EuroSkills Test Project

ICT Specialists (39)
Module C – Network Environment

Submitted by:

Christian Schöndorfer - AT (TL)
Raphaël Lienard - BE
Almut Leykauff-Bothe - DE
Igors Bumanis – LV
José Medeiros - PT

Introduction to Test Project

Contents

This Test Project proposal consists of the following two documentations/files:

1. ES2023_TP_39_Modlule_C_pre_EN.docx
2. ES2023_TP_39_Module_C_pre_CML.yaml

Introduction

Network technology knowledge is becoming essential nowadays for people who want to build a successful career in any IT engineering field. This test project contains a lot of challenges from real life experience, primarily IT integration and IT outsourcing. If you are able to complete this project with the high score, you are definitely ready to service the network infrastructure for any multi-branch enterprise.

Description of project and tasks

Current test project is designed using a variety of network technologies with which you should be familiar within the Cisco certification tracks. Tasks are broken down into following configuration sections:

- Basic configuration
- Campus and branch LAN
- Public internet
- Enterprise routing
- Unified communications infrastructure

Some tasks are pretty simple and straight, some may be tricky. You may see that some technologies are expected to work on top of other technologies. It is important to understand that if you cannot come up with any solution in the middle of such technology stack it doesn't mean that the rest of your work will not be graded at all. For example, you may not configure IPv4 routing that is required for VPN because of IP reachability but you can use static routes and then continue to work with VPN configuration and everything that runs on top. You won't receive points for IPv4 routing in this case but you will receive points for everything that you made on top as long as functional testing is successful.

Instructions to the Competitor

- Read all tasks in each section before proceeding with any configuration. The completion of any item may require the completion of any previous or later item.
- Before starting the test project, confirm that all devices in your topology are in working order. During the test project, if any device is locked or inaccessible for any reason, you must recover it. When you complete this test project, ensure that all devices are accessible to the grading Experts. A device that is not accessible for grading cannot be marked and may cause you to lose substantial points.
- Knowledge of implementation and troubleshooting techniques is part of the skills being tested in the configuration section of the Test Project.

- Points are awarded for working configurations only. Test the functionality of all the requirements before you complete this test project. As you configure one part, you may break a previous requirement or configuration.
- No partial points can be granted for any aspect; all requirements need to be fulfilled to receive the points for the aspect. Some requirements depend on other aspect's requirements, either before or after the current aspect.
- Save your configurations frequently.
- Use alpha-numeric characters only in any variable name (access-list, prefix-list, route-map, etc); that is, do not use any punctuation or special characters (.,;:'/|\?!_-(){}*&^%$#@).
- Make sure that all your configurations are still working after equipment reboot.
- Whenever you are required to configure a password, use password Passw0rd if otherwise is not stated.
- All virtual machines are pre-installed. Use admin\Passw0rd credentials to access windows virtual machines and root\ Passw0rd to access linux virtual machines

