Working tasks of the 47th National WorldSkills Competition

SKILL N°39

IT NETWORK SYSTEMS ADMINISTRATION

Proposed by :
Alexis Charton, WorldSkills France's Regional Expert
Jean-Michel Bouillet , WorldSkills France's Regional Expert

Based on an original idea from :
Alexandre MICHEL, WorldSkills France's National Expert

Table of contents

Table des matières

1. INTRODUCTION

Task Duration	10 days

Document release's availability	12 December 2023

1.1. CONTEXT

As you know, France will host the next WorldSkills Competition in Lyon on September 2024. In order to organize this incredible event, a dedicated company has been created intitled "WorldSkills Lyon 2024" (WSL2024) which is in charge of the overall organization.

Due to the important necessary number of tasks which will be performed by WSL2024 teams, WSL2024 will hire lot of new people in order to reach around 120 employees within the company.

As expected, like other company that growing up, the IT needs have been increased and the WSL2024's IT infrastructure have to be renewed regarding LAN and WAN architecture.

To organize the WorldSkills Competition 2024, WSL2024 needs to collaborate and exchange data with WorldSkills France (WSFR). While WSFR is moving to another office, it has been decided that WSFR will use WSL2024's IT infrastructure and be connected to it using a private MAN connection.

As a recently graduated network engineer, your manager has decided to involve you and your team on this project in order to build the network infrastructure which has been partially designed by the network architect, and to deploy network services on different operating systems.

More than implementing each required technology and settings, the functional aspect is the most important. Don't forget to test what you've implemented.

1.2. TEST PROJECT'S INFRASTRUCTURE

To realize this project, you will use virtual and real systems:

- Virtual machines are hosted on several VMware ESXi and Proxmox VE
- Network devices are real hardware equipments except the two Firewalls REMFW (VM Cisco CSR1000) and HQFWSRV (VM Linux)

In order to connect VM and network devices between them, you will have to configure Portgroups in VMware ESXi

To connect to ESXi and to Proxmox, use the information provided on the separated sheet.

1.3. ADDITIONAL NOTES

When a password is required & not specified, you should use "**P@ssw0rd**" (zero digit between "w" and "r").

2. TASKS DESCRIPTION NETWORK INFRASTRUCTURE

2.1. BASIC CONFIGURATION

Configure on all network devices the following settings:

- Hostname as specified on diagrams
- DNS domain as "**wsl2024.org**"
- Disable DNS resolution
- Enable password as "**P@ssw0rd**" (zero digit between "w" and "r")
- Username "admin" with password **"P@ssw0rd"** (**zero digit between "w" and "r"**) with the maximum level of rights
- None of the passwords should be displayed as plain text on configuration
- For the remote connection, use SSHv2 only based on username credentials:
    - Encryption will use a RSA with a 2048 key size
    - Remote connection to device should be only allowed from Management network
    - The following banner should be displayed just after entering the username:
      /!\ Restricted access. Only for authorized people /!
    - Session should be closed after five minutes of inactivity and twenty minutes in absolute

2.2. SWITCHING CONFIGURATION

On the switched infrastructure (CORESWX and ACCSWX), the following VLAN should be present:

VLAN ID	VLAN name	VLAN description
10	Servers	Used for Servers
20	Clients	Used for Clients
30	DMZ	Used to access the DMZ
99	Management	Used for management
100	CORESW1-EDGE1	Used for connection between CORESW1 and EDGE1
200	CORESW2-EDGE2	Used for connection between CORESW2 and EDGE2
300	IBGP_peering	Used for iBGP peering between EDGE1 and EDG2
666	Blackhole	Native VLAN for trunk links

All the VLAN above should be distributed using VTPv2:

- CORESW1 and CORESW2 are VTP servers
- ACCSW1 and ACCSW2 are VTP clients
- All VLAN modifications should be made on CORESW1 as often as possible
- Use "**P@ssw0rd**" as VTP password and "**wsl2024.org**" as VTP domain

On the four switches, configure the necessary interfaces base on both provided information and diagrams on appendix:

- For inter-switch connections:
    - In addition of the native, only necessary VLAN of the infrastructure should be allowed on each trunk link
    - No negotiation should be used for trunk establishment.
    - Standard protocol should be used for LAG establishment. Both core switches can try to initiate the LAG negotiation
- For hosts connections:
    - Host connections are only located on ACCSWX switches
    - Ports should be explicitly configured as access ports and assigned according to the following information:
        - VLAN 10: Port Gi0/3
        - VLAN 20: Port Gi0/4
        - VLAN 30: Port Gi0/5

- VLAN 99: Port Gi0/6

- For all other ports of all switches, they should be explicitly configured as access port, assigned to Blackhole VLAN and deactivated.
- For all host ports, only three maximum MAC addresses should be learned dynamically. In case of violation, port should be deactivated and tried to reactivate automatically after 30 seconds.

Configure STP based on the following information:

- Rapid-PVST should be used.
- Topology should be based primarily on CORESW1 and secondly on CORESW2
- On host ports, STP should be disabled. In case of STP traffic received, ports should be blocked

IP ADDRESSING

You have to terminate the IP addressing for your networks, keep in mind that you have to optimize the address space and to use only the necessary amount of IP addresses that you need.

- Always use the last IP address for the gateway
- Always use the first IP addresses for your servers with static configuration
- Always use DHCP for your clients with enough IP addresses in the range

- Core network
  - internal branches to HQ site use 10.N.254.0 sub networks, and the network 10.116.N.0 for the remote site connection
  - external branches to the Internet use two networks: 91.N.222.96 and 31.N.126.12
- Internet side: all IP addresses are static
  - 3 servers and 2 clients are available
  - from the Internet two networks are available 217.N.160.0 (redirected to the DMZ) and 191.5.157.32 (for VPN and webmail access)
- HQ site .
  - 30 servers are planned to be active in the future
  - 300 clients will be available
- Remote Site
  - 10 servers are planned
  - 80 clients will be available
- The managing network has the capacity to supervise all the active network equipment and all the servers (including VM, real hosts or Barebone Hypervisors).

2.3. ROUTING CONFIGURATION

Configure all necessary TCP/IP settings on all network devices. All devices should have access to the Internet and/or private MAN.

All necessary information regarding routing for the topology is available in the appendix.

