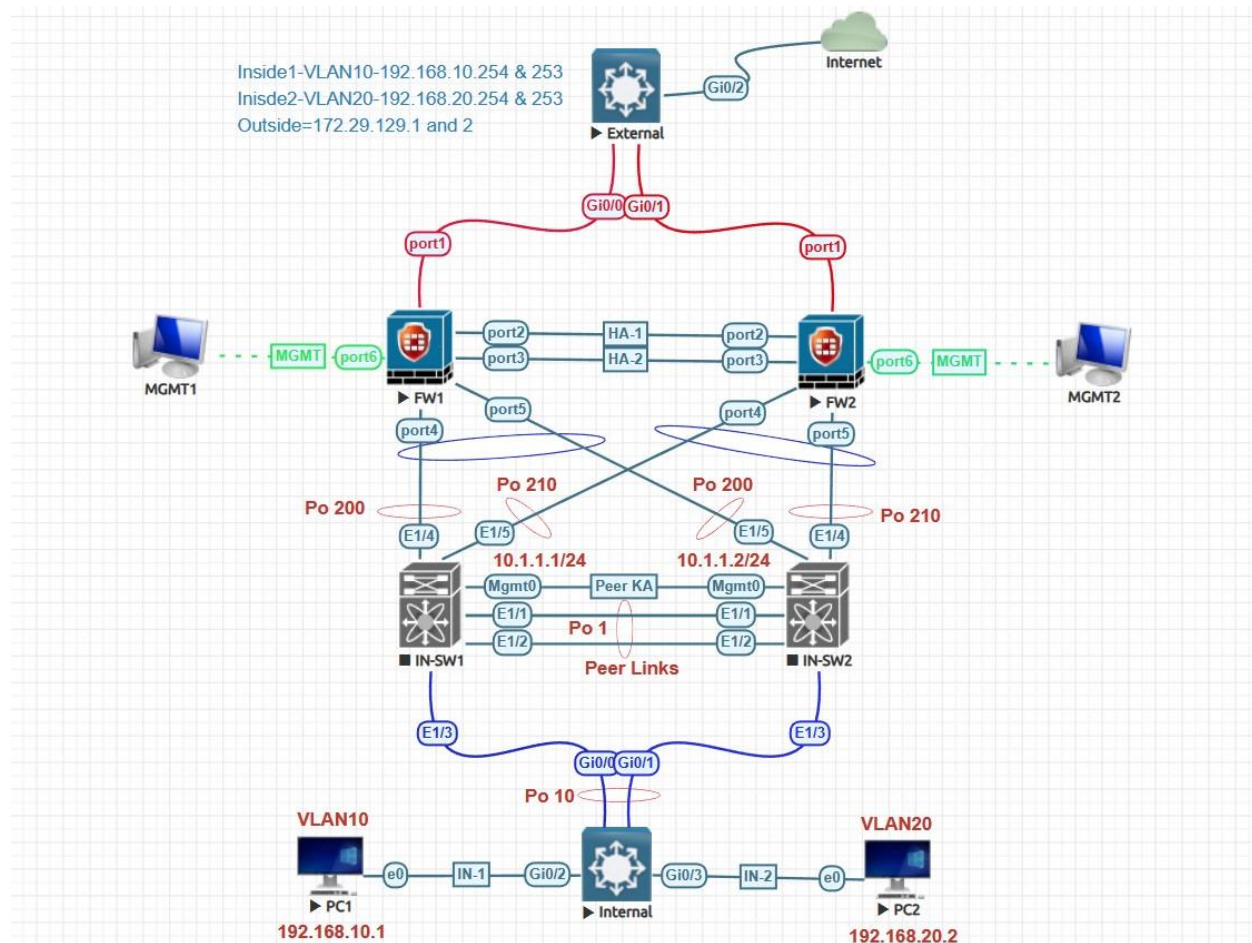


vPC with Firewall Lab:



IN-SW1 Role	Primary
IN-SW2 Role	Secondary
IN-SW1 Priority	20
IN-SW2 Priority	30
Peer Links	E1/1 and E1/2
Keep Alive Link	Mgmt0
IN-SW1 Mgmt0 IP Address	10.1.1.1/30
IN-SW2 Mgmt0 IP Address	10.1.1.2/30
vPC Domain	1
Peer Link Portchannel	1
Member PortChannel	10, 200 and 210
Member Ports	E1/1, E1/3 and E1/5
Member Ports vPC	10, 200 and 210
ACS Switch Ports	G0/0 and G0/1
ACS Switch Images	viosl2-adventerprisek9-m.ssa.high_iron_20190423
Nexus EVE-NG Image	nxosv9k-9.3.6

