Test project

state championship IKT

November 2014, Salzburg

DI Christian Schöndorfer
DI Clemens Kussbach
DI August Hörandl

Version 2.1

Table of content

Inhaltsverzeichnis

Common annotations

- The championship has to be done in individual performance, no talks are allowed between students.
- All results must be documented (see remarks in declaration).
- Your documentation must be submitted every day; it must be printed and every page of your documentation has to be signed. Only printed and signed documents can be used for evaluation.
- Your documentation needs to be created in MS Word,
    - It has a titlepage with your name, station-number, date, page-count.
    - Each page has a page number and your name.
    - Your documented solution has to refer to the chater and task numbers in this specification.
    - Your document must include either the configuration file with your changes marked or a screenshot for GUI based configurations.
    - The final document has to be uploaded to the skill server at the end of each day.
- If the test parameters specification is missing, or "seemingly wrong", provide appropriate assumptions autonomously.
- All passwords are used (unless otherwise specified in this document) to use with cisco / cisco.
- For each day you will get some logical network plan. You have to fulfill these network plan with logical addresses, physical interfaces, network-ID's, name of devices and so on. As a complement to the logical network plan also a physical network plan must be created.
- Each competition day has it's own tasks so you will get each day a new conceptual formulation. At the end of each day you will have to print out your documentation; but the jury will also have a look on your configuration. So if you do not give the proper passwords your settings cannot be checked and you might not receive any points!
- Have special focus on your time management; The tasks must not be done in the order of explanation.
- Carefully read the whole explanations before you start your configuration work.
- For documentation you can use one of the notebooks, these should be preconfigured. If you are missing office, you can find installation images on Skills server (see later on more information).
- The skills server also provides internet access.
- The printer is also located at skills server.
- If you are not able to finish your configuration you can still work on it the next day -> give some notes in documentation. But therefore you can only earn half points.
- The whole address concept can be found at appendix A.

DAY ONE – Part one: Networking; Basic infrastructure

Below is a schematic representation of the network to be configured on day one:

