HICKLING

FEASIBILITY STUDY OF A NATIONAL HIGH SPEED COMMUNICATIONS NETWORK FOR RESEARCH, DEVELOPMENT AND EDUCATION

VOLUME C: TECHNICAL ANALYSIS

FEASIBILITY STUDY OF A NATIONAL HIGH SPEED COMMUNICATIONS NETWORK FOR RESEARCH, DEVELOPMENT AND EDUCATION

VOLUME C: TECHNICAL ANALYSIS

Submitted to:

INDUSTRY, SCIENCE AND TECHNOLOGY CANADA

Prepared by:

HICKLING
Science and Technology Division

and

COMGATE ENGINEERING ASSOCIATES LTD.

In association with:

THE ALBERTA RESEARCH COUNCIL

THE CGI GROUP

LANG MICHENER LAWRENCE & SHAW

HICKLING REF:3201
March, 1990

NOTE

This is Volume C of a study prepared by James F. Hickling Management Consultants Ltd. (HICKLING) on behalf of Industry Science and Technology Canada (ISTC), entitled "Feasibility Study of a High Speed Communications Network For Research, Development and Education". There are five volumes in this study:

1. Main Report
2. Volume A: Participant Needs
3. Volume B: Economic Analysis
4. Volume C: Technical Analysis
5. Volume D: Implementation Analysis

PREFACE

This study was commissioned by Industry, Science and Technology Canada to investigate the feasibility of establishing a National High–Speed Communications Network for the Canadian research, development and education communities. The network would have greater capacity and functionality than existing networks. While the undertaking of this study is not to be construed as a commitment by the federal government to the establishment of a network, the study will provide a solid basis for such an initiative should it be found prudent.

HICKLING is indebted to Dr. Digby Williams, Director of the Microelectronics Technology Office, and Mr. Joseph Padden, Senior Technologies Advisor for the Information Technologies Industry Branch, Industry, Science and Technology Canada, for their expert technical and managerial advice in the conduct of this study. The authors would also like to offer thanks to the more than 400 individuals who participated in expert panel sessions, in–person interviews, and surveys; the study would not have been possible without their input. Of course, any errors or omissions are the sole responsibility of HICKLING.

The report was authored by David Arthurs, Phil Kennis, and Daniel Hara of HICKLING; and Roger Choquette and Anthony Capel of COMGATE. Significant contributions were made by Dr. Saul Greenberg of the Alberta Research Council; Dr. Frederick Eshragh, Dr. Kalman Toth, and Dr. Samy Mahmoud of CGI; John Lawrence and Andree Wylie of Lang Michener Lawrence & Shaw; Elmer Hara of the University of Regina; and Fred Cassedai.

OVERVIEW

A number of technical issues were examined to provide background material for the *Feasibility Study for a High Speed National Research, Development and Education Network*. The sections in this volume are designed to provide background information in sufficient detail to permit the expected capabilities of the Network to be estimated and to allow preliminary cost estimates to be made. The sections explore feasible technical approaches for the Network. User needs, implementation and economic topics are discussed in separate documents.

These sections propose an example physical Network design only. The specific physical design can only be created when the participants in the Network have been identified and only after other Implementation and Policy issues have been resolved. Information generated as a result of these sections was used to brief potential Network participants during the study. These presentations highlighted the need to satisfy industrial as well as academic clients, and promoted the full support of ISO based protocols with a coexistence and a migration plan for TCP/IP. The general tone of the presentations followed the tone of these sections.

The ***Network Costs*** section reports on the estimated cost of implementing the Network. It addresses Network costs in terms of personnel, capital, installation, and annual operating costs over a five year period for three optional physical configurations. This section uses data transmission costs from the *Data Transmission Services* section and capital equipment costs and general Network physical architecture from the *Network Architecture and Migration Plan* section.

The ***Network Architecture and Migration Plan*** section proposes both logical and physical architectures for the Network. The section proposes that the Network objectives are best met by specifying an overall logical networking architecture which accommodates the interconnection of existing and future subnetworks following the OSI model. A general physical implementation is presented which accommodates growth in both user requirements and the underlying technologies.

The ***Data Transmission Services*** section surveys the wide area data transmission services offered by the common carriers and highlights the tariffs under which services may be offered to the Network.

The ***Impact of ISDN*** section reviews the evolving ISDN technologies to determine their impact on the Network. It concludes that the ISDN impact today is small, although access to the Network may ultimately be a valid user option and the Network may ultimately be used to facilitate ISDN research and development.

The ***Conformance and Protocol Test*** section discusses the need for protocol testing facilities and services. Testing will be required to assure that new equipment will not interfere with the ongoing operation of the Network. It also suggests that testing services offered by third parties should be offered over the Network.

The ***Network Management and Technical Centre*** section discusses the need for Network technical staffing. It is suggested that two main groups will be required. The network operations group should plan, acquire and maintain the ongoing operation of the Network and ensure that the policies of the Network owners are implemented. The second `informational' group would support the Network's clients, promote the Network and distribute technical information.

The *Network Addressing, Directory and Routing* section points out that the users and resources will need to be uniquely identified and that a service will be required to allow users to easily determine the resources available on the Network. It also discusses the need for a uniform Network Service.

The ***Protocols and Use of Standards*** section discusses the requirement for standards, and surveys those which are relevant to the Network. It discusses the support of ISO and TCP/IP based standards. It recommends full support for a North American ISO based standards profile with interim support for TCP/IP.

The *Low Cost Access Methods* section surveys methods for low cost access to the Network. This is considered essential to providing universality of access, especially access in remote regions of Canada and access from small users.

The ***High Speed Transmission Methods, Technology and Networking*** section discusses long distance transmission methods and switching approaches. This section concentrates on the existing and evolving technologies for transmission and switching, and discusses how these technological changes will impact the Network.

The *Network Security and Access Control* section discusses the issues that must be considered when planning for the Network. It points out that only minimal security is feasible for the basic Network and that suitable physical and personnel security plans will be required to provide this minimum level.

TABLE OF CONTENTS

PAGE

1. NETWORK COSTS

1.1 SUMMARY

The purpose of this section is to report on the estimated cost of implementing the Network. The section addresses the Network costs in terms of personnel, capital and installation and annual operating costs over a five year period for three optional Network physical configurations.

The three Network configuration options are:

1. **Terrestrial Backbone (Option I):**
   A terrestrial backbone initially configured with 22 nodes linked with 19 DS–1 and 3 DS–0 channels and upgraded to DS–3 links in year 4.

2. **Multi-Media Backbone (Option II):**
   Option I supplemented with a parallel satellite subnetwork initially configured with two nodes and upgraded to four in year 4.

3. **Multi-Access, Multi-Media Backbone (Option III):**
   Option II supplemented with 10 access nodes located outside the major urban areas with each access node linked to the backbone with 1 DS–0 channel with a doubling of the link capacity in year 4.

The cost estimates for the five year period range from $50.5 M for Option I to 57.9 M for Option III.

1.2 INTRODUCTION

The Network's budget has been constructed for a period of five years. The cost component of the budget, which is the subject of this section, will be an important determinant of initial funding requirements.

This part of the section introduces the cost components analyzed in the Study, follows with an introduction to the three Network physical configuration options used in the development of cost estimates and provides a summary of the cost results.

The remaining parts of the section address the three major cost classifications of personnel costs, capital and installation costs and annual operating costs for each of the Network configuration options.

1.2.1 Cost Components

The following cost components have been identified:

1. **Personnel Costs** which include

   a. Salaries and benefits of Network executive, managerial and staff personnel.
   b. The overhead costs associated with the Network personnel expressed as a percentage of salaries.
   c. The education and training of Network personnel.

2. **Capital & Installation Costs** which include

   a. The capital costs of Network nodes expressed in terms of Small Nodes, Large Nodes without Services and Large Nodes with Services[1]
   b. The installation costs of the Network channels
   c. The capital costs of equipment and software for the Network Management and Technical Centres.

3. **Annual Operating Costs** which include

   a. Channel rental costs.
   b. Connection charges to international networks.
   c. Equipment maintenance costs expressed as a percentage of capital costs.
   d. Costs associated with the development of Network services, as sponsored by the Network.
   e. Marketing costs for the development of the Network subscriber base
   f. Other operating costs including travel, printing, telephone, courier, etc...

1.2.2 Network Physical Configuration Options

The three Network physical configurations used for the development of cost estimates are:

Option I: **Terrestrial Backbone.** A terrestrial backbone initially configured with 22 nodes linked with 19 DS–1 and 3 DS–0 channels.

Option II: **Multi-Media Backbone.** Option I supplemented with a parallel satellite subnetwork.

Option III: **Multi-Access, Multi-Media Backbone.** Option II supplemented with 10 access nodes located outside the major urban areas and linked to

[1] See the Network Architecture and Migration Plan for details on the node configurations.

the terrestrial backbone with DS–0 channels.

1.2.3 Summary of Costs

Tables I, II and III summarise the cost results for each option. The remaining parts of the section detail the assumptions used in the development of the estimates for each of the cost categories under each option.

