Triple Play Security

In This Chapter

This chapter provides information about configuring specific security aspects for Triple Play services, including configuration process overview, and application notes.

Please note that the7750 SR supports many additional security features, which are described in the 7750 SR OS System Management Guide.

Topics in this chapter include:

Triple Play Security Features

Anti-Spoofing Filters

This section describes the Alcatel-Lucent 7750 SR acting as a Broadband Subscriber Aggregator (BSA).

Anti-spoofing is useful to prevent certain packets gaining unauthorized network access. Such packets originate from within a network and with an invalid source address.

Enabling anti-spoof filtering on a subscriber-facing SAP causes the anti-spoof table to be populated with all static and dynamic host information available on the SAP. Enabling anti-spoof filtering on the SAP will fail if any static hosts are defined without the proper addresses specified for the selected anti-spoof filter type.

When enabled, forwarding IP packets that ingress the SAP is dependent on a successful anti-spoof table match with an entry in the table. DHCP and non-IP packets (including ARP) are not subject to anti-spoof filtering. If an entry does not match the ingress packet, the packet will be silently discarded while incrementing the SAP discard counter.

Anti-spoof filtering is only allowed on VPLS SAPs, IES SAP-based IP interfaces, and VPRN SAP-based IP interfaces. Anti-spoof filtering is not available on IES or VPRN SDP bound IP interfaces. Anti-spoof filtering is not supported on Epipe and other VLL type services. Support for anti-spoofing is dependent on SAP based service interfaces.

Note that anti-spoofing filters, with type **ip-mac**, must be enabled to do Enhanced Subscriber Management (as described in section Triple Play Enhanced Subscriber Management on page 827).

Topics in this section are:

Anti-spoofing Filter Types

A SAP or interface that supports anti-spoof filtering can be configured to use one of three types of anti-spoof tables. The type of table used by the SAP is dependent on the type of anti-spoof filtering desired, only one anti-spoofing table type is supported per SAP:

- When only the incoming source MAC address is to be verified, the source MAC table must be defined (anti-spoof type = **mac**).
- When only the incoming source IP address is to be verified, the source IP table must be defined (anti-spoof type = **ip**).
- When both the incoming source MAC and source IP addresses are to be verified, the combination source IP and source MAC table must be defined (anti-spoof type = **ip-mac**).

Note that setting the anti-spoof filter type for the SAP is dependent on pre-existing static host definitions, for example, attempting to set the SAP anti-spoof filtering to mac will fail if any static hosts exist that do not have a defined MAC address.

The anti-spoof table of a SAP or interface will be populated from the DHCP lease state table and from any statically defined hosts on the SAP or interface.

Filtering Packets

Packets from a client that match an anti-spoof filter entry when anti-spoof filtering is enabled are allowed to be further processed by the system. The matching packet is still subject to other forwarding criteria including potentially ACL filtering.

All packets that are not exempt from anti-spoofing and do not match a entry in the anti-spoof table are discarded. Every discard event will increment the SAP discard packet counter. The discard event is not logged or alarmed, but a threshold alarm could be configured for the counter (see Configuring System Monitoring Thresholds in the 7750 SR OS Basic System Configuration Guide).

Not all ingress packets are subject to the anti-spoof filtering when enabled. Non-IP packets are exempt for anti-spoof filter lookups and are allowed to be further processed by the system. This includes ARP requests and replies, as well as PPPoE packets. The only IP packets exempt from anti-spoof filtering are DHCP packets destined to the server UDP port 67. DHCP packets destined to the client UDP port number (port 68) are not exempt.

Layer 2 Triple Play Security Features

Topics in this section include:

MAC Pinning

This section describes the Alcatel-Lucent 7750 SR acting as a Broadband Subscriber Aggregator (BSA).

DHCP snooping and IP/MAC auto-filters can be employed to prevent Theft of Service (by a malicious user spoofing another user's address). However, these auto-filters do not discard non-IP packets such as PPPoE packets, thus potentially allowing a MAC address to be relearned on another SAP. MAC pinning closes this loophole, by not allowing a MAC address to be relearned on another SAP.

When MAC pinning is enabled, a MAC address learned on one SAP or SDP can not be re-learned on another SAP or SDP in the same VPLS, until the FIB entry for the MAC address times out. (Note that in case MAC aging is disabled, MAC entries on a SAP/SDP with MAC pinning enabled will effectively become permanent.)

