RADIUS User Guide

Dialogic® BorderNet™ Session Border Controller (SBC)

Release 3.8.1

June 2019

Table of Contents

Copyright and Legal Notice

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation and its affiliates or subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations.

Please see **http://www.dialogic.com/company/terms-of-use.aspx** for more details.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Corporation at the address indicated below or on the web at www.dialogic.com.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 6700 Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements**.

Dialogic, Dialogic Pro, Dialogic Blue, Veraz, Brooktrout, Diva, BorderNet, PowerMedia, PowerVille, PowerNova, MSaaS, ControlSwitch, I-Gate, Mobile Experience Matters, Network Fuel, Video is the New Voice, Making Innovation Thrive, Diastar, Cantata, TruFax, SwitchKit, Eiconcard, NMS Communications, SIPcontrol, Exnet, EXS, Vision, inCloud9, NaturalAccess and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Corporation and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 6700 Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Revision History

Revision	Release Date	Notes
1.0	June 2019	Initial version of document

1. Introduction

1.1 Purpose of this Document

This document describes the **RADIUS** feature in the **BorderNet Session Border Controller (SBC) v3.8.1.**

1.2 Contact Us

For a list of Dialogic locations and offices, please visit: **https://www.dialogic.com/contact.aspx**.

2. User Authentication

With regard to user authentication, there are many options for a user to login to a system.

The BorderNet/EMS will eventually support the following common ones:

- **LDAP** - Accessing a user database such as an Active Directory, which stores users' details and roles.
- **RADIUS** - a protocol for AAA used to access a RADIUS server that holds users' details and services. RADIUS was originally designed to deliver AAA services for dial-up internet.
- **Local storage** of users' passwords and privileges in the system without the need to query an external server.

3. About RADIUS User Authentication

Remote Authentication Dial-In User Service (RADIUS), was originally designed to deliver **Authorization, Authentication, Accounting (AAA)** services for dial-up internet. As such, most of its parameters are network access oriented and are aimed to supply different networking properties for the user accessing the network services. Typical parameters include service type, protocol type, IP address to assign the user (static or dynamic), access list to apply, or a static route to install in the NAS routing table.

A **Network Access Server (NAS)** operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned.

The RADIUS server response includes a list of attribute-value pairs that describe the parameters to be used for a session.

As part of its authentication capabilities, the RADIUS protocol is widely used for user authentication which is not necessarily related to network access. On top of the regular PAP/CHAP password authentication, it can also support a variety of other user authentication protocols like EAP-TTLS, EAP-TLS and PEAP.

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and the RADIUS server, to eliminate the possibility that someone snooping on an unsecure network could determine a user's password.

RADIUS uses UDP as the transport layer, and therefore it implements reliability options on the application (RADIUS) level. If no response is returned within a predetermined length of time, the request is re-sent a number of times. The client can also forward requests to an alternate server or servers in the event that the primary server is down or unreachable.

RADIUS message types include the following:

- **Access-Request** - This is the first message sent from the client to the server, asking permission to access the network. It contains user and network information for authentication and authorization. An Access-Request can include multiple attributes, each containing some information regarding the requested service.
- **Access-Accept** - Sent from the server to the client, granting permission to access the network. An Access-Accept message can provide specific configuration information for the client, such as IP address, QoS profile, user authorization or any other attribute needed.
- **Access-Reject** - Sent from the server to the client, denying permission to access the network. Can include reject cause and a message to the user.
- **Access-Challenge** - Sent by the server to issue a challenge to which the user must respond. The client then re-submits its original Access-Request with the extra information required by the Access-Challenge.

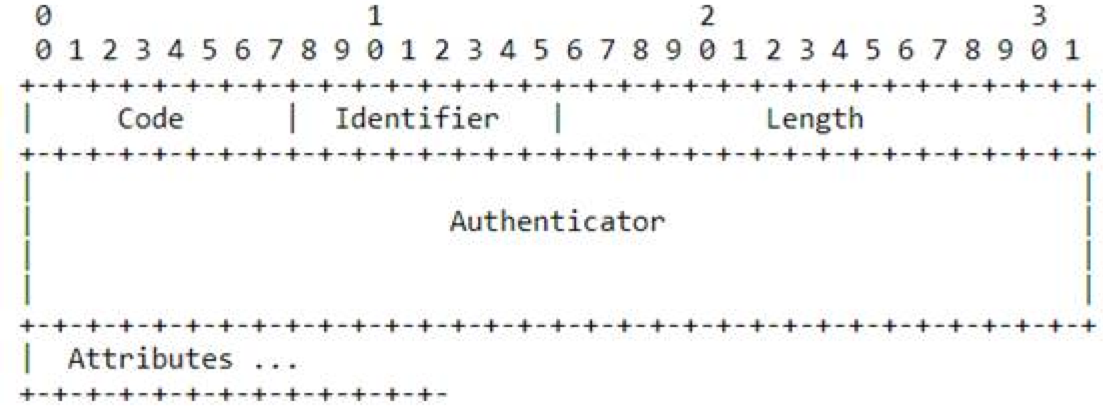
3.1 RADIUS Packet Format

RADIUS packet format consists of the following elements:

- **Code** - identifies the type of RADIUS packet (Access-Request, Access-Accept, Accounting-Request etc.)
- **Identifier** - helps in matching requests and replies (a response has the same Identifier as its request), and detecting duplicate requests (the Identifier must be changed for each new request). On receipt of a response to an Access-Request, the Identifier

field is matched with the pending Access-Request.

