HP ProCurve
SKA 3.1 Certifiering

Innehållsförteckning

1. Bakgrund

Detta dokument beskriver vilka funktioner och konfigurationer som används på HP ProCurve switchar för att uppfylla de krav som sätts av SSnF för SKA 3.1 Certifiering.

2. Minimikrav för SKA 3.1

Kraven nedan är kopierade direkt från SSnFs SKA Dokument som beskriver krav och tester för SKA 3.1.

1. Så kallad DHCP-snooping ska finnas på accessportarna, d v s. en kund ska inte kunna vara DHCP-server åt någon annan kund.

2. Det ska inte gå att sätta en fast IP-adress och komma vidare från porten som kunden är ansluten i.

3. När kunden fått en eller flera adresser via DHCP ska bara den eller de adresserna kunna skicka trafik ut från den porten.

4. Om inte adressen förnyas via DHCP-servern ska den adressen stängas av i switchporten.

5. Alla typer av spoofing/poisoning ska förhindras för TCP/IP och ARP-protokollen. D v s de av DHCP godkända adresserna är de enda adresserna som ska förekomma som sourceaddress i TCP/IP och ARP paket.

6. Alla försök till spoofing/poisoning bör kunna loggas till t.ex syslogserver för att trojaner/virus och hackare ska kunna spåras.

7. Spårbarhet ska läggas in i DHCP-förfrågningarna i ”L2-läge”, accessswitchen ska inte vara DHCP-relay.

8. Det bör finnas filtreringsmöjligheter mellan kundportar så att t.ex godtyckliga TCP/UDP-portar kan filtreras bort mellan kunder

9. Om fasta IP-adresser används ska switchporten bara tillåta den för porten definierade IP-adressen som source-adress i TCP/IP och ARP-paket.

10. UPnP ska alltid vara spärrat mellan acessportar.

11. IPv6 ICMP6 router advertisment och IPv6 DHCP-servrar ska spärras mellan kundportar.

3 Beskrivning av funktioner i HP ProCurves switchar

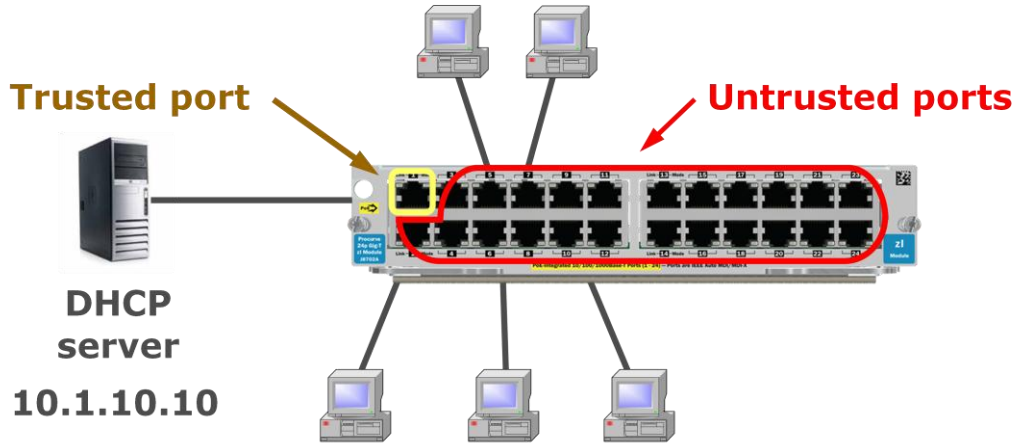
3.1 DHCP Snooping

DHCP Snooping skiljer på ”pålitliga” och ”opålitliga” portar. Funktionen används för att:

- Droppa DHCP Server paket från opålitliga portar
- Filtrera DHCP klient paket
- Bygga en databas med IP-adresser till MAC-adresser kopplat till portar

Konfiguration av DHCP Snooping

```
dhcp-snooping
dhcp-snooping vlan 10
interface a1 dhcp-snooping trust
dhcp-snooping authorized-server 10.1.10.10
```



3.2 DHCP Snooping Option 82

Med Option 82 kan switchen lägga till information i klienternas DHCP förfrågningar som DHCP Servern kan använda sig av för att applicera rätt policy på DHCP förfrågningar. Option 82 ger också möjlighet att spåra vilken IP Adress som sitter på vilken switch och vilken port.

Option 82 kan alltid läggas till DHCP Snooping är påslaget, oavsett om switchen är konfigurerad som DHCP-Relay eller inte.

Konfiguration av Option 82

```
dhcp-snooping option 82 remote-id subnet-ip
dhcp-snooping option 82 untrusted-policy replace
```

3.3 Dynamic ARP Protection

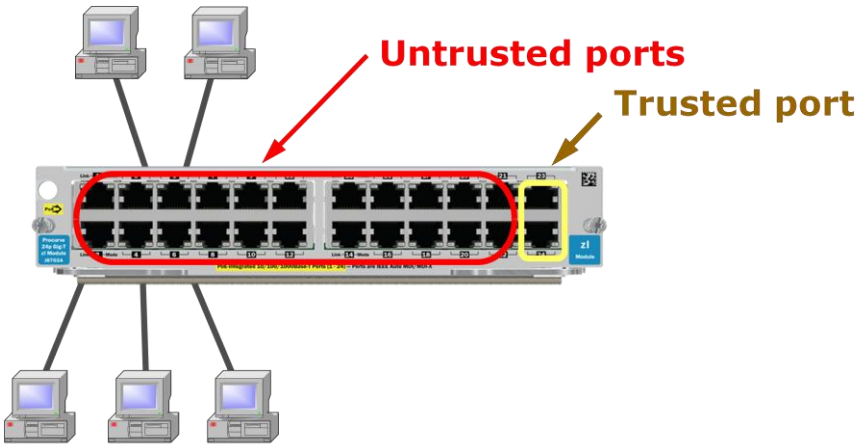
Dynamic ARP protection delar upp portarna i ”Pålitliga” och ”Opålitliga”. På ”opålitliga” portar verifierar den alla ARP förfrågningar och svar genom att jämföra den med sin IP- till MAC databas som skapas via DHCP Snooping. Detta gör det möjligt för switchen att filtrera ogiltiga ARP förfrågningar och svar.

