Test Project
ES2014_TP2010_HU

APPENDIX 1.
Description of project and tasks – DAY 1

Submitted by:
Name: Zoltán Sisák
Member Country: Hungary

Table of Content

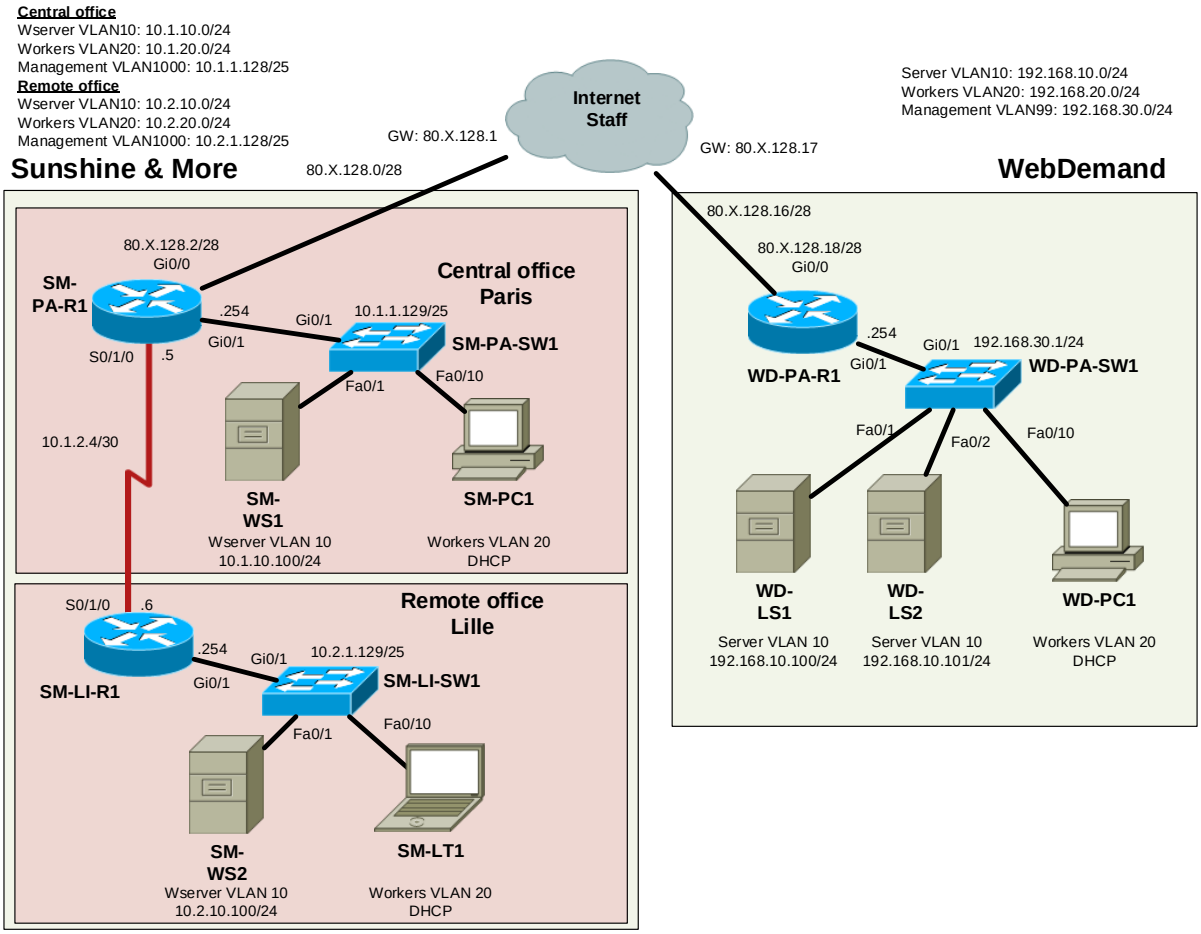
Whenever a password is not specified, you should use **Lille2014** as password on all servers, clients and devices.

IMPORTANT! If you do not use the proper password, and your settings cannot be checked, you might not receive any points for your solution!