MAC pinning is implicitly enabled when DHCP auto-filters are enabled, and cannot be disabled. For MAC addressing learned during DHCP address assignment (when DHCP snooping function is active at least on one port of the VPLS), the MAC address is tied to a given SAP for the duration of the DHCP lease.

When a SAP or spoke SDP is part of a Residential Split Horizon Group (RSHG), MAC pinning is automatically enabled at creation of the SAP, but can be disabled if desired.

MAC Protection

In a Layer 2 environment, a malicious subscriber could create a denial-of-service attack by sending Ethernet frames, with as source MAC address the address of a gateway (for example, the IP next hop upstream). As MAC learning is typically enabled, this would move the learned gateway MAC from the uplink SAP or SDP to the subscriber’s SAP, causing all communication to the gateway to be disrupted. If a local content server is attached to the same VPLS, a similar attack could be launched against it.

Communication between subscribers can be disallowed using Split Horizon Groups, but this by itself will not be sufficient to prevent such an attack.

The solution is to create a mechanism to explicitly protect some MAC addresses against being relearned on other SAPs.

The **mac-protect** feature on the Alcatel-Lucent 7750 SR allows a list of special MAC addresses to be configured in a VPLS. Two checks can then be made on incoming packets against these protected MAC addresses:

- **[no] auto-learn-mac-protect**: Used to enable the automatic protection of source MAC addresses learned on the associated object. MAC protection is used in conjunction with restrict-protected-src, restrict-unprotected-dst and mac-protect. When this command is applied or removed, the MAC addresses are cleared from the related object.
- **restrict-protected-src**: Used to prevent denial-of-service attacks. If the source MAC address of a packet from a subscriber matches a protected entry, probably this subscriber tried to impersonate the gateway or server. Such packets are discarded, a trap is generated, and the SAP on which it arrived is placed operationally down.
- **restrict-unprotected-dst**: Used to force traffic from subscribers to only go towards a few defined destinations (the gateways or servers). Any packet from a subscriber whose destination MAC address does not match a protected entry is discarded.

DoS Protection

This section describes the mechanisms and limitations of DoS protection related to subscriber management snooping functions. This feature is only supported on 7750 SR-Series and 7450 ESS-Series redundant chassis models. In subscriber aggregation networks, these routers play an active role in several protocols. Subscribers either intentionally or unknowingly interfere with the operation of the node's processing capacity (for example, excessive ARP handling) or other user traffic.

Routing protocols such as OSPF and ISIS could also be a threat as packets can be injected by customers (erroneously or maliciously) which could cause high CPM overload. Service providers are concerned about DoS protection including DoS attacks when acting as a subscriber aggregation device and guarding against DoS attacks using unprovisioned protocols.

Subscriber Aggregation Network

In a subscriber aggregation network, multiple devices such as the 7750 SR, 7450 ESS, and 7710 SR routers provide access to a DHCP or a RADIUS server. These servers usually do not scale high enough to provide the means to control access to snooping functions through a controlled queue. It is possible, under severe conditions, that the network could become unavailable if the node cannot handle requests from subscribers.

Because the IOMs cannot be scaled to provide a per-subscriber queue to control traffic, a monitoring function, handled by the CPM, is provided. With this monitoring system, the CPM tracks the number of control plane messages set per subscriber and limits the rate to a specified level and provides feedback using event generation to alert a centralized system of a possible DoS attack.

The CPM provides a prioritized access to the CPU. Since the number of control packets expected from a subscriber should have a low rate, and under normal conditions, the system will provide a rate limit on a per subscriber/MAC basis and will drop a subscriber control packet before it is queued or processed by the CPU. The system will be configured with expected arrival rate of per MAC/subscriber control packet rates and optionally total rate per interface/SAP.

The system maintains a per-second running rate monitor per SAP and per MAC. If an entry is using more than the configured rate, the system will not forward that packet to be queued. Every existing subscriber host will be monitored. A subscriber host will be flagged and the system observed with an excessive rate of control packets. In the case of PPPoE, the CPM will monitor subscriber hosts before the IP address is provided by the SAP/MAC/session-id combination.

The control protocols affected by this mechanism include:

- ARP (in arp-reply-agent)
- DHCP (for discover and renew)
- ICMP
- PPPoE
- IGMP

Network Control Filtering

Alcatel-Lucent's 7750 SR, 7450 ESS, and 7710 SR can block network control traffic for unconfigured protocols. For example, if OSPF is not configured on an IP interface, all OSPF-related traffic should be dropped before the traffic reaches the CPU.

