

# **Day 4**

## **IT Network Systems Administration – Trade 39**

**WSC 2011 London**

## Overview

1	EXAM .....	3
1.1	CONTENTS .....	3
1.2	INTRODUCTION .....	3
1.3	DESCRIPTION OF PROJECT AND TASKS .....	3
1.4	NETWORK DIAGRAM .....	4
1.5	PART 1 .....	5
1.6	PART 2 .....	6
1.7	PART 3 .....	7
2	APPENDIX .....	8
2.1	Specifications .....	8
2.1.1	WINDOWS SERVER SPECIFICATIONS .....	8
2.1.2	DOMAIN GROUP/OU LIST (CREATE OU AND GROUP!) .....	8
2.1.3	DOMAIN USERLIST .....	8
2.1.4	GPOs .....	9
2.1.5	LINUX SERVER SPECIFICATIONS .....	9
2.1.6	NOTEBOOK SPECIFICATIONS .....	9
2.1.7	MONITOR STATION SPECIFICATIONS .....	9
2.1.8	INTERNET SERVER SPECIFICATIONS (FOR TESTING) .....	9
2.1.9	NETWORK SPECIFICATIONS .....	9
2.1.10	WIRELESS NETWORK SPECIFICATIONS .....	10
2.1.11	VMWARE VIRTUAL MACHINE SPECIFICATIONS .....	11
2.2	INSTRUCTIONS .....	12
2.2.1	INSTRUCTIONS TO THE COMPETITOR .....	12
2.2.2	EQUIPMENT, MACHINERY, INSTALLATIONS AND MATERIALS REQUIRED .....	12

# 1 EXAM

## 1.1 CONTENTS

This Test Project proposal consists of the following document/file:

1. TP39\_day4-v2.65

## 1.2 INTRODUCTION

The competition has a fixed start and finish time. You must decide how to best divide your time.

## 1.3 DESCRIPTION OF PROJECT AND TASKS

„Moneystor“ has concerns about the security in their network, so they employ you to analyze the network . You found several security issues and decided to recreate the whole network. The aim of the project is to deploy a high secure network infrastructure with monitor capabilities.

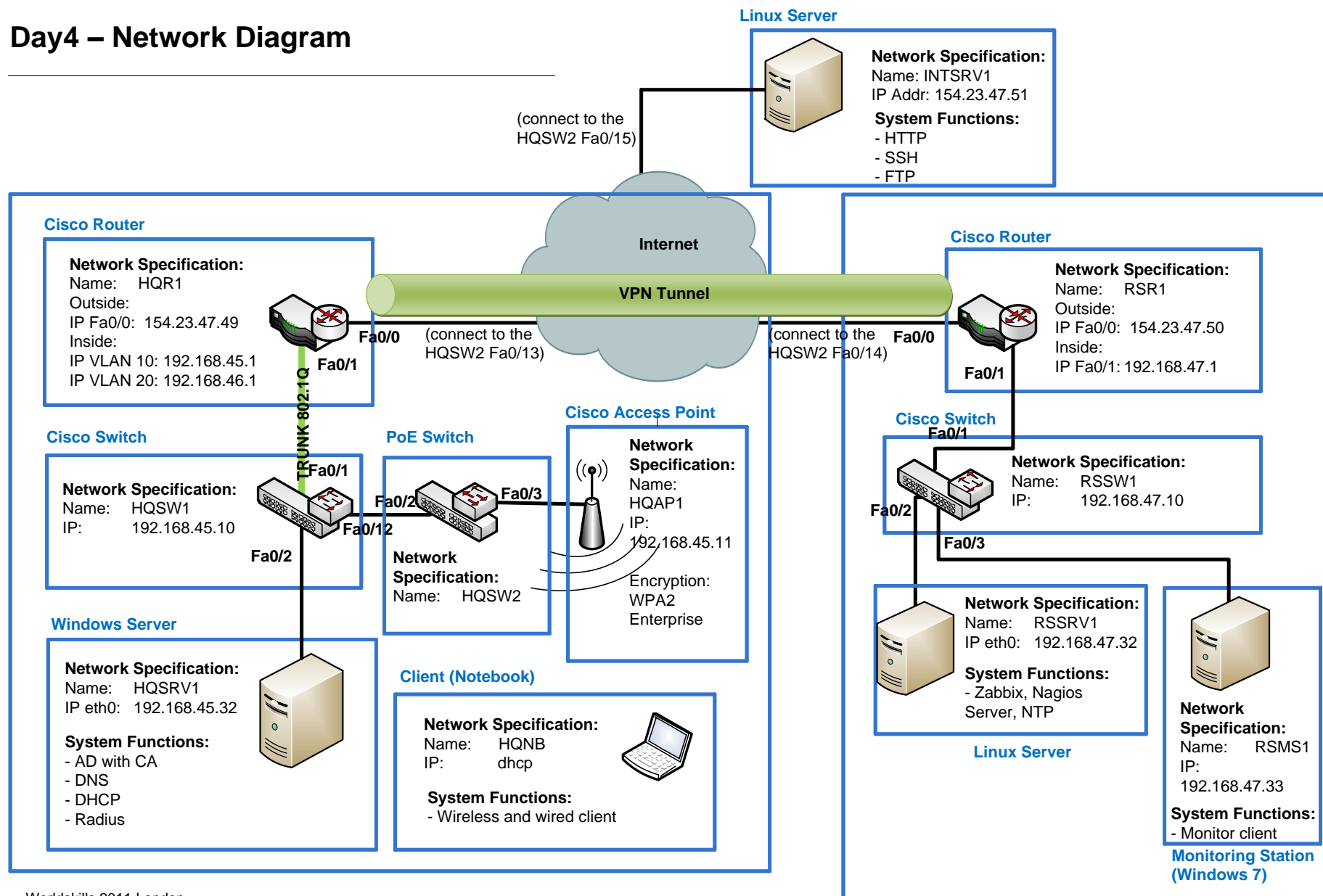
The company is divided in two sites. The HQ site, where the main server is homed and the clients connect to and the remote site with the monitor server. The sites are connected with a strong IPSEC VPN authenticated by certificates. You'll find additional information in the attachment.

