IPv4 DHCP Hosts

In This Chapter

This section provides information about IPv4 DHCP host configurations.

Topics in this section include:

Applicability

This section is applicable to the 7450 ESS, 7750 SR and 7710 SR series and was tested on SR-OS 7.0 R6. The 7750 SR-c4 is supported from 8.0R4 and higher. This note is related only to the use of IPv4.

For Bridged CO, configuration and troubleshooting commands are taken from a 7450 ESS (typically positioned as BSA); this functionality is also available on 7750 SR and 7710 SR.

For Routed CO, configuration and troubleshooting commands are taken from a 7750 SR; this functionality is also available on 7710 SR. Routed CO is supported on 7450 ESS-7 or ESS-12 in mixed-mode since 8.0R1.

Summary

In the Triple Play Service Delivery Architecture (TPSDA), a subscriber is defined as a collection of hosts pertaining to a single access connection (such as a DSL line) and identified by a subscriber identifier. A subscriber host is an end user terminal within the subscriber home (for example, a PC, set-top box, home gateway) that is identified in the network with a unique (IP address; MAC address) tuple for IPoE or (PPPoE session ID; MAC address) tuple for PPPoE.

Following host types are distinguished:

- Static hosts
  - → ip-mac
  - → ip-only
- Dynamic hosts
  - → ARP-host
  - → DHCP-host
  - → PPPoE-host

This section provides configuration and troubleshooting commands for DHCP-hosts.

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

Overview

The network topology for a Bridged CO environment is displayed in Figure 320 and for a Routed CO environment in Figure 321.

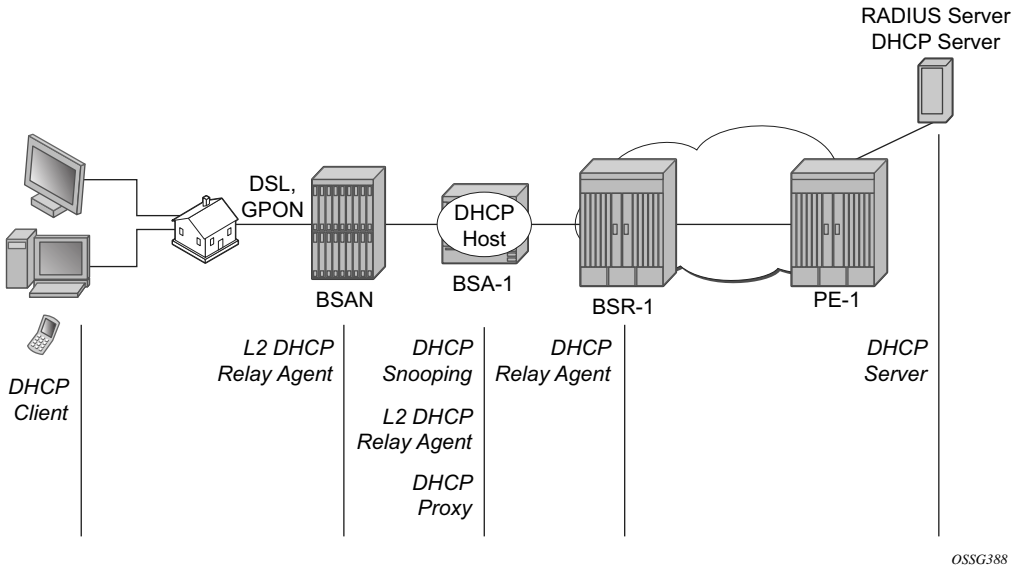

Figure 320: Bridged CO Network Topology

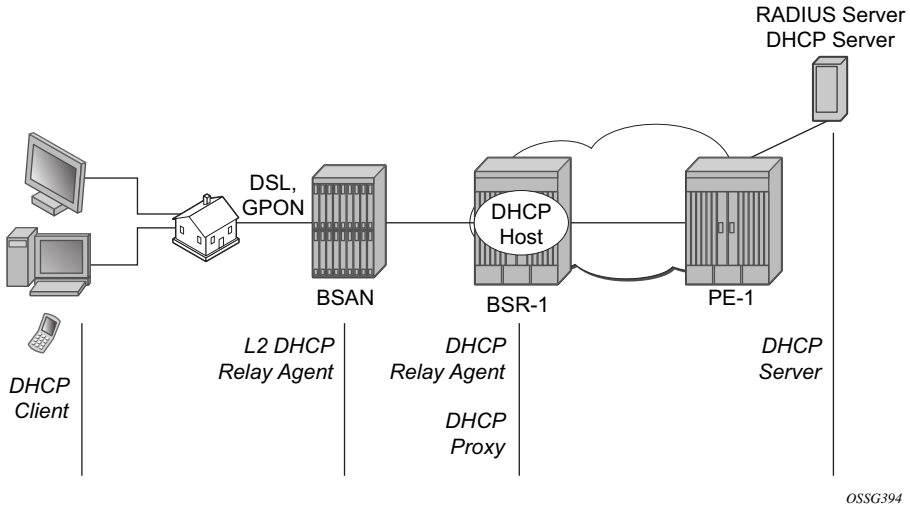

Figure 321: Routed CO Network Topology

Following configuration tasks should be done first and are not detailed in this configuration note:

- Basic service router configurations such as system interface, IGP, MPLS, BGP.
- Bridged CO service topology: VPLS on BSA-1, terminated in a VPRN or IES service on BSR-1.
- Routed CO service topology: VPRN or IES service with subscriber and group interface on BSR-1.
- External DHCP server: Server configuration and connectivity in the VPRN or base router instance.
- External RADIUS server: server configuration and connectivity in the VPRN or base router instance (Enhanced Subscriber Management (ESM) only).

This section focuses on DHCP hosts instantiated in a VPLS service on BSA-1 (Bridged CO) or in a VPRN service subscriber interface on BSR-1 (Routed CO). Note that in case of Routed CO, it is also possible to instantiate the DHCP hosts in the base routing instance using an IES service.

Most of the DHCP host functionality is available with Basic Subscriber Management (BSM). When ESM is required, it is explicitly stated in the section.

Review of the DHCP Protocol

The DHCP protocol is used by a DHCP server to dynamically assign IP addresses and other optional configuration parameters to DHCP clients. These parameters are leased by the DHCP server for a duration specified by the lease time.

The DHCP lease process is outlined in Figure 322.

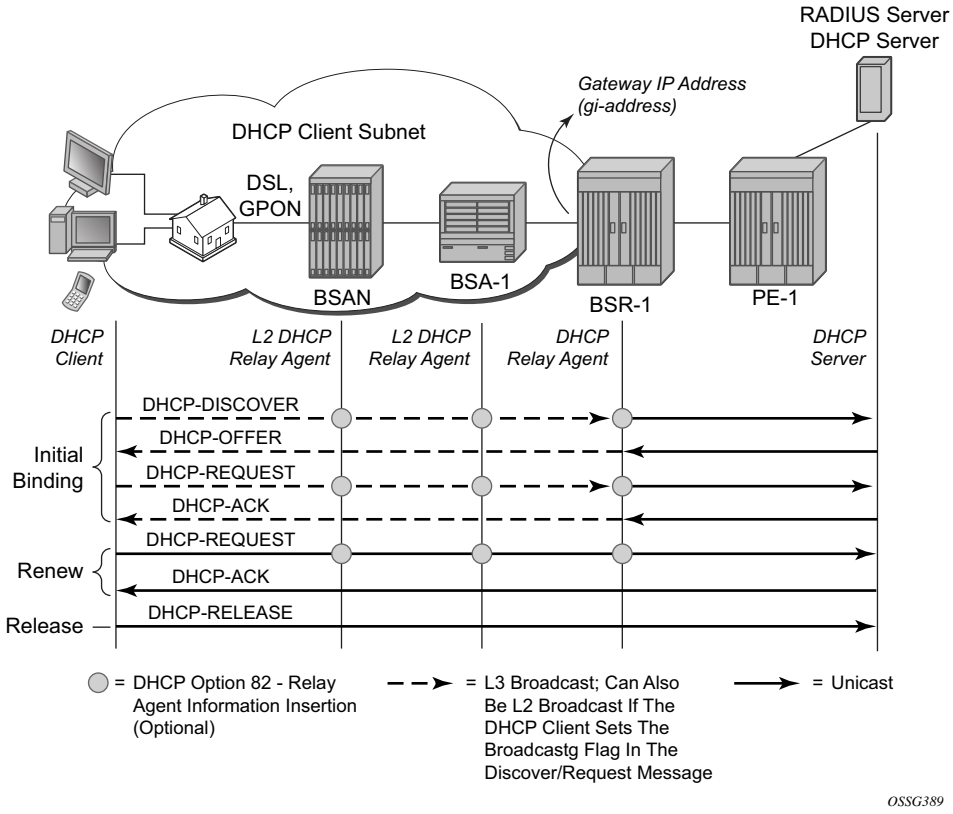

Figure 322: DHCP Lease Process

When a DHCP client boots, a DHCP discover message is broadcasted on the local subnet (dest-ip = 255.255.255.255).

A DHCP server in the local subnet responds with a unicast DHCP offer message containing the *your ip address* field as well as other configuration parameters in the option fields (such as subnet mask, default gateway, DNS server IP addresses, lease time, etc.).

The DHCP client responds with a DHCP request message to accept the parameters specified in the DHCP offer. The DHCP request is also broadcasted on the local subnet.

The DHCP server acknowledges the DHCP request with a unicast DHCP ack message.

When the DHCP client receives a DHCP ack from the server, it is said to be in the bound state.

When half of the lease time has expired, the DHCP client tries to renew the lease. It will send a unicast DHCP request message to the DHCP server. The DHCP server will reply to the request with a unicast DHCP ack to the client.

If the renew failed, a rebind is attempted by default at 7/8 of the lease time. It will send a broadcast DHCP request message.

Before disconnecting from the local subnet, a DHCP client may return its lease by sending a DHCP release message to the DHCP server.

In case there is no DHCP server in the subnet of the DHCP client, a DHCP relay agent is needed to forward the broadcast DHCP discover/request messages on behalf of the DHCP client to a DHCP server located on a different subnet. The DHCP relay agent will add the gateway IP address field to the messages and send them as unicast to the DHCP server IP address. The DHCP server in this case will respond by unicast to the DHCP relay agent. The DHCP relay agent forwards the DHCP server messages as broadcast on the DHCP client subnet.

Configuration

DHCP Snooping

DHCP client packets (discover, request, release) must be snooped (intercepted and sent to the control plane for further processing) to allow for DHCP Option 82 insertion, RADIUS or local user database authentication and releasing the DHCP host session state.

For Bridged CO, DHCP snooping must be enabled explicitly on the subscriber SAP:

```
Bridged CO
configure
    service
        vpls 1 customer 1 create
- - - snip - - -
            sap 1/1/2:1 split-horizon-group "rshg-1" create
                description "sub-1"
                dhcp
                    snoop
                    no shutdown
                exit
            exit
```

DHCP server packets (offer, ack, nak, etc.) must be snooped to allow for DHCP Option 82 removal, lease state population and/or ESM functions.

For Bridged CO, DHCP snooping must be enabled explicitly on all SDPs and/or SAPs that provide connectivity to the DHCP server:

Bridged CO:

```
configure
    service
        vpls 1 customer 1 create
- - - snip - - -
            spoke-sdp 1:1 create
                dhcp
                    snoop
                exit
            exit
```

For Routed CO, DHCP snooping is implicitly enabled by configuring a DHCP relay agent (DHCP Relay Agent on page 2039): All DHCP messages received on a routed network interface will be snooped (for example, intercepted and sent to the control plane for further processing).

DHCP Relay Agent

For Bridged CO, the DHCP relay agent function is configured at the IP edge (BSR):

Bridged CO:

```
configure
    service
        vprn 1 customer 1 create
- - - snip - - -
            interface "int-BSA1-p2mp-1" create
                description "Bridged CO"
                address 10.1.0.254/16
                dhcp
                    server 172.16.0.1
                    trusted
                    gi-address 10.1.0.254
                    no shutdown
                exit
                ip-mtu 1500
                spoke-sdp 1:1 create
                exit
            exit
```

For Routed CO, the DHCP relay agent function must be configured at BSR-1 group-interface level where the DHCP host will be instantiated:

Routed CO:

```
configure
    service
        vprn 1 customer 1 create
- - - snip - - -
            subscriber-interface "sub-int-1" create
                description "Routed CO"
                address 10.2.0.254/16
                group-interface "group-int-1" create
                    dhcp
                        server 172.16.0.1
                        trusted
                        gi-address 10.2.0.254
                        no shutdown
                    exit
```

The server IP address should point to the DHCP server and must be reachable in the same routing instance as where the (subscriber-)interface is defined.

The **trusted** command makes the interface a trusted interface to allow Option 82 insertion by a Layer 2 DHCP relay agent (see DHCP Options (Relay Agent Information) on page 2041).

The gi-address must be a local configured IP address on the (subscriber-)interface. The relayed DHCP messages to the DHCP server will have the outgoing interface IP address as source IP address. To change the default behavior and use the configured gi-address as source IP address, specify the optional **src-ip-addr** flag:

CLI Syntax: **gi-address 10.2.0.254 src-ip-addr**

A Layer 2 DHCP relay agent (such as BSAN or BSA) can add DHCP Option 82 information and leave the gi-address field to 0.0.0.0. The gi-address is the gateway IP address, filled in by the DHCP relay agent. An incoming DHCP discover with Option 82 present and gi-address field = 0.0.0.0 will be dropped by the DHCP relay agent according the RFC. The Rx Untrusted Packets and client Packets Discarded counters are increased in the DHCP statistics.

Output from DHCP debug log on BSR-1:

```
DROPPED DHCP Boot Request on Interface group-int-1 (1/1/3:1) Port 67
Problem: message is received from an untrusted client
```

Therefore, the DHCP relay agent should be configured as trusted to allow DHCP Option 82 insertion by a Layer 2 DHCP relay agent.

DHCP Options (Relay Agent Information)

In Bridged CO, when DHCP snooping is enabled on a VPLS SAP, DHCP Option 82 relay agent information can be altered or added on an incoming DHCP discover/request. This is sometimes referred to as a Layer 2 DHCP relay agent function.

In Routed CO, a DHCP relay agent can alter or add the DHCP Option 82 relay agent information on an incoming DHCP discover/request.

Supported DHCP Option 82 sub-options and their format are listed in Table 24:

Table 24: Supported DHCP Option 82 Sub-Options

Option 82 Sub-Option	Format	Example
Opt82 [1] Circuit ID (Routed CO)	ifindex — 32 bit virtual router ID followed by a 32 bit ifindex in hex	00 00 00 02 00 00 00 04
	sap-id [sap id in ascii]	1/1/3:1
	ascii3-tuple [system-name|service-id|group-interface|sap-id]	
	vlan-ascii-tuple [system-name|service-id|group-interface|dot1p|vlan-id]	“BSR-1|1|group-int-1|0|1”
Opt82 [1] Circuit ID (Bridged CO)	ascii-tuple [system-name|service-id|sap-id]	“BSA-1|1|1/1/2:1”
	vlan-ascii-tuple [system-name|service-id|sap-id |dot1p|vlan-id]	“BSA-1|1|1/1/2:1|0|1”
Opt82 [2] Remote ID (Bridged and Routed CO)	MAC [client hw address in hex]	fe fd 00 02 45 00
	string (max. 32 chars)	“Opt-82 [2] – Remote ID”
Opt82 [9] Vendor Specific (Bridged and Routed CO)	[1] system-id [hostname in ascii]	“BSA-1” or “BSR-1”
	[2] client-mac-address [client hw address in hex]	fe fd 00 02 45 00
	[3] service-id	1
	[4] sap-id [sap id in ascii]	“1/1/2:1”
	[5] string (max. 32 chars)	“Opt-82 [9] [5] – string”
Opt82 [9] Vendor Specific (Routed CO)	[13] pool-name [dhcp pool name from Radius/ Local User DB in ascii	“dhcp-pool-1”

Note: The application for Option 82 Circuit-ID format vlan-ascii-tuple is to preserve the Dot1p marking of DHCP packets in the downstream direction (DHCP server to client). The dot1p value of the incoming DHCP discover/request is recorded as part of the Option 82 Circuit ID. The outgoing DHCP offer/ack packets are marked with the Dot1p value found as part of the Circuit ID echoed by the DHCP server.

Possible actions on incoming DHCP discover/request:

- Replace:

  → At ingress:

  If present, remove all the Option 82 information from the incoming DHCP discover/request. Insert the configured DHCP options before forwarding to the DHCP relay agent or DHCP server

  → At egress:

  Remove all Option 82 information from the incoming DHCP offer/ack before forwarding to the client.

Bridged CO:

```
configure
    service
        vpls 1 customer 1 create
- - - snip - - -
            sap 1/1/2:1 split-horizon-group "rshg-1" create
                dhcp
                    snoop
                    option
                        action replace
                        circuit-id
                        remote-id string "Opt-82 [2] - Remote ID"
                        vendor-specific-option
                            system-id
                            client-mac-address
                            service-id
                            sap-id
                            string "Opt-82 [9][5] - Vendor
```

Routed CO:

```
configure
    service
        vprn 1 customer 1 create
- - - snip - - -
            subscriber-interface "sub-int-1" create
                description "Routed CO"
                address 10.2.0.254/16
                group-interface "group-int-1" create
                    dhcp
                        option
                            action replace
                            circuit-id
                            remote-id string "Opt-82 [2] Remote ID"
```

```
                vendor-specific-option
                    system-id
                    client-mac-address
                    pool-name
                    service-id
                    sap-id
                    string "Opt-82 [9][5] string"
                exit
            exit
            server 172.16.0.1
            trusted
            gi-address 10.2.0.254
            no shutdown
        exit
```

Drop:

Drop all incoming DHCP discover/request with Option 82 information present.

The Client Packets Dropped counter is increased in the DHCP statistics:

Bridged CO:

```
A:BSA-1# show service id 1 dhcp statistics
=====================================================
DHCP Statistics, service 1
=====================================================
Client Packets Snooped               : 130
Client Packets Forwarded             : 125
Client Packets Dropped               : 5
Client Packets Proxied (RADIUS)      : 0
Client Packets Proxied (Lease-Split) : 0
Server Packets Snooped               : 64
Server Packets Forwarded             : 64
Server Packets Dropped               : 0
DHCP RELEASEs Spoofed                : 0
DHCP FORCERENEWs Spoofed             : 0
=====================================================
A:BSA-1#
```

Routed CO:

```
*A:BSR-1# show router 1 dhcp statistics
```

or

```
*A:BSR-1# show service id 1 dhcp statistics
=========================================================
DHCP Global Statistics, service 1
=========================================================
Rx Packets                           : 28469
Tx Packets                           : 28402
Rx Malformed Packets                 : 0
Rx Untrusted Packets                 : 4
```

```
Client Packets Discarded             : 4
Client Packets Relayed               : 14251
Client Packets Snooped               : 12
Client Packets Proxied (RADIUS)      : 0
Client Packets Proxied (Lease-Split) : 0
Server Packets Discarded             : 0
Server Packets Relayed               : 14191
Server Packets Snooped               : 7
DHCP RELEASEs Spoofed                : 0
DHCP FORCERENEWs Spoofed             : 0
=======================================================
*A:BSR-1#
```

Output from the DHCP debug log:

Bridged CO — BSA-1 VPLS service:

```
"SVCMGR: Dropped DHCP Packet
VPLS 1, SAP 1/1/2:1
   Problem: port config doesn't allow BOOTP/DHCP packets with Option 82"
```

Routed CO BSR-1 VPRN service:

```
"PIP: DHCP
instance 2 (1), interface index 4 (group-int-1),
   DROPPED DHCP Boot Request on Interface group-int-1 (1/1/3:1) Port 67
   Problem: action drop is configured and packet contains Option 82
```

- Incoming DHCP discover/request without Option 82 information will be forwarded to (Bridged CO) or processed by (Routed CO) the DHCP relay agent as is, ignoring the configured options.

Bridged CO:

```
configure
    service
        vpls 1 customer 1 create
- - - snip - - -
            sap 1/1/2:1 split-horizon-group "rshg-1" create
                dhcp
                    snoop
                    option
                        action drop
                    exit
                    no shutdown
                exit
```

Routed CO:

```
configure
    service
        vprn 1 customer 1 create
- - - snip - - -
            subscriber-interface "sub-int-1" create
                description "Routed CO"
                address 10.2.0.254/16
                group-interface "group-int-1" create
                    dhcp
                        option
                            action drop
                        exit
                        server 172.16.0.1
                        trusted
                        gi-address 10.2.0.254
                        no shutdown
                    exit
```

Keep (default):

- At ingress – Incoming DHCP discover/request without Option 82 information will be forwarded to (Bridged CO) or processed by (Routed CO) the DHCP relay agent as is, ignoring any configured option.
- At ingress for incoming DHCP discover/request with Option 82 information present – Configured vendor specific options will be merged with the existing Option 82 information before sending to (Routed CO) or processing by (Routed CO) the DHCP relay agent. Configured Circuit ID and Remote ID options will be ignored.
- At egress — Remove Option 82 vendor specific information from the incoming DHCP offer/ack before forwarding to the client. Other existing DHCP Option 82 information is kept.

Bridged CO:

```
configure
    service
        vpls 1 customer 1 create
- - - snip - - -
            sap 1/1/2:1 split-horizon-group "rshg-1" create
                dhcp
                    snoop
                    option
                        action keep
                    exit
                    no shutdown
                exit
```

Routed CO:

```
configure
    service
        vprn 1 customer 1 create
- - - snip - - -
            subscriber-interface "sub-int-1" create
                description "Routed CO"
                address 10.2.0.254/16
                group-interface "group-int-1" create
                    dhcp
                        option
                            action keep
                        exit
                        server 172.16.0.1
                        trusted
                        gi-address 10.2.0.254
                        no shutdown
                    exit
```

DHCP Lease State

The DHCP lease state is an internal database structure that keeps track of the DHCP host states. The DHCP lease state enables subscriber management functions (per-subscriber QoS and accounting) and security functions (dynamic anti-spoof filtering) on the DHCP host.

The DHCP lease information for a specific host is extracted from the DHCP ack message. Table 25 displays some typical information stored in the DHCP lease state. The table does not display all information: additional data is added for managed SAPs, DHCPv6, etc.

Table 25: Information in DHCP Lease State

Parameter	Comment
Service ID	Service where the DHCP host is connected
IP Address	IP address of the DHCP host
Client HW Address	Ethenet MAC address of the DHCP host
Subscriber-interface (Routed CO only)	Subscriber interface name where the DHCP host is instantiated
Group-interface (Routed CO only)	Group interface name where the DHCP host is instantiated
SAP	SAP where the DHCP hosts is connected
Remaining Lifetime	The remaining time before the DHCP host is deleted from the system (updated each time a DHCP renew/rebind occurs)
Persistence Key	Lookup key for this host in the persistency file (see further)
Sub-Ident	ESM: Subscriber ID of the DHCP host
Sub-Profile-String	ESM: Subscriber profile string of the DHCP host
SLA-Profile-String	ESM: SLA profile string of the DHCP host
App-Profile-String	ESM: Application profile string of the DHCP host
Lease ANCP-String	ESM: ANCP string for this DHCP host
Lease Int Dest Id	ESM: Internal destination ID for this DHCP host
Category-Map-Name	ESM: Volume and Time based accounting
Sub-Ident origin	ESM: Origin for the Subscriber ID for this host (None, DHCP, RADIUS, etc.)
Strings origin	ESM: Origin for the ESM strings for this host (None, DHCP, RADIUS, etc.)

Table 25: Information in DHCP Lease State (Continued)

Parameter	Comment
Lease Info origin	ESM: Origin for the IP configuration for this host (None, DHCP, RADIUS, etc.)
Ip-Netmask	The IP netmask for this DHCP host
Broadcast-Ip-Addr	The broadcast IP address for this host
Default-Router	The default gateway for this host
Primary-Dns	The primary DNS server for this host
Secondary-Dns	The secondary DNS server for this host
Primary-Nbns	The primary NetBIOS name server for this host
Secondary-Nbns	The secondary NetBIOS name server for this host
ServerLeaseStart	Time and date that the lease for this host started (first DHCP ack received)
ServerLastRenew	Time and date that the lease for this host was last renewed
ServerLeaseEnd	Time and date that the lease for this host will expire
Session-Timeout	Lease time specified by the DHCP server
DHCP Server Addr	IP address of the DHCP server that allocated the lease for this host
Circuit Id	DHCP Relay Agent information Option 82 Circuit ID content
Remote Id	DHCP Relay Agent information Option 82 Remote ID content
RADIUS User-Name	ESM: Username used in the RADIUS authentication access request

For Bridged CO, the population of the DHCP lease state must be enabled through configuration. The number of leases allowed on the VPLS SAP must be specified. When omitted, a single DHCP host is allowed per SAP.

Bridged CO:

```
configure
    service
        vpls 1 customer 1 create
- - - snip - - -
            sap 1/1/2:1 split-horizon-group "rshg-1" create
                dhcp
                    snoop
                    lease-populate 10
                    no shutdown
                exit
```

For Routed CO, DHCP lease state population is enabled by default on a group interface with DHCP configured as **no shutdown** The number of leases allowed on each SAP of the group-interface must be configured (by default a single DHCP host is allowed on each SAP):

Routed CO:

```
configure
    service
        vprn 1 customer 1 create
- - - snip - - -
            subscriber-interface "sub-int-1" create
                description "Routed CO"
                address 10.2.0.254/16
                group-interface "group-int-1" create
                    dhcp
                        server 172.16.0.1
                        trusted
                        lease-populate 10
                        gi-address 10.2.0.254
                        no shutdown
                    exit
```

To check the DHCP lease state for a particular service, use the **show service id** *service-id* **dhcp lease-state** command. Detailed output as well as additional output filtering is available:

Bridged CO:

```
A:BSA-1# show service id 1 dhcp lease-state ?
  - lease-state [sap <sap-id>|sdp <sdp-id:vc-id>|interface
    <interface-name>ip-address <ip-address[/mask]>|chaddr <ieee-address>|mac
    <ieee-address>|{[port <port-id>] [no-inter-dest-id | inter-dest-id
    <inter-dest-id>]}] [detail]
```

Routed CO:

```
*A:BSR-1# show service id 1 dhcp lease-state ?
  - lease-state [wholesaler <service-id>] [sap <sap-id>|sdp <sdp-id:vc-id>|
    interface <interface-name>|ip-address <ip-address[/mask]>|chaddr
    <ieee-address>|mac <ieee-address>|{[port <port-id>] [no-inter-dest-id |
    inter-dest-id <inter-dest-id>]}] [detail]

Bridged CO
*A:BSA-1# show service id 1 dhcp lease-state detail
===============================================================================
DHCP lease states for service 1
===============================================================================
Service ID           : 1
IP Address           : 10.1.0.100
Client HW Address    : fe:fd:00:02:45:00
SAP                  : 1/1/2:1
Remaining Lifetime   : 00h09m50s
Persistence Key      : 0x00000001

Sub-Ident            : ""
Sub-Profile-String   : ""
SLA-Profile-String   : ""
App-Profile-String   : ""
Lease ANCP-String    : ""
Lease Int Dest Id    : ""
Category-Map-Name    : ""

Sub-Ident origin     : None
Strings origin       : None
Lease Info origin    : DHCP

Ip-Netmask           : 255.255.0.0
Broadcast-Ip-Addr    : N/A
Default-Router       : 10.1.0.254
Primary-Dns          : N/A
Secondary-Dns        : N/A
Primary-Nbns         : N/A
Secondary-Nbns       : N/A

ServerLeaseStart     : 11/20/2009 14:00:18
ServerLastRenew      : 11/20/2009 14:00:18
ServerLeaseEnd       : 11/20/2009 14:10:18
Session-Timeout      : 0d 00:10:00
DHCP Server Addr     : 172.16.0.1

Relay Agent Information
  Circuit Id         : BSA-1|1|1/1/2:1
  Remote Id          : Opt-82 [2] - Remote ID
Radius User-Name     : ""
-------------------------------------------------------------------------------
Number of lease states : 1
===============================================================================
*A:BSA-1#
```

Routed CO:

```
*A:BSR-1# show service id 1 dhcp lease-state detail
===============================================================================
DHCP lease states for service 1
===============================================================================
Service ID           : 1
IP Address           : 10.2.0.100
Client HW Address    : fe:fd:00:02:45:00
Subscriber-interface : sub-int-1
Group-interface      : group-int-1
SAP                  : 1/1/3:1
Remaining Lifetime   : 00h09m48s
Persistence Key      : N/A

Sub-Ident            : ""
Sub-Profile-String   : ""
SLA-Profile-String   : ""
App-Profile-String   : ""
Lease ANCP-String    : ""
Lease Int Dest Id    : ""
Category-Map-Name    : ""

Sub-Ident origin     : None
Strings origin       : None
Lease Info origin    : DHCP

Ip-Netmask           : 255.255.0.0
Broadcast-Ip-Addr    : N/A
Default-Router       : 10.2.0.254
Primary-Dns          : N/A
Secondary-Dns        : N/A
Primary-Nbns         : N/A
Secondary-Nbns       : N/A

ServerLeaseStart     : 11/26/2009 18:03:24
ServerLastRenew      : 11/26/2009 18:03:24
ServerLeaseEnd       : 11/26/2009 18:13:24
Session-Timeout      : 0d 00:10:00
DHCP Server Addr     : 172.16.0.1

Relay Agent Information
  Circuit Id         : Circuit-ID sub-1
  Remote Id          : Remote-ID sub-1
Radius User-Name     : ""
-------------------------------------------------------------------------------
Number of lease states : 1
===============================================================================
*A:BSR-1#
```

DHCP Host Session: Set-up, Operation and Release

Snooping the DHCP communication between a DHCP client and a DHCP relay agent/server facilitates the DHCP host instantiation: Upon the reception of a DHCP ack message from the server, the DHCP lease state is populated. With ESM enabled, a DHCP host is also instantiated. The DHCP host will appear in the subscriber-host table for the service with origin set to □HCP□

Bridged CO:

```
*A:BSA-1# show service id 1 subscriber-hosts
===============================================================================
Subscriber Host table
===============================================================================
Sap                    IP Address      MAC Address       PPPoE-SID Origin
  Subscriber
-------------------------------------------------------------------------------
1/1/2:1                10.1.0.100      fe:fd:00:02:45:00 N/A       DHCP
  sub-1
-------------------------------------------------------------------------------
Number of subscriber hosts : 1
===============================================================================
*A:BSA-1#
```

Routed CO

```
*A:BSR-1# show service id 1 subscriber-hosts
===============================================================================
Subscriber Host table
===============================================================================
Sap                    IP Address      MAC Address       PPPoE-SID Origin
  Subscriber                             Fwding state
-------------------------------------------------------------------------------
1/1/3:1                10.2.0.100      fe:fd:00:02:45:00 N/A       DHCP
  N/A                                    Fwding
-------------------------------------------------------------------------------
Number of subscriber hosts : 1
===============================================================================
*A:BSA-1#
```

If ESM is enabled, the subscriber-host will also appear in the active subscriber table:

Routed CO:

```
A:BSR-1# show service active-subscribers
===============================================================================
Active Subscribers
===============================================================================
-------------------------------------------------------------------------------
Subscriber sub-1 (sub-profile-1)
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
(1) SLA Profile Instance sap:1/1/3:1 - sla:sla-profile-1
-------------------------------------------------------------------------------
IP Address      MAC Address       PPPoE-SID Origin
```

```
-------------------------------------------------------
10.2.0.100      fe:fd:00:02:45:00 N/A       DHCP
-------------------------------------------------------------------------------
Number of active subscribers : 1
===============================================================================
*A:BSA-1#
```

Troubleshooting the DHCP session set-up is done with DHCP debugging:

Bridged CO:

```
*A:BSA-1# debug service id 1 dhcp ?
  - dhcp
  - no dhcp

 [no] detail-level    - Configure the DHCP tracing detail level
 [no] mac             - Show DHCP packets for a particular MAC address
 [no] mode            - Configure the DHCP tracing mode
 [no] sap             - Show DHCP packets for a particular SAP
 [no] sdp             - Show DHCP packets for a particular SDP
```

Routed CO:

```
*A:BSR-1# debug router 1 ip dhcp ?
  - dhcp [interface <ip-int-name>]
  - dhcp mac <ieee-address>
  - dhcp sap <sap-id>
  - no dhcp [interface <ip-int-name>]
  - no dhcp mac <ieee-address>
  - no dhcp sap <sap-id>
- - - snip - - -
 [no] detail-level    - Configure the DHCP tracing detail level
 [no] mode            - Configure the DHCP tracing model
```

For example:

Bridged CO:

```
*A:BSA-1# show debug
debug
    service
        id 1
            dhcp
                mode egr-ingr-and-dropped
                detail-level medium
            exit
        exit
    exit
exit
```

Routed CO:

```
*A:BSR-1# show debug
debug
    router "1"
        ip
            dhcp
                detail-level medium
                mode egr-ingr-and-dropped
            exit
        exit
    exit
exit
```

Note: The example above will log all DHCP packets on the service. When thousands of DHCP hosts are active, more granular filtering is required: for example look only to dropped packets or look only to packets from a particular MAC address.

To display the debugging information, a dedicated log should be created:

```
*A:BSA-1# configure log
*A:BSA-1>config>log# info
----------------------------------------------
        log-id 1
            description "Send debug log to the current telnet/ssh session"
            from debug-trace
            to session
        exit
----------------------------------------------
*A:BSA-1#
```

The following shows sample DHCP debug log output (detail-level medium):

Bridged CO:

```
28 2009/11/23 12:53:05.28 CET MINOR: DEBUG #2001 Base SVCMGR
"SVCMGR: TX DHCP Packet
   VPLS 1, SAP 1/1/2:1

   BootReply to UDP port 68
   ciaddr: 0.0.0.0           yiaddr: 10.1.0.100
   siaddr: 0.0.0.0           giaddr: 0.0.0.0
   chaddr: fe:fd:00:02:45:00    xid: 0x6b230c18

   DHCP options:
   [82] Relay agent information: len = 25
      [1] Circuit-id: MyCircuitID
      [2] Remote-id: MyRemoteID
   [53] Message type: Ack
   [54] DHCP server addr: 172.16.0.1
   [51] Lease time: 1200
   [1] Subnet mask: 255.255.0.0
   [3] Router: 10.1.0.254
   [255] End
"
```

During the lifetime of a DHCP host, the DHCP lease state is updated in the system: for example, the remaining lifetime after a DHCP renew. To check lease details from the DHCP host during its lifetime, consult the DHCP lease state details:

```
*A:BSA-1# show service id 1 dhcp lease-state detail
- - - snip - - -
   # see above for a sample output
```

If the remaining lifetime timer expires before the DHCP session is renewed or rebound, the DHCP lease state is cleared. If ESM is enabled, the DHCP host is removed from the system.

A DHCP host can be manually deleted from the system using following clear command:

```
*A:BSA-1# clear service id 1 dhcp lease-state ?
  - lease-state [no-dhcp-release]
  - lease-state [port <port-id>] [inter-dest-id <intermediate-destination-id>]
    [no-dhcp-release]
  - lease-state [port <port-id>] no-inter-dest-id [no-dhcp-release]
  - lease-state ip-address <ip-address[/mask]> [no-dhcp-release]
  - lease-state mac <ieee-address> [no-dhcp-release]
  - lease-state sap <sap-id> [no-dhcp-release]
  - lease-state sdp <sdp-id:vc-id> [no-dhcp-release]

*A:BSA-1# clear service id 1 dhcp lease-state ip-address 10.1.0.100
```

The DHCP lease state is deleted and all related state (such as, anti-spoof filter, ARP table entry). If ESM is enabled, the DHCP host is removed from the system. Optionally, a DHCP release is sent to the DHCP server to notify that the IP address can be released. This is reflected in the DHCP statistics in the DHCP RELEASEs Spoofed counter. Use the **no-dhcp-release** flag in the clear command if no DHCP release is to be sent when issuing the **clear** command.

To display a summary overview of the DHCP configuration on a particular service:

Bridged CO:

```
*A:BSA-1# show service id 1 dhcp summary
===============================================================================
DHCP Summary, service 1
===============================================================================
Sap/Sdp                 Snoop  Used/       Arp Reply   Info     Admin
                               Provided    Agent       Option   State
-------------------------------------------------------------------------------
sap:1/1/2:1             Yes    1/2         Yes         Keep     Up
sap:1/1/2:2             Yes    0/1         Yes         Keep     Up
sdp:1:1                 Yes    N/A         N/A         N/A      N/A
-------------------------------------------------------------------------------
Number of Entries : 3
-------------------------------------------------------------------------------
===============================================================================
*A:BSA-1#
```

Routed CO:

```
*A:BSR-1# show service id 1 dhcp summary
===============================================================================
DHCP Summary, service 1
===============================================================================
Interface Name                   Arp      Used/                Info    Admin
  SapId/Sdp                      Populate Provided             Option  State
-------------------------------------------------------------------------------
group-int-1                      No       1/2                  Keep    Up
-------------------------------------------------------------------------------
Interfaces: 2
===============================================================================
*A:BSA-1#
```

The Used/Provided field indicates the number of active versus the number of allowed DHCP leases on the SAP, SDP or interface.

To check the DHCP statistics, use the following command:

Bridged CO:

```
*A:BSA-1# show service id 1 dhcp statistics
=====================================================
DHCP Statistics, service 1
=====================================================
Client Packets Snooped               : 474
Client Packets Forwarded             : 474
Client Packets Dropped               : 0
Client Packets Proxied (RADIUS)      : 0
Client Packets Proxied (Lease-Split) : 0
Server Packets Snooped               : 472
Server Packets Forwarded             : 469
Server Packets Dropped               : 3
DHCP RELEASEs Spoofed                : 0
DHCP FORCERENEWs Spoofed             : 0
=====================================================
*A:BSA-1#
```

Routed CO:

```
*A:BSR-1# show router 1 dhcp statistics
===============================================================================
DHCP Global Statistics (Service: 1)
===============================================================================
Rx Packets                           : 28532
Tx Packets                           : 28450
Rx Malformed Packets                 : 0
Rx Untrusted Packets                 : 4
Client Packets Discarded             : 20
Client Packets Relayed               : 14259
Client Packets Snooped               : 29
Client Packets Proxied (RADIUS)      : 0
Client Packets Proxied (Lease-Split) : 0
Server Packets Discarded             : 0
Server Packets Relayed               : 14199
```

```
Server Packets Snooped               : 21
DHCP RELEASEs Spoofed                : 1
DHCP FORCERENEWs Spoofed             : 0
===============================================================
*A:BSA-1#
```

Note additional filtering can be done to retrieve DHCP statistics per SAP, SDP or interface.

To clear the DHCP statistics:

Bridged CO:

```
*A:BSA-1# clear service id 1 dhcp statistics ?
  - statistics [sap <sap-id> | sdp <sdp-id:vc-id> | interface <ip-int-name|
    ip-address>]
```

Routed CO:

```
*A:BSR-1# clear router 1 dhcp statistics
  - statistics [<ip-int-name|ip-address>]

 <ip-int-name|ip-ad*> : ip-int-name    - 32 chars max
                        ip-address     - a.b.c.d
```

DHCP Hosts Advanced Topics

High Availability

The DHCP lease state supports High Availability (HA): the lease state is synchronized to the standby CPM. When the active CPM fails, all DHCP hosts stay active without service interruption.

DHCP Lease State Persistency

A DHCP session does not have a keep-alive mechanism to detect unavailability. A new DHCP session set up is only attempted after expiration of the DHCP lease time. A node reboot causing the loss of DHCP lease state and the corresponding anti-spoof filters could therefore result in unacceptable long service outages.

The DHCP lease state can be made persistent across node reboots: DHCP lease state is restored from a persistency file stored on the compact flash file system. As a result, DHCP sessions will only loose connectivity during the time of reboot without being completely disconnected.

To activate the DHCP lease state persistency:

```
configure
    system
        persistence
            subscriber-mgmt
                description "DHCP lease state persistency"
                location cf2:
            exit
        exit
```

A dedicated persistency file will be created on the specified compact flash file system. The file is initialized to store the maximum number of allowed hosts; its size is fixed to avoid file system space problems during operations.

```
*A:BSA-1# file dir cf2:

 Volume in drive cf2 on slot A has no label.

 Volume in drive cf2 on slot A is formatted as FAT32.

Directory of cf2:\

11/23/2009  02:01p           536871424 submgmt.005
               1 File(s)              536871424 bytes.
               0 Dir(s)              1558183424 bytes free.
```

Each time a DHCP ack is received from the DHCP server, the persistency file is updated together with the lease state. If the file update fails, an event is generated to indicate that persistency can not be guaranteed.

The content of the persistency file may vary between different SR-OS software releases. When upgrading, the persistency file is automatically upgraded to the new format. To downgrade the persistency file to a lower SR-OS release version, use the following command:

```
*A:BSA-1# tools perform subscriber-mgmt downgrade ?
  - downgrade target-version <target> [reboot]

 <target>             : The version you want to downgrade to
                          7.0 (current)  - submgmt.005
                          6.0            - submgmt.004
                          5.0            - submgmt.003
                          4.0            - submgmt.pst
 <reboot>             : reboot system after successful conversion
```

The content of the persistency file can be looked at using the following command:

```
*A:BSA-1# show service id 1 dhcp lease-state sap 1/1/2:2 detail
===============================================================================
DHCP lease states for service 1
===============================================================================
Service ID           : 1
IP Address           : 10.1.0.99
Client HW Address    : fe:fd:00:02:46:00
SAP                  : 1/1/2:2
Remaining Lifetime   : 00h07m17s
Persistence Key      : 0x00000005
- - - snip - - -
===============================================================================
*A:BSA-1#


*A:BSA-1# tools dump persistence submgt record 0x00000005
-----------------------------------
Persistency File Record
-----------------------------------
Filename    : cf2:\submgmt.005
Key         : 00000005
Last Update : 2009/11/23 14:58:17 (UTC)
Action      : UPDATE
Data :
 Host Type      : DHCP lease state
 Service ID     : 1
 SAP ID         : 1/1/2:2
 IP             : 10.1.0.99
 CHADDR         : fe:fd:00:02:46:00
 NH MAC         : fe:fd:00:02:46:00
 Srvr Lse Start : 2009/11/23 14:30:02 (UTC)
 Srvr Last Renew: 2009/11/23 14:58:17 (UTC)
 Srvr Lse End   : 2009/11/23 15:08:17 (UTC)
 Srvr Addr      : 172.16.0.1
 Option82       : 10 bytes
 Option60       : 0 bytes
 Sub-ID         : NULL
```

```
 Sub-prof-ID    : NULL
 SLA-prof-ID    : NULL
 App-prof-ID    : NULL
 ANCP-Str       : NULL
 Int-dest-ID    : NULL
 Cat-map-str    : NULL
 Dhcp6 Pfx len  : 32
 Dhcp6 CfgPfxLen: 0
 Dhcp6 Client Id: NULL
 Dhcp6 Iaid     : 0
 Dhcp6 Iaid Typ : 0
 Dhcp6 Client Mg: ::
 Sub-Id is def  : NO
 MSap SvcId     : 0
 MSap PolicyId  : 0
 MSap IfIndex   : 0
 Managed routes : None
 BgpPrngPlcyAttr: None
 Class Attr     : 0 bytes
 Radius Username:
===============================================================================
*A:BSA-1#
```

Limiting the Number of DHCP Hosts

The maximum number of DHCP lease state entries for a VPLS SAP, for an IES/VPRN interface or for each SAP on an IES/VPRN group-interface is defined when enabling the lease-populate. When omitted, a single DHCP host is allowed:

```
configure
    service
        vpls 1 customer 1 create
- - - snip - - -
            sap 1/1/2:2 split-horizon-group "rshg-1" create
                dhcp
                    snoop
                    lease-populate 10
                    no shutdown
                exit
```

When trying to instantiate a new DHCP host while the configured number of leases is reached, the DHCP ack is dropped (DHCP debug log output):

```
13 2009/11/23 15:35:27.85 CET MINOR: DEBUG #2001 Base SVCMGR
"SVCMGR: Dropped DHCP Packet
   VPLS 1, SAP 1/1/2:10

   Problem: lease-populate limit (10) exceeded on SAP 1/1/2:2
- - - snip - - -
```

The following event is generated:

```
158 2009/11/23 15:35:27.86 CET WARNING: DHCP #2002 Base Maximum number of lease states*
"Lease state for (CiAddr = 10.1.0.98, ChAddr = fe:fd:00:02:47:00, leaseTime = 600) was not
stored because the number of DHCP lease states on SAP 1/1/2:2 in service 1 has reached its
upper limit"
```

With ESM enabled, the following limits also apply:

- sla-profile host-limit — This parameter defines the maximum number of dynamic subscriber hosts per subscriber for this sla-profile. Static hosts are not counted in the host-limit.

```
configure
    subscriber-mgmt
        sla-profile "sla-profile-1" create
            host-limit 2
```

If the configured host-limit is reached for a subscriber, access is denied for a new host, an event is generated and the corresponding DHCP ack message is dropped:

```
866 2009/11/25 12:04:04.42 CET WARNING: DHCP #2005 Base Lease State Population Error
"Lease state table population error on SAP 1/1/2:1 in service 1 - subscriber sub-1 sla-pro-
file sla-profile-1, host-limit (2) exceeded"
```

Note: An optional parameter **remove-oldest** can be specified behind the host-limit. In this ca se, the new host is accepted and the DHCP lease state for the oldest host (with the least remaining lease time) is cleared. A DHCP release is sent to the DHCP server.

- multi-sub-sap — This parameter defines the maximum number of subscribers (dynamic and static) that can be simultaneously active on this SAP. By default only a single subscriber is allowed (no multi-sub-sap).

Bridged CO:

```
configure
    service
        vpls 1 customer 1 create
            sap 1/1/2:1 split-horizon-group "rshg-1" create
                sub-sla-mgmt
                    multi-sub-sap 2
```

Routed CO:

```
configure
    service
        vprn 1 customer 1 create
            subscriber-interface "sub-int-1" create
                group-interface "group-int-1" create
                    sap 1/1/3:1 create
                        sub-sla-mgmt
                            multi-sub-sap 2
```

If the limit is reached, a new subscriber will be denied access, an event is generated and the corresponding DHCP ack message is dropped:

```
1404 2009/11/25 13:20:03.47 CET WARNING: DHCP #2005 Base Lease State Population Error
"Lease state table population error on SAP 1/1/2:1 in service 1 - Number of subscribers
exceeds the configured multi-sub-sap limit (2)"
```

DHCP Host Connectivity Verification

Because the DHCP protocol does not have a keep-alive mechanism and IP address renewal is not frequent enough, alternative mechanisms are needed to track reachability of DHCP hosts.

1. Subscriber Host Connectivity Verification (SHCV)

   The first alternative is called Subscriber Host Connectivity Verification (SHCV). A periodic unicast ARP is sent to the DHCP host. The connectivity test is failed:

   - If for X consecutive unicast ARP requests no ARP reply is received within the specified retry-timeout ([10 — 60] seconds, default 10). The number of retries (X-1) is specified by the retry-count ([2 — 29], default 2). Hence, the minimum 3 unicast ARP requests are send before connectivity is lost.
   - If the ARP reply contains an inconsistent IP/MAC compared with the local DHCP lease state

     For a failed connectivity test, an event is raised and optionally the DHCP lease state is removed from the system: cleaning up of all related resources (e.g. anti-spoof table) and sending a DHCP release to the DHCP server. When ESM is enabled, the DHCP host is removed as well in this case.

The interval for the periodic checks can be configured between 1 and 6000 minutes. If not specified, the default value of 10 minutes will be used.

The maximum time for DHCP host connectivity loss detection in this case is:

```
( (host-connectivity-verify interval) + ( (retry-count) * (retry-timeout) ) )
```

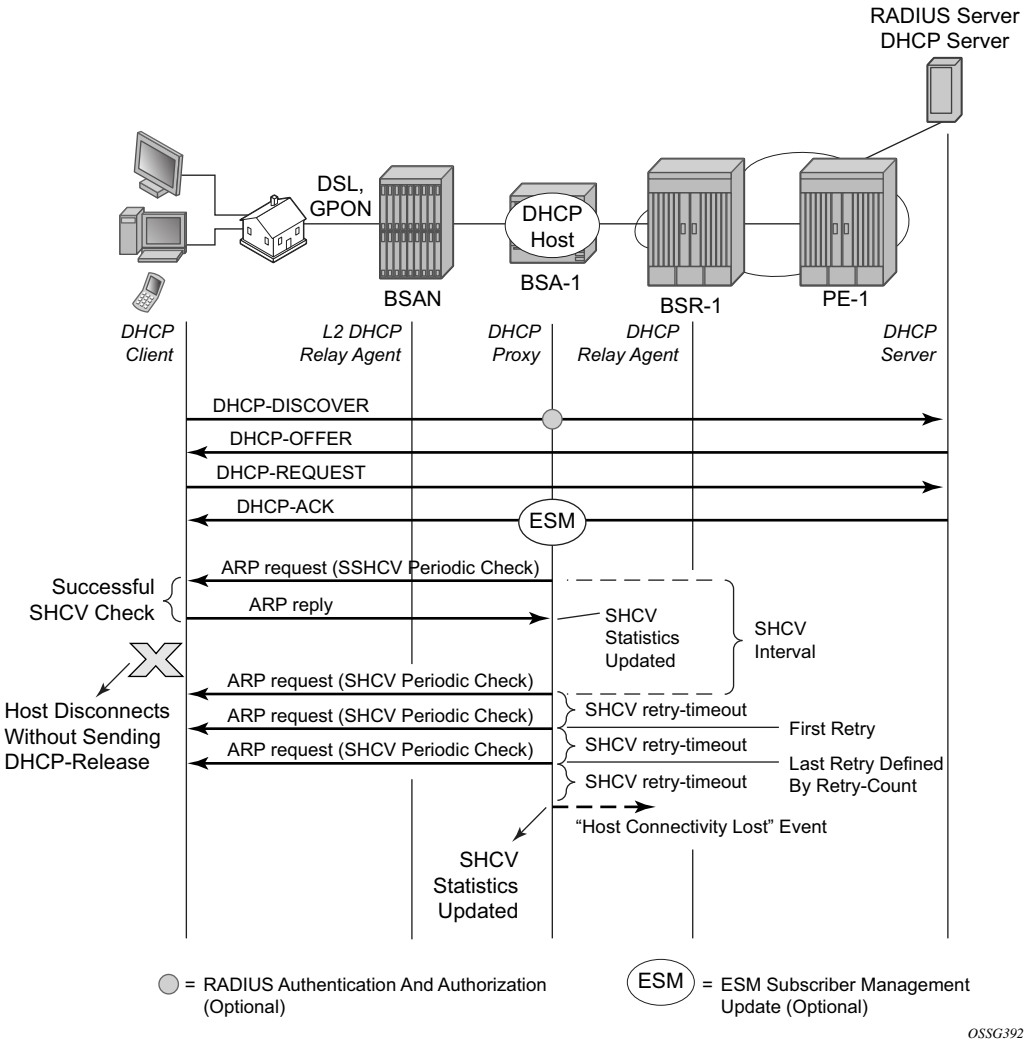

Figure 323: Subscriber Host Connectivity Verification

```
*A:BSA-1>config>service>vpls>sap# host-connectivity-verify ?
  - host-connectivity-verify source-ip <ip-address> [source-mac
    <ieee-address>] [interval <interval>] [action {remove|alarm}] [timeout
    <retry-timeout>] [retry-count <count>]

 <ip-address>          : a.b.c.d
 <ieee-address>        : xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx
 <interval>            : [1..6000] minutes
 <{remove|alarm}>      : keywords
 <retry-timeout>       : [10..60] seconds
 <count>               : [2..29]
```

Bridged CO:

```
configure
    service
        vpls 1 customer 1 create
            sap 1/1/2:2 split-horizon-group "rshg-1" create
                host-connectivity-verify source-ip 0.0.0.0 interval 1 action remove
            exit
```

Note: the configured source IP should be an unused unique IP address in the DHCP client subnet or alternatively use source-ip 0.0.0.0. As the host-connectivity-verify application is sending a unicast ARP to the DHCP host, its ARP table is updated with the configured source-ip and source-mac (chassis MAC if not configured). If you would use an existing IP address, the DHCP host ARP table gets poisoned, breaking the connectivity to that host.

Routed CO:

```
configure
    service
        vprn 1 customer 1 create
            subscriber-interface "sub-int-1" create
                group-interface "group-int-1" create
                    host-connectivity-verify interval 1 action alarm
```

Note: the source IP is not configurable. The source-ip used in the unicast ARP is fixed to the local subscriber interface address in the subnet of the DHCP hosts that is checked for connectivity.

To verify the result of the connectivity check:

```
*A:BSA-1# show service id 1 host-connectivity-verify statistics
===============================================================================
Host connectivity check statistics
===============================================================================
Svc   SapId/          DestIp          Timestamp              Time since  Oper
Id    SdpId           Address         last-reply/conn-lost   Reply/Lost  State
-------------------------------------------------------------------------------
1     1/1/2:2         10.1.0.99       11/23/2009 17:26:45    0d 00:00:44 Up
-------------------------------------------------------------------------------
1 host-connectivity states : 1 Up / 0 Down / 0 Retry pending
===============================================================================
*A:BSA-1#
```

In case the connectivity is lost with the host, following event is generated:

```
836 2009/11/23 17:28:24.74 CET WARNING: SVCMGR #2206 Base Host connectivity lost
"host connectivity lost on 1/1/2:2 in service 1 for inetAddr = 10.1.0.99,
chAddr=fe:fd:00:02:46:00."
```

With action alarm, the lease-state is not removed in case the connectivity is lost with the host. The event is still generated and the statistics show:

```
*A:BSA-1# show service id 1 host-connectivity-verify statistics
===============================================================================
Host connectivity check statistics
===============================================================================
Svc   SapId/          DestIp          Timestamp              Time since  Oper
Id    SdpId           Address         last-reply/conn-lost   Reply/Lost  State
-------------------------------------------------------------------------------
1     1/1/2:2         10.1.0.99       11/23/2009 17:38:28    0d 00:01:42 Down
-------------------------------------------------------------------------------
1 host-connectivity states : 0 Up / 1 Down / 0 Retry pending
===============================================================================
*A:BSA-1#
```

Event in case of restored connectivity:

```
839 2009/11/23 17:41:07.74 CET WARNING: SVCMGR #2207 Base Host connectivity restored
"host connectivity restored on 1/1/2:2 in service 1, for inetAddr = 10.1.0.99,
chAddr=fe:fd:00:02:46:00."
```

Connectivity to a DHCP host can also be checked using an OAM command:

```
*A:BSA-1# oam host-connectivity-verify service 1 sap 1/1/2:2
===============================================================================
Triggering host connectivity verify for service 1 sap 1/1/2:2 ...
Waiting 3 seconds ...

===============================================================================
Host connectivity check statistics
===============================================================================
Svc   SapId/          DestIp          Timestamp              Time since  Oper
Id    SdpId           Address         last-reply/conn-lost   Reply/Lost  State
-------------------------------------------------------------------------------
1     1/1/2:2         10.1.0.99       -                      -           -
-------------------------------------------------------------------------------
1 host-connectivity states : 0 Up / 0 Down / 1 Retry pending
===============================================================================
*A:BSA-1#
```

Note that in this case, no action is triggered. If the connectivity test is successful, the host-connectivity-verify statistics are updated with the new timestamp last-reply. If the connectivity test fails, the host-connectivity state becomes Retry Pending (oper state unknown) until an automatic test is scheduled again in the next interval.

To troubleshoot host-connectivity-verify, enable following debug log (additional filtering is possible on ip address, mac address and/or SAP):

```
debug
    service
        id 1
            host-connectivity-verify
            exit
        exit
    exit
exit
```

DHCP Lease Split

The second alternative is using a DHCP proxy server with the lease-split option.

A finer granularity of DHCP lease time is used between the DHCP client and the DHCP proxy server than between the DHCP proxy server and the DHCP server.

The maximum time for DHCP host connectivity loss detection in this case is the configured DHCP lease-split lease time.

DHCP communication is snooped between the DHCP client and DHCP server. In the DHCP ack message, the offered lease-time from the DHCP server is replaced with the configured DHCP proxy server lease-split lease time. Note that the lease time is only updated if the configured lease-split lease time is less than half of the original lease time value. The minimum value for the proxy server lease-split lease time is 5 minutes. When the DHCP client renews the DHCP session, the DHCP proxy server sends a DHCP ack on behalf of the DHCP server as long as the next renew time is earlier than half of the DHCP server expiry time for this session. With ESM enabled, RADIUS re-authentication will occur only when the DHCP request must be sent to the DHCP server. In other words, configuring a DHCP proxy with lease-split does not put extra load on the RADIUS server.

In the example below, the DHCP server offers a lease time of 960 seconds. The lease time in the offer sent to DHCP client will be updated with the lease time of 300 seconds as configured in the DHCP proxy server lease-split on BSA-1.

Bridged CO:

```
configure
    service
        vpls 1 customer 1 create
            sap 1/1/2:2 split-horizon-group "rshg-1" create
                dhcp
                    proxy-server
                        lease-time min 5
                        no shutdown
                    exit
```

Routed CO:

```
configure
    service
        vprn 1 customer 1 create
            subscriber-interface "sub-int-1" create
                group-interface "group-int-1" create
                    dhcp
                        proxy-server
                            lease-time min 5
                            no shutdown
                        exit
```

Note: the emulated server address in the DHCP proxy-server configuration does not have to be configured for lease-split operation. This parameter is needed for an alternative use of the DHCP proxy server: RADIUS based IP configuration of a subscriber host. This is out of the scope of this configuration note.

If DHCP lease split is operational for a DHCP host, it will be shown in the Remaining Lifetime field of the detailed lease-state output. Note that the Session Timeout field is the original offered lease time from the DHCP server.

```
*A:BSA-1# show service id 1 dhcp lease-state detail
===============================================================================
DHCP lease states for service 1
===============================================================================
Service ID           : 1
IP Address           : 10.1.0.99
Client HW Address    : fe:fd:00:02:46:00
SAP                  : 1/1/2:2
Remaining Lifetime   : 00h04m26s (Lease Split)
Persistence Key      : 0x0000000e

Sub-Ident            : ""
Sub-Profile-String   : ""
SLA-Profile-String   : ""
App-Profile-String   : ""
Lease ANCP-String    : ""
Lease Int Dest Id    : ""
Category-Map-Name    : ""

Sub-Ident origin     : None
Strings origin       : None
Lease Info origin    : DHCP

Ip-Netmask           : 255.255.0.0
Broadcast-Ip-Addr    : N/A
Default-Router       : 10.1.0.254
Primary-Dns          : N/A
Secondary-Dns        : N/A
Primary-Nbns         : N/A
Secondary-Nbns       : N/A

ServerLeaseStart     : 11/23/2009 17:38:27
ServerLastRenew      : 11/24/2009 15:27:57
ServerLeaseEnd       : 11/24/2009 15:37:57
Session-Timeout      : 0d 00:10:00
DHCP Server Addr     : 172.16.0.1

Relay Agent Information
  Circuit Id         : UML246
RADIUS User-Name     : ""
-------------------------------------------------------------------------------
Number of lease states : 1
===============================================================================
*A:BSA-1#
```

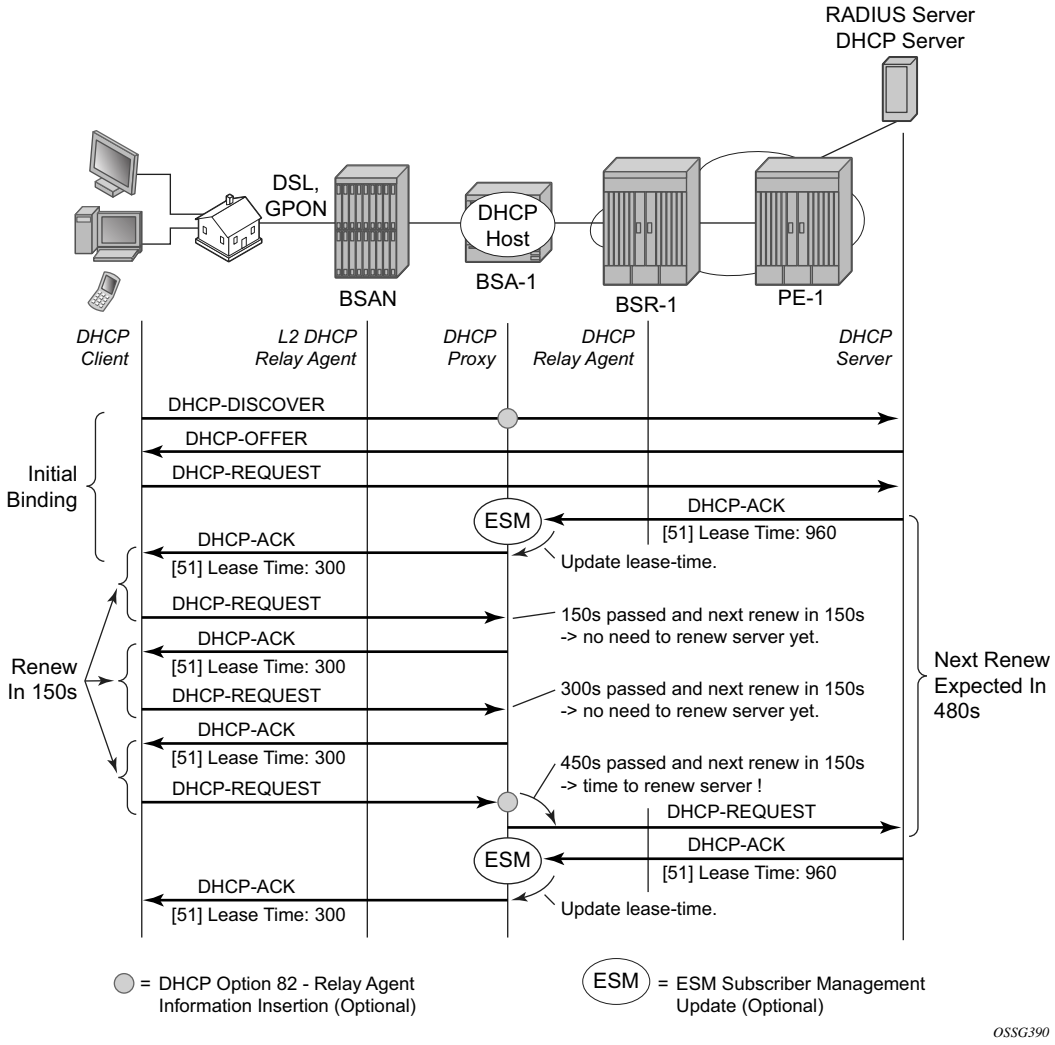

Figure 324: DHCP Proxy Server: Lease Split Operation

When the DHCP client disconnects without sending a DHCP release in the network, the DHCP lease state in the BSA/BSR will be removed only when the DHCP lease time expires. With DHCP proxy server lease-split, the DHCP client disconnection can be sped up. In the example below, the DHCP client disconnection is detected in less than 5 minutes (lease-split lease time) while it would have taken up to 16 minutes without the lease-split. Note that the values are illustrative; in reality the DHCP lease times will be higher.

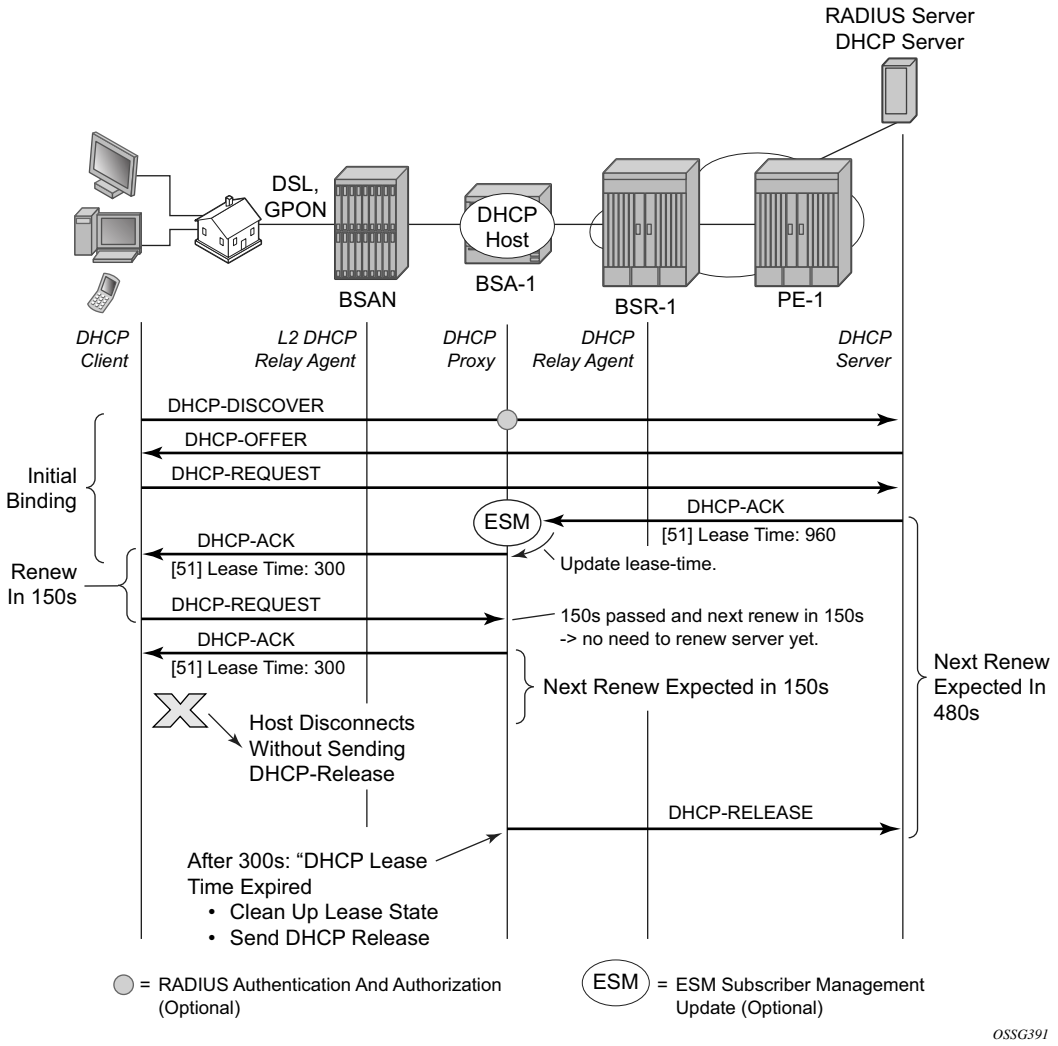

Figure 325: DHCP Proxy Server: Lease Split Operation, DHCP Client Disconnected

DHCP Host Mobility

A field technician verifying DSLAM operation often connects and disconnects from different ports rapidly. This will require the node to clear its own DHCP host state, the DHCP server state as well as flush MAC addresses learned within the VPLS network or clear ARP entries from the routing instance.

A DHCP request comes in on SAP2. On SAP1 there exists a lease state with the same Client Hardware address. The packet is dropped and a forced SHCV check verifies the existing lease state on SAP1. Three consecutive checks are launched with a timeout of 10 seconds. If the host indeed moved form SAP1 to SAP2, the connectivity check will fail on SAP1. The existing lease state is deleted and a DHCP release message is sent to the DHCP server. Any subsequent DHCP session setup will proceed as normal.

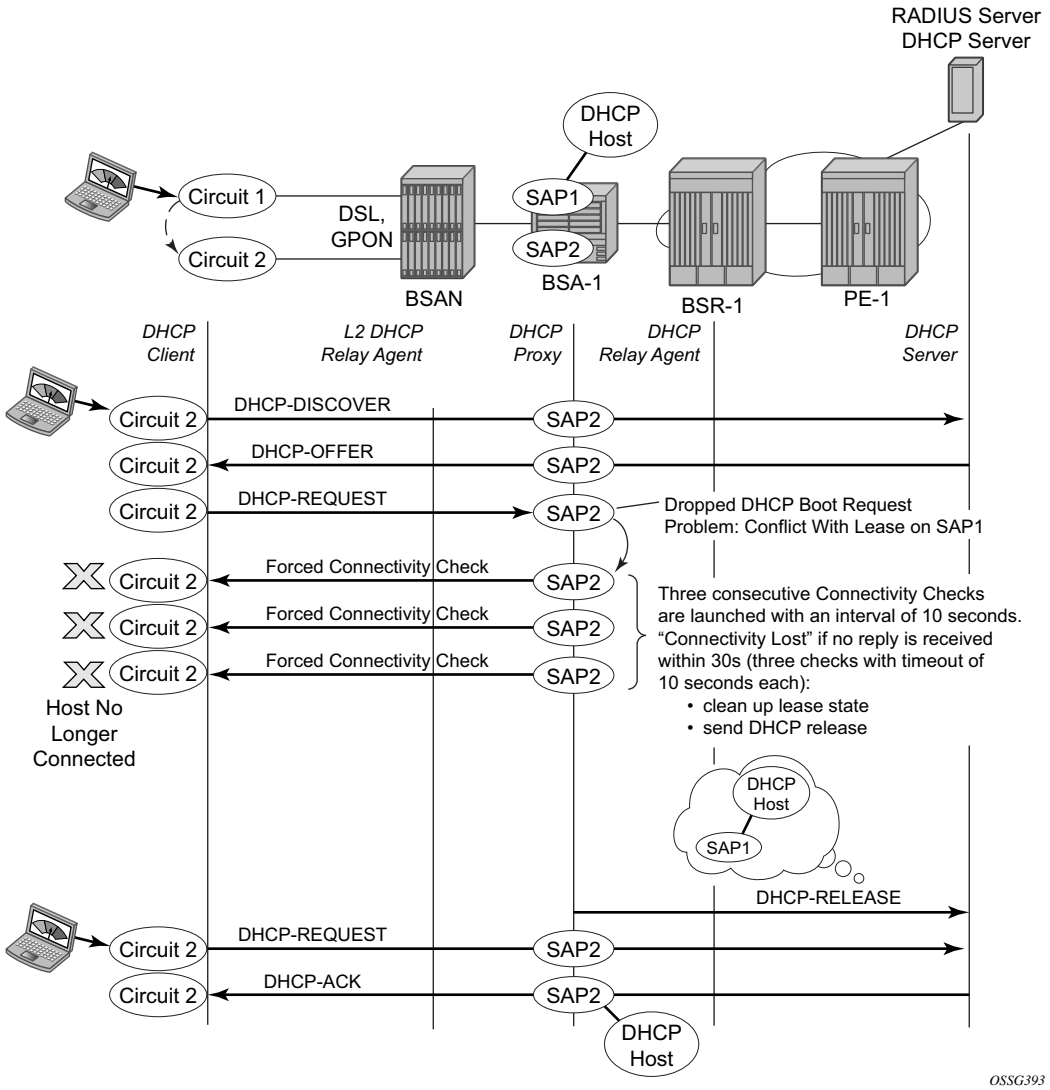

Figure 326: DHCP Host Mobility

Note that for host mobility to function, host-connectivity-verification must be enabled. Next to periodic connectivity checks, it also enables forced checks triggered by moving hosts.

For Bridged CO, host-connectivity-verify must be enabled on the SAPs. When no interval is specified, it will default to 10 minutes for the periodic connectivity checks.

Bridged CO:

```
configure
    service
        vpls 1 customer 1 create
```

```
            sap 1/1/2:1 split-horizon-group "rshg-1" create
                host-connectivity-verify source-ip 10.1.0.253
            exit
            sap 1/1/2:2 split-horizon-group "rshg-1" create
                host-connectivity-verify source-ip 10.1.0.253
            exit
```

Note: the configured source-ip should be an unused unique ip address in the DHCP client subnet or alternatively use source-ip 0.0.0.0. As the host-connectivity-verify application is sending a unicast ARP to the DHCP host, its ARP table is updated with the configured source-ip and source-mac (chassis MAC if not configured). If you would use an existing IP address, the DHCP host ARP table gets poisoned, breaking the connectivity to that host.

For Routed CO, host-connectivity-verify must be enabled on the group-interface. When no interval is specified, it will default to 10 minutes for the periodic connectivity checks.

Routed CO:

```
configure
    service
        vprn 1 customer 1 create
            subscriber-interface "sub-int-1" create
                group-interface "group-int-1" create
                    host-connectivity-verify
```

Note: the source IP address is not configurable. The source-ip used in the unicast ARP is fixed to the local subscriber interface address in the subnet of the DHCP hosts that is checked for connectivity.

Conclusion

This section provides configuration and troubleshooting commands for dynamic DHCP hosts. DHCP 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.