NATIONAL FINAL
ENTERPRISE ICT TEAM

(4. EUROSKILLS 2014 IN LILLE, FRANCE)

ENTERPRISE ICT
TEAM 2013

DAY 1

SZU Wien 3, Ungargasse 69

21. – 23.11.2013

General Information

Your team is part of the installation and operational department of a Lille (France) based company, which provides complete IT solutions to its customers. Your team has recently been charged with supporting the IT system of two companies in TGM and SZU. Your team's tasks are to build the two companies' infrastructure and to configure their network and software services.

HARDWARE

The following equipment is required to deal with the challenges of this day. Additional components in the rack may be used, anyhow it is advised to configure only active network components and PC's described in this paper.

Quantum	Component
1	2911 Router
2	2960 Switches
2	Servers
2	PC's

Table: hardware list

The available hardware for your project has been used on another site of your company. Therefore it might be possible that some devices have been used in an environment and still have active configurations. Normally the password "**lille**" was used on these components.

Keep in mind that such devices may need initial configuration steps before doing the main set-up.

SOFTWARE

The following software products are available:

Software Package
Windows Server 2012
Windows Client 8.1
Debian 7.1.0
Debian 6.0.7
Vmware ESXi 5.1
Vmware Vsphere Client 5.1
Putty, TerraTerm (Telnet Client)
NetMon, WireShark (Network Analyzer)

Table: software on the data media

CABLING & MORE

Your team will have a data medium on your workplace, where the required software (see list above) is stored.

You also have several cables of the following types:

Cable Color	Cable Type
Blue	Straight cable (RJ45)
Red	Straight cable (RJ45)
Yellow	Crossover cable (RJ45)
Light Blue	Console cable (RJ45-DB9)
Blue	Serial cable (V35-SSC)

Table: cable types

Before you begin

Please read the full instructions carefully and study the network details (topology diagram and address tables etc.).

Try to assign an appropriate workflow to the team members and think of an efficient time management.

Hints

The implementation of the whole network structure has to be done by using the ports (Fa0/1, Gi0/2 etc.) as listed in the information tables.

Keep in mind to verify your configuration and check all your configuration steps. Also save your work regularly.

If technical assistance is needed, write your question on the designated form, which can be found at the end of this document. After receiving your help request, the jury will give an answer, if possible.

Overview of the competition tasks

Day 1

You will have to do all working tasks specified in this document.

In this paper, all working tasks are divided into the three scopes 'Network', 'Microsoft Windows' and 'Linux'. The distribution of singular working tasks to team members can be

done individually as the competition ranking is based on the total score of the complete team.

Day 2

In the morning of day 2, you will receive an additional document containing the missions for this day. Continuing the work of day 1, the network implementation and services have to be completed.

Day 3

In the morning of day 3, you will get new jobs to do. Based on the finalized network structure, additional planning and optimization and other tasks may have to be done.

Before you finish your work

Keep in mind that all your work has to be finished before 18:00, so save all your configuration early enough.

All written notes and used papers must be left on the workplace in the appropriate folder.

Note: the jury will rate your work during the night, so please keep all your devices running - anyhow, ensure that all configuration and required services are available, even if a reboot will happen.

All working tasks should be done precisely to implement all claimed network functionalities and services.

General Network Information

The following diagram shows the target topology for one location of our company, which is connected to an ISP by the router RT1.

The ISP allows restricted access to the internet, so each team is allowed to establish a link with Microsoft.com for using the license services.

You need to use a network 10.9.x.0/24 for all outgoing network traffic, 'x' specifying the team number (as seen on your rack).

The internet connection will be established by using a 100BaseT link, connected to the specified network outlet.

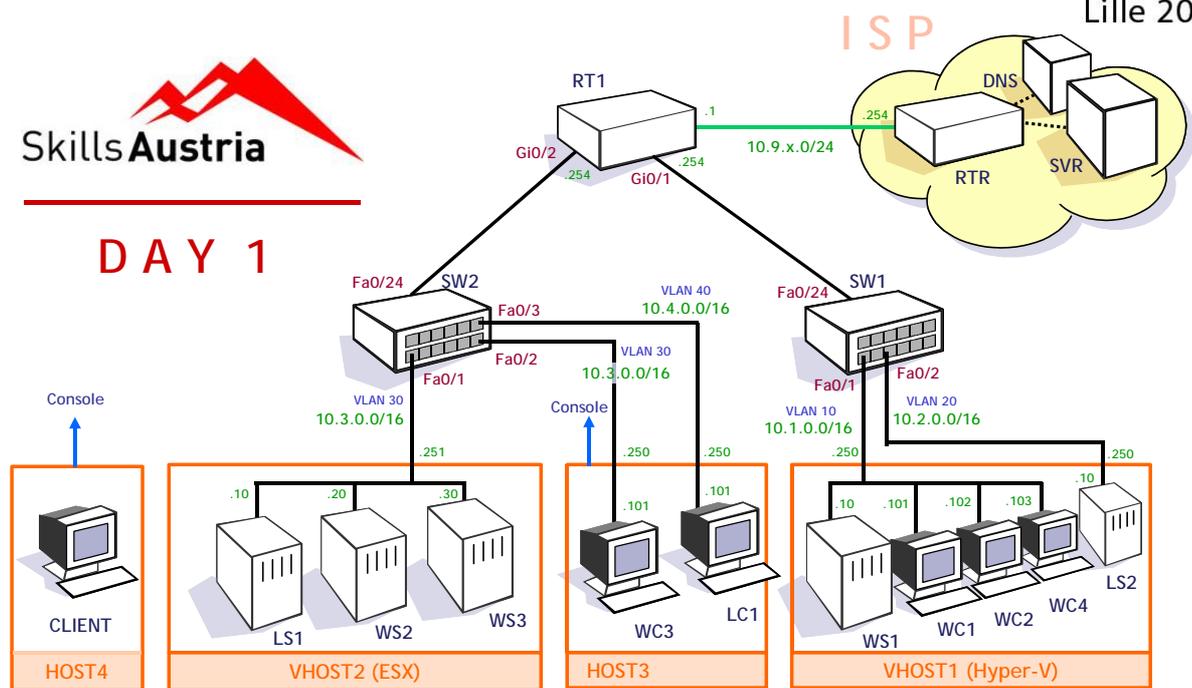| Team	IP Network	Gateway & DNS	Network Connector	Backup Connector
1	19.9.1.0/24	10.9.1.254	C06	C07
2	19.9.2.0/24	10.9.2.254	D09	D10
3	19.9.3.0/24	10.9.3.254	A06	A07
4	19.9.4.0/24	10.9.4.254	B08	B09
5	19.9.5.0/24	10.9.5.254	C13	C14

Table: Internet access

If trouble shooting has to be done, ICMP and DNS protocols are also forwarded by the ISP router.

The network uses multiple VLAN's, which have to be serviced by two switches SW1 and SW2.

The network infrastructure consists of two hardware based servers and two hardware based clients. The following graph displays the hardware components as a box with an orange frame. The PC symbols within the boxes represent virtual machines - details can be seen in the following sections.

Each PC has two network interface cards, indicated by black lines crossing the frame border.

When doing configuration tasks by using console cables, it is recommended to connect them to the serial ports of Host3 and Host4.

Network topology (you will find an enlarged image in the appendix)

Addressing

According to the following tasks, all existing hardware and all virtual servers obtain static IP addresses. Be sure to use these addresses (listed in the topology view) to guarantee the complete functionality of the network.

It is recommended to verify the needed dynamic configuration of IP addresses on all user machines (WC1, WC4, and LC1) using appropriate DHCP services. These services can be implemented either on the existing active network components or on the available Linux or Windows server systems.

Naming and Passwords

Host names have to be defined as seen in the topology diagram and/or information found in the appendix.

Example: VHOST1, WS1 etc. for PC's and SW1, RT1 for networking components.

As most of the devices have to be configured by setting usernames and passwords, the following default password should be used, if no other password is specified in the detailed instructions.