- **Authenticator** - used to authenticate the reply from the RADIUS server, and in encrypting user passwords. When it is used in an Access-Request, it is called a Request Authenticator. When it is used in any kind of response, it is called a Response Authenticator.
- **Attributes** - carry the specific authentication, authorization, information and configuration details for the request and reply. Attributes are formatted as **Type-Length-Value (TLV)**
- The following diagram illustrates the RADIUS packet format.



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

3.2 Attributes for Different Scenarios

There are many different attributes (TLVs) specified for different scenarios and options. The following are some attributes which are relevant to the BorderNet/EMS user authentication.

- **User name** (type 1) - name of the user to be authenticated.
- **User password** (type 2) - hidden password of the user to be authenticated. Used when PAP is applied, so the password is not sent on the clear. It is only used in Access-Request packets. The password protection process is as follows:
  - The password is first padded at the end with nulls to a multiple of 16 octets.
  - A one-way MD5 hash is calculated over a stream of octets consisting of the shared secret followed by the Request Authenticator.
  - The hashed value is XORed with the first 16 octet segment of the password.
  - The final result is placed in the first 16 octets of the String field of the user password attribute.
- **CHAP password** (type 3) - Challenge-Handshake Authentication Protocol (CHAP) is only used in Access-Request packets. For CHAP, the Network Access Server (NAS) generates a random challenge (preferably 16 octets) and sends it to the user, who returns a CHAP response along with a CHAP ID and CHAP username. The NAS then sends an Access-Request packet to the RADIUS server with the CHAP username as the user name and with the CHAP ID and CHAP response as the CHAP password.
- The CHAP challenge value is found in the CHAP-Challenge Attribute (60) if present in the packet, otherwise in the Request Authenticator field (The request Authenticator is used as the challenge instead).
- **NAS IP address** (type 3) - IP Address of the NAS which is requesting authentication of the user. The NAS can be any element requesting authentication, and not specifically only a network access server.
- **NAS identifier** (type 32) - a string identifying the NAS originating the Access-Request. It is only used in Access-Request packets. Can be an FQDN or any other application specific value.
- **Class** (type 25) - is by the server to the client in an Access-Accept response. It provides the ability to map a user to different authorization groups, such as 'Administrator' / 'ReadOnly' etc. The field is generic and can contain any value which is coordinated by the client and server.

- **CHAP challenge** (type 60) - contains the CHAP Challenge sent by the NAS to a CHAP user. It is only used in Access-Request packets. If the CHAP challenge value is 16 octets long it MAY be placed in the Request Authenticator field instead of using this attribute. The CHAP challenge value, if present in the packet, is otherwise in the Request Authenticator field which is used as the challenge instead.
- **Reply message** (type 18) - indicates a text which may be displayed to the user. When used in an Access-Accept, it is the success message. When used in an Access-Reject, it is the failure message.
- **Mandatory** - the following mandatories are relevant:
  - An Access-Request MUST contain either a user password or a CHAP password or State. An Access-Request MUST NOT contain both a user password and a CHAP password.
  - An Access-Request MUST contain either a NAS IP address or a NAS identifier (or both).
  - An Access-Accept does not have any mandatory attributes it must include. With regular user authentication and authorization as will be applied with the BorderNet, a Class attribute will be included.

3.3 PAP and CHAP

PAP - Password Authentication Protocol

PAP was originally defined for PPP (Point-to-Point Protocol) connections and used a username and password which were sent as clear text over the PPP connection. For that reason, it is unsafe to use it over links which can be eavesdropped.

When used with RADIUS, the username is sent as clear text, however the password is sent hidden in the user password attribute. The protection process relies on the MD5 algorithm, which has been proven to be insecure.

CHAP - Challenge-Handshake Authentication Protocol

With CHAP, the password is not sent from the client to the server. It uses a 3-way handshake in order to authenticate the user.

- The authenticator sends a 'challenge' message to the peer.
- The peer responds with a value calculated using a 'one-way hash' function, using a pre-shared secret and the received challenge.
- The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is successful.

When used with RADIUS, the NAS generates a random challenge (preferably 16 octets) and sends it to the user, who returns a CHAP response along with a CHAP ID and CHAP username. The NAS then sends an Access-Request packet to the RADIUS server with the CHAP username as the username and with the CHAP ID and CHAP response as the CHAP password. The random challenge can either be included in the CHAP challenge attribute or, if it is 16 octets long, it can be placed in the Request Authenticator field of the Access-Request packet.

