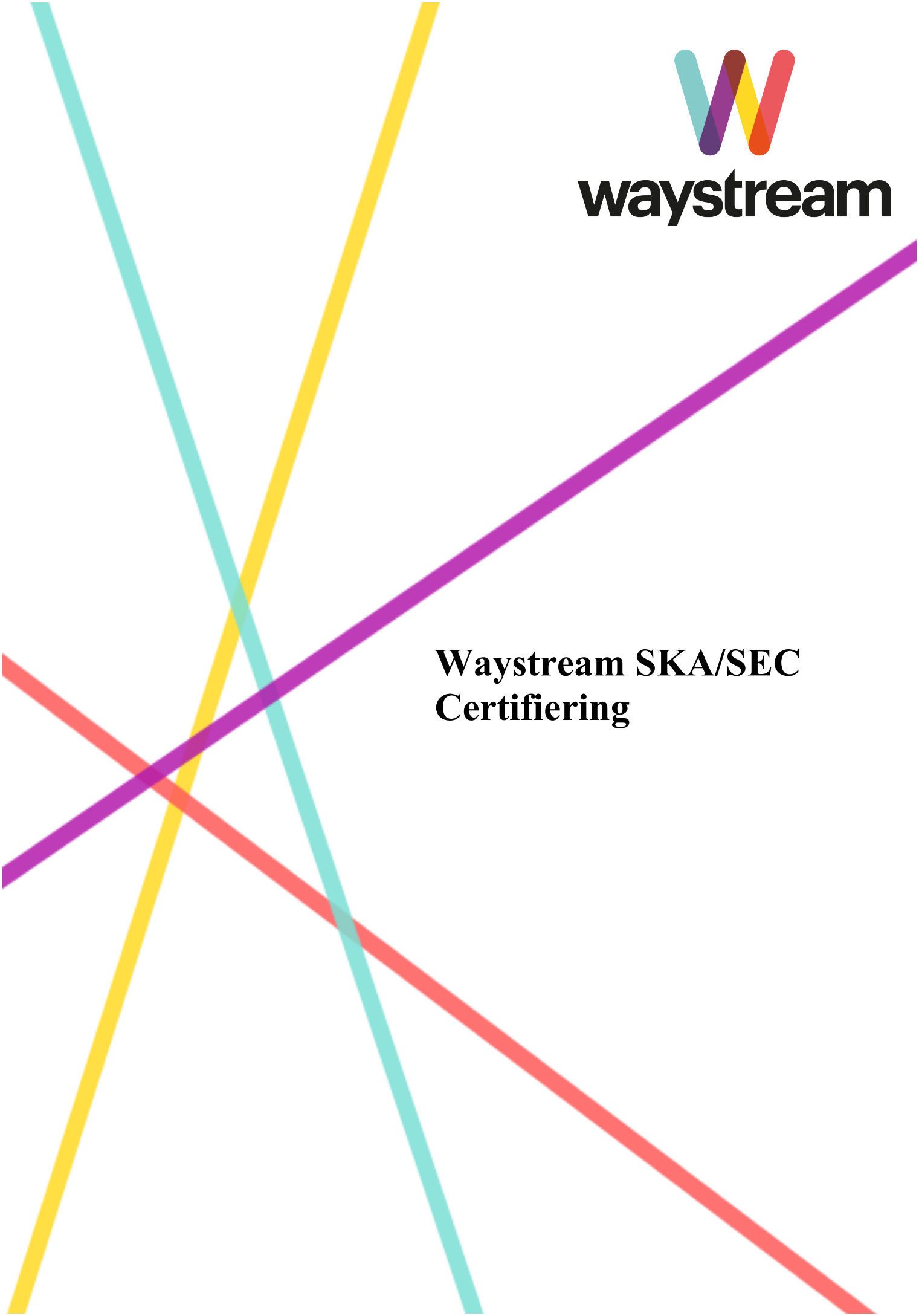

Waystream SKA/SEC Certifiering

1 Waystream

1.1 Bakgrund

Waystream är en del av det som tidigare var PacketFront.

