Sun & Wind

"Office ICT Team" test project

v.1.4 EN (2008.09.16)

Scenario:

1. The company named "Sun & Wind" is a multinational manufacturer of equipment for exploitation of renewable energy sources, intended for home use. The central office, and until now the only office, is located in Luzern, Switzerland. To expand its operations in Europe, new offices will be opened in ten countries across western and central Europe. Your team has been charged with planning and implementing the ICT system of your national office, according to the guidelines provided by the central office, as well as the initial start of the business process.

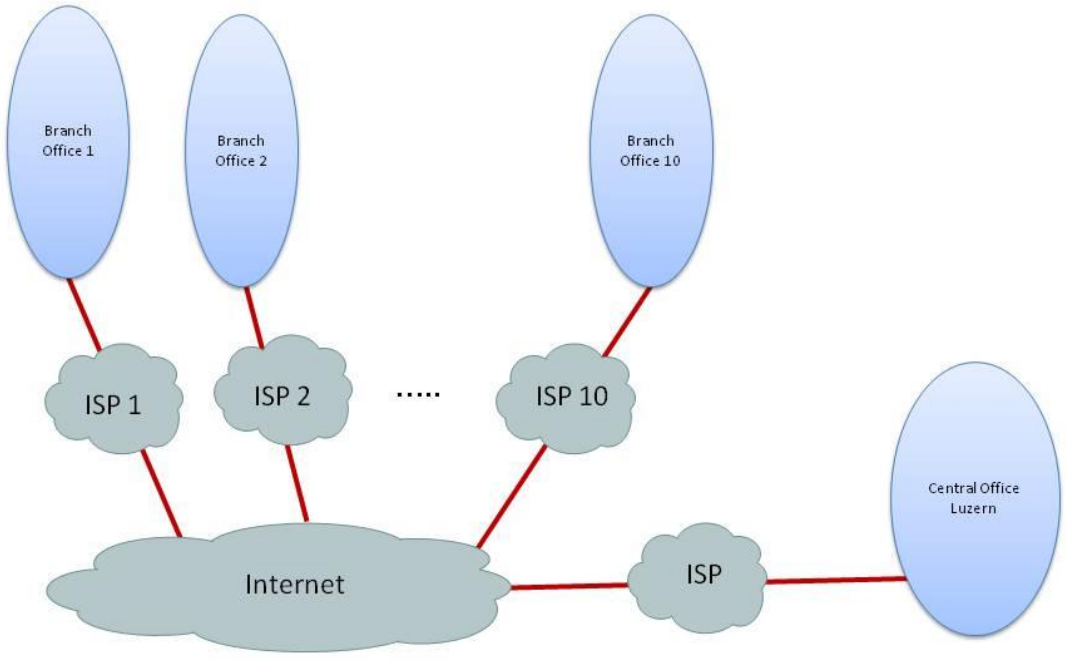
   Economical factors are very important to the company, therefore the branch offices should connect to the central office in such a way, that no structural changes will be needed in Luzern.

   To implement the network, each branch office will receive an identical set of equipment. All the computers are an integral part of the branch office's infrastructure. The operating system may not be changed, and all equipment provided must be used.

   The equipment supplied consists of:

   a. 1 Dell Vostro with Windows Server 2003
   b. 1 Dell Vostro for Linux server
   c. 3 Workstations with Windows XP for documenting and configuration
   d. 1 Laptop with Windows XP for the project manager
   e. 2 Cisco Catalyst 2950/2960 switches
   f. 2 Cisco 2801 routers

g. 1 Cisco Aironet access point
h. 50 meters of UTP cat5 patch cable and RJ45 connectors
i. Crimping and cable testing tools
j. A multi-function printer
k. At least 2 headsets with microphone
l. All needed software:
    i. Windows Server 2003 R2 CD-set
    ii. Exchange 2003 CD-set
    iii. Office 2007 Professional CD-set
    iv. Open Office
    v. MS Project
    vi. Visio + Cisco Icon Library
    vii. Linux distributions (OpenSuSe, Debian, CentOS and Ubuntu)
    viii. Additional materials will be available on CD, or downloadable from the Luzern server (Drupal 6.x + modules, Flash Operator, WSUS, GPMC, Zoiper, KIAX, pictures and descriptions for product catalog etc.), as well as a .CSV file with user data for your branch office.



2. Each branch office is connected to the internet via their local ISP with a high-speed (100 Mbit/s) internet connection. For the duration of the contest, this internet connection will be emulated by an UTP cable to each team's site. The branch office IP-networks are defined in Annex I. The network at the branch office should be built according to the organizational structure of the main office, and all security aspects of the entire company should be taken into account. Access should be provided for the following organizational units:
    a. Company management
    b. Business Administration
    c. ICT system management
    d. Sales and marketing

    The organizational units are spread over one building. The offices are located at both sides of a staircase. In this staircase, because of monument protection, only one thin cable gutter can be installed, which can take 2 UTP cables. Between the two parts of the building the highest possible level of the bandwidth and reliability is expected. In the hall of the building a permanent workstation for demonstration purposes will be installed, for which a copper wire connection cannot be provided. In the offices, for the moment only company management will use mobile equipment, for this suitable network access has to be provided. Only management and the demonstration workstation should be allowed to use the wireless network using WPA. Furthermore, the radio power of the AP has to be set to the lowest level, and the SSID must be hidden.

    For reasons of transparency, unity, central management and simplicity, the domain of the branch office will be independent from the existing domain at the central office, with a domain name of xyz.sunandwind.eu (see Annex I for naming). The basis of the ICT services in the branch office will be the local Windows 2003 R2 server. This server will be domain controller and file-server; the Windows clients will use these resources as domain members. Within the internal network all workstations will be served by a local DHCP server for correct IP configuration, name resolution for the own domain will be provided by a local DNS server, the windows DNS server at Luzern will resolve all other addresses. For email, task and calendar services a local Exchange server and Outlook 2007 and/or Outlook Web Access will be used. For secure operation of OWA, a local certificate server at your branch office will provide the certificate. To increase the

security level of the workstations, the introduction of a patch management system (WSUS 3 SP1) will be needed, which will operate autonomously, but connects to the WSUS server in the central office for downloading of patches. Workstations should receive WSUS settings using GPO.

To ensure secure communication between the branch offices and the main office, an IPSEC VPN will be implemented. However, the dedicated equipment for this has not arrived yet. Therefore a temporary VPN solution will be provided with the available Cisco routers. The ICT team at the central office sent a sample configuration, which you'll find in Annex II. Within this private company network your local net should be routed with OSPF area 1.

Taking into consideration the economical aspects, further network services have to be implemented with free software. The company at the moment cannot provide a dedicated server for these purposes, so one of the workstations has to be used for these tasks. This server will provide external DNS services, operate the IP telephone center and will host a Content Management System. Most of these services will be accessible from the internet, so this server will be placed in the DMZ.

3. With regard to the local network and internet access, the following security aspects have to be taken into account:

   Between the units, and to the internet, only the following types of traffic will be allowed:

   i. Each organizational unit should be able to reach the internet, but workstations by default will only have web-access.
   ii. All equipment should be configured with basic security
   iii. The services on the Linux-server should be available to every unit.
   iv. For company management and system management there is no internet limitation.
   v. Each organizational unit should have access to the Windows Server 2003, which will be operated in the system management unit. Otherwise, no traffic is allowed between organizational units. Should you need to make exceptions because of the structure of the network, then this should be explained and documented in detail for the IT audit team.
   vi. To provide secure communications, using the services of the Windows Server 2003, a server certificate (PKI system) will be needed.

vii. To increase the security level of the workstations, a patch management system (WSUS 3 SP1) will be needed.

4. To keep operational expenses low, the company implements an IP-telephone system for internal and external phone-calls. At the central office there is a server operating as IPT-proxy, in the branch offices the before mentioned server will operate as telephone center. The procurement of IP-telephones has been delayed, so during the transition period soft phones with headset will provide the necessary services. Each workstation should be able to handle IP-phone calls.

   The correct operation of telephone system can be tested by calling a phone installed at the central office. To maintain a unified software infrastructure, an Asterisk PBX should be installed at the branch offices; concerning soft phones an IAX-client is suggested. The local system has to support IAX only for the moment, SIP will not be needed. The central system has been configured such, that the local systems can be connected using number-based trunking. The phone numbers within the company consist of 5 numbers, and start with a 9. The following two numbers indicate the branch office, see Annex I for details. The remaining 2 numbers can be freely used within the branch office.

Your tasks:

1. Create a plan of work (consisting of a functional design, a technical design and a time schedule) for the two days of the competition. This should contain activities of individual team members as well as activities of the team as a whole.
2. Design the company's network according to the specifications given. The design should contain logical diagrams, IP addressing scheme and the running network services.
3. Build the physical layer of the network. Missing cables you should build yourself with the available materials. All network equipment provided should be used. Install wireless access as specified.
4. Label all workstations according to their role in the network, and put one into each Organizational Unit.
5. Install and configure the network according to the specifications, including configuration of the routers and switches, and installation of the servers and the services running on them. When configuring the network, take into account the security guidelines. After finishing your work, the mother company will hold an IT audit, where they will assess the quality of the implementation and the application of security guidelines.
6. Install and configure the internal server's operating system, TCP/IP settings and name. Install according to specifications the domain controller functions and the desired network services. Create user directories, login scripts, and define domain DFS, file quota and file screening.