Equipment, machinery, installations and materials required

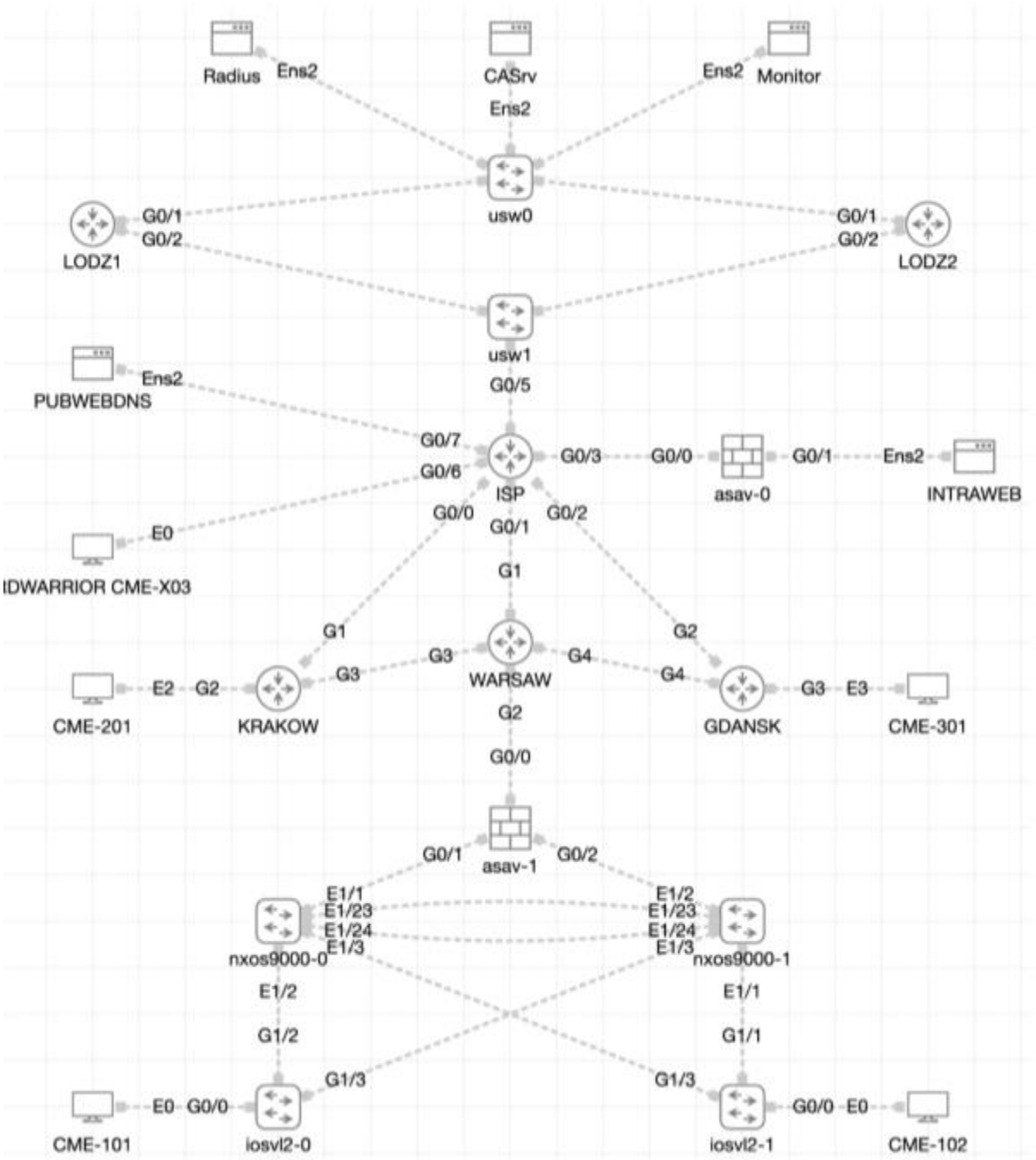
- The ESXi infrastructure has been preconfigured. You should not modify the configuration as it may interfere with the implementation of the project.
- All virtual machines have been created and some software has been installed and configured. You can accept that configuration or change it as you see fit.
- It is possible, although it was not intentional, that you will find something misconfigured, either in the virtual machines, the ESXi infrastructure, or in both. If you do find something misconfigured, it is up to you to correct it.
- All stations are identical and therefore the playing field is equal to everyone.
- The ISP (please see the topology) is already configured and you may not change its configuration.

Test Project objectives

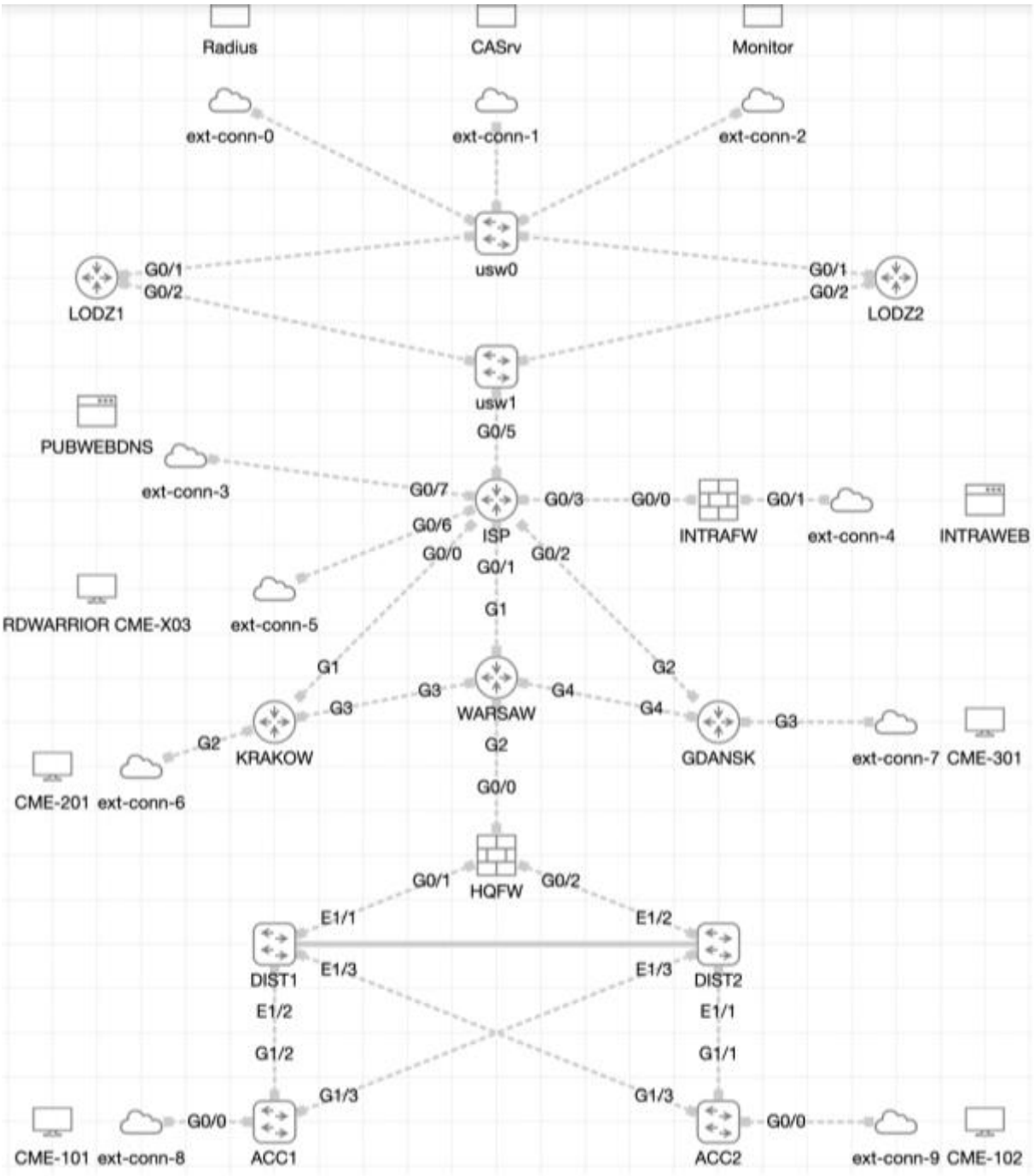
You will implement the project using Cisco CML. A file containing the following topology is located in your desktop (ES2023_TP_39_Module_C_pre_CML.yaml).

