Internet Engineering Task Force (IETF)
Request for Comments: 8559
Updates: 5176, 5580
Category: Standards Track
ISSN: 2070-1721

A. DeKok
FreeRADIUS
J. Korhonen

April 2019

Dynamic Authorization Proxying in the Remote Authentication Dial-In User Service (RADIUS) Protocol

Abstract

RFC 5176 defines Change-of-Authorization (CoA) and Disconnect Message (DM) behavior for RADIUS. RFC 5176 also suggests that proxying these messages is possible, but it does not provide guidance as to how that is done. This specification updates RFC 5176 to correct that omission for scenarios where networks use realm-based proxying as defined in RFC 7542. This specification also updates RFC 5580 to allow the Operator-Name attribute in CoA-Request and Disconnect-Request packets.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8559.

Table of Contents

1. Introduction

RFC 5176 [RFC5176] defines Change-of-Authorization (CoA) and Disconnect Message (DM) behavior for RADIUS. Section 3.1 of [RFC5176] suggests that proxying these messages is possible, but it does not provide guidance as to how that is done. This omission means that in practice, proxying of CoA packets is impossible.

We partially correct that omission here by explaining how proxying of these packets can be done by leveraging an existing RADIUS attribute, Operator-Name (Section 4.1 of [RFC5580]). We then explain how this attribute can be used by proxies to route packets "backwards" through a RADIUS proxy chain from a home network to a visited network. We then introduce a new attribute: Operator-NAS-Identifier. This attribute permits packets to be routed from the RADIUS server at the visited network to the Network Access Server (NAS).

This correction is limited to the use case of realm-based proxying as defined in [RFC7542]. Other forms of proxying are possible but are not discussed here. We note that the recommendations provided in this document apply only to those systems that implement proxying of CoA packets, and then only to those that implement realm-based CoA proxying. This specification neither requires nor suggests changes to any implementation or deployment of any other RADIUS systems.

We also update the behavior described in [RFC5580] to allow the Operator-Name attribute to be used in CoA-Request and Disconnect-Request packets, as further described in this document.

This document is a Standards Track document in order to update the behavior described in [RFC5580], as [RFC5580] is also a Standards Track document. This document relies heavily upon and also updates some of the behaviors described in RFC 5176, which is an Informational document; because the applicability statements in Section 1.1 of [RFC5176] do not apply to this document, this document does not change the status of [RFC5176].

We finally conclude with a discussion of the security implications of this design and show that they do not decrease the security of the network.

1.1. Terminology

This document frequently uses the following terms:

CoA

: Change of authorization, e.g., CoA-Request, CoA-ACK, or CoA-NAK, as defined in [RFC5176]. [RFC5176] also defines Disconnect-Request, Disconnect-ACK, and Disconnect-NAK. For simplicity, where we use "CoA" in this document, we mean a generic "CoA-Request or Disconnect-Request" packet. We use "CoA-Request" or "Disconnect-Request" to refer to the specific packet types.

Network Access Identifier (NAI)

: The user identity submitted by the client during network access authentication. See [RFC7542]. The purpose of the NAI is to identify the user as well as assist in the routing of the authentication request. Please note that the NAI may not necessarily be the same as the user's email address or the user identity submitted in an application-layer authentication.

Network Access Server (NAS)

: The device that clients connect to in order to get access to the network. In Point-to-Point Tunneling Protocol (PPTP) terminology, this is referred to as the PPTP Access Concentrator (PAC), and in Layer 2 Tunneling Protocol (L2TP) terminology, it is referred to as the L2TP Access Concentrator (LAC). In IEEE 802.11, it is referred to as an Access Point.

Home Network

: The network that holds the authentication credentials for a user.

Visited Network

: A network other than the home network, where the user attempts to gain network access. The visited network typically has a relationship with the home network, possibly through one or more intermediary proxies.

