# Test Project Proposal – Island/Day 4
**TP39_40CA_EN**

Submitted by:
Name: Kelvin Ng
Member Country: SG


WorldSkills International Secretariat
Keizersgracht 62-64, 1015 CS Amsterdam, The Netherlands
www.worldskills.org, Tel: +31 23 5311071, Fax: +31 23 5310816

## CONTENTS

This Test Project proposal consists of the following document/file:
1. TP39_40CA_DAY4_EN.doc

## INTRODUCTION

The competition has a fixed start and finish time. You must decide how best divide your time. All hardware will be rebooted before marking is started. You may choose any package for implementation of the services. Wherever possible, we will test only on the functionality of the requirements followed by coding if it is not possible.

**You are strongly advised to continually save your work/setup/configuration as you progress.**

## DESCRIPTION OF PROJECT AND TASKS

A multi-national financial company, Todayworks Inc has recently completed a business merger and would like to re-set up a new network to integrate their operations in China to support their businesses in the Asia Pacific region. You are a network engineer hired by Todayworks Inc to implement this project.

After investing in the appropriate network and security equipment, servers, notebooks, PC and wireless access point. The company has assigned you to design, setup, configure and secure all the network installation and resources to support the new integrated businesses in Asia Pacific. The network topology is given by the CIO as shown below in Figure 1.

You are to provide a proof of concept (POC) to the management to show that the design in Figure 1 will work based under the conditions stated below. Base on the logical network diagram given in Figure 1, you will need to work out appropriate sub-network addresses, IP addresses to all network interfaces, connected switch port numbers and VLAN assignment and any statically assigned IP addresses.

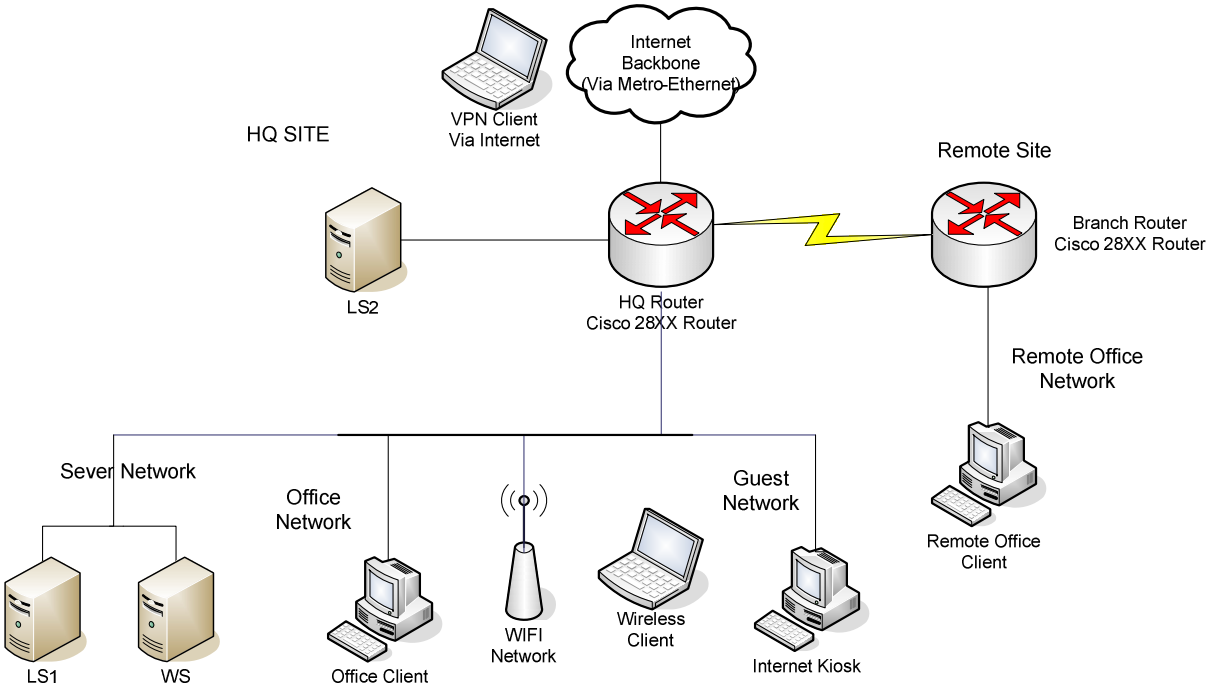


Figure 1. Logical Network Diagram

Note: LS1, WS , Office Client and Internet Kiosk are 4 virtual machines on the same PC hardware. Clients in Remote Office Network, wireless client and VPN Client is to be simulated using the Notebook.

