

Configuring DHCP with CLI

This section provides information to configure DHCP using the command line interface.

- [Common Configuration Tasks on page 382](#)
 - [Enabling DHCP Snooping on page 382](#)
 - [Configuring Option 82 Handling on page 384](#)
 - [Enabling DHCP Relay on page 385](#)
 - [Configuring Local User Database Parameters on page 386](#)

Common Configuration Tasks

Topics in this section are:

- [Enabling DHCP Snooping on page 382](#)
 - [Configuring Option 82 Handling on page 384](#)
 - [Enabling DHCP Relay on page 385](#)
 - [Configuring Local User Database Parameters on page 386](#)
-

Enabling DHCP Snooping

DHCP snooping is the process of copying DHCP packets and using the contained information for internal purposes. The BSA and BSR can use the snooped DHCP information to build anti-spoofing filters, populate the ARP table, send ARP replies, etc.

For VPLS, DHCP snooping must be explicitly enabled (using the snoop command) on the SAP or SDP where DHCP messages ingress the VPLS instance. It is recommended to enable snooping on both the interface to the DHCP server (to snoop ACK messages) and the interface to the subscriber (to snoop RELEASE messages)

For IES and VPRN IP interfaces, lease-populate enables DHCP snooping for the subnets defined under the IP interface. The number of allowed simultaneous DHCP sessions on a SAP or IES interface can be limited using the lease-populate command with the parameter number-of-entries specified. Enabling lease-populate and snoop commands is effectively enabling “standard subscriber management” as described in [Standard and Enhanced Subscriber Management on page 871](#).

The following output displays an example of a partial BSA configuration with DHCP snooping enabled in a service:

```
*A:ALA-48>config>service# info
-----
...
    vpls 600 customer 701 create
        sap 1/1/4:100 split-horizon-group "DSL-group2" create
            description "SAP towards subscriber"
            dhcp
                lease-populate 1
                option
                    action replace
                    circuit-id
                    no remote-id
                exit
                no shutdown
            exit
        exit
    mesh-sdp 2:800 create
        dhcp
            snoop
        exit
    exit
    no shutdown
exit
...
-----
*A:ALA-48>config>service#
```

Configuring Option 82 Handling

Option 82, or “Relay Information Option” is a field in DHCP messages used to identify the subscriber. The Option 82 field can already be filled in when a DHCP message is received at the router, or it can be empty. If the field is empty, the router should add identifying information (circuit ID, remote ID or both). If the field is not empty, the router can decide to replace it.

The following example displays an example of a partial BSA configuration with Option 82 adding on a VPLS service. Note that snooping must be enabled explicitly on a SAP.

```
A:ALA-1>config>service>vpls#
-----
      no shutdown
      description "Default tls description for service id 1"
      sap 1/1/11 split-horizon-group "2dslam" create
        dhcp
          no description
          snoop
          no lease-populate
          option
            action replace
            circuit-id ascii-tuple
            no remote-id
          exit
        no shutdown
      exit
    exit
  -----
A:ALA-1>config>service>vpls#
```

Enabling DHCP Relay

Note that lease populate and DHCP relay are different features in which are not both required to be enabled at the same time. DHCP relay can be performed without populating lease tables.

The following example displays DHCP relay configured on an IES interface:

```
A:ALA-48>config>service>ies>if# info
-----
      address 10.10.42.41/24
      local-proxy-arp
      proxy-arp
        policy-statement "ProxyARP"
      exit
      sap 1/1/7:0 create
        anti-spoof ip
      exit
      arp-populate
      dhcp
        description "relay_ISP1"
        server 10.200.10.10 10.200.10.20
        lease-populate 1
        no shutdown
      exit
-----
A:ALA-48>config>service>ies>if#
```

Configuring Local User Database Parameters

A local user data base defines a collection of hosts. There are 2 types of hosts: PPPoE and DHCP. A local user database can be used for the following:

- Perform authentication for PPPoE clients. For this only the hosts declared under PPPoE are used.
- Perform authentication and address management for the local DHCP server. For this both PPPoE and DHCP sections can be used depending on the client type indicated by a vendor-specific suboption inside Option 82 of the DHCP message.

Each host can be identified by a set of values. However, at any point in time only four of these values are taken into account for DHCP as defined by the **dhcp match-list** option and only three are considered for PPPoE as defined in the **pppoe match-list** option.

When trying to find a matching host, attempts are made to match as many items as possible. If several hosts match an incoming DHCP packet, the one with most match criteria is taken.

One host entry can map on several physical clients. For instance, when using a circuit ID, by masking when the interface-id is used, the host-entry is used for all the clients on that same interface.

DHCP host identification, called from the local DHCP server, includes:

- Circuit ID from OPTION 82. Note that for this field there is the possibility to mask the circuit ID (the **mask** command) before looking for the host.
- MAC address
- Remote ID from Option 82
- Option 60 from DHCP message, note that only first 32 bytes are looked at
- SAP ID from vendor-specific suboption of Option 82
- Service ID from vendor-specific suboption of Option 82
- String from vendor-specific suboption of Option 82
- System ID from vendor-specific suboption of Option 82

PPPOE host identification, called from the local DHCP server or from PPPoE host identification includes:

- Circuit ID
- MAC address
- Remote id
- User name, either complete user name, domain part only, or host part only

When a host cannot be inserted in the lookup database, it will be placed in an unmatched-hosts list. This can occur due to:

- Another host with the same host-identification exists. Note that only the host-identification that is specified in the match-list is taken into account for this.
- A host has no host-identification specified in the match-list.

When used for PPPOE-authentication, the fields are used as follows:

- password — Verifies the PPPoE user password. This is mandatory. If no password is required then it must be explicitly set to **ignore**.
- address:
 - no address — No address information. The address must be obtained by other means, either radius or DHCP-server.
 - gi-address — No meaning in this context. The address must be obtained by other means, either RADIUS or DHCP-server.
 - use-pool-from-client — No meaning in this context, address must be obtained by other means, either RADIUS or DHCP-server.
 - pool-name — The address must be obtained by other means, either RADIUS or a DHCP-server. When a DHCP server is used, this pool-name will be included in Option 82 vendor-specific suboption.
 - ip-address — This ip-address will be offered to the client.
- Identification-strings — Returns the strings used for enhanced subscriber management (ESM).
- Options — Only DNS servers and NBNS server are used, others are ignored.

When used from DHCP-server following applies:

- password — not used.
- address — Defines how the address should be allocated for this host.
 - no address — The host is not allowed. The clients mapping to this host will not get an IP address.
 - gi-address — Finds the matching subnet and an IP address is taken from that subnet.
 - pool-name — A free IP address is taken from that pool.
 - ip-address — This ip-address will be offered to the client.
 - use-pool-from-client — Use the poolname in the Option 82 vendor-specific suboption. If no poolname is provided there, falls back to the DHCP server default (none or use-gi-address).
- identification-strings — The operator can specify subscriber management strings and in which option the strings are sent back in dhcp-offer and dhcp-ack messages.
- options — The operator defines which options specific to this host should be sent back in the dhcp-offer and dhcp-ack messages. Note that the options defined here override options defined on the pool-level and subnet-level inside the local DHCP server.

The circuit ID from PPPoE or from Option 82 in DHCP messages can be masked in following ways:

Common Configuration Tasks

- **prefix-length** — Drop a fixed number of bytes at the beginning of the circuit-id.
- **suffix-length**— Drop a fixed number of bytes at the end of the circuit-id.
- **prefix-string** — The matching string will be dropped from the beginning of the circuit-id. The matching string can contain wildcards (*). For example: incoming circuit-id "mybox|3|my_interface|1/1/1:22" masked with "*|*|" will leave "my_interface|1/1/1:22".
- **suffix-string** — The matching string will be dropped at the end of the circuit-id. For example: incoming circuit-id "mybox|3|my_interface|1/1/1:22" masked with "|*" will result in "mybox|3|my_interface".

The following is an example of a local user database used for PPPoE authentication:

```
*A:ALA-48>config>subscr-mgmt# info
-----
...
    local-user-db "pppoe user db"
        description "pppoe authentication data base"
        ppp
            match-list username circuit-id
            mask prefix-string "*|*|" suffix-string "|*"
            host "john" create
                host-identification
                    username "john" no-domain
                exit
                password pap "23T8yPoe0w1R.BPGHB98i0qhJf7Z1ZGCtXBKGnjrIrA" hash2
                no shutdown
            exit
            host "test.com" create
                host-identification
                    username "test.com" domain-only
                exit
                password ignore
                no shutdown
            exit
            host "john@test.com" create
                host-identification
                    username "john@test.com"
                exit
                password pap "23T8yPoe0w0T1flyCb4hskknvTYLqA2avvBB567g3eQ" hash2
                identification-strings 122 create
                    subscriber-id "john@test.com"
                    sla-profile-string "sla prof1"
                    sub-profile-string "subscr profile 1"
                    ancp-string "ancp string"
                    inter-dest-id "inter dest"
                exit
                no shutdown
            exit
            host "john@test.com on interface group-if"
                host-identification
                    circuit-id string "group-if"
                    username "john@test.com"
                exit
                password pap "23T8yPoe0w1R.BPGHB98i0qhJf7Z1ZGCtXBKGnjrIrA" hash2
                address 10.1.2.3
```



```

        no shutdown
        exit
    exit
    no shutdown
    exit
...
-----
*A:ALA-48>config>subscr-mgmt#

```

The following are some examples when a user tries to set up PPPoE:

- john@test.com tries to setup PPPoE with circuit-id "pe_23|3|group-if|1/1/1": host "john@test.com on interface group-if" will match, the PAP password is checked and the IP address 10.1.2.3 is given to PPPoE to use for this host.
- john@test.com (on another interface): host "john@test.com" will match, the PAP password is checked, and identification strings are returned to PPPoE.
- alcatel@test.com: host "test.com" will match, no password check, the user is allowed.
- john@alcatel.com: host "john" will match and the password will be checked.
- anybody@anydomain: will not match and will not be allowed.

The following is an example of a local user database used for DHCP server for DHCP clients:

```

*A:ALA-50>config>subscr-mgmt# info
-----
...
    local-user-db "dhcp server user db"
        description "dhcp server user data base"
        dhcp
            match-list circuit-id mac
            mask prefix-string "*|*|" suffix-string "|*"
            host "mac 3 on interface" create
                host-identification
                    circuit-id string "group-if"
                    mac 00:00:00:00:00:03
                exit
                address 10.0.0.1
                no shutdown
            exit
            host "maskedCircId" create
                host-identification
                    circuit-id string "group-if"
                exit
            address pool "pool 1"
            identification-strings 122 create
                subscriber-id "subscriber 1234"
                sla-profile-string "sla prof 1"
                sub-profile-string "sub prof 1"
                ancp-string "ancpstring"
                inter-dest-id "inter dest id 123"
            exit
            options
                netbios-name-server 1.2.3.4
                lease-time min 2
            exit

```

Common Configuration Tasks

```
        no shutdown
        exit
    exit
    no shutdown
    exit
...
-----
*A:ALA-50>config>subscr-mgmt#
```

The following is an access example:

- MAC 00:00:00:00:00:03 on circuit-id "pe5|3|group-if|1/1/1": host "mac 3 on interface" is matched and address 10.0.0.1 is offered to the DHCP client.
- Another MAC on circuit-id "pe5|3|group-if|2/2/2": host "maskedCircId" is matched and an address is taken from "pool1" (defined in the DHCP server). The identification-strings will be copied to Option 122 in the dhcp-offer and dhcp-ack messages. The options defined here will also be copied into dhcp-offer and dhcp-ack messages.
- The circuit-id "pe5|3|other_group_if|1/1/3": no host is matched. The client will only get an IP address if on DHCP server level you defined the *use-gi-address* parameter and the gi-address matches a subnet.
-

The following is an example of a local user database used for a DHCP server, only for PPPoE clients:

If PPPoE does not get an IP address from RADIUS or the local-user-db used for authentication, the internal dhcp-client will be used to access a DHCP server which can be in the same node or in another node. These request are identified by inserting Option 82 suboption client-id in the dhcp-discover and dhcp-request messages. When the DHCP server receives this request and has a user-db connected to it, then the PPPoE section of that user-db is accessed.

```
*A:ALA-60>config>subscr-mgmt# info
-----
...
    local-user-db "pppoe user db"
        description "pppoe authentication data base"
        ppp
            match-list username
            host "internet.be" create
                host-identification
                    username "internet.com" domain-only
                exit
                address "pool_1"
                no shutdown
            exit
            host "john@internet.com" create
                host-identification
                    username "john@internet.com"
                exit
            identification-strings 122 create
                subscriber-id "john@test.com"
                sla-profile-string "sla prof1"
                sub-profile-string "subscr profile 1"
```

```

        ancp-string "ancp string"
        inter-dest-id "inter dest"
    exit
    address use-gi
    no shutdown
exit
host "malicious@internet.com"
host-identification
    circuit-id string "group-if"
    username "internet@test.com"
    exit
    no shutdown
    exit
exit
no shutdown
exit
...
-----
*A:ALA-60>config>subscr-mgmt#

```

The following is an access example:

- john@internet.com: GI is used to find a subnet and a free address will be allocated from that subnet. Identification strings are returned in Option 122.
- anybody@internet.com: pool_1 will be used to find a free IP address.
- malicious@internet.com: no address is defined. This user will not get an IP address.

The following is an example of associating a local user database to PPPoE for authentication

```

A:pe5>config>service>vprn#
-----
    subscriber-interface "tomylinux" create
    address 10.2.2.2/16
    group-interface "grp_pppoe3" create
    pppoe
    pap-chap-user-db "pppoe"
    exit
    exit
-----
A:pe5>config>service>vprn#

```

The following is an example of associating a local user database to a local DHCP server.

```

A:pe7>config>router>dhcp#
-----
    local-dhcp-server my_server
    description "my dhcp server"
    user-db "data base 1"
    ...
    exit
-----
A:pe7>config>router>dhcp#

```

In PPPoE access scenario's without access node or with access nodes that do not insert PPPoE vendor specific tags "Circuit-ID" and/or "Remote-ID", it may be required to configure this

Common Configuration Tasks

information in the local user database so that they can be picked up in pre-authentication phase and used for RADIUS authentication and reporting in RADIUS accounting messages. For example:

```
>config>subscr-mgmt

    local-user-db "ludb-1" create
        ppp
            match-list username
            host "host-1" create
                access-loop-information
                    circuit-id string "LUDB inserted circuit-id"
                    remote-id string "LUDB inserted remote-id"
                exit
                host-identification
                    username "cpe-1@domain1.com"
                exit
                auth-policy "auth-policy-1"
                password ignore
                no shutdown
            exit
        exit
    exit
```