# EuroSkills Herning 2025 - EuroSkills 2025

# **IT Network Systems Administration**

## **National Final**

## 24th-25th April 2024

## Budapest, Hungary

# **Day 1**

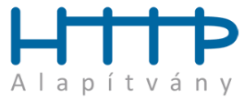
Velkommen [Welcome] again to our company, the Lego Group!

# We were very satisfied with your work in the previous rounds and hired you for the last but most important project. For now, the final network and server devices have arrived in our new factory called BlokFabrik in Billund (Denmark). In the final round your task will be to continue the implementation of our infrastructure and use more advanced and more secure technologies. In the past few days, we have got a huge number of orders for Lego collections, so it’s time to start!

# Held og lykke [Good luck] and have a nice time in Denmark!

# **Preliminary Notice**

1. **X always means your desk number.**
2. All **devices will be rebooted** before marking. Ensure that all your settings are kept during reboots.
3. **Do NOT protect the console access to Cisco devices!** If we won’t be able to login to a device on its console line without using password or any other authentication parameter, then **we are not going to mark any task that you completed on the device.**
4. Use the password ***Euro2025+*** everywhere, where you need to configure password, passphrase or anything like that.





## Accessing infrastructure

You will access all network devices in Cisco Modeling Labs from any web browser on your laptop at *network.cml* URL. Your credentials will be given separately. You will see an *ES2025-National-Final\_POD-<X>* lab topology containing all the network devices.

You will access test servers and clients sitting in place of external connectors from VMware Workstation at *vmware.euroskills* URL. Your credentials will be given separately. You will have access to five VMs, all of them have Debian 12 (CLI only) OS. You can use *root* user to login to this VMs.

## Preliminary configuration

To make ICMP packets pass through the ASA firewall, enable ICMP protocol inspection with the commands below (in global config mode):

