat file or database. Most RADIUS servers have the capability of interfacing to a database containing user details. A user's entry contains attributes, with information such as their user name, password and the types of service that they are permitted to use.

When a customer adds a new user, they would be entered into their user information file. Users can be added or removed as needed. Different users can be configured for different types of services. For example user1 may be limited to 1 hour per day connection time and user 2 may be granted unlimited access per day.

Here is an example of a configuration for John Smith:

Attribute Name	Attribute Number	Example Value	Explanation	Mandatory / Optional in Access Accept.	Section
Username	1	Jsmith			
Password	2 or 3	!hello50	Password is checked against the password the user enters (Attribute 2 or 3)	Optional	5.5.4
User-Service	6	Framed-User	Can only use a protocol that uses packets	Mandatory	5.4
Framed-Protocol	7	PPP	Protocol for framing is PPP	Mandatory	5.4
Framed-IP-Address	8	141.122.251.21	IP Address (Pools can also be used)	Mandatory	5.5.2
Framed-IP-Netmask	9	255.255.255.255	IP Netmask	Mandatory	5.5.3
Primary-DNS	135	10.10.10.1	Clients Primary DNS	Optional	5.5.7
Secondary-DNS	136	10.10.10.2	Clients Secondary DNS	Optional	5.5.7
Assign-DNS	137	Yes	Supports selection of the Primary & Secondary DNS.	Optional	5.5.7
Maximum-Time	27	60	Maximum length of any session (in minutes)	Optional	5.5.6
Other				Optional	5.3

Table 5.5.1

The syntax of the user's configuration needs to be specific. Incorrect configuration values may cause a user to be unable to connect. Many RADIUS servers also enable users to configure default profiles for users. If all users have some parameters in common then this could be defined as a template.

5.5.1 IP Remote network Interface Section

Where multiple connections exist to terminate dial in sessions to a Service Provider's network from Telstra IP Remote it is possible to select which connection a users session is directed to via the authentication message.

Each connection has associated with it one or more Pools of IP addresses. If a user is allocated a specific IP address by the Service Provider's RADIUS server then the session is sent to the connection associated with the pool that the IP address is contained in. If a pool has been specified to allocate the IP address from then the session is terminated on the access associated with the pool. A third option is to allow the IP Remote RADIUS proxy to allocate the most appropriate IP Remote interface to terminate the session on. The Least Cost Routing feature does this.

5.5.2 IP Address Allocation

Users can be assigned specific IP addresses (depends on network configuration) or be configured to receive IP addresses from pools.

When a service provider connects to the Telstra service they instruct Telstra to provision IP pools. Each IP pool consists of one or more ranges of IP addresses. A single IP pool can consist of multiple distinct ranges of IP addresses. Each pool is associated with a IP Remote network interface.

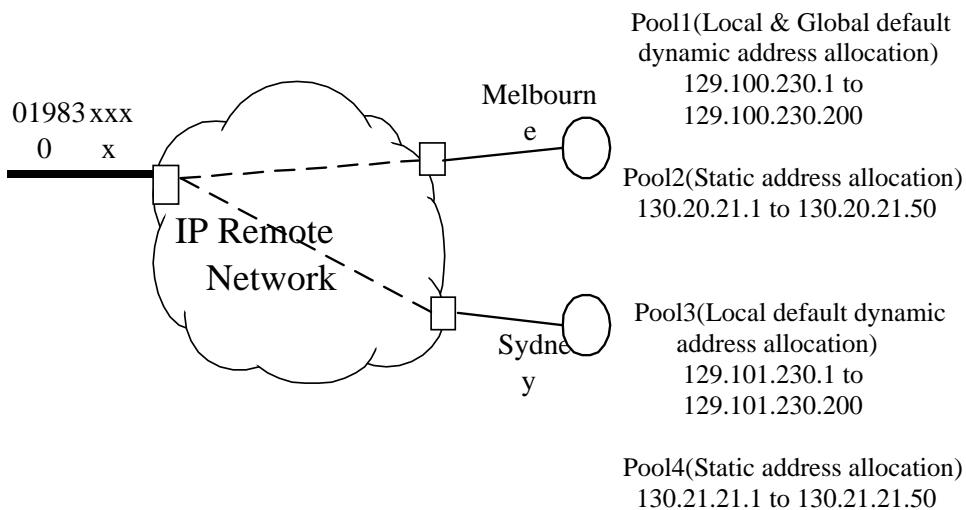
As well as specifying IP pool numbers the addresses contained within these pools and their associated network interface, a pool may be selected as a global or local default. More details on the use of local and global default pools can be found in sections 5.5.2.2 and 7.5.2.3