2.3.1. CORE SWITCHES

Core switches should provide gateway redundancy by using an active/passive FHRP Cisco proprietary protocol for the networks 10.N.10.0,10.N.20.0 and 10.N.99.0:

- VIP information is provided on diagrams
- Priority should be 110 for CORESW1 and 100 for CORESW2
- In case of CORESW1's failure, CORESW2 should route the traffic
- Active router is based on checking IP reachability of the respective EDGEX router's uplink interface (Fa0/1.100 for EDGE1 and Fa0/1.200 for EDGE2)
- In case of CORESW1 come back alive, CORESW1 should take over the traffic routing
- Configuration should be exactly the same on both device (except priority)

For all unknown destinations, core switches should route traffic to their respective uplink router as described on the routing diagram.

2.3.2. EDGE ROUTERS

Edge routers should provide gateway redundancy by using an active/passive FHRP Cisco proprietary protocol for the network 217.N.160.0

- VIP information is provided on diagrams.
- Priority should be 110 for EDGE1 and 100 for EDGE2
- In case of EDGE1's failure, EDGE2 should route the traffic
- Active router is based on checking IP reachability of the respective CORESWX router's uplink interface (Gi0/1.100 for CORESW1 and Gi0/1.200 for CORESW2)
- If EDGE1 comes back alive, then EDGE1 should take over the traffic routing.
- Configuration should be exactly the same on both device (except priority)

In order to create logically two different networks WAN connections (Internet & Private MAN) by using only one physical interface, create two logical sub-interfaces by encapsulated traffic according to the following information:

Device	VLAN ID	Description
EDGE1	13	Used for MAN connection
	14	Used for INET connection
EDGE2	15	Used for MAN connection
	16	Used for INET connection

Internet

EDGE routers can reach the LAN networks by using a summarized /16 static route according to the routing diagram.

EDGE routers provide Internet access for all private subnets by using NAT/PAT based on their WAN interface's IP address.

EDGE routers' Internet connectivity is ensured by eBGP connection with WANRTR (VRF INET). Internet access redundancy is ensured by iBGP peering between EDGE routers.

For BGP, all public IP subnets should be announced and exchanged between the three routers. Independent providers IP will be used for HQINFRASRV's services access from the Internet.

Traffic to the Internet should be primarily routed by EDGE1 router based on BGP's intra-AS attribute.
For returned traffic or traffic initiated from Internet to EDGE routers, be sure that WANRTR chooses primarily to send traffic to EDGE1. To reach this order, no configuration should be made on WANRTR but only on EDGE routers.

EDGE routers provide connectivity from the internet to the corporate network for two services:

- To access the Corporate Web server HQWEBSRV using the public IP 217.N.160.X via the firewall HQFWSRV

- To access the VPN server using PAT/NAT to translate traffic from the public IP 191.5.157.33 Port 4443 to the VPN Access Server HQINFRASRV with the private IP 10.N.10.X

- To access the webmail server using PAT/NAT to translate traffic from the public IP 191.5.157.33 Ports 80/443 to the webmail server HQMAILSRV with the private IP 10.N.10.X

Private MAN

In order to connect WSFR's workers by REMCLT VM connected to REMFW to WSL2024's infrastructure, REMFW router, and EDGE routers establish OSPF adjacencies with WANRTR router (VRF MAN).

All private networks should be exchanged between those four routers. Only the necessary interfaces of these four routers should exchange OSPF hello messages. OSPF exchanges should be authenticated using MD5. No OSPF external routes should appear on EDGE routers.

WANRTR should choose EDGE1 as the primary path.

In order to save bandwidth, no DR/BDR election should have occurred on any link.

When WANRTR's interface facing REMFW's private MAN connection (10.116.N.X) goes to down status, it should be re-enabled automatically and display "**Interface have been re-enabled automatically due to down status**" on device console.

VM located on private IP networks can communicate with each other. When REMCLT VM is connecting to REMFW, VM can access to both corporate resources and Internet.

For all unknown destination, REMFW should route traffic to WANRTR router as described on the routing diagram.

2.3.3. WANRTR ROUTER

WANRTR use VRF to split network traffic between Internet (VRF INET) and private MAN (VRF MAN)

3. TASKS DESCRIPTION IT SERVICES INFRASTRUCTURE

3.1. BASIC CONFIGURATION

ALL SERVERS

Configure on all servers the following settings:

- Time zones have to be configured on all servers and use HQINFRASRV as time reference. Use authentication to secure NTP communication.
- Hostname as specified on diagrams.
- DNS domain as "**wsl2024.org**"
- All linux servers should be remotely managed with SSH . Configure Fail2Ban to ban the IP address of the initiator after 3 unsuccessful logins (SSH, FTP,....)

OPERATING SYSTEM

- HQINDRASRV, HQWEBSRV, REMDCSRV and REMINFRASRV are based on Windows 2022 Server:

- DNSSRV, INETSRV1, INETSRV2, REMPROXSRV, HQINFRASRV, HQMAILSRV, SUPSRV, HQFWSRV are running Linux Debian 11

3.2. HQ SITE CONFIGURATION

HQINFRASRV

DNS

This server is the DNS server and hosts the **wsl2024.org** zone for the infrastructure network. All others DNS requests are forwarded to DNSSRV. The following DNS records are configured:

Type	FQDN / Alias	IP address / FQDN
A	hqdcsrv.hq.wsl2024.org	10.N.10.X
A	hqinfrasrv.wsl2024.org	10.N.10.X
A	hqmailsrv.wsl2024.org	10.N.10.X
A	hqfwsrv.wsl2024.org	217.N.160.X
CNAME	hqwebsrv.hq.wsl2024.org	hqfwsrv.wsl2024.org
CNAME	www.wsl2024.org	hqfwsrv.wsl2024.org
CNAME	webmail.wsl2024.org	hqmailsrv.wsl2024.org
CNAME	pki.hq.wsl2024.org	hqdcsrv.hq.wsl2024.org
A	vpn.wsl2024.org	217.N.160.X
A	supsrv.wsl2024.org	10.N.99.X
A	accsw1.wsl2024.org	10.N.99.X
A	accsw2.wsl2024.org	10.N.99.X
A	coresw1.wsl2024.org	10.N.99.X
A	coresw2.wsl2024.org	10.N.99.X
A	edge1.wsl2024.org	10.N.254.X
A	edge2.wsl2024.org	10.N.254.X
A	wanrtr.wsl2024.org	10.116.N.X
A	remfw.wsl2024.org	10.N.100.X

DNSSec should be configured on this server with a certificate issued by HQDCSRV

DHCP

HQINFRASRV provides DHCP service for Clients and Management networks of the HQ site with all necessary options in order to allow those networks to access to corporate services and Internet

This server provides dynamic IP addresses for clients located on HQ.