We recommend making copies of the original file and making continuous backup copies as you progress through the implementation. You may keep several files, but the file that will be subject to assessment is the one with the original name. Review the topology, the narrative and the desired outcome so that you can plan adequately and create a solution based on the best practices used in the industry.

CML-based-Topology (logic):



CML-based-Topology (with VM-connectors in CML):



Basic Address Concept:

Enterprise Routing Domain

KRAKOW	172.16.10.0/24	INTRAWEB	172.16.30.0/24
GDANSK	172.16.20.0/24	LODZ	172.16.40.0/24
DIST1 <-> HQFW	172.20.1.0/30	DIST2 <-> HQFW	172.20.2.0/30
WARSAW	172.20.3.0/24	HQFW <-> WARSAW	172.20.4.0/30
WARSAW <-> KRAKOW	10.0.10.0/30	WARSAW <-> GDANSK	10.0.20.0/30

Internet Routing Domain

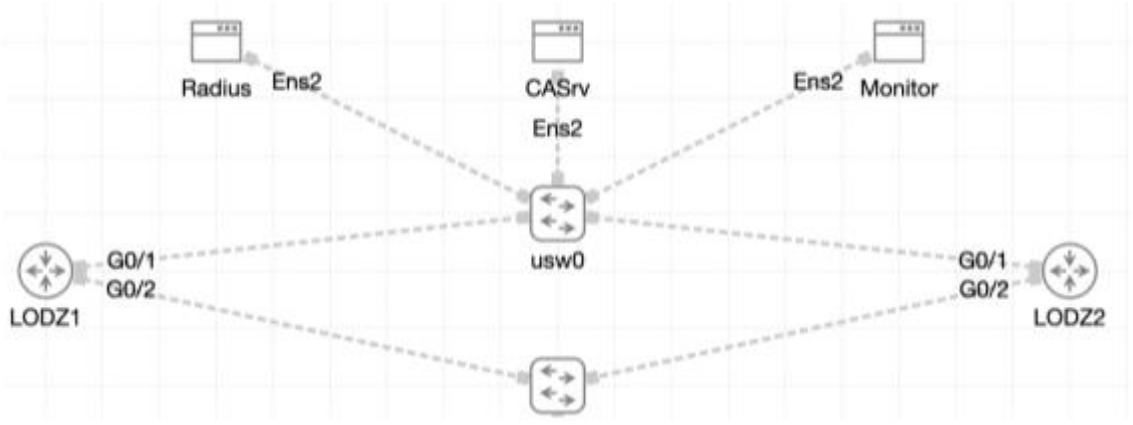
ISP <-> KRAKOW	100.10.9.4/30	ISP <-> GDANSK	94.121.72.0/24
ISP <-> INTRAFW	65.32.147.0/24	ISP <-> LODZ	18.31.192.0/24
ISP <-> WARSAW	132.87.2.0/24	ISP <-> PUBWEBDNS	87.250.250.0/24
ISP <-> Road Warrior	100.71.60.252/30	Loopback0	8.8.8.8/32