Av det gamla PacketFront som hade en helhetslösning för öppna stadsnät med management system, routrar, switchar, samt CPEer, utvecklas och säljs idag nämnda routrar och switchar som fristående oberoende produkter av Waystream.

Routern eller layer3 switchen om man så vill, ASR6000 är den tredje generationen av ASRer, där den ursprungliga ASR4000 introducerades redan 2002.

Layer2 switchen MS4000 introducerades på marknaden 2012.

Waystreams produkter baseras på nät-operativsystemet iBOS, vilken hade fick sin första kommersiella release 2002 och har sedan dess utvecklats med funktionalitet och rättningar.

Mycket att av funktionerna i Waystreams produkter är utvecklade baserat på krav från Waystreams största kundgrupp, de nordiska stadsnäten.

1.2 Certifierade Produkter

1.2.1 ASR6000

ASR6000 är en Gigabit Ethernet baserad router/layer3 switch.

Den har 24 gigabit kundportar och två 10Gigbit upplänksportar. Den finns i två modeller, där kundportarna antingen är SFP eller RJ45 baserade.

Med en hybridarkitektur baserad på både en switch-asic och NPU, kan ”wire-speed” switching levereras i kombination med avancerade tjänste- och monitorerings funktioner.

Med ASR6000 behövs inga centrala BNGs, då den gör hela BNG funktionalisten ute i access lagret. Den kan även användas som en distribuerad BNG för att aggregera en L2 baserad access nivå.

1.2.2 MS4000

MS4000 är en Gigabit Ethernet layer2 switch.

Den har 24 gigabit kundportar och två 10Gigbit upplänksportar. Den finns i två modeller, där kundportarna antingen är SFP eller RJ45 baserade.

Med en hybridarkitektur baserad på både en switch-asic och NPU, kan ”wire-speed” switching levereras i kombination med avancerade tjänste- och monitorerings funktioner.

MS4000 är utvecklad för att sitta ute accessen i bredbandsnät och stödjer där olika topologier som C-VLAN och S-VLAN.

1.2.3 iBOS

Operativsystemet iBOS är basen i Waystreams produkter. Förutom vanlig routing och switching finns här avancerade funktioner i många fall speciellt utvecklade för öppna bredbandsnät. Exempel på det är är QoS implementeringen och scriptmotorn ScriBOS

QoS

iBOS ger möjlighet att realisera avancerade för QoS funktioner, vilka kan användas för att realisera tjänster i bredbandsnäten. Tack vare NPUn som sitter i både ASR6000 och MS4000 fås en avancerad klassificerings och schedulering mekanismen med WFQ, vilken ger både upp och nedströms shaping. En iBOS baserad enhet både läsa och sätta P-bitar och DSCP värden.

ScriBOS

Att automatisera hanteringen av bredbandsnätet har alltid varit ett signum Waystream. Då som nu kan externa management system, som BECS, Brikks, NetAdmin, etc vara en viktig pusselbit för skapa automation. Waystreams produkter innehåller även en Scriptmotor, ScriBOS, som gör att automation också kan skapas och hanteras lokalt i ASRen själv.

Exempel på funktioner där script kan köras och automatiskt utföra funktioner för konfiguration, monitorering, autentisering och accounting är DHCP, DHCPv6, 802.1x och PPPoE forwarding.

ScriBOS script för DHCP och DHCPv6 används i SKA testerna

RPM

RPM står för Real Time Protocol Monitoring. Med RPM påslaget blir iBOS en probe som kan titta på RTP strömmar och t.ex. mäta jitter och räkna tappade paket. RPM värden kan läsas ut via en MIB och t.ex. presenteras av Netrounds platform.