IN-SW1 Switch Configuration
Change hostname
switch(config)# hostname IN-SW1
Enable Features for vPC
IN-SW1(config)# feature vpc IN-SW1(config)# feature lacp
Configure Keep Alive Link
IN-SW1(config)# interface mgmt 0 IN-SW1(config-if)# ip address 10.1.1.1/30 IN-SW1(config-if)# no shutdown
Configure vPC Domain & Set Priorities
IN-SW1(config)# vpc domain 1 IN-SW1(config-vpc-domain)# role priority 20 IN-SW1(config-vpc-domain)# peer-keepalive destination 10.1.1.2 source 10.1.1.1 vrf management
Configure Peer Link
IN-SW1(config)# interface ethernet 1/1-2 IN-SW1(config-if-range)# switchport mode trunk IN-SW1(config-if-range)# switchport trunk allowed vlan 10,20 IN-SW1(config-if-range)# spanning-tree port type network IN-SW1(config-if-range)# channel-group 1 mode active IN-SW1(config-if-range)# no shutdown
Configure Peer Link Port-Channel
IN-SW1(config)# interface port-channel 1 IN-SW1(config-if)# no shutdown IN-SW1(config-if)# switchport IN-SW1(config-if)# switchport mode trunk IN-SW1(config-if)# switchport trunk allowed vlan 10,20 IN-SW1(config-if)# spanning-tree port type network IN-SW1(config-if)# vpc peer-link
Configure Member Ports
IN-SW1(config)# interface ethernet 1/3 IN-SW1(config-if)# channel-group 10 mode active IN-SW1(config-if)# no shutdown
Configure Member Port-Channel
IN-SW1(config)# interface port-channel 10 IN-SW1(config-if)# no shutdown IN-SW1(config-if)# switchport IN-SW1(config-if)# switchport mode trunk IN-SW1(config-if)# switchport trunk allowed vlan 10,20 IN-SW1(config-if)# vpc 10

Configure Member Ports

```
IN-SW1(config)# interface ethernet 1/4  
IN-SW1(config-if)# channel-group 200 mode active  
IN-SW1(config-if)# no shutdown
```

Configure Member Port-Channel

```
IN-SW1(config)# interface port-channel 200  
IN-SW1(config-if)# no shutdown  
IN-SW1(config-if)# switchport  
IN-SW1(config-if)# switchport mode trunk  
IN-SW1(config-if)# switchport trunk allowed vlan 10,20  
IN-SW1(config-if)# vpc 200
```

Configure Member Ports

```
IN-SW1(config)# interface ethernet 1/5  
IN-SW1(config-if)# channel-group 210 mode active  
IN-SW1(config-if)# no shutdown
```

Configure Member Port-Channel

```
IN-SW1(config)# interface port-channel 210  
IN-SW1(config-if)# no shutdown  
IN-SW1(config-if)# switchport  
IN-SW1(config-if)# switchport mode trunk  
IN-SW1(config-if)# switchport trunk allowed vlan 10,20  
IN-SW1(config-if)# vpc 210
```

Create VLANs

```
IN-SW1 (config)# vlan 10  
IN-SW1 (config-vlan)# exit  
IN-SW1 (config)# vlan 20  
IN-SW1 (config-vlan)# exit
```