Protocols are blocked based on whether that particular protocol is configured to run on the given IP interface. It is not required to re-configure the permitted protocols.

Protocol traffic control by this mechanism includes:

- OSPFv2
- OSPFv3
- IS-IS
- RSVP-TE
- LDP
- RIP
- PIM

- MLD
- IGMP
- BGP
- BFD
- L2PT
- PPP
- DHCP

VPLS Redirect Policy

This section describes the Alcatel-Lucent 7750 SR acting as a Broadband Subscriber Aggregator (BSA) with Layer 2 aggregation towards a Broadband Subscriber Router (BSR).

In a Triple Play network it may be desired to route some traffic from/to subscribers through a Deep Packet Inspection (DPI) device, for example, to limit peer-to-peer traffic. However such a DPI device typically has limited bandwidth available, so only those packets that need inspection should be sent to it.

In a Layer 3 network, such policy-based redirection can be achieved using “next-hop redirect” ACL entries. In a layer 2 (VPLS) aggregation network, the same result can be achieved using “redirect to SAP” or “redirect to SDP” policy.

Refer to the ACL Next-Hop for VPLS section in the 7750 SR OS Services Guide.

ARP Handling

ARP Reply Agent

This section describes the Alcatel-Lucent 7750 SR acting as a Broadband Subscriber Aggregator (BSA).

In Triple Play networks, typically downstream broadcast is not allowed on subscriber SAPs. As a result, subscribers can not receive ARP requests from the network. Instead, 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.

When the keyword **sub-ident** is added in the ARP reply agent configuration, also the subscriber identity is checked. If an upstream ARP request is targeted to the same subscriber, it is dropped. Otherwise, it is flooded to all VPLS interfaces outside the received Split Horizon Group (SHG).

Static hosts can be defined on the SAP using the **host** command. Dynamic hosts are enabled on the system by enabling the **lease-populate** command in the SAP's **dhcp** context. In the event that both a static host and a dynamic host share the same IP and MAC address, the VPLS ARP reply agent will retain the host information until both the static and dynamic information are removed. In the event that both a static and dynamic host share the same IP address, but different MAC addresses, the VPLS ARP reply agent is populated with the static host information.

In brief, the ARP Replay Agent operation is as follows:

- For ARP request received from a customer SAP:
  - → first check in DHCP lease state table - if no match: discard
  - → if (**sub-ident** enabled) and (destination = same subscriber): discard
  - → otherwise: flood to all SAPs/SDPs outside this SHG
- For ARP request received from the network:
  - → lookup IP address in DHCP lease state table - if no match: discard
  - → otherwise: respond with MAC address from the DHCP lease state table

Dynamic ARP Table Population

This section describes the Alcatel-Lucent 7750 SR acting as a Broadband Subscriber Aggregator (BSA) with Layer 3 forwarding towards the network.

In an IES or VPRN service, the system's ARP table can be populated dynamically using entries in the DHCP lease state table (in turn populated from snooping DHCP ACK messages (see DHCP Snooping on page 344)), and from static hosts defined on the SAP. In the router ARP table these are indicated with state managed.

In the event that both a static host is created with the same IP and MAC address as an existing managed entry, creation will fail and a trap is generated.

In the event that a DHCP Lease needs to be populated with the same IP and MAC address as an existing static host entry, creation will fail and a trap is generated.

No **static-arp** creation is possible when combined with **arp-populate**.

Local Proxy ARP

This section describes the Alcatel-Lucent 7750 SR acting as a Broadband Subscriber Aggregator (BSA) with Layer 3 forwarding towards the network.

Local proxy ARP allows the Alcatel-Lucent 7750 SR to respond to ARP requests received on an interface, for an IP address which is part of a subnet assigned to the interface. When the local proxy ARP feature is enabled, the switch responds to all ARP requests for IP addresses belonging to the subnet with the MAC address of the interface, and forwards all traffic between hosts in the subnet.

This feature is intended to be used in situations (such as DSL aggregation networks) when hosts belonging to the same subnet are prevented from directly communicating with each other over the subnet by the configuration of the switch (or DSLAM) to which they are connected.

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 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, thus allowing multiple customers to share the same IP subnet.

Web Portal Redirect

This section describes the Alcatel-Lucent 7750 SR acting as a Broadband Subscriber Aggregator (BSA).

