Auburn University
MCSE Design Project
CSE 698

Internal Revenue Service
Internal Communications Systems Re-Engineering

Spring 1996

Submitted by:

Rudy Navarro
Graduate Student
College of Engineering
Department of Computer Science and Engineering (CSE)

Submitted to CSE Graduate Committee:
Dr. L. Murphy (Chairman)
Dr. H. Carr
Dr. L. Moore

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The IRS is re-engineering their internal networks and moving from an SNA to an OSI processing environment. This is occurring along with a downsizing effort, as directed by Congress, to reduce the main processing areas from ten to three locations, along with a reduction in administrative offices.

The objective of the paper that follows is to propose a new network infrastructure for the main processing areas that will incorporate a more modern type of data transport technology (e.g., bandwidth dynamic, growth orientated, etc). In order to do this properly, the first part of the project will be a requirements analysis (Chapter 2), followed by a systems engineering statement (Chapter 3). Upon completion and in conjunction with these efforts, a design for a new network backbone (e.g., ATM, FRAME RELAY transport system) for the IRS will be proposed, with a description of methods and justifications.

ACRONYMS

ADP	Automated Data Processing
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
BBN	Backbone Network
BISDN	Broadband Integrated Services Digital Network
CBR	Constant Bit Rate
CBS	Core Business System
CDV	Cell Delay Variations
COBOL	Common Business Oriented Language
COTS	Commercial-Off-The-Shelf
CS	Computing Segment
CSL	Convergence Sublayer
CSCS	Customer Service Command Segment
CSR	Customer Service Representative
DASD	Direct Access Storage Device
DNIC	Data Network Interface Connection
EDI	Electronic Data Interchange
FEC	Forward Error Correction
FECN/BECN	Forward/Backward Explicit Congestion Notification
FEP	Front End Processor
FMS	Fast Resource Management
FSS	Field Service Segment
GOSIP	Government Open Systems Interconnection Plan
IAS	Information Analysis Segment
IRS	Internal Revenue Service
ISA	Integrated Systems Architecture
ISDN	Integrated Services Digital Network
JLC	Job Language Code
LAB	Local Access Board
LAN	Local Area Network
LIC	Line Interface Connector
LU	Logical Unit
Mbps	Megabits Per Second
MIN	Multistage Interconnecting Networks
MIPS	Million Instruction Per Second
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
NCP	Network Control Programming
OCR	Optical Character Recognition
OOD	Object Oriented Design
OSI	Open System Intercorrection
PAD	Packet Assembler/Disassembler
PCM	Pulse Code Modulation
PDU	Protocol Data Unit
PPP	Point-to-point Protocol

PU	Physical Unit
QLLC	Qualified Logical Link Control
QoS	Quality of Service
RISC	Reduced Instruction Set Computer
SAR	Segmentation and Reassembly
SLIP	Serial Line Interface Protocol
SDLC	Synchronous Data Link Control
SDU	Service Data Unit
SNA	Systems Network Architecture
SPF	Shortest Path First
SPS	Submission Processing Segment
SVC	Switched Virtual Channel
TA	Transitional Architecture
TCP/IP	Transport Control Protocol/Internet Protocol
TQM	Total Quality Management
TQO	Total Quality Organization
TSM	Tax Systems Modernization
TSPS	Tax Support Processing System
TPSA	Tax Processing Systems Architecture
VBR	Variable Bit Rate
VCI	Virtual Channel Identifiers
VCR	Virtual Circuit Routing
VPI	Virtual Path Identifiers
VTAM	Virtual Telecommunications Accessing Method
WAN	Wide Area Network

CHAPTER 1

1. INTRODUCTION

1.1 Overall Internal Revenue Service (IRS) Project History

The Internal Revenue Service (IRS) which reports to the Department of the Treasury, is the government agency responsible for collecting taxes from American citizens. The IRS organization was established in the early 1920s and was granted a charter to solicit taxes and investigate both personal and corporate noncompliance or criminal activity involving tax law compliance.

In order to maintain the massive amounts of information necessary to ensure the operation of their agency, the IRS must manage record keeping to a much higher degree than do most corporations. Congressional IRS oversight committees have installed operational philosophies and laws to ensure that the IRS would maintain these records at a level of integrity sufficient to show the American people that the IRS is equitable, fair, and above all, accountable for their actions.

In order to comply with these congressional mandates, the IRS has been historically at the forefront of most of the Automated Data Processing (ADP) discoveries of the last fifty years. As other agencies of the Federal government started to discover the benefits of ADP technologies and ponder the deployment of these technologies, the IRS already had systems in place and operational. According to Dale Burtyk, IRS manager of network security," with the exception of the NASA space program, no other agency has been as responsible for the growth of ADP technology in this country as the IRS."

In the past, the IRS used mainframe computers with massive distributed databases to account for the storage and/or retrieval of over 275 million individual tax returns and over 50 million business returns. The communications systems used in support of this operation were massive and difficult to manage. Over time, new computer languages such as Job Language Code (JLC) and Common Business Oriented Language (COBOL) were developed specifically for the IRS operation and then introduced into the general technology community.

At present, the IRS employs over 125,000 people in support of this complex system. This includes the operation and maintenance of 12 computing centers; 36 tax submission centers; and over 250 customer service, administration, and record archiving service centers throughout the country. These operations include all facets of ADP support, such as data, text, and graphics, in addition to special network operations such as TeleVideo, audio conferencing, and network management.

During the past ten years, the IRS has made only minor and incremental upgrades to their systems while many other agencies of the federal government have undergone major changes in computing capabilities. The differences in base computing technology between agencies has caused intercommunication problems. The inability to exchange and share information between specific agencies has created major concerns and the seamless ability to exchange information between agencies is considered vital for the proper operation of government.

1.2 Overall IRS Project Philcsophies

To address this situation, as well as operating budget reductions, the IRS oversight committee established the TAXMOD 2000 project. This project is a government sponsored effort to change the IRS operational philosophies while modernizing the ADP systems, thus increasing the agency's efficiency well into the 21st century. TAXMOD 2000 objectives were developed utilizing the following paraphrased basic project developmental philosophies and requirements[1]:

a) The IRS will modernize all ADP computing systems utilizing non-proprietary based criteria that will allow multiple hardware, software, and communications vendor integration.

b) While utilizing the 1987 government mandated "OPEN SYSTEMS/GOSIP" (Government Open Systems Interconnection Plan) philosophy, the IRS will develop and follow a software and hardware technology path which will be expandable.

c) The IRS modernization effort will assist in the evolution of consolidation and reduction of the number of operations and customer service centers. The goal: to enhance and streamline communications systems, making the overall operation more efficient and less expensive.

d) Institute and comply with all mandates and regulations involving the Freedom of Information Act of 1986 and Privacy Act of 1988.

e) Develop and institute a communications security philosophy that will incorporate a global "end-to-end"/"user-to-user" security strategy for private line and dial up capabilities for both center and field personnel.

f) Ensure both the ability to retrieve active and archived information and, upon demand, provide this information to operational personnel and/or the customer. This function will operate under an "open" and "need to know" security mandate.

g) Maintain data integrity of all current informational databases. This will be accomplished by ensuring error free data transport and proper development/implementation of upgraded software and hardware systems integration. This effort will guarantee access to all current and legacy database systems without loss or degradation of daily operational Quality of Service (QoS).

1.3 Overall IRS Systems Design Area Identification:

Utilizing the defined project philosophies, the IRS identified a number of investigative subject areas for this modernization effort. These areas include, but are not limited to, the following.

---

[1]IRS TAXMOD Project Management Statement, 1990.

1) Hardware computing and control systems:
    a) mainframes
    b) miniframes
    c) desktop PCS
    d) workstations, high/low end
    e) servers, high/low end
    f) portable systems:
        1) notebooks
        2) personal digital assistants
    g) data storage, retrieval and archive systems:
        1) CD optical disk and jukeboxes
        2) digital tape
        3) multiple hard disk file systems

2) Software operating systems:
    a) UNIX
    b) MS-DOS
    c) Windows:
        1) Windows 3.X
        2) Windows NT
        3) Windows Client/Server
        4) Windows for Workgroups
        5) Windows Workstations

3) Software applications systems:
    1) databases
    2) customer Accounting
    3) customer control
    4) file access control
    5) user Access control

4) ADP user support:
    1) E-mail
    2) payroll
    3) access control
    4) personnel
    5) inventory control
    6) internal accounting
    7) documentation support
    8) operational administrative support
    9) office automation:
        a) word processing
        b) spreadsheets
        c) appointment control
        d) desktop publishing

5) Communications systems and control:
    1) re-engineering network transport systems:
        a) LAN
        b) WAN
    2) on-net/off-net access control:
        a) Public access/dial-up
    3) Multiple government agency access
    4) Internet
    5) Configuration control
    6) Network management:
        a) LAN
        b) WAN
        c) inband/out-of-band
        d) on-net/off-net

6) Security:
    1) informational
    2) communications:
        a) LAN
        b) WAN
        c) on-net/off-net
        d) inband/out-of-band
    3) personnel access:
        a) internal
        b) external
    4) accounting

7) Administrative support systems

1.4 Communications Development Focus Area

The focus of this CSE 698 project will be the communication portions of the TAXMOD 2000 project, which provides a multiplicity of investigative areas.

The defined overall effort of the IRS is to review, redevelop, re-engineer, and redeploy all communications systems. This emphasis positions communications systems as the primary support foundation of the overall ADP modernization effort.

Therefore, the communications effort should be subject to, but not limited by, the following engineering specifications:

1) Development of a communications infrastructure strategy, utilizing IRS documentation and requirements, ensuring the successful reduction of the current computer processing centers from 10 to 3 locations, and customer/tax submissions service centers from 36 to 9 locations, without any loss of service.

2) Review wide area network (WAN) communications systems utilizing non-proprietary Open Systems philosophy. This will require eliminating and replacing current network control systems with specifically identified equipment that utilizes a reliable, faster, and more open network scheme.

3) Development and design of a high speed dynamic backbone WAN network capability that will utilize a modern packet transport scheme to transport data in a faster, more efficient manner. In addition, this backbone system should integrate with all current and future LAN systems and support remote, off line, and dial-in operations.

4) Utilization of modern design/simulation techniques to design the overall WAN and network support systems. These systems should be designed with the ability to grow as the processing requirements, network usage requirements, and bandwidth requirements grow.

5) As system response time is a critical criterion, the communications effort is vital to this requirement. The network system should be designed with the ability to support the development of minimal system response time.

1.5 Project Scope

For the CSE 698 project, scope will be limited to in depth investigation of specific questions. All results will be based on IRS project documentation and previously detailed information. The following investigative areas were developed with the understanding that the IRS tax modernization project is a critical undertaking employing hundreds of people. The following questions will be used to define the scope of this paper as well as the investigative effort.

The questions are:

1) Why is the IRS transitioning from the present network technology? This section will include an analysis of performance specifications, resizing requirements, and other user issues.

2) What are the present and projected future IRS applications? (This data will be used to help answer question #1).

3) What are the benefits of the proposed network transition? This will include an analysis of transitioning the current IRS network technology to a network technology utilizing a proposed WAN network architecture.

CHAPTER 2

2. BUSINESS AND TECHNOLOGY TRANSITION

This chapter will identify some of the key IRS operational and technological core elements driving the transition decision. In addition, an analysis of the identified key elements will be undertaken. This analysis will identify the correlation between the newly established business strategy and the application of modern technology.

2.1 Core Business Systems

Traditional IRS functional systems (e.g., Taxpayer Services, Collections, Examination, Returns Processing, etc.) have evolved over the past 40 years into autonomous parallel organizations. This autonomous development has produced highly specialized entities that provide excellent support in their specific field. However, lack of true integration has limited the ability to provide a cohesively administered tax support structure.

This type of segmentation can result in inefficient products, wasted efforts, and/or duplicated services. In 1986, Congress mandated that the IRS reorganize itself from within and modernize both its operational management philosophies and its technological base. This effort began with the initial goal of becoming a Total Quality Organization (TQO) utilizing a business effort focusing on Total Quality Management (TQM).

This new systems management approach encouraged analysis and improvement from a cross functional perspective, and eliminated traditional barriers to functional integration. The basic premise of this new approach was to develop a better understanding of what products and services customers received from the IRS and the cost, in customer terms, of those products and services (e.g., time, money, burden, etc). Once these basic criteria were identified, they provided the template for a systems design architecture with the essential goal of increasing the products and services value to the customer.

The results of an intensive IRS self evaluation indicated the need for a well-defined mission to help guide the new management philosophy. This mission incorporates six newly developed Core Business Systems (CBS)[2] as management goals. These CBSs reflect the new philosophies that will drive and manage the IRS for the next ten years. They are:

1) Value Tracking; to determine, communicate, and track the extent to which taxpayers value the products and services provided by the IRS.

2) Informing and Educating; to enable the taxpayer to comply with the tax laws through effective and efficient information and educational activities.

3) Managing Accounts and Assisting; to receive, maintain, and provide account and revenue information and assist taxpayers in account related matters.

---

[2]IRS Business Development Investigation Document, 1992.

4) Ensuring Compliance; to preserve the integrity of the voluntary tax system by continually measuring compliance behavior, identifying non-compliance, determining root causes, and taking action to improve compliance.

5) Resourcing; to plan, acquire, and manage resources which will enable the IRS to provide the best customer value.

6) Developing and Managing Systems; to enable and assist the IRS by leveraging information technology in order to provide business processes that produce the highest net customer value.

Full incorporation of the CBSs requires fundamental management changes throughout the IRS. These changes, supported by the Tax Systems Modernization (TSM) operational efforts and the introduction of new information systems technology, will enable the IRS to achieve the following identified business objectives:

Reduce taxpayer burden: Currently, the traditional IRS business approach requires the taxpayer to engage in lengthy and protracted dealings possibly involving several agents. This correspondence is initially paper-based and culminating in face-to-face meetings for final resolution. New procedures facilitated by the TSM will enable taxpayer inquiries and correspondence to be electronically submitted from home and/or office directly to an IRS investigations or customer service worker. This will eliminate and/or minimize the time and number of inquires and/or correspondences necessary to resolve specific taxpayer issues.

Increase voluntary compliance: Voluntary compliance strategies are being devised that combine traditional enforcement actions with education and outreach. The IRS plans to publish "on-line" current tax laws and codes. This will allow information access to a large majority of taxpayers who have access to the Internet or to a computer with a dial-up modem.

Improve quality driven productivity and customer satisfaction: The IRS spends a great percentage of taxpayer dollars each year processing paper, reworking errors, maintaining outdated computing and communications equipment, and pursuing enforcement efforts through correspondence with taxpayers.

The IRS will realize substantial business cost reductions and achieve major quality-driven gains by modernizing computing and communications capabilities, empowering employees, and changing its core business strategy.

2.2 Computing and Communications Systems Modernization

The Computing and Communications portion of the overall TSM effort is a multi-billion dollar redesign and improvement project with a primary goal of transforming obsolete IRS computing and communications systems (most of which were designed in the 1960s and 1970s) into modern, high technology, high-speed information and communications systems.

By taking advantage of technological advances the TSM will enable the IRS to transform the current, paper-based batch processing system into a totally electronic environment. This will allow information to be accepted, used (cataloged and/or archived), retrieved, and delivered back to the taxpayer electronically.

By utilizing the Government Open Systems Interconnection Plan (GOSIP), the new computing and communications system will have greater flexibility and growth potential.

2.2.1 SNA Computing Technology Overview

During the 1960s and early 1970s, the IRS led the government utilization of computing and communications systems. All of the systems were based on the Systems Network Architecture (SNA) style of computing technology. The SNA systems were configured as depicted in Figure 1.

Mainframe Computers - Mainframes are centralized processing engines that utilize a central control time sharing system that ensures all jobs requested are processed in a sequential manner. These machines are floor space dominant, environmentally dependant, and require constant programmer attention.

Mainframe technology processing power ranges from small systems of less than 5 million instructions per second (MIPS) to systems of just over 100 MIPS. Most of these systems are proprietary in nature; i.e., all of the application software and hardware peripherals needed for proper usage must come form the same vendor. This escalates normal operating cost and periodic upgrading becomes a costly burden.

Of the many operating programs necessary, the Virtual Telecommunications Accessing Method (VTAM) provides the main program control system for all aspects of the communications capability. VTAM is cumbersome, programming intensive, and requires many computer cycles to complete a small access transaction.

Front End Processors - All WAN and LAN communications requiring mainframe accessing are controlled by Front End Processors (FEP). These controllers are massive software and hardware systems that are essentially stand alone computers. They utilize a software operating system called Network Control Programming (NCP) which communicates directly with and is controlled by the VTAM mainframe program. All of the various network access links are physically connected into the FEP, mainframe machine by Local Access Boards (LABs). Each LAB controls a number of Line Interface Connectors (LICs).

Each LAB can accommodate a maximum bandwidth of 1.544 Megabits per second (Mbps). In addition, the FEP LABs physically control alternative WAN carriers and network interface capabilities such as packet switching, Token Ring LANs, and small bandwidth multiplexers. The NCP program in turn controls:

1) Bandwidth allocation for each LIC;

2) Number of LICs associated with each LAB;

3) LIC/LAB input sequence control for mainframe access;

4) Various network protocols associated with bandwidth carriers and networks such as X.25 packet switching, 802.5 LANs, RS-232c serial links and T-1 wideband carriers; and

5) Various protocol requirements for all LAN access.

FEPs suffer from the same space constraints environmental controls, and programming intensive maintenance as do mainframe systems.

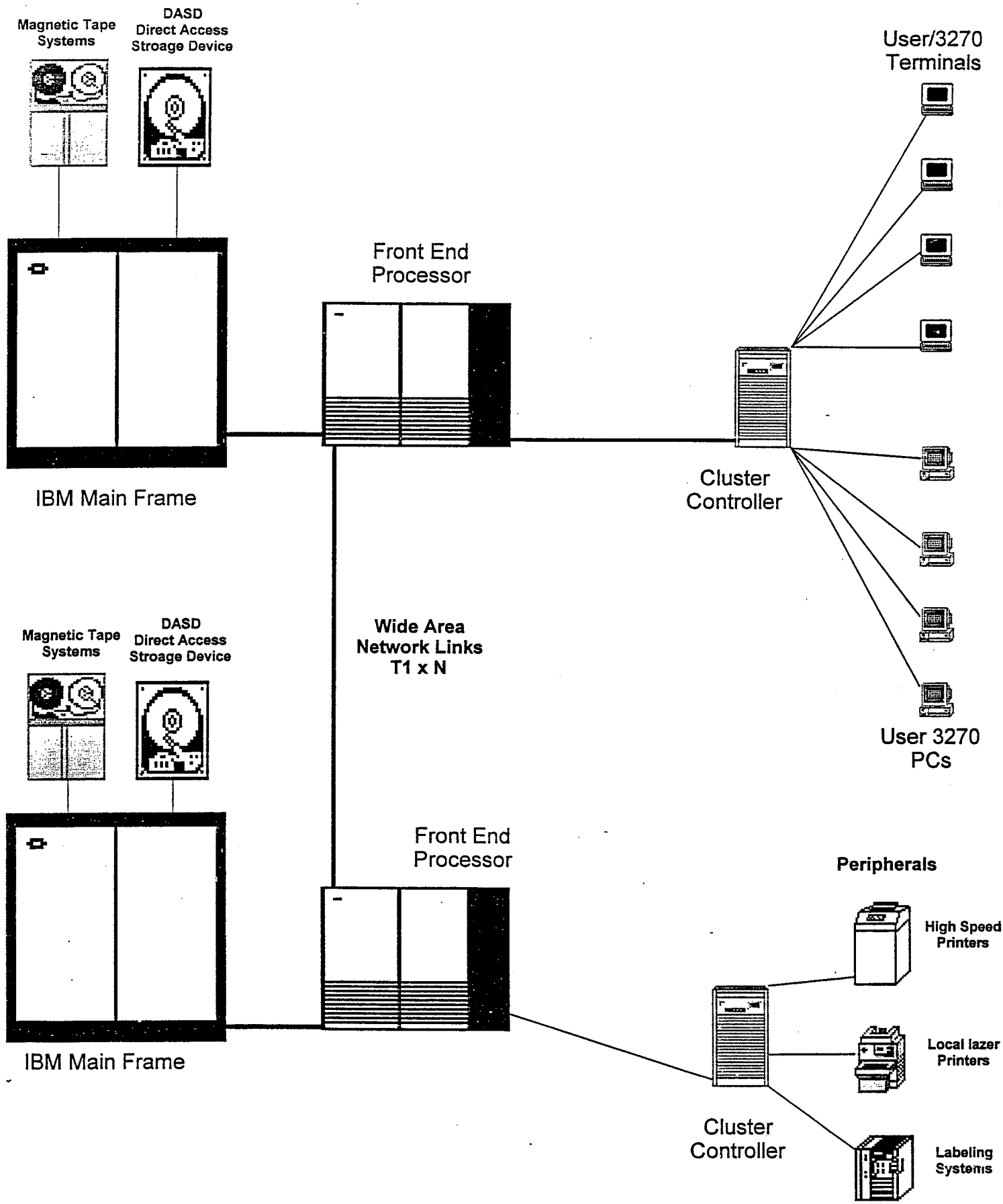


Figure 1 Basic SNA Configuration

Figure 1. Basic SNA Configuration.