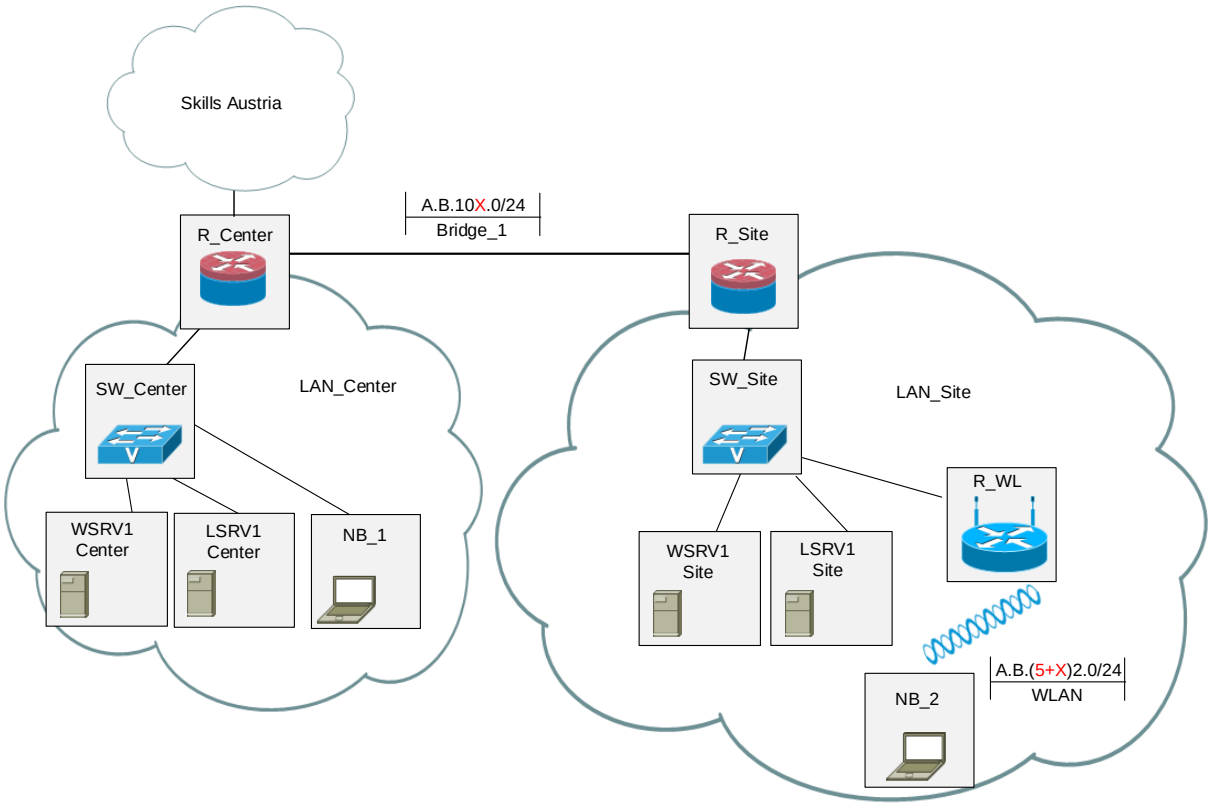


Figure 1.1: Logical szenario first day

All devices needed for this topology can be found in the original wrappings; so your first goal is to unpack all devices and build up the physical topology.

For security reasons: Make a backup of all your Router-IOS Versions on Skills-Server or USB-Stick.

Be careful: you should have two routers with security - featureset, one with voice featureset.

In detail, solve the following configuration tasks:

1.1.1. All devices are powered on and connected. ***Documentation->*** draw your physical network plan and adapt your logical network plan.

1.1.2. basic configuration for all network devices:

- 1.1.2.1 Hostname.
- 1.1.2.2 logging synchronous.
- 1.1.2.3 Banner motd „Staatsmeisterschaft 2014“.
- 1.1.2.4 no domain-lookup.
- 1.1.2.5 Local user: „cisco“ and password „cisco“, max priv.
- 1.1.2.6 Administration only by Telnet and SSH (if supported).
- 1.1.2.7 no http server.
- 1.1.2.8 no login on aux .
- 1.1.2.9 all interfaces have descriptions.

Documentation -> show running-config of all devices at the end of day.

1.1.3 specific configuration

- 1.1.3.1 configure interfaces on R_Center and R_Site (Appendix A).

1.1.3.2 Administration of R_Center is only all allowed from WSRV1 Center and LSRV1 Center; also R_Site is only allowed to be administrated by WSRV1 Site and LSRV1 Site.

1.1.3.3 R_Site and R_Center are routed via OSPF; area = X0.

1.1.3.4 SW_Center has a management-IP .100 in management-vlan 102; Management-vlan is terminated by R_Center.

1.1.3.5 Administration of SW_Center is ony allowed by R_Center.

1.1.3.6 Also configure LAN_Site in the same way. Management-IP of SW_Site is .200 in VLan 202.

1.1.3.7 Configure your access point to support connectivity form NB_2 only to local LAN_site (VLAN 201) by choosing a realistic and meaningful configuration.

1.1.3.8 Configure your physical server.

- The installation images can be found on the skills server. The skills server is located behind Switch Skills Austria (See Appendix_B). To get connected combine R_Center with the switch. Address see Appendix B; X is the number of your working place; X is also the number of "your" interface on switch Skills Austria.
- On the share "Data" on Skills server you can find all needed Images, Isos and also the network plan.
- Create a bootable usb stick; usb tools can also be found on skills server.
- Install ESXi 5.5 on your server.
- Configure two virtual networks; each virtual network contains two network interfaces; One virtual network for SW_Center (access ports VLan 101), one for SW_Site (accessport VLAN 201); so you don't have to configure VLAN-ID's in VCenter.
- For Administration of ESXi VCenter should be installed on NB_1.
- Test connectivity: From all servers and all notebooks the "Internet" should be reachable.

DAY ONE – Part two: "Microsoft"

On this first day, you will deploy one Windows Serer 2012 R2 at each site and install basic networking services. Referring to the network map, WSRV1-Center will become the first Domain Controller of the domain "worldskills.austria". WSRV1-Site on the other hand will be a branch office Domain Controller with minimal interface and functionality. To realise those servers consider the following configuration details:

1.2.1 Putting Windows Servers into operation

1.2.1.1 Take two copies of the preinstalled virtual machine "W2k12R2_Master_en" which you can find on the skills server, save them on the storage of your physical server giving them the names WSRV1-Center and WSRV1-Site. Alternatively you can perform a clean install using the ISO-images of the installation media available on the skills server. Remark: The Master-VM is fully updated and "syspreped". The administrator's password is "secret123!".