Scope configuration:

- Subnet : 10.N.20.X
- Netmask : To be defined
- Range : To be defined
- Gateway : To be defined
- Name server : hqdcsrv.hq.wsl2024.org
- Domain : hq.wsl2024.org
- NTP server : hqinfrasrv.wsl2024.org
- Lease : 2 hours

VPN

Configure OpenVPN Server to allow VPNCLT to be connected on HQ site as a remote client from the Internet.

The tunnel should be configured with:

- Protocol: OpenVPN
- Port : 4443
- Network : 191.5.157.33
- Authentication: certificate and user/password from Active Directory.

Clients will have an IP address from the DHCP Service on the Clients network.

Clients should be able to reach resources hosted both on HQ and Remote site once the VPN is connected.

Use a certificate issued by HQDCSRV to establish the connection.

Storage:

Configure the storage on his server:

- Configure physical volumes with LVM using the two 5Gb extra attached disks.
- Configure a volume group with the two physical volumes with LVM named “vgstorage”
- Configure a logical volume named /dev/vgstorage/lvdatastorage (2Gb) with LVM.
- Configure a logical volume /dev/vgstorage/lviscsi (2Gb)
- Format volume lvdatastorage with ext4
- Mount volume “lvdatastorage” as /srv/datastorage

Configure an iSCSI LUN on /dev/vgstorage/lviscsi and allow HQMAILSRV to mount this LUN.

Files Server:

Create 3 local users Jean, Tom and Emma

Configure Samba on this server to host two file shares:

- Name : Public
  - Path : /srv/datastorage/shares/public
  - Rights : Read-Only for everyone

- Name : Private
  - Path : /srv/datastorage/shares/private
  - Hidden share
  - Files starting with "." Should be hidden.
  - Only clients located on HQ should be able to access this share
  - Files with extension ".exe" and ".zip" can't be uploaded on this share
  - Rights:
    - Read/write for Tom and Emma
    - Read only for Jean

Bonus: Configure Authentication of the Samba users on Active Directory

HQMAILSRV

Storage:

Using ZFS create a pool named zfspool with this configuration:

- RAID 5 array with 3 disks of 1Go
- activate encryption
- create a volume named data and mounted on /data
- move the /home users directory to /data/home

Backup:

You have to schedule an automated backup of the users directory /data/home every day at 10PM with rsync to the iSCSI drive on HQINFRASRV

MAIL

This server hosts email services SMTP & IMAP

Configure a server SMTP and IMAP as secure email services by using certificate issued by HQDCSRV

Clients should be able to send email using SMTPS and receive with IMAPS protocols. Non-securised protocols are not allowed.

All users described in Appendix should have a mailbox located on their home folders and an email address with "@wsl2024.org" domain.

- Configure two distribution group:
  - "all@wsl2024.com" that contains all users.

- "admin@wsl2024.org" that contains only IT users
- Configure a rule to restrict sending attachment with ".zip" format.

Bonus : Configure SMTP and IMAP authentication with Active Directory

Webmail

Install and configure a webmail service on this server to allow users to connect to their mailbox with a web browser.

This service should be available at https://webmail.wsl2024.org from internal and external clients.

Configure a redirection from http to https.

DNS

This server is the secondary (or slave) DNS Server and hosts the **wsl2024.org** zone for all the corporate networks. All unknown DNS requests are forwarded to DNSSRV.

DHCP failover

This server provide DHCP failover service in association with the primary server HQINFRASRV. in normal state the two server assign 50% of the IP Address range.

VoIP

This server is a Voice over IP server based on Asterisk.

Each user should have a three digit telephone number beginning with 1xx for the HQ site and 2xx for the Remote site.

Each service has a group number beginning with 3xx

A voice trunk SIP is available between this server and REMPROXSRV, the voice over IP Asterisk server for the remote site.

Please provide us a phone book excel sheet decided by your team.

HQDCSRV

Active Directory

Configure this server as root of the forest, primary domain controller and global catalog for the domain hq.wsl2024.org . He's hosting his own DNS server for the hq.wsl2024.org and rem.wsl2024.org zones. All others DNS requests are forwarded to wsl2024.org

On this server, create the users, groups and organization units listed in Appendix, respecting the AGDLP Method.

Users, Groups and OU

The HQ site is represented by one Organizational Unit that contains theses OU :

• Users that contains users, create one sub OU for each Department and Place in this OU users belonging to this Department.

• Computers that contains computers objects. Place in this OU, Computers and Servers (except controller) belonging to this Site

• The OU “Groups” contains all groups. Place in this OU all groups belonging to this Site

• Create one OU at root named “Shadow groups” and create one global group named “OU_Shadow” containing all users in OU “HQ”. When creating a new user for this Site, the user should automatically be added to this group in the following minute.

Users Provisioning

Provision 1000 users with SamAccountName/UserPrincipalName wslusrXXX (where wslusr001 is the first user and wslusr1000 is the last). Place them in following Active Directory Organizational Unit:

OU=AUTO,OU=USERS,DC=wsl2024,DC=org

• 500 first users must be placed in security Global group “FirstGroup”

• 500 last users must be placed in security group Global group “LastGroup”

Groups must be placed in OU=Groups,DC=wsl2024,DC=org

ADCS

Configure Enterprise Subordinate Certification Authority with following subject name: CN=WSFR-SUB-CA

Certificate for this SubCA must be issued by RootCA hosted on DNSSRV.

Adjust CRL Publishing Parameters:

• CRL publication interval: every day

• Delta CRL publication interval: every minute

• Delta CRL Overlap: every 12 hours

Only CRLs and Delta CRLs published must be used for certificates revocation checks accessing this URL: http://pki.hq.wsl2024.org.

Also configure AIA distribution point on the same site/folder.

When a new CRL is published, the CRL file must be automatically created in folder C:\inetpub\PKI.