In a Triple Play network it may not be desired (or feasible) to perform manual provisioning of new services and service changes. The ideal way of working is automatic provisioning, with the end-user supplying his details at a retailer, or (if physical connectivity is already present through an on-line customer portal).

The 7750 SR supports a special ACL that automatically redirects subscribers to a predefined URL. This is done by sending a HTTP 302 (moved) message to the subscriber, regardless of the requested URL.

The message flow is as follows (see Figure 39 below):

a. The subscriber gets an IP address using DHCP (if the customer is trying to use a static IP he will be blocked by the anti-spoofing filter).
b. The subscriber tries to connect to a website (TCP SYN, TCP ACK, HTTP GET).
c. The 7750 SR intercepts the HTTP GET request and discards it.
d. The 7750 SR then responds to the subscriber with a HTTP 302 message (service temporarily unavailable/moved), containing a new target URL (that of the portal) configured by the operator. This target URL can include the subscriber's IP and MAC addresses as part of the portal's URL string.
e. The subscriber's web browser will close the original TCP connection and open a new connection to the web portal, where the subscriber can sign up or change his/her service Profile.
f. After approving the changes, the web portal updates the ACL (directly or through another system such as the Alcatel-Lucent 5750 SSC) to remove the redirection policy.
g. The subscriber can now connect to the original site.

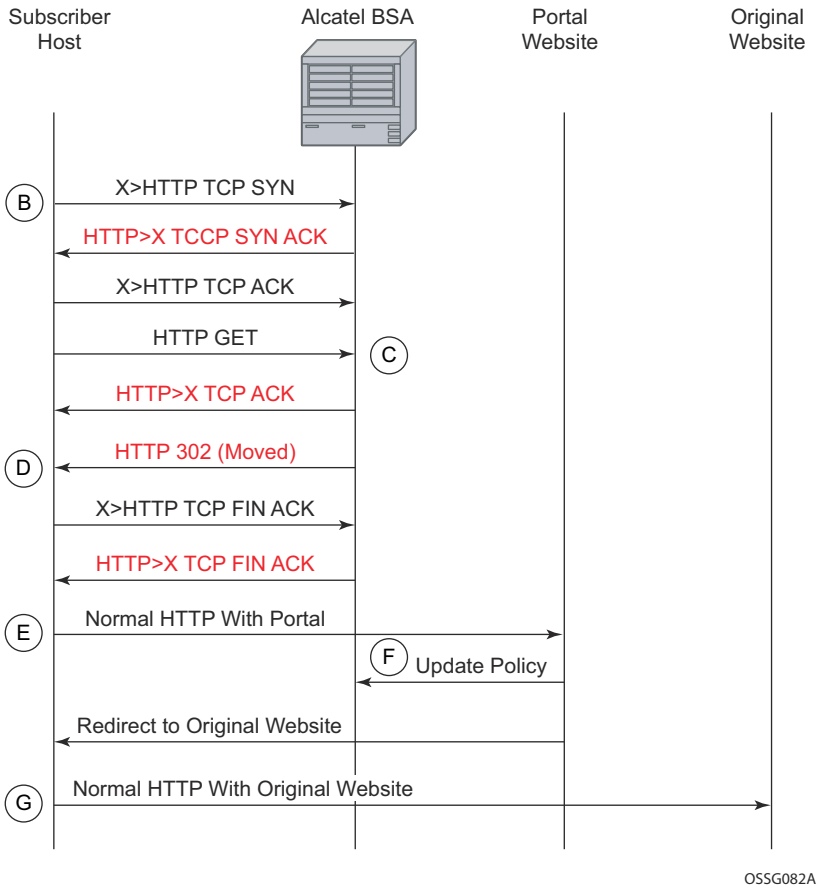

Figure 39: IP Illustration of Message Flow in Web Portal Redirect

The items in red text in Figure 39 are messages the 7750 SR will send (masquerading as the destination), regardless of the destination IP address or type of service.

The following displays information that can optionally be added as variables in the portal URL (http-redirect url):

- $IP – Customer's IP address
- $MAC – Customer's MAC address
- $URL – Original requested URL
- $SAP – Customer's SAP
- $SUB – Customer's subscriber identification string"

Note that the subscriber's IP and MAC address variables are populated from the anti-spoofing list, and thus anti-spoofing must be enabled (see section Anti-Spoofing Filters on page 650).

Since most web sites are accessed using the domain name, the 7750 SR will need to allow DNS queries, and an ACL entry to this effect should be included in the filter (see example in section Configuring Web Portal Redirect on page 675).