Dynamic ARP Protection har också stöd för ytterliggare kontroller som t ex:
- Verifiering av käll MAC adress
- Verifiering av destinations MAC adress
- IP Adress

OBS!
Denna funktion kräver att DHCP Snooping är påslaget i switchen.

Konfiguration av Dynamic ARP Protection

```
arp-protect
arp-protect vlan 8
arp-protect trust a23-a24
```



3.4 Source IP Lockdown

Source IP lockdown arbetar tillsammans med DHCP Snooping för att ”låsa” en IP Adress till en specifik port för att undvika IP Spoofing.

Source IP Lockdown fungerar både för dynamiska och statiska IP adresser

OBS!
Denna funktion kräver att DHCP Snooping är påslaget i switchen.

Konfiguration av Source IP Lockdown i dynamisk miljö

```
ip source-lockdown a1-a24
```

Konfiguration av Source IP Lockdown för en statisk ”låsning”

```
ip source-binding  <vlan-id> <ip-address> <mac-address>
[ethernet] <port-number>
```

3.5 Source Port Filtering

Source Port Filtering är en funktion för att styra vilka portar som får prata med vilka oavsett VLAN tillhörighet. Det innebär att all layer 2 trafik kan filtreras eller tvingas upp till en Switch/Router och vända om användarna skall kommunicera med varandra. Denna funktion filtrerar automatiskt UpnP och IPv6 mellan användar portar.

Konfiguration av Source Port Filtering

```
filter source-port "1" drop 2-49
```

Exempelkonfiguration

```
J4899B Configuration Editor; Created on release #H.10.67

hostname "SKA_Edge"
interface 50
   name "Uplink"
exit
ip default-gateway 192.168.1.1
snmp-server community "public" Unrestricted
vlan 1
   name "DEFAULT_VLAN"
   untagged 49-50
   ip address 192.168.1.2 255.255.255.0
   no untagged 1-48
   exit
vlan 10
   name "Users"
   untagged 1-48
   tagged 50
   exit
filter source-port "1" drop 2-49
filter source-port "2" drop 1,3-49
filter source-port "3" drop 1-2,4-49
filter source-port "4" drop 1-3,5-49
filter source-port "5" drop 1-4,6-49
filter source-port "6" drop 1-5,7-49
filter source-port "7" drop 1-6,8-49
filter source-port "8" drop 1-7,9-49
filter source-port "9" drop 1-8,10-49
filter source-port "10" drop 1-9,11-49
filter source-port "11" drop 1-10,12-49
filter source-port "12" drop 1-11,13-49
filter source-port "14" drop 1-13,15-49
filter source-port "13" drop 1-12,14-49
filter source-port "15" drop 1-14,16-49
filter source-port "16" drop 1-15,17-49
filter source-port "17" drop 1-16,18-49
filter source-port "18" drop 1-17,19-49
filter source-port "19" drop 1-18,20-49
filter source-port "20" drop 1-19,21-49
filter source-port "21" drop 1-20,22-49
filter source-port "22" drop 1-21,23-49
filter source-port "23" drop 1-22,24-49
filter source-port "24" drop 1-23,25-49
filter source-port "25" drop 1-24,26-49
filter source-port "26" drop 1-25,27-49
filter source-port "27" drop 1-26,28-49
filter source-port "28" drop 1-27,29-49
filter source-port "29" drop 1-28,30-49
```

```
filter source-port "30" drop 1-29,31-49
filter source-port "31" drop 1-30,32-49
filter source-port "32" drop 1-31,33-49
filter source-port "33" drop 1-32,34-49
filter source-port "34" drop 1-33,35-49
filter source-port "35" drop 1-34,36-49
filter source-port "36" drop 1-35,37-49
filter source-port "37" drop 1-36,38-49
filter source-port "38" drop 1-37,39-49
filter source-port "39" drop 1-38,40-49
filter source-port "40" drop 1-39,41-49
filter source-port "41" drop 1-40,42-49
filter source-port "42" drop 1-41,43-49
filter source-port "43" drop 1-42,44-49
filter source-port "44" drop 1-43,45-49
filter source-port "45" drop 1-44,46-49
filter source-port "46" drop 1-45,47-49
filter source-port "47" drop 1-46,48-49
filter source-port "48" drop 1-47,49
filter source-port "49" drop 1-48
dhcp-snooping
dhcp-snooping authorized-server 10.1.10.10
dhcp-snooping option 82 untrusted-policy replace remote-id
subnet-ip
dhcp-snooping vlan 10
interface 50
   dhcp-snooping trust
   exit
ip source-lockdown 1-48
arp-protect
arp-protect trust 50
arp-protect validate src-mac
arp-protect vlan 10
```