Experimental Handoff Extension to RADIUS

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

In order to decrease handoff latency, the concept of pre-emptive provisioning is under investigation. This document describes an experimental extension to the RADIUS protocol that enables a RADIUS server to notify a NAS of a prospective handoff. This enables the NAS to reserve resources and obtain the session parameters prior to arrival of the client, potentially reducing handoff times. Whether the approach described in this document is effective, deployable or secure is a subject of current research. As a result, implementation of this extension for purposes other than research is not recommended at this time.
Table of Contents

1. Introduction ............................................. 3
   1.1 Terminology ............................................. 4
   1.2 Requirements language .................................. 5
2. Packet format ............................................. 5
   2.1 Notify-Request .......................................... 7
   2.2 Notify-Accept ........................................... 7
   2.3 Notify-Reject ........................................... 8
3. Attributes ................................................... 9
   3.1 Previous-Called-Station-Id .............................. 9
   3.2 Table of attributes ..................................... 11
4. Security considerations .................................... 13
   4.1 IPsec usage guidelines .................................. 13
   4.2 Replay protection ....................................... 15
5. IANA considerations ...................................... 15
6. Normative references ..................................... 15
7. Informative references ................................... 16
ACKNOWLEDGMENTS .............................................. 17
AUTHORS’ ADDRESSES .......................................... 17
Intellectual Property Statement ............................... 18
Full Copyright Statement ..................................... 18
1. Introduction

In wireless networks such as IEEE 802.11, described in [IEEE80211], it may be desirable to improve the speed at which handoff can be completed. Where RADIUS Accounting [RFC2866] is implemented, RADIUS Accounting packets will be generated each time the client connects to a NAS. Accounting packets from a single session, across multiple NASes, are uniquely identified by the Acct-Multi-Session-Id attribute, described in [RFC2866] and [Congdon].

The sequence of NASes contacted by clients as they move creates a graph representing the mobility paths of the clients. We call this graph a neighbor graph with NASes as the vertices and the mobility paths between the NASes as the edges. Thus, the number of neighbors for a given NAS is given by the degree function applied to the vertex representing the given NAS, e.g.

\[
\text{deg}(v_A) \text{ where } \text{deg is the degree function } \text{and } v \rightarrow \text{int.}
\]

Through knowledge of the neighbor graph, it is possible for a RADIUS server to anticipate client movements and provide advance notice of a potential handoff to the NAS. This advance notice, known as a Notify-Request in this specification, allows the NAS to reserve resources and obtain the session authorization parameters prior to arrival of the client. This removes the latency of the RADIUS exchange from the critical path for processing a handoff, decreasing handoff latency substantially, as described in [IEEE-02-758, IEEE-03-084]. Assuming that the coverage area is over-lapping, this technique can support handoffs at vehicular velocities. The creation and maintenance of neighbor graphs at an AS is described in [Mishra].

An alternate approach to using neighbor graphs uses a matrix of probabilities and is described in [8021XHandoff].

By nature, client behavior is not completely predictable, so that the handoff advance notice is only advisory. The client identified in the advance notice may never contact the NAS, or may contact it long after the initial notice is received. As a result, the NAS will typically free reserved resources after a suitable waiting period, known as the Reservation-Lifetime. A client contacting the NAS after the Reservation-Lifetime has expired will be unable to complete a handoff, and will need to do a fast resume, such as is supported in EAP TLS [RFC2716].
The extension described in this document enables a RADIUS Server to send Notify-Requests to NASes, and to receive Notify-Responses. The Notify-Request identifies the session to be handed off. Attributes included within the Notify-Request are described in Section 2.1. If the NAS has resources available to reserve, and if it is enabled to support this handoff extension, then it will respond with a Notify-Accept. If resources are not available (such as when previous resource commitments leave insufficient resources remaining), or if the NAS does not wish to support the handoff for any other reason, the NAS will respond with a Notify-Reject, specifying the reason why the requested handoff reservation could not be carried out.

After the NAS responds with a Notify-Accept, it will typically issue an Access-Request to the RADIUS server. This allows the NAS to obtain the authorizations for the session before it is contacted by the client. The contents of the Access-Request sent by the NAS will depend on the form of access it is providing, so that it cannot be specified in detail here. However, for use with IEEE 802.11, it is expected that an Access-Request will be sent with a NAS-Port-Type=802.11 and a Service-Type=Handoff. For other access methods, a different NAS-Port-Type value might be sent, along with a different value for Service-Type.