Default password: "Skills_2013!"

NETWORKING

The main task for the networking scope is to establish a connection between the company PC's and also allowing access to the internet.

General Tasks

In order to manage this job, you need to do the following sub tasks:

- § Study the network infrastructure carefully
- § Network Topology & Cabling
- § Security Configuration
- § Management Configuration

Network Topology & Cabling

Add reasonable information to the topology diagram and put labels on the components, if needed.

It is recommended to use the same hardware assignment and numbering scheme of ports as described in the appendix.

Build up the network topology by using the available LAN cables. The LAN cables are available in different colours and lengths. It is strongly recommended to use red cables for the links between routers and switches, blue cables to connect end devices and yellow cables (cross-over) for uplinks.

The internet connection can be realised by using the blue patch cable with an "Internet" tag which is available on your working desk.

Information for addressing and other network parameters can be found in the attached network diagram and appendix.

Connect the LAN and WAN cables and configure IP addresses as specified in the network diagram and appendix.

Servers and end-user machines need to be logically separated. For this purpose, create VLANs as specified in the appendix.

For both locations the gateway of the created VLANs should be the last available address in the given range.

Security Configuration

Create a basic configuration for all active components, which consists of hostname and the domain "null.nil". To secure the active components, define passwords for console and telnet access by using the default password.

Enable Telnet access to the router from the sites. The username for Telnet is "admin" and the password is "Skills_2013!".

For the used router and switches, set the login message to warn from unauthorized use.

The router RT1 has to be configured to allow SSH access for the user "skills" with 1024 bit key, use the default password.

Configure the interfaces on all active components and create VLAN's to interconnect all logically separated network devices. Use all specifications as seen in the appendix.

On all network devices set the console and enable secret password.

All passwords on all devices should be "Skills_2013!".

On all routers and switches use the appropriate domain-name.

Management Configuration

For administrative use, all active components must be accessible from all hosts. This should allow you to do testing procedures easily and provide an efficient workflow.

To reduce management traffic, unneeded services on the routers and switches should be deactivated.

Configure all access ports of the switches by enabling options for **portfast** and **BPDU guard** to provide higher network security.

Unused ports according to the list should be disabled and assigned to an unused VLAN.

Configure the switches and routers to support end-to-end connectivity between all devices and do all needed configuration to allow access to the Microsoft license server (e.g. activation.sls.microsoft.com).

Therefore a link to the ISP router has to be established and configured. The ISP has a default gateway of 10.9.x.254 and a DNS server with the same IP address. The 'x' represents the team number.

Information & Hints

Your team will also have two console cables for configuring the network devices.

WINDOWS

General Information

Language /Keyboard

You can configure German or German 101 keyboard, but you must use the english language.

Hint: be careful with your keyboard language, setting passwords etc.

Computer Names

All computers with the beginning letter **W** are Windows machines. All computers with the beginning letter **L** are Linux machines. The second character signs the way the computer is used: **S** means server and **C** means clients. A postfix with a number completes the full computer name.

Name	Type	System
WSx	Server	Windows Server 2012 R2
LS1	Server	Debian Linux 6.0.7
LS2	Server	Debian Linux 7.1.0
WCx	Client	Windows 8.1
LCx	Client	Debian Linux 7.1.0
VHOSTx	Virtual Host	Used as virtualization parent with an operating system for virtualization
HOSTx	Host	can be used as well as Client system and as parent for virtualization

Table: computer names and types

OS information

All computers in the table above should have a basic OS and IP address. The only exceptions are WC2 and WC4 which don't need an operating system.

Basic Information for Server & Client

VHost1:

Computer name:	VHost1
Operating System:	Windows Server 2012 R2
Virtualization:	HyperV

Administrator name:	Administrator
Administrator password:	Skills_2013!
Virtualized Computers	WS1, WC1, WC2, WC4, LS2

Hint: this machine uses two network interfaces for connecting to the network.

There is one exception to the rules above: on WC2 and WC4 no operating system has to be configured.

VHost2:

Computer name:	VHost2
Operating System:	ESX 5.1
Virtualization:	ESX
Administrator name:	root
Administrator password:	Skills_2013!
Virtualized Computers inside	LS1, WS2, WS3

Hint: this machine uses only one network interfaces for connecting to the network.

Host3:

Computer name:	Host3
Operating System:	Windows 8.1
Virtualization:	HyperV
Administrator name:	MainUser
Administrator password:	Skills_2013!
Virtualized Computers inside	LC1, WC3

Hint: this machine uses two network interfaces for connecting to the network.

This machine should be used as a managing workstation (Vmware Vsphere client) for the ESX server.

Host4:

Computer name:	Host4
Operating System:	Windows 8.1
Virtualization:	None
Administrator name:	MainUser
Administrator password:	Skills_2013!
Virtualized Computers inside	none
General information for virtualization	

All virtualization host machines use virtual switches to connect their clients to the network.

All virtualization host machines should use intelligent configuration parameters to use the hardware resources as efficiently as possible (example: use dynamic RAM etc.).

All virtualized server/client machines must start automatically on the virtualization host.

IP addressing scheme

You get the IP addressing information for all machines from the network diagram mentioned above.

All clients IP addresses are served by DHCP, the address range is xxx.xxx.xxx.101-125 for all networks.

Hard Disk Configuration Information

Basic hard disk configuration

All computers should have a basic OS – installed on their first physical hard disk – as described before. The size of the hard disk should be chosen with reasonable care and have enough space for later higher demands.

Additional hard disk assignments

On the computers WS1 and WS2 the following hard disk assignments should be configured in addition to basic tasks.

WS1:

Configure a software-based RAID 5 fault tolerant hard disk system as device with drive letter D.

WS2:

Configure a software-based mirrored fault tolerant hard disk system as device with drive letter D.

Remote server and client management

Each window server and client must be configured in that way that remote management of the following is possible:

   §   desktop (remote desktop)

   §   computer (remote computer management)

   §   hard disks (remote hard disk management)

The firewall must be active on each device because of security risks.

Connectivity Test

The connectivity of all computers must be tested with a simple ping to the IP address, no internal name server has been implemented yet.

Windows Activation

The windows license activation (servers/clients) can be done via your ISP router, as specified in the network part.

Use your ISP address gateway (10.9.x.254) as DNS server for activation.

All machines with a windows operating system should be activated at the end of the first day.

Installation Media

You get the following DVD sets for installation:

- § Server 2012R2
- § Windows 8.1
- § ESXi 5.1
- § Debian 7.1.0
- § Debian 6.0.7

All drivers and other tools for installation and configuration are put on the second physical hard disk of VHOST 1.

Hint: essential drivers for the machines are marked with "**$-**" at the beginning.

All DVD ISO's are also stored on this hard disk.

You can find additional documentation in the directory "documentation".

Hint: the OS ISO's for installation should be put on a shared device.

Second hard disk

During this day you will install and configure the VHOST2 by using ESXi. Use the available installation media. Set the IP address and the default gateway using the settings specified in the appendix.

A management client is needed for administration of the ESXi server. The HOST3 PC runs Windows 8.1 with the basic network configuration as specified in the appendix.

Do the IP configuration for the HOST3 by using the addressing scheme in the appendix. Both network interface cards will be used to connect different VLAN's and will each support the virtual machines (WC3 and LC1) installed using Hyper-V. The specified software can be found on the available media.

The virtual client WC3 is a Windows 8.1 based system. The virtual client LC1 is a Linux based system with Debian 7.1.0, when installing the OS, the DVD #1 will be needed.

During the installation process you will have to configure user accounts by defining the users "**root**" and "**skills**" by applying the default password "Skills_2013!".

Activate the Netfx3 feature for windows to allow the installation of Vmware Vsphere client by starting the following command line instruction:

```
Dism /online /enable-feature /featurename:NetFx3 /All /Source:D:\sources\sxs /LimitAccess
```

After executing the instruction above, install the Vsphere client software from the data medium.