With the BorderNet, there is no PPP connection and the user should not be aware of the CHAP process. The BorderNet should generate both the challenge and CHAP-ID, and then compute the hashed value to be sent to the RADIUS server.

3.4 Implementation of RADIUS in BorderNet

The following overview is relevant for the implementation of RADIUS authentication in the BorderNet.

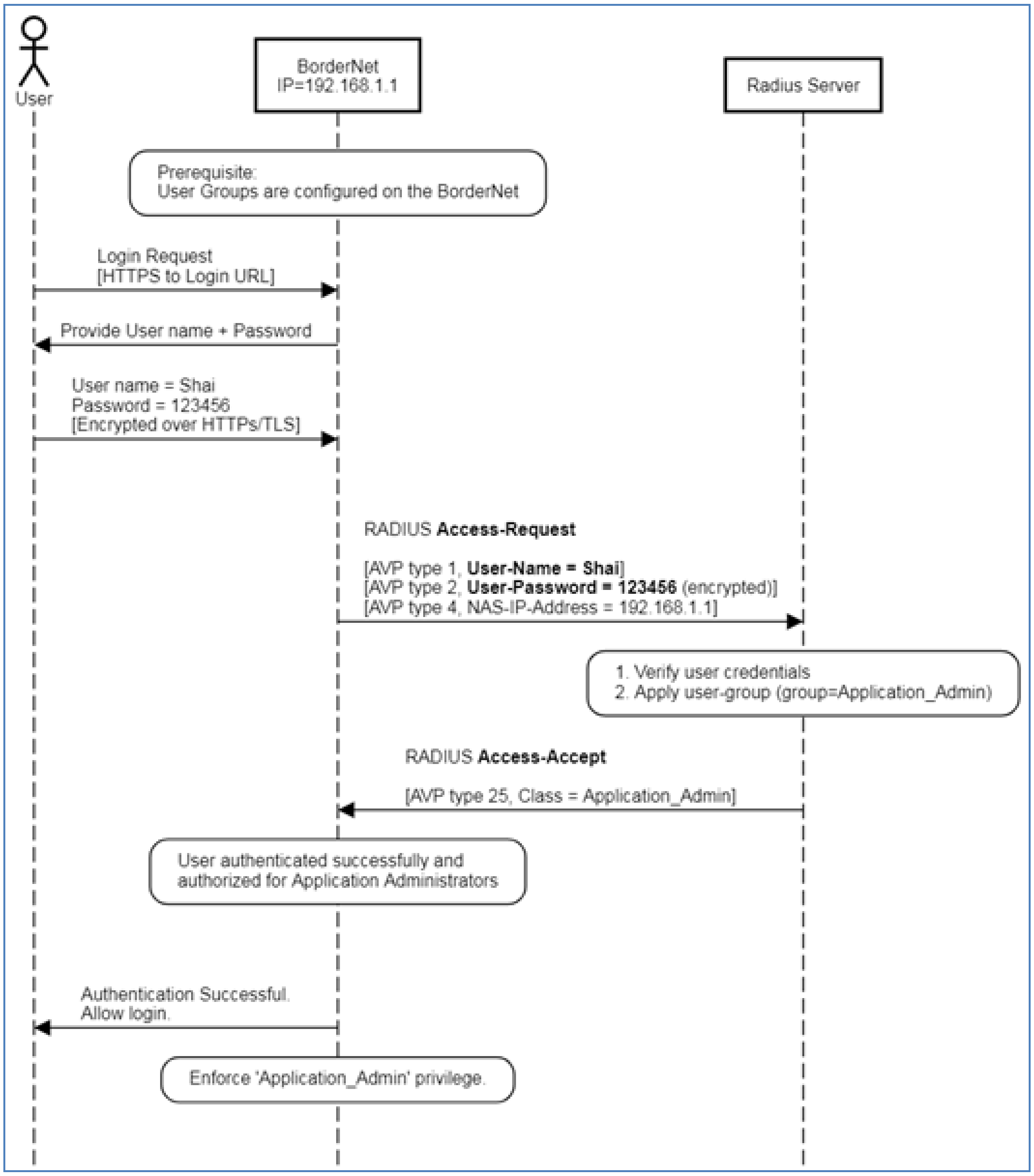
- RADIUS is used for user authentication and authorization.
  - Accounting is not supported.
  - Authentication - by username and password.
  - Authorization - by obtaining a privilege (user-groups) from the RADIUS server, to be applied for the authenticated user.
- The user password supports the regular user password (Type=2) attribute (PAP), or CHAP. Using different EAP options is not in scope.
- Redundant RADIUS servers use the same shared secret and the same UDP port. Switching between the primary and alternate RADIUS servers does not require rebuilding the message with a new shared secret.
- The destination UDP port used for the RADIUS connection is not configurable, due to some complications required in the code. Instead, it is fixed with a value of 1812 (formal RADIUS port). It can be re-evaluated once a customer request is received.

4. BorderNet RADIUS Authentication Scenarios

Following are some regular scenarios for user authentication in BorderNet with RADIUS.

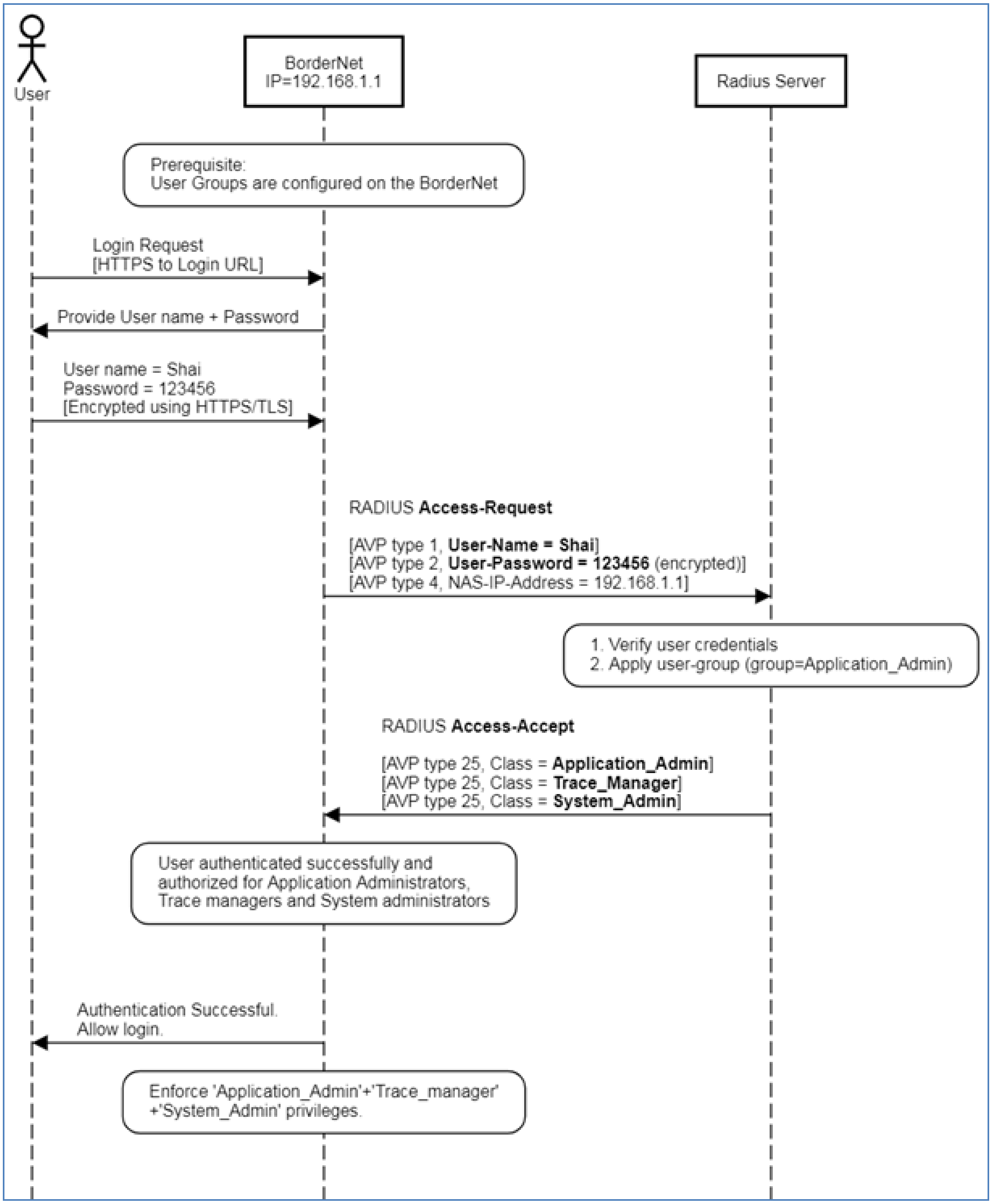
4.1 Successful Login

On successful authentication, the BorderNet sends the username and password to the RADIUS server via an Access-Request message, and receives an Access-Accept message confirming the username and password. The Access-Accept message contains one or more Class attributes which determine the user group this user is assigned to.


User
BorderNet
IP=192.168.1.1
Radius Server
Prerequisite:
User Groups are configured on the BorderNet
Login Request
[HTTPS to Login URL]
Provide User name + Password
User name = Shai
Password = 123456
[Encrypted over HTTPs/TLS]
RADIUS **Access-Request**
[AVP type 1, **User-Name = Shai**]
[AVP type 2, **User-Password = 123456** (encrypted)]
[AVP type 4, NAS-IP-Address = 192.168.1.1]
1. Verify user credentials
2. Apply user-group (group=Application_Admin)
RADIUS **Access-Accept**
[AVP type 25, Class = Application_Admin]
User authenticated successfully and
authorized for Application Administrators
Authentication Successful.
Allow login.
Enforce 'Application_Admin' privilege.

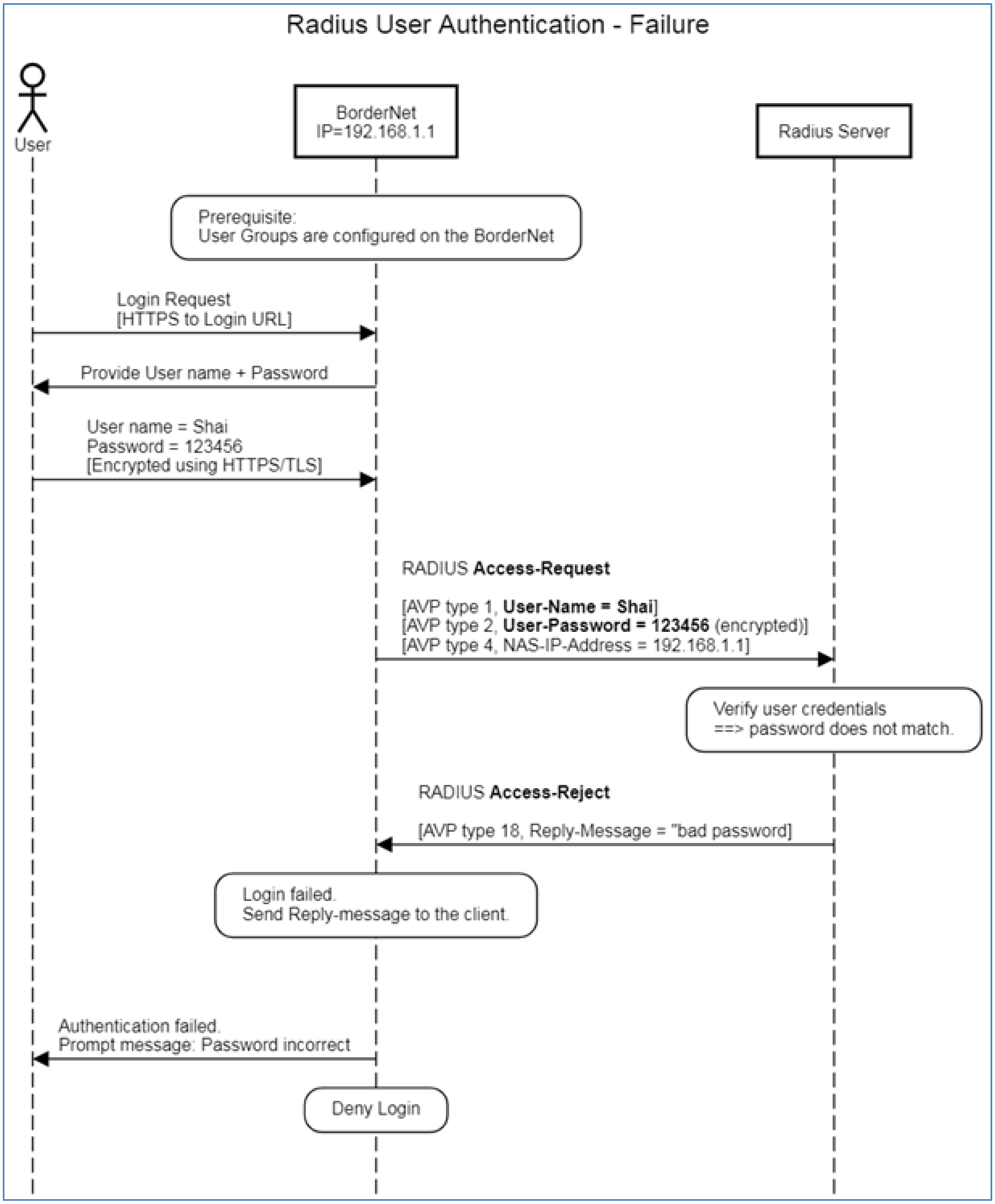
4.2 Multiple User Groups - Successful Login

The below diagram shows a successful login with an Access-Accept which contains several Class attributes. Each Class attribute contains a different user-group which is assigned to the user, and by applying all user-groups the proper user privilege is deployed.


User
BorderNet
IP=192.168.1.1
Radius Server
Prerequisite:
User Groups are configured on the BorderNet
Login Request
[HTTPS to Login URL]
Provide User name + Password
User name = Shai
Password = 123456
[Encrypted using HTTPS/TLS]
RADIUS **Access-Request**
[AVP type 1, **User-Name = Shai**]
[AVP type 2, **User-Password = 123456** (encrypted)]
[AVP type 4, NAS-IP-Address = 192.168.1.1]
1. Verify user credentials
2. Apply user-group (group=Application_Admin)
RADIUS **Access-Accept**
[AVP type 25, Class = **Application_Admin**]
[AVP type 25, Class = **Trace_Manager**]
[AVP type 25, Class = **System_Admin**]
User authenticated successfully and
authorized for Application Administrators,
Trace managers and System administrators
Authentication Successful.
Allow login.
Enforce 'Application_Admin'+'Trace_manager'
+'System_Admin' privileges.

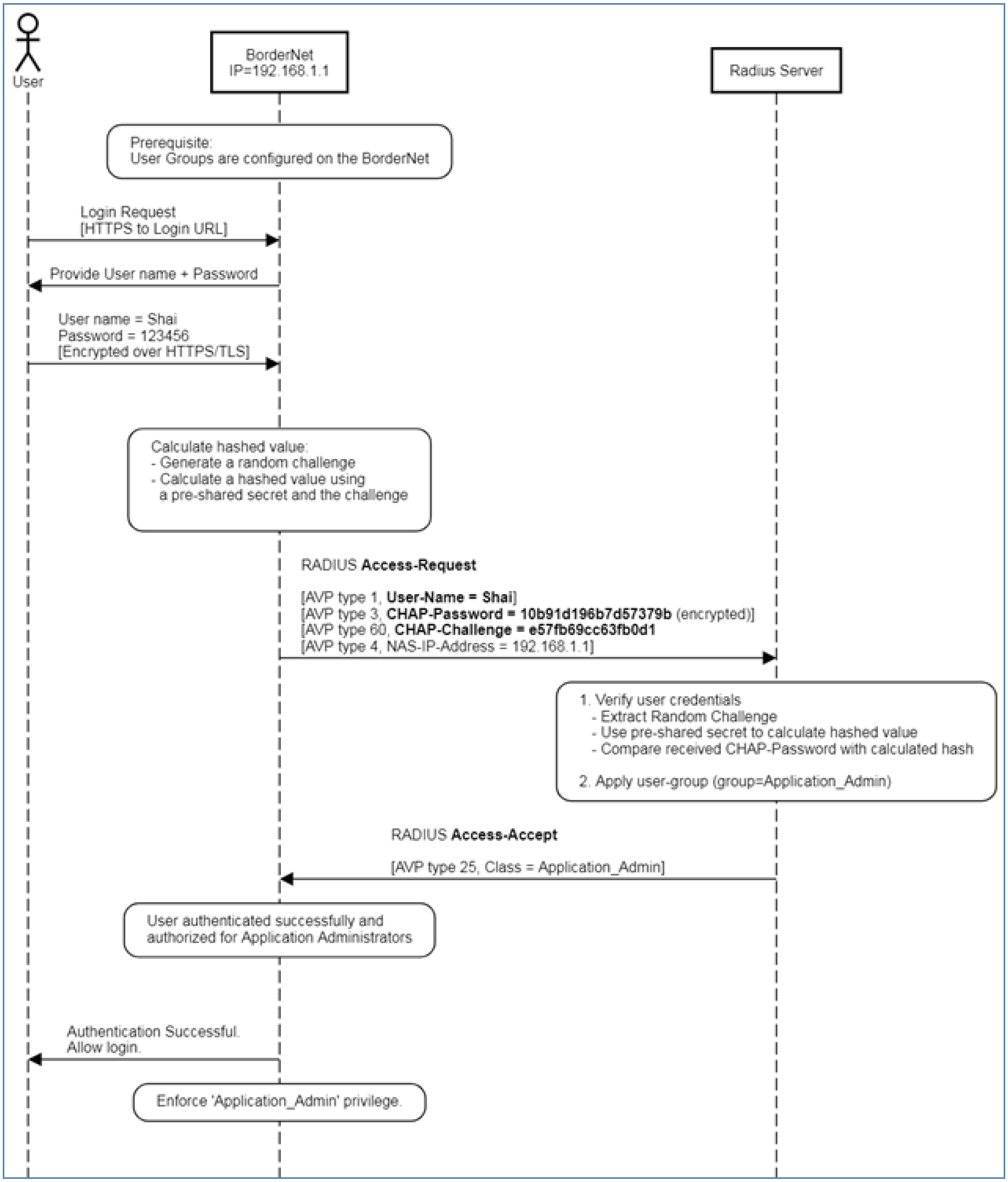
4.3 Failed Login

On a failed authentication, the BorderNet sends the username and password to the RADIUS server via an Access-Request message, and receives an Access-Reject message declining the username and password.


Radius User Authentication - Failure
User
BorderNet
IP=192.168.1.1
Radius Server
Prerequisite:
User Groups are configured on the BorderNet
Login Request
[HTTPS to Login URL]
Provide User name + Password
User name = Shai
Password = 123456
[Encrypted using HTTPS/TLS]
RADIUS Access-Request
[AVP type 1, User-Name = Shai]
[AVP type 2, User-Password = 123456 (encrypted)]
[AVP type 4, NAS-IP-Address = 192.168.1.1]
Verify user credentials
==> password does not match.
RADIUS Access-Reject
[AVP type 18, Reply-Message = "bad password]
Login failed.
Send Reply-message to the client.
Authentication failed.
Prompt message: Password incorrect
Deny Login

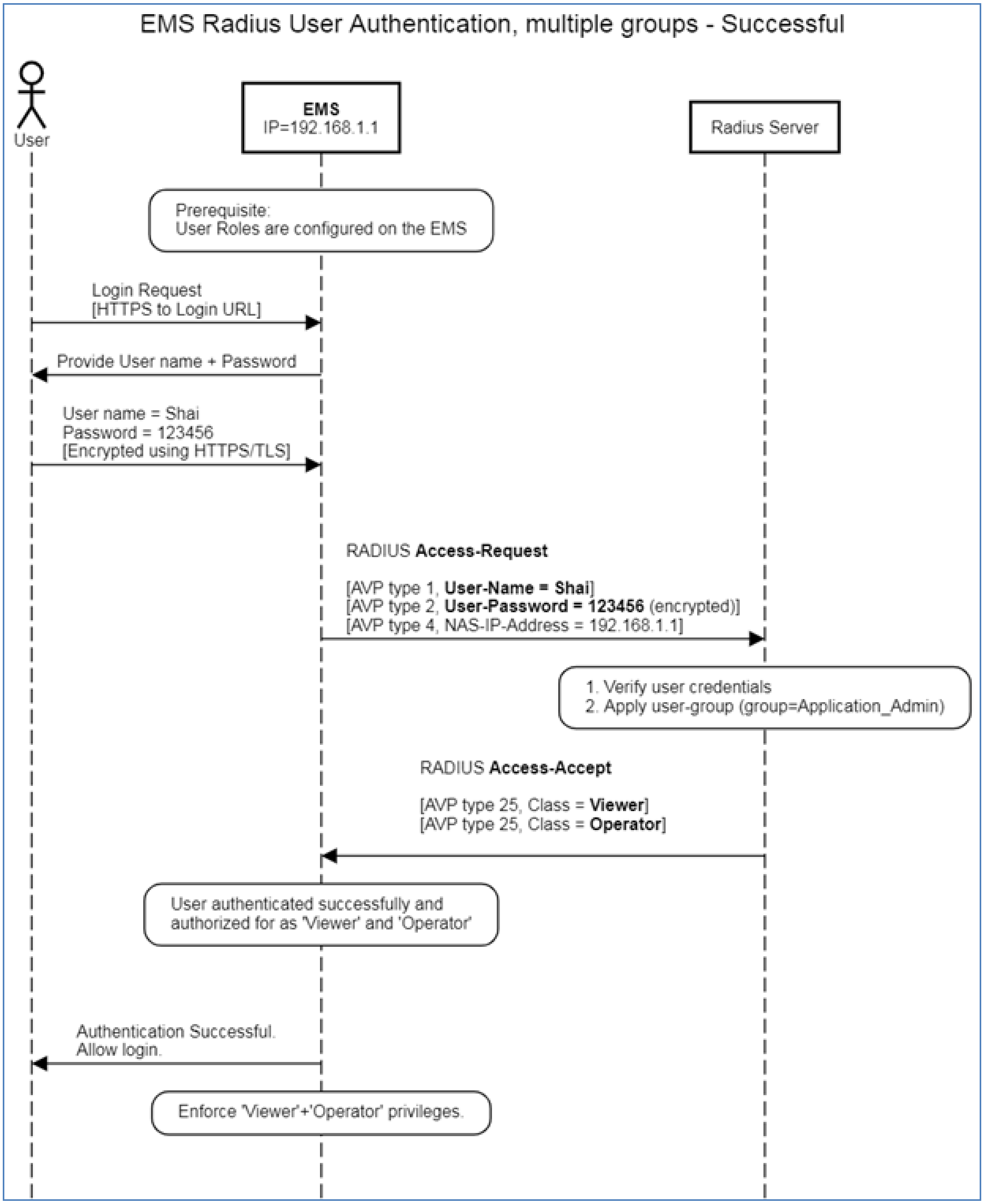
4.4 CHAP Authentication

On CHAP authentication the BorderNet uses the CHAP password and CHAP challenge attributes, and populates them as described in the CHAP procedure.


