# Physical Topology

#

# Logical Topology



Please, note that the configurations given below can certainly be clean-up and tuned. Some commands are still embedded for testing purposes.

Note also that the text highlighted in yellow delimits the optional CLI configuration for the LISP Map-server as a backup mechanism used for the endpoint notifications, however it is strongly recommended to enable the map-server.

# DC-1

## LISP IGP ASSIST

hostname DC-1-App

feature ospf

feature pim

feature lisp

feature interface-vlan

feature hsrp

username admin password 5 $5$Kmvcx74m$O72Q6kalrKvrI2YUSuWZNSn9uOJ9DvDRdThjJIICE43  role vdc-admin

no password strength-check

ip domain-lookup

snmp-server user admin vdc-admin auth md5 0x97398a8af05b050f6493212b17e58757 priv 0x97398a8af05b050f6493212b17e58757 localizedkey

rmon event 1 log description FATAL(1) owner PMON@FATAL

rmon event 2 log description CRITICAL(2) owner PMON@CRITICAL

rmon event 3 log description ERROR(3) owner PMON@ERROR

rmon event 4 log description WARNING(4) owner PMON@WARNING

rmon event 5 log description INFORMATION(5) owner PMON@INFO

ip pim rp-address 10.10.10.10 group-list 224.0.0.0/4

ip pim ssm range 232.0.0.0/8

!

! Start:

! LISP MAP-SERVER Alternative notification process

! This is optional but recommended as alternative/backup

! solution for EID notification

ip lisp itr-etr

ip lisp map-server

lisp site DATA\_CENTER

  eid-prefix 10.1.0.0/16 instance-id 1 accept-more-specifics

  eid-prefix 20.1.0.0/16 instance-id 2 accept-more-specifics

  authentication-key 3 9125d59c18a9b015

ip lisp locator-vrf default

ip lisp etr map-server 10.10.10.10 key 3 9125d59c18a9b015

ip lisp etr map-server 20.20.20.20 key 3 9125d59c18a9b015

!

! End-of LISP MAP-SERVER

!