Using the Vsphere client, install one linux server (LS1) and two windows server (WS2 and WS3) on the VHOST2. Linux Debian 6.0.7 will be used for the virtual server LS1. You may want to copy the DVD images to the **datastore** from ESXi to speed up the installation process.

In addition to the default settings, the values for RAM equal 2048 MB and hard disk space equal 20 GB should be adapted.

Windows installation information can be found in the Microsoft documentation part.

Define a testing procedure to do efficient connectivity checks for all end devices.

TESTING PROCEDURES

The main goal of day 1 is to set up all machines and guarantee full functionality for end-to-end communication and services. Use the matrix of the appendix to create a check list, which consists of tested services and end-to-end communication for all configured devices. Successful and failed testing results should be indicated by appropriate symbols.
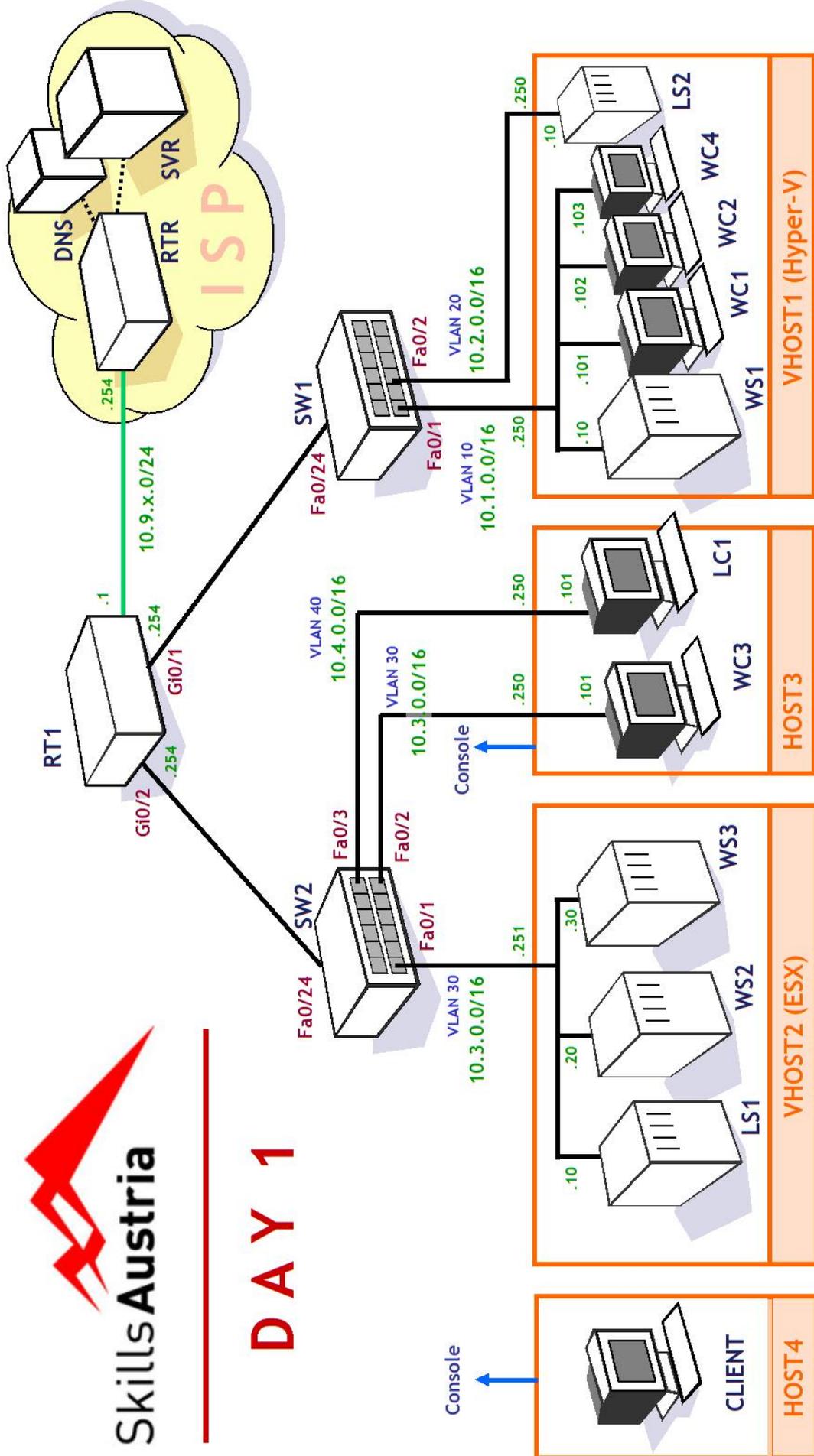
Device Information

Router 0

Device	Interface	IP Address	Connected to...
RT0 (Router 0)	Fa0/0	100.10.1.1/29	¨ RT1
	Fa0/1	100.20.1.1/29	¨ RT2
	Fa0/2	200.100.10.254/24	¨ RT3
	Fa0/11	100.50.1.1/24	¨ HOST4
	Fa0/12	200.100.10.254/24	¨ PHONE2
	Lo0	200.200.200.200/24	-

Table Information

Router 1

Device	Interface	IP Address	Connected to...
RT1 (Router 1)	Gi0/0	100.10.1.2/29	¨ RT0
	Gi0/2	10.x.0.254/16	¨ SW2
	Se0/0	192.168.1.1/30	¨ RT2

Table Information

Router 2

Device	Interface	IP Address	Connected to...
RT2 (Router 2)	Gi0/1	100.20.1.2/29	¨ RT0
	Gi0/2	10.x.0.254/16	¨ SW1
	Se0/0	192.168.1.2/30	¨ RT1

Table Information

Router 3

Device	Interface	IP Address	Connected to...
RT3 (Router 3)	Gi0/2	200.100.10.254/24	¨ RT0

Table Information

Emergency Phone

Device	Interface	IP Address	Connected to...

PHONE2 (Emergency)	Int1	200.100.10.*/24	¨ RT0

Table Information

SW1 (Switch 1)

Device	Interface	IP Address	Connected to…
SW1 (Switch 1)	Fa0/0	VLAN 10	¨ VHOST1 (Int1)
	Fa0/1	VLAN 20	¨ VHOST1 (Int2)
	Fa0/12	VLAN 100	¨ PHONE1
	Fa0/24	?	¨ RT2

Table Information

Test Matrix

Device				
RT1				
SW1				
SW2				
LS1				
WS2				
WS3				
WC3				
LC1				
WS1				
WC1				
WC2				
WC3				
LS2				

Table: check matrix 1

Device				
RT1				
SW1				
SW2				
LS1				
WS2				
WS3				
WC3				
LC1				
WS1				
WC1				
WC2				
WC3				
LS2				

Table: check matrix 2

NATIONAL FINAL
ENTERPRISE ICT TEAM

(4. EUROSKILLS 2014 IN LILLE, FRANCE)

ENTERPRISE ICT
TEAM 2013

DAY 2

SZU Wien 3, Ungargasse 69

21. – 23.11.2013

General Information

Your team is the installation and operational team of a Lille (France) based company, which provides complete IT solutions to its customers. Your team was recently charged with supporting the IT system of two companies in TGM and SZU. Your team's tasks are to build the two companies' infrastructure, and to configure their network and software services.

HARDWARE

The following equipment is required to deal with the challenges of this day. Additional components in the rack may be used, anyhow it is advised to configure only active network components and PC's described in this paper.

Quantum	Component
3	2911 Router
2	3560 Switches
2	2960 Switches
2	IP-Phones 69XX/79XX
2	Servers
2	PC's

Table: hardware list

SOFTWARE

The following software products are available:

Software Package
Windows Server 2012
Windows Client 8.1
Debian 7.1.0
Debian 6.0.7
Vmware ESXi 5.1
Vmware Vsphere Client 5.1
IP Communicator
Virtual Audio Driver
VPN Client
Putty, TerraTerm (Telnet Client)
NetMon, WireShark (Network Analyzer)
MIBs (???)

Table: software on the data media

CABLING & MORE

Your team will have a data media on your working place, where the required software (see list above) has been stored.