1.2.1.2 Connect both servers with the correct virtual switches that you configured earlier, in accordance with the network map.

1.2.1.3 On both servers, increase the size of the first hard disk from 20 GB to 60 GB. Then add a second hard disk (50 GB, SCSI, thin provisioned) as file storage.

1.2.1.4 **Document** the virtual hardware and network configuration of both servers in a tabular form.

1.2.2 Perform on both servers a basic configuration and **document** your settings **using CMD command outputs** (no screenshots).

1.2.2.1 Set hostnames and primary DNS suffix **(Documentation!).**

1.2.3.2 Network configuration **(Documentation!)**

- Perform first a switch-independent NIC-teaming of both adapters, giving it the name of the local network.
- Configure IPv4-Address, subnet mask, standard gateway as given by the IP-address concept.
- Configure the DNS server in the appropriate way for their roles as first and second DCs.

1.2.2.3 Configure the local firewall to allow incoming ICMP traffic from all local networks.

1.2.2.4 Set time zone and local time **(Documentation!)**

1.2.2.5 Leave automatic Windows updates disabled.

1.2.2.6 Verify and **document** IPv4-based connectivity with R_Center, skills Austria server and the internet.

1.2.2.7 Install the second hard disk by configuring a single partition and logical volume E: with the name "DATA".

1.2.3 WSRV1-Center as first Domain Controller

1.2.3.1 Deploy Active Directory Domain Services with following settings

- Root domain:
  - DNS-Name: worldskills.austria
  - NetBIOS-Name: WORLDSKILLS
- Functional Levels of Forest and Domain: Windows Server 2012 R2
- Including DNS-Server
- DSRM Password: verysecret123!

1.2.3.2 **Document** this configuration using the powershell-script provided at the end of the configuration dialog.

1.2.3.3 Configure DNS such as IPv4 reverse lookups are processed for existing and future IP-hosts as well. Database replication should be realized using Active Directory and allowed for all DNS-servers of the domain. Any host with an A-record should always get a corresponding pointer-record.

1.2.3.4 Configure a public DNS-server as forwarder for any public DNS-requests. Verify and **document** (using CMD-outputs) some forward and reverse lookup requests to public IP-Hosts.

1.2.3.5 Verify and **document** the proper functionality of Active Directory, especially of all basic services and of integrated DNS using appropriate on-board CMD-tools.

1.2.4 WSRV1-Site as branch-office DC

1.2.4.1 Prepare the Active Directory by configuring named sites and IP-ranges as given by the network map. Use names "Center" and "Site". Configure intra-site replication to happen every 15 minutes 24 hours a day.

1.2.4.2 Install Active Directory Domain Services on WSRV1-Site and promote it to a DC with following configuration details:

- same domain as WSRV1-Center
- Site: "Site",
- Global Catalog Server
- Other: same installation parameters as WSRV1-Center

1.2.4.3 **Document** this configuration using again the powershell-script provided at the end of the configuration dialog.

1.2.4.4 Configure DNS such as IPv4 reverse lookups are processed for existing and future IP-hosts as well on the site's IP-network. Database replication should be realized using Active Directory and allowed for all DNS-servers of the domain.

1.2.4.5 Verify and adapt DNS-Client settings on both Domain Controllers for best DNS performance. **Document** your settings.

1.2.4.6 Verify and **document** Active Directory replication between the sites using appropriate on-board CMD-tools.

1.2.4.7 Configure NTP on the domain-time propagating Domain Controller using LSRV1-Center as NTP-server. Verify and **document** the configuration using the appropriate CMD-tools.

1.2.4.8 Integrate WSRV1-Site into the Server-Manager of WSRV1-Center in order to centralize administration of the domain

1.2.4.9 Configure WSRV1-Site as Windows Server Core (no graphical interface) in order to minimize the need of system resources and reduce potential exposure to security risks.

1.2.4.10 Using the notebooks NB_1 and NB_2 test and **document** the IPv4 connectivity and name resolution between both sites.

DAY ONE – Part three: "Linux"

The configuration in figure 1.1 includes two Linux servers. Use the provided virtual hard disk (Pre installed Cent OS, root/"ciscocisco") or the iso-files to install the server.

On each server you will have to create local users, install and configure the ssh-server, the time server and the Apache web server. The server "in the center" will act as a print server.

You should document ALL your configurations. Small changes in existing configurations should be marked accordingly. Every additional commands necessary for the installation or configuration should be provided.