Please use the details on the topology (IP addresses, interfaces, etc.) accurately during your implementation.

The X in the IP-addresses and names represents your team-number.

1. TOPOLOGY



2. YOUR TASKS AT SUNSHINE & MORE

2.1. NETWORK-ADMINISTRATOR TASKS

After your company was requested to build the new IT system, the topology and implementation plan were designed by the engineering group of your company. Configure the equipment according to the plan and instructions.
Note: Team member who is responsible for the network administration tasks can use SM-LT1 laptop for configuring Cisco devices via console, but SM-LT1 is also have own role in the network.

1. Build the physical infrastructure of the new network of 'Sunshine & More' according to the topology design.
2. Connect your network to the Internet through line 1 from your ISP. The ISP provided the 80.X.128.0/28 GW: 80.X.128.1/28 IP address range for your network. (X is the number of your team)

3. Make it possible that the 10 latest saved configuration can be reloaded on every router.
4. For manageability and transparency, configure the names of the devices according to the names in the topology design. Use sunshine.local as domain-name.
5. Create a user **SMadmin** on all devices, which should be able to login with SSH (SSHv2). To increase security, no login with telnet should be possible.
6. On all routers and switches set the login message to warn against unauthorized use.
7. Future network monitoring requires synchronization of the clocks with the Internet time-server with IP-address 85.20.12.100 on all network devices using NTP protocol with MD5 authentication. Key ID: **14**, key: **GoToLille!**
8. Servers and end-user machines need to be logically separated. For this purpose, create 3 VLANs in the center with the IDs and names below. You need to apply the instructions of the engineering group.
    a. VLAN 1000, Management, IP range: 10.1.1.128/25.
    Assigned ports on **SM-PA-SW1:** Fa0/20-24
    VLAN 10, Wserver, IP range: 10.1.10.0/24
    Assigned ports on **SM-PA-SW1:** Fa0/1-9
    VLAN 20, Workers, IP range: 10.1.20.0/24
    Assigned ports on **SM-PA-SW1:** Fa0/10-19
9. In the remote office you will have to create the same three VLANs, but there the IP addressing changes in such way, that the second octet of the above addresses changes to 2:
    a. VLAN 1000, Management, IP range: 10.2.1.128/25
    Assigned ports on **SM-LI-SW2:** Fa0/20-24
    VLAN 10, Wserver, IP range: 10.2.10.0/24
    Assigned ports on **SM-LI-SW2:** Fa0/1-9
    VLAN 20, Workers, IP range: 10.2.20.0/24
    Assigned ports on **SM-LI-SW2:** Fa0/10-19
10. In both locations the gateway in the created VLANs should be the last address in the range.
11. For remote configuration the switches should uniformly have the first address in the created Management VLANs.
12. User machines receive addressing information from a central DHCP server running on **SM-WS1**.
13. The two sites are connected via leased line. On this line configure PPP protocol with CHAP authentication. Use addresses from the 10.1.2.4/30 network.
14. For routing between the central and remote offices use EIGRP protocol. The router-id should be the first two useable IP addresses from range 10.1.1.0/25. Ensure that the routers use unicast routing messages instead multicast messages. Routers should send out EIGRP messages only on their relevant interfaces.

15. Both locations should access the Internet through router **SM-PA-R1**. Configure access by setting the default gateway to the Internet, and advertise this to the remote office.
16. All devices in the network should be able to access the Internet. Configure dynamic NAT with overloading using 2 free addresses from your ISP.
17. The leased line between the central and remote office has limited capacity, so traffic has to be limited. Solve this by blocking Web-traffic originates from remote office clients (VLAN 20) to the interval of 17 and 23 o'clock every day.

