# Network and System Defence
# Final Projects AY 2023/2024

## General rules for both projects:

### Addressing:

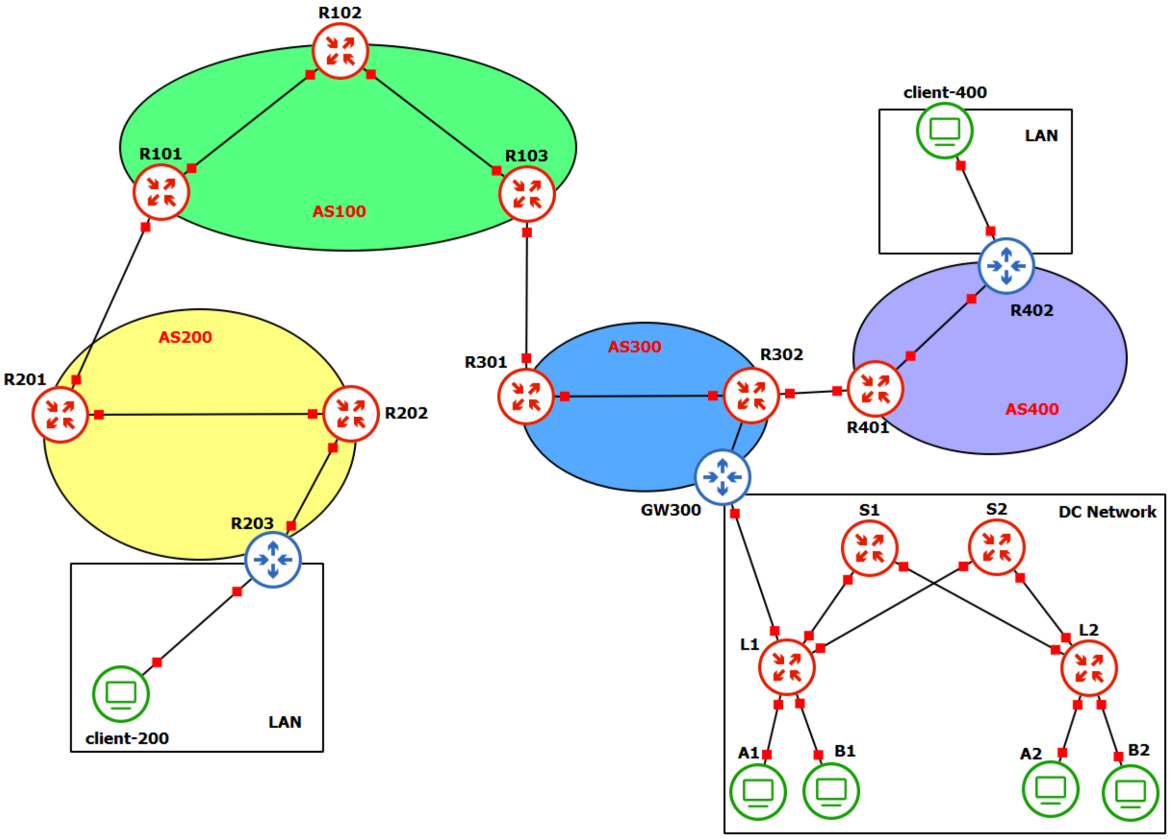
- Assign the IP addresses at will, but pay attention to the IP address pool you choose:
  - Private address ranges for private networks
  - Public address ranges for the ASes
  - /30 private networks for point-to-point links between routers

### Legend:

- Red nodes are FRR routers (nsdcourse/frr:latest)
- Green nodes are simple clients (nsdcourse/basenet:latest)
- Blue nodes are Linux routers (nsdcourse/basenet:latest)
- Blue switches (with the 3D icon) are simple GNS3 L2 switches
- The leaf-spine topology in Project 1 is composed of Cumulus Linux VMs

**NOTE:** Any assignment not explicitly specified in this document is up to your discretion.

# Project #1



## AS100

- AS100 is a transit Autonomous System providing network access to two customers: AS200 and AS300
    - Configure eBGP peering with AS200 and AS300
    - Configure iBGP peering between border routers
    - Configure OSPF
    - Configure LDP/MPLS in the core network

## AS200

AS 200 is a customer AS connected to AS100, which provides transit services.

- Setup eBGP peering with AS100
- Configure iBGP peering
- Configure internal routing as you wish (with or without OSPF)
- ***R203*** is **not** a BGP speaker
    - It has a default route towards R202
    - It has a public IP address from the IP address pool of AS200
    - It is the Access Gateway for the LAN attached to it
        - Configure dynamic NAT

        - Configure a simple firewall to allow just connections initiated from the LAN

**Client 200**

- This device is sensitive, so it must be configured to use ***Mandatory Access Control***.
- OpenVPN → see later dedicated section.