IN-SW2 Switch Configuration
Change hostname
switch(config)# hostname IN-SW2
Enable Features for vPC
IN-SW2(config)# feature vpc IN-SW2(config)# feature lacp
Configure Keep Alive Link
IN-SW2(config)# interface mgmt 0 IN-SW2(config-if)# ip address 10.1.1.2/30 IN-SW2(config-if)# no shutdown
Configure vPC Domain & Set Priorities
IN-SW2(config)# vpc domain 1 IN-SW2(config-vpc-domain)# role priority 30 IN-SW2(config-vpc-domain)# peer-keepalive destination 10.1.1.1 source 10.1.1.2 vrf management
Configure Peer Link
IN-SW2(config)# interface ethernet 1/1-2 IN-SW2(config-if-range)# switchport mode trunk IN-SW2(config-if-range)# switchport trunk allowed vlan 10,20 IN-SW2(config-if-range)# spanning-tree port type network IN-SW2(config-if-range)# channel-group 1 mode active IN-SW2(config-if-range)# no shutdown
Configure Peer Link Port-Channel
IN-SW2(config)# interface port-channel 1 IN-SW2(config-if)# no shutdown IN-SW2(config-if)# switchport IN-SW2(config-if)# switchport mode trunk IN-SW2(config-if)# switchport trunk allowed vlan 10,20 IN-SW2(config-if)# spanning-tree port type network IN-SW2(config-if)# vpc peer-link
Configure Member Ports
IN-SW2(config)# interface ethernet 1/3 IN-SW2(config-if)# channel-group 10 mode active IN-SW2(config-if)# no shutdown
Configure Member Port-Channel
IN-SW2(config)# interface port-channel 10 IN-SW2(config-if)# no shutdown IN-SW2(config-if)# switchport IN-SW2(config-if)# switchport mode trunk IN-SW2(config-if)# switchport trunk allowed vlan 10,20 IN-SW2(config-if)# vpc 10

Configure Member Ports
IN-SW2(config)# interface ethernet 1/4 IN-SW2(config-if)# channel-group 210 mode active IN-SW2(config-if)# no shutdown
Configure Member Port-Channel
IN-SW2(config)# interface port-channel 210 IN-SW2(config-if)# no shutdown IN-SW2(config-if)# switchport IN-SW2(config-if)# switchport mode trunk IN-SW2(config-if)# switchport trunk allowed vlan 10,20 IN-SW2(config-if)# vpc 210
Configure Member Ports
IN-SW2(config)# interface ethernet 1/5 IN-SW2(config-if)# channel-group 200 mode active IN-SW2(config-if)# no shutdown
Configure Member Port-Channel
IN-SW2(config)# interface port-channel 200 IN-SW2(config-if)# no shutdown IN-SW2(config-if)# switchport IN-SW2(config-if)# switchport mode trunk IN-SW2(config-if)# switchport trunk allowed vlan 10,20 IN-SW2(config-if)# vpc 200
Create VLANs
IN-SW2 (config)# vlan 10 IN-SW2 (config-vlan)# exit IN-SW2 (config)# vlan 20 IN-SW2 (config-vlan)# exit

Internal Switch Configuration
Change hostname
Switch(config)#hostname Internal
Configure Port-channel
Internal(config)#interface range g0/0-1 Internal(config-if-range)#switchport trunk encapsulation dot1q Internal(config-if-range)#switchport mode trunk Internal(config-if-range)#channel-protocol lacp Internal(config-if-range)#channel-group 10 mode active Internal(config-if-range)#no shutdown Internal(config-if-range)#exit Internal (config)#exit
Internal(config)#interface port-channel 10 Internal(config-if)#switchport trunk encapsulation dot1q Internal(config-if)#switchport mode trunk Internal(config-if)# switchport trunk allowed vlan 10,20 Internal(config-if)#no shutdown Internal(config-if)#exit
Create VLANs
Internal(config)# vlan 10 Internal(config-vlan)# exit Internal(config)# vlan 20 Internal(config-vlan)# exit
Assign Ports to VLANs
Internal(config)# interface g0/2 Internal(config-if)# switchport mode access Internal(config-if)# switchport access vlan 10 Internal(config-if)# no shutdown Internal(config-if)# exit
Internal(config)# interface g0/3 Internal(config-if)# switchport mode access Internal(config-if)# switchport access vlan 20 Internal(config-if)# no shutdown Internal(config-if)# exit

Firewalls Configuration:

Firewalls Basic Configuration
FortiGate-VM64-KVM # config system global FortiGate-VM64-KVM (global) # set hostname FW1 FortiGate-VM64-KVM (global) # end
FW1 # config system interface FW1 (interface) # edit port6 FW1 (port6) # set ip 192.168.114.200/24 FW1 (port6) # set allowaccess https http telnet ssh ping FW1 (port6) # end
FortiGate-VM64-KVM # config system global FortiGate-VM64-KVM (global) # set hostname FW2 FortiGate-VM64-KVM (global) # end
FW1 # config system interface FW1 (interface) # edit port6 FW1 (port6) # set ip 192.168.114.210/24 FW1 (port6) # set allowaccess https http telnet ssh ping FW1 (port6) # end