vlan 1,10,20,100,200,210

ip prefix-list HOST-ROUTES seq 5 permit 0.0.0.0/0 eq 32

route-map ADV-HOST-ROUTES deny 5

  match interface Null0

route-map ADV-HOST-ROUTES permit 10

  match ip address prefix-list HOST-ROUTES

vrf context GREEN

  ip pim ssm range 232.0.0.0/8

  ip lisp itr-etr

  lisp instance-id 2

  ip lisp locator-vrf default

  lisp dynamic-eid LISP\_EXTENDED\_SUBNET

    database-mapping 20.1.1.0/24 10.10.10.10 priority 1 weight 50

    map-notify-group 239.1.1.2

    no route-export away-dyn-eid

vrf context RED

  ip pim ssm range 232.0.0.0/8

  ip lisp itr-etr

  lisp instance-id 1

  ip lisp locator-vrf default

  lisp dynamic-eid LISP\_EXTENDED\_SUBNET

    database-mapping 10.1.1.0/24 10.10.10.10 priority 1 weight 50

    map-notify-group 239.1.1.1

    no route-export away-dyn-eid

vrf context management

interface mgmt0

  vrf member management

interface Vlan10

  no shutdown

  vrf member RED

  lisp mobility LISP\_EXTENDED\_SUBNET

  lisp extended-subnet-mode

  ip address 10.1.1.251/24

  ip ospf passive-interface

  ip pim sparse-mode

  hsrp 10

    preempt

    priority 110

    ip 10.1.1.254

interface Vlan20

  no shutdown

  vrf member GREEN

  lisp mobility LISP\_EXTENDED\_SUBNET

  lisp extended-subnet-mode

  ip address 20.1.1.251/24

  ip ospf passive-interface

  ip pim sparse-mode

  hsrp 20

    preempt

    priority 110

    ip 20.1.1.254

interface Vlan100

  no shutdown

  vrf member RED

  ip address 100.1.1.10/24

  ip router ospf 100 area 0.0.0.0

interface Vlan200

  no shutdown

  vrf member GREEN

  ip address 200.1.1.10/24

  ip router ospf 100 area 0.0.0.0

interface Ethernet1/7

  mtu 9216

  ip address 9.9.9.1/24

  ip ospf network point-to-point

  ip router ospf 1 area 0.0.0.0

  ip pim sparse-mode

  no shutdown

interface Ethernet1/17

  switchport

  switchport mode trunk

  switchport trunk allowed vlan 10,20,210

interface Ethernet1/18

  switchport

  switchport access vlan 100

interface Ethernet1/19

  switchport

  switchport access vlan 10

interface Ethernet1/26

  switchport

  switchport access vlan 200

interface Ethernet1/27

  switchport

  switchport access vlan 20

interface Ethernet1/28

  ip address 192.168.1.1/24

  ip ospf network point-to-point

  ip router ospf 1 area 0.0.0.0

  ip pim sparse-mode

  no shutdown

interface loopback10

  description LISP Loopback

  ip address 10.10.10.10/32

  ip router ospf 1 area 0.0.0.0

  ip pim sparse-mode

cli alias name wr copy run start

cli alias name back switchback

line vty

router ospf 100

  router-id 1.1.1.1

  vrf GREEN

    redistribute lisp route-map ADV-HOST-ROUTES

  vrf RED

    redistribute lisp route-map ADV-HOST-ROUTES

no system default switchport shutdown

## ASA Firewall

ASA Version 9.1(5)

!

hostname FW-DC-1

enable password B2OJ16CjxKNubigD encrypted

names

!

interface GigabitEthernet0/0

 nameif RED

 security-level 100

 ip address 100.1.1.254 255.255.255.0

 ospf cost 10

 ospf authentication null

!

interface GigabitEthernet0/1

 nameif GREEN

 security-level 100

 ip address 200.1.1.254 255.255.255.0

 ospf cost 10

 ospf authentication null

!

interface GigabitEthernet0/2

 nameif Inter-DMZ

 security-level 100

 ip address 30.1.1.1 255.255.255.0

 ospf cost 10

 ospf authentication null

!

!

interface Management0/0

 management-only

 nameif management

 security-level 100

 ip address 10.60.9.142 255.255.255.0

!

banner login Viva España

ftp mode passive

same-security-traffic permit inter-interface

same-security-traffic permit intra-interface

object-group icmp-type ICMP-traceroute-full

 description Allo ICMP Traceroute

 icmp-object echo

 icmp-object echo-reply

 icmp-object information-reply

 icmp-object information-request

 icmp-object mask-reply

 icmp-object mask-request

 icmp-object time-exceeded

 icmp-object traceroute

 icmp-object unreachable

 icmp-object alternate-address

 icmp-object conversion-error

 icmp-object mobile-redirect

 icmp-object parameter-problem

 icmp-object redirect

 icmp-object router-advertisement

 icmp-object router-solicitation

 icmp-object source-quench

 icmp-object timestamp-reply

 icmp-object timestamp-request

access-list RED\_access\_in extended permit icmp any any

access-list RED\_access\_in extended permit tcp any any eq ssh

access-list RED\_access\_in extended permit icmp any any object-group ICMP-traceroute-full

access-list GREEN\_access\_in extended permit icmp any any

access-list GREEN\_access\_in extended permit tcp any any eq ssh

access-list GREEN\_access\_in extended permit icmp any any object-group ICMP-traceroute-full

access-list Inter-DMZ\_access\_in extended permit icmp any any

access-list Inter-DMZ\_access\_in extended permit tcp any any eq ssh

access-list Inter-DMZ\_access\_in extended permit icmp any any object-group ICMP-traceroute-full

pager lines 24

logging asdm informational

mtu RED 1500

mtu GREEN 1500

mtu Inter-DMZ 1500

mtu management 1500

no failover

icmp unreachable rate-limit 1 burst-size 1

asdm image disk0:/asdm.bin

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

access-group RED\_access\_in in interface RED

access-group GREEN\_access\_in in interface GREEN

access-group Inter-DMZ\_access\_in in interface Inter-DMZ

!

router ospf 100

 router-id 10.1.1.5

 network 30.1.1.0 255.255.255.0 area 0

 network 100.1.1.0 255.255.255.0 area 0

 network 200.1.1.0 255.255.255.0 area 0

 area 0

 log-adj-changes

!

route management 0.0.0.0 0.0.0.0 10.60.9.254 1

timeout xlate 3:00:00

timeout pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00

timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

timeout tcp-proxy-reassembly 0:01:00

timeout floating-conn 0:00:00

dynamic-access-policy-record DfltAccessPolicy

user-identity default-domain LOCAL

aaa authentication telnet console LOCAL

aaa authentication ssh console LOCAL

http server enable

http server idle-timeout 30

http 10.60.9.0 255.255.255.0 management

http 0.0.0.0 0.0.0.0 management

no snmp-server location

no snmp-server contact

snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

crypto ipsec security-association pmtu-aging infinite

crypto ca trustpool policy

telnet 0.0.0.0 0.0.0.0 management

telnet timeout 1440

no ssh stricthostkeycheck

ssh 0.0.0.0 0.0.0.0 management

ssh timeout 60

ssh key-exchange group dh-group1-sha1

console timeout 0

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

username admin password zhS.hbQ2iQKjyhpF encrypted privilege 15

username cisco password ekb1Pkkpej1hIT.O encrypted privilege 15

!

class-map inspection\_default

 match default-inspection-traffic

!

!

policy-map type inspect dns preset\_dns\_map

 parameters

 message-length maximum client auto

 message-length maximum 512

policy-map global\_policy

 class inspection\_default

 inspect dns preset\_dns\_map

 inspect ftp

 inspect h323 h225

 inspect h323 ras

 inspect rsh

 inspect rtsp

 inspect esmtp

 inspect sqlnet

 inspect skinny

 inspect sunrpc

 inspect xdmcp

 inspect sip

 inspect netbios

 inspect tftp

 inspect ip-options

!

service-policy global\_policy global

prompt hostname context

no call-home reporting anonymous

Cryptochecksum:9f88aabe3c0409315eb521677fb89348

: end

FW-DC-1#

## OTV

!Command: show running-config

!Time: Sat Feb  6 18:17:11 1971

version 7.3(0)DX(1)

switchname DC1-OTV

feature ospf

feature pim

feature otv

feature dhcp

username admin password 5 $5$rppyiE/a$8w/uABrL/FW/em9BHvgrHYMBtZjNIuF89vX5s1MEGv

/  role vdc-admin

no password strength-check

ip domain-lookup

ip access-list ALL\_IPs

  10 permit ip any any

mac access-list ALL\_MACs

  10 permit any any

ip access-list HSRP\_IP

  10 permit udp any 224.0.0.2/32 eq 1985

  20 permit udp any 224.0.0.102/32 eq 1985

mac access-list HSRP\_VMAC

  10 permit 0000.0c07.ac00 0000.0000.00ff any

  20 permit 0000.0c9f.f000 0000.0000.0fff any

arp access-list HSRP\_VMAC\_ARP

  10 deny ip any mac 0000.0c07.ac00 ffff.ffff.ff00

  20 deny ip any mac 0000.0c9f.f000 ffff.ffff.f000

  30 permit ip any mac any

vlan access-map HSRP\_Localization 10

        match mac address HSRP\_VMAC

        match ip address HSRP\_IP

        action drop

vlan access-map HSRP\_Localization 20

        match mac address ALL\_MACs

        match ip address ALL\_IPs

        action forward

vlan filter HSRP\_Localization vlan-list 10,20

snmp-server user admin vdc-admin auth md5 0x4dbc65fadfdc7c5b02e1f697a648b4ff pri

v 0x4dbc65fadfdc7c5b02e1f697a648b4ff localizedkey

rmon event 1 log description FATAL(1) owner PMON@FATAL

rmon event 2 log description CRITICAL(2) owner PMON@CRITICAL

rmon event 3 log description ERROR(3) owner PMON@ERROR

rmon event 4 log description WARNING(4) owner PMON@WARNING

rmon event 5 log description INFORMATION(5) owner PMON@INFO

vlan 1,10,20,210

otv site-vlan 210

mac-list HSRP-vmac-deny seq 5 deny 0000.0c07.ac00 ffff.ffff.ff00

mac-list HSRP-vmac-deny seq 10 deny 0000.0c9f.f000 ffff.ffff.f000

mac-list HSRP-vmac-deny seq 20 permit 0000.0000.0000 0000.0000.0000

route-map stop-HSRP permit 10

  match mac-list HSRP-vmac-deny

service dhcp

ip dhcp relay

ipv6 dhcp relay

vrf context management

interface mgmt0

  vrf member management

interface Overlay1

  otv join-interface Ethernet1/10

  otv control-group 239.1.1.100

  otv data-group 232.10.1.0/24

  otv extend-vlan 10, 20

  no shutdown

interface Ethernet1/9

  switchport

  switchport mode trunk

  switchport trunk allowed vlan 10,20,210

interface Ethernet1/10

  ip address 192.168.1.2/24

  ip ospf network point-to-point

  ip router ospf 1 area 0.0.0.0

  ip igmp version 3

  no shutdown

interface Ethernet1/16

  no shutdown

cli alias name wr copy run start

cli alias name back switchback

line vty

router ospf 1

  router-id 1.1.1.1

otv-isis default

  vpn Overlay1

    redistribute filter route-map stop-HSRP

otv site-identifier 0001.0001.0001

no system default switchport shutdown

ip arp inspection filter HSRP\_VMAC\_ARP vlan 10,20

# DC-2

## LISP IGP ASSIST

!Command: show running-config

!Time: Wed Dec 21 19:09:58 2016

version 7.3(0)DX(1)

hostname DC-2-App

feature ospf

feature pim

feature lisp

feature interface-vlan

feature hsrp

username admin password 5 $5$xwoustla$VlvkLOCJ2Hob.CTUF39xInRaZCGjWpjwapeEugB1.h5  role vdc-admin

no password strength-check

ip domain-lookup

snmp-server user admin vdc-admin auth md5 0x268770638e60cdb13100bdf706cfcd40 priv 0x268770638e60cdb13100bdf706cfcd40 localizedkey

rmon event 1 log description FATAL(1) owner PMON@FATAL

rmon event 2 log description CRITICAL(2) owner PMON@CRITICAL

rmon event 3 log description ERROR(3) owner PMON@ERROR

rmon event 4 log description WARNING(4) owner PMON@WARNING

rmon event 5 log description INFORMATION(5) owner PMON@INFO

ip pim rp-address 10.10.10.10 group-list 224.0.0.0/4

ip pim ssm range 232.0.0.0/8

!

! Start:

! LISP MAP-SERVER Alternative notification process

! This is optional but recommended as alternative/backup

! solution for EID notification

ip lisp itr-etr

ip lisp map-server

lisp site DATA\_CENTER

  eid-prefix 10.1.0.0/16 instance-id 1 accept-more-specifics

  eid-prefix 20.1.0.0/16 instance-id 2 accept-more-specifics

  authentication-key 3 9125d59c18a9b015

ip lisp locator-vrf default

ip lisp etr map-server 10.10.10.10 key 3 9125d59c18a9b015

ip lisp etr map-server 20.20.20.20 key 3 9125d59c18a9b015

!

