Technical Documentation – Addressing & Configuration

---

1. Overview

This section documents the IP addressing scheme used throughout the network and serves as a technical reference for configuration and troubleshooting.

Design principles:

- Clear functional separation by subnet
- Summarizable and scalable addressing
- One subnet per security or service domain
- Redundant default gateways via HSRP

All routing, firewall rules, and services are based on this addressing plan.

---

2. IP Addressing Schema

2.1 Management Network

Purpose	Subnet	Notes
Device Management	192.168.10.0 /24	Switches, infrastructure management
Default Gateway (HSRP)	192.168.10.1	Core MLS virtual IP

2.2 User LAN

Purpose	Subnet	Notes
Wired User Network	172.16.0.0 /16	All departments
Default Gateway (HSRP)	172.16.0.1	Core MLS virtual IP

2.3 Wireless LAN

Purpose	Subnet	Notes
WLAN Clients	10.20.0.0 /16	Centrally managed by WLC
Default Gateway (HSRP)	10.20.0.1	Core MLS virtual IP

2.4 VoIP Network

Purpose	Subnet	Notes
Voice VLAN	172.30.0.0 /16	IP Phones & CME
Default Gateway	172.30.0.1	Voice Gateway Router
DHCP Option 150	172.30.0.1	TFTP / Call Manager

2.5 Inside Server Network

Purpose	Subnet	Notes
Internal Servers	10.11.11.32 /27	DHCP, DNS, RADIUS
Default Gateway (HSRP)	10.11.11.33	Core MLS virtual IP

Server	IP Address
RADIUS	10.11.11.36
DNS	10.11.11.37
DHCP	10.11.11.38

2.6 DMZ Network

Purpose	Subnet	Notes
DMZ Servers	10.11.11.0 /27	Public-facing services
Default Gateway	10.11.11.1	Firewall DMZ interface

2.7 Transit & Point-to-Point Networks

Link	Subnet
Core ↔ Firewall	10.2.2.0 /30, 10.2.2.4 /30
Firewall ↔ ISP A	105.100.50.0 /30
Firewall ↔ ISP B	197.200.100.0 /30
ISP ↔ Cloud	20.20.20.0 /30, 30.30.30.0 /30

---

3. Configuration Sections

The following sections contain device-specific configuration commands based on the addressing schema above.

- Access Switch Configuration
- Core Multilayer Switch Configuration
- Firewall Configuration
- Routing (OSPF)
- Wireless Controller Configuration
- VoIP Gateway Configuration

Each section is intentionally kept command-focused without additional explanation.

Configuration Reference & Verification

Note: verifiation screen shots can be found sperately

Access Switch – Base Configuration with SSH resticted Access

en
conf t
hostname SM-SW
line console 0
password cisco
login
exec-timeout 3 0
logging synchronous
exit

enable password cisco
banner motd ##ONLY AUTHORISED ACCESS!!##
no ip domain-lookup
service password-encryption

username cisco password cisco
ip domain-name cisco.com
crypto key generate rsa general-key modulus 1024

ip ssh version 2
line vty 0 4
login local
transport input ssh
end
wr

access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 deny any
line vty 0 4
access-class 1 in
exit
do wr

show run | section line vty
show ip ssh
sho users

VLAN Configuration (Access Switch)

int range fa0/1-2
switchport mode trunk
switchport trunk native vlan 891

vlan 10
name MGT
vlan 20
name LAN
vlan 50
name WLAN
vlan 70
name VOIP
vlan 199
name BLACKHOLE
exit

int fa0/3
switchport mode access
switchport access vlan 20
exit

int fa0/7
switchport mode access
switchport access vlan 20
exit

int fa0/4
switchport mode access
switchport voice vlan 70
exit

int fa0/6
switchport mode access
switchport voice vlan 70
exit

int fa0/5
switchport mode access
switchport access vlan 50

exit

int range fa0/8-24
switchport mode access
switchport access vlan 199
shut
exit

int range gig0/1-2
switchport mode access
switchport access vlan 199
shut
exit
do wr

