World Bank

Pilot Network Report

Government Computer Capacity
Improvement Project (#19119)

September 2001

The Hashemite Kingdom of Jordan
Amman

Project Deliverable #5 : Final

Submitted by:
PADECO
PADECO CO., LTD.

Contents

Foreword 1

List of Abbreviations 2

Executive Summary 4

Section 1 : Introduction 6
- 1.1 Background 6
- 1.2 Purpose of the Paper 6
- 1.3 LANs, MANs and WANs 7
- 1.4 Scope of Work 8
  - 1.4.1 Logical connectivity 8
  - 1.4.2 Civil Service Bureau 10

Section 2 : Approach 12
- 2.1 Approach 12
- 2.2 Layered Design 12
  - 2.2.1 Application Section 13
  - 2.2.2 Administration Section 14
  - 2.2.3 Connectivity Section 14

Section 3 : Applications 16
- 3.1 Introduction 16
  - 3.1.1 Existing Data Exchange Between Pilot Agencies 16
- 3.2 Government Financial Management System (GFMS) 18
  - 3.2.1 Introduction 18
  - 3.2.2 GFMS “Vision” 19
  - 3.2.3 Decentralized Administration with Centralized Information Systems 20
  - 3.2.4 Benefits from Integration 21
  - 3.2.5 Financial Processes and Information Systems 21
  - 3.2.6 Enterprise Resource Planning (ERP) systems 28
  - 3.2.7 Human Resource Information System 34
  - 3.2.8 Critical Success Factors 36
  - 3.2.9 Recommendations 38
- 3.3 Collaborative Computing 39
  - 3.3.1 Introduction 39
  - 3.3.2 Groupware Applications 40
  - 3.3.3 Workflow Applications 42
  - 3.3.4 Enterprise Directory Services 43
  - 3.3.5 Electronic Mail (E-mail) 46

Section 4 : Administration 52
- 4.1 Introduction 52
- 4.2 Network (MAN) Administration 53
  - 4.2.1 Introduction 53
  - 4.2.2 Network Committee 53
  - 4.2.3 Recommendations 55

4.3 Security and LAN Administration 55
4.3.1 Introduction 55
4.3.2 Security issues 56
4.3.3 LAN Administration issues 60
4.4 IT Management 65
4.4.1 IT Management Overview 65
4.4.2 Project Team Observations 66
4.4.3 Best Practices 66
4.4.4 Recommendations 68

Section 5 : Connectivity 70
5.1 Introduction 70
5.1.1 Determining the best connectivity option 70
5.1.2 Other factors to consider 70
5.2 Public versus Private Networking 71
5.2.1 Introduction 71
5.2.2 Private Networks 72
5.2.3 Point-to-Point Private Lines 73
5.2.4 Public Networks 74
5.3 Existing Network Studies 75
5.3.1 Introduction 75
5.3.2 Prime Ministry Report 75
5.3.3 NIC Report 76
5.3.4 E-Government Government Secure Intranet (GSI) 77
5.4 Public Network Options in Jordan 78
5.4.1 Introduction 78
5.4.2 The Law 79
5.4.3 Jordan Telecom Corporation (JTC) 80
5.4.4 Batelco Jordan 83
5.5 Connectivity Options 86
5.5.1 Introduction 86
5.5.2 Considerations 86
5.5.3 Option 1 : Star topology based on JTC HDSL/ATM technology 91
5.5.4 Option 2 : Mesh topology based on JTC HDSL/ATM technology 95
5.5.5 Option 3 : Mesh topology based on BJ Frame Relay technology 98
5.6 Recommendations 100
5.6.1 Overview 100
5.6.2 Recommendations 100

Section 6 : Summary of Recommendations 102
6.1 Introduction 102
6.2 Application Section Recommendations 102
6.3 Administration Recommendations 106
6.4 Connectivity Recommendations 111

Section 7 : Proposals 112
7.1 Introduction 112
7.2 Application Project Proposal 113
7.2.1 Overview 113
7.2.2 Web-based Human Resource Information System (wb-HRIS) Project 114
7.2.3 Activities 115
7.3 Administration/Connectivity Project Proposal 116
7.3.1 Overview 116
7.3.2 Pilot Network Project 116
7.3.3 Activities 117

Appendix A : Data Exchange Questionnaire 118

Appendix B : SAP Public Sector Solutions 120

Appendix C : JTC Proposal..... 136

Appendix D : BJ Proposal..... 154

Foreword

This report represents the final output and completion of the *Government Computer's Capacity Improvement* (GCCI) project's component to design a pilot network linking key financial and administrative institutions (Prime Ministry, Ministry of Finance, Central Bank of Jordan, Ministry of Planning, Department of Statistics, Civil Service Bureau and the National Information Centre) within the Royal Government of Jordan.

The report contains the project team's findings and recommendations. It has been written and submitted by Padeco, Co., Ltd., the consulting firm awarded the contract for the services.

The consulting team is grateful for the input and advice received from the Ministry of Planning, especially Mrs. Ihab Abd Alrahim and Mr. Munir Asad, as well as the IT Directors of each of the pilot institutions, including:

- Mr. Bashar Sarayrah, Prime Ministry
- Dr. Youssef Nusseir, National Information Centre
- Mr. Hani Al Shantir, Ministry of Finance
- Ms. Zainab Al Dabbagh, Department of Statisitics
- Mr. Jamal Qassim, Central Bank of Jordan
- Mr. Samer AlNasser, Civil Service Bureau

List of Abbreviations

ACL	Access Control List
AD	Active Directory
ADSL	Asymmetric Digital Subscriber Loop
ATM	Asynchronous transfer Mode
BGP	Border Gateway Protocol
BRI	Basic Rate Interface
CBJ	Central Bank of Jordan
CCTV	Closed Circuit Television
CPU	Central Processing Unit
DHCO	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Department of Statistics
DSL	Digital Subscriber Line
ED	Enterprise Directory
EDS	Enterprise Directory Services
EGP	External gateway protocol
ERP	Enterprise Resources Planning (ERP)
ESW	Externally Sourced Workers
FTP	File Transfer Protocol
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
GCCI	Government Computer Capacity Improvement
GFMS	Government Financial Management System
GSI	Government Secure Intranet
HRIS	Human Resource Information System
IP	Internet Proticol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
JTC	Jordan Telecom Company.
LAN	Local Area Network
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
MAN	Metropolitan area network
MIB	Management Information Base
MoF	Ministry of Finance
MOICT	Information and Communication Technology
MoP	Ministry of Planning
NDS	Novell Directory Services
NIC	National Information Centre
NIC	Network Interface Card
OSPF	Open shortest path first protocol
PDA	Personal Digital Assistants
PKI	Public-key infrastructure
PM	Prime Ministry
POP	Point of Presence
PRI	Primary Rate Interface
PVC	Permanent Virtual Circuit
RAM	Random Access Memory

ROI	Return on investment
SMS	System Management Server
SNMP	Simple Network Management Protocol
TCO	Total Cost of Ownership
TCP/IP	Transmission Control Protocol/Internet Protocol
ToR	Terms of Reference
TRC	Telecommunication Regulatory Commission
UTP	Unshielded Twisted Pair
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Protocol
Wb-HRIS	Web-based Human Resource Information System

Executive Summary

Although this report focuses on the design of a pilot network, it really comprises three separate studies, each with a different target audience and purpose, that address a range of issues associated with establishing a network.

The reason for this diverse report lies in the reality of data communication networks themselves-- they are inherently more complicated than just a means to transfer information from one organisation to another. Installing a data network quickly produces an array of questions such as:

- How is the network to be used and how is its cost to be justified?
- Who will manage and administer the network? Who will have access to what information? What security risks will it introduce to each organisation?
- What is the most cost effective, reliable and flexible way to link the organizations? What factors need to be considered in the network's design and configuration?

The original purpose for designing the pilot network is to improve the efficiency of government operations and to provide the infrastructure for the eventual introduction of a Government Financial Management System (GFMS). However, the project team feels that to justify the network's expense, the Government must first add value to it by implementing software applications that use the network and promote collaboration between agencies.

An integrated GFMS is urgently needed in the Government. There are over 108 separate, heterogeneous financial and administrative systems currently in use, and the overhead and expense of developing and maintaining these information systems is placing an excessive burden on the IT departments of the line ministries and agencies. Furthermore, these diverse systems prevent the Government from having real-time, comprehensive and easily verifiable information about fiscal operations. Before the Government can develop its "front office" services to the public through on-going e-government initiatives, it must radically improve its "back office" business processes and procedures. In e-government parlance, it needs to strengthen its "G2G" operations before it will be able to effectively provide "G2B" and "G2C" services.

Lessons learned from other countries show that it is best to build an integrated GFMS in a step-by-step approach that allows the Government to benefit from its experiences. Also, the Government should strive to reduce its development cost and risks by exploring the use of widely-available Enterprise Resource Planning (ERP) solutions. ERP solutions are quickly becoming the norm for large corporations and Governments to improve their business functions through state-of-the-art technologies, while also reducing IT costs and the need for increasingly scare IT professionals.

The project team recommends that the Government initiate its GFMS by studying the implementation of a web-based, integrated Human Resource Information System (HRIS). The HRIS can be centralized in Civil Service Bureau, but accessible in all line agencies and ministries. This "centralized information

system with decentralized administration" model should be used for all future GFMS modules.

In addition to introducing GFMS application, the Government should consider introducing more collaborative software solutions such as intranets, collective authoring, and workflow routing. However, before these solutions are introduced, the Government must urgently strengthen its use of e-mail in its daily operations. E-mail usage throughout the Government is shockingly low, and threatens the successes of all other IT based initiatives, including e-government. The project team provides a number of recommendations for improving and encouraging the use of e-mail.

Data networks also introduce new security risks and challenges to the pilot agencies. Before connectivity is established through the network, the "readiness" of each agency to protect itself and the others must be evaluated. Security and Local Area Network (LAN) administration in each of the pilot agencies must be improved to insure that information made accessible by the network remain secure and available to only those who have been granted authorization.

Improving security and LAN administration requires looking further at the overall IT management of each agency. The lessons learned from the GCCI project, and in interviewing the pilot agencies, reveal that all of the IT departments within the Government are struggling with common issues that affect their operation and ability to provide better IT services to their organizations. These issues include: excessive turnover of experienced IT staff, increasing user expectations and demands (including external pressures such as e-government), difficulties in keeping pace with the speed of IT developments and rapidly changing technologies, as well as a general lack of understanding and support from upper management.

It is recommended that the Government focus on improving IT management in all line ministries and agencies, with an understanding that IT provides the cross-cutting services and abilities to radically improve business operations and reduce bureaucracy, contributing to true public sector reform. The first step in this process is to initiate a dialogue among IT departments and their management, and to develop guidelines and better business models for the operation of IT departments.

Finally, the project team has evaluated a number of options available for establishing data connectivity between the pilot agencies. Included in these options are two configurations that are provided by Jordan Telecomm Corporation (JTC) and one solution provided by Jordan's sole data network service provider, Batelco Jordan (BJ).

From these options the project team recommends that the Government consider obtaining the configuration provided by Batelco since they have the licensing and experience to provide a secure, reliable, and managed network solution.

1

Section 1 : Introduction

1.1 Background

The Government of Jordan is currently faced with the difficult task of improving the transparency and efficiency of its public administration, while also limiting the size and complexity of its civil service. In this new environment of increased scrutiny of government actions, heightened accountability and shrinking resources, the Government has a real need for public sector reform and improved fiscal management. To achieve this, the Government must focus on streamlining existing workflows and improving its use of information technology. Overall, the Government needs to make better use of its people by helping them to increase their productivity and effectiveness; providing better services to the public at a lower cost.

The Government is taking steps in the right direction. The latest National Development Plan focuses on public sector reform to address key areas such as strategic planning, legal and judiciary reform, and improved financial management. The Government has also made a firm commitment towards e-government; providing services through the Internet and encouraging both its administration and the public to make active use of this technology. The support for e-government demonstrates the Government's eagerness to reform its bureaucracy through the use of new technologies and processes.

1.2 Purpose of the Paper

In November 2000, the Government, with the assistance from the World Bank and with the Japanese Government, initiated the *Government Computer Capacity Improvement Project*, with an objective to design a network to connect six key financial agencies[1] in a pilot scenario. The purpose for the pilot network is to create a basis for the eventual introduction of a GFMS.

This paper represents the deliverable of this project activity, and is written with the following objectives:

- To explore the means to which the pilot network can enable the Government to operate more efficiently and effectively, thereby justifying its cost. In particular, the paper will analyze the broad financial processes of the Government, and explain the benefits that can be obtained from the integration and consolidation of these processes using the pilot network.

- To review existing IT management, network administration, and data security in the key agencies and to provide recommendations for strengthening these functions; and

[1] Prime Ministry (PM), Ministry of Finance (MoF), Ministry of Planning (MoP), National Information Centre (NIC), Central Bank of Jordan (CBJ), Department of Statistics (DoS).

- To investigate connectivity options between the key agencies and recommend the most cost-effective option

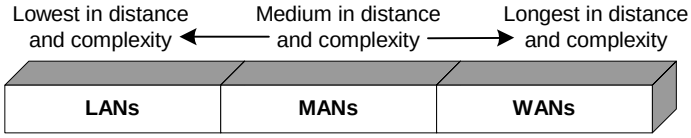
Based on these objectives, the *purpose of the paper* is to provide recommendations for the "next steps" towards establishing a network among the pilot institutions--- including recommendations on how to effectively use the network to improve the Government.

Although the report focuses on the pilot networking of six key Government organizations, the concepts and issues involved in this study are directly applicable to the entire Government.

1.3 LANs, MANs and WANs

Because there are many different forms of computer networks, it is necessary to begin with a brief description of the terminology used in this report.

Computer networks are classified according to their reach and complexity on a spectrum of three types: local area networks, metropolitan area networks, and wide area networks.



A **local area network** (LAN), at the low end of the spectrum, connects all of the computers, printers and other resources that are located within the same building or complex. LANs typically connect each resource (computer or printer) to a cable and interlink the cables at a hub in a star-like configuration. Because of their simplicity and value, LANs are the most common computer networks and most Government offices (including all of the pilot agencies) currently have some form of connectivity.

A **metropolitan area network** (MAN) spans a greater distance than a LAN and usually has more complicated networking equipment for midrange communications. A MAN links multiple LANs within a city, metropolitan region, or even a small country like Jordan. For example, a MAN will connect the LANs of the main buildings of various Government ministries together into a single network. There are two main ways to create a MAN: 1) via a direct cable, microwave, radio or satellite connection between each LAN, or 2) by utilizing the existing phone/communication infrastructure of the region. Both of these options will be reviewed later in this report.

A **wide area network** (WAN) reach the farthest distances and are the most complex. WANs link LANs or MANs across large countries or the globe and rely on the global telecommunication infrastructure. Many WANs are privately owned and managed through direct satellite linkages, however most WANs make use of the public networks, including the Internet.

The basis of this report is to design a network that interlinks key Government agencies that are all located in the Greater Amman area and can be serviced by a

sole telecommunication authority. Therefore, the report will focus on the means of establishing a *Metropolitan Area Network (MAN)* within Amman.

This report will use the terms "network" and MAN interchangeably.

1.4 Scope of Work

1.4.1 Logical connectivity

The project's Terms of Reference (ToR) states that the project team is to "design a pilot network connecting the key ministries"[2], suggesting that the scope of work should be limited to the analysis of the options and costs associated with establishing a MAN interconnecting the individual LANs of each ministry.

However, at the onset of the project it became apparent that before connectivity is established, the Government needs strengthen security and IT management as well as to justify the expense of the network. Therefore, at the request of the Government, the scope of work for this component has been broadened to review and analyze the administrative and security processes of the network, as well as to explore a possible application--- an integrated Government Financial Management System.

In doing so, the project team has expanded the design of the network to include both *physical connectivity* (providing a conduit for data exchange) between the key ministries, and *logical connectivity* (interoperability standards and guidelines, and administration necessary to maintain the MAN). This new approach is based on the following issues:

- *Existing studies*: two existing studies have been completed regarding connectivity between government organizations, one from the Prime Ministry's (PM) office and one from the National Information Centre (NIC). The PM report focused on the establishment of a completely private network connecting the major Ministries via direct fiber-optic cable between the physical locations. The NIC report reviewed two options available at the time: increased bandwidth through existing NIC channels, and connectivity via Jordan Telecom Corporation (JTC), the national phone company. The recommendations of both reports have not been implemented, presumably because of the costs and complexity of the options.

  In addition, the Ministry of Information and Communication Technology is currently undertaking a study to implement a Government Secure Intranet (GSI) linking a pilot group of Ministries. The proposed approach of the GSI plans is similar to the connectivity recommendation presented in this report.

- *Local networking options*: the networking choices available in Jordan are rapidly improving and transforming, making the best option for physical connectivity unclear at this point in time. As technologies and prices change, the best option available today may not be the best option at the time of implementation.

  The changing environment is due to a series of mergers and acquisitions in the Jordan's telecommunication sector-- starting with the privatization of JTC and

[2] Project Terms of Reference, Deliverables Item iii), pg. 4

subsequent 40% purchase by France Telecom (and Amman-based Arab Bank) in January 2000. Since that time, JTC has also purchased the nation's largest Internet Service Provider (ISP), Global One, while the second largest ISP, National Equipments & Technical Services (NETS), was purchased by Bahrain's Batelco. NET's parent company is First Telecommunications Group (FTG) which is the nation's largest privately managed frame relay data network.

The personal involvement of His Majesty King Abdullah into the establishment of state-of-the-art data communication infrastructure in Jordan has also accelerated the rate of change. His Majesty issued a direct challenge to JTC & France Telecom to create a fiber-optic communication backbone by the end of 2000. The result of the challenge is JTC's new ATM transmission network which was inaugurated in February 2001 connecting the Greater Amman area with the FLAG global network in Aqaba.

These mergers and investments have resulted in substantially improved services at much lower prices. However, the pricing structures are still in flux and the reliability of the new services are unknown.

- *Readiness for connectivity*: Security remains the predominate concern about connectivity. When connectivity is established via a public network such as the Internet, the main fear is generally unauthorized access of information from unknown third-parties. However, even in a completely private network (for example, through direct fiber-optic connections) where secure communication between nodes exists, there remains the real problem of misuse of information and accidental disclosure from authorized users.

  The project team recognizes that before connectivity is established, minimal security guidelines must be decided and met by *all* agencies involved in the pilot network. The guidelines will establish the policies, standards and procedures, which promote the safety and confidentiality of each agency's data and information.

  Since connectivity between Government agencies involves the linking of each agency's individual Local Area Network (LAN), a prerequisite to the wider network's security is good LAN administration in each agency. An unsecured LAN is a weak link to the security of both the local network's resources and the data of all remote Ministries. Therefore, each Ministry *must be confident* of the LAN security of the other Ministries before connectivity between the agencies is established.

- *Operating cost*: The biggest obstacle to establishing a MAN is cost. Unlike LANs which involve large upfront capital investment but minimal operating costs, MANs typically need little, if any, initial hardware purchases but have high running expenses. These expenses are directly related to the bandwidth required, which in turn depends on the data traffic expected between sites. The higher the traffic, the more bandwidth needed and more expensive the network. As such, the design of a network is highly dependent on its expected use and available budget.

  The project team recognizes that it is difficult to justify the operating costs of a MAN unless significant immediate benefit can be realized. To establish benefits from the network, applications, such as the Government Financial

Management System (GFMS), which rely on constant data connectivity must be created first.

1.4.2 Civil Service Bureau

The project team has also included the Civil Service Bureau (CSB) into the list of key agencies involved in the pilot network study. This decision is based primarily on the consideration of a Human Resource Information System (HRIS) being the logical next step towards the implementation of a GFMS.

As such, this report includes the CSB into the network design and into all further cost considerations.

2

Section 2 : Approach

2.1 Approach

Based on the initial findings of the project team and the request of the Government, the design of the pilot network has been expanded to include the logical next steps towards establishing the network and preparing for a GFMS.

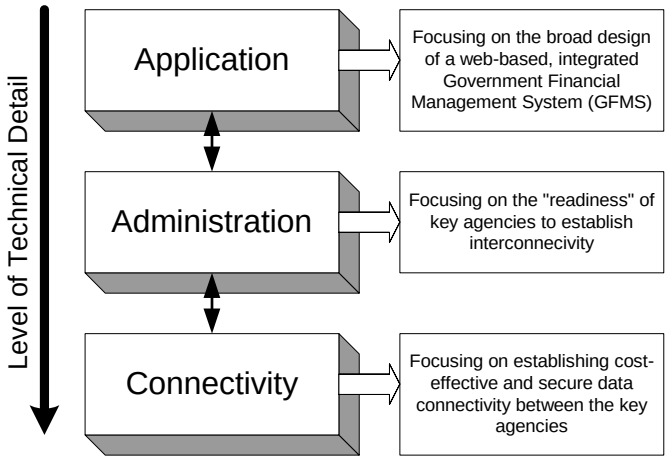
The paper addresses the following questions about the pilot network:

- how will the network be used?
- how will the network be administered, including securing information and providing reliable and useful access?
- what are the best options for connectivity, and how much will it cost to operate?

The project team hopes to highlight that establishing a network is more complex than simply providing connectivity. The cost of the network must be justified by introducing innovated applications that improve the effectiveness of Government operations. Network security and reliability depends on good IT management and administration in each linked agency. Connectivity should only be made when the network is determined to be useful, reliable and secure.

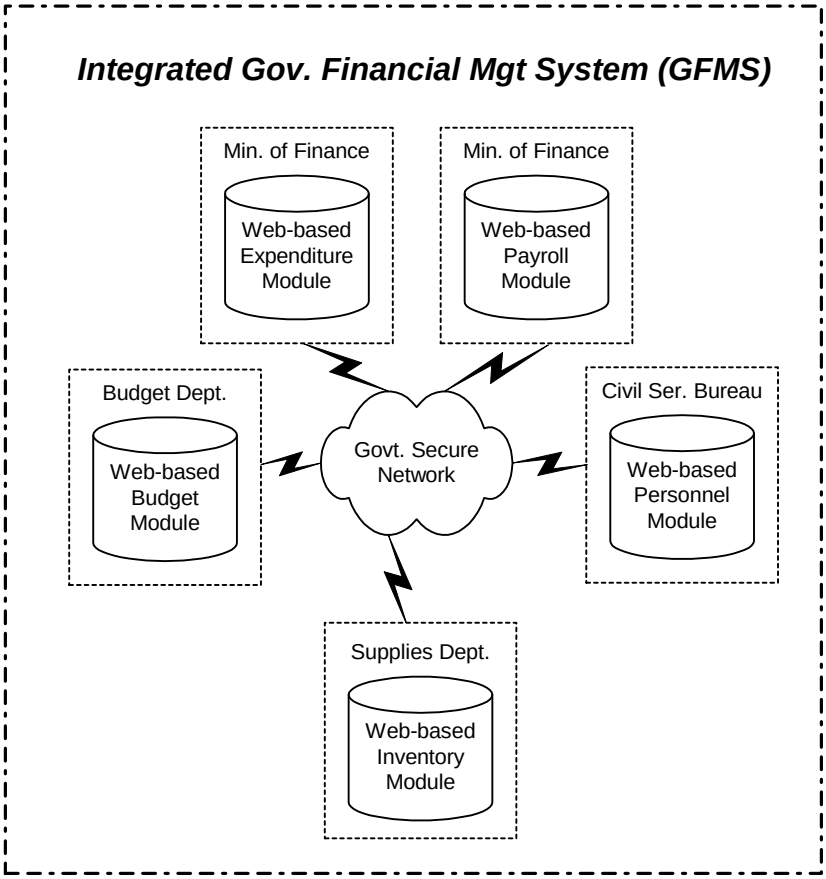
2.2 Layered Design

The project team has adopted a layered approach to the design of the network covering three main topics: Application, Administration and Connectivity as illustrated in the figure below:



2.2.1 Application Section

The report's *application section* concentrates on one of the main uses of the network-- the Government Financial Management System (GFMS). The section analyses the processes of a typical GFMS, providing a broad overview of the functions of each component and the linkages that exist between them.



The main purpose of this section is to introduce new concepts in the approach towards financial administration in Jordan. In particular, it introduces the idea of *decentralized administration with centralized information systems* using web-based Information Systems (wb-IS). In this situation, administrative processing remains in each line agency, but the information systems used by the administrative units are centralized and housed in the organisation *best suited* for their management and support. The report will explain the many advantages of this configuration.

The Government currently relies on each line agency to manage their own fiscal affairs with oversight by the Ministry of Finance (MoF) and Audit Bureau[3]. This has required that each agency develop its own information systems to support these functions. As a result, a recent NIC study found that the Government has over 108 separate administrative systems, including 81 separate accounting systems.

[3] However, the Ministry of Finance manages the financial administration of 22 line agencies which are too small to support separate financial units.

To improve its financial management, as well as to prepare for future advances in e-government, the Government needs to consolidate and integrate these systems. In doing so, the Government will substantially reduce the cost and overhead attributed to the maintenance and support of these systems. Removing these duplicate, redundant information systems will also allow the IT departments to focus on the core functions of each line ministry and to produce systems that assist in those functions.

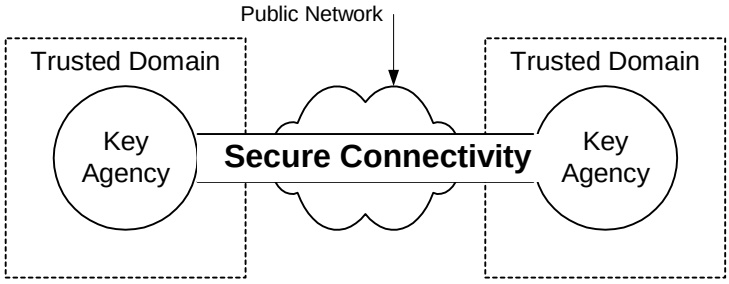
The introduction of a web-based GFMS will enable the line ministries to continue the current responsibility and administration of their own fiscal activities, but will centralize and eliminate the overhead and burdens of developing and maintaining the associate information systems.

The section will also explore other applications of the network such as enterprise directory services and collaborative "groupware" solutions such as shared bulletin boards, workflow technologies (including document routing).

2.2.2 Administration Section

The Administration section of the report focuses on the individual key agencies and their "readiness" to connect together into a MAN. The section reviews the current IT management and LAN administration in each of the key agencies, and provides recommendations for improvements.

An important issue to highlight is that the use of advanced technologies can provide safe and secure data transfers between organizations, but it cannot protect information from unauthorized access or negligence from users *within* the secure network. As illustrated in the figure below, secure connectivity can only be established between two agencies if each agency "trusts" the other agency's internal security. An unsecured agency is a weak link in the chain and poses a security threat to all other agencies on the network.



The report's Administrative Section analyses the current situation within each key agency and suggests some "best practices" for improving the security integrity and capacity of each organisation.

2.2.3 Connectivity Section

The report's last section, Connectivity, reviews the broad options available for establishing data communication between the agencies and explores the most cost-effective options.

As noted earlier in this report, there are many options currently available in Jordan for creating a network between the key agencies. Each option differs in speed, reliability, security, flexibility and cost.

The report's connectivity section will explore the two main types of MAN options available: i) creating a completely private network by establishing a direct connection between each LAN, or ii) using the public telecommunication infrastructure of the region.

The report will review the main options for connectivity available in Jordan and will recommend the best approach for this point in time. However, it must be noted that because of the rapid changes in Jordan's telecommunication sector, the project's recommendations may not remain the best options at the time of implementation. As noted above, as the technologies and costs change the best connectivity options might vary.

3

Section 3 : Applications

3.1 Introduction

A network's design is based on its anticipated use. This section of the report describes how the pilot network can be used and what benefits can be derived from it.

Maintaining a MAN is expensive and to justify the cost the Jordanian Government must realize substantial benefits from it. While there will be immediate gain from improved communication and access to distributed resources, the real benefit will be derived from new applications that make full use of the network.

As previously mentioned, the most significant application to justify the expense of the network is the long-term development of an integrated GFMS. Since a GFMS relies on full interaction and data exchange among different organizations, a data network is necessary. This report section will review a GFMS and why it is important to establish such a system.

In addition to a GFMS, benefits can also be realized by other collaborative software applications such as improved electronic mail, online "meetings" and discussions, public bulletin boards and other groupware functions.

The Government will want to consider building an "intranet" for internal use. Intranets are basically an internal internet --- in other words, a network that uses Internet protocols and services to connect computers at a single location or at locations throughout the country or the world. Most intranets are set up primarily to make documentation of one sort or another more widely and more easily available.

However, one of the main concerns of the project team is the Government's current low use of e-mail. Most collaborative software relies heavily on e-mail and the Government's low usage jeopardizes the success of future initiatives. Recommendations for improving e-mail use throughout the Government are provided in this report section.