2.2. WINDOWS SERVER TASKS

1. On host machine Host-W you will find a virtual machine called **SM-WS1**. It is a pre-installed Windows Server 2012 R2 Standard, sealed with sysprep.
2. Configure the following basic setting on server **SM-WS1**:
    a. Default keyboard setting should be 'US'.
    b. The machine name should be according to the topology drawing.
    c. The IPv4 address of the machine should be 10.1.10.100/24.
    d. Install the Domain Controller role.
        i. The domain DNS name should be **sunshine.local,** the NetBIOS name **sunshine.**
        ii. The forest level should be the highest achievable.
        iii. Create an AD integrated DNS service on this domain controller.
    e. On the functioning domain controller pre-configure the remote office services:
        i. Rename the default location to **Paris.**
        ii. Create a second location called **Lille.**
        iii. Configure the subnet of both locations according to the topology.
        iv. This server should be configured for **Paris.**
    f. Configure DNS to forward all non-resolvable requests to the DNS server of the ISP at 85.20.12.100.
    g. Configure DHCP so that all domain clients receive the required IP settings
        i. Parent domain: sunshine.local; DNS Server: 10.1.10.100 and 10.2.10.100; WINS: -; Scope Name: Par_Network; Starting IP: 10.1.20.90; Ending IP: 10.1.20.99; Default gateway: 10.1.20.254; Subnet mask: 255.255.255.0; IPv6 DHCP: disabled
        ii. Parent domain: sunshine.local; DNS Server: 10.1.10.100 and 10.2.10.100; WINS: -; Scope Name: Lil_Network; Starting IP: 10.2.20.90; Ending IP: 10.2.20.99; Default gateway: 10.2.20.254; Subnet mask: 255.255.255.0; IPv6 DHCP: disabled
    h. Create the following organizational units in Active Directory:

```
Corp
Corp\Office
Corp\Sales
Corp\ITAdmin
PC
```

    i. The client machines which will be joined to the domain should be placed automatically to the `PC` organizational unit.
    j. Create a **G_Office**, a **G_ITAdmin** and a **G_Sales** security group in the corresponding OU.
    k. Create a shared folder called **Homes**. User's home directories will be placed on this share. Ensure that users can access only their own home folder.

l. All users should have own home directory which should be accessible using logical drive `H:`
m. Create a user template with the following settings:
    i. Name: **_SalesUser**
    ii. User should be disabled and password changing is not allowed.
    iii. Group membership: **G_Sales** group.
n. Create user accounts **sa_user1** and **sa_user2** using **_SalesUser** template. These users should belong to the **Sales** OU**.**Within the **ITAdmin** OU the following users should be created: **Cisco**, **OpenSource**, **SMAdmin**. **SMAdmin** should have Administrator rights and be member of the Enterprise Admins group. The **Cisco** and **OpenSource** users should be members of the **G_ITAdmin** group. The **Cisco** user should be delegated to the **Sales** OU in such way, that he has rights to add users and groups, and modify and delete those.
o. Create user accounts **of_user**. This user should belong to the **Office** OU**.**
p. **sa_user2** is only allowed to login between 8.00-14.00 o'clock Monday till Saturday.
q. For all users and computers configure the setting not to show the last logged in user.
r. The special group policies below should be assigned to the proper OU:
    i. GPO name: **Office GPO**; limitation: not allowed to change lock screen.
    ii. GPO name: **Sales GPO**
    policy: users should not have access to the registry, and are not allowed to access the command line.
    iii. GPO name: **Laptops**
    policy: on all laptop computers (include laptops which joining to domain at the future) not allowed to change desktop background.
    iv. GPO name: **Local admin**
    policy: members of **G_ITAdmin** group should have local administrator rights when login to an existing domain client computer.

3. On **SM-WS1** install the Active Directory Certificate Services role.
    a. Let the server type be Enterprise Root CA.
    b. The CA server name should be SunshineCA, and valid for 10 years.
4. The **SM-PC1** should be configured according to the instructions below:
    a. Create a user called **Admin**.
    b. Configure the client to gain IPv4 settings from a DHCP server.
    c. Join the client to the domain.
    d. Move **SM-PC1** manually to the **Office** OU.

e. Download and install RSAT (Remote Server Administration Tools) from *http://www.rsat.com* and enable the Server Manager MMC on the client machine. Allow remote Server Manager access on **SM-WS1**.

5. On host machine **Host-W** you will find a virtual machine called **SM-WS2**. It is a pre-installed Windows Server 2012 R2 Standard, sealed with sysprep. Configure the following basic setting on server **SM-WS2**:
    a. The IPv4 address should be 10.2.10.100/24.
    b. Join this server to the domain.
    c. Install the directory services role.
        i. The server should be a DC for the existing domain.
        ii. The server belongs to the Lille site.
        iii. There should be a GC and a DNS server on this machine.
        iv. Synchronization interval on the site link should be 15 minutes.
    d. Install and configure DHCP services on **SM-WS2**, so if **SM-WS1** fails **SM-WS2** should take its place and provide IP addresses for the clients. 10% of the address pool is reserved for **SM-WS2**.
6. The **SM-LT1** laptop should be configured with the following settings:
    a. Configure the client to gain IPv4 settings from a DHCP server.
    b. Join the client to the domain.
7. On both servers you have to create a new virtual harddrive with size of . Create a partition using the whole disk space and assign drive letter `K:` to this partition.
8. Install the Windows Server Backup service on both servers.
9. Configure timed backup:
    a. Every day at 6:00 and 22:00 o'clock backup should start.
    b. Make a backup of system state and the `C:\Users\` folder only.
    c. Backup should be stored on drive `K:` .
    d. With the settings of the timed backup, create a backup now at once on both servers.

Attention! This backup could take up to 25-30 minutes!

3. YOUR TASKS AT WEBDEMAND

3.1. NETWORK-ADMINISTRATOR TASKS

After your company was requested to build the new IT system for 'WebDemand', the topology and plan were designed, complete with the necessary instructions to configure the network. Configure the equipment according to the plan and instructions from the engineering group.

1. Build the physical infrastructure of the new network of 'WebDemand' according to the topology design.
2. Connect your network to the Internet through line 2 from your ISP. The ISP provided the 80.X.128.16/28 GW: 80.X.128.17/28 IP address range for your network
3. For manageability and transparency, configure the names of the devices according to the names in the topology design. Use webdemand.fr as domain-name.
4. Create a user **WDadmin** on all devices, which should be able to login with SSH (SSHv2). To increase security, no login with telnet should be possible!
5. On all routers and switches used, set the login message to warn against unauthorized use.
6. Future network monitoring requires synchronization of the clocks with the Internet time-server with IP-address 85.20.12.100 on all network devices using the NTP protocol with MD5 authentication. Key ID: **14**, key: **GoToLille!**
7. Servers and end-user machines need to be logically separated. For this purpose, create 3 VLANs in the center with the IDs and names below. You need to apply the instructions of the engineering group.
    a. VLAN 99, Management, IP range: 192.168.30.0/24
    Assigned ports on **WD-PA-SW1:** Fa0/20-24
    b. VLAN 10, Server, IP range: 192.168.10.0/24
    Assigned ports on **WD-PA-SW1:** Fa0/1-9
    c. VLAN 20, Workers, IP range: 192.168.20.0/24
    Assigned ports on **WD-PA-SW1:** Fa0/10-19
8. In both locations the gateway in the created VLANs should be the last address in the range.
9. For remote configuration the switches should uniformly have the first address in the created Management VLANs.
10. User machines receive addressing information from a DHCP server. Make it possible, that the workstations in the Workers VLAN-ban receive information from the DHCP-server.
11. Ensure internet access for all devices on the network using dynamic NAT with overloading on the outgoing interface.
12. The web-site *www.webdemandX.hu* of the company should be accessible from the outside on the last IP-address received from the ISP.

3.2. LINUX ADMINISTRATOR TASKS

You find all Debian DVD ISOs on www.debian.org website.