Site name must be **PKI** (located on **C:\inetpub\PKI**)

Create WSFR_Services on-demand template certificate for all services

Create WSFR_Machines computer autoenrollment template certificate for all domain machines (servers and clients)

Create WSFR_Users user autoenrollment template certificate for all domain users

Storage

This server hosts all documents, storage purposes, DNS and Web services for WSI.

DATA partition:

- Attach 3 extra hard drive with a size of 1 Go (each) to this machine.
- Format these disk into a RAID-5 and
- NTFS partition called “DATA” (D:\).
- Enable deduplication on this volume.

File services

There are three shared folders:

1. Home drives

Create a file share for wsl2024.org users ‘home drives’:

- Share path: \\hq.wsl2024.org\users
- Local path: D:\shares\datausers
- Restrict permissions as needed:
    - Administrators must have Full control access on all folders
    - Users can only access their personal folder.
    - Users can only see their personal folder.
- Limit the storage quota to 20Mb
- Restrict all executables files saving
- Personal folder will be mounted on user’s sessions (use U: letter as mount point).

2. Department

- Located on D:\shares\Department
- Mounted with letter S:
- Users can only access their department folder
- Users can only see their department folder

3. Each department have a folder inside it named Public

- Located on C:\shares\Public
- Mounted with letter P:
- All users of the department have RW rights on this folder.

GPO

Configure Root CA certificate on the Root CA magazine and the Sub CA on the Sub CA magazine on every Windows hosts

Configure Edge to display the intranet as default home page and prevent user to change it

Users are not allowed to access to control pane except administrators

The enterprise logo have to displayed on every Windows hosts

HQFWSRV

This server should be configured with nftable to secure inbound communications and expose internal resources on the Internet.

Rules to apply on the network card exposed to Internet in the VLAN 30:

- Web request (http and https) should be forwarded to the web server HQWEBSVR
- MS RDS (Remote Desktop Services) should be forwarded to the server HQWEBSVR
- All unused ports should be closed.

Please consider that the VLAN 10 is only used for authentication on Active Directory

Keep in mind that some services may need some other ports to be open (example: IPSec VPN, SSH, etc).

Be sure to test every service after each firewall modification.

HQCLT

HQCLT VM is used to simulate workers located in headquarters. It should be able to access both corporate resources and the Internet.

IP addressing should be performed by DHCP from HQINFRASRV.

HQWEBSRV

This server should be configured with a web server and remote desktop server (RDS) to allow access to the corporate resources from the Internet:

- HQWEBSRV hosts HTTP and HTTPS websites (HTTP is automatically redirected to HTTPS) available both on private and publics networks by using the FQDN www.wsl2024.org. Public IP address in the subnet 217.N.160.X

- This server hosts MS-RDS to allow access to Excel and Word MS-Office applications for all users via a web browser.

- This server hosts a website https://authentication.wsl2024.org . To access the website an Active Directory authentication is required. Only Sales Active Directory group can have access.

SUPSRV

This server provides different tools to make an active supervision of all equipment: network devices and servers.He's delivering automation scripts in order to simplify the architecture maintenance.

Supervision:

You have to monitor environmental parameters of the network switches and routers, the CPU charge and the amount of free RAM of each server. For this goal, your team can choose your preferred solution i.e. Nagios, PRTG, Zabbix,…

This server will generate alarms for predefined events (i.e. temperature too high, fan down,...) , and in this case the IT group wall receive email warnings

Automation:

You have to use Ansible Playbook to define several automation scripts:

- Operating systems: update and upgrade the packages of all linux servers at midnight
- network equipment: on demand backup actual versions and deploy new versions of startup-config via a local tftp server
- active and configure snmp on all network equipment to use it with the supervision server.
- Install the telnet client on all windows servers.

All the scripts are stored into the FTPS server on INETSRV

MGMTCLT

MGMTCLT VM is used to access the configuration interface of the supervision server SUPSVR

3.3. REMOTE SITE CONFIGURATION

REMFW

This router act also as a firewall and should be configured with access lists to secure inbound communications between Remote Site and HQ site

- Only allowed services should be open from HQ site (SSH, DNS, HTTPS, Microsoft services, etc)
- All unused ports should be closed.

REMDCSRV

REMDCSVR is a server with Active Directory Services. He's in the forest hq.wsl2024.org a primary domain controller and global catalog for the domain rem.wsl2024.org. He's hosting his own DNS server for the rem.wsl2024.org zone and a replication of the hq.wsl2024.org zone. All others DNS requests are forwarded to wsl2024.org

DHCP

REMDCSRV provides DHCP service for Clients of the remote network with all necessary options in order to allow those networks to access to corporate services and Internet

This server provides dynamic IP addresses for client located on Remote site

Scope configuration:

- Subnet :10.N.100.0
- Netmask : To be defined
- Range : To be defined
- Gateway : To be defined
- Name server : remdcsrv.rem.wsl2024.org
- Domain : rem.wsl2024.org
- NTP server : hqinfrasrv.hq.wsl2024.org
- Lease : 2 hours

Configure Dynamic DNS to create the associated record corresponding to the distributed IP address.

DNS

DNSSec should be configured on this server with a certificate issued by HQDCSRV.

Active Directory

The remote site is represented by one Organizational Unit that contains two OU :

- Workers that contains users
- Computers that contains computers objects
- The OU “Groups” contains all groups.

The following GPO are configured and linked to each site OU :

- Members of IT group are local administrators
- Control Panel is blocked for everyone except for IT group members
- Mapping shares Department and Public
- Configure Root CA certificate on the Root CA magazine and the Sub CA on the Sub CA magazine on every Windows hosts

DFS

Create a DFS Domain root with REMINFRASRV

There are two shared folders:

1. Home drives

Create a file share for wsl2024.org users ‘home drives’:

- Share path: \\rem.wsl2024.org\users
- Local path: C:\shares\datausers
- Restrict permissions as needed:
  - Administrators must have Full control access on all folders
  - Users can only access their personal folder.
  - Users can only see their personal folder.

Limit the storage quota to 20Mb

2. Department share

- Located on C:\shares\Department
- Mounted with letter S:
- Users can only access their department folder.
- Users can only see their department folder.