The screenshot shows the FortiGate WebUI configuration page for the 'port6' interface. The left sidebar contains a navigation menu with categories like Network, Policy & Objects, Security Profiles, and VPN. The main content area is titled 'Edit Interface' and includes the following configuration details:

- Name:** port6
- Alias:** MGMT
- Type:** Physical Interface
- VRF ID:** 0
- Role:** Undefined
- Dedicated Management Port:** Disabled (radio button)
- Addressing mode:** Manual (selected), DHCP, Auto-managed by IPAM, One-Arm Sniffer
- IP/Netmask:** 192.168.114.200/255.255.255.0
- Secondary IP address:** Disabled (radio button)
- Administrative Access:**
 - IPv4: HTTPS, FMG-Access, HTTP, SSH, PING, SNMP

- Dashboard >
- Network** >
- Interfaces ☆
- DNS
- Packet Capture
- SD-WAN
- Static Routes
- Policy Routes
- RIP
- OSPF
- BGP
- Routing Objects

Edit Interface

Name port2

Alias

Type Physical Interface

VRF ID ⓘ

Role ⓘ

Dedicated Management Port

Address

Addressing mode Manual DHCP Auto-managed by IPAM One-Arm Sniffer

IP/Netmask

Secondary IP address

- Dashboard >
- Network** >
- Interfaces ☆
- DNS
- Packet Capture
- SD-WAN
- Static Routes
- Policy Routes
- RIP
- OSPF
- BGP
- Routing Objects

Edit Interface

Name port3

Alias

Type Physical Interface

VRF ID ⓘ

Role ⓘ

Dedicated Management Port

Address

Addressing mode Manual DHCP Auto-managed by IPAM One-Arm Sniffer

IP/Netmask

Secondary IP address

Dashboard > **Edit Interface**

Network > **Interfaces** ☆

DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects >

Name: port1
Alias: WAN
Type: Physical Interface
VRF ID: 0
Role: WAN
Estimated bandwidth: 0 kbps Upstream, 0 kbps Downstream

Dedicated Management Port

Address

Addressing mode: Manual DHCP
IP/Netmask: 172.29.129.189/255.255.255.0
Secondary IP address:

Network > **Interfaces** ☆

DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects

Name: port4
Alias: LINK-1
Type: Physical Interface
VRF ID: 0
Role: Undefined

Dedicated Management Port

Address

Addressing mode: Manual DHCP Auto-managed by IPAM One-Arm Sniffer
IP/Netmask: 0.0.0.0/0.0.0.0
Secondary IP address:

Network > **Interfaces** ☆

DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects

Name: port5
Alias: LINK-2
Type: Physical Interface
VRF ID: 0
Role: Undefined

Dedicated Management Port

Address

Addressing mode: Manual DHCP Auto-managed by IPAM One-Arm Sniffer
IP/Netmask: 0.0.0.0/0.0.0.0
Secondary IP address:

Physical Interface 6				
HA-1 (port2)	Physical Interface		0.0.0.0/0.0.0.0	
HA-2 (port3)	Physical Interface		0.0.0.0/0.0.0.0	
LINK-1 (port4)	Physical Interface		0.0.0.0/0.0.0.0	
LINK-2 (port5)	Physical Interface		0.0.0.0/0.0.0.0	
MGMT (port6)	Physical Interface		192.168.114.200/255.255.255.0	PING HTTPS SSH HTTP
WAN (port1)	Physical Interface		172.29.129.189/255.255.255.0	PING

Tunnel Interface 1				
NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0	

- Dashboard >
- Network >
- Interfaces ☆
- DNS
- Packet Capture
- SD-WAN
- Static Routes
- Policy Routes
- RIP
- OSPF
- BGP
- Routing Objects
- Multicast
- Policy & Objects >
- Security Profiles >
- VPN >

New Interface

Name:

Alias:

Type: 802.3ad Aggregate

VRF ID:

Interface members: LINK-1 (port4) ✕
LINK-2 (port5) ✕
+

Role: LAN

Address

Addressing mode: Manual DHCP Auto-managed by IPAM

IP/Netmask:

Create address object matching subnet:

Name: AGG-IN address

Destination:

Dashboard > Network > Interfaces > New Interface

Name: VLAN10
 Alias: VLAN10
 Type: VLAN
 VLAN protocol: 802.1Q 802.1AD
 Interface: AGG-IN (AGG-IN)
 VLAN ID: 10
 VRF ID: 0
 Role: LAN