In detail, solve the following configuration tasks:

1.3.1 Provide each server with a network configuration:
1.3.1.1 Use a static network configuration, ipv4 only
1.3.1.2 Set the host name.
1.3.2 Create local users on each server:
1.3.2.1 User name "admin" with password "admin". This user should be able to do "sudo" to become root.
1.3.2.2 User name "linux00" – "linux19" with password "linux". These users should **not** be able to do "sudo" to become root. You should use a script to create these users.
1.3.3 Install and configure the ntp server on both Linux computers.
1.3.3.1 The server shall synchronize each other.
1.3.3.2 Both server should synchronize to "the internet" (at least two public servers) too. Include the output of "ntpq -p" on both servers in your document.
1.3.3.3 All other computers synchronize to the timeserver in the same net.
1.3.4 Install and configure the ssh server on both Linux computers.
1.3.4.1 For security reasons: No password authentication is allowed, only ssh keys.
1.3.4.2 There should be no ssh access for the root user.
1.3.4.3 The users "linux00" and "admin" need ssh keys. You may use the same keys on both servers.
1.3.4.4 These local users are able to login on the "other" server.
1.3.4.5 The adminstrator on the notebook should be able to do a ssh login as user "admin" on both servers.
1.3.5 Install and configure the apache web server on both Linux computers.
1.3.5.1 Create a small individual "Welcome Page" on each server.
1.3.5.2 The user "linux00" should have a personal home-page. This page should only

be reachable within the local network.

1.3.6 Install and configure the cups print server on the Linux server in the center.

1.3.6.1 Clients from center and site should be able to use this server.

1.3.6.2 Configure a printer which forwards all jobs to the printer on the skills server.

- This printer should be the default printer on all other computers.

1.3.6.3 As a fallback: configure a queue to print to the locally attached printer. You may “borrow” the printer from the skills server – but only for up to 15 minutes.

1.3.7 All services should start on system start.

DAY TWO – Part one: Networking; Basic infrastructure

Expand the topology from day on to an IP-based telephony, and other security-related configurations of the active components.

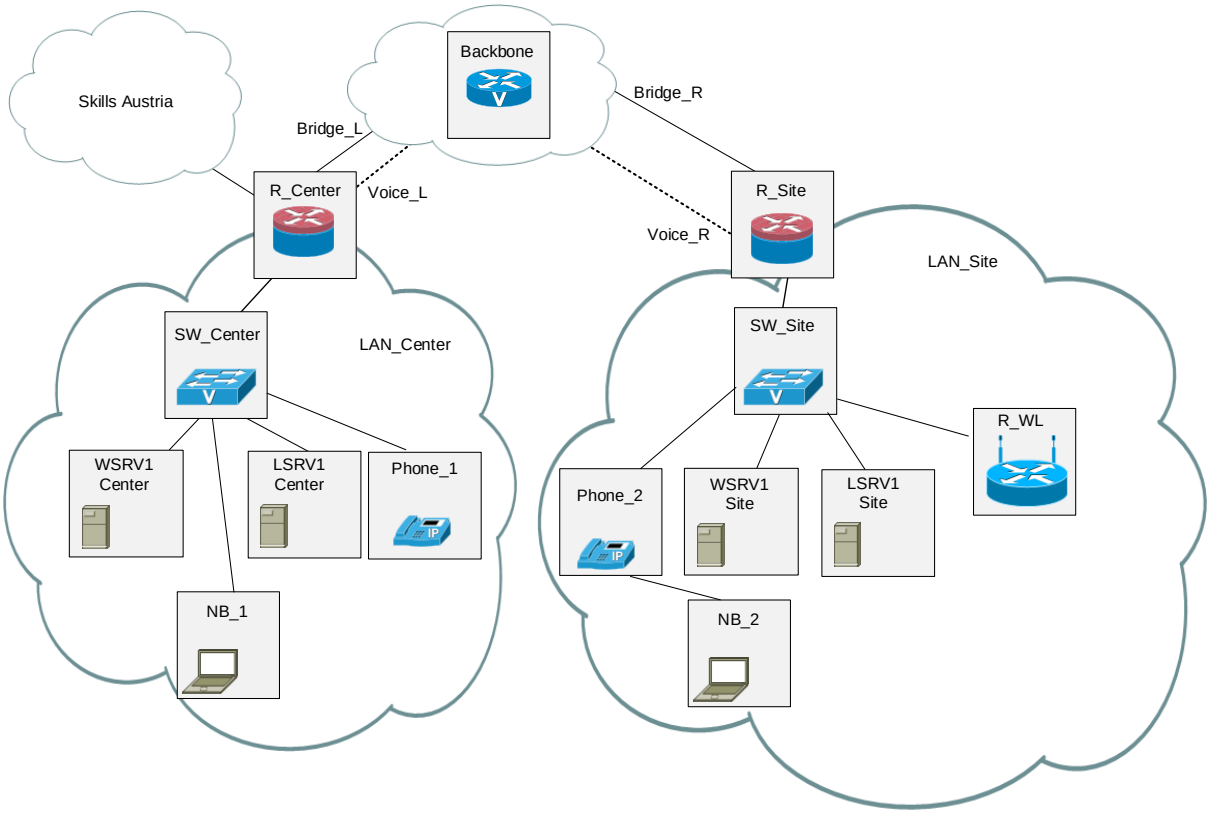


Figure 2.1: Topology day two

Router_Backbone simulates „the internet“ and also is Router_Backbone your CME.

2.1.1 Take basic configuration of Router_Backbone as mentioned under 1.1.2. Administration of Router_Backone ist allowed by R_Center and R_Site (Management VLANs). If there are not enough interfaces on your routers take it to a sensible solution!

2.1.2 Change the IP ranges according to the network plan (Bridge_L, Bridge_R, Voice_L, Voice_R).

2.1.3 Adapt the OSPF process: Networks LAN_Center (VLAN 101), Bridge_L, Bridge_R, LAN_Site (VLAN 201) and WLAN should be routed by OSPF to the “Skills Austria network = Internet”. The networks Voice_L and Voice_R should be routed statically.

2.1.4 Configure telephony-service

2.1.4.1 CME is located on Router_Backbone; install needed files for your 7962 Phones into flash:/VoIP-Files/. You can find these files on skills server -> Data -> Day 2.

2.1.4.2 Phone_1 should register by number 100 and phone_2 by number 200.

2.1.4.3 Configure a system message with your name.

2.1.4.4 On Switch SW_Center and SW_Site configure two VLAN’s; one for voice (103,203) and one for notebooks (104, 204). The VLAN for notebooks should be native; the VLAN for ip based telephony should be marked as voice-vlan. Make meaningful assumptions for IP addresses.

2.1.4.5 All VLAN‘s from 2.1.4.4 are supported with DHCP by R_Center (locally VLAN’s) and R_Site.

2.1.4.6 TFT Server is Router_Backbone.

2.1.4.7 NB_2 ist located behind Phone_2. NB_2 is allowed to ping ONLY the following Servers: WSRV1 Center and LSRV1 Center, also WSRV1 Site and LSRV1. For these connectivities adapt your routing. ***Documentation ->*** Tracerout from NB_2 to Server WSRV1 Center.

2.1.5 Configure on WSRV1 Center a radius-server. All necessary passwords are cisco.

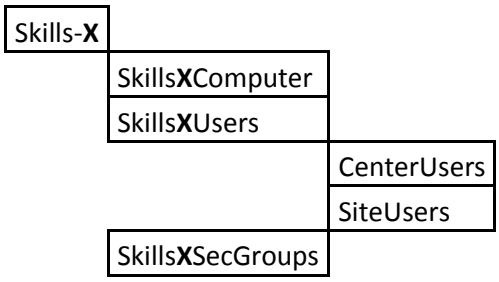
2.1.6 Expand the authentication on R_Center and R_Site by AAA authentication via radius-server. For security reasons also allow local users for authentication. The radius user is class/class. Additional radius attributes must not be configured.

DAY TWO – Part two: "Microsoft"

In your Microsoft Network, today's task is to configure the logical Active Directory structure and to provide users at any site with resources, rights and individual configurations. Additionally there is a replicating Distributed File System to be installed in the domain for local and fast access to company files. Finally you will implement data security by realising daily backups of relevant company data.

Consider now the following configuration details and specifications.