1.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Problem Statement

This section describes how RADIUS proxying works, how CoA packets work, and why CoA proxying as discussed in [RFC5176] is insufficient to create a working system.

2.1. Typical RADIUS Proxying

When a RADIUS server proxies an Access-Request packet, it typically does so based on the contents of the User-Name attribute, which contains an NAI [RFC7542]. This specification describes how to use the NAI in order to proxy CoA packets across multiple hops. Other methods of proxying CoA packets are possible but are not discussed here.

In order to determine the "next hop" for a packet, the proxying server looks up the "realm" portion of the NAI in a logical Authentication, Authorization, and Accounting (AAA) routing table, as described in Section 3 of [RFC7542]. The entry in that table contains information about the next hop to which the packet is sent. This information can be IP address, shared secret, certificate, etc. The next hop may also be another proxy, or it may be the home server for that realm.

If the next hop is a proxy, that proxy will perform the same realm lookup and then proxy the packet as above. At some point, the next hop will be the home server for that realm.

The home server validates the NAI in the User-Name attribute against the list of realms hosted by the home network. If there is no match, then an Access-Reject is returned. All other packets are processed through local site rules, which result in an appropriate response packet being sent. This response packet can be Access-Accept, Access-Challenge, or Access-Reject.

The RADIUS client receiving that response packet will match it to an outstanding request. If the client is part of a proxy, the proxy will then send that response packet in turn to the system that originated the Access-Request. This process continues until the response packet arrives at the NAS.

The proxies are typically stateful with respect to ongoing request/response packets but are stateless with respect to user sessions. That is, once a response has been sent by the proxy, it can discard all information about the request packet, other than what is needed for detecting retransmissions as per Section 2.2.2 of [RFC5080].

The same method is used to proxy Accounting-Request packets. Proxying both Access-Request and Accounting-Request packets allows proxies to connect visited networks to home networks for all AAA purposes.

2.2. CoA Processing

[RFC5176] describes how CoA clients send packets to CoA servers. We note that a system comprising the CoA client is typically co-located with, or is the same as, the RADIUS server. Similarly, the CoA server is a system that is either co-located with or the same as the RADIUS client.

In the case of packets sent inside of one network, the source and destination of CoA packets are locally determined. There is thus no need for standardization of that process, as networks are free to send CoA packets whenever they want, for whatever reason they want.

2.3. Failure of CoA Proxying

The situation is more complicated when proxies are involved. [RFC5176] suggests that CoA proxying is permitted, but [RFC5176] does not make any suggestions as to how that proxying should be done.

If proxies were to track user sessions, it would be possible for a proxy to match an incoming CoA packet to a user session and then to proxy the CoA packet to the RADIUS client that originated the Access-Request for that session. There are many problems with such a scenario.

The CoA server might not, in fact, be co-located with the RADIUS client, in which case it might not have access to user session information for performing the reverse path forwarding.

The CoA server may be down, but there may be a different CoA server that could successfully process the packet. The CoA client should then fail over to a different CoA server. If the reverse path is restricted to be the same as the forward path, then such failover is not possible.

In a roaming consortium, the proxies may forward traffic for tens of millions of users. Tracking each user session can be expensive and complicated, and doing so does not scale well. For that reason, most proxies do not record user sessions.

Even if the proxy recorded user sessions, [RFC5176] is silent on the topic of what attributes constitute "session identification attributes". That silence means it is impossible for a proxy to determine if a CoA packet matches a particular user session.

The result of all of these issues is that CoA proxying is impossible when using the behavior defined in [RFC5176].

3. How to Perform CoA Proxying

The solution to the above problem is to use realm-based proxying on the reverse path, just as with the forward path. In order for the reverse path proxying to work, the proxy decision must be based on an attribute other than User-Name.

The reverse path proxying can be done by using the Operator-Name attribute defined in Section 4.1 of [RFC5580]. We repeat a portion of that definition here for clarity:

> This attribute carries the operator namespace identifier and the operator name. The operator name is combined with the namespace identifier to uniquely identify the owner of an access network.