Table I: Network Costs, Option I – Terrestrial Backbone ($K)

Item	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Personnel						
Salaries & Benefits	1,290	1,497	1,687	1,771	1,859	8,104
Overhead	774	898	1,012	1,063	1,115	4,862
Education & Training	34	40	46	53	58	231
Total Personnel Costs	**2,098**	**2,435**	**2,745**	**2,887**	**3,032**	**13,197**
Capital & Installation						
Network Nodes	3,100	–	–	720	–	3,820
Installation, Channels	255	–	–	195	–	450
Tech/Management Centres	400	60	60	60	60	640
Total Capital & Installation	**3,755**	**60**	**60**	**975**	**60**	**4,910**
Annual Operating Costs						
Channel Rental	3,000	3,000	3,000	6,000	6,000	21,000
International Connections	600	600	600	1,200	1,200	4,200
Equipment Maintenance	350	350	360	380	400	1,840
Service Development	750	788	827	868	911	4,144
Marketing	100	105	110	116	122	553
Other Operating	100	120	138	145	150	653
Total Operating Costs	**4,900**	**4,963**	**5,035**	**8,709**	**8,783**	**32,390**
Total Expenditures	**10,753**	**7,458**	**7,840**	**12,571**	**11,875**	**50,497**

Table II: Network Costs, Option II - Multi-Media Backbone ($K)						
Item	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Personnel						
Salaries & Benefits	1,290	1,497	1,687	1,771	1,859	8,104
Overhead	774	898	1,012	1,063	1,115	4,862
Education & Training	34	40	46	53	58	231
Total Personnel Costs	**2,098**	**2,435**	**2,745**	**2,887**	**3,032**	**13,197**
Capital & Installation						
Network Nodes	3,100	–	–	720	–	3,820
Installation, Channels	305	–	–	270	–	575
Tech/Management Centres	400	60	60	60	60	640
Total Capital & Installation	**3,805**	**60**	**60**	**1,050**	**60**	**5,035**
Annual Operating Costs						
Channel Rental	3,350	3,350	3,350	7,400	7,400	24,850
International Connections	600	600	600	1,200	1,200	4,200
Equipment Maintenance	350	350	360	380	400	1,840
Service Development	750	788	827	868	911	4,144
Marketing	100	105	110	116	122	553
Other Operating	100	120	138	145	150	653
Total Operating Costs	**5,250**	**5,313**	**5,385**	**10,109**	**10,183**	**36,240**
Total Expenditures	**11,153**	**7,808**	**8,190**	**14,046**	**13,275**	**54,472**

Table III: Network Costs, Option III – Multi-Access/Multi-Media Backbone ($K)

Item	Year 1	Year 2	Year 3	Year 4	Year 5	Total
<u>Personnel</u>						
Salaries & Benefits	1,290	1,497	1,687	1,771	1,859	8,104
Overhead	774	898	1,012	1,063	1,115	4,862
Education & Training	34	40	46	53	58	231
Total Personnel Costs	**2,098**	**2,435**	**2,745**	**2,887**	**3,032**	**13,197**
<u>Capital & Installation</u>						
Network Nodes	4,100	–	–	970	–	5,070
Installation, Channels	398	–	–	363	–	761
Tech/Management Centres	400	60	60	60	60	640
Total Capital & Installation	**4,898**	**60**	**60**	**1,393**	**60**	**6,471**
<u>Annual Operating Costs</u>						
Channel Rental	3,550	3,550	3,550	7,800	7,800	26,250
International Connections	600	600	600	1,200	1,200	4,200
Equipment Maintenance	450	450	460	505	525	2,390
Service Development	750	788	827	868	911	4,144
Marketing	100	105	110	116	122	553
Other Operating	100	120	138	145	150	653
Total Operating Costs	**5,550**	**5,613**	**5,685**	**10,634**	**10,708**	**38,190**
Total Expenditures	**12,546**	**8,108**	**8,490**	**14,914**	**13,800**	**57,858**

1.3 PERSONNEL COSTS

1.3.1 Introduction

The following personnel cost estimates are provided for the years 1991 to 1995 inclusive:

a. Salaries and benefits of Network executive, managerial and staff personnel.
b. The overhead costs associated with the Network personnel expressed as a percentage of salaries.
c. The education and training of Network personnel.

It is anticipated that an Executive Director for the Network will be appointed by the Board of Directors and that he or she will be responsible for hiring staff necessary to fulfil to operate and manage the Network. Personnel costs are assumed to be identical for all three options.

1.3.2 Personnel Costs

Staffing in support of the Executive Director is outlined in Table IV.[2]

Personnel costs are outlined in Table V and were developed a follows:

a. Annual staff salaries including benefits:

* Executive Director:	$75,000
* Manager:	$65,000
* Staff Support:	$50,000
* Administrative Support:	$35,000

b. Staff overheads are assumed at 60% of the annual salary. Overhead includes office space.

c. Education and training is estimated at $2,000 per year per staff professional.

[2] See the Issue Paper on the Network Management and Technical Centre for a discussion of the functions associated with these staff positions.

Table IV : Personnel Staffing

Position	Number					
	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Executive Director	1	1	1	1	1	5
Planning and Acquisitions						
Manager	1	1	1	1	1	5
Staff Support	2	2	2	2	2	10
Maintenance & Operations						
Manager	1	1	1	1	1	5
Staff Support	5	6	6	6	6	29
Marketing & Service Dev.						
Manager	1	1	1	1	1	5
Staff Support	3	3	3	3	3	15
Client Services						
Manager	1	1	1	1	1	5
Staff Support	5	6	6	6	6	29
Finance & Admin.						
Manager	1	1	1	1	1	5
Admin. Support	4	5	8	8	8	33
Total	25	28	31	31	31	146

Table V: Personnel Costs ($K)

Item	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Executive Director	$75	79	83	87	91	$415
Managers	325	341	358	376	395	1,795
Staff Support	750	893	937	984	1,033	4,597
Admin. Support	140	184	309	324	340	1,297
Overhead (60%)	774	898	1,012	1,063	1,115	4,862
Education and Training	34	40	46	53	58	231
Total	2,098	2,435	2,745	2,887	3,032	13,197

1.4 CAPITAL AND INSTALLATION COSTS

1.4.1 Introduction

Capital & Installation Costs include

a. The capital costs of Network nodes.[3]
b. The installation costs of the Network channels
c. The capital costs of equipment and software for the Network Management and Technical Centres.

1.4.2 Capital and Installation Costs and the Network Options

The three Network physical configuration options have different capital and installation costs associated with the Network nodes and channels.

The capital costs associated with the Network Management and Technical Centres are identical for the three options and include the costs of the Network Emulation Facility as well as staff workstations, equipment and software required in addition to office equipment estimated as part of the staff overhead under personnel costs. These capital costs are estimated at $400,000 in year 1 ($250,000 for the Emulation Facility and $150,000 for the workstations and software), with annual additions of 15% of the original capital costs for the remaining four. These costs are included in each of the cost summaries for each of the three options.

[3] See the Network Architecture and Migration Plan for a discussion of the components associated with the three node configurations as well as the Network Emulation Facility.

The inflation factor of 5% is not applied to the cost estimates in this section as it is foreseen that market forces as well as technology improvements will tend to keep these costs relatively flat over the next five years.

1.4.3 Capital and Installation Costs – Option I

The cost estimates for Option I are based on the initial Network configuration and subsequent additions identified in Table VI. Node additions after year 1 reflect the enhancement of a node's functionality while the modernisation of nodes reflect the replacement of node routers with more capable ones.

Table VI: Network Configuration, Option I

Item	Additions (units)				
	Year 1	Year 2	Year 3	Year 4	Year 5
Small Nodes	8	–	–	–	–
Large Node without Services	10	–	–	–	–
Large Node with Services	4	–	–	2	–
Modernisation, Small	–	–	–	8	–
Modernisation, Large	–	–	–	8	–
Modernisation, Large with Services	–	–	–	6	–
Channels, DS–0	3	–	–	–	–
Channels, DS–1	19	–	–	–	–
Channel Upgrades to DS–1	–	–	–	2	–
Channel Upgrades to DS–3	–	–	–	19	–

Table VII translates the configuration of Table VI into Capital and Installation Costs. The capital costs of the nodes are derived from the unit cost estimates developed in the Network Architecture and Migration Plan. The channel installation costs are derived from the Data Communication Services Section which discussed the relevant carrier tariffs. The costs of the Technical and Management Centres are as previously discussed.

Table VII: Capital & Installation Costs, Option I

Item	Additions ($K)					
	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Small Nodes	800	–	–	–	–	800
Large Nodes without Services	1,500	–	–	–	–	1,500
Large Nodes with Services	800	–	–	100	–	900
Modernisation, Nodes	–	–	–	620	–	620
Installation, Channels[4]	255	–	–	195		450
Technical/Management Centres	400	60	60	60	60	640
Total Capital & Installation	3,755	60	60	975	60	4,910

1.4.4 Capital & Installation Costs - Option II

The cost estimates for Option II are based on the Network configuration of Option I (see Table VI), supplemented with a parallel satellite subnetwork initially encompassing two Network nodes (Montreal and Vancouver, with a Yellowknife–Vancouver link already included in Option I), and migrating to a 4 node subnetwork by year 4. For purposes of the cost estimates, the satellite earth stations are leased through the tariff offering. The incremental capital and installation costs associated with Option II are identified in Table VIII.

Table VIII: Incremental Capital and Installation Costs, Option II

Item	Additions ($K)					
	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Installation, Channels[5]	50			75		125

[4] Channel installation charges are based on $9,300 per node (installation and service charges of the proposed Megaroute tariff) for 21 nodes and installation charges of $25,000 for 2 nodes with satellite links (Yellowknife and Vancouver). It is anticipated that the installation costs of DS–3 channels will approach the current installation costs of DS–1 channels.

[5] Channel installation charges of $25,000 are estimated for civil works at each ground station location.

1.4.5 Capital & Installation Costs - Option III

The cost estimates for Option III are based on the initial Network configuration of Option I (see Table VI), supplemented with the parallel satellite subnetwork of Option II, and an additional 10 small nodes connected to the backbone with 1 DS–0 link, and migrating to 2 DS–0's by year 4.

The incremental capital and installation costs associated with Option III are identified in Table IX.

Table IX: Incremental Capital & Installation Costs, Option III

Item	Additions ($K)					
	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Small Nodes	1,000	–	–	250	–	1,250
Installation, Channels[6]	93	–	–	93	–	186
Incremental Capital & Installation	1,093	–	–	343	–	1,436

1.5 ANNUAL OPERATING COSTS

1.5.1 Introduction

The following annual operating costs estimates are provided for the years 1999 to 1995 inclusive:

a. Channel rental costs.
b. Connection charges to international networks.
c. Equipment maintenance costs expressed as a percentage of capital costs.
d. Costs associated with the development of Network services, as sponsored by the Network.
e. Marketing costs for the development of the Network subscriber base
f. Other operating costs including travel, printing, telephone, courier, etc...