Reasonable use requirements apply for IP Addressing. The service provider should estimate the number of addresses required to service all concurrent calls and add an additional 10% of addresses. The additional 10% are required due to the RADIUS Proxy's allocation of minimum IP bundles across redundant hardware. Where an excessive number of IP addresses have been specified Telstra will endeavour to rationalise the request by negotiation.

Telstra must have provisioned all IP addresses used for dial up users as part of a pool. An example is below:

Pool Number	Local Default	Global Default	Connects to an Interface in:	IP Address Range	Service Provider uses for
1	✓	✓	Melbourne	129.100.230.1 to 129.100.230.200	General users
2			Melbourne	130.20.21.1 to 130.20.21.50	Users with fixed IP addresses
3	✓		Sydney	129.101.230.1 to 129.101.230.200	General users
4			Sydney	130.21.21.1 to 130.21.21.50	Users with fixed IP addresses

Table 5.5.2.1 Sample IP address pool usage



Example IP Address Configuration

Type of allocation desired	HSP RADIUS Access-Accept response	RADIUS Proxy will
----------------------------	-----------------------------------	-------------------

Fixed IP address	Framed-IP-Address = 129.20.21.10	Allocate exact IP address to user (IP address must still be predefined IP address pool).
From an IP address Pool	Framed-IP-Address = 255.255.255.3	Allocate user next free IP address from pool 3 (Pool 3 must be predefined).
From default pool or use least cost routing if implemented	Framed-IP-Address = 255.255.255.254	Allocate address from an appropriate default pool. In the example service config above an address would be allocated from pool 1.

Table 5.5.2.2 Address Allocation

5.5.2.1 Fixed IP Address Allocation

A specific IP address can be allocated to individual account so that they are given the same IP address whenever they authenticate.

If you intend using this option then you will need a separate pool defined that you do not allocate from using the other two methods. You may choose to use pool 1 as a “general use” pool that the RADIUS Proxy allocates IP addresses from and define a pool 2 that contains specific IP addresses reserved for individual users. More complex schemes are supported as long as this basic rule is followed. The first table in section 5.5.2.1 shows an example of how IP address pools may be used.

If a Service Provider's RADIUS tries to allocate an IP address that is already in use by another dial user then first the session using the address will be cleared. If specific IP addresses are allocated then ensure that only one dial up user is allocated the address. Note: However if 128Kbps (2 ISDN calls) are to be allowed, the same IP address may be allocated to that user for the second connection.

If the Service Provider's RADIUS assigns an IP address that has not been configured in the RADIUS Proxy then the authentication will fail.

5.5.2.2 RADIUS Proxy Managed Pools

It is possible for the service provider's RADIUS server to tell the Telstra RADIUS Proxy to assign an IP address from a pool. Some product options may require allocation from the default pool.

Pools are specified by the use of the Framed-IP-Address attribute. This attribute is normally used to allocate a specific IP address but can also be used to indicate which IP pool to use.

If the first three numbers of the IP address are 255 then the last number is treated as a pool number. A framed address value of "255.255.255.3" tells the RADIUS Proxy to use the IP Pool number 3.