Server-infrastructure in LODZ

Lodz is a city in central Poland and a former industrial center. At this location we have 3 services:

- Radius Service
  - Used to authenticate logins via Telnet to LODZ1 and LODZ2. Two users: regular and super. Unlike the user regular, user super automaticity goes into privilege exec mode.
- CASrv-Service
  - Enterprise Certificate Authority
- Monitor Service
  - Hosts a SNMP and TFTP server along with a publicly accessible web site (lodz.pl)

At LODZ we have redundancy both – in the internal and external networks:



PUBWEBDNS

Apache2/Nginx web server (euroskills.pl), BIND9 DNS server for the enterprise

INTRAWEB

Intranet web server (ict.pl)

Road Warrior

Connects to the network via Cisco AnyConnect VPN client. You decide the single, or multi, entry point and configure the DNS server in PUBWEBDNS with the appropriate entries to resolve vpn.ict.pl The possible entry points are Warsaw, Krakow, or Gdansk and depending on which option is chosen the CMS extension will be 103, 203 or 303.

Campus and Branch LAN

1. Configure VLAN distribution feature on DIST1. When adding any new VLAN to DIST1, this VLAN should be automatically distributed to DIST2, ACC1 and ACC2.
2. DIST1 should be the root bridge for all VLANs and DIST2 should take over in case DIST1 fails.
3. Configure link aggregation between DIST1 and DIST2. Use any LAG protocol.
4. During normal network operation DIST1 should act as a next hop for HQ subnet. In case of DIST1 crash or physical links failure, DIST2 should act as the next hop.
5. Implement layer2 security features on the access switches at the Warsaw site.

Campus and Branch LAN

1. euroskills.pl and lodz.pl must be accessible from anywhere, both public and private networks.
2. Implement the necessary security measures on Warsaw site border to expose the minimum services towards the public internet.
3. ict.pl should not be accessible on public internet - only inside enterprise domain.

Enterprise Routing Domain

1. Ensure end-to-end connectivity between all virtual machines inside enterprise routing domain.
2. All traffic between sites must be encrypted with IPsec while traversing via public internet.
3. Links between Warsaw and Krakow and Warsaw and Gdansk must serve as arouting failover to branch networks and internet access in case of public internet is down. Implement a secure layer 2 protocol on this link.
4. Implement secure remote access for the Road Warrior so a secure access to all services running inside enterprise routing domain can be provided Add A record vpn.ict.pl with IP address of VPN termination device to PUBWEBDNS DNS server.
5. LODZ2 should act as stateless failover for all traffic from Lodz towards the internet and enterprise routing domain and vice versa. In case of LODZ1 failure LODZ2 should take over all roles of LODZ1 so all network services will continue normal operation.

Services Integration

1. Synchronize time on all network equipment using NTP (time zone is UTC +2 / Central European Summer Time (CEST). Use ISP as the root NTP server. In case you are configuring hierarchical NTP infrastructure use WARSAW as a corporate NTP server.

2. Client machines in Krakow and Gdansk, as well as IP phones in Warsaw, should receive IP addresses via DHCP service.
3. Add the Warsaw router and the DIST1 switch to the network monitoring platform in lodz.pl via SNMP.
4. For the WARSAW router implement configuration backup to TFTP server located on the Monitor server. A new backup copy should be created each time the configuration is saved on the device.
5. Implement local user root\Passw0rd with privilege level 15 on all network devices (only for VTY lines).
6. For LODZ1 and LODZ2 user super should automatically land in privileged mode. User regular lands in user exec mode. Both users should be created in the TFTP server. Use local authentication in case remote authentication server is not available.

Unified Communications Infrastructure

1. Configure Call Manager Express on Warsaw (1xx), Krakow (2xx) and Gdansk (3xx).
2. Configure Local Directory Services so that users can lookup other users' extension number via the Directory catalog.
3. Configure conferencing services to support at least three parties in a conference call.
4. Configure Call Park on extension 199 to allow any user to park a call so that any other user can pick it up upon dialing the call park extension.
5. When CME-101 or CME-102 are on park, they should hear music. Use MOH.au file located on Warsaw router flash.
6. Configure Call Park on extension 999 to allow any user to park the call so that any user can pick up the call upon dialing the call park extension.
7. While remotely connected to the enterprise routing domain, Road Warrior must be able to register softphone on VPN endpoint and communicate with all sites normally.