1.5.2 Channel Rental Costs

The channel rental costs reflect the physical configuration of each of the three options as derived from the proposed Megaroute and Anikom tariffs under a three year contract. It is envisaged that the Yellowknife–Vancouver DS–0 link may require an SFT, however Anikom 500 rates have been used for budget estimate purposes.

[6] Channel installation charges are based on DS–0 links to an additional 10 nodes.

There are incremental channel rental costs for options II and III relative to Option I associated with the additional satellite channels and DS–0 links respectively.

The DS–3 rates as currently proposed by the carriers are approximately 8 times the rates for DS–1 channels[7]. For purposes of this estimate, it is assumed that DS–3 rates by year 4 will be twice the current DS–1 rates[8].

1.5.3 Connection Charges to International Networks

This item reflects interconnection to the Internet. Three national connections are envisaged. The costs of these interconnection reflect the cost of DS–1 links to an Internet node in the U.S. (upgraded to DS–3 in year 4). The cost estimates for the three links are based on an average link mileage of 150 miles. Interconnection costs are identical for the three options.

1.5.4 Equipment Maintenance Costs

Annual equipment maintenance costs are estimated at 10% of the installed equipment base.

1.5.5 Service Development Costs

The service development costs reflect the funding of service development by the Network. The estimate is based on the funding of three software development teams of five people each. These costs are identical for the three options.

1.5.6 Marketing Costs

Marketing costs reflect advertising costs in addition to the personnel costs previously identified and are identical for the three options. Marketing costs are estimated at 25,000 per quarter for the first year, with the 5% inflation factor applied for the remaining years.

1.5.7 Other Operating Costs

Other operating costs include travel, printing, telephone and courier expenses and are estimated at 5% of personnel costs. These costs are identical for the three options.

[7] See the Issue Paper on Data Communication Services.

[8] A Special Facility Tariff (SFT) applied for by Bell Canada on 18 January, 1989 proposed to offer a DS–3 facility to Teleglobe Canada from Montreal to the U.S. border at approximately twice the new proposed DS–1 rates. See Bell Canada Special Facilities Tariff (proposed), CRTC 7396, Item F–1303, Issued 1989 01 18.

1.5.8 Annual Operating Costs - Option I

Table X: Annual Operating Costs, Option I ($K)

Item	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Channel Rental	3,000	3,000	3,000	6,000	6,000	21,000
International Connections	600	600	600	1,200	1,200	4,200
Equipment Maintenance	350	350	360	380	400	1,840
Service Development	750	788	827	868	911	4,144
Marketing	100	105	110	116	122	553
Other Operating	100	120	138	145	150	653
Total Operating Costs	4,900	4,963	5,035	8,709	8,783	32,390

1.5.9 Incremental Annual Operating Costs - Option II

The incremental annual operating costs for Option II reflect the satellite channel and earth station rental charges of the satellite subnetwork.

Table XI: Incremental Annual Operating Costs, Option II ($K)

Item	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Channel Rental	350	350	350	1,400	1,400	3,850

1.5.10 Incremental Annual Operating Costs - Option III

The incremental annual operating costs for Option III reflect the DS–0 channels rental charges associated with the additional ten small nodes as well as increased maintenance costs. The cost estimate has assumed a doubling of link capacity by year 4 and an average link mileage of 200 miles.

Table XII: Incremental Annual Operating Costs, Option III ($K)

Item	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Channel Rental	200	200	200	400	400	1,400
Equipment Maintenance	100	100	100	125	125	550
Incremental Operating Costs	300	300	300	525	525	1,950

2. NETWORK ARCHITECTURE AND MIGRATION PLAN

2.1 SUMMARY

This section proposes logical and physical architectures which will meet the requirements of a High Speed National Network for Research and Development. The proposed physical architecture will be used to estimate the costs of the Network for budgetary purposes. This section does not provide final cost estimates, these are provided elsewhere. The section proposes that the Network objectives are best met by specifying an overall logical networking architecture which accommodates the interconnection of existing and future subnetworks. The High Speed R & D Subnetwork, the primary emphasis of this study, would enhance the performance of this assembly of subnetworks and would be used to influence the overall growth of the Network. In addition to this architecture, standards must be specified both to permit the straightforward integration of subnetworks, and to provide uniform user access to all networked systems. It is suggested that the standards above the Network Layer may be selected to match each community of user, and standards below the Network Layer may be selected to match the underlying subnetworking technology. This will provide a migration path, to accommodate the growth in user requirements and the growth in underlying technologies. It is pointed out that the availability of ISO based Router devices will critically affect the implementation schedule of the Network.

2.2 INTRODUCTION

This section discusses both logical and physical architectures for a High Speed National Network for Research and Development and indicates possible migration paths so that the network may continue to meet the needs of its users into the future. The logical architecture must follow the Open System Interconnection (OSI) model. The physical architecture is proposed for budgetary purposes only, this section does not suggest a specific physical implementation since the range of participants in the network are not yet defined and funding sources have not been committed.

For the development of a logical architecture, the Network must first be discussed in terms of the entire assembly of communications equipment and subnetworks (including existing subnetworks). This top level approach must lead to an architecture that will integrate existing and future networking initiatives.

For the development of costing information, the Network must be discussed in terms of the additional physical components and transmission links that must be installed to bind together the existing subnetworks to form the Network. That is, the part of the Network that will need to be added to existing regional and other subnetworks to make the entire assembly operate in the desired way. In a previous section this part was called the High Speed R & D Subnetwork.

The overall context of the Network will be discussed first, to propose a suitable OSI architecture that will permit the integration of other subnetworks into the overall structure. This is required in any case, since future Networks (e.g. commercial versions of the Network) are likely to be constructed this way: being an assembly of private, public, national, and international subnetworks. These subnetworks may involve different administrations, and will also include different subnetworking technologies. Thus the R & D Network will need to accommodate different technologies, e.g. satellite, fibre optic, metallic, and microwave technologies. Finally we note that voice, image, etc., must also be supported.

2.3 RELEVANCE TO STUDY

An overall objective for the Network is to provide an architecture which will provide user friendly access to remote applications, which will facilitate the development of information technology products and services, and which will provide a smooth transition path for users as their needs change. This architecture should be a prototype for future networks, e.g. commercial networks, to facilitate the development of products and services applicable to these future networks. This section explores potential Network architectures which can meet these needs.

In addition, this section presents sufficient physical details and component costs to permit the *Cost Estimation* section to estimate those Network component costs not already presented in the *Data Transmission Services* section.

2.4 BACKGROUND

The Open System Interconnection (OSI) model has become the standard with which data communication systems are described. Although not yet commonly used for voice or video applications, the OSI model is sufficiently flexible that it provides a strong foundation for these descriptions as well. Due to this flexibility, and its endorsement by Canada and the international community, the OSI model forms the basis for the discussions in this section.

Each network element will need to be described in terms of its communications capabilities. Communications capabilities may be modularized following the OSI model and the allocation of functions to network elements described using OSI diagrams. These diagrams provide a first approximation to the relative complexity of the network elements. Since component costs are related to complexity, this provides a method of estimating costs per network element.

Based on these logical diagrams, physical network designs may be proposed which will serve the necessary areas of Canada. These designs provide an estimate of the number of network elements required.

The Network element costs and quantity requirements presented in this section, along with other information, will be combined in the *Cost Estimation* section to arrive at final Network cost estimates.

2.5 THE OSI ARCHITECTURE

The International Organization for Standardization (ISO) produced the Open System Interconnection Basic Reference Model (OSI model) to provide a framework for the subsequent specification of communication standards. The model is **abstract**: it is not meant to specify an implementation, rather it is a means for description only to that extent necessary to define an implementation with sufficient rigor to ensure compatibility with another implementation developed using the same specification. The objective is to provide a specification without constraining the implementation or use of any specific technology. In addition, the model provides a method of segmenting the communications task into logically self–contained modules (called layers), defining a language for the specification of each module, and defining the interrelationship between modules.

Thus the OSI model not only provides a framework for the issue of specific standards, it also provides an abstract specification tool for communications systems.

A basic introduction to the specific layers of the Open System Interconnection model was provided in the *Protocols and Use of Standards* section. A more general overview of the OSI description method is provided in the following section.

2.5.1 The OSI Description Methodology

This section provides a brief introduction to OSI architectural diagrams as used in this section.