### Important Notes:

1. *The HQSW2 switch will be used for two purposes. The Fa0/2-12 port range will be used to connect PoE enabled devices to the network. (In this arrangement HQAP1 wireless access point is the only PoE device). The other FastEthernet ports simulate the Internet cloud. You must not change HQSW2 switch configuration.*
2. *INTSRV1 server is for only testing purpose and it is situated in the Internet cloud. You can reach several services on it. You need only to configure the IP settings. See the appendix for the details.*
3. *Please configure and setup VmWare virtual machines according to the information in the appendix.*

## 1.4 NETWORK DIAGRAM

## Day4 – Network Diagram



## 1.5 PART 1

### Work Task Windows Server (HQSRV1)

Note: Please use the default configuration if you are not given the details.

- Please configure the server with the settings specified in the appendix
- Install the services
  - Configure Active Directory
    - Create the Active Directory accounts with the information from appendix
    - Create a certification authority which provides certificates for the IPSEC VPN connection
    - Create OUs and groups listed in the appendix
    - Create users listed in the appendix
    - Enable GPOs specified in the appendix
  - DNS
    - Create a reverse zone for 192.168.47.0 network with PTR record for RSSRV1 Linux server
    - Create an A record for the RSSRV1 Linux server with its local IP address
  - DHCP Server
    - Range:
      - 192.168.45.100-192.168.45.254
      - 192.168.46.100-192.168.46.254
    - Add default gateway and DNS server options
  - Network Policy and Access Services
    - Enable Network Policy and Access Services to provide Radius service for the wireless clients' authentication and for AAA authentication on the HQR1 router
    - The shared secret key must be London2011 for the Radius server.

### Work Task Linux Server (RSSRV1)

Note: Please use the default configuration if you are not given the details.

- Please configure the server with the settings specified in the appendix
- Install the services
  - NAGIOS
    - Install NAGIOS
    - Change NAGIOS admin user to „admin“ and password to „London2011“
    - Add RSR1 router to the NAGIOS host
    - Monitor the DNS and DHCP Services of the Windows Server
  - Zabbix
    - Install Zabbix
    - Change Zabbix admin user to „admin“ and password to „London2011“
    - Add a graph of CPU usage of RSR1 Router
  - Firewall
    - Implement firewall setting on the RSSRV1 server

- Allow SSH connection only for RSMS1 workstation
- There is no other local restriction
- NTP
  - Install NTP Server on the RSSRV1 Linux Server

## 1.6 PART 2

### Work Task Network

Note: Please use the default configuration if you are not given the details.

- Connect the LAN cables and configure IP addresses based on the network diagram
- Router configuration on both **HQR1** and **RSR1** routers:
  - Use Fa0/0 interface for outside
  - Configure an IPSEC VPN tunnel authenticated with certificates from the Windows certificate server. In that case if you cannot setup the VPN tunnel authentication with certificate you have to use preshared key authentication with “London2011” key, but in this case you will not be given the maximum point for this task.
  - All traffic between the two sites should be sent through the secure tunnel.
  - Configure EIGRP with authentication by using the key string “London2011” between the HQ site and the remote site, so that both sites can communicate.
- **HQR1** router configuration:
  - Configure trunking on HQR1 router Fa0/1 inside interface to HQSW1 switch
  - Enable AAA Login with aaadmin user on the router, use the HQSRV1 Windows server as RADIUS server
  - Create local failover user if RADIUS server is not available using specifications from the appendix
  - Enable SSH access
  - Configure HQR1 as the primary DNS server for the outside network with moneystor.com as domain. Create A record for the RSSRV1 Linux Server with its public address (see later) and hostname rssrv1.
  - Enable PAT using HQR1 router public IP address to ensure Internet access for all of the inside hosts
  - Prevent all traffic from the Internet to inside, but ensure tunnel functionality and DNS service on HQR1 router for the Internet
  - Allow only HTTP and ssh from inside to the Internet
- **RSR1** router configuration:
  - Enable SNMP for monitoring
  - You must be able to reach Zabbix and Nagios web interface from the Internet using RSR1 public IP address.
  - Prevent all traffic from the Internet except web services on RSSRV1 server
- **HQSW1 Switch configuration**
  - Define VLANs. For the details see the appendix.
  - Use port Fa0/1 for HQR1 router Fa0/1 (trunk)
  - Use port Fa0/2 for HQSRV1 Windows server, make sure that only this device can connect to this port

**Important Note:**

*Because of the VmWare virtualization you have to consider that both VmWare host machine interface and the virtual machine interface MAC Address appear on the switch port.*

- In case of violation of the port security the port of the switch must recovery automatic in 30 seconds
- Use Fa0/12 port for the HQSW2 Fa0/2 port
- Configure the IP address listed in the network diagram
- Enable STP PortFast on all of the access ports
  - Note: *The purpose of this task is to speed up your work and the marking. This task will not be marked.*
- **HQSW2** Switch configuration
  - You must not configure this switch
  - Use Fa0/2 port for HQSW1 Fa0/12
  - Use Fa0/3 port for HQAP1 Access Point Ethernet
  - Use Fa0/13 port for HQR1 router Fa0/0 interface
  - Use Fa0/14 port for RSR1 router Fa0/0 interface
  - Use Fa0/15 port for INTSRV1 Debian Server
- **RSSW1** Switch configuration
  - Use Fa0/1 port for RSR1 router inside interface
  - Use Fa0/2 port for RSSRV1 Linux server
  - Use Fa0/3 port for RSMS1 workstation
  - All other ports are shutdown
  - Enable SNMP. See the appendix for the details
  - Configure the IP address listed in the network diagram
  - Enable STP PortFast on all of the access ports
    - Note: *The purpose of this task is to speed up your work and the marking. This task will not be marked.*
- **HQAP1** Access Point configuration
  - Connect HQAP1 Access Point Ethernet port to HQSW2 port Fa0/3
  - Use WPA2 Enterprise as encryption protocol. Use HQSRV1 as Radius Server.
  - See appendix for the details

## 1.7 PART 3

### Work Task HQNB Notebook

Note: Please use the default configuration if you are not given the details.

- Please configure the HQNB notebook with the settings specified in the appendix
- Join the HQNB notebook into the domain
- Configure the WLAN

### Work Task RSMS1 workstation

Note: Please use the default configuration if you are not given the details.

- Please configure the RSMS1 workstation with the settings specified in the appendix
- Create link to the Nagios and Zabbix webpage on the local Competitor user's desktop for monitoring

- Synchronize the clock with the NTP server on the RSSRV1 Linux server

### Work Task INTSRV1 server

Note: Please use the default configuration if you are not given the details.

