Configuring Triple Play Security with CLI

This section provides information to configure Residential Broadband Aggregation services using the command line interface. It is assumed that the reader is familiar with VPLS, IES and VPRN services.

Topics in this section include:

Common Configuration Tasks

Topics in this section are:

Configuring Anti-Spoofing Filters

Anti-spoofing filters are used to prevent malicious subscribers sending IP packets with a forged IP or MAC address, and thus mis-directing traffic. The anti-spoofing filter is populated from the DHCP lease state table, and DHCP snooping must be enabled on the SAP.

There are three types of filters (MAC, IP and IP+MAC), one type is allowed per SAP.

The following displays an IES service interface configuration with anti-spoofing.

```
A:ALA-48>config>service>ies# info
----------------------------------------------
            interface "test123" create
                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
                    lease-populate 1
                    no shutdown
                exit
            exit
            no shutdown
----------------------------------------------
A:ALA-48>config>service>ies#
```

Configuring Triple Play Security features

Topics in this section are:

Configuring MAC Pinning

The following example displays a partial BSA configuration with MAC pinning enabled on a SAP:

```
A:ALA-48>config>service# info
----------------------------------------------
vpls 800 customer 6001 create
     description "VPLS with residential split horizon for DSL"
     stp
          shutdown
     exit
     sap 2/1/4:100 split-horizon-group "DSL-group2" create
          description "SAP for RSHG"
               mac-pinning
     exit
     no shutdown
----------------------------------------------
A:ALA-48>config>service#
```

Configuring MAC Protection

Preventing Access By Residential Subscribers Using Protected (Gateway) MAC Addresses

The first step is to create a list of MAC addresses to be protected, the second step is to prevent access using these source addresses inside an SHG or a SAP.

The following example displays a partial BSA configuration with some protected MAC addresses on any SAP created inside the SHG:

```
A:ALA-48>config>service# info
----------------------------------------------
vpls 800 customer 6001 create
     no shutdown
     split-horizon-group "mygroup" create
          restrict-protected-src
     exit
     description "VPLS with residential split horizon for DSL"
     mac-protect
          mac 00:00:17:FE:82:D8
          mac 93:33:00:00:BF:92
     exit
----------------------------------------------
A:ALA-48>config>service#
```

Restricting Access By Residential Subscribers To a Small List Of Upstream MAC Addresses:

The first step is to create a list of MAC addresses to be protected, the second step is to restrict access to these addresses only from an SHG or a SAP. (If the MAC address of an upstream server is not known, it can be discovered using e.g. the cpe-ping OAM tool.)

The following example displays a partial BSA configuration with restricted access to some MAC addresses from a specified SAP (an unrestricted access from any other SAP within the VPLS):

```
A:ALA-48>config>service# info
----------------------------------------------
vpls 800 customer 6001 create
     no shutdown
     description "VPLS with restricted access on a SAP"
     mac-protect
          mac 00:00:17:FE:82:D8
          mac 93:33:00:00:BF:92
     exit
     sap 1/1/4:30 create
          restrict-unprotected-dst
     exit
----------------------------------------------
A:ALA-48>config>service#
```

Configuring VPLS Redirect Policy

Figure 26 displays an IP filter entry configuration for VPLS redirect policy.