REMINFRASRV

This server is a Active Directory Domain Member

This server provide fault tolerance in the Remote Site for different services: DNS, DHCP, DFS

REMPROXSRV

Web Proxy

This server should act as an internet proxy server for HTTP/HTTPS protocols.

He's filtering access to forbidden internet websites based on different blacklists.

You have to define a personalized filter blocking the web page bad.html stored in INETSRV.

VoIP

This server is a Voice over IP server based on Asterisk.

Each user should have a three digit telephone number beginning with 1xx for the HQ site and 2xx for the Remote site.

Each service has a group number beginning with 3xx

A voice trunk SIP is available between this server and HQMAILSRV the voice over IP Asterisk server for the HQ site.

REMCLT

REMCLT VM is used to simulate a MAN client

IP addressing should be performed by DHCP from REMINFRASVR

It should be able to access both corporate resources and the Internet.

3.4. INTERNET SITE CONFIGURATION

On the Internet side, every host IP is static according to the diagram.

DNSSRV

DNS

This server provides DNS services for public networks and hosts **worldskills.org** and **wsl2024.org** zones.

The following DNS records are configured:

Type	FQDN / Alias	IP address / FQDN
A	inetsrv.worldskills.org	8.8.N.X
CNAME	www.worldskills.org	inetsrv.worldskills.org
CNAME	ftp.worldskills.org	inetsrv.worldskills.org
A	wanrtr.worldskills.org	8.8.N.X
A	hqfwsrv.wsl2024.org	217.N.160.X
A	vpn.wsl2024.org	191.5.157.33
A	webmail.wsl2024.org	191.5.157.33
CNAME	www.wsl2024.org	hqfwsrv.wsl2024.org
CNAME	authentication.wsl2024.org	hqfwsrv.wsl2024.org

Please enable DNSSEC on this Server

Certificate Authority

Configure Root Certification Authority with following details :

- Country = FR
- Province = Auvergne Rhone-Alpes
- City = Lyon
- Organization = Worldskills France
- Email = npresso@wsl2024.org
- OU = Worldskills France Lyon 2024
- CN = WSFR-ROOT-CA

This server will issue the Enterprise SubCA of HQDCSRV.

He provides certificates to secure all services on the Internet side with the domain worldskills.org

INETSRV

INETSRV hosts web services such as websites HTTPS, HTTPS (HTTP is automatically redirected to HTTPS) and FTP Services are respectively accessible by using **www.worldskills.org** and **ftp.worldskills.org**.

All certificates are provided by DNSSRV

Web server

You have to configure two web servers which provide High Availibility. For this goal you have to use Docker containers for each ngnix web server

PHP support is enabled

Configure a start page which displays the IP address of the client and the type and version of web browser used by the client and the actual date and time.

Configure a page named bad.html with a dangerous content

As a basic security measure, make sure that no sensitive information is displayed in the HTTP headers and the footer.

FTP

This server is used for scripts Storage

Configure ProFTPd as secured FTPS server :

- Create user named devops
- Allow uploading / downloading file from FTP

VPNCLT

VPNCLT VM is used to simulate a VPN client.

The VM is a member of the hq.wsl2024.org domain.

It uses OpenVPN to establish a connection to HQINFRASRV, to access all the corporate resources.

INETCLT

CLT VM is used to simulate an Internet client

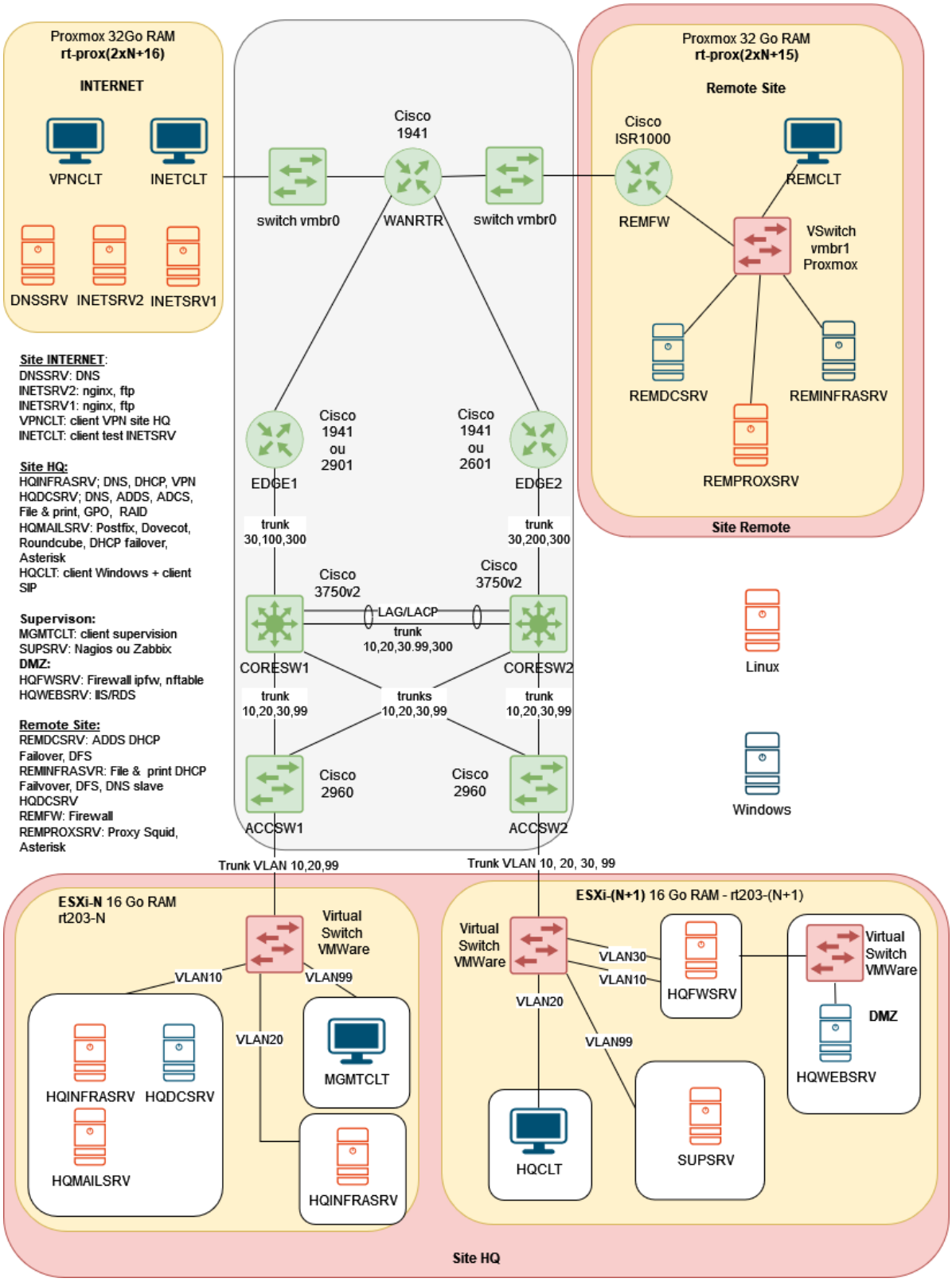
it should be able to access all Internet services and corporate site www.wsl2024.org.