You also have several cables of the following types:

Cable Color	Cable Type
Blue	Straight cable (RJ45)
Red	Straight cable (RJ45)
Yellow	Crossover cable (RJ45)
Light Blue	Console cable (RJ45-DB9)
Blue	Serial cable (V35-SSC)

Table: cable types

Before you begin

Please read the full instructions carefully and study the network details (topology graph and address tables etc.).

Try to assign an appropriate workflow to the team members and think to do a minimal time management.

Hints

The implementation of the whole network structure has to be done by using the ports (Fa0/1, Gi0/2 etc.) as listed in the information tables.

Keep in mind to verify your configuration and check all your configuration steps. Also save your work regularly.

If technical assistance is needed, write your question on the designated form, which can be found at the end of this document. After receiving your help request, the jury will reply an answer, if possible.

Overview of the competition tasks

Day 2

Today you will need to complete additional missions, which continue the work from yesterday. To fully realize all network implementation and services tasks, you may have to complete unfinished configuration jobs from yesterday.

Day 3

In the morning of day 3, you will receive new jobs to do. Based on the finalized network structure, additional planning and optimization and other tasks may have to be done.

Before you finish your work

Keep in mind that all your work has to be finished before 17:15, so save all your configuration early enough.

All written notes and used papers must be left on the workplace, in the appropriate folder.

Note: the jury will rate your work during the night, so please keep all your devices running - anyhow, ensure that all configurations and required services will be available, even if a reboot will happen.

All working tasks should be done exactly to implement all claimed network functionalities and services.

A short documentation should be done which contains information about the realized configuration and functionality of all services. You may need to do some additional tasks on day 3 which have to be managed by using all given instruction papers and your personal written documentation.

General Network Information

The following diagram shows the extended topology of our company, which contains additional hardware to create a network for further company locations (e.g. HQ).
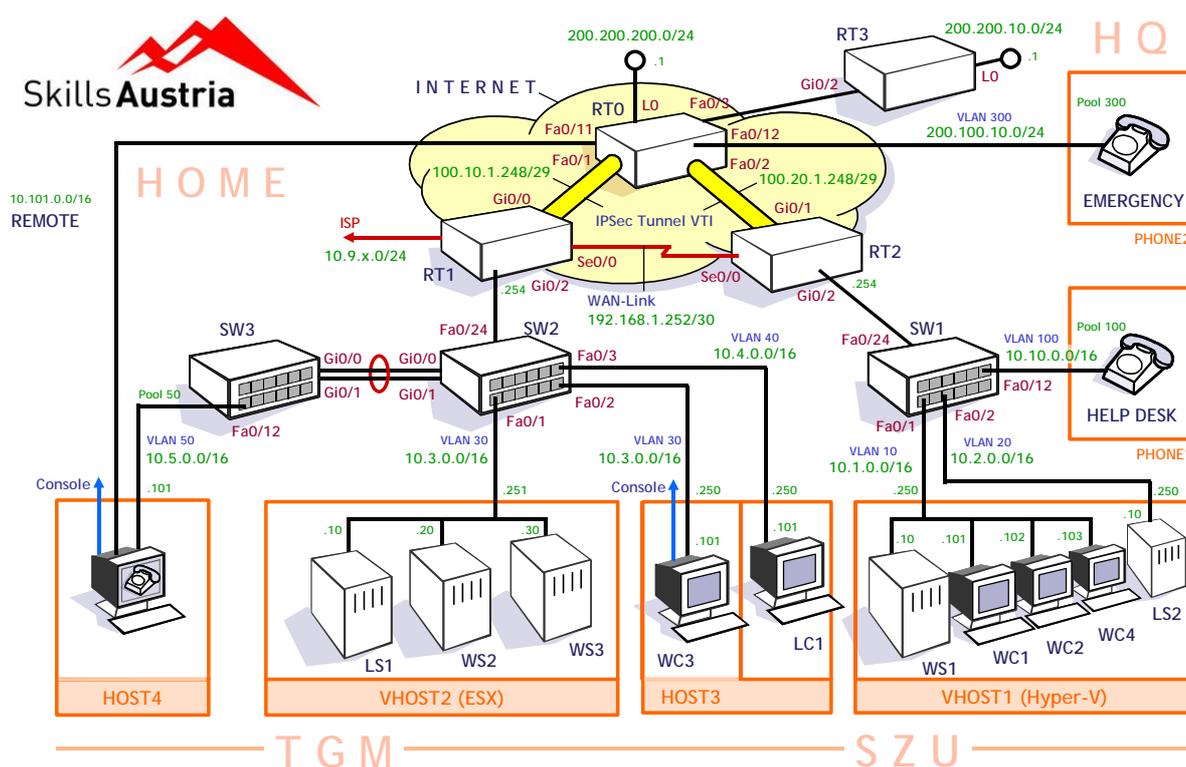
** ISP nach Erfordernissen **

The network uses multiple VLAN's, which have to be serviced by two switches SW1 and SW2.

The network infrastructure consists of two hardware-based servers and two hardware-based clients. The following graph displays the hardware components as a box with an orange frame. The PC symbols within the boxes represent virtual machines - details can be seen in the following sections.

Each PC has two network interface cards, indicated by black lines crossing the frame border.

When doing configuration tasks by using console cables, it is recommended to connect them to the serial ports of Host3 and Host4.

Network topology (you will find an enlarged image in the appendix)

Addressing

According to the following tasks, all existing hardware and all virtual machines obtain IP addresses using a static or a dynamically method. Be sure to use the dedicated addresses (listed in the topology view and in the appendix) to guarantee the complete functionality of the network.

Like in day 1, hostnames have to be defined as seen in the topology graph and the tabled in the appendix.

Example: VHOST1, WS1 etc. for PC's and SW1, RT1 for networking components.

As most of the devices have to be configured by setting usernames and passwords, the following default password should be used, if no other password is specified in the detailed instructions.

Default password: "Skills_2013!"

NETWORKING

The first job is to build a corporate network for the companies TGM and SZU, which provide basic functionalities.

The switches and routers should support the OSI layers 2 and 3 specifications described in graphic diagram.

Locations

The **SZU** domain consists of the servers WS1, WS2 and WS3, WC1 to WC4.

The **TGM** domain consists of the servers LS1 and LS2 and the client LC1.

The client WC5 will be temporarily used for two locations for testing purposes and remote access from **home**, for this competition all services have to be implemented on the same PC.

The locations **HQ** and **Help Desk** actually need only IP telephony services, so there is no actual demand for further network functionality.

The listed locations and their devices will need to be connected by using the active components as seen in the network topology.

Rebuild the physical infrastructure according to the topology design and appendix.

Routing

Router RT1 & RT2 Configuration

Both locations are connected with a leased line. On this line configure the PPP protocol with CHAP authentication. Use this line for the data traffic between the locations.

NOTE: on RT1 for the CHAP authentication you must use local user database AAA authentication for PPP.

A backup connection between the TGM office and the SZU office through the internet has to be provided. This has to be solved with a permanent site-to-site VTI VPN.

Use pre-shared key authentication with key "Skills_2013!".

This VPN connection should be used only when the leased line connection between the two routers fails.

You have to configure an EIGRP autonomous system 100 for routing. Configure EIGRP with authentication by using the key string "Skills_2013!" between TGM and SZU to allow communication.

Permit routing traffic only on the necessary interfaces.

Configure the default route for the internet.

Since both offices have a gateway to the internet, the possibility for two default gateways in the network exists. If one of the office's internet connections fails, then use the other office's ISP connection.

Configure SSH on both routers.

Enable a SSH access with a 1024 bit key. The routers should be accessible only via SSH (telnet is not permitted) from the site. Use the user "skills" and the domain "null.nil".

Ensure the authentication with RADIUS server. The RADIUS server is windows NPS.

Use the local database on the device for the authentication method for the fall-back mechanism. Configure local users based on the RADIUS server users with maximum rights.