! End-of LISP MAP-SERVER

!

vlan 1,10,20,100,200,210

ip prefix-list HOST-ROUTES seq 5 permit 0.0.0.0/0 eq 32

route-map ADV-HOST-ROUTES deny 5

  match interface Null0

route-map ADV-HOST-ROUTES permit 10

  match ip address prefix-list HOST-ROUTES

vrf context GREEN

  ip pim ssm range 232.0.0.0/8

  ip lisp itr-etr

  lisp instance-id 2

  ip lisp locator-vrf default

  lisp dynamic-eid LISP\_EXTENDED\_SUBNET

    database-mapping 20.1.1.0/24 20.20.20.20 priority 1 weight 50

    map-notify-group 239.1.1.2

    no route-export away-dyn-eid

vrf context RED

  ip pim ssm range 232.0.0.0/8

  ip lisp itr-etr

  lisp instance-id 1

  ip lisp locator-vrf default

  lisp dynamic-eid LISP\_EXTENDED\_SUBNET

    database-mapping 10.1.1.0/24 20.20.20.20 priority 1 weight 50

    map-notify-group 239.1.1.1

    no route-export away-dyn-eid

vrf context management

interface mgmt0

  vrf member management

interface Vlan1

interface Vlan10

  no shutdown

  vrf member RED

  lisp mobility LISP\_EXTENDED\_SUBNET

  lisp extended-subnet-mode

  ip address 10.1.1.252/24

  ip ospf passive-interface

  ip pim sparse-mode

  hsrp 10

    preempt

    priority 120

    ip 10.1.1.254

interface Vlan20

  no shutdown

  vrf member GREEN

  lisp mobility LISP\_EXTENDED\_SUBNET

  lisp extended-subnet-mode

  ip address 20.1.1.252/24

  ip ospf passive-interface

  ip pim sparse-mode

  hsrp 20

    preempt

    priority 120

    ip 20.1.1.254

interface Vlan100

  no shutdown

  vrf member RED

  ip address 102.1.1.20/24

  ip router ospf 100 area 0.0.0.0

interface Vlan200

  no shutdown

  vrf member GREEN

  ip address 202.1.1.20/24

  ip router ospf 100 area 0.0.0.0

interface Ethernet1/7

  mtu 9216

  ip address 9.9.9.2/24

  ip ospf network point-to-point

  ip router ospf 1 area 0.0.0.0

  ip pim sparse-mode

  no shutdown

interface Ethernet1/17

  switchport

  switchport mode trunk

  switchport trunk allowed vlan 10,20,210

interface Ethernet1/18

  switchport

  switchport access vlan 100

interface Ethernet1/19

  switchport

  switchport access vlan 10

interface Ethernet1/26

  switchport

  switchport access vlan 200

interface Ethernet1/27

  switchport

  switchport access vlan 20

interface Ethernet1/28

  ip address 192.168.2.1/24

  ip ospf network point-to-point

  ip router ospf 1 area 0.0.0.0

  ip pim sparse-mode

  no shutdown

interface loopback20

  description LISP Loopback

  ip address 20.20.20.20/24

  ip router ospf 1 area 0.0.0.0

  ip pim sparse-mode

cli alias name wr copy run start

cli alias name back switchback

line vty

router ospf 100

  router-id 1.1.1.2

  vrf GREEN

    redistribute lisp route-map ADV-HOST-ROUTES

  vrf RED

    redistribute lisp route-map ADV-HOST-ROUTES

no system default switchport shutdown

## ASA Firewall

ASA Version 9.5(1)

!

hostname FW-DC-2

enable password B2OJ16CjxKNubigD encrypted

names

!

interface GigabitEthernet0/0

 nameif RED

 security-level 100

 ip address 102.1.1.254 255.255.255.0

 ospf cost 10

 ospf authentication null

!

interface GigabitEthernet0/1

 nameif GREEN

 security-level 100

 ip address 202.1.1.254 255.255.255.0

 ospf cost 10

 ospf authentication null

!

interface GigabitEthernet0/2

 nameif Inter-DMZ

 security-level 100

 ip address 30.1.1.2 255.255.255.0

 ospf cost 10

 ospf authentication null

!

interface GigabitEthernet0/3

 shutdown

 no nameif

 no security-level

 no ip address

!

interface GigabitEthernet0/4

 shutdown

 no nameif

 no security-level

 no ip address

!

interface GigabitEthernet0/5

 shutdown

 no nameif

 no security-level

 no ip address

!

interface GigabitEthernet0/6

 shutdown

 no nameif

 no security-level

 no ip address

!

interface GigabitEthernet0/7

 shutdown

 no nameif

 no security-level

 no ip address

!

interface Management0/0

 management-only

 nameif management

 security-level 100

 ip address 10.60.9.143 255.255.255.0

!

ftp mode passive

same-security-traffic permit inter-interface

same-security-traffic permit intra-interface

object-group icmp-type ICMP-Traceroute-full

 icmp-object alternate-address

 icmp-object conversion-error

 icmp-object echo

 icmp-object echo-reply

 icmp-object information-reply

 icmp-object information-request

 icmp-object mask-reply

 icmp-object mask-request

 icmp-object mobile-redirect

 icmp-object parameter-problem

 icmp-object redirect

 icmp-object router-advertisement

 icmp-object router-solicitation

 icmp-object source-quench

 icmp-object time-exceeded

 icmp-object timestamp-reply

 icmp-object timestamp-request

 icmp-object traceroute

 icmp-object unreachable

access-list GREEN\_access\_in remark ICMP

access-list GREEN\_access\_in extended permit icmp any any

access-list GREEN\_access\_in extended permit tcp any any eq ssh

access-list GREEN\_access\_in extended permit icmp any any traceroute

access-list RED\_access\_in remark icmp

access-list RED\_access\_in extended permit icmp any any

access-list RED\_access\_in extended permit tcp any any eq ssh

access-list RED\_access\_in extended permit icmp any any traceroute

access-list Inter-DMZ\_access\_in remark icmp

access-list Inter-DMZ\_access\_in extended permit icmp any any

access-list Inter-DMZ\_access\_in extended permit tcp any any eq ssh

access-list Inter-DMZ\_access\_in extended permit icmp any any traceroute

access-list Inter-DMZ\_access\_in extended deny icmp host 10.1.1.2 any inactive

pager lines 24

logging asdm informational

mtu RED 1500

mtu GREEN 1500

mtu Inter-DMZ 1500

mtu management 1500

no failover

no monitor-interface service-module

icmp unreachable rate-limit 1 burst-size 1

asdm image disk0:/asdm.bin

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

access-group RED\_access\_in in interface RED

access-group GREEN\_access\_in in interface GREEN

access-group Inter-DMZ\_access\_in in interface Inter-DMZ

router ospf 100

 router-id 10.1.1.6

 network 30.1.1.0 255.255.255.0 area 0

 network 102.1.1.0 255.255.255.0 area 0

 network 202.1.1.0 255.255.255.0 area 0

 area 0

 log-adj-changes

!

route management 0.0.0.0 0.0.0.0 10.60.9.254 1

timeout xlate 3:00:00

timeout pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00

timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

timeout tcp-proxy-reassembly 0:01:00

timeout floating-conn 0:00:00

user-identity default-domain LOCAL

aaa authentication telnet console LOCAL

aaa authentication ssh console LOCAL

http server enable

http server idle-timeout 30

http 10.60.9.0 255.255.255.0 management

http 0.0.0.0 0.0.0.0 management

no snmp-server location

no snmp-server contact

crypto ipsec security-association pmtu-aging infinite

crypto ca trustpoint \_SmartCallHome\_ServerCA

 no validation-usage

 crl configure

crypto ca trustpool policy

crypto ca certificate chain \_SmartCallHome\_ServerCA

 certificate ca 6ecc7aa5a7032009b8cebcf4e952d491

telnet 0.0.0.0 0.0.0.0 management

telnet timeout 1440

no ssh stricthostkeycheck

ssh 0.0.0.0 0.0.0.0 management

ssh timeout 60

ssh key-exchange group dh-group1-sha1

console timeout 0

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

dynamic-access-policy-record DfltAccessPolicy

username admin password zhS.hbQ2iQKjyhpF encrypted privilege 15

!

class-map inspection\_default

 match default-inspection-traffic

!