4. APPENDICES

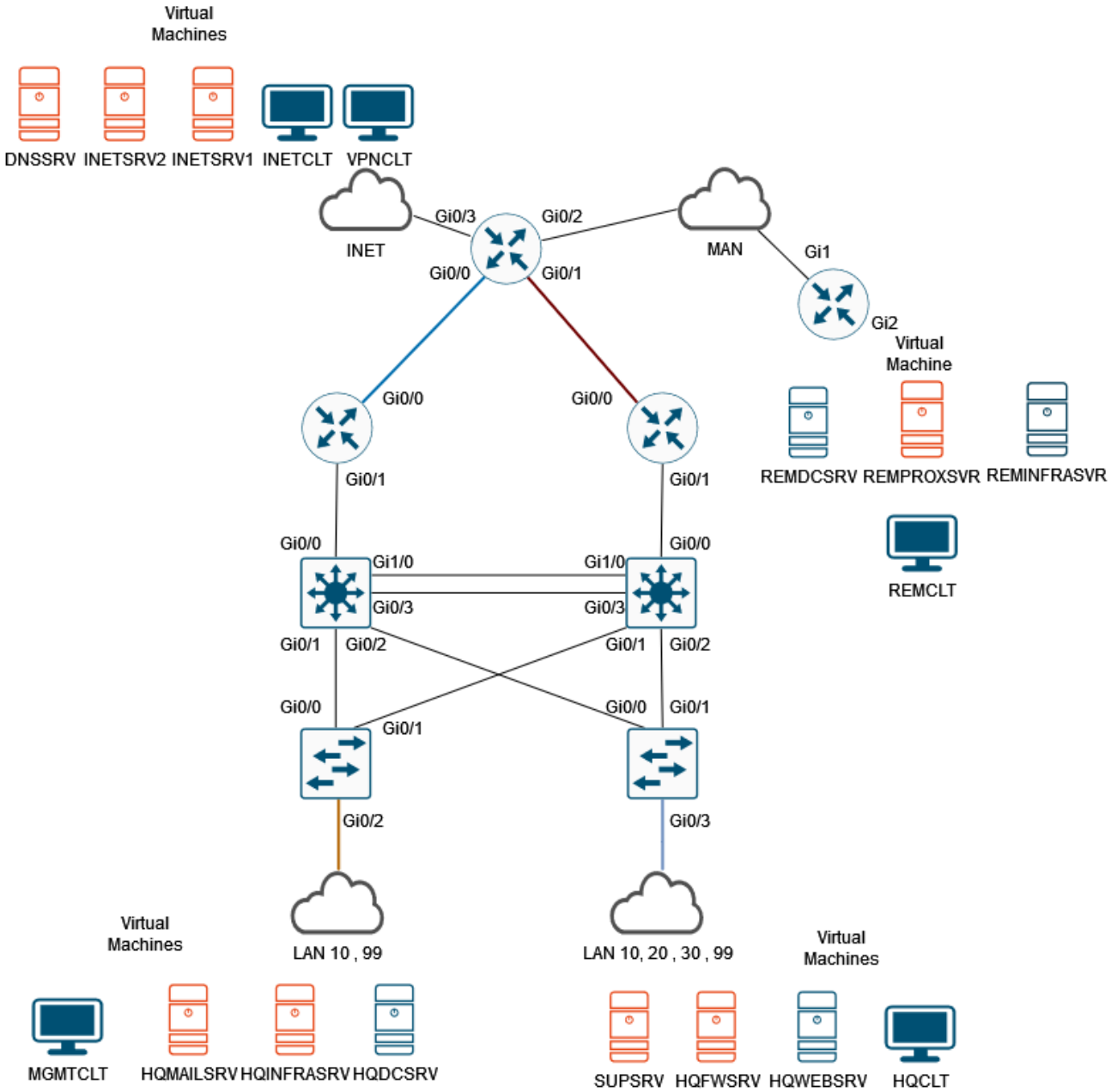
4.1. USERS AND GROUPS ACTIVE DIRECTORY

Name	Login	AD group	Site	email	Office Number
Vincent TIM	vtim	IT	HQ	vtim@wsl2024.org	1XX
Ness PRESSO	npresso	Direction	HQ	npresso@wsl2024.org	1XX
Jean TICIPE	jticipe	Factory	HQ	jticipe@wsl2024.org	1XX
Rick OLA	rola	Sales	HQ	rola@wsl2024.org	1XX
Ela STIQUE	estique	Warehouse	REM	estique@wsl2024.org	2XX
Clotilde Morin	cmorin	Direction	REM	cmorin@wsl2024.org	2XX
Denis Peltier	dpeltier	IT	REM	dpeltier@wsl2024.org	2XX