Controllers - Peripheral nodes in SNA networks. The primary function is connection of terminal devices such as visual display units, printers, etc. Cluster controllers accept the local link from an FEP and control user link access. The cluster controller maintains strict user link and connection specifications and is limited in its operational configuration flexibility.

Physical Units (PU) / Logical Units (LU) - PUs and LUs are attached to the user links that originate from the cluster controller. PUs are physically attached units such as user 3270 terminals, visual display systems, and 3270 emulation cards in desktop computers. LUs are printers, terminals, or disk drives attached to a PU, thus becoming an extension of the PU.

2.3 SNA Communications Technology Overview:

SNA networks were originally conceived and designed as WANs. The SNA concept was to distinguish between local and remote links. Local links were used to link host systems and communications controllers as well as host systems and local cluster controllers.

Remote links were used to connect "off site" cluster controllers. Remote links could be operated in-house or over public networks, like the public telephone network, utilizing dedicated half or full duplex lines or a form of packet switching topology. The dedicated links used a Synchronous Data Link Control (SDLC) protocol. The packet switching system used an X.25 switch access protocol with a Qualified Logical Link Control (QLLC) data control protocol. Node and system addressing and identification control is intensive.

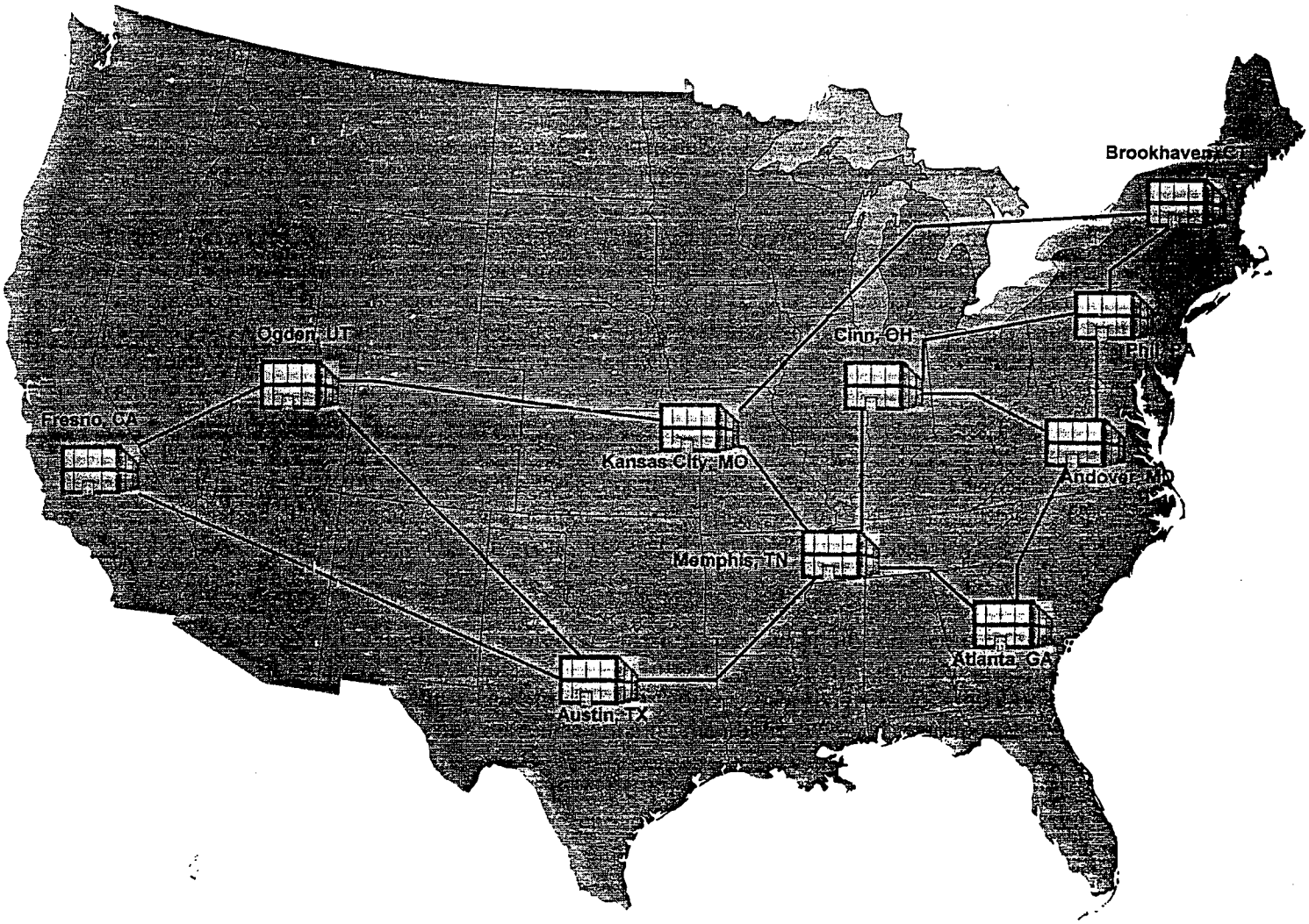
The host-system and communications-controller level of an SNA network is organizationally subdivided into sub-areas and domains. A sub-area consists of the sub-area master node and all peripheral nodes assigned to the master node. This subdivision into sub-areas is a key element for network addressing.

A level above the sub-areas are the control domains which can be interpreted as administrative units. All of the resources managed by a single host system form a domain. When a specific terminal attached to a cluster controller needs to transmit data to the mainframe computer or generate a request for service, the link protocol will dedicate the entire link to that terminal for the duration of the traffic transport or service request time. This ensures that the system will have enough bandwidth to transport the data within a reasonable time frame with a minimum of errors.

Currently, the IRS must provide carrier bandwidth for interconnecting and transporting the required processing traffic to all of its current locations. Carrier bandwidth is defined as the bandwidth capacity of the interconnecting lines. In order to accomplish this task, the IRS currently uses hubbing and/or "store and forward" capability which allows remote office locations to communicate with each other by going through one or more of the submission centers. Please see Map 1 for a current submission center and carrier network configuration:

***Note:** For the sake of System definition, this map only reflects the Computing and Submission Processing Center locations.

The submissions centers emulate tandem or "hop" locations. For example, if the Dallas regional office wants to send data to the Cleveland regional office, it will use this hop capability to transport the data to the destination. The data flow path is shown in Figure 2.



Legend:

1) Denotes combination Service and Computing Center 

2) All Thick lines are T-1 Links

MAP 1 Current IRS Submission and Computing Centers Configuration

Map 1. Current Network Configuration.

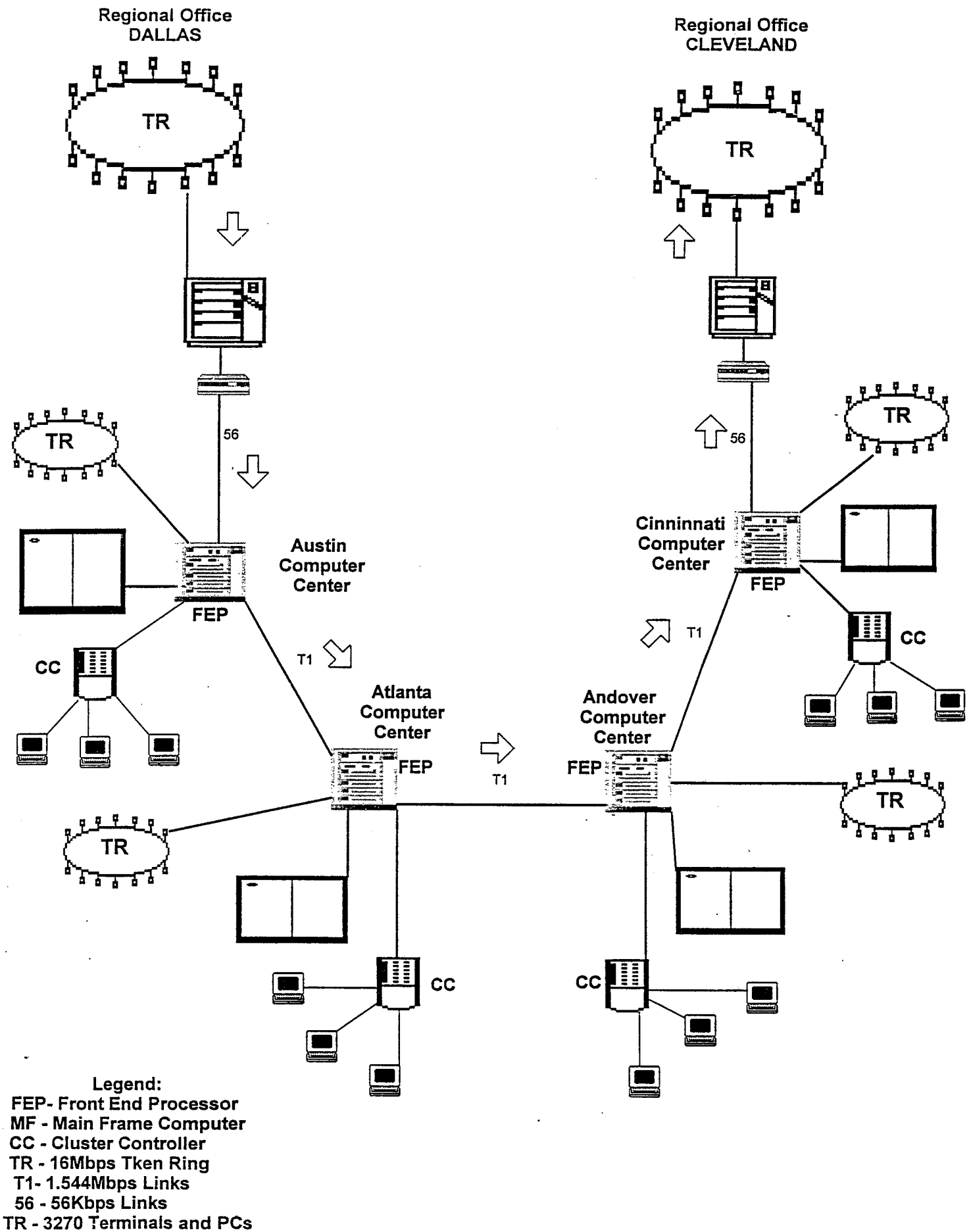


Figure 2 Tandem Configuration

Figure 2. Tandem "Hop" Configuration.

The IRS Internet working communications lines have 3 basic classifications and operational definitions:

Private network, unswitched systems: These are IRS only and dedicated small-to-large bandwidth carriers ranging from 2400bps to 1.544Mbps (T-1) speeds. Predominately used to permanently provide, as required, large and small bandwidth network capacity between all of the IRS major locations. Therefore, all of the 10 submission processing centers mainframe to mainframe processor traffic is directed to the 1.544Mbps lines. The remaining offices are provided subrate (lower than T-1) bandwidth as needed. As shown in Map 1, each submission processing computer center has a minimum of two T-1 carriers.

Public network, X.25 switched systems: This system provides the ability to use public switched bandwidth, upon demand, to transport processing traffic. This provides remote and regional locations, without a daily traffic transport requirement, the ability to upload and download files and other required data, while utilizing mainframe processing capability when and if needed. This time control element is important when the need for processing power is low or sporadic, and the cost of data transport capability is high.

This type of system acts much like the public telephone voice system. It generally utilizes the X.25 protocol controlled customer links of up to 56kbps to gain data switch access. The data switch reads the data destination address and sets up a temporary or "virtual" circuit for data transport. Once the data transport is completed, the switch then breaks the virtual circuit idling the customer link. The only constant "up or on" condition is the customer link communication with the closest serving X.25 switch.

Public network, switched, dial-up systems: This provides the ability for remote offices, on-the-road investigators, or at home telecommuters to dial into the submission processing center and retrieve information as needed. System Access requires a modem (modulator-demodulator unit) to dial into a modem pool located at the submission center utilizing the public switched telephone voice network.

This level of technology only guarantees data transmission at relatively low speeds because of its basic design for voice or analog transmission (recent advances in technology have greatly increased the path transmission rate of ordinary voice-grade connections). Therefore, successful transmission of more bandwidth-intensive applications utilizing this type of transport is questionable at best.

The following configuration drawing, Figure 3, shows a base topology of how the various operating centers and office locations interconnect.

2.4 System Operational Considerations

During the past twenty years, the IRS, as an organization, has increased its normal daily operation by over 350%[3] . The number of employees has tripled. This increase in workload and personnel however, has not been matched by an increase in computing and communications support efforts and capabilities.

Another mitigating factor is IRS support in attempting to strengthen the national law enforcement efforts as well as meet the demand for public access to specific information. Congressional response was to mandate that the IRS share detailed individual and corporate financial accounting information with other entities of the federal government. The current IRS SNA based technology limited the ability to comply with this mandate.

---

[3]IRS Current Systems Operations Management Statement, 1992-R1, 1993- R2

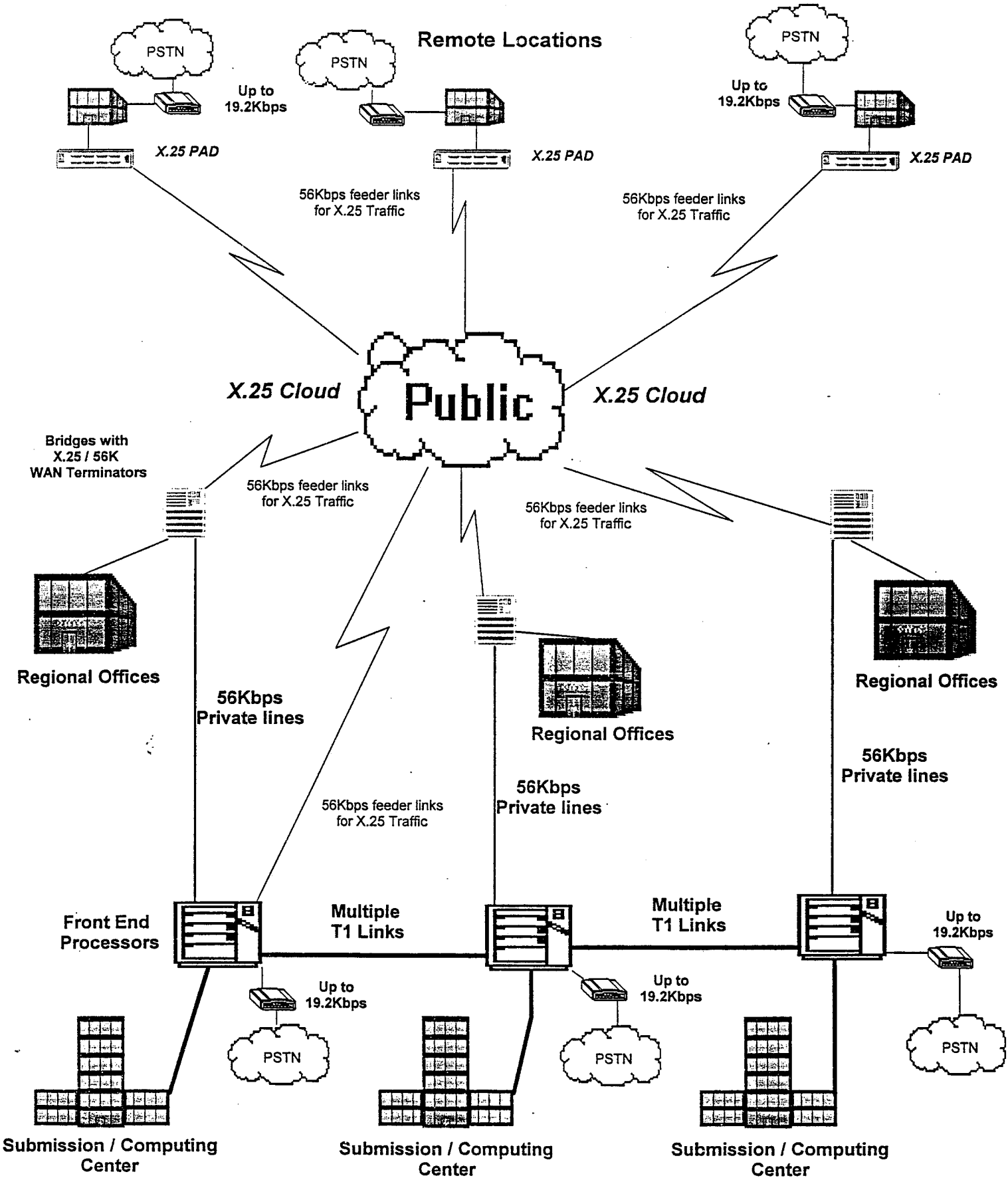


Figure 3 Interconnection and Communications Basic Configuration

Figure 3. Interconnection and Communications Basic Configuration.

Unless extremely well defined, SNA systems, as an operational standard, are not robust enough to run multiple applications concurrently without some detectable loss of processing power or an obvious increase in user-computer application response time. System strength is found in functioning in a sequential operation mode on a single application.

With the growth of desktop computing, more people have mainframe access which increases the demand on a central processor. Among the effects of this increase in demand are slow response time for the users, lost or corrupted data, long delays during database queries, and large uncontrollable blocks of down time.

SNA systems are also limited in utilization of Commercial-Off-the-Shelf (COTS) software without involved customization efforts. The ability to just go to a computer store and buy specialized application software is currently non-existent.

2.6 Current Location Configuration

Currently, the IRS operates a collection of different sized office operations dispersed throughout the continental U.S. and abroad. The current IRS operation direction is to reduce the number of operational locations by consolidating and increasing the operations and processing power for the remaining locations.

The IRS uses the following titles to classify and size the various office locations. Table 1 defines title versus size and supporting network map; Map 1, shows the physical locations of the submission and computing centers only:

Table 1. Current (1995) Configuration

Title	Number/Locations	Personnel/Location
Regional Offices	7	+2,500
Submission and Computing Service Centers	10	+3,000
Customer Service Centers	23	+1,250
Corporate/Agency Washington DC Area	15	+3,500
Misc US/Overseas Locations	25	+150
Archive Control Centers	2	+750
Estimated Total	80	+127,750

Table 1 does not reflect independent access granted to specific corporations. The scope of the current operation in supporting so many people over such a large geographical area, easily consumes all of the current computing and communications resources.

2.7 Current Traffic and Transport Bandwidth Configuration

In order to fully understand the scope and depth of the data traffic, the following area will focus only on the submission and computing services center.

While the 10 computing and submission centers operate under a 3-shift umbrella, the complexity of the system and the mass of data traffic, in some cases, can result in unacceptable delay. Table 2 will show the current processing demands placed on the computing system.

The requests, defined below, operate at each location, and are then multiplied by 10 to determine the overall system processing requests requirements. Each request for processing service will develop a file of specific size and will address one of the operational modules used for processing directional control.

These files are shown as individuals. It must be understood that one or more combinations are derived from these individual files to build one complete tax submission folder.

The current processing and traffic configuration do not incorporate off site dial-in requirements, E-mail requirements, interagency processing and data requests, or normal administrative processing requirements. The administrative processing requirements may include personnel records, payroll, standard operational accounting, personnel access control, and internal auditing systems. In addition, the table does not reflect the inter-computing center traffic generated by normal operations.