   Create the necessary users, groups and organizational units. You will receive a .csv file with names, roles and unit of all workers. They should all be able to logon to the domain, and have an Exchange mailbox. Workstations should be joined to the domain.

   Create and configure group policies for logging, password and lockout, Desktop/Control Panel limitations, IE settings, folder redirection.
7. Install Exchange server, create mailboxes and distribution groups, and install according to specifications secure OWA access.
8. Install and configure a local patch management system, connect it to the central server and configure the XP clients to immediately install patches from the local server.
9. Install name resolution of the xyz.sunandwind.eu domain for the outside world. At least you should resolve public services like www.xyz.sunandwind.eu.
10. Install the IP-telephone system for the branch office. In addition to the basic services, voicemail should automatically function outside business hours (18:00h – 9:00h). On the workstation of the secretary there will be a console, which provides monitoring of free,

occupied and not-logged-on extensions. For this purpose the central system manager suggests Asterisk Flash Operator panel (http://www.asternic.org).

11. The unified image of the company should also appear on the public web-page of the branch office. For this, the mother company supplied a pre-defined theme for the Drupal Content management System. Install and apply this theme, and define different level of users in the CMS.
12. For introduction of the company on the local market, a company portfolio has to be created. For this product descriptions a pictures are available on the central server. Create a brochure introducing the company, promotional slides (at least 3) for an advertisement kiosk, and a simple web site. This web site has to be created within the CMS, using the predefined company theme.
13. At the end of the competition, detailed documentation should be completed about your work. Besides, in a 10 minute presentation you should show the work you have done during the competition.
14. If the team has any questions, the project manager should contact the CEO of the company (the chief Expert)

Submitted by:
Name: Zoltán Sisák, Marcel Dormanns, Zsolt Nagy
Member Country: HU

Annex I – Naming and IP-addressing

		IP Addresses							
Location	**Subdomain**	**Local net**	**Public net**	**ISP Gateway**	**Local tunnel net**	**Windows Server**	**Asterisk server**	**Tunnel endpoint**	**Internal IPT #**
Luzern		192.168.0.0	200.8.9.48			192.168.0.2	200.8.9.51	200.8.9.50	900xx
Amsterdam	NL	192.168.1.0	200.8.9.64	200.8.9.1	192.168.255.2	192.168.1.2	200.8.9.67	200.8.9.66	901xx
Budapest	HU	192.168.2.0	200.8.9.80	200.8.9.5	192.168.255.6	192.168.2.2	200.8.9.83	200.8.9.82	902xx
London	GB	192.168.3.0	200.8.9.96	200.8.9.9	192.168.255.10	192.168.3.2	200.8.9.99	200.8.9.98	903xx
Brussels	BE	192.168.4.0	200.8.9.112	200.8.9.13	192.168.255.14	192.168.4.2	200.8.9.115	200.8.9.114	904xx
Helsinki	FI	192.168.5.0	200.8.9.128	200.8.9.17	192.168.255.18	192.168.5.2	200.8.9.131	200.8.9.130	905xx
Prague	CZ	192.168.6.0	200.8.9.144	200.8.9.21	192.168.255.22	192.168.6.2	200.8.9.147	200.8.9.146	906xx
Ljubljana	SI	192.168.7.0	200.8.9.160	200.8.9.25	192.168.255.26	192.168.7.2	200.8.9.163	200.8.9.162	907xx
Ankara	TR	192.168.8.0	200.8.9.176	200.8.9.29	192.168.255.30	192.168.8.2	200.8.9.179	200.8.9.178	908xx
Bratislava	SK	192.168.9.0	200.8.9.192	200.8.9.33	192.168.255.34	192.168.9.2	200.8.9.195	200.8.9.194	909xx
Berlin	DE	192.168.10.0	200.8.9.208	200.8.9.37	192.168.255.38	192.168.10.2	200.8.9.211	200.8.9.210	910xx

Annex II – Sample 'Poor man's VPN' (IP-addresses are illustration only)


```
!VPN tunnel central
interface Tunnel0
 ip address 192.168.255.1 255.255.255.252
 tunnel source 200.201.202.1
 tunnel destination 200.201.202.46
!
interface FastEthernet0/0
 ip address 192.168.0.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 200.201.202.1 255.255.255.252
!


! VPN tunnel branch-office
interface Tunnel0
 ip address 192.168.255.2 255.255.255.252
 tunnel source 200.201.202.46
 tunnel destination 200.201.202.1
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 200.201.202.46 255.255.255.240
!
```