Mirroring

Med mirroring fås möjlighet att analysera kundtrafik med t.ex. Wireshark. Mirroring funktionen kopierar trafiken på en kundport till en annan port alternativt in i en GRE tunnel. Skickar man trafiken in i en GRE tunnel, kan andra ändan av GRE tunneln vara inne på NOCen där wireshark PCn då sitter

2 SKA/SEC IPv4

2.1 ASR6000

Då ASR6000 är en Layer3 enhet ligger klienter alltid på skilda broadcast domäner och klienter får en naturlig avgränsning där access-listor kan styra vad som skall få gå mellan klienter. Dock är implementeringen innovativt gjord, så klienter kan ha IP adresser ur samma subnät, fastän de ligger L3 mässigt skilda på olika interface

Sedan har diverse funktionalitet lagts till för att skapa ytterligare säkerhet, samt en automatiserad hantering, anpassad för sitta i bredbandsnät.

2.1.1 DHCP hantering

För DHCP hantering i SKA testerna har det inbyggda ScriBOS DHCP scriptet i kombination med en extern DHCP server använts för att hantera DHCP processen.

DHCP scriptet i ASRen triggas när en DHCP request kommer in på ett klient interface. Scriptet kan sättas upp att sätta “giaddr” till en interface IP adress i ASRen, alternativt kan DHCP option 118 användas, vilket anger vilket IP subnät man vill klienten skall ha.

Olika IP subnät kan delas ut på olika interface och ASR6000 kan också differentiera olika typer av klienter på ”vendor ID” i mac adressen. Så t.ex. om en kund har en settop box, så kan den identifieras och få en IP adress från ett subnät och en annan IP adress kan ges ut till firewall eller valfri klient för att nå Internet.

Ett exempel på det är när en DHCP förfrågan kommer in från en klient kan körs ett DHCP script automatiskt, som dels vidarebefordrar DHCP paketet till DHCP servern. När sedan en ”DHCP offer” kommer tillbaka konfigurerar scriptet upp klient interfacet för den givna adressen och lägger till en IP route i routing tabellen.

2.1.2 Säkerhetsfunktioner

ASRen har en rad säkerhetsfunktion utöver den givna access-listan

De viktigaste är “IP strict-client” på ett klient interface, vilket ger skydd mot spoofing och man-in-the-middle attacker. ScriBOS scriptet i ASR6000 för DHCP eller annat externt system konfigurerar då upp en “policy-map” där IP adress och mac-adress knyts ihop, samt att ett statiskt ARP entry läggs till för IP och mac adress. Det gör att ingen annan MAC adress eller IP adress släpps förbi på interfacet än det som faktiskt varit med i DHCP processen.

2.1.3 Tjänstehantering

Med ScriBOS DHCP scriptet hanterar man inte bara DHCP processen, utan man kan också lägga på tjänstespecifik konfiguration för den tjänst en kund använder. Det normala är att lägga på en bandbreddsbegränsning, men det finns också möjlighet att lägga på tjänstespecifik access-lista, accounting och en QoS parameter.

2.1.4 Konfigurationsbeskrivning

I konfigurationen har en tjänst som kallas ”internet_20M” lagts till på kundinterfacen.

Tjänsten definieras med ”service-definition” contexten med en ingress och egress shaper på 20Mbit/s.

DHCP server och vilka klienter som skall ha tjänsten definieras i contexten ”service-selection”. Här anges ip adress för DHCP servern, vilken source adress DHCP relay paketet skall ha, vilket IP subnät man vill ha en IP adress ur samt om DHCP option 82 om interfacet skall läggas på. Till detta anges vilka MAC Vendor ID (typisk tex matcha settop boxar eller

VoIP enheter), alternativt som i exemplet matcha alla övriga mac adresser för en Internet tjänst