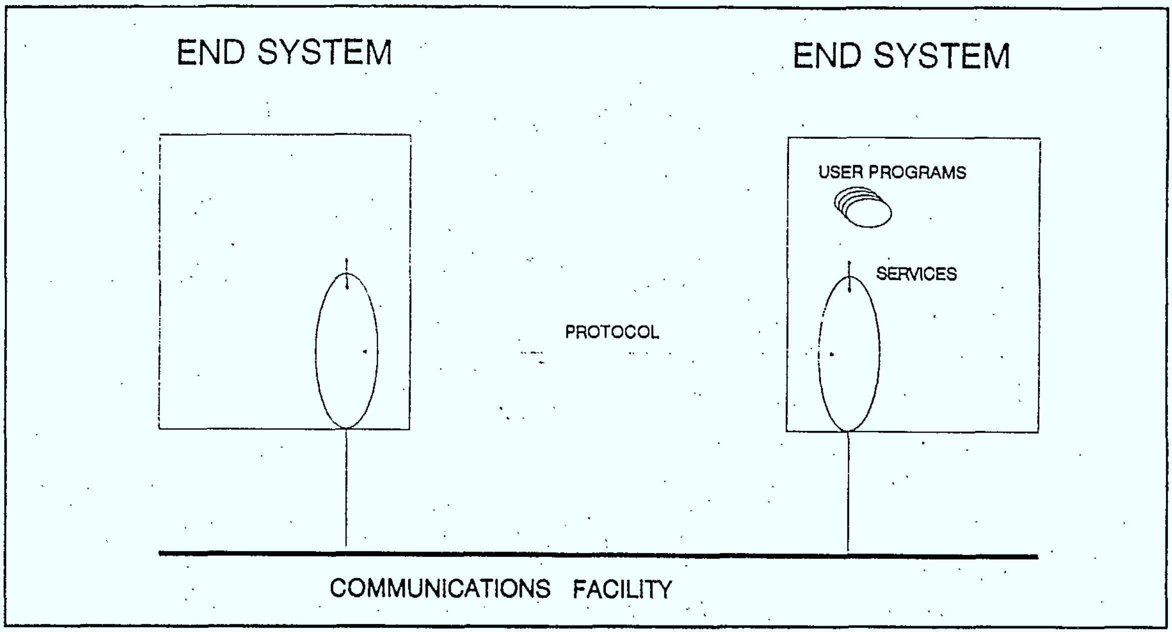

Figure 1: Interface Between End Systems

Figure 1 begins the introduction by showing two End Systems (ESs) who wish to communicate. Each ES might be a computer containing an operating system and one or more application programs. The operating system provides a range of services to the application programs and one type of service is a *communications service*. In practice such a service might be provided by `device drivers' and these must implement protocols compatible with the remote ES (which is a *peer* system). In the OSI model, a **Service Definition** describes the services offered to the application program and a **Protocol Specification** describes the peer–to–peer protocols used to implement the services. One observes in this figure that the Services are implemented internally to the system, e.g. through the use of proprietary operating system calls; while Protocols are exposed to the world and must be compatible with all external systems with which communications is required. This implies that the internal implementation of the Service in specific ways is not required for compatibility. The Protocol Specification, on the other hand, must be implemented in such a way that the external manifestation is compliant.

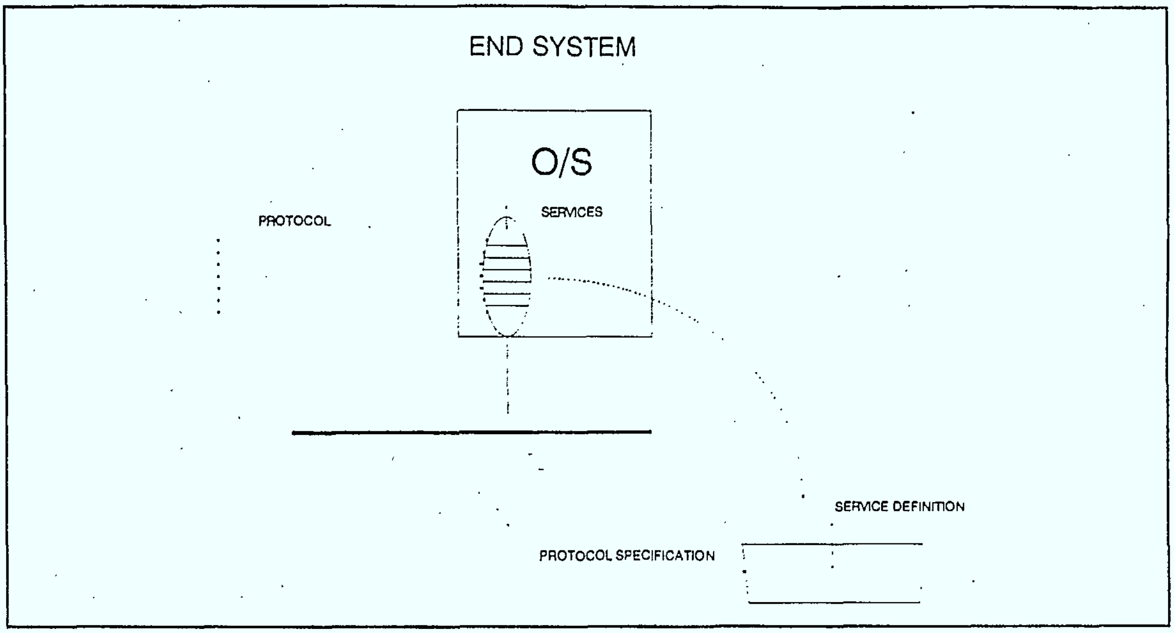

Figure 2: Refinement of Interface Between End Systems

Figure 2 further refines the OSI concept by showing how the functions of the communications `device driver' may be subdivided into modules (layers). For the OSI model there are seven layers. The specific layers of the OSI model are described in the *Protocols and Use of Standards* section. Each layer is specified using a Service Definition and a Protocol Specification. The layer supplies the defined service to the layer above using the services of the layer below. This value adding functionality is implemented using mechanisms in common with its peer layer – that is, using the specified protocols in common with its peer layer. These figures are **abstract**: compatibility only requires that all implementations be capable of being described in the terms discussed. Implementations capable of being described in this way are considered to be `Open Systems' in the OSI sense.

When describing the proposed Network the concept of abstraction is continued: no specific implementation constrains are implied by the logical network diagrams.

2.5.2 The OSI Networking Architecture

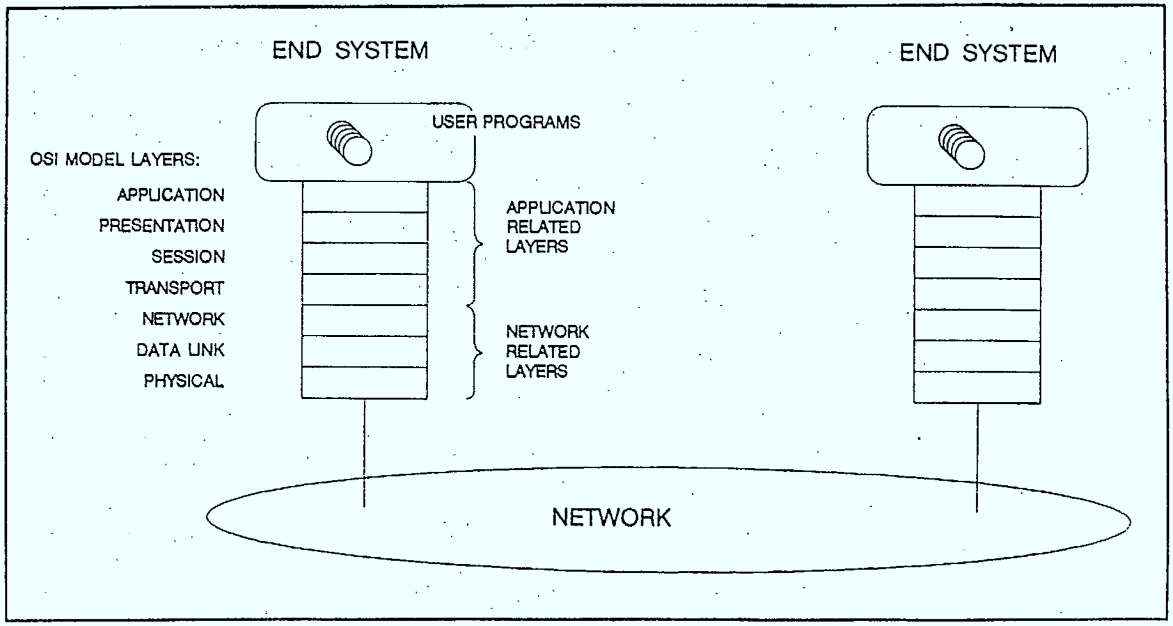

Figure 3: General OSI Network Architecture

To accommodate the idea of networking, that is the idea of a shared facility providing the end system interconnection of Figure 1, the general architecture of Figure 3 is provided. When the communications functions were modularized by the ISO, the functions related to networking data transmission were allocated to the lower three layers of the model: the Network, Data Link and Physical layers.

The capability of internetworking may be provided in several ways. The method pioneered by the ARPA network uses an internetworking function (using an Internet Protocol) placed over all of the subnetworks so that routing elements between each subnetwork may determine the next step in the transmission path (each subnetwork would not alter the end–to–end address information). A second method, currently used by the international telecommunications carriers, use hop–by–hop translation devices which translate addressing information at each subnetwork boundary to that required by the next subnetwork.

Typically the first approach discussed above has been used to provide a connectionless Network Service, each packet containing sufficient Internet Protocol information to allow the individual routing of each packet independently of all others. Typically the second approach has been used to provide a connection–mode Network Service, context information for each connection being maintained at each subnetwork interconnection.

Both approaches are considered to be valid OSI approaches. The selection of one method over the other is subject to considerable debate. Some will argue that Europe is tending towards the connection–mode approach, while North America is tending towards the connectionless approach. Current Canadian and United States government profiles specify the connectionless Internet approach, and the widespread Internet in the United States also follows this approach.

This section assumes the use of the connectionless Internet approach. The selection of the alternate connection–mode would not significantly alter the estimated network costs, although equipment availability may be restricted. It is believed that the connectionless approach will facilitate interworking with the international research Internet, and will provide maximum consistency with evolving North American networking trends.

