HP Networking

Secure Enduser Connection Guidelines

SKA-certifierad
SSNF
2010
Säker-Kund-Anslutning

Background

This document outlines the functionality offered by the HP Networking A-Series switches to fully comply to the SEC IPv4 (previously SKA) certification requirements.

Note that this document only includes a brief description of each functionality involved. For a more detailed description of each function described, refer to the model-specific configuration guide.

Comware® Operating System

Since all A-Series products share the same common operating system - Comware® - the features described herein is available on a broad range of products scaling from low-end to high-end.

A-Series

For customers with large or complex deployments seeking advanced technology to drive competitive advantage through their IT infrastructure at a lower cost of ownership.

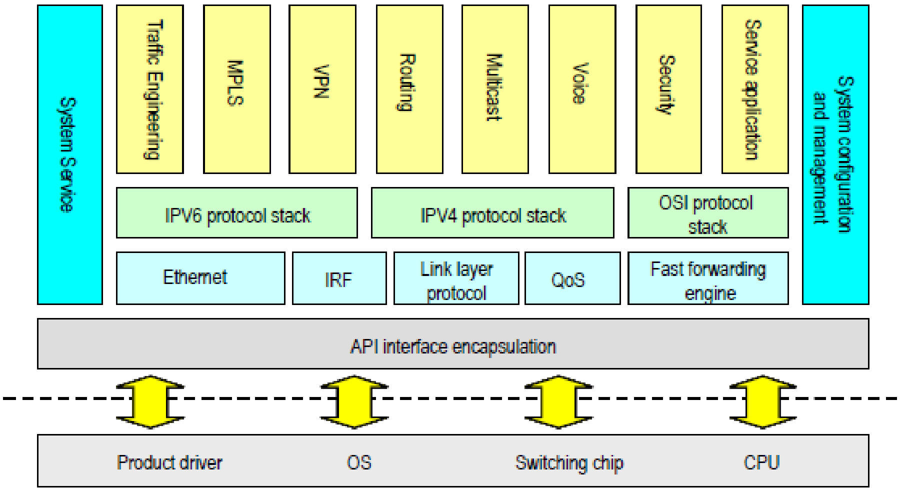


Figure 1: Comware System Architecture

SEC Functionality

The SEC requirements are primarily focused on network deployments with shared broadcast domains between multiple subscribers. Although this is only one of many network designs available (CVLAN, QinQ etc) the security aspects are still applicable in each case to some extent.

The following sections describes the specific functionality available in HP A-Series switches to address these security issues.

DHCP Snooping

As a DHCP security feature, DHCP snooping can implement the following:

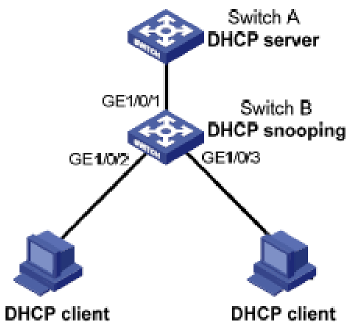
- Ensure DHCP clients obtain IP addresses from authorized DHCP servers
- Record IP-to-MAC mappings of DHCP clients

The entries recorded by the DHCP snooper can be utilized for additional security mechanism as described below.

DHCP Snooping Information (Option 82)

Option 82 allows the switch to inject the location information of the DHCP client in the DHCP requests. This allows for client traceability and is a vital security function in all networks.

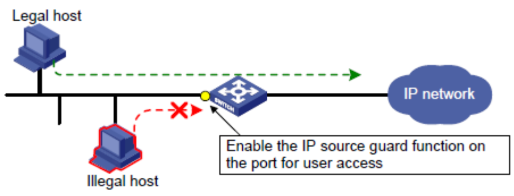
Configuration Example



Switch B

```
dhcp-snooping
interface GigabitEthernet 1/0/1
 dhcp-snooping trust
interface GigabitEthernet 1/0/2
  dhcp-snooping information enable
interface GigabitEthernet 1/0/3
  dhcp-snooping information enable
```

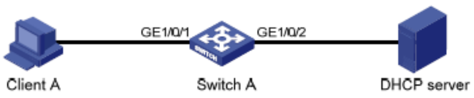
IP Source Guard


Legal host
IP network
Enable the IP source guard function on the port for user access
Illegal host

IP source guard is intended to work on a port connecting users. It filters received packets to block illegal access to network resources, improving the network security.

IP source guard is most often used in conjunction with with the dynamic binding entries created by the DHCP snooping mechanism. Manual binding entries can be created to support environments where static IP assignments are used.

Configuration Example



Switch A

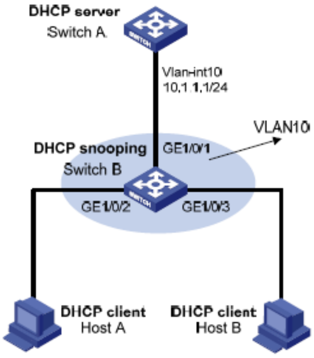
```
dhcp-snooping
interface GigabitEthernet 1/0/2
 dhcp-snooping trust
interface GigabitEthernet 1/0/1
  dhcp-snooping information enable
  ip check source ip-address mac-address
```

ARP Detection

The ARP detection feature is configured on an access device to allow only the ARP packets of authorized clients to be forwarded, hence preventing user spoofing and gateway spoofing.

ARP detection can be based on statically configured objects as well as IP source guard binding entries/DHCP snooping entries.