Attribute Name	Attribute Number	Example Value	Explanation
Framed-IP-Address	8	255.255.255.3	Allocate an address from pool 3
Framed-IP-Netmask	9	255.255.255.255	Netmask for Single host

Table 5.5.2.2.1

For example if IP address pool 3 contained addresses from 129.101.230.1 to 129.101.230.200 and a framed IP address of 255.255.255.3 was returned by the service provider's RADIUS then the dial in client would be allocated the next free address which might be 129.101.230.20.

5.5.2.3 IP address selection from default pool or via Least Cost Routing

When a framed IP address of 255.255.255.254 is returned in the access accept packet by the service provider's RADIUS the RADIUS Proxy will either allocate an IP address from the global default pool or *if configured to do so*, the Least Cost Routing feature will be used to select an IP address from the most appropriate IP address pool (see below for how to configure Least Cost Routing feature).

The IP address pool to be used as the global default is specified at service application time. All IP Remote services should have one IP address pool nominated as the global default.

To configure the Least Cost Routing feature the HSP must have a-priori indicate which pools are eligible for consideration. These are known as 'local default' pools, and are nominated when the HSP fills out their Telstra IP Remote application form. It is only possible to nominate one local default pool per IP Remote charging zone. The RADIUS Proxy will decide which of the nominated IP address pools to allocate from. The aim is to deliver the end-user's session to the closest interface owned by the HSP they have called. In order for this feature to make any sense, the HSP should have more than one interface, in different locations. The pool selection decision is based upon the lowest IP Remote call cost for the call origin to one of the HSP's interfaces. If the cheapest call cost is the same to 2 or more HSP interfaces then the interface will be selected base on the shortest distance between call origin and one of the HSP's interfaces.

If no IP addresses are available in the local default, then the IP address out of the nominated 'global default' may be used. This may not be the closest (or the cheapest) interface, but the call will be successful

The Proxy implements the algorithm for 'closest interface' based upon the call origin - ie. The end users telephone number. Using this method it is possible, for example, that calls from a location in NSW close to the QLD border may actually be closer to Brisbane than Sydney and thus be connected to that interface.

5.5.3 Framed IP Netmasks

For normal dial up users the IP netmask should be defined as a host route or 32-bit netmask:

```
Framed-IP-Netmask = 255.255.255.255.
```

The effect of this is to specify that there is only one IP address for the dial up customer and they do not have a route to any other addresses.

If you allocate an IP address and a different netmask such as below, it will assume there is a network rather than a single user.

```
Framed-IP-Address = 150.136.243.1,  
Framed-IP-Netmask = 255.255.255.0
```

This indicates to the Telstra network that the dial up user is a router and has a path to all addresses in the network 150.136.243.0/24. If another dial up user is given an IP address in the range 150.136.243.x when the first user is still connected then their connection will not work as all IP addresses in the range will route to the original dial up call. Once connected the dial in client may not change IP address, hence the first user will need to disconnect before the IP range can be reused.

5.5.4 User Passwords

User passwords are stored in the Service Provider's RADIUS server or in some back-end system. Telstra's RADIUS nodes do not have a table of usernames or passwords of Service Provider's users.

It is recommended that users be instructed to choose passwords that are hard to guess. This means that using names or words found in a dictionary should be avoided. A password should contain different types of characters such as upper and lower case letters, numbers and other non alphanumeric characters and should be at least six characters long.

External options include Unix passwords, a database or other authentication system. If you are running the RADIUS on a Unix platform then the user can have the same password as that used for their Unix user account. Windows NT usernames and passwords can also be used in conjunction with some authentication servers.

Third party authentication systems such as Enigma Logic Safe Word and Security Dynamics ACE system are also useable with RADIUS.

Password expiration is also available on some servers and can be configured with a given expiration lifetime.

5.5.5 Idle Limit

Attributes accepted: - Attr 28 = Idle-Timeout (in seconds).
Attr 244 = Idle-Limit (in seconds)

The idle limit is the number of seconds that the connection can remain inactive before it will be disconnected. The Telstra default setting is 1800 seconds (30 minutes), however this can be specified as a selected network default

between 30 to 36000 seconds (10 hours). The network setting can be over-written by the service provider on a per session basis as part of the RADIUS authentication process.