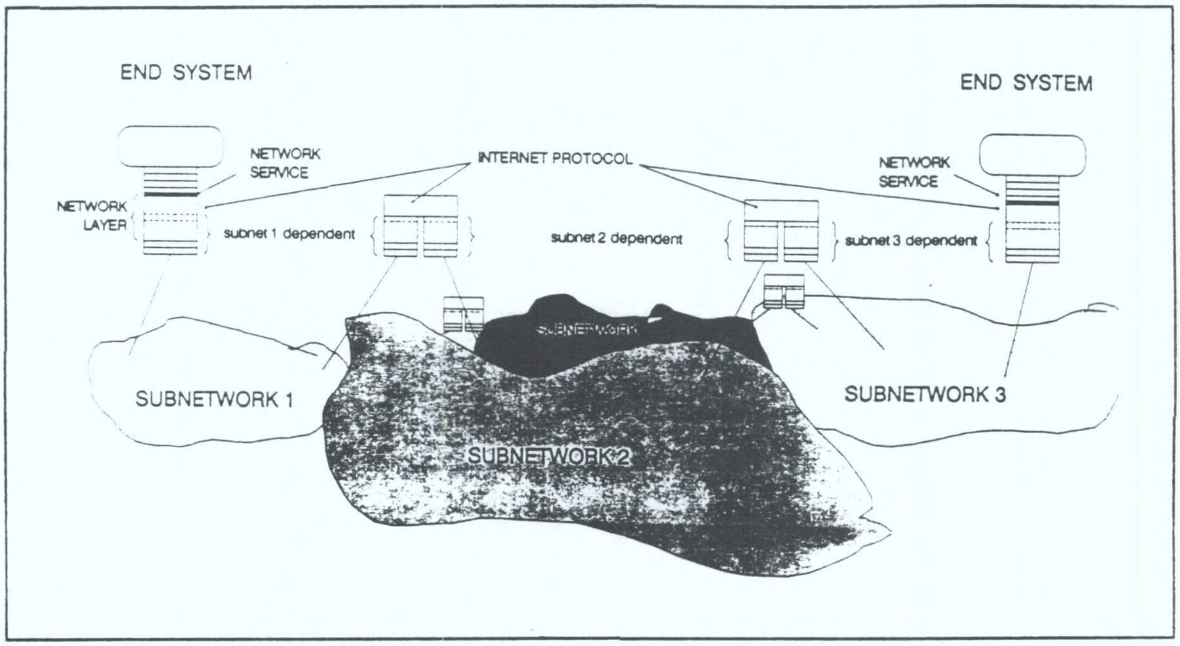

Figure 4: OSI Internetworking

For networks composed of many subnetworks, the upper third of the Network Layer is considered to implement network–wide functions (see Figure 4) while the lower

two thirds, plus the Data Link and Physical layers, are directly related to each subnetwork. Intercommunications between subnetworks is performed by a routing function which is included in the upper third of the Network Layer. These routing functions use an Internet Protocol.

2.5.3 The Network Service

The **Network Service** is a network–wide uniform service provided to the protocol layers above. The layers above the Network Layer are responsible for adding additional value to the basic network service to provide, for example, a file transfer service, a mail service, etc. These upper layers are also subject to standardization and this will be discussed in a later section.

The Network Service specification provides a convenient point at which the capabilities of the Network can be separated from the functions related to the provisions of application specific functions (e.g. electronic mail). Any upper layer functions which only require the services defined by the Network Service specification may operate over the Network without further regard to the underlying details of the Network itself.

The specification of the Network Service will be a key issue in the logical definition of the Network. This was discussed to some extent in the *Network Addressing, Directory and Routing* section and it was pointed out that the Network Service is specified in terms of Qualities of Service, and types of service such as connection and connectionless service types were discussed.

Although the discussion so far has been derived from the OSI model which was originally created for data applications, these concepts may be applied to all forms of communications including voice and video communications. Voice applications, for example, may require a Network Service with Qualities of Service which limit propagation delay but permit higher than normal (for data) residual error rates.

2.5.4 Application Specific Services

The upper four layers of the OSI model are concerned with the provision of the required services to applications[1]. Typical applications are File Transfer, Job Control, Electronic Mail, Voice, Video, etc. These applications will be served by a selection of upper layer standards and for a specific application to interoperate with an identical remote application it will be necessary to ensure that these selections are the same. If the end systems containing the applications have access to the network–wide Network Service discussed in the previous section, then it will only be necessary to ensure that the protocols of the upper four layers of the model are compatible.

Maintenance and management functions are considered `user' application functions, and their presence and standardization will be essential to the correct operation of the Network a whole. The same is true for the Directory function. Thus it will be necessary to standardize certain specific `user layer' functions (ISO standards for Network Management and Directory Services are under development).

The standards issued by the ISO generally have options associated with them. These options permit the services to be customized to the applications. For example, for the ISO Transport Layer, five classes of operation are defined (Transport Class 0 through 4) and these provide varying degrees of enhancement to the basic Network Service. Figure 5 demonstrates the concept of compatible application specific upper layers. In this figure it is assumed that some applications (Applications 1 and 2) can share certain layer protocol options while others require either other options or completely different protocols. For example, Applications 1 and 2 might be Electronic Mail and File Transfer applications which can share the enhanced services offered by Transport Class 4, Application 3 might be a voice application which only

[1] There is often confusion about the Application Layer of the OSI model. The Application Layer does not include the application programs, rather it provides application tailored services to these programs. Thus the user's application programs reside above the seventh layer of the model – this is called by some the `User Layer'.

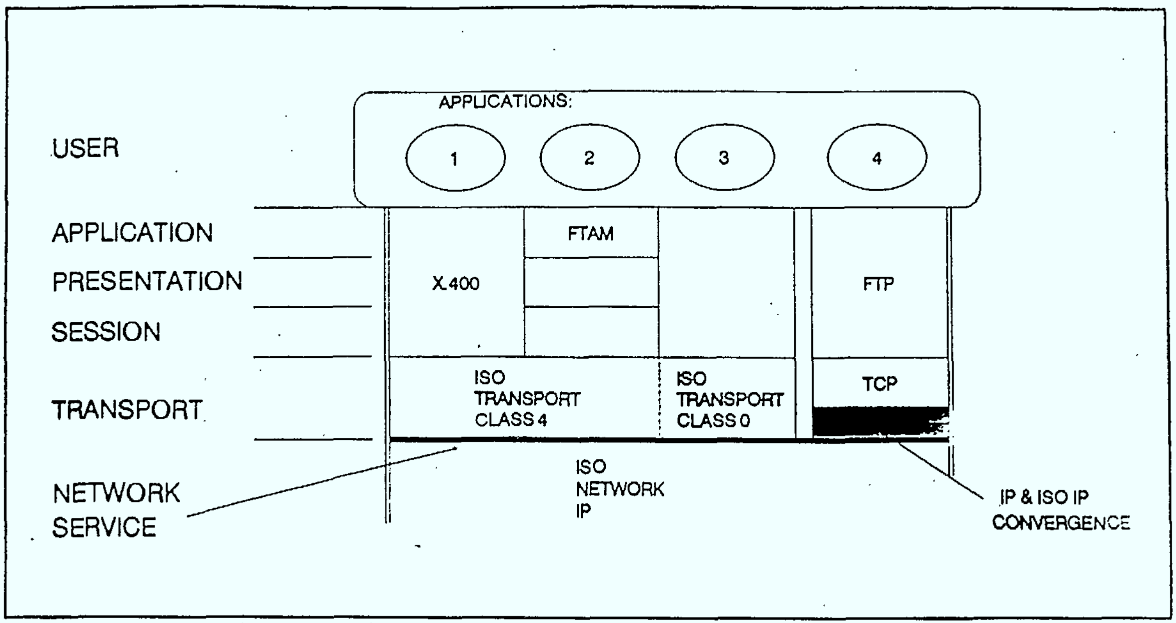

Figure 5: Application Specific Upper Layers

requires Transport Class 0, and Application 4 might be an FTP[2] application which requires the TCP Transport layer protocol[3] normally associated with TCP/IP.

The particular selections of protocols and options recommended for a given application is also the subject of standardization. These are called profiles, and these were discussed in the *Protocols and Use of Standards* section.

2.6 MIGRATION REQUIREMENTS

Migration strategies are required to allow the Network to grow with its users and its underlying technology base. Users of the Network include the traditional application oriented R & D users and those who use the Network itself for research and development. Growth include the growth in the amount of information moved, the types of information moved, and the services (and qualities of service) that must be supported. The underlying technology base includes the protocols used to support the services and the physical equipment which is used to implement the protocols and services (including data transmission equipment). It is proposed that the Network use ISO based standards, and this will represent the application of leading edge standards technology.

[2] FTP – File Transport Protocol, MIL–STD–1780, is a file transport protocol commonly used in conjunction with TCP/IP.

[3] The figure assumes that a binding between TCP and the Network Service is created.

Current applications and users on existing networks must be provided with a smooth transition to the new (e.g. higher data rate) services. All users may not need access to the full capabilities (e.g. capacity) of the network until their needs mature, however interim services must be consistent with the future service (although possibly at a lower rate and different qualities of service). A clear migration plan will facilitate user planning and at least two aspects are initially identified that must be considered: a user viewpoint and a network development viewpoint. For users, a menu of service offerings should be available at any stage so that the particular needs of users can be addressed in a cost effective manner. For network development, a migration path which allows the addition of capacity, service quality and new technologies with minimum disruption is required.

2.6.1 User Migration

Users will migrate to new services when they become available at an acceptable price, or when the user's desire for a service develops beyond the cost of the service. The price of the service not only consists of the traditional costs associated with access, but also includes costs associated with equipment and software that the user must acquire to adapt existing equipment to the desired service. For example, if the existing user equipment uses a TCP/IP protocol stack in his End System, then the cost of accessing a service using an ISO stack will include the cost of the local upgrade.

Users will want to upgrade (or downgrade) by type of service and quality of service. Types of service include data services such as file transfer, electronic mail, etc.; and non–data services such as image, voice, etc. Within each service, there may also be grades of quality of service such as speed (data rate), maximum propagation delay, etc. We have also discussed the support of both TCP/IP and ISO domains, and this would translate into the provision of multiple services for the same type of application. For example, we should provide file transfer services using either FTP (one of the TCP/IP mechanisms) or FTAM (the ISO mechanism). If gateways are included to translate between FTP and FTAM, then a translation service would be offered as well.

It is expected that many users will want access to all data services. To encourage a transition towards the ISO data services, an offering profile might include the standard provision of ISO data services and optional access to TCP/IP data services. The quality of the service may differ. For example, small users may initially want access at low speed with an option to upgrade as their needs develop. The provision of non–traditional services such as voice and image may not initially be required by all users. Indeed, these services may not be available at all during the initial deployment of the Network.