Configuration Example



Switch B

```
dhcp-snooping
vlan 10
 arp detection enable
interface GigabitEthernet 1/0/1
 dhcp-snooping trust
 arp detection trust
interface GigabitEthernet 1/0/2
  dhcp-snooping information enable
  ip check source ip-address mac-address
arp detection validate dst-mac ip src-mac
```

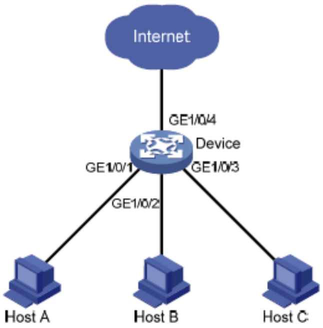
L2 Port Separation

Assigning access ports to different VLANs is a typical way to isolate Layer 2 traffic for data privacy and security, but this approach can utilize a lot of VLAN resources. To isolate Layer 2 traffic without using VLANs, 2 separate features are available.

Port Isolation

To use the feature, you assign ports to a port isolation group. Ports in an isolation group are called isolated ports. An isolated port does not forward any Layer 2 traffic to any other isolated port on the same switch, even if they are in the same VLAN. Still, an isolated port can communicate with any other port outside the isolation group, provided that they are in the same VLAN.

Configuration Example



```
dhcp-snooping
interface GigabitEthernet 1/0/1
 port-isolate enable
interface GigabitEthernet 1/0/2
  port-isolate enable
interface GigabitEthernet 1/0/3
  port-isolate enable
```

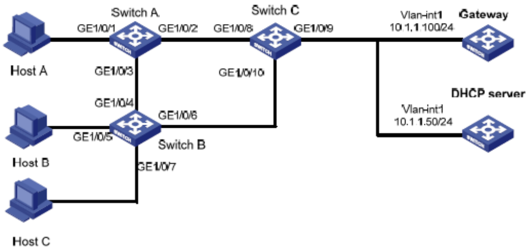
MAC-Forced Forwarding (MACFF)[1]

MACFF (RFC 4562) is developed to provide a solution for Layer 2 isolation and Layer 3 communication between hosts in the same broadcast domain.

An MACFF enabled device intercepts an ARP request and then returns the MAC address of a gateway (or server) to the sender. In this way, the sender is forced to send packets to the gateway for traffic monitoring and attack prevention.

MACFF is often used in cooperation with the DHCP snooping, IP Source Guard and ARP detection features to enhance network security by implementing traffic filtering and Layer 2 isolation on the access switches.

Configuration Example



Switch A

```
dhcp-snooping
vlan 100
 mac-forced-forwarding auto
interface GigabitEthernet 1/0/2
 mac-forced-forwarding network-port
 dhcp-snooping trust
interface GigabitEthernet 1/0/3
  mac-forced-forwarding network-port
  dhcp-snooping trust no-user-binding
```

Switch B

```
dhcp-snooping
vlan 100
 mac-forced-forwarding auto
interface GigabitEthernet 1/0/6
 mac-forced-forwarding network-port
 dhcp-snooping trust
interface GigabitEthernet 1/0/4
  mac-forced-forwarding network-port
  dhcp-snooping trust no-user-binding
```

[1] MACFF is available in some models only

ACLs

An access control list (ACL) is a set of rules for identifying traffic based on criterias such as the source IP address, destination IP address and port number. ACLs are essentially used for packet filtering. A packet filter drops packets that match a deny rule and permits packets that match a permit rule.

The HP A-Series switches has full support for global and port-based advanced IPv4/IPv6/L2 header ACLs.

Configuration Example

The following example describes how to utilize an ACL to block all inbound multicast traffic on interface GigabitEthernet1/0/1:

```
acl number 3001 name DENY-MCAST
 rule 10 deny ip destination 224.0.0.0
15.255.255.255
 rule 99 permit
interface GigabitEthernet 1/0/1
  packet-filter 3001 inbound
```

IPv6

Internet Protocol version 6 (IPv6), was designed by the Internet Engineering Task Force (IETF) as the successor to Internet Protocol version 4 (IPv4). The significant difference between IPv6 and IPv4 is that IPv6 increases the IP address size from 32 bits to 128 bits.

As of today not many broadand access networks are fully IPv6 enabled. Since most modern computer OSes have IPv6 enabled by default though, security considerations still has to be made in how to prohibit undesired IPv6 traffic between subscribers.

In addition to the port isolation techniques described earlier, HP A-Series switches provides support for advanced IPv6 ACLs which allows for great flexibility in filtering IPv6 traffic.

Configuration Example

The following example describes how to utilize an ACL to block inbound ICMPv6 and DHCPv6 traffic on interface GigabitEthernet1/0/1:

```
acl ipv6 number 3003
 rule 10 deny icmpv6
 rule 20 deny udp destination
FF02::1:2/128 destination-port eq 547
interface GigabitEthernet 1/0/1
  packet-filter 3003 inbound
```

The following example describes an Ethernet frame header ACL that only allows IPv4 and ARP frames:

```
acl number 4004
 rule 10 permit type 0800 ffff
 rule 20 permit type 0806 ffff
 rule 99 deny
```

UPnP

Universal Plug and Play (UPnP) is a distributed framework which leverages existing web technologies and network protocols for connecting different computing resources and intelligent electronic devices.

In the HP A-Series switches, the port isolation techniques described above provides full protection of UPnP traffic between subscriber ports. In addition, one can utilize ACLs to achieve fine-grained control on how UPnP network mechanisms should be filtered. For instance, the ACL configuration example above will effectively block SSDP multicast traffic utlized by UPnP devices for service discovery.

SKA-certifierad
SSNF
2010
Säker-Kund-Anslutning

For more information

For more information about the HP Networking portfolio, visit www.hp.com/networking