Router RT1 Configuration

Remove the existing DHCP pools.

Create a Remote Access VPN

Define a DHCP pool (name: "VPNRAPOOL") as specified in the appendix.

Configure a client configuration group:

Group name:	VPNGROUP
Group key:	Skills_2013!

Make sure RADIUS is used for authenticate the VPN clients.

Use the local database on the device for the authentication method for the fall-back mechanism. Configure local users based on the RADIUS server users with maximum rights.

Configure a transform set with tag VPNSET and use an Encapsulating Security Protocol (ESP) transform with a 3DES cipher with ESP and the SHA hash function.

IPSEC VTI Tunnel Configuration

Configure an ISAKMP policy with the priority tag 10, authentication type pre-shared. Use authentication key "Skills_2013!", AES 256 encryption, SHA as your hash algorithm, and Diffie-Hellman group 5 key exchange for this IKE policy. Give the policy a life time of 30 minutes.

Configure a transform set with tag S2S_SET and use an encapsulating security protocol (ESP) transform with an AES 256 cipher with ESP and the SHA hash function.

Create a Voice VLAN as specified in the appendix.

Provide DHCP service for voice devices.

Router RT2 Configuration

Remove the DHCP pools.

Configure an IPSEC VTI tunnel in the same way as already done on RT1.

Configure a transform set with tag S2S_SET and use an Encapsulating Security Protocol (ESP) transform with an AES 256 cipher with ESP and the SHA hash function.

Create a Voice VLAN as specified in the appendix.

Provide DHCP service for voice devices.

Router RT0 Configuration

Create necessary routed interfaces as specified in the diagram.

Create a loopback interface to simulate the ISP web server.

Activate the web server on the layer 3 device.

Switching

Switch SW1 Configuration

Modify/Create VLANs as specified in the appendix.

Ports not used according to the list should be disabled and assigned to the unused VLAN.

Provide port security on SW1 on switchport Fa0/1 used by SZU VLAN. Only the needed addresses are permitted. Use the least possible value for configuration of the max. secure mac addresses.

Note: because of the virtualization you have to consider that both host machine interface and virtual machine interface MAC address appear on the switch port.

Switch SW2 & SW3 Configuration

Modify/Create VLANs as specified in the appendix

Ports not used according to the list should be disabled and assigned to the unused VLAN

Provide port security on SW2 on switchport Fa0/1 und Fa0/3 used by TGM VLAN. Only the needed addresses are permitted Use the least possible value for configuration of the max. secure mac addresses. In case of violation of port security the ports of the switch must recover automatically after 30 seconds.

Propagation of VLAN information should be done using secure VTP. Configure SW2 switch as VTP server. Use TGM as your VTP domain name.

Configure EtherChannel group 1 between the switches based on the network diagram.

Allow only the necessary VLANs over the EtherChannel.

Router RT0 Layer-2 Configuration

Create necessary VLANs as specified in the diagram.

Configure dot1x authentication for the port connected to WC3 and also for the ports fa0/10-23 on the switch SW2.

Ensure the authentication with your windows RADIUS server. As fallback authentication method, the local database on the device has to be used. Set up a local user base on the RADIUS server and add users with maximum rights.

VOICE

Router RT3 Configuration

RT3 should use the highest address from its network.

Provide DHCP service for the voice device.

RT3 should provide time services to all of your network devices. Use a stratum value of 8.

Create a Loopback interface (200.200.10.1/24) to source NTP services.

The client devices must use NTP authentication by using the key string "Skills_2013!"

VOIP Configuration

Note: if the Cisco IP Communicator doesn't register for the own CME, then disable the connection between the two offices and renew the registration.

Provide voice communication between the two offices

Configure Call Manager Express on RT1

IP addresses for the phones are served from RT1 for the designated VLAN.

Further parameters needed for operation of VoIP are also provided by RT1

Emergency call has to be configured on the phones at number 9111. This number has to be forwarded to IPv4 address 200.100.10.254.

Create a telephony service at the TGM office, the phone numbers should start with 11..

The maximum ephone number is 10, the maximum directory number is 10. The phone line should be assigned to button 1.

Display a label "TELE1" and a system message "TGM" on the CIPC phone.

Configure Call Manager Express on RT2

IP addresses for the phones are served from RT2 for the designated VLAN.

Further parameters needed for operation of VoIP are also provided by RT2

Emergency call has to be configured on the phones at number 9111. This number has to be forwarded to IPv4 address 200.100.10.254.

Create the same telephony service as in the TGM office, but the phone numbers should start with 12..

The maximum ephone number is 10, the maximum directory number is 10. The phone line should be assigned to button 1.

Display a label "TELE2" and a system message "SZU" on the IP phone.

Configure Call Manager Express on RT3, details follow

IP address for the emergency phone is served from RT3

Further parameters needed for operation are provided by RT3 as well.

The maximum ephone number is 10, the maximum directory number is 10. The phone line should be assigned to button 1.

Display a label "EMERGENCY" and a system message "Headquarter" on the emergency phone.

IP SERVICES & OTHER TASKS

NTP Configuration

The network devices RT1, RT2 and SW1 – SW3 must be synchronized with your NTP server (RT3) with authentication by using the key string "Skills_2013!"

NAT Configuration

Servers and end devices in the network should be able to access the internet. Configure dynamic NAT with overloading using 2 free addresses from your public range on RT1 and RT2.

WORK TASK NETWORK MANAGEMENT

Syslog Configuration

All of your network devices should send syslog messages to the syslog server on LS2.

Do not send debugging messages.

Set up a secure implementation of network management by using the SNMP protocol

You must be able to manage RT1, RT2 and RT3 via SNMPv2c from Zabbix on LS1.

Use "noskills" as the **read-only** community string and "allskills" as the **read&write** community string.

Configure a unique SNMP community string for traps "trapskills"

FTP/TFTP Configuration

Configure your active components to create daily backups automatically to the server LS1.

For security reasons, the backup traffic should be encapsulated.

ACL Configuration

Use access control lists for limiting web traffic on SZU from Windows clients to the interval of 12 and 14 o'clock every day.

Remote access for administration of all active devices should be restricted to allow host LC1 only.

The web server should be accessible for selected user groups, namely workstations and PC's from VLAN 10 only.

QoS Configuration

Use QoS to mark EIGRP, Telnet and SSH traffic between the offices on the serial link, details will follow

Set the IP precedence field to 7 for critical packets (EIGRP)

Set the IP precedence 5 for interactive packets (Telnet and SSH)

WINDOWS

During day 2 you will configure servers and clients in the domain szu.local.

WS1 will function as a DC, DNS, DHCP, IIS, CA etc. server.

WS2 will function as file server, DHCP Failover, second DNS, RD Web Access, etc. server.

WS2 is not a domain controller.

WS3 will function as iSCSI storage server.

WC1, WC3 will function as client and test machine for DHCP, NAP, web server etc.

WC2 ,WC4 will function as client for WDS multicast deployment

You will see basic network configuration information in the network diagram.

All machines have the same basic specification and configuration, as done on day 1.

Active Directory

Install and configure Active Directory services on WS1.

ACTIVE DIRECTORY SPECIFICATIONS

Domain name:	szu.local
DSRM passwords:	STM_2013! or Skills_2013!"

Create OUs and groups

Server and Client Organization in the AD

All machines W* are domain members of the domain szu.local , if not, you have to put them into the domain, the only exceptions are **WC2 ,WC4**.

WS1 is part of the organizational unit domain controllers.

WS2, WS3 are organized in the ouServers.

WC1 is part of the ouWC1, WC3 is part of the ouWC3.

DOMAIN GROUP/OU LIST

Groupname/OU Name	OU Location	Group Location
HR	Domain root	ouHR / grpHR
Finance	Domain root	ouFinance /grpFinance
Management	Domain root	OuManagement /grpFinance

Table: domain groups

Create OUs and groups as specified in the table.