To properly match the services of the Network to the full range of users, it will be necessary to offer ranges and grades of service. These ranges and grades must have varying costs so that they most exactly match user needs.

2.6.2 **Network Migration**

The Network must provide a plan for growth and for the integration of new technologies and standards. Growth will occur in the number of users and the amount and kind of information to be handled. Since new technologies and standards are expected to be developed using the Network, a methodology should be established to permit trial use in a manner which has minimal impact on ongoing Network operations.

The Network must have an architecture which can accept new (and unknown today) technologies and allow them to be integrated with the current Network technology. This implies the creation of flexible and standardized internal interfaces which are as technology and implementation independent as is possible. Such interfaces are available by using the ISO abstraction approach previously discussed.

The proposed architecture facilitates network growth by providing a standard subnetwork interface based on the ISO Internet approach. This will allow new subnetworking technologies to be developed independently and integrated into the Network by the construction of suitable routing elements which conform to the Internet protocols.

2.7 USER VIEWS

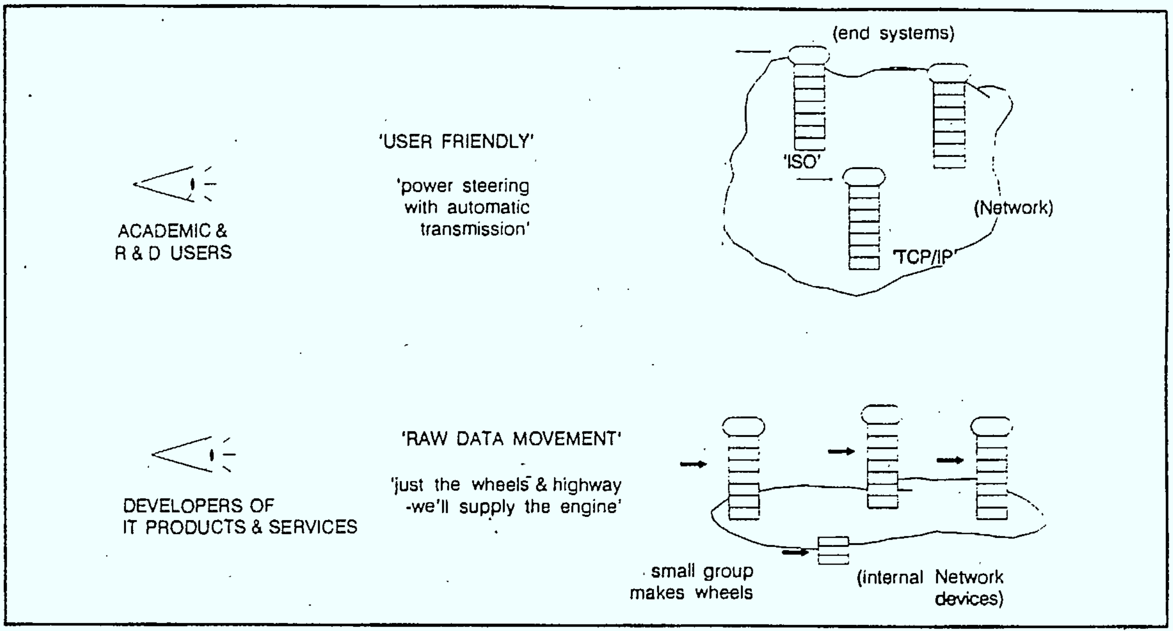

Figure 6: User Views of Network

For the purpose of defining the Network architecture users may be divided into two groups. The first group desires user friendly access to network services and does not want to be concerned about the communications details. The second group consists of those users who are in the communications business and they will wish to be fully involved with the communications mechanisms. In general, the second group will create the environment desired by the first group. Figure 6 depicts these views of the Network.

Within the first group who wish user friendly access, there are three sub–groups: those wishing to access remote applications using ISO protocols, those wishing to access applications using the more traditional TCP/IP protocols, and those wishing to use other protocols.

1. Access using ISO based protocols will be the preferred approach. Maximum support for ISO based applications will promote the migration to these protocols.

2. Access using TCP/IP based protocols will be supported as an interim measure. Support for TCP/IP based applications will draw from existing implementations and the existing academic community. Certain foreign and regional subnetworks will only be accessible using TCP/IP.

3. Access to other protocols, and other instances of ISO and TCP/IP protocols, above the Network Layer will be supported only to the extent that they may co–exist on the Network. For example, this will permit the offering of protocol testing services over the Network. This sub–group will be expected to completely support themselves and must be well–behaved[4] Network users.

Within the second group who are interested in the communications details, there are three sub–groups: those wishing to supply or experiment with upper layer protocols (above the Network Layer), those wishing to work on the Network Layer, and those interested in the lower layers.

1. For work above the Network Layer, the users must conform to the Network Layer service specification and must operate within a closed group of Network Addresses[5]. These requirements are similar to those of the third sub–group mentioned above.

2. Work within the Network Layer will be difficult to accommodate in the on–line part of the Network, although the existence of the Network will certainly promote the development of this part. It is suggested that an off–line Network Emulation be constructed to support this work. This emulation will need to include multiple Routers interconnected with a simulation of long distance T1 (or satellite, etc.) subnetworks. This emulation might be sited at the Technical Centre.

3. Work in the lower part of the Network Layer (SNAcP) and below will be subnetwork technology dependent. It is expected that early development of such technologies will generally be made by a single vendor, since the use of standardized protocols at these layers is less common for wide area subnetworks. Certain satellite and mobile host applications (e.g. cellular radio subnets) may be exceptions. In general, the development of these technologies will initially be carried out using purpose–built facilities. Once the basic operation of the new subnetwork technology has been verified it may be integrated into the Network for operational trials using an appropriate Router interface[6].

Figure 7 encapsulates the options for the latter group into an `hour–glass' concept. Maximum flexibility occurs above and below the Network Layer with the Network Layer acting as the unifying point.

[4] Their behaviour may be enforced by suitable `fire–wall' provisions in the appropriate Router device.

[5] For example, through the use of distinct Transport Selector values (these are part of the ISO Network Address – refer to the *Network Addressing, Directory and Routing* issue paper).

[6] For example, by developing the appropriate Subnetwork Dependant Convergence and Subnetwork Access protocols (SNDCP and SNAcP refer to the above issue paper).

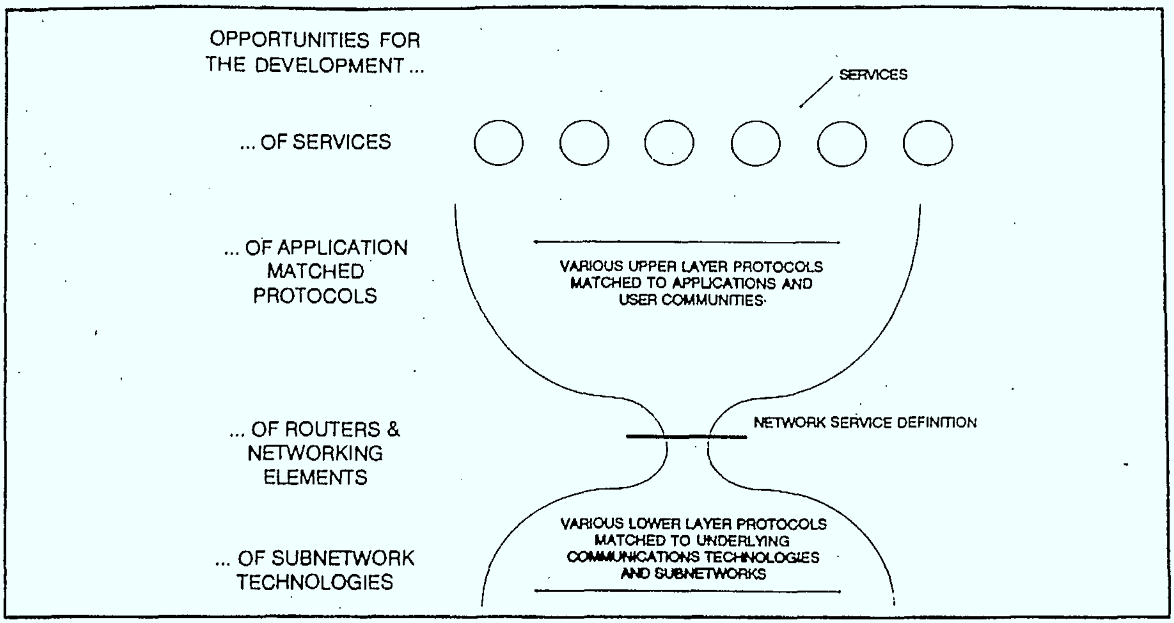
OPPORTUNITIES FOR THE DEVELOPMENT ...
... OF SERVICES
... OF APPLICATION MATCHED PROTOCOLS
... OF ROUTERS & NETWORKING ELEMENTS
... OF SUBNETWORK TECHNOLOGIES
SERVICES
VARIOUS UPPER LAYER PROTOCOLS MATCHED TO APPLICATIONS AND USER COMMUNITIES
NETWORK SERVICE DEFINITION
VARIOUS LOWER LAYER PROTOCOLS MATCHED TO UNDERLYING COMMUNICATIONS TECHNOLOGIES AND SUBNETWORKS

Figure 7: The Hour–glass of Protocols

2.8 PROPOSED NETWORK LOGICAL ARCHITECTURE

It is proposed that the overall Network will consist of a number of interconnected subnetworks. Some of these subnetworks exist today, some will be developed in the future, and at least one (the High Speed R & D Subnetworks) may be created as a direct result of the current feasibility study. Such an infrastructure will have maximum flexibility: able to respond to the growth in user requirements by adding capacity and services, and changing technologies and market opportunities by facilitating the introduction of new products and services. This architecture is also consistent with the ISO concept of networking, and supports the interconnection of foreign networks.

