worldskills
Europe

EuroSkills Test Project

Industry 4.0 + HP2

Task D

ES2021_TP_Industry_4.0_HP2

Contents

List of Documents

No.	Document	Description
1	SIEMENS_BA_SCALANCE-S610_76.pdf	Industrial Ethernet Security SCALANCE S615, Operating Instructions
2	SIEMENS_PH_SCALANCE-S615-WBM_76.pdf	Industrial Ethernet Security SCALANCE S615, Web Based Management
3	SIEMENS_BA_SCALANCE-XC-200_76.pdf	Industrial Ethernet switches SCALANCE XC-200 Operating Instructions
4	SIEMENS_PH_SCALANCE-XB-200-XC-200-XF-200BA-XP-200-XR-300WG-WBM_76.pdf	Industrial Ethernet switches SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG Web Based Management Configuration Manual

Introduction

You as a specialist for IT security are now asked to separate the existing network by applying VLAN techniques and configuring a firewall to prepare the system for secure remote access.

Description of project and tasks

VLAN and Firewall Controlled Access

A customer running a production system has requested an extension of the network by an additional subnet for energy measurement devices (ENERGY) and an additional management subnet (MAINT) for limited maintenance access to web servers in production and energy network. In addition to the existing infrastructure two new subnets must be created and integrated into the network devices using an appropriate VLAN configuration. In a second step the access between the networks shall be controlled by specific firewall rules. Finally, the management of the network devices must be limited to the maintenance network.

In the new network structure, the energy measurement box will be placed in the ENERGY network segment.

NetLab IT system with router S615 (“rt-netlab”, left) and switch XC208 (“sw-netlab”, right)

Your task will be completed when:

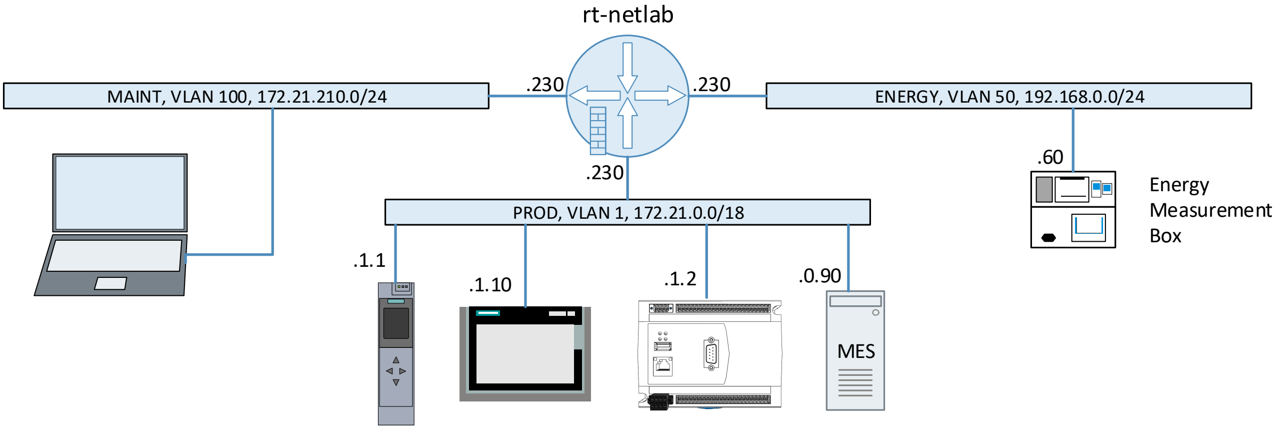
1. Three VLANs have been setup on the NetLab network devices, one for the energy measurement system, one for network management, and one for the production network, in accordance with Specification 1.
   The OPC server of the energy measurement box must be reachable from the MES PC.
   All network devices get their time information from the MES PC.
2. All firewall protection is set up as requested in Specification 2. You have documented the effectiveness of the firewall ruleset by providing port scans according to Specification 2 after the activation of specific firewall rules.
3. All management interfaces of network devices are only visible in the maintenance network.

Subtask 1

VLAN configuration

In the first step all network devices shall be reset to their factory defaults and a VLAN separated network structure shall be implemented.

