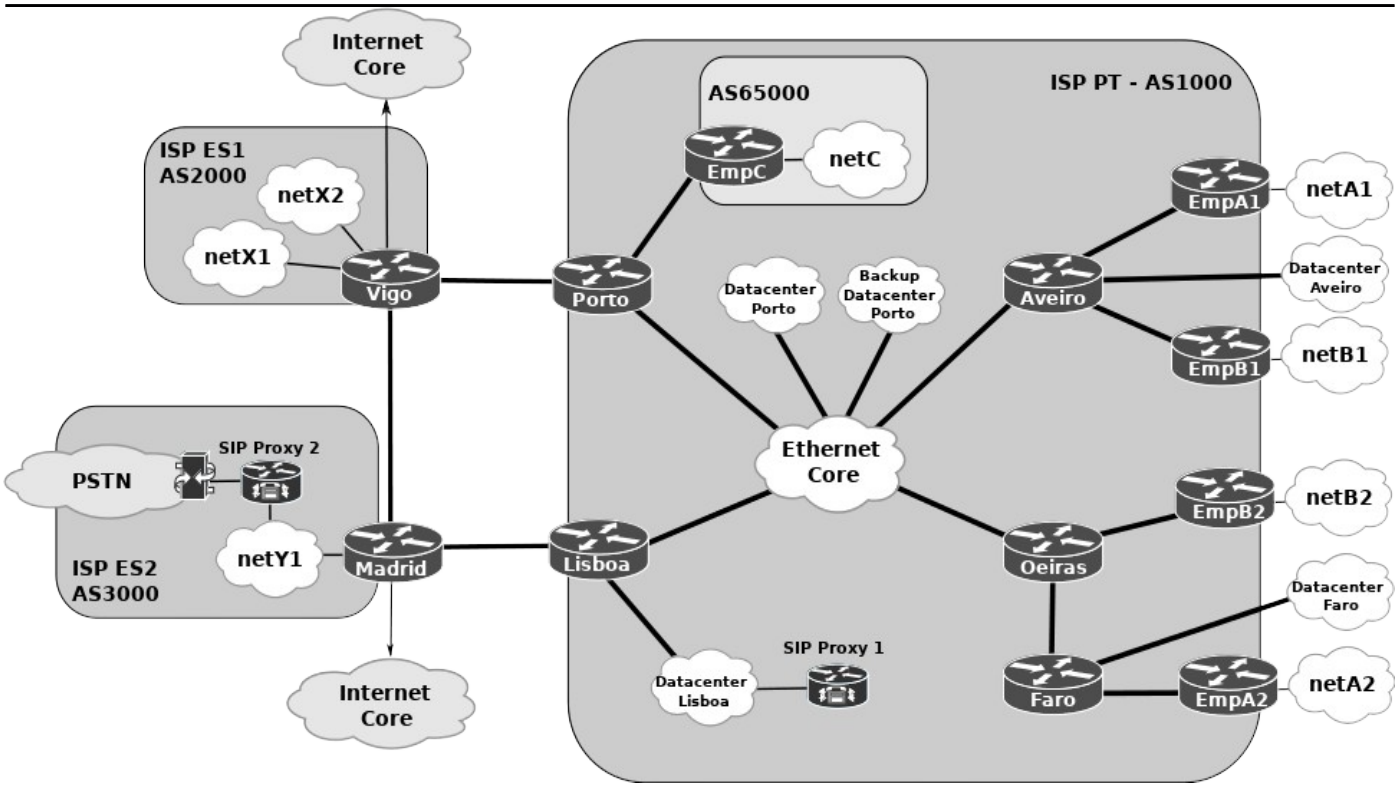
Arquitetura de Redes Avançadas
Project

Professors:
Paulo Salvador (salvador@ua.pt); Susana Sargento (susana@ua.pt); João Paulo Barraca (jpbarraca@ua.pt)

- **The project must be deployed and tested using GNS3.**
- **All engineering choices must have a valid justification.**



Scenario description:

- Assume that you are the engineer responsible for ISP PT (AS1000) depicted above. All other ISPs are configured with default/minimal BGP configurations.
- AS1000 has one peering relation with ISP ES1 (AS2000) via Porto, and one peering relation with ISP ES2 (AS3000) via Lisboa.
- ISP PT is a non-transit AS.
- ISP PT has two corporate clients/partners (A, B), to which provides IP inter-connectivity and a VoIP service with PSTN inter-connectivity (through SIP Proxy 1).
- Corporate client C, has a single location in Porto, however is a private BGP autonomous system (AS 65000).
- Corporate clients A and B have two branches, one in Aveiro and another in Oeiras/Faro.
- ISP PT has three independent datacenters in Lisboa, Aveiro, Faro, and two more in Porto (core).
- Both ISP ES1 and ISP ES2 provide IP interconnection to the Internet Core.
- ISP ES2 provides PSTN interconnection through SIP Proxy 2.