Figure 8 provides an overview of the proposed Network Architecture. User friendly access using ISO, TCP/IP and other protocols are shown as separate `domains' at the top of the figure. While each are shown co–existing on the Network, they will not inherently be able to interoperate. Interoperation with multiple domains may be performed in either of two ways[7]: either the user installs multiple protocol suites within the end system to permit operation into multiple domains, or the user makes use of a Gateway device to translate between the domains. The lower part of the figure shows how the Network actually consists of multiple subnetworks. These subnetworks may be implemented with various technologies and may physically overlap one another. The interconnection of subnetworks is performed by the Routers.

Connections to foreign networks (subnetworks) will require the use of special Router devices, these will include suitable convergence functions to match the lower layers of the foreign

[7] Implementations using both of these approaches have been described by various sources.

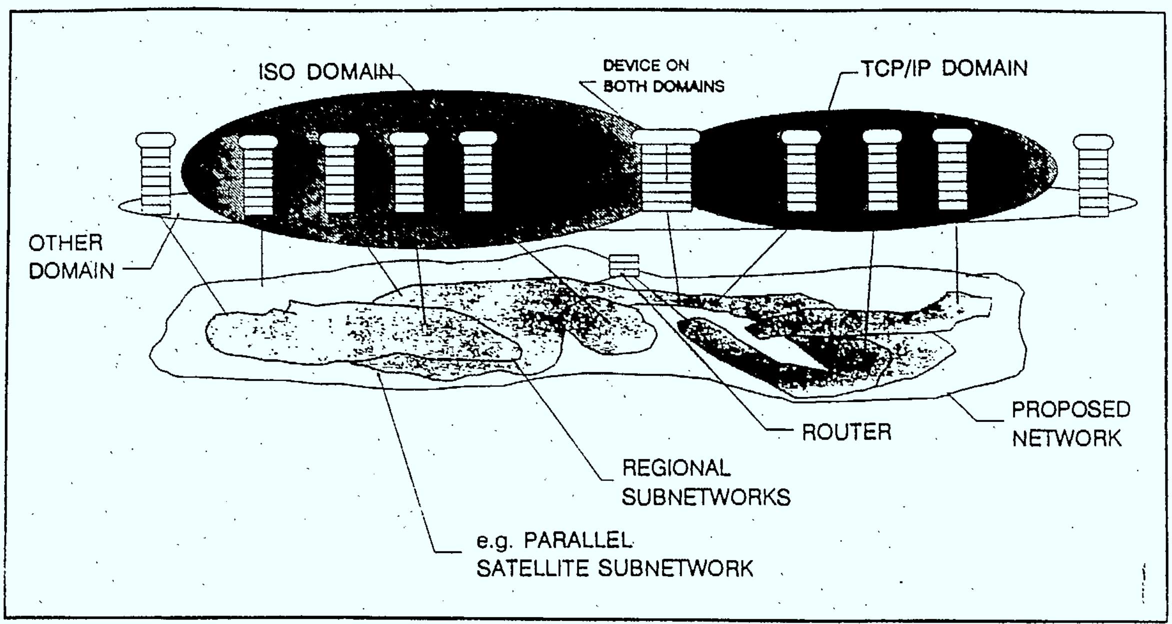

Figure 8: Proposed R & D Network Architecture

subnetwork. Upper layer compatibility of the foreign networks would be handled by considering them as a domain within the Canadian Network: TCP/IP foreign networks would join the TCP/IP domain on the Canadian Network. As the foreign networks migrate to OSI, as is expected, these interconnections may be simplified.

2.9 PROPOSED NETWORK PHYSICAL ARCHITECTURE

This section translates the logical architecture discussed in the previous section into example physical implementations. The purpose of proposing physical designs at this early stage is to permit preliminary estimates of cost and equipment availability to be made.

The new equipment required to implement the Network may be classified under two categories: the high speed transmission links between the nodes of the Network and the routing components within each node which interconnect the links and provide interfaces to certain users.

2.9.1 Transmission Components

High speed transmission subnetworks based on carrier provided T1 lines, satellite links, etc. are proposed. The physical architecture includes both T1 and explicitly specified satellite links. Carrier provided T1 lines may generally implement data transmission using metallic, radio, satellite and fibre components; thus all current long distance transmission technologies may be included. Satellite links are explicitly identified since the propagation delay and performance of these channels is expected to differ significantly from terrestrial circuits.

At the present time, only a few multi–vendor standards exist for the lower protocol layers for long distance transmission. Such links are generally implemented as point–to–point circuits, with protocols defined by the manufacturer of the end–point devices. At the lowest layer, the T1 framing format and electrical specifications are normally used. Data Link layer protocols for error control, etc., are generally proprietary. For point–to–point links supported by a single vendor, this approach is acceptable since the lower protocol layers are invisible to the rest of the Network. For point–to–point links between different vendor equipment, common protocols must be used.

It is possible that the satellite subnetwork could offer its services in a form other than as a point–to–point service. For example, the satellite subnetwork could offer a packet switching capability. The possibility of such a service, which is more closely matched to the requirements of the overall Network, should be an area of further investigation after the completion of this feasibility study.

For the proposed physical architecture it is assumed that standard clear T1 channels will be leased from the carrier. Satellite links, and lower speed links, are expected to use other formats, these will be selected to be compatible with the Routers to be used.

Costing of the transmission subnetwork channels are subject to regulation and obtained from current tariff lists, refer to the *Data Transmission Services* section.

2.9.2 Network Routing Nodes

Figure 9 is used to describe a general routing node. This node contains both an ISO IP Router and Network Processing elements. The processing elements are used to support an initial set of services to end users and to interface to certain local subnetworks. The exact quantity and detail of these components will vary from node to node, and this configuration is provided for example only. The final node configurations may vary from this example, but these variations are not expected to alter cost estimates significantly. This architecture will meet the expansion and growth requirements of the Network by permitting the addition of processing elements as access needs become more formally defined. This architecture also permits the addition of subnetwork links as capacity requirements change.

The ISO IP Router is the element responsible for interconnecting subnetworks. In the example figure, nine subnetwork interface lines are shown, eight are used to support long distance data transmissions while one is used to interface to a local area network. This particular configuration is based on a Router configuration offered by Proteon for TCP/IP networks. Other configurations for ISO IP Routers are expected to be available from Canadian vendors in the near future for the proposed Network. For the final design it will be critical to assess the availablility and maturity of these ISO IP Router devices.

Wide area networking in this example is shown using point–to–point links as discussed in the previous section. Each link forms a subnetwork with Routers at each end of the link. Each link is considered a separate subnetwork since switching between them can only occur via the Router and each link operates independently of the others, possibly using different data rates and media. Other wide area subnetworking approaches may be supported simultaneously, and some of these may include data switching between multiple end–points. For example, a satellite subnetwork could interconnect several Routers and supply transmission and data switching capabilities between the Routers. In this case it would be necessary for the Routers to include suitable subnetwork convergence protocols to match the satellite subnetwork access

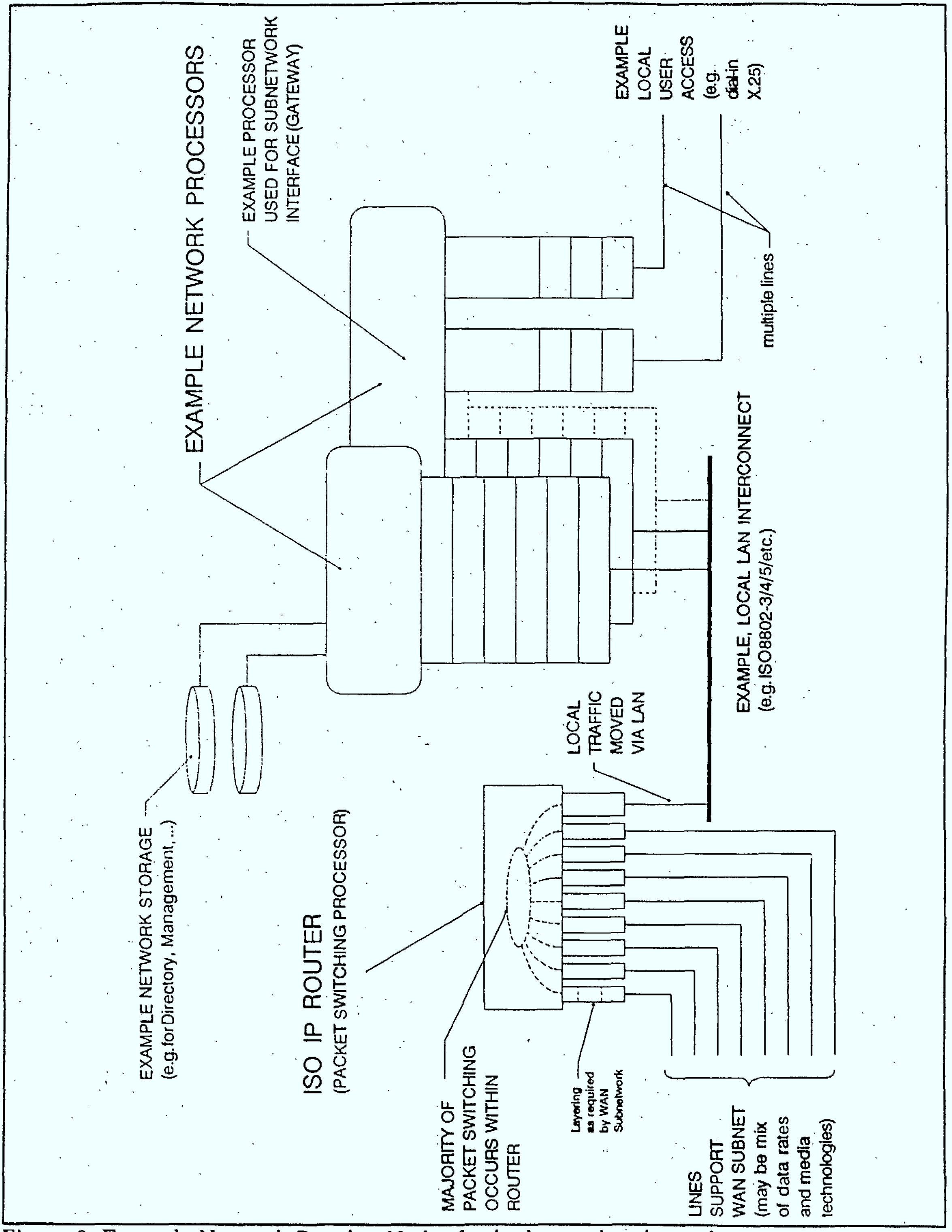
EXAMPLE NETWORK PROCESSORS
EXAMPLE PROCESSOR USED FOR SUBNETWORK INTERFACE (GATEWAY)
EXAMPLE LOCAL USER ACCESS (e.g. dial-in X.25)
multiple lines
EXAMPLE, LOCAL LAN INTERCONNECT (e.g. ISO8802-3/4/5/etc.)
LOCAL TRAFFIC MOVED VIA LAN
EXAMPLE NETWORK STORAGE (e.g. for Directory, Management, ...)
ISO IP ROUTER (PACKET SWITCHING PROCESSOR)
MAJORITY OF PACKET SWITCHING OCCURS WITHIN ROUTER
Layering as required by WAN Subnetwork
LINES SUPPORT WAN SUBNET (may be mix of data rates and media technologies)