User logon name	Password	Group member / OU Location
hr01-hr29	Skills_2013!	ouHR / grpHR
f01-f29	Skills_2013!	ouFinance /grpFinance
m01-mf29	Skills_2013!	ouManagement /grpManagement

Table: domain user

Create users und group membership as specified in the table, all user accounts must be active.

Configure home and profile directory for all users

     D:\User\Homes\

     D:\User\Profiles\

with their login name.

Secure access for the users to their directories must be guaranteed.

To speed up user management you can or better should use a script to generate the users

```
hr01,hr02.............        hr29
f01,f02................        f29
m01,f02................        m29
```

Configure shared data access folders (rw) for the users in

     D:\Data\HR

     D:\User\Finance

     D:\User\Management

depending on their group membership.

Configure a shared data access folder for the administrator D:\User\Administrator

Configure a login script for the administrator to connect drive letter R: to this shared folder.

Configure login scripts for HR, Finance and Management to connect with drive letter S: to their shared folders.

Assign these login scripts via group policies to ouHr, ouFinance and ouManagement.

USER SCRIPTING

Create a csv File User.csv.

```
Lastname;Firstname;Password
Davolio;Nancy;P@$$w0rd!1
Fuller;Andrew;P@$$w0rd!2
Leverling;Janet;P@$$w0rd!3
```

```
Peacock;Margaret;P@$$w0rd!4
Buchanan;Steven;P@$$w0rd!5
Suyama;Michael;P@$$w0rd!6
King;Robert;P@$$w0rd!7
Callahan;Laura;P@$$w0rd!8
Dodsworth;Anne;P@$$w0rd!9
Lucas;Wong;P@$$w0rd!1
Isobel;Jackson;P@$$w0rd!2
Madeleine;Dale;P@$$w0rd!2
Jay;Howell;P@$$w0rd!3
Michael;George;P@$$w0rd!4
Jade;Stephenson;P@$$w0rd!5
Harley;Lord;P@$$w0rd!6
Grace;Riley;P@$$w0rd!7
Adam;Porter;P@$$w0rd!8
Edward;Cole;P@$$w0rd!9
```

Create a script which creates the users with the following rules from the file User.csv.

Name your script ImportUsers.??? and put this file and the imported file user.csv on the administrator desktop on WS1 for testing.

Put the user in the OU ouImportedUsers in the root of szu.local.

The login name is generated with the first letter of the firstname and the whole lastname.

The email address of the user is generated with the whole first name, the whole last name, the character @ and the domain name szu.local.

Example:
```
Davolio;Nancy

Login name: NDavolio
Emailaddress: nancy.davolio@szu.local
```

DNS

Configure a DNS Server for szu.local

Create a reverse zone for the internal IP range. 10.1.xxx.xxx.

Create a secondary zone for tgm.local

Create a DNS failover or backup system on WS2 that in case the DNS service stops working on WS1, the DNS services for szu.local and tgm.local is still working (for this purpose you should use secondary zones). In case the DNS service on WS1 fails, the WCx clients have to look up the DNS name on WS2.

Create hostnames for your websites.

You get the IP addressing information for all machines from the network diagram as shown above.

All clients IP addresses are served by DHCP.

Configure a DHCP server on WS1 to serve all WCx (WC1, WC3) clients in the domain szu.local.

All windows DHCP clients are served from a WS1 or WS2.

Create a failover to WS2, in case the DHCP service stops working on WS1, the DHCP services in szu.local is still working on WS2.

IP addressing scheme

You get the IP addressing information for all machines from the network diagram as shown above.

The client DHCP IP address range is xxx.xxx.xxx.101-125 for all networks.

Hint: all Linux DHCP Clients are served from a Linux server.

Group policy management

User

Configure the group policy management for the OU HR

Configure the policy to disable the viewing of the last login screen (gpoNoLoginName).

Do not display the last logon name on the login screen.

Create gpoHRDesktop to personalize the Desktop of the HR organizational unit.

Create a picture(Paint) picHR on the share "Desktops".

Personalize the desktop wallpaper with this picture for all users in ouHR.

Create gpoFavoriteSzu to display a new entry with the URL- target www.szu.local in the IE favorites.

Computer

Configure Group Policy for ouWC1:

Software installation

On the clients in ouWC1 the Adobe Reader has to be installed via group policies.

The adobe.msi installation file can be found on the second hard disk of WS1.

Software restriction

On the client WC1 it is prohibited to run the application "wordpad" via software restriction.

IIS

Create a website www.szu.local. This website can only be accessed anonymously from 10.1.xx.xx.

Create and use the following start page index.htm:

> "Welcome on www.szu.local"

Create a website http://management.szu.local. This website can only be accessed from members of the grpManagemnt.

Create and use the following start page index.aspx:

> "Welcome management on management.szu.local"

Write an aspx file index.aspx for testing the aspx functionality.

Use aspx code for that purpose, not only html code.

For other external use of www.szu.local create a secure website https://ws1.szu.local. This website can be accessed from anywhere.

For that purpose you get the certificate for this secure website from your own CA in your Active Directory on WS1.

If needed you have to configure the necessary or required steps on your DNS server WS1 for those websites.

CA

You get the certificate for this secure website from your own CA in your Active directory on WS1.

File Service Resource Manager und Disk Quotas

It is not allowed to save files of types *.avi, *.wav, and *.mp3 in the directory noFilmsMusic on hard disk D:

Generate a report that includes duplicate files and its owners on hard disk C:

Disk quotas finance users

Limit the disk space of finance users in directory D:\User\Homes\ to 5 MB.

Limit the disk space of finance users in directory D:\User\Profiles\ to 10 MB.

Limit the disk space on disk drive D: to 20 MB for all users in grpFinance.

Create a directory \Projects on WS1 and WS2. Replicate and synchronize them between both computers the directories using DFS.

For testing put in the files:

Starts with
DfsTest01.txt
..
..
..
until
DfsTest19.txt.

DHCP failover

Configure a DHCP failover, if DHCP stops working on WS1, WS2 will still serve the WC* clients with IP addresses in the configured scopes.

The synchronization of WS1 and WS2 servers must be done automatically.

NAP ENFORCEMENT FOR DHCP

Configure NAP enforcement for DHCP on ouWC1 and the according DHCP scope.

If the clients in ouWC1 are not running a firewall, the health validation is false.

If the clients in ouWC1 are running a firewall, the health validation is true.

The health state and health validation are only depending on the windows firewall state.

You can test it with WC1.

SNMP

Activate SNMP on WC3 with the community string *noskills* for monitoring (only reading) WC3 in Zabbix on LS1.

iSCSI Storage and Target

Configure a fault tolerant hard disk storage in WS3 (minimum at least four hard disks) that can be reached from WS1 via the iSCSI target.

Connect from WS1 to the iSCSI storage on WS3.

You should be able to use this iSCSI storage - physically on WS3 - as the iSCSI target on WS1. This device should be assigned as drive letter **Z:**

Remote Desktop Web Access

Configure a remote desktop for web access on WS2.

If additional components on the server WS2 are needed, you have to install and configure those components or features.

The users of the grpFinance should be able to make a calculation via a remote desktop. Therefore they should see only calc in their remote desktop web frontend.

The users of the grpHR should only see Paint via remote desktop web frontend.

The users of the group management should be able to work with both programs.

The management must be able to use paint and calc via remote desktop web access.

Windows deployment services

Configure a deployment service on WS1.

You should configure a basic windows 8.1 deployment for WC2 and WC4.

Both client machines should be deployed with windows 8.1 with the deployment service.

On behalf of better network performance you should use multicast deployment.

The multicast deployment of windows 8.1 should automatically start when two machines are pending.

You don't have to implement a zero or light touch deployment.

The way to start the client installation can be done manually until the operating system is pending for the multicast deployment on WC2 and WC4.

Windows Backup and Restore

Use Windows Backup to backup once the directories

 D:\User\Homes\

 D:\User\Profiles\

to drive Z: .

Afterwards restore the directories from the backup in Z: to the new directories

 D:\Restored\User\Homes\

 D:\Restored \User\Profiles\

General

Your first job on this day is to set up a basic networking functionality on all Linux hosts according to the information specified in the topology view.