2.1.5 Konfiguration ASR6000

Grundkonfiguration

I SKA testerna för IPv4 användes interface Gigbitethernet 1 mot server och Gigbitethernet 21-24 för klienter. Övriga interface är raderade i exemplet nedan.

```
ASR6K-SKA-Test# show running-config
! version ibos-asr6k-6.3.5-ED-R (ibos-asr6k-6.3.5-ED-R.bz2)
interface loopback0
 ip address 10.20.100.18 255.255.255.255
 no shutdown

interface gigabitethernet1
 ip address 10.21.254.1 255.255.255.0
 no shutdown

interface gigabitethernet21
 ip access-group cust-in in
 ip strict-clients
 arp proxy
 ip dhcp relay script
 parameter dhcp service seq 10 service-definition Internet_20M service-selection Internet_20M_IPv4
 no shutdown

interface gigabitethernet22
 ip access-group cust-in in
 ip strict-clients
 arp proxy
 ip dhcp relay script
 parameter dhcp service seq 10 service-definition Internet_20M service-selection Internet_20M_IPv4
 no shutdown

interface gigabitethernet23
 ip access-group cust-in in
 ip strict-clients
 arp proxy
 ip dhcp relay script
 parameter dhcp service seq 10 service-definition Internet_20M service-selection Internet_20M_IPv4
 no shutdown

interface gigabitethernet24
 ip access-group cust-in in
 ip strict-clients
 arp proxy
 ip dhcp relay script
 parameter dhcp service seq 10 service-definition Internet_20M service-selection Internet_20M_IPv4
 no shutdown

interface tengigabitethernet1
 no shutdown
 port uplink

interface tengigabitethernet2
 no shutdown
 port uplink

interface downstream0
 no shutdown

router ospf
 router-id 10.20.100.18
```

```
 redistribute kernel metric 10 route-map ospf_redist_kernel
 redistribute connected metric 10 route-map ospf_redist_connected
 redistribute static metric 10 route-map ospf_redist_static
 area 0.0.0.200 nssa
 network 10.20.100.18/32 area 0.0.0.200
 network 10.20.254.0/24 area 0.0.0.200

hostname ASR6K-SKA-Test

access-list cust-in
 seq 10 deny icmp any any redirect
 seq 20 deny udp any host 239.255.255.250 1900
 seq 30 deny udp any host 224.0.0.251 5353
 seq 40 deny udp any host 224.0.0.252 5355
 seq 50 deny ipv6 any any
 seq 100 permit ip any any

service-definition Internet_20M
 parameter dhcp policy-conditioner-egress shape 20000 green mark 0
 parameter dhcp policy-conditioner-ingress shape 20000 green mark 0

service-selection Internet_20M_IPv4
 parameter dhcp match snpa any relay
 parameter dhcp relay-to dhcp-server 10.21.254.10 source-interface loopback0 subnet 10.21.1.0 option-82

!end
ASR6K-SKA-Test#
```

Konfiguration när klient har anslutit

När en klient anslutit interface gigabitethernet 21 och ScriBOS DHCP scriptet körts har konfiguration lagts till av DHCP scriptet.

```
interface gigabitethernet21
 !volatile policy Internet_20M conditioner ingress shape 20000 green mark 0
 !volatile policy Internet_20M conditioner egress shape 20000 green mark 0
 !volatile policy-map 10.21.1.2/32 seq 10 policy Internet_20M
 ip strict-clients
 arp proxy
 ip dhcp relay script
 !volatile interface arp entry 10.21.1.2 0004.23b9.6209 client

interface downstream0
 !volatile ip address 10.21.1.254 255.255.255.0
 no shutdown
```

Tittar man på vilka IP interface som nu finns, så har ett downstream0 interface automatiskt lagts till av Scribos scriptet, vilket skapat default gateway adressen för klienten.

```
ASR6K-SKA-Test# sh ip int br
Interface              IP-Address      Netmask         SNPA            Protocol
------------------------------------------------------------------------------
downstream0            *10.21.1.254    255.255.255.0   0008.ae87.0240  up
loopback0              *10.20.100.18   255.255.255.255 0000.0000.0000  up
gigabitethernet1       *10.21.254.1    255.255.255.252 0008.ae87.0240  up
```