Figure 9: Example Network Routing Node, for budget estimation only

protocol as discussed previously in Section 4.2.

The Local Area Network (subnetwork) interconnection in the figure is representative of several potential routing node configurations:

1. For large users with their own dedicated Router, a LAN interconnection would provide direct ISO access to the National Network at the highest possible speed and lowest processing overhead.

2. As exactly shown in the figure, the LAN may be used to interconnect one or more computing devices to the Network to support various service or gateway functions. Service functions might include Directory functions (refer to *Network Addressing, Directory and Routing* section), Maintenance and Billing functions (refer to *Network Management and Technical Centre* section), Electronic Mail User Agents (if supplied – e.g. as per CCITT X.400), and other services offered by the Network. Gateway functions might include interfaces to other subnetworks with differing protocols. Such subnetworks may include foreign networks, public networks (circuit switched or packet) used to support low cost access to the Network, industrial networks requiring enhanced access security, etc.

It must be emphasized that this node is presented for example only, non–technical factors will determine the level of local access provided to the High Speed Network backbone component. The amount of equipment within a node will depend upon the location and requirements of the node. To simplify the discussion it is convenient to define basic capabilities for a node, and then to classify the nodes based on the capabilities that it requires. Since the costs of a node are related to its capabilities, this method permits general node cost estimates to be made. The following capabilities are defined for the purpose of budgeting:

1. Router capable of interconnecting up to five subnetworks, e.g. a minimum node capability.

2. Router capable of interconnecting up to ten subnetworks, e.g. for nodes in major centres.

3. Local Area Network Interconnection and miscellaneous costs, e.g. used for all nodes with capabilities listed below.

4. Network Processor to support service function, e.g. where required and convenient for the Network.

5. Network Processor to support gateway function for up to four external subnetworks at less than 64kbps or one external subnetwork at 1.5 Mbps, e.g. to support X.25 public access, NSFnet interface.

6. Network Processor to support local access at speeds up to 9600 bps for up to sixteen

(16) users[8].

Not included here are allowances for building or other capital costs associated with housing and supporting the equipment. It is expected that these costs and maintenance costs will be accounted for elsewhere.

Certain government and industrial users may wish to acquire their own Router capability. It is assumed that these large users will bear the costs of such aequipment.

The cost of three node types are estimated and the configurations of the smallest and largest shown in Figure 10.

2.9.2.1 Small Routing Node

A typical small node located in a remote area might consist of:

Quantity	Capability	Description	Unit Cost	Total Cost
1	1	Small Router	25,000	25,000
1	3	Local LAN	15,000	15,000
1	5	Gateway	20,000	20,000
2	6	Local Access	20,000	40,000
				100,000

2.9.2.2 Large Routing Node

A typical large node which does not include any network service functions might consist of:

Quantity	Capability	Description	Unit Cost	Total Cost
1	2	Large Router	35,000	35,000
1	3	Local LAN	15,000	15,000
2	5	Gateway	20,000	40,000
3	6	Local Access	20,000	60,000
				150,000

[8] Local access will be required for Network staff and others not serviced by a regional network. This size was selected as a convenient size increment, additional capacity might be obtained by adding processors.

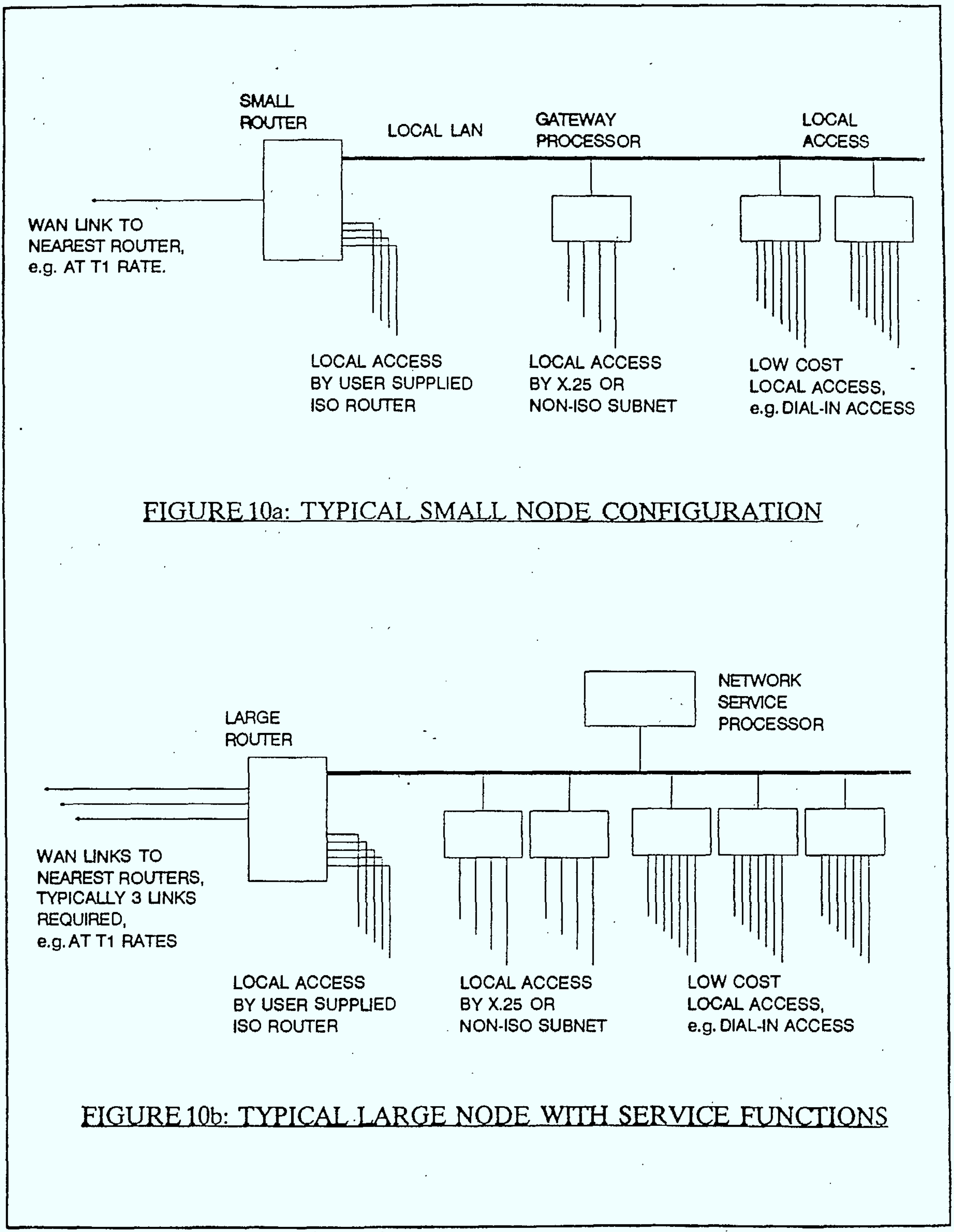
SMALL ROUTER
LOCAL LAN
GATEWAY PROCESSOR
LOCAL ACCESS
WAN LINK TO NEAREST ROUTER, e.g. AT T1 RATE.
LOCAL ACCESS BY USER SUPPLIED ISO ROUTER
LOCAL ACCESS BY X.25 OR NON-ISO SUBNET
LOW COST LOCAL ACCESS, e.g. DIAL-IN ACCESS

FIGURE 10a: TYPICAL SMALL NODE CONFIGURATION

NETWORK SERVICE PROCESSOR
LARGE ROUTER
WAN LINKS TO NEAREST ROUTERS, TYPICALLY 3 LINKS REQUIRED, e.g. AT T1 RATES
LOCAL ACCESS BY USER SUPPLIED ISO ROUTER
LOCAL ACCESS BY X.25 OR NON-ISO SUBNET
LOW COST LOCAL ACCESS, e.g. DIAL-IN ACCESS

FIGURE 10b: TYPICAL LARGE NODE WITH SERVICE FUNCTIONS

Figure 10: Typical Node Configurations

2.9.2.3 Large Routing Node with Service Support

A typical large node which includes a network service function might consist of:

Quantity	Capability	Description	Unit Cost	Total Cost
1	2	Large Router	35,000	35,000
1	3	Local LAN	15,000	15,000
1	4	Network Service	50,000	50,000
2	5	Gateway	20,000	40,000
3	6	Local Access	20,000	60,000
				200,000

2.9.2.4 Example Network Physical Design

Figure 11 provides an example physical layout for the Network. Several options are available based on this figure and these, along with full cost details, are discussