AAA / RADIUS

REMOTE AUTHENTICATION DIAL IN USER SERVICE

INTRODUCTION TO RADIUS, A PROTOCOL FOR AUTHENTICATION, AUTHORIZATION AND ACCOUNTING SERVICES

Peter R. Egli
peteregli.net

Contents

1. AAA - Access Control (1/2)

What is AAA?

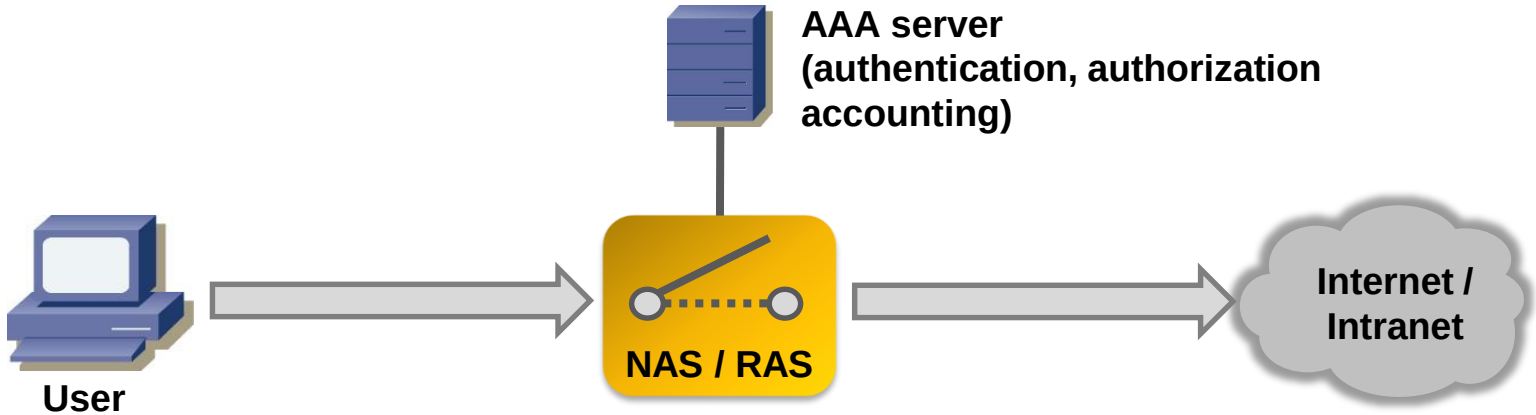
The term AAA (say "triple A") subsumes the functions used in network access to allow a user or a computer to access a network and use its resources.

Authentication:
Is the one I'm talking to the one he pretends to be (is a user authentic)?

Authorization:
Find out what the user is allowed to do (and what not).

Accounting:
Log the user's activity to charge him accordingly. Accounting information may be used to track the user's usage for charging but also for auditing purposes.

AAA is used in scenarios where a NAS (network access server) or a RAS (remote access server) acts like a switch granting or denying access to the Internet or Intranet for a user based on AAA authentication and authorization.



1. AAA - Access Control (2/2)

Most important AAA protocols:

1. RADIUS RFC2865:
Remote Authentication Dial In User Service.

2. TACACS+ RFC1492:
Terminal Access Controller Access Control System by Cisco.

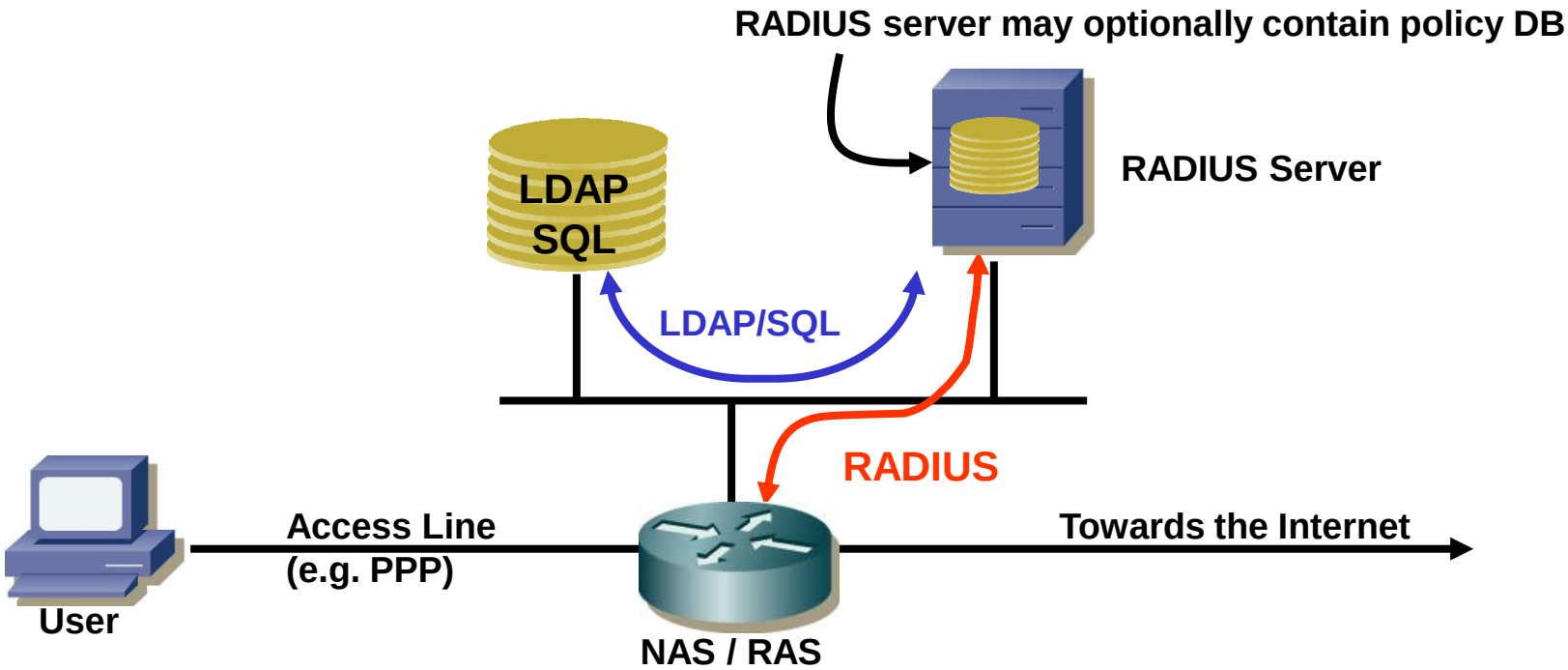
3. Diameter RFC3588:
Diameter is not an acronym. Diameter is a successor to RADIUS that should fix some of the shortcomings of RADIUS.
Diameter uses reliable transport connections, i.e. runs on TCP or SCTP (Stream Control Transmission Protocol).

➔ Nota Bene:
RADIUS (and TACACS+) are AAA access control protocols, but do not define a policy (who is granted access, what is the user allowed to do etc.). These protocols merely provide a means to transport such information between a client and an authentication server.
The policy is implemented as an application on the RADIUS server (possibly doing LDAP/SQL lookups to obtain access rules).

2. RADIUS architectures (1/2)

Scenario 1:

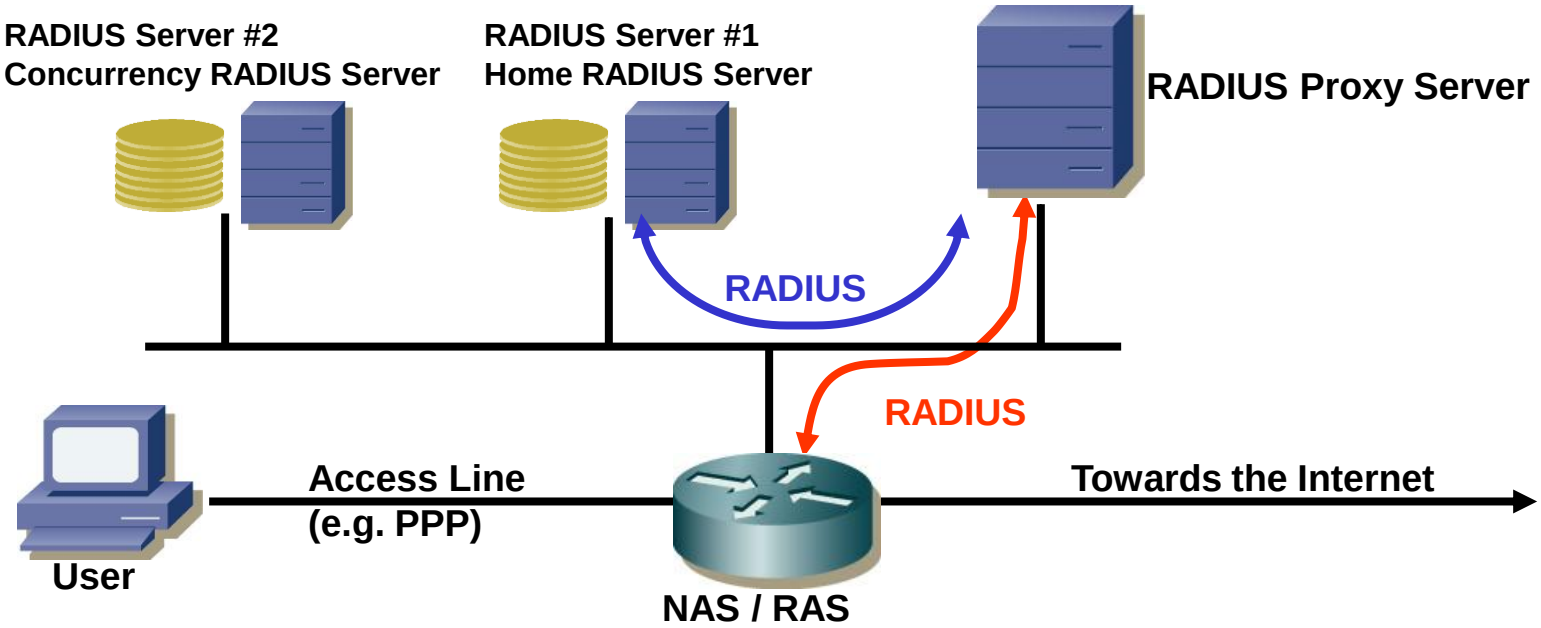
In this scenario, a front-end NAS (network access server) or RAS (remote access server) performs authentication of a user with a backend RADIUS server.
The NAS/RAS sends user information (credentials) to the RADIUS server carried in RADIUS packets. The RADIUS server implements the access policy (who is granted access with what authorizations) or may retrieve policies from a database through LDAP (Lightweight Directory Access Protocol).



2. RADIUS architectures (2/2)

Scenario 2:

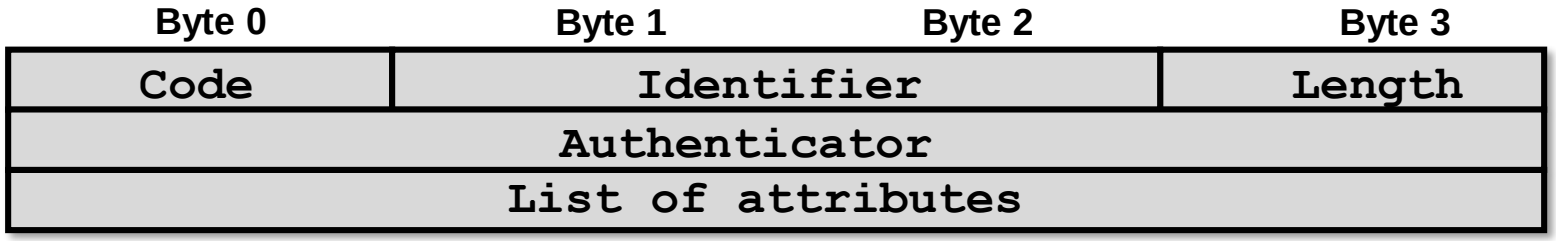
In this scenario, a first RADIUS server does not perform authentication but acts as a proxy that routes RADIUS requests to the appropriate home RADIUS server.
The routing is based on username and realm.
The home RADIUS server performs the actual authentication by accessing a user DB.
A concurrency RADIUS server may be employed to make sure that a user is not logged in more than once, e.g. in scenarios with multiple RADIUS servers for redundancy / load balancing.



3. RADIUS RFC2865 protocol

RADIUS uses UDP (port 1842) since it is a simple ‚Request-Reply' protocol (Accept/Request).

RADIUS packet format:



Code field: Defines the packet type (Access-Request, Access-Accept, Access-Reject, Access-Challenge, Accounting-Request, Accounting-Response).

Identifier: ID to match requests and replies.

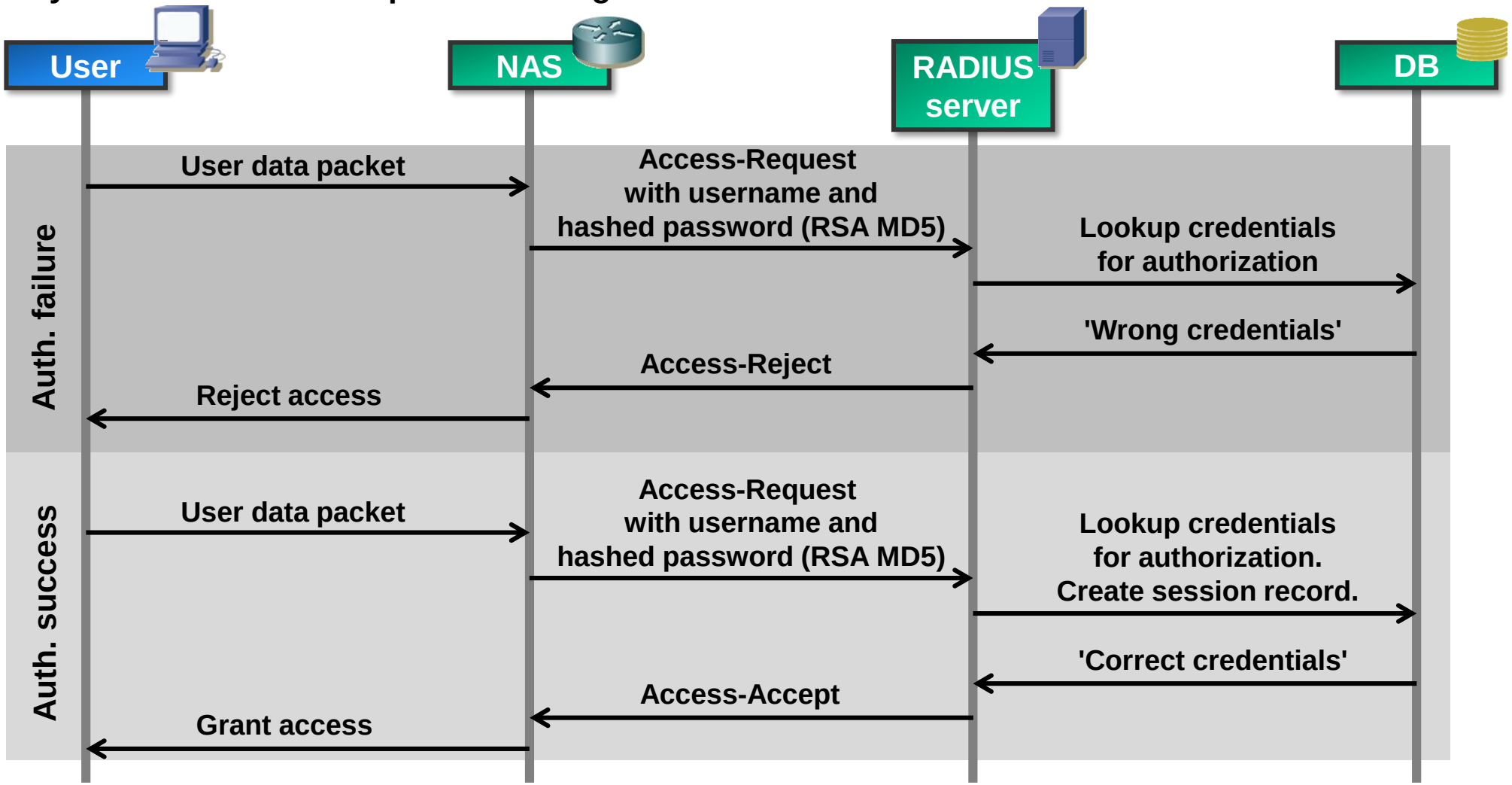
Length: Length of packet.

Authenticator: Used to authenticate the RADIUS transaction itself. The authenticator authenticates the reply from the server. The RADIUS client sends a challenge in the Access-Request packet and the RADIUS server returns a challenge-response in the Authenticator field (shared secret between NAS and RADIUS server).

Attributes: AAA-information such as username, password, CHAP-Password, callback-phone-# etc. The attribute encoding is as follows:

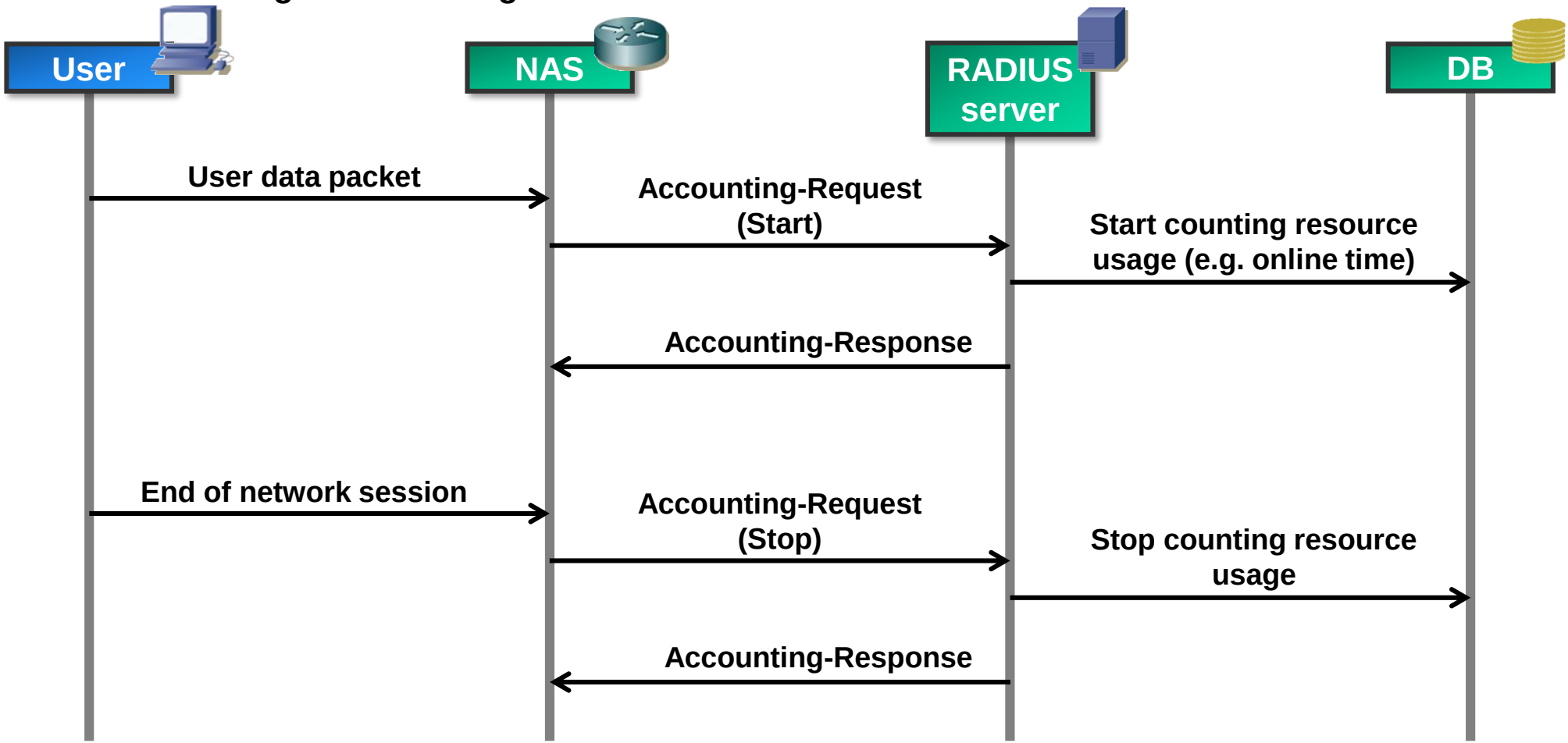
4. RADIUS transaction

A RADIUS transaction typically starts with an Access-Request carrying user credentials followed by a RADIUS server response with a grant or denial of access.



5. RADIUS accounting RFC2866 (1/2)

Once a network session is up and running (successful authentication), the NAS may request to start counting network usage of the user.



5. RADIUS accounting RFC2866 (2/2)

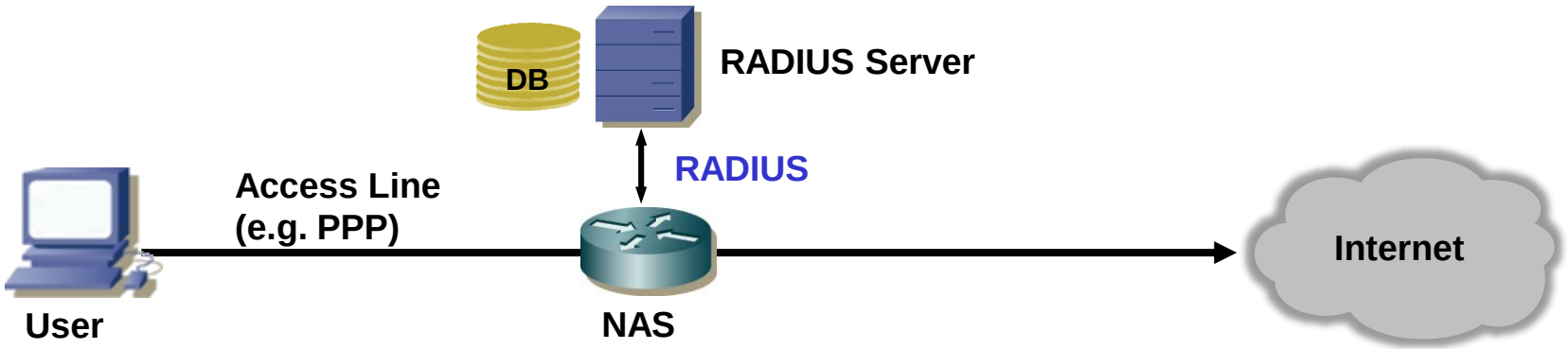
Accounting with RADIUS is specified in a separate RFC (RFC2866).
A set of special accounting RADIUS attributes (attribute values 40 – 59) are used to transfer accounting data between the RADIUS client (NAS) and server.

Value	Type	Description
40	Acct-Status-Type	Indicates start or stop of accounting.
41	Acct-Delay-Time	Delay between event causing accounting request and server response (used to compensate for processing delay time).
42	Acct-Input-Octets	Used by client to report number of received octets to server.
43	Acct-Output-Octets	Used by client to report number of transmitted octets to server.
44	Acct-Session-Id	Used by client to identify user session to server.
45	Acct-Authentic	Used by client to report authentication method to server, e.g. user autenticated by NAS itself, user authenticated by RADIUS or user authenticated by external protocol.
46	Acct-Session-Time	Used by client to report to server how many seconds the user session is running.
47	Acct-Input-Packets	Used by client to report number of packets received by a user.
48	Acct-Output-Packets	Used by client to report number of packets sent by a user.
49	Acct-Terminate-Cause	Used by client to report cause of service termination (e.g. error, termination upon user request, timeout).
50	Acct-Multi-Session-Id	Similar to Acct-Session-Id, but used to link multiple sessions to one for correlation in log file.
51	Acct-Link-Count	Used by client to report number of links used by user.

6. RADIUS applications (1/2)

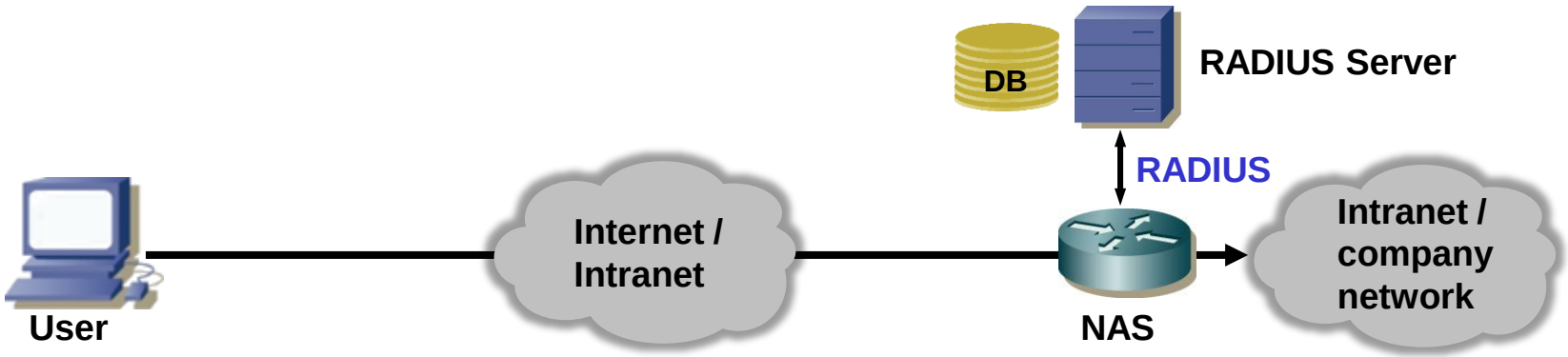
NAS network access (ISP):

A user dials in on a NAS server run by the Internet provider.
Prior to granting access to the Internet, the NAS authenticates the user with RADIUS.



RAS Intranet access (enterprise dial-in):

This application is similar to the NAS scenario. The RAS (Remote Access Server) sits at the edge of the company network and authenticates a user prior to granting access to the network.



6. RADIUS applications (2/2)

802.1X backend control for Ethernet and WLAN network access:

IEEE 802.1X is a generic protocol for authentication and authorization in IEEE 802 based networks.

The 802.1X supplicant ('the user') sends an EAPOL (Extensible Authentication Protocol Over LAN) message to the 802.1X authenticator (switch, access point).

The switch or access point enables the Ethernet or WiFi port if the backend authentication based on credentials provided via 802.1X is successful.

Using a central server for authentication (username and password storage) eases administration in large networks.