Table 2. Current System Processing Requests

Type of Request	Average File Size (Kbits) Per Request	Yearly Requests Total
Module 1 /1040A	75-100	3,000,000
Module 2 /1040	350-750	5,000,000
Module 3 /1040 Speciality Forms	150-250	10,000,000
Module 4 /Business and Speciality Forms	250-650	2,000,000
Module 5 /Estates, Gifts, MISC.	250-450	3,500,000
Module 6 / Non-profit	275-500	1,500,000
Module 7/ Formed Correspondence	150-450	4,000,000
Module 8/ Internal Data Requests Investigations	Unknown	Unknown
Database, processing, balancing, and conciliation	Unknown	Unknown
Record Achieving and Inventory Reconciliation	Unknown	Unknown
Ad Hoc Operations	Unknown	Unknown
Daily Operations	Unknown	Unknown
Module 9/ AD Hoc Correspondence	100-750	4,000,000

CHAPTER 3

3. SYSTEMS ARCHITECTURE AND ANALYSIS

There are two important areas of advancement being accomplished by the system modernization project. First, new system architecture and applications platforms, and second, the technological impact this will have on service and information accessibility.

This chapter will present and analyze the old systems architecture and applications in conjunction with the new systems architecture and applications that will replace them. This effort is a modified "Systems Engineering and Analysis" adapted to IRS defined requirements and constraints.

It is important to note that functions are different from applications. For this paper, functions will be considered the actions that need to be accomplished, and applications will be defined as software programs used to accomplish those specific functions.

The approach will allow the comparative analysis to be addressed from a communications networking point of view.

3.1 Developmental and Transitional Systems Architectures

The TSM effort is viewed as an evolutionary process that spans every functional area involved in the normal and ad hoc operations of the IRS. System complexity and loss of central management control dictated a modular approach to system redesign. In order to design a systems architecture which incorporates multiple IRS functionality, four major levels of architecture development were required.

I. The initial system architecture was used purely for current system concept and feasibility validation. This area addressed the current systems and placed into a layered hierarchical graphic the theoretical area of function, functional traffic demands, areas of responsibility, and accountability.

This was known as the as the Base TSM Architecture. Its main focus was to serve as a disciplined communications vehicle. This would allow isolated functional areas to communicate and establish a basis for technical and functional analysis and define the requirements analysis task of the project which were covered in Chapter 2.

II. The second architecture level addressed system functionality and applications utilization. This level included operational segments of various programs, necessary integration of cross referenced operations requirements, and defined the foundation for the final overall operational architecture.

This is known as the Tax Processing Systems Architecture (TPSA). This analysis validated the tax processing core functions and looked at the iterative process of describing the functional and technical systems, applications, extensions and refinements. This area is considered a critical part of the overall systems analysis effort.

The TSPA is composed of six functional areas. Each function has multiple operations which communicate and interact with other reports from the IRS operational foundation. Figure 4 shows the TSPA architecture and includes the six functional areas and their processing flow paths.

Currently, these six segments are using the normal IRS communications equipment and networking environment. The age and unreliability of the current processing and transport environment lends itself to duplication of effort. The IRS views this duplication of services in each functional area as being a faster and more reliable operations support than relying on slow communications.

Functional area definitions:

Submission Processing Segment (SPS): Converts paper documents into electronic images and perfected American Standard Code for Infromation Interchange (ASCII) data; provides images and data to other systems for processing. Operations are located in the major tax return submission centers.

SPS provides the following services:

1) Automated Document Handling; controls incoming documenation.

2) Data Capture; converts paper documents to electronic images (i.e., scanning and extraction of character data).

3) Tax Data Perfection; performs the following checks; code and edit, entity, math computations, etc.

4) Data Correction; supports manual corrections required by 3 above

5) Archive Management; stores and controls all documentation.

Computing Segment (CS); Provides for the automatic processing of electronic file returns, tax-related database management, revenue acccounting, compliance, issues detection, and compliance research. Its central location in Figure 4 is indicative of the CS critical nature. This segment is the focal point of the entire IRS modernization effort.

CS provides the following services and functions:

1) Account Management; receives account update transactions, establishes new accounts, performs in-depth detection on accounts, maintains summary account records and responds to to informations request from other areas.

2) Tax Data Perfection; identical to submission processing.

3) Revenue Accounting; receives payment data from cash management, records, and balances; then reconciles and reports tax related financial functions.

4) Data Verification; receives data from external sources, identifies the source, authenticates the transaction, decrypts the transaction, and stores the transaction. This area is operated under the security umbrella.

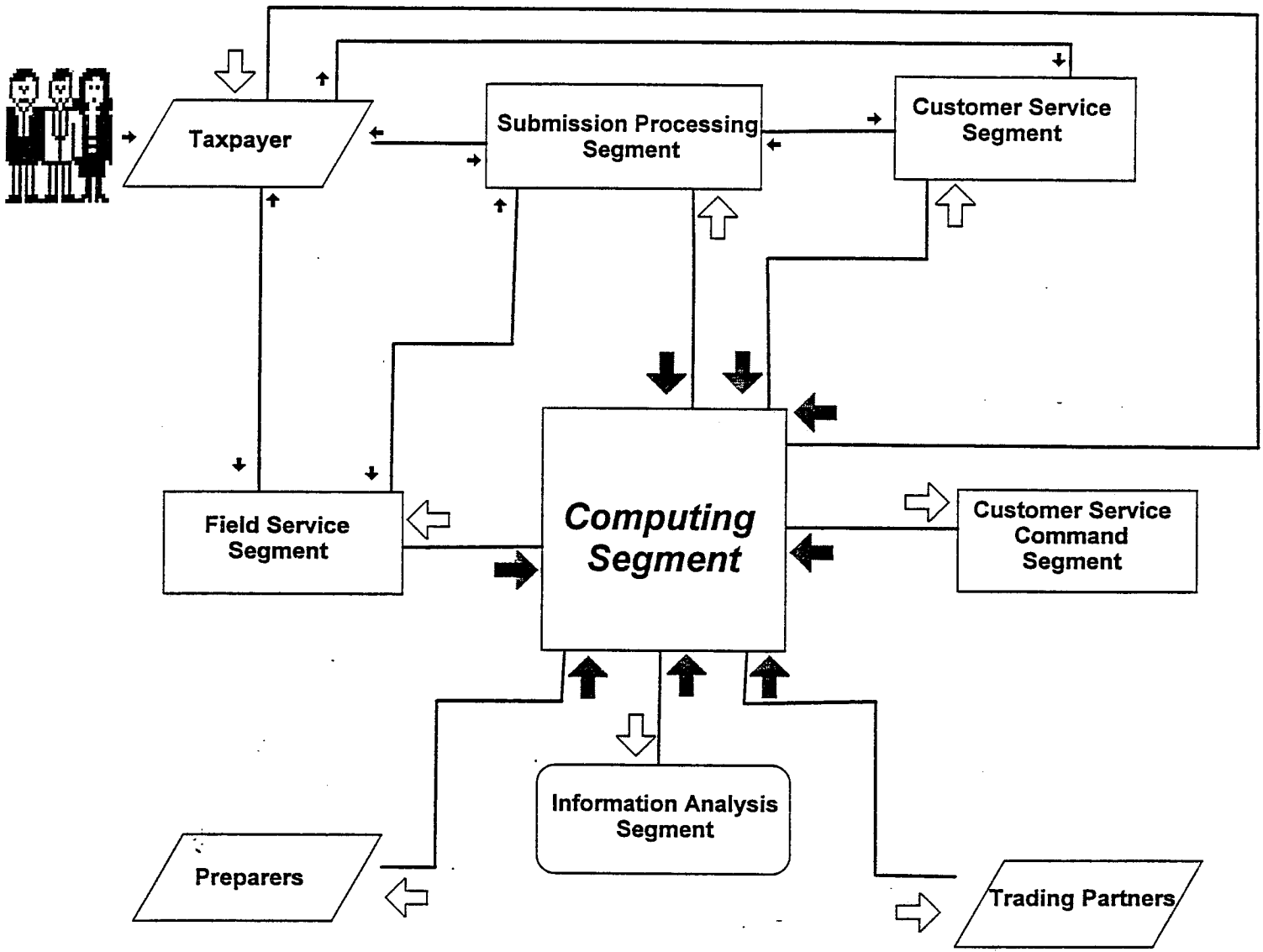


FIGURE 4 Tax Processing System Architecture

Figure 4. Tax Processing System Architecture.

5) Electronic Filing; receives electronically filed tax returns, information returns, and financial data.

6) Electronic Data Interexchange (EDI); controls the exchange of information between the IRS and both the public and private sector and allows information access to other government agencies.

7) Cash Management; recieves data electronically from third party finanacial agents.

8) Case Management; recieves, issues, establishes, and stages cases; and generates notices for case fault investigation and resolution.

9) Submission Index Maintenance; maintains the information index for document or elctronic submission location and status and supports user interface.

10) Production Statistics Collection; accepts and controls production analysis data from all operating areas of the IRS.

11) Name Search; finds taxpayer indentification information.

12) Cross Reference Index; maintains cross reference information of taxpayer accounts.

13) Entity Validation; assigns each account to a specific computing center based on functional criteria (zip-codes, etc).

14) Information Returns Processing; accepts the different types of media through which information returns are submitted and makes that data available to other areas of the IRS.

15) Rollup Processing; receives operational data from other areas of the IRS and generates specific reports based on recieved information.

16) Reference Data Manitenance; maintains the master reference information databases and provides this information to other segments as requested.

17) Rates; maintains the master rate databases and provides this information to other areas of the IRS.

18) Compliance Research Analysis; maintains a database populated with over 100 million taxpayer accounts used specifically for compliance analysis. The IRS currently operates under a compliance effort focusing on yield per individual case. This effort will soon change to a market-driven approach emphasizing overall yield. The market-driven approach plus an increased effort to reach the taxpayer through education, outreach, and other informational programs, is estimated to significantly increase voluntary compliance.

19) Forms Distribution; processes requests for forms and publications.

20) Security Audit Analysis; examines security data and provides data for security trends analysis.

Customer Service Segment (CSS); performs all case processing and taxpayer assistance that does not involve face-to-face interaction with the taxpayer. Generates and answers white mail, responds to requests

for turn around documents or any issues that require further information or assistance from the taxpayer. At this level, all interaction with the taxpayer is via telephone or written correspondence.

CSS also supports IRS external TSMA interfaces to federal, state, and local government tax databases, credits bureaus and commerial informational and accounting databases. The functions described will be located throughout the customer service center locations.

CSS provides the following functions:

1) Case Processing; provides research and problem resolution functionaility to the Customer Service Representative (CSR) who is analyzing a case or providing service to a customer.

2) Case Management; provides support in three major areas; case staging, managing case inventories and workload assignments, and controlling case processing requests.

3) Case Workload data collection; provides the means to query and collect data for caseload management.

4) Tax Data Perfection; same as previously stated

5) Rates; as stated in 2b.

6) Taxpayer Interface support/Virtual Workstation Support; allows a customer's telephone keypad to act a as virtual workstation and allows input or query data as needed.

7) Security Administration; validates the taxpayer identification number and CSR level of access capability.

8) Reference Support; controls and supports the reference material and resources.

Field Service Segment (FSS); performs the case processing involving face to face interaction with the taxpayer. The majority of this effort is directed toward resolving collection cases not closable by mail or telephone. FSS accounts for the majority of remote accessing experienced by the network architecture. This area supports documentation transference, laptop computer support, document imaging, and other support functions for field personnel.

Customer Service Command Segment (CSCS); provides for the management of the CSS. Includes operational load balancing between the centers, automatic call distribution, call overloads resolution, and personnel controls. This area also manages emergency recovery systems for customer services areas.

Information Analysis Segment (IAS); establishes the policies, procedures, and programs for the administration of IRS laws, related status, and administrative directives that direct, control, and coordinate the overall IRS operation. In addition, this segment investigates compliance research and establishes taxpayer educational programs.

IAS provides the following functionality:

1) Compliance Research Support; supports the CS segment compliance research analysis function. This includes the evaluation of taxpayer compliance data and identifing national and local market segments targeted for compliance educational activities.

2) Policy Deployment Function; this area supports the generation, review, approval, and distribution of national, regional, and district level IRS policies, procedures, and programs. Data of this type includes interpretive legal positions, tax legislation, and education programs.

3) Management Information Analysis; supports the collection, analyzation, and summarization of management and financial information at various levels within the IRS.

4) Office Automation Tools; provides and supports a wide range of capabilities to facilitate the performance of management and administrative tasks. The tools and utilities provided by this function include word processing, spreadsheets, statistical analysis, graphics, management and scheduling tools, and E-mail.

III. This area names additional systems required to integrate and utilize by the current system in order to perform IRS functions. This effort contributes further to the analysis of the overall system processing effort.

Tax Support Processing Systems (TSPS); includes the systems that directly or indirectly support the normal and ad hoc IRS operations. The TSPS is a separate area of management and development that solicits information from functional areas and supports those areas with engineering development efforts outside of the functional area charter.

This area includes the involvement and development of support complementary systems and engineering specialities efforts such as:

1) Privacy and Security;
2) Communications Systems Development (all forms);
3) System Development Standards;
4) Strategic Data Planning; and
5) Systems Transition and integration planning .

Other support areas include; Configuration Management Systems, Network Management Systems, and Standards Controls (utilizing and enforcing GOSIP and POSIX mandates). This effort describes all of the current administrative and management functions that control and utilize the current IRS system.

Security; This paper is focusing on the communications aspect of the IRS modernization system. However, because security is such a vital support function involving the communications systems, both internal and external to the IRS, the current IRS effort in this area will be briefly discussed.

Security is a major concern for the IRS. The IRS has been given the responsibility of safeguarding the financial information of the general population. The IRS needs to provide a security architecture that will put into place all of the necessary safeguards in order to minimize the threat of intrusion by unauthorized personnel. To this end, the IRS has identified three primary threats:

1) Improper Disclosure; unauthorized subject access to taxpayer, employee, or IRS-derived information.

2) Unauthorized Data or Process Modification; any subject who uses any direct IRS or indirect IRS supported system without authority, to modify, append, change, or delete any IRS identified data or processes.

3) Denial of Service; defined as the malicious disruption of IRS critical or non-critical activities or availability and access by authorized or non-authorized users.

The focus of TSM is to develop countermeasures that minimize threats to financial information. These countermeasures will include development and deployment of a combination of administrative and electronic methods to ensure security compliance. These measures are:

- Personnel administration; to ensure the trustworthiness of select personnel put into positions of responsibility. This includes access level controls and accountability for data and record modifications. This area is functional at all segment levels and at all locations.

- Application level control; to ensure the ability to notify, track, and compile any level of intrusion for specialized accounts. This ability must be built into the applications so that it is transparent to the user. This effort should notify the security area when specialized folders or records have been accessed, and what operations are currently being applied to those specific records. Security verification efforts can either validate the operation or notify the user's supervisor that an unauthorized operation is currently underway.

Security Based Communications; This includes a multiplicity of approaches such as: the standard link and network Encryption that encrypts the physical level of the LAN and WAN networks and multiple based software approaches such as Selective Application level encryption, and Digital Signatures and Authentication Token systems such as Kerberos.

1) Single user, dial-in access encryption: The remote user, (i.e., a Case Investigator), located at a customer premises, uses a dial-up modem to call into a computing center and once the connection is complete, activates a modem-based encryption unit to transmit and receive sensitive data (see Figure 5).

2) Remote location X.25 physical layer encryption; a general application utilized in local offices which uses an X.25 packet switching system to communicate with the computing centers. This allows the encryption to be selective for only specialized LANs, resident to an X.25 Packet Assembler/Disassembler (PAD) unit, to feed to a selective host computer which then converts the X.25 Data Network Interface Connection (DNIC) address to Transport Control Protocol/ Internet Protocol (TCP/IP) address and allows the data to be directed to the correct terminal. See Figure 6 for visual layout.

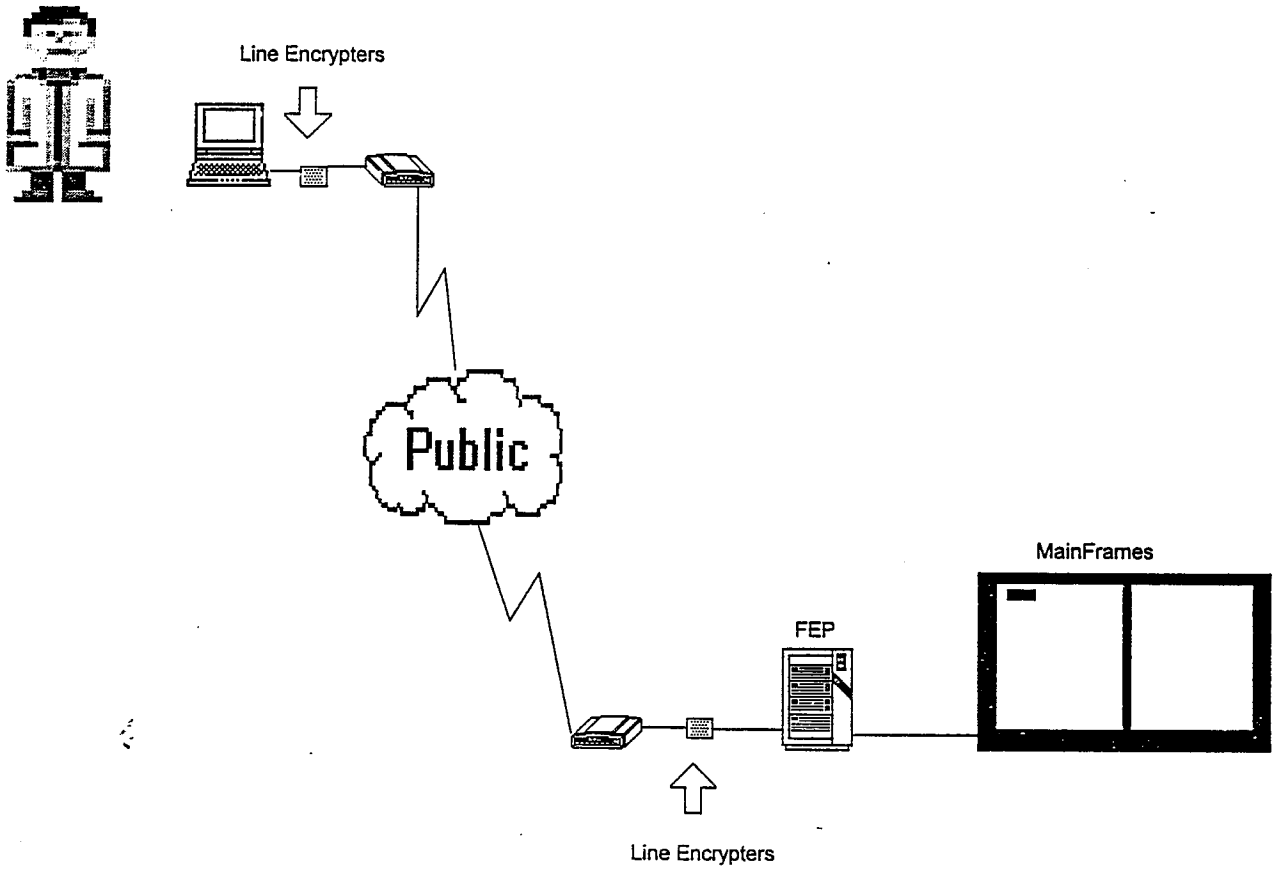


Figure 5 Single User Dial-up Encryption

Figure 5. Single User Dial-Up Encryption.

3) End-to-End Global or Selective Encryption; encrypts all data from its original location to its destination, utilizing all networks at the physical layer (see Figures 7.1 and 7.2).