2.2.1 Logical Active Directory structure



2.2.1.1 Configure container objects of the above given logical AD structure of the worldskills.austria domain.

2.2.1.2 Configure Skills**X**Computer to be the default container for new AD-integrated clients.

2.2.1.3 Protect all containers from erroneous deletion.

2.2.1.4 Verify the correctness and **document** this new branch of the logical AD structure.

2.2.2 Create user accounts and security groups as specified by the table below and put them in the right AD container.

Users	Department/Group	Site
Office01 to Office40	Office	Center
Office41 to Office50	Office	Site
Admin01 to Admin05	Business Administration	Center
Admin06 to Admin10	Business Administration	Site
IT01 to IT10	IT	Center
Sell01 to Sell40	Marketing	Center
Sell41 to Sell50	Marketing	Site
All Users from Center	StaffCenter	Center
All Users from Site	StaffSite	Site
All Users (from any site)	Staff	-

2.2.2.1 Use “pw2change!” as temporary password for all user accounts. Users will have to change their password at the first logon.

2.2.2.2 Write a script to create all user accounts with given properties. Use Excel or another spreadsheet-tool to prepare the script and giving the opportunity to quickly create a new script for another batch of user names. **Document** this configuration step by adding one line of your script and one of your spreadsheet (showing the formulas) to your documentation.

2.2.3 Integrating clients into the domain.

2.2.3.1 Integrate NB_1 and NB_2 in the AD domain.

2.2.3.2 Verify and **document** IPv4-connectivity, name-resolution and successful AD-logon.

2.2.4 Implement File Services

2.2.4.1 Create on both servers a folder structure that supports the following specifications:

- All data are stored on the data volumes of the servers.
- Home-directories are mapped as drive **U:** for each user and are replicated between both servers.
- Company data folders have assigned access rights as described in the table below. All data have to be replicated between both servers and accessed by providing an automatically mapped drive **S:** to every user.

Folder	Access
Skills_Data	Staff: Read
Skills_Data\Strategy	Business Administration: Change
Skills_Data\Marketing	Marketing: Change Business Administration, Office: Read
Skills_Data\IT	IT: Change Business Administration: Read
Skills_Data\Organization	Office: Change Staff: Read

- Configure access in a way to provide visibility of folders only to those users that have at least read-rights for them.
- Use a security group nesting strategy (such as AGDLP/IGDLA) to provide an access-rights scheme allowing for future growth.

2.2.4.2 Verify and **document** the folder structure, implemented shares and access rights as well as the replication state of the folders using CMD-outputs.

2.2.5 Implement daily backups on WSRV1-Center.

2.2.5.1 Attach a third virtual hard disk to your virtual server (50 GB, SCSI, thin provisioned) and install it as a single volume with name “backup”.

2.2.5.2 Install the Windows Server Backup feature.

2.2.5.3 Configure a daily backup job as follows:

- Backup source: E:\Skills_Data
- Full VSS-Backup
- Once a day at 23:00
- Backup target: the new hard disk as exclusively reserved backup disk

2.2.5.4 Perform one first backup and **document** the success by copying the backup-log into your documentation.

DAY TWO – Part three: "Linux"

You will add your personal cloud to your network: owncloud.

Do **not** use the package manager to install the software "out-of-the-box" as this version is rather old – you want to install the newest version 7.x. Use the provided installation file or adjust the repositories for your distribution.

In detail, solve the following configuration tasks:

2.3.1 Install Owncloud and all necessary packages. Do NOT use sqlite as a database.
  2.3.1.1 You should add a hard disk with 100 GB and use it as the storage for owncloud.
  2.3.1.2 Owncloud should automatically start on system startup.
2.3.2 Create the owncloud-users "linux" and "admin".
  2.3.2.1 The owncloud-user "admin" should be allowed to administrate local users.
2.3.3 Allow users login in with their "Windows" credentials.
2.3.4 Configure access to the resources on the owncloud server for one user on the notebook:
  2.3.4.1 Access the calendar with outlook. Include a screen shot of one appointment displayed on owncloud web interface and within Outlook.
  2.3.4.2 Map the user's data to the drive O: on the notebook. Include a screen shot to document your success.

DAY THREE – Part one: Networking; Basic infrastructure

Secure the communications between Site and Center, upgrade the router to a firewall.

