RADIUS Authentication Information for IPC Customers

Document no: Version 0.1
Confidential

Compiled by: Steven Walters
Eddie Stassen

Publication date: 13 February 2008

Notes

In no event shall Telkom SA Limited be liable to the customer for any special, indirect, incidental or consequential damages in any way arising out of, or relating to, the abusive use of the hardware and software described in this document.

Telkom SA Limited reserves the right to amend this document at any time. This document does not represent a commitment on the part of Telkom SA Limited.

To ensure ongoing quality of our products it is essential that only test equipment with a valid calibration certificate be used during the maintenance/test of units or systems.

TABLE OF CONTENTS

1. OVERVIEW

This document describes the requirements to do RADIUS authentication of broadband access to IAPs (Internet Access Providers) applying for IPC (IPConnect) services.

1.1 Prerequisites

In order to perform RADIUS authentication the following are required:

- AAA PVC with a bandwidth of at least 64kbps. Although the bandwidth requirements for RADIUS is modest, it is important that the line used for RADIUS authentication is not congested at any time as this could result in either failed authentication or lost accounting records.
- An RFC compliant RADIUS server. Telkom does not prescribe the use of any specific RADIUS software as long as the software conforms to the RADIUS RFC's.
- A realm needs to be configured on Telkom's RADIUS proxy servers. Online applications for realms
- can be accessed via https://www.telkom-ipnet.co.za
- It is assumed that the ISP will have a good working knowledge of RADIUS as well as the various systems that make up the ISP RADIUS infrastructure (Operating Systems, networking, databases, etc)

1.2 Overview of the RADIUS process

Figure 1 show the sequence of events when an ADSL Internet user authenticates:

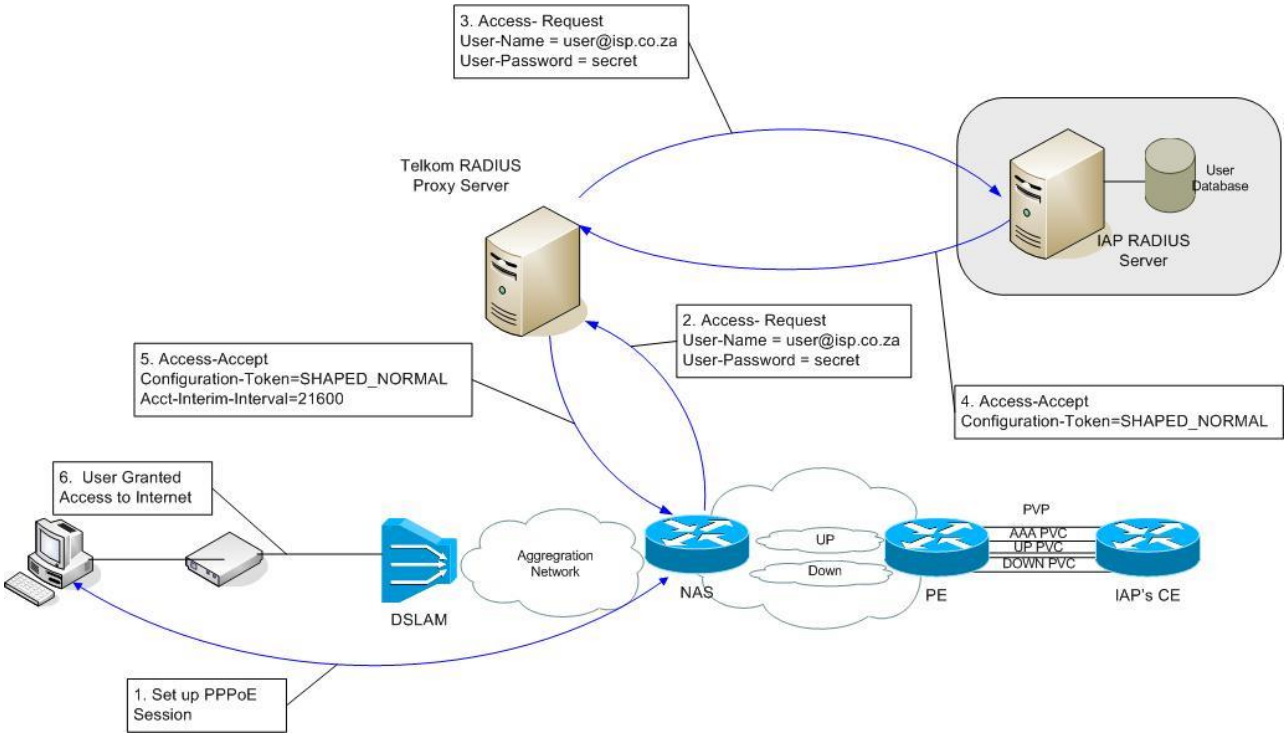

Figure 1

1. The user initiates the PPPoE connection by switching on the router or PC.
2. During the PPP authentication phase, the NAS generate a RADIUS *Access-Request* packet and forwards it to the Telkom's RADIUS proxy server. The packet will amongst other attributes, contain the username and password of the user.
3. The Telkom RADIUS proxy server inspects the realm part of the username (*'isp.co.za'* in this example), and forwards the request via AAA PVC to the ISP RADIUS server.
4. The ISP RADIUS server verifies the user credentials via its internal database, and if valid, sends an *Access-Accept* message back to the Telkom RADIUS proxy server. The *Access-Accept* message must contain attributes describing the service to be given to the user.
5. The Telkom RADIUS proxy server inspects the received *Access-Accept* packet, and if valid, forwards the packet to the originating NAS. Default or extra attributes may be added to the packet by the proxy server.
6. The NAS completes the set up of the PPP session and the user is granted access.
7. All the data traffic from the end user will reach the IAP via the UP VPN and PVC.
8. All the data traffic from the IAP will reach the end user via the DOWN VPN and PVC.

1.3 Realm Creation

Online applications for realms can be accessed via https://www.telkom-ipnet.co.za. Visit http://www.saix,net if

user access is required. For every realm to be created the following information need to be provided:

- Radius IP Address
- Radius Ports
- Radius Secret
- Radius Priority, used when multiple servers are present

1.4 IP Addresses and Pools

1.4.1 Radius Server

A public IP address is required for the customer's RADIUS server.

1.4.2 PVC IP Pool

An IPC service exist of 3 x PVCs (AAA, UP and Down). 3 x /30 IP Address pools are required for these PVCs. The IP Address block for the AAA PVC needs to be public but the IP Address blocks for the UP and Down PVCs can be either public or private.

1.4.3 NAS IP Pools

An IP address pool is required for every ADSL NAS in the network. Telkom will provide the block of address for private IPs. If public IPs are required, the customers must provide the block of addresses.

2. AUTHENTICATION

2.1 General

The following should be adhered to:

- Responses **must** be sent to all *Access-Request* packets when the contents are valid from a RADIUS perspective. A packet not valid on an application level, e.g. missing an attribute, should at least elicit and *Access-Reject* response, but never ignored.
- *Access-Accept* packets **must** contain the attributes listed as mandatory in the following sections. While sending empty *Access-Accept* packets may appear to work under certain circumstances, the behaviour is not guaranteed.
- ISP's should monitor the response times of their RADIUS servers. Currently Telkom will issue a retransmit if no response is received after 4 seconds. Generally it is expected that response times to *Access-Requests* should be well into the sub-second range.

2.2 Attributes present in Access-Request packets

The following attributes may be presents in *Access-Request* packets. This is not an exhaustive list and other attributes may be present at times:

Attribute Name	Value	Type	RFC	Description
User-Name	1	String	2865	The name of the user to be authenticated
User-Password	2	String	2865	This Attribute indicates the password of the user to be authenticated
NAS-Port-Type	61	Unsigned Integer (32 bits)	2865	This Attribute indicates the type of the physical port of the NAS which is authenticating the user. Commonly has a value 5 (Virtual) for ADSL
NAS-Port	5	Unsigned Integer (32 bits)	2865	This Attribute indicates the physical port number of the NAS which is authenticating the user
NAS-Port-Id	87	String	2869	This Attribute contains a text string which identifies the port of the NAS

				which is authenticating the user
Telkom-Access-Type	26 (VSA) Vendor 1431, Value 1	String	N/A	Telkom VSA indicating Access Technology. Has the value “DSL” for ADSL access.
NAS-IP-Address	4	IP Address	2865	This Attribute indicates the identifying IP Address of the NAS which is requesting authentication of the user
Connect-Info	77	String	2869	This attribute is sent from the NAS to indicate the nature of the user's connection. Usually has the value “AutoshapedVC” for ATM connected ADSL Users
Service-Type	6	Unsigned Integer (32 bits)	2865	This Attribute indicates the type of service the user has requested, or the type of service to be provided. In the case of ADSL, will have the value 2 (Framed)
Framed-Protocol	7	Unsigned Integer (32 bits)	2865	This Attribute indicates the framing to be used for framed access. In the case of ADSL will have the value 1 (PPP)

2.3 Attributes in Access-Accept packets

The following attributes are allowed in *Access-Accept* packets. All attributes not listed here will be stripped and ignored by the Telkom RADIUS proxy servers.