Define a testing procedure to do efficient connectivity checks for all end devices.

Ensure that all installed components are correctly installed and working.

Network services to be installed on LS1 or LS2

Server LS1

§   DNS service (bind9) for domain tgm.local and as slave for szu.local (DNS server WS1)

§   Set up a DHCP service for LC1 and the address range 150 to 170 for the last octet in the appropriate pool

§   Configure a mySQL database server and a corresponding client using the default user and password

§   Apache2 HTTP services with php5 and mySQL support

§   Configure FTP service (proftpd) with user ftp, which is a member of the group ftpusers

Users which are not members of the group ftpusers should have no access to the ftp service. Use /srv/ftp as home directory.

Maybe a FTP client is helpful for testing.

§   TFTP service (tftpd-hpa) for router and switch backups and configure the path /srv/tftp as default.

It is possible to test the TFTP service with a compatible client.

§   Activate SNMPv2c to support the projected network monitoring. Set the community strings "noskills" as readonly and "allskills" as readwrite.

§   NTP client service with RT3 as NTP server

§   For management purposes, the packages cacti (cacti-perl mrtg rrdtool librrds) and zabbix (zabbix-server-mysql zabbix-frontend-php zabbix-agent) should be installed.

The web interface with database connection to the MySQL server should be activated and tested.

Server LS2

§   Use the service syslog (rsyslog) for all available active networking components

Every component (syslog client) should get its own syslog file located in the default syslog directory (for example /var/log/syslog-RT2.log).

§ SNMPv2c service to support the planned network monitoring

§ NTP client service with RT3 as NTP server

Network Management

Furthermore, the following network monitoring tasks must be done on LS1. The specified parameters should be implemented in the monitoring systems and visualized on the web interface, if needed.

Cacti

The devices LS1, LS2 and RT3 are dedicated for monitoring with SNMP and a graphic should be created, especially using either the parameter "In/OutBits for a specified LAN interface" or "Memory Usage". Configure user "admin" and password "admin" for the appropriate web interface.

Zabbix

The devices LS1, RT1, RT2, RT3, and HOST4 should be monitored using the SNMPv2c protocol.

Retrieve all available MIB variables and visualize at least the MIB parameter "CPU load" as a graphic on the web interface.

Use the user "Admin" and password "zabbix" for web access.

Documentation

Please write a short documentation about your implemented network monitoring tasks and refer to the relevant topics in the "Network Management" section above.

Telephony Configuration

According to the basic configurations for telephony services described in the section "Networking" a few special tasks should be added.

Especially the implementation of the Cisco IP Communicator software makes some additional points necessary:

Install the virtual audio driver "Sound Driver VSC1.5" first, which can be found on the media device in the same directory as the "IP Communicator" software.

Tasks to perform:

§ Install and implement IP Communicator with the settings specified in the appendix.

§ Verify the functionality

Appendix
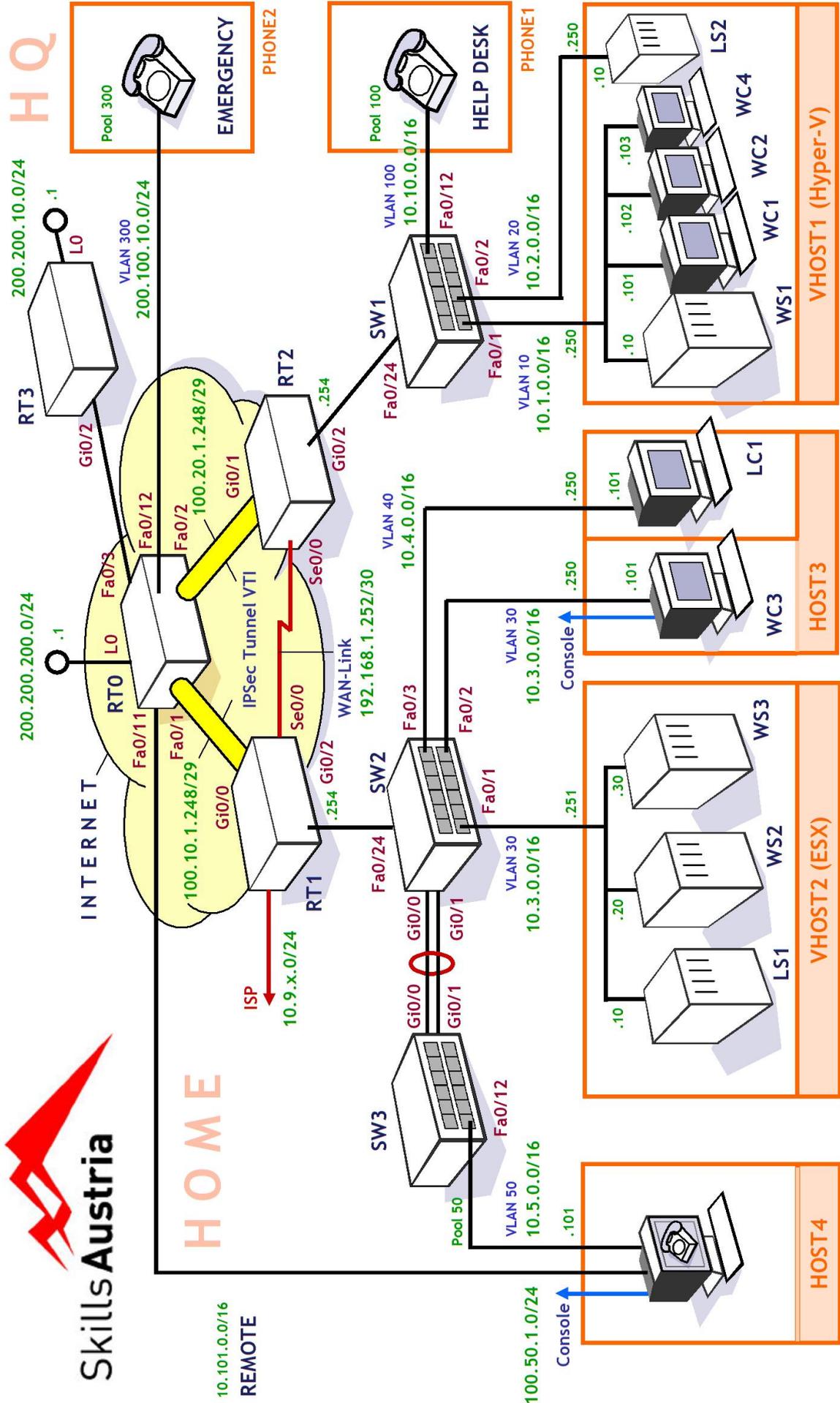
Test Matrix I

Device				
RT0				
RT1				
RT2				
RT3				
SW1				
SW2				
SW3				
LS1				
LS2				
WS1				
WS2				
WS3				
LC1				
WC1				
WC2				
WC3				
Phone1				
Phone2				
Phone3				

Table: check matrix 1

Test Matrix II

Device				
RT0				
RT1				
RT2				
RT3				
SW1				
SW2				
SW3				
LS1				
LS2				
WS1				
WS2				
WS3				
LC1				
WC1				
WC2				
WC3				
Phone1				
Phone2				
Phone3				

Table: check matrix 2

*** TRASH ***

Router 0

Device	Interface	IP Address	Connected to...
RT0 (Router 0)	Fa0/0	100.10.1.1/29	¨ RT1
	Fa0/1	100.20.1.1/29	¨ RT2
	Fa0/2	200.100.10.254/24	¨ RT3
	Fa0/11	100.50.1.1/24	¨ HOST4
	Fa0/12	200.100.10.254/24	¨ PHONE2
	Lo0	200.200.200.200/24	-

Table Information

Router 1

Device	Interface	IP Address	Connected to...
RT1 (Router 1)	Gi0/0	100.10.1.2/29	¨ RT0
	Gi0/2	10.x.0.254/16	¨ SW2
	Se0/0	192.168.1.1/30	¨ RT2

Table Information

Router 2

Device	Interface	IP Address	Connected to...
RT2 (Router 2)	Gi0/1	100.20.1.2/29	¨ RT0
	Gi0/2	10.x.0.254/16	¨ SW1
	Se0/0	192.168.1.2/30	¨ RT1

Table Information

Router 3

Device	Interface	IP Address	Connected to...
RT3 (Router 3)	Gi0/2	200.100.10.254/24	¨ RT0

Table Information

Emergency Phone

Device	Interface	IP Address	Connected to...