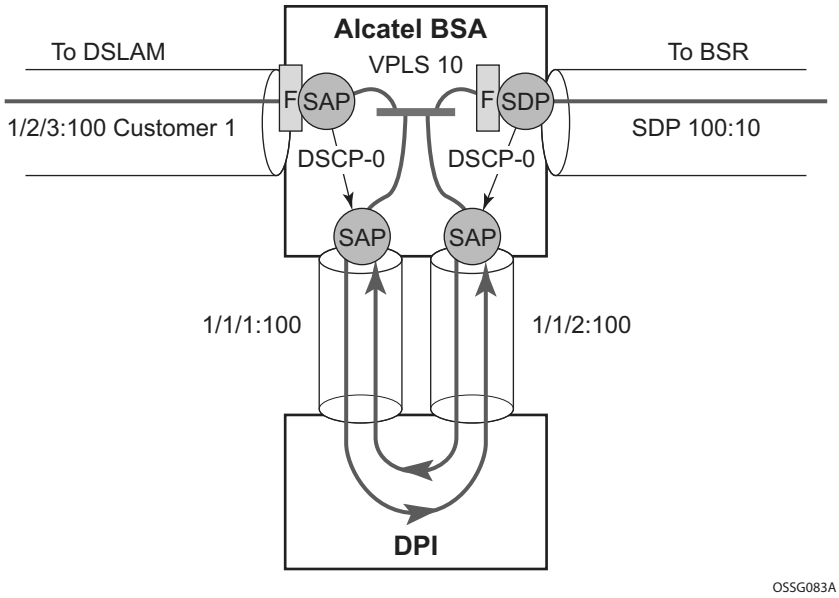

Figure 26: VPLS Redirect Policy Example

Information about defining and applying IP and MAC filters is described in the7750 SR Router Configuration Guide .

Creating the Filter

The following displays a redirect filter entry:

```
A:ALA-A>config>filter# info
----------------------------------------------
     ip-filter 10
          default-action forward
          entry 10
               match
                    dscp be
               exit
               action forward next-hop sap 1/1/1:100
               exit
          exit
     exit
     ip-filter 11
          default-action forward
          entry 10
               match
                    dscp be
               exit
                    dscp be
               exit
               action forward next-hop sap 1/1/2:100
          exit
     exit
----------------------------------------------
A:ALA-A>config>filter#
```

Applying the Filter to a VPLS Service

The following displays how the redirection filter configured above is assigned to the ingress SAP from the DSLAM, and the ingress SDP from the BSR:

```
A:ALA-A>config>service>vpls# info
----------------------------------------------
     vpls 10 customer 1 create
          description "vpls10"
               sap 1/2/3:100 create
                    ingress ip filter 10
               exit
               sap 1/1/1:100 create
               exit
               sap 1/1/2:100 create
               exit
               mesh-sdp 100:10 create
                    ingress ip filter 11
               exit
          exit
     exit
----------------------------------------------
A:ALA-A>config>service>vpls#
```

Configuring ARP Handling

Topics in this section are:

Configuring Proxy ARP

The implementation of proxy ARP with support for local proxy ARP allows the 7750 SR to respond to ARP requests in the subnet assigned to an IES or VPRN interface.

Configuring this command will allow multiple customers to share the same IP subnet.

The following example displays an IES proxy ARP configuration:

```
A:ALA-48>config>service>ies# info
----------------------------------------------
            interface "test123" create
                address 10.10.42.41/24
                local-proxy-arp
                proxy-arp-policy "ProxyARP"
                exit
            exit
            no shutdown
----------------------------------------------
A:ALA-48>config>service>ies#
```

Configuring Local Proxy ARP

When local proxy ARP is enabled on an IP interface, the 7750 SR responds to all ARP requests for IP addresses belonging to the subnet with it's own MAC address, and forwards all traffic between hosts in that subnet. Local proxy ARP is disabled by default.

Note: When local-proxy-arp is enabled under a IES or VPRN service, all ICMP redirects on the ports associated with the service are automatically blocked. This prevents users from learning each other's MAC address (from ICMP redirects).

The following example displays a local proxy ARP IES configuration:

```
A:ALA-A>config>service>ies# info
----------------------------------------------
         interface "test" create
              shutdown
              address 10.10.36.2/24
              local-proxy-arp
         exit
----------------------------------------------
A:ALA-A>config>service>ies#
```

Configuring ARP Reply Agent in a VPLS Service

When ARP reply agent is enabled, the 7750 SR will respond to ARP requests from the network, with information from the DHCP lease state table.

In the upstream direction (towards the network), the ARP reply agent intercepts ARP requests on subscriber SAPs, and checks them against the DHCP lease state table. The purpose is to prevent a malicious subscriber spoofing ARP request or ARP reply messages and thus populating the upstream router's ARP table with incorrect entries.