The new network segments are shown in the figure below.


rt-netlab
.230
.230
.230
MAINT, VLAN 100, 172.21.210.0/24
ENERGY, VLAN 50, 192.168.0.0/24
PROD, VLAN 1, 172.21.0.0/18
.60
Energy Measurement Box
.1.1
.1.10
.1.2
.0.90
MES

Network plan showing the target layer 3 architecture

You have to configure router and switch to meet the requirements given in the specification below. All network components shall receive their time from the MES PC providing a time server using the NTP protocol to guarantee consistent logging.

Set up this infrastructure and validate the functions by accessing the services and by port scans.

Document your port scans with screenshots.

.

Specification 1: VLAN Configuration

No.	Item description	Value
	Subnetworks' address ranges	
1.10	Production (PROD)	172.21.0.0/18
1.11	Energy measurement (ENERGY)	192.168.0.0/24
1.12	Maintenance (MAINT)	172.21.210.0/24
1.13	External Network (EXT), not needed during commissioning	DHCP
	Basic configuration of the router "rt-netlab"	
1.20	IP address in PROD	172.21.0.230/18
1.21	IP address in MAINT	172.21.210.230/24
1.22	IP address in ENERGY	192.168.0.230/24
1.23	Username	admin
1.24	Password	SkillsI4.0
1.25	Receive time from NTP time server	172.21.0.90
	Basic configuration of the switch "sw-netlab"	
1.30	IP address (during subtask 1)	172.21.0.240/18
1.31	Username	admin
1.32	Password	SkillsI4.0
1.33	Receive time from NTP time server	172.21.0.90
	Configuration of the switch "sw-cp-lab"	
1.40	IP address (during subtask 1)	172.21.0.241/18
1.41	Username	admin

1.42	Password	SkillsI4.0
1.43	Receive time from NTP time server	172.21.0.90
	Configuration of the PLC of the Energy Measurement Box	
1.50	IP address	192.168.0.60/24
1.51	Gateway	192.168.0.230
	Network Setup	
1.60	Physical network connections according to the network plan (see below)	

No.	Item description	Value
	MES PC	
1.70	IP address	172.21.0.90/18
1.71	Gateway	172.21.0.230
	VLAN ID 1	
1.80	Name	PROD
1.81	Ports on rt-netlab	1 (in untagged mode) 4 (member of trunk)
1.82	Ports on sw-netlab	1,2,6,8 (in untagged mode) 5 (member of trunk)
1.83	Subnet IP address rt-netlab	172.21.0.230/18
	VLAN ID 50	
1.90	Name	ENERGY
1.91	Port on rt-netlab	2 (in untagged mode) 4 (member of trunk)
1.92	Ports on sw-netlab	3 (in untagged mode) 5 (member of trunk)

1.93	Subnet IP address rt-netlab	192.168.0.230/24
	VLAN ID 100	
1.100	Name	MAINT
1.101	Port on rt-netlab	3 (in untagged mode) 4 (member of trunk)
1.102	Ports on sw-netlab	7 (in untagged mode) 5 (member of trunk)
1.103	Subnet IP address rt-netlab	172.21.210.230/24
	Trunk Ports	
1.110	Port on rt-netlab	4
1.111	Port on sw-netlab	5
	Firewall rules	
1.120	All traffic from MAINT to PROD	Allowed
1.121	All traffic from MAINT to ENERGY	Allowed
1.122	All traffic from PROD to ENERGY	Allowed
	Documentation	
1.130	Screenshot of Proneta scan (graphics and name/IP table) after configuration	
1.131	Screenshot of NTP client setup page of router and switches after successful time synchronization	
1.132	Screenshots of all VLAN configurations (“General” and “Port Based VLAN” tab) of router and switch.	
1.133	Screenshot of the router’s “Layer 3 ǀ Subnets ǀ Overview” tab after configuration	
1.134	Screenshot of the router’s “Security ǀ Firewall ǀ IP Rules” tab after configuration	