!

policy-map type inspect dns preset\_dns\_map

 parameters

 message-length maximum client auto

 message-length maximum 512

policy-map global\_policy

 class inspection\_default

 inspect dns preset\_dns\_map

 inspect ftp

 inspect h323 h225

 inspect h323 ras

 inspect rsh

 inspect rtsp

 inspect esmtp

 inspect sqlnet

 inspect skinny

 inspect sunrpc

 inspect xdmcp

 inspect sip

 inspect netbios

 inspect tftp

 inspect ip-options

!

service-policy global\_policy global

prompt hostname context

call-home reporting anonymous

Cryptochecksum:e897f5686b469fa4ee43d8dcefbf5870

: end

## OTV

version 7.3(0)DX(1)

switchname DC-2-OTV

feature ospf

feature pim

feature otv

feature dhcp

username admin password 5 $5$JVgTenQM$Zdy2/wZyjvw/Qn9hY0atYiWenNSgw3pefQ0feL1SVe

3  role vdc-admin

no password strength-check

ip domain-lookup

ip access-list ALL\_IPs

  10 permit ip any any

mac access-list ALL\_MACs

  10 permit any any

ip access-list HSRP\_IP

  10 permit udp any 224.0.0.2/32 eq 1985

  20 permit udp any 224.0.0.102/32 eq 1985

mac access-list HSRP\_VMAC

  10 permit 0000.0c07.ac00 0000.0000.00ff any

  20 permit 0000.0c9f.f000 0000.0000.0fff any

arp access-list HSRP\_VMAC\_ARP

  10 deny ip any mac 0000.0c07.ac00 ffff.ffff.ff00

  20 deny ip any mac 0000.0c9f.f000 ffff.ffff.f000

  30 permit ip any mac any

vlan access-map HSRP\_Localization 10

        match mac address HSRP\_VMAC

        match ip address HSRP\_IP

        action drop

vlan access-map HSRP\_Localization 20

        match mac address ALL\_MACs

        match ip address ALL\_IPs

        action forward

vlan filter HSRP\_Localization vlan-list 10,20

snmp-server user admin vdc-admin auth md5 0xe7d5cd2da086e568a44184f4fefd3c76 pri

v 0xe7d5cd2da086e568a44184f4fefd3c76 localizedkey

rmon event 1 log description FATAL(1) owner PMON@FATAL

rmon event 2 log description CRITICAL(2) owner PMON@CRITICAL

rmon event 3 log description ERROR(3) owner PMON@ERROR

rmon event 4 log description WARNING(4) owner PMON@WARNING

rmon event 5 log description INFORMATION(5) owner PMON@INFO

vlan 1,10,20,210

otv site-vlan 210

mac-list HSRP-vmac-deny seq 5 deny 0000.0c07.ac00 ffff.ffff.ff00

mac-list HSRP-vmac-deny seq 10 deny 0000.0c9f.f000 ffff.ffff.f000

mac-list HSRP-vmac-deny seq 20 permit 0000.0000.0000 0000.0000.0000

route-map stop-HSRP permit 10

  match mac-list HSRP-vmac-deny

service dhcp

ip dhcp relay

ipv6 dhcp relay

vrf context management

interface mgmt0

  vrf member management

interface Overlay1

  otv join-interface Ethernet1/10

  otv control-group 239.1.1.100

  otv data-group 232.10.1.0/24

  otv extend-vlan 10, 20

  no shutdown

interface Ethernet1/9

  switchport

  switchport mode trunk

  switchport trunk allowed vlan 10,20,210

interface Ethernet1/10

  ip address 192.168.2.2/24

  ip ospf network point-to-point

  ip router ospf 1 area 0.0.0.0

  ip igmp version 3

  no shutdown

interface Ethernet1/16

cli alias name wr copy run start

cli alias name back switchback

line vty

router ospf 1

  router-id 2.2.2.2

otv-isis default

  vpn Overlay1

    redistribute filter route-map stop-HSRP

otv site-identifier 0002.0002.0002

no system default switchport shutdown

ip arp inspection filter HSRP\_VMAC\_ARP vlan 10,20