Attribute Name	**Value**	**Type**	**RFC**	**Status**	**Default Value**	**Description**
Cisco-AVPair	26(VSA) Vendor 9 Value 1	String	N/A	MANDATORY	None	Should be used to convey service specific information. See next section for detail.
Session-Timeout	27	Unsigned Integer (32 bits)	2865	OPTIONAL	None	This Attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. Telkom will allow any value greater than 3600 (1 hour). If no value or an invalid value is specified, there will be no session timeout, i.e. indefinite session duration.
Acct-Interim-Interval	85	Unsigned Integer (32 bits)	2869	OPTIONAL	21600 (6 hours)	This attribute indicates the number of seconds between each interim accounting update in seconds for this specific session. Telkom will allow values greater than or equal to 3600 (1 hour). Smaller values will be ignored and the default value used instead
X-Ascend-Client-	135	IP Address	Vendor Proprietary	OPTIONAL	None	This attribute must be used to specify the primary DNS

Primary-DNS			Attribute			server to be used by the client .
X-Ascend-Client-Secondary-DNS	136	IP Address	Vendor Proprietary Attribute	OPTIONAL	None	This attribute must be used to specify the secondary DNS server to be used by the client

2.4 RADIUS Profile

The RADIUS profiles for IP Connect users ***must*** contain at least the following attributes:

```
Cisco-AVPair = 'ip:ip-unnumbered=LoopbackXXXX',
Cisco-AVPair = 'ip:addr-pool=YYYY'
```

Where:

YYYY is the address pool name from which an IP Address should be allocated to the user
LoopbackXXXX is the Loopback Interface associated with the address pool

Both will be allocated to you during the activation of the IP Connect service.

Additionally the DNS servers to use may also be specified. This can be done using either the *Cisco-AVPair* attribute, e.g.

```
Cisco-AVPair = "ip:dns-servers=a.a.a.a b.b.b.b"
```

Or (preferred):

```
X-Ascend-Client-Primary-DNS = a.a.a.a
X-Ascend-Client-Secondary-DNS = b.b.b.b
```

Replace 'a.a.a.a' and 'b.b.b.b' with the IP addresses of your DNS primary and secondary DNS servers respectively.

3. ACCOUNTING

3.1 General

The same principles as mentioned in 2.1 apply, but specific attention should be paid to response times to *Accounting-Request* packets, since the processing of accounting packets generally require more overhead than *Access-Requests*. It is important that backend databases are properly managed to ensure decent response times.

Field

Keep the following in mind:

- With potentially unlimited session times and high speed access, it is imperative that your RADIUS server/accounting database uses the *Acct-In/Output-Gigawords* counters to keep track of wraparounds of the normal *Acct-In/Output-Octets* counters.
- Ensure that the *Class* attribute is stored in your database in order to detect the service used for a particular session.
- Duplicate accounting should be *expected*. Ensure that your database can detect and discard duplicate Accounting packets. A simple way would be to have a primary key/unique index on the concatenation of *User-Name, NAS-IP-*Address and *Acct-Session-Id*.

3.2 Accounting Attributes

The attributes listed below are not meant to be an exhaustive list, but describes only those most relevant to the ADSL service. The relevant RFC's should be consulted for more information where required. Attribute Names are aligned to those used in the relevant RFC's where applicable, but depending on the RADIUS implementation and dictionaries used, may be named differently. The Value field listed should therefore be

considered to be the authoritative reference to the particular attribute. There is also no guarantee that all these attributes will be present in every relevant packet.