1.1. Terminology

This document uses the following terms:

**Authenticator**

An Authenticator is an entity that requires authentication from the Supplicant. The Authenticator may be connected to the Supplicant at the other end of a point-to-point LAN segment or 802.11 wireless link.

**Authentication Server**

An Authentication Server is an entity that provides an Authentication Service to an Authenticator. This service verifies from the credentials provided by the Supplicant, the claim of identity made by the Supplicant.

**Network Access Server (NAS)**

The device providing access to the network.

**Service**

The NAS provides a service to the user, such as IEEE 802 or PPP.

**Port Access Entity (PAE)**

The protocol entity associated with a physical or virtual (802.11) Port. A given PAE may support the protocol functionality associated with the Authenticator, Supplicant or
Session  Each service provided by the NAS to a user constitutes a session, with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended. A user may have multiple sessions in parallel or series if the NAS supports that, with each session generating a separate start and stop accounting record. Where the client is mobile and is able to handoff between NASes, multiple related sessions may be uniquely identified by the Acct-Multi-Session-Id attribute.

Supplicant

A Supplicant is an entity that is being authenticated by an Authenticator. The Supplicant may be connected to the Authenticator at one end of a point-to-point LAN segment or 802.11 wireless link.

1.2. Requirements language

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Packet format

Exactly one Notify-Request, Notify-Accept or Notify-Reject packet is encapsulated in the UDP Data field. For the Notify-Request packet, the UDP Destination Port field is TBD. When a reply is generated, the source and destination ports are reversed.

A summary of the data format is shown below. The fields are transmitted from left to right.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
Code

The Code field is one octet, and identifies the type of RADIUS packet. When a packet is received with an invalid Code field, it is silently discarded. RADIUS codes (decimal) for this extension are assigned as follows:

- TBD - Notify-Request
- TBD - Notify-Accept
- TBD - Notify-Reject

Identifier

The Identifier field is one octet, and aids in matching requests and replies. The RADIUS server can detect a duplicate request if it has the same client source IP address and source UDP port and Identifier within a short span of time.

Length

The Length field is two octets. It indicates the length of the packet including the Code, Identifier, Length, Authenticator and Attribute fields. Octets outside the range of the Length field MUST be treated as padding and ignored on reception. If the packet is shorter than the Length field indicates, it MUST be silently discarded. The minimum length is 20 and maximum length is 4096.

Authenticator

The Authenticator field is sixteen (16) octets. The most significant octet is transmitted first. This value is used to authenticate the messages between the client and RADIUS server.

Request Authenticator

In Notify-Request Packets, the Authenticator value is a 16 octet MD5 [RFC1321] checksum, called the Request Authenticator. The Request Authenticator is calculated the same way as for an Accounting-Request, specified in [RFC2866].

Note that the Request Authenticator of a Notify-Request can not be done the same way as the Request Authenticator of a RADIUS Access-Request, because there is no User-Password attribute in a Notify-Request.

Response Authenticator

The Authenticator field in a Notify-Accept or Notify-Reject packet is
called the Response Authenticator, and contains a one-way MD5 hash calculated over a stream of octets consisting of the Notify-Response Code, Identifier, Length, the Request Authenticator field from the Notify-Request packet being replied to, and the response attributes if any, followed by the shared secret. The resulting 16 octet MD5 hash value is stored in the Authenticator field of the Notify-Accept or Notify-Reject packet.

Attributes

Attributes may have multiple instances, in such a case the order of attributes of the same type SHOULD be preserved. The order of attributes of different types is not required to be preserved.

2.1. Notify-Request

Description

A Notify-Request packet is sent by the RADIUS server to the NAS to notify it of the potential handoff of a specified session.

Code

TBD - Notify-Request

Identifier

The Identifier field MUST be changed whenever the content of the Attributes field changes, and whenever a valid reply has been received for a previous request. For retransmissions where the contents are identical, the Identifier MUST remain unchanged.