3.1.1 Existing Data Exchange Between Pilot Agencies

The project team started the design of the network by looking at the existing applications and current exchanges of data between the pilot agencies.

Initial interviews with the IT Directors of the pilot agencies determined that very little data is currently being electronically transferred between the organizations. There are no established communications links other than through the Internet. The agencies currently rely on web sites for publishing information, or on informal exchanges via e-mail, diskettes, or occasional transfers of databases. All of the pilot agencies have a web site, and the NIC continues to support the National Information System (NIS) which has links to a wide variety of information.

The CBJ and MOF have established a dial-up connection between the two organizations so as to provide the CBJ access to MOF's debt management software, DMFAS. Although the modems and analog lines are ready, the connection is not being used because the MOF has not yet officially inaugurated the DMFAS system.

To determine *desired* data exchanges between agencies, the project team developed and circulated a questionnaire (attached as Appendix A). IT Directors were asked to distribute the questionnaires to the heads of all departments and to assist in collating the results.

The questionnaires showed that although there is currently little need for real-time, direct access to databases within other ministries, there is a strong need for *information* from the agencies.

However, the exchange of financial and economic data between the pilot agencies and the MOF and CBJ were the most cited examples of the desired data exchanges. Practically every agency requested more access to budget, expenditure and personnel information housed in the financial organizations.

3.2 Government Financial Management System (GFMS)

3.2.1 Introduction

The objective of the pilot network is to facilitate communication and data exchange between various key government agencies so as to encourage synergistic business processes and thus improve the overall efficiency and effectiveness of the Government.

However, a network by itself cannot achieve the above goals. To encourage synergistic activities and to streamline processes, the Government must implement integrated software and managerial systems that facilitate data exchange and automate various activities, and provide comprehensive, real-time information for decision making. The two components-- the network and the information systems-- must go hand in hand to achieve any real benefit.

The Government of Jordan has long taken advantage of computerisation to improve its financial management but it has not applied a comprehensive, integrated approach to its financial systems. Computerisation of fiscal activities has been ad hoc, and individual line agencies have been left to design and develop their own systems. This has resulted in duplicated efforts, excessive expenditure in software and hardware, and inefficient use of limited IT personnel. Furthermore, the Government is unable to obtain real-time, comprehensive and uniform information about its fiscal operations from these heterogeneous, distributed systems.

The link between good information systems and improved public expenditure management has long been understood and promoted by the World Bank and others. Financial management information systems provide decision makers and managers with the tools necessary to control aggregate spending, prioritize expenditures across various programs and projects, and improve operational efficiencies.

To increase the performance of government requires the integration of individual financial information systems. The integration must be both *vertical*-- through the planning, budgeting, and financial management cycle, and *horizontal*-- through accounting, personnel cash management and auditing activities.

Developing an integrated, GFMS is not an easy task by any means. It should be viewed as a long-term, multi-phased vision that will require endless improvements and modifications. While some countries attempt a “big-bang” approach to developing a GFMS whereupon the entire system is designed and implemented at once, the generally recommended method is that the system be modularized and created step-by-step. The modular approach is recommended in Jordan based on the large number of existing operational systems, including debt, tax and expenditure control, and the complexity and time required to move towards integration.

One of the recommended options available to the Government of Jordan to quickly and efficiently establish a GFMS is to make use of one of the many Enterprise Resource Planning (ERP) systems that currently exist in the marketplace. ERP systems are developed using the best practices found in other countries and allow the Government to focus on the business application of the software rather than its design and development. While the purchase and implementation of an ERP solution is expensive, the Government will likely find

that the overall cost/benefit is substantially higher than developing similar applications locally.

This section of the report will look at the broad processes of establishing a GFMS in Jordan as a potential primary application to the pilot network. The section also reviews ERP solutions and details some of the larger vendors in this field.

However, this section is not an exhaustive design of a GFMS, nor does it provide recommendations towards an individual solution. The purpose of this section is to encourage the Government to recognize the critical need for a GFMS and to initiate the necessary steps towards its eventual implementation.

3.2.2 GFMS "Vision"

The GFMS 'vision' is to create a single uniform management system that is used by all Government agencies and that is accessible using the Internet. The GFMS will strive to create excellence in accounting, which is the foundation for almost every form of analytical performance management. This includes the ability to:

- collect accurate, timely, complete, reliable, and consistent information;
- satisfy agency management needs and reporting;
- support government wide and agency level policy decisions;
- support the preparation and execution of agency budgets;
- facilitate the preparation of financial statements, and other financial reports in accordance with existing legislative and Ministry of Finance reporting requirements;
- provide information to central agencies for budgeting, analysis, and government wide reporting, including consolidated financial statements; and
- provide a complete audit trail to facilitate audits.

The GFMS will retain the "value" or "quality" of fiscal information as it is reported up the organisation, avoiding the common problem of deterioration of accuracy as data is summarized several times while it moves up the reporting layers. A GFMS will provide comprehensive, real-time and accurate information at any level, at any time.

The basic idea behind a GFMS is that all data is entered only once at the most appropriate location. All data is stored in shared databases that are accessible by any information system or application that require it. Core data elements (definitions) and tables are standardized and incompatibilities are eliminated.

Jordan's relatively small size and compact Government makes the establishment of an integrated GFMS a very realistic goal. There is a general acceptance of information systems in most Government operations and most civil servants are aware of the benefits of computerisation.

3.2.3 Decentralized Administration with Centralized Information Systems

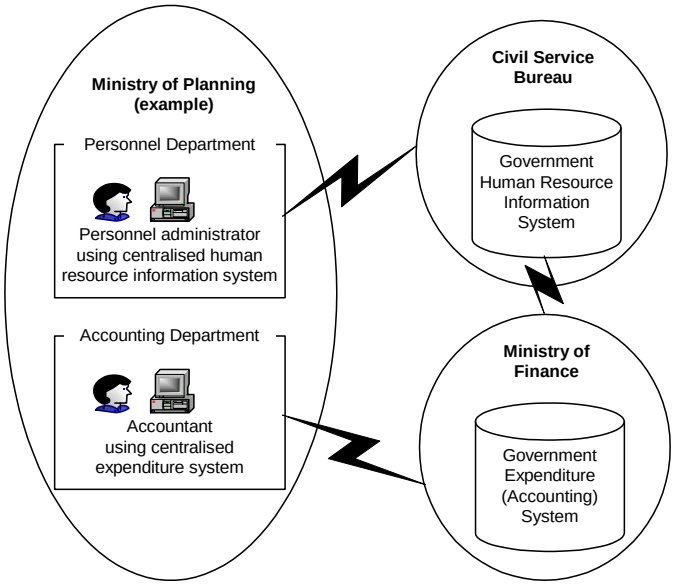
There are two main reasons why the Jordanian Government has not previously adopted an integrated approach to its administrative and financial systems:

- There is a culture of decentralization of administrative tasks to each line agency and ministry. Each agency and ministry is responsible for its own personnel, payroll and accounting operations[4], and maintains the staff necessary for these functions; and

- In the past, it was technically very difficult to establish centralized information systems. Jordan's data communication infrastructure was previously very limited and expensive.

Recent technological changes, however, have made the creation of centralized information systems much easier. The widespread adoption and use of the Internet, and the invention of web-based information systems, allow the Government to more easily realize the benefits of integrated financial systems--providing a very open, portable and scalable platform to base the application.

The GFMS should embrace the *decentralized administration with centralized information systems* model. This model allows for existing business processes and procedures to remain as is in each line ministry or agency, but removes the associated burden of developing and maintaining separate information systems. The information systems are physically housed in the agency or agencies that are best suited for their development, maintenance and analysis. The figure below illustrates the decentralized administration with centralized information system model:



The model is analogous to most current uses of the world wide web. For example, when a person accesses their e-mail from website (like Hotmail or Yahoo), he/she does not know where or how the physical data is stored, yet

[4] The Ministry of Finance does handle the financial administration functions of 22 smaller agencies that do not have the internal capacity to handle these functions.

retains “ownership” of the information by entering the necessary username and password.

The model is also not very different than the current situation in the line agencies. Most accounting and personnel departments, for example, currently use information systems that are physically located elsewhere in the organization’s IT department and are accessed via the LAN. In the above model, the only real difference is that the information systems are no longer located in the organisation.

3.2.4 Benefits from Integration

By integrating its administrative systems, the Jordanian Government can expect to realize a large number of substantial benefits and cost savings. In particular, integration will result in:

- **safer and more accessible data storage** - integration will provide a single storage point for similar data, eliminating the inconsistency risks inherent in multiple databases and systems. A single database of similar information is easier to access and query, and leads to a higher quality of information.

- **considerable cost savings** - integration, and a move towards web-based applications, will allow the Government to consolidate resources and remove duplicated efforts. Redundant personnel will be freed to work on organisation-specific applications and to concentrate on specific core functions. Immediate cost savings will be realized in reduced hardware and software maintenance costs. The Government will also obtain a highly reusable software environment -- thereby eliminating the current, endless cycle of replacing obsolete and out-of-fashion software applications.

- **more flexibility in administrative policies** - an integrated system allows new administrative procedures to be quickly implemented in one or two core systems, providing flexibility to define new administrative policies and legislation. For example, a decision to modify employee pension contributions is easily changed in the single, integrated personnel system, as opposed to requiring modifications in tens of distributed systems.

- **nationwide (and global) access to administrative systems** - a web-based, integrated administrative system can be accessed by any organisation with common telephone connectivity. Single administrative offices in remote regions will have similar access to information and data as those located in the nation’s capital. Eventually, information can even be transmitted to wireless devices and thus provide access to even the most remote locations.

- **standardized administrative procedures** - integrated administrative systems require all offices to conduct work in the same manner. This will enforce standardized administrative procedures, reduce bureaucratic steps, and ease the movement of administrative personnel between organizations.

3.2.5 Financial Processes and Information Systems

The scope of the financial management systems that comprise a GFMS varies depending on one’s viewpoint of fiscal management. While there are fairly well defined core systems (including budget preparation and execution, cash management, revenue administration, personnel management and auditing),

there can be tens of other systems and subsystems that in some way link to the main core processes. These subsystems can include such specialized business processes such as debt management and asset management, or address specific areas such as customs management or pensions systems.

In their authoritative paper, *Information Systems for Government Fiscal Management*,[5] Ali Hasim and Bill Allan have summarized the systems and associated fiscal management processes that make up a typical GFMS. In the following tables, these systems, as defined by Hasim and Allan, are compared against the current situation in Jordan:

[5] World Bank Sector Series, 1999, pg. 6

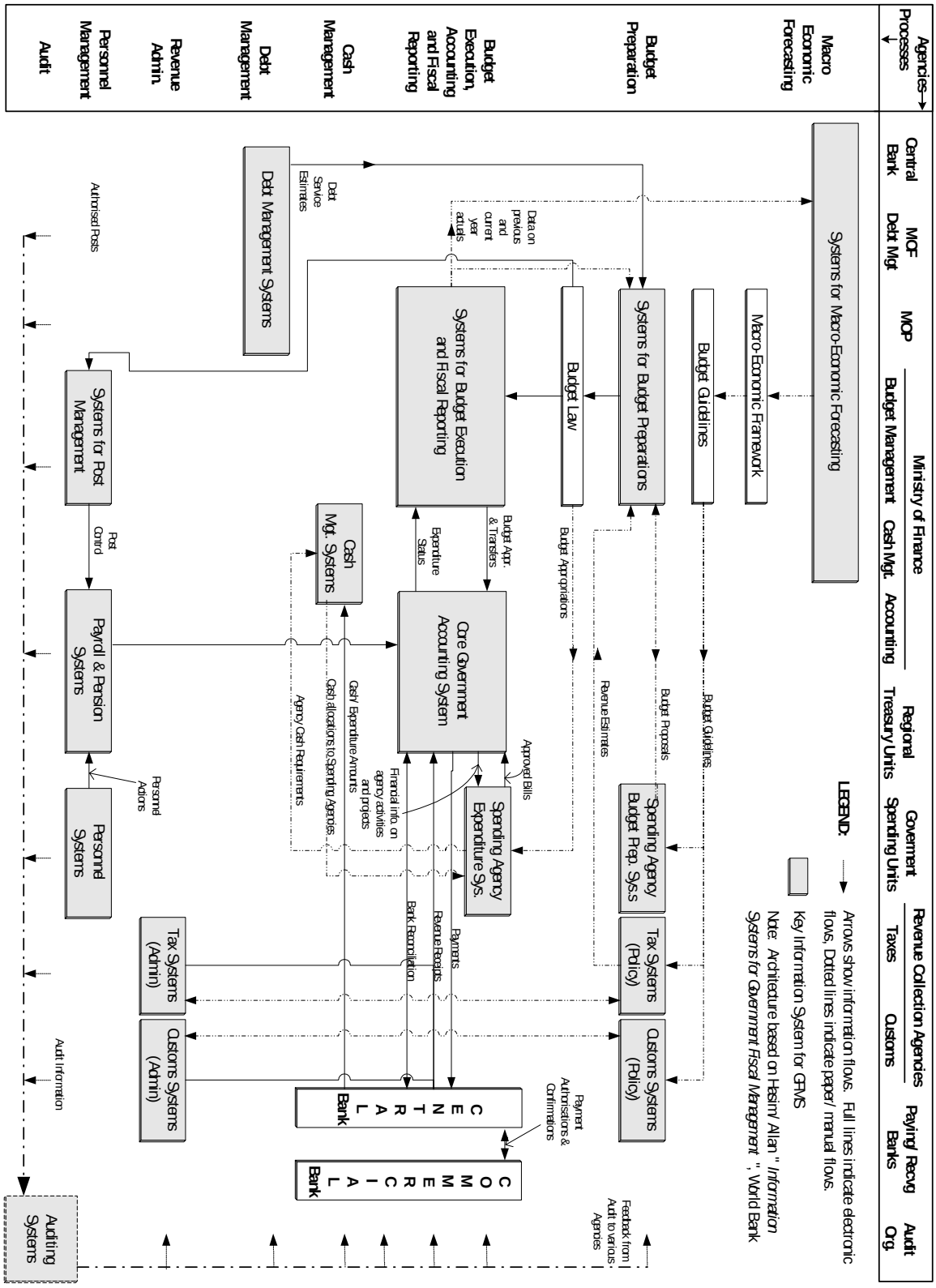
Government Fiscal Management Processes	Information System Support	Current Systems in the Jordanian Government
Macro Economic Forecasting This process assists expenditure and resource planning by developing a macroeconomic framework linking the growth of national income, savings, investment and balance of payments to public expenditures and revenue. The process helps in the development of: aggregates of the government budget, notably revenues, expenditures, and the overall fiscal deficit and its financing; the balance between the capital and recurrent components of the budget; composition of expenditures to the main sector spending agencies; revenue forecasts consistent with macro-economic assumptions; forecasts of non-tax revenues based on macroeconomic projections; estimates of resources available from domestic and external borrowings; projections of current expenditure.	***Information Systems to Support Macro Economic Forecasting*** This group of systems assist the MOF with macro fiscal forecasting and development of the macroeconomic framework. This is in turn used by the MOF to advise cabinet on aggregate budget parameters and guidelines for budget agencies to submit budget estimates. These systems require data from external economic databases, and the assumptions regarding GNP, inflation rates, and the central government deficit. In addition they require information on programs and projects that the government intends to implement, data on estimates of tax and non-tax revenues, and data on domestic and external borrowings.	***Jordanian Macro Economic Systems*** The Government has no comprehensive macro economic information systems, although the National Information System (NIS) assists to consolidate much of this information together. Most macro economic forecasting and modeling is performed ad hoc by the MoF using spreadsheets, manually deriving data from a variety of sources. The Ministry of Trade and Industry and the Central Bank both have systems that aggregate economic data and produce statistics. None of these systems are coordinated or interconnected.
Budget Preparation The process of budget preparation starts with the development of a budget circular indicating economic prospects, broad policy objectives, how the budget is expected to attain them, and sectoral allocations/ceilings consistent with the macroeconomic framework. The next step is the preparation and analysis of line agency expenditure proposals and revenue forecasts and their consolidation into an annual budget document after a series of discussions at cabinet level, between line ministries, the MOF, the budgetary committees of parliament and approval by legislature. These discussions focus on how the budget proposals would meet the policy objectives outlined in the budget circular, on inter-se priorities of the various proposals, the validity of the resource requirements contained in these proposals and how they can best be accommodated in the overall budgetary envelope.	***Systems to Assist in Budget Preparation and Approval*** The Budget preparation systems receive details of ongoing and planned programs and projects from the various line agencies, consolidate them, and produce from them the documents that form the basis of the negotiations between the line agencies and MOF. After finalisation of the budget by cabinet, the systems produce the approved budget estimates. The systems record and maintain the budgetary proposals and income estimates of all government agencies and record any changes during the budget preparation, approval and amendment processes. To assist in the evaluation of the budget proposals the system should be able to access and generate the baseline data on the manpower component, the maintenance, and other operating expenses from the relevant past-year databases. Examinations of the capital expenditures requires data on the status (physical and financial) of government-approved projects (both locally and foreign-funded). The budget preparation systems need to be supplemented with tools (such as those for cost-benefit analysis, evaluation, and performance measurement) that assist the sector and core agencies (MOF) in deciding between alternative program proposals.	***Jordanian Budget Preparation Systems*** Annual Budget Guidelines are prepared manually by the MoF. There is no comprehensive system to assist line ministries and agencies develop budget proposals. Each organization develops its budget proposals in a different way, usually manually or with spreadsheets. Budget proposals are received in paper format, and manually re-entered by the General Budget Department (GBD) into an Oracle system ("General Budget System") that assists in the preparation and printing of the Budget Law. The system also produces a large number of summary reports that provide information on planned revenues, expenditures, loans to be received, and estimated debt servicings.

Government Fiscal Management Processes	Information System Support	Current Systems in the Jordanian Government
Budget Execution, Accounting, and Fiscal Reporting This set of processes covers the functions associated with implementing the budget, including the procurement of goods and services in accordance with budget estimates, the recording and accounting of all government transactions, and development of periodic reports to monitor the overall flow of spending or use of appropriations over the course of the year, highlighting major deviations from the planned budget and suggesting corrective measures.	***Systems for Budget Execution, Accounting and Fiscal Reporting*** These systems are the centerpiece of the GFMS network, the primary repository of financial data, and serve as the basis of the government's Financial Management Information System (FMIS). These systems are used to perform the processes associated with budget execution, monitoring and control to obtain the status of actual expenditures on ongoing projects. These systems also monitor and evaluate the overall budget implementation process and produce the necessary fiscal reports. In addition, these systems would provide useful financial information to the line ministries, and spending units (in their respective areas) to enable them to better manage their work programs. System support is focused on four main systems: (1) budget and warrant control; (2) accounts payable; (3) accounts receivable; and (4) the treasury or financial general ledger system. Together they constitute the government's Core Accounting System. The first of these is concerned with maintaining data on spending authority. These systems maintain data on approved budgeted appropriations (both capital and recurrent), sources of financing for programs and projects, budget transfers, and supplementary allocations, fund releases (warrants) against budgetary allocations over the course of the year. The second and third group of systems are used to process transactions electronically as they occur, and record data on commitments and actual expenditures against budgeted allocations.	***Jordanian Budget Execution and Accounting Systems*** To monitor the budget execution, the General Budget Department (GBD) has developed a “Budget Follow Up System” (BFS) that is designed to compare the monthly financial transactions of each agency against their budget allocations. The system also generates reports showoing actuals versus budgeted revenues and expenditures. Although the BFS was developed in-house four years ago, it has never really been implemented to its original vision. The GBD wants to continue to modify it. All line agencies are responsible for developing their own expenditure and accounting systems. The MoF has created a standard system using FoxPro that was offered to 49 institutions. The status of those systems is unknown, and the MoF has been forced to stop providing support due to limited staff and resources. All of the systems are stand-alone installations. The NIC has reported that there are 108 different financial systems currently in use throughout the Government.
Cash Management This includes the processes of developing agency and central cash flows forecasts, the release of funds to spending agencies, the monitoring of cash flows and expected cash requirements, the issue and redemptions of government securities for financing government programs.	***Cash Management Systems*** The cash management systems assist Government to maintain an up-to-date picture of the government’s liquidity position and cash requirements. It obtains information on actual agency expenditures and cash balances in government (including agency) accounts from the general ledger. Revenue inflows, borrowings, loan disbursements, treasury bills, government bonds, and cash deposit maturities are obtained either from the general ledger or from the specific systems for these areas, for example, the debt management system. Using this information, the government can decide on (a) budget ceilings and fund releases to line agencies; and (b) the timings of the issues and redemptions of government securities to provide short-term financing for shortfalls.	***Jordanian Cash Management Systems*** The CBJ and MoF both have some form of cash management systems. The CBJ maintains a banking system that allows it to monitor account balances, etc.. There are no specific systems to manage capital market operations or auctions. Almost all activites are tracked using a wide-variety of custom developed spreadsheets and rely on the individuals who created them. The MoF has a limited treasury and central accounts system.

Government Fiscal Management Processes	Information System Support	Current Systems in the Jordanian Government
Debt Management This process defines the tasks associated with maintenance of records on all contracted public debt on an individual loan basis and classified according to source and type of loan. This process also assists economic and policy analysis by determining, for example, the debt implications of different fiscal and deficit financing policies by preparing projections of debt service commitments under existing and anticipated contracts.	***Debt Management System*** These systems maintain information on public domestic and external borrowings. This includes information contained in loan documents and transactions and issues of government securities. In addition to accounting information, these systems also provide important information required in the formulation of fiscal policy, such as forecasts of draw down and debt-servicing liabilities, and debt implications of various fiscal and deficit financing policies. Payments related to government borrowings are carried out by the central system based on the data in the debt management system. Loan receipts recorded in government accounts are processed by the central accounting system and then used to update the debt database maintained by the debt management system.	***Jordanian Debt Management Systems*** Since 1998, the Government has been moving towards consolidation of its debt information using UNCTAD Debt Management and Financial Analysis System (DMFAS). Previously, the Government maintained two different systems: a GTZ-financed application built and maintained by the MOP, and a Foxpro database and a collection of spreadsheets maintained by the MOF. The new DMFAS is nearing completion and is housed in the MOF. It contains information about all public debt, although disbursement data of external development loans is still sourced from the MOP. Eventually the Government should merge all systems and provide access to the sole DMFAS system to both the MOP and CBJ, with links to the eventual GFMS. Current difficulties in switching to DMFAS are due to technical problems with the application resulting in a lack of confidence is its capacity and accuracy. A clear mandate on debt management also needs to be established between the MOF and MOP.
Revenue Administration The process deals with formulation and administration of tax policies and covers the actual levy and collection of revenues including taxes and duties as load down in these policies, and the valuation and collection of non tax revenues, such as stamp duties, user fees, charges for services, etc.	***Systems for Revenue Administration*** This group of systems assist the government in the processes associated with the formulating tax and tariff policies and the subsequent collection of tax and non tax revenue. A number of separate systems are involved in this group: for example, those supporting the administration and collection of income taxes, customs duties or VAT, and those supporting the collection of various types of non-tax revenues, such as stamp duties. The revenue administration systems provide summary information on revenue collections to the Core Accounting Systems. Revenues collected by the tax and customs administration departments would be recorded at an aggregate level in the Financial Ledger System, and would be reconciled with deposits made in the banking system.	***Jordanian Revenue Systems*** All revenues systems used by the various Tax Departments have been developed in-house. A VAT system is currently being installed with British assistance (with Pricewaterhouse & Coopers). However the system is not operational, and the Government feels that it requires many custom modifications. The system is not designed to be linked to any other systems. In Customs, the Government have installed ASYCUDA in 1998 and it is currently being used by all offices and many larger private sector importers.

Government Fiscal Management Processes	Information System Support	Current Systems in the Jordanian Government
Personnel Administration This covers the activities associated with the development and maintenance of government's human resource policies including manpower planning, complement control, civil service pay and pension policies, and the fiscal impact of these policies and administration.	***Human Resource Information Systems*** The aspects of personnel management which are relevant from the point of view of the GFMS are the processes associated with post management and complement control and with payroll and pension payments. The corresponding system modules therefore form important elements in the GFMS network of information systems. The payroll, pensions and employee advances systems periodically post summaries to the central system.	***Jordanian Personnel Systems*** Every line ministry and agency has developed its own personnel and payroll systems. All of the systems are unique and heterogenous. Many of the systems are on their 2nd or 3rd revision. The Civil Service Bureau (CSB) has a database of all civil services (and applicants) but admits that the data, which voluntarily submitted by each agency,, is far from accurate. The General Budget Department (GBD) also produces a "manpower table" every year as part of the budget preparation exercise. CSB plays a little role in this process, and most data is received manually by each agency and re-entered.
Auditing The process deals with formulation and administration of tax policies and covers the actual levy and collection of revenues including taxes and duties as load down in these policies, and the valuation and collection of non tax revenues, such as stamp duties, user fees, charges for services, etc.	***Systems to Support Auditing*** Auditing takes place at two levels: internal audit at line ministries during the course of the fiscal year, and external audit by the auditor general through random checks and on the final accounts for the fiscal year. These systems assist the internal and external audit agencies in their functions.	***Jordanian Auditing Systems*** All Government insitutions have an internal audit department, which reports directly to top management. Most auditing is performed manually, although some agencies, like the inspection and control department, have a custom-developed application. The Central Audit Bureau has a simple "auditing book system" developed in FoxPro, but it generally does not rely on information systems for its auditing operations.

Information Systems Architecture for GFMS



3.2.6 Enterprise Resource Planning (ERP) systems

3.2.6.1 Overview

Developing a GFMS is an enormous task and most organizations realize that it is not cost-beneficial or possible to develop such systems themselves. As such, most large companies and many Governments are turning to Enterprise Resources Planning (ERP) software as a means to quickly and cost effectively obtain GFMS solutions.

An ERP software application package is a suite of pre-engineered, ready-to-implement, integrated software modules that cater to all the business functions of an organisation.

ERP packages reflect the idea that the "sum is greater than the parts"--- in other words, that integration of individual systems is much more powerful than the standalone systems apart. ERPs consider every transaction to be part of the inter-linked business processes that make up the entire organisation.

The Jordanian Government should actively review ERP solutions as a means to quickly develop integrated, powerful and complete financial information systems. The use of ERP solutions is a very realistic option for the Government to solve its current IT needs rapidly, using state-of-the-art technologies and processes.

ERP solutions are very industry-specific. Many of the large ERP vendors supply solutions that are custom designed for the public sector. These solutions contain a large database of "best practices" that promote efficient processing through automated workflows and better integration of common tasks.

The implementation of ERP solutions also provide the opportunity for organizations to "re-engineer" existing business processes and tasks. The procurement and installation of an ERP package, and public sector reform will go hand-in-hand.

3.2.6.2 ERP Benefits

The key benefits of ERP solutions are integration, flexibility and reusability. The following summarizes the many benefits of ERP packages:

- **built in best practices** - The advantage of implementing an off-the-shelf ERP package is that it has already completed broad research and has vast experience in defining and establishing best business practices. The Government benefits from the analysis and efforts of thousands of other customers.

- **hierarchical access to detailed data** - Because of its cohesive design, a user can continue to "drill down" on information to access the core data elements that make up the information. For instance, if a user is looking at an agency's expenditure information--- with the proper authentication, he/she can then double-click and see all of the transaction data that make up the expenditures.

- **centralized data** - ERP packages provides organizations with a centralized control point, eliminating the duplication of records and creating consistency in

record input. Centralized data is easier to support, maintain and analyze. In fact, without centralized databases the Government will never be able to get a true comprehensive picture of its fiscal activates.

- **real-time information** - as soon as a transaction is entered into an ERP package it is instantly available throughout the organisation. Users experience immediate online notification of transactions. There's no need to wait for paper verification. The ERP system updates everything instantaneously.

- **audit trails** - for every transaction you complete in most ERP packages, the system creates a *document*, or internal record of the activity. Users can view the history of all documents that apply to their jobs. This feature enables organizations to quickly and easily maintain audit trails, often an arduous task when working with separate systems.

- **accessibility** - ERP packages make it easy to find information through searches. Users can create standard or customized reports. Data accessibility is restricted only to specified user rights.

- **tracking** - the extensive monitoring and auditing features of most packages also allow the customers to obtain tracking information about workflows and processes. The Government will be able to easily determine where bottlenecks are occurring in business processes.

- **minimized mistakes** - because most of the ERP packages have been extensively analyzed and tested, the software is very thorough. Data entry mistakes are caught when they occur and the software uses its built-in intelligence to avoid logical mistakes also.