Attribute Name	Value	Type	RFC	Description
Acct-Session-Id	44	String	2866	This attribute is a unique Accounting ID to make it easy to match start and stop records in a log file. They are unique for a NAS between reboots, but should not be considered globally unique. Can be used in conjunction with **User-Name** and **NAS-IP-Address** to form a unique identifier for this accounting record.
User-Name	1	String	2865	Name of the user for this session
Acct-Session-Time	46	Unsigned Integer (32 bits)	2866	This attribute indicates how many seconds the user has received service for.
Framed-IP-Address	8	IP Address	2865	The IP Address assigned to the user for this session
NAS-Port-Type	61	Unsigned Integer (32 bits)	2865	This Attribute indicates the type of the physical port of the NAS. Commonly has a value 5 (Virtual) for ADSL
NAS-Port	5	Unsigned Integer (32 bits)	2865	This Attribute indicates the physical port number of the NAS
NAS-Port-Id	87	String	2869	This Attribute contains a text string which identifies the port of the NAS
Telkom-Access-Type	26 (VSA) Vendor:1431, Value:1	String	N/A	Telkom VSA indicating Access Technology. Has the value “DSL” for ADSL access.
NAS-IP-Address	4	IP Address	2865	This Attribute indicates the identifying IP Address of the NAS for this session
Connect-Info	77	String	2869	This attribute is sent from the NAS to indicate the nature of the user's connection. Usually has the value “AutoshapedVC” for ATM connected ADSL Users
Service-Type	6	Unsigned Integer (32 bits)	2865	This Attribute indicates the type of service that was provided. In the case of ADSL, will have the value 2 (Framed)
Acct-Delay-Time	41	Unsigned Integer (32 bits)	2866	This attribute indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request
X-Ascend-Xmit-Rate	255	Unsigned Integer (32 bits)	N/A	Indicates the Transmit speed as set on the NAS
X-Ascend-Data-Rate	197	Unsigned Integer (32 bits)	N/A	Indicates the Receive speed as set on the NAS
Acct-Input-Octets	42	Unsigned Integer (32 bits)	2866	This attribute indicates how many octets have been received from the port over the course of this service being provided (Upload)
Acct-Output-Octets	43	Unsigned Integer (32 bits)	2866	This attribute indicates how many octets have been sent to the port over the course of this service being provided

				(Download)
Acct-Input-Gigawords[1]	52	Unsigned Integer (32 bits)	2869	This attribute indicates how many times the Acct-Input-Octets counter has wrapped around 2^{32} (4 Gigabyte) over the course of this service being provided
Acct-Output-Gigawords	53	Unsigned Integer (32 bits)	2869	This attribute indicates how many times the Acct-Output-Octets counter has wrapped around 2^{32} (4 Gigabyte) over the course of this service being provided
Acct-Terminate-Cause	49	Unsigned Integer (32 bits)	2866	This attribute indicates how the session was terminated: RFC Standard values are: 1 User Request 2 Lost Carrier 3 Lost Service 4 Idle Timeout 5 Session Timeout 6 Admin Reset 7 Admin Reboot 8 Port Error 9 NAS Error 10 NAS Request 11 NAS Reboot 12 Port Unneeded 13 Port Pre-empted 14 Port Suspended 15 Service Unavailable 16 Callback 17 User Error 18 Host Request Other values may also be used
Class	25	String	2865	The content of this field is set by Telkom and is described below.
X-Ascend-Session-Svr-Key	151	String	N/A	A key that identifies the session on the NAS, and can be used in *Disconnect-Messages*

3.2.1 The Class Attribute

Telkom will use the **Class** attribute to convey extended information about the session in Accounting-Request packets. The Class field will be ASCII encoded and the general format will be:

Class= *field1;field2;field3…*

i.e. a number of fields separated by semi-colons. (ASCII value $3B_{16}$) For the purpose of this document of field1 is of relevance, fields 2 and onwards are reserved for Telkom internal use. Please note that the field separator (';') will only be present when multiple fields are present.

1 The *'Gigaword'* attributes will only be present if non-zero

At present *field1* will be three characters in length, but may be extended in future. The field is to be interpreted as **IXX**, where the "I" indicates an IPC service.