Note that if the Event-Timestamp attribute is included the Notify-Request then the Event-Timestamp value will be updated when the packet is retransmitted, changing the content of the Attributes field and requiring a new Identifier and Request Authenticator.

Request Authenticator

The Request Authenticator of an Accounting-Request contains a 16-octet MD5 hash value calculated according to the method described in "Request Authenticator" in Section 2.

Attributes

The Attribute field is variable in length, and contains a list of Attributes. Within the Notify-Request, Attributes are used to uniquely identify the user session that may potentially be handed off
to the NAS, and to describe the services expected to be provided. Where RADIUS is not protected by IPsec, the Event-Timestamp attribute MUST be included so as to protect against replay attacks. Section 3.4 provides more detail on the attributes permitted within the Notify-Request packet.

2.2. Notify-Accept

Description

The NAS responds to the Notify-Request with a Notify-Accept if the NAS agrees to prepare for a handoff of the specified session.

Code

TBD - Notify-Accept

Identifier

The Identifier field is a copy of the Identifier field of the Notify-Request which caused this Notify-Accept.

Response Authenticator

The Response Authenticator of a Notify-Accept contains a 16-octet MD5 hash value calculated according to the method described in "Response Authenticator" in Section 2.

Attributes

The Attribute field is variable in length, and contains a list of Attributes. Within the Notify-Accept, attributes are used to provide the RADIUS server with the session identifiers that will be used by the NAS in subsequent Access-Request and Accounting-Request packets. This includes the User-Name and Acct-Multi-Session-Id attributes originally provided by the RADIUS server in the Notify-Request, as well as an Acct-Session-Id allocated by the NAS for the handoff, should it occur. The Idle-Timeout attribute, when included in the Notify-Accept, provides the RADIUS server with the time that the NAS is willing to reserve resources for the handoff. Where RADIUS is not protected by IPsec, the Event-Timestamp attribute MUST be included so as to protect against replay attacks. Section 3.4 provides more detail on the attributes permitted within the Notify-Accept packet.

2.3. Notify-Reject

Description
The NAS responds to the Notify-Request with a Notify-Reject if the NAS does not have the resources to make the required handoff preparations, or wishes to decline for any other reason.

Code

TBD - Notify-Reject

Identifier

The Identifier field is a copy of the Identifier field of the Notify-Request which caused this Notify-Reject.

Response Authenticator

The Response Authenticator of a Notify-Accept contains a 16-octet MD5 hash value calculated according to the method described in "Response Authenticator" in Section 2.

Attributes

The Attribute field is variable in length, and contains a list of Attributes. Within the Notify-Reject, attributes are used to provide the RADIUS server with the reason why the Notify-Request could not be honored. If the NAS is configured so as not to support the Handoff extension, then an Acct-Terminate-Cause attribute with a value of Admin Reset (5) is included. If the service described in the Notify-Request is not supported, then an Acct-Terminate-Cause attribute with a value of Service Unavailable (15) is included. If resources are not available, then an Acct-Terminate-Cause of Port Preempted (13) is included. Where RADIUS is not protected by IPsec, the Event-Timestamp attribute MUST be included so as to protect against replay attacks. Section 3.4 provides more detail on the attributes permitted within the Notify-Reject packet.