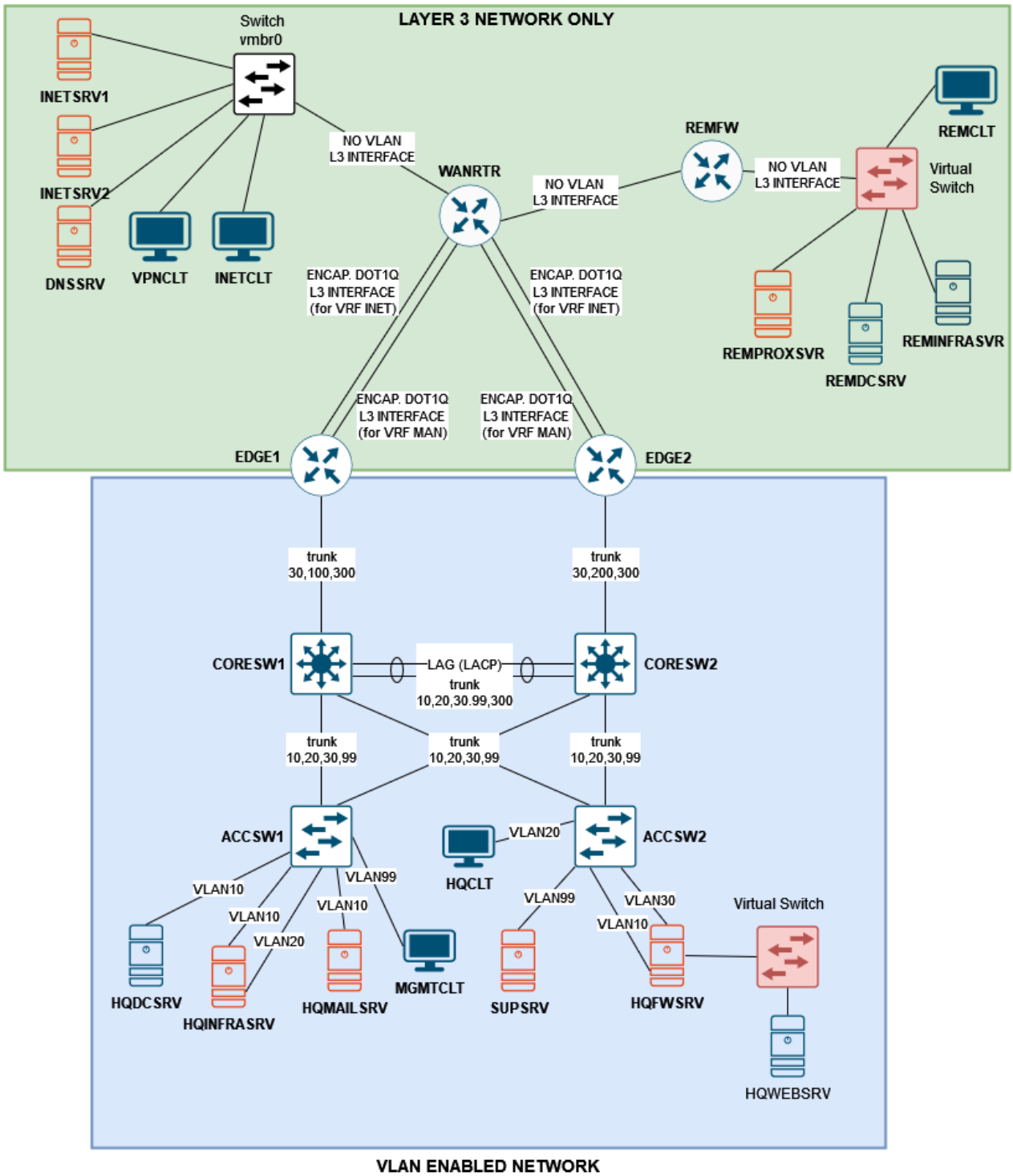
4.2. PHYSICAL DIAGRAM – SIMPLIFIED



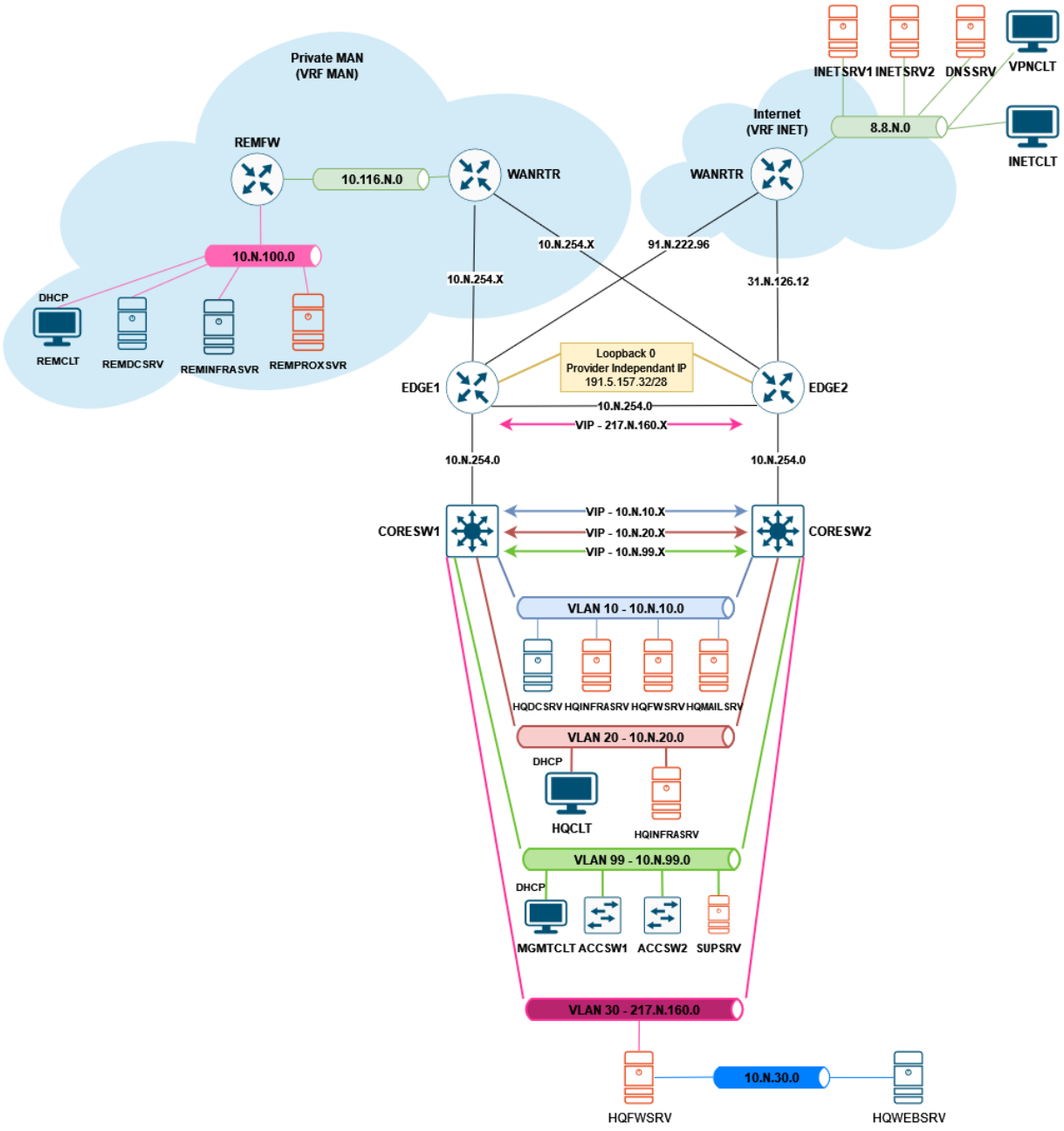
4.3. PHYSICAL DIAGRAM – DETAILLED



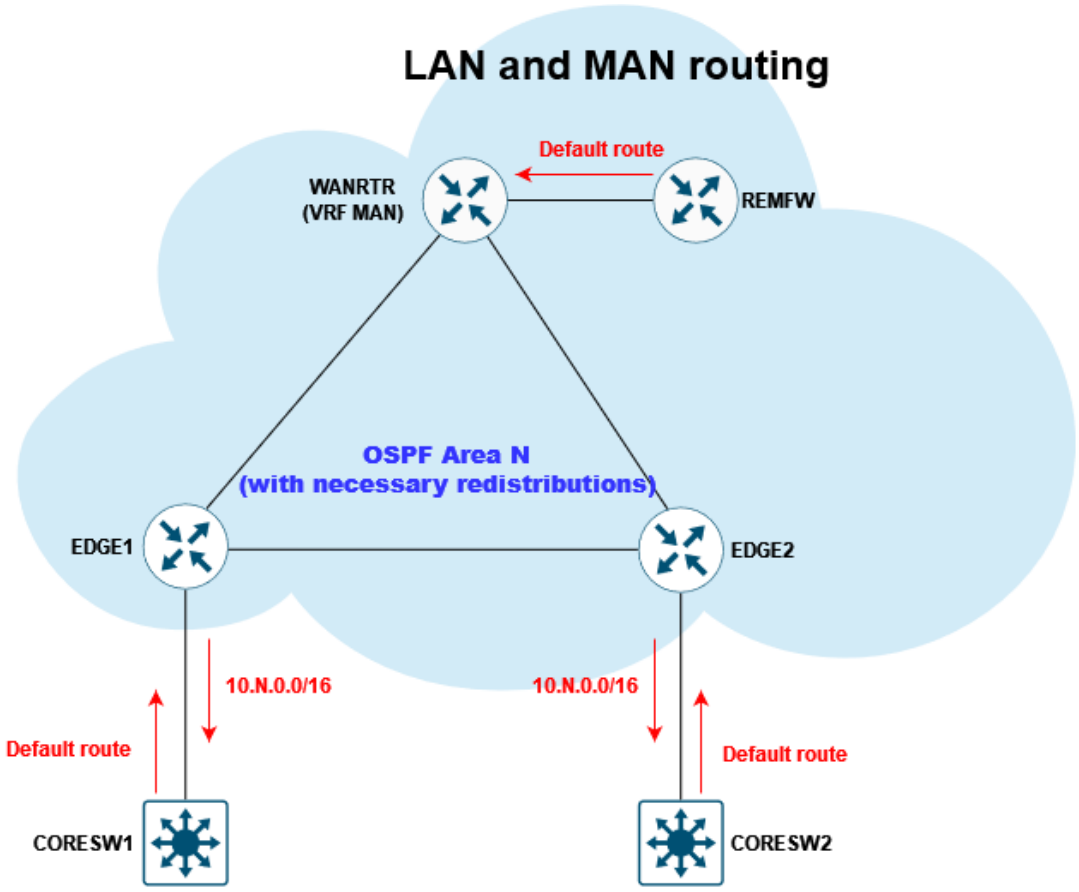
