ARP Hosts

In This Chapter

This section describes advanced ARP host configurations.

Topics in this section include:

Applicability

This section describes ARP hosts and is applicable to 7450 ESS, 7750 SR and 7710 SR series and was tested on SR-OS 7.0 R5. The 7750 SR-c4 is supported from 8.0R4 and higher.

Summary

In business access area, both DHCP and PPPoE are used. However, it is possible that CPE network facing interfaces are statically configured. In such cases, the first packet the network on the user side sees is ARP to the Broadband Service Aggregator (BSA) or Broadband Service Router (BSR) interface. In order to accommodate such configurations, Alcatel-Lucent Enhanced Subscriber Management (ESM) feature set supports the ARP host.

In practise this means that authentication, self-provisioning and Service Level Agreement (SLA) enforcement can be triggered by reception of ARP packets.

The BRAS node will learn the IP-MAC association based on received arp-request packet and will provision subscriber-hosts based on results from RADIUS authentication, the same way this would happened through DHCP or PPPoE.

This section provides configuration and troubleshooting commands for arp-hosts. Features common to other host-types and not unique to arp-hosts are not described in this note. (Not exhaustive list: RADIUS managed routes, routed subscriber with dynamic BGP peering, Wholesale/Retail, Managed SAPs configurations, ESM related host limitation mechanisms, host High-Availability, multi-chassis peer synchronization).

Knowledge of the Alcatel-Lucent Triple Play Service Delivery Architecture (TPSDA) concepts is assumed throughout this document.

Warning:

• Enhanced Subscriber Management and RADIUS authentication are mandatory for the use of ARP hosts.

Overview

ARP host is supported in bridged CO (VPLS) and routed CO (Subscriber Interface). And it is triggered by the first arp packet from the host. ARP host is also supported in a wholesale/retail context and on managed SAPs (MSAP).

The IP and MAC addresses are extracted from the ARP request. They are copied in the access-request message send to the RADIUS server:

- RADIUS attribute [1] Username = IP address
- Alcatel-Lucent VSA [26][27] Client Hardware Address = MAC address

RADIUS will, on successful authentication, reply with an access-accept message on which the ESM will create the ARP host. ESM string assignment options are out of scope for this scenario.
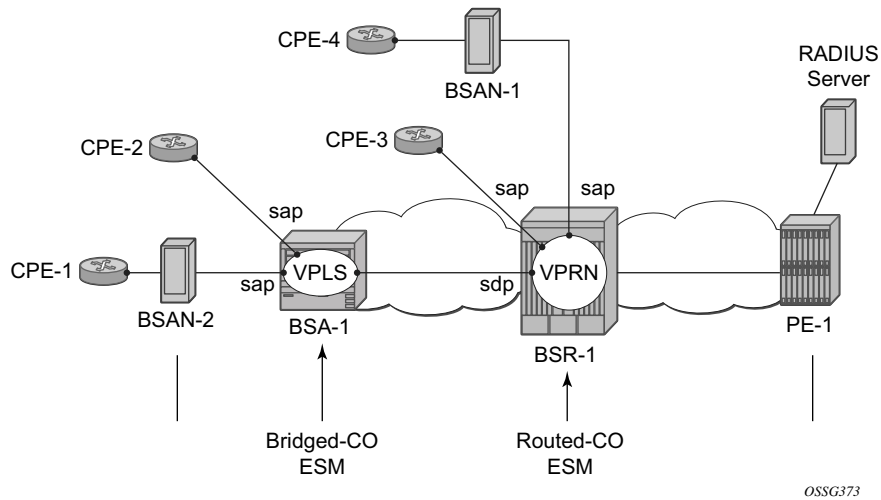

Figure 304: Bridged CO and Routed CO Example

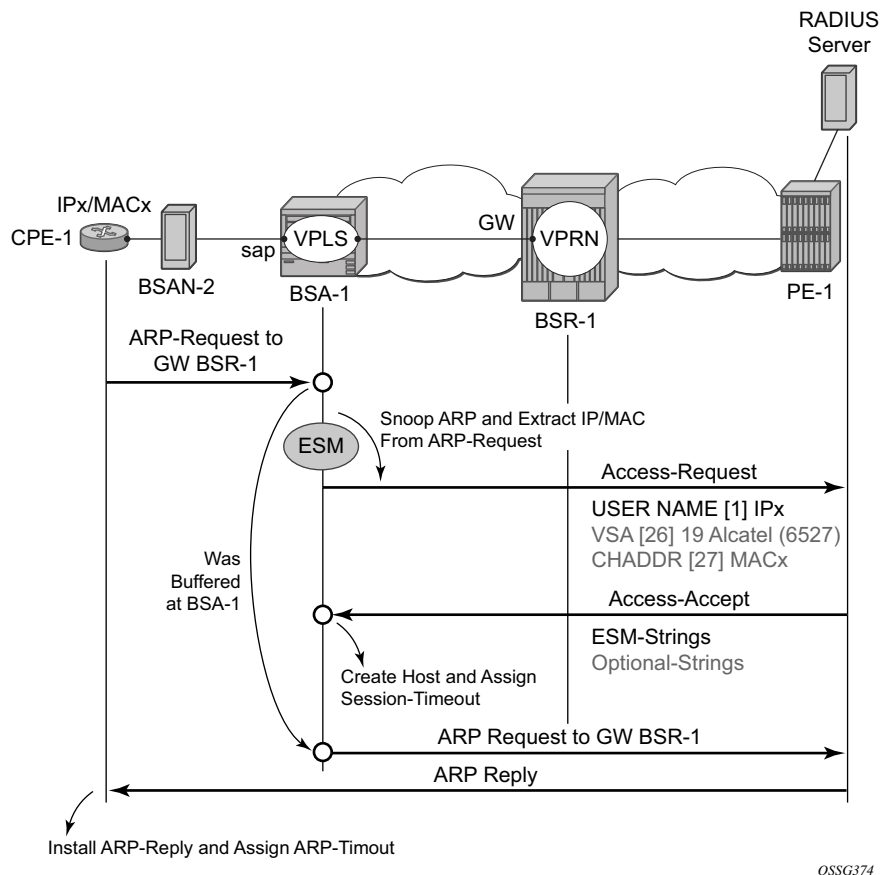# Configuration

ARP Hosts in a Bridged CO Environment

Figure 305: ARP Hosts in a Bridged CO Environment Example

ARP-host-specific enabling for Bridged CO is achieved by a composite service, VPLS on BSA node and VPRN/IES on BSR node. RADIUS authentication and subscriber management, which mandates IP-MAC or NH-MAC type anti-spoofing, are mandatory for ARP hosts.

```
configure
    service
      vpls 2 customer 1 create
            description "ARP host - Bridged CO"
             sap 1/1/3:1 create
                authentication-policy "authentication-1"
                anti-spoof ip-mac
                sub-sla-mgmt
                    sub-ident-policy "sub-id-default"
                    no shutdown
                exit
                arp-host
                    no shutdown
                exit
            exit
            spoke-sdp 12:2 create
            exit
            no shutdown
```

The RADIUS authentication policy does not require specific parameter settings. The RADIUS username attribute will contain always the host IP address which makes the authentication policy parameter user-name-format irrelevant for ARP hosts.

```
configure
    subscriber-mgmt
        authentication-policy "authentication-1" create
        password ALU
        radius-authentication-server
            server 1 address 172.16.1.1 secret ALU
        exit
        re-authentication         # optional if re-authentication is required
        accept-authorization-change # optional is RADIUS Disconnect is required
    exit
```

The CPE ARPs are snooped and the first CPE ARP triggers a RADIUS accept-request and subsequent ARPs will trigger RADIUS re-authentication only if the ARP host configurable min-auth-interval is expired and the above re-authentication parameter is set. The initial ARP is only forwarded to the BSR-1 upon successful RADIUS authentication by means of a RADIUS access-accept message. The same RADIUS access-accept message and the passing the several sessions limit checks, triggers the creation of the host.

The BSR-1 node requires a VPRN/IES as part of the composite service. No ARP-host-specific parameters are required on the BSR-1 for the bridged CO model.

BSR-1

```
configure
    service
        vprn 1 customer 1 create
            route-distinguisher 64496:1
            auto-bind ldp
            vrf-target target:64496
            interface "int-BSA1-p2mp-1" create
                description "ARP host - Bridged CO"
                address 10.2.0.6/29
                ip-mtu 1500
                spoke-sdp 21:2 create
                exit
            exit
```

ARP Hosts in a Routed CO Environment
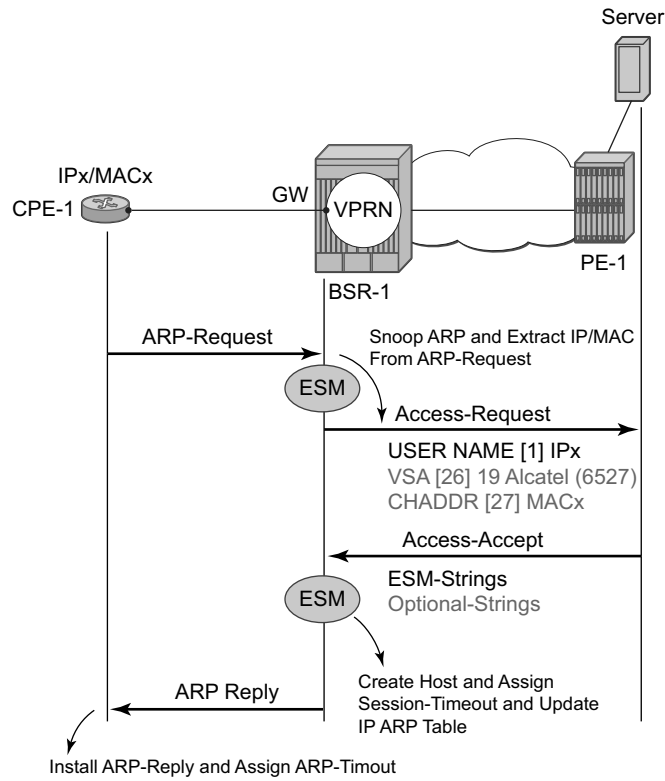
Figure 306: ARP Hosts in a Routed CO Environment Example

ARP-host-specific enabling for routed CO is identical for VPRN and IES services. RADIUS authentication and subscriber management, which mandates IP-MAC or NH-MAC type anti-spoofing, are mandatory for ARP hosts.

The initial ARP will, only upon successful RADIUS authentication and passing the several sessions limit checks, create the ARP host. The ARP reply or update of IP ARP table is not performed on any unsuccessful RADIUS authentication.

```
configure
    service
        vprn 1 customer 1 create
            route-distinguisher 64496:1
            auto-bind ldp
            vrf-target target:64496
                description "ARP host - Routed CO"
                address 10.1.0.6/29
                group-interface "group-int-1" create
                    authentication-policy "authentication-1"
                    sap 1/1/1:1 create
                        anti-spoof ip-mac
                        sub-sla-mgmt
                            sub-ident-policy "sub-id-default"
                            no shutdown
                        exit
                    exit
                    arp-host
                        no shutdown
                    exit
                exit
```

RADIUS User Configuration Bridged/Routed CO

The username in the RADIUS access request is always the static configured IP address from the CPE and configured as key in the RADIUS users file. The RADIUS Framed-Route attribute is not required and is silently ignored (if returned to BSA/BSR node).

```
"10.1.0.1"        Auth-Type := Local, User-Password == ALU
                  Alc-Subsc-ID-Str = "arp-host-routed-%{User-name}",
                  Alc-Subsc-Prof-Str = "sub-profile-1",
                  Alc-SLA-Prof-Str = "sla-profile-1"

"10.2.0.1"        Auth-Type := Local, User-Password == ALU
                  Alc-Subsc-ID-Str = "arp-host-bridged-%{User-name}",
                  Alc-Subsc-Prof-Str = "sub-profile-1",
                  Alc-SLA-Prof-Str = "sla-profile-1"
```

Setup and Debugging of ARP Host

Identical methodologies, for bridged or Routed CO, are used to debug/setup and troubleshoot ARP hosts. Routed CO is used as an example through the rest of this section on ARP hosts.

There are two modes of ARP host debugging: all and dropped-only. The dropped-only mode shows all cases where the creation of the ARP host will be unsuccessful.

By default all ARP hosts enabled under a service will be monitored. More specific filtering on a particular IP, MAC or SAP is optional.

All main traps are by default cyclic logged in log-id 99 and can be viewed anytime.

```
debug service id 1 arp-host mode all
```

ARP host mandate RADIUS authentication and a separate debug option is available for RADIUS interaction.

```
debug radius detail
```

CPE-3 with static configured IP1 10.1.0.1 sends an ARP to the BSR-1 gateway.

```
2009/11/27 11:48:23.36 CET MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Access-Request
  user 10.1.0.1  policy authentication-1"

13 2009/11/27 11:48:23.35 CET MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Transmit
  Access-Request(1) 172.16.1.1:1812 id 10  len 79
    USER NAME [1] 8 10.1.0.1                        # Always IP-address
    PASSWORD [2] 16 2/kDsiOVlrs2FQHK4PR47E
    NAS IP ADDRESS [4] 4 192.0.2.2
```

```
      VSA [26] 19 Alcatel(6527)
        CHADDR [27] 17 00:00:0a:01:00:01                # Always included

2009/11/27 11:48:23.48 CET MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Receive
  Access-Accept(2) id 10  len 87 from 172.16.1.1:1812
    VSA [26] 19 Alcatel(6527)
      SUBSC ID STR [11] 17 arp-host-routed-10.1.0.1
    VSA [26] 15 Alcatel(6527)
      SUBSC PROF STR [12] 13 sub-profile-1
    VSA [26] 15 Alcatel(6527)
      SLA PROF STR [13] 13 sla-profile-1

2009/11/27 11:48:23.48 CET MINOR: DEBUG #2001 vprn1 ARP Host
"ARP Host: Created ARP host
  VPRN 1, SAP 1/1/1:1

  IP: 10.1.0.1
  MAC: 00:00:0a:01:00:01

2009/11/27 11:48:23.48 CET WARNING: SVCMGR #2500 Base Subscriber created
"Subscriber arp-host-routed-10.1.0.1 has been created in the system"
```

The user name in the RADIUS access-request contains the CPE's IP address independent from the user-name-format defined in authentication policy. The MAC address of the ARP host is included in the RADIUS access-request as VSA (Alc-Client-Hardware-Addr) independent on the include-radius-attribute mac-address parameter from the authentication policy.

The **show service id 1 arp-host** command displays all active ARP hosts on this service.

```
A:BSR-1# show service id 1 arp-host
===============================================================================
ARP host table, service 1
===============================================================================
IP Address      Mac Address      Sap Id             Remaining        MC
                                                    Time             Stdby
-------------------------------------------------------------------------------
10.1.0.1        00:00:0a:01:00:01 1/1/1:1           03h59m59s
-------------------------------------------------------------------------------
Number of ARP hosts: 1
```

More specific filters such as **sap**, **ip-address**, **mac** and others can be used to show dedicated ARP hosts created on the BSR.

```
A:BSR-1# show service id  1 arp-host ip-address 10.1.0.1 detail
===============================================================================
ARP hosts for service 1
===============================================================================
Service ID          : 1
IP Address          : 10.1.0.1
MAC Address         : 00:00:0a:01:00:01
Subscriber-interface : sub-int-1
Group-interface     : group-int-1
SAP                 : 1/1/1:1
Remaining Time      : 03h44m05s

Sub-Ident           : "arp-host-routed-10.1.0.1"
```

```
Sub-Profile-String   : "sub-profile-1"
SLA-Profile-String   : "sla-profile-1"
-snip-
RADIUS-User-Name     : "10.1.0.1"

Session Timeout (s)  : 14400
Start Time           : 11/27/2009 11:48:23
Last Auth            : 11/27/2009 11:48:23
Last Refresh         : 11/27/2009 11:48:23
Persistence Key      : N/A
-------------------------------------------------------------------------------
Number of ARP hosts : 1
```

Dynamic created ARP hosts are added as /32 addresses in the routing table marked with protocol type Sub Mgmt. Routes with this protocol type are not exported into vpn-ipv4 by the default vrf-target policy. A separate vrf-export policy is required to achieve this.

```
A:BSR-1# show router 1 route-table 10.1.0.0/24 longer
===============================================================================
Route Table (Service: 1)
===============================================================================
Dest Prefix                              Type    Proto    Age         Pref
      Next Hop[Interface Name]                                 Metric
-------------------------------------------------------------------------------
10.1.0.0/29                              Local   Local    02d01h32m   0
      sub-int-1                                                 0
10.1.0.1/32                              Remote  Sub Mgmt 00h00m05s   0
      [group-int-1]                                             0
```

Specific ARP host counters can be shown or cleared using the CLI command **show/clear service id 1 ARP host statistics**.

```
A:BSR-1# show service id  1 arp-host statistics
===============================================================================
ARP host statistics
===============================================================================
Num Active Hosts           : 1
Received Triggers          : 1
Ignored Triggers           : 0
SHCV Checks Forced         : 0
Hosts Created              : 1
Hosts Updated              : 0
Hosts Deleted              : 0
```

The ARP hosts mandate Enhanced Subscriber managed (ESM) and therefore an anti-spoofing configuration (IP-MAC or NH-MAC). The anti-spoofing table with active hosts can be viewed with the command **show service id 1 subscriber-hosts**.

```
A:BSR-1# show service id  1 subscriber-hosts
===============================================================================
Subscriber Host table
===============================================================================
Sap               IP Address     MAC Address      PPPoE-SID Origin
  Subscriber
-------------------------------------------------------------------------------
```

```
1/1/1:1                  10.1.0.1        00:00:0a:01:00:01 N/A       ARP-Host
  arp-host-routed-10.1.0.1
-------------------------------------------------------------------------------
Number of subscriber hosts : 1
```

An ARP host can be manually deleted from the system using one of the two following methods:

- **clear service id 1 arp-host**
- RADIUS disconnect message

Using the first method, **clear service id 1 arp-host** and omitting any more specific parameter than ARP host will result in the removal of all ARP hosts in this service. Extra filters like **ip-address**, **mac** or **sap-id** are used to remove a specific ARP host.

```
A:BSR-1# *A:BSR-1# clear service id  1 arp-host ?
- arp-host
  - arp-host { mac <ieee-address> | sap <sap-id> | ip-address
    <ip-address[/mask]> }
  - arp-host [port <port-id>] [inter-dest-id <intermediate-destination-id> |
    no-inter-dest-id]

A:BSR-1# *A:BSR-1# clear service id  1 arp-host ip-address 10.1.0.1
```

Using the second method, RADIUS disconnect always result in the removal of a unique host because **nas-port-id** and **framed-ip-address** are mandatory parameters in the RADIUS disconnect message. This RADIUS disconnect message is used also for other host-types.

```
nas-port-id = 1/1/1:1
framed-ip-address=10.1.0.1
```

RADIUS disconnect messages are, for security reasons, rejected by default and are allowed iso enabled by setting **accept-authorization-change** parameter in the authentication policy. The **debug radius detail** command and **show subscriber-mgmt authentication coa-statistics** can be used during troubleshooting.

```
7 2009/12/05 06:51:35.49 CET MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Receive
  Disconnect Request(40) id 140  len 35 from 172.16.1.1
    NAS PORT ID [87] 7 1/1/1:1
    FRAMED IP ADDRESS [8] 4 10.1.0.1
"
8 2009/12/05 06:51:35.49 CET MINOR: DEBUG #2001 vprn1 ARP Host
"ARP Host: Removed ARP host
  VPRN 1, SAP 1/1/1:1

  IP: 10.1.0.1
  MAC: 00:00:0a:01:00:01
"

9 2009/12/05 06:51:35.49 CET MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Transmit
  Disconnect Ack(41) 172.16.1.1:32769 id 140  len 20
```

In both cases the ARP host with an IP address is removed from the system and all related state (such as an anti-spoof filter and an IP ARP entry).

ARP Host Session Timeout

The ARP host session timeout is a time value between 300 and 14400 seconds and becomes the remaining time on the moment the first ARP request results in a successful host creation.

The host is removed from the system on the moment the remaining time becomes zero. The reset of remaining time to session timeout is done by any subsequent arp-request or arp-reply for this host.

The default assigned session timeout on ARP host creation time is 14400 seconds but this value can be overruled by the optional RADIUS attribute session-Timeout and not by the node group-interface arp-timeout parameter.

RADIUS values lower than 300 seconds will be silently adjusted to 300 seconds and values above 14400 seconds are topped silently to 14400 seconds.

```
"10.1.0.1"          Auth-Type := Local, User-Password == ALU
                    Alc-Subsc-ID-Str = "arp-host-routed-%{User-name}",
                    Alc-Subsc-Prof-Str = "sub-profile-1",
                    Alc-SLA-Prof-Str = "sla-profile-1",
                    Session-Timeout = 900        # value in seconds

A:BSR-1# show service id 1 arp-host
===============================================================================
ARP host table, service 1
===============================================================================
IP Address      Mac Address      Sap Id              Remaining        MC
                                                     Time             Stdby
-------------------------------------------------------------------------------
10.1.0.1        00:00:0a:01:00:01 1/1/1:1            0h14m59s
-------------------------------------------------------------------------------
Number of ARP hosts: 1

A:BSR-1# show service id  1 arp-host detail
===============================================================================
ARP hosts for service 1
===============================================================================
Service ID         : 1
IP Address         : 10.1.0.1
MAC Address        : 00:00:0a:01:00:01
Subscriber-interface : sub-int-1
Group-interface    : group-int-1
SAP                : 1/1/1:1
Remaining Time     : 0h14m59s

--snip--

Session Timeout (s) : 900
Start Time         : 12/05/2009 07:36:15
Last Auth          : 12/05/2009 07:36:15
Last Refresh       : 12/05/2009 07:40:15
Persistence Key    : N/A
-------------------------------------------------------------------------------
Number of ARP hosts : 1
```

Typical time related parameters of the ARP host are:

Table 19: ARP Host Time-Related Parameters

Parameter	Comment
Session Timeout	Time value in seconds and retrieved by default or by the RADIUS Accept message and pasted into the remaining time on moment of ARP host creation or RADIUS re-authentication.
Remaining Time	The remaining time before the ARP host is deleted from the system (updated each time an arp request/reply is seen for this host).
Start Time	Time and date when this host was created (first ARP received).
Last Auth	Time and date when this host was last RADIUS authenticated.
Last Refresh	Time and date when last ARP was received for this host.

ARP hosts do not have an expiry timer in the ARP table and have type **managed**.

```
A:BSR-1# show service  id 1 arp 10.1.0.1
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address       Type    Expiry    Interface        SAP
-------------------------------------------------------------------------------
10.1.0.1        00:00:0a:01:00:01 Managed 00h00m00s group-int-1       1/1/1:1
```

An automatic mechanism is foreseen to handle the possible asynchrony between the arp session timeout values installed on the BSR and the arp timeouts installed on the CPE. This mechanism is mostly effective in case the timeout on the CPE > timeout BSR. In this latter case, the BSR session would expire resulting in a host removal with a delete of the corresponding anti-spoof entry because the CPE ARP request is coming too late. This CPE ARP request will however recreate the session but requires the complete setup of the host RADIUS authentication included. This mechanism causes unwanted service interruption for this ARP host.

A better approach, which is implemented in an automatic way, and illustrated in Figure 307 is an ARP request triggered from the BSR towards the CPE prior to the session timeout. A CPE ARP reply will then reset the remaining lifetime of the ARP host to the session timeout. If the ARP reply is received outside the **min-auth-interval** window and the parameter re-authentication from the authentication policy is set, than RADIUS re-authentication is executed. This re-authentication mechanism is described further in the throttling toward the RADIUS section.
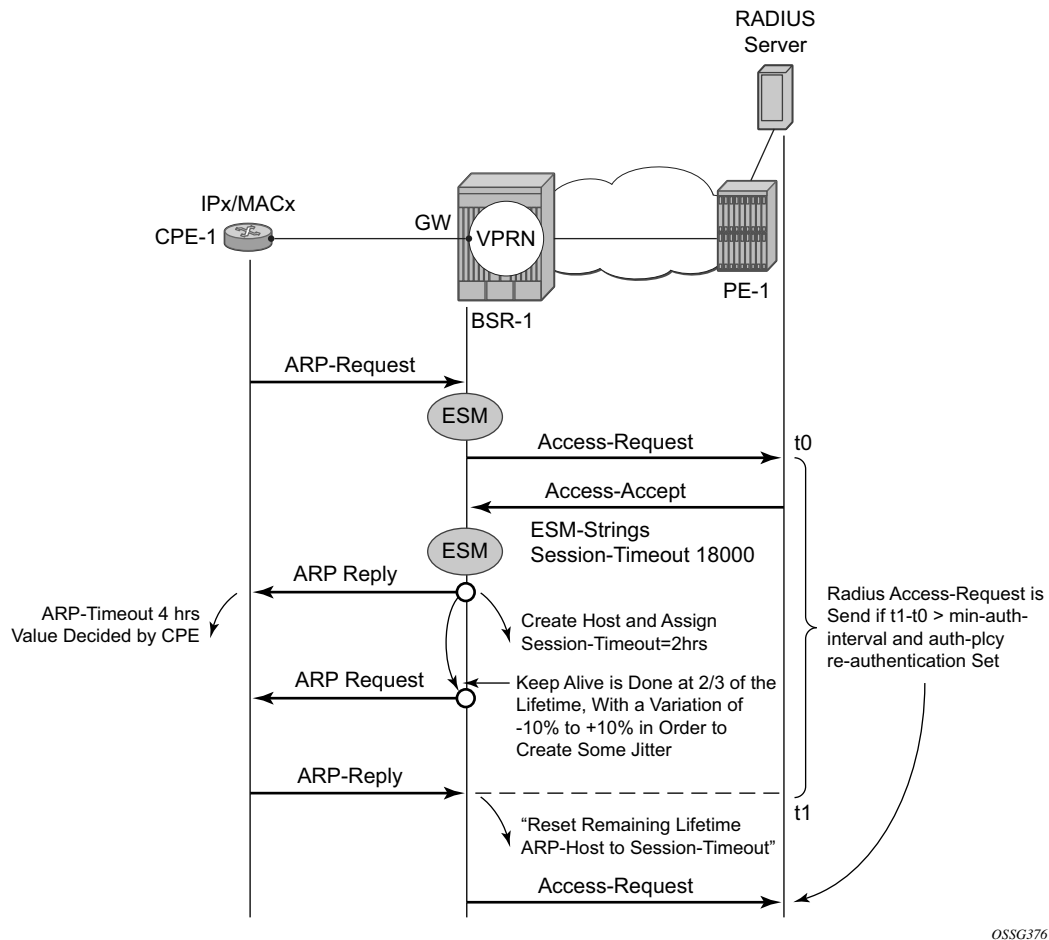
OSSG376

Figure 307: ARP Host Session Timeout Example

This mechanism, also known as automatic Subscriber Host Connectivity Verification (SHCV), will prevent that the host will be deleted and re-created, resulting in undesired service interruptions, in case asynchronous CPE-BSR arp session values would be used.

The **debug service id 1 host-connectivity-verify** command shows the sequence of events and can be used during troubleshooting. Debugging and ARP host counters show below the automatic SHCV mechanism with an active CPE.

```
3 2009/11/28 20:14:08.23 CET MINOR: DEBUG #2001 vprn1 SHCV
"SHCV: Forced Check Scheduled
   VPRN 1, SAP 1/1/1:1
   ARP host 10.1.0.1 00:00:0a:01:00:01"

4 2009/11/28 20:14:08.23 CET MINOR: DEBUG #2001 vprn1 SHCV
"SHCV: Periodic Check
   VPRN 1, SAP 1/1/1:1
```

```
    ARP host 10.1.0.1 00:00:0a:01:00:01"

5 2009/11/28 20:14:08.23 CET MINOR: DEBUG #2001 vprn1 SHCV
"SHCV: Received Reply
    VPRN 1, SAP 1/1/1:1
    ARP host 10.1.0.1 00:00:0a:01:00:01"

6 2009/11/28 20:14:08.23 CET MINOR: DEBUG #2001 vprn1 ARP Host
"ARP Host: Updated ARP host
    VPRN 1, SAP 1/1/1:1

    IP: 10.1.0.1
    MAC: 00:00:0a:01:00:01


A:BSR-1# show service id  1 arp-host statistics
===============================================================================
ARP host statistics
===============================================================================
Num Active Hosts          : 1
Received Triggers         : 2    # arp reply received from host(2)
Ignored Triggers          : 0
SHCV Checks Forced        : 1    # arp request send to arp-host(1)
Hosts Created             : 1
Hosts Updated             : 1    # session-timeout updated (3)
Hosts Deleted             : 0
```

CPEs that are not active and therefore do not respond on arp-requests as part of the automatic SHCV check will be rechecked three times with 10 second intervals.

The number of retries and the interval cannot be changed. A trap is generated but the ARP host is not removed and will remain until the session-timeout expires or until the host will revive. This mechanism is displayed in Figure 308.
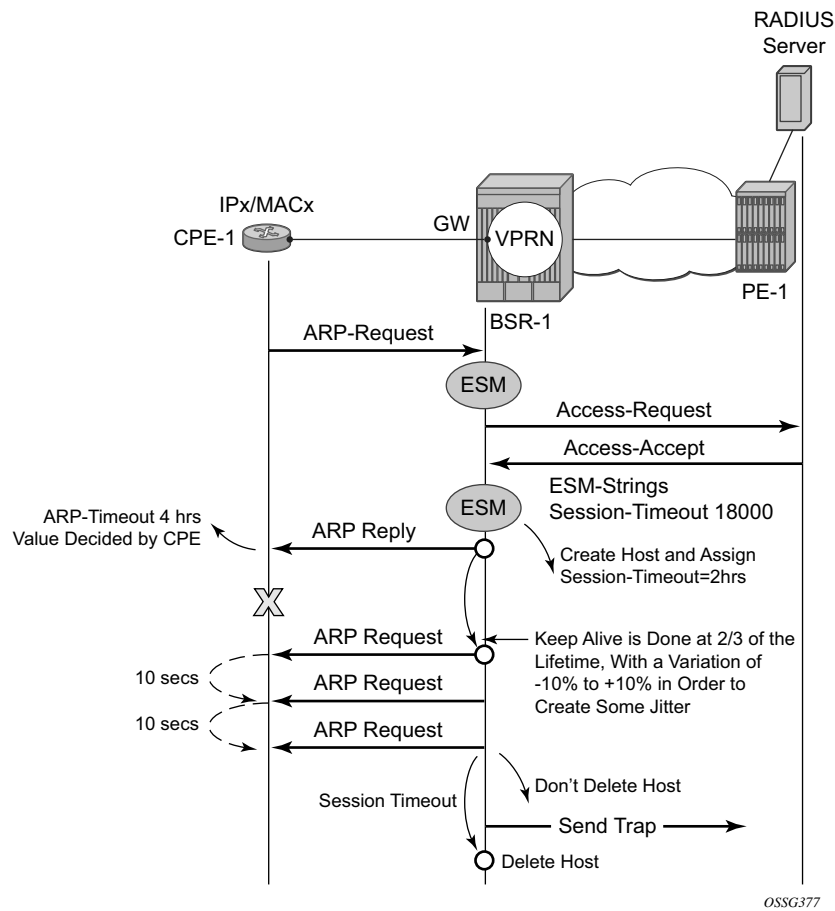
Figure 308: Trap Generation Example

```
8 2009/11/28 20:29:28.34 CET MINOR: DEBUG #2001 vprn1 SHCV
"SHCV: Forced Check Scheduled
   VPRN 1, SAP 1/1/1:1
   ARP host 10.1.0.1 00:00:0a:01:00:01"

29 2009/11/28 20:29:28.34 CET MINOR: DEBUG #2001 vprn1 SHCV
"SHCV: Periodic Check
   VPRN 1, SAP 1/1/1:1
   ARP host 10.1.0.1 00:00:0a:01:00:01"

30 2009/11/28 20:29:38.30 CET MINOR: DEBUG #2001 vprn1 SHCV
"SHCV: Periodic Check
   VPRN 1, SAP 1/1/1:1
   ARP host 10.1.0.1 00:00:0a:01:00:01"

31 2009/11/28 20:29:48.30 CET MINOR: DEBUG #2001 vprn1 SHCV
"SHCV: Periodic Check
   VPRN 1, SAP 1/1/1:1
```

```
      ARP host 10.1.0.1 00:00:0a:01:00:01"

32 2009/11/28 20:29:58.30 CET WARNING: SVCMGR #2206 vprn1 Host connectivity lost
"host connectivity lost on 1/1/1:1 in service 1 for inetAddr = 10.1.0.1, chAddr=
00:00:0a:01:00:01."

33 2009/11/28 20:29:58.30 CET MINOR: DEBUG #2001 vprn1 SHCV
"SHCV: Connectivity Lost
   VPRN 1, SAP 1/1/1:1
   ARP host 10.1.0.1 00:00:0a:01:00:01"configure
```

Throttling Toward RADIUS

A new arp-request from the ARP host will trigger RADIUS re-authentication only when the min-auth-interval is expired. The minimum RADIUS authentication interval between two consecutive authentication attempts for the same ARP host is by default 15 minutes but can range between 1 and 6000 minutes.

```
configure
    service
        vprn 1 customer 1 create
            --snip--
                arp-host
                    min-auth-interval 60   # value in minutes
                    no shutdown
                  exit
                exit
```
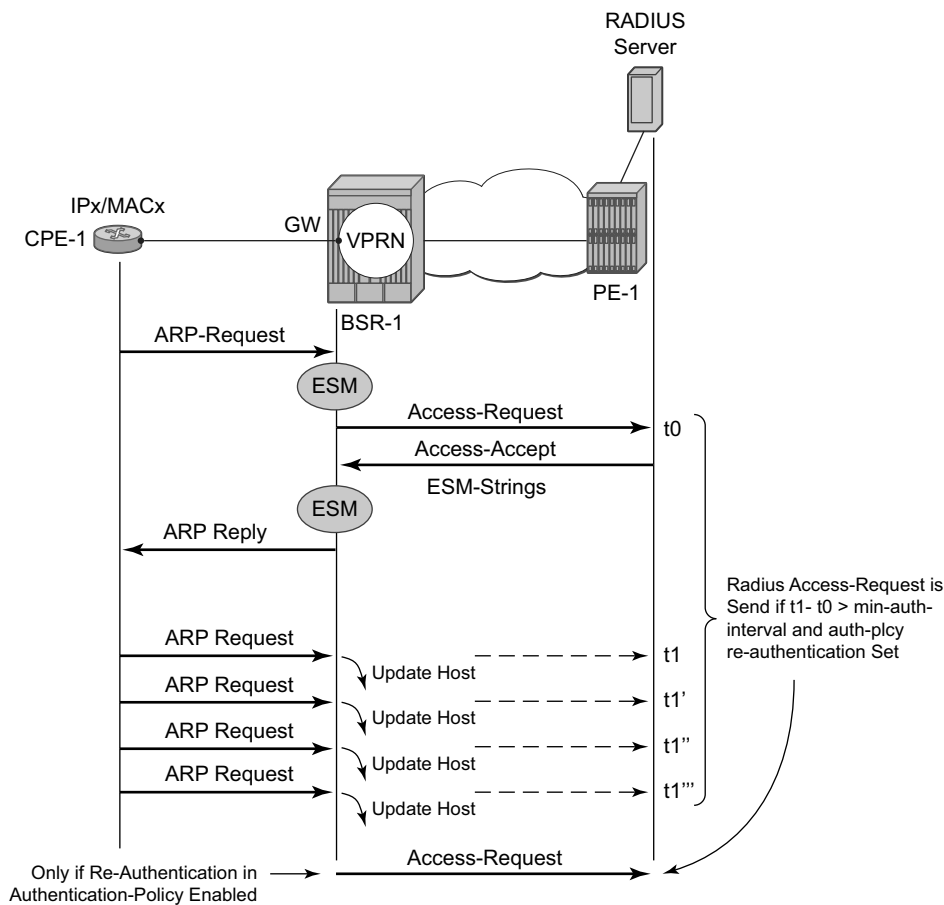

Figure 309: Throttling Toward RADIUS Example

```
A:BSR-1# show service id  1 arp-host detail
===============================================================================
ARP hosts for service 1
===============================================================================
Service ID      : 1
IP Address      : 10.1.0.1
MAC Address     : 00:00:0a:01:00:01

--snip--
Session Timeout : 14400
Start Time      : 11/27/2009 14:05:07    # Timestamp □arp-host created (first arp)
Last Auth       : 11/27/2009 14:05:07    # Timestamp □arp-host authenticated (RADIUS)
Last Refresh    : 11/27/2009 14:40:31    # Timestamp □new arp seen from arp-host
```

ARP Host Mobility

In order for ARP host mobility to function, host-connectivity-verification must **not** be enabled. This is different compared to DHCP host mobility.

The implementation for routed CO is displayed in Figure 310 and works the same for bridged CO. The **mac-pinning** command in routed CO context has no influence on this behavior.

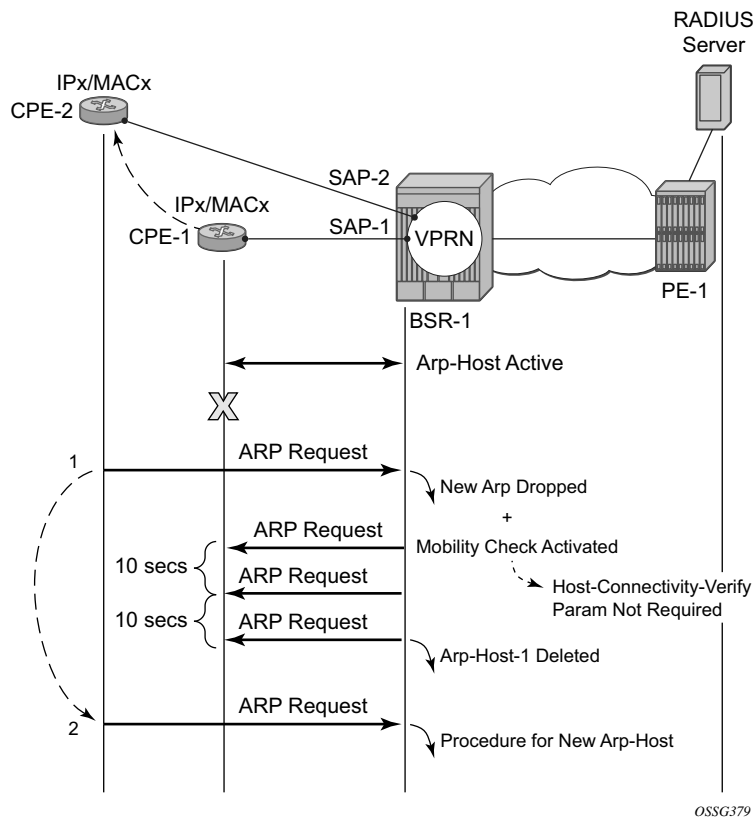**Figure 310: ARP Host Mobility Example**

ARP Host Persistency

ARP hosts can be made persistent across reboots and do not differ with other host types like DHCP hosts.

```
configure system
       persistence
             subscriber-mgmt
                  location cf2:
             exit
       exit
```

The persistence key and the index into the persistency file are linked to the arp-host on host creation time.

```
A:BSR-1# show service id  1 arp-host detail
===============================================================================
ARP hosts for service 1
===============================================================================
Service ID          : 1
IP Address          : 10.1.0.1
MAC Address         : 00:00:0a:01:00:01
--snip--
Persistence Key     : 0x00000004
```

The content of the stored record is viewed with the tools dump persistency command using the persistency key as a record number.

```
A:BSR-1# tools dump persistence submgt record 0x00000004
-----------------------------------
Persistency File Record
-----------------------------------
Filename    : cf2:\submgmt.005
Key         : 00000004
Last Update : 2009/11/27 13:05:07 (UTC)
Action      : ADD
Data :
 Host Type      : ARP host
 Service ID     : 1
 SAP ID         : 1/1/1:1
 IP             : 10.1.0.1
 NH MAC         : 00:00:0a:01:00:01
 Created        : 2009/11/27 13:05:07 (UTC)
 Session Timeout: 14400 (seconds)
 Sub-ID         : arp-host-routed-10.1.0.1
 Sub-prof-ID    : sub-profile-1
 SLA-prof-ID    : sla-profile-1
 App-prof-ID    : NULL
 ANCP-Str       : NULL
 Int-dest-ID    : NULL
 Cat-map-str    : NULL
 Sub-Id is def  : NO
 MSap SvcId     : 0
 MSap PolicyId  : 0
 MSap IfIndex   : 0
 Managed routes : None
```

```
BgpPrngPlcyAttr: None
Class Attr     : 1 bytes
RADIUS Username: 10.1.0.1
```

Session Limitation Options

The maximum number of allowed arp-hosts in a bridged CO model can be configured by the per SAP parameter host-limit in the range of 1 to 32767.

```
configure
    service
        vpls 2
          --snip
          sap 1/1/3:1
                arp-host
                    host-limit 1            # default value 1
                    no shutdown
                  exit
              exit
               exit
```

The maximum number of allowed arp-hosts in a routed CO model can be configured by the per group interface parameter host-limit in the range of 1 to 32767 and/or by the **sap-host-limit** parameter.

```
configure
    service
        vprn 1
          --snip--
                arp-host
                    host-limit 1           # default value
                    sap-host-limit 1       # default value
                    no shutdown
                  exit
              exit
```

Warning:

• Specific ESM-related host limit mechanisms such as **sla-profile host-limit** and **sub-sla-mgmt multi-sub-sap** apply also for ARP hosts but are not further elaborated in this section.

Debugging **arp-host mode dropped-only** indicates the dropped reason and a logging trap is included in the standard log 99.

```
2009/11/27 20:45:53.80 CET MINOR: DEBUG #2001 vprn1 ARP Host
"ARP Host: Dropped trigger
  VPRN 1, SAP 1/1/1:1

  Problem: Interface limit (1) of ARP hosts reached

  IP: 10.1.0.2
  MAC: 00:00:0a:01:00:02


2009/11/27 20:45:53.81 CET WARNING: SVCMGR #2520 vprn1 ARP Host Population Error
"ARP host table population error on SAP 1/1/1:1 in service 1 - Interface limit (
1) of ARP hosts reached"
```

Increasing the **sap-host-limit** to 100 and the host-limit to 2000 results in the following summary:

```
A:BSR-1# show service id  1 arp-host summary
===================================================================
ARP host Summary, service 1
===================================================================
Interface Name                   Used     Provided  Admin State
  Sap
-------------------------------------------------------------------
group-int-1                      2        2000      inService
  1/1/1:1                        2        100
-------------------------------------------------------------------
Interfaces: 1
```

Conclusion

This note provides configuration and troubleshooting commands for dynamic ARP hosts. ARP hosts can be instantiated in a Layer 2 bridged CO (VPLS) environment as well as in a Layer 3 Routed CO (IES/VPRN subscriber interface) context.