Notes:

- Additional values may be added to these subfields in future as new services become available.
- Certain RADIUS servers (most notably freeRadius) interpret the Class field not as ASCII, but as binary and may display the attributes in hexadecimal format (e.g. 'NS1' is displayed as '0x4e5331'). The simplest way to display/store this in ASCII is to edit the dictionary file and change the 'type' of Class to 'string'

4. DISCONNECTING USERS

4.1 Introduction

RFC3576 (http://www.ietf.org/rfc/rfc3576.txt) describes the RADIUS Disconnect Messages that can be used to disconnect a user during an active session. Telkom has implemented this feature on the ADSL Internet network and it is available to IAPs as and additional feature to aid in controlling the usage of individual users. This document describes the specifics in respect of the Telkom implementation of RFC3576. Familiarity with the RFC is assumed.

4.2 Description

To effect a user disconnect, the ISP must send a RFC3576 conforming *Disconnect-Request* packet to the Telkom RADIUS proxy servers. The proxy server will respond with either a *Disconnect-ACK* or *Disconnect-NAK* response depending on the outcome of the request.
The Telkom implementation follows the RFC with the following stipulations:

1. *Disconnect-Request* packets ***must*** contain the following attributes:

Attribute	Description
User-Name	The name of the user to be disconnected
NAS-IP-Address ~~Either one of :~~ ~~Framed-IP-Address[2]~~ ~~X-Ascend-Session-Svr-Key~~	The IP Address of the NAS as sent in the *NAS-IP-Address* attribute in the RADIUS Start-Accounting Record. ~~The IP address the user was assigned for the active session.~~ ~~The session key uniquely identifying the session on the NAS (preferred)~~
Acct-Session-Id ~~NAS-IP-Address~~	This attribute is a unique Accounting ID to make it easy to match start and stop records in a log file. ~~The IP Address of the NAS as sent in the *NAS-IP-Address* attribute in the RADIUS Start-Accounting Record.~~

2. *Disconnect-Request* messages ***must*** originate from one of the RADIUS servers associated with the authentication of realm of the user. (i.e. the ISP's RADIUS server(s))

3. *Disconnect-Request* messages can be sent to any of the following Telkom RADIUS proxy servers:

IP Address	UDP Port
196.43.1.8~~6~~8~~8~~	1700

2

In future the use of *Framed-IP-Address* in *Disconnect-Requests* may be discontinued and only the *X-Ascend-Session-Svr-Key* may be supported.

196.43.1.89	1700

4. The same shared secret as is used between the Telkom RADIUS proxy servers and the IAP's RADIUS server must be used to generate the *Authenticator* field in the *Disconnect-Request* packet.

5. Additional allowed attributes as specified in RFC3576 par. 3.2 ***may*** be present in the *Disconnect-Request* message, but will be ignored.

4.3 Error Messages

In addition to the error/completion codes originating from the NAS itself, the Telkom proxy servers may return the following error codes in a *Disconnect-NAK* if the request is considered invalid:

Condition	Error Code
User-Name attribute absent or Acct-Session-Id absent or *NAS-IP-Address* absent ~~*User-Name* attribute absent~~	402 ~~402~~
No realm in the user name or *User-Name* has invalid realm part ~~No realm in the user name~~	503 ~~503~~
Invalid *NAS-IP-Address or* RFC3576 disallowed attribute in request ~~*User-Name* has invalid realm part~~	404 ~~503~~

4.4 *NAS-IP-Address* ~~*absent402Invalid NAS-IP-Address404Framed-IP-Address or X-Ascend-Session-Svr-Key absent402RFC3576 disallowed attribute in request404*~~General Usage Guidelines

- Telkom will rate limit incoming *Disconnect-Messages* from clients in order to prevent overloading our systems. Currently the limit is set at 1 request per second but may be changed without notice should the situation require it. Received messages exceeding the set limit will be discarded silently.
- Telkom will log all requests originating from IAPs. Misuse or incorrect usage of this service which may have an adverse effect on network performance will result in the originating IP being blocked, without prior notice, from using the service.

5. TELKOM PROXY SERVER ADDRESSES

IAPs must ensure that their RADIUS servers will accept requests from the following RADIUS proxy servers.

Site	Server Address
Bellville (Cape Town)	~~196.43.3.70~~ 196.43.3.76
	196.43.3.77
	196.43.3.86
	196.43.3.87
Rosebank (Johannesburg)	~~196.43.1.86~~ ~~196.43.1.87~~196.43.1.76
	~~196.43.1.88~~196.43.1.77
	196.43.1.86~~196.43.1.89~~
	196.43.1.87~~196.43.1.91~~
	196.43.1.88~~196.43.1.92~~
	196.43.1.89~~196.43.1.93~~

6. SAMPLE RADIUS PACKETS

Following are examples of typical Accounting packets.

