Podrška korisnicima, eskalacija problema i sigurnosnih incidenata

AMRES

Akademska mreža Srbije

AMRES eduroam servis

Problemi u radu eduroam servisa?

1. Korisnik ne može da se poveže
2. Sigurnosni incidenti
   - Autentifikovan korisnik izaziva sigurnosni incident - mora postojati mogućnost da se utvrdi ko je
   - Klasični WLAN napadi:
     - spamovanje autentifikacionim zahtevima – DoS ili provaljivanje kredenicijala
     - disasocijacija povezanih klijenata
     - *poisoning* MAC-tabela

Log fajlovi se koriste da bi se rešavali problemi u pristupu i sigurnosni incidenti

Logovi

- Davalac Resursa MORA:
  1. Čuvati Autentifikacione logove
  2. Biti u mogućnosti da na osnovu prijavljene IP adrese i vremena utvrdi MAC adresu korisnika – npr. DHCP log ili RADIUS Accounting

- Davalac Ideniteta MORA:
  1. Čuvati Autentifikacione logove

- Svi serveri MORAJU biti sinhronizovani sa tačnim izvorom vremena - NTP

Radius Log fajlovi

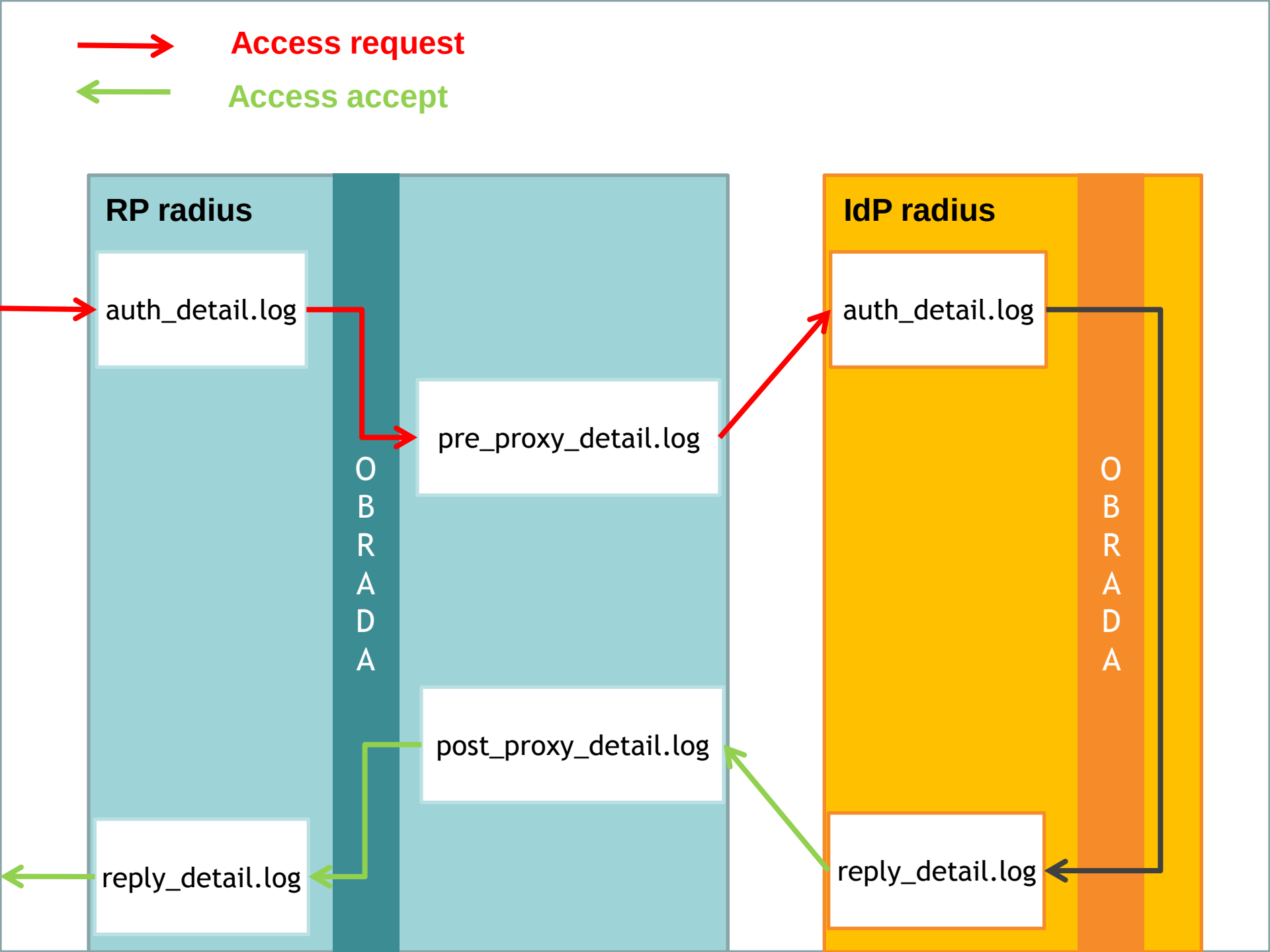
- Logovi koji postoje u FreeRADIUSu:

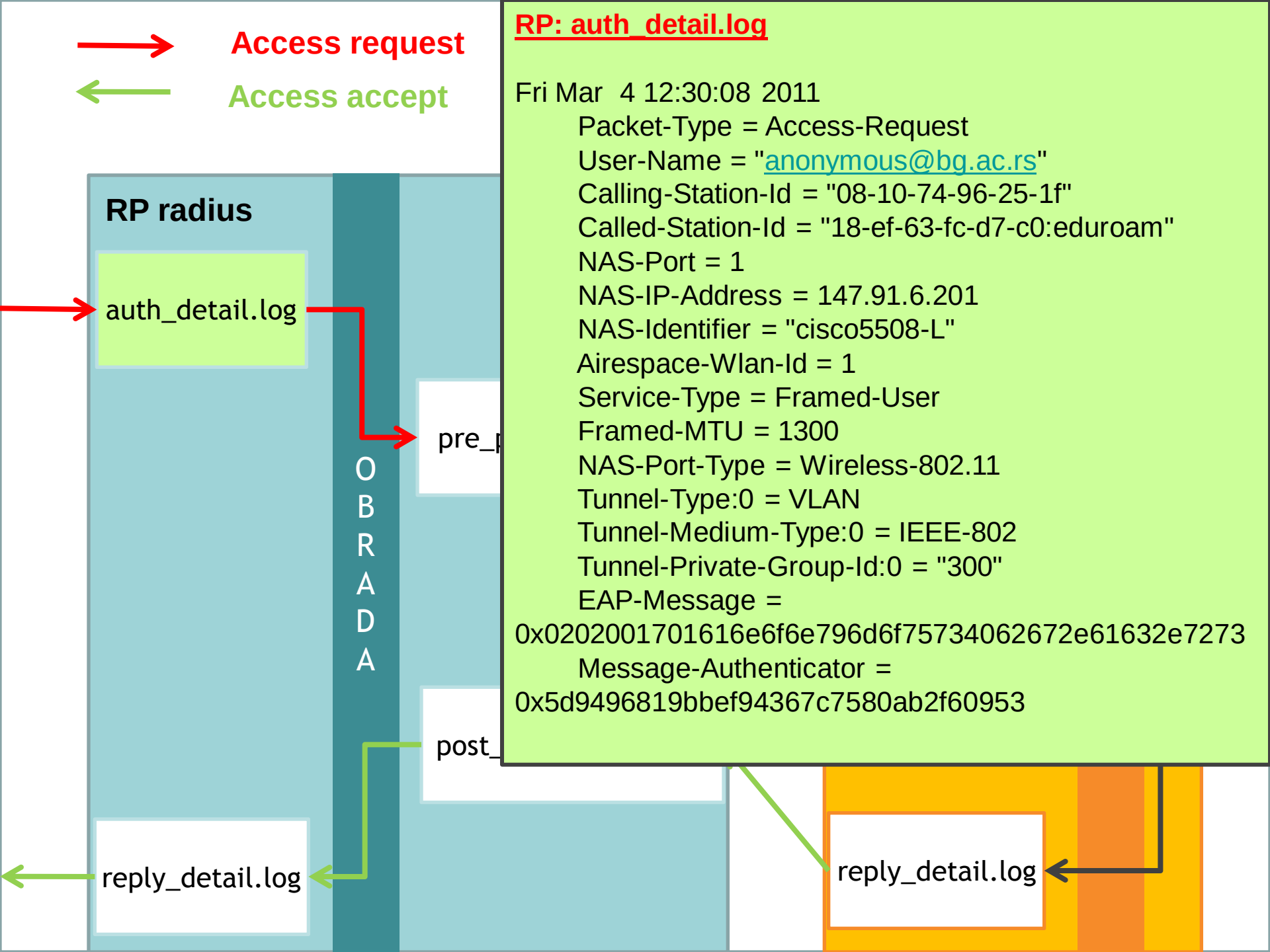
  auth_detail.log – kada primi Auth zahtev od klijenta

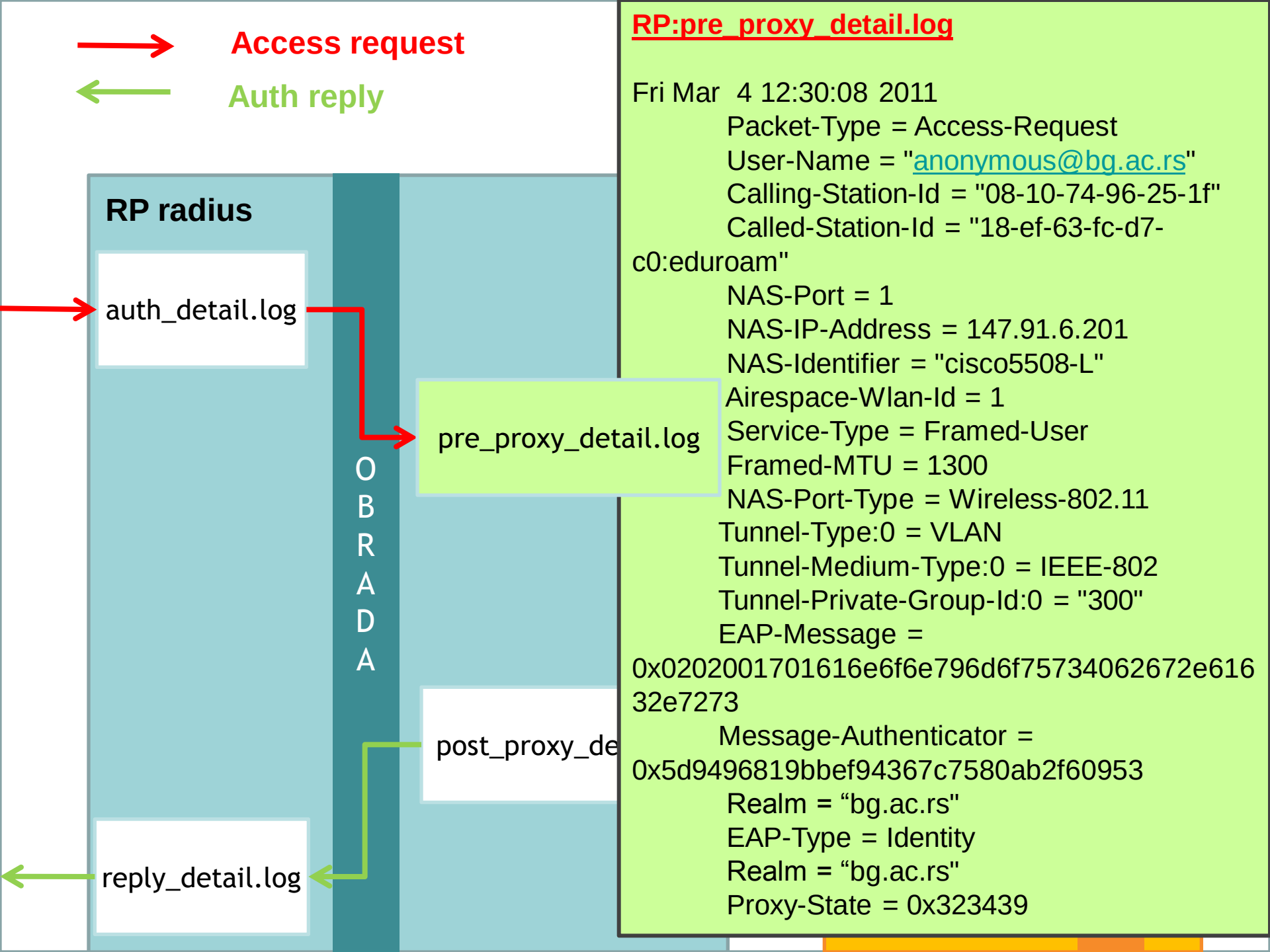
  pre_proxy_detail.log – pre nego što proksira Auth zahtev

  post_proxy_detail .log – kada dobije Auth odgovor

  reply_detail.log – pre nego što pošalje Auth odgovor klijentu


Access request
Access accept
RP radius
auth_detail.log
OBRADA
pre_proxy_detail.log
post_proxy_detail.log
reply_detail.log
IdP radius
auth_detail.log
OBRADA
reply_detail.log

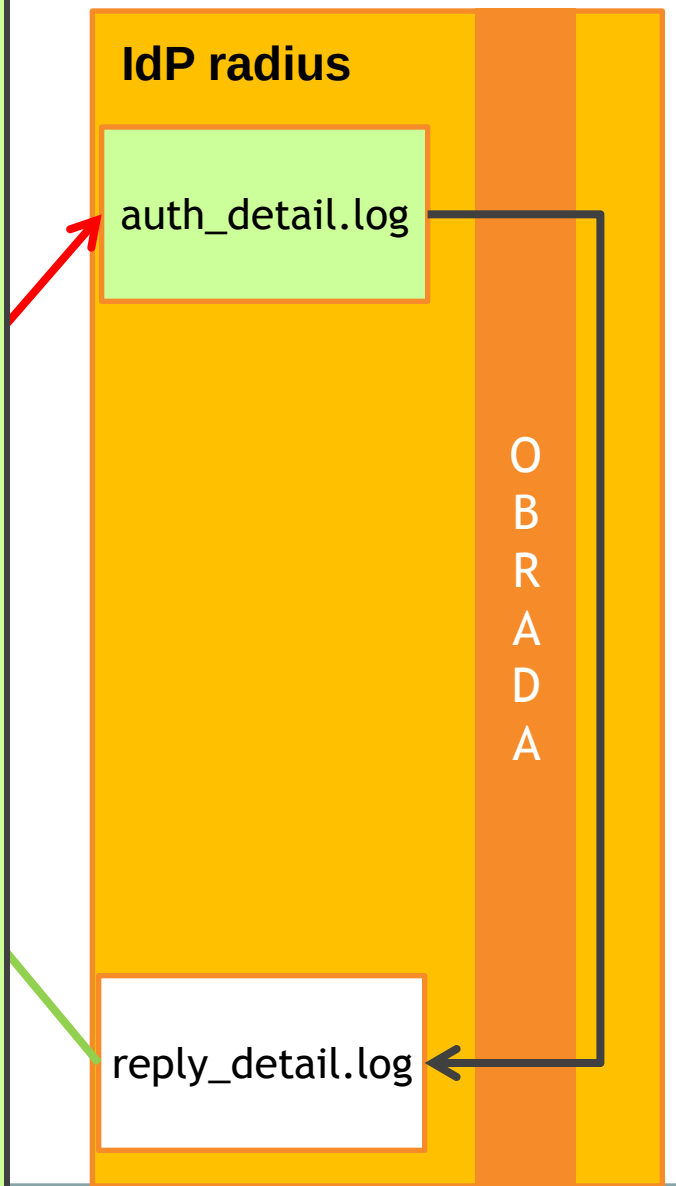

Access request
Access accept
RP: auth_detail.log
Fri Mar 4 12:30:08 2011
Packet-Type = Access-Request
User-Name = "anonymous@bg.ac.rs"
Calling-Station-Id = "08-10-74-96-25-1f"
Called-Station-Id = "18-ef-63-fc-d7-c0:eduroam"
NAS-Port = 1
NAS-IP-Address = 147.91.6.201
NAS-Identifier = "cisco5508-L"
Airespace-Wlan-Id = 1
Service-Type = Framed-User
Framed-MTU = 1300
NAS-Port-Type = Wireless-802.11
Tunnel-Type:0 = VLAN
Tunnel-Medium-Type:0 = IEEE-802
Tunnel-Private-Group-Id:0 = "300"
EAP-Message =
0x0202001701616e6f6e796d6f75734062672e61632e7273
Message-Authenticator =
0x5d9496819bbef94367c7580ab2f60953
RP radius
auth_detail.log
pre_
OBRADA
post_
reply_detail.log
reply_detail.log

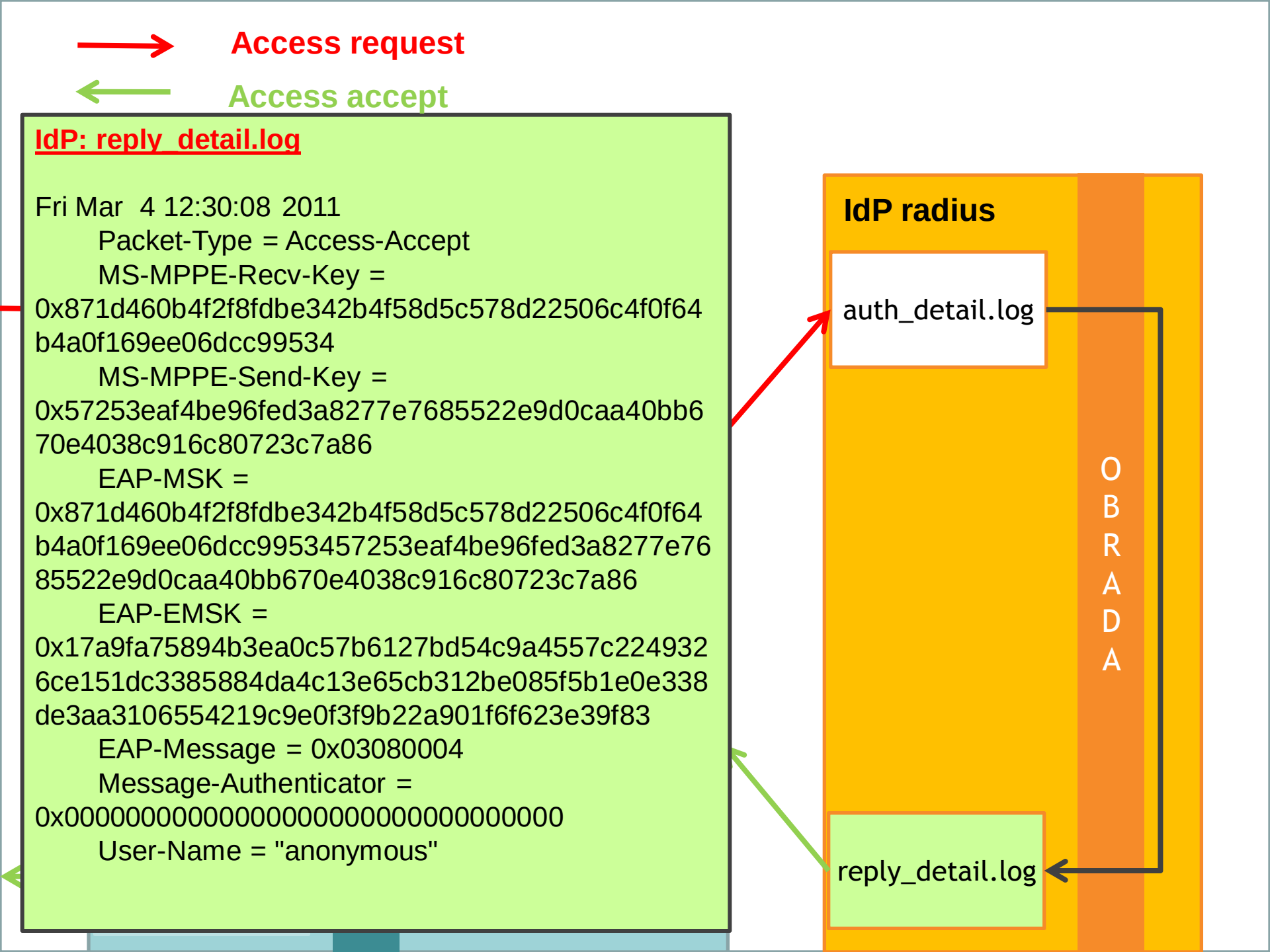

Access request
Auth reply
RP radius
auth_detail.log
pre_proxy_detail.log
OBRADA
post_proxy_de
reply_detail.log
RP:pre_proxy_detail.log
Fri Mar 4 12:30:08 2011
Packet-Type = Access-Request
User-Name = "anonymous@bg.ac.rs"
Calling-Station-Id = "08-10-74-96-25-1f"
Called-Station-Id = "18-ef-63-fc-d7-c0:eduroam"
NAS-Port = 1
NAS-IP-Address = 147.91.6.201
NAS-Identifier = "cisco5508-L"
Airespace-Wlan-Id = 1
Service-Type = Framed-User
Framed-MTU = 1300
NAS-Port-Type = Wireless-802.11
Tunnel-Type:0 = VLAN
Tunnel-Medium-Type:0 = IEEE-802
Tunnel-Private-Group-Id:0 = "300"
EAP-Message = 0x0202001701616e6f6e796d6f75734062672e61632e7273
Message-Authenticator = 0x5d9496819bbef94367c7580ab2f60953
Realm = “bg.ac.rs"
EAP-Type = Identity
Realm = “bg.ac.rs"
Proxy-State = 0x323439

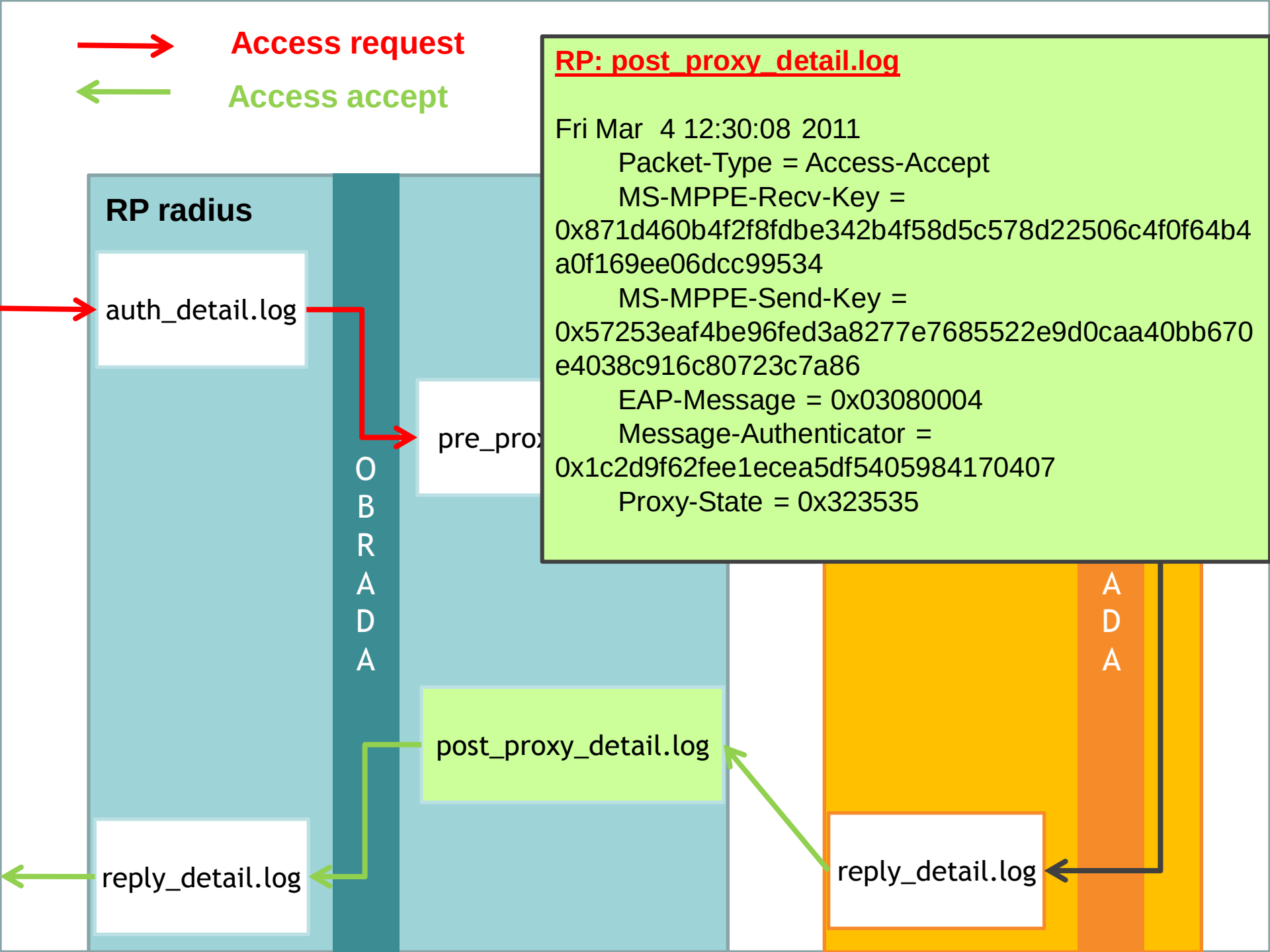
IdP: auth_detail.log

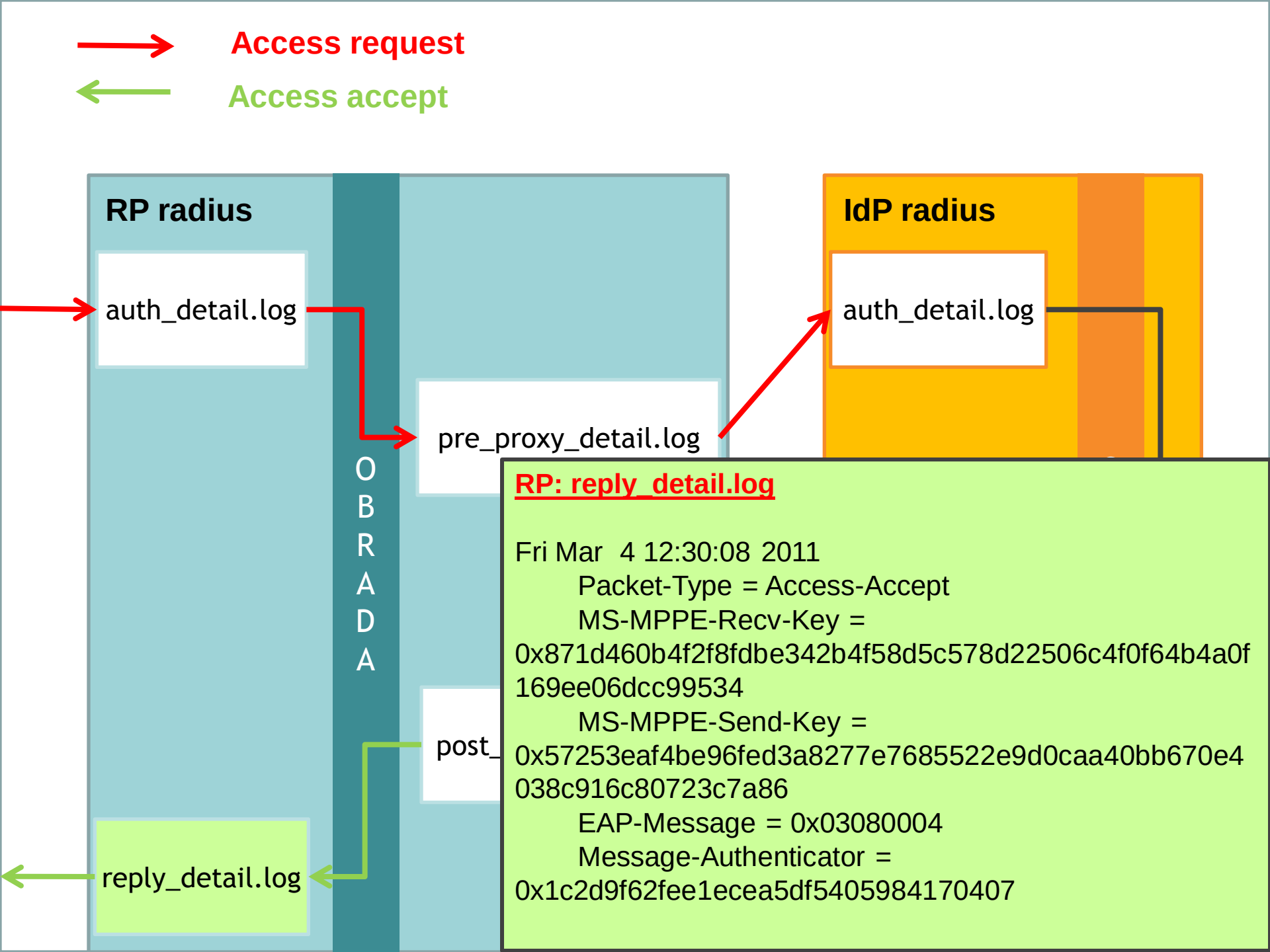
```
Fri Mar  4 12:30:08 2011
        Packet-Type = Access-Request
        User-Name = "anonymous@bg.ac.rs"
        Calling-Station-Id = "08-10-74-96-25-1f"
        Called-Station-Id = "18-ef-63-fc-d7-c0:eduroam"
        NAS-Port = 1
        NAS-IP-Address = 147.91.6.201
        NAS-Identifier = "cisco5508-L"
        Service-Type = Framed-User
        EAP-Message =
0x0208004b15001703010040 4cb330ef510dea4afe853bea
208fc47513eb6667ebd376dadcc2e533ee38b1234d0b8d20
02fae7363ebe237746543669af83aa1f3b308d0
3dce2fe5b66500e0e
        State = 0x1ad0eedc1fd8fb67cc870211b3b0e90b
        Message-Authenticator =
0x920ee41de02e598726c6656d41eaeb91
        Proxy-State = 0x323535
        Proxy-State = 0x313738


Fri Mar  4 12:30:08 2011
        Packet-Type = Access-Request
        User-Name = "marina@bg.ac.rs"
        FreeRADIUS-Proxied-To = 127.0.0.1
```




Access request
Access accept
IdP: reply_detail.log
Fri Mar 4 12:30:08 2011
Packet-Type = Access-Accept
MS-MPPE-Recv-Key = 0x871d460b4f2f8fdbe342b4f58d5c578d22506c4f0f64b4a0f169ee06dcc99534
MS-MPPE-Send-Key = 0x57253eaf4be96fed3a8277e7685522e9d0caa40bb670e4038c916c80723c7a86
EAP-MSK = 0x871d460b4f2f8fdbe342b4f58d5c578d22506c4f0f64b4a0f169ee06dcc9953457253eaf4be96fed3a8277e7685522e9d0caa40bb670e4038c916c80723c7a86
EAP-EMSK = 0x17a9fa75894b3ea0c57b6127bd54c9a4557c2249326ce151dc3385884da4c13e65cb312be085f5b1e0e338de3aa3106554219c9e0f3f9b22a901f6f623e39f83
EAP-Message = 0x03080004
Message-Authenticator = 0x00000000000000000000000000000000
User-Name = "anonymous"
IdP radius
auth_detail.log
OBRADA
reply_detail.log


Access request
Access accept
RP: post_proxy_detail.log
Fri Mar 4 12:30:08 2011
Packet-Type = Access-Accept
MS-MPPE-Recv-Key = 0x871d460b4f2f8fdbe342b4f58d5c578d22506c4f0f64b4a0f169ee06dcc99534
MS-MPPE-Send-Key = 0x57253eaf4be96fed3a8277e7685522e9d0caa40bb670e4038c916c80723c7a86
EAP-Message = 0x03080004
Message-Authenticator = 0x1c2d9f62fee1ecea5df5405984170407
Proxy-State = 0x323535
RP radius
auth_detail.log
pre_prox
OBRADA
post_proxy_detail.log
reply_detail.log
reply_detail.log
ADA


Access request
Access accept
RP radius
auth_detail.log
pre_proxy_detail.log
post_
reply_detail.log
OBRADA
IdP radius
auth_detail.log
RP: reply_detail.log
Fri Mar 4 12:30:08 2011
Packet-Type = Access-Accept
MS-MPPE-Recv-Key =
0x871d460b4f2f8fdbe342b4f58d5c578d22506c4f0f64b4a0f
169ee06dcc99534
MS-MPPE-Send-Key =
0x57253eaf4be96fed3a8277e7685522e9d0caa40bb670e4
038c916c80723c7a86
EAP-Message = 0x03080004
Message-Authenticator =
0x1c2d9f62fee1ecea5df5405984170407

Mesto smeštanja RADIUS logova - FreeRADIUS

- Po *default*u:

  `/radacct/ip_adresa_klijenta/tip_loga-datum`

- Konfiguriše se u modulu `/raddb/modules/details.log`, primer za auth-detail

```
detail auth_log {
        detailfile = ${radacctdir}/%{Client-IP-
Address}/auth-detail-%Y%m%d

        #  This MUST be 0600, otherwise anyone can read
the users passwords!
        detailperm = 0600

        # You may also strip out passwords completely
        suppress {
                User-Password
        }
}
```

Mesto smeštanja RADIUS logova - FreeRADIUS

- Primer konfiguracije – svi logovi iz jednog dana se smeštaju u zajednički folder

```
detail auth_log {
        detailfile = ${radacctdir}/%Y%m%d/eduroam/auth-detail
        detailperm = 0600
        suppress {
                User-Password
        }
 }
```

Uključivanje logovanja FreeRADIUS - Davalac Identiteta

- U konf. fajlovima za `eduroam` i `eduroam-inner-tunnel` virutelne servere (raddb/sites-avalaible/eduroam i raddb/sites-avalaible/eduroam-inner-tunnel)

```
authorize {
    ..
      auth_log
    ..
}
```

uključuje auth_detail.log

```
post-auth {
  ..
      reply_log
  ..
}
```

uključuje reply_detail.log

Uključivanje logovanja FreeRADIUS - Davalac Resursa

- U konf. fajlu za `eduroam` virutelni server (raddb/sites-avalaible/eduroam)

```
authorize {
    ..
    auth_log
    ..
}
```

uključuje auth_detail.log

```
pre-proxy {
..
   pre_proxy_log
  ..
}
```

uključuje pre_proxy_detail.log

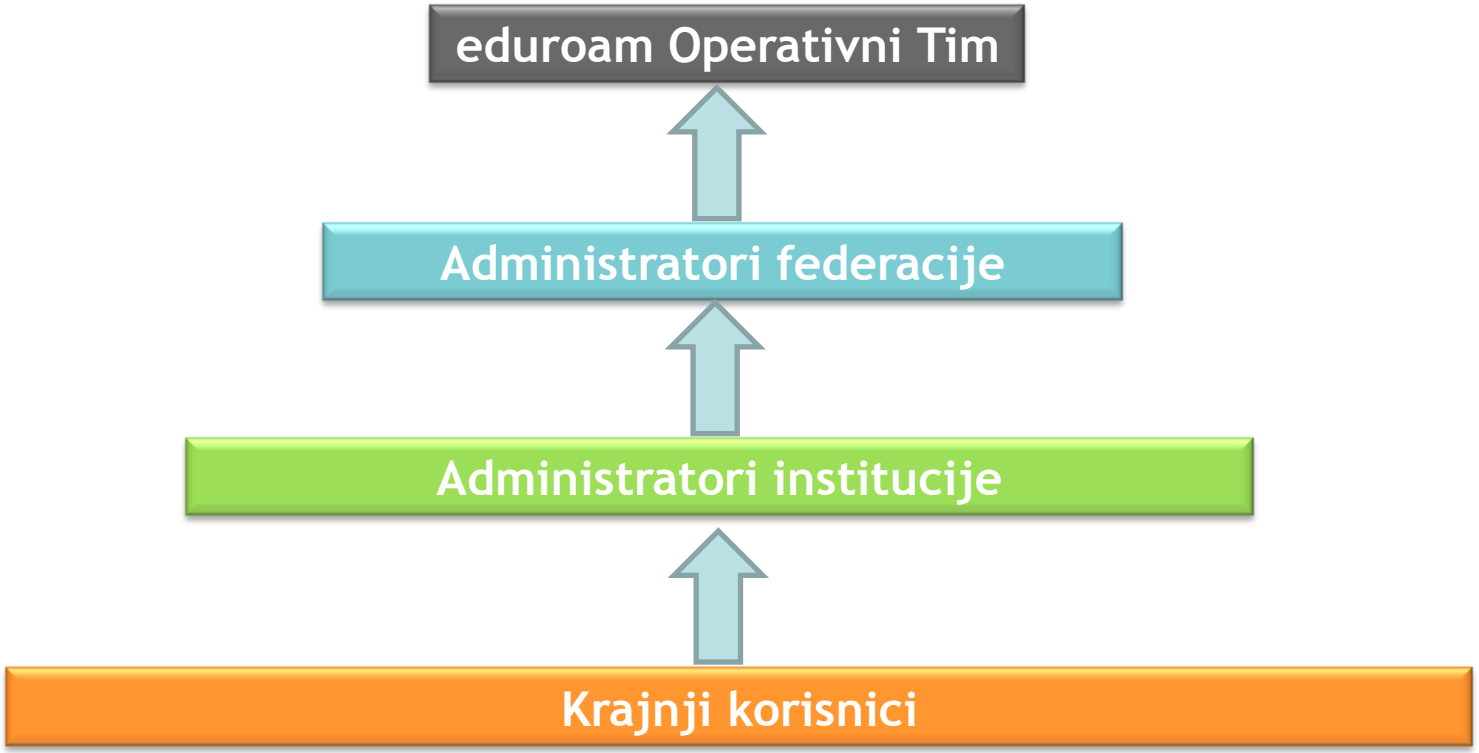
```
post-auth {
  ..
  reply_log
  ..
}
```

uključuje reply_detail.log

```
post-proxy {
  ..
  post_proxy_log
  ..
}
```

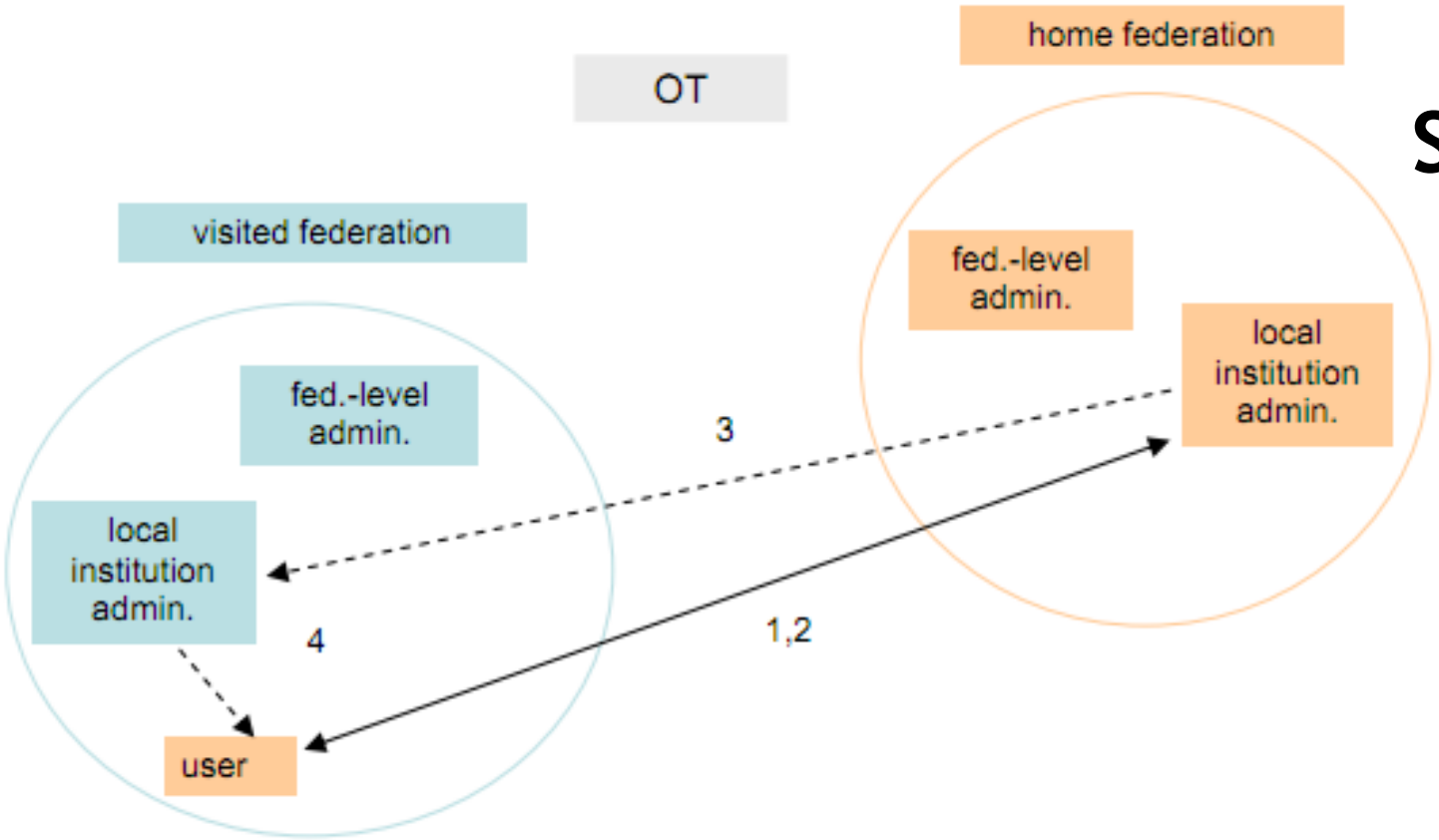
uključuje post_proxy_detail.log

Rešavanje problema u pristupu



- Krajnji korisnik o problemu ili incidentu obaveštava **svoju matičnu instituciju**
- Pogledati moguće scenarije u nastavku

Scenario 1.

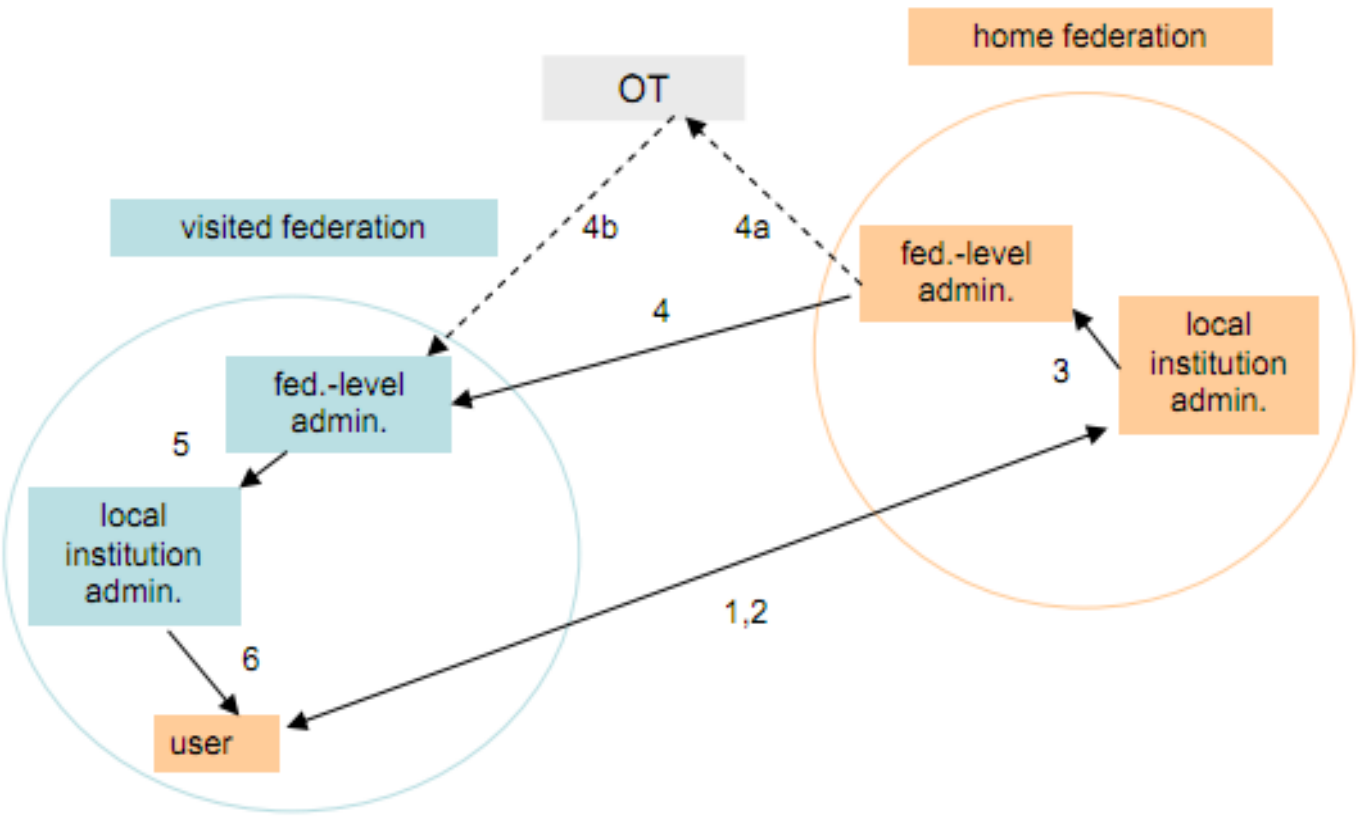


1. Korisnik zove svoju matičnu instituciju
2. Administratori matične institucije:
   - proveravaju validnost korisnikovih kredencijala
   - asistiraju u podešavanju korisnikvog uređaja
   - proveravaju da li stiže zahtev za autentifikacijom
3. Adminstratori matične institucije obaveštava administratore posećene institucije
4. Administratori posećene institucije pomažu korisniku

Pomažu korisniku

DA ->korak 3
NE-> Scenario 2

Scenario 2.



3. Admin. matične institucije kontaktiraju admini. matične federacije; lokalni problem ?

DA ->rešava se
NE-> 4, 4a, 4b

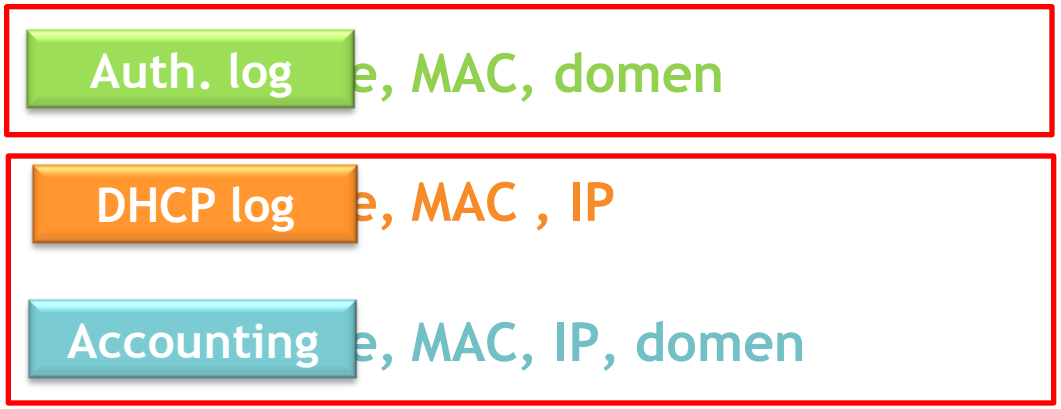
4. 4a. 4b. Admin. matične federacije eskaliraju problem admin. posećene federacije i OT eventualno

5. Admin posećene federacije kontatkiraju admin posećene institucije i rešavaju problem

6. Admin posećene institucije obaveštavaju korisnika o rešenju

Rešavanje sigurnosnih incidenata

1. CSIRT služba dobija prutužbu sa informacijama o **IP adresi** i **vremenu** dešavanja incidenta
2. CSIRT služba kontaktira davaoca resursa. Nalazi **MAC** adresu korisnika i **realm** korisnika iz neke kombinacije:



obavezno

Bilo koji način da se mapira Vreme IP i MAC

3. CSIRT služba dalje kontaktira:

   ista fed.: matičnu inst.

   druga fed.: eduroam OT-> matičnu fed.->matičnu inst.

4. Matična institucija na osnovu MAC adrese i vremena nalazi **korisničko ime** iz Auth logova

Blokiranje domena i korisnika

- U slučaju sigurnosnih pretnji ili nekog incidenta koji ne može biti blagovremeno rešen davaoci resursa mogu da konfigurišu svoj autentifikacioni server tako da blokira:
  - ceo domen davaoca identetata
  - pojedinačnog korisnika

- O ovome se MORA u najkraćem roku obavestiti AMRES !

Radius Accounting

- Ukoliko NAS podržava RADIUS Accounting, RP RADIUS može čuvati ove informacije u SQL bazi
- Prednost što se mogu beležiti i informacije o vremenu trajanja sesije, prenetoj količini podataka i sl.

User-Name	Calling-Station-Id	Client-IP-Address	Called-Station-Id	NAS-IP-Address
anonymous@rgf.bg.ac.rs	00-21-63-A2-DC-E5	147.91.183.204	00-0B-6B-B6-59-C3:...	147.91.183.2

Timestamp Start	Timestamp Stop	Acct-Unique-Session-Id	Acct-Session-Time
2011-03-04 12:02:58	2011-03-04 13:37:39	01c33e1795264c03	5681

Acct-Input-Octets	Acct-Output-Oc...	Acct-Input-Pac...	Acct-Output-Pa...	Acct-Terminate-Cause
218899	253432	1905	1062	User-Request

Radius Accounting

- Tri vrste Accounting paketa
  - *Accounting start*
  - *Accounting interim update*
  - *Accounting stop*

- Primer konfiguracije cisco NASa:

```
cisco# aaa accounting network start-stop radius
cisco# aaa accounting update periodic minutes
cisco# aaa accounting delay-start
```

Radius Accounting - FreeRADIUS

Aktiviranje u konf. fajlu za eduroam virutelni server (raddb/sites-avalaible/eduroam)

```
accounting {
    ..
        #  Log traffic to an SQL database.
        #  See "Accounting queries" in sql.conf
#       sql
        eduroam
    ..
}
```

Radius Accounting - FreeRADIUS

sql.conf

```
sql eduroam {
        database = "mysql"
        driver = "rlm_sql_${database}"
        server = "localhost"
        login = "marko"
        password = "b1gS3cRet"
        radius_db = "radius"
        acct_table1 = "eduroam-acc"
           .
           .
           .
        deletestalesessions = yes
        sqltrace = yes
        sqltracefile = ${logdir}/sqltrace.sql
        num_sql_socks = 5
        connect_failure_retry_delay = 60
        lifetime = 0
        max_queries = 0
        nas_table = "nas"
        $INCLUDE sql/${database}/eduroam.conf
}
```

Radius Accounting - FreeRADIUS

- eduroam.conf

```
accounting_start_query = "INSERT into EDUROAM_ACC SET\
        `User-Name` = '%{User-Name}',\
        `Calling-Station-Id` = '%{Calling-Station-Id}',\
        `Called-Station-Id` = '%{Called-Station-Id}',\
        `NAS-IP-Address` = '%{NAS-IP-Address}',\
        `NAS-Port` = '%{NAS-Port}',\
        `Timestamp Start` = NOW(),\
        `Client-IP-Address` = '%{Framed-IP-Address}'\
        `Acct-Unique-Session-Id` = '%{Acct-Unique-Session-Id}'
    "
```

Radius Accounting - FreeRADIUS

- eduroam.conf

```
accounting_update_query = "UPDATE EDUROAM_ACC SET\
        `Acct-Session-Time` = '%{Acct-Session-Time}',\
        `Acct-Input-Octets` = '%{Acct-Input-Octets}',\
        `Acct-Output-Octets` = '%{Acct-Output-Octets}',\
        `Acct-Input-Packets` = '%{Acct-Input-Packets}',\
        `Acct-Output-Packets` = '%{Acct-Output-Packets}'\
    `Client-IP-Address` = '%{Framed-IP-Address}'\
WHERE `Acct-Unique-Session-Id` = '%{Acct-Unique-Session-Id}'\
LIMIT 1
"
```

Radius Accounting - FreeRADIUS

- eduroam.conf

```
accounting_stop_query = "UPDATE EDUROAM_ACC SET\
    `Timestamp Stop` = '%S',\
    `Acct-Session-Time` = '%{Acct-Session-Time}',\
    `Acct-Input-Octets` = '%{Acct-Input-Octets}',\
    `Acct-Output-Octets` = '%{Acct-Output-Octets}',\
    `Acct-Input-Packets` = '%{Acct-Input-Packets}',\
    `Acct-Output-Packets` = '%{Acct-Output-Packets}',\
    `Acct-Terminate-Cause` = '%{Acct-Terminate-Cause}',\
    `Client-IP-Address` = '%{Framed-IP-Address}'\
WHERE `Acct-Unique-Session-Id` = '%{Acct-Unique-Session-Id}'\
LIMIT 1
"
```