I routing tabellen finns klientnätet nu med, vilket med fördel redistribueras in i ett routing protocol.

```
ASR6K-SKA-Test# show ip route
Codes: K - kernel, C - connected, S - static, CL - client
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default
```

```
Gateway of last resort is 10.21.254.10 to network 0.0.0.0

Codes   Destination
--------------------------------------------------------------------------------
S*      0.0.0.0/0 [1/0] via 10.21.254.10, gigabitethernet1, 00:18:18
C       10.20.100.18/32 is directly connected, loopback0, 00:18:19
K CL    10.21.1.2/32 is directly connected, gogabitethernet21, 00:17:19
C       10.21.254.0/24 is directly connected, gigabitethernet1, 00:18:09
ASR6K-SKA-Test#
```

För klient subnätet 10.21.1.0/24 syns här endast hostadresser i routing tabellen och default gw adressen ligger inte med alls. Det gör att trots att ASRen är en L3 enhet, kan adresser ur ett IP subnät med automatik spridas över fler ASRer.

2.2 MS4K

I SKA testerna konfigureras en Layer2 switch som MS4000 för en S-VLAN setup, vilket är ju mer utmanande att hantera än en ren C-VLAN lösning, där varje kundinterface har sitt eget VLAN typiskt upp till en BNG (T.ex. ASR6000 kan agera i den rollen)

I SKA testerna görs ingen tjänstehantering i MS4K, det är annars möjligt att lägga på shaping och annan QoS hantering.

2.2.1 Säkerhet

För att hantera kundanslutning på ett säkert sätt finns diverse funktioner i MS4K. Grunden ligger i vad vissa kallar Private-VLAN, men i iBOS är ett UNI/NNI koncept där kundportar (UNI) bara får kommunicera mot upplänkar (NNI).

För att göra hela L2-domänen säker med flera switchar, kan MAC Forced Forwarding läggas på. Detta var dock inte del av SKA/SEC testerna

För att hindra spoofing attacker används DHCP snooping på kund porten, med vilken en policy-map dynamiskt konfigureras som gör att bara den utdelade IP adressen tillåts på porten.

Till detta kan access-listor läggas på kundporten.

2.2.2 Konfigurationsberskrivning

Kundportarna är konfigurerade för VLAN 2, vilket representerar service-vlanet. Trafiken ut på kundporten är otaggad.

På porten konfigureras om VLANet skall vara av UNI eller NNI typ. UNI representerar kundportar, NNI upplänkar.

På kundporten konfigureras DHCP snooping per VLAN. Ett logiskt VLAN interface öppnas också, då själva snoopingen knyts dit.

På kundportarna har en access-lista kallad ”cust-in” applicerats. Denna hindrar i IPv4 testerna;

- IPv6 trafik
- IP redirects
- Utvalda IP multicast grupper

Kundporten är också konfigurerad för med en ”ip dhcp auto-policy” för dynamisk konfiguration av en policy-map för en snoopad DHCP klient. Tillsammans med ”ip strict-

clients” gör detta att inga andra klienter än de som fått en DHCP adress tilldelad kan köra över från kunden. Detta säkrar upp nätet och hindrar spoofing attacker.