6.1 Accounting Start Packet

Acct-Session-Id = "4/0/9/51.225_002114F5"	This value is unique for a particular NAS only
Framed-Protocol = PPP	
Framed-IP-Address = 41.244.201.40	
User-Name = "user1@isprealm.co.za"	
X-Ascend-Connect-Progress = LAN-Session-Up	
Acct-Authentic = RADIUS	
Acct-Status-Type = Start	
NAS-Port-Type = Virtual	Will usually have the value *Virtual* or *Ethernet*
NAS-Port = 1877084385	The two attributes are equivalent. *NAS-Port-Id* is a text representation on *NAS-Port*
NAS-Port-Id = "4/0/9/51.225"	
Connect-Info = "AutoShapedVC"	
Class = 0x4c5331	*Class* value expressed in Hexadecimal
Service-Type = Framed-User	
NAS-IP-Address = 196.43.27.20	This is the actual NAS where the PPP session is
X-Ascend-Session-Svr-Key = "A9511209"	Can be used as a *key* in Disconnect messages
Acct-Delay-Time = 0	
Telkom-Access-Type = "DSL"	

6.2 Accounting Interim Update Packet

Acct-Session-Id = "7/0/8/21.173_0A58286A"	
Framed-Protocol = PPP	
Framed-IP-Address = 41.241.32.62	
User-Name = " user1@isprealm.co.za "	
X-Ascend-Connect-Progress = LAN-Session-Up	
X-Ascend-PreSession-Time = 0	
X-Ascend-Xmit-Rate = 384000	
X-Ascend-Data-Rate = 384000	
Acct-Session-Time = 134224	
Acct-Input-Octets = 2882622	Upload Bytes since start of session
Acct-Output-Octets = 16933601	Download Bytes since start of session
Acct-Input-Gigawords = 0	The *Gigaword* counters will usually not be present unless either one has a non zero value.
Acct-Output-Gigawords = 1	
X-Ascend-Pre-Input-Octets = 87	
X-Ascend-Pre-Output-Octets = 43	
Acct-Input-Packets = 15963	
Acct-Output-Packets = 20834	
X-Ascend-Pre-Input-Packets = 3	
X-Ascend-Pre-Output-Packets = 3	
Acct-Authentic = RADIUS	
Acct-Status-Type = Interim-Update	
NAS-Port-Type = Virtual	
NAS-Port = 1697201837	
NAS-Port-Id = "7/0/8/21.173"	
Connect-Info = "AutoShapedVC"	
Class = 0x4e5331	
Service-Type = Framed-User	
NAS-IP-Address = 196.43.27.16	

```
X-Ascend-Session-Svr-Key = "60EF942C"
Acct-Delay-Time = 0
Telkom-Access-Type = "DSL"
```

6.3 Accounting Stop Packet

```
Acct-Session-Id = "4/1/7/2.647_030CCA7E"
Framed-Protocol = PPP
Framed-IP-Address = 41.240.24.240
User-Name = " user1@isprealm.co.za "
Acct-Authentic = RADIUS
X-Ascend-Connect-Progress = LAN-Session-Up
X-Ascend-PreSession-Time = 1
X-Ascend-Xmit-Rate = 384000
X-Ascend-Data-Rate = 384000
Acct-Session-Time = 15596
Acct-Input-Octets = 1020261
Acct-Output-Octets = 3898796
X-Ascend-Pre-Input-Octets = 163
X-Ascend-Pre-Output-Octets = 72
Acct-Input-Packets = 6620
Acct-Output-Packets = 7306
X-Ascend-Pre-Input-Packets = 8
X-Ascend-Pre-Output-Packets = 6
Acct-Terminate-Cause = User-Request        RFC standard disconnect reason
X-Ascend-Disconnect-Cause = 45             Ascend/Cisco specific disconnect reason
Acct-Status-Type = Stop
NAS-Port-Type = Virtual
NAS-Port = 1507427975
NAS-Port-Id = "4/1/7/2.647"
Connect-Info = "AutoShapedVC"
Class = 0x4e5331
Service-Type = Framed-User
NAS-IP-Address = 196.43.27.72
X-Ascend-Session-Svr-Key = "F7C77F7F"
Acct-Delay-Time = 0
Telkom-Access-Type = "DSL"
```