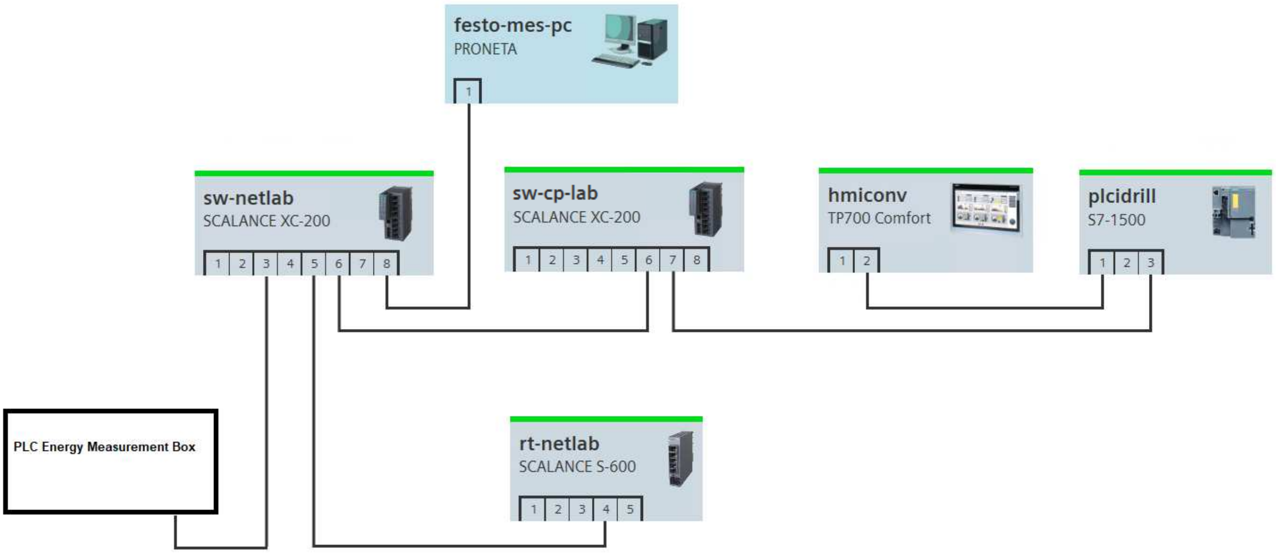


Figure: Network plan with physical connections and port numbers

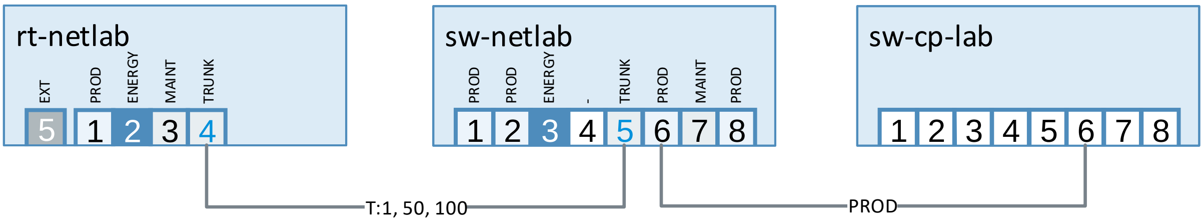


Figure: VLAN to port assignments

Subtask 2

Between the three networks the firewall shall be configured with more specific rules. The firewall rule set shall guarantee that only authorized access to the energy and production networks is possible from the maintenance network and access between production and energy network is also limited.

Set up these rules and validate them by access trials for allowed and rejected traffic. Validate the firewall setting by port scans as defined in Specification 2.

Specification 2: Firewall Rules

The following table gives the requirements for the access that shall be allowed between different networks.

As an external connection is not part of this commissioning of additional internal networks no rules for the external network will be given. Thus, no access shall be possible to or from the external network.

No.	Item description	Value
	Firewall access requirements	
2.10	All HTTPS access from the maintenance network to the production network shall be allowed.	
2.11	All access attempts from the maintenance network to the Siemens PLC via HTTP shall be rejected and logged on info level by the firewall. No other access types shall be logged.	
2.12	From the maintenance network every target in the production network shall be reachable by PING.	
2.13	From the maintenance network **only** the energy measurement box shall be reachable by HTTP protocol.	
2.14	From the maintenance network every target in the energy network shall be reachable by PING.	
2.15	From the production network **only** the MES PC may reach any target in the energy network using OPC UA.	
2.16	All systems in the maintenance network may send NTP messages to the production network **only** to the MES PC.	
	Protocol specific ports	
2.20	HTTP	80/TCP
2.21	HTTP on CECC	8080/TCP