All PCs are preinstalled with either Debian Linux 5.0, Windows 2008 Server or Windows Vista. The relevant files, software and ISOs are provided in C:\software or /software in the respective PCs. You are to mount or map the respective ISOs to install additional packages or services. You are to configure and secure the network based on the following requirements:

1. Debian Linux 5.0 was pre-installed on LS1 and LS2 with the root password of *pass123* and MS Windows Server 2008 was pre-installed on WS with the administrator password of *pass123*. The notebook has been preinstalled with Windows Vista and the administrator password is set to *pass123*. You should use the notebook as a client to test internal wireless connectivity, external VPN network connectivity and remote Office Network client connectivity. For the different connectivity tests, the notebook should be automatically assigned an IP address by the DHCP server.

2. The company office premises are located at two sites and you need to ensure they communicate securely. Your first task is to devise an IP addressing scheme for the public and private network using VLSM. The ISP has assigned a public IP network address of 200.10.10.0/24 and a domain name of Todayworks.com. The public IP network addresses are to be used for the remote site IP assignment and Internet connectivity. In addition, the company has decided to use a class C private IP address of 192.168.0.0/24 for the HQ site networks. You are to configure NAT at HQ Router.

3. The company has a total of **50 users in Office network (192.168.0.0/26)** in the HQ site and intends to setup a total of **5 servers in DMZ zone (192.168.0.120/29)** and **10 servers in Server Network (192.168.0.96/28)** zone. The **WIFI network (192.168.0.64/27)** must also cater for another **20 users**. The **Guest network (192.168.0.112/29)** will housed another **5 PCs to allow visitors** to surf the Internet. You are to **reserve 6 VPN IP (192.168.0.136/29)** addresses for the VPN remote clients accessing via the Internet. There is another **30 users in the remote office network (200.10.10.0/27)**. The IP addresses for the LS1, WS and LS2 servers are **192.168.0.98, 192.168.0.99 and 192.168.0.122** respectively. The IP address to be used for static translation for the LS2 server in DMZ is **200.10.10.35**. When assigning IP addresses, you are to start with the lowest IP address (in the ascending order) beginning with network equipment first. (E.g. you would assign the IP addresses first to the routers/switches/firewall router/AP followed by servers/computers). The switch is to be used for the internal network connections (Server network, Office network, WIFI network and guest network in the HQ site). You are to assign **2 switch ports each** for the Server, Office, WIFI and Guest networks. See Annex 1 for detailed switch connection.

4. You are to configure OSPF area 0 with message-digest of *ospfsecret* for the serial connections between HQ and remote routers. Do not define any static or default route on HQ and Remote routers. The serial link between BR and RR is a 128000 bps Point to Point Link that you subscribe from a service provider. You are to use the password *pppsecret* to configure this link authentication. The company wants to have some security on this serial link, so that the hacker would not be able to sniff the authentication password sent by the routers. The password to be used for all network devices' privilege access is "*pass123*".

5. The routers and the switch should be first authenticated with AAA using Radius server and only accounts in Annex 2 is to be used for the authentication process, via console login. In the event of authentication server being unavailable, you are to authenticate using the local username localAAA and password *pass123*. Configure the switch so that the users in Annex2 are granted a few privilege commands as defined in Annex 3. Only SSH traffic for remote administration are allowed. .

6. You are to configure LS1 as a TFTP and NTP server. All internal network equipment (Routers and Switches) are to be synchronized to LS1 master timeserver. The TFTP server should hold the IOS image for the HQ router and the router must boot from its IOS from this TFTP server.

7. The wireless Access Point (AP) must be configured to support WPA with PEAP authentication via RADIUS. Configure the SSID as SowiseX where X is your workstation number. You are to configure the AP to allow only authorized wireless clients to access to the network. Authorization is based on MAC addresses. Only the notebook provided can connect to the AP. For security reasons, you are to configure 802.1x port-based authentication on the switch using PEAP authentication via RADIUS for all client computers connected to Office network. The Fast Ethernet ports on the switch connecting to the office network should also secure the office PC so that only one MAC address is allowed on a port and shutting down that switch port if another MAC address attempts to communicate via the port. WS server is also a Windows 2008 Network Policy Server (NPS) to ensure that the clients in the internal network and remote office have their anti-virus enabled before they are connected to the network. The NPS will also act as the Radius Server.