...followed a few paragraphs later by a description of the REALM namespace:

> REALM ('1' (0x31)):
>
> > The REALM operator namespace can be used to indicate operator names based on any registered domain name. Such names are required to be unique, and the rights to use a given realm name are obtained coincident with acquiring the rights to use a particular Fully Qualified Domain Name (FQDN). ...

In short, the Operator-Name attribute contains an ASCII "1", followed by the realm of the visited network. For example, for the "example.com" realm, the Operator-Name attribute contains the text "1example.com". This information is precisely what is needed by intermediate nodes in order to perform CoA proxying.

The remainder of this document describes how CoA proxying can be performed by using the Operator-Name attribute. We describe the following:

- how the forward path has to change in order to allow reverse path proxying
- how reverse path proxying works
- how visited networks and home networks have to behave in order for CoA proxying to work

We note that as a proxied CoA packet is sent to only one destination, the Operator-Name attribute MUST NOT occur more than once in a packet. If a packet contains more than one Operator-Name, implementations MUST treat the second and subsequent attributes as "invalid attributes", as discussed in Section 2.8 of [RFC6929].

3.1. Changes to Access-Request and Accounting-Request Packets

When a visited network proxies an Access-Request or Accounting-Request packet outside of its network, a visited network that wishes to support realm-based CoA proxying SHOULD include an Operator-Name attribute in the packet, as discussed in Section 4.1 of [RFC5580]. The contents of the Operator-Name attribute should be "1", followed by the realm name of the visited network. Where the visited network has more than one realm name, a "canonical" name SHOULD be chosen and used for all packets.

Visited networks MUST use a consistent value for Operator-Name for any one user session. That is, sending "1example.com" in an Access-Request packet and "1example.org" in an Accounting-Request packet for that same session is forbidden. Such behavior would make it look like a single user session was active simultaneously in two different visited networks, which is impossible.

Proxies that record user session information SHOULD also record Operator-Name. Proxies that do not record user session information do not need to record Operator-Name.

Home networks SHOULD record Operator-Name along with any other information that they record about user sessions. Home networks that expect to send CoA packets to visited networks MUST record Operator-Name for each user session that originates from a visited network. Failure to record Operator-Name would mean that the home network would not know where to send any CoA packets.

Networks that host both the RADIUS client and RADIUS server do not need to create, record, or track Operator-Name. That is, if the visited network and home network are the same, there is no need to use the Operator-Name attribute.

3.2. Proxying of CoA-Request and Disconnect-Request Packets

When a home network wishes to send a CoA-Request or Disconnect-Request packet to a visited network, it MUST include an Operator-Name attribute in the CoA packet. The value of the Operator-Name attribute MUST be the value that was recorded earlier for that user session.

The home network MUST look up the realm from the Operator-Name attribute in a logical "realm routing table", as discussed in Section 3 of [RFC7542]. That logical realm table is defined therein as:

> ... a logical AAA routing table, where the "utf8-realm" portion acts as a key, and the values stored in the table are one or more "next hop" AAA servers.

In order to support proxying of CoA packets, this table is extended to include a mapping between "utf8-realm" and one or more next-hop CoA servers.

When proxying CoA-Request and Disconnect-Request packets, the lookups will return data from the "CoA server" field instead of the "AAA server" field.

In practice, this process means that CoA proxying works exactly like "normal" RADIUS proxying, except that the proxy decision is made using the realm from the Operator-Name attribute instead of using the realm from the User-Name attribute.

Proxies that receive the CoA packet will look up the realm from the Operator-Name attribute in a logical "realm routing table", as with home servers, above. The packet is then sent to the proxy for the realm that was found in that table. This process continues with any subsequent proxies until the packet reaches a public CoA server at the visited network.

Where the realm is unknown, the proxy MUST return a NAK packet that contains an Error-Cause Attribute having value 502 ("Request Not Routable").