policy-map global\_policy

class inspection\_default

inspect icmp

## Network Tasks

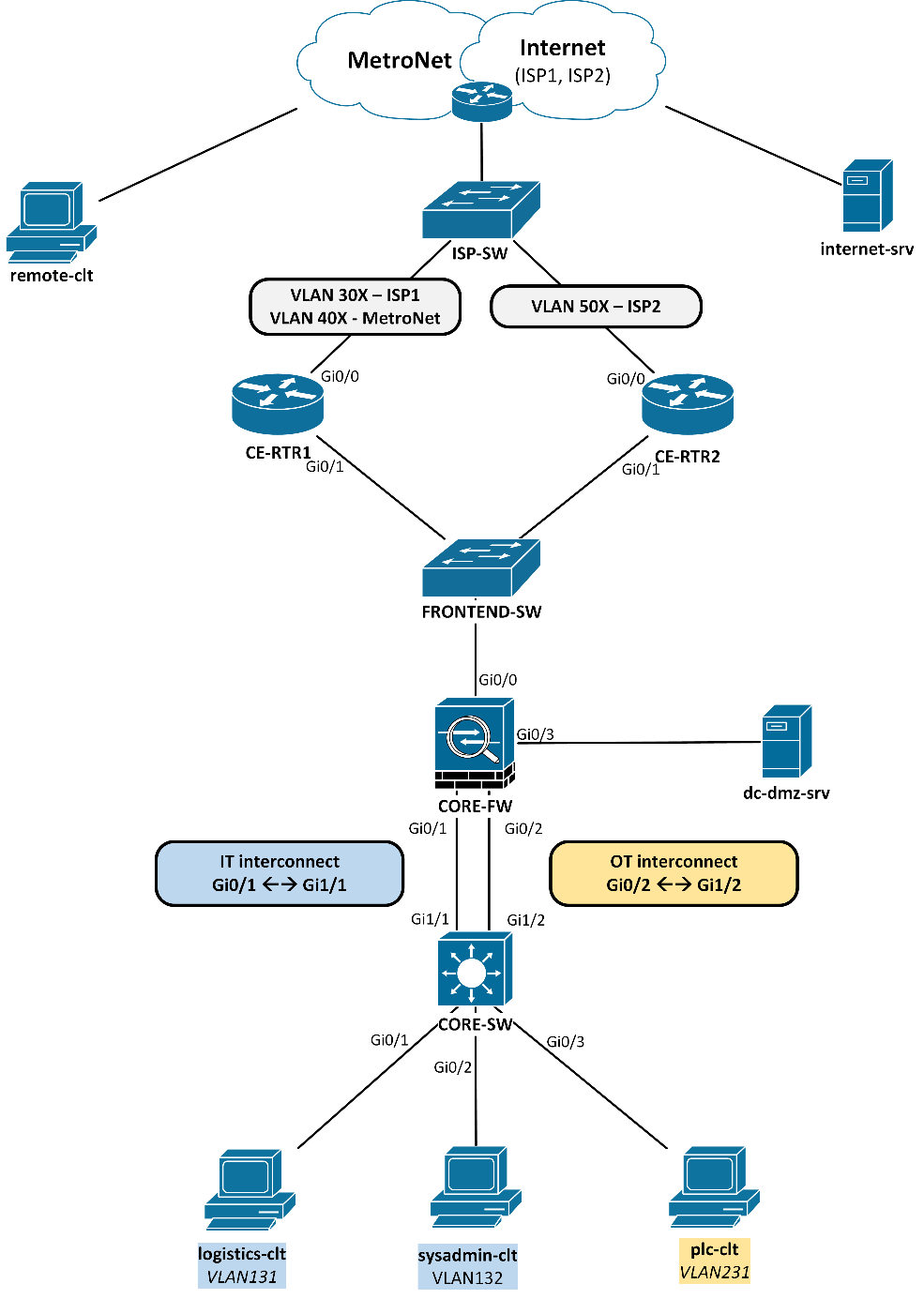
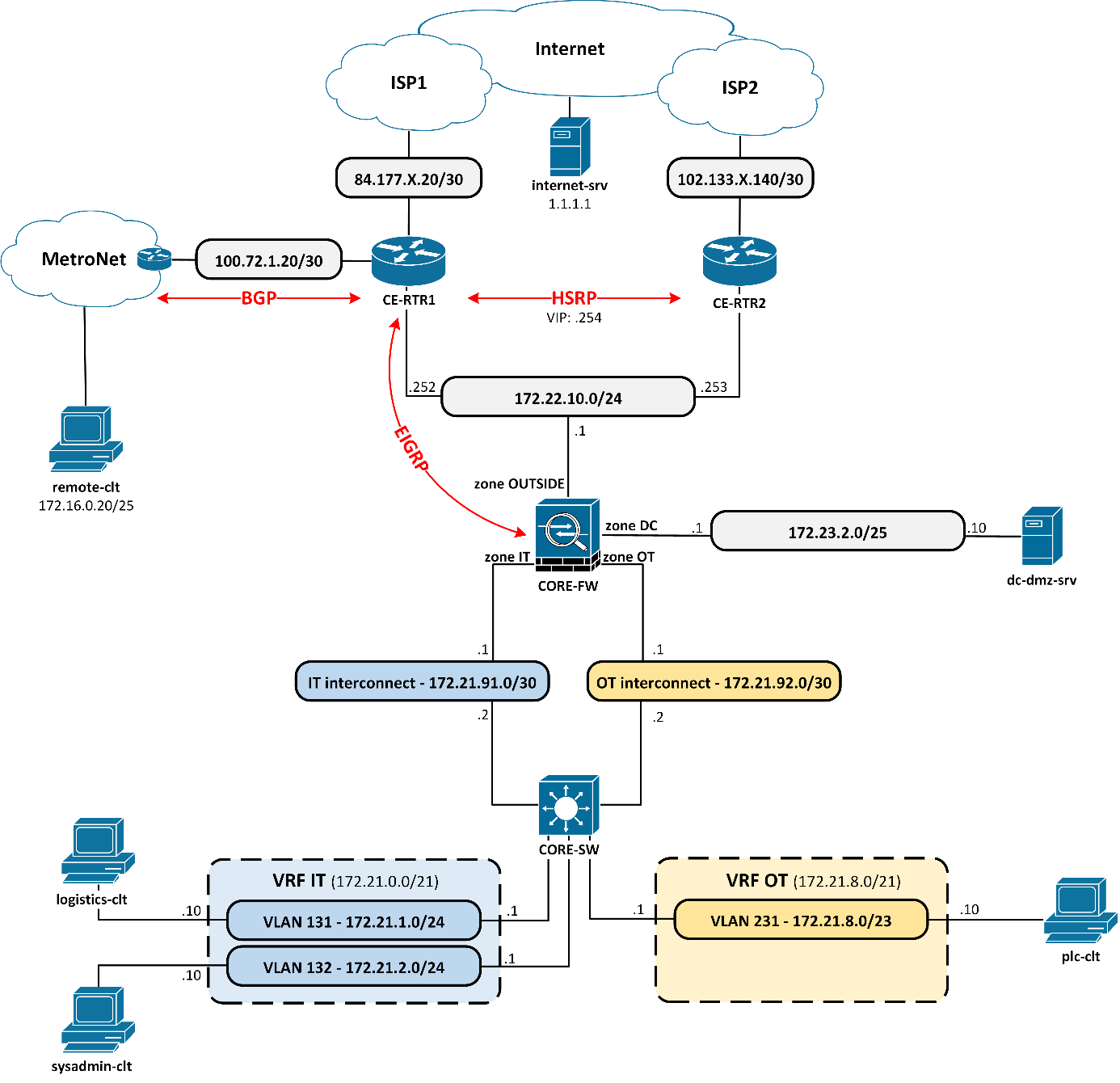