8. As the company internal network contains highly confidential information, you must ensure it is protected and no outside traffic is allowed to access the network. You need to configure a zone-based firewall (ZBF) on the HQ Router as shown in Annex 4. Create policies to allow traffic from higher security zone to access to lower security zones. In addition, you are to specify a policy map that performs URI inspection to block download of executable files with extension exe and com. You also need to ensure

incoming traffic from the internet is restricted to the LS2 server' ports which are having running services. The LS2 server must be accessible from the Internet using a static translation.

9. Install and configure an internal DNS service on LS1 and WS, LS1 being the main and WS being the backup, to serve all the translations of internal network resources. The client will automatically register their name with the DNS servers after they have been assigned with an IP address by the DHCP server in LS1. In addition, install and configure a public DNS service on LS2 to serve the internet query of the internet accessible services.

10. Install and configure a transparent proxy server to cache all web traffic to improve the entire network performance. All internal web accesses will bypass the proxy.

11. All the client machines in both sites are expected to login via the WS server. The users are to login to the network using the accounts found in Annex 4. Their home drive which is stored in LS1 will be automatically mapped to drive Z, using their authenticated credential. For the Internet Kiosk users in the Guest Network with guest account, users can only do internet browsing via the proxy server, LS2. Disable the following functions: Run command, Task Manager, Change Password, Shutdown PC, Command Prompt and Lock Computer on the Internet Kiosk.

12. The company website, http://www.todayworks.com, consists of static pages that stored locally in LS2. Create a simple Welcome page.

13. An IPSec tunnel must be built between the two sites. This tunnel must be created between the HQ Router and the Branch Router using a pre-shared key *"pass123* ". Ensure that the office users from both sites are able to access each other networks and the services hosted in DMZ. All packets coming from the remote site's internal network to the HQ site's internal network (and vice-versa) must be sent through the tunnel.

14. The company also wants to provide the facility of remote VPN for the office users. Configure the HQ router as a remote access VPN gateway using L2TP/IPSEC with CHAP/MS-CHAP2. You are to assign IP addresses from VPN subnet to the authenticated clients. The clients have to be authenticated using certificates with user accounts from the RADIUS server in the domain. You can use the certificate services from Microsoft or Linux.

15. You have to configure the notebook to have a VPN connection to the HQ Router using Windows Vista default VPN client. Create a shortcut to this connection named VPN on the desktop of the local administrator. For testing purposes, you are to configure a DHCP server on HQ router interface connected to the notebook. Use 200.1.1.0/24 subnet for this purpose. You are to enable the http service on HQ router for testing purposes.

## ENSURE ALL CONFIGURATIONS ARE SAVED BEFORE YOU LEAVE YOUR STATION. ALL MACHINES WILL BE REBOOTED BEFORE MARKING STARTS.

**Remember to save the configuration of all network devices and reboot your network devices and PCs before you complete your project.**

**Annex 1: 12 Ports Switch Connections**

| Switch Port | Connects to |
|---|---|
| 1 | HQ Router |
| 2, 3 | Server network |
| 4, 5 | Office network |
| 6, 7 | WIFI network |
| 8, 9 | Guest network |

**Annex 2: User Accounts for AAA authentication**

| Username | Privilege Level (for Switch only) | Password |
|---|---|---|
| Viewer | 5 | *pass123* |
| Admin | 15 | *pass123* |

**Annex 3: Privilege Level and associated commands**

| Privilege Level | Commands |
|---|---|
| 5 | dir<br>test<br>verify |

**Annex 4: Zones for Zone Based Firewall**

| Zone | Network | Security Level |
|---|---|---|
| Internal | Office, WIFI, Server, Remote Office | Highest |
| DMZ | DMZ | Medium |
| Guest | Guest | Low |
| Outside | Internet | Lowest |

**Annex 5: User Accounts to be created in Windows 2008 Server and LS2 server**

| Username | OU | Password |
|---|---|---|
| Mary, Peter, Richard | Operation | *pass123* |
| Guest | Guest | *pass123* |

**END OF PROJECT**

**REMINDER**

Save your work!
All hardware will be rebooted before marking is started.