The following example displays a partial BSA configuration with ARP Reply Agent enabled on a SAP:

```
A:ALA-48>config>service# info
----------------------------------------------
...
     vpls 800 customer 6001 create
          description "VPLS with ARP Reply Agent active"
          sap 2/1/4:100 split-horizon-group "DSL-group2" create
             arp-reply-agent sub-ident
          exit
          sap 3/1/4:200 split-horizon-group "DSL-group2" create
              arp-reply-agent sub-ident
          exit
          no shutdown
...
----------------------------------------------
A:ALA-48>config>service#
```

Configuring Remote Proxy ARP

The following example displays the IES configuration to enable remote proxy ARP:

```
A:ALA-49>config>service>ies# info
----------------------------------------------
            interface "test-1A" create
                address 10.10.26.3/24
                remote-proxy-arp
            exit
            no shutdown
----------------------------------------------
A:ALA-49>config>service>ies#
```

Configuring Automatic ARP Table Population in an IES or VPRN Interface

The following example displays the IES DHCP configuration to enable automatic population of the ARP table using snooped DHCP information on an IES or VPRN interface:

```
A:ALA-1>config>service>ies>if# info
----------------------------------------------
                arp-populate
                dhcp
                    description "snooping_only"
                    lease-populate 1
                    no shutdown
                exit
----------------------------------------------
A:ALA-1>config>service>ies>if#


A:ALA-1>config>service>vprn>if# info
----------------------------------------------
                dhcp
                    description "test"
                    lease-populate 1
                    no shutdown
                exit
----------------------------------------------
A:ALA-1>config>service>ies>if#
```

Configuring CPU Protection

CPU Protection can be used to protect the SR OS router in subscriber management scenarios. Refer to the SR OS System Management Guide for information about CPU Protection operation and configuration.

Configuring Web Portal Redirect

The generic CLI structure for defining and applying IP and MAC filters is described in the 7750 SR Router Configuration Guide.

The following example displays an IP filter entry configuration for web-portal redirect:

```
A:ALA-A>config>filter# info
----------------------------------------------
     ip-filter 10 create
          description "filter to forward DNS and web traffic to my portal; redirect all
other web traffic to the portal and drop everything else"
          default-action drop
          entry 10 create
               description "allows DNS traffic"
                    match protocol 17
                    dst-port 53
               exit
               action forward
          exit
          entry 20 create
               description "allows web traffic destined to portal (IP address 10.0.0.1)"
               match protocol 6
                    dst-port eq 80
                    dst-ip 10.0.0.1
               exit
               action forward
          exit
          entry 30
               description "redirects all web traffic to portal"
               match protocol 6
                    dst-port eq 80
               exit
               action http-redirect http://www.myportal.com/defaultportal
/login.cgi?ip=$IP&mac=$MAC&orig_url=$URL&usb=$SUB
          exit
     exit
----------------------------------------------
A:ALA-A>config>filter#
```

- Filter entry 10 in the example output allows the customer to access DNS to get the IP address of the original website they are trying to view.
- Entry 20 allows HTTP packets destined to the captive portal itself to be forwarded. Note that the actual IP address (a.b.c.d) needs to be entered, not the DNS name (“www.myportal.com”). The IP address can be easily resolved from the 7750 SR CLI using the “ping” command.
- Entry 30 (which is the last option that does not drop the customer packets) checks for HTTP protocol and then starts the redirection process:
  - → The 7750 SR will intercept the HTTP GET from the subscriber and respond with an HTTP 302 (temporarily moved) with the URL configured in the filter entry. This URL can contain some variables, notably the customer IP and MAC addresses to allow the portal to create an entry for the customer. The original requested URL is also included to redirect the client site back to the original requested site when the process is done.
  - → The client will then close the connection with the original IP address and open a connection to the redirected server. Entry 20 will allow this connection.

The following displays how the redirection filter configured above is assigned to an ingress SAP:

```
A:ALA-A>config>service>vpls# info
----------------------------------------------
     vpls 3 customer 6 create
          description "VPLS with web portal redirection filter applied"
          sap 2/1/5:0 create
               ingress
                    filter ip 10
               exit
          exit
          no shutdown
     exit
----------------------------------------------
A:ALA-A>config>service>vpls#
```