## AS300

AS 300 is a customer AS connected to AS 100, which provides transit services. It also has a lateral peering relationship with AS 400.

- Setup eBGP peering with AS400 and AS100
- Configure iBGP peering
- Configure internal routing as you wish (with or without OSPF)
- ***GW300*** is **not** a BGP speaker
    - It has a default route towards R302
    - It has a public IP address from the IP address pool of AS300
    - It is the Access Gateway for the Data Center network attached to it
        - Configure dynamic NAT
        - OpenVPN server → see later dedicated section

## DC Network

DC Network is a leaf-spine Data Center network with two leaves and two spines. There are 2 tenants (A and B) in the cloud network, each hosting two virtual machines connected to leaf1 and leaf2. The tenants are assigned **one** broadcast domain each.

- Realize VXLAN/EVPN forwarding in the DC network to provide L2VPNs between the tenants' machines
- In L1, enable the connectivity to the external network. In other words, both tenants' machines must reach the external network through the link between L1 and R303, including the encapsulation in OpenVPN tunnels when necessary.

## AS400

AS 400 has a lateral peering relationship with AS 300.

- Setup eBGP peering with AS400 and AS100
- ***R402*** is **not** a BGP speaker
    - It has a default route towards R401
    - It has a public IP address from the IP address pool of AS400
    - It is the Access Gateway for the LAN attached to it
        - Configure dynamic NAT
        - Configure OpenVPN→ see later dedicated section

**Client 400**

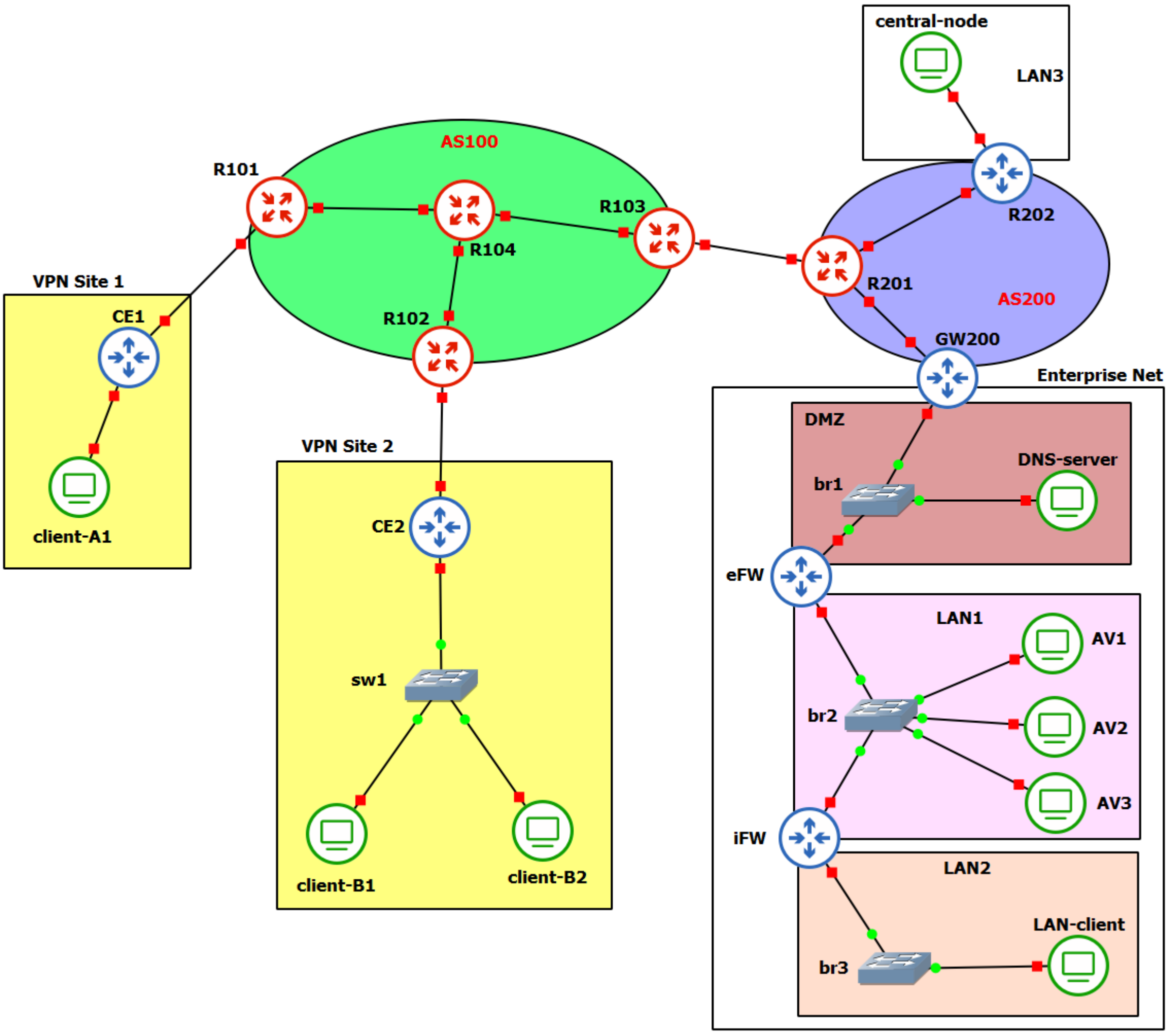
- This is a simple LAN device with a default route through R402.

