

**Achievement of Market-Friendly Initiatives and Results Program
(AMIR 2.0 Program)**

Funded By U.S. Agency for International Development

**Jordan e-Government Project
Government Institutions Requirements to Join
SGN and eMail initiative**

Final Report

**Deliverable for ICTI Component, Workplan Activity No. 433.2
Consultancy Agreement No. 278-C-00-02-00210-00**

July 2003

This report was prepared by EDS in collaboration with Chemonics International Inc., prime contractor to the U.S. Agency for International Development for the AMIR Program in Jordan.

List of Contents

LIST OF CONTENTS	1
0.1 DOCUMENT HISTORY	3
0.2 CHANGES FROM LAST ISSUE	3
0.3 ACKNOWLEDGEMENTS.....	3
0.4 DISTRIBUTION LIST	3
0.5 REFERENCED DOCUMENTS.....	3
0.6 ABBREVIATIONS.....	3
0.7 GLOSSARY	4
1. INTRODUCTION.....	5
1.1 OBJECTIVES	5
1.2 ACKNOWLEDGEMENTS.....	5
2. CLIENT DESKTOP.....	6
2.1 RECOMMENDED APPROACH TO ENSURE INSTITUTION’S DESKTOPS MEET REQUIREMENTS.....	6
2.2 INVENTORY	6
2.3 PERSONAL DIRECTORY INFORMATION.....	6
2.4 EMAIL REQUIREMENTS.....	7
2.4.1 <i>Government Institution with an existing eMail service.....</i>	<i>7</i>
2.4.2 <i>Government Institution that has no existing eMail service.....</i>	<i>7</i>
2.5 HARDWARE SPECIFICATIONS	8
2.5.1 <i>Upgrading existing Desktops.....</i>	<i>8</i>
2.5.2 <i>Replacing Desktops.....</i>	<i>8</i>
2.6 SOFTWARE SPECIFICATIONS.....	8
2.6.1 <i>Existing non Standard software on Desktops outside the requirements.....</i>	<i>8</i>
2.7 RFP SCOPE.....	9
3. LAN.....	10
3.1 RECOMMENDED APPROACH TO ENSURE INSTITUTION’S LAN MEET REQUIREMENTS.....	10
3.2 LAN/WAN/SERVER HARDWARE INVENTORY	10
3.3 NETWORK DIAGRAM.....	11
3.4 LAN DIAGRAM.....	11
3.5 SECURE COMMUNICATIONS ROOM.....	12
3.6 IP ALLOCATION DETAILS	12
3.7 ISP CONNECTIVITY.....	13
3.8 NT DOMAINS.....	14
4. NEXT STEPS	15
4.1 DESKTOPS.....	15
4.2 IP PLAN	15
4.3 NETWORK DESIGN	16
4.4 ISP SERVICE.....	16
4.5 NAMING CONVENTIONS	16
4.6 NETWORK DESIGN AND IP PLAN IMPLEMENTATION	17
4.6.1 <i>DHCP</i>	<i>17</i>
4.6.2 <i>Network Design changes.....</i>	<i>17</i>
4.7 ACTIVE DIRECTORY	17
4.8 EMAIL ROLLOUT	18
4.8.1 <i>Institutions with existing eMail service.....</i>	<i>18</i>
4.8.2 <i>Institutions with no existing eMail service.....</i>	<i>18</i>
5. TRAINING.....	19
5.1 ADMINISTRATOR TRAINING.....	19
5.2 USER TRAINING.....	19
APPENDIX A – USER/DESKTOP INVENTORIES	21
FIGURE 1 - USER & DESKTOP INVENTORY	21

FIGURE 2 - EMAIL INVENTORY	22
FIGURE 3 – PERSONAL DIRECTORY INFORMATION.....	23
FIGURE 4 – ANALYSIS REPORT	24
APPENDIX B – NETWORK INVENTORY.....	25
FIGURE 5 - INSTITUTION LAN/WAN/SERVER HARDWARE INVENTORY	25
FIGURE 6 - QUESTIONNAIRE FOR COMMUNICATIONS ROOM AND FACILITIES.....	26
APPENDIX C – QUESTIONNAIRE FOR ISP SERVICE.....	29
APPENDIX D – QUESTIONNAIRE FOR NT DOMAIN	31
APPENDIX E – IP SCENARIOS FOR JOINING INSTITUTIONS	33
APPENDIX F – SAMPLE FINAL NETWORK DESIGN	35
APPENDIX G – NAMING CONVENTIONS	36
FUNCTION & DESCRIPTION LISTINGS	36
DOMAIN CONTROLLERS.....	36
MEMBER SERVERS.....	36
WORKSTATIONS	37
ACTIVE DIRECTORY	37
PORTAL NAME	37
USERS	38
NETWORK EQUIPMENT NAMING CONVENTION.....	39
APPENDIX H – CHECKLIST FOR EMAIL MIGRATION	40
APPENDIX I – LETTER OF COMMITMENT FOR USER TRAINING.....	41

0.1 Document History

Version	Status	Reviewed/Approved by	Date
0.1	Draft	Shatha & Abed	8th May 2003
1.0	Issue		25 th July 2003

0.2 Changes From Last Issue

Version	Date Updated	Revision Author	Summary of Major Changes Made	Reviewed By	Review Date

0.3 Acknowledgements

N/A

0.4 Distribution List

Abdelmajeed Shamlawi'	AMIR
Shatha Ahmad	MoICT
Kendall Lott	EDS
Allan Gormley	EDS

0.5 Referenced Documents

Reference Number	Title	Note

0.6 Abbreviations

DMZ	Demilitarized Zone
DNS	Domain Name Service
GOJ	Government of Jordan
LAN	Local Area Network
MoICT	Ministry of Information & Communications Technology
NIC	National Information Center
PC	Personal Computer
SGN	Secure Government Network
DL	Distribution List
ACL	Access Control List

0.7 Glossary

This section defines the following terms that are used in this report:

DMZ	A Demilitarized Zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network. The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls.
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially <i>intranets</i> . All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
Internet - also known as the World Wide Web (www)	A worldwide network of linked PCs. Information is published to the public in graphical format on Internet Web sites for anyone to view. Many national governments now have one portal site to which users are initially directed, before being redirected (often by a search engine built into the portal) to the Web site of the government department that they are seeking. (For an example, see www.ukonline-Gov.uk)
LAN	A network restricted to government users, which links PCs within a ministry. It uses protocols such as Token-Ring to share electronic files around the LAN. The format of these files is generally limited and will not usually include the graphical and enhanced formats that are available on an intranet.
Secure Government Network	An intranet that is provided by a government for the exclusive use of its civil servants. It will be provided with high levels of security to prevent any non-government users from gaining access to it. This type of network is also known as a Government Secure Intranet (GSI). Each Ministry will probably have its own intranet Web site that will provide information to intranet users.

2. Client Desktop

2.1 Recommended approach to ensure institution's Desktops meet requirements.

- Local IT Dept complete the user/desktop inventory.
- Inventory inspected to determine the upgrades required, memory, new desktop or OS.
- Detail numbers of users/desktops requiring configuration
- eMail user details including non standard email accounts
- Testing of non-standard software and determine if any software upgrades required.
- Decision made on whether the Institution will be included in this phase of the project
- Analysis report completed and added to RFP, this provides the vendor with the requirements to upgrade all the desktops, template found in [Appendix A – Figure 4](#).
- Vendor purchases and installs/upgrades hardware and software.
- Vendor and local IT dept upgrade OS systems as required ensuring all are at least W2K

When all the above steps have been completed then the institution's desktop meet the joining requirements. No desktop should exist on the SGN that does not meet these criteria.

2.2 Inventory

Note: All user and their desktops must be included in this inventory as one of the requirements is that all users are included and that no user desktop remains on the network that does not meet the minimum hardware specifications.

The initial step is to complete a complete Desktop Inventory; the template for this is found in [Appendix A – Figure 1](#). This needs to include all users Desktops in the organization.

The fields that need to be completed are:

- | | |
|-------------------------------|---|
| ➤ UserID | NT login Name if exists |
| ➤ Name | Name of User in English |
| ➤ Title | Job Title |
| ➤ Department | |
| ➤ Type L/D | Laptop/ / Desktop |
| ➤ Manufacturer / Model | Example Dell DeskPro |
| ➤ LAN Y/N | Does it have a working Ethernet NIC? |
| ➤ Memory | RAM in MB |
| ➤ Processor & Speed | Example PIII 1GHz |
| ➤ HD size | Total Size of Primary Hard drive eg 20GB |
| ➤ HD Free | Free space, this is important if an OS upgrade required. |
| ➤ Operating System | Current OS system installed |
| ➤ Antivirus software | |
| ➤ IE Version | |
| ➤ Outlook Version | Need to specify whether Outlook Express or Full Client also which version i.e. Outlook 2000 SP1 |
| ➤ Other Relevant Applications | Other mailing software packages in use, non-standard software, if the desktop is being upgraded this is important. |
| ➤ Email Address | Existing eMail address if user is to be migrated. |
| ➤ Phone | |
| ➤ Office location | Using a convention allowing the desktop to be easily found by an implementation team. (Might be an idea to include site map.) |

2.3 Personal Directory information

Along with the above Inventory, an additional table must be completed; this table is detailed in [Appendix A – Figure 3](#), all fields are required unless stated otherwise. This information will be entered within the user properties during the project implementation. Having this information collected prior to the project start is a requirement as

it can cause major delay during the implementation. This task is the responsibility of the institution project manager.

Note: All the fields must be completed in English, as they will be entered into the user properties.

2.4 eMail Requirements

2.4.1 Government Institution with an existing eMail service

If an existing eMail server exists, the existing email addresses for users need to be included in the inventory (2.1). If a user has multiple aliases, these need to be included in the same inventory.

The following are example of additional services that may be used by the institution that also need to be migrated.

2.4.1.1 Functional eMail accounts

Existing email addresses that are not user specific rather function accounts, example IT department, Human Resources (these accounts generally have multiple users accessing them, need to be documented separately in the eMail inventory attached [Appendix A](#), the following details are required.

Email address	Email address currently in use, example HumanResources@Inst.gov.jo	
New name	Required if different to meet naming standards detailed in Appendix G	
Owner of functional account	Name of the user who owns this account, i.e. the person that determines who needs access; this person does not need to be the principle user.	Title of Owner
List of users who need access	Name of User in English who needs access to this account.	Level of access required by each user, example UserA full Access, UserB read only.

2.4.1.2 Distribution Lists

A distribution list contains a grouping of users. The list is used to send eMail to a number of users without having to include each user separately. By default there is a distribution list that contains all the users within an institution. The access list on this DL is very strict.

Name of distribution List	Existing Name that is displayed in the Global Address List	
New name	Required if different to meet naming standards detailed in Appendix G	
Owner of Distribution list	Name of the user who owns this distribution list, i.e. the person that determines who needs to be included.	Title of Owner
List of user	Each member of the list listed	
List of users that can send to the DL	A separate list of users who can send emails to this DL is required.	

2.4.2 Government Institution that has no existing eMail service

In this case there will be no migration to be completed and only user accounts will be created by the vendor, however training will be given to the local IT staff who will then be able to create any functional eMail accounts and Distribution Lists as required.

2.5 Hardware Specifications

The objective is to connect all users desktops on the LAN to the new domain; therefore they must have at least windows 2000 operating system installed. To ensure that this is possible the following details the hardware requirements.

2.5.1 Upgrading existing Desktops

Any Desktop with a processor of PIII can be upgraded if required to meet the minimum specifications for a Desktop to have Windows 2000 operating installed. This minimal configuration is:

- PIII 1GHz
- 128 MB RAM
- 2GB of free space on the hard drive

Note: Generally only the RAM is upgraded.

2.5.2 Replacing Desktops

Any Desktop that cannot meet this requirement must be replaced. The minimum specification of a new desktop purchased is:

- PIII 1 GHz.
- 256MB RAM
- 20GB Hard Drive
- 16MB AGP Graphics Card
- CD ROM Drive
- 1.44MB Floppy Drive
- Integrated NIC and Sound
- 15" Monitor (No Brand specific equipment)
- Windows XP Professional

Note: this specification is based on Dell hardware; other hardware of similar specification will be accepted.

2.6 Software specifications

Apart from having at least Windows 2000 operating system installed, the client desktop must also have at least Office 2000 and Outlook 2000 installed.

Note: The default language on the system must be configured to be English; otherwise the Outlook client will not be able to connect with the exchange server.

2.6.1 Existing non Standard software on Desktops outside the requirements

It is the responsibility of the local IT department to ensure that all required existing software on desktops that will be reconfigured is detailed in the inventory. The local IT department must also ensure that this software will work with the new operating system. Testing must be completed for non-standard software to ensure that there will be no issues, also if a software upgrade is required, this must be tested and the software added as part of the RFP, again the responsibility of the local IT department.

Note: This may mean a separate project needs to be invoked, i.e. in the case of a client server application like Oracle, the backend server may also require an upgrade. This will be the responsibility of the local IT department and will not be included in the RFP and must be completed before the institution can join the SGN.

2.7 RFP Scope

Once the local IT department has completed all the above inventories the RFP can be completed for the desktop section.

The details required for each institution are:

- Ram upgrades including Model and make of desktop
- Number of replacement desktops required
- Client Application Software upgrade requirements, including the existing version and required version and no of licenses and media
- Number of desktops to be added to the active directory, have anti virus configured and email client configured
- Number of email accounts to be migrated
- Number of user accounts/email addresses to be created
- Number of non standard email accounts required to be created (this is obtained from the inventory of distribution lists and functional emails, [Appendix A– Figure 2](#))

3. LAN

3.1 Recommended approach to ensure institution's LAN meet requirements

- Completed Institution LAN/WAN/Server Hardware Inventory
- Detailed LAN/WAN diagram
- Detailed existing IP inventory
- New detailed LAN/WAN diagram if required
- New IP Plan
- Managed changeover to new LAN/WAN diagram and IP Plan
- Connect to SGN
- Migrate Internet Traffic

3.2 LAN/WAN/Server Hardware Inventory

An assumption is that each institution already has an existing Ethernet Network; this is a basic requirement for joining the SGN, the user desktops must be connected to this LAN with an IP address.

The Inventory sheet is found in [Appendix B – Figure 5](#). This needs to include all equipment not already detailed as a user desktop. This would include Servers, firewalls, routers and any desktops that have been built for a function and not a users desktop, i.e. Desktop with HP Openview for monitoring the network.

It is important that all equipment not covered by the desktop inventory is included; this should include details of the Ethernet Networking equipment for example switches and hubs.

Department / Institution	If the hardware is specific to a department within an institution then this needs to be notes, i.e. Server used by Finance department.
ISP	Details of any ISP link connected
Firewall Y/N	Is this device running as a firewall?
Router Type	Is this device a router, if so what type, please note a server with routing switched on and having multiple interfaces is acting as a router.
Server / firewall Name	Name of device, should be the same as that on the network diagram.
Machine Type	Cisco, Dell, Sun etc with the make and model details
RAM	
Hard Disk	
Server usage	All the functions of this device, i.e. possible Firewall, Web Proxy and DNS on same device. Domain controller, DHCP server, Web Server, Database server, etc
IP Address	Please list all IP addresses on the device.
OS / Database	NT4, W2K (server/workstation), Sun Solaris, Linux, HP Unix, Cisco IOS, please state version and service pack applied and relevant patches.
Functions	WAN Router, ISP Router, Web Server etc
Remote Sites	If remote sites connected, please state details for, number of links, types of links, speed of links, locations etc

Notes: Please complete a separate entry for each piece of hardware, not all fields are relevant, please leave non-relevant fields blank or enter N/A (not applicable). Please ensure that all devices connected to the LAN are noted even if not maintained by the main IT department, all devices on the LAN can affect the security.

For the Active directory to be installed within the government institution, two servers are required

Domain controllers recommended Specs

- Processor: 1 processor, Pentium III 700 MHz speed or more.
- Memory: 512 MB RAM or More
- Locally attached storage
 - o Drive controller: SCSI 3
 - o Hard Drives: 20GB or more
 - o Hard Drive bays: 2-4

· Network Interface Card: One 10/100 Fast Ethernet adapters supporting PXE (Pre-boot Execution Environment).

3.3 Network Diagram

The following sample network diagram gives an overview of how the network may look. This diagram needs to contain all the main devices however it does not need to contain all the database servers if they are all on the LAN, it is sufficient to group these. All devices with multiple network connections or not on the main LAN do need to be shown with the routers, firewalls, web servers, DNS servers and Proxy servers. In the sample network shown there are two ISP connections but the two networks are not connected, all such details need to be clearly shown.

This diagram is given as a example; the diagram supplied by the government does not have to be identical but does need to show all the following:

- All external connections
- All IP networks
- Devices with multiple network connections
- Web Servers
- Routers, Firewalls, Proxy and DNS servers
- Any non standard IP devices on the network example Mainframe, Time clock, etc

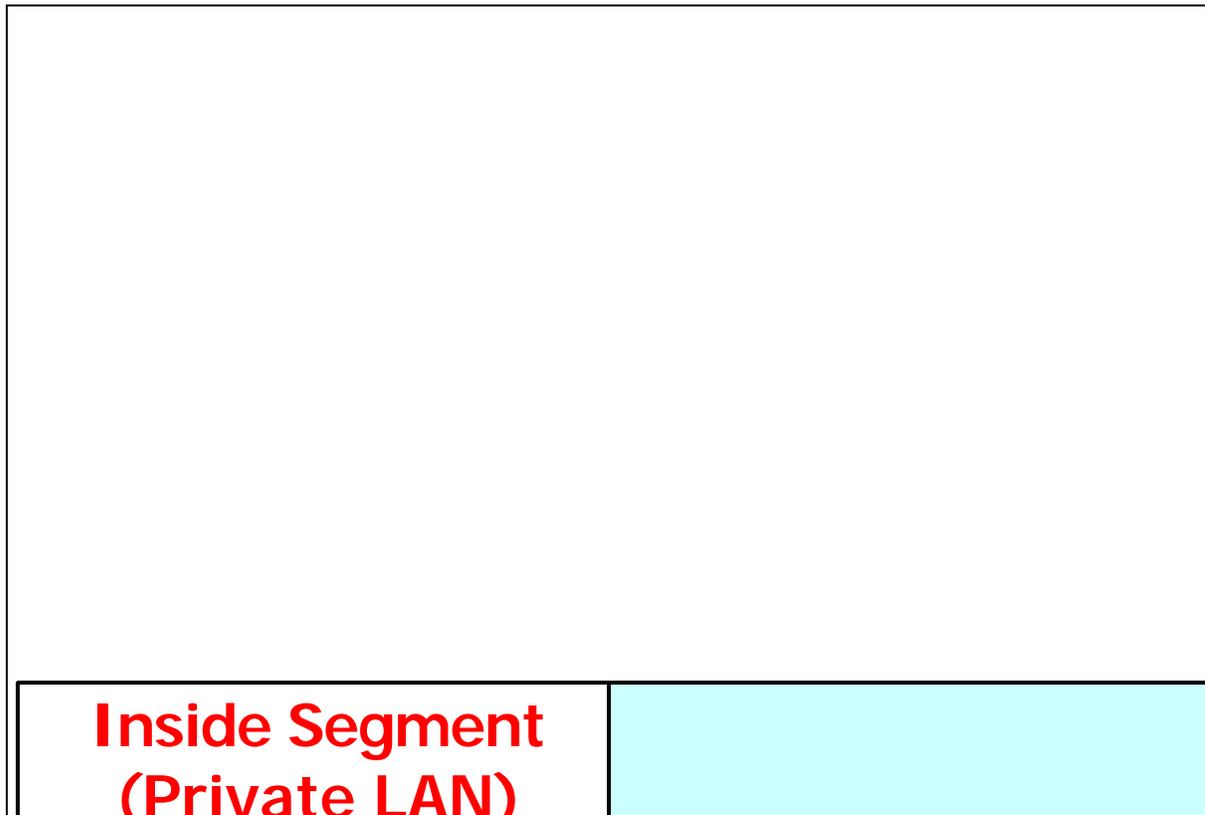
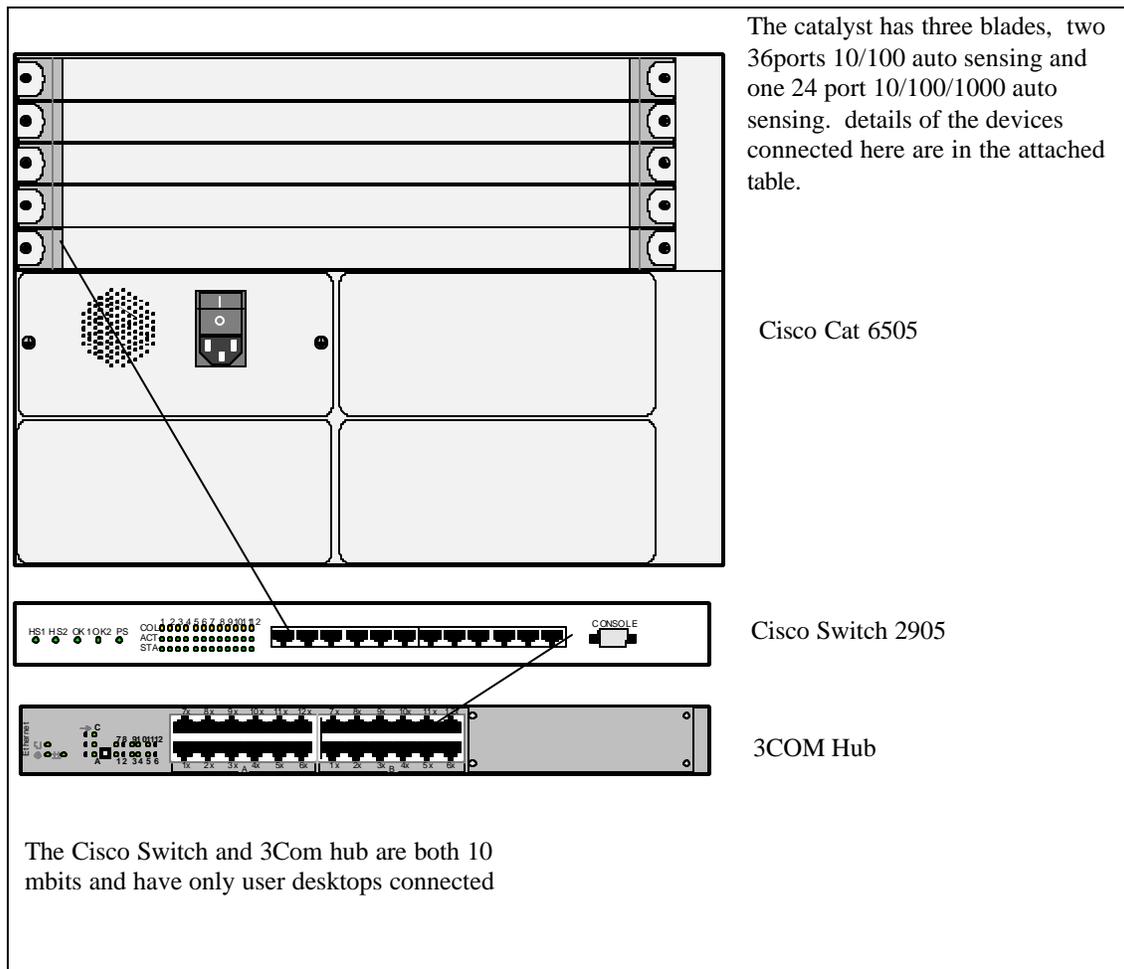


Diagram 1 – Sample Network Diagram

3.4 LAN Diagram

For each LAN within the network diagram above, a LAN diagram is required. This is to detail how the Ethernet LAN is connected. This can be as simple as the diagram attached, the objective of this information is to detail how the LAN is interconnected and where all the key devices are connected, for example the router.



Further details can be supplied in a table like the one shown below.

Catalyst 6505

Blade 1 is 36 (0-35) port auto sensing 10/100

Blade 2 is 36 (0-35) port auto sensing 10/100

Blade 3 is

<i>Port Details</i>	<i>Device attached</i>
Blade 1 Port 0	

3.5 Secure Communications Room

Here the detail of the room where the SGN hardware is to be housed is required. A questionnaire is included in [Appendix B, Figure 6](#). This needs to be completed. The requirements that must be met are:

- Secure access to the physical room, must be restricted to required personnel only
- Power and Ethernet LAN connections
- Floor space for the SGN cabinet
- Workable solution to get JTC lines into the room

3.6 IP allocation details

Using the Network diagram to define the different networks that exist within the government institution, details of all IP addresses currently used need to be documented.

A possible way of completing this is to separate the devices that need static IP addresses from the user desktop, complete the tables as follows:

LAN name Main local LAN in Amman office (shown in the network diagram – private LAN)

IP Network 10.39.20.0
Subnet 255.255.255.0
Default Router 10.39.20.254

Device Name	IP Address
ISP Router	10.39.20.254
WAN Router	10.39.20.5
Server1	10.39.20.80
Server2	10.39.20.89
IP Printer A	10.39.20.76
IP Printer B	10.39.20.79
Etc	

Desktop	IP address
HumanRes1	10.39.20.109
Personal2	10.39.20.203
User Q	10.39.20.187
HumanRes2	10.39.20.165
User A	10.39.20.218

Diagram 2 – Sample IP tables

The Device names from these tables should directly match the Inventories already completed. The same device may appear on multiple tables as it may have multiple interfaces.

This information is required so that a migration to the new IP addressing schema used within the SGN will be easily completed. The IP migration can take the following approach:

- Collect all the IP information
- Create the new IP plan
- Migrate all static IP devices that do not require static addresses to DHCP (mainly desktops)
- Plan the migration for non-working hours
- Change the DHCP settings to the new IP range and change the static settings on all devices.

At this stage the Network is ready to join the SGN, the new addressing must be completed before this connection can be made.

3.7 ISP Connectivity

In [Appendix C](#), A copy of the questionnaire that needs to be completed for each ISP connection that the government institution has is found. This is important as Internet connectivity is the first place security is required, a full picture is required to ensure that all connectivity is as secure as possible.

The approach with regard to ensuring this security is as follows:

- Complete the network diagram
- Complete the ISP questionnaire
- Draw up the final network design having the ISP service going through the SGN
- Implement the final design and remove the external links from the government institution

The questionnaire requires the following information:

ISP Supplier	Example NIC, Global One
Bandwidth	Example 64K
Current Contract	Enter the start and finish date of the existing contract with the ISP supplier
Notice required for terminating existing contract	
Is there any technical reason why the NIC cannot be used for this service:	If Yes, please detail the technical reason, example service not provided etc

ISP Services	<i>For each of the following please detail the services required example Web browsing on port 80 apart from the real IP addresses</i>
Real IP addresses used	If a range of IP addresses are being used that were given by the ISP, these need to be supplied here including details of which ones are in use and for what function.
Web Servers hosted	If Web Servers are published via this link, detail the server name as defined in the network diagram.
DNS Services used	If DNS services are being published via this ISP link, please detail the device name and the domain name hosted. If the ISP provider is also supplying or maintaining this service please detail.
Web Browsing	If Web Browsing is allowed over this link, detail the restriction that are implemented, i.e. web proxy denies access to a number of sites, Access to users allowed on IP address etc

Note: This questionnaire needs to be completed for each ISP connection to the Institution even if not maintained by the main IT department and owned by a department as all links on the LAN effect the overall security.

3.8 NT Domains

If an exiting NT domain exists within the government institution, then the Questionnaire in [Appendix D](#) needs to be completed. The following information is required:

NT Domain name & version	Domain Name, NT4 or W2K Active directory
Primary Domain Controller	Device name as given in hardware inventory
Backup Controller(s)	Device Name(s) as given in hardware inventory
Member Server(s)	Servers that belong to the domain but are not domain controllers
User details	Are profiles used, home directories, what standards applied? Details required for migration.
Desktops members of the domain?	If Yes, please details if this applies to all desktops or just a number of them. Are there policies or profiles associated with them?
File Servers	Full details of the resources and how users are allowed access for migration purposes to new domain.
User Groups	All details required to migrate to new domain
Print Servers	All details required migrating to new domain, any special configuration must be noted.
Other Domain resources	Example, user groups used on proxy server to give different levels or deny access to the internet.

The information for this questionnaire will be used in the migration from the existing domain to the new child domain. All shared resources will be recreated, member servers will be moved to the new domain and when users migrated to the new login the existing resources will remain unchanged, and their profile, shares and printers will be migrated.

4. Next Steps

Once all the inventories detailed in the previous two sections are completed and all the required details provided to MoICT. Then a decision is taken as to whether the institution is part of the forthcoming project. Once the institution has been accepted as part of the phase the following steps are completed.

- RFP completed by MoICT
- The RFP is released, proposals received evaluated by MoICT and vendor awarded the RFP.
- Vendor appoints project Management team
- Project Plan amended and kick off meeting held for all to agree plan

Then within the government institution:

- Vendor to review inventory of Distribution lists and functional emails.
- Vendor will review inventories and finalise scope at the ministry side for:
 - Upgrades (Software and Hardware)
 - Replacements (Software and Hardware)
 - Additional (Software and Hardware)
- Vendor will determine upgrades, replacements and additions to the Operations Centre and any other parties if required.
- Vendor will procure all required items as determined from above.
- Vendor will implement all procured items including upgrades, replacements and additions for Hardware and Software.
- Vendor in conjunction with the institution to complete final network design and IP plan.
- Vendor in conjunction with the institution compiles the lists of new login names and email addresses and determines the domain names that will be used within the implementation.
- If required DHCP is installed and all the desktops configured to be DHCP clients (this may have to wait for the purchase of the new domain servers)
- Vendor will train two system administrators from each ministry
- Vendor will train all government institution users on Outlook.

Once purchasing is completed:

- RAM installed and new desktops rollout to users, any remaining OS upgrades completed
- Networking equipment installed and institution joined to SGN
- Internet service configured via the SGN
- The child domain is installed and all the users created and desktops added to the domain
- eMail migration or rollout completed
- All related software (Outlook, anti virus, Operating Systems and ie)

4.1 Desktops

The implementation team start with the desktops, they work with the Local project/IT team to ensure that all upgrades are completed, this will be planned to work with the delivery dates or Ram and new Desktops.

This task is completed when all the user desktops within the institution have the minimum hardware requirements, OS system Office/Outlook installed.

4.2 IP Plan

The implementation team work with the local project/IT team to produce the final network design and IP plan. [Appendix E](#) has details of the IP scenarios that may be used.

When completing the IP Plan, differentiate between equipment and assign ranges, example Servers have a static range, Printers a separate static range, Desktops a DHCP range etc.

Note: The Appendix is the IP Scenarios as of the date of publication of this document, please reference the Ops Centre Manager for the latest version, these scenarios are templates, institutions with specific requirements may use the guidelines to create another template that will then be added to the documentation within the Ops Centre.

4.3 Network Design

An example of a final network design is provided in [Appendix F](#). It does not cover all scenarios, for example if an existing firewall exists for the web server then the firewall will be moved to the DMZ, essentially the approach is to change as little as possible in the existing set-up, the ownership of the LAN remains fully with the local IT team, the only objective of the project is to increase security where possible. Each Network will be looked at separately and the designs given here are as an example only.

The vendor will work in conjunction with the local team to achieve the most secure workable solution.

4.4 ISP Service

When completing the network design the ISP service will probably be where the changes will be implemented. The goal of the project is to have the most secure network possible. To achieve this one of the goals is that the only external links to the government network are through the Ops Centre; therefore all ISP services will be provided this way. Currently the ISP service provider is NIC as per the recommendation of the Prime Minister. In the future this service will be upgraded to be fully redundant as the more services and institutions that are using the Operations centre the higher the level of service required. This can be provided in two ways, the NIC upgrading its service to become fully redundant or the Operations Centre having a separate agreement with a different ISP, this is a future decision.

Today, the service is provided by the NIC and unless an institution has a technical issue that the NIC cannot facilitate at this time, all ISP traffic will use this service. The operations Centre has a range of IP addresses that are available for Internet facing services

In the event that the NIC cannot provide the service, the approach is that the alternative ISP provider links to the Operations Centre and the traffic will still utilise the SGN. Rules will be applied to the traffic ensuring that it will be routed correctly. This will ensure that all external links are monitored using an intrusion detection system and subject to periodic security checks.

Note: There may be an additional piece of hardware required to supply this service.

Real IP addresses at this stage need to be assigned by the Operations Centre as required to the institution based on the details supplied within the ISP Questionnaire. Even if the existing service provider is the NIC, the range of IP addresses in use need to be changed as the Operations Centre node has a class C range assigned which facilitates routing and maximises use of the IP networks.

4.5 Naming Conventions

[Appendix G](#) is details of the current naming conventions standards, however these are not keep up to date within this document and for the latest version of the domain and user standards the document ***Naming Conventions.doc*** should be referenced, this is maintained by the Operations Centre. The document ***IP Plan doc.doc*** should be referenced for the latest standards with regard to networking equipment.

Using these conventions, the domain name needs to be confirmed by the local institution. It is usual for the same name to be used in all areas of the naming convention but this is not necessary. The domain name example MOF is then used for the following:

- Active Directory domain name example MOF.GOV
- Active directory site name
- eMail address example user@mof.gov.jo
- Web site example www.mof.gov.jo
- Location name for naming convention for networking equipment

The implementation team with the local team complete the login names and email addresses for the users. Also convert the workstations to the new naming convention. The original user/desktop inventory sheet should be used adding the following two new fields:

- New Login/eMail Name
- New Workstation Name

Note: The login name should always be the same as the eMail name.

4.6 Network Design and IP Plan implementation

Once all the previous stages are complete the implementation team work with the local team to changeover to the new design. There are numerous ways this can be achieved; some work during working hours some outside, done in stages. An example of a staged approach with minimal risk is detailed below; this can be customised to suit the needs of the institution. Not all institutions will have all the following to complete, example DHCP may already be in use.

4.6.1 DHCP

DHCP installed. This may require waiting for the new servers to arrive, if this is the case, the initial build of the server will not be as a child domain and the DHCP service will have to be migrated at a later stage. Using the existing IP addressing scheme, choose a range that will be used by the desktops, initially this may mean reserving a lot of individual addresses until the desktops utilising these have been converted. Care must be taken to ensure that the range allowed with DHCP does not include existing static devices else there is a danger of creating IP conflicts and disrupting the users.

The desktops are then visited and converted to DHCP, ensuring that all static entries are removed. The settings for default router, subnet mask, DNS and Wins need to be obtained from the DHCP server, else there will be issues at the changeover to the new IP schema. Care should also be taken if Wins is in use on the network that the local device refreshes by either a reboot or a manual refresh. This change can be completed at the same time that the desktops is being visited to perform upgrades. It must be completed before the desktops are visited to enter the domain.

Once all the desktops have been converted to DHCP, all that remains is the settings within DHCP to be changed with the remaining static devices.

4.6.2 Network Design changes

In some instances changes may be agreed that can be completed before the new networking equipment is installed and connected. An example would be a server with multiple network cards by passing the firewall on the LAN. In this instance work would be completed on the firewall to ensure that the server functioned as expected with only one network connection, maybe on the DMZ of the local firewall.

The new IP address plan can be implemented before the new hardware is installed. This will normally mean that an intermediate plan is also required as the final addressing will not be completed until the SGN is fully functional, for example the default router.

Once the hardware is installed the majority of the design changes can be completed, example moving the web server to the DMZ of the SGN firewall. The ISP service will not be changed at this stage, as the SGN link is not active, except that it will now be routed via the DMZ of the SGN firewall.

At this stage the SGN link can be activated, this is required to install the child domain and it is recommended that the link is active at least a week before moving the ISP traffic. This ensures that all monitoring is configured, fully tested and that the link is confirmed as stable. The ISP traffic is routed via the SGN and all external links from the LAN.

4.7 Active Directory

The SGN link must be active before the child domain is installed. Prior to this the Operations Centre will have created the child domain and associated administrative accounts. These accounts will have full admin access of the child domain and no access of any other domain within the enterprise directory. Once the child domain is established within the institution, the enterprise administrator and any other external accounts should be removed from the access lists, this means that the child domain is fully independent of the remainder of the enterprise and full control is maintained by the local IT team.

The implementation team will build the two new servers to the standard build, documented in *server build standards.doc*, this documented is maintained by the Operations Centre and they will provide the latest copy. If required DHCP and the Antivirus distribution server is also installed. If one of the servers has already been used as the DHCP server, this service will now need to be moved so the server can be rebuilt within the domain.

All user accounts are created and the personal information collected at the beginning of the project is entered in the user properties. eMail accounts and mailboxes are created, aliases set-up if required as detailed earlier. Desktops are added into the domain. The client Antivirus can be configured at this time.

4.8 eMail Rollout

There are two different scenarios with regard to eMail depending on whether the service already existed.

4.8.1 Institutions with existing eMail service

In Institutions where eMail already exists, unless the number of users is very small, all the desktops should be added to the domain and the users created before any work commences with the client eMail. A planned approach is required to ensure that the users have continuous use of their eMail service. This is achieved by changing the DNS MX record the evening prior to the start of the migration, this means that all new emails will be directed to the exchange server within the Operations Centre and the old eMail server will still be accessible and will still send emails but is in fact just an archive store.

When the implementation team visit the users to configure their Outlook client to see the new exchange server, they will also copy the archive mails from the old server to the local drive of the desktop for the user to have access. At this stage the user will cease to connect to the old server and when all the users have the new configuration the old server should be decommissioned. Care needs to be taken during the migration as the last users migrated will not have had access to their new mail from the DNS record change. Users that depend on eMail and have the highest volume of usage should be prioritised and completed at the beginning of the migration.

In some cases where the institution is heavily dependant on eMail, it would be advised to perform the migration over a weekend or other holiday.

Note: there is a checklist to be completed before the migration can start to minimise on issue that may occur. This is found in [Appendix H](#).

4.8.2 Institutions with no existing eMail service

In Institutions where there is no prior eMail service. The client configuration can be completed the same time the desktop is added to the domain, meaning that the user is only visited once. This is a low risk scenario and the time taken to rollout the whole user community is not critical.

5. Training

5.1 Administrator Training

As part of the Project RFP, two administrators nominated by the Institution Project Manager in conjunction with the Local IT team will be trained.

The details required:

- Full Name of Administrator
- Job Title and Description

The training provided is Microsoft MCSA with the following modules. This training will be arranged with the vendor at times that all the government institutions agree to.

Microsoft Windows 2000 Network and Operating System Essentials: (approximately 20 Hours)

Supporting Microsoft Windows 2000 Professional & Server: (approximately 44 Hours)

Managing MS Windows 2000 Network Environment: (approximately 52 Hours)

Implementing and Managing Microsoft Exchange 2000: (approximately 44 Hours)

Note: In the past the training happened in the afternoon from 16:00 to 20:00 and each module was scheduled separately for a number of consecutive days. There were breaks between the modules.

5.2 User Training

As part of the project RFP, all users will receive training in Outlook. The basic training will cover the following items but is not limited to this:

Getting Started with Outlook 2000:

- Start Microsoft Outlook 2000.
- Navigate in the Outlook Bar.
- Review e-mail messages and attachments.
- Reply to and forward e-mail messages.
- Save e-mail messages and check sent messages.
- Format and print a copy of e-mail messages.
- Customize your Inbox.

Creating and Sending E-mail Messages:

- Compose and send messages.
- Use the address Book.
- Add attachments to messages.
- Mark messages confidential or urgent.
- Retrieve messages sent in error.

Organizing and Managing the Inbox:

- Organize e-mail messages for fast reviewing.
- Set up file folders for organizing e-mail messages.
- Flag e-mail messages for follow-up.
- Create Rules to handle e-mail messages automatically.

Using Internet Explorer for Outlook Web Access:

- Introducing Internet Explorer.
- Using Internet Explorer for Outlook Web Access.
- Handling messages.

Outlook Test.

Each user completes an evaluation of the training

The User training will be split into three categories:

Outlook Training:

The majority of the users will complete this training.

Advanced Outlook Training:

These classes are created for the user who already has a basic computing knowledge example ECDL or who have already been Outlook users. The main reason for the distinction was to try and place students in classes that would suit their pace and ability.

VIP Outlook Training:

This category was created, as personnel in some institutions may be more willing to attend this training.

It is the responsibility of the HR training personnel to determine which category each user should be placed within. This will need to be completed early in the project as the Vendor will then use these numbers to create a schedule and with the HR training personnel assign students to their classes.

Each student prior to attending the training will sign a letter of commitment. This is attached in [Appendix I](#). This letter must be signed by the student at least three days before training starts and passed onto the training coordinator prior to training commencing.

Figure 2 - eMail inventory (to be completed by local institution)

Government Institution

Functional eMail accounts

Existing eMail address	New eMail address	Display Name	Owner & Title	Access list	Level of access
HR@moict.gov.jo	HumanResources@moict.gov.jo	MoICT Human Resources	Maha Brown – HR manager	Mohammad	Ful Access/Send As
				Abed	Read
				Laura	Read/Write
				Daoud	Read/Write/Send As

Distribution Lists

Existing Name of DL	New Name of DL	Owner & Title	List of members	Access List
IT@moict.gov.jo	IT@moict.gov.jo	Nareeman – IT Manager	Daoud	Mohammad
			Shatha	Nareeman
			Samir	
			Maha	

e 3 – Personal Directory Information (to be completed by local institution for all users)

ment Institution:

roject Manager:

one / Mobile:

2nd Name	3rd Name	Last Name	Directorate/ Unit	Job Title	Job Description	National ID	OfficeTelep hone	OfficeTelephone Extension	Direct Line	Office Fax	Work Mobile	Home Telephone	Gender	Salutation	Empl hoto
?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
Mamdouh	Daoud	Suboh	Accounting/ Auditing	Chief Accountant	Optional Field	971104431	06-4641258	139		06-4641259	079-564352	Optional Field	Male/Fe male	i.e. Mr. Mrs or Ms. and name prefix (Excellency)	Option field if emplo wants pictur be publis in his profile

The details in the above table need to be supplied in English, as this is the language that it will be entered into the personal directory system.

Figure 4 – Analysis Report (to be completed by MoICT)

Government Institution _____

From the **User/Desktop Inventory** complete the following:

	Details	Number	Other Comments
A	Total User Desktops		
B	Desktops that meet Hardware Criteria		
C	Desktops that meet Hardware Criteria with working NIC		
D	Desktops to have RAM Upgrade		More details attached
E	Desktops to have RAM Upgrade with working NIC		
F	Desktops that require replacing		
G	Excluding F, Desktops that need an OS upgrade		
H	Existing eMail users		

Note: Items B + D + F must equal A

Note: For the Ram Upgrades, the data regarding those desktops must be extracted from the full inventory and attached. The details are required so that a correct costing can be completed as RAM for different makes and models vary. The required fields are shown below:

Name	Type L/D	Manufacturer / Model	LAN Y/N	Memory	Processor & Speed	HD size	HD Free	Operating System
------	----------	----------------------	---------	--------	-------------------	---------	---------	------------------

From the **eMail Inventory**

I	Number of functional eMail accounts		
J	Number of distributions lists		

From the **Personnel Directory Information** complete the following:

K	Total Number of Users to be created		
----------	-------------------------------------	--	--

Note: It is assumed that this number is the same as the number of eMail users required and students for the outlook training. Please note if this is not the case.

Is there an NT domain to be migrated within the government Institution? _____

Appendix B – Network Inventory

Figure 5 - Institution LAN/WAN/Server Hardware Inventory (to be completed by local institution)

Department / Institution	ISP	Firewall Y/N	Router Type	Server / firewall Name	Machine Type	RAM	Hard Disk	Server usage	IP Address	OS / Database	Functions	Remote Sites
Institution			e.g. CISCO 2500	XXXX	Intel, Bull, Risc etc			Choose: Email, Web, Application, Proxy, Database, Firewall	nnn.nnn.nnn.nnn	W2K Server, NT4 Workstation, UNIX, Oracle, SQL etc	e.g. Hosts web page	No or Number e.g. 10

Figure 6 - Questionnaire for Communications Room and Facilities (to be completed by local institution)

Government Institution _____

Date Completed _____

Completed By _____

Location of Secure Room _____

Please detail the physical security that is in place and how it is implemented: (example card reader with access granted by the local IT manager, currently all six members of the IT team and the manager are the only people with access). Give details for each entry even if it is permanently locked, i.e. who has the key?

Please give details on the room layout. (Example, raised floor with managed cabling underneath, all sockets in the room are connected to the UPS, average temp of the room is 18°C with the AC, currently has 3 cabinets with networking equipment and 4 tables with the existing servers, enclose any diagrams that exist)

Please detail how the external links are connected to the Secure room (example, JTC provide termination in the basement on the east of the building, CAT5 cabling is run from there to a patch board in the secure room, distance is 10 meters)

Are there any other features? (Example, fire hazard prevention system, close circuit security system etc)

Does the room have the following facilities?

UPS	YES ___	NO ___	Is there a UPS 16Amp socket available	_____
AC	YES ___	NO ___		
Ethernet port on LAN	YES ___	NO ___	Are there 2 Ethernet ports available	_____
Floor space for cabinet	YES ___	NO ___		
Grounding availability	YES ___	NO ___	Is it available for the SGN rack	_____

Note: The cabinet is 42U free floor standing and can has a floor step of 600mm*1000mm. The position of the rack should be such that it is not located beside a wall and should be possible to walk all around and remove any of the side panels easily (unless it is placed beside another rack)

Appendix C – Questionnaire for ISP Service (to be completed by local institution)

Government Institution _____

Date Completed _____

Completed By _____

ISP Supplier _____

Bandwidth: _____

Current Contract: _____

Start: _____

Finish: _____

Notice required for terminating existing contract: _____

Is there any technical reason why the NIC cannot be used for this service: (tick appropriate answer)

Yes: € If yes, please give details

No €

ISP Services used:

Real IP addresses used (please complete table)

<i>IP address& Server</i>	<i>Published name</i>
197.25.86.102 - Webserver	www.mof.gov.jo

Web Servers hosted: (tick appropriate answer)

Yes: € If yes, please give details

No €

DNS Services used: (tick appropriate answer)

Yes: € If yes, please give details

No €

Web Browsing: (tick appropriate answer)

Yes: € If yes, please give details

No €

Note: Complete this questionnaire for each ISP connection to the Institution

Appendix D – Questionnaire for NT Domain (to be completed by local institution)

Government Institution _____

NT Domain Name & Version _____

Primary Domain Controller: _____

Backup Controller(s): _____

Member Server(s) _____

User Account Details _____

Are user desktops members of this domain?

Yes: € If yes, please give details _____

No €

File Server(s) _____

If File servers in use, complete the following table:

Shared Resource	Users access
\\fileserver\sharename	Global group – Finance – Full Control
	Global Group – Admin – Read only
\\fileserver\sharename\resource	User – Mohammad Mufti

If Groups are being used for access control, complete the following tables:

Global Group	Members
Finance	Mohammad Mufti
	Feras Bashar
Admin	Emad Taweel

Local Group	Members
Personal	Aish Zuhdi
	Adwaya Muhtasb

Print Server(s) _____

If Print servers in use, complete the following table:

Shared Resource	Details	Access Control
\\printserver\printsharename	Finance Printer, HP LaserJet III, IP address etc	All Domain Users - Print

Is the NT domain used to give access to any other resources?

Yes: € If yes, please give details _____

No €

Appendix E – IP Scenarios for joining institutions

Assumption we used in this design

In the design we will have two main scenarios, in which all the members of the Jordan e-government ministries and agency will fall under

The format of the Jordan E-Government IP addressing is **10.AAAOOOOO.SSSSNNN.HHHHHHHH**.

Where, AAA represents the area ID, 8 areas are available

OOOOO represents the organization ID (each area will have 32 organizations)

SSSSS represents the sub organization ID (each organization will have up to 32 sub organizations connected to it)

NNN represents the subnet in each sub organization (each sub organization will have 8 subnets)

HHHHHHH represents the host within each subnet (up to 254 host per subnet).

Distribution of IP addresses within each subnet	
IP addresses within each Subnet	To be used for
1-4	Routers
5-10	For Firewalls and other Network Equipments
11-244	For PCs and printers

First Scenario

The first scenario covers all the members with only on class C network in the network side, and this scenario is the recommended scenario

The format of this scenario IP addressing is **10.AAAOOOOO.SSSSNNN.HHHHHHHH**.

It is going to be divided as follows:

10.AAAOOOOO.0.0 -->10.AAAOOOOO.7.0	Netmask 255.255.248.0	Reserved
10.AAAOOOOO.8.0 -->10.AAAOOOOO.15.0	Netmask 255.255.248.0	Main site
10.AAAOOOOO.16.0 -->10.AAAOOOOO.23.0	Netmask 255.255.248.0	Reserved for main site
10.AAAOOOOO.24.0 -->10.AAAOOOOO.31.0	Netmask 255.255.248.0	Reserved for large sites
10.AAAOOOOO.32.0 -->10.AAAOOOOO.39.0	Netmask 255.255.248.0	Reserved for large sites
10.AAAOOOOO.40.0 -->10.AAAOOOOO.47.0	Netmask 255.255.248.0	Reserved for large sites
10.AAAOOOOO.48.0 -->10.AAAOOOOO.55.0	Netmask 255.255.248.0	Reserved for large sites
10.AAAOOOOO.56.0 -->10.AAAOOOOO.63.0	Netmask 255.255.248.0	Reserved for large sites
10.AAAOOOOO.64.0 --> 10.AAAOOOOO.127.0	Netmask 255.255.252.0	Reserved for medium sites
(16 networks)		
10.AAAOOOOO.128.0 --> 10.AAAOOOOO.2557.0	Netmask 255.255.254.0	Reserved for small sites (64 networks)

Second Scenario

This scenario covers only the exceptional networks, where the number of users within a LAN is more than one CLASS C. However, it should be highlighted at this stage that such a solution would have issue with scalability and performance, and it should be replaced with a structured setup where L3 switching would play a major role

The format of this scenario IP addressing is **10.AAAOOOOO.SSSNNHH.HHHHHHHH**.

Only for the main site

10.AAAOOOOO.0.0 -->10.AAAOOOOO.31.0
 Netmask 255.255.224.0 |

Reserved

10.AAA00000.32.0 -->10.AAA00000.63.0 Netmask 255.255.224.0
 10.AAA00000.64.0 --> 10.AAA00000.127.0 Netmask 255.255.252.0
medium site (16 networks)
 10.AAA00000.128.0 --> 10.AAA00000.2557.0 Netmask 255.255.254.0
networks)

Main site
reserved for Large to
reserved for small sites (64

For consistency of the design, all the Organizations will have the same IP scheme, but with a different mask depending on the adopted scenario

Example Scenario 1 (Network 10.35.0.0)

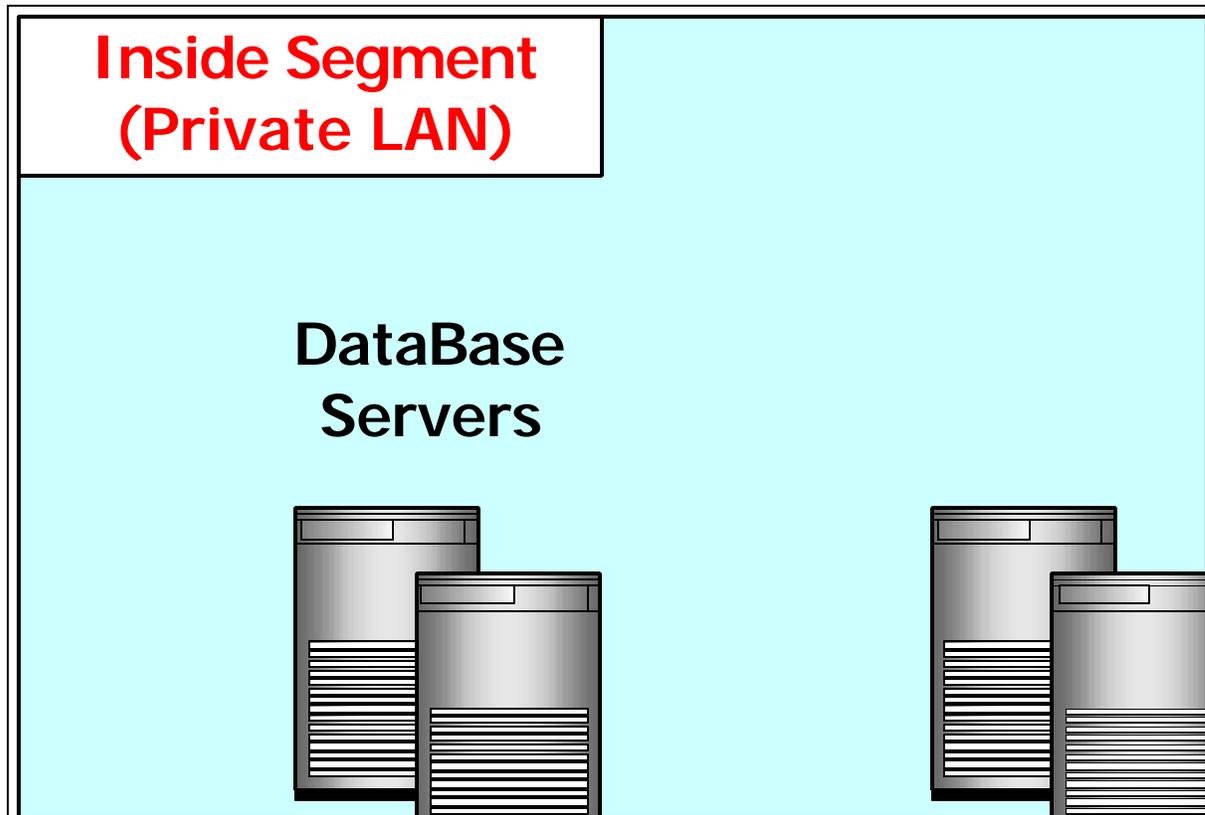
Device Name	S0/0	Loopback 0	BRI 0/0	Fast Ethernet 0/0
SGN Router	10.35.9.10/30	10.35.9.4 /32	10.35.9.14 /30	10.35.10.1/24

Device Name	Outside Segment	Internal Segment	Stateful Failover	WEB Server Segment	Old Internet Segment
Main PIX Firewall	10.35.10.5 /24	10.35.11.5/24	10.35.9.17/30	10.35.12.5 /24	10.35.13.5 /24
Failover PIX Firewall	10.35.10.6 /24	10.35.11.6 /24	10.35.9.18/30	10.35.12.6 /24	10.35.13.6/24

Device Name	Int VLAN 1
SGN Switch 1	10.35.10.10 /24
SGN Switch 2	10.35.10.11 /24
Internal Switch 1	10.35.11.10 /24
Internal Switch 2	10.35.11.11 /24

Device Name	S0/0	Loopback 0	BRI 0/0	Fast Ethernet 0/0
WAN Router 1	10.35.129.10/30	10.35.129.4 /32	10.35.129.14 /30	10.35.130.1/24
WAN Router 2	10.35.131.10/30	10.35.131.4 /32	10.35.131.14 /30	10.35.132.1/24
WAN Router 3	10.35.133.10/30	10.35.133.4 /32	10.35.133.14 /30	10.35.134.1/24
WAN Router 4	10.35.135.10/30	10.35.135.4 /32	10.35.135.14 /30	10.35.136.1/24
WAN Router 5	10.35.137.10/30	10.35.137.4 /32	10.35.137.14 /30	10.35.138.1/24
WAN Router 6	10.35.139.10/30	10.35.139.4 /32	10.35.139.14 /30	10.35.140.1/24
WAN Router 7	10.35.141.10/30	10.35.141.4 /32	10.35.141.14 /30	10.35.142.1/24
.
WAN Router 63	10.35.253.10/30	10.35.253.4 /32	10.35.253.14 /30	10.35.254.1/24

Appendix F – Sample Final Network Design



Appendix G – Naming conventions

Function & Description Listings

Function & Description Listings	Function and Number Abbreviation
Domain Controller	DCO
Front End Exchange Server	FEX
Back End Exchange Server	BEX
Load Balancing Exchange Server	LBX
Cluster Exchange Server	CLX
DHCP Server	DHC
WINS Server	WIN
Web Server	WEB
File and Print Server	FPR
Application Server	APP
Workstation	WS
Router	RTR
Switch	SWT
Firewall	FWL
Site	ST
First server in as many	01
Second server in as many	02
First Workstation in as many	001
Second Workstation in as many	002

Domain Controllers

The naming convention will be based on the domain association and a function with a two (2) digit serial number.

(Domain Name – Function –Serial Number)

So: GOV – DCO - 01 will appear as GOVDCO01.

This would be the first Domain Controller for the root domain in the Operation Centre.

Examples:

Root Domain - First Domain Controller	GOVDCO01
Root Domain - Second Domain Controller	GOVDCO02
Ministry of Finance – First Domain Controller	MOFDCO01
Ministry of Finance – Second Domain Controller	MOFDCO02

Member Servers

The naming convention will be based on the Domain Association and a function Description (3 letters) and a two (2) digit serial number.

(Domain Association - Function –Serial Number)

So: GOJ - FEX - 01 will appear as

GOJFEX01

This would be the first Front End Exchange Mail Server under the GOJ domain in the Operation Centre.

Examples:

Operation Centre Exchange Back End Virtual Server	GOJVEX01
Operation Centre Exchange Back End Cluster Server 1 ST Pair	GOJCLX01
Operation Centre Backup Server	GOJBCK01
Any Ministry (e.g. MOICT) First File and Print Server	MOICTFPR01
Any Ministry (e.g. AMM) Third Application Server	AMMAPL03

Workstations

The naming convention will be based on the Domain Association and a function Description (2 letters) and a three (3) digit serial number.

(Domain Association - Function –Serial Number)

Example: MOF - WS - 009 will appear as MOFWS009
This would be the ninth workstation under the MOF domain in the Ministry of Finance.

Active Directory

Logical components

Root Domain Name

This Root domain is to be placed in the Operation Centre.
Root Domain GOV.

Child Domains Names

The Child domain names will reflect the name of the Institution it represents:

Government of Jordan	GOJ.GOV
Prime Ministry	PM.GOV
Ministry of Finance	MOF.GOV

Sites (ST)

Naming convention for the Sites will be based on Location followed by and Underscore and a function (ST) for site, followed by a two (2) digit serial number.

Physical Location _ ST - Serial Number

Operation Centre Site (GOV & GOJ domains)	NIC_ST01
Prime Ministry Site	PM_ST01
Ministry of Finance	MOF_ST01

Site links

Naming convention for the Site Links will be addressed as follows:

Link source point _ Link destination point

Example: A Prime Ministry Link to the Operation Centre appears as: RM_NIC

Organization Units

Organization Units (OU) will be the primary object of representation for Internal Departments within each ministry. The OU names will be reflective of the department they represent. Please refer to the Data collection documents provided by the ministries themselves for further info.

Portal Name

The e-Government Project will be represented on the World Wide Web and thru other Internet services with the Portal Name of:

www.gov.jo

Web Access

Users of the World Wide Web can access it by typing the address: www.gov.jo

Users

Users' accounts will reside in the Active Directory. The users will need a "*Log on*" name to access the domain and resources on the Network. Users will also need a user name account for using the E-mail application on the Network. We unified both names so a user will need to remember and use only one name for the domain log on and e-mail account.

Users Naming Convention

The naming convention will be used in the UPN form; (Universal Principal Names).

User's first name.1st initial of last name @domain.gov.jo

For example, a city of Amman employee with a name of:

Mohammad Abdel-rahman Ibrahim AL-Majali

Would have the following UPN: mohammad.m@amm.gov.jo

Name rules that apply:

- A person's first name is always used.
- A dot following the first name is always used to separate the first name from the last name letter and not allow for indicating a female name for a male person. For an example, Samir.a without the dot becomes Samira, which is a female name.
- A letter representing the 1st initial of the person's last name is always used.

Duplicate Name recommendations that can be used:

- If multiple identical first name and a last name initial combinations occur, then a second letter is used and then may be as many letters as ministries see appropriate can be used after the dot (.).
- The second and subsequent letters used after the dot are the choice of the administrator in each ministry and don't have to follow a certain rule as long as they differentiate the identical users.
- Any prefix to the last name is always dropped before that last name initial letter is considered. Al-Majali is considered only Majali, so is Al-Khasawneh as Khasawneh and so forth.
- (Abu) is not considered a prefix.
- Any long compound first name will be reduced to the first part of the name. A first name of Mohammad-Ameen will be reduced to Mohammad or Ameen according to the user's request. A first name of Abdel-rahman is not considered compound, however we should drop the dash (-).

Users Log on Name

User Log on name is the same as the User UPN, universal principle name.

Users E-mail Address

User E-mail Account is the same as the User UPN, universal principle name followed by the .JO.

For the same example above:

Mohammad Abdel-rahman Ibrahim AL-Majali

Would have the following e-mail address: *mohammad.m @amm.gov.jo*

Special Cases

Some Standard Positions or titles will be allowed for a standard E-mail account. These names will be reserved for these special cases, some of which are:

For the each Ministry :	<i>min @ min.gov.jo</i>
For the “ Minister ”:	<i>minister @ min.gov.jo</i>
For the “ Secretary General ”:	<i>sg@ min.gov.jo</i>
For the “ Mayor ” at Amman City:	<i>mayor @ amm.gov.jo</i>
For the “ Deputy Mayor ” at Amman City:	<i>dmayor @amm.gov.jo</i>
For the “ Under Secretary ” at Amman City:	<i>wakeel @amm.gov.jo</i>

Network Equipment Naming Convention

The following format is used to name the data center network equipment:

Location-Segment Name-equipment-Interface type and number

Where, Location: DC = Data Center

Segment Name:	INT = Internet FE = Front End BE = Back End FO = Fail over SGN = Secure Government segment SS = Service segment
----------------------	--

Equipments:	R = Router VPN = VPN 3030 PIX = PIX firewalls IDS = Intrusion detection system SCA = Secure Content Accelerator CON = Content Modules or content switches 650X=613 LAN switch.
--------------------	--

Interface:	L0 = Loopback0 FE n=Fast Ethernet Number n GE = Gigabit Ethernet
-------------------	--

Appendix H – Checklist for eMail Migration



Acceptance Criteria for eMail Migration

- AntiVirus installed on all Desktop with updates happening on a regular basis
- LAN connected to SGN
- Child Domain servers installed in the ministry (if applicable)
- Scope list completed and agreed (Must contain the fields Workstation Name, User Name, Logon account name, old email address (es))
- All user accounts created with associated mailboxes
- All Workstations added to the domain
- Users created and Workstations added to domain are same as scope
- All Workstations checked for correct version of Outlook
- Users notified about the migration
- Critical users list completed and received
- Plan of action for Migration/Rollout. I.e. no of users/dept per day, ministry has arranged access to the relevant areas.

Ministry's Test Acceptance Confirmation

I have read and agree that all statements above are accurate and conclusive.

Ministry's Name: _____

Name: _____

Signature: _____

Date: _____