- Please configure the server with the IP settings specified in the appendix

## 2 APPENDIX

### 2.1 Specifications

#### 2.1.1 WINDOWS SERVER SPECIFICATIONS

Computer name:	HQSRV1
DNS domain:	moneystor.lan
User name:	administrator
Administrator password:	London2011
IP address:	192.168.45.32
Domain NetBios Name:	MONEYSTOR

#### 2.1.2 DOMAIN GROUP/OU LIST (CREATE OU AND GROUP!)

<b>Groupname/OU Name:</b>
Manager
Worker

#### 2.1.3 DOMAIN USERLIST

<b>Username:</b>	<b>Password:</b>	<b>Restrictions:</b>
aaadmin	London2011	
<b>Username:</b>	<b>Password:</b>	<b>Group:</b>
Worker01	London2011	Worker
Manager01	London2011	Manager



### 2.1.4 GPOs

<b>OU NAME:</b>	<b>Restrictions:</b>
Manager	none
Worker	Only allow to open the browser, block all other applications

### 2.1.5 LINUX SERVER SPECIFICATIONS

Computer name:	RSSRV1
User name:	root
Root password:	London2011
Domain name:	moneystor.lan
IP address:	192.168.47.32

### 2.1.6 NOTEBOOK SPECIFICATIONS

Computer name:	HQNB
IP address:	DHCP

### 2.1.7 MONITOR STATION SPECIFICATIONS

Computer name:	RSMS1
IP address:	192.168.47.33/24

### 2.1.8 INTERNET SERVER SPECIFICATIONS (FOR TESTING)

Computer name:	INTSRV1
IP address:	154.23.47.51/29

### 2.1.9 NETWORK SPECIFICATIONS

<b>HQ site</b>
----------------

VLAN Managers (ID: 10, Management VLAN)	192.168.45.0/24	Ports on HQSW1: Fa0/2-12 Gi0/1-2
VLAN Workers (ID: 20)	192.168.46.0/24	Ports on HQSW1: Fa0/13-24
HQR1 inside addresses	192.168.45.1/24, 192.168.46.1/24	
<b>Remote site</b>		
Default VLAN	192.168.47.0/24	
<b>Internet</b>		
HQR1 public address	154.23.47.49/29	
RSR1 public address	154.23.47.50/29	
INTSRV1 address	154.23.47.51/29	
<b>Tunnel</b>		
HQR1 tunnel interface address	10.0.0.1/24	
RSR1 tunnel interface address	10.0.0.2/24	
<b>Users and passwords</b>		
Enable password on Cisco devices	None	
Local user name and password on HQR1 router (failover user):	admin / London2011	
<b>SNMP</b>		
SNMP community string	London2011	
<b>Radius Server</b>		
Shared secret key	London2011	

### 2.1.10 WIRELESS NETWORK SPECIFICATIONS

WLAN SSID	MoneyStorxx (xx is your station number)
Wireless LAN Security	WPA2 Enterprise

## 2.1.11 VMWARE VIRTUAL MACHINE SPECIFICATIONS

### HQ HOST PC

- You will use this host for HQ site and for Internet testing with two virtual machines:
  - *Windows Server 2008* virtual machine as HQSRV1 Windows Server (onboard NIC)
  - *Debian Marking* virtual machine as INTSRV1 Debian Server (for testing Internet services, top add-in NIC)
    - Note: *Debian Marking* is in the C:\London\VMs\DebianMarking folder. You have to open this VM in the VmWare Workstation.
- **Don't open or run any other VM on this host PC!**

### RS HOST PC

- You will use this host for RS site
  - *Debian* virtual machine as RSSRV1 Debian Server (top add-in NIC)
  - *Windows 7* as RSMS1 Monitoring Station (bottom add-in NIC)
- **Don't open or run any other VM on this host PC!**

## 2.2 INSTRUCTIONS

### 2.2.1 INSTRUCTIONS TO THE COMPETITOR

- Do not bring any materials with you to the competition.
- Mobile phones are not to be used.
- Do not disclose any competition material / information to any person during each day's competition.
- Read the whole competition script prior to you starting work.
- Be aware different tasks attract a percentage of the overall mark. Plan your time carefully.

### 2.2.2 EQUIPMENT, MACHINERY, INSTALLATIONS AND MATERIALS REQUIRED

Server:

- 2xPC - High Powered Desktop
- OS (Windows 7) preinstalled

Notebook:

- Notebook
- OS (Windows 7) preinstalled

Network:

- 2x2611XM Cisco Router
- 2x2950 Cisco Switch
- 1xPoE enabled Cisco Switch
- Cisco 1231 Wireless Access Point

Additional software:

- Operating System (Windows 7)
- Operating System (Server 2008 r2 Enterprise)
- Operating System (Debian 6)