PHONE2 (Emergency)	Int1	200.100.10.*/24	¨ RT0	Lille 2014

Table Information

TGM

*

SW1 (Switch 1)

Device	Interface	IP Address	Connected to…
SW1 (Switch 1)	Fa0/0	VLAN 10	¨ VHOST1 (Int1)
	Fa0/1	VLAN 20	¨ VHOST1 (Int2)
	Fa0/12	VLAN 100	¨ PHONE1
	Fa0/24	?	¨ RT2

Table Information

APPENDIX (VITO)

APPENDIX NETWORK (CISCO)

NETWORK SPECIFICATIONS

SZU Office

Public IP subnet   100.20.1.0/29

VLAN 10   10.1.0.0/16   Port on SW1: Fa0/1

VLAN 20   10.2.0.0/16   Port on SW1: Fa0/2

VLAN 77   unused   all unused ports

VLAN MGMT (ID: 99)   10.99.0.0/16   Interface on SW1: VLAN99

VLAN VOICE (ID: 100)   10.100.0.0/16 Port on SW1: Fa0/12

RT2 inside addresses   10.1.0.254, 10.2.0.254, 10.10.0.254, 10.99.0.254/16, 192.168.1.2

RT2 outside addresses   100.20.1.1/29, DG: 100.20.1.6

DHCP pool for Voice   10.10.0.100-150

SW1 10.99.0.1/16

Tunnel IP   10.0.0.2/30

Phone Number for TELE2   1201

Phone Name and Label for TELE2   TELE2

CME SZU System Message SZU

TGM Office

Public IP subnet   100.10.1.0/29

VLAN 30   10.3.0.0/16   Port on SW2: Fa0/1, Fa0/2

VLAN 40   10.4.0.0/16   Port on SW2: Fa0/3

VLAN 78   unused   all unused ports

VLAN MGMT (ID: 98)   10.98.0.0/16   Interface on SW2 and SW3: VLAN98

VLAN VOICE (ID: 50)   10.5.0.0/16   Port on SW3: Fa0/12

RT1 inside addresses   10.2.0.254, 10.3.0.254, 10.4.0.254, 10.5.0.254, 10.98.0.254/16, 192.168.1.1

RT1 outside addresses   100.10.1.1/29, DG: 100.10.1.6

DHCP pool for Voice   10.5.0.100-150

DHCP pool for VPN client 10.101.0.101-150/16

SW2 10.98.0.2/16

SW3 10.98.0.3/16

Tunnel IP   10.0.0.1/30

Phone Number for TELE1   1101

Phone Name and Label for TELE1   TELE1

CME TGM System Message   TGM

INTERNET

Public IP networks   100.10.1.0/29,   100.20.1.0/29,   100.50.1.0/24,   200.100.10.0/24,
200.200.200.0/24

VLAN 300   200.100.10.0/24

RT0 addresses   100.10.1.6/29,   100.20.1.6/29,   100.50.1.254/24,   200.200.200.254/24
(Loopback-Interface)

RT3 address   200.100.10.254/24, 200.200.10.1/24 (Loopback-Interface)

DHCP pool for Voice   200.100.10.100-110

Phone Number for EMERGENCY   9111

Phone Name and Label for EMERGENCY   EMERGENCY

CME EMERGENCY System Message   Headquarter

NATIONAL FINAL
ENTERPRISE ICT TEAM

(4. EUROSKILLS 2014 IN LILLE, FRANCE)

ENTERPRISE ICT
TEAM 2013

DAY 3

SZU Wien 3, Ungargasse 69

21. - 23.11.2013

General Information

Today you have to solve the last missions to complete the competition. For doing so, you will have to do network design tasks as well as optimizations as listed on the following pages.

The previously configured network of your company in Lille makes a good job for the actual situation, but needs to be improved for the future.

To find the best solution, it is necessary for the management team from Lille to get a detailed document including a description for each extension according to the following sections.

Before you begin

Please read the following pages to see the demands for additional functionality and try to follow the instructions carefully. Try to assign an appropriate workflow to the team members and think of an efficient time management. Today you will only have 2½ hours to complete all tasks.

Overview of the competition tasks

Day 3

Today you will need to plan enhanced functionality for your network to optimize and harden your infrastructure. This will have to be done on paper, so no configuration in real equipment will be done today.

You are allowed to use all instruction papers of the previous days as well as the notes you have already taken.

Creating a written documentation on the given papers according to the following structure:

§ Network Design

§ Network Security

§ Quality of Service

All members of your team will have to work together to realize a single documentation containing solutions for the given sections.

Before you finish your work

Keep in mind that all your work has to be finished before **11:30**. Make sure that you will have finished your work and enclosed the document in the given folder before this time mark.

A Design

A new location will be built up in the near future, using the router RT3 to integrate this company site.

The site will support multiple divisions, mainly a technical and sales group, but also members of the help desk and network administration. Additionally three seminar rooms for up to 50 participants will be available in the new building.

More information about the staff will be given in the table below:

Organisational Unit	Members	Remarks
Chief executive	2	WLAN, IP-Phone, Tablet and a new video conferencing system
Sales	20	Apple Workstations
Technicians	25	Windows PC's
Help desk	40	PC's, SIP IP-Phones (30) and SCCP-Phones (10)
Network admin	5	Sun Workstations (Solaris OS) with Dual-Gigabit-NIC's
Guests	150	LAN and WLAN connectivity, IP-Telephony Head sets in one room

Table: company department details

You should suggest which active components will be bought to build up the company network for the new location. Please also add a network diagram showing the network topology for this site.

Design a logical structure for the given organisational units by defining VLAN's and IP networks. Use the dedicated network address ranges as defined as follows:

§   IP Range X   172.30.248.0/255.255.254.0

§   IP Range Y   10.32.64.128/255.255.255.128

It is also necessary to find a solution how to implement your services by integrating the site in the existing network of the company.

You have to decide how many servers and clients are useful and which services and protocols should be implemented on the new site.

Make a short summary including both, your motivation for the decisions and documentation of the benefits for the given network design.

B   Security

Prepare a solution to secure the new network by considering the following requirements:

Chief executive

The two members of the top management need to have access to any department of the company (at least on this site).

The video conferencing system will be used to realize conferences between different locations of the company. The transferred information is highly secure and should not be monitored by unauthorized users.

Sales

The sales group is using the SAP environment which shouldn't be accessible from other departments. Therefore a basic security concept has to be designed.

Other organisational units

Discuss important demands for additional security which should be implemented for the other organisational groups. Explain your solutions in a short summary.

C   Quality of Service

Work on a solution to implement quality of service in the company network. Quality of service has to be realized by using the DiffServ model.

The demands of the following departments for traffic prioritization are be seen in the table below:

Department	Demand
Chief executive	High speed priority for all outgoing traffic
Network Admin	Reliable network
Guests	Lower bandwidth
All others	No special demands

Table: traffic demands

Please keep in mind that different services (video traffic, telephony etc.) may need diverse solutions for traffic prioritization and queuing. For example, you can use three classes (Voice, Management, Telnet/SSH) to classify the network traffic.

In a short summary you include your main goals and your solutions to implement QoS. A good documentation includes an appropriate policy and a description for each traffic class.

Conclusion

All the written papers of today have to be put in your folder in chronological order and left on the workplace.

All folders will be collected by the jury members at 11:30. Then the closing analysis for calculating the final score will start.

In the meantime you are advised to be patient until the presentation of the winners will take place.