Addressing mode: Manual DHCP Auto-managed by IPAM
 IP/Netmask: 192.168.10.254/24
 Create address object matching subnet:
 Name: VLAN10 address
 Destination: 192.168.10.254/24
 Secondary IP address:

Administrative Access
 IPv4: HTTPS PING FMG-Access
 SSH SNMP FTM

Dashboard > Network > Interfaces > New Interface

Name: VLAN20
 Alias: VLAN20
 Type: VLAN
 VLAN protocol: 802.1Q 802.1AD
 Interface: AGG-IN (AGG-IN)
 VLAN ID: 20
 VRF ID: 0
 Role: LAN

Addressing mode: Manual DHCP Auto-managed by IPAM
 IP/Netmask: 192.168.20.254/24
 Create address object matching subnet:
 Name: VLAN20 address
 Destination: 192.168.20.254/24
 Secondary IP address:

Administrative Access
 IPv4: HTTPS PING FMG-Access

+ Create New Edit Delete Integrate Interface Search					
Name	Type	Members	IP/Netmask	Administrative Access	
802.3ad Aggregate 4					
AGG-IN (AGG-IN)	802.3ad Aggregate	LINK-1 (port4) LINK-2 (port5)	0.0.0.0/0.0.0.0		
VLAN10 (VLAN10)	VLAN		192.168.10.254/255.255.255.0	PING	
VLAN20 (VLAN20)	VLAN		192.168.20.254/255.255.255.0	PING	
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection	
Physical Interface 4					
HA-1 (port2)	Physical Interface		0.0.0.0/0.0.0.0		
HA-2 (port3)	Physical Interface		0.0.0.0/0.0.0.0		
MGMT (port6)	Physical Interface		192.168.114.200/255.255.255.0	PING HTTPS SSH HTTP	
WAN (port1)	Physical Interface		172.29.129.189/255.255.255.0	PING	

Dashboard > **DNS Settings**

Network > DNS

DNS servers: Use FortiGuard Servers Specify

Primary DNS server: 8.8.8.8

Secondary DNS server: 8.8.4.4

Local domain name:

Dashboard > **New Static Route**

Network > Static Routes

Destination: Subnet Internet Service

0.0.0.0/0.0.0.0

Gateway Address: 172.29.129.254

Interface: WAN (port1)

Administrative Distance: 10

Comments: Write a comment... 0/255

Status: Enabled Disabled

Advanced Options

Dashboard > Network > Policy & Objects > Firewall Policy

New Policy

Name: VLAN10-Policy

Incoming Interface: VLAN10 (VLAN10)

Outgoing Interface: WAN (port1)

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT DENY

Inspection Mode: Flow-based Proxy-based

Firewall / Network Options

NAT:

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Dashboard > Network > Policy & Objects > Firewall Policy

New Policy

Name: VLAN10-Policy

Incoming Interface: VLAN10 (VLAN10)

Outgoing Interface: WAN (port1)

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT DENY

Inspection Mode: Flow-based Proxy-based

Firewall / Network Options

NAT:

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Dashboard > High Availability

Mode: Active-Passive

Device priority: 128

Cluster Settings

Group name: HAG

Password: [Redacted]

Session pickup:

Monitor interfaces: WAN (port1)

Heartbeat interfaces: HA-1 (port2), HA-2 (port3)

Heartbeat Interface Priority

port2: 512

port3: 0

Management Interface Reservation

Dashboard > Network > Interfaces

Edit Interface

Name: port2

Alias: HA-1

Type: Physical Interface

VRF ID: 0

Role: Undefined

Dedicated Management Port

Address

Addressing mode: Manual | DHCP | Auto-managed by IPAM | One-Arm Sniffer

IP/Netmask: 0.0.0.0/0.0.0.0

Secondary IP address:

Dashboard > **Network** > **Interfaces** > **Edit Interface**

Name: port3
 Alias: HA-2
 Type: Physical Interface
 VRF ID: 0
 Role: Undefined

Dedicated Management Port

Address

Addressing mode: **Manual** DHCP Auto-managed by IPAM One-Arm Sniffer
 IP/Netmask: 0.0.0.0/0.0.0.0
 Secondary IP address:

Network > **Interfaces** > **Edit Interface**

Name: port4
 Alias: LINK-1
 Type: Physical Interface
 VRF ID: 0
 Role: Undefined

Dedicated Management Port

Address

Addressing mode: **Manual** DHCP Auto-managed by IPAM One-Arm Sniffer
 IP/Netmask: 0.0.0.0/0.0.0.0
 Secondary IP address:

Network > **Interfaces** > **Edit Interface**

Name: port5
 Alias: LINK-2
 Type: Physical Interface
 VRF ID: 0
 Role: Undefined

Dedicated Management Port

Address

Addressing mode: **Manual** DHCP Auto-managed by IPAM One-Arm Sniffer
 IP/Netmask: 0.0.0.0/0.0.0.0
 Secondary IP address:

Network

- Interfaces
- DNS
- Packet Capture
- SD-WAN
- Static Routes
- Policy Routes
- RIP
- OSPF
- BGP
- Routing Objects
- Multicast
- Policy & Objects
- Security Profiles
- VPN

Name: port6

Alias: MGMT

Type: Physical Interface

VRF ID: 0

Role: Undefined

Dedicated Management Port

Address

Addressing mode: Manual | DHCP | Auto-managed by IPAM | One-Arm Sniffer

IP/Netmask: 192.168.114.210/255.255.255.0

Secondary IP address:

Administrative Access

IPv4

- HTTPS
- FMG-Access
- HTTP
- SSH
- PING
- SNMP

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

System

- Administrators
- Admin Profiles
- Firmware
- Fabric Management
- Settings
- HA
- SNMP
- Replacement Messages
- FortiGuard
- Feature Visibility
- Certificates

High Availability

Mode: Active-Passive

Device priority: 100

Cluster Settings

Group name: HAG

Password:

Session pickup:

Monitor interfaces: WAN (port1)

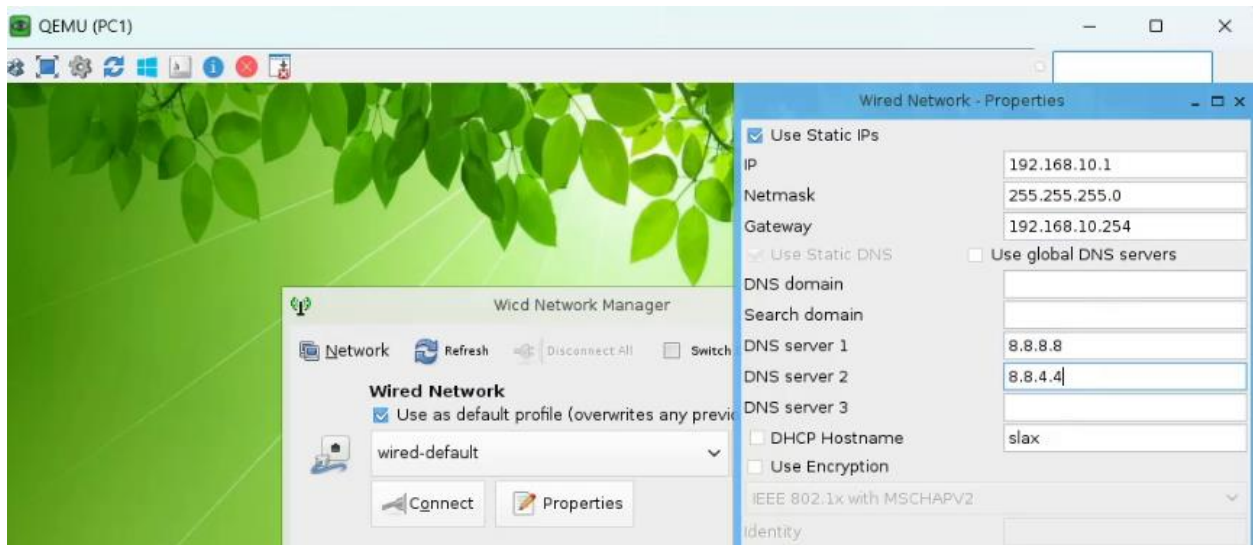
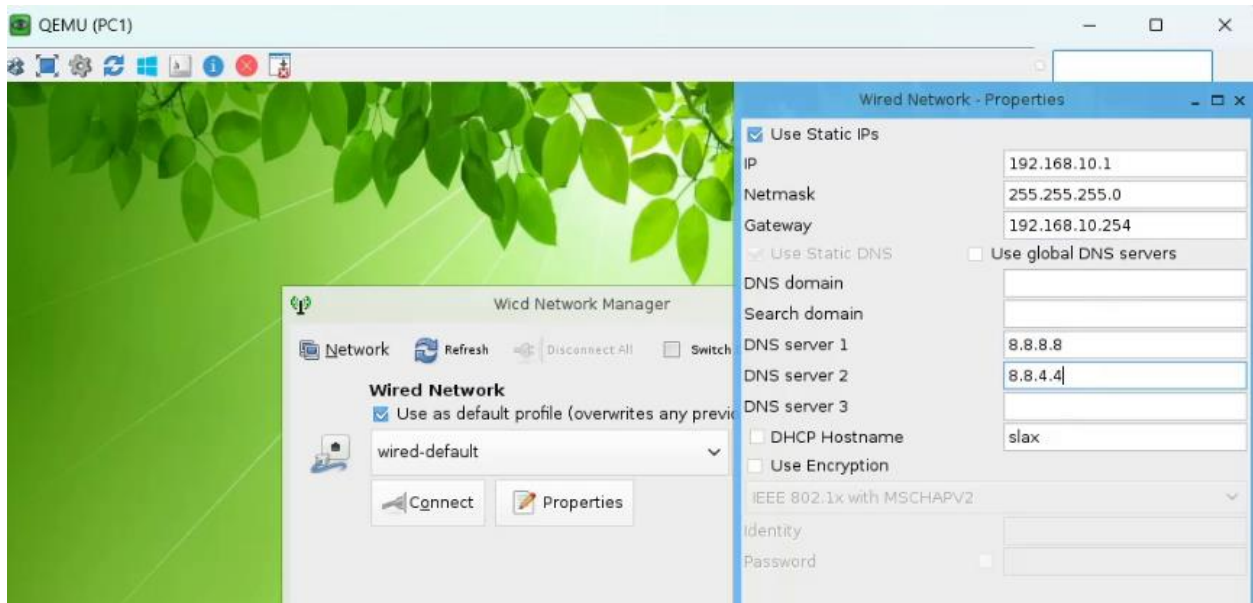
Heartbeat interfaces: HA-1 (port2), HA-2 (port3)