INSIDE SERVER SW

int range fa0/1-3
switchport mode trunk
switchport trunk native vlan 891

vlan 10
name MGT
vlan 20
name LAN
vlan 50
name WLAN
vlan 70
name VOIP
vlan 90
name INSIDE-SERVER
exit

int fa0/4
switchport mode access
switchport access vlan 50

int range fa0/5-7
switchport mode access
switchport access vlan 90
end wr

CORE-MLSs

int range gig1/0/3-8
switchport mode trunk
switchport trunk native vlan 891

vlan 10
name MGT

vlan 20
name LAN
vlan 50
name WLAN
vlan 70
name VOIP
vlan 90
name INSIDE-SERVER
end
wr

show vlan brief

SPANNING TREE & BPDUGUARD

INSIDER SERVER SW

int range fa0/4-24
spanning-tree portfast
spanning-tree bpduguard enable

ACCESS SW

conf t
int range f0/3-24
spanning-tree portfast
spanning-tree bpduguard enable
end
wr

DMZ SW

conf t
int range f0/1-24
spanning-tree portfast
spanning-tree bpduguard enable
end
wr

show spanning-tree summary

Etherchannel (LACP)

CORE-MLS1

int range gig1/0/9-11
channel-group 1 mode active
exit
interface Port-channel 1
switchport mode trunk
exit
do wr

CORE-MLS2

int range gig1/0/9-11
channel-group 1 mode passive
exit
interface Port-channel 1
switchport mode trunk
exit
do wr

show ethnerchannel port
show etherchannel summary
show interfaces port-channel 1

Enable routing on MLSs

ip routing
---
configure IP & Subnetmask as seen in the Topologie Pic

HSRP (LACP)

CORE-MLS1

int vlan 10
no shut
ip add 192.168.10.3 255.255.255.0
standby 10 ip 192.168.10.1
ip helper-address 10.11.11.38
exit

int vlan 20
no shut
ip add 172.16.0.3 255.255.0.0
standby 20 ip 172.16.0.1
ip helper-address 10.11.11.38
exit

int vlan 50

no shut
ip add 10.20.0.2 255.255.0.0
standby 50 ip 10.20.0.1
ip helper-address 10.11.11.38
exit

int vlan 90
no shut
ip add 10.11.11.34 255.255.255.224
standby 90 ip 10.11.11.33
exit
do wr

CORE-MLS2

int vlan 10
no shut
ip add 192.168.10.2 255.255.255.0
standby 10 ip 192.168.10.1
ip helper-address 10.11.11.38
exit

int vlan 20
no shut
ip add 172.16.0.2 255.255.0.0
standby 20 ip 172.16.0.1
ip helper-address 10.11.11.38
exit

int vlan 50
no shut
ip add 10.20.0.3 255.255.0.0
standby 50 ip 10.20.0.1
ip helper-address 10.11.11.38
exit

int vlan 90
no shut
ip add 10.11.11.35 255.255.255.224
standby 90 ip 10.11.11.33
exit
do wr

show start
show standby brief

Static IP to DMZ & INSIDE SERVER

DHCP
10.11.11.38/27
DGW 10.11.11.33
DNS: 10.11.11.37

DNS
10.11.11.37/27
DGW 10.11.11.33
DNS: 10.11.11.37

RADIUS
IP: 10.11.11.36/27
DGW: 10.11.11.33
DNS: 10.11.11.37

DMZ

<IP ADDR OF SERVER>/27 (255.255.255.224)
DGW: 10.11.11.1
DNS: 10.11.11.37

DHCP config

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
WLAN-POOL	10.20.0.1	10.11.11.37	10.20.0.11	255.255.0.0	1000	0.0.0.0	10.20.0.10
LAN-POOL	172.16.0.1	10.11.11.37	172.16.0.11	255.255.0.0	1000	0.0.0.0	0.0.0.0
MGT	192.168.10.1	10.11.11.37	192.168.10.11	255.255.255.0	200	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0

OSPF

CORE-MLS1

router ospf 1
router-id 1.1.1.1
network 10.2.2.0 0.0.0.3 area 0
network 10.2.2.4 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 0
network 172.16.0.0 0.0.255.255 area 0
network 10.20.0.0 0.0.255.255 area 0
network 10.11.11.32 0.0.0.31 area 0

do wr

CORE-MLS2

router ospf 1
router-id 2.2.2.2
network 10.2.2.8 0.0.0.3 area 0
network 10.2.2.12 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 0
network 172.16.0.0 0.0.255.255 area 0
network 10.20.0.0 0.0.255.255 area 0
network 10.11.11.32 0.0.0.31 area 0

do wr

ISP-A

router ospf 1
router-id 1.1.3.3
network 105.100.50.0 0.0.0.3 area 0
network 105.100.50.4 0.0.0.3 area 0
network 20.20.20.0 0.0.0.3 area 0
do wr