5.5.6 Maximum Session Length

Attributes accepted: - Attr 27 = Session-Timeout. (In seconds)
Attr 125 = Ascend-Maximum-Call-Duration (in minutes)

Attribute 27 Session-Timeout places an upper limit on the length of the users session. Once the user has been connected for the maximum session length they will be automatically disconnected. The user will be disconnected regardless of whether they are utilising the connection. The Telstra default setting for maximum session length is 6.9 days (or 166 hours). The network setting can be over-written by the service provider on a per session basis as part of the RADIUS authentication process. Telstra encourage the use of the RFC attribute 27 Session-Timeout to control the length of a users session, it is suggested that the maximum length of a session be limited to 10 hours (36000seconds). Attribute 27 Session-Timeout limits the length of only a single session. If it is desired to limit the user to a maximum of a fixed time per day then the session length field should be used in conjunction with another mechanism on the Service Provider's RADIUS to prevent users connecting once their cumulative allocated time has been exhausted.

Attribute 125 Ascend-Maximum-Call-Duration limits the connect time of individual channels in call. When the time expires in a single channel call the call is disconnected. When the time expires for a channel in a multichannel call, the IP Remote network disconnects only the single channel, leaving the call connected. Permitted values for this attribute are integers from 0 to 1440. A value of 0 (zero) does not limit the connect time. There is no Telstra default value for Attribute 125 Ascend-Maximum-Call-Duration. Also note that the connect time will actually be slightly longer than the specified value as the IP Remote network only checks the timer once per minute.

5.5.7 DNS Entries

There are two attributes available so that the IP addresses for a client's DNS can be specified.

Attribute Name	Attribute Number	Example Value	Explanation
Primary-DNS	135	10.10.10.1	Clients Primary DNS
Secondary-DNS	136	10.10.10.2	Clients Secondary DNS
Assign-DNS	137	Yes	Supports selection of the Primary & Secondary DNS.

Table 5.5.7.1 DNS attributes

The attributes allow for a primary and secondary DNS server address to be downloaded to a client at authentication time. The attributes are optional. If no values are provided as RADIUS attributes, then the client's machine must have DNS values manually configured in order to use the DNS functionality.

5.6 IPX

Telstra will withdraw IPX support from the IP Remote service at 10a.m. Australian Eastern Daylight Saving Time on 31st March 2004. On and from that date, customers will not be able to use any applications that are dependent on IPX protocol after this time when connecting to IP Remote service.

Customers are responsible for reviewing any software applications they may have that are still dependent on IPX protocol. Customers should contact their software provider for further information and assistance to migrate off IPX protocol.

From 1 March 2003, IPX will not be available to new IP Remote customers.

5.7 Authentication Methods

When a user connects to the network, passwords can be transferred by either CHAP or PAP/Terminal server methods. The network will accept whichever method is sent.

When connecting to the network most clients will by default select the more secure authentication method which is CHAP. Using CHAP means that the password is encrypted in such a way that the RADIUS server cannot decrypt it. This is okay for most authentication situations except where a decrypted version of the password is required by the RADIUS server.

Some of the authentication situations that need the RADIUS to have a decrypted version of the password include:

- Windows NT usernames and passwords
- Unix passwords
- Third party authentication methods eg SecurID.*
- Changing Passwords

Using PAP/terminal server for authentication will ensure that the password can be decrypted at the RADIUS server. It should be noted that the only way to force a Windows 95/98 dial up networking client to use PAP/terminal server password types is to use the terminal window or a login script.

MS CHAP is not yet available.

* please refer to **section 5.7.1** for information on the changes to Global Roaming service which may have an impact on how the customer uses Third party authentication methods such as Watchword and SecurID.

5.7.1 Global Roaming – Authentication Methods

The following features will not be supported on IP Remote Global Roaming service as of 30th June 2004.

- Terminal server window (also known as terminal server mode or unframed user);
- Two Factor Authentication using watchword;
- SecurID users on windows operating system 95/98(including 98SE)/NT4/ME; and
- SecurID New Pin Mode.

