

Test Project – Day 3

TP39_39JP_EN

Submitted by:

Name: Pascal Fuks, Rodney Dorville, Guilherme Panes, Masahiko Murase

Member Country: BE, SG, BR, JP, SA

CONTENTS

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

1. TP39_39JP_DAY3_EN.doc

INTRODUCTION

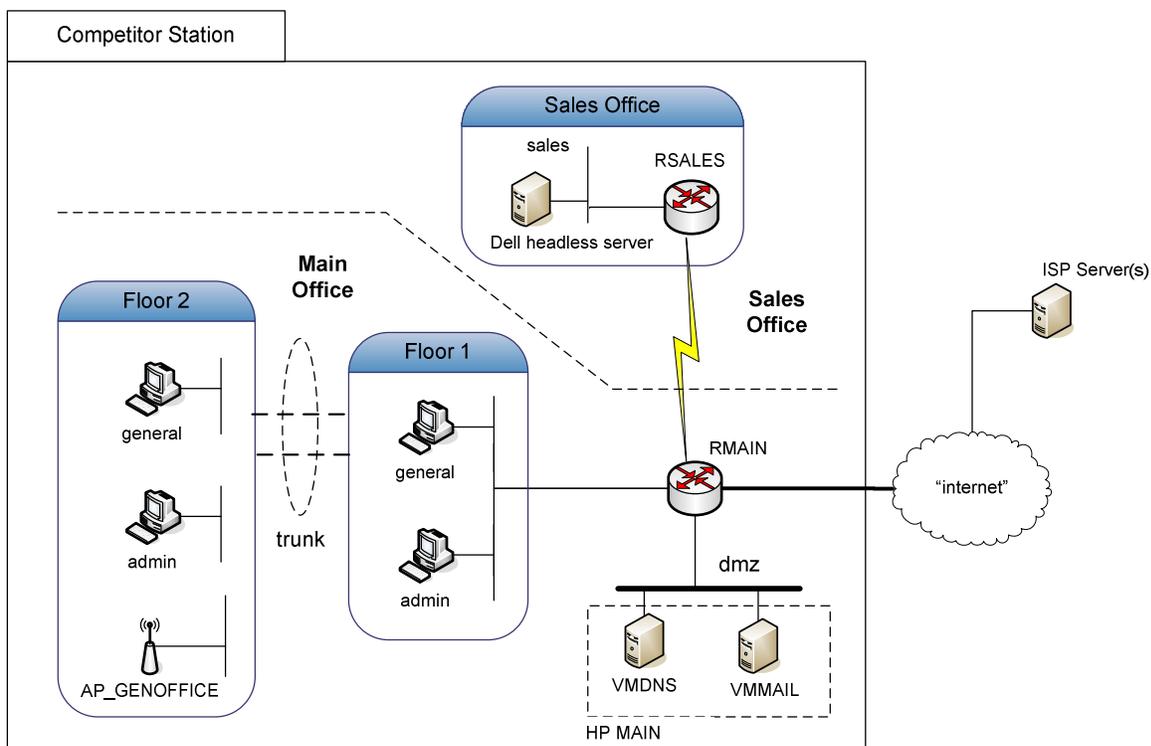
The competition has a fixed start and finish time. You must decide how best divide your time.

All hardware will be rebooted before marking is started.

You may choose any package for implementation of the services, we will test only on the functionality of your application.

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

DESCRIPTION OF PROJECT AND TASKS



Scenario

Acme Corp. has just established a new General office and a Sales office. The General office is located on 2 floors of Building A. The Sales office is located across the road in Building B.

Building A

Acme Corp. are located on Floor 1 and Floor 2. Each floor has a number of managers and office members categorised in VLANs admin and general. The servers are located in this building and are administered by the VLAN admin users. The office has internet connectivity via Router "RMAIN". Building A company servers on this network are located on the VLAN dmz.

Building B

The Sales Office is located in Building B which is across the road. This office supports a small sales team who are in NETWORK sales and a small server (SALES). This office is connected to the General office via a serial Leased Line from Router "RMAIN" to Router "RSALES".

ISP services

The ISP will provide the following services:

- (i) Link to internet
- (ii) DNS server
 - a. Forwarder
 - b. Reverse zone for your Public IP addresses.
- (iii) NTP
- (iv) Certificate Authority
- (v) Web services
- (vi) SMTP relay

The ISP has allocated a domain name (acmeXX.com) to your corporation (XX is your station number). You have also been allocated a /28 IP-block as shown in Table 1 Public assigned address.

Station (XX)	Public assigned IP	Domain Name	NS record	
			Nameserver	IP addresses
01	202.209.01.0/28	acme01.com	ns1.acme01.com	202.209.01.1
02	202.209.02.0/28	acme02.com	ns1.acme02.com	202.209.02.1
03	202.209.03.0/28	acme03.com	ns1.acme03.com	202.209.03.1
04	202.209.04.0/28	acme04.com	ns1.acme04.com	202.209.04.1
05	202.209.05.0/28	acme05.com	ns1.acme05.com	202.209.05.1
06	202.209.06.0/28	acme06.com	ns1.acme06.com	202.209.06.1
07	202.209.07.0/28	acme07.com	ns1.acme07.com	202.209.07.1
08	202.209.08.0/28	acme08.com	ns1.acme08.com	202.209.08.1
09	202.209.09.0/28	acme09.com	ns1.acme09.com	202.209.09.1
10	202.209.10.0/28	acme10.com	ns1.acme10.com	202.209.10.1
11	202.209.11.0/28	acme11.com	ns1.acme11.com	202.209.11.1
12	202.209.12.0/28	acme12.com	ns1.acme12.com	202.209.12.1
13	202.209.13.0/28	acme13.com	ns1.acme13.com	202.209.13.1
14	202.209.14.0/28	acme14.com	ns1.acme14.com	202.209.14.1
15	202.209.15.0/28	acme15.com	ns1.acme15.com	202.209.15.1
16	202.209.16.0/28	acme16.com	ns1.acme16.com	202.209.16.1
17	202.209.17.0/28	acme17.com	ns1.acme17.com	202.209.17.1
18	202.209.18.0/28	acme18.com	ns1.acme18.com	202.209.18.1
19	202.209.19.0/28	acme19.com	ns1.acme19.com	202.209.19.1
20	202.209.20.0/28	acme20.com	ns1.acme20.com	202.209.20.1
21	202.209.21.0/28	acme21.com	ns1.acme21.com	202.209.21.1

Table 1 Public assigned address

You will find a cross-reference of the page number of the Figures and Tables on the last page of this document.

Tasks:

1. Using the network diagram (Figure 1 Network Diagram) and the connectivity table (Table 7 Network Connectivity), implement the necessary connections for your company.
2. Router RSALES and Switch SW2 was purchased second-hand. Reset the password and upgrade the IOS of RSALES to version 12.4. A copy of the IOS is available on the Laptop in the Software directory on the Desktop.

If you cannot reset RSALES and/or SW2, or if you accidentally erase the flash image and do not know how to restore it, please inform the Experts who will assist you in the recovery. You will only be loose the marks in these areas.

You can still continue with the Project if you cannot upgrade the IOS version. You can continue with the tasks using the original IOS version.

Please refer to Table 9 Assistance Request if you need assistance.

3. Configure the Router RMAIN for routing services between your company and the Internet. Use the following table (Table 2 Router's External Address) to assign the Router's external address:

Station	ISP gateway
01	192.168.01.1 /30
02	192.168.02.1 /30
03	192.168.03.1 /30
04	192.168.04.1 /30
05	192.168.05.1 /30
06	192.168.06.1 /30
07	192.168.07.1 /30
08	192.168.08.1 /30
09	192.168.09.1 /30
10	192.168.10.1 /30
11	192.168.11.1 /30
12	192.168.12.1 /30
13	192.168.13.1 /30
14	192.168.14.1 /30
15	192.168.15.1 /30
16	192.168.16.1 /30
17	192.168.17.1 /30
18	192.168.18.1 /30
19	192.168.19.1 /30
20	192.168.20.1 /30
21	192.168.21.1 /30

Table 2 Router's External Address

4. Configure NAT services on router RMAIN. Table 3 NAT and Hostname Assignment shows the address mapping for NAT. External hosts must be able to access the internal services using the outside addresses.

Service	hostname	inside address	outside address
			202.209.XX.0/28
DNS	ns1	10.10.30.2	1
Web	www	10.10.30.3	2
Mail	smtp	10.10.30.3	3
Secure Web	https	10.10.30.3	4
DNS secondary	ns2	10.10.50.2	5
Not-used			6-13
Outgoing		all clients	14

Table 3 NAT and Hostname Assignment

5. RMAIN serial link to RSALES has the IP address 172.16.254.1/30. This link must have authentication using the password "20071117".
You may set any clock rate above 128K for this link and decide on the DCE/DTE endpoints.
6. ****This task will be marked based on configuration****
- The traffic on the serial link between RMAIN and RSALES needs to be limited.
The following limitations are to be configured on router RSALES:
- A 64 Kbps data transfer limit between the routers RMAIN and RSALES.
 - A rate limit of 3 Kbps for all TELNET communications to router.
7. The VLANs general, admin and dmz are connected to RMAIN using 802.3.
Building A consists of the users of VLANs general and admin which are located on Floors 1 and 2.
In addition, wireless connectivity is provided by AP_GENOFFICE for users of VLANs general and guests. You have two switches SW1 and SW2 for this purpose.
- Ensure that you provide link aggregation on the switches for redundancy.
- Please refer to Table 7 Network Connectivity for the port assignments.
8. For security reasons, please do not connect your wireless access AP to your network until you are ready to configure or test. You should use the following SSIDs:
- | | |
|---------|------------------------------------|
| corpXX | SSID for VLAN <u>general</u> users |
| guestXX | SSID for VLAN <u>guest</u> users |
- where XX is your station number.
You will need to secure your AP using WPA-TKIP in both SSIDs. Write down the passphrase that you have used in Table 8 Your Installation Information. We suggest that you use a 4-digit passphrase for convenience.
- Wireless users should be automatically routed to their respective networks.
9. VLAN guest users will only be allowed HTTP access to the Internet and no access to all other resources in the company network.
VLAN admin users will not be allowed any Internet access.

10. All networks in the company use OSPF.
 Routing information is authenticated using the MD5 password “20071117”.
11. Use Table 4 Network Parameters for your LAN Networks.

VLAN/NETWORKS	
general	10.10.10.0/24
admin	10.10.20.0/24
dmz	10.10.30.0/24
guest	10.10.40.0/24
Sales (NO VLAN)	10.10.50.0/24
Use the first address for the router	
Switch management	
SW1	10.20.1.1/24
SW2	10.20.1.2/24
Router OSPF Information	
RMAIN	10.30.1.1/30
RSALES	10.30.1.2/30
SNMP Communities (Version 1)	
ReadOnly	

Table 4 Network Parameters

12. The network devices are to be setup using the information in Table 5 Network Device Logins:

Device	Hostname	username	exec password	enable password
Router	RMAIN	boss	1234	7890
Router	RSALES			
Switch	SW1			
Switch	SW2			
AP	AP_GENOFFICE			

Table 5 Network Device Logins

13. In router RMAIN, create a locally authenticated user “bigboss” with MD5 password “1357” that automatically places the user in the highest enable upon login.

14. The company's servers are located on the VLAN dmz however located on a single physical platform "MAIN" server. Network services are provided using Virtual Machines running on this server under VMWare Server software. MAIN has been pre-installed for you on the HP server, together with the VMWare server software.

You can manage the physical/virtual servers using the following login information:

default user/password: user/1234
root/password: root/7890

The network servers are to be hosted as Virtual Machines running on MAIN. A base image of the Virtual Machine is provided for you for this purpose.

You have to restore the Virtual Machine image from the tape drive.

However, if you unable to perform this task, you may use the older version of the Virtual Machine image, which can be found in the directory **/home/vm**.

Information:

You may choose any package for implementation of the services, we will test only on the functionality of your application.

Please complete the Table 8 Your Installation Information on the package used and any relevant information needed to test your configuration.

You must **NOT** install any additional packages in server MAIN.

15. Use a Virtual Machine (VMDNS) to provide the following services for your company.
- Dynamically assigned IP addresses for all company's networks.
 - Primary DNS services for internal and external name resolution. You have to provide reverse zone services for internal network as well. The ISP has provided a DNS server at **100.100.100.1**. Refer to Table 3 NAT and Hostname Assignment for the hostname configurations.
 - Syslog
 - TFTP
 - NTP
16. Use another Virtual Machine (VMMAIL) to provide the following services for your company:
- SMTP services with Webmail and anti-virus. You have to install **ClamAV** package as the anti-virus.
 - Secure Web Services
 - RADIUS
 - SNMP
 - Web Graphic tool for traffic monitoring

17. Configure RMAIN to log up to level NOTICE to the Syslog server (VMDNS).
Log this information in the file **router.log**.

A new log file is created after every 15 minutes. The existing **router.log** file should be renamed to **router_<date>_<time>.log**

where

<date>_<time> is in the format YYYYMMDD_HHMM

e.g.

router_20071117_0900.log = log backed up at 09:00hrs 17th Nov 2007

18. All final configurations of the routers RMAIN, RSALES, switches SW1 and SW2 must be saved on the TFTP server (VMDNS). Name your configuration files with the equipment name with extension **.cfg** (e.g. **RMAIN.cfg**)

19. Install and configure NTP services on VMDNS. You are to synchronise your time with the ISP NTP server located at IP:**100.100.100.1**.

After you have setup your NTP server, configure your router RMAIN and server MAIN to synchronise with your NTP server.

20. Configure firewall rules to secure network access to and from server VMDNS using security standards to allow only the services that the server handles and uses.

21. The default settings of each user for SMTP are

- a. Limit size of attachments to 1 MByte.
- b. Reject outgoing mail with incomplete domain names (FQDN) and mail which do not have a MX or NS record associated with your domain.

22. After you have installed your SMTP services, you should test your configuration by sending an e-mail to test@experts.com.

This is an automatic response system.

Print out a copy of the return e-mail with headers for marking. Remember to write your Station Number and Country Code on the printout and to sign the printout.

23. In order to test your anti-virus configuration, you will need to send an e-mail to virus@experts.com.

This is an automated response which will contain a virus-test-code.

Print out evidence that this response is blocked. Remember to write your Station Number and Country Code on the printout and to sign the printout.

24. The company wishes to implement Secure Web Services. You have to request for a certificate from the ISP for this purpose using e-mail. Please send your request to admin@experts.com.

You will get a response within 15 minutes (the last request for the certificate is 16:00 hrs).

25. Create a web page using the following HTML code:

```
<html>
<head><title>Station XX Secure Web Services</title></head>
<body>
  <h1>Station XX Secure Web Services</h1>
</body>
</html>
```

Replace XX with your Station number.

26. A secure TELNET access is required for Switch SW1 and wireless access point AP_GENOFFICE. Table 6 Telnet Access using RADIUS shows the authentication and authorization for TELNET access to these devices with RADIUS on VMMAIL.

Group	Username	Password	Access
support	supp1	1234	Exec access
	supp2	1234	
super	superv	7890	Allow all resources

Table 6 Telnet Access using RADIUS

27. You are to provide Web Graphic monitoring of the traffic on RMAIN s0/0/0 and CPU usage for both RMAIN and SW1.
Please remember to fill Table 8 Your Installation Information indicating the URL for the display.

28. A Dell computer is provided as a server to be located in the Sales Office. This is a headless machine (i.e. no keyboard/mouse/display are allowed). A base installation of Debian has been installed on this machine.

Configure this system as follows:

- a. DNS secondary server for your company
- b. SSH logins with passwords must be disallowed.

Your laptop contains a SSH Client software (PuTTY). Use **1234567890** as the passphrase to authorize logins.

Please inform the Experts if you do not know how to manage the Dell computer.

Please refer to Table 9 Assistance Request if you need assistance.

END OF PROJECT

REMINDER

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

INSTRUCTIONS TO THE COMPETITOR

Do not bring any materials with you to the competition.

Mobile phones are not to be used.

The competition has been designed to give you too much to do in the time allocated.

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

Any technical problems must be reported immediately. Equipment will be checked and if found faulty will be replaced and extra time will be agreed with the competitor. However if the equipment is found to be working correctly, no extra time will be given.

You may ask questions during the competition to judges who will always work in pairs; however the judges reserve the right not to answer. All answers given will be written down and where appropriate given to all other competitors.

EQUIPMENT, MACHINERY, INSTALLATIONS AND MATERIALS REQUIRED

Supplied Equipment:

1. HP Server
 - a. Debian 4.0 base pre-installed, English, U.S. QWERTY keyboard.
default user/password: user/1234
root/password: root/7890
 - b. IP Address: 10.10.30.254/24
 - c. VMWare Server v1.04 pre-installed

2. Dell Computer
 - a. Debian 4.0 base pre-installed, English, U.S. QWERTY
default user/password: user/1234
root/password: root/7890
 - b. IP Address: 10.10.50.2/24
 - c. Serial port COM1 enabled, 9600, n,8,1

3. HP Laptop
 - a. Windows XP Operating System, not password protected
 - b. Software Directory on Desktop
 - i. PuTTY
 - ii. WinSCP
 - iii. Cisco Router IOS v12.4 image
 - iv. VMWare Client software

4. Cisco Router 2811 RMAIN
5. Cisco Switch 2960 SW1
6. 2nd hand Cisco Router 2811 RSALES
7. 2nd hand Cisco Switch 2960 SW2
8. PCI Switch Hub
9. Canon iP90v printer
10. HP DAT Tape drive and tape
11. Connection cables

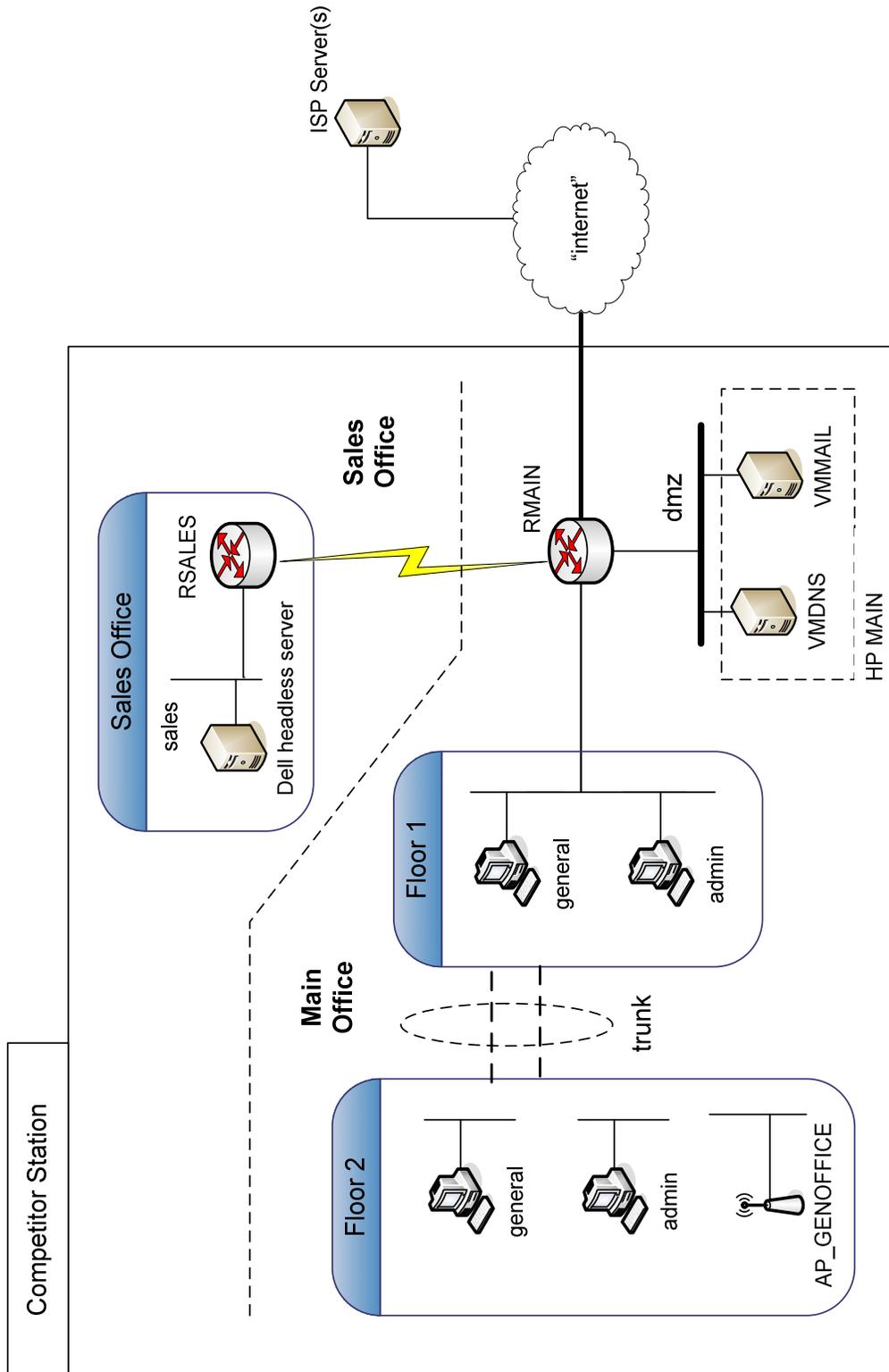


Figure 1 Network Diagram

Equipment	Interface	Description	Comment
Router RMAIN	Fa0/0	Connection to ISP provider	Provided by experts
	FA0/1	VLAN <u>dmz</u>	
		VLAN <u>general</u>	
		VLAN <u>admin</u>	
	s0/0/0	Connection to RSALES	
Router RSALES	Fa0/0	NETWORK <u>sales</u>	Use the PCI switch hub
	s0/0/0	Connection to RMAIN	
Switch SW1	Gi0/1	Connection to RMAIN	
	Gi0/2	VLAN <u>dmz</u>	
	Gi0/3		
	Gi0/4	VLAN <u>general</u>	
	Gi0/5		
	Gi0/6	VLAN <u>admin</u>	
	Gi0/7	trunk	
	Gi0/8		
Switch SW2	Gi0/1	VLAN <u>general</u>	
	Gi0/2		
	Gi0/3	VLAN <u>admin</u>	
	Gi0/4		
	Gi0/5	Connection to AP_GENOFFICE	
	Gi0/6	Not used	
	Gi0/7	trunk	
	Gi0/8		

Table 7 Network Connectivity

Table 8 Your Installation Information

Service	Package Name	Information for test
DHCP		
DNS		
SMTP		
TFTP		TFTP root directory:
WebMail		URL for webmail access:
NTP		
Graphic Monitoring Tool		URL to display graphs: If applicable user: password:
Syslog		Location of log files:
RADIUS		
SSH	PuTTY on Laptop	Login: user Passphrase: 1234567890
WPA-TKIP passphrase		Passphrase: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Web Page		URL:

Table 9 Assistance Request

Station No: _____

Candidate Country: _____

I have asked for, and received assistance in the following areas:

Task	Candidate Signature	2 Expert's Signatures	Time
RSALES reset/ recovery			
SW2 reset / recovery			
RSALES IOS image recovery			
Non headless SALES server used			

Marking Summary

	Topics	Description	Marks
1	Routing	NAT, routing on a stick, OSPF, Frame Relay or PPP, access-lists, dhcp forwarding, static routing,password recovery, IOS upgrade	6.25
2	Switching	VTP, VLANs, wireless VLAN, switch recovery,Link aggregation	3.75
3	System Administration	Headless server, AAA using Radius, Authentication using SSH, Local user priv 15, restore from tape	3.75
4	Base Services	DHCP, Email, Antivirus, Run VMs, Syslog, Apache, webmail, TFTP Server	4.25
5	Advanced Services	DNS - internal/external, NTP, SNMP,	2.5
6	Security	Certificates, serial link authentication, cisco password in MD5, ip-tables inside VM	3
7	Management	Graphic tool for traffic, traffic shaping per interface/protocol on router	1.5
		Total	25

Table 10 Marking Summary

Table of contents:

Figure 1 Network Diagram.....	12
Table 1 Public assigned address.....	3
Table 2 Router's External Address.....	4
Table 3 NAT and Hostname Assignment.....	5
Table 4 Network Parameters.....	6
Table 5 Network Device Logins.....	6
Table 6 Telnet Access using RADIUS.....	9
Table 7 Network Connectivity.....	13
Table 8 Your Installation Information.....	14
Table 9 Assistance Request.....	15
Table 10 Marking Summary	16