3. Attributes

3.1. Previous-Called-Station-Id

Description

This Attribute allows the RADIUS server to send in the Notify-Request packet the link layer address of the NAS that the user last connected to. For IEEE 802.1X Authenticators, this attribute is used to store the bridge or Access Point MAC address in ASCII format, with octet values separated by a "-". Example: "00-10-A4-23-19-C0". In IEEE 802.11, where the SSID is known, it SHOULD be appended to the Access Point MAC address, separated from the MAC address with a ":".
Example "00-10-A4-23-19-C0:AP1". In the case of a dialup network, this would be the phone number that the user called, using Dialed Number Identification (DNIS) or similar technology. It is only used in Notify-Request packets.
A summary of the Previous-Called-Station-Id Attribute format is shown below. The fields are transmitted from left to right.

```
0                   1                   2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |  String ... |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

**Type**

TBD

**Length**

>=3

**String**

The String field is one or more octets, containing the link layer address that the user session last connected to. The actual format of the information is site or application specific. A robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.
### 3.2. Table of Attributes

The following table provides a guide to which attributes may be found in which kinds of packets, and in what quantity. If an attribute is not mentioned in this table, then it is not permitted in Notify-Request, Notify-Accept or Notify-Reject packets.

<table>
<thead>
<tr>
<th>Notify Request</th>
<th>Notify Accept</th>
<th>Notify Reject</th>
<th>#</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1</td>
<td>0-1</td>
<td>0</td>
<td>1</td>
<td>User-Name [Note 1]</td>
</tr>
<tr>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>NAS-IP-Address [Note 2]</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>Service-Type [Note 10,11]</td>
</tr>
<tr>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>Framed-Protocol [Note 10]</td>
</tr>
<tr>
<td>0-1</td>
<td>0-1</td>
<td>0</td>
<td>28</td>
<td>Idle-Timeout [Note 3]</td>
</tr>
<tr>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>30</td>
<td>Called-Station-Id [Note 4]</td>
</tr>
<tr>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>31</td>
<td>Calling-Station-Id [Note 1]</td>
</tr>
<tr>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>32</td>
<td>NAS-Identifier [Note 2]</td>
</tr>
<tr>
<td>0+</td>
<td>0+</td>
<td>0+</td>
<td>33</td>
<td>Proxy-State</td>
</tr>
<tr>
<td>0</td>
<td>0-1</td>
<td>0</td>
<td>44</td>
<td>Acct-Session-Id [Note 7]</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0-1</td>
<td>49</td>
<td>Acct-Terminate-Cause [Note 8]</td>
</tr>
<tr>
<td>0-1</td>
<td>0-1</td>
<td>0</td>
<td>50</td>
<td>Acct-Multi-Session-Id [Note 6]</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>55</td>
<td>Event-Timestamp [Note 9]</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>61</td>
<td>NAS-Port-Type [Note 10]</td>
</tr>
<tr>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>TBD</td>
<td>Previous-Called-Station-Id [Note 5]</td>
</tr>
</tbody>
</table>

[Note 1] The User-Name attribute, if provided in the Notify-Request MUST be echoed in the Notify-Accept, and subsequent Access-Request packets. If the User-Name attribute is not provided, then it is assumed that the identity is provided by the Calling-Station-Id field, which MUST be present.

[Note 2] A Notify-Request MUST contain either a NAS-IP-Address or a NAS-Identifier (or both).

[Note 3] Within a Notify-Request, the Idle-Timeout attribute provides a suggested amount of time for which the NAS may reserve resources for a potential handoff. If an Idle-Timeout attribute is included within the Notify-Request, then if the NAS is unable to reserve resources for this period of time, then it MUST include an Idle-Timeout attribute in the Notify-Accept, if sent, specifying the time it is willing to commit to. The RADIUS server should assume that the resources have been released at time Event-Timestamp + Idle-Timeout.

[Note 4] Within a Notify-Request, the Called-Station-Id refers to the NAS to which the Notify-Request is sent. If it this does not match the actual value of the NAS Called-Station-Id, then a Notify-Reject...
MUST be sent.

[Note 5] Within a Notify-Request, the Previous-Called-Station-Id refers to the NAS from which the handoff is expected to occur. If the handoff does not occur from that NAS, then the NAS receiving the handoff MAY reject access. In the case where NAS-Port-Type = 802.11, and the Previous-Called-Station-Id contains an SSID, then if the handoff occurs, the client MUST be granted access only to this SSID. If the attempts to connect to another SSID, then the NAS MUST deny network access to the client. If the SSID field is omitted, then a value of ANY is assumed.

[Note 6] Within a Notify-Request, the Acct-Multi-Session-Id provides a unique identifier for the client sessions during handoffs between NASes. The Acct-Multi-Session-Id is echoed in subsequent Access-Request and Accounting-Request packets.