- **substantial technology savings** - ERP packages allow organizations to avoid the endless cycle of rewriting obsolete software applications, and always playing "catch up" with the latest technologies and trends. As technologies change and as innovations appear in the industry, the ERP package will be upgraded and improved. Customers only have to follow the upgrade path which is substantially easier than following industry movements and trends.

3.2.6.3 Shared and uniform databases

Because all ERP packages share a common set of shared databases, they basically integrate the different processes necessary to conduct business into a centralized pool that facilitates data sharing and eliminates redundancy. The advantages of this approach are:

- Data is only entered once into the system;

- Data analysis is simplified because it has been standardized and centralized;

- The entire system is based on reliable file structure;

- It is easier to build new modules that interlink with existing systems; and

- New possibilities in data mining and warehousing emerge.

3.2.6.4 Focus on business not software

The most important benefit of ERP solutions is that they allow the Government to focus on its business without being held back by software development and its complications and risks. ERP is first and foremost a business tool that allows the organisation a unique opportunity to re-engineer existing procedures and practices. In other words, by implementing a ERP package the Government will have the opportunity to initiate a wide-range of administrative reforms that can transform the existing bureaucracy.

Most ERP solutions have a variety of good business practices built into them. SAP, the largest ERP solution provider, core product, R/3, has over 8000 business processes stored in its central database. Customers can compare existing business processes to these "best practices". Typically, during the implementation analysis exercise, customers usually choose to eliminate many unnecessary steps and thus streamline their entire operations.

3.2.6.5 ERP "Fit"

A main concern with ERP packages is how well they "fit" existing bureaucratic workflows. When a discrepancy is found, customers have two options: they can modify existing processes to match the software, or customize the software.

Both options are readily used in ERP installations, however, as mentioned above, the majority of customers find that the processes built into the software are industry "best practices" and warrant evaluation and possible acceptance.

3.2.6.6 ERP Costs

ERP solutions are big, complex and expensive. The packages are priced based on variety of factors including the modules installed, the number of sites, and the number and types of users.

Estimating ERP costs is very difficult and greatly depends on the size of the organisation, the ERP package chosen, the amount of customization, and the availability of local expertise. Furthermore, it is difficult to compare costs from one country to another. In the United States, the Meta Group reports that on average, companies took 23 months to get an ERP system up and running, at a cost of $10.6 million for the implementation and another $2.1 million for maintenance over a two-year period.[6]

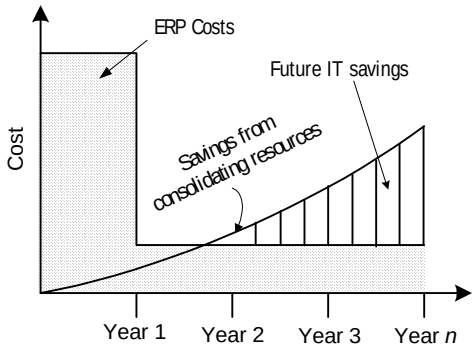
Although there is no doubt that ERP solutions are expensive to purchase and implement, the following points should be considered:

- approximately one-half to two-third of implementation costs are related to hardware, internal staff, training and consultancy[7]. These same costs would apply whether an ERP package is purchased or a similar product is developed in-house.

- organizations usually pay large upfront licensing fees for ERP software followed by minimal annual renewals. This means that the Government would be able to capitalize most costs upfront (hopefully with donor assistance) and

[6] Stein, Tom. "Making ERP Add Up", Information Week Online, 24 May, 1999. (http://www.informationweek.com/735/erp.htm)
[7] Dietz, Lisa Ramsay, What Every Business Needs to Know About SAP, Chapter 9.

then enjoy reduced annual expenditures as it recognizes long-term savings from consolidation of existing applications and resources. The figure below illustrates the potential future savings:



- an ERP solution allows the Government to avoid lengthy application design and development cycles. Therefore, it will realize the benefits of the software faster and achieve a quicker return on investment (ROI) than through traditional software development.

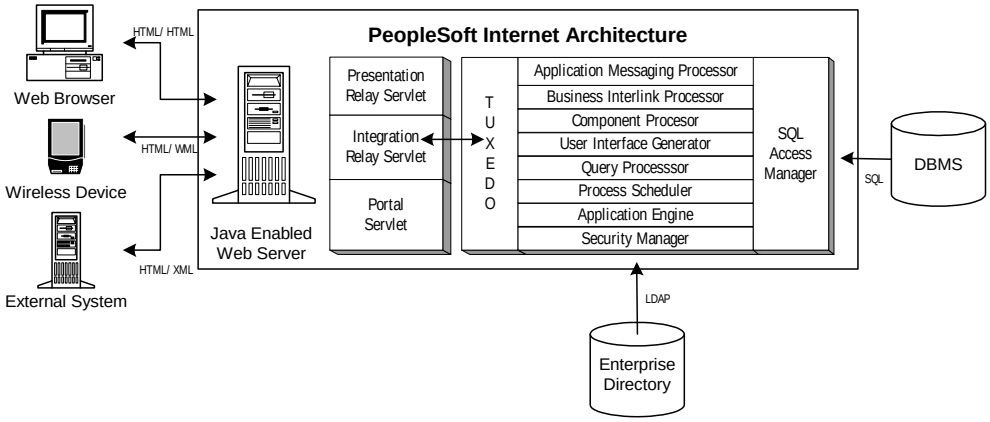
- the "failure to perform" risk of custom developed software applications is enormous. Typically over 50% of all in-house computer applications are never completed, and over 80% never fully satisfy user requirements[8]. This factor alone usually justifies the added expense of an ERP solution, whereupon an organisation can virtually eliminate this risk through proper analysis and pre-purchase evaluations.

3.2.6.7 ERP Internet Access

The most exciting feature of the latest crop of ERP solutions is their focus on using the Internet for access to the systems. In doing so, users can now access the applications using any standard web browser and operating system, even over a low-bandwidth connection (such as mobile phones or PDAs[9]). This means that a user familiar with popular web sites such as Yahoo! should be able to access and execute any ERP application with equal ease. The figure below shows the Internet Architecture of one of the leading ERP providers, PeopleSoft, and illustrates how the system can be accessed by web browsers via HTML, wireless devices via WML, and external systems via XML.

The figure also shows how the application links to the Enterprise Directory using LDAP and to an external RDBS using SQL. Enterprise Directories and LDAP are discussed in Section 3.3.4 .

[8] Kale, Vivek, Implementing SAP/R3: A Guide for Business and Technology Managers, pg. 23.
[9] Personal Digit Assistants



3.2.6.8 Market Leaders

Because of the huge benefits found in implementing ERP solutions global ERP sales have been substantially increasing during the past decade. While there are hundreds of vendors, the top four, SAP, Peoplesoft, Inc., JD Edwards & Company, and Baan International, account for 64 percent of total ERP market revenue[10]. These vendors continue to play a major role in shaping the landscape of the ERP industry and expanding product functionality. A brief review of the major vendors is provided below.

3.2.6.9 SAP, AG

SAP, AG is the largest suppliers of ERP software, and the third-largest software company in the world. Headquartered in Waldolf, Germany, and founded in 1972 by five former IBM systems engineers, SAP now employs more than 24,000 people in more than 50 countries. SAP software is used by companies of all sizes, including more than half of the world's top 500 companies. SAP had revenues of over 6.27 billion euros ($5.26 billion) in 2000.

Today, SAP R/3 (SAP's first application operating in a client/server system architecture) is used by more than 13,000 customers in over 100 countries. SAP currently provides business solutions for 22 major industry sectors including oil and gas, health care, automotive, and high tech and electronics, and public sector.

At the heart of SAP Public Sector are the financial accounting applications for public administration. It provides functions for public budget planning, management of appropriations, cash accounting and annual budgeting in public sectors based on FI (Financial Accounting) and CO (Controlling) applications. SAP Public Sector is a completely integrated, modular, ready-to-run standard business software package. Alongside Financial Accounting, it provides modules for Human Resources, Logistics, Property and Facility Management, Project Systems, Workflow and Treasury.

SAP, AG maintains offices in Saudi Arabia and Dubai. An Arabic version of the SAP website can be viewed at: http://www.saparabia.com/arabic/index.htm.

A complete list of SAP Public Sector Solutions are provided in Appendix B.

[10] Anonymous, ITToolbox ERP Solutions, Market Survey Results.

3.2.6.10 Baan

Baan was founded in The Netherlands in 1978. It is wholly-owned by Invensys pc, and has an annual turnover of about $2.5 billion. The company is one of the top software firms in the world.

Baan is using an approach in which customers and experts from different sectors of industry, as well as advisors from different universities, help develop the best practices in its software. The company focuses on 7 core industry solutions including Aerospace and Defense, Automotive, High Technology, Industry, Construction, Metals & Paper, and Telcos.

Baan focuses primarily on private sector industries and does not have a specific public sector solution package. Their solutions are used by leading manufacturing and service companies worldwide. Unlike other ERP packages, Baan products are not designed to be modular and typical installations involve the entire software package.

3.2.6.11 JD Edwards

JD Edwards has produced software for over 20 years and is one of the leading ERP solution providers. It has 5,000 employees operating in 60 countries servicing customers worldwide. It software is used in 21 different languages. In 2000, JD Edward had revenues of $1 billion.

JD Edwards concentrates on providing business-to-business software solutions that enable collaborative commerce. JD Edwards latest collaborative product, OneWorld Xe, is a web-enabled version of their ERP software design to promote the exchange of information and data among businesses. Other main business solutions include:

- Advanced Planning
- Fulfillment Management
- Customer Relationship Management
- Procurement Management
- Project Management
- Asset Management
- Financial Management; and
- Workforce Management.

JD Edwards is represented in Jordan by United Business Machines (UBM). UBM is the only IBM authorized re-marketer, and one of the leading IT providers in the Jordanian market. UBM works with regional firms like United FOQ in Egypt, to provide customization of JD Edward OneWorld products.

An Arabic version of OneWorld Xe has been recently completed.

3.2.6.12 PeopleSoft

PeopleSoft is a pioneer in the client-server ERP industry. Its original product, and continuing strength, lies in Human Resource and Customer Relations Management. PeopleSoft employs more than 8,000 people worldwide, and had 2000 revenues of over $2 billion. More than 4,700 organizations in 107 countries run on PeopleSoft eBusiness applications.

In 2000, PeopleSoft released a revamp of its product line, called PeopleSoft 8, which is entirely web-enabled and involves absolutely no code on client computers--- thereby making it the first ERP solution provider to offer a "pure" internet solution.

PeopleSoft has a wide-range of Public Sector solutions including top-to-bottom budget planning and execution, grant accounting and administration, citizen relation management, and tax and revenue administration.

3.2.7 Human Resource Information System

The implementation of a GFMS in Jordan should be viewed as a high priority to support both the on-going public sector and civil service reform initiatives, as well as to provide the foundation and infrastructure for future e-government endeavors.

As previously mentioned, the implementation of the GFMS should occur in a step-by-step coordinated manner that allows sufficient time to both increase the capacity and abilities of the Government, as well as to gain experience from initial efforts.

The project team therefore suggests that the first step toward creating a GFMS is to begin by creating a small-scale, yet extremely powerful "proof-of-concept" of establishing centralized information systems using web technologies.

While any module or sub-system can be used for the application pilot project, the project team recommends that Government begin its GFMS *by focusing on civil service management and the creation of human resource information system (HRIS)*. There are many immediate benefits from this tactic and the team's recommendation is based on the following considerations:

- **HRISs are generally the simplest sub-system to implement (however this does not imply that the task is easy!).** HRISs require fewer organizational and legislative changes to existing processes and have limited impact on other business functions. However, a HRIS requires links to other financial sub-systems including budget and expenditure, and can substantially reduce bureaucratic administrative procedures;

- **A HRIS will provide all civil servants a purpose for using computers and the internet.** This is a powerful change agent towards improving the use of computers and electronic services in the Government.

  HRISs that contain automated workflow processing, such as electronic leave/vacation requests, will encourage civil servants to modify existing bureaucracies and to understand the concepts behind e-government. An HRIS will provide all employees an opportunity to make use of IT for a purpose other than word processing and communication.

Yet, existing processes can remain for less technologically-savvy employees and agencies. The situation is analogous to the use of Automated Teller Machines (ATMs) in banking--- users realize the convenience and benefits of ATMs as and when they become comfortable with the technology.

- **A HRIS contains information that is important to the widest range of users--- from top management to individual employees.** Unlike other financial systems, the data found in an HRIS is of use to everyone. If desired, basic directory information (name, department, phone number, e-mail address) can be made available to the public via the internet. Individual employees can access subsets of their own information to verify accuracy and to help support current data.

  A well-maintained HRIS is essential for providing:

  - information about the size and scope of the civil service. This information is critical to any future civil service reform efforts;

  - directory assistance information, especially current e-mail and contact data. An improvement in the Government's use of e-mail and general electronic communication is completely dependent on easy access to directory information. An integrated, comprehensive HRIS is a critical component to this development;

- **A HRIS can be used by every line ministry and organisation regardless of staff size and complexity.** This is an important consideration for eventual rollout and implementation and demonstrates the tremendous power of decentralized information systems. Any line agency or office with a computer and an internet connection will be "on-line" and capable of managing their own personnel needs.

- **A HRIS will provide the first opportunity to re-engineer existing bureaucratic procedures and workflows.** The lessons learned from this exercise will be invaluable in future attempts to modify and automate other financial administrative tasks. It will be the first step towards a comprehensive (GFMS) solution.

3.2.8 Critical Success Factors

As noted above, the implementation is a GFMS is a long, difficult goal that includes a wide variety of reform processes including: modification of existing work habits and flows, streamlining bureaucratic procedures, and introducing new technologies and systems.

The risks associated with these reform processes are huge, and the attempts to implement such systems in other countries have had a variety of successes. The World Bank, in its involvement in many of these attempts has ascertained a list of critical factors for success. These factors, as described by Ali and Hassan[11] are as follows:

3.2.8.1 Government Commitment and Management Support

The improvement of fiscal management systems requires continued Government commitment to public sector reform and to the strengthening of the core financial management institutions. Since the introduction of a GFMS can be viewed as a means to re-engineering existing business processes and procedures, the implementation of these changes need Government support at the highest levels.

Management must fully understand the long-term benefits of integrating existing systems and moving towards the standardization of fiscal processes. They must realize that any change to existing procedures will require compromise and adaptation to new ideas and work habits. In particular, management must understand that the implementation of integrated systems is an eventual "win-win" scenario for both the central Government and the individual line agencies, and that "control" is not removed from their respective organizations, but rather added to it in the form of improved efficiencies and information.

The Jordanian Government has the highest level of support for public sector reform and improved electronic delivery of services under the leadership of His Majesty King Abdullah II. This is a unique situation among countries, and an opportunity that should be exploited by both the Government and the donor community. The Government should demonstrate the nation's pursuit to become a regional IT leader by effectively utilizing the technology in its own fiscal administration.

3.2.8.2 Inter-Agency Coordination

By definition, an integrated GFMS requires cooperation and support from all stakeholders. The active participation and involvement of line ministries is especially important in the design and selection of software and the move towards implementation.

A core requirement to the implementation of a GFMS is an understanding between all Government agencies to the rights of other agencies to information and data. Information access rights need to be clearly established by law.

Information access also requires systematic data sharing arrangements, protocols and schedules between systems.

[11] Hasim, A., and Allan, W., 1999. "Information Systems for Government Fiscal Management." World Bank Sector Studies Series, pg. 30, Washington, DC.

It is recommended that a series of steering groups and committees which represent all of the agencies involved in the process be formed and involved in all aspects of the GFMS development and management. While ownership and management of individual modules are the responsibility of individual line agencies, the systems should always be viewed as a Government asset and any changes to core modules need to be approved and accepted by all stakeholders.

3.2.8.3 Organizational Capacity and Skills

A variety of skills and expertise are necessary to create a GFMS. Existing staff will need to be retrained and their computer skills bolstered.

It is recommended that the Government make full use of the private sector in this endeavor. Missing skills or tasks can be outsourced to the private firms, and local and international consultants can play a vital role in re-engineering existing business processes and procedures. If the Government chooses an ERP solution, specialist in the ERP software will need to be hired to assist the Government in the installation and application of the software.

The Government may also need to review the salary scales of staff in key areas to retain them in the civil service. If this is not possible, than the Government should focus more on the use of the private sector in implementing the GFMS.

An on-going training policy will need to be defined and establish to provide continuous professional training to staff.

3.2.8.4 Setting Priorities for Systems Implementation

As noted, a GFMS is comprised of many systems and subsystems. It is advised that the Government take a step-by-step approach to implementing these modules. The implementation sequence and priority of each module is an important factor in the overall success of the GFMS.

The systems for budgeting, accounting, revenue administration, payroll and personnel management constitute the basic transaction processing systems for the overall GFMS.

However these same systems are usually the most difficult to implement and most likely to effect the performance of the other systems if ill-designed.

The project team recommends that the Government initiate the implementation of the GFMS by focusing on an integrated human resource information system (HRIS). The systems will provide the Government invaluable lessons in the problems that are likely to be encountered, and will demonstrate the benefits of integration to upper management. Ideally, the success of the HRIS will buoy the confidence and support of all agencies towards reforming the remainder of the financial systems.

3.2.8.5 Formal Project Planning

The implementation of a GFMS is a substantial undertaking. It is very important that all of the agencies involved in the process are aware of its magnitude and complexity. Formal project planning methodologies should be used to design and implement the system.

The Government will need a variety of people with proper project management and planning skills with experience in contracting and negotiations.

3.2.8.6 System and Data Administration

Coordinating mechanisms should be created to ensure that a common set of policies, and standards is in place for managing data and systems government-wide. The standards should cover the protocols for communications, data entry, editing, and updating screen-input and output formats, back-up and recovery, security, contingency and disaster recovery planning, as well as technical and user documentation.

3.2.8.7 Local Technical Support

Private sector support and the availability of local assistance is essential to the development of a GFMS. It is preferable that the design, implementation and long-term maintenance of the systems and modules be outsourced to a private firm or consortium of firms. Long-term contracts for system maintenance and support are recommended.

3.2.8.8 Management of Change

A successful implementation of computer-based systems require not only the proper technological and business modifications, but also an understanding of the social, cultural and political environment of the organizations. Because the systems have a direct impact on the way people do their day-to-day work, it is necessary that appropriate change management procedures be instituted. The procedures should ensure that the staff feel comfortable with the new work environment and are willing to commit to and accept the new work flows.

Typically, the initial fear behind new computer systems is that they will eliminate jobs and remove authority and from key individuals. By definition, streamlining or even re-engineering of some work procedures redefines existing power relationships and changes relative authority.

To be successful, any project implementation plans need to address these issues and allay fears.

3.2.9 Recommendations

As noted above, the project team highly recommends that the Government move towards integrating its distributed, heterogeneous financial information systems into a interlinked and standardized system. The team further encourages the Government to quickly consider this process as a prerequisite to future e-government activities and initiatives.

As stated earlier, the implementation of a GFMS is a long and complex process that will require long-term management support. There is little alternative if the Government wishes to improve its existing financial management and information accuracy.

The project team recommends the following actions towards initiating a GFMS:

Recommendation #3.3.1 : *Form a working committee of stakeholders*

As mentioned in the Critical Success Factors above, an integrated GFMS requires the full support of all agencies associated with the fiscal management. The Prime Ministry or related organisation should appoint a working committee with high-level representation from each of these agencies to initiate and oversee the GFMS process.

Recommendation #3.3.2 : *Begin the process of implementing an HRIS*

As described in Section 3.2.7 above, the project team recommends that the Government begin its step-by-step implementation of a GFMS by implementing a web-based HRIS. The lessons learned from this project will provide invaluable experience before the more complex task of developing the core accounting systems is attempted.

3.3 Collaborative Computing

3.3.1 Introduction

The purpose of establishing a network among the pilot agencies is to provide access for data communication and to promote collaborative efforts. In doing so, the Government hopes to benefit from the synergies of individuals working together, and to improve the efficiency of bureaucratic processes.

However, to realize these collaborative benefits new technologies and work processes need to be introduced and institutionalized into daily activities. For IT-based change to be effective, technology, business processes, and organization need to be adapted to each other.

Collaborative software plays a key role in this adaptation by providing the means to modify existing organizational behavior. Business process re-engineering, or BPR, involves the critical analysis and radical redesign of existing business processes to achieve improvement in performance. The marriage of these two concepts can help drive the Government to reduce bureaucracy and encourage efficient workflows.

Collaborative computing can be generally divided into two different types of applications: *groupware* and *workflow* software.

Groupware applications provides functions to promote team work and improve efficiency through:

- increasing information sharing;
- reducing communication overheads; and
- providing co-ordination.

Workflow applications help to define, create and manage the execution of work processes through the use of software. These applications are generally able to

interpret process definitions and interact with workflow participants to track and to complete specific business activities.

This section reviews and recommend various collaborative software solutions that should be considered by the Government to add value to the pilot network.

3.3.2 Groupware Applications

Groupware is software for teamwork. Groupware works because it aids communication in an organisation and helps staff work together on joint tasks. It also equips them with the information needed to complete their work and can help decision making. Groupware has grown to cover a vast range of potential applications. Groupware is only possible with the availability of a network within and between organizations that provides the infrastructure for improved communication.

3.3.2.1 Groupware's 3 C's

Groupware assists teams of people to work together because it provides key group functions; the "three Cs" of communication, collaboration and coordination:

Communication is the core groupware feature which allows information to be shared or sent to others using electronic mail (e-mail). The use of e-mail in the Government is discussed later in this section. Groupware for conferencing is sometimes known as computer mediated communication (CMC) software.

Collaboration is the act of joint co-operation in solving a business problem, or undertaking a task. Groupware may reduce some of the problems of traditional meetings such as: finding a place and a time to meet, a lack of available information or even dominance by one forceful individual in a meeting. Groupware improves the efficiency of decision making and its effectiveness by encouraging contributions from all group members.

Coordination is the act of making sure that a team is working effectively and meeting its goals. This includes distributing tasks to team members, reviewing their performance or perhaps steering an electronic meeting.

3.3.2.2 Groupware Functions

The following table illustrates some of the main groupware functions and lists the main applications with those functions:

Groupware Function	Application	Notes
E-Mail and Messaging	E-mail and electronic form processing	Original groupware function
Document management and information sharing	Improved information sharing	Currently the main use of intranets and LANs
Collaborative Authoring	Team development of documents and	Annotation, revision marking and tracking, and version control are

	spreadsheets	key elements to this function
Conferencing	Text conferencing, video-conferencing, white boarding	Relates to electronic meeting support functions
Time management	Calendar and group scheduling	Simplifies the arrangement and coordination of meetings and schedules
Team management	Task assignment and follow-up. Collaborative project management.	Lets team members interactively participate in project management activities

3.3.2.3 Groupware Software

Groupware is usually comprised of many software packages from different vendors . However, because collaboration requires interoperability there is an increasing need for standards for data exchange between the applications. There are three main software suites that are commonly used for groupware functions: Microsoft Exchange, IBM Lotus Notes, and Novell Groupwise.

3.3.2.4 Microsoft Exchange

Microsoft has packaged most of its groupware functions into its Microsoft Exchange Server and Microsoft Outlook software products. Outlook, which is bundled with Microsoft Office and is widely available, provides the front-end user interface, while Exchange Server operates the “back office” messaging and data exchange.

However, Microsoft Exchange is not just an e-mail program with scheduling and forms functions, but rather it is an entire messaging and information management environment that provides the infrastructure for a variety of workgroup communications add-in applications. Some of the popular add-ins include network faxing, document routing, and document management. Microsoft developed the Exchange Server product to provide an operating and communications environment that supports the addition of these new capabilities without the replication of administration, operation, or management of the add-in product. The global environment approach of Exchange minimizes administration and support, improves the efficiency in routing messages, and in turn maximizes the overall reliability of information management. Exchange also has the advantage of being tightly integrated with Microsoft Office products which are widely used and understood.

3.3.2.5 IBM Lotus Domino/Notes

IBM Lotus Domino/Notes is a well established groupware product that offers a wide range of groupware functionality. Sharing and distribution of information in the enterprise happens by users accessing a document database or built-in mail.

The Notes database allows unstructured text and documents to be easily stored and viewed as well as alphanumeric information.

For many years Notes was synonymous with groupware and it defined the term. However the widespread use of the internet and Microsoft Exchange, and other "open" solutions, slowed its spread. IBM has since revamped its products, introduced its web-messaging server, Domino R5 in 1999, and has redesigned its software for use over the internet. It remains one of the largest groupware product in use, and a serious contender to Microsoft Exchange.

3.3.2.6 Novell GroupWise

GroupWise version 6 was released in April 2001 and is the latest renovation of the long-time groupware product. GroupWare is a full-featured offering that provides messaging and collaboration, including e-mail, calendaring, group scheduling, task management, document management, automated workflow and electronic discussions all through a Universal Mailbox.

This version provides substantial improvement in five key areas: access, scalability, reliability, NDS[12] integration, and multiple-platform support. GroupWise wireless support also enables users to connect to the Universal Mailbox from any WAP[13]-enabled device such as Mobile phones or personal digital assistants (PDAs).

The entire GroupWise system can be managed through Novell's browser-based NDS eDirectory management interface. GroupWise also provides seamless integration with Lotus Notes/Domino and Microsoft Exchange servers.

3.3.3 Workflow Applications

Whereas groupware focus on function, workflow applications focus on the process. Workflow is generally defined as the computerized facilitation or automation of a business process. The business process may be as simple as routing a document between colleagues, or as complex as processing a tax payment from receipt to deposit. A well designed workflow system assists in both the execution of the task (.i.e., moving the document from person to person) and the reporting of the task (.i.e., number of documents processed per person or the status/location of a particular document.)

Workflow applications are generally built around a workflow server that manages the transactions. Since each business process is unique, the applications allow for the rapid modeling of each step and the inherent logic at each stage. Defining and modeling the business processes is critical to the application.

3.3.3.1 Document Scanning

Most workflow systems include document scanning and storage. Digital images are useful in many workflow applications since they are used for easy access to and storage of supporting documentation such as letters from citizens or other government agencies or departments.

[12] Novell Directory Services : a enterprise directory solution
[13] Wireless Access Protocol : the most common means of accessing the Internet on mobile devices

Unfortunately, many Government agencies are currently trying to implement document imaging systems, especially for use with “divan” or document dispatching applications, without the accompanying workflow technology or business process analysis. To implement an automated workflow, a thorough analysis and modeling of business processes must be completed.

3.3.3.2 Workflow Systems

Unlike groupware software, there are literally hundreds of different workflow solutions available in the market for virtually every industry and application. Many workflow solutions are custom developed, or are hybrids of existing groupware products such as Microsoft Exchange or Lotus Notes.

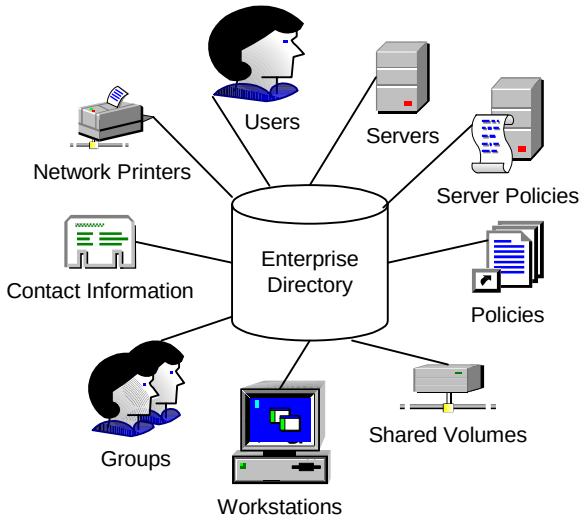
However among the more popular commercial products are:

- IBM’s Flowmark (www.software.ibm.com/flowmark)
- Eastman Software Workflow (www.eastmansoftware.com)
- Paragon’s Filenet (www.filenet.com)
- Staffware (www.staffware.com)

In addition to the above products, most ERP products such as PeopleSoft and SAP have workflow technologies built into them.

3.3.4 Enterprise Directory Services

Another core application that can make use of the pilot network is an Enterprise Directory. An Enterprise Directory (ED), and Enterprise Directory Services (EDS), is in its simplest form is a repository for user names and other resource information similar to a powerful telephone directory. The ED can then be searched to find any object linked to the network. However, an ED can easily be expanded to provide much more functionality. For example, an ED can also store information about the organisation itself-- its departments, groups and hierarchical structure. It can also maintain security and policy information, knowing who has the right to access what.



In general, an ED is a database that stores information about the enterprise and the network. How the database is used depends largely on the ED implemented and the needs of the organisation. An ED is often combined with groupware or workflow software to obtain integrated solutions and to assist the collaborative software in understanding the organization's structure.

Typically a ED is used for the following tasks:

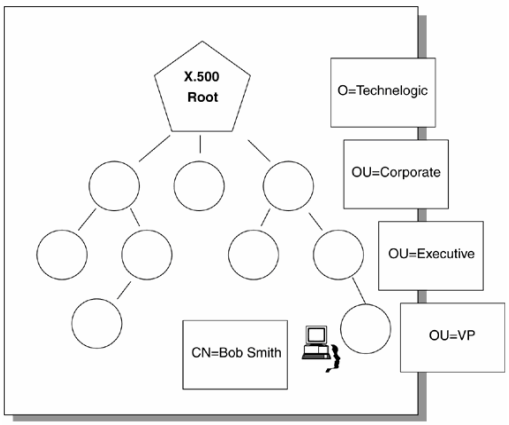
- to provide a global, unified naming service for all elements in a network;
- to translate between network names and addresses;
- to provide descriptions about the objects (resources) connected to the network; and
- to ensure unique names of all of the network's objects (resources).

3.3.4.1 Standards

Early in the development of ED technology, the computer industry had the vision of establishing links between organization's EDs to form a global directory of all people and computers. Using the internet, anyone might query the world to find another user's e-mail address and contact information.

To achieve this, it was necessary to define standards to allow the various EDs to communication with each other and to share directory information. Two of the most common standards are X.500 and LDAP[14].

First released in 1988, the X.500 standards define a specification for a global, distributed directory based on hierarchically named information objects that users can browse and search using specific fields. X.500 uses a model of a set of directory servers, each holding a portion of a global directory information base. The figure below shows a typical X.500 hierarchical naming scheme:



[14] Lightweight Directory Access Protocol

LDAP, on the other hand, is only a protocol, and it does not define a broader set of directory concepts such as those offered by X.500. Whereas X.500 helps define the ED, LDAP focuses on how to access it. Basically, the LDAP protocol provides a lightweight mechanism for passing text-based queries from an LDAP client to an LDAP server by way of TCP/IP.

3.3.4.2 Microsoft Active Directory

Microsoft's Active Directory (AD) is the company's first real attempt at providing an ED solution. It is the directory service packaged with Windows 2000 Server and, Windows 2000 Enterprise. It provides all of the basic functionality of directory services: an information source, a single point of administration, a way to commonly define rules, and a method to query objects in the directory. Furthermore, it is fully X.500 and LDAP compliant.

To many, AD is the single most significant addition to the Windows 2000 product line and represents the main justification to upgrade or change existing network operating systems. The benefits are widespread--- from providing a very powerful electronic "yellow pages" of users, contact information and workstations, to allowing a single logon to multiple networks and obtaining access to any resource available. A well-formed AD will eliminate the many surveys that are currently necessary to determine comprehensive information about the number of computers in the Government, the types of users, etc.. Network administrators can manage both their users and computers, maintaining a dynamic inventory of both.

A summary of the key features of Active Directory are:

- **a scalable enterprise directory** : an AD can model an enterprise of any size. The AD can be partitioned into separate Domains to maintain manageability while also providing a comprehensive hierarchical structure. Support for the new concept of *transitive trusts* further eases administrative burdens, cutting down on the amount of trust relationships that need to be managed by administrators. A transitive trust simply means that if Domain A trusts Domain B, and Domain C trusts Domain B, then Domain A trusts Domain C.

- **common rules and policies** : AD also introduces the concept of *schemas*. Essentially, a schema provides a way to apply a common set of rules for the way that *objects* (such as people, workstations, or printers) in the directory are described and categorically defined. Further, the schema allows for the creation of custom objects (such as groups or software) and object attributes (group name or software version) within the directory hierarchy.

- **DNS and namespace** : the cornerstone of AD is the *namespace*, which defines the organization and the Windows 2000 network. The namespace is the key to defining, locating, and using resources on an AD-enabled network. As mentioned above, AD uses X.500 and LDAP internet standards as the underlying technologies to define and query the directory. AD also uses another internet standard, DNS[15], to define the organization's namespace. This makes AD extremely compatible with the internet and provides a simple and scalable naming solution.

[15] Domain Name System

- **querying objects** : as described above, a key function of AD is the ability to query the directory for information about the various objects it contains. For example, this allows anyone with access the ability to quickly determine someone's e-mail address or phone number. It also allows someone to learn of which laser printers are located in a specific Ministry that have the capability to print in color, etc..

- **security definition and control** : AD also maintains the *Access Control List* of all objects in the database. This list is used to determine access rights and responsibilities of people and computers. AD's security features represents its main use in most organizations.

- **fault tolerance** : AD replicates itself throughout the hierarchical structure of the network. This eliminates problems contributed to faults in the network or slow connections between nodes.

3.3.5 Electronic Mail (E-mail)

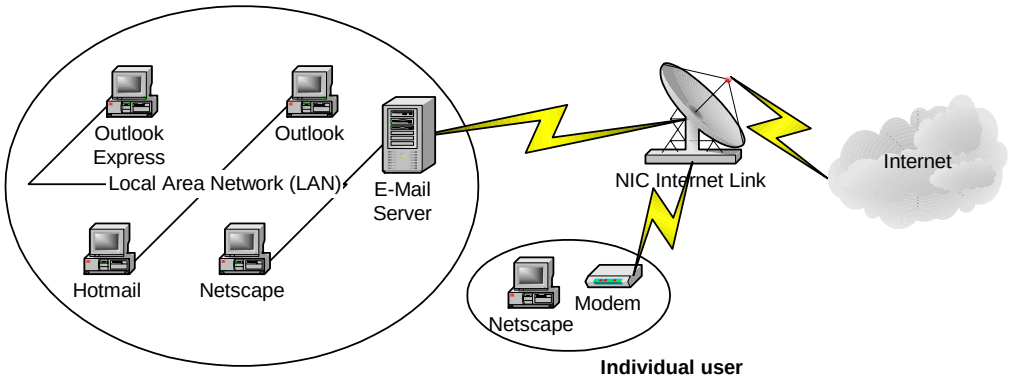
3.3.5.1 The importance of e-mail

The core technology of all collaborative and ERP software solutions is electronic mail (e-mail). E-mail has become the communications backbone of most organizations and is quickly replacing voicemail and facsimile copies as the preferred means of relaying messages and information.

E-mail usage throughout the Government is shockingly low, and threatens the successes of all other IT based initiatives, including e-government.

The importance of widespread e-mail use within the Government cannot be overemphasized. The Government should make this a top priority issue as any future e-government initiatives, no matter how enthusiastic, cannot be effective until e-mail is commonly used throughout the civil service.

Many line ministries currently have their own e-mail servers and provide much of their staff with e-mail accounts. However, a large percentage of civil servants still rely on personal e-mail addresses, established through third-party providers like Hotmail and Yahoo, for their access. The figure below illustrates these two most common e-mail access methods:



Typical Govt. organisation with LAN and internet access via NIC

Individual user with dial-up access using Hotmail or Yahoo, etc..

3.3.5.2 Project team observations

The project team has made the following observations about e-mail use within the Government:

- there is a lack of understanding among civil servants about the use and capabilities of e-mail and e-mail applications. This is especially apparent in upper management who are failing to take a leadership role and adequately encouraging its use. In many departments, e-mail is welcomed by the staff but ignored by its management;

- there are no policies and guidelines about the official use of e-mail in Government operations. This fact is quickly cited by many staff as an explanation towards their limited use of e-mail, however the project team has observed that e-mail is not being used for informal or non-official communication either;

- there are no comprehensive policies to specify who should have e-mail access, and therefore e-mail distribution is highly dependent on the views and opinions of line management ;

- the Government lacks an Enterprise Directory that provides the valid work-related e-mail addresses of all civil servants;

- most line agencies are highly vulnerable to prevalent e-mail viruses that affect productivity and discourage the continued use of data communication; and

- many government organizations lack the technical knowledge as to how to setup and maintain an e-mail server.

3.3.5.3 Recommendations

Based on the above observations, the project team recommend that the Government pursue the following actions:

Recommendation #3.4.1 : *Consolidate e-mail servers to a central site (NIC)*

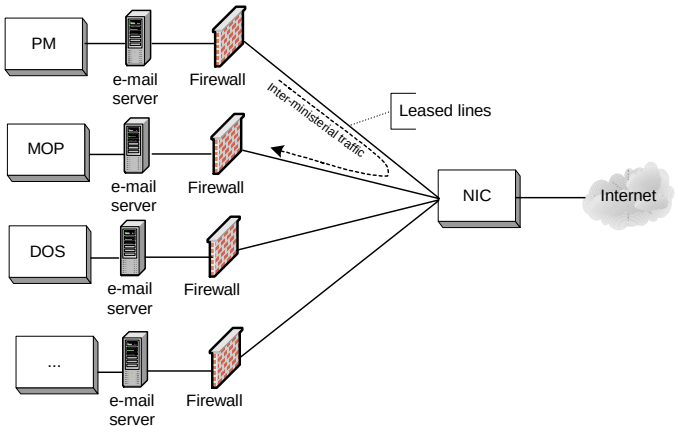
The Government should not rely on the technical skills and abilities of each line agency for e-mail usage. Individual line agency e-mail servers should be consolidated and moved to a central site, creating a "server farm[16]". The project team recommends the National Information Centre (NIC) be considered for the central site because of its role as network operation center and primary ISP to the Government. The LAN Administrators of each agency can continue to administer their agencies' e-mail usage, however the physical servers should be moved to the central site.

The Government should also consolidate web servers for the same reasons and benefits.

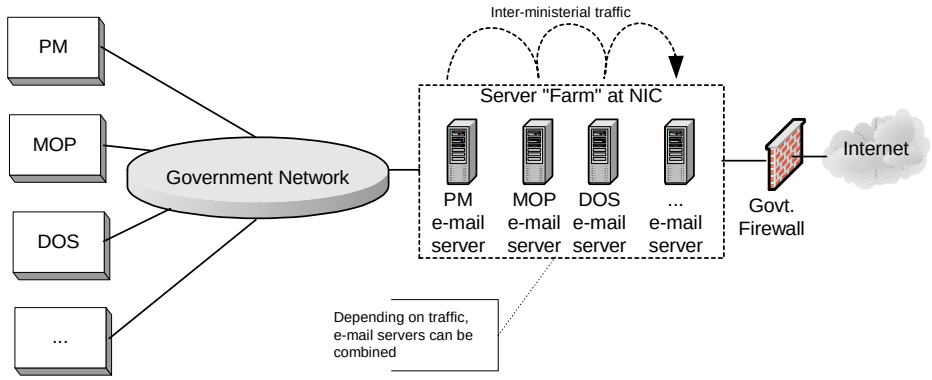
The figures below illustrates the current and recommended e-mail configurations for the Government:

[16] a "server farm" is a facility that houses and maintains a wide variety of hardware servers. By housing all servers in one location, organizations can more easily provide physical security, as well as state-of-the-art fire and power protection.

Current E-Mail Server Architecture



Recommended E-Mail Server Architecture



The consolidation of e-mail servers will have the following benefits:

- **improved reliability** - the central site can provide round-the-clock maintenance and support. E-mail servers will be less dependent on the data communication linkage between the line agency and the Government ISP (NIC).

- **improved protection** - the central site can install and support one firewall and security zone that will protect all servers uniformly. It is much easier to maintain the security and integrity of one firewall than dozens of distributed and separately maintained firewalls. Industrial-strength (and expensive) virus protection can be purchased to protect all sites, thereby providing economies of scale.

- **reduced reliance on individual skills** - the e-mail communication of most agencies currently depends on the skills and resources of its LAN administrator. By consolidating e-mail servers, the Government can reduce its need for trained e-mail administrators and reduce its reliance on the individual skills of key staff.

- **easier to implement and maintain an Enterprise Directory** - a consolidated server farm will make it easier for the Government to implement and maintain an Enterprise Directory such as Active Directory, etc. . The server farm will reduce the overhead traffic connecting each individual site.

- **reduced bandwidth requirements** - as illustrated in the recommended figure above, inter-ministerial traffic remains within the server farm thereby reducing the overall bandwidth requirements to individual line agencies.

- **substantial cost savings** - the Government will realize substantial cost savings by allowing smaller agencies to share hardware servers, and by reducing the number of firewalls and virus protection applications required by all line agencies. Furthermore, each line agency will require less bandwidth to their individual locations and will require less personnel to maintain and operate the site.

Recommendation #3.4.2 : *Clarify e-mail access rights*

The use of e-mail in the Government is too important to leave to the discretion of individual ministerial management. The Government should quickly define and adopt a policy the provides for full e-mail access for all civil servants regardless of their employment status.

To provide e-mail to non-administrative personnel and those without computer access, the Government should consider having public workstations made available in each Ministry that allow for e-mail and internet use. Low-cost "web computers" are available in the marketplace that have limited capacity and are designed for e-mail and internet access only. These computer typically cost less than $500 and can easily be installed in a controlled location in each organisation.

To encourage e-mail use, the Government should move to send all circulars and employee notifications, as well as general news and information about Government activities via e-mail.

Recommendation #3.4.3 : *Develop policies towards e-mail use and validity*

In the absence of legislation that recognizes the legality of electronic messaging, and until the Government formally adopts a security infrastructure like PKI which avails electronic signatures and other protection measures, a broad policy which defines the valid uses of e-mail should be defined and distributed.

The policy should inform civil servants as to Government e-mail rules and requirements and as to what forms of e-mail use are acceptable.

The policy should serve to protect the Government from unauthorized uses and abuses of e-mail using Government facilities, as well as to

encourage the use of e-mail in non-official communications.

Recommendation #3.4.4 : *Initiate an extensive e-mail training programme for all civil servants*

The Government should design and implement a long-term training programme that provides all civil servants with an in-depth knowledge of how e-mail works and the variety of options available. Employees should be taught how to use collaborative software features available with e-mail, and how to manage their information. Employees should also be instructed on proper e-mail etiquette and the procedures and regulations of e-mail use in the Government.

Recommendation #3.4.5 : *Standardize e-mail programs (clients) and servers*

Like with word processing, the Government can realize substantial productivity benefits if everyone uses the same vendor's e-mail programs and servers. To make e-mail globally interchangeable, most basic e-mail programmers only provide a limited feature set. However, if an organisation has standardized on a single vendor product, than it can expand this feature set to include a variety of powerful options that can improve workflows and productivity.

Because of the Government's recent blanket licensing of Microsoft products, the project team recommends that it consider standardizing on the use of Microsoft Outlook and Microsoft Exchange Server. These two products provide a wide range of collaborative groupware features that can be used within the Government if everyone uses the same applications.

Standard applications will also substantially reduce the technical support needs.

Recommendation #3.4.6 : *Implement an Enterprise Directory*

The benefits derived from a well-designed Enterprise Directory are described in Section 3.3.4 above. The Government should move to install an Enterprise Directory so as to facilitate e-mail addressing and to provide "white pages" of all civil servants. This task has been identified as a "fast-track" project under the on-going e-government initiative.

4

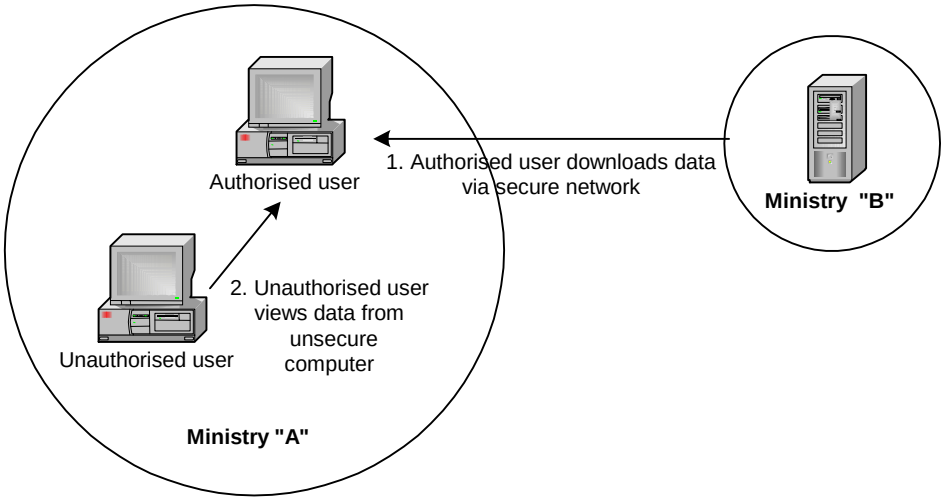
Section 4 : Administration

4.1 Introduction

In designing the pilot network a number of issues must be addressed:

- who will manage the network?
- how can the security of the information on the network be assured?
- who will decide what information can be accessed by whom?
- what needs to be done prior to establishing connectivity?

This section focuses on these issues and concentrates on the “readiness” of the key agencies to connect together. Because a network introduces new security threats to each agency, it is important that each agency attached to the network maintain a basic level of security and work to maintain “best practices” in their daily LAN administration and IT management.



The above figure illustrates one of the simple security dilemmas of establishing network access between two organizations. In the example, an authorized user in Ministry “A” accesses and downloads data from Ministry “B”. However, because of Ministry “A”’s poor internal security, an unauthorized user in Ministry “A” obtains access to the data.

Before connectivity is made between organizations, each agency must be able to “trust” the security and administration of the other agencies. This trust is found through the creation and compliance of mutually-established security policies and practices.

In addition to security concerns, it must be understood that the benefits of the network will not be realized unless the computer capabilities of each Ministry meets a minimum level of expertise. For example, it makes little difference if one can easily send e-mail to another agency, if the recipient in that agency does not know how to use their e-mail program.

Finally, an important assumption in establishing the network is that the data and information in each agency is available to be shared with the other agencies. Information sharing, and the right of access to public data, are hurdles that must be resolved before the pilot network will be successful.

4.2 Network (MAN) Administration

4.2.1 Introduction

The management and administration of an inter-organizational network like the pilot network requires coordination and mutual cooperation among LAN administrators of each of the key agencies. It also requires a governing body, or committee, that oversees the activities of each agency and establishes standards and guidelines.

MAN administration is a superset LAN administration tasks and skills which are covered in the next section. Good LAN administration will lead to a well-functioning MAN, however there are larger issues such as link control and monitoring, security, access rights and routing that need to be considered.

The main objectives of MAN administration are the following:

- network reliability and performance;
- security;
- information sharing; and
- access control.

Some of the MAN administration will depend on the design and infrastructure of the network. As described in the Connectivity section of this report, there are third-party data communication providers, such as Batelco, that effectively manage the reliability and performance of the MAN for the customer, thereby eliminating those issues. On the other hand, if the Government chooses to build it's own infrastructure (private cables between agencies), then the issues of link control and performance increase substantially in complexity.

4.2.2 Network Committee

A prerequisite to establishing a MAN is to form a governing body, or network committee, of representative LAN administrators. In addition to technical staff, it may be necessary to have representation from upper management to resolve issues of information sharing and data access.

The network committee will need to address the following subjects:

- **network reliability and performance** - insuring that the link to each agency remains functional and performs adequately depends on operational guidelines

and policies established by the committee. Within this subject, the committee will need to:

a. Establish a network operation center that maintain responsibility for monitoring links and notifying administrators when problems occur;

b. Design the routing tables that direct traffic through the network and re-route when problems occur;

c. Establish hardware and software standards to promote interoperability and data exchange;

d. Determine network monitoring guidelines and establish baselines. This will include agreement on standard monitoring protocols such as SNMP[17], and locations of MIB[18]s; and

e. Define procedures to handle faults in the network, including logging mechanisms and response teams.

- **security** - as previously mentioned, a secure network depends on the participation of all organizations connected to the network. The committee should establish security guidelines and policies, along with minimum security standards that must be met by all agencies. The committee should designate a security auditing group to periodically review and assess the adherence to the stated policies, and define procedures for handling breaches in procedures.

  This is perhaps the most difficult subject to be handled by the Committee and will require full management and legislative support. All IT related Government organizations, including the National Information Centre and the Ministry of Information and Communication Technology, should be included in the development and adaptation of Government security policies.

  The policies should include standards for physical security, data protection, access management, logging, and certification control.

- **information sharing** - information sharing defines what data is to be shared and to whom. This subject is non-technical and may require high-level discussion within each organisation. It can also include resource sharing, such as making access to printers, plotters, cd-writers, jukeboxes, hard-drives, etc., available to groups of network users.

  The committee should develop broad guidelines and policies toward sharing information and resources within the network. The policies should classify information into: unrestricted, restricted, secret and top-secret. Individual agencies will need to review their data stores and decide on each data's category.

  The committee's information sharing guidelines will need to address how network users request access to information, how to publicize what information is available, and the procedures necessary to grant access.

[17] Simple Network Management Protocol - is an industry-standard protocol that's supported by most networking equipment manufacturers, including Microsoft, and is used to detect problems in networks.
[18] Management Information Base - a management program that reads SNMP and stores information about the status of each network device and link.

- **access control** - access control is directly linked to information sharing subject described above, but concerns the technical aspects of making or restricting access to data. The committee will need to establish mechanisms for granting access rights and for monitoring those rights.

  To simplify management of access rights, the Committee should adopt a standard enterprise directory scheme as described in Section 3.3.4 above. A well established enterprise directory will contain the access rights of all network users and will simplify login and verification. The directory will also help to prevent mistakes which result in breaches in security.

4.2.3 Recommendations

Prior to establishing connectivity between the key agencies, the project team recommends that the Government undertake the following recommendations:

Recommendation #4.2.1 : *Establish a Network Governing Body*

All agencies involved in the pilot network project should form a network governing body, or committee, to oversee the management and administration of the MAN. The committee should address the following subjects: network reliability and performance, security, information sharing and access control. The committee should have full management and legislative support.

Recommendation #4.2.2 : *Develop an Enterprise Directory*

A critical component of the MAN will be an Enterprise Directory (as described in Section 3.3.4 of this report.) The Directory will maintain access rights of all network users and allow for single login access to all network resources.

4.3 Security and LAN Administration

4.3.1 Introduction

Information security begins with good LAN administration. In addition to providing a means to share resources such as computers, printers and software, LANs also allow organizations to secure and protect information. Unfortunately, as described further below, most of the Government agencies are not making use of these security features. The project team has found that existing LANs are primarily used as a means to provide access to the internet and e-mail, as well as to occasionally share software and documents.

Good LAN administration also protects the organisation from accidental loss of data and information. Currently few, if any, stand-alone PCs in any of the pilot agencies are backed up on a regular basis. This is understandable--- without the proper portable backup devices (i.e., portable tape-drives or optical disks) it is difficult and time-consuming to backup the large amount of data currently found on stand-alone computers.

This section will review the LAN administration found in each of the key agencies and will point out improvement and provide recommendations.

4.3.2 Security issues

4.3.2.1 Security Overview

Information security is intended to protect an organization's resources, data and programs, computers and networks, from intentional or accidental losses, modifications, damage, destruction, denial or disclosure. Protection is achieved by implementing appropriate controls, which will:

- prevent (or limit the likelihood of) the occurrence of a security violation;
- detect those violations that may occur;
- mitigate or limit any consequential damage;
- facilitate recovery; and
- provide an audit trail to enable subsequent investigations.

A control is a policy, method, practice, procedure, device, software, or programmed machine designed to achieve protection of information assets. These controls are derived from the four primary objectives of information security: confidentiality, integrity, availability and audit ability. These are defined below:

- *Availability:* is ensuring that the network and information are accessible and in usable form when they are required by authorized people for authorized purposes;
- *Confidentiality*: is protecting sensitive information from unauthorized disclosure;
- *Integrity*: is preserving the accuracy, authenticity and completeness of information by preventing unauthorized or accidental creation, modification, replays or deletion;
- *Audit ability*: is ensuring that any action or transaction can be reconstructed and connected to a specific individual, and that compliance with the key controls can be verified.

Information security is implemented through appropriate physical, logical and/or procedural measures, supplemented by security audits to ensure that they are operating correctly and meeting their objectives.

The project team has done a superficial security evaluation of the key agencies and has identified the following issues:

4.3.2.2 Physical Security Observations

Physical security is primarily concerned with the protection of assets (both data and real) from theft or destruction and consists of tools and techniques such as locks, gates, CCTV [19] and alarms.

[19] Closed Caption Television

- Most of the key agencies, with the notable exception of the Prime Ministry and the Central Bank of Jordan, have minimal physical security. This is primarily the result of the agencies being currently perceived as low security targets (which explains the good physical security at the PM & CBJ.) ;

- While most server rooms are isolated and protected, they remain vulnerable to unauthorized access;

- None of the buildings (with exception of CBJ) maintained CCTV which will assist in detecting security intrusions;

- Few, if any, workstation PCs are physically locked or secured to the desks. As noted below, unlocked computers are a risk because data files remain on local hard-drives.

4.3.2.3 Logical Security Observations

Logical security focuses on protecting access to information and includes tools and techniques such as access control lists, user identification and cryptographic techniques including data encryption and digital signatures.

- With the exception of some workstation BIOS passwords and restriction to servers there is little, if any, logical security of any kind currently used in the pilot agencies.

- Almost none of the workstations require authentication from an access control list (ACL) (i.e., authentication from a file server) to access local resources. This is because most workstations are using Windows 95/98 which, by default, does not require ACL authentication. Windows 95/98 ACL authentication can be activated by using Group Policies along with a Windows NT/2000 server.

  Because of the tendency to store documents and information on local hard-drives, this is perhaps the most significant security breach. Failure to authenticate from an ACL means that anyone who turns on the computer can access the documents on the local hard-drive. While ACL authentication is not a secure means to prevent access to local drives (easily sidestepped by booting with a floppy disk) it does prevent casual access.

- Digital signatures or other PKI cryptographic techniques are not being used;

- There is no evidence of use of data encryption;

- Most employees utilize Outlook Express or Eudora e-mail client software which have no password protection;

- There is little, if any, internet security in place in the agencies. Only a few agencies deploy firewalls or proxy servers to deter internet hackers from accessing systems. A few agencies provide internet security by separating internal networks from external ones. Failure to install internet security is the most immediate concern of the project team.

- While virus protection is installed on most workstations, there is little system-wide protection, especially of e-mail. Most LAN administrators admitted that client virus databases are updated infrequently.

4.3.2.4 Procedural Security Observations

Procedural security involves security policies, standards, guidelines, procedures, and control activities (followed by people) such as the administration of access rights to an agency's systems and the management of cryptographic keys.

- The project team could not find any documented security policies, guidelines or procedures in use by the key agencies. The NIC reported that they have written and distributed security guidelines in the past, but admits that they have not been implemented.

- There is no management of access rights to servers and systems. Usually full access remains with the LAN administrator or administrators. There is no documentation in any agency over which users have rights to which systems. Access rights are usually provided on an ad-hoc basis.

- Internet/e-mail access is provided on a case-by-case basis.

- Backup protection of workstation data are the responsibility of their users. However, no agency had the means to adequate backup a large volume of user data if requested. Most administrators recommend that users copy important files to floppy disks.

- Backup routines of server data are not documented or logged. Off-site storage of tapes is not being utilized in any agency.

- Password enforcement schemes are weak. There are no policies to protect passwords or to promote password integrity.

- It is presumed that there is limited auditing of online access. There is no evidence of documented procedures on how to handle security violations.

4.3.2.5 Security Recommendations

The consultants recognize that all organizations must maintain a balance between security and cost (both in money and hindrances). Full security is impossible and *adequate* security is a relative concept.

Therefore, the following recommendations are based on common best practices found in other countries and organizations.

Recommendation #4.3.1 : *Improve physical security*

Line agencies should restrict access to information and electronic data, and should improve the monitoring of people within IT organizations. In particular the following options should be considered:

- Install CCTV in each agency to record movements in hallways and access to offices, especially server rooms;

- Install automatic locks on all server rooms and on the offices of important IT personnel.

Recommendation #4.3.2 : *Enforce ACL access to workstations and LANs*

A user should not have access to information on a workstation or a server unless they have been authenticated by an ACL.

- provide access in each organisation to a Windows 2000 server to provide ACL control and monitoring;
- Upgrade as many desktop computers as possible to Windows 2000 professional;
- Standalone desktop computers should be connected to a LAN if possible, and treated as "low security" if they cannot be.
- Install group policies and require authentication on all pre-Win 2000 computers.

Recommendation #4.3.3 : *Establish a PKI infrastructure*

A study of establishing a public-key infrastructure (PKI) is currently being made by the e-government taskforce of the Ministry of Information and Communication Technology (MOICT). The project team encourages the Government to begin investigating PKI solutions and its requirements. In particular the Government should determine what are the technology's business drivers, what level of security is appropriate, where is the existing system vulnerable, and what are the legal and regulatory compliance constraints?

Recommendation #4.3.4 : *Employ local security firms*

There are a number of private local firms that specialize in information security and perform security audits. Security is a specialized field of study, and most organizations have a difficult time following its latest trends and technologies. As such, the Government should make use of the specialized services of private security companies and occasionally hire these firms to conduct security audits.

Recommendation #4.3.5 : *Improve virus monitoring*

Viruses are a constant threat to the Government. Besides being a nuisance and hampering productivity, they also erode confidence in the use of IT and discourage individuals from making full use of the technology.

Traditionally, viruses protection has focused on individual computers by loading software such as Norton or McAfee on each workstation. Unfortunately, this technique has proven to be ineffective as virus databases are constantly out of date, leaving the computers vulnerable to the quick-to-appear and short-lived "fad" viruses that occasionally sweep through a country.

The Government should adopt a new approach to fighting viruses and focus at the server level, including e-mail servers. Since the NIC serves as the ISP for most Government agencies, efforts to fight viruses should be consolidated there. Incoming internet traffic can

be scanned at source. Consolidating e-mail servers (see Recommendation **3.4.1**) will further protect against viruses by providing a single monitoring point.

Recommendation #4.3.6 : *Employ a common firewall solution*

The Government is currently relying on each LAN administrator to implement security measures ad hoc. Unfortunately, implementing and maintaining a firewall to protect against external attacks is a complex and time-consuming task, that currently very few LAN administrators are handling successfully. The Government should pursue a standard firewall solution that can be centrally managed, yet distributed to all line ministries and agencies. The is especially important if connectivity between agencies is established, as it will also protect against internal attacks.

4.3.3 LAN Administration issues

4.3.3.1 LAN Administration Overview

LAN administration is a difficult job and usually constitutes the core function of most IT departments. LAN administration is also a nebulous task-- as it involves a variety of tasks ranging from hardware maintenance to help desk support. The term "LAN administration", therefore, is often synonymous with the general functions of the IT department itself.

The importance of good LAN administration lie in the importance of the LAN. As government services and workflow become more electronic, the LAN provides the backbone to the entire enterprise. As more departments and employees rely on IT to perform their daily work, a secure and dependable data network and the availability of good support services becomes critical to getting the job done.

LAN administrators are also charged with the difficult job of promoting new ideas and work habits. Because administrators control the software tools and services available on the LAN, they indirectly control the abilities of the organization's other employees. For example, it is usually up to the LAN administrator to determine what software is available for use and what versions are supported. LAN administrators also need to recommend new technologies into the organizations. As the organization's employees become more knowledgeable of computers, this dependence is reduced.

4.3.3.2 Project Team Observations

The following observations were made by the project team in their review of LAN administration in the pilot agencies. The project team emphasizes that these observations are not criticisms of existing LAN administration, but should be viewed as opportunities for improvement.

- **Centralized file storage** - none of the agencies reviewed require that user information and files be stored on the central file server. In a networked environment, an organisation can maximize its security and loss prevention by encouraging (or forcing) users to save all personal files on the central file server instead of their individual computers. Centralized storage provides the following advantages:

a. much better security, especially from unauthorized access to workstations and from physical theft;

b. easier to back up entire organisation; and

c. administrative access to user files, if necessary.

- **Non-core tasks** - Much of administrators' time is spent managing non-core tasks such as e-mail and website. LAN administrators should strive to remove any non-core tasks and systems unrelated to the operations of their organizations. In particular, the administrators should focus on outsourcing the operation of their e-mail and web servers to a third-party, or to the NIC as cited in **Recommendation 3.4.1**, especially if their websites are static and require minimal maintenance. Also, LAN administrators should encourage websites to be created and maintained by professional web developers.

- **Network monitoring** - None of the agencies utilize any network monitoring or metering software. The key agencies are not taking advantage of the substantial benefits of SNMP and network management tools such as Microsoft's System Management Server (SMS) (as described in the box below) which are available through the Government's blanket licensing agreement with Microsoft.

A Brief Overview Microsoft's System Management Server (SMS) 2.0

Microsoft's SMS offers LAN administrators remote desktop management of their LAN in four primary areas:

1. Inventory and resource management - provides the ability to gather and maintain a workstation's hardware and software configuration in a central database that is easy to access and interpret. SMS's Hardware Inventory Client Agent can "auto discover" IP devices and automatically collect information about a particular computer's CPU, RAM size, hard drive space, etc.. The Software Inventory Client Agent collects information about programs and file types stored on clients.

2. Diagnosis and troubleshooting - provides the tools to analyze hardware and software on remote workstations. In addition to tools such as HealtMon and Network Monitor which analyze network performance and provide reporting, SMS also includes Remote Tools which gives administrators the ability to gain keyboard and mouse control of an SMS client.

3. Package distribution - provides the ability to install applications and updates and execute programs on remote workstations. This feature allows administrator to build "packages" of applications that should reside on each workstation. New applications are automatically installed.

4. Application management - provides the ability to track, restrict, and license application usage on a user's workstation as well as to monitor product compliance issues. SMS allows the administrator to restrict what and when applications (including games such as FreeCell and Solitary!) are allowed to be run. SMS is instrumental in conforming to software licensing requirements.

- **Documentation** - LAN administrators are not fully documenting operations procedures and inventories. The project team identified few written policies or procedures about the LAN administrator's roles and responsibilities. Complete, up-to-date network documentation provides an invaluable reference when training or troubleshooting, and is especially important when high turnover exists. When a problem occurs, concise network documentation provides valuable information about how the network is configured and where to find remedial resources. LAN Administrators should maintain the following minimum documentation:

  a. *Address List* - A list containing all addresses on a network, including the hardware addresses of specific computers. For example, an ideal list would include the MAC address of each computer's NIC, its IP address, its physical location, and identify its primary user.

  b. *Cable map* - A detailed outline of the cable installation for the network. A cable map for a twisted-pair network would include cable type (e.g., Category 3 or 5 UTP), wall-jack numbers and office locations, and the corresponding ports on the patch panel or concentrator. It also would

include the maximum speed of the cable and the speed at which the cable will be used, if the two do not coincide.

c. *Contact list* - Sometimes called an escalation procedure, this documentation should include the names and contact information of those to be informed in the event of a network problem or failure. This encompasses not only network administrators, but also vendor contacts and phone numbers and information about internet links (JTC and NIC).

d. *Equipment list* - Documentation should be kept that includes the date the equipment was purchased, its serial numbers, vendor information, and warranty information. This can be automatically generated if SMS is installed in the network

e. *Network history* - A single, comprehensive document that outlines all upgrades applied to the network, as well as what problems have occurred, along with their symptoms, solutions, dates, contacts, procedures, and results.

f. *Network map* - A comprehensive network map that includes hardware locations and cabling.

g. *Policies and procedures* - All tasks performed by a network administrator should be documented. Established policies for user and group configuration and naming conventions are prime examples. Also, procedures that outline the steps necessary to set up or delete network users, perform a backup, or restore a file should be documented and updated as necessary. This may seem time-consuming, but it will pay off quickly because it eases the training process when new people join the network. Should the network administrator be unavailable, an accurate set of procedures ensures that the Department isn't affected.

h. *Server configuration* - A separate list for each server that details the hardware configuration, and software installed (including version number), the type of data stored (file server, database server, e-mail server, etc.), and the schedule and location of backups.

i. *User administration* - A list that outlines the types of users listed on the network, the naming conventions used, and network resource assignment for users (e.g., which drives are mapped at logon, etc.) should be maintained. If an enterprise directory is implemented, this list can be automatically generated from it.

- **Resource sharing** - the project team observed that many IT departments are not making full use of the resource sharing capabilities of the LANs. Most agencies have a very high percentage of printers related to computers, suggesting that resources are not being adequately spent. Most departments are still purchasing state-of-the-art workstations with large capacity hard drives instead of relying on file servers and centralized servers.

  LAN administrators should investigate the possibility of using terminal services and other client/server concepts to maximize their IT investments.

- **Internet management** - Most IT departments are currently have no Internet management software, including proxy servers, content filtering or usage monitoring software, implemented in their departments. Until the Government

has sufficient internet bandwidth to all agencies that non-work related internet access is irrelevant (at least from the bandwidth viewpoint), LAN administrators should consider monitoring internet use.

A number of commercial products, including Resource Watch and Web Monitor, track employee use of the internet and provide full reports detailing the sites visited, average time spent on sites, and total time logged onto the internet. These feedback reports have prove successful in helping management control their employee's usage.

4.3.3.3 Recommendations

To improve LAN administration in the key agencies the project team recommend the following actions:

Recommendation #4.3.4 : *Outsource non-core activities*

LAN administrators should try to outsource non-core activities, including e-mail and web management to third parties, as described in **Recommendation 3.4.1**. Other activities available for outsourcing include hardware maintenance and preventive maintenance, network configuration and monitoring, and security.

Recommendation #4.3.5 : *Centralize storage of user files*

Workstations and servers should be reconfigured to store user files on a central file server rather than on the hard-drives of individual computers. This provides additional security over physical theft of data, and allows for easier backups.

Recommendation #4.3.6 : *Implement network administration software*

By implementing network administration software, such as Microsoft's System Management Server 2.0, LAN administrators can better monitor and document their network. Network monitoring software and protocols are very important when connectivity with other agencies is established.

Recommendation #4.3.7 : *Improve directory management*

LAN administrators should be concerned with both *where* and *how* user files are stored. Before interconnectivity is launched, LAN administrators need to know what files are stored on the LAN and where they are. Access control is simplified if the Administrator enforces policies regarding where a user can store files (and if those files are stored on a central file server.)

Recommendation #4.3.8 : *Documentation*

Network documentation should be improved. LAN Administrators should strive to maintain all of the documentation listed in Section 4.3.3.2. Much of the documentation can be automated if the proper management software is installed.

Recommendation #4.3.9 : *LAN administration workshops and newsletters*

The project team highly recommends that the Government, with the assistance of a central IT-related agency like the MOITC or NIC, hold occasional workshops and conferences to discuss administration issues and way to improve the use of computers in each organisation.

An alternative is to create newsletters informing LAN administrators of the latest software trends and ideas.

Recommendation #4.3.10 : *Develop standard administrative procedures*

Before e-government and interconnectivity is implemented, the Government should focus on defining standard LAN administrative procedures, including the "best practices" mentioned in this report. Interoperability standards and guidelines should be adopted and met.

The development and maintenance of the procedures should be the responsibility for one of the central IT agencies like the MOITC or NIC.

4.4 IT Management

4.4.1 IT Management Overview

The improvement of basic LAN administration and security in each Government agency is only a portion of the tasks required for better overall IT management.

While the improvement of IT management appears to exceed the scope of network design, the project team recognizes that the broader goal of increased utilization of IT in each agency relies on the eventual strengthening of overall IT management skills.

A government organization's efficiency and effectiveness is becoming increasingly dependent on the functions and roles of its IT department. IT departments are providing the means and the solutions for reducing bureaucracy and improving workflow. As the Government moves to provide more electronic delivery of services (a fundamental component of e-government) it will continue to rely on the capability and strengths of its IT department.

IT management, however, is enormously complex. Expensive resources, high employee turnover, increasing demand, and a wildly fast-paced industry all contribute to its complexity. As global demand for IT professionals and skills continues to accelerate, the ability of the Government to acquire and maintain capable employees will continue to deteriorate. An IT department must adapt to rapid changes in technology while operating in bureaucracies that are fundamentally resistant to change.

Improving IT management requires innovated changes to existing policies and norms. This section will further explore the challenges to current IT departments and will provide recommendations for future consideration.

4.4.2 Project Team Observations

4.4.2.1 Business Plans

As a result of another objective of the ongoing project, the consulting team worked with approximately twenty government organizations to assist them to complete IT business plans. To kick-start the process, the project held a two-day workshop in Ma'in during 20-21st of March, that was attended by both the IT department heads and a key policy/business representative of each organisation. Following the workshop, the project team continued to work with each of the organizations.

The feedback from the workshop participants clearly highlighted the need for improved IT management in the Kingdom. The project team observed the following problems in most of the IT departments:

- **High employee turnover** - because of the low salaries against those found in the private sector and abroad, all departments are finding it very difficult to keep good staff. Most IT departments have a shortage of experienced employees and the situation is expected to worsen. This severely impacts their ability to improve the computer capacity of the Government.

- **Lack of management awareness** - the upper management of most government organizations are not fully aware the unique problems faced by IT departments. Management usually realize that hardware is important, but fails to understand the business impact of improved IT management and support. Most managers completely rely on the IT directors to recommend new technologies and solutions, showing little interest in it themselves. IT is not yet perceived as a change agent to new business processes and workflows.

- **Excessive demand** - there is always an unlimited demand for more information and for improved efficiencies. As employees become more aware of information systems and IT, the demand placed on IT departments for new applications and systems increases. Most departments are faced with a backlog of new systems that have been requested by their organizations, yet do not have the resources or capacity to develop them.

- **Lack of training** - the fast pace of the IT industry makes it extremely difficult for the IT staff to stay abreast of new technologies and trends. Most departments feel that they are incapable of providing the services required for the future, including those necessary key e-government strategies. Most of the security and LAN administrative issues identified in this report are attributed to a lack of knowledge by the staff.

- **Limited resources** - practically all departments feel that they do not have enough hardware and personnel to take full advantage of IT in their respective organizations. In particular, most departments need more computers to increase employee penetration percentages and to encourage use among all staff.

4.4.3 Best Practices

The problems faced by the Government's IT departments <u>are not</u> unique to Jordan. Identical problems are faced my most governments around the world. Solutions and best practices have been explored and tested in other countries. Among the more common solutions are:

- **Outsourcing** - This is the single most effective management innovation that organizations can implement. Outsourcing removes non-core activities from the government and transfers them to the private sector. The benefits are enormous and include:

    a. *Reduced reliance on staff and staff skills* - as more services are outsourced, the government requires less staff and less training. Employee turnover becomes less of an issue.

    b. *Access to latest technologies* - organizations can tap the latest skills and innovations without having to retrain its employees. The burden of staying abreast of the new technologies is shifted to the private sector. The best technological solutions will be presented by the companies competing for the contract.

    c. *Accurate costing* - IT is expensive. However the true cost of most in-house IT solutions are hidden, leading to incorrect cost/benefit analysis. For example, when organizations decide to develop information systems and databases they generally do no consider the full cost of additional employees (long-term benefits, retirement, sick leave, training, etc.) or the running maintenance and support costs.

    Outsourcing allows IT departments to obtain accurate costs of developing and supporting information systems. These costs can then be used by management to determine if the systems are beneficial to the government or if alternative solutions can be found.

    d. *Increased sustainability* - in-house developed information systems are too often dependent on the individual programmer or programmers that developed them. High employee turnover results in higher maintenance costs as new employees must become familiar with the coding and structure of the existing system. Outsourcing places the increased maintenance costs to the private firm that developed the system. The ability to maintain and support the system becomes the company's responsibility and not the governments.

    e. *Improved private sector* - outsourcing assists the private sector to develop and innovate. As public sector services are shifted to the local business, companies will be able to leverage their resources and experiences to other markets. Outsourcing is therefore one of the most effective means of encouraging and supporting Jordan's fledging IT industry.

- **Contract Hire** - Another management innovation is to hire externally sourced workers (ESW). The extensive use of contract employees is a commonly used technique in both the United States and Europe by both the private and public sectors. Typically, Government organizations will contract or outsource specific services to the private sector. Contract hires work full-time in the government yet are hired on a limited contract basis. The benefits of this strategy include:

    a. *Elimination of salary ceilings* - Contract hire allows the government to pay market rates for IT professionals. This will reduce employee turnover.

b. *Reduced training and re-training costs* - As technologies changes, the government can quickly acquire necessary skills without retraining its staff.

- **Elimination of non-core systems** - As noted earlier in this report, an important observation by the project team is the number of non-core systems that have been developed and are being maintained by the IT departments. Non-core systems easily make up to between 80-90% of existing applications that need to be maintained and are waiting to be developed.

  Most agencies are designing and developing their own administrative systems including budgeting, expenditure, personnel and payroll. The majority of staff resources are dedicated to these common systems.

  Government IT departments should strive to eliminate any systems or functions that are not directly related to the operations of their line agency. Functions such as e-mail and web support should be also be outsourcing or moved to a consolidate server farm as recommended above (Recommendation #**3.4.1**). In doing so, departments will strengthen their internal security and reduce cost.

- **Business-savvy management** - Most government IT departments are managed by technical personnel with little or no formal business training. In as much as IT directors requiring a better understanding of IT issues and problems, they must also be trained in basic business and personnel management.

4.4.4 Recommendations

Based on the above observations, the project team recommends the following actions:

Recommendation #4.4.1 : *Conduct Management/IT Department Workshops*

The tremendous success of the project's two-day workshop in Ma'in demonstrated the need for additional opportunities for IT directors and upper management to share experiences and to discuss common problems. Upper management need a better understanding of the unique problems associated with IT and how to improve the return on their IT investment.

The project team highly recommends that the Government initiate a series of moderated workshop/meetings to facilitate this invaluable exchange of information and support.

Additional workshops should be held to showcase individual administrative systems that have been developed in line agencies. These systems and experiences can be shared with other agencies.

Recommendation #4.4.2 : *Review IT Management and Operations*

Related to the workshops recommended above, the Government should fully review the role of IT in Government and seek to modify the operations of IT departments. Because of IT's cross-cutting function in all agencies, the effectiveness of an organisation is usually directly related to the effectiveness of its IT department. The

Government should understand this correlation, and strive to modernize its management in all departments. In particular, the project team recommends that Government:

- revise its existing model of IT management and focus on outsourcing all non-essential IT processes so as to maintain a minimal staff necessary for in-house IT needs;
- reduce line agency reliance on their IT departments and recognize that the appropriate use of IT, including training, is the responsibility of all department heads;
- view IT departments as "consultants", not "implementers". IT department's primary responsibility should be to advise, contract and manage the private sector to perform necessary IT work within the agencies. The Government should try to minimize the amount of IT work that it implements in-house.

Recommendation #4.4.3 : *Eliminate non-core information systems*

As noted earlier, the project team has identified that IT departments are spending the majority of their time and resources on developing and maintaining information systems that are unrelated to the core business of the line agency. In addition, most of these systems are duplicated in other agencies, including payroll, personnel, expenditure, budget and mail dispatch (divan) systems.

IT departments should immediately cease all development of non-core systems and focus on utilizing systems created and supported by other line agencies.

As noted in **Recommendation #3.4.1**, the line agencies should also seek to consolidate their web and e-mail servers to a central site. Eliminating these servers will reduce IT administration costs and improve reliability and security.

Recommendation #4.4.4 : *Encourage Strategic Planning for all Ministries*

While assisting IT departments to complete their IT plans, the project team noted the lack of formal strategic planning in most ministries and agencies.

IT management and development should be inherently tied to its parent organization's strategic business plans. If the parent organisation does not know which direction it wants to head, then there's no surprise that the IT department cannot help it get there.

5

Section 5 : Connectivity

5.1 Introduction

This report section focuses on establishing data connectivity between the institutions in the pilot network design. There are a number of options available in Jordan to provide data communications between the pilot organizations, and this section will fully explore these options and provide recommendations.

Existing data networking providers will be evaluated and their respective technologies and merits will be identified.

There are also previous studies on establishing interconnectivity between Government ministries and agencies. The on-going e-government initiative in the Ministry of Information and Communication Technology (MoITC) is also designing a Government Secure Intranet (GSI) that includes linking a subset of line ministries. These studies and initiatives will be reviewed and evaluated.

5.1.1 Determining the best connectivity option

The best option for connectivity is determined by evaluating three variables:

- Price;
- Reliability (Service); and
- Flexibility.

Each of the three variables is important, but also need to be taken in context with the other two. However, the significance of each variable is subjective and individual opinions may differ from that of the project team.

In addition to these variables, the following other factors should also be considered.

5.1.2 Other factors to consider

- **Bandwidth usage** - Determining an *appropriate* network solution also requires understanding both the anticipated use of the connectivity and the estimated bandwidth[20] required. As the Government implements new applications that make use of the network, bandwidth requirements will increase and the best option may change over time.
- **Available skills** - The Government must also consider its existing skills level and available technical resources in determining the best networking option. As noted below, some networking options require that the government acquire

[20] The data transfer capacity of a digital communication system

and maintain skilled network administrators. The availability and cost of these network administrators must be included when comparing the prices of private and public network solutions.

- **External factors** - Finally, external factors such as anticipated and real price changes and politics will influence connectivity decisions. The data networking environment in Jordan is rapidly evolving. As additional players enter the marketplace, and as existing players are merged or removed, the best networking option may also change. A danger of this shifting environment is that new technologies are being introduced but have not been fully tested, and promised services and support may not be realized. Lastly, the Government's indirect involvement in the data communication business (it remains a 51% share holder of the Jordan Telecommunication Corporation) may also influence decisions.

5.2 Public versus Private Networking

5.2.1 Introduction

At the most basic level one must choose between using a public data service or building a private network. Each approach has its own advantages and different investment requirements, not only in equipment, but also in personnel to operate and maintain the network.

Public data services have become extremely popular, as demonstrated by the their tremendous growth in recent years both within Jordan and the world. These services leverage a shared backbone network on which carriers provision many customer network connections. Public data services remove much of the burden of managing the MAN from the network manager's shoulders because the carrier manages the network. Equipment requirements are reduced as well, since there is no need to invest in the switching technology that the carriers use.

On the other hand, private data networks can be built using leased line connections between routers (or frame relay switches) and digital modems. In this scenario, one owns (or leases) the equipment, including the routers and digital modems (DSU/CSU[21]) , and the network manager retains control of the LAN. The network manager can reconfigure the connections on demand.

To choose between private and public data networks, the Government should address are several considerations, including:

- at what point does the Government want control of the network?
- does the Government have the staff for building, managing and maintaining the MAN?
- what is the current investment in data equipment?

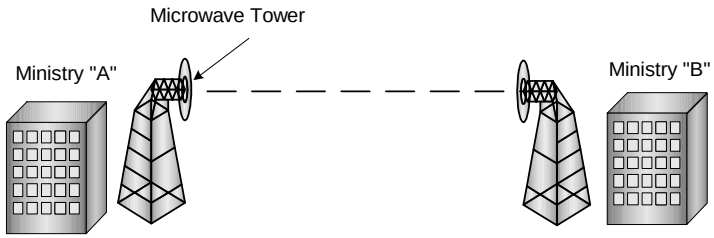
[21] DSU/CSU (Data Service Unit/Channel Service Unit) are the devices that provide access to digital lines.

5.2.2 Private Networks

The technically best way to define a private network is to determine who owns (or is responsible for) the equipment that make up the “cloud” which connects the user’s end-devices (computers, LANs, etc..).

A very simple example of a purely private network is a LAN where the organisation owns both the end devices (computers) and also the network equipment (the hubs and switches) that connect them.

An expansion of this concept involves interlinking different buildings or complexes into a MAN or a WAN. An organisation can design and build a private network that links the buildings through microwave, wireless or fiber-optic connections. If the buildings are in different cities or countries, the organization may use satellite or VSAT technologies to establish connectivity. The illustration below shows a purely private network using microwave technologies:



The **advantages** of these privately owned networks are:

- the user enjoys all of the possible bandwidth, all of the time;
- they can be very secure;
- after initial investment, follow-on operational costs are minimal.

The **disadvantages** to private owned networks are:

- depending on architecture, initial investments can be very high-- especially if there are many network nodes[22];.
- they require extensive support and maintenance, which can be very expensive;
- they are inflexible in terms of increasing or decreasing bandwidth;
- they are inflexible in relocate network nodes.
- reliability depends on the technology used and the quality of maintenance staff;
- redundancy significantly adds to the initial investment.

The Jordanian Government has already built and maintains at least three purely private, wide area networks, they include:

- A network within the Department of Public Security which is primarily used to connect police stations within Jordan. The network includes fiber optic links in the major cities and microwave links that interconnect remote areas.

[22] A network node is defined as an access point on the network. The pilot network which strives to interconnect seven agencies would have seven nodes, etc..

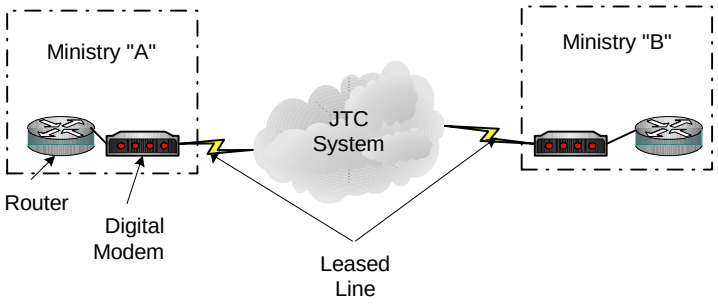
- The Royal Airforce network that is currently being upgraded to a full fiber-optic backbone that runs from Amman to Aqaba. The network is primarily used to connect major military installations within Jordan.

- An Armed Forces network that covers approximately 90 percent of Jordan's geographic area and is based on microwave technologies.

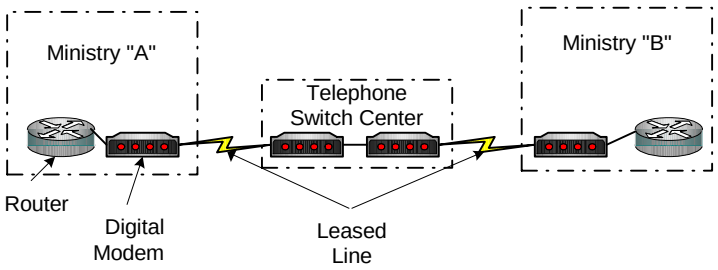
In addition, the NIC has connected over a hundred public sector organizations using a combination of fiber-optic private lines, leased public lines, and dial-up facilities.

5.2.3 Point-to-Point Private Lines

A hybrid of the private networks above are those that rely on the public telecommunication provider (JTC in Jordan) to provide point-to-point dedicated, or private, data communication circuits (or "leased lines"). In these cases, the owner no longer owns or is responsible for the equipment in the network "cloud", but relies on the local telecommunication infrastructure.



In the figure above, the network equipment that connects the two ministries is owned by JTC and is hidden from detail in the cloud. If we look into the cloud, we will reveal the following:



The **advantages** of using private lines are:

- initial investment cost is very low;
- dedicated bandwidth;
- very flexible in terms of speed upgrades and physical relocation of offices;
- security remains very high;
- does not require dedicated network staff to maintain and monitor interconnectivity *outside the premises* of the organisation. However, in the example above, if the end equipment (the modem and router) are owned by the Ministry, they will still require staff to maintain and monitor this equipment.

The **disadvantages** to private, point-to-point based networks are:

- they are not practical for connecting multiple sites to each other-- to mesh[23] *n* nodes together, one needs *n* (*n* -1) / 2 private leased lines. In smaller networks, this can be overcome by using a central node in a star configuration.
- operating costs are usually higher because of the line leases;
- inefficient bandwidth management-- bandwidth that is only occasionally used is maintained at all times.
- distance-sensitive: the further the distances of the nodes the higher the costs.
- reliability depends on the quality of service provided by the telecommunication provider.

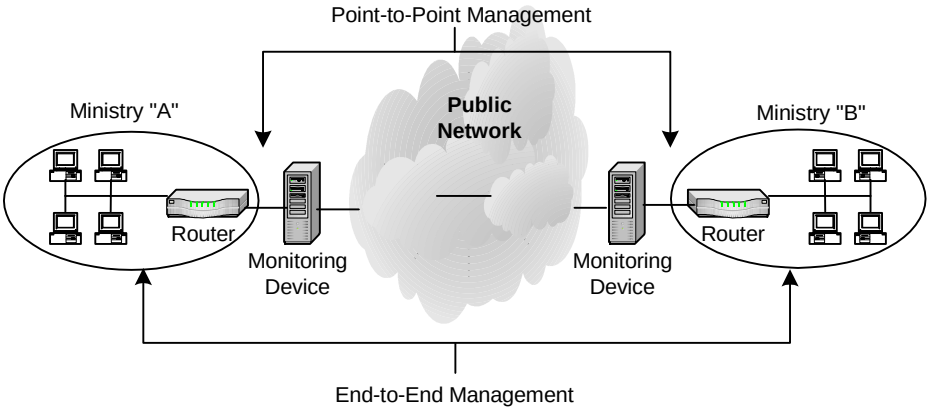
Most ministries and line agencies currently use some form of point-to-point private lines to establish internetworking with the Internet through NIC. Government agencies have established these private lines at speeds ranging from 64kb to 1024kb.

5.2.4 Public Networks

Public networks can be classified into two groups: unmanaged and managed. The most popular unmanaged public network is undoubtedly the Internet. While in the past, most unmanaged public networks such as the Internet were not used for corporate or organizational wide-area-networks. However, with the advent of Virtual Private Network (VPN) technologies, more organizations are exploring this concept.

A managed public network uses a shared infrastructure (and is usually based on an existing telecommunication provider) to deliver networking services to a variety of different customers. Bandwidth is allocated to each customer, and all customers share the expense of the networking equipment and operations.

An important distinction in managed networks is where the responsibility of the network provider stops. As illustrated below, network management can stop before the customer's premises or include it.



Batelco Jordan (formerly First Telecommunications Group (FTG)) is an example of one of Jordan's largest and most popular public network providers. Batelco Jordan offers end-to-end managed, public networking services based on frame

[23] Mesh means any-to-any connectivity in the case of a fully meshed network and a subset of that in a partially meshed network.

relay[24] technology. Batelco Jordan provides its customers with the equipment (digital modems, routers and network management software) required for connectivity on a lease basis. It also manages and monitors the customer's connectivity and bandwidth, and provides a one-stop-shop for all repairs and maintenance.

The **advantages** of using a managed public network are:

- little, if not zero, initial investment as all equipment is leased;
- lower management costs and no need for technical staff;
- lower monthly costs than a private lines in a star-configuration;
- very flexible, add or upgrade nodes without replacing hardware;
- professionally managed and monitored network, including a *one-stop-shop* for network problems and repairs;
- efficient bandwidth management. Some network technologies (like frame relay) let you occasionally use more bandwidth then you've paid for at peak times. Monitoring helps to see that the customer does not pay for more capacity then they typically use.

The **disadvantages** of using a managed public network are:

- costlier than unmanaged networks, if the customer has the skills and resources required to monitor the connectivity;
- reliability depends on the quality of service of the network provider;

5.3 Existing Network Studies

5.3.1 Introduction

There have been numerous studies within the Government that have looked at creating MANs and WANs linking line agencies and agencies with their branches. At least three of these studies have analyzed connecting a large number of institutions together. These studies are reviewed below:

5.3.2 Prime Ministry Report

5.3.2.1 Overview

In a report submitted to the Prime Ministry on July 30th, 2000, the Royal Air Force Electronic Telecommunications Directorate, at the request of the Ministry of Post and Telecommunications, designed a private fiber-optic network that would connect 32 ministries and institutions within the Greater Amman area.

The network design was based on Gigabyte Ethernet Switch technology, providing full compatibility with existing LANs and operating at very high speeds.

[24] Frame Relay is a switching technology that defines how data is transported on layer 2 (Data Link Layer) of the Open Systems Interconnection (OSI) model.

The report investigated the site locations of each of the fourteen proposed node, and eighteen sub nodes, and specified the manholes and conduits necessary to lay the fiber optic cabling.

The report did not provide a cost estimate. It is unclear what the outcome of the report was, but the Prime Ministry has stated that they do not plan on implementing the network design.

5.3.2.2 Review

As described above in section 5.2.2 , private network have inherent disadvantages: they require a very high capital investment and are inflexible. The network design in the Prime Ministry reflects both of these problems. While the speed and privacy of the network is laudable, it would be difficult to manage and operate successfully.

The project team recommends that the Government avoid private wide-area networks whenever possible.

5.3.3 NIC Report

5.3.3.1 Overview

In September 2000, the NIC prepared a report titled "Information Network Infrastructures of Government Institutions." The report served to review the present status of all computer networks in public sector institutes and to provide an analysis for connecting them all together into a Government-wide WAN.

Among the findings of the report are the following observations about the status of Government networking in September 2000:

- 95% of all Government institutions have a LAN, although the operability and use of the LANs is not described.

- 102 institutions (63 public institutions within the Government hierarchy and 39 outside) are connected to the NIC. Of these institutes, they are connected in the following manner:

  - 62 use dial-up connections
  - 20 use analog leased lines
  - 19 use digital lines, including 12 that are connected via fiber[25]

- 23 institutions do not have connections to the NIC, but some have internet access through private companies.

The report noted that the Government's past success in achieving high connectivity is due to the establishment of NIS[26].

5.3.3.2 Strategies for Connectivity

The report presented two strategies for improving the data connectivity of all government institutes.

[25] It is presumed that NIC is the 102nd connected institution.
[26] National Information System

The first strategy suggested connecting all institutions via 256kbs digital leased lines with JTC to the NIC. Each institution would be upgraded with the necessary communication hardware, including digital modems and routers, necessary to establish the connection. The overall cost of this strategy was determined as follows:

Component	Cost
Equipment Costs - digital modems - routers - servers	**JD 930,000** (180,000) (150,000) (500,000)
Annual Operational Costs (cost of leased 256kbs lines)	**JD 100,000**

The second strategy suggested the institutions be connected by 2mbs E1 links to JTC's ATM backbone network. The author reported that the benefits of this architecture were higher speeds and improved reliability. The overall cost of the second strategy was suggested as follows:

Component	Cost
Equipment Costs - digital modems - routers - servers	**JD 930,000** (180,000) (150,000) (500,000)
Annual Operational Costs (cost of leased 256kbs lines)	**JD 550,000**

5.3.3.3 Review

The NIC's report suggest two very valid options for connectivity. Both strategies keep the NIC as the main exit/entry point to the network, and would provide interconnectivity if configured properly. As suggested below, the study does not provide a mechanism for separating internet traffic from the Government network for added security.

The NIC's report also demonstrates the difficulties in accurately forecasting network costs. A few months after the report was issued, JTC formally launched their ATM backbone and substantially reduced costs. The new prices roughly provide the full 2mbs access at the annual costs suggested for the 256kbs.

5.3.4 E-Government Government Secure Intranet (GSI)

5.3.4.1 Overview

In the Implementation Plan presented to His Majesty King Abdullah II in September 2000, the E-Government Task Force of the Economic Consultative Committee (ECC) noted the importance of data networks and listed the

development of a "Government Secure Intranet" (GSI) as a major task within its Infrastructure Component 1 : Access Media Program.[27]

Since September 2000, the E-Government Task Force has acquired the assistance of both Microsoft and Cisco to assist it in developing a pilot secure intranet that links approximately seven public institutions.

As of the this writing, the GSI design has not been finalized, however the recommendations that are currently being evaluated include:

- a data center (perhaps using the existing NIC) should be established that will serve as a focal point for all internet and intranet traffic. E-mail and web-server will be consolidated at this data center.
- to maintain security, the Government should separate its Internet and intra-agency network traffic. This calls for each line ministry to maintain two routers: one for Internet traffic and one for intranet.
- data communication should utilize the frame relay technology being offered by Batelco Jordan. Individual PVC will be configured for optimal bandwidth.
- separate firewalls will be established at each site to protect inter-agency traffic, and a central firewall will be established at the data center to protect the entire network from the Internet.

5.3.4.2 Review

In discussion with representatives from both Microsoft and Cisco (NCR), the project team has determined that all parties share the same general vision for intra-Government data communication and for a pilot network. Almost all of the recommendations offered by GSI technical team are exactly in-line with those listed in this report.

The project team believe that the this report and the GSI initiative complement each other and are a positive step for the Government. While the GSI initiative focuses on establishing secure and reliable connectivity (a goal shared by this report), the GCCI project has expanded on this objective by exploring potential applications and management issues that will add value to any network proposed.

5.4 Public Network Options in Jordan

5.4.1 Introduction

As described in Section 5.2 above, the most cost-efficient and flexible network design is based on the use of public network facilities. By using the local telecommunication infrastructure, organizations save the expense and complexity of establishing direct cable or wireless (microwave) links.

In this section of the report, the two main public network options, Jordan Telecommunication Corporation (JTC) and Batelco Jordan (BJ), available in Jordan are reviewed. The technologies used by each company are briefly described and their merits highlighted.

[27] Launching E-Government in Jordan : A Proposed Approach, pg 4-16.

5.4.2 The Law

While this report views both JTC and BJ as separate, independent options the reality is more complex, and there exists issues over the legal boundaries of the services being offered by the JTC. Also, BJ's services are directly related to JTC's services so the two entities are not wholly separate.

During its privatization in January 2000, JTC was given, until December 31, 2004, the "sole and exclusive right and license in Jordan to operate (i) a Public Switched Voice Services, and the PTTN, including, for greater certainty, the provision of leased circuit services and all PTTN network facilities to other Public Telecommunication Services Providers."[28]

At the same time, however, the Telecommunication Regulatory Commission (TRC)[29] separated communication services and licensing requirements into two different roles:

- **Public Telecommunications Service Provider role**, which requires a Public Telecommunications Services License. JTC is the sole holder of this License until 2004, and is solely responsible for the transmission facilities that carry telecommunications in Jordan; and

- **Data Communication Service Provider role**, which requires a Data Communication License. Data communication is defined as: "a form of telecommunication intended for the transfer of information represented in a manner suitable for automatic processing between data processing equipment, but specifically excluding the transmission of real-time voice."[30] The TRC has specified that JTC cannot be a Data Communication Licensee. As of March, TRC had granted 22 data licenses, of which 20 are operational.

The scope of JTC's legal activities has generated some confusion. In the e-government implementation plan presented to His Majesty in September, it is stated that "Currently, JTC is the only licensed entity in Jordan that can build data networks; no other entity can make data networks available until 2004."[31] The same statement was made to the project team by JTC. Of course, the term "data network" used here is not well defined.

BJ, on the other hand, points out that while JTC does have the responsibility and exclusivity to build telecommunication transmission networks, it *does not* have a data communication license which prevents it from providing data networking services on that network.

The legality of the arrangement, therefore, seems to depend on where JTC draws the line on the data services it provides. JTC is obviously necessary to provide "point-to-point" networking services that link customer premise equipment (CPE)[32]. However, it is questionable if they have the right to provide the CPE, assist the customer to configure or manage it, and to monitor the customer's data throughput.

[28] License Agreement, dated 23 January, 2000 between Telecommunications Regulatory Commission (TRC) and Jordan Telecommunications Company (JTC), pg. 8.
[29] The TRC has been mandated with overseeing and regulating the Telecommunication Industry, in particular the activities of JTC to avoid any anti-competitive practices.
[30] Batelco Jordan Company Profile, pg. 3.
[31] *Launching E-Government in Jordan: A Proposed Approach*, pg. 2-3.
[32] Equipment used at the customer's location, regardless of whether this equipment is leased or owned.

The significance of this issue is that if the Government wishes JTC to provide a fully managed solution, it will want to investigate its legality to do so.

5.4.3 Jordan Telecom Corporation (JTC)

5.4.3.1 Background

On 1 January, 1997 JTC began operations as a new company wholly-owned by the Government but enjoying financial and administrative independence. Three years later, JTC signed an agreement with JITCO[33], a shareholding company formed by France Telecom and the Arab Bank, to purchase a 40% share of the corporation. A further 8% of JTC is owned by The Social Security Corporation and 1% by an employee savings fund.

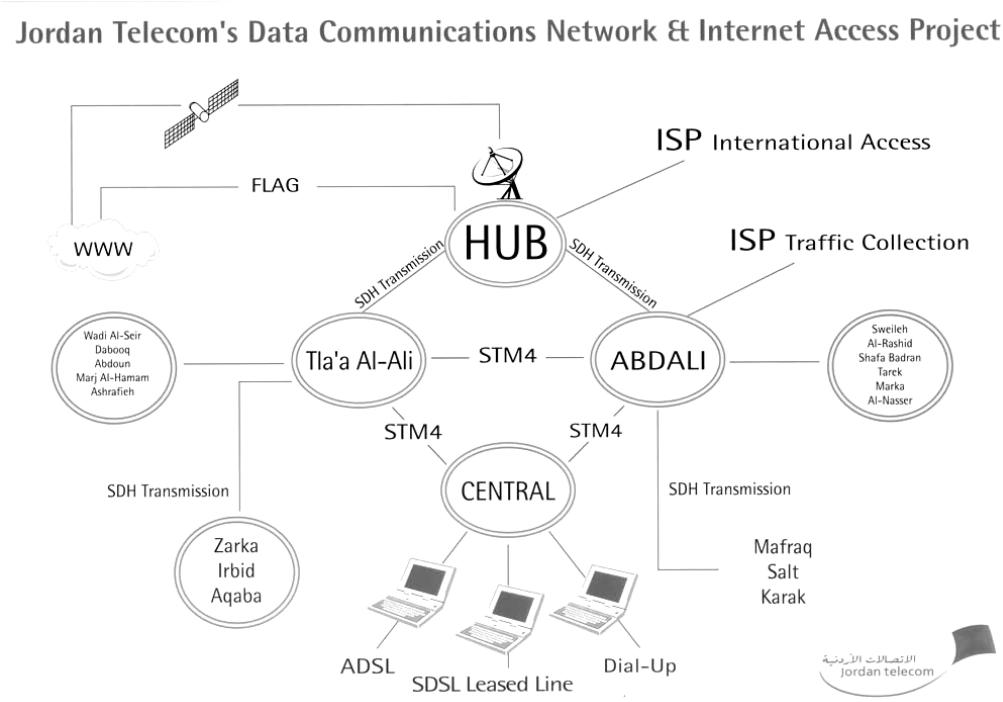
With technical and monetary support from France Telecom, JTC has remodeled itself to be a regional leader in telecommunication services. In 2000, the company launched a mobile phone service, MobileCom, as well as completed its ATM[34] data communication network within the Greater Amman area. In the first half of 2001, the company expanded the network through Jordan and completed its purchase of GlobalOne, the nation's leading Internet Service Provider.

JTC remains the nation's sole licensee for building and managing telecommunication transmission facilities until 2004.

5.4.3.2 Data Communication Network and Internet Access Project

In December 2000, JTC completed the first phase of its data communication network that included the creation of a national HUB, and includes national switching and international connectivity through FLAG and satellite. The network was built with the technical assistance of two global leaders in networking, Cisco and Alcatel. The diagram below shows the network's basic architecture.

[33] 88% France Telecom and 12% Arab Bank.
[34] Asynchronous Transfer Mode - A network technology capable of transmitting data, voice, video, and frame relay traffic in real time.



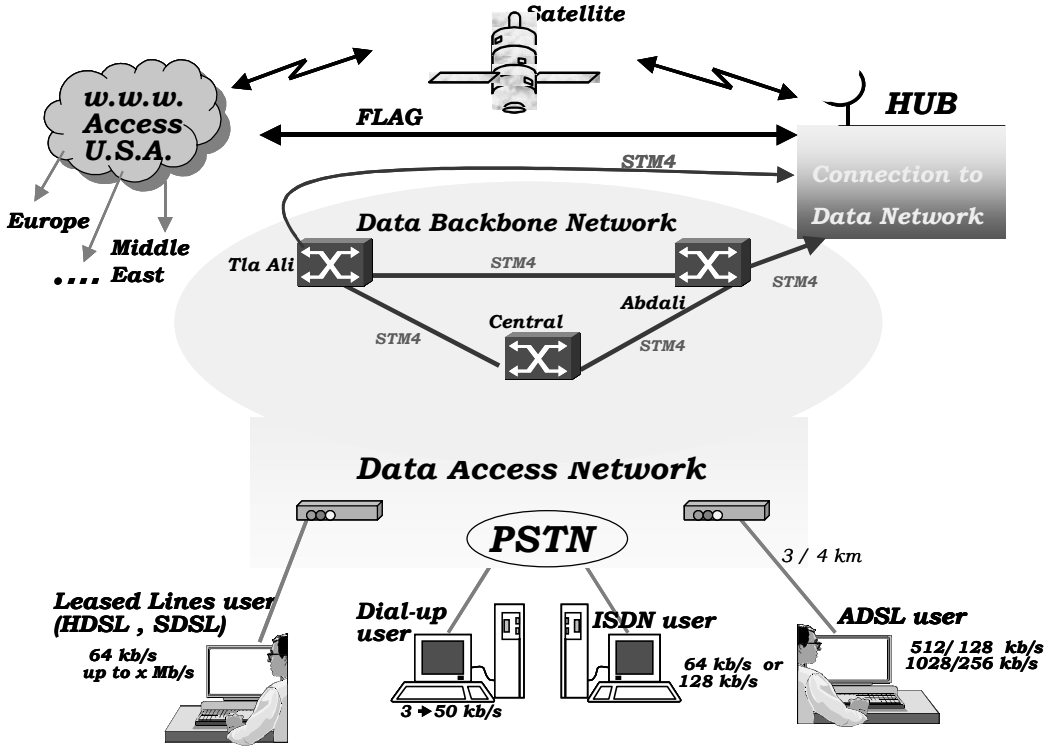
The remaining phases, which provide coverage to the entire nation have been completed throughout the first half of 2001.

The network is IP based on ATM switches, and is centered around three core points of presence (POP) at Tla'a Al-Ali, Abdali and Downtown (Central) in Amman.

The completion of the estimated $4.2 million project is a major accomplishment for Jordan and JTC. It provides Jordan with a state of the art telecommunication backbone that is capable of substantial growth and expansion. The current infrastructure is capable of handling around 70mbs and is expected to be expanded to over 180mbs. The nation's entire data communication needs are currently less than 30mbs.

JTC built the data network as a means to provide cheaper and faster data access to the Internet. Shortly after completing the network, JTC announced the availability of ADSL[35] service within the Greater Amman area. The diagram below illustrates JTC's vision for internet access via the new network:

[35] Asymmetric Digital Subscriber Line - a high-speed data access method that uses ordinary phone lines.



The following is a brief description of some of the technologies that JTC uses and recommends for their data communication network.

5.4.3.3 DSL

DSL (or Digital Subscriber Line) is a family (sometimes referred to as simply xDSL) of different technologies that are similar in nature but intended for different users and applications. As its name implies, the technology relies on a digital circuit within the telecommunication carrier, and therefore is not suitable for analog environments.

Three three main technologies in the DSL family are : ADSL (Asymmetric Digital Subscriber Line), HDSL (High-Bit-Rate Speed Digital Subscriber Line) and SDSL (Symmetric Digital Subscriber Line). Each of the three are described below:

- **ADSL** provides high-speed digital access over ordinary telephone lines, as long as the subscriber is within 3 to 4 km of a Point of Presence (POP). ADSL delivers high-speed download and upload speeds in a versatile manner over such lines. ADSL gets its name from its inherent asymmetry. The upstream[36] bandwidth is less than the downstream[37] bandwidth. Originally designed for voice and video transmission, ADSL has proven very successful for Internet access since most traffic is downstream.

  ADSL is primarily intended for residential, and small or medium offices to connect to the Internet because it uses existing single pair, copper phone lines and allows the existing line to be used for both voice and data. JTC does not

[36] Upstream means the data stream from the subscriber to the network
[37] Downstream means the data stream from the network to the subscriber

offer ADSL services for general connectivity (i.e., for linking branch offices, etc..), and their current pricing structure is based on Internet access only. However, if JTC changes its approach, ADSL technology may become a viable option for smaller Government offices in the future.

- **SDSL** is a faster speed variant of ADSL technology that uses the same speeds for upstream and downstream communication (hence the 'symmetry' in its name). SDSL can still use a single copper pair line--- the same one used for ordinary analog telephone lines—provided these lines are within a limited distance of a POP. SDSL usually offers a data rate up to 1024 kbps. Thus, it is designed for applications, such as video-conferencing, that require identical downstream and upstream transmission rates.

- **HDSL** can be viewed as the big brother in the DSL family. As with ADSL and SDSL, HDSL architectures are based on copper loops between the subscriber premises and the central office, and present the same distance limitations. The difference between the other technologies is that HDSL requires 2 pairs (although variants use 1 and 3 pairs) of copper wire, thus requiring custom installation of cabling. HDSL cannot support both voice and data.

  HDSL operates over standard leased lines (or circuits) and supports speeds in multiples of 64k up to 2.048 mbs.

  HDSL is the best technology for the Government to connect to the JTC communication infrastructure, as long as distance limitations are met.

5.4.3.4 ATM

Asynchronous Transfer Mode (ATM) is a packet-oriented transfer mode that uses an asynchronous time division multiplexing technique. ATM is as adept at handling real-time traffic, such as voice and video, and bursty LAN traffic. It is scaleable from the currently available E1 rates (2048kbs) to full optical speeds (622 Mbps).

This combination of capabilities means that ATM is the first technology capable of delivering or carrying all forms of traffic over a single network infrastructure, ultimately providing significant improvements in network flexibility, efficiency, and price performance. JTC has selected ATM as the transfer mode for its data communication backbone.

Because ATM requires expensive hardware, it is generally used in large, traffic-intensive networks, but it's price is expected to decrease and it is viewed as the leading network transfer mechanism for the future.

5.4.4 Batelco Jordan

5.4.4.1 Background

Batelco Jordan (BJ) was previously First Telecommunications Group (FTG) and is a public company established in 1996 to manage and operate telecommunication and value-added network solutions.

The company is one of Batelco Middle East companies, which includes Batelco Telecom, Bahrain's main telecommunication company. Batelco maintains a

strategic partnership with Cable and Wireless, the largest owner of fiber submarine cables and the lead player in the IP backbone of the world.

BJ is a “value-added reseller” of network services meaning that it offers services based on other carriers’ (JTC) networks. It does not own any of it’s own cables or infrastructure, but layers its services on top of the existing infrastructure owned by JTC.

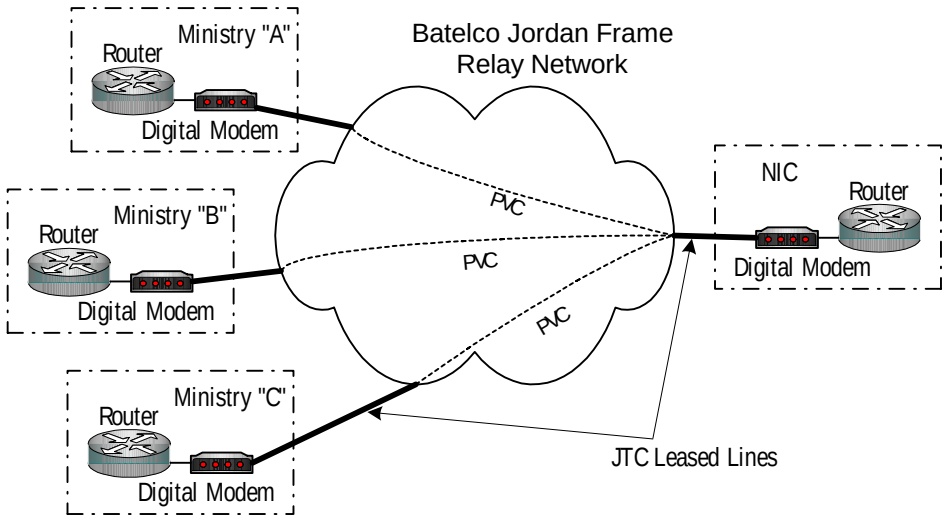
BJ has a wide variety of customers within Jordan including most of the major banks and supermarkets, as well as Royal Jordanian, the national air carrier. It is also the primary network provider for Automatic Teller Machines (ATMs) in the Kingdom.

BJ is currently working with a number of Government institutions, including the Ministry of Water & Irrigation, to provide data communication solutions. CBJ is currently exploring using BJ’s services as the backbone for communications between the CBJ and the commercial banks.

5.4.4.2 Frame Relay

BT’s primary data networking service is based on its frame relay network.

Frame relay is a packet-switching protocol that allows LANs to interconnect using a single point-to-point link to a frame relay “cloud” that properly routes traffic. Frame relay makes use of Permanent Virtual Circuits (PVCs) that are logical paths established between two locations. Since the path is fixed, a PVC is the equivalent of a dedicated line, but over a packet-switched public network. This is illustrated in the diagram below:



Each PVC is assigned a Committed Information Rate (CIR), which should represent the average rate at which traffic is sent over the network. Frame relay ports statistically allocate network capacity to active PVCs, so that when one is idle, another may use the entire port. Information that is sent above the CIR of the PVC is marked eligible for discard by the network in case it becomes congested. PVCs and CIR allow the customer to have bandwidth on demand when required--allowing them to occasionally have higher speeds then average to handle a burst of data.

There are many advantages in using frame relay services:

- **bandwidth management** - significant savings can be found in using purchased bandwidth more efficiently. Also, because most of the Government's traffic will be "bursty" or in short, intense segments, a frame relay network will allow the customer to have a higher perceived value of bandwidth then what they have paid for.

- **flexibility** - since connections are made in software, frame relay networks are very easy to reconfigure. If the CIR on a PVC needs to be increased or decreased it can be done fairly easily, as long as the local loop does not have to be changed.

- **reliability** - frame relay networks are designed to automatically route around network failures such as fiber cuts and other service-affecting problems. In general, because of the technology design and network management, frame relay networks are substantially more reliable and have a higher availability than comparable private line solutions.

- **management** - as with all managed network solutions, frame relay service reduce the day-to-day management of the WAN. Because they are an end-to-end solution, the customer requires far less in-house skill and expertise than with unmanaged networks.

- **security** - frame relay technology uses layer 2 (data link) of the OSI model. Layer 2 is not vulnerable to IP[38] attacks that are frequently targeted at layer 3 (networking) transports.

5.4.4.3 Services

BJ's frame relay network currently has 23 nodes across Jordan, with expansion plans to 30 in the near future. Current node locations are in all of the major cities and throughout the Amman metropolitan area.

It has a staff of well-trained engineers and access to technical resources from Batelco Middle East and Cable & Wireless.

BJ's primary value is that it is a single point of contact for network problems. BJ maintains a Network Management Section that monitors all network activities including all issues related to the carrier (JTC). All problems are solved by BJ regardless of whether they are related to BJ's operations or JTC. Where the repairs must be made by JTC technicians, BJ will oversee the repair and the resumption of network services.

[38] Internet Protocol

5.5 Connectivity Options

5.5.1 Introduction

This section reviews the following three options available for connecting the seven pilot agencies:

- Option 1 : Star topology based on JTC HDSL/ATM technology;
- Option 2 : Mesh topology, based on JTC HDSL/ATM technology; and
- Option 3 : Mesh topology, based on BJ Frame Relay.

For each option, there is a high and low speed configuration provided.

The project team has only considered connectivity options that rely on the public telecommunication infrastructure of Jordan, and do not investigate private networks. This is because the network design of the initial seven agencies is a pilot study, and should be applicable to the entire Government in the future. Private networks are rarely cost efficient when operated on a large scale, and involve many network nodes. The use of existing telecommunication infrastructure, as noted in previous sections, is a better option for large, multi-node networks.

The project team also recommend that the Government support the large investment made by JTC in developing their nationwide data communication network. Although the Government has the resources to build duplicate private networks, this does not encourage JTC to expand their infrastructure and provide reliable, quality services.

Finally, there are a number of issues that should be initially considered. These are described in the following section.

5.5.2 Considerations

5.5.2.1 Estimated Traffic (Bandwidth Requirements)

The amount of estimated traffic on the network has a direct implication on the design of the network. The more traffic expected, the higher the bandwidth required, and the more expensive the network.

At present, the project team estimates that in the near future there will minimum traffic on the pilot network due to little current data sharing and a lack of software applications that promote interagency workflow. As stated in the Application section (see page 16) of this report, the Government should strive to add value to the network by installing software that encourages collaborative work between agencies and increase traffic.

The Government should reserve the option to increase bandwidth as traffic increases. Therefore, a good network design will provide scalability with minimal financial impact.

5.5.2.2 Redundancy

Network redundancy in case of failure is an important aspect of network design, and depends on the amount and "importance" of the network traffic. The amount of redundancy, if any, is a matter of opinion and cost.

Most modern routers support ISDN BRI or PRI modules which have the ability to re-route traffic through a secondary path if the primary path fails. When a line failure occurs, a typical scenario is for the router to automatically dial another router (through an ISDN line) and use that router to pass traffic to the network.

Routers can be configured to dial into a central router (requiring PRI module) or sequencing to a peer router (requiring only BRI modules in each).

Obviously this results in a drastic reduction in performance, and depending on the urgency of the data this option may not be acceptable. A higher-cost option is to provide full redundancy by purchase duplicate leased lines and/or to maintain full backup routers.

Ultimately, the answer to how much redundancy should be designed into the system lies in the budget available for the network, and the willingness of the Government to accept outages.

Because the project team expects that the initial traffic on the pilot network will be low, it does not recommend full redundancy at this time. Depending on financing, the Government may wish to purchase the BRI/PRI modules upfront, or wait until they are decided to be necessary.

5.5.2.3 Internet Connectivity

All of the organizations involved in the pilot network design have Internet access through the NIC. This connectivity is made through individual leased lines.

There are two options available, the Government can maintain two different networks: one for Internet access and the other for Government data traffic, or it can choose to combine the two. The merits of each option are presented below:

- **Option 1: Retain separate internet connectivity from pilot network** - With this option, current internet connectivity via leased lines to the NIC will remain as is, and the pilot network will operate independently and will only support inter-agency traffic.

  The main benefits of this option are security and redundancy. A separate network is not vulnerable to attacks from the internet, which is the largest threat to security. Also, redundancy reduces the possibility of loss of both access to the network and the internet at the same time.

  The main drawbacks are cost and additional management. The Government will pay for two lines which given the "bursty" traffic flow of internet traffic is inefficient. A single line of higher capacity would be provide more speed for both applications. Lastly, network administrators are left with the burden of supporting and monitoring two networks.

- **Option 2: Combine internet connectivity into the pilot network** - Another option is replace the existing leased line architecture to the NIC and route all

internet traffic through the pilot network. Traffic directed towards the internet will be routed through the NIC and everything else will go to individual offices.

The main benefits of this option are increased savings and easier management. As noted above, the Government can increase the bandwidth of existing connectivity and obtain higher access speeds for both internet and inter-agency traffic. Any redundancy features built into the single network will provide higher economies of scale.

The main drawbacks are substantially reduced security and more complicated network design (and costing). Since the Government currently has little protection from internet attacks, this threat is serious. Some of the pilot agencies are already using separate networks as their primary defense against internet hacks-- as it remains the most effective means of protecting in-house systems.

Lastly, this option makes the network design and configuration much more complex. Provisions must be made for providing access to the internet, without access to the pilot network and vice versa.

The project team recommends that for the near future the Government continue to maintain separate networks between for Internet access and inter-agency connectivity, as this is the most effective means of maintaining security. However, as the technical skills of the Government increase and data security is improved, the Government should consider combining the two networks.

5.5.2.4 "Point-to-Point" versus "End-to-End"

Public network providers usually offer two different classes of service: "point-to-point" and "end-to-end". Point-to-point service means that they do not provide the necessary "end" hardware, including digital modems and/or routers. End-to-end service includes this equipment, although sometimes the service only includes the digital modems (or CSU/DSU) equipment.

Service choice depends largely on the monthly lease fees over purchase fees. However, other factors should also be considered, including:

- **anticipated frequency of change** - if the Government anticipates that it will be frequently upgrading speeds as new applications create greater traffic, then it should consider end-to-end agreements;

- **technical skills and resources** - if the Government wants to reduce its reliance on its network administrators, it should consider end-to-end agreement since the maintenance and configuration burden lies with the network provider;

- **risk aversion** - an important consideration is to reduce risk and simplify troubleshooting. An end-to-end solution eliminates the risk of having the network provider place blame for network problems on the end hardware, while having the vendor of the end hardware blame the network provider. This is a common situation and an important risk to consider.

Based on the current situation in Jordan, the project team highly recommend that the Government does not consider point-to-point solutions. Some of the options provided are supposedly offered by JTC as point-to-point configurations (the customer is responsible for purchasing the end-equipment) but this has never

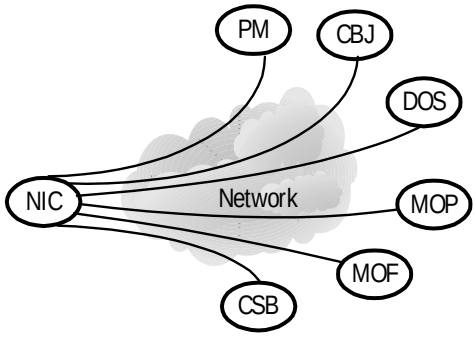
been tested in practice. The common consensus is that eventually JTC will insist that it provide the CSU/DSU (digital modems) equipment as this must be compatible with their existing equipment. The risks associated with purchasing equipment to be managed by JTC in their internal networking are too great. For example, agreements will need to be completed that handle contingencies such as power protection, mishandling by JTC staff, theft, service changes, etc..

5.5.2.5 Mesh versus Star Topology

There are two basic network topologies that are being considered for the pilot network design: "Mesh" and "Star".

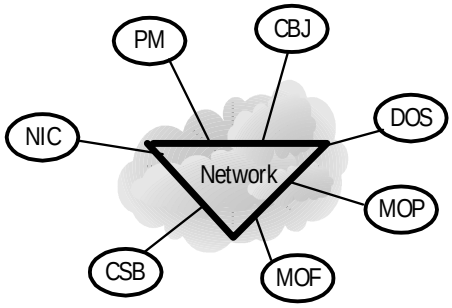
Both topologies have their comparative advantages and disadvantages, and the choice of topology has a significant impact on the cost and reliability of the network. The Government has to consider the merits of each topology carefully before designing on the final design of the network.

A "star" topology requires a central node, or hub, as illustrated below:



All network nodes are connect either physically or logically to this central node, and all traffic is routed to it. In the above example, data that is sent from the PM to the CBJ is goes through the NIC.

A "mesh" technology does not rely on a central node. All network nodes are connected to a central backbone which delivers traffic directly to the correct address on the network, as illustrated below:



A "mesh" topology assumes that each node has direct access to all other nodes on the network. In a private line scenario, this would require a "mesh" of *n(n-1)/2* lines to interconnect all nodes. Although, public networks rely on an internal "ring" or "bus" backbone instead of *n(n-1)/2* lines, the topology is still referred to as a "mesh".

The **advantages** of a "mesh" topology are:

- the failure of any one node has a minimal impact on the network;
- usually lower costs, as each node only needs to connect to its nearest POP[39]; and
- if the service provider manages the network within the "cloud", then the customer requires less networking skills and has less responsibilities.

The **disadvantages** of a "mesh" topology are:

- the reliability of the overall network depends on the ability of the service provider to manage the "cloud".

5.5.2.6 Network Operations Center

As demonstrated in the "star" topology example above, some network designs require a central node or hub.

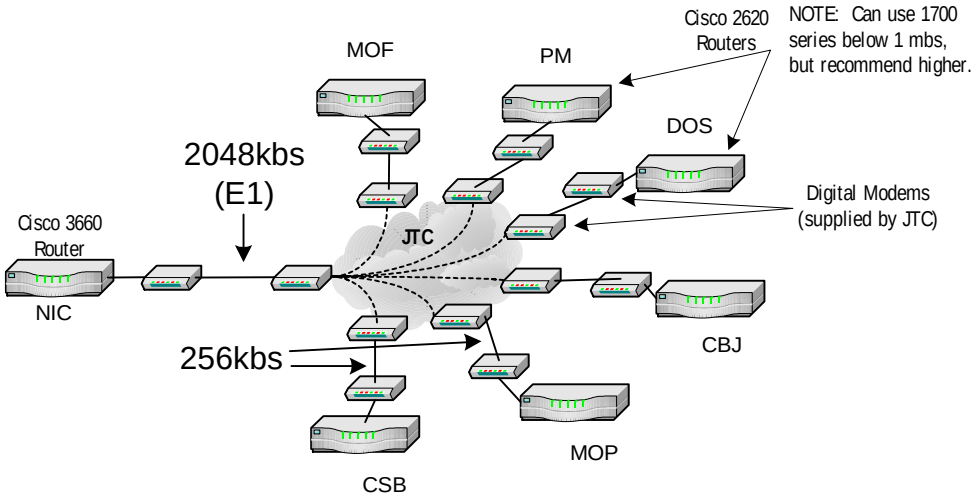
The project team highly recommends that the NIC perform the role as network operations center and central node to the Government network. The NIC has the necessary technical expertise and capacity for this function.

As such, whenever necessary, this report places the central node as the NIC. However, this can easily be modified to be any other node if necessary.

[39] Point of Presence - a regional location of the telecommunication carrier (JTC) that serves as an entry point into a greater network.

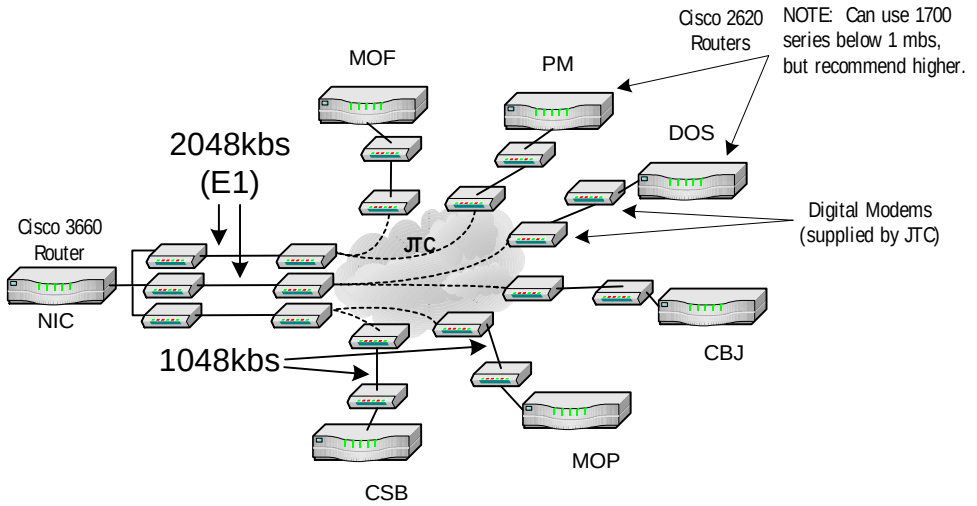
5.5.3 Option 1 : Star topology based on JTC HDSL/ATM technology

5.5.3.1 Description



This option connects each network node using SDSL or HDSL digital modems (depending on speed) to the JTC ATM network. Circuits are configured between each node and a central node (which, for this report is designated as the NIC). All traffic flows through the central node to other nodes. The speed of the circuit between the central node and the network must meet or exceed the sum of the other nodes. In the above example, 6 x 256kbs = 1512kbs, so a single E1 link is used.

Since the maximum transmission speed of a circuit is 2048mbs (E1), as the speed of each network node is increased, additional lines may be required between the central node and the network. These additional lines also require additional modems to be added to the configuration. The figure below demonstrates this scenario for a 1048kbs network, in which 6 X 1024kbs = 6144 kbs; which is supported by 3 x 2048kbs (E1) lines, requiring 4 additional modems:



5.5.3.2 Advantages

The main advantages of this option are:

- **Centralized management** - the network can be easily centrally managed by the central node (NIC). There is little, if any, reliance on the carrier (JTC) to manage network traffic.

- **Simple configuration** - the routing tables and configuration of the network is relatively simple. All traffic is routed from each node to the central node.

- **Internet access** - since the NIC is the Internet Service Provider of the Government, the star configuration using NIC as the central hub is efficient if the Government decides to consolidate its inter-agency and Internet traffic. Since it is anticipated that there will be more Internet traffic than inter-agency traffic, this configuration *may* provide the optimal speeds. However, as noted above, it is recommended that the Government maintain completely separate networks for Internet and inter-agency traffic (requiring duplicate lines and routers, etc..)

5.5.3.3 Disadvantages

The main disadvantages of this option are:

- **Single point of failure** - a failure at the central node (NIC) will cripple the entire network.

- **Bottleneck** - although the configuration ensures that sufficient bandwidth is available at the central node, there remains the risk of bottlenecking traffic within the NIC. The central router must be capable of handling the entire network's traffic.

- **Inflexible** - adding new nodes to the network requires modifying the capacity of the central node. Periodic additions to the network will not be economically viable. Too many network nodes will require a complete re-design of the central node.

- **Distance sensitive** - the option provided works well if the network nodes are all in relatively close proximity to the central node. However, if distant nodes (Aqaba, Karak) are attached, the cost of establishing the leased circuit may increase.

5.5.3.4 Cost

- **Monthly operating costs**

The table below shows prices provided by JTC for the above configuration[40]. The prices are based on an end-to-end solution in which JTC provides all digital modems. The Government will need to purchase its own routers, as represented in the second table.

JTC Star Option End-to-End Solution (without routers) Component Prices (JD)	256kbs	512kbs	1024kbs	2048kbs
Installation Fees per Line	700	700	700	700
Installation Sales Taxes (13%) per Line	91	91	91	91
Total One-time Installation Cost for 6 Lines	***4,746***	***4,746***	***4,746***	***4,746***
USD Equivalent	***$6,703***	***$6,703***	***$6,703***	***$6,703***
Monthly Fees per Line	78	142	270	494
Monthly Fees Sales Tax (13%) per Line	11	16	35	64
Total Monthly Line Fees for 6 Lines	**531**	**966**	**1,833**	**3,352**
Total Number of Modems Required	14	16	18	24
Monthly Modem Lease Charges per Unit	34	34	34	34
Monthly Modem Sales Tax (13%) per Unit	5	5	5	5
Total Monthly Modem Lease Fees	**544**	**622**	**700**	**933**
Total Monthly Fees (Lines + Modems)	***1,076***	***1,587***	***2,533***	***4,284***
USD Equivalent	***$1,520***	***$2,242***	***$3,578***	***$6,051***

- **Hardware (capital) costs**

The table below shows estimated costs for the hardware (routers) to support the above configuration. Cisco brand routers have been chosen as an example, but the Government may find equivalent, cheaper routers.

Also, the routers below were chosen for their expandability and for their G.703 compatibility. Cheaper lower-end models are available, but are not recommended, and should only be considered if there are budget constraints.

The router prices also the cost of a single ISDN BRI modules for redundancy, however the cost of the ISDN service (from JTC) has not been included in the analysis as it is the same for all three options.

[40] Please refer to JTC Price Proposal in Appendix C

JTC Star Configuration Hardware Component Prices (JD)	256kbs	512kbs	1024kbs	2048kbs
Six 2620 Routers with G.703 E1 Module and ISDN BRI Module [41]	23,364	23,364	23,364	23,364
One 3660 Router with Redundant Power	7,930	7,930	7,930	7,930
Number of G.703 E1 Modules Required	1	2	3	6
Total Cost of G.703 E1 Module[42] as Required	1,840	3,680	5,520	11,040
Total Hardware Cost	***33,134***	***34,974***	***36,814***	***42,334***
USD Equivalent	***$46,799***	***$49,398***	***$51,997***	***$59,794***

- **Three year projected costs**

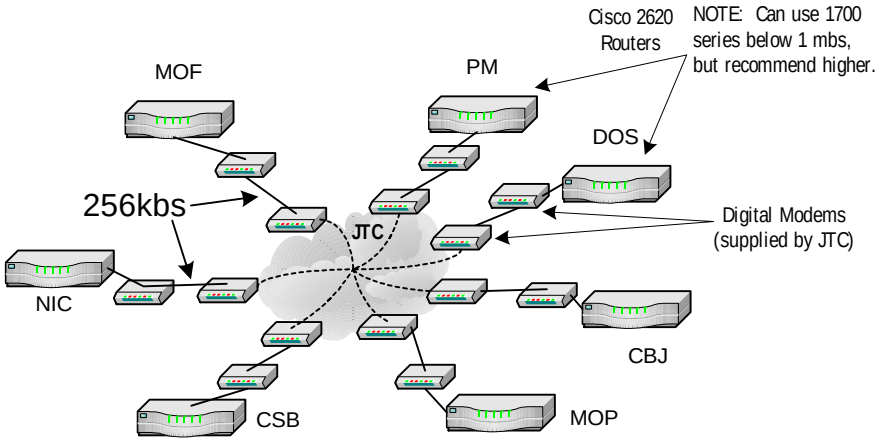
To facilitate comparisons between options, the table below represents all costs projected over a period of three years. Further analysis can be easily performed for scenarios greater than three years.

JTC Star Configuration 3 Year Projected Total Costs (JD)	256kbs	512kbs	1024kbs	2048kbs
Installation Fees	4,746	4,746	4,746	4,746
Total Hardware Cost	33,134	34,974	36,814	42,334
Monthly Line/Modem Lease for 36 months	38,736	57,132	91,188	154,224
Total 3 Year Projected Cost	***76,616***	***96,852***	***132,748***	***201,304***
USD Equivalent	***$108,215***	***$136,797***	***$187,497***	***$284,328***

[41] Approximately JD 3894 ($5500) each.
[42] Approximately JD 1840 ($2600) each.

5.5.4 Option 2 : Mesh topology based on JTC HDSL/ATM technology

5.5.4.1 Description



This option connects each network node using SDSL or HDSL digital modems (depending on speed) to the JTC ATM transmission network. Unlike the star topology in Option 1, there is no central node in this configuration, and traffic is routed directly from node to node using JTC's ATM switches.

5.5.4.2 Advantages

The main advantages of this option are:

- **No point of failure** - unlike the star configuration, the mesh configuration has no single point of failure and therefore it is much more reliable. There is also no potential bottleneck.

- **highly flexible/expandable** - the mesh configuration is highly expandable and allows for unlimited additional nodes with no major network redesign. Nodes can also be moved or reconfigured with little effort. Since the proposed routers can support speeds from 256kbs to E1, increases in bandwidth requires minimal additional hardware purchases.

- **no distance penalty** - since each node only needs to connect to the network carrier's nearest POP, there is no penalty if a network node is in a different city. However, because the above configuration is based on DSL technology, there is a limitation to which a node must be near a POP.

- **more efficient routing** - a mesh configuration allows traffic to be routed more efficiently, thorough less switches and modems, thereby limiting the possibility of hardware failure.

5.5.4.3 Disadvantages

The main disadvantage of this option is:

- the reliability of the overall network depends on the ability of JTC to properly monitor and manage the network. As noted in Section 5.4.2 , there remain an important issues whether JTC to can legally provide managed data communication services. This option may not be legally available.

5.5.4.4 Cost

- **Monthly operating costs**

The table below shows prices provided by JTC[43] for the mesh configuration. The prices are similar to the star configuration with the following exceptions:

- Seven lines are required to be leased instead of six; and

- The number of modems required remains constant regardless of network speed.

JTC Mesh Option End-to-End Solution (without routers) Component Prices (JD)	256kbs	512kbs	1024kbs	2048kbs
Installation Fees per Line	700	700	700	700
Installation Sales Taxes (13%) per Line	91	91	91	91
Total One-time Installation Cost for 7 Lines	***5,537***	***5,537***	***5,537***	***5,537***
USD Equivalent	***$7,821***	***$7,821***	***$7,821***	***$7,821***
Monthly Fees per Line	78	142	270	494
Monthly Fees Sales Tax (13%) per Line	11	16	35	64
Total Monthly Line Fees for 7 Lines	**621**	**1,126**	**2,139**	**3,911**
Total Number of Modems Required	14	14	14	14
Monthly Modem Lease Charges per Unit	34	34	34	34
Monthly Modem Sales Tax (13%) per Unit	5	5	5	5
Total Monthly Modem Lease Fees	**544**	**544**	**544**	**544**
Total Monthly Fees (Lines + Modems)	***1,165***	***1,670***	***2,683***	***4,455***
USD Equivalent	***$1,645***	***$2,359***	***$3,790***	***$6,292***

- **Hardware (capital) costs**

The table below shows estimated costs for the hardware (routers) to support the mesh configuration. The same assumptions and recommendations remain as the star configuration.

[43] Please refer to JTC price proposal in Appendix C

The hardware difference of the mesh configuration is that since there is no central hub, all nodes can use the same router type. There is no need for a powerful Cisco 3600 series router at the central hub.

JTC Mesh Configuration Hardware Component Prices (JD)	256kbs	512kbs	1024kbs	2048kbs
Seven 2620 Routers with G.703 E1 Module and ISDN BRI Module[44]	27,258	27,258	27,258	27,258
Total Hardware Cost	27,258	27,258	27,258	27,258
USD Equivalent	***$38,500***	***$38,500***	***$38,500***	***$38,500***

- **Three year projected costs**

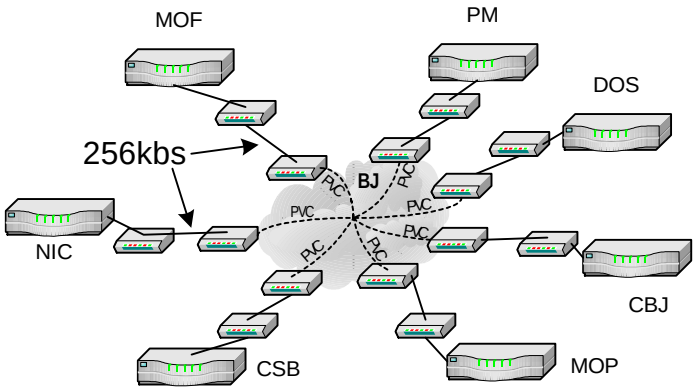
The table below shows the same three year projected costs as in the Star configuration.

JTC Mesh Configuration 3 Year Projected Total Costs (JD)	256kbs	512kbs	1024kbs	2048kbs
Installation Fees	5,537	5,537	5,537	5,537
Total Hardware Cost	27,258	27,258	27,258	27,258
Monthly Line/Modem Lease for 36 months	41,940	60,120	96,588	160,380
Total 3 Year Projected Cost	***74,735***	***92,915***	***129,383***	***193,175***
USD Equivalent	***$105,558***	***$131,236***	***$182,744***	***$272,846***

[44] Approximately JD 3894 ($5500) each.

5.5.5 Option 3 : Mesh topology based on BJ Frame Relay technology

5.5.5.1 Description



5.5.5.2 Advantages

All of the same advantages of a mesh configuration noted in Option 2 are available with this option, however the use of Frame Relay technology and Batelco Jordan offer the following additional advantages:

- **Single point of service** - by employing a private firm to manage the data network, the Government is provided a "one-stop-shop" for all network problems-- substantially reducing the need for experienced networking professionals in the civil service. This is a first step towards improving Government IT management by outsourcing technical services to specialists in the private sector. Since BJ provides all hardware, software and configuration, they are a single point of service for any problems related to the network.

- **Bandwidth Management** - Frame Relay technology allows for much better management of available bandwidth. The CIR of each PVC can be set to a rate that is higher or lower than other PVCs, allowing for a more optimal configuration based on expected traffic. For example, if one Ministry primarily accesses the database of another Ministry, the PVC rate for that path (and in some situations, that application) can be increased to provide better service.

- **Layer 2 security** - Frame relay transport at Layer 2 of the OSI model provides better security than comparable IP transports at Layer 3 (which are frequently targeted for attack.)

- **Legality** - As noted in Section 5.4.2 , the extent to which JTC can legally provide data networking services is unclear at this point. There is no doubt, however, that BJ's solutions are entirely legal under existing laws.

5.5.5.3 Disadvantages

The main disadvantage of Option #3 is the Government's reliance on BJ to provide all networking services. However, all of the nation's major banks, as well as the CBJ, currently rely on BJ's operations so the risk of discontinuation or deterioration of service is less likely.

5.5.5.4 Cost

- **Monthly operating costs**

BJ has provides both point-to-point and end-to-end services[45]. To facilitate comparisons between costs, this report will only provide their costing of end-to-end services which include all necessary hardware--- including digital modems (supplied by JTC) *and routers (with ISDN BRI modules)*. BJ offers both a one-year and three-year service contract; the one year requires an initiation charge. The first table below shows the costs for a one year contract:

BJ Frame Relay Option End-to-End Solution with Routers One - Year Contract Component Prices (JD)	256kbs	512kbs	1024kbs	2048kbs
Initiation Charge for 7 nodes	4,472	4,472	4,472	4,472
Initiation Charge Sales Tax (13%)	581	581	581	581
Total Initiation Charge with Tax	***5,053***	***5,053***	***5,053***	***5,053***
USD Equivalent	***$7,137***	***$7,137***	***$7,137***	***$7,137***
Monthly Charge for 7 nodes[46]	***1,512***	***1,960***	***2,856***	***4,424***
Monthly Charge Sales Tax (13%)	197	255	371	575
Total Monthly Charges with Tax	***1,709***	***2,215***	***3,227***	***4,999***
USD Equivalent	***$2,414***	***$3,129***	***$4,558***	***$7,061***

- **Three year projected costs**

The table below shows the projected costs for three years of service:

BJ Frame Relay Option 3 Year Projected Total Costs Component Prices (JD)	256kbs	512kbs	1024kbs	2048kbs
Total charges of 7 nodes for 36 months [47]	***91,224***	***107,352***	***139,608***	***196,056***
Sales Tax (13%)	11,859	13,956	18,149	25,487
Total 3 Year Projected Cost	***103,083***	***121,308***	***157,757***	***221,543***
USD Equivalent	***$145,597***	***$171,339***	***$222,821***	***$312,914***

[45] Please refer to BJ price proposal attached as Appendix D.
[46] Annual charges per node are as follows: 256Kbs- JD2592, 512Kbs- JD3360, 1Mbs- JD 4896, E1- JD 7584
[47] Annual charges per node are as follows: 256Kbs- JD4344, 512Kbs- JD5112, 1Mbs- JD 6648, E1- JD 9336

5.6 Recommendations

5.6.1 Overview

The table below shows a summary of the 3 options presented above. The summary table shows the projected costs over three years for each option:

Options Three year Projected Costs	256kbs	512kbs	1024kbs	2048kbs
Option 1 - JTC Star Configuration	***76,616***	***96,852***	***132,748***	***201,304***
USD Equivalent	***$108,215***	***$136,797***	***$187,497***	***$284,328***
Option 2 - JTC Mesh Configuration	***74,735***	***92,915***	***129,383***	***193,175***
USD Equivalent	***$105,558***	***$131,236***	***$182,744***	***$272,846***
Option 3 - BJ Frame Relay Service	***103,083***	***121,308***	***157,757***	***221,543***
USD Equivalent	***$145,597***	***$171,339***	***$222,821***	***$312,914***

5.6.1.1 Price considerations

In evaluating the summary table above, it is necessary to include the following considerations:

- Options 1 & 2 do not include the manpower costs of managing the entire network, including salary, training, and benefits. The Government will need the services of at least two full time networking specialists to provide minimal 8am to 3pm support. This consideration will *increase* the cost of Options 1 & 2.

- The equipment purchased in Options 1 & 2 is expected to have a useful life of greater than three years, thereby leaving a residual value. This consideration will *decrease* the cost of Options 1 & 2.

- Options 1 & 2 do not include network monitoring and management hardware and software (SNMP & RMON) that check the performance of the network. Since Option 3 is a managed solution, this equipment is not required as it is in handled by BJ. This consideration will *increase* the cost of Option 1 & 2.

- It is unclear what is the financial impact of substantially increasing bandwidth during the contract with Option 3. If this occurs, it will likely *increase* the cost of Option 3.

5.6.2 Recommendations

Recommendation #5.6.1 : *Select Batelco Frame Relay services*

The project team, after evaluating the connectivity options' advantages, disadvantages and costs recommend that the Government select Option 3 using Batelco's Frame Relay services

with a mesh configuration. Although the cost over three years is calculated at approximately 35% more than the JTC mesh option, the project team recognizes that reductions in manpower and risks, as well as the increased reliability of a managed network solution, justify the increased cost.

The project team also recognizes that Batelco has substantial experience in managing and maintaining public networks in Jordan, and has proven its reliability to the Banking sector. Until both the Government and JTC have similar experience, Batelco should remain the network provider of choice.

Recommendation #5.6.2 : Conduct a networking workshop with all stakeholders.

As noted in Section 5.1.1 , the choice of the best network option is subjective and the project team recognizes that the two other solutions provide comparative solutions. The project team *highly* encourages the Government to conduct a workshop with representatives from Batelco, JTC, NIC and the LAN administrators of the pilot agencies to fully explore and debate the relative merits of each option, using this study as a basis for the discussions. The Government should also include financing options, which are unknown at this time, into the decision process.

6

Section 6 : Summary of Recommendations

6.1 Introduction

This section contains a summary of the recommendations provided throughout the report. They are presented in the categories listed in the report itself.

6.2 Application Section Recommendations

Recommendation #3.3.1 : *Form a working committee of stakeholders*

As mentioned in the Critical Success Factors above, an integrated GFMS requires the full support of all agencies associated with the fiscal management. The Prime Ministry or related organisation should appoint a working committee with high-level representation from each of these agencies to initiate and oversee the GFMS process.

Recommendation #3.3.2 : *Begin the process of implementing an HRIS*

As described in Section 3.2.7 above, the project team recommends that the Government begin its step-by-step implementation of a GFMS by implementing a web-based HRIS. The lessons learned from this project will provide invaluable experience before the more complex task of developing the core accounting systems is attempted.

Recommendation #3.4.1 : *Consolidate e-mail servers to a central site (NIC)*

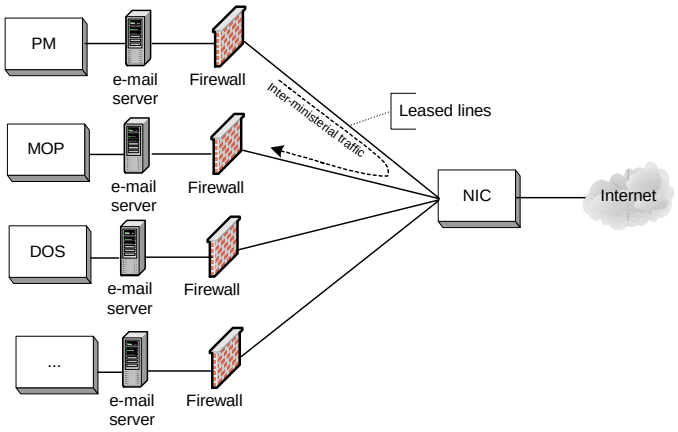
The Government should not rely on the technical skills and abilities of each line agency for e-mail usage. Individual line agency e-mail servers should be consolidated and moved to a central site, creating a "server farm[48]". The project team recommends the National Information Centre (NIC) be considered for the central site because of its role as network operation center and primary ISP to the Government. The LAN Administrators of each agency can continue to administer their agencies' e-mail usage, however the physical servers should be moved to the central site.

The Government should also consolidate web servers for the same reasons and benefits.

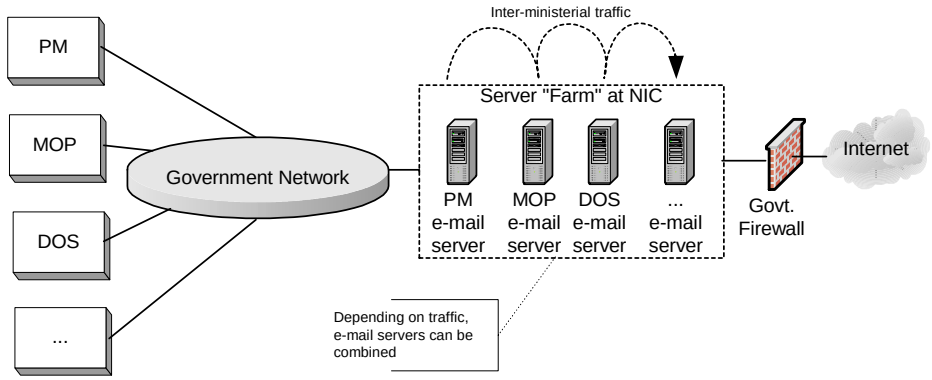
The figures below illustrates the current and recommended e-mail configurations for the Government:

[48] a "server farm" is a facility that houses and maintains a wide variety of hardware servers. By housing all servers in one location, organizations can more easily provide physical security, as well as state-of-the-art fire and power protection.

Current E-Mail Server Architecture



Recommended E-Mail Server Architecture



The consolidation of e-mail servers will have the following benefits:

- **improved reliability** - the central site can provide round-the-clock maintenance and support. E-mail servers will be less dependent on the data communication linkage between the line agency and the Government ISP (NIC).

- **improved protection** - the central site can install and support one firewall and security zone that will protect all servers uniformly. It is much easier to maintain the security and integrity of one firewall than dozens of distributed and separately maintained firewalls. Industrial-strength (and expensive) virus protection can be purchased to protect all sites, thereby providing economies of scale.

- **reduced reliance on individual skills** - the e-mail communication of most agencies currently depends on the skills and resources of its LAN administrator. By consolidating e-mail servers, the Government can reduce its need for trained e-mail administrators and reduce its reliance on the individual skills of key staff.

- **easier to implement and maintain an Enterprise Directory** - a consolidated server farm will make it easier for the Government to implement and maintain an Enterprise Directory such as Active Directory, etc. . The server farm will reduce the overhead traffic connecting each individual site.

- **reduced bandwidth requirements** - as illustrated in the recommended figure above, inter-ministerial traffic remains within the server farm thereby reducing the overall bandwidth requirements to individual line agencies.

- **substantial cost savings** - the Government will realize substantial cost savings by allowing smaller agencies to share hardware servers, and by reducing the number of firewalls and virus protection applications required by all line agencies. Furthermore, each line agency will require less bandwidth to their individual locations and will require less personnel to maintain and operate the site.

Recommendation #3.4.2 : *Clarify e-mail access rights*

The use of e-mail in the Government is too important to leave to the discretion of individual ministerial management. The Government should quickly define and adopt a policy the stipulates full e-mail access for all civil servants regardless of their employment status.

To provide e-mail to non-administrative personnel and those without computer access, the Government should strive to have public workstations made available in each Ministry that allow for e-mail and internet use. Low-cost "web computers" are available in the marketplace that have limited capacity and are designed for e-mail and internet access only. These computer typically cost less than $500 and can easily be installed in a controlled location in each organisation.

To encourage e-mail use, the Government should move to send all circulars and employee notifications, as well as general news and information about Government activities via e-mail.

Recommendation #3.4.3 : *Develop policies towards e-mail use and validity*

In the absence of legislation that recognizes the legality of electronic messaging, and until the Government formally adopts a security infrastructure like PKI which avails electronic signatures and other protection measures, a broad policy which defines the valid uses of e-mail should be defined and distributed.

The policy should inform civil servants as to Government e-mail rules and requirements and as to what forms of e-mail use are acceptable.

The policy should serve both to protect the Government from unauthorized uses and abuses of e-mail using Government facilities, as well as to encourage the use of e-mail in non-official

communications.

Recommendation #3.4.4 : *Initiate an extensive e-mail training programme for all civil servants*

The Government should design and implement a long-term training programme that provides all civil servants with an in-depth knowledge of how e-mail works and the variety of options available. Employees should be taught how to use collaborative software features available with e-mail, and how to manage their information. Employees should also be instructed on proper e-mail etiquette and the procedures and regulations of e-mail use in the Government.

Recommendation #3.4.5 : *Standardize e-mail programs (clients) and servers*

Like with word processing, the Government can realize substantial productivity benefits if everyone uses the same vendor's e-mail programs and servers. To make e-mail globally interchangeable, most basic e-mail programmers only provide a limited feature set. However, if an organisation has standardized on a single vendor product, than it can expand this feature set to include a variety of powerful options that can improve workflows and productivity.

Because of the Government's recent blanket licensing of Microsoft products, the project team recommends that it consider standardizing on the use of Microsoft Outlook and Microsoft Exchange Server. These two products provide a wide range of collaborative groupware features that can be used within the Government if everyone uses the same applications.

Standard applications will also substantially reduce the technical support needs.

Recommendation #3.4.6 : *Implement an Enterprise Directory*

The benefits derived from a well-designed Enterprise Directory are described in Section 3.3.4 above. The Government should move to install an Enterprise Directory so as to facilitate e-mail addressing and to provide "white pages" of all civil servants. This task has been identified as a "fast-track" project under the on-going e-government initiative.

6.3 Administration Recommendations

Recommendation #4.2.1 : *Establish a Network Governing Body*

All agencies involved in the pilot network project should form a network governing body, or committee, to oversee the management and administration of the MAN. The committee should address the following subjects: network reliability and performance, security, information sharing and access control. The committee should have full management and legislative support.

Recommendation #4.2.2 : *Develop an Enterprise Directory*

A critical component of the MAN will be an Enterprise Directory (as described in Section 3.3.4 of this report.) The Directory will maintain access rights of all network users and allow for single login access to all network resources.

Recommendation #4.3.1 : *Improve physical security*

Line agencies should restrict access to information and electronic data, and should improve the monitoring of people within IT organizations. In particular the following options should be considered:

- Installing CCTV in each agency to record movements in hallways and access to offices;
- Install automatic locks on all server rooms and on the offices of important IT personnel.

Recommendation #4.3.2 : *Enforce ACL access to workstations and LANs*

A user should not have access to information on a workstation or a server unless they have been authenticated by an ACL.

- provide access in each organisation to a Windows 2000 server to provide ACL control and monitoring;
- Upgrade as many desktop computers as possible to Windows 2000 professional;
- Standalone desktop computers should be connected to a LAN if possible, and treated as “low security” if they cannot be.
- Install group policies and require authentication on all pre-Win 2000 computers.

Recommendation #4.3.3 : *Establish a PKI infrastructure*

A study of establishing a public-key infrastructure (PKI) is currently being made by the e-government taskforce of the Ministry of Information and Communication Technology (MOICT). The project team encourages the Government to begin investigating PKI solutions

and its requirements. In particular the Government should determine what are the technology's business drivers, what level of security is appropriate, where is the existing system vulnerable, and what are the legal and regulatory compliance constraints?

Recommendation #4.3.4 : *Employ local security firms*

There are a number of local, private firms that specialize in information security and perform security audits. Security is a specialized field of study, and most organizations have a difficult time following its latest trends and technologies. As such, the Government should make use of the specialized services of private security companies and should occasionally hire these firms to conduct security audits.

Recommendation #4.3.5 : *Improve virus monitoring*

Viruses are a constant threat to the Government. Besides being a nuisance and hampering productivity, they also erode confidence in the use of IT and discourage individuals from making full use of the technology.

Traditionally, viruses protection has focused on individual computers by loading software such as Norton or McAfee on each workstation. Unfortunately, this technique has proven to be ineffective as virus databases are constantly out of date, leaving the computers vulnerable to the quick-to-appear and short-lived "fad" viruses that occasionally sweep through a country.

The Government should adopt a new approach to fighting viruses and focus at the server level, including e-mail servers. Since the NIC serves as the ISP for most Government agencies, efforts to fight viruses should be consolidated there. Incoming internet traffic can be scanned at source. Consolidating e-mail servers (see Recommendation **3.4.1**) will further protect against viruses by providing a single monitoring point.

Recommendation #4.3.6 : *Employ a common firewall solution*

The Government is currently relying on each LAN administrator to implement security measures ad hoc. Unfortunately, implementing and maintaining a firewall to protect against external attacks is a complex and time-consuming task, that currently very few LAN administrators are handling successfully. The Government should pursue a standard firewall solution that can be centrally managed, yet distributed to all line ministries and agencies. The is especially important if connectivity between agencies is established, as it will also protect against internal attacks.

Recommendation #4.3.4 : *Outsource non-core activities*

LAN administrators should try to outsource non-core activities, including e-mail and web management to third parties, as described in **Recommendation 3.4.1**. Other activities available for outsourcing include hardware maintenance and preventive maintenance, network

configuration and monitoring, and security.

Recommendation #4.3.5 : *Centralize storage of user files*

Workstations and servers should be reconfigured to store user files on a central file server rather than on the hard-drives of individual computers. This provides additional security over physical theft of data, and allows for easier backups.

Recommendation #4.3.6 : *Implement network administration software*

By implementing network administration software, such as Microsoft's System Management Server 2.0, LAN administrators can better monitor and document their network. Network monitoring software and protocols are very important when connectivity with other agencies is established.

Recommendation #4.3.7 : *Improve directory management*

LAN administrators should be concerned with both *where* and *how* user files are stored. Before interconnectivity is launched, LAN administrators need to know what files are stored on the LAN and where they are. Access control is simplified if the Administrator enforces policies regarding where a user can store files (and if those files are stored on a central file server.)

Recommendation #4.3.8 : *Documentation*

Network documentation should be improved. LAN Administrators should strive to maintain all of the documentation listed in Section 4.3.3.2. Much of the documentation can be automated if the proper management software is installed.

Recommendation #4.3.9 : *LAN administration workshops and newsletters*

The project team highly recommends that the Government, with the assistance of a central IT-related agency like the MOITC or NIC, hold occasional workshops and conferences to discuss administration issues and way to improve the use of computers in each organisation.

An alternative is to create newsletters informing LAN administrators of the latest software trends and ideas.

Recommendation #4.3.10 : *Develop standard administrative procedures*

Before e-government and interconnectivity is implemented, the Government should focus on defining standard LAN administrative procedures, including the "best practices" mentioned in this report. Interoperability standards and guidelines should be adopted and met.

The development and maintenance of the procedures should be the responsibility for one of the central IT agencies like the MOITC or NIC.

Recommendation #4.4.1 : *Conduct Management/IT Department Workshops*

The tremendous success of the project's two-day workshop in Ma'in demonstrated the need for additional opportunities for IT directors and upper management to share experiences and to discuss common problems. Upper management need a better understanding of the unique problems associated with IT and how to improve the return on their IT investment.

The project team highly recommends that the Government initiate a series of moderated workshop/meetings to facilitate this invaluable exchange of information and support.

Additional workshops should be held to showcase individual administrative systems that have been developed in line agencies. These systems and experiences can be shared with other agencies.

Recommendation #4.4.2 : *Review IT Management and Operations*

Related to the workshops recommended above, the Government should fully review the role of IT in Government and seek to modify the operations of IT departments. Because of IT's cross-cutting function in all agencies, the effectiveness of an organisation is usually directly related to the effectiveness of its IT department. The Government should understand this correlation, and strive to modernize its management in all departments. In particular, the project team recommends that Government:

- revise its existing model of IT management and focus on outsourcing all non-essential IT processes so as to maintain a minimal staff necessary for in-house IT needs;
- reduce line agency reliance on their IT departments and recognize that the appropriate use of IT, including training, is the responsibility of all department heads;
- view IT departments as "consultants", not "implementers". IT department's primary responsibility should be to advise, contract and manage the private sector to perform necessary IT work within the agencies. The Government should try to minimize the amount of IT work that it implements in-house.

Recommendation #4.4.3 : *Eliminate non-core information systems*

As noted earlier, the project team has identified that IT departments are spending the majority of their time and resources on developing and maintaining information systems that are unrelated to the core business of the line agency. In addition, most of these systems are duplicated in other agencies, including payroll, personnel, expenditure, budget and mail dispatch (divan) systems.

IT departments should immediately cease all development of non-core systems and focus on utilizing systems created and supported by other line agencies.

As noted in **Recommendation #3.4.1**, the line agencies should also seek to consolidate their web and e-mail servers to a central site. Eliminating these servers will reduce IT administration costs and improve reliability and security.

Recommendation #4.4.4 : *Encourage Strategic Planning for all Ministries*

While assisting IT departments to complete their IT plans, the project team noted the lack of formal strategic planning in most ministries and agencies.

IT management and development should be inherently tied to its parent organization's strategic business plans. If the parent organisation does not know which direction it wants to head, then there's no surprise that the IT department cannot help it get there.

6.4 Connectivity Recommendations

Recommendation #5.6.1 : *Select Batelco Frame Relay services*

The project team, after evaluating the connectivity options' advantages, disadvantages and costs recommend that the Government select Option 3 using Batelco's Frame Relay services with a mesh configuration. Although the cost over three years is calculated at approximately 35% more than the JTC mesh option, the project team recognizes that reductions in manpower and risks, as well as the increased reliability of a managed network solution, justify the increased cost.

The project team also recognizes that Batelco has substantial experience in managing and maintaining public networks in Jordan, and has proven its reliability to the Banking sector. Until both the Government and JTC have similar experience, Batelco should remain the network provider of choice.

Recommendation #5.6.2 : Conduct a networking workshop with all stakeholders.

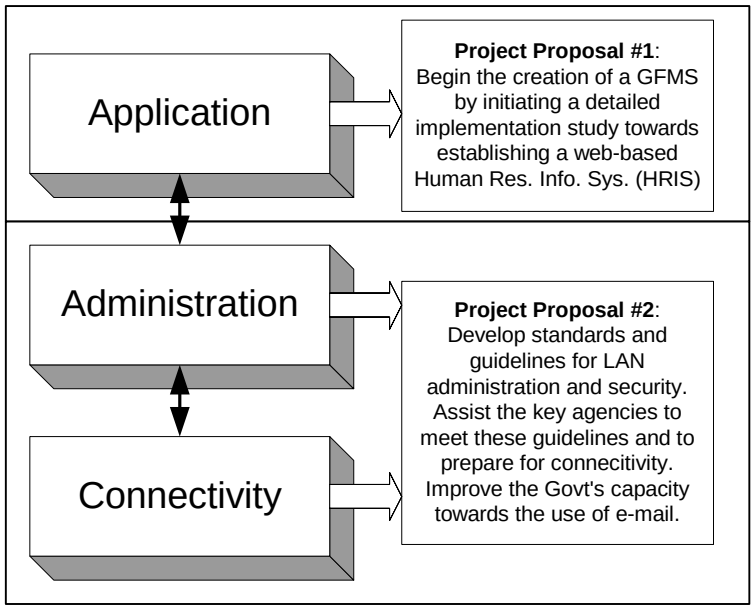
As noted in Section 5.1.1 , the choice of the best network option is subjective and the project team recognizes that the two other solutions provide comparative solutions. The project team *highly* encourages the Government to conduct a workshop with representatives from Batelco, JTC, NIC and the LAN administrators of the pilot agencies to fully explore and debate the relative merits of each option, using this study as a basis for the discussions. The Government should also include financing options, which are unknown at this time, into the decision process.

7

Section 7 : Proposals

7.1 Introduction

As stated in the project ToR, the objective of the pilot network design is to recommend proposals for subsequent projects to improve the efficiency and economy of the financial functions of the Government.



Based on the current situation in Jordan, the project team proposes that the Government pursue two follow-on project actions:

- An *application project proposal* to begin acquiring the information systems that will facilitate and promote data exchange between the government agencies. These information systems will form an integrated GFMS that will assist the Government to radically improve its financial administration, streamline its bureaucracy, and strengthen its ability to provide key economic and fiscal information.

  The project team recommends a long-term, multi-phased approach to this task and suggests that the first phase begin by undertaking a detailed, implementation study towards establishing a centralized human resource information system among the key agencies and the Civil Service Bureau; and

- An *administration/connectivity project proposal* to strengthen the IT departments of the key agencies and prepare them for eventual connectivity. The agencies will be strengthened by establishing guidelines and procedures

for LAN administration, e-mail, IT Management and security. The necessary hardware/software for connectivity will be procured and installed.

Provisional descriptions of the proposed projects are provided below. Based on consensus and approval of the proposed ideas, more detailed project proposals, including detailed tasks and input requirements, will be included in the final network design.

7.2 Application Project Proposal

7.2.1 Overview

The *application project proposal* is intended to add value to the pilot network while also providing the means to improve the financial administration of the Government. To build an integrated GFMS, however, is an enormous task that will ultimately transform the Government's entire fiscal management and business processes. The Bank's experience in other countries have proven that such GFMS systems are tremendously successful in their ability to modernize government and improve the transparency and efficiency of services.

One of the leading e-government "best practices" is to start small and scale accordingly. As such, the project team suggests that the first step toward creating a GFMS is to begin by creating a small-scale, yet extremely powerful "proof-of-concept" of establishing centralized information systems using web technologies.

While any module or sub-system can be used for the application pilot project, the project team recommends that Government begin its GFMS *by focusing on civil service management and the creation of human resource information system (HRIS)*. There are many immediate benefits from this tactic and the team's recommendation is based on the following considerations:

- *HRISs are generally the simplest sub-system to implement (however this does not imply that the task is easy!)*. HRISs require fewer organizational and legislative changes to existing processes and have limited impact on other business functions. However, a HRIS requires links to other financial sub-systems including budget and expenditure, and can substantially reduce bureaucratic administrative procedures;

- *A HRIS will provide all civil servants a purpose for using computers and the internet*. This is a powerful change agent towards improving the use of computers and electronic services in the Government.

  HRISs that contain automated workflow processing, such as electronic leave/vacation requests, will encourage civil servants to modify existing bureaucracies and to understand the concepts behind e-government. An HRIS will provide all employees an opportunity to make use of IT for a purpose other than word processing and communication.

  Yet, existing processes can remain for less technologically-savvy employees and agencies. The situation is analogous to the use of Automated Teller Machines (ATMs) in banking--- users realize the convenience and benefits of ATMs as and when they become comfortable with the technology.

- *A HRIS contains information that is important to the widest range of users---from top management to individual employees.* Unlike other financial systems, the data found in an HRIS is of use to everyone. If desired, basic directory information (name, department, phone number, e-mail address) can be made available to the public via the internet. Individual employees can access subsets of their own information to verify accuracy and to help support current data.

  A well-maintained HRIS is essential for providing:

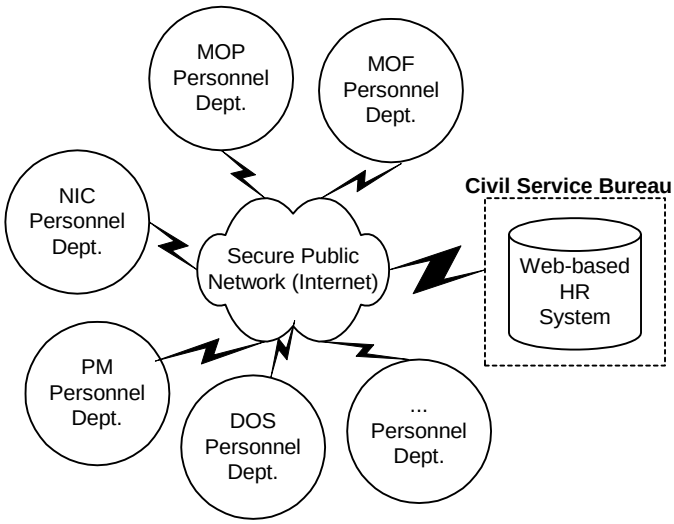
  - information about the size and scope of the civil service. This information is critical to any future civil service reform efforts;

  - directory assistance information, especially current e-mail and contact data. Improvements in the Government's use of e-mail and general electronic communication is completely dependent on easy access to directory information. An integrated, comprehensive HRIS is a critical component to this development;

- *A HRIS can be used by every line ministry and organisation regardless of staff size and complexity.* This is an important consideration for eventual rollout and implementation and demonstrates the tremendous power of decentralized information systems. Any line agency or office with a computer and an internet connection will be "on-line" and capable of managing their own personnel needs.

- *A HRIS will provide the first opportunity to re-engineer existing bureaucratic procedures and workflows*. The lessons learned from this exercise will be invaluable in future attempts to modify and automate other financial administrative tasks.

7.2.2 Web-based Human Resource Information System (wb-HRIS) Project



The project will create a detailed study that investigates the technological, economical, organizational, and legislative feasibilities of developing a web-based Human Resource Information System (wb-HRIS). The information system can

be centralized in the Civil Service Bureau and utilized by the personnel units of line agencies. The information system will be a leading "G2G[49]" component in the overall e-government framework.

A wb-HRIS will be the first step towards the eventual establishment of an integrated GFMS with decentralized processing of data. The system should provide the following modules:

- Position management
- Recruitment
- Personnel
- Payroll
- Health Management
- Training Management
- Career Development; and
- Performance Evaluation

The system should be accessible via a normal internet web browser such as Internet Explorer or Netscape. This will promote the concept of decentralized administration with centralized information systems -- allowing the database to remain located in the core agency responsible for the function.

7.2.3 Activities

The project will complete the following activities/tasks:

i evaluate existing human resources procedures, and regulatory requirements and define system specifications;

ii conduct a "buy vs. build" analysis, and if necessary, review existing commercial wb-HRIS and identify the most appropriate system for Jordan;

iii determine net costs of the system based on anticipated costs and expected savings. Full cost analysis should be performed for both up-front expenditures and long-term operational costs/savings;

iv identify training and financial/personnel strengthening requirements;

v create a complete roll-out plan for implementing the wb-HRIS, including prerequisite steps.

[49] Government to Government

7.3 Administration/Connectivity Project Proposal

7.3.1 Overview

The *administration/connectivity project proposal* is intended to assist the establishment of the pilot network. The project will focus on strengthening each agency's LAN administration, security and IT management, and preparing each agency for intra-governmental connectivity.

The project will also improve the Government's use and capacity for e-mail and data exchange. While e-mail is currently available in most government offices, it is not being effectively used. Various studies have demonstrated that the wide-spread use of e-mail is a prerequisite to any future e-government activities as well as the primary purpose of networks.

The goal of the pilot network is to provide a foundation for the exchange of information and data between the key agencies. As noted above, a major application of this network can be a Government Financial Management System (GFMS).

7.3.2 Pilot Network Project

The implementation of the pilot network can be viewed in two parts:

i Installing the necessary security and management framework to ensure a secure and operational network, and

ii Establishing connectivity.

The project will assist the agencies to establish and meet security guidelines, and set up the necessary management framework to coordinate and administer the LAN. By implementing recommended "best practices", the agencies will be capable of providing reliable computing and network services.

While the focus of the project will remain with the key agencies involved in the pilot network study, the standards, guidelines, and technological solutions that are created can be adopted by the rest of the Government agencies in the future.

7.3.2.1 Connectivity

The project will prepare the key agencies for connectivity. Actual connectivity between the agencies will occur when the Government determines the benefits of connectivity exceed the expected operating costs. As noted earlier in this report, operating costs are decreasing rapidly and are expected to become less of an issue in the future.

The project will focus on connectivity via a secure public network which involves cryptographic techniques such as VPN ("Virtual Private Network") technologies to provide secure communication.

7.3.2.2 Institutional issues

In addition to strengthening the IT units of the key agencies and preparing each agency for connectivity, the project will need to address other institutional issues such as:

- information sharing between agencies and establishment of policies towards access and distribution of data-- who will have access to what and how?
- network operation and management-- which departments will be responsible for the oversight and maintenance of the network?
- security auditing-- who will monitor that each agency continues to meet the established security and interoperability guidelines?

7.3.3 Activities

The project will complete the following activities/tasks:

i Form a Network Steering Committee among the pilot agencies to develop guidelines for network security, interoperability and LAN administration. The resulting standards and guidelines should be formally adopted by all agencies;

ii Help each individual agency to meet the established guidelines;

iii If necessary, establish an appropriate Network Operation Center, mostly likely with the assistance of the National Information Centre, to oversee the operations and maintenance of the network;

iv Analyze and improve e-mail usage among the key agencies. Review and implement the optimal configuration for e-mail exchange among the agencies, and provide formal training to all necessary employees. The legalities of e-mail in the Government should also be addressed;

v Procure and implement the necessary hardware and software to establish VPN connectivity;

vi Assist the appropriate Government agency to address core IT institutional issues such as information sharing/distribution, outsourcing, and contract servicing. Help to develop IT management and the role of IT departments throughout the Government.

vii If appropriate, assist the key agencies to establish connectivity and to initiate the pilot network.

A

Appendix A : Data Exchange Questionnaire

Data Exchange Analysis

PLEASE PHOTOCOPY ADDITIONAL SHEETS AS NECE SSARY!!

Agency: _____ Name: _____

Department: _____ Date: _____

Data / Information	Currently Received?	From?	Frequency		Format	
			Current	Desired	Current	Desired
Description of the data: Reason for needing the data:	☐ Yes ☐ No ☐ Sometimes	☐ PM ☐ MoP ☐ MoF ☐ CBJ ☐ DoS ☐ NIC	☐ Real-time ☐ Daily ☐ Weekly ☐ Monthly ☐ Bi-Annually ☐ Annually ☐ Occasionally ☐ Other	☐ Real-time ☐ Daily ☐ Weekly ☐ Monthly ☐ Bi-Annually ☐ Annually ☐ Occasionally ☐ Other	☐ Electronic ☐ Custom Report ☐ Published Report ☐ Directly ☐ Other	☐ Electronic ☐ Custom Report ☐ Published Report ☐ Directly ☐ Other
Description of the data: Reason for needing the data:	☐ Yes ☐ No ☐ Sometimes	☐ PM ☐ MoP ☐ MoF ☐ CBJ ☐ DoS ☐ NIC	☐ Real-time ☐ Daily ☐ Weekly ☐ Monthly ☐ Bi-Annually ☐ Annually ☐ Occasionally ☐ Other	☐ Real-time ☐ Daily ☐ Weekly ☐ Monthly ☐ Bi-Annually ☐ Annually ☐ Occasionally ☐ Other	☐ Electronic ☐ Custom Report ☐ Published Report ☐ Directly ☐ Other	☐ Electronic ☐ Custom Report ☐ Published Report ☐ Directly ☐ Other
Description of the data: Reason for needing the data:	☐ Yes ☐ No ☐ Sometimes	☐ PM ☐ MoP ☐ MoF ☐ CBJ ☐ DoS ☐ NIC	☐ Real-time ☐ Daily ☐ Weekly ☐ Monthly ☐ Bi-Annually ☐ Annually ☐ Occasionally ☐ Other	☐ Real-time ☐ Daily ☐ Weekly ☐ Monthly ☐ Bi-Annually ☐ Annually ☐ Occasionally ☐ Other	☐ Electronic ☐ Custom Report ☐ Published Report ☐ Directly ☐ Other	☐ Electronic ☐ Custom Report ☐ Published Report ☐ Directly ☐ Other
Description of the data: Reason for needing the data:	☐ Yes ☐ No ☐ Sometimes	☐ PM ☐ MoP ☐ MoF ☐ CBJ ☐ DoS ☐ NIC	☐ Real-time ☐ Daily ☐ Weekly ☐ Monthly ☐ Bi-Annually ☐ Annually ☐ Occasionally ☐ Other	☐ Real-time ☐ Daily ☐ Weekly ☐ Monthly ☐ Bi-Annually ☐ Annually ☐ Occasionally ☐ Other	☐ Electronic ☐ Custom Report ☐ Published Report ☐ Directly ☐ Other	☐ Electronic ☐ Custom Report ☐ Published Report ☐ Directly ☐ Other

Please return to your IT Dept. by 30 April, 2001

Page ____ of ____

B

Appendix B : SAP Public Sector Solutions

C

Appendix C : JTC Proposal

D

Appendix D : BJ Proposal