Proxies that receive a CoA packet MUST NOT use the NAI from the User-Name attribute in order to make proxying decisions. Doing so would result in the CoA packet being forwarded to the home network, while the user's session is in the visited network.

We also update Section 5 of [RFC5580] to permit CoA-Request and Disconnect-Request packets to contain zero or one instance of the Operator-Name attribute.

3.3. Reception of CoA-Request and Disconnect-Request Packets

After some proxying, the CoA packet will be received by the CoA server in the visited network. That CoA server MUST validate the NAI in the Operator-Name attribute against the list of realms hosted by the visited network. If the realm is not found, then the CoA server MUST return a NAK packet that contains an Error-Cause Attribute having value 502 ("Request Not Routable").

Some home networks will not have permission to send CoA packets to the visited network. The CoA server SHOULD therefore also validate the NAI contained in the User-Name attribute. If the home network is not permitted to send CoA packets to this visited network, then the CoA server MUST return a NAK packet that contains an Error-Cause Attribute having value 502 ("Request Not Routable").

These checks make it more difficult for a malicious home network to scan roaming networks in order to determine which visited network hosts which realm. That information should be known to all parties in advance and exchanged via methods outside the scope of this specification. Those methods will typically be in the form of contractual relationships between parties or membership in a roaming consortium.

The CoA server in the visited network will also ensure that the Operator-NAS-Identifier attribute is known, as described below. If the attribute matches a known NAS, then the packet will be sent to that NAS. Otherwise, the CoA server MUST return a NAK packet that contains an Error-Cause Attribute having value 403 ("NAS Identification Mismatch").

All other received packets are processed as per local site rules and will result in an appropriate response packet being sent. This process mirrors the method used to process Access-Request and Accounting-Request packets (described above).

Processing done by the visited network will normally include sending the CoA packet to the NAS, having the NAS process it, and then returning any response packets back up the proxy chain to the home server.

The only missing piece here is the procedure by which the visited network gets the packet from its public CoA server to the NAS. The visited network could use NAS-Identifier, NAS-IP-Address, or NAS-IPv6-Address, but these attributes may have been edited by an intermediate proxy or the attributes may be missing entirely.

These attributes may be incorrect because proxies forwarding Access-Request packets often rewrite them for internal policy reasons. These attributes may be missing, because the visited network may not want all upstream proxies and home servers to have detailed information about the internals of its private network and may remove them itself.

We therefore need a way to identify a NAS in the visited network via a method that affords privacy and does not use any existing attributes. Our solution is to define an Operator-NAS-Identifier attribute, which identifies an individual NAS in the visited network.

3.4. Operator-NAS-Identifier

The Operator-NAS-Identifier attribute is an opaque token that identifies an individual NAS in a visited network. It MAY appear in the following packets: Access-Request, Accounting-Request, CoA-Request, or Disconnect-Request. Operator-NAS-Identifier MUST NOT appear in any other packets.

Operator-NAS-Identifier MAY occur in a packet if the packet also contains an Operator-Name attribute. Operator-NAS-Identifier MUST NOT appear in a packet if there is no Operator-Name in the packet. As each proxied CoA packet is sent to only one NAS, the Operator-NAS-Identifier attribute MUST NOT occur more than once in a packet. If a packet contains more than one Operator-NAS-Identifier, implementations MUST treat the second and subsequent attributes as "invalid attributes", as discussed in Section 2.8 of [RFC6929].

An Operator-NAS-Identifier attribute SHOULD be added to an Access-Request or Accounting-Request packet by a visited network, before proxying a packet to an external RADIUS server. When the Operator-NAS-Identifier attribute is added to a packet, the following attributes SHOULD be deleted from the packet: NAS-IP-Address, NAS-IPv6-Address, and NAS-Identifier. If these attributes are deleted, the proxy MUST then add a new NAS-Identifier attribute,

in order to satisfy the requirements of Section 4.1 of [RFC2865] and Section 4.1 of [RFC2866]. The contents of the new NAS-Identifier attribute SHOULD be the realm name of the visited network.