[Note 7] The Acct-Session-Id, if present in Notify-Accept packets, denotes the accounting session id allocated by the NAS for the prospective handoff, should it occur. The Acct-Session-Id is echoed in subsequent Access-Request and Accounting-Request packets.

[Note 8] The Acct-Terminate-Cause is present only in Notify-Reject packets, and specifies the reason for the rejection.

[Note 9] When RADIUS is not protected by IPsec, the Event-Timestamp attribute MUST be present in all packets in order to prevent replay attacks. This is discussed in Section 4.

[Note 10] The Service-Type, NAS-Port-Type and Framed-Protocol attributes are used to specify the services that are to be provided to the handed off session. The Service-Type and NAS-Port-Type attributes MUST be present in the Notify-Request; when used with 802.11, it is expected that a NAS-Port-Type=802.11 and a Service-Type=Handoff will be included. The Service-Type is echoed in the subsequent Access-Request. If the NAS is not able to provide the specified service, then it MUST send a Notify-Reject.

[Note 11] The Service-Type value of Handoff, when used by the NAS in an Access-Request packet, indicates that a handoff request is being anticipated and that the RADIUS server should send back an Access-Accept to allow the prospective handoff to occur, or an Access-Reject to deny the prospective handoff. The decision is typically based on the User-Name, Called-Station-Id or Calling-Station-Id. As with a normal Access-Request, the User-Name attribute is expected to be filled in. Note that the service provided when Service-Type=Handoff differs from that provided when Service-Type=Call Check.
With Handoff, the NAS MUST authenticate the user during the handoff prior to allowing access, using credentials provided by the RADIUS server, whereas with a Service-Type=Call Check, the authentication is implicit and access is permitted or denied purely based on the Called-Station-Id or Calling-Station-Id.

The following table defines the meaning of the above table entries.

| 0  | This attribute MUST NOT be present in packet. |
| 0+ | Zero or more instances of this attribute MAY be present in packet. |
| 0-1| Zero or one instance of this attribute MAY be present in packet. |
| 1  | Exactly one instance of this attribute MUST be present in packet. |

4. Security considerations

4.1. IPsec usage guidelines

Implementations of this specification SHOULD support IPsec [RFC2401] along with IKE [RFC2409] for key management. IPsec ESP [RFC2406] with non-null transform, and per-packet authentication, integrity and replay protection SHOULD be used, along with IKE for key management.

Within RADIUS [RFC2865], a shared secret is used for hiding of attributes such as User-Password, as well as in computation of the Response Authenticator. In RADIUS accounting [RFC2866], the shared secret is used in computation of both the Request Authenticator and the Response Authenticator.

Since in RADIUS a shared secret is used to provide confidentiality as well as integrity protection and authentication, only use of IPsec ESP with a non-null transform can provide security services sufficient to substitute for RADIUS application-layer security. Therefore, where IPSEC AH or ESP null is used, it will typically still be necessary to configure a RADIUS shared secret.

Where RADIUS is run over IPsec ESP with a non-null transform, the secret shared between the NAS and the RADIUS server may not be configured. In this case, a shared secret of zero length MUST be assumed. However, a RADIUS server that cannot know whether incoming traffic is IPsec-protected MUST be configured with a non-null RADIUS shared secret. When IPsec ESP is used with RADIUS, DES-CBC SHOULD NOT be used as the encryption transform, and per-packet authentication, integrity and replay protection MUST be used.

A typical IPsec policy for an IPsec-capable RADIUS client is "Initiate IPsec, from me to any, destination port UDP 1812". This causes an IPsec SA to be set up by the RADIUS client prior to sending RADIUS traffic to any RADIUS server. If some RADIUS servers contacted by the client do not
support IPsec, then a more granular policy will be required.

For a client implementing this specification the policy would be "Accept IPsec, from any to me, destination port UDP TBD". This causes the RADIUS client to accept (but not require) use of IPsec. It may not be appropriate to require IPsec for all RADIUS servers connecting to an IPsec-enabled RADIUS client, since some RADIUS servers may not support IPsec.

For an IPsec-capable RADIUS server, a typical IPsec policy is "Accept IPsec, from any to me, destination port 1812". This causes the RADIUS server to accept (but not require) use of IPsec. It may not be appropriate to require IPsec for all RADIUS clients connecting to an IPsec-enabled RADIUS server, since some RADIUS clients may not support IPsec.