Customers will not be able to use these features when they use Global Roaming from 30th June 2004 onwards. These features will continue to be available for use within Australia. Customers are responsible for ensuring that any end users who may be affected by the above changes are migrated to alternative solutions in order to continue using Global Roaming.

Customers utilising Terminal server window or Scripts will need to set their client to login using PPP mode. This means the customer or their end users would need to change the client to a mode that is compatible with their Radius (AAA) server. For example if their Radius supports CHAP then their clients will need to support CHAP or if their RADIUS supports PAP then their clients will need to support PAP.

Once Terminal Mode is turned off by the Customer, the IP Remote network will offer CHAP authentication first and then PAP authentication.

Windows 95,98,98SE,NT4 and ME operating systems using PPP mode will respond to either accepting the first protocol offered which is CHAP and then PAP. This requires the Radius (AAA) server to be compatible with the protocol selected by the user operating systems. If this is not compatible then the authentication request will fail. For example, a customer who has Windows 98 and Radius that supports PAP only will experience non-connectivity of their service.

5.8 Data Rates

Telstra indicates the connection data rates in the Access Request packet and the Accounting Request (Stop) packet.

Attribute Name	Attribute Number	Example Value	Explanation
Data-Rate	197	26400	Negotiated rate for upload.
Xmit-rate	255	50667	Negotiated rate for download.

Table 5.8.1 Data rate attributes

6 Accounting

The RADIUS protocol also describes messages for accounting. When a session is initiated a "start" accounting record is generated. The start record shows information such as user name and IP address allocated. At the end of the user session a "stop" record is generated. The stop record contains session information such as the user name, the IP address used, the session duration and the amount of data packets transferred.

The service provider's RADIUS server must acknowledge receipt of these messages within the aforementioned timeout (7seconds) or else risk losing this information.

6.1 Accounting Records

6.1.1 Start and Stop Time

The RADIUS Protocol does not include an explicit start or stop time in the information conveyed for accounting. The start or stop time of a session is determined by the RADIUS server when it receives the record and by the delay time. When a RADIUS server receives a stop or start record, the server time stamps it with a time based on its own system clock. To allow for any delay, before the record was received, the delay attribute includes the number of seconds the record was delayed before being sent.

As the RADIUS server uses its own system clock for determining session start or stop time it is essential that if accurate times are needed that the clock is set carefully and kept accurate.

6.1.2 Start Records

A start record is generated at the commencement of a session. Here is an example of the information contained in a start record:

Attribute	Attribute Number	Example Value	Explanation
Time		Tues Oct 1 9:30:11 1997	Time Record received by RADIUS
User-Name	1	"jsmith"	Name user logged in with
NAS-Identifier	4	144.130.4.5	IP Address of RADIUS Proxy
NAS-Port	5	141	RADIUS Proxy Port
NAS-Port-Type	61	Async	Port Type
Acct-Status-Type	40	Start	Type of accounting record - start or stop
Acct-Delay-Time	41	10	Seconds delay before record was forwarded
Acct-Session-Id	44	"479[[]375815128"	Accounting Record Identifier
Framed-Protocol	7	PPP	Framing protocol used
Called-Station-Id	30	"0396344321" or "0198304321"	The number called by the user is dependant on the product.
Calling-Station-Id	31	"0396403xxx"	Telephone number the user dialled from. Complete numbers can be provided for authorised Service Providers.
Rating Advice	249	"A1"	Real time call zone advice
Framed-IP-Address	8	145.200.200.20	IP Address allocated to user

Table 6.1.2.1 sample RADIUS Accounting start record

6.1.3 Stop Record

A stop record is generated at the end of any users session and includes such things as the session length, the session end time and the disconnect cause. For example:

Attribute	Attribute Number	Example Value	Explanation
Stop Time		Tue Oct 1 11:56:57 1996	Stop time of session. Calculated from time received and delay time.
User-Name	1	"jsmith"	Name user logged in with
NAS-Identifier	4	144.130.4.5	IP Address of RADIUS Proxy
NAS-Port	5	141	RADIUS Proxy Port
NAS-Port-Type	61	Async	Port Type
Acct-Status-Type	40	Stop	Type of accounting records
Acct-Input-Octets	42	121980	Octets sent to the network
Acct-Output-Octets	43	616916	Octets received from the network
Acct-Input-Packets	47	4736	packets sent to the network
Acct-Output-Packets	48	3917	packets received from the network
Acct-Delay-Time	41	10	seconds delay before record was forwarded
Acct-Session-Time	46	8813	length of session in seconds
Acct-Session-Id	44	"479[]375815128"	Accounting Record Identifier
Disconnect-Cause	195	185_rmt_end_hung_up	Reason for disconnection
Data-Rate	197	28800	Speed of connection - upload (bps)
Xmit-Rate	255	45333	Speed of connection - download (bps)
Called-Station-Id	30	"4321"	Last 4 digits of number called by user. (Changes as per Start message).
Calling-Station-Id	31	"0396403xxx"	Telephone number the user dialled from. (Changes as per Start message).
Framed-IP-Address	8	145.200.200.20	IP Address allocated to user
Framed-Protocol	7	PPP	Framing protocol used
Rating Advice	249	"A1"	Real time call zone advice

Table 6.1.3.1 Sample RADIUS Accounting stop record

6.1.4 Session Duration

The session length in seconds is included in the stop record. The session duration commences when a dial up users authentication request is accepted and the session commences. The session duration is calculated by the Dial Gateway where the user was connected, and this is used to calculate IP Remote charges.

6.1.5 Called & Calling Station Id

These fields contain the telephone numbers the user *called* and *called from* respectively.

The called number will provide the Full National number ie 0A BCDE FGHI.

The calling number consists of an area code and the first part of the telephone number from which the call was made. For privacy reasons the last three digits of the number have been replaced with the letter x. The called and calling number/station id's are contained in both the start and stop records.

6.1.6 Account Delay Time

This specifies the delay from when the user session ended and when the accounting record was sent to the Service provider's RADIUS. As RADIUS servers time stamp record is based on when they receive the records, this field is needed to obtain an accurate record of session details. It is used mainly when a message is resent after no acknowledgment is received.

6.1.7 Account Session Identifier

The RADIUS Proxy will send a session ID which is made up of a decimal and a string field, separated by '['. eg Attribute 44 = 123[[]a1b2c3d4e5xyz. The Accounting Session Identifier is a string used to identify the stop and start records for a users session. The identifier can be used to match the stop and start records so it can be determined if a user is still logged in. For start and stop records referring to the same session, there are a number of attributes that will be the same - these include: account-session-id, username, Framed-IP-address and NAS-Port. It is not needed to match start and stop records to calculate session duration, as this is included in the stop records details.

6.1.8 Disconnect Causes

The disconnect cause is a code that indicates why the call was terminated. The code enables a HSP to determine why the session ended and whether the user initiated this or if it happened for some other reason.

6.1.8.1 Specific Disconnect Causes

	Value	Explanation	
General	0	No information available	
	1	Call was not completed.	
	2	Reason unknown. Default code for disconnects not explicitly defined.	
	3	Call disconnected	
	4	Failure to authenticate calling-party number.	
	5	RADIUS timeout during authentication.	
	Modem	7	Pre-T310 Send Disc timer triggered
		9	No modem is available to accept call.
		10	No carrier detected.
		11	Loss of carrier.
12		Failure to detect modem result codes.	
Terminal Server	20	User exited terminal server.	
	21	Timeout waiting for user input.	
	22	Disconnect due to exiting Telnet session.	
	23	Could not switch to SLIP/PPP; the remote end has no IP address.	
	24	Disconnect due to exiting raw TCP.	
	25	Maximum number of login attempts exceeded.	
	26	Raw TCP disabled.	
	27	Control-C detected.	
	28	Terminal server session cleared ungracefully	
	35	Multilink Protocol Plus session cleared due to the lack of Multilink PPP null packets.	
PPP	40	PPP LCP negotiation timed out.	
	41	PPP LCP negotiation failed. Usually a PAP/CHAP mismatch error.	
	42	PPP PAP authentication failed.	
	43	PPP CHAP authentication failed.	
	44	PPP remote authentication failed.	
	45	PPP received Terminate Request from remote end.	
	46	Upper layer requested that the session be closed.	
	47	LCP closed because no Network Core Protocols were open. Typically there is no agreement on the type of routing or bridging that is supported for the session.	
	48	LCP closed because MP could not identify the call to which to add the new channel.	
	49	LCP closed as no more channels could be added to MP session	
Other General	100	Session timed out.	
	101	Username is invalid.	
	105	Session terminated due to encapsulation negotiation.	
	106	MP session timeout occurred	
	120	Call refused because the detected protocol is not supported	
	150	Disconnect requested	
	160	V110 synchronisation timeout exceeded	

	170	PPP authentication timed out
	171	Disconnected the call when the PPP interface was released.
	180	Local hangup
	181	Call cleared
	185	Call disconnected because remote end hang up
	190	Resource has been deactivated
	195	Maximum session time reached
RADIUS Proxy	10028	Dial Gateway port reused

Table 6.1.8.1.1 RADIUS Accounting disconnect codes

6.1.9 Real Time Call Zone Advice

The charging for a IP Remote session is based on a zone calculation and a Local or Austwide value. Advice of the zoning of the user's session is delivered in the form of a string attribute.

The codes are made up of a letter and number such as: "XN".

Where X is:

- L for Local
- A for Aust wide
- N for No real time advice available

and N is:

- 1 for zone 1
- 2 for zone 2
- 3 for zone 3

Possible codes are:

Zone	Local	Austwide	Not Available
N =1	L1	A1	N1
N =2	L2	A2	
N =3	L3	A3	

Table 6.1.9.1 Rating Codes

6.1.10 IP Remote Global Roaming

No real time AOC is available for IP Remote Global Roaming, ie. it is always N1.

7 Acronyms

AOC	Advice of Charge
CHAP	Challenge Handshake Authentication Protocol
CPE	Customer Premises Equipment
DNS	Domain Name Server
HSP	Host Service Provider
IETF	Internet Engineering Task Force (Internet Standards Body)
IP	Internet Protocol
IPX	Internetworking Packet Exchange
ISDN	Integrated Services Digital Network
MP	Multipoint Point to Point Protocol
PAP	Password Authentication Protocol
PPP	Point to Point Protocol (Protocol for connection between user and Dial Gateway)
PSTN	Public Switch Telephone Network
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comment (A standard or informational document of the IETF)
SLIP	Serial Line Internet Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
UDP	User Datagram Protocol

8 Glossary

Dial IP	Obsoleted by Telstra IP Remote.
Dial Gateway	Telecommunications equipment that handles dial in users calls.
Internet Protocol	Internet Protocol (IP) is the protocol used for addressing in the Internet and other TCP/IP networks.
TCP/IP	The protocol stack used in the Internet and other networks
UDP	User Datagram Protocol.

9 References

RADIUS

The two standard documents that define the RADIUS protocol are:

RFC 2865 - "*Remote Authentication Dial In User Service (RADIUS)*", C. Rigney et al, June 2000.

RFC 2866 - "*RADIUS Accounting*", C. Rigney, June 2000.

Detailed Information on the RADIUS standards working group and RADIUS RFCs can be found at:

<http://www.ietf.org>. These standards can be downloaded from a number of archives including: <ftp://archie.au/rfc>

Access Protocols

PPP is defined in:

RFC 1661 - "*Point-to-Point Protocol (PPP)*"

RFC 1994 - "*PPP Challenge Handshake Authentication Protocol (CHAP)*".

Internet Protocols

A useful general reference on TCP/IP is:

"*Internetworking with TCP/IP*", Volume 1, D. E. Comer, 1995, Prentice-Hall.