When a server receives a packet that already contains an Operator-NAS-Identifier attribute, no such editing is performed.

The Operator-NAS-Identifier attribute MUST NOT be added to any packet by any other proxy or server in the network. Only the visited network (i.e., the operator) can name a NAS that is inside of the visited network.

The result of these requirements is that for everyone outside of the visited network there is only one NAS: the visited network itself. Also, the visited network is able to identify its own NASes to its own satisfaction.

This usage of the Operator-NAS-Identifier attribute parallels the Operator-Name attribute as defined in Section 4.1 of [RFC5580].

The Operator-NAS-Identifier attribute is defined as follows.

Description

An opaque token describing the NAS a user has logged into.

Type

241.8 (assigned by IANA from the "short extended space" [RFC6929] of the "RADIUS Attribute Types" registry).

Length

4 to 35.

Implementations supporting this attribute MUST be able to handle between one (1) and thirty-two (32) octets of data. Implementations creating an Operator-NAS-Identifier attribute MUST NOT create attributes with more than sixty-four (64) octets of data. A 32-octet string should be more than sufficient for future uses.

Data Type

The data type of this field is "string". See Section 3.5 of [RFC8044] for a definition.

Value

This attribute contains an opaque token that can only be interpreted by the visited network.

This token MUST allow the visited network to direct the packet to the NAS for the user's session. In practice, this requirement means that the visited network has two practical methods for creating the value.

The first method is to create an opaque token per NAS and then to store that information in a database. The database can be configured to allow querying by NAS IP address in order to find the correct Operator-NAS-Identifier. The database can also be configured to allow querying by Operator-NAS-Identifier in order to find the correct NAS IP address.

The second method is to obfuscate the NAS IP address using information known locally by the visited network -- for example, by XORing it with a locally known secret key. The output of that obfuscation operation is data that can be used as the value of Operator-NAS-Identifier. On reception of a CoA packet, the locally known information can be used to unobfuscate the value of Operator-NAS-Identifier, in order to determine the actual NAS IP address.

Note that there is no requirement that the value of Operator-NAS-Identifier be checked for integrity. Modification of the value can only result in the erroneous transaction being rejected.

We note that the Access-Request and Accounting-Request packets often contain the Media Access Control (MAC) address of the NAS. There is therefore no requirement that Operator-NAS-Identifier obfuscate or hide in any way the total number of NASes in a visited network. That information is already public knowledge.

4. Requirements

4.1. Requirements on Home Servers

The Operator-NAS-Identifier attribute MUST be stored by a home server along with any user session identification attributes. When sending a CoA packet for a user session, the home server MUST include verbatim any Operator-NAS-Identifier it has recorded for that session.

A home server MUST NOT send CoA packets for users of other networks. The next few sections describe how other participants in the RADIUS ecosystem can help enforce this requirement.

4.2. Requirements on Visited Networks

A visited network that receives a CoA packet that will be proxied to a NAS MUST perform all of the operations required for proxies; see Section 4.3.2. We specify this requirement because we assume that the visited network has a proxy between the NAS and any external (i.e., third-party) proxy. Situations where a NAS sends packets directly to a third-party RADIUS server are outside the scope of this specification.

The visited network uses the contents of the Operator-NAS-Identifier attribute to determine which NAS will receive the packet.

The visited network MUST remove the Operator-Name and Operator-NAS-Identifier attributes from a given CoA packet prior to sending that packet to the final CoA server (i.e., NAS). This step is necessary due to the limits specified in Section 2.3 of [RFC5176].

The visited network MUST also ensure that the CoA packet sent to the NAS contains one of the following attributes: NAS-IP-Address, NAS-IPv6-Address, or NAS-Identifier. This step is the inverse of the removal suggested above in Section 3.4.

In general, the NAS should only receive attributes that identify or modify a user's session. It is not appropriate to send to a NAS attributes that are used only for inter-proxy signaling.

4.3. Requirements on Proxies

There are a number of requirements on both CoA proxies and RADIUS proxies. For the purpose of this section, we assume that each RADIUS proxy shares a common administration with a corresponding CoA proxy and that the two systems can communicate electronically. There is no requirement that these systems be co-located.

4.3.1. Security Requirements on Proxies

Section 6.1 of [RFC5176] has some security requirements on proxies that handle CoA-Request and Disconnect-Request packets:

> ... a proxy MAY perform a "reverse path forwarding" (RPF) check to verify that a Disconnect-Request or CoA-Request originates from an authorized Dynamic Authorization Client.

We strengthen that requirement by saying that a proxy MUST perform a reverse path forwarding check to verify that a CoA packet originates from an authorized Dynamic Authorization Client. Without this check, a proxy may forward packets from misconfigured or malicious parties and thus contribute to the problem instead of preventing it. Where the check fails, the proxy MUST return a NAK packet that contains an Error-Cause Attribute having value 502 ("Request Not Routable").

Proxies that record user session information SHOULD verify the contents of a received CoA packet against the recorded data for that user session. If the proxy determines that the information in the packet does not match the recorded user session, it SHOULD return a NAK packet that contains an Error-Cause Attribute having value 503 ("Session Context Not Found"). These checks cannot be mandated due to the fact that [RFC5176] offers no advice on which attributes are used to identify a user's session.

Because a RADIUS proxy will see Access-Request and Accounting-Request packets, we recognize that it will have sufficient information to forge CoA packets. The RADIUS proxy will thus have the ability to subsequently disconnect any user who was authenticated through itself.

We suggest that the real-world effect of this security problem is minimal. RADIUS proxies can already return Access-Accept or Access-Reject for Access-Request packets and can change authorization attributes contained in an Access-Accept. Allowing a proxy to change (or disconnect) a user session post-authentication is not substantially different from changing (or refusing to connect) a user session during the initial process of authentication.

The biggest problem is that there are no provisions in RADIUS for "end-to-end" security. That is, the visited network and home network cannot communicate privately in the presence of proxies. This limitation originates from the design of RADIUS for Access-Request and Accounting-Request packets. That limitation is then carried over to CoA-Request and Disconnect-Request packets.

We therefore cannot prevent proxies or home servers from forging CoA packets. We can only create scenarios where that forgery is hard to perform, is likely to be detected, and/or has no effect.

4.3.2. Filtering Requirements on Proxies

Section 2.3 of [RFC5176] makes the following requirement for CoA servers:

> In CoA-Request and Disconnect-Request packets, all attributes MUST be treated as mandatory.

This requirement is too stringent for a CoA proxy. Only the final CoA server (i.e., NAS) can decide which attributes are mandatory and which are not.

Instead, in the case of a CoA proxy, we say that all attributes MUST NOT be treated as mandatory. Proxies implementing this specification MUST perform proxying based on Operator-Name. Other schemes are possible but are not discussed here. Proxies SHOULD forward all packets either "as is" or with minimal changes.

We note that some NAS implementations currently treat signaling attributes as mandatory. For example, some NAS implementations will NAK any CoA packet that contains a Proxy-State attribute. While this behavior is based on a straightforward reading of the above text, it causes problems in practice.

We update Section 2.3 of [RFC5176] as follows: in CoA-Request and Disconnect-Request packets, the NAS MUST NOT treat as mandatory any attribute that is known to not affect the user's session -- for example, the Proxy-State attribute. Proxy-State is an attribute used for proxy-to-proxy signaling. It cannot affect the user's session, and therefore Proxy-State (and similar attributes) MUST be ignored by the NAS.

When Operator-Name and/or Operator-NAS-Identifier are received by a proxy, the proxy MUST pass those attributes through unchanged. This requirement applies to all proxies, including proxies that forward any or all of Access-Request, Accounting-Request, CoA-Request, and Disconnect-Request packets.

All attributes added by a RADIUS proxy when sending packets from the visited network to the home network MUST be removed by the corresponding CoA proxy from packets traversing the reverse path. That is, any editing of attributes that is done on the "forward" path MUST be undone on the "reverse" path.

The result is that a NAS will only ever receive CoA packets that either contain (1) attributes sent by the NAS to its local RADIUS server or (2) attributes that are sent by the home server in order to perform a change of authorization.

Finally, we extend the above requirement not only to Operator-Name and Operator-NAS-Identifier but also to any future attributes that are added for proxy-to-proxy signaling.

5. Functionality

This section describes how the two attributes work together to permit CoA proxying.

5.1. User Login

In this scenario, we follow a roaming user who is attempting to log in to a visited network. The login attempt is done via a NAS in the visited network. That NAS will send an Access-Request packet to the visited RADIUS server. The visited RADIUS server will see that the user is roaming and will add an Operator-Name attribute, with value "1" followed by its own realm name, e.g., "1example.com". The visited RADIUS server MAY also add an Operator-NAS-Identifier attribute. The NAS identification attributes are also edited, as required by Section 3.4, above.

The visited server will then proxy the authentication request to an upstream server. That server may be the home server, or it may be a proxy. In the case of a proxy, the proxy will forward the packet until the packet reaches the home server.

The home server will record the Operator-Name and Operator-NAS-Identifier attributes, along with other information about the user's session, if those attributes are present in a packet.

5.2. CoA Proxying

At some later point in time, the home server determines that (1) a user session should have its authorization changed or (2) the user should be disconnected. The home server looks up the Operator-Name and Operator-NAS-Identifier attributes, along with other user session identifiers as described in [RFC5176]. The home server then looks up the realm from the Operator-Name attribute in the logical AAA routing table, in order to find the next-hop CoA server for that realm (which may be a proxy). The CoA-Request is then sent to that CoA server.

The CoA server receives the request and, if it is a proxy, performs a lookup similar to the lookup done by the home server. The packet is then proxied repeatedly until it reaches the visited network.

If the proxy cannot find a destination for the request or if no Operator-Name attribute exists in the request, the proxy will return a CoA-NAK with Error-Cause 502 ("Request Not Routable").

The visited network will receive the CoA-Request packet and will use the Operator-NAS-Identifier attribute (if available) to determine which local CoA server (i.e., NAS) the packet should be sent to. If there is no Operator-NAS-Identifier attribute, the visited network may use other means to locate the NAS, such as consulting a local database that tracks user sessions.

The Operator-Name and Operator-NAS-Identifier attributes are then removed from the packet; one of NAS-IP-Address, NAS-IPv6-Address, or NAS-Identifier is added to the packet; and the packet is then sent to the CoA server.

If no CoA server can be found, the visited network returns a CoA-NAK with Error-Cause 403 ("NAS Identification Mismatch").

Any response from the CoA server (NAS) is returned to the home network via the normal method of returning responses to requests.

6. Security Considerations

This specification incorporates by reference Section 11 of [RFC6929]. In short, RADIUS has many known issues; those issues are discussed in detail in [RFC6929] and do not need to be repeated here.

This specification adds one new attribute and defines new behavior for RADIUS proxying. As this behavior mirrors existing RADIUS proxying, we do not believe that it introduces any new security issues. We note, however, that RADIUS proxying has many inherent security issues.

6.1. RADIUS Security and Proxies

The requirement that packets be signed with a shared secret means that a CoA packet can only be received from a trusted party or, transitively, received from a third party via a trusted party. This security provision of the base RADIUS protocol makes it impossible for untrusted parties to affect the user’s session.

When RADIUS proxying is performed, all packets are signed on a hop-by-hop basis. Any intermediate proxy can therefore forge packets, replay packets, or modify the contents of any packet. Any system receiving correctly signed packets must accept them at face value and is unable to detect any forgery, replay, or modifications. As a result, the secure operation of such a system depends largely on trust instead of on technical means.

CoA packet proxying has all of the same issues as those noted above. We note that the proxies that see and can modify CoA packets are generally the same proxies that can see or modify Access-Request and Accounting-Request packets. As such, there are few additional security implications in allowing CoA proxying.

The main security implication that remains is that home networks now have the ability to disconnect or change the authorization of users in a visited network. As this capability is only enabled when mutual agreement is in place, and only for those parties who can already control user sessions, there are no new security issues with this specification.

6.2. Security of the Operator-NAS-Identifier Attribute

Nothing in this specification depends on the security of the Operator-NAS-Identifier attribute. The entire process would work exactly the same if the Operator-NAS-Identifier attribute simply contained the NAS IP address that is hosting the user's session. The only real downside in that situation would be that external parties would see some additional private information about the visited network. They would still, however, be unable to leverage that information to do anything malicious.

The main reason to use an opaque token for the Operator-NAS-Identifier attribute is that there is no compelling reason to make the information public. We therefore recommend that the value be simply an opaque token. We also state that there is no requirement for integrity protection or replay detection of this attribute. The rest of the RADIUS protocol ensures that modification or replay of the Operator-NAS-Identifier attribute will either have no effect or have the same effect as if the value had not been modified.

Trusted parties can modify a user's session on the NAS only when they have sufficient information to identify that session. In practice, this limitation means that those parties already have access to the user's session information. In other words, those parties are the proxies who are already forwarding Access-Request and Accounting-Request packets.

Since those parties already have the ability to see and modify all of the information about a user's session, there is no additional security issue with allowing them to see and modify CoA packets.

In short, any security issues with the contents of Operator-NAS-Identifier are largely limited by the security of the underlying RADIUS protocol. This limitation means that it does not matter how the values of Operator-NAS-Identifier are created, stored, or used.

7. IANA Considerations

Per Section 3.4 of this document, IANA has allocated one new RADIUS attribute (the Operator-NAS-Identifier attribute) from the "short extended space" of the "RADIUS Attribute Types" registry as follows:

Value: 241.8
Description: Operator-NAS-Identifier
Data Type: string
Reference: RFC 8559

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC5080] Nelson, D. and A. DeKok, "Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes", RFC 5080, DOI 10.17487/RFC5080, December 2007, <https://www.rfc-editor.org/info/rfc5080>.

[RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, DOI 10.17487/RFC5176, January 2008, <https://www.rfc-editor.org/info/rfc5176>.

[RFC5580] Tschofenig, H., Ed., Adrangi, F., Jones, M., Lior, A., and B. Aboba, "Carrying Location Objects in RADIUS and Diameter", RFC 5580, DOI 10.17487/RFC5580, August 2009, <https://www.rfc-editor.org/info/rfc5580>.

[RFC6929] DeKok, A. and A. Lior, "Remote Authentication Dial In User Service (RADIUS) Protocol Extensions", RFC 6929, DOI 10.17487/RFC6929, April 2013, <https://www.rfc-editor.org/info/rfc6929>.

[RFC7542] DeKok, A., "The Network Access Identifier", RFC 7542, DOI 10.17487/RFC7542, May 2015, <https://www.rfc-editor.org/info/rfc7542>.

[RFC8044] DeKok, A., "Data Types in RADIUS", RFC 8044, DOI 10.17487/RFC8044, January 2017, <https://www.rfc-editor.org/info/rfc8044>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

8.2. Informative References

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, DOI 10.17487/RFC2866, June 2000, <https://www.rfc-editor.org/info/rfc2866>.

Authors' Addresses

Alan DeKok
The FreeRADIUS Server Project

Email: aland@freeradius.org

Jouni Korhonen

Email: jouni.nospam@gmail.com