Test Project

ES2014_TP2010_HU

APPENDIX 2.
Description of project and tasks – DAY 2

Submitted by:
Name: Zoltán Sisák
Member Country: Hungary

Table of Content

1. The Surroundings....2
2. Your tasks at Sunshine & More 4
2.1. Network-administrator tasks 4
2.2. Windows tasks 7
2.3. Linux server tasks 9

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. THE SURROUNDINGS

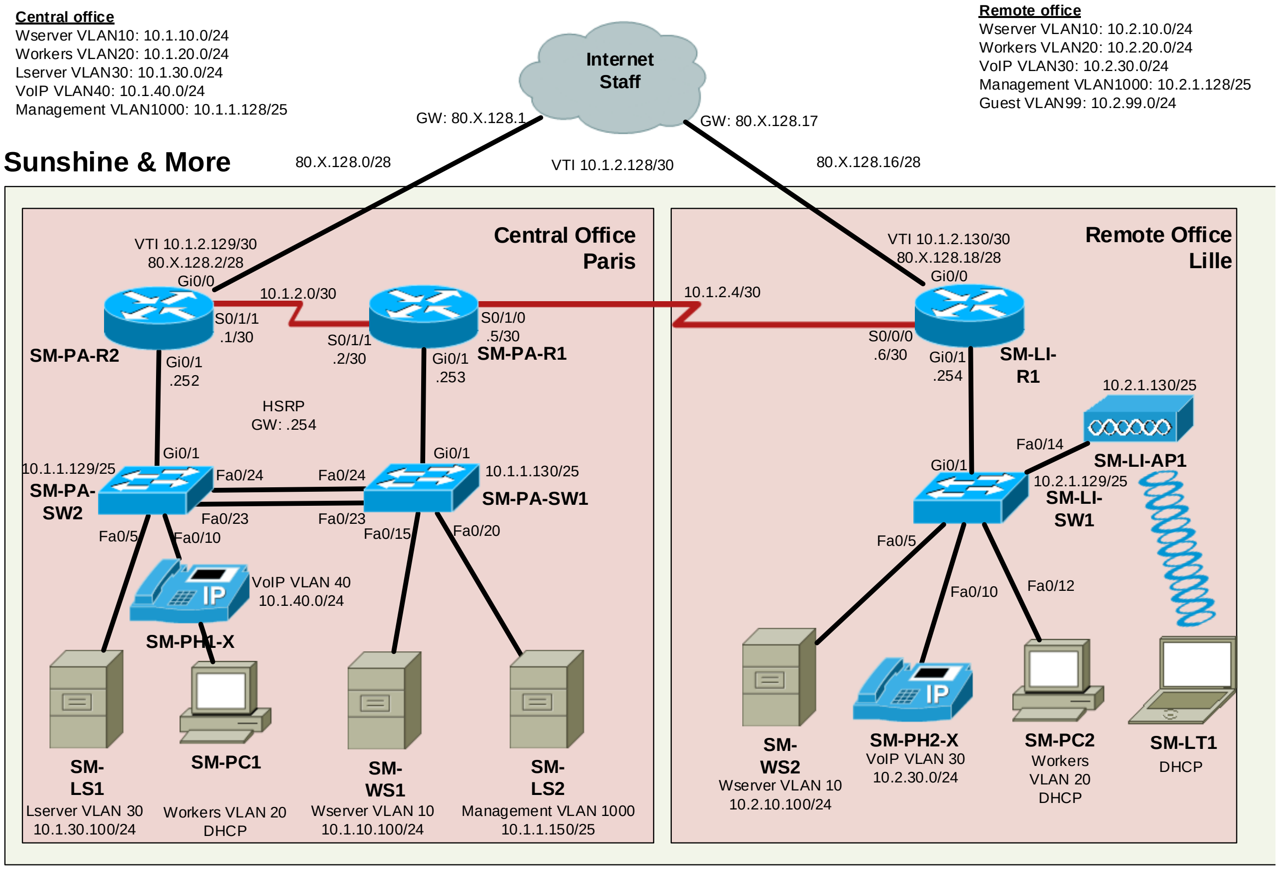
The multinational travel agency 'Sunshine & More' achieved a substantial financial growth in the past year. Management therefore decided to buy 'WebDemand', because this company provides development and operational services, to be able to support the expanding range of tasks. After the acquisition the two separate infrastructures have to be merged, so major changes are required in the infrastructure and implementation of services.

The leaders of 'Sunshine & More' agree that 'Network Solution' will be contracted to implement the reorganization of the IT infrastructure. Since your team built the infrastructure at both companies, the leadership of 'Network Solution' charges your team with the implementation.

During your work, you will have to modify a functioning infrastructure and services according to the new design. The topology of the perfectly configured and running infrastructure, including logical addressing, is described in the diagram.

For the consistent naming procedure of 'Sunshine & More' some devices and servers previously belonged to "WebDemand' should be renamed according to the following table.

Name used previously	New name
WD-PA-R1	SM-PA-R2
WD-PA-SW1	SM-PA-SW2
WD-PC1	SM-PC2
WD-LS1	SM-LS1
WD-LS2	SM-LS2


Central office
Wserver VLAN10: 10.1.10.0/24
Workers VLAN20: 10.1.20.0/24
Lserver VLAN30: 10.1.30.0/24
VoIP VLAN40: 10.1.40.0/24
Management VLAN1000: 10.1.1.128/25
Internet
Staff
Remote office
Wserver VLAN10: 10.2.10.0/24
Workers VLAN20: 10.2.20.0/24
VoIP VLAN30: 10.2.30.0/24
Management VLAN1000: 10.2.1.128/25
Guest VLAN99: 10.2.99.0/24
GW: 80.X.128.1
GW: 80.X.128.17
Sunshine & More
80.X.128.0/28
VTI 10.1.2.128/30
80.X.128.16/28
Central Office
Paris
Remote Office
Lille
VTI 10.1.2.129/30
80.X.128.2/28
Gi0/0
VTI 10.1.2.130/30
80.X.128.18/28
Gi0/0
10.1.2.0/30
10.1.2.4/30
S0/1/1
.1/30
S0/1/1
.2/30
S0/1/0
.5/30
S0/0/0
.6/30
SM-PA-R2
SM-PA-R1
SM-LI-
R1
Gi0/1
.252
Gi0/1
.253
Gi0/1
.254
HSRP
GW: .254
Gi0/1
Gi0/1
Gi0/1
10.1.1.129/25
SM-PA-
SW2
Fa0/24
Fa0/24
10.1.1.130/25
SM-PA-SW1
Fa0/23
Fa0/23
Fa0/5
Fa0/10
Fa0/15
Fa0/20
10.2.1.130/25
Fa0/14
SM-LI-AP1
10.2.1.129/25
SM-LI-
SW1
Fa0/5
Fa0/10
Fa0/12
VoIP VLAN 40
10.1.40.0/24
SM-PH1-X
SM-
LS1
Lserver VLAN 30
10.1.30.100/24
SM-PC1
Workers VLAN 20
DHCP
SM-
WS1
Wserver VLAN 10
10.1.10.100/24
SM-
LS2
Management VLAN 1000
10.1.1.150/25
SM-
WS2
Wserver VLAN 10
10.2.10.100/24
SM-PH2-X
VoIP VLAN 30
10.2.30.0/24
SM-PC2
Workers
VLAN 20
DHCP
SM-LT1
DHCP

2. YOUR TASKS AT SUNSHINE & MORE

2.1. NETWORK ADMINISTRATOR TASKS

1. During migration, configure the devices transferred from 'WebDemand' with the expected settings valid for 'Sunshine & More' topology (hostname, username, domain name: ‘sunshine.local’).
2. The physical infrastructure has to be rebuilt according to the topology on the diagram. According to the new plans, both the central office in Paris as well as the remote office in Lille has their own dedicated internet connection. The dedicated leased line between the two offices still exists and provides the backup connection between the two sites.

SM-PA-SW1	Fa0/1-10	VLAN 20
SM-PA-SW1	Fa0/11-15	VLAN10
SM-PA-SW1	Fa0/20-22	VLAN1000
SM-PA-SW1	Gi0/1	Trunk
SM-PA-SW1	Gi0/2	Disabled
SM-PA-SW2	Fa0/1-5	VLAN30
SM-PA-SW2	Fa0/6-10	VLAN20, VLAN40
SM-PA-SW2	Fa0/11-22	VLAN20
SM-PA-SW2	Gi0/1	Trunk
SM-PA-SW2	Gi0/2	Disabled
SM-LI-SW1	Fa0/1-5	VLAN10
SM-LI-SW1	Fa0/6-10	VLAN20, VLAN30
SM-LI-SW1	Fa0/11-13	VLAN20
SM-LI-SW1	Fa0/14	Trunk
SM-LI-SW1	Fa0/15-24	VLAN20
SM-LI-SW1	Gi0/1	Trunk
SM-LI-SW1	Gi0/2	Disabled

3. The serial line between **SM-PA-R1** and **SM-PA-R2** routers will be replaced for a fiber connection in the future to carry high speed traffic between the central office. At this time this connection serves redundancy only.
4. The primary connection between the central office and the remote office through the internet has to be ensured. To secure this connection, this has to be solved by a permanent site-to-site IPSec VPN with VTI.
5. Configure IP addresses and VLANs on both sites according to the new topology.
6. To increase the security, RADIUS based authentication for console and remote access has to be configured on the network devices. As fallback authentication method, the local database on the devices has to be used. Configure a local **localadmin** user on the devices with maximum rights.
7. Also allow telnet access on the vty lines.

8. Routing should be reconfigured taking into account the following:
   a. Ensure handling of the backup connection between the two sites using routing protocol parameter.
   b. Both offices have own gateway to the internet. Both internet connection should be used as a backup line for the other sites if its connection fails. This should be solved with advertising parameters.
9. In the central office you need to create a redundant default gateway according to the following:
   a. For the clients in the central office, a HSRP standby group connects to each VLAN, with **SM-PA-R2** as primary and **SM-PA-R1** as secondary gateway.
   b. If **SM-PA-R2** or its internet connection fails, **SM-PA-R1** should be the default router, therefore the hosts can still reach the external network. As soon as **SM-PA-R2** works properly again, the active role should return to the normal state.
10. The clients can reach the internet only through a proxy. Traffic from the proxy server's subnet and wireless Guest VLAN 99 goes with NAT to the internet; traffic from other sources should not be translated. Packet with private addresses from the company may not get out.
11. For network monitoring you will have to ensure that time on all devices is synchronized. Exact time is provided by **SM-LS1**.
12. Network monitoring will be done by systems running on Linux-based **SM-LS2**. Ensure that level 0 - 6 messages are forwarded there, and that all network devices can be queried with using network monitoring protocol.
13. The access ports of the switches should activate quickly.
14. According to the security guidelines, the access ports have to be configured to allow only communication from connected devices on the diagram. The switch automatically shuts down the port when any other device connects to it, but enables after 30 seconds.
15. When the broadcast or multicast traffic on the trunk lines between **SM-PA-SW1** and **SM-PA-SW2** more or equal then 10% of the lines' bandwidth, shut down the affected ports, but enables after 30 second.
16. Disable Cisco Discovery Protocol on all access switch ports where it is not necessary.
17. The company management decided to introduce an experimental IP-telephone network. Introduction of VoIP takes place with two phones at the moment with the following configurations:
   a. Configure telephony service on **SM-LI-R1** router.
   b. IP addresses of both phones are served by **SM-WS1.**
   c. The IP phones should be configured according to the following requirements:
      - **SM-PH1-*X***
         - ✓ Configured name: **SM-PH1-*X***.
         - ✓ Phone number: *X*111
         - ✓ Phone line should be assigned to button 1.

- **SM-PH2-*X***
    - ✓ Configured name: **SM-PH2-*X***.
    - ✓ Phone number: *X*112
- Emergency call has to be configured on both phones with number 911. This number has to be forwarded to IPv4 address 85.20.12.99 with codec g711ulaw.

18. Configure two WLANs on **SM-LI-AP1** with the following settings:
    a. SSID: SMWLANCorp*X*; VLAN 20, WPA2-EAP, AD authentication. Authentication must be provided using both domain controllers (SM-WS1 and SM-WS2).
    b. SSID: SMWLANGuest*X*; VLAN 99; Open authentication
    (Use **SM-LT1** laptop for testing purpose.)
19. VLAN 99 will be used as guest VLAN. Only Internet access should be enabled for this VLAN. Assigned access port on SM-LI-SW1: Fa0/15.

2.2. WINDOWS TASKS

1. The resolution of DNS requests from the Windows AD-Clients that cannot be resolved locally should be handled by the DNS server on **SM-LS1.**
2. For reasons of security, passwords in the windows domain should be complex, the previous six passwords should be stored, and all users must modify their password every 30 days.
3. Create new DHCP scopes for the VoIP VLANs. Exclude the first 10 IP and last 4 usable addresses.
4. Because of the modified network surroundings, set the NTP source to the proper local time-server on both Windows Servers.
5. Also, solve with group policy that the domain computers can reach the internet with IE through the company's proxy server.
6. Configure quota and file-filtering settings on **SM-WS1** according to the following requirements:
    a. Prepare a quota-profile which applies a 100MB hard quota, and two levels of notification exclusively into the event log. Level 1: 80% and level 2: 95%.
    b. Quota should be applied to all subdirectories in the home-directory.
    c. Prepare a hard file-filter profile, preventing copying of .exe files and results in a warning into the event log.
    d. Filtering should be applied to all subdirectories in the home-directory.
7. To provide data collection solution between the central and remote offices, you have to execute the following steps:
    a. Create a directory `ReceivedData` on the system disk of server **SM-WS1**, and a directory `Distribution` on the system disk of server **SM-WS2.**
    b. Copy the contents of directory `C:\Windows\AppPatch` to `Distribution` on **SM-WS2**.
    c. Prevent the replication of files with .torrent extension.
    d. Replication group name should be **SM-WS2-WS1**
    e. Replication should take place from the designated folder on the remote office server to the designated folder on the central server.
    f. After the first replication, configure timing for data transfer to take place every weekday between 4 PM and 4 AM only, but using full bandwidth.
8. To support secure operation of applications, use the possibilities of the PKI (Public Key Infrastructure) technologies.
    a. Use **SM-WS1** as Certificate Authority.
    b. The same computer should have a web server with a private key based certificate.

9. To make the applications widely available, use the advantages of Windows Server 2012 R2 terminal services on **SM-WS1**.
    a. All domain users should be able to use terminal services.
    b. Publish Paint, WordPad and Calculator as RemoteApp.
    c. The applications should also be accessible through the Web Access portal with SSL.
    d. Enable and configure SSO (single-sign-on). An AD user already logged in the computer should be able to connect with Remote Desktop Connection to the **SM-WS1** server or start any published application without further authentication or warning message.
    e. The default page of Internet Explorer should be *https://sm-ws1.sunshine.local/rdweb* on every domain computer.

2.3. LINUX SERVER TASKS

During the integration, WebDemand's Linux servers were renamed and reinstalled. Primary tasks of the servers will be to provide web-access and network management services.
During the competition you have to use two new virtual machines on **Host-L** called **SM-LS1** and **SM-LS2**. On both servers a basic Debian system is pre-installed. The task is to configure the network and the services on the servers. On both servers you can use the root or smadmin users.

1. Confirm the company's security policy ensuring that each Linux server can only accessed remotely by SSH on port 2222. Remote **root** login has to be prohibited.
2. Add **smadmin** to the root group. *su* command is permitted only for the members of the root group.
3. Create **ciscoadmin1**, **ciscoadmin2**, **script** system users on both Linux servers.
4. Management of 'Network Solution' decided, that computers can access the internet (http and https traffic) only through a central proxy server. For this purpose you will have to install and configure proxy service on **SM-LS1** as follows:
   a. The proxy serves must not be used from the VoIP VLAN.
   b. The proxy service should listen on port 9090, users should be authenticated using the Active Directory database.
5. One more task of **SM-LS1** is to forward internet DNS queries to the ISP DNS server at IP-address 85.20.12.100.
6. To provide unified time for network management services, **SM-LS1** serves the time reference (NTP) in the network. Exact time is retrieved from the ISP NTP server at IP-address 85.20.12.100.
7. **SM-LS2** provides AAA services for the network devices. From the previously defined Linux system accounts only **ciscoadmin1**, **ciscoadmin2** and **script** should be able to logon to the devices. The users should receive level 15 privilege after logon.
8. You have to ensure that all log messages sent by the Cisco network devices and Linux servers are received and stored by the syslog server on **SM-LS2.**
   a. The log messages should be stored in the `/logs` directory, in a separate file for each device or server. For example, messages coming from device **SM-PA-R1** should appear in file `/logs/SM-PA-R1`.
   b. Every other message arriving with local7 facility should go to file `othercisco.log`.
   c. Send authentication log from **SM-LS1** to **SM-LS2**.
   d. Use logrotate rules to start with an empty `othercisco.log` when the file size exceeded 1KByte. Schedule logrotate to run in every 5 minutes. Maximum 3 versions should be kept.
9. Send an e-mail to **smadmin** on **SM-LS2**, when **SM-PA-R1** becomes the active gateway instead of **SM-PA-R2**.

10. Management would like to monitor continuously the network resources and servers. On server **SM-LS2** install Nagios system. The service should be accessible on *http://sm-ls2.sunshine.local/nagios3* URL. Rename Nagios administrator user from **nagiosadmin** to **esadmin.** Make sure that **esadmin** has access to the web interface.
    The system has to provide the following functionality:
    a. Resource-groups should be created with the following names: *Routers*, *Switches, Servers, Access Points.*
    b. All the network devices should be added to their respective groups.
    c. The system should monitor accessibility of the network devices.
    d. Nagios should build a connection map (network diagram, device dependencies).
    e. Monitor the accessibility of the servers and status of the installed HTTP and SSH services on all Linux and Windows servers. Furthermore, CPU and RAM load should be monitored.
    f. Devices on the network map should appear with their appropriate images.

11. For graphing network traffic and CPU load install Cacti on server **SM-LS2** with the following settings:
    a. After installation delete user **guest** and create a new user **esadmin**. Assign the same rights to **esadmin** than **admin** has**.**
    b. Add all network equipment with the following settings:
        - ***Description***: hostname of the device.
        - ***Hostname***: IP address of the device.
        - Device accessibility should be checked with PING/ICMP.
        - Use of SNMPv2c is compulsory.
        - The SNMP read only community should be: **es2014community**.
    c. Gather statistics on all interfaces which is in up state.
    d. Monitor CPU load on each device.
    e. Graphics for CPU and interface statistics have to be presented taking into account the following:
        - Graphics should be organized under the `SunshineAndMore` tree.
        - Every device should be presented in its own branch of the tree.
    f. For all devices the CPU load graphic should be sized 200x700.

12. Install TFTP service and create scripts for saving the configuration of switches and routers.
    a. Install TFTP service on SM-LS2. The TFTP server should use `/tftpboot` directory.
    b. Create /tftpboot/backup folder. Backup of the actual config files must be stored using the following name format: <Device_Name>-YY-MM-DD-hh-mm.tar.gz. (E.g. SM-PA-R1-14-10-03-14-15.tar.gz)
    c. The scripts should be located in the `/script` directory.
    d. Create a script under the name `savecfg.` The function of the `savecfg` script is to login to the network device with **script** user, copy running-config to the TFTP server. The device IP address and the file name has to be specified in the script parameter list according to the following example*: ./savecfg 10.1.1.252 sm-pa-r1*
    e. Create a script under the name `backupconf.` The function of the `backupconf` script is to create backup of the configuration of all devices. This script will call `savecfg` script.
    f. Schedule the `backupconf` script to run in every 10 minutes.
13. Create DHCP pool for VLAN 99 on **SM-LS1** with the following requirements.
    a. Exclude the first 10 addresses.
    b. DNS server: 85.20.12.100
14. Synchronize the time on **SM-PC2** using the **SM-LS1** server.