- ISPs and Corporate clients have the following IPv4 and IPv6 IP networks:

ISP PT - core and internal point-to-point links	192.100.1.0/24 10.0.0.0/8	2001:100:1::/48
Datacenter Lisboa	192.100.2.0/24	2001:100:2::/48
Datacenter Aveiro	192.100.3.0/24	2001:100:3::/48
Datacenter Faro	192.100.4.0/24	2001:100:4::/48
(Backup) Datacenter Porto	192.100.5.0/24	2001:100:5::/48
Corporate client A	110.1.1.0/24	3001:11::/48
Corporate client B	110.2.1.0/24	3001:21::/48
Corporate client C	110.3.1.0/24	3001:31::/48
ISP ES1 - netX1	200.100.1.0/24	2201:200:100::/48
ISP ES1 - netX2	200.200.1.0/24	2201:200:200::/48
ISP ES2 - netY1	65.0.1.0/24	2201:65:0:/48
External BGP peering links	4.4.4.0/26	2001:4:4::/60

Deployment requirements/tasks:

1. Basic mechanisms and BGP (6 points)

- Provide full IPv4 and IPv6 between ISP PT clients and Internet Core, according to scenario constrains (above) and ISP networking good practices.
- Implement the following MP-BGP routing constrains (within ISP PT):
  - IP traffic towards Internet should be preferably routed via ISP ES2.
  - IP traffic towards all AS3000 originated networks, should be preferably routed via Porto (ISP ES1) from Aveiro, and via Lisboa (ISP ES2) from Oeiras.
  - IP traffic for remote SIP proxy 2 (to network netY1) cannot be routed via Porto using the peering link to ISP ES1.

  Note: You must assume that (i) ISPs ES1 and ES2 receive multiple network prefixes from the Internet Core, and (ii) those prefixes are sent to all its BGP peers.

2. MPLS (6 points)

- Client A requested one bi-directional channel with dedicated bandwidth of 20Mbps between the Aveiro and Faro branches for all HTTP (port 80) and HTTPS (port 443) traffic. Deploy the required MPLS tunnels and respective routing mechanisms.
- Deploy a MPLS VPN for Corporate client B (interconnecting Aveiro and Oeiras branches).

3. VoIP - SIP (2 points)

- Deploy a VoIP - SIP service for all ISP PT corporate clients. The service provides VoIP connectivity (through SIP proxy 1) between internal clients and forwards all other calls (including PSTN numbers) to ISP ES2 SIP proxy. The assigned (PSTN compatible) telephone numbers are: for Corporate client A 23410xxxx and 28910xxxx and for Corporate client B 23411xxxx and 21911xxxx.

4. CDN (3 points)

- Deploy a CDN routing service (Conditional DNS) for corporate clients. The DNS server is located in the Lisboa Datacenter, and must be able to redirect clients to the closest Datacenter according to their location, i.e., terminals in Aveiro to the Aveiro Datacenter, terminals in Faro to the Faro Datacenter, and all other internal or external terminals to the Lisboa Datacenter.
- Improve the CDN routing service (Conditional DNS) by including a link/router/server load/availability condition in the decision process.

5. SDN (Open vSwitch) (3 Points):

- Convert the Ethernet Core to an Open vSwitch (OVS) core to implement: (i) traffic blocking from Internet to a corporate client based on a specific rule defined by management, and (ii) redirect traffic from Datacenter A to Backup Datacenter B upon a management request (you must assume that backup servers have the same IPv4 addresses as the main servers).

Extras (1 Point each):

- Students may propose additional services/mechanisms to incorporate into the project (subject to professors' approval). Professors may also suggest other additions upon completion of the mandatory requirements.

Deployment and Demonstration notes:

- During demonstration, if necessary due to lack of computational resources, some routers/VMs may be turned off (where/when irrelevant to mechanisms being shown).
- For tasks 1 to 4, the Ethernet core may be implemented using a single L2 switch.
- For task 5, the network core may be implemented using a single Virtual Machine with Linux/OVS. Task 5 may be deployed in a different GNS3 project.
- Datacenters (without services deployed) may be simulated using a single L2 switch and VPCS.
- To test SIP deployment just make SIP proxy 2 "answer" all calls forwarded towards him as a simple client.