4.4. LOGICAL DIAGRAM – LAYER 2

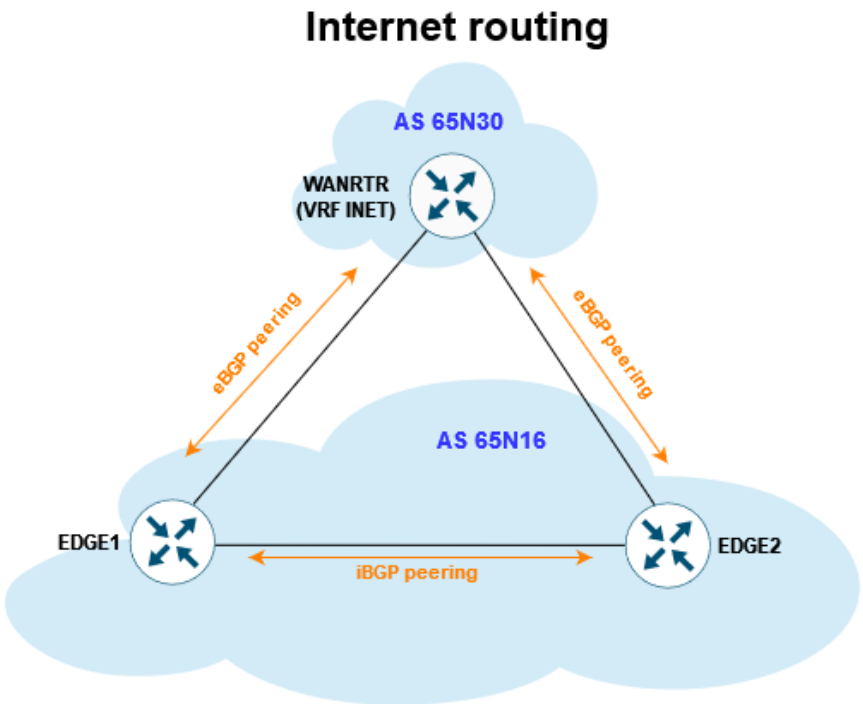


4.5. LOGICAL DIAGRAM – LAYER 3



4.6. LOGICAL DIAGRAM – ROUTING DIAGRAM





4.7. LOGICAL DIAGRAM – DNS