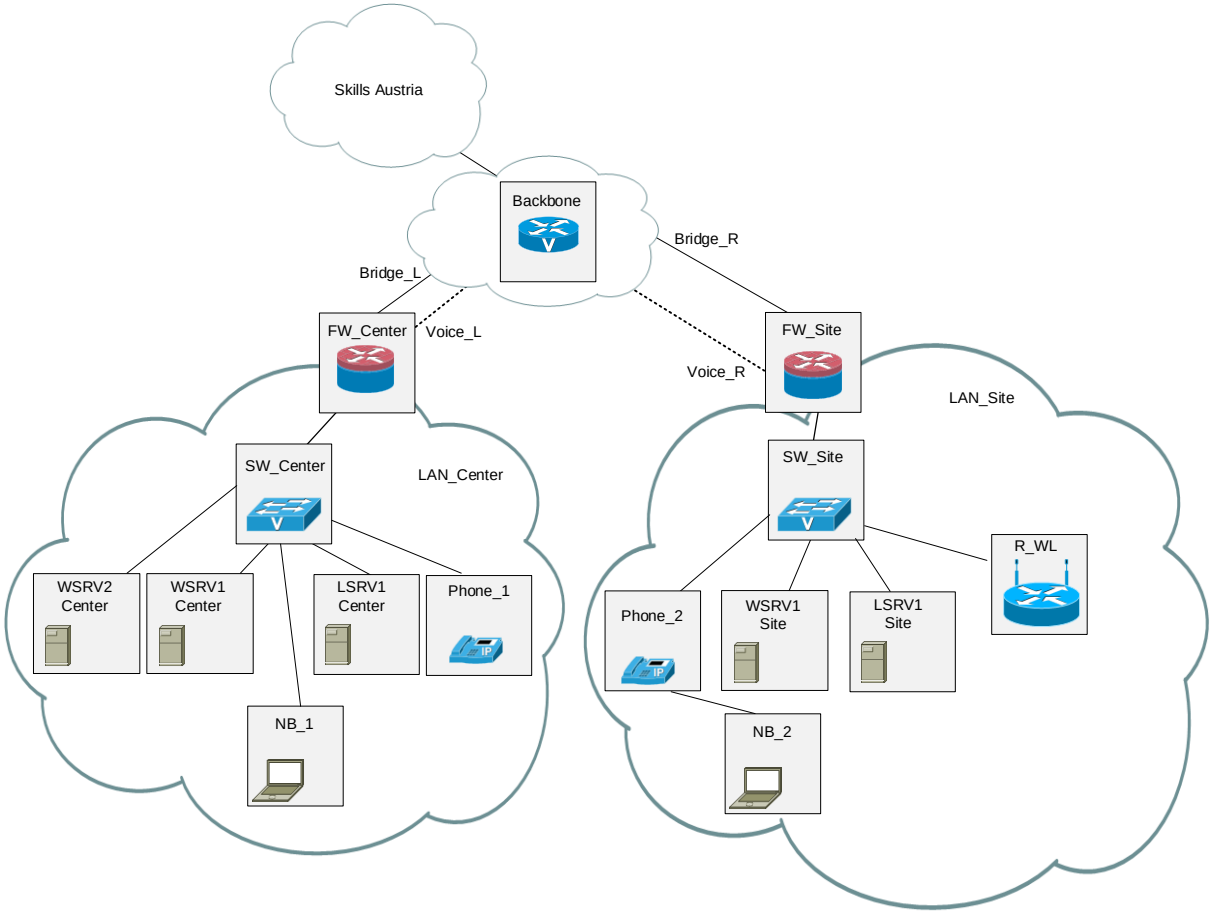


Figure 3.1: Topology day three

3.1.1 Migrate your Internet-Uplink from R_Center to Backbone. Delete your LOCAL OSPF process.

- **But be careful – don't discard your domain replication!**
- **Routing to Skills Austria (Internet) must still be routed by OSPF (still propagate necessary networks)!!**

3.1.2 Upgrade R_Center and R_Site to a stateful Firewall FW_Center and FW_Site.

3.1.3 Following functions shoul be work properly after configuring NAT/ PAT, access-lists and VPN

- All Servers and all Notebooks should reach the internet (via http, dns and icmp)
- All Servers should reach all other servers via VPN (tcp, udp and icmp)
- IP Based Telefony
- Domain Replication via VPN

3.1.4 Now create the following access-lists:

- access list „Outside-in-Bridge_L" on FW_Center; direction incoming. No new traffic except traffic specified in 3.1.3 is allowed. important notice: Use CBAC!
- access list "Outside-in-Voice-L" on FW_Center, direction incoming. No new traffic except traffic specified in 3.1.3 is allowed. important notice: Use CBAC!