2.2.3 Konfiguration MS4000

Använd grundkonfiguration för MS4K

```
interface vlan2
 ip dhcp snoop information-tag
 no shutdown

interface tengigabitethernet 1
 description Uplink Interface
 vlan member 2
 vlan untagged 2
 port uplink
 port type nni vlan 2

interface gigabitethernet21
 description Customer Interface
 vlan member 2
 vlan untagged 2
port type uni vlan 2
ip dhcp snoop information-tag policy drop
ip access-group cust-in in
ip strict-clients
arp proxy
ip dhcp auto-policy-map snoop vlan 2
 no shutdown

interface gigabitethernet22
description Customer Interface
 vlan member 2
 vlan untagged 2
 port type uni vlan 2
 ip dhcp snoop information-tag policy drop
 ip access-group cust-in in
 ip strict-clients
 arp proxy
 ip dhcp auto-policy-map snoop vlan 2
 no shutdown

interface gigabitethernet23
description Customer Interface
 vlan member 2
 vlan untagged 2
 port type uni vlan 2
 ip dhcp snoop information-tag policy drop
 ip access-group cust-in in
 ip strict-clients
 arp proxy
 ip dhcp auto-policy-map snoop vlan 2
 no shutdown

interface gigabitethernet24
description Customer Interface
 vlan member 2
 vlan untagged 2
 port type uni vlan 2
 ip dhcp snoop information-tag policy drop
 ip access-group cust-in in
 ip strict-clients
 arp proxy
 ip dhcp auto-policy-map snoop vlan 2
 no shutdown

access-list cust-in
 seq 10 deny icmp any any redirect
 seq 20 deny udp any host 239.255.255.250 1900
 seq 30 deny udp any host 224.0.0.251 5353
```

```
seq 40 deny udp any host 224.0.0.252 5355
seq 50 deny ipv6 any any
seq 100 permit ip any any
```

Konfiguration när klient har anslutit

När en klient anslutit interface gigabitethernet 21 och fått en IP adress genom DHCP så lägger DHCP snooping automatiskt till en ”policy-map” rad som gör att bara klienten med den spcifika mac adressen och tillhandhållna IP adressen tillåts passera porten.

”ip strict-client” klient kommandot gör att bara klient trafik som matchas mot ”! Volatile policy-map…” kommandot släpps igenom

```
MS4K-SKA-TEST# show running-configuration context interface gigabitethernet21
! version ibos-ms4k-6.3.5-ED-R (ibos-ms4k-6.3.5-ED-R.bz2)
interface gigabitethernet21
 !volatile policy-map vid 2 snpa 0011.43f2.7e97 10.21.1.1/32 seq 10 policy
 vlan member 2
 vlan untagged 2
 port type uni vlan 2
 ip dhcp snoop information-tag policy drop
 ip access-group cust-in in
 ip strict-clients
 arp proxy
 ip dhcp auto-policy-map snoop vlan 2
 no shutdown
```

Show clients kommandot kan användas för att se vilka klienter som är snoopade

```
MS4K-SKA-TEST# show clients
Address        SNPA          Lease      Type   Interface
-------------------------------------------------------------------------------
10.21.1.1      0011.43f2.7e97  T-74       snoop  gigabitethernet21

MS4K-SKA-TEST# show clients detailed

  L2 Interface : gigabitethernet21
     Interface : vlan2
    IP Address : 10.21.1.1
         SNPA : 0011.43f2.7e97
         Type : DHCP (Snooped)
    Created on : Thu May 26 11:34:25 2016
    Expires in : 1m6s
      Last in : INFORM (16s ago)
     Last out : ACK (24s ago)
  Broadcast in : 4
    Unicast in : 0
       Vendor : "MSFT 5.0"
     option_1 : "255.255.255.0"
     option_3 : "10.21.1.254"
    option_12 : "way-pc06"
    option_43 : "\xdc\x01\x00"
    option_46 : "\x08"
    option_50 : "10.21.1.1"
    option_51 : "90"
    option_53 : "INFORM"
    option_54 : "10.21.254.10"
    option_55 : "1 15 3 6 44 46 47 31 33 249 43 252"
    option_60 : "MSFT 5.0"
    option_61 : "ether 0011.43f2.7e97"
    option_81 : "\x00\x00\x00way-janbjo.int.waystream.com"
    option_82 : "circuit-id: gigabitethernet23\x002 remote-id: 0008AE8915A0"
   option_116 : "\x01"
   option_255 : ""
```