Figure 1 – Layer 1-2 topology

 Figure 2 – Layer 3 topology

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VLAN ID** | **VLAN name** | **IP subnet** | **Gateway** | **VRF** |
| 131 | BLOKFABRIK\_LOGISTICS | 172.21.1.0/24 | 172.21.1.1 | IT |
| 132 | BLOKFABRIK\_SYSADMIN | 172.21.2.0/24 | 172.21.2.1 | IT |
| 231 | BLOKFABRIK\_PLC | 172.21.8.0/23 | 172.21.8.1 | OT |

Table 1 - VLAN assignments

1. Configure the **hostname** and **domain name** for every network device based on the diagram (except unmanaged switches). Use *lego.local* as domain name.
2. Create all **VLANs** on the core switch according to the table above. Configure the endpoint facing interfaces as access ports in the appropriate VLANs. Ensure when an end device is connected to any of these ports, they are going immediately to forwarding state. Set up that any port will be disabled when they detect BPDUs.
3. Configure VLAN **SVI interfaces** for the VLANs listed above as their default gateway according to topology. Use the first usable IP address for them.
4. Configure **routed interfaces** between the core switch and firewall. Use the interconnect subnets in the topology.
5. Separate the factory’s two main parts from each other using **VRF-lite technology** on the core switch. Create IT and OT VRFs and place the appropriate interfaces into them according to topology (different color represent different VRF).
6. Create default **static routes in both VRFs** on the core switch pointing to the ASA, therefore clients in different VRFs should communicate with each other only through the firewall.
7. Set up **firewall interfaces** with IPs and zones according to the topology. You can use arbitrary security levels to fulfill the requirements of other tasks.
8. Set up **HSRP** in the 172.22.10.0/24 segment between the routers. Use the last available IPv4 address as virtual IP. By default, CE-RTR1 needs to be the active member. If CE-RTR1 or its uplink connection to ISP1 fails (physical link failure or inaccessible ISP device via ICMP), then CE-RTR2 should take over the role of the active member. As soon as CE-RTR1 or its uplink connection is working properly again, it has to regain the role of the active gateway. Use MD5-based authentication for HSRP messages using the common passphrase.
9. Configure **static routes on the firewall** using the following guidelines:
   1. Point the default static route to the HSRP VIP address.
   2. Route the VRF supernets statically toward the core switch’s respective IP.
10. Both **routers’ ISP lines** should use the first usable address from the provided public networks. Point the default static routes on both routers to the last usable address from the pools respectively. The 172.22.10.0/24 subnet should be translated dynamically (overloading) to the ISP facing interfaces’ IP address.
11. Use **NAT on the firewall** to meet the requirements below:
    1. dc-dmz-srv should be translated statically to IP address 172.22.10.10.
    2. Both VRFs (IT and OT, whole supernets) should be translated dynamically to the ASA’s OUTSIDE interface.
12. Use **ACLs** and appropriate security levels **on the core firewall** to fulfill the requirements below:
    1. Only VLAN 132 subnet from IT VRF should access VLAN 231 subnet in OT VRF via SSH (TCP/22). Any other access from IT to OT VRF or vice versa is prohibited.
    2. Both IT and OT VRFs should access DC and OUTSIDE zones via any port and protocol.
    3. Resources outside the factory nor DC zone should not access clients located in IT or OT VRFs.
    4. Resources outside the factory should access only dc-dmz-srv located in the DC via HTTP and ICMP protocol.
13. Advertise the factory’s 172.22.10.0/24 IP subnet via **BGP** to the MetroNet line. Use common BGP password when peering with the MetroNet route reflector (RR). Your AS number will be 2025, and the provider owns 2024. Ensure that only RFC-1918 Class B prefixes are accepted with subnet mask greater than or equal to /24.
14. Configure **EIGRP** protocol between the firewall and CE-RTR1 through the OUTSIDE segment. Use AS number 2025. Use MD5 authentication to form adjacency. Redistribute all routes learned from BGP to the EIGRP process.
15. Configure **unicast Reverse Path Forwarding check (uRPF)** (strict mode) on the core switch in the OT VRF to prevent IP spoofing attacks. To test functionality, use the following command on plc-clt:

hping3 -c 3 -a 172.21.5.10 -p 80 -S 172.23.2.10

1. When accessing the Internet while web browsing from IT or OT VRFs, every factory client should use transparent web proxy service running in the DC. To restrict them to use proxy, configure **policy-based routing on the ASA** while considering the following guidelines:
   1. Only HTTP (TCP/80) traffic coming from IT or OT VRFs (whole VRF supernets) should be redirected.
   2. Traffic going to any RFC-1918 private IP addresses should not be redirected.
   3. The IP next-hop should be set to 172.23.2.10.