## OPENVPN

Setup OpenVPN to realize a VPN between client-200, R402’s LAN, and the DataCenter network.

- **Client-200** is an OpenVPN client
- **R402** is an OpenVPN client, providing VPN access to and from the LAN attached to it.
- **GW300** is the OpenVPN server, providing VPN access to and from the Data Center network. In particular, the network belonging to tenant A must be accessible through the VPN.

# Project #2



## AS 100

- AS100 has a BGP peering relationship with AS200 and provides a BGP/MPLS VPN to two sites of one customer (in yellow).
    - Configure eBGP peering with AS200
    - Configure iBGP peering between border routers
    - Configure OSPF
    - Configure LDP/MPLS in the core network
    - R101 is the provider edge for VPN Site 1
    - R102 is the provider edge for VPN Site 2

## VPN Site 1

VPN Site 1 has just one customer edge (CE1) and one LAN client (client-A1).

## VPN Site 2

VPN Site 2 has one customer edge (CE2) and two clients in the LAN (client-B1 and client-B2).
Configure MACSEC in the LAN (you can configure it statically with iproute2 or automatically with MKA).

## AS200

AS 200 has a lateral peering relationship with AS 100.

- Setup eBGP peering with AS100
- ***R202*** is **not** a BGP speaker
    - It has a default route towards R201
    - It implements a VPN with IPSEC towards eFW → see later dedicated section
- ***GW200*** is **not** a BGP speaker
    - It has a default route towards R201
    - It is the edge gateway for the Enterprise Network behind it

## LAN3

LAN3 is a simple LAN with one device (the central-node).

## Enterprise Network

In the Enterprise network, we have multiple sub-networks interconnected by some L3 devices:

- **DMZ** is the Demilitarized Zone
    - It is a sub-network with address range taken from the AS200 IP pool
    - It hosts a **DNS server** which implements the following services:
        - DNSSEC enabled authoritative nameserver for "***nsdcourse.xyz***", which publishes the records for the "***www***" subdomain
            - NOTE: obviously, don't ***actually*** register the domain. Consequently, you do not have to publish any DS record in any parent zone
        - Apache2 simple web server accessible through "www.nsdcourse.xyz"
        - **NOTE:** you will have to create a custom docker image and install Bind9 (you can start from the "nsdcourse/basenet")
    - **eFW** is a Linux router implementing an external Firewall and forwarding packets between the DMZ and LAN1
- **LAN1** is the LAN which hosts three antivirus runners → see later dedicated section
    - **iFW** is a Linux router implementing an internal Firewall and forwarding packets between the LAN1 and LAN2
- **LAN2** is a simple LAN with one client device (LAN-client)

- **Security Policy for the Firewalls. Configure the Firewalls and the GW200 accordingly:**
    - LAN-client can access the external network (both the "Internet" and the DNS server) only the connection is originated by it
    - Traffic from/to the AVs is enabled exclusively between the AVs and the *central-node* in LAN3

    - From the external network, allow inbound connections for the following types of traffic:
        - DNS requests to *DNS-server*
        - HTTP traffic to *DNS-server*
        - IPSEC traffic to *eFW*

## IPsec configuration

Configure an IPSec tunnel between R202 and eFW to create a site-to-site VPN between LAN3 and LAN1, using strongswan. This is needed for the end-to-end communication between the central node and the AVs.

## Antivirus Runners and Central Node

You are expected to create a virtualized environment to test binaries for the presence of malware. In particular, you have to setup three virtual machines or containers in LAN1, each hosting a different AV of your choice.

A central node (in LAN3) will allow dropping an executable and distributing it to the various testing nodes. The testing nodes will scan/run the executables and deliver results to the central node, which will build a report to the user, showing what threats (if any) were discovered in the binary.

Given the criticality of this infrastructure, certain precautions must be taken:

1. Runner nodes must be subject to snapshots so that they can be restarted in a 'clean' state each time a new scan has to be started.
2. To prevent the exfiltration of threats on the network, nodes must be protected by firewalls. Refer to the “Enterprise Networks” section for the specific policies.

In the central node, if needed, setup an external internet connection through a NAT GNS3 node (not displayed in the figure).