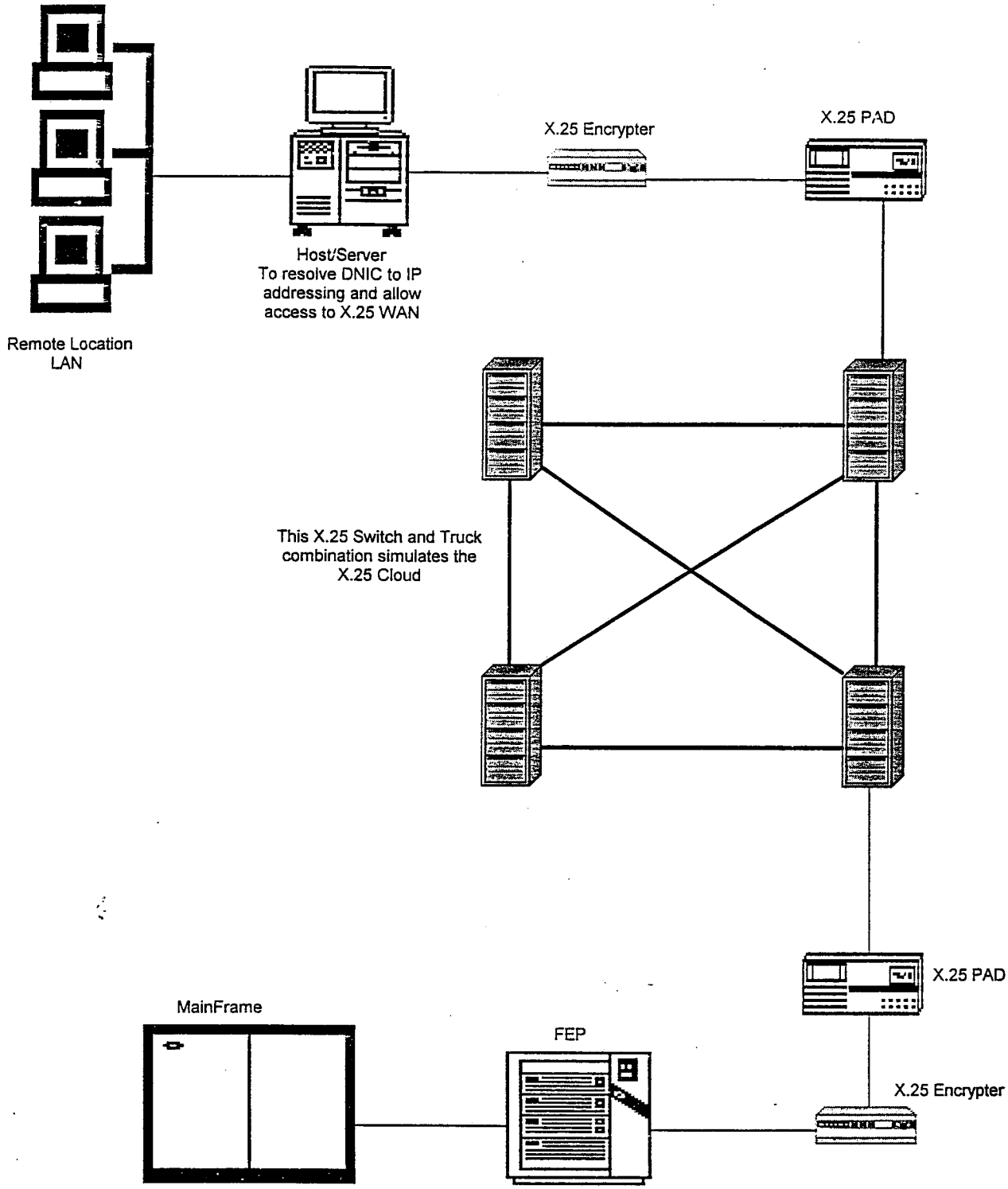
- End-to-End Global Encryption; allows encrypted data to flow from one secure network to another. The Global portion indicates that the entire network located behind the link encryption is secure. This technique removes the option of selectivity from the terminal user. See Figure 7.1 for visual layout.

- End- to-End Selective Encryption; gives the operator the option of whether to encrypt the data. This is accomplished by putting a physical layer network encrypter in line and between the terminal and the network connection. This option allows multiple encrypter and non-encrypted terminals to reside on the same network. See Figure 7.2 for visual layout.

4) Applications or Operations level security; includes Digital Signatures, Kerberos Authentication Tokens, or Applications level encryption.

- Digital Signatures: A fairly new field. A trusted entity provides a series of numbers known only to it and the issuing agency. This, in turn, validates the operation by ensuring that the user is who he says he is, and is then authenticated by a independent source (like a Notary Public would do for a written signature). This provides the basis for general electronic tax filing without the requirement of having to send a paper tax form to back up the electronic submission.

- Authentication Tokens; Authentication tokens in a software module assigned a unique identification code and located in the terminal accounting and setup configuration. In turn, a non co-located server is required which possesses the user terminal ID code with the level of access requested based on the normal user ID password.



Option 2 :
The link encrypters can be re located to the X.25 trunks.
But this means that the X.25 cloud must be dedicated
to only the IRS.

Figure 6 Remote Location X.25 Encryption

Figure 6. Remote Location X.25 Encryption.

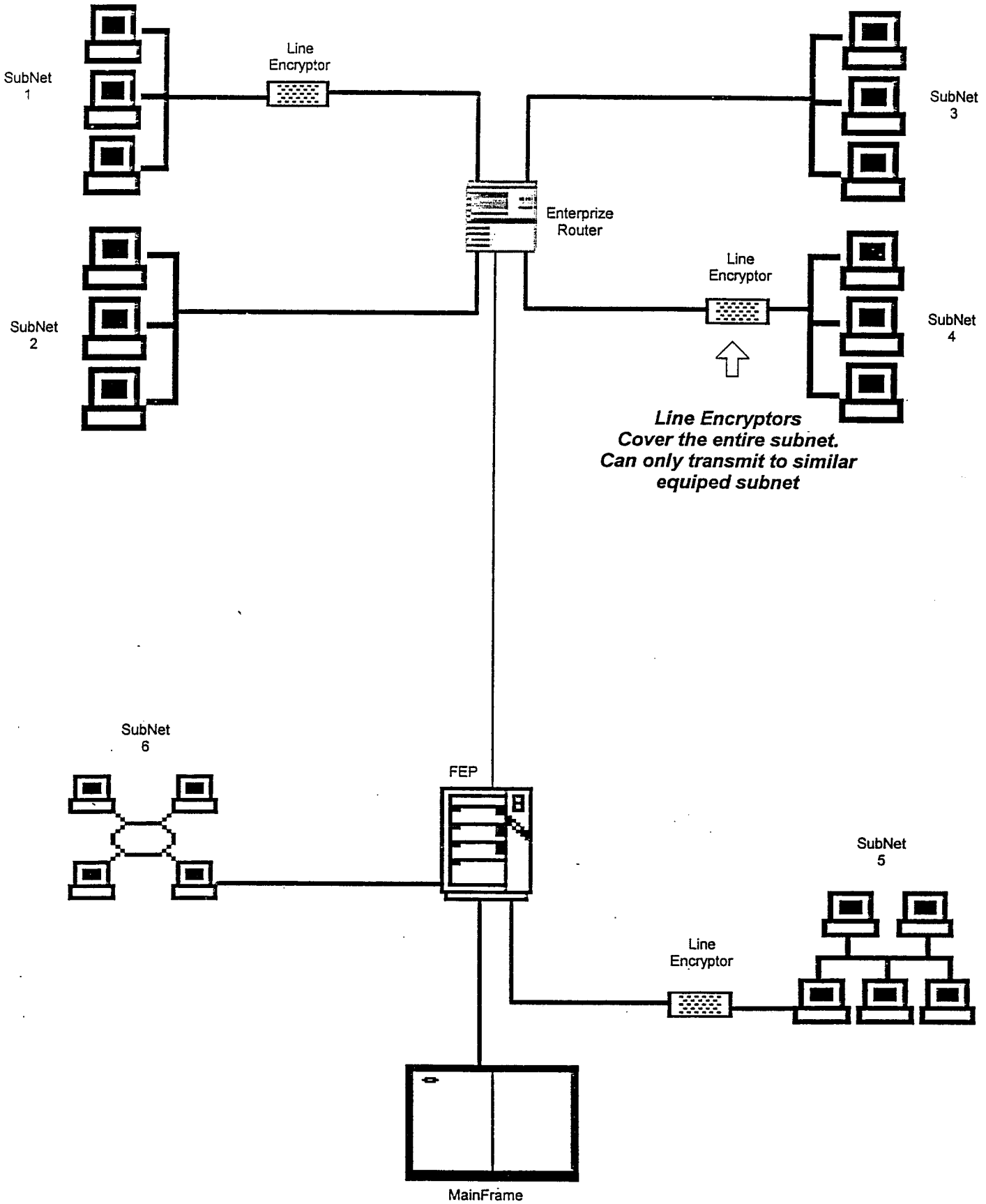


Figure 7.1 Global End to End Encryption

Figure 7.1. Global End-to-End Encryption.

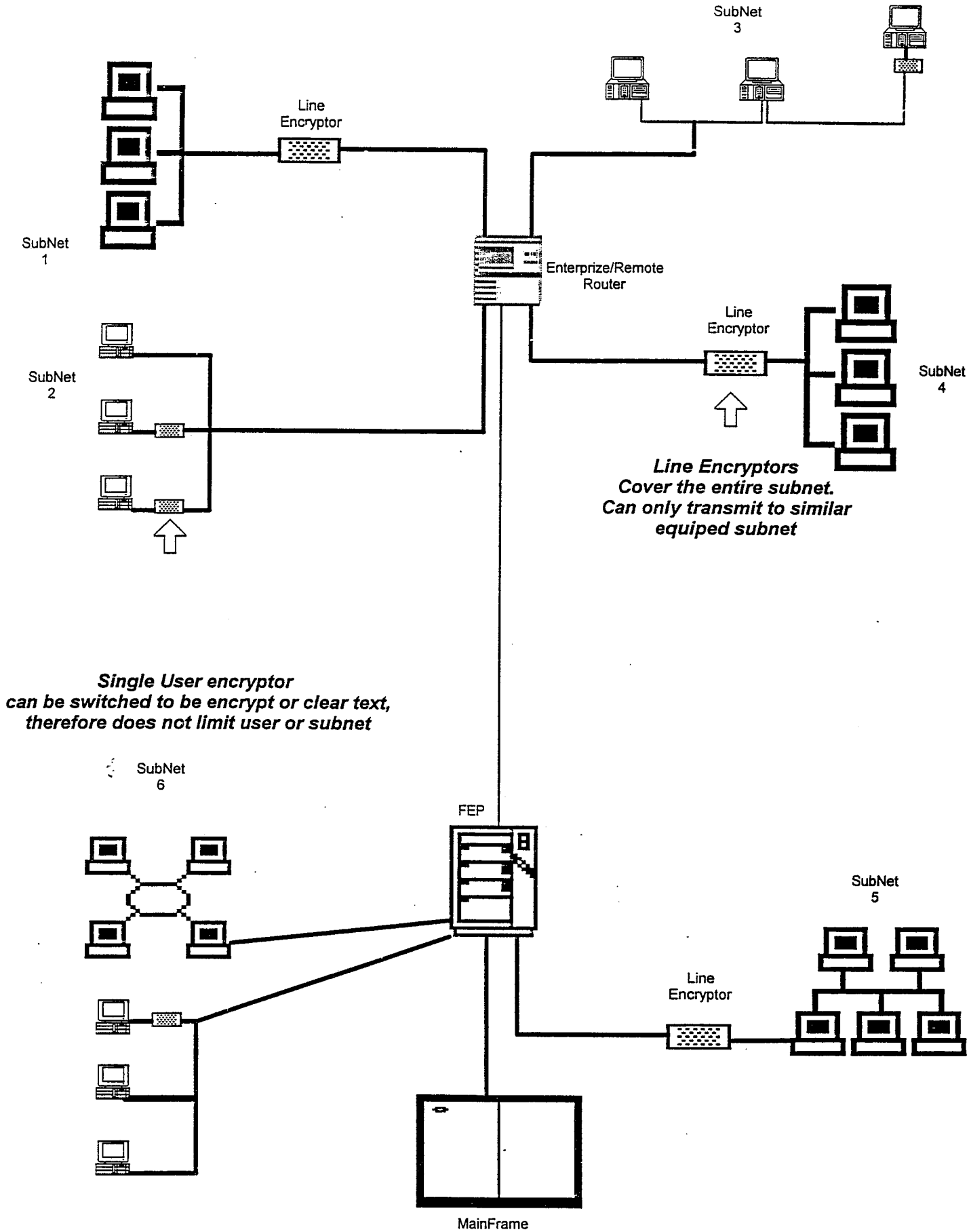


Figure 7.2 Selective End to End Encryption

Figure 7.2. Selective End-to-End Encryption.

Once this reconciliation has occurred, each time the user accesses a network or application resource, a verification effort would occur. If successful, a token would be issued to the user's terminal and would be exchanged for service from the resource. This requires permission to use the resources or access will be denied.

- Keberos; a UNIX-based security effort that also works on a token passing effort with a user validation service. Historically, Keberos was known as the three-headed dog that guarded the gates of Hell, this Keberos server guards all of the secure network resources allowing usage only by those that are authenticated.

- Applications Level; incorporates the security into the applications programs themselves. This means that, by design, you can encrypt portions of text and leave other portions as clear text For example, a specialized form for financial data has been developed in a Sybase DBMS system. You can enter personal data in specific fields and financial data in the other fields. Once this is accomplished you can send this form to another system user and the application will either encrypt the personal information, the financial information, or both. It is up to the applications development management team to determine what areas to encrypt. There are more advanced applications which allow the user to choose what areas to encrypt.

IV. Transitional Architecture (TA); This architecture details additional steps and functional areas necessary to show the transition between the old systems architecture and the new systems architecture (see Figure 8). It involves the development of three additional architectural segments that attach themselves to the TSPA architecture previously detailed.

These added segments are:

1) **Program Development Segment;** supports the development and engineering effort of identifying, designing and deploying specialized applications programs deemed "out of the mainstream" for normal IRS operations. This area is configured with the software, hardware, and communications efforts necessary to develop and maintain TA configuration items. This includes the tools and facilities to develop software, perform unit testing, and subsystem testing, and configuration management. This effort is to maintain operational continuity between today's technical position and that of the future.

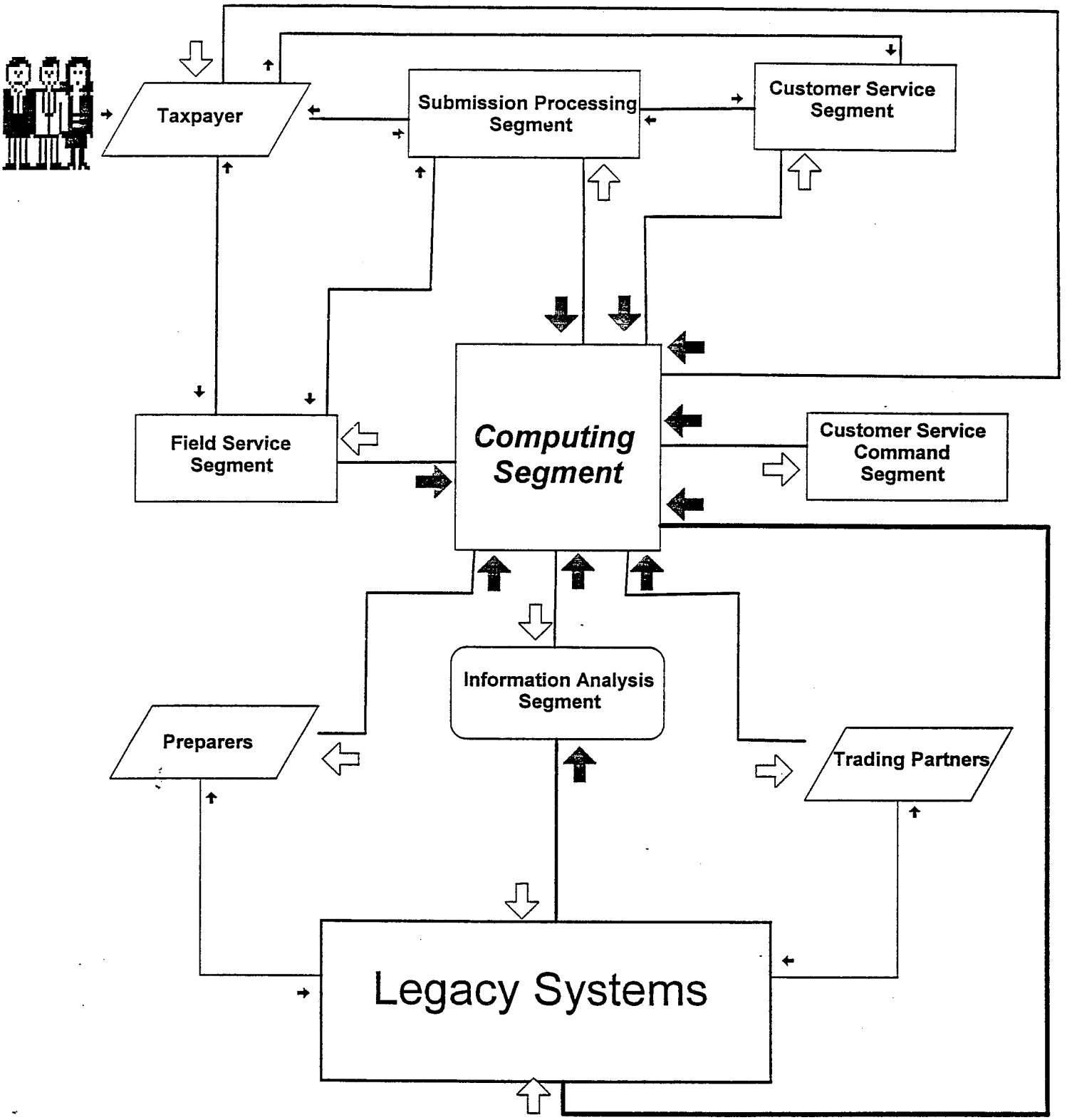


FIGURE 8 Transitional Architecture

Figure 8. Transitional Architecture.

2) **Program Development Support Segment;** provides for shared support equipment (communications, processing, etc) and developmental resources (database libraries, process data, etc) to support the development and maintenance of the TA software. The TA software is a "middle ground" transitional software that will allow the transport and manipulation of data between the new databases and the old databases, thus providing data baselines which will contain the master copy of all development data objects. It also controls the effort of transitioning from an SNA based communications systems to a OSI based communications systems.

3 **Systems Integration and Testing Segment;** supports the Program development area by providing the equipment and resources necessary to support the segment level integration of the TA and conducts the system and user acceptance testing of the TA. It also provides test data and the development of test cases necessary for segment-level systems verification and validation.

Together, all nine segments are known as "target segments." As these target segments are phased in and tested, the role of the legacy sites will change. They will no longer be bound by the functionality currently assigned. Instead, they will house one or more of the target segments and perform the functions of that specific segment.

In the previous chapters it was stated that the various IRS locations and their operations are composed in an hierarchy. This hierarchy allows for a logical flow of information within the IRS. The hierarchy is as follows low to high:

a) Local Offices;
b) District Offices;
c) Service Centers; and
d) Computing Centers.

As the IRS operation evolves into a more tightly controlled operation supported by the TSPA architecture and the TA transitional architecture, some rearrangement of function will naturally occur. Once initial computing upgrades are installed, the IRS needs to show some strong short term service improvements. The following will address the changes imposed by the TA architecture and satisfy the need to show immediate improvement.

1) The Service Centers main mission is to process tax returns and related documents and provide manual entry of specific data or forms as needed. Presently, the added improvements include; electronic scanning of all incoming documents with high speed scanners that utilize a multi-level gray scale Optical Character Recognition (OCR) applications software. They also access and collect tax revenue, secure delinquent returns, and make adjustments to tax liabilities.

2) The Computing Centers operations such as maintaining master account file data, providing data on delinquencies, processing refunds, bills, notices, audits, and supporting research operations has not changed. The workload however, will increase. It is expected that in five years, computing center operations will increase by 350%.

   At present, all Computing centers operate exclusively in the batch processing mode with magnetic tape as the predominant interface medium. The future direction is for all database machines to utilize "Reduced Instruction Set Computers"(RISC) technology. This type of robust technology will provide for the efficient use of high speed networking technology by direct connection to the

main bus feeders. This will allow WAN technology, such as ATM/Frame Relay, and LAN technology, such as FDDI, to be used to transport and account for data more dynamically.

For example, some of the smaller database processor engines will use Pyramid RISC Computers. These computers provide for a slotted CPU shelf, with each slot capable of accommodating an additional CPU card of up to 25 MIPS capability. Therefore, as CPU processor requirements reach the threshold, operators can add CPU cards and increase the power of the processor engine as needed.

Another example is data storage. Currently, the computing centers archive the data on SNA-based direct access storage devices (DASD). Because of several considerations (the age of the present technology, the constant updating of operational software), the inability to dynamically add storage capability without programming support and environmental consideration (i.e., floor space and climate controls) see the most immediate impact by the new technologies.

These new technologies introduce high-volume optical storage devices. Devices such as the Optical Platter and Compact Disc technology provide immediate capacity and long term growth capability that is needed to accommodate the overwhelming amount of processed data.

V. The final IRS architecture has not yet been established. The temporarily titled configuration used by the IRS to accommodate for the fourth architecture is known as the **Integrated Systems Architecture (ISA)**. The ISA a living, dynamic developmental approach virtually undergoing daily changes. For this level, the IRS is employing a concept called a "living architecture." This concept is based on applying the best of the "Large Systems Development" and "Spiral Systems Life Cycle" approaches .

The ISA concept is based on the following theoretical premise:

1) The IRS is mandated to use a GOSIP-based open system approach which provides maximum flexibility in systems design.

2) Discovery, acceptance, or development of new customer service opportunities cannot be controlled.

3) Because of the inability to integrate specific "new" and legacy applications, specific long-term applications development will need to maintained.

4) Long-term applications development effort could, at any period of time, change systems development specific life cycle effects.

5) Because of simultaneous and segmented development efforts, any changes introduced into the new system will affect all other applications that are dependent on that system. This effect should be minimized by employing a constant process and project review effort.

6) Systems cutover will be from the bottom up, and all functional applications cutover will be a piloted effort rather than a "hot cut approach."

CHAPTER 4

4.1 PROPOSED NETWORK TECHNICAL ARCHITECTURE:

4.1.1 DESIGN METHODOLOGY

At this time, designing an effective network requires many disciplines and foci. LANs, WANs and MANs each require unique efforts in design and balance. Some LAN and MAN information will need to be included for the sake of continuity and clarity, but design and integration of the three different network types will not be addressed in this chapter or the remainder of this project. The designs issues, functions and actions stated in this chapter and the remainder of this project will focus upon and affect only the WAN broadband portion of the IRS network re-engineering effort.

It is assumed that the reader has a base knowledge of LAN, MAN, and WAN networking technology andTherefore this paper will forego the effort of explaining the basic technology for the following sections. Technology identification and applicable standards will be injected as needed.

A. Networks as Objects

Upon completion of the requirements and systems analysis described in Chapters 2 and 3, a physical network design was developed and recommended. This effort ensured that the proposed physical architecture design addressed all of the documented requirements. The physical design method was deemed necessary to show the subtle and different technical design considerations between systems level and physical level architectures. The Object Oriented Design (OOD) approach will be used for the proposed network architecture. The following are some properties of the OOD:

1) "The Object Concept is that objects (no matter what you define an object to be) have a permanence and identity apart from any operation upon them."[4]

2) Objects are seen as an integral entity that:

- dynamically states conditions,
- behave in certain discernable ways,
- are manipulated by various form of stimuli both internal and external to the object,
- have a defined stand (interface) in relation to other objects,
- have enough identity to allow the object to function normally under both a stand alone condition as well as part of a larger system without any loss of original processing or functional intent, and
- are literal and do not consider attributes such as time, cosmetics, or emotions.

---

[4] Grady Booch, Object Oriented Design, 1991, page 77

3) Objects are also:

- Tangible with boundaries that may or may not be well defined.
- Entities that must communicate and collaborate with other entities to provide some higher level functionality.

The OOD approach was used in relation to the IRS network development because it takes into account all of the conditions under which a network must perform. OOD provides the ability to treat each network as an object. This enables the object to have a reusable base design that provides for tuning the network object as needed for a specific application. Also the OOD ensbles the designers to modularize, see Figure 9, the design. So if any section needs to be changed, tuned, or removed, it will not impact the overall system. For example:

1) Networks are designed to be dynamic. Traffic patterns are an unknown variables that can be "best-guessed" but not pinpointed. The state or usage condition of the network at any one moment in time can never be accurately forecast. They should be designed with the worst case traffic pattern scenario being the major consideration.

2) Networks can be designed to be application specific, or support a wide range of applications. This consideration allows the network to be designed and operated in a specific predetermined way and with the focus on supporting it main commitment.

3) Specifically designed networks can respond to outside traffic, inside traffic, can dynamically add bandwidth if the current traffic demands are overwhelming, and can restrict traffic to only specific areas or users.

4) Network objects can be defined to be relational to other objects (network). Networks can be designed to function as hierarchical, peer to peer, stand alone, terminators, carriers, or just message passers. Add the security issue into the network design and the network can now take on the encryption characteristic and become a type of traffic filter[5].

In order for the entire network system to be properly designed, the system must be disassembled into identifiable pieces and designed from both LAN into WAN and WAN into LAN so that both types of networks can be integrated smoothly. This is known as network segmentation. Once the traffic and usage patterns have been identified, it will then be determined where the traffic needs to go and how it should get there. Then the design will be segmented to show the terminating networks and all of the interconnecting networks which provide routing capabilities and options and make them available to the traffic engineering and control systems, please refer to Figure 9.

Once the basic network layers have been laid out according to their traffic load potential and analyzed for possible traffic patterns, the hard work of developing possible traffic routing schemes begins.

B. Broadband Design Considerations:

During the course of this project, the IRS has determined and informed the author that all WAN and broadband design efforts will involve and focus upon ATM and Frame Relay. Considering this decision, background information addressing ATM design considerations will need to be briefly explained. Technology may change, but the basic principles do not and must always be reviewed when attempting new efforts.

---

[5] Darren L. Spohn, Data Network Design, 1994, page 675

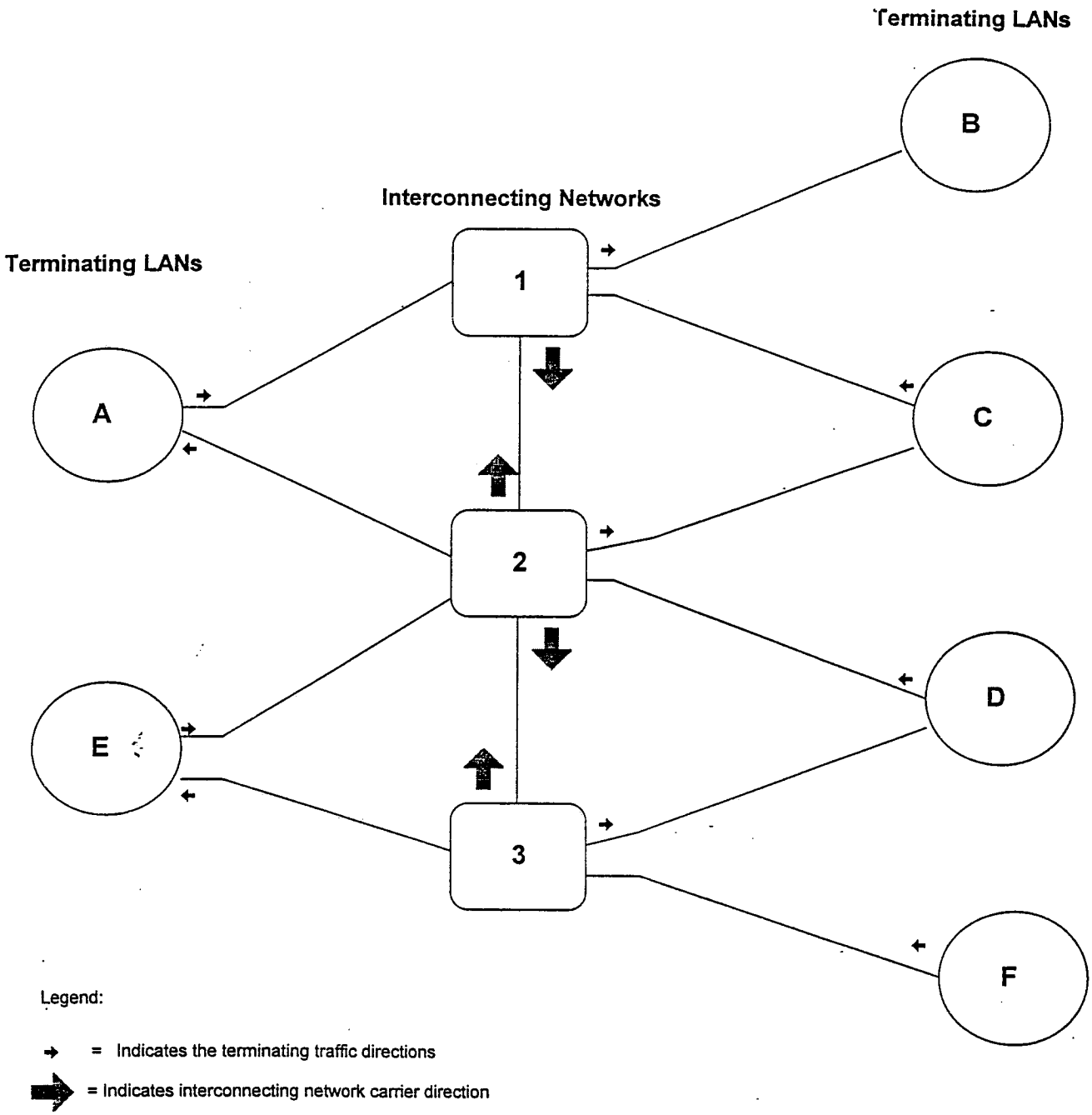


Figure 9 Basic Segmented Network Design

Figure 9. Basic Segmented Network Design

In the broadband communications (Backbone Network [BBN]) network environment, users expect everything to be perfect. There should be zero downtime, zero percent blocking, and unlimited bandwidth to handle all of the traffic all of the time. Users expect this from the backbone network. ***Acceptance of this ideology is expensive and unrealistic.*** Therefore the object of the BBN is to achieve a balance between network cost and availability.

When compared to local area and access networks, the BBNs provide a much more efficient and cost-effective link by using and providing some of the same key services over a much broader area. Some of these specific services are:

1) intelligent network services,
2) dynamic bandwidth allocation,
3) distributed network management,
4) redundancy and route protection,
5) efficient utilization of resources,
6) efficient economics of scale, and
7) advanced technology integration.

By categorizing network requirements into four basic categories, the IRS was able to provide a balance point for their BBN ideology. These four areas are:

1) interfaces,
2) protocols,
3) architectures, and
4) features, functions and services.

1) Interfaces:

Interface integration within any BBN should always be standards-based. To make the cost of the BBN as reasonable as possible, the IRS is planning on integrating and utilizing as much of the backbone in its everyday operations as possible. This means that a variety of transport protocols will be mapped to the BBN. These protocols will include but not be limited to:

- ISDN.
- BISDN[6] (includes ATM, plus PCM voice and LAPD [Link Access Procedure on "D" channel]).
- 24 DS0 carriers.
- 1.544 DS1.

[6] ISDN, BISDN, and Frame Relay and ATM, William Stallings, Prentice Hall, 1995, Page 436.

- ATM at 40 Mbps (DS3).
- Optical Carrier speed of at least 155 Mbps.

Also, because of the simple, unintelligent push of data traffic on the BBN, a function of the BBN switching and/or terminating equipment will be to identify the appropriate protocol for the transported traffic.

2) Protocol:

Even though access to the BBN consists of various protocols, such as X.25, SMDS, and/or Frame relay, all must be mapped to a common BBN protocol. The IRS is under two mandates when considering BBN protocol adaption. First, as a part of the federal government, the IRS is directed to provide a certain amount of its public traffic to the FTS 2000 contract. This contract is a general government contract where the Federal Telephones Services Division must provide a good percentage of its non-sensitive carrier and switched services. Therefore the IRS needs to ensure that the BBN is adapting to a SONET/SDH type of transmission protocol. Second, for the switched data traffic, the Frame Relay, ATM, or X.25 must be used. In the case of pure connection-less data networks, the government mandate for GOSIP and POSIX cannot be implemented. The IRS, therefore, is using TCP/IP as an interim transition protocol to the GOSIP and POSIX standards.

3) Architecture:

Because of the regulatory issues involved in new communications architecture development, backbone architecture development has always been ahead of access architecture development in the terms of technology, features, and services provided the end-user.[7] Because the IRS, as well as other major users, believe the BBN should provide numerous advantages to the end user at minimal cost, the BBN architecture must always improve and look for cost cutting alternatives. This means that when the BBN design is complete, the cost must balance the effect of the design and provide as much "bang for the dollar" as possible.

4) Features, Functions and Services:

The features, functions, and service that the BBN provides must vary with the type of technology supported. The IRS has selected an ATM-based technology because of its unlimited growth potential. Because ATM is mappable to equivalent OSI stack layers, it has the ability to support all types of transport interfaces and is, therefore, tunable in the type of features, functions, and services provided to the IRS end users[8].

C. Traffic Engineering

Network traffic comes in many shapes and sizes, conforms to many protocols and formats, travels in many types of patterns, and requires special methods of processing and handling. Traffic cannot be specifically predicted, but can be reasonably assessed. A number of questions and validation efforts must be in place

---

[7] Broadband Communications, B. Kumar. McGraw-Hill, 1994, page 392

[8] ATM, M. DePrycked, Horwood Series, 1993, page 112.

to ensure that the network is handling as much traffic information as is possible during the course of the network design. The IRS, as stated in the previous chapters, has a wide spectrum of traffic patterns and those patterns are dependent on, but not limited to the following:

1) time of year;
2) current or long-term investigation or accounting efforts;
3) processing growth requirements;
4) new technology directions;
5) growth in the user base;
6) new application development; and
7) daily work time patterns,
   a) peak hours/traffic hours,
   b) specific hours of bulk data transfer, and
   c) random time but predictable averages.

Once the tangible numbers are known, based on the above criteria and Table 2 (see Chapter 2), an analysis should be developed between the current operating network and the proposed new network. This effort will allow properly informed decisions for the procurement of network equipment, transport facilities, access capabilities, capacity planning, performance measurements, and network management efforts.

Traffic engineering in the BBN area is very complicated. It must take into account specific design conditions such as traffic segmentation (explained above) and traffic source (to be explained below). For example, if the BBN access speeds are very high, a failure in the link can cause immense damage to the IRS. Thus as a basic part of the network design, the general traffic patterns, should be split between two BBN access controllers. This will eliminate the condition known as "single point of access failure" which can result in traffic loss[9].

Traffic Source:

Since the primary function of the BBN is to interconnect access or LAN systems, most of the traffic comes from access networks. Data traffic is generated by nodes on the access network connected to the BBN. This design aspect generated IRS specific problems.

1) Because of the operational autonomy of the various divisions of the IRS, no solid information on traffic or traffic patterns could be developed.

2) This prohibits identifying the amounts, patterns and destinations of the transported data. Different types of data have different types of traffic patterns.

3) In order to provide a "starting point" on pattern determination, the IRS provided some past project network traffic parameters. Upon evaluating these parameters, the instruction was to expand on those numbers utilizing the files identified in Table 2. It was then determined that the consolidated information should be used to generate an 80% traffic load and bandwidth usage pattern.

---

[9]ATM, D. McDysan / D. Spohn, McGraw-Hill, 1994, page 456

With this generic approach the ability to developed a best "first guess" effor was realized. Another approach used is known as the "gravity method"[10]. This methodology is based on the assumption that each node, regardless of application, receives the same amount of data it transmits, as a starting point, over a specified time period.

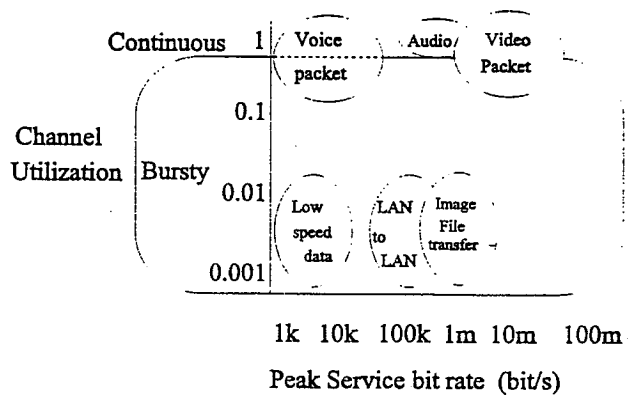
This approach gives the worst case scenario as the traffic between each pair of nodes in the network for a specific amount of time thus allowing enough information to start a preliminary design effort that will provide baseline information for establishing the base Quality of Services parameters such as:

- **Propagation Delay**: Dependant upon the time traffic resides on the network en route to its destination, thus providing an element for the determination of long-term traffic patterns.

- **User Response Time:** The time which is related to traffic pattern verses available network resources.

D) Traffic Engineering with Multimedia Considerations:

Traffic engineering takes on a whole new philosophical approach when the considerations of multimedia traffic[11] are taken into account. The services supported by a fully evolved multimedia network, which is what the IRS expects to develop, can be expected to produce a wide range of traffic flow characteristics. Controlling the channel utilization and determining the robustness of the base network is the first step in traffic management on a ATM multimedia based network, refer to Graph 1.



Graph 1. Multimedia Traffic Characteristics.

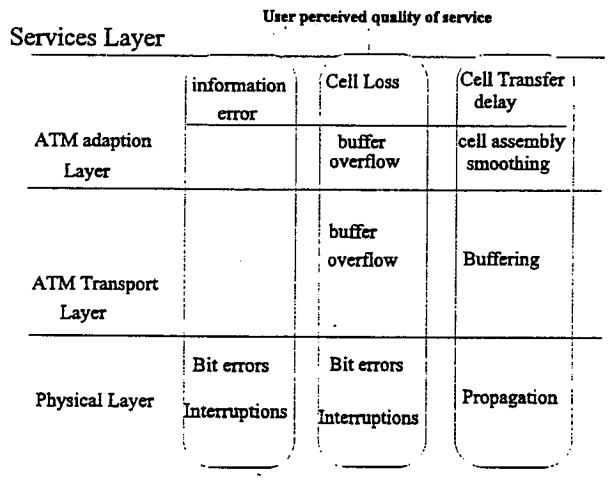
Graph 1 provides some of the rough ranges of the maximum bit rate and the utilization of a channel at this rate for some of the general service categories. With ATM as the integrated BBN transport network, an

---

[10] Broadband Communications, B. Kumar, McGraw Hill, 1994, page 394.

[11] Multimedia traffic management principals for guaranteed ATM network performance, GM Woodruff and R Kositpaiboon, IEEE journal on selected areas in communications, Vol. 8 April 1993

ATM adaption function is required to assemble the traffic flow from an originating user terminal, or end system, into fixed length cells with the assigned Virtual Channel Identifier (VCI). At the receiving end, cells must be disassembled for packet orientated service. Packets are reassembled for isochronous or constant bit rate (CBR) services, such as voice. Cells must be smoothed by the buffering as they may experience variable transfer delay across the network due to buffering at multiplexers and switches. Graph 2 displays the functions and their associated layers.



Graph 2. Layered view of ATM Performance Impairments.

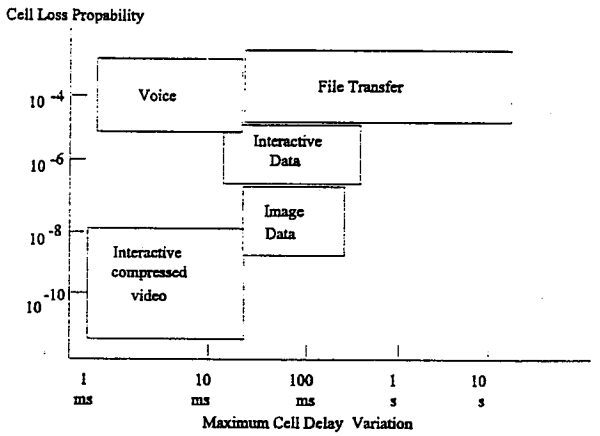
ATM impairments can be classified into three types:

1) Information error within the cell. Information errors can be caused by physical layer bit error and interruptions.

2) Cell loss:
   a) uncorrectable bit errors in the header,
   b) buffer overflow/overload at multiplexing or switching nodes, or
   c) adaption layer smoothing overflow.

3) Cell transfer delay:
   a) physical propagation delay,
   b) buffer overflow/overload at multiplexing or switching nodes, or
   c) adaption layer cell assembly and smoothing buffer delay.

This performance framework can be translated as both a user quality of service and requirements compliance issue. In engineering traffic patterns and in developing a management plan, which incorporates various aspects of traffic engineering versus quality of service, we will finalize this effort with an analysis of cell loss probability. Various services which will be offered on the network can expect and will incorporate a certain amount of cell loss. These service areas cell loss proability ranges can be seen in Graph 3.



Graph 3. ATM Cell Loss Probability Ranges.

As depicted in Graph 3, the ranges of cell loss among the services are wide. Isochronous and interactive services will have the most stringent delay requirements. Image and compressed video applications may have stringent loss requirements, and certain data applications may neither be delay or loss sensitive. The actual values of the requirements are dependant on the propagation delay, type of coding scheme, adaption method, subjective testing, and analysis scale used as well as other issues not considered relevant to this research.

E. Routing

Routing is defined as a network layer protocol that identifies networks paths that allow the traffic packets to get from the source to the destination through one or more sub or interconnecting networks (Figure 10). This requires that all of the subnetworks "know" and cooperate with each other, and that the chosen routing scheme also be responsive to link and node failures as well as sub or interconnecting network congestion. The IRS believes that the most efficient traffic routes should be designed initially and "tuned" as necessary.

The main functions of routing are the selection of the source, destination path, and the responsibility of packet delivery along the chosen path. The ultimate measurement of performance in a routing scheme is the Quality of Service or QoS factor. This factor is based on packet throughput (packets-per-second) and packet delay (average vs. maximum).

During the course of network routing development the following questions must be addressed.

1) In this particular system is routing necessary?

When you provide connectivity to both co-located intra-connecting networks and non-co-located inter-connecting networks, there will always be multiple transmission paths. Thus, the approach to designing co-located network routing vs. non-co-located network routing must consider different criteria.

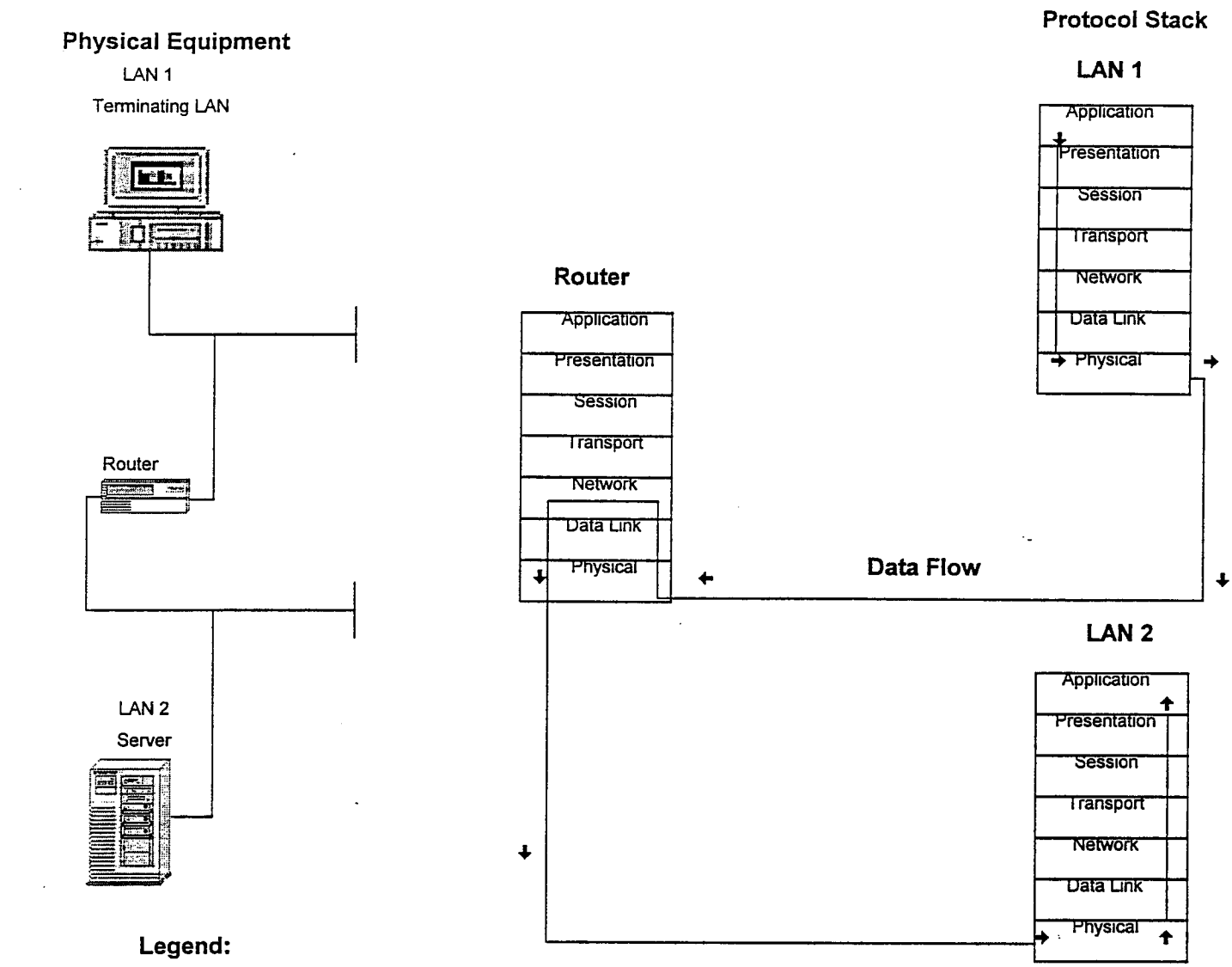
Isolated LANS are usually stand alone, application specific networks supporting specific individual departments. Their sole purpose is to provide local server or application services to the local users. These systems are usually located in a small to medium physical location and administered locally, refer to Figure 11.

Co-located LANS are usually interconnected with some type of singular or multiple high speed support networks. This support network's sole purpose is to connect all of the isolated local networks and provide a dynamic routing path capability for the passage of traffic packet, refer to Figure 12 .

In a multiple, non-collocated network environment, interconnecting bandwidth is critical and can, with modern network technology such as ATM or SONET, dynamically grow as the traffic demands increase, but this approach is very expensive.

Even the IRS, one of the largest accounting organizations in the world, is not immune to system operating costs. The IRS employs operations branches in various locations throughout the country and has the requirement to pass data to each of these locations. Routing is seen as critical function in order to establish operational efficiency while promoting cost savings,

Part of the network analyzing effort will be to determine which is the most efficient routing philosophy and how to apply it to the new network environment.



Legend:

1) Operates at OSI network Layer

2) Logically seperates networks

3) Dependant upon network layer protocol

4) Must obtain knowlwdge of network topology

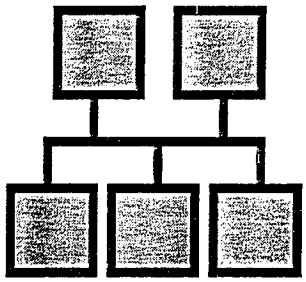
5) Main source of internetwork communications capability

6) Arrows indicated data flow for above example.
Normal traffic is bi-directional

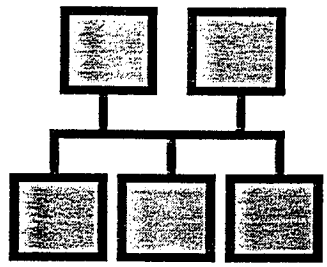
Figure 10 Basic Routing Protocol Adaption

Figure 10. Basic Routing Protocol Adaption.

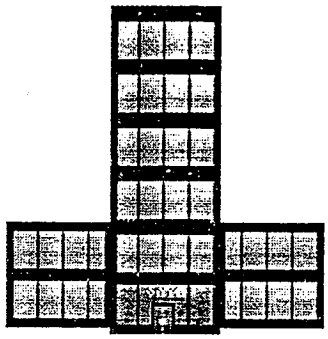
3th floor Financial Investigation Services



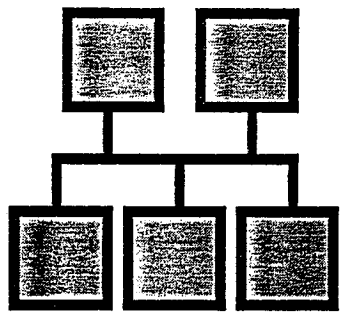
4th floor General Personnel services



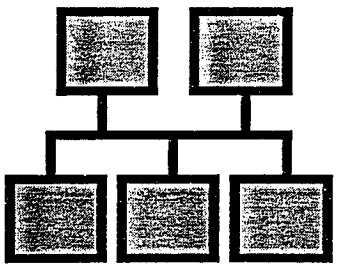
IRS Service Center



1st floor Building Maintenence Systems



2nd floor General Accounting Systems



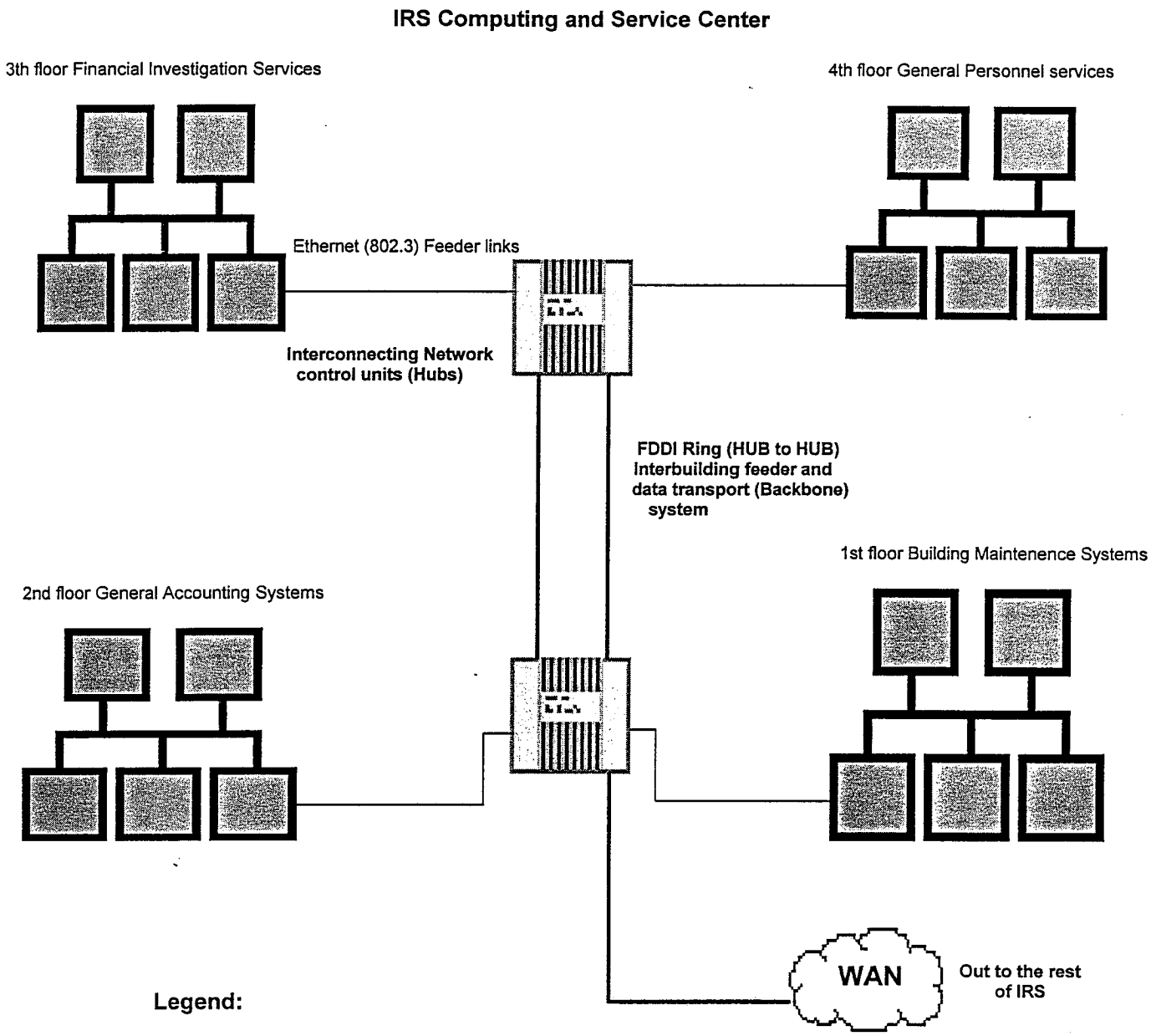
Legend:

All systems shown are standards based 802.3 systems, serving a specific application for a specific department or location.

No interconnection is needed for the individual systems to handle the specific application

Figure 11 Isolated / Co-Located LANs

Figure 11. Isolated/Co-located LANs.



Legend:

All systems shown are standards based 802.3 systems, serving a specific application for a specific department or location.

All locations show interconnection capability, Routing functionality is internal to Hubs

Figure 12 Non-Isolated / Co-Located LANs

2

Figure 12. Non-isolated/Co-located LANs.

) Who will make the routing decisions?

a) Usually, the first layer routing table decisions are made by the system management team which consists of both the system engineer and system administrator. They, as a team, will determine some of the basic routing choices based on the category of traffic and the need to accommodate user QoS requirements. After the basic choices are completed, the system, through the use of system software, will assume control and determine the best routing choice based on a comparison of the routing tables and the operational condition of the interconnecting links.

3) When are the routing decisions made?

a) Routing decisions are dynamically made at the time of need. This decision takes into account the type of transport, Datagram or Virtual Circuit, of the network system.

1) Datagram Routing[12]: in this type of routing, known as ARPANET routing, the links are constantly monitored, typed, and measured by the amount of congestion on that particular link. This information is constantly updated and refreshed for a packet-by-packet analysis of each available route.

This style of routing has inherent usage issues. First, this technique may allow any two consecutive packets in a data stream to use totally different links in order to get to the same destination. This may place the packets in an "out of order" sequence at the destination. It would then be up to the transport layer of the OSI 7 Layer model to place the packets back into sequential order for usage.

The second issue with this style of routing is the algorithms oscillations phenomenon. Thus, selecting routes through one area of the network increase the lengths of the corresponding links. As a result, at the next routing update the algorithm tends to select routes through different areas. This results in making the first area the most desirable at the subsequent routing update, with an oscillation resulting.

The first Datagram/ARPANET routing algorithm was based on a time delay of 625 msec, utilizing the Bellman-Ford method:

$$Di := \min_{j}[dij + Dj]$$

Di - shortest distance estimate
I - given node destination
dij - link length
i,j - queue of link at time of update

Therefore, link lengths were changing very rapidly, reflecting statistical traffic fluctuations as well as the effect of routing updates. To overcome this problem and stabilize the system, a large positive constant was added to link length. This resulted in the Shortest Path First (SPF) algorithm. This system kept track of

[12]Data Networks, D. Bertsekas/R. Gallager, 1992, Prentess-Hall p.374.

all of the lengths by recording packet travel times across each path and updating the delay of the paths every 10 seconds. In addition, each node monitors its own outgoing links and broadcasts these times to the networks every 60 seconds. Upon receipt of this information, every node recalculates the shortest path to each node using a form of Dijkstra's routing algorithm:[13]

$$0)P=1;D1=0;Di=di1;\square\square 1$$

1) Find I ¢ P such that $Di = \min_{j \text{ ¢ } P} Dj$
and add I to P
check: does P contain N nodes
Yes=>Stop; No=>Goto step 2.
2) For all j/p, update
$Dj = \min\{Dj, dji+Di\}$
Then goto Step 1
<u>*Fact*</u> *N-1 Iterations;*
Number of operations proportional to N^2;
{Di} at terminations are correct.

2) Virtual Circuit Routing (VCR):[14] store-and-forward switching in which a particular path is set up when a session is initiated and is maintained during the life of that session. This is like circuit switching in the sense of using a fixed path, but is virtual in the sense that the capacity of each link is shared by the sessions using that link on demand basis rather than by fixed allocations. Also, at times a user priority must be set to ensure proper utilization of the established circuit.

A) For ATM, VCR involves the establishment of virtual paths using Virtual Path Identifiers (VPI) and VCI multiplexed over a physical circuit between one or more switches. VPI and VCI are switch-to-switch based identifiers and values and can change as traffic passes through each switch. Not end-to-end values.

B) For X.25, VCR is physically built between end-to-end, and only one user at a time can be placed on each virtual circuit. Once the transmission is complete, the virtual circuit is removed.

Note: In both transport situations, error correction and flow control are optional.

For some of the IRS networks that will continue to use X.25 switch services, the virtual circuit routing will consist of two parts.[15] First select a route when the virtual circuit is being initiated, and second, ensure that each packet of the session follows the assigned route. Generally, in both

---

[13]CSE 632 Auburn University Computer Science and Engineering Networks Class, Dr. L. Murphy.

[14]X.25 and Related Protocols, Uyless Black, IEEE press, 1992.

[15]Data Networks, Bertsekas and Gallager, Prentice Hall, 1992.

ATM and X.25 user sessions, there is usually two separate virtual circuits carrying traffic in opposite directions, but not necessarily over the same links. The routing decisions are usually done separately, for each direction.

Virtual circuits have much in common with Datagram routing in that there is a cost function *Dij for each link (I, j)* that depends on the link flow. And additional parameters such as link capacity, processing and propagation delay, and a priority factor for the virtual circuits currently on the link.

If all of the virtual circuits have the same priority, the link cost function has the following form:

$$Dij(Fij) = \frac{Fij}{Cij\text{-}Fij} + dijFij$$

Dij - cost function per link
Fij - total data rate on the link
dij - is the processing and propagation delay
Cij - is the link capacity

When more than one priority (M) level exists for virtual circuits, the link cost function has the following form:

$$Dij\ (F(\hat{}1)ij.....F(\hat{}M)ij) = \sum_{k=1}^{M} PkF^{k}_{ij} \frac{1}{Cij - \sum^{M}_{K=1} F^{k}_{ij}} + dij$$

Fij = is the total link flow for virtual circuit of priority k
pk = is a positive weighting factor

Finally, any establishment of new virtual circuits is accomplished by assignment on a path that is shortest for the corresponding circuit. This path is calculated at the destination node of the virtual circuit on the basis of network topology and flow as well the most recently received parameters for each network link.

Upon completion of the traffic pattern determination and the establishment of a VPI/VCI path, the ATM/BBN traffic between two nodes can be established. For this link, between two distinct nodes, the calculation is fairly simple. However, the IRS networks as a whole are so complex that no two nodes are directly connected. This is because the traffic must pass through multiple hops and store and forward areas before it reaches its destination.

Refer to Figure 13 for further explanation:

Traffic Source

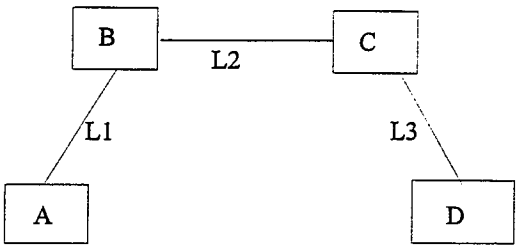


Figure 13. Traffic Matrix.

This network consists of four nodes and three links. For traffic to travel from node A to node D it must pass through all three links and nodes B and C. The traffic of L1 is :

Traffic in one direction = traffic (AD)

Traffic in other direction = traffic (DA) + traffic (BA) + traffic (CA)

Therefore the bandwidth size of link 1 should be based on the maximum of two directions. Also, for links 2 and 3, the total traffic in both directions of each link must be estimated and the link bandwidth should be the maximum of the traffic in two directions. When the suggested design for the IRS is submitted, all intermediate traffic must be taken in consideration. There should be sufficient bandwidth added to cover uncertainties and extra capacity designed in each link.

Routing in the ATM BBN depends on the type of algorithm employed. In ATM networks, most routing algorithms are based the ATM Forum's P-NNI Sub-Working Task Group's recommendation. This recommendation will incorporate currently accepted algorithms, such as those stated above, with some adaption for domain control and multilevel routing based on distance, cost, QoS, or a selected combination. The mid-point common carriers, such as AT&T, MCI, and US Sprint, continue to use the previously stated algorithms and have adapted these algorithms to their ATM service environment.

In privately controlled broadband routing, system administrators must contend with different types of routing environments. In dynamic routing, the routing decisions reflect the changes in the base traffic patterns. This is the "bandwidth on demand area." This seems to be best accomplished with a distributed routing algorithm using the dynamic routing philosophy. This type of algorithm requires the nodes to periodically exchange explicit routing information with each of its neighbors. Once this information is collected, the link sizes are calculated based on the loading factor for that particular time.[16] For this IRS

[16]Broadband Network Design, B. Kumar, McGraw Hill, 1994, p 396

effort it was assumed (because the industry standard traffic is assumed to be 80% of link capacity) that the links are never loaded more than 80% at peak traffic time (thus always maintaining a 20% loading factor). Therefore the link bandwidth in one direction (assuming the bandwidth is equal in both directions) can be given as:

$$\text{link bandwidth } (l_{i,j}) = \sum_{j=l,\, l=l}^{j=m,i,\, l=m} \text{point to point traffic from I to j} +$$

$$\text{transit traffic between I and j} + 20\% \text{ loading factor}$$

where

I, j = node on the network
$l_{i,j}$ = link between node I and j

Thus, total link capacities are obtained by summing all of the individual link capacities. Link capacity does not mean the total traffic traversing the network. Sufficient bandwidth must always be in reserve to handle uncertainties so that almost all traffic can be rerouted without bring down the network. Therefore, it can be established that unless the data is being transported over an isolated network, some type of routing will need to be in place. This will ensure that, whether the data is riding across the country or just within a specific building or environment, the data will utilize the most cost effective route available. Thus, ultimately supporting the overall QoS effort.

Finally, because of the connection orientated nature of ATM, routing brings an additional advantage with respect to security. By using specific call set-up procedures, security can be implemented on a per call basis as opposed to a per packet basis (users do not have to automatically access security resources). The network could intelligently determine which traffic should be passed upon to which transport resource based on source and destination identities. Furthermore, user authentication, which restricts users from having access to all or specified network services, can be implemented. The connection orientated ATM process ensures that traffic is only sent to the destination for which it was intended, there is no waste of transport resources with unnecessary broadcasts and thus no compromise of security. This type of behavior also eliminates the need for broadcast or protocol filters. In the long run, this will enhance overall system efficiency.

F. ATM Delay Variations

Delay on any BBN system impacts the overall QoS effort. Delays of any type prevent the system from delivering the requested information in a reliable and prompt manner. When the system is first designed, the focus should be on providing the best QoS possible. This involves providing enough bandwidth and paths to minimize the user-perceived delay. In an ATM environment this delay is called[17] Cell Delay Variations (CDV).

CDV is an ATM QoS parameter which measures the clumping that can occur when cells are multiplexed from multiple sources, originating in the system or at any switch, multiplexer, or intermediate system in

[17] ATM Theory and Applications, D. McDysan / D. Spohn, McGraw-Hill, 1994, p449

the network. This condition becomes critical when supporting delay sensitive applications such as video, audio, and interactive data. To accommodate for this condition, the ATM adaption Layer Type 1 (AAL1) will be used (bit rate does not vary over time). The term AAL1 fixed bit rate means that the bit rate of the traffic is both constant and synchronized between the sender and receiver. The AAL1 uses type 1 Protocol Data Units (PDUs) to support applications requiring a CBR transfer to and from the layer above the AAL. The IRS believes that this approach is a good start in establishing baseline operations. As the traffic changes, usage becomes more apparent and applications development becomes more pronounced. The IRS will review this and apply the AAL layer (such as layer 5) as needed.

The AAL1 is divided into two sublayers, convergence sublayer (CSL) and Segmentation and Reassembly sublayer (SAR). The CSL needs a clock to ensure system synchronization and, according to IEEE ATM standard I.363, obtains this clocking from multiple sources. CSL is responsible for the following :

1) Accommodating CDVs and delivering AAL-Service Data Units (SDUs) to the user at a constant bit rate.

2) Detecting lost or missequenced cells.

3) Providing source clock frequency recovery at the receiver.

4) Providing Forward Error Correction (FEC) on the user payload for specific clock applications.

5) Providing FEC on the AAL1 header.

Currently the CDV cannot be accurately captured or measured, therefore accommodations for the CDV must be estimated. The accumulation of CDV across multiple switching nodes can be approximated by the square root rule from the ATM Forum B-ICI specification. This states that the end-to-end CDV is approximately equal to the CDV for an individual switch multiplied by the square root of the number of switching nodes in the end-to-end connection.

No variation was added at the beginning per node because 1) extremes in variation are unlikely to occur simultaneously and 2) extremes tend to cancel each other out. In any steady state ATM transmission there is always a CVD delay. The delay per node varies. Some are high, others low. By looking at the probability distribution, the delay can assume certain values at various points along the network. Table 3, developed by Hughes ATM Systems, ATM Engineering Division, points out the specific QoS attibutes that cell delay and cell loss can affect in an ATM network

Table 3. ATM Link Performance Parameters.

Parameter	QoS Attribute
Cell Error Ratio	Accuracy
Severly Errored Cell Block Ratio	Accuracy
Cell Loss Ratio	Dependability
Cell Misinsertion Rate	Accuracy
Cell Transfer Delay (latency)	Speed
Cell Delay Variation (jitter)	Quality
Mean Cell Transfer Delay	Speed

A main consideration of network design is eliciting the desired network behavior as it operates under extreme adverse conditions. These conditions can be: significant system failure, traffic overload, or unexpected peak traffic patterns.

1) **Significant system failure**. Defined as loss of one or more critical trunks, paths and or switches in the system. In a private system this can be critical. The general rule is that no element can be isolated by a single trunk or switch. There should be the ability to run with a certain amount of loss from any private network. The public network is built to handle this situation. The most critical point where this rule applies is the local access area to the public network. There should always be redundant paths and multiple points of access to the public network.

2) **Traffic overloads**. In the ATM area the network marks excessive traffic for selective cell discard with those cells in excess of the base contract being discarded first. However, if the network is over booked with contracted traffic parameters this effort may not be sufficient, because congestion can drive a switch or multiple points in a network into overload, thereby reducing the traffic carrying capacity if congestion collapse occurs. In order to prevent this possible situation, the IRS had to develop and implement a mechanism to detect congestion, determine its cause, and provide the network management area some feedback in order for them to isolate the various traffic sources and achieve the required traffic balance. Part of this effort used both the Fast Resource Management (FMS) control area of the switch in conjunction with both the forward and backward explicit congestion notification (FECN/BECN), combined with the basic TCP/IP protocol stack's capability of asking for selective retransmissions of certain loss or out of order packets.

3) **Unexpected traffic patterns**. The IRS has already attempted to answer this question by applying two fundamental telecommunication approaches. The first being the bandwidth reservation concept and the second being fair allocation of shared resources. Current ATM Switched Virtual Channel (SVC) capability allows an application to request the network to reserve bandwidth for its exclusive use, somewhat similar to circuit switching. With the current SVC protocols, there is the need to break down the circuit and rebuilt it to add bandwidth. However, the new SVC protocol adaption will be able to add bandwidth on demand. In either scenario, the bandwidth will still need to be estimated. Another possibility is to use dynamic flow control, where feedback from the network, regarding congestion, is used to throttle back network bandwidth resources in a fair and equitable manner. Thus isolating applications and truly giving equal bandwidth where most needed.

G. Design Conclusions

In order to properly design and engineer a network, it requires more than equipment and connections. Solid engineering procedures and principals that will account for and analyze specific items in relation to the network in terms of normal operations and unexpected growth are required.

1) Network/Object identification: The isolated network as objects must be identified. Each with its own life and operation. Determining when, where, and how to interconnect them in the most beneficial and efficient manner as possible. This prevents distribution of local traffic, yet allows users to obtain outside services as needed.

2) Routing: Ensures that the traffic takes both the shortest and most cost effective path possible. Also, this ensures an equal distribution of traffic placed over multiple links, therefore removing

the possibility of single points of failure. This also enables the network to interconnect and efficiently route through various forms of carriers and includes quality in-depth traffic engineering to determine decisions on routing tables, backup route and over routing choices

3) Quality of Service: Requires understanding and estimating various forms of delay, such as traffic overload and pattern deviation delay, Cell Delay Variations, Cell switch stacking, and partial or overall system failure. QoS also looks at tuning the system with regard to customer requirements such as file transport schedules, response time, distributed file element consolidation, and proactive system development due to undefined growth.

QoS also accounts for and estimates overall system "UP TIME." Simply put, the customer is concerned only if the system goes down and how long will it be before the system is back in operation. This estimation takes into account system reliability and availability by estimating the following effects, Mean Time Between Failures (MTBF), Mean Time to Failure (MTTF), and Mean Time to Repair (MTTR).

The overall system reliability effect can be estimated as:

$$MTBF = MTTF + MTTR$$

And, the overall system availability effect can be estimated as:

$$\text{Availability} = \frac{MTTF}{(MTTF + MTTR)} \times 100\%$$

It is a common experience that once the base network is in place, the real applications development begins. New applications development puts strain on the network, which is then expanded and adds to the application demands, thus becoming a never ending cycle. Therefore, without taking into account the proper engineering steps stated above, you will never be able to address the needs of the customer by developing a network that is usable, flexible, and growth oriented.

4.2 IRS WAN NETWORK ARCHITECTURE

The proposed technical architecture is comprised of a multi-layer communications approach. The new communications will address several different conditions and accommodation of each condition. Map 2 shows the IRS Computing Centers locations reduction from ten to three.

1) Memphis, Tennessee
2) Detroit, Michigan
3) Martinsburg, Virginia

In conjunction with this reduction the IRS will reduce the number of Service Centers to five locations:

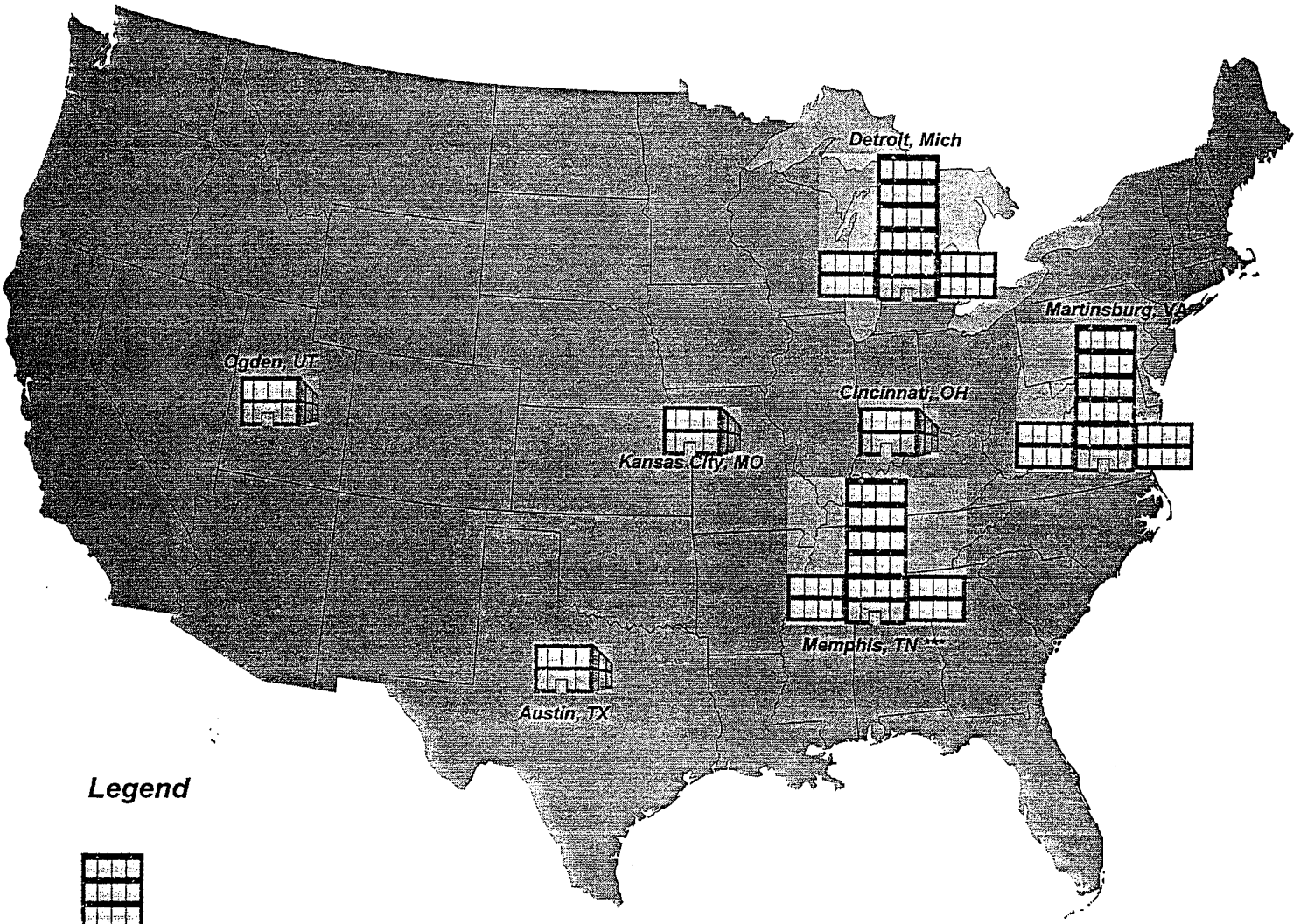
1) Ogden, Utah
2) Kansas City, Missouri
3) Austin, Texas
4) Memphis, Tennessee
5) Cincinnati, Ohio

These major locations will support the numerous of small administrative and investigation offices throughout the United States.

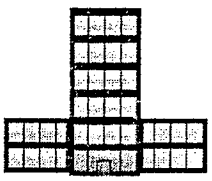
In order to address and support such a massive reduction in both office locations, personnel, and operational resources, many heterogeneous network configurations had to be investigated and implemented. Once in place, the different networks had to blend into one homogeneous network where data flowed form one technology-based topology to another without major problems. The proposed architecture had to be divided into four layers, with each layer having its own unique set of requirements. The four proposed network architecture layers are:

1) remote/on customer site access capabilities,
2) small or remote office locations,
3) customer service and large computing and archive centers.

In designing this architecture, all of the above design aspects were used which shows a logical hierarchey mapping to the communications infrastructure.



Legend



This denotes a Computing Center location.
24 hour a day operation.

This denotes a Service Center Location
12 to 18 hour a day operation

*** This denotes Memphis, TN as having
a combination Computing and Service center.
24 hour operation

Map 2 New Service and Computing Center Locations

Map 2. New Service and Computing Center Locations.

4.2.1 Remote/On customer site access capabilities:

The IRS, investigates and audits hundreds of private and commercial customers. Because of the magnitude of this effort, it is necessary for the IRS investigators to visit customer sites and inspect accounting records. Also, because of the new ideology of sharing information between government bureaus, law enforcement field activities may need to access IRS data records. With the issuance of both the GOSIP and POSIX mandates, the IRS has made major changes in their "Dial-Up" access capabilities. Refer to Figure 14 for further explanation.

The IRS has provided each investigative unit with the following technology: specially configured laptop computers with internal encryption modems each with their own unique encryption key. The laptops are also configured for TCP/IP utilizing either the Serial Line Interface Protocol (SLIP) or the Point-to-Point protocol (PPP). Each protocol extends the IRS internal Network to the dialed-in laptop and makes it look like a normal node with its own IP address and operational capability. This enables the error correction to be passed from the physical layer to a higher layer in the OSI stack and lets the session layer check packets and request only retransmissions of damaged packets.

The modems used, are outbound only and link the system together with line speeds of 28.8Kbps or, with compression,* speeds as high as 57.4kbps.

* **Note** Using compression with encryption is not considered highly reliable and is still viewed as a major research area. Therfore to reliably use the compression mode, the encryption capability must be terminated and dial in connections must be acheved through an alternative access point.

Once the user has dialed into the modem pool, where one access number might equal a hunt group of up to 24 modems, each with a 1-to-1 corresponding encryption device, the corresponding encryption device will inturn initiate multiple, simultanious functions. These functions are:

1) Connection to the modem and holding up the link with a DTR high.

2) Solicitation of the encryption key manager to check the validity of the user key.

3) If the key is not valid the encrypter will drop DTR and kill the connection.

4) If the key is valid, the the encryption unit will unencrypt the data and pass clear text to the host entry server, who will validate access capabilities and permission levels and also handle the first level of routing for the incoming data or service requests.

This sytem allows field personnel to maintain a dail-in priority list with alternative phone numbers into any service center or computing center as needed. The IRS has been selective about using ISDN as a standard for remote dial-in services, because only a percentage of the country's major metropolitan areas contain this capability. As ISDN grows then a review will be initiated.

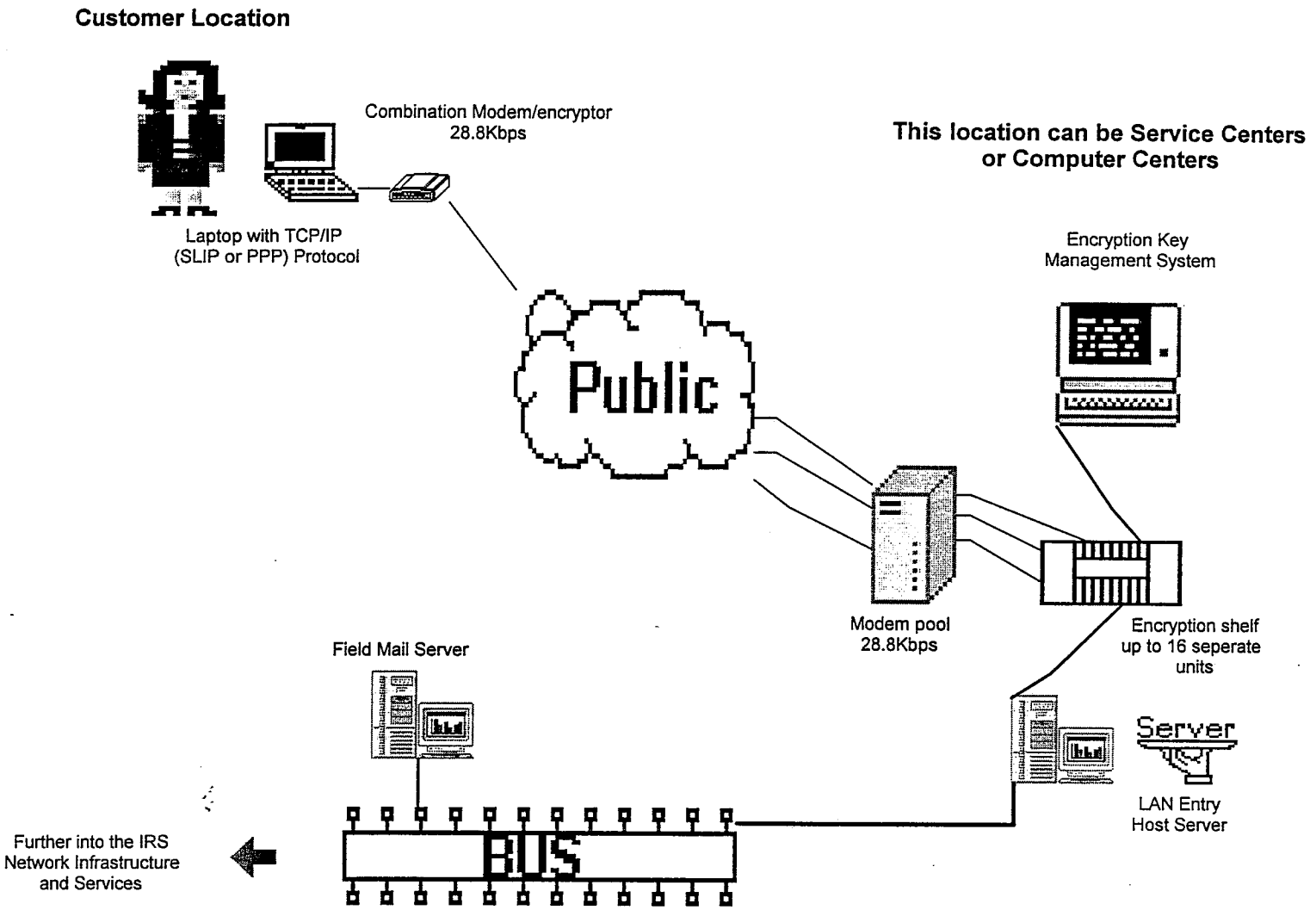


Figure 14 Remote / Customer Site Aceesss

4

Figure 14. Remote/Customer Site Access.

.2.2 Small office locations

These are the offices located off-site and provide service to the remote customer. The exact location of these offices has not been fully determined, but the basic configuration will show approximately 27 locations coast-to-coast, serving between 500 thousand and 1 million people per location. These offices will provide services such as forms, tax code clarification, general user direction and guidance, and a location for auditing purposes. Because the locations are still undetermined but basically known, we will show this architecture based on the four locations reflected in Figure 15. This will serve as a template for connecting the remaining locations.

Small office traffic will consist mainly of E-mail, minimal ad hoc reporting requirements, personnel issues, updating specific public information efforts, and daily office operation control systems. Therefore, the necessity for large bandwidth capability is minimal. The IRS elected to keep the switched transport capability in place for this office catagory. In keeping this transport capability in place, the costs are maintained at a low level, and data can be transport in a reliable manner.

TCP/IP-based LANs with X.25 WAN service is the technology employed at this level. Fast Packet transport was researched and also found to be favorable for this situation. However, not all of the preliminary locations have this type of service. A strong percentage of the preliminary locations do not even have ISDN. Therefore, the most common denominator had to be chosen and a migration path established.
The IRS understands the traditional approach to X.25 systems, with some of the main features being

1) Call control packets, used for setting and clearing virtual circuits, carried on the same channels as the data itself. Commonly known as in-band signalling

2) Multiplexing of virtual circuits is facilitated at layer 3 (X.25 packet layer), refer to Figure 16.

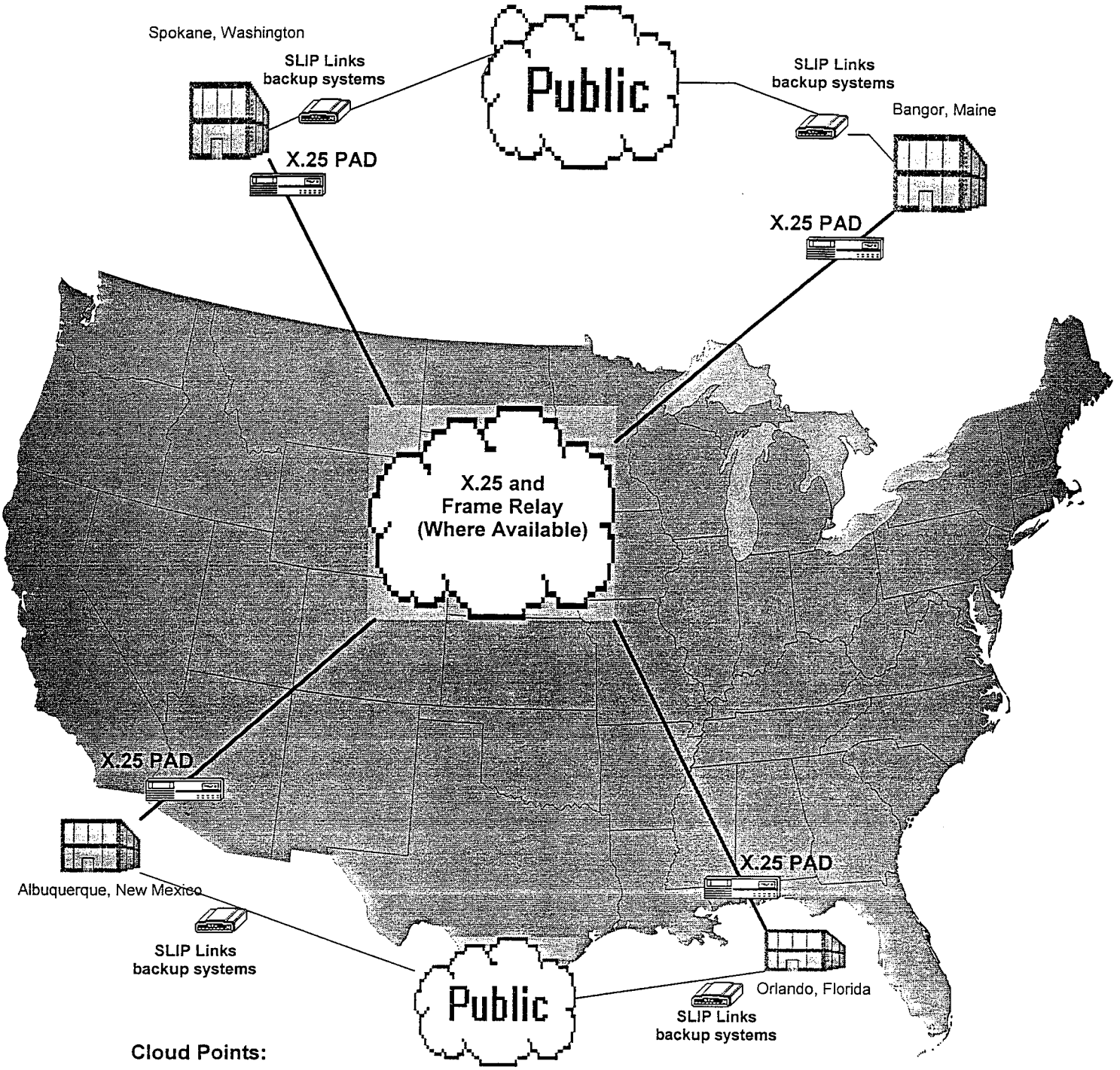
3) Referring to Figure 16, both layer 2 and layer 3 include flow control and error control capabilities.

All of the above combined with the base operational technology of X.25 will produce considerable overhead. Frame Relay is designed to eliminate, to the extent possible, the overhead employed by X.25 systems. It does this by employing some of these functions:

1) Call control signaling is carried on a separate logical connection (much like a SS7 signaling system) from the user data. This means the intermediate nodes need not maintain state tables or process messages relating to call control on an individual per call basis

2) Multiplexing is accomplished at layer 2 and not layer 3 which makes protocol processing more efficient.

3) There is no hop-to-hop flow control and error control. End-to-end flow control and error control are the responsibility of a higher layer. Frame Relay also has the option of not employing any error correction.



Cloud Points:

1) If there is only X.25, then the links are a maximum of 56Kbps.

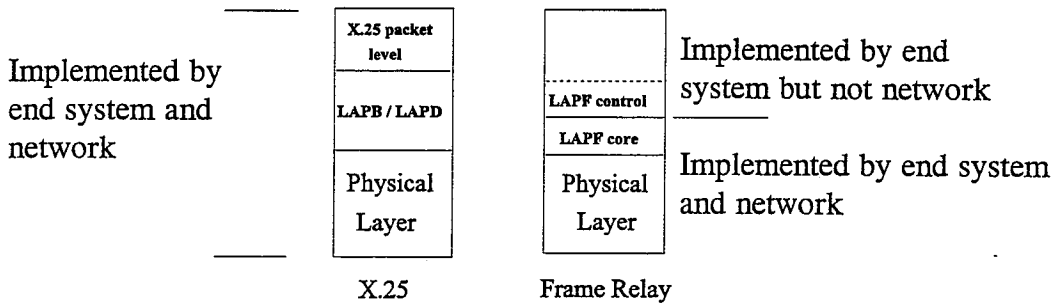
2) If there is Frame Relay then we can go as high as T-1 depending on the traffic and bandwidth demands

3) All backup/dial-up systems are 28.8Kbps

Figure 15 Small Office Locations Proposed Network

Figure 15. Small Office Locations Proposed Network.

Figure 16
X.25 / Frame Relay
Protocol Stack Comparison



It is understood that X.25, contains some of the same basic functions as and has a strong integration capability with Frame Relay. The following are some of these functions:

1) Flag Generation/recognition
2) Transparency
3) FCS generation/recognition
4) Recognition of invalid frames
5) Discarding of incorrect frames
6) Address translation
7) Fill interframe time
8) Multiplexing of logal channels

That is why Frame Relay for these offices will be the ultimate transport migration path, but will have to be accomplished as services become available in the selected areas.

The small office is also employing a form of dial back-up if the need to reroute traffic becomes an issue. This will be TCP/IP based SLIP or PPP controlled lines. The dialup patterns will show a first and second connection choice capability based on Service Center location and availability. These dialup lines can also be used to send bulk traffic or secure traffic that the IRS does not want transported over the public network.

The IRS views the small office location as a solid IRS presence to the general population. If any small office's area data traffic is overwhelming and the local public infrastructure maintains the technology to do so, the IRS system has the growth capbility to direct connect the system to that small office as needed.

4.2.3 Customer Service and Computing Centers

This area is the heart of the IRS WAN BBN network design effort. A strong integration and meshing of the different systems must be effected to ensure that availability and reliability percentages will be close to 100% 24 hours a day. In this area, the IRS will utilize a deployment of both ATM and Frame Relay capabilities that will ensure:

1) Multiple paths per location, keeping delay and congestion down and QoS high,

2) External access support for dial-in functions as required

3) Alternate path routing in the event of large carrier or service area loss.

4) Alternate path and optional routing for ad hoc large traffic demands or specific time of day service demands.

5) Intelligent ATM switching and trunking control capabilities able to handle different but simultaneous traffic classifications such as:

   a) Class A; CBR for connection oriented, synchronous traffic (i.e., compressed voice or video) for use with AAL1.

   b) Class B; Variable Bit Rate (VBR) for connection orientated, synchronous traffic (i.e., compressed voice and video) for use with AAL 2.

   c) Class C; VBR for connection oriented, asynchronous traffic (i.e.,TCP/IP, IPX, X.25, Frame Relay,) for use with AAL 5, AAL 3/4

   d) Class D; VBR for connection less asynchronous traffic, (i.e., broadcasting, multi-location one way video, SMDS service, large scale message handling) for use with AAL5.

   f) Class X; User definable no AAL specified

6) The use of intelligent ATM switching and access control Hubs that employ a multilayer switching fabric and highspeed backplanes that allow for integration and control of various protocols in one centralized location. The ATM switching area should focus on providing Multistage Interconnecting Networks (MIN) fabrics that are:

   a) Flexible and layered bxb switching elements that are traffic sensitive and have the ability to control deterministic and nondeterministic routing requirements.

   b) Solid and consistent enough to be the foundation for large scale chip integration. This would allow for ad hoc improvements and steady growth capabilities.

   c) Employ a self-routing property. This property would require Log(b)N digits to route a cell from input to output as fast and efficiently as possible.

      e) Finally, consist of multiple Log(b)N stages. With each stage having N/b basic switching elements. This would supply the ability to provide route choice to other carriers or the local MAN servicing multiple LAN environments with minimal switching delay.

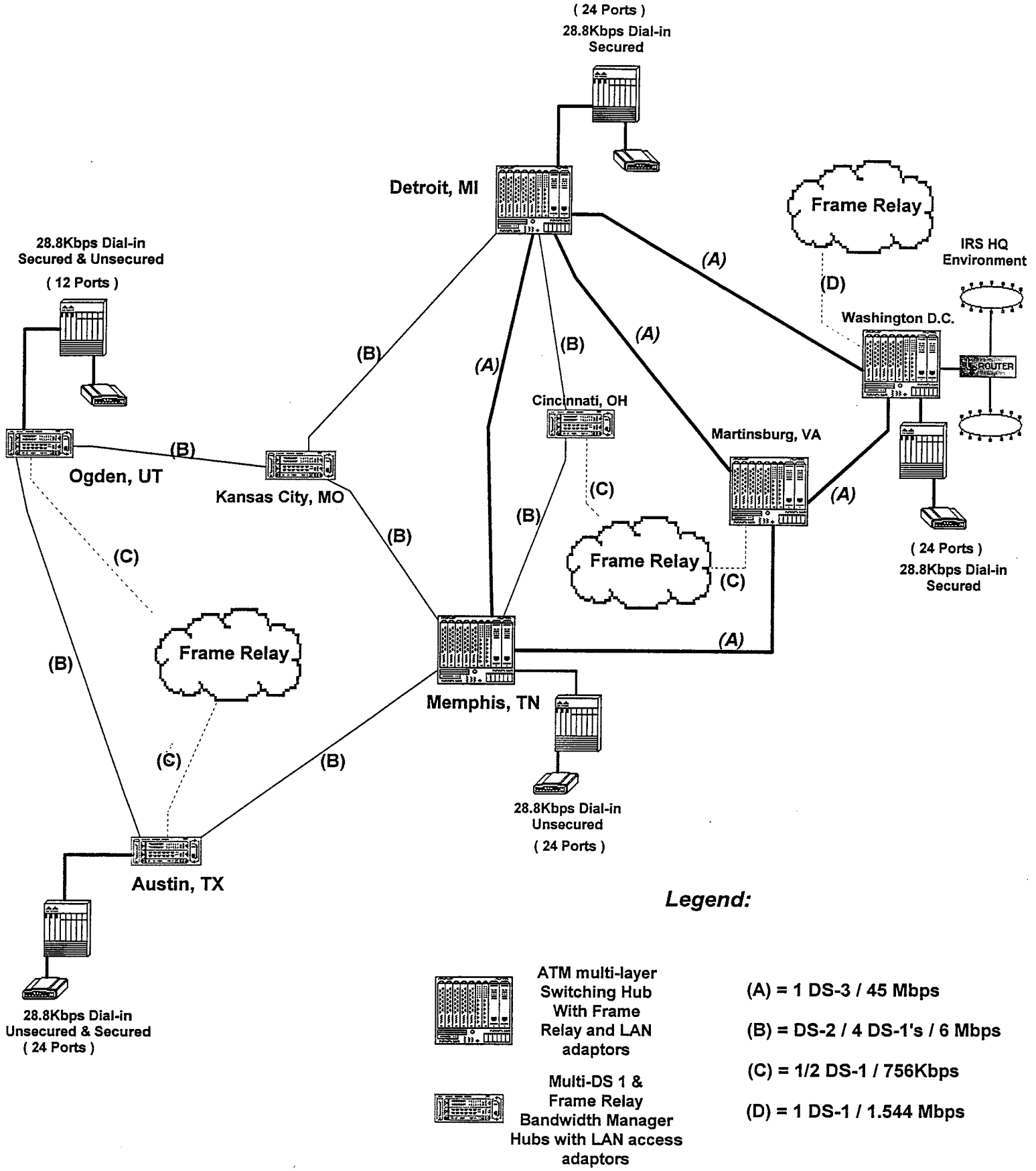


Figure 17 Proposed IRS Wide Area (WAN) Network Architecture

Figure 17. Proposed IRS Wide Area Network (WAN) Architecture.

Research has shown[18] that self-routing multilayer switching networks are very suitable for packet switching large applications because the routing functions to be performed are minimal and high speeds and low input/output queue times can be obtained. In addition, since MINs have the ability to allow cells to pass through its fabric in parallel, a reduction in cell loss will also be experienced.

Architecture Justification:

The following section will address the justification for the proposed architecture. The IRS consolidation will cause increased traffic flow, changes in operations, and uncertain growth patterns requiring this architecture to be considered an initial development for overall WAN communications systems.

In viewing the Computing Centers and their interaction requirements with the main headquarters, a triple triangle approach was adopted.

1) The first triangle was the Detroit-Martinsburg-Memphis topology. These areas are the achiving centers of the IRS and will also be the main tax systems processing areas. They will need to be constantly updating all of the "Mirrored" databases maintained by the IRS. It is believed, this required database reconsiliation could generate massive amounts of data and if not stringently scheduled, will originate more than enough traffic to cause a perceived slow down in services. Thus the bandwidth of the links between the switches will be 45 Mbps.

2) The second triangle is the Detroit-Washington-Martinsburg topology. This is justified by two conditions. First, the main headquarters for the IRS is in Washington, D.C. The local environment will employ a number of people in multiple office locations. Access to all of the IRS available information and services will be critical to this operation. Also, in this environment, adhoc requests for information from other agencies as well as the IRS will not be unusual. Therefore, we must provide the best service capability possible to satisfy ad hoc requests.

   Second, Martinsburg will be a major center of technology for multiple agencies of the federal government including: FBI, IRS, and Tresury Department, among others. Information pertaining to criminal investigations by various Agencies will be supported by this center. As in the first triangle, the requirement of service is regarded as being the top priority.

3) The third triangle is the Martinsburg-Detroit-Memphis topology. This ensures the database and archive validity by ensuring multiple routs to each location.

The Service Centers also have multiple path topology consisting of DS-2/4 DS-1/ 6Mbps links. Because the service centers will be supporting up to 27 local centers, no Service Center maintains less than two paths, as well as some type of backup capability. The five Centers have the ability to do multiple traffic path transport as a normal operation. Because of current and future growth support issues, each location employs a Bandwidth Management and Router system that can expand and add bandwidth as needed.

---

[18] ATM Research Solutions, Martin De Prycker, Ellis Horwood publishing, 1993

Should the centers located at Cincinnati, Ogden, and Austin lose their main two outbound carriers, a frame relay access has been established as an alternative to ensure minimal business as usual until the main systems recover.

The Frame relay capability consists of 1/2 DS-1/756Kbps links to a local frame relay switch. This service is provided by the government sponsored FTS 2000 contract, the routing will be controlled by the service provider of the FTS 2000 contract. In order to ensure efficency in this Frame relay environment, terminal switches have been established in both Martinsburg and Washington. This gives the frame realy traffic alternate paths so that the IRS traffic will not experience congestion at one location.

Multiple sites have also been selected to support the dial-up service requirement. This service will provide primary and alternate path support for the IRS dial-up requirements. The main locations will be 1-800 numbers routed to Memphis, for unsecured, and Detroit, for secured, dial-in access. For occasions when dial-up traffic is high, operating personnel are telecommuting, or emergeny situations require an alternate dial-in capability, systems have been established in the Ogden and Austin service centers.

Finally, for criminal investigations involving more than the IRS, or operations involving high level IRS management, a secured access for field support has been established in Washington, DC. Also not shown is the Internet access capability which will be established in both Washington, DC and Memphis, Tennessee. Memphis, Tennessee was chosen because it is both a combination Computing Center and Service Center, with an operational population larger than the other locations. However, with the alternate path capability, access to the Internet should not be an issue from any location.

All secure dial-in service will be inbound only and unsecured, dial-in will be full duplex service.

CONCLUSION

The IRS is currently undergoing a major modernization effort. This effort is focused on re-engineering all of the IRS Computing and Communications systems. Thus allowing the IRS to both upgrade all of the systems into a non-proprietary growth oriented environment, enhancing all provided public services, while initiating major reductions in both operating costs and possible personnel. This paper focused upon the Wide Area Network (WAN) portion of this modernization effort. It depicts the position of the IRS today verses their position in the future, and how they propose to accomplish this task.

REFERENCES

BOOKS

ATM: Foundation for Broadband Networks, Ulyess Black, Prentice Hall, 1995.

Data Networks, Bertsekas/Gallager, Prentice Hall, 1992.

X.25 and Related Protocols, Ulyess Black, IEEE Press, 1992.

ATM Switching Systems, Chen/Liu, Artech House, 1995.

Tele Traffic Technologies in ATM Networks, H. Saito, Artech House, 1993.

ATM: Performance Issues, R. O. Onvural, Artech House, 1993.

ATM: Theory and Application, McDysan/Spohn, McGraw-Hill, 1994.

Network Protocol Handbook, M. Naugle, McGraw-Hill, 1994.

Asynchronous Transfer Mode, M. De Prycker, Ellis-Norwood, 1993.

Broadband Communications, B. Kumar, McGraw-Hill, 1994.

Internetworking, M. Miller, MT Books, 1992.

ISDN and BISDN with Frame Relay and ATM, William Stallings, Prentice-Hall, 1995.

Data Network Design, D. L. Spohn, McGraw-Hill, 1993.

Inter Connections, Radia Perlman, Addison-Wesley, 1992.

Gigabit Networking, Graig Partridge, Addison-Wesley, 1993.

Telecom System Engineering, Roger Freeman, Wiley Press, 1990.

Telecom Transmission Engineering, Roger Freeman, Wiley Press, 1992.

Telecom Engineering Reference Manual, Roger Freeman, Wiley Press, 1993.

1st, 2nd, and Next Generation LANs, Daniel Minoli, McGraw-Hill, 1993

Systems Network Architecture, W. Schafer/H. Mgulen, Addison-Wesley, 1992.

Data Pro Reference Library, 1994.

TECHNICAL RESOURCES

"ATM Forum," Accessed through the Internet

TECHNICAL PAPERS

"ATM - Quarterly Standards," Hughes Network Systems.

"ATM Technology," Cabletron Systems.

"ATM Switching Systems," Fore Systems.

"ATM Technical Profile," Net Systems.

"Multimedia Traffic Management Principals for Guarenteed ATM Performance," Woodruff and Kositpaiboon, IEEE Journal, Vol. 8, April 1993.

BUSINESS AND SYSTEM INFORMATION

Internal Revenue Service TAX MOD 2000 Project Literature.