2.22	HTTPS	443/TCP
2.23	OPC UA	4840/TCP
2.24	NTP	123/UDP
	ICMP services	
2.30	Echo Request (ping)	Type 8
	Documentation	
2.41	Result of nmap scan to show visibility of PROD automation devices from MAINT	nmap.exe -sS 172.21.1.1 172.21.1.2 172.21.1.10
2.42	Result of nmap scan to show visibility of ENERGY measurement device from MAINT	nmap.exe -sS 192.168.0.60
2.43	Screenshot of “Security I Firewall I IP Services” tab	
2.44	Screenshot of “Security I Firewall I ICMP Services” tab	
2.45	Screenshot of “Security I Firewall I IP Rules” tab	
2.46	Screenshot of rejected traffic on “Information I Log Tables I Firewall Log”	

Subtask 3

Management Interfaces

To make network administration easier and to keep management interfaces (http/https) of network and production systems separated, all http/https management interfaces of router and switches shall only be visible in the maintenance network.

There shall be no visibility of management interfaces from the production or energy network.

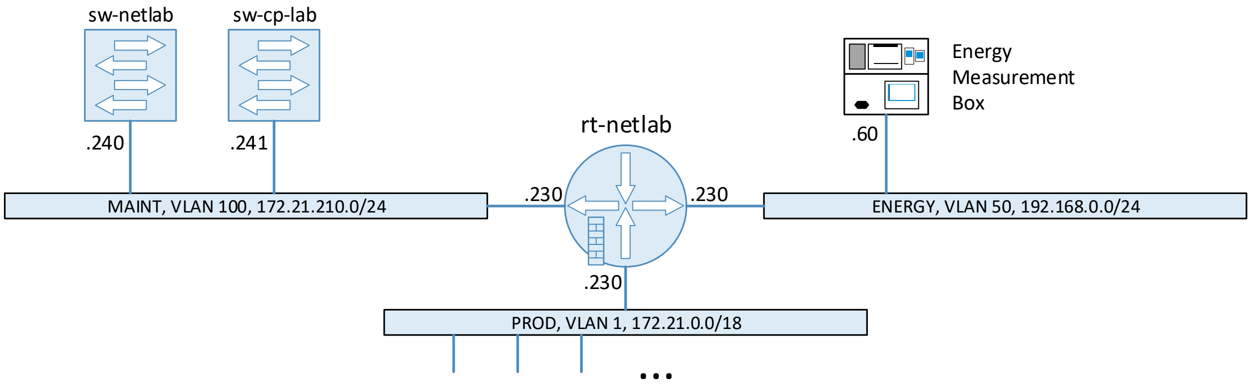

sw-netlab
sw-cp-lab
Energy Measurement Box
.240
.241
rt-netlab
.60
.230
.230
MAINT, VLAN 100, 172.21.210.0/24
ENERGY, VLAN 50, 192.168.0.0/24
.230
PROD, VLAN 1, 172.21.0.0/18
...

Figure: Network devices’ management interfaces are visible on maintenance network

This new configuration shall achieve the following

1. All network devices (router and switches) can be located by PRONETA in the maintenance network segment.
2. All network devices (router and switches) can be managed from the maintenance network segment via their web-based interfaces.
3. All network devices can update their internal clocks using NTP towards the MES PC.

For managing the access possibilities to management interfaces on the router use the “Predefined” rule set.

Notice: For the evaluation of Subtask 3 after the competition, prepare one notebook to be part of the maintenance network by setting IP address, mask, and gateway.

Instructions to the Competitor

The task and related documents will be provided on a USB stick. In the end of the task the created documentation must be provided in this USB stick back to the jury.

During the competition use of personal computers are allowed, however the final solution must be implemented on the provided MES Server PC. It is allowed to connect monitor(s), a keyboard, and mouse to the PC or to access it via Remote Desktop Connection (see *MES Server PC Documentation*, in the folder “Documents”).

During the marking, only solutions running on the competition system are evaluated, unless requested differently.

Equipment, machinery, installations, and materials required

ITEM	QUANTITY	MATERIAL	DESCRIPTION	NOTES

Marking Scheme

TASK	SUBTASK	BY JUDGEMENT	BY MEASUREMENT	TOTAL
D	VLAN Configuration	1	5	6
	Firewall Rules	1	8	9
	Management Interfaces	0	3	3
TOTAL		2	16	18