For servers implementing this specification, the policy would be "Initiate IPsec, from me to any, destination port UDP TBD". This causes the RADIUS server to initiate IPsec when sending RADIUS extension traffic to any RADIUS client. If some RADIUS clients contacted by the server do not support IPsec, then a more granular policy will be required.

Where IPsec is used for security, and no RADIUS shared secret is configured, it is important that trust be demonstrated between the RADIUS client and RADIUS server by some means. For example, before enabling an IKE-authenticated host to act as a RADIUS client, the RADIUS server should check whether the host is authorized to provide network access. For example, the RADIUS server can be configured with the IP addresses (for IKE Aggressive Mode with pre-shared keys) or FQDNs (for certificate authentication) of RADIUS clients.

Alternatively, if a separate CA exists for RADIUS clients, then the RADIUS server can configure this CA as a trusted root for use with IPsec. However, unlike SSL/TLS, IKE does not permit certificate policies to be set on a per-port basis, such a policy would need to apply to all uses of IPsec on RADIUS clients and servers. Assuming that only certificate authentication is supported in the deployment, a management station initiating an IPsec-protected telnet session to the RADIUS server would need to obtain a certificate chaining to the RADIUS client CA. Issuing such a certificate might not be appropriate if the management station was not authorized as a RADIUS client.

Where RADIUS clients may obtain their IP address dynamically (such as an Access Point supporting DHCP), Main Mode with pre-shared keys [RFC2409] SHOULD NOT be used, since this requires use of a group pre-shared key; instead, Aggressive Mode SHOULD be used. Where RADIUS client addresses are statically assigned either Aggressive Mode or Main Mode MAY be used.
With certificate authentication, Main Mode SHOULD be used.

Care needs to be taken with IKE Phase 1 Identity Payload selection in order to enable mapping of identities to pre-shared keys even with Aggressive Mode. Where the ID_IPV4_ADDR or ID_IPV6_ADDR Identity Payloads are used and addresses are dynamically assigned, mapping of identities to keys is not possible, so that group pre-shared keys are still a practical necessity. As a result, the ID_FQDN identity payload SHOULD be employed in situations where Aggressive mode is utilized along with pre-shared keys and IP addresses are dynamically assigned. This approach also has other advantages, since it allows the RADIUS server and client to configure themselves based on the fully qualified domain name of their peers.

Note that with IPsec, security services are negotiated at the granularity of an IPsec SA, so that RADIUS exchanges requiring a set of security services different from those negotiated with existing IPsec SAs will need to negotiate a new IPsec SA. Separate IPsec SAs are also advisable where quality of service considerations dictate different handling RADIUS conversations. Attempting to apply different quality of service to connections handled by the same IPsec SA can result in reordering, and falling outside the replay window. For a discussion of the issues, see [RFC2983].

4.2. Replay protection

Since this specification utilizes the Request Authenticator field for integrity protection and authentication, rather than as a nonce, no liveness or protection against replay is provided by the RADIUS header.

Where IPsec is not used, in order to provide replay protection, the Event-Timestamp (55) attribute, described in [RFC2869] MUST be included. When this attribute is present, the RADIUS server MUST check that the Event-Timestamp is current within an acceptable time window. This implies the need for time synchronization within the network, which can be achieved via a variety of mechanisms, including secure NTP, as described in [NTPAuth]. A default time window of 300 seconds is recommended.

5. IANA Considerations

This specification requires assignment a UDP port, in addition to RADIUS Type codes for Notify-Request, Notify-Accept, and Notify-Reject. Assignment of Attribute Type codes are also required for the following attributes: Previous-Called-Station-Id. A new value is requested to be allocated for the Service-Type attribute for Handoff.
6. Normative references


7. Informative references


Acknowledgments

The authors would like to acknowledge the following people for contributions on this document: Tim Moore (Microsoft), Min-ho Shin (University of Maryland), Nick Petroni (University of Maryland), Adam Sulmicki (University of Maryland), Insun Lee (Samsung Electronics), Kyunghun Jang (Samsung Electronics).

Authors’ Addresses

William A. Arbaugh
Department of Computer Science
University of Maryland, College Park
A.V. Williams Building
College Park, MD 20742

EMail: waa@cs.umd.edu
Phone: +1 301 405 2774

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.
Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved. This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."
Expiration Date

This memo is filed as `<draft-irtf-aaarch-handoff-00.txt>`, and expires August 22, 2003.