INTERNET-DRAFT
Title:
draft-chiba-radius-dynamic-disconnect-00.txt
Expires April 2002

Murtaza S. Chiba
Cisco Systems, Inc.

Gopal Dommety
Cisco Systems, Inc.

Mark Eklund
Cisco Systems, Inc.

David Mitton

November 2001

# Dynamic Disconnect



Abstract

This document describes the current practices for dynamically disconnecting a user session on the NAS.
The protocol uses RADIUS messages to send the disconnect request, but unlike RADIUS, the NAS in this case acts as a server and listens on a UDP port for requests originating from a client.

## 1.0 Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST — This word, or the adjective "required", means that the definition is an absolute requirement of the specification.

MUST NOT — This phrase means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the adjective "recommended", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.

MAY This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which does include the option.

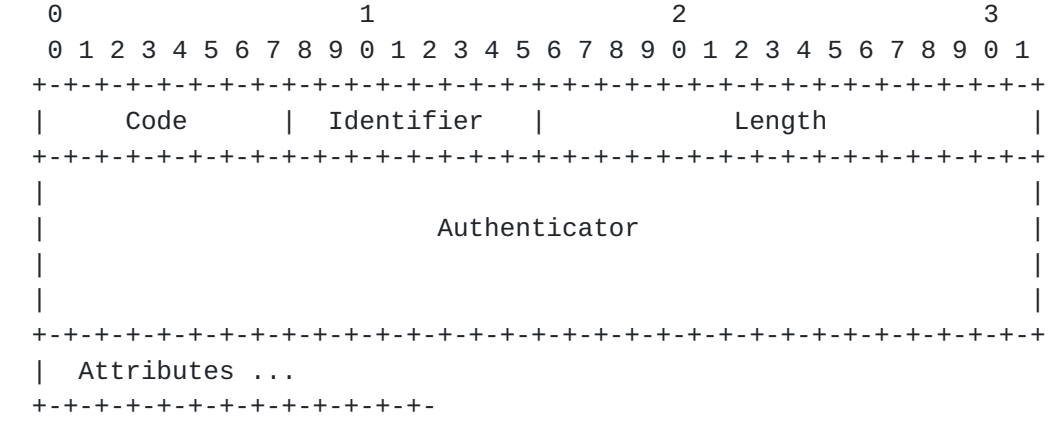
## 1.1 Introduction

The RADIUS protocol sends all the authorization information for a particular user in the Access-Accept packet and there are no further authorization exchanges between the NAS and the RADIUS server for the entire duration of the user session.
To overcome this limitation, various vendors have implemented a reverse RADIUS protocol in which the NAS listens on a port for messages initiated from a client. These messages currently belong to two groups:

1) Disconnect messages, and
2) Change of Filters messages

The disconnect messages cause a user session to be terminated immediately, whereas change of filter messages modify the applicable packet filters for the user session and is the subject of this draft.

The packet format consists of the fields: Code, Identifier, Length, Authenticator and the Attributes in the Type, Length and Value (TLV) formats. All the fields hold the same meaning as those described in RADIUS[1].



### 1.2 Current Practices

**This draft outlines the details for Disconnect Requests only and** will not attempt to detail Change of Filters which is considered as beyond the scope of this draft.

#### 1.2.1 Disconnect-Request (DR)

As mentioned earlier, the packet of disconnect is used to dynamically end a user session on a NAS. Current practices use the UPD port 1700 for sending requests. For responses the ports are reversed. The response packets do not contain any attributes, but the request message contains either, or all of the following identification attributes:

Username(1): This the name of the user associated with the session
Acct-Session-Id(44): This is derived from a RADIUS accounting Start
Framed-IP-Address(8): This is the IP Address associated with the session

Note:The numbers in parenthesis denote the attribute number in RADIUS.
The ability to use all/some of the identifiers to map to unique/multiple session(s) is beyond the scope of this document.


Codes used:
40 - Disconnect-Request
41 - Disconnect-ACK
42 - Disconnect-NAK

A Disconnect Request is followed by a response of either, Disconnect-Ack if the NAS successfully disconnects the user, or a Disconnect-NAK if it was unable to disconnect the user.

### 1.3 Security Considerations

**To prevent modification of the packets, a 16 byte Authenticator** is calculated employing the same algorithm as the one used for Accounting-Requests[3].
To prevent replay attacks it is recommended that the Acct-Session-ID and Username combination be present in the disconnect requests. Further, it is also recommended to include the Event-Timestamp(55)[4] attribute to prevent replay attacks.
The protocol, in addition, is susceptible to the same vulnerabilities as RADIUS and it is recommended to use IPSec to

afford better security.

## 1.4 Example Traces of current Disconnect Requests

Disconnect Request with Username:

```
 0: xxxx xxxx xxxx xxxx xxxx 2801 001c 1b23    .B.....$.-(....#
16: 624c 3543 ceba 55f1 be55 a714 ca5e 0108    bL5C..U..U...^..
32: 6d63 6869 6261
```

Disconnect Request with Acct-Session-ID:

```
 0: xxxx xxxx xxxx xxxx xxxx 2801 0018 ad0d    .B..... ~.(.....
16: 8e53 55b6 bd02 a0cb ace6 4e38 77bd 2c0a    .SU.......N8w.,.
32: 3930 3233 3435 3637                        90234567
```

Disconnect Request with Framed-IP-Address:

```
 0: xxxx xxxx xxxx xxxx xxxx 2801 001a 0bda    .B....."2.(.....
16: 33fe 765b 05f0 fd9c c32a 2f6b 5182 0806    3.v[.....*/kQ...
32: 0a00 0203
```

## 1.4 References

[1] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[2] Mitton, D., "Network Access Server Requirements: Extended RADIUS Practices", RFC 2882, July 2000.

[3] Rigney, C., "RADIUS Accounting", RFC 2866 June 2000.

[4] Rigney, C., Willats W., Calhoun P., "RADIUS Extensions", RFC 2869, June 2000

## 1.5 Copyright

English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

## 1.6 Acknowledgements

Funding for the RFC Editor function is currently provided by the Internet Society.

## 1.7 Author's Address

Murtaza Chiba
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

Tel: (408) 525-7198
mchiba@cisco.com

Gopal Dommety
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

Tel: (408) 525-1404
gdommety@cisco.com

Mark Eklund
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

Tel: (865) 671-6255
meklund@cisco.com

David Mitton
david@mitton.com