1. On host machine **Host-L** you will find two virtual machines called **WD-LS1** as **WD-LS2**. Install Debian on both of them. The required user should be **wdadmin**.
2. **WD-LS1** has 3 disks of 125GB each. Partitioning should be as follows:
    a. Create two RAID1 and one RAID5 arrays in software.
    b. Except for the SWAP-partition all partitions should use the EXT4 file system.
    c. In the RAID1 arrays one of the disks should be in standby mode.
    d. One of the RAID1 arrays will be used for the root partition and should be 20 GB. The other array will be used for the SWAP partition and should be 5 GB.
    e. The remaining 100GB per disk should become a RAID5 array with LVM. Create a layout as follows:
        i. temp (20 GB) /tmp
        ii. var (20 GB) /var
        iii. home (40 GB) /home
        iv. remaining space remains empty
3. Set **WD-LS1** IP address to 192.168.10.100/24. The server should serve as a DHCP server for the company's client and server VLAN.
    a. For the workers VLAN, the first available IP address should be 192.168.20.10, the last 192.168.20.19. Netmask 255.255.255.0 and DNS server **WD-LS1**.
    b. For the server VLAN, the first available IP address should be 192.168.10.10, the last 192.168.10.19. Netmask 255.255.255.0 and DNS server **WD-LS1**.
    c. In the Server VLAN one specific device should get a predefined IP by DHCP. IP: 192.168.10.9, MAC: C8-CB-B8-C2-EF-33
4. **WD-LS1** also serves as a DNS server for the equipment and services of the client. The DNS uses the server at 85.20.12.100 provided by the ISP for resolution of external addresses. The domain name of the company is **webdemand.corp**. Add all servers and network devices and all future DNS names required for services.
5. Create a Certificate Authority with **SM-WS1** certificated root key, in directory /etc/ssl/CA under the common name **WebDemandCA**. Install **SM-WS1** root certificate as trusted CA certificate on all linux machines.
6. On **WD-LS1** install Apache2 web server with the following settings:
    a. The web server should provide the following services depending on where the request came from. The wwwroot directory is at the path specified between brackets.
        i. The intranet at *intranet.webdemand.corp* (`/www/intranet`) can only be accessed from the Workers VLAN. Request from other ranges should result a 'Forbidden' response from the web server.
        ii. The site *www.webdemandX.hu* (`/www/external`) serves requests from external sources from the internet. This should be the default

site on the server. Add the name *www.webdemandX.hu* to your DNS server as well.

   b. For each web site create a homepage identifying the site. (e.g.: the site *intranet.webdemand.corp* receives us with „Welcome to the company's Intranet Site!").
   c. Because of confidential documents on the web sites configure all sites to use HTTPS as well. For this task, create new server certificate with the previously created (linux) CA. Ensure all computer in the company network (with any operating system) verify this certificate successfully (without showing security warning message) on all website.

7. On host machine **Host-L** you will find an additional virtual machine called **WD-PC1**. **WD-PC1** serves as a testing client for all internal services of the company. On the client a basic Debian system is pre-installed; your task is to install Gnome graphical interface and the necessary applications for testing. Following settings should be considered when configuring the client:
   a. The created user during the installation is **projectuser1**.
   b. The machine should receive network address from DHCP.
8. When installing **WD-LS2** server, you do not have to use the RAID and volume parameters of **WD-LS1**! Create a 95GB root partition and a 5GB SWAP partition. Hostname should be **WD-LS2**, the IP address 192.168.10.101/24.
9. Create the following users on server **WD-LS2**: **webadmin**, **admin**, **projectuser1**, **projectuser2**.
10. On **WD-LS2** configure the following shares and rights using SAMBA service:
    a. The name of the usergroup should be **WEBDEMAND.**
    b. Create and share the `/project` and `/www` directories.
    c. User **projectuser1** should be granted full access to `/project`. User **webadmin** should get read-only access.
    d. Only user **webadmin** has access to `/www`, with full rights.
11. Server **WD-LS2** provides internal email for the company users using IMAP and SMTP protocols.
12. For easy access to the company's email install and configure the Squirrelmail web-based client. The application should be accessible on *webmail.webdemand.corp*, only with secured (HTTPS) connection. Use the CA on **WD-LS1** to create certificates.
    The email-address format should be *username@webdemand.corp*. Ensure, that the users on **WD-LS2** (**webadmin, admin, projectuser1, projectuser2**) can email each other using the web-interface. As proof, user **webadmin** should send a short email to all other users.
13. Install Icedove or Thunderbird e-mail client on **WD-PC1** and configure for **projectuser1** to have access to his e-mail box.

14. Ensure that servers **WD-LS1** and **WD-LS2** synchronize their time with the server at IP-address 85.20.12.100, provided by the ISP.