3.1.5 Both firewalls perform some kind of PAT.

- For all necessary traffic specified in 3.1.3 the firewalls perform a PAT on the „outside-IF" of the Firewalls (Bridge_L or Bridge_R).

3.1.6 Configure between FW_Center and FW_Site a sito-to-site VPN on the basis of IPSEC.

- For IPSEC use pre-shared keys (cisco/cisco).
- Parameters for isakmp policy and IPSEC SA's can be chosen idependent and useful.
- VPN – interested traffic is server based communication.

3.1.7 The VoIP based traffic must not be encrypted.

DAY THREE – Part two: "Microsoft"

Your third and last day's Microsoft challenge will be the deployment of Remote Desktop Services at the main site and the application of all kinds of policies to users and computers of the domain. In order to realise these services, consider the following configuration details.

3.2.1 Implementing a member server at the main site

3.2.1.1 In the same way as on the first day of this championship, create a new virtual machine either by taking another copy of the preinstalled virtual machine "W2k12R2_Master_en" or by performing a clean install.

- Give it the name of WSRV2-Center.
- Connect it to the correct virtual network.
- Increase the size of the first hard disk from 20 GB to 60 GB.
- **Document** the virtual hardware and network configuration of both servers in a tabular form.

3.2.1.2 Perform a basic configuration as for the other servers and **document** your settings using CMD command outputs.

3.2.1.3 Verify and **document** IPv4-based connectivity with the servers of both sites and the internet as well as name resolution within the domain.

3.2.1.4 Integrate WSRV2-Center as member-server into the domain worldskills.austria and verify that the computer account is created in the OU SkillsXComputer.

3.2.2 Deploying Remote Desktop Services

3.2.2.1 Install and configure RDS according to following specifications:

- session based desktop deployment
- WSRV2-Center assumes the roles of the RD-Connection Broker, the RD-Session Host and the RD-Licensing Host
- RD-Gateway and RD-Web Access are not used within this deployment
- RD Collection for full desktop access
- Assign RD-access to a new security group called "RDUser", which members are the users of the departments Business Administration and IT.

3.2.2.2 Configure all user accounts to save Remote Desktop Profiles in a new Folder (TS-Profiles) on the data drive of WSRV1-Center. For this folder a hidden share with access rights only for RDUsers has to be created.

3.2.2.3 Install Microsoft Office 2013 on the terminal server to be used by all authorized RD users.

3.2.3 Configure administrative rights and policies

3.2.3.1 Delegate the administration of user accounts at the branch office to the user Admin10.

3.2.3.2 Implement password policies within the whole domain as follows:

- Minimum password length: 8 characters
- Complex passwords
- Password history up to 10 passwords
- Maximum password age: 60 days

3.2.3.3 Implement audit policies within the domain controllers OU as follows:

- Audit any account management
- Audit failed account logon events
- Audit any policy changes

3.2.3.4 Implement a desktop wallpaper policy for Center users showing the string "Center" in the right upper corner of the desktop.

3.2.3.5 Implement a restricted firewall policy for all client that permits RDP traffic only to and from WSRV2-Center. This firewall policy must only apply to Office, Business Administration and Marketing Staff.

3.2.4 Verify and **document** using meaningful screenshots with one user of every department at each site:

- Home directories availability
- S: drive availability
- TS user profiles availability
- Remote Desktop Services access
- Group Policies application

DAY THREE – Part three: "Linux"

You have to install Nagios to oversee the whole network. This service will be located on the linux server in center and will check all servers and network devices.

In detail, solve the following configuration tasks:

3.3.1 Install nagios and necessary nagios plugins.
3.3.2 Create a new user "nagios" with password "cisco" to do all nagios configurations. This user should replace the default nagios user.
3.3.3 Nagios should check:
3.3.3.1 All devices (including the VPN endpoints) are ping-able.
The resulting map should reflect the topology of your network.
3.3.3.2 The ntp servers are running.
3.3.3.3 The ssh server is reachable on both Linux servers.
3.3.3.4 Both Linux web servers deliver an index page.
3.3.3.5 The Linux server in site has at least 1 GB free disk space.
3.3.3.6 The Windows server in center has at least 1 GB free disk space.
3.3.3.7 Your print server is working.
3.3.3.8 The skills server is reachable – name this "The Internet".
3.3.4 Include a screen shot of the resulting nagios map in your document.
3.3.5 Nagios should start on system start.