ISP-B

router ospf 1
router-id 1.1.4.4
network 197.200.100.0 0.0.0.3 area 0
network 197.200.100.4 0.0.0.3 area 0
network 30.30.30.0 0.0.0.3 area 0
do wr

CLOUD R

router ospf 1
router-id 1.1.5.5
network 20.20.20.0 0.0.0.3 area 0
network 8.0.0.0 0.255.255.255 area 0
network 30.30.30.0 0.0.0.3 area 0
do wr

show start
show ip ospf neighbor
show ip route ospf

CONFIG FIREWALL IP, ZONES, Security level

FW1:
hostname FW1

int gig1/4
ip addr 10.2.2.2 255.255.255.252
no shut
nameif INSIDE1
security-level 100
exit

int gig1/2
ip addr 10.2.2.10 255.255.255.252
no shut
nameif INSIDE2
security-level 100
exit

int gig1/5
ip addr 10.11.11.1 255.255.255.224
no shut
nameif DMZ
security-level 70
exit

int gig1/3
ip addr 105.100.50.2 255.255.255.252
no shut
nameif OUTSIDE1
security-level 0
exit

int gig1/1
ip addr 197.200.100.2 255.255.255.252
no shut
nameif OUTSIDE2
security-level 0
exit

wr mem

-

FW2:
hostname FW2

int gig1/4
ip addr 10.2.2.14 255.255.255.252
no shut
nameif INSIDE2
security-level 100
exit

int gig1/2
ip addr 10.2.2.6 255.255.255.252
no shut
nameif INSIDE1
security-level 100
exit

int gig1/1
ip addr 105.100.50.6 255.255.255.252
no shut
nameif OUTSIDE1
security-level 0
exit

int gig1/3
ip addr 197.200.100.6 255.255.255.252
no shut
nameif OUTSIDE2
security-level 0
exit

wr mem

show interface ip brief
show run interface g1/5

Firewall routing OSPF + Static routes

FW1

route OUTSIDE1 0.0.0.0 0.0.0.0 105.100.50.1
route OUTSIDE2 0.0.0.0 0.0.0.0 197.200.100.1 70

router ospf 1
router-id 1.1.8.8
network 105.100.50.0 255.255.255.252 area 0
network 197.200.100.0 255.255.255.252 area 0
network 10.11.11.0 255.255.255.224 area 0
network 10.2.2.0 255.255.255.252 area 0
network 10.2.2.8 255.255.255.252 area 0

exit
wr mem

FW2

route OUTSIDE1 0.0.0.0 0.0.0.0 105.100.50.5
route OUTSIDE2 0.0.0.0 0.0.0.0 197.200.100.5 70

router ospf 1
router-id 1.1.9.9
network 105.100.50.4 255.255.255.252 area 0
network 197.200.100.4 255.255.255.252 area 0
network 10.2.2.4 255.255.255.252 area 0
network 10.2.2.12 255.255.255.252 area 0
exit
wr mem

Firewall inspection policy config

FW1

object network INSIDE1-OUTSIDE1
subnet 172.16.0.0 255.255.255.0
nat (INSIDE1, OUTSIDE1) dynamic interface

object network INSIDE2-OUTSIDE1
subnet 172.16.0.0 255.255.255.0
nat (INSIDE2, OUTSIDE1) dynamic interface

object network INSIDE1-OUTSIDE2
subnet 172.16.0.0 255.255.255.0
nat (INSIDE1, OUTSIDE2) dynamic interface

object network INSIDE2-OUTSIDE2
subnet 172.16.0.0 255.255.255.0
nat (INSIDE2, OUTSIDE2) dynamic interface

object network INSIDEw1-OUTSIDEw1
subnet 10.20.0.0 255.255.0.0
nat (INSIDE1, OUTSIDE1) dynamic interface

object network INSIDEw2-OUTSIDEw1
subnet 10.20.0.0 255.255.0.0
nat (INSIDE2, OUTSIDE1) dynamic interface

object network INSIDEw1-OUTSIDEw2
subnet 10.20.0.0 255.255.0.0
nat (INSIDE1, OUTSIDE2) dynamic interface

object network INSIDEw2-OUTSIDEw2

subnet 10.20.0.0 255.255.0.0
nat (INSIDE2, OUTSIDE2) dynamic interface

object network DMZ-OUTSIDE1
subnet 10.11.11.0 255.255.255.224
nat (DMZ, OUTSIDE1) dynamic interface