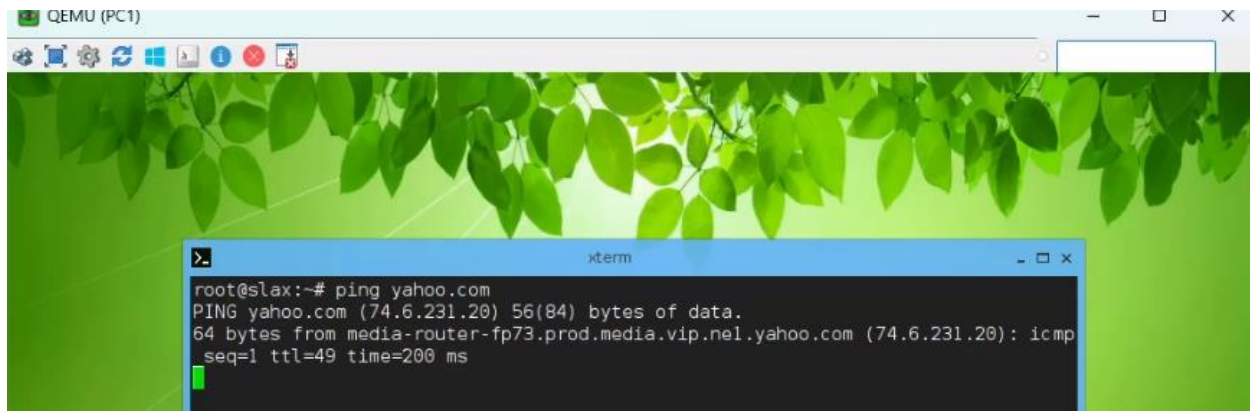
Heartbeat Interface Priority

port2: 512

port3: 0

Management Interface Reservation





Cisco vPC Command	Purpose
show feature	Displays whether the vPC is enabled or not
show vpc brief	Displays brief information about the vPCs
show vpc consistency-parameters	Displays the current status of parameters
show running-config vpc	Displays running configuration information for vPCs
show port-channel capacity	Displays how many port channels are configured
show vpc statistics	Displays statistics about the vPCs
show vpc peer-keepalive	Displays info about the peer-keepalive messages
show vpc role	Displays the vPC peer's state
show vpc orphan-ports	Displays orphan port details