User
BorderNet
IP=192.168.1.1
Radius Server
Prerequisite:
User Groups are configured on the BorderNet
Login Request
[HTTPS to Login URL]
Provide User name + Password
User name = Shai
Password = 123456
[Encrypted over HTTPS/TLS]
Calculate hashed value:
- Generate a random challenge
- Calculate a hashed value using
a pre-shared secret and the challenge
RADIUS **Access-Request**
[AVP type 1, **User-Name = Shai**]
[AVP type 3, **CHAP-Password = 10b91d196b7d57379b** (encrypted)]
[AVP type 60, **CHAP-Challenge = e57fb69cc63fb0d1**
[AVP type 4, NAS-IP-Address = 192.168.1.1]
1. Verify user credentials
- Extract Random Challenge
- Use pre-shared secret to calculate hashed value
- Compare received CHAP-Password with calculated hash
2. Apply user-group (group=Application_Admin)
RADIUS **Access-Accept**
[AVP type 25, Class = Application_Admin]
User authenticated successfully and
authorized for Application Administrators
Authentication Successful.
Allow login.
Enforce 'Application_Admin' privilege.

4.5 EMS Authentication

The EMS authentication process is similar to the BorderNet process, but the Class attribute carries the user roles as defined in the EMS.



EMS Radius User Authentication, multiple groups - Successful

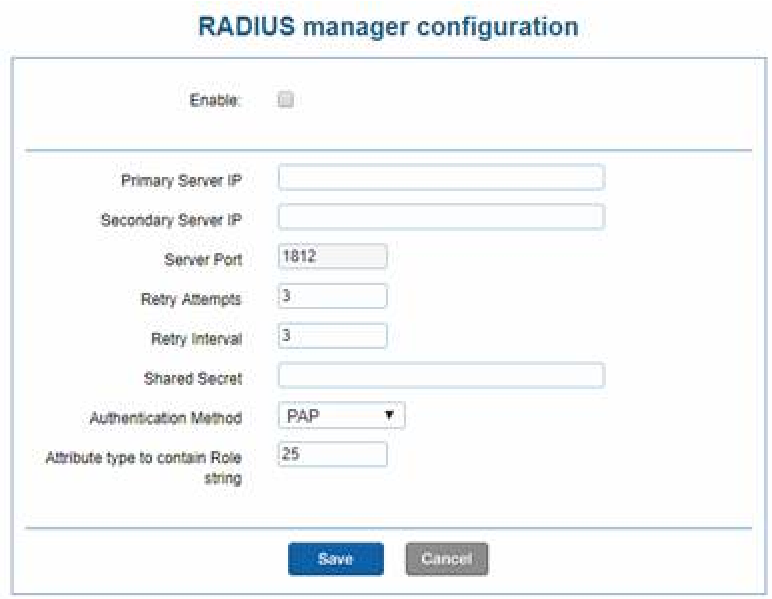
User
EMS
IP=192.168.1.1
Radius Server
Prerequisite:
User Roles are configured on the EMS
Login Request
[HTTPS to Login URL]
Provide User name + Password
User name = Shai
Password = 123456
[Encrypted using HTTPS/TLS]
RADIUS Access-Request
[AVP type 1, User-Name = Shai]
[AVP type 2, User-Password = 123456 (encrypted)]
[AVP type 4, NAS-IP-Address = 192.168.1.1]
1. Verify user credentials
2. Apply user-group (group=Application_Admin)
RADIUS Access-Accept
[AVP type 25, Class = Viewer]
[AVP type 25, Class = Operator]
User authenticated successfully and
authorized for as 'Viewer' and 'Operator'
Authentication Successful.
Allow login.
Enforce 'Viewer'+'Operator' privileges.

5. RADIUS Configuration

You can perform RADIUS configuration in BorderNet.

→ To perform RADIUSConfiguration:

1. From the **System** drop-down menu, select **RADIUS Configuration.**
   The **RADIUS Manager Configuration** screen opens.



RADIUS manager configuration

Enable: □

Primary Server IP:

Secondary Server IP:

Server Port: 1812

Retry Attempts: 3

Retry Interval: 3

Shared Secret:

Authentication Method: PAP ▾

Attribute type to contain Role string: 25

2. Edit the parameters according to the options detailed below.
   - **Enable**. Enable/Disable RADIUS functionality. Uses IPv4 only.
   - **Primary Server IP**. Main IP address of RADIUS server.
   - **Secondary Server IP** Secondary RADIUS server, if Primary Server not responding.
   - **Server Port**. Destination UDP port of requests sent to the RADIUS server. Default value 1812.
   - **Retry Attempts**. No of attempts before switching to Secondary Server. Possible values 1-10. Default value = 3.
   - **Retry Interval**. Time in seconds between each retry attempt. Values 1-90. Default value = 3.
   - **Shared Secret**. Password shared between the BorderNet and the RADIUS server. String.
   - **Authentication Method**. Type of authentication protocol used to deliver username and password. PAP/CHAP. Default = PAP.
   - **Attribute Type to Contain Role String**. Attribute type in the **Access-Accept** message, to contain user role. The type parameter in the RADIUS specification is one octet, so it can have values of 1-255. Default is the **Class** attribute (type=25).
3. Click **Save**.