object network DMZ-OUTSIDE2
subnet 10.11.11.0 255.255.255.224
nat (DMZ, OUTSIDE2) dynamic interface

exit
wr mem

show start
show nat
show xlate

FW2

object network INSIDE1-OUTSIDE1
subnet 172.16.0.0 255.255.255.0
nat (INSIDE1, OUTSIDE1) dynamic interface

object network INSIDE2-OUTSIDE1
subnet 172.16.0.0 255.255.255.0
nat (INSIDE2, OUTSIDE1) dynamic interface

object network INSIDE1-OUTSIDE2
subnet 172.16.0.0 255.255.255.0
nat (INSIDE1, OUTSIDE2) dynamic interface

object network INSIDE2-OUTSIDE2
subnet 172.16.0.0 255.255.255.0
nat (INSIDE2, OUTSIDE2) dynamic interface

object network INSIDEw1-OUTSIDEw1
subnet 10.20.0.0 255.255.0.0
nat (INSIDE1, OUTSIDE1) dynamic interface

object network INSIDEw2-OUTSIDEw1
subnet 10.20.0.0 255.255.0.0
nat (INSIDE2, OUTSIDE1) dynamic interface

object network INSIDEw1-OUTSIDEw2
subnet 10.20.0.0 255.255.0.0
nat (INSIDE1, OUTSIDE2) dynamic interface

object network INSIDEw2-OUTSIDEw2
subnet 10.20.0.0 255.255.0.0

nat (INSIDE2, OUTSIDE2) dynamic interface

exit
wr mem

show nat
show xlate

Inspection policy

FW1

access-list RES extended permit icmp any any
access-list RES extended permit tcp any any eq 80
access-list RES extended permit tcp any any eq 53
access-list RES extended permit udp any any eq 53
access-group RES in interface DMZ
access-group RES in interface OUTSIDE1
access-group RES in interface OUTSIDE2

wr mem

FW2

access-list RES extended permit icmp any any
access-list RES extended permit tcp any any eq 80
access-list RES extended permit tcp any any eq 53
access-list RES extended permit udp any any eq 53
access-group RES in interface OUTSIDE1
access-group RES in interface OUTSIDE2

wr mem

to verify try to ping from a PC the FTP server and the PC in the US or China

---

Configure WLC (see WLC-config1-11 screenshots)

next we connect a PC to WLC make give the PC an IP to ping the WLC and
then open the webbrowser
paste the WLC IP into the webbrowser and create an admin acc

user: admin
pw: Admin123

Set up WLANs (EMPLOYEES, ...)
pw: Cisco123

then apply and reboot the system

and log in und https://10.20.0.10

login and the go to the tap wirless there you should see all you Access Point.IF not got to them and turn DHCP off and on and wait

Go to Wlans and create a new one

after creating a WLAN check the status box on the general option

then under security -> Layer 2 chose Layer 2 Security: WPA+WPA2

scroll down and check the boxes as seen in the picture
and add a pw, we will use Cisco123 for all Wlans as PW

Then create two more like the others

and connect the laptops with
CORPORATE

the tablest with
AUDITORS

and the Smartphones with
GUEST

and turn on DHCP on every device

VoIP config on Voice Gate Router

int fa0/0
no shut
exit

int fa0/0.70
ip add 172.30.0.1 255.255.0.0
encapsulation dot1Q 70
ip add 172.30.0.1 255.255.0.0
ip dhcp pool VOIP-POOL
network 172.30.0.0 255.255.0.0
default-router 172.30.0.1
option 150 ip 172.30.0.1
exit

telephony-service
max-ephones 30
max-dn 30
ip source-address 172.30.0.1 port 2000
auto assign 1 to 30

exit

ephone-d 1
number 401
exit

ephone-d 2
number 402
exit

ephone-d 3
number 403
exit

ephone-d 4
number 404
exit

ephone-d 5
number 405
exit

ephone-d 5
number 405
exit

ephone-d 6
number 406
exit

ephone-d 7
number 407
exit

ephone-d 8
number 408
exit

ephone-d 9
number 409
exit

ephone-d 10
number 410
exit

do wr
show telephony-service
show ephone registered

wait a secound then the VOIP Phone should pick up a Line Nr

to verify go on two diffrent VoIP phones and try to call each other (VoIP_Phone_con.png)