Guidance on the use of RADIUS attributes on the Internet2 eduroam service

Version: 1.0

Contents

1. Glossary 3
2. Introduction 5
3. Summary of Guidance 6
4. Use of Attributes 7
   - 4.1. Processing of Attributes 7
   - 4.2. Confidentiality and Integrity of Attributes 9
   - 4.3. Additional Considerations 10
5. Attribute Requirements 11
6. Attribute Descriptions 14
   - 6.1. End User and Supplicant Identity 14
     - 6.1.1. User-Name 14
     - 6.1.2. Calling-Station-Id 14
   - 6.2. Service Provider Identity 15
     - 6.2.1. NAS-IP-Address 15
     - 6.2.2. NAS-Identifier 15
     - 6.2.3. Operator-Name 16
     - 6.2.4. Eduroam-SP-Country 16
   - 6.3. RADIUS Session Management 16
     - 6.3.1. Framed-MTU 16
     - 6.3.2. Proxy-State 17
     - 6.3.3. Internet2-Loop-Detection 17
     - 6.3.4. State 17
     - 6.3.5. Configuration-Token 17
     - 6.3.6. Error-Cause 18
   - 6.4. Authentication and Key Distribution 18
     - 6.4.1. EAP-Message 18
     - 6.4.2. Message-Authenticator 18
     - 6.4.3. MS-MPPE-Send-Key 19
     - 6.4.4. MS-MPPE-Recv-Key 19
7. TLRS Attribute Processing 20
   - 7.1. User-Name 20
   - 7.2. Operator-Name 20
   - 7.3. Eduroam-SP-Country 20
   - 7.4. Proxy-State 20
   - 7.5. Internet2-Loop-Detection 20

7.6. EAP-Message 20

1. Glossary

802.1X	An IEEE standard for port-based network access control. It allows an authenticator (such as wireless controller) to authorize access to the network by a supplicant (such as a laptop).
Attribute	RADIUS Attributes carry the specific authentication, authorization, information and configuration details for a RADIUS client's access request and a RADIUS server's reply.
EAP	See Extensible Authentication Protocol.
eduroam	eduroam is an international WiFi internet access roaming service for users in research, higher education and further education. See https://eduroam.org.
Extensible Authentication Protocol	An authentication framework which supports multiple authentication methods over various network media, such as WiFi. It is defined by RFC 3579.
Identity Provider	An eduroam system entity that is responsible for authenticating its affiliated end users. An example of an Identity Provider is a college.
IDP	See Identity Provider.
RADIUS	Acronym meaning Remote Authentication Dial In User Service. RADIUS enables a RADIUS client, such as a NAS, to communicate with RADIUS for the purpose of authorizing a user's access request for a network service. It is defined by RFC 2865.
RADIUS client	A system entity that sends RADIUS messages. An example of a RADIUS client is a wireless controller.
RADIUS proxy	A system entity that can act as an intermediary between a RADIUS client and a RADIUS server. A RADIUS proxy is an entity that is both a RADIUS server (receiving messages from a RADIUS client) and a RADIUS client (forwarding these messages to another RADIUS server). The InCommon eduroam TLRS is an example of a RADIUS proxy.
RADIUS server	A system entity that responds to RADIUS messages. An example of a RADIUS server is FreeRADIUS.
Realm	One of the two components of an NAI (the other component being the username). In eduroam, the realm is used by

	Service Providers to route authentication requests towards the appropriate Identity Providers.
Service Provider	An eduroam system entity that is responsible for providing a network service to end users who have been authenticated by their Identity Provider.
SP	See Service Provider.
Supplicant	A supplicant is an 802.1X entity that seeks to be authenticated by an authenticator that provisions access to the network. Supplicants are usually implemented as software that is part of a device's operating system. The terms supplicant and device are often used interchangeably.
TLRS	See Top Level RADIUS Server.
Top Level RADIUS Server	A RADIUS proxy operated by InCommon for the US eduroam service. These forward requests between eduroam organizations domestically and internationally. InCommon operates a TLRS on the East and West Coasts.
NAI	See Network Access Identifier.
NAS	See Network Access Server.
Network Access Identifier	An identifier that can be used to facilitate the interdomain authentication of an End User. It is used to route authentication requests and sometimes identify the End User that is the subject of authentication. It is defined by RFC 7542.
Network Access Server	A system that provides access to a network service. An wireless access point is an example of a Network Access Server.
Username	One of the two components of an NAI (the other component being the realm). The username may be used to uniquely identify an End User at the Identity Provider associated with the given realm.
Virtual LAN	A technique for segregating devices sharing the same physical network into discrete logical broadcast domains.
VLAN	See Virtual LAN.
WPA-Enterprise	A wireless security specification promulgated by the Wi-Fi Alliance.

2. Introduction

RADIUS attributes are used to carry data within RADIUS messages, such as Access-Requests and Access-Challenges. They enable RADIUS' core function of authentication, but they also have other uses. These include:

- provisioning configuration to a device, such as a network address and routing information
- provisioning configuration to a network access server (NAS), such as encryption keys, and
- geolocation of devices.

Many attributes have been standardised within IETF RFCs. Vendors are also free to define attributes for their own products. These two types of attribute are known as *standard* and *vendor-specific* attributes, respectively.

Attributes are important in eduroam.

- WPA-Enterprise is used to provision users' network access; this uses both standard and vendor-specific attributes for purposes including authentication and key distribution.
- Eduroam encourages the use of other standard attributes to address certain requirements, and it defines its own vendor-specific attributes to address other needs of the service. These requirements and needs are discussed in detail in subsequent sections.

RADIUS attributes are rudimentary structures compared to other constructions that serve a similar purpose in other domains (e.g., SAML attributes for Web Single Sign-On). This makes them simple to understand and use, but it also imposes limitations.

Therefore, while RADIUS is designed to support interdomain (or federated) operation, issues can arise if attributes are not used appropriately. For example:

- some attributes are necessary to provision the eduroam service to an end user;
- others are not necessary but their use confers some benefit;
- others might degrade the performance of the eduroam service; and
- others might expose the end user or an organization to harm.

The use of attributes within eduroam has evolved since its inception, and consequently there can be a lack of clarity about their use. The goal of this document is to provide clear and effective guidance on the appropriate use of attributes within the InCommon eduroam service.

3. Summary of Guidance

This section provides a summary of the guidance provided in this document.

1. Organizations should only send or ingest the attributes set out in Table 1, and avoid the use of others. This will avoid several potential issues described in later sections. These attributes are either “necessary” (i.e., eduroam cannot technically function without these) and “discretionary” (i.e., can assist with some eduroam use-cases). Organizations can enforce this through policy on their NASs, RADIUS proxies and authentication servers (e.g., to prevent a RADIUS authentication server from sending VLAN attributes for users authenticating at an eduroam SP).

End User and Supplicant Identity			**Service Provider Identity**				**RADIUS Session Management**						**Authentication and Key Management**			
Necessary		Disc.	Necessary		Discretionary		Necessary				Discretionary		Necessary			
User-Name	Calling-Station-Id	Chargeable-User-Identity	NAS-IP-Address	NAS-Identifier	Operator-Name	Eduroam-SP-Country	Framed-MTU	Proxy-State	Internet2-Loop-Detection	State	Configuration-Token	Error-Cause	EAP-Message	Message-Authenticator	MS-MPPE-Recv-Key	MS-MPPE-Send-Key

Table 1

2. Organizations should use RADIUS proxies to aggregate traffic and enforce policy on attributes centrally, where possible. This can facilitate operational activities such as configuration and troubleshooting.

3. Organizations may send other attributes, but they should consider any potential consequences (e.g., assigning a visitor to an inappropriate VLAN, if ingesting VLAN identifiers from eduroam). It may be possible to address the use-case using the RADIUS Configuration-Token attribute, which an IDP can use to signal a user profile to an SP.

4. IDPs should use EAP methods that support anonymous EAP identities to avoid user identifiers being transmitted in cleartext in the RADIUS User-Name attribute.

5. IDPs should send the RADIUS Chargeable-User-Identity attribute, particularly if they are using anonymous EAP identities.

6. SPs should use opaque values for their NAS' RADIUS NAS-Identifier attribute that do not describe the geographic location of the NAS.

7. Organizations with geographically dispersed eduroam systems, nationally or internationally, should consider how best to manage and protect attributes as they transit less trusted networks.

8. Organizations are encouraged to use tools such as tcpdump and Wireshark to inspect and validate the attributes that they are sending/ingesting.

4. Use of Attributes

There are many eduroam-compatible products that use RADIUS attributes. It would not be feasible to provide documentation for every product, and therefore this section offers general, product-agnostic guidance on the use of attributes.

In the event of uncertainty relating to this guidance and specific products, organizations are encouraged to contact the InCommon helpdesk for support.

4.1. Processing of Attributes

The processing of attributes includes operations such as

- a RADIUS client (e.g., a wireless controller) inserting an attribute into a RADIUS packet, or
- a RADIUS proxy removing an attribute from a RADIUS packet or modifying its value, or
- a RADIUS server consuming and acting on a RADIUS packet's attributes values.

Products that use RADIUS are typically deployed within a single administrative domain (e.g., a college). In this case, the RADIUS infrastructure is centrally managed and acquired from just one or two vendors. It is not generally necessary to consider the processing of attributes within these environments.

However, eduroam consists of thousands of different domains and scores of vendors. In this environment, it is essential to consider attribute processing to ensure the user experience, interoperability, privacy, and security.

The main considerations relate to the transmission of attributes between eduroam organizations.

- NAS products (e.g., wireless controllers) generally offer little control concerning which attributes are transmitted in their RADIUS Access-Requests packets. An SP RADIUS proxy receiving a RADIUS Access-Request from a local NAS will, by default, forward it externally without modification and so potentially expose sensitive data (e.g., location information).
- Similarly, an SP RADIUS proxy receiving a RADIUS Access-Accept packet transmitted by an external IDP RADIUS server will, by default, forward those messages to local NASs. This can lead to unintended outcomes (e.g., the remote IDP RADIUS server specifying a VLAN for the user that is meant for local NASs but is applied by the SP's NAS).

Therefore, it is recommended that both SPs and IDPs enforce policies that ensure that attributes are processed appropriately.

- SPs should implement an SP RADIUS proxy server (ideally two or more, for redundancy) between their NASs and the Top Level RADIUS Servers (TLRS). This proxy provides a layer of policy enforcement for both ingress and egress.
- If it is not possible to implement an SP RADIUS proxy, SPs should configure their NASs to only use those attributes that are necessary for the provision of the eduroam service.
- Similarly, IDPs should configure their RADIUS servers to only send those attributes that are needed by an SP to provide the eduroam service. These attributes are discussed in sections 5 and 6.
- IDPs that are also SPs can connect their RADIUS authentication server(s) to the same RADIUS proxy(s). This will route all RADIUS packets through a single logical point of policy enforcement, which can assist activities such as the configuration and troubleshooting.

The following diagrams illustrate how this guidance can be implemented within some common deployment scenarios. The NAS is typically a system such as a wireless controller.

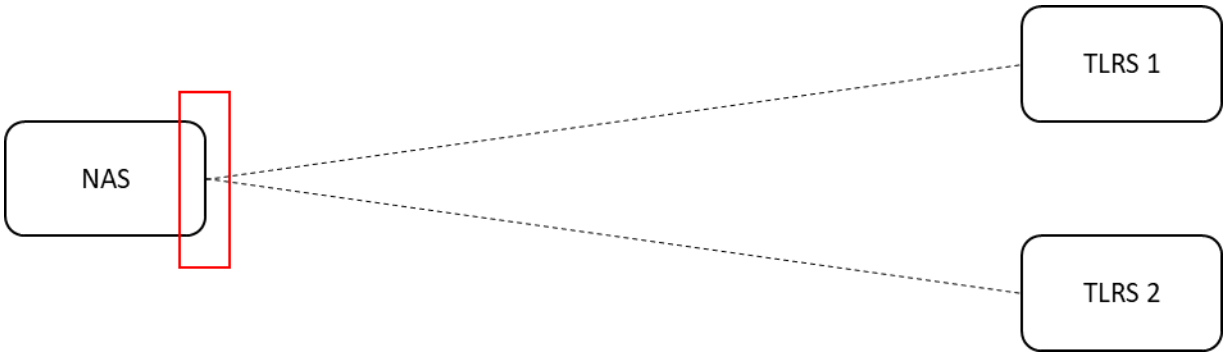

Figure 1

In Figure 1, an SP's single NAS is connected to both TLRS 1 and 2. This is a common scenario for smaller SPs having a single NAS where deployed an SP RADIUS server would increase cost and complexity. The NAS' RADIUS configuration (red) has been configured to process those attributes necessary for eduroam.

As discussed previously, NASs often do not provide the functionality needed to control the processing of RADIUS attributes. In this eventuality, one or more SP RADIUS proxies can be used to enforce policy (red) on RADIUS attributes, both ingress and egress.

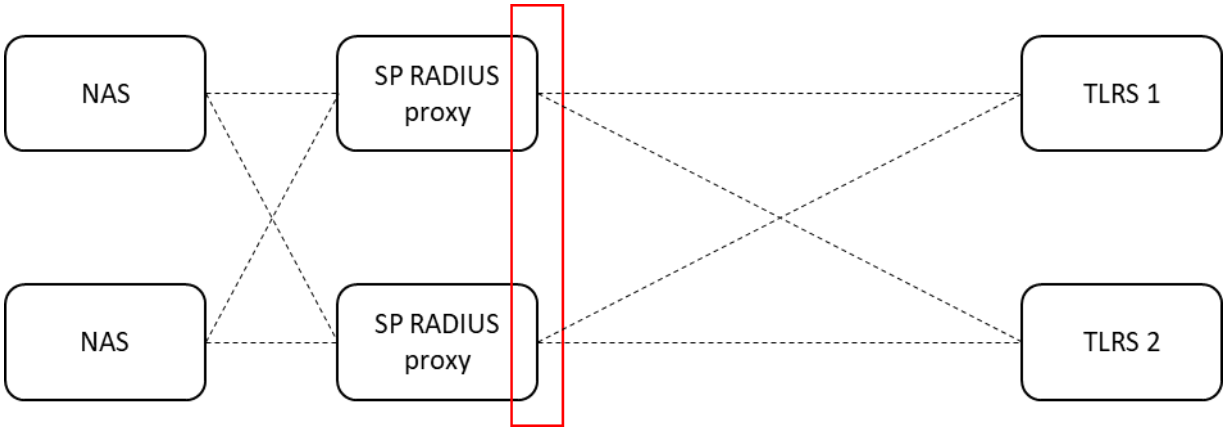

Figure 2

In Figure 2, two NASs have been connected to two SP RADIUS proxies which, in turn, are connected to TLRS 1 and 2. Policy (red) is enforced by the two proxies and so it is not necessary to enforce policy at the NASs. This can make it easier to apply policy for networks with multiple NASs.

To achieve the greatest benefit, the SP RADIUS proxy(ies) should be deployed close to the NAS so that messages can be processed before they transit less trusted networks.

Many eduroam organizations are both SP and IDP. In this case, the RADIUS authentication server can also be connected to the RADIUS proxy(ies). This scenario is shown in Figure 3.

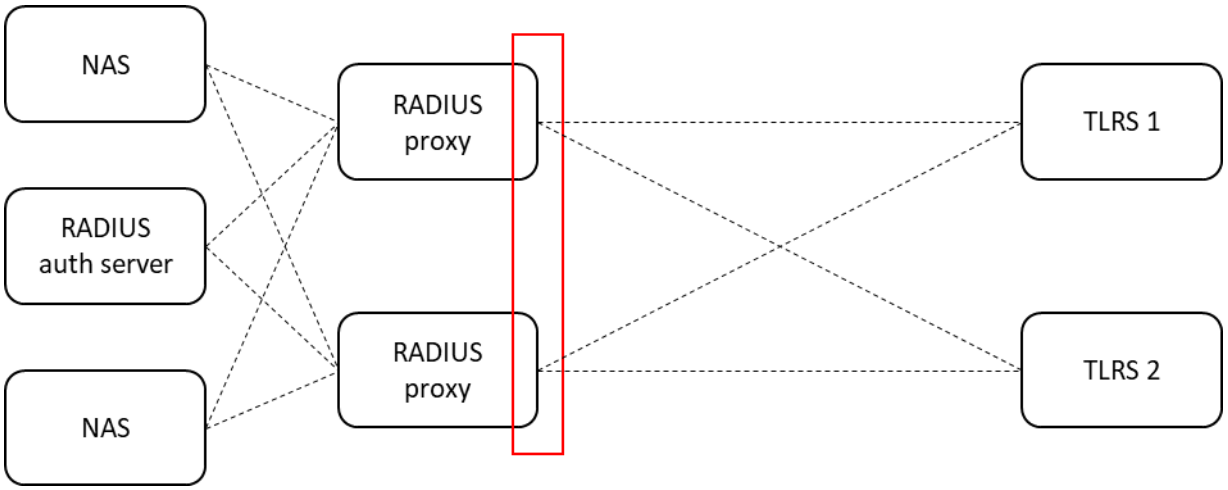

Figure 3

Many other configurations are possible. In Figure 4, the RADIUS authentication and proxy functions have been consolidated.

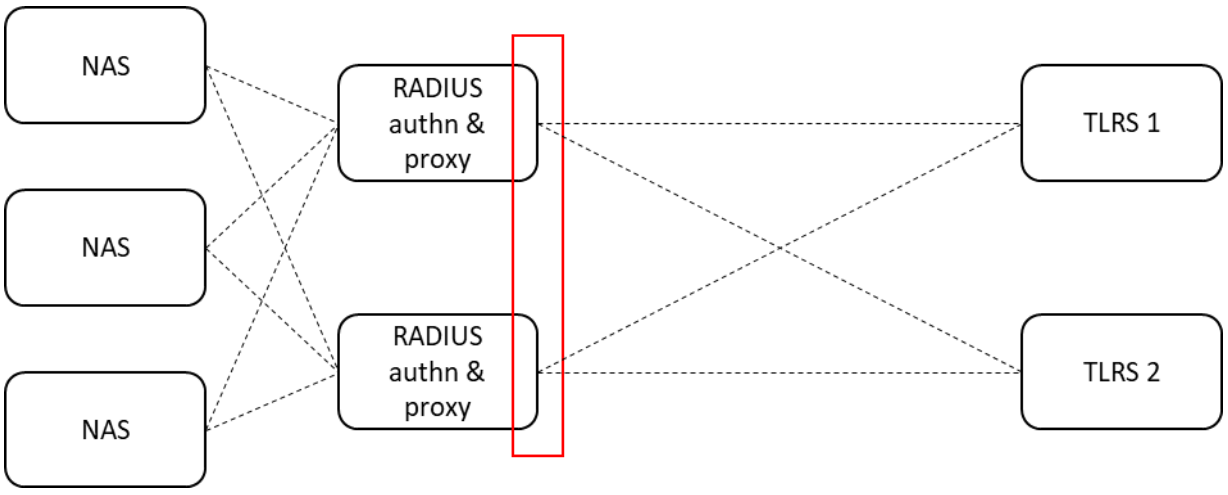

Figure 4

The most appropriate configuration will depend on a number of factors; these include

- whether the organization is an SP, IDP, or both;
- the organization's structure and geographic location of its infrastructure; and
- the RADIUS attribute processing capabilities of its eduroam systems.

These examples are provided as an explanatory tool and are not prescriptive.

4.2. Confidentiality and Integrity of Attributes

Most RADIUS attributes are transmitted in cleartext. Consequently, they can be read by an actor with access to the network between the SP's NAS and the IDP's RADIUS server. Examples of these actors include Internet Service Providers and other National Roaming Operators (NRO) who connect eduroam organizations in their countries.

The integrity of attribute values is assured between adjacent RADIUS clients, proxies, and server. However, a RADIUS proxy between an SP RADIUS client (such as a NAS) and an IDP RADIUS server can modify, insert, and remove attributes without detection. Therefore, this assurance does not extend across one or more RADIUS proxies. Figure 5 illustrates how the integrity of attributes (and RADIUS packets in general) is assured between adjacent RADIUS systems (green) but not across proxies (red).

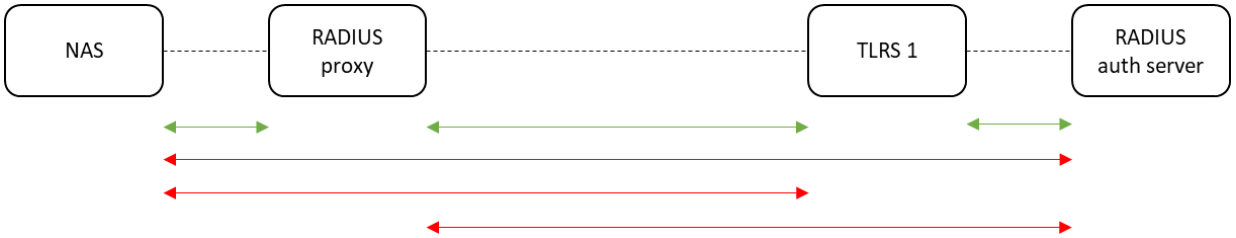

Figure 5

Given these properties, organizations are encouraged to observe the following guidelines.

- Attributes should only be transmitted by SPs and IDPs where they are needed to provision the service. Section 0 identifies these "necessary" attributes and section 6 describes their use.
- There are legitimate use cases that cannot be satisfied by the necessary attributes alone. Sections 5 and 6 also discuss some "discretionary" attributes that can address these use cases.
    - For example, the Configuration-Token attribute can be sent by an IDP to signal to the SP that the user is a student. The SP can use this information to allocate the user to an appropriate VLAN. This avoids the use of VLAN-specific attributes outside of the campus network, which would expose network configuration data.
- In both cases, attribute values should be opaque to avoid leaking information. For example:
    - the User-Name attribute, which is necessary, should take an anonymous value; and
    - the Configuration-Token attribute, given in the previous example, could take a value of "User-Type=3" rather than "User-Type=Student".
- Similarly, attribute values that could yield high-impact outcomes should be avoided. For example, it would probably be unwise to define a value for Configuration-Token that granted access to access to sensitive networks (e.g., a datacenter VLAN).

4.3. Additional Considerations

Organizations are encouraged to consider the following.

- IDPs should pay attention to the differences in processing when its users are connecting locally or remotely. For example, as previously discussed, an IDP may want to provision its own wireless controllers with VLAN attributes for its own users; however, these attributes should not, in most cases, be sent externally.

- In some cases (for example, where two universities are collaborating closely) it may be desirable for an IDP or SP to exchange attributes that are neither “necessary” nor “discretionary” (such as the VLAN attributes). In these instances, it may be better for organizations to connect their RADIUS systems directly rather than via the TLRS.
- If RADIUS messages (and their attributes) are transiting less trusted networks, consider the use of IP Security (IPSec) or a Virtual Private Network (VPN) technology to maintain confidentiality and integrity between endpoints.
- If your organization has premises in other jurisdictions, consider if it would be more appropriate to connect their eduroam systems to a US-based RADIUS proxy, rather than a locally-operated proxy. This will not stop local actors from eavesdropping, but it will prevent unauthorized changes to attribute values.

5. Attribute Requirements

This section describes the attribute requirements for the InCommon eduroam service.

These attributes constitute the minimal set of attributes needed for eduroam to work. Without them, the technology will either not function or be significantly impaired. There is no requirement in policy to use these attributes.

Attributes are categorized as follows.

- **Necessary attributes**. These attributes are needed by one, some, or all RADIUS systems to provision the eduroam service.
- **Discretionary attributes**. These attributes are not necessary to provision the eduroam service but their use can offer benefits. Discretionary attributes are either:
    - **Recommended**: the attribute offers a benefit and so its use is recommend, but it is not necessary for eduroam to work.
    - **Optional**: the attribute offers little or no benefit in general but may offer value in some scenarios.

Figure 1 overleaf summarizes the necessary (“N”) and discretionary (“R” or “O”) attributes on egress and ingress for each system entity and every round-trip in the authentication transaction.

Table 2 sets out the same information in tabular format.

Organizations are encouraged to use packet capture tools such as Wireshark or tcpdump on their RADIUS servers to inspect and validate the attributes within each stage of the authentication. They are also encouraged to contact the InCommon helpdesk if any assistance is required.

Section 6 describes how each of these attributes should be used (e.g., appropriate values, etc).

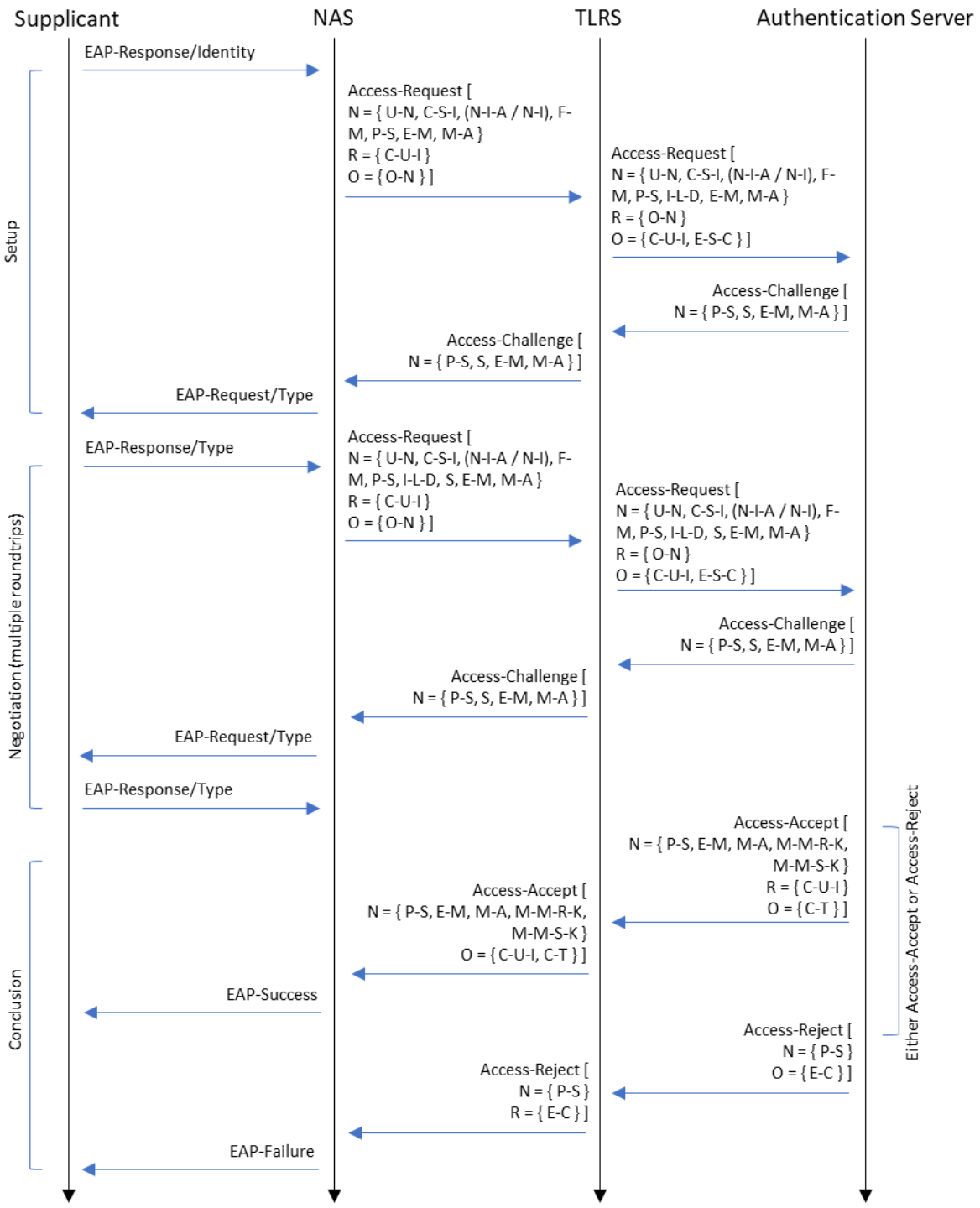
Supplicant
NAS
TLRS
Authentication Server
Setup
Negotiation (multiple roundtrips)
Conclusion
EAP-Response/Identity
Access-Request [N = { U-N, C-S-I, (N-I-A / N-I), F-M, P-S, E-M, M-A } R = { C-U-I } O = { O-N }]
Access-Request [N = { U-N, C-S-I, (N-I-A / N-I), F-M, P-S, I-L-D, E-M, M-A } R = { O-N } O = { C-U-I, E-S-C }]
Access-Challenge [N = { P-S, S, E-M, M-A }]
Access-Challenge [N = { P-S, S, E-M, M-A }]
EAP-Request/Type
EAP-Response/Type
Access-Request [N = { U-N, C-S-I, (N-I-A / N-I), F-M, P-S, I-L-D, S, E-M, M-A } R = { C-U-I } O = { O-N }]
Access-Request [N = { U-N, C-S-I, (N-I-A / N-I), F-M, P-S, I-L-D, S, E-M, M-A } R = { O-N } O = { C-U-I, E-S-C }]
Access-Challenge [N = { P-S, S, E-M, M-A }]
Access-Challenge [N = { P-S, S, E-M, M-A }]
EAP-Request/Type
EAP-Response/Type
Access-Accept [N = { P-S, E-M, M-A, M-M-R-K, M-M-S-K } R = { C-U-I } O = { C-T }]
Access-Accept [N = { P-S, E-M, M-A, M-M-R-K, M-M-S-K } O = { C-U-I, C-T }]
EAP-Success
Access-Reject [N = { P-S } O = { E-C }]
Access-Reject [N = { P-S } R = { E-C }]
EAP-Failure
Either Access-Accept or Access-Reject

Figure 6

	Function	End User and Supplicant Identity			Service Provider Identity			RADIUS Session Management						Authentication and Key Management			
	Status	Necessary		Disc.	Necessary		Discretionary	Necessary				Discretionary		Necessary			
Transaction Phase	Message exchange *A-R = Access-Request* *A-C = Access-Challenge* *A-A = Access-Accept* *A-Rej = Access-Reject*	User-Name	Calling-Station-Id	Chargeable-User-Identity	NAS-IP-Address	NAS-Identifier	Operator-Name	Egress-Domain-SP-Country	Framed-MTU	Proxy-State	Internet2-Loop-Detection	State	Configuration-Token	Error-Cause	EAP-Message	Message-Authenticator	MS-MPPE-Recv-Key	MS-MPPE-Send-Key
Setup	Egress of initial A-R	N	N	R	N (Either)		O		N	N					N	N		
	Ingress of initial A-R	N	N	O	N (Both)		R	O	N	N	N				N	N		
	Egress of initial A-C									N		N			N	N		
	Ingress of initial A-C									N		N			N	N		
Negotiation	Egress of subsequent A-Rs	N	N	R	N (Either)		O		N	N	N	N			N	N		
	Ingress of subsequent A-Rs	N	N	O	N (Both)		R	O	N	N	N	N			N	N		
	Egress of subsequent A-Cs									N		N			N	N		
	Ingress of subsequent A-Cs									N		N			N	N		
Conclusion	Egress of A-A			R						N			O		N	N	N	N
	Ingress of A-A			O						N			O		N	N	N	N
	Egress of A-Rej									N				O				
	Ingress of A-Rej									N				R				

Table 2

N = Necessary
R = Recommended

O = Optional

6. Attribute Descriptions

This section describes the necessary and discretionary attributes for the InCommon eduroam service.

Table 3 below explains how the attributes are described.

Section	Description
Definition	The location(s) of the normative definition of the attribute
RADIUS attribute type	The value of the RADIUS attribute type for this attribute (for vendor-specific attributes, the Vendor-ID and Vendor-Type fields are also provided)
Status	Indicates whether the attribute is necessary or discretionary
Summary	A brief description of the attribute's function
Eduroam usage	A description of how this function works for eduroam specifically
TLRS treatment	A description of how the attribute is treated by the TLRS

Table 3

The TLRS treatment descriptor provides a pointer to the relevant sub-section in section 7. These descriptions are collated in that section to provide a consolidated view of the TLRS' attribute processing.

6.1. End User and Supplicant Identity

This section describes those attributes related to end user and supplicant identity.

6.1.1. User-Name

Definition: RFC 2865 (section 5.1) and RFC 3580 (section 3.1)

RADIUS attribute type: 1

Status: Necessary

Summary: The User-Name attribute is used to route RADIUS Access-Request packets towards an IDP and, for some EAP authentication methods, to identify the user to the IDP for authentication. In the eduroam context, the User-Name attribute takes the value of the EAP-Response/Identity packet that is emitted by the supplicant.

Eduroam usage: IDPs MUST configure their supplicants to emit an EAP-Response/Identity packet taking the value of a NAI. The realm portion of the NAI MUST take a value of a realm (or a subdomain thereof) that the IDP has registered with InCommon. To maintain end user privacy, IDPs SHOULD configure their supplicants to emit an anonymous NAI using an ambiguous fixed username portion (e.g., "anonymous@realm.edu").

TLRS treatment: See section 7.1.

6.1.2. Calling-Station-Id

Definition: RFC 2865 (section 5.31) and RFC 3580 (section 3.21)

RADIUS attribute type: 31

Status: Necessary

Summary: The Calling-Station-Id attribute is used by the SP to identify the MAC address of the supplicant.

Eduroam usage: The MAC address of the supplicant can be used for troubleshooting issues, measuring use of the service, and tracking and preventing abuse of the network. In recent years, most popular platforms have implemented MAC address randomization. There is no standard for randomization and therefore the platforms have adopted different randomization strategies. However, given our current understanding, it is reasonable to assume that most supplicants will provide a random but persistent MAC address. This MAC address will be the same at different SPs. Therefore, IDPs should consider that Service Providers can still collude to track their end users, despite the randomization.

6.2. Service Provider Identity

This section describes those attributes related to Service Provider identity.

6.2.1. NAS-IP-Address

Definition: RFC 2865 (section 5.4) and RFC 3580 (section 3.3)

RADIUS attribute type: 31

Status: Necessary

Summary: The NAS-IP-Address attribute is used by the SP to identify the IP address of the NAS. Either this attribute or the NAS-Identifier attribute MUST be present in a RADIUS Access-Request packet. The NAS-Identifier attribute is preferred.

Eduroam usage: This attribute is not treated specially in eduroam.

TLRS treatment: None.

6.2.2. NAS-Identifier

Definition: RFC 2865 (section 5.32) and RFC 3580 (section 3.21)

RADIUS attribute type: 31

Status: Necessary

Summary: The NAS-Identifier attribute is used by the SP to identify the NAS using a text string. Either this attribute or the NAS-Identifier attribute MUST be present in a RADIUS Access-Request packet. The NAS-Identifier attribute is preferred.

Eduroam usage: SPs sometimes use NAS-Identifier values that describe the NAS' location (e.g., "wlc-library"). This can reduce end user privacy by revealing their

approximate location. Therefore, where possible, SPs SHOULD use opaque NAS-Identifier values (e.g., “wlc-1234”).

TLRS treatment: None.

6.2.3. Operator-Name

Definition: RFC 5580 (section 4.1)

RADIUS attribute type: 126

Status: Discretionary

Summary: This attribute carries the SP’s operator name. The operator name is combined with the namespace identifier to uniquely identify the owner of an access network.

Eduroam usage: The Operator-Name attribute can be used by an IDP to generate a value for the Chargeable-User-Identity attribute. The attribute can be inserted into RADIUS Access-Request by either by SP or NRO.

TLRS treatment: See section 7.2.

6.2.4. Eduroam-SP-Country

Definition: https://wiki.geant.org/display/URN/OID+Repository#OIDRepository-.3-eduroam

RADIUS attribute type: 26 (Vendor-ID of 25178 and Vendor-Type of 10)

Status: Discretionary

Summary: This attribute carries the code for the Service Provider’s country. The TLRS inserts this attribute into all RADIUS Access-Request packets sent by SPs. SPs MAY send this attribute but the value will be replaced by the TLRS.

Eduroam usage: This attribute is defined by GÉANT for the European eduroam service. It has been adopted by InCommon for the US eduroam service.

TLRS treatment: See section 6.3.

6.3. RADIUS Session Management

This section describes those attributes related to RADIUS session management.

6.3.1. Framed-MTU

Definition: RFC 2865 (section 5.12) and RFC 3580 (section 3.10)

RADIUS attribute type: 12

Status: Necessary

Summary:	The Framed-MTU attribute is used by the SP to indicate the maximum length of the EAP packets that the IDP should use to avoid its RADIUS packets exceeding the MTU on an intermediate link.
Eduroam usage:	The IDP MAY choose to override the Framed-MTU attribute's value and use a locally-configured value. This can help to avoid MTU-related issues with some EAP methods.
TLRS treatment:	None.

6.3.2. Proxy-State

Definition:	RFC 2865 (section 5.33)
RADIUS attribute type:	33
Status:	Necessary
Summary:	The Proxy-State attribute can be used by a proxy to match a RADIUS Access-Request packet that it forwards towards a RADIUS authentication server with the corresponding RADIUS Access-Challenge packet. In the case of a chain of RADIUS proxies, which is typical in eduroam, each server adds their own instance of the attribute.
Eduroam usage:	This attribute is not treated specially in eduroam.
TLRS treatment:	See section 7.4.

6.3.3. Internet2-Loop-Detection

Definition:	Proprietary
RADIUS attribute type:	26 (Vendor-ID of 5923 and Vendor-Type of 1)
Status:	Necessary
Summary:	The Internet2-Loop-Detection attribute is added by the TLRS to RADIUS Access-Request packets that they receive from SPs. The TLRS also inspects incoming packets for the attribute which, if identified, indicates that a loop is forming between the TLRS and the SP.
Eduroam usage:	This attribute is defined by InCommon for the US eduroam service. It is not known to be used elsewhere.
TLRS treatment:	See section 7.5.

6.3.4. State

Definition:	RFC 2865 (section 5.24)
RADIUS attribute type:	24
Status:	Necessary

Summary:	The State attribute can be used by a RADIUS server to match a RADIUS Access-Challenge packet with a NAS' RADIUS Access-Request packet. It is often used by RADIUS servers to track concurrent EAP sessions.
Eduroam usage:	This attribute is not treated specially in eduroam.
TLRS treatment:	None.

6.3.5. Configuration-Token

Definition:	RFC 2869 (section 5.12)
RADIUS attribute type:	78
Status:	Discretionary
Summary:	The Configuration-Token attribute can be sent by a RADIUS server to a RADIUS proxy to indicate a type of user profile to be used.
Eduroam usage:	It is recommended that this attribute be used to support scenarios where the SP needs to provision user access on the basis of their profile (e.g., the type of user). For example, an IDP and SP could agree to use a certain value of this attribute so that a "student" profile is applied by the SP, provisioning access to a certain local VLAN. The codification of the range of allowed usage of this value is outside the scope of this document.
TLRS treatment:	None.

6.3.6. Error-Cause

Definition:	RFC 5176 (section 3.5) and draft-ietf-radext-radiusv11 (section 6.4)
RADIUS attribute type:	101
Status:	Discretionary
Summary:	The Error-Cause attribute can be used by a RADIUS server to provide more detail on the cause of a failed authentication.
Eduroam usage:	This attribute is not treated specially in eduroam.
TLRS treatment:	None

6.4. Authentication and Key Distribution

This section describes those attributes related to authentication and key distribution.

6.4.1. EAP-Message

Definition:	RFC 3579 (section 3.1) and RFC 3580 (section 3.27)
RADIUS attribute type:	79
Status:	Necessary

Summary:	The EAP-Message attribute encapsulates EAP packets between the NAS and a RADIUS authentication server. A single RADIUS packet can include one or more instances of the attribute if the EAP packet is too large to fit within a single attribute instance. The NAS and the RADIUS authentication server are responsible for fragmenting and defragmenting EAP packets.
Eduroam usage:	This attribute is not treated specially in eduroam.
TLRS treatment:	See section 7.6.

6.4.2. Message-Authenticator

Definition:	RFC 3579 (section 3.2) and RFC 3580 (section 3.28)
RADIUS attribute type:	80
Status:	Necessary
Summary:	The Message-Authenticator attribute is used to authenticate and integrity-protect RADIUS packets carrying the EAP-Message attribute. It ensures that the EAP-Message attribute(s) have been sent by a trusted RADIUS client or server and have not been tampered with.
Eduroam usage:	This attribute is not treated specially in eduroam.
TLRS treatment:	None

6.4.3. MS-MPPE-Send-Key

Definition:	RFC 2548 (section 2.4.2) and RFC 3580 (sections 3.16 and 4)
RADIUS attribute type:	26 (Vendor-ID of 311 and Vendor-Type of 16)
Status:	Necessary
Summary:	The MS-MPPE-Send-Key attribute is generated by the IDP RADIUS authentication server and sent to the NAS as part of EAP key management.
Eduroam usage:	This attribute is not treated specially in eduroam.
TLRS treatment:	None

6.4.4. MS-MPPE-Recv-Key

Definition:	RFC 2548 (section 2.4.2) and RFC 3580 (sections 3.16 and 4)
RADIUS attribute type:	26 (Vendor-ID of 311 and Vendor-Type of 17)
Status:	Necessary
Summary:	The MS-MPPE-Recv-Key attribute is generated by the IDP RADIUS authentication server and sent to the NAS as part of EAP key management.
Eduroam usage:	This attribute is not treated specially in eduroam.
TLRS treatment:	None

7. TLRS Attribute Processing

This section describes special processing that the TLRS reserves for some attributes.

In general, the TLRS aims for transparency by avoiding modification or disruption of RADIUS message exchanges between SPs and IDPs.

7.1. User-Name

The TLRS inspects Access-Requests for common defects (e.g., a missing realm) and, if one is found, returns a RADIUS Access-Reject packet to the SP.

7.2. Operator-Name

The TLRS inserts the Operator-Name attribute into all RADIUS Access-Request packets originating from an SP connected directly to the TLRS with a value of the associated SP's registered realm name. An SP MAY send this attribute but the value will be replaced by the TLRS.

7.3. Eduroam-SP-Country

The TLRS inserts the Eduroam-SP-Country attribute into all RADIUS Access-Request packets with a value of "US".

7.4. Proxy-State

The TLRS returns a RADIUS Access-Reject packet if a RADIUS Access-Request packet contains 10 or more instances of the Proxy-State attribute. This prevents loops from exceeding 10 hops.

7.5. Internet2-Loop-Detection

The TLRS inserts the Internet2-Loop-Detection attribute into every packets that it sends. It returns a RADIUS Access-Reject packet if an incoming RADIUS Access-Request packet contains this attribute because its presence indicates a loop. This attribute prevents loops from exceeding 1 iteration.

7.6. EAP-Message

The TLRS inspects the EAP-Message packet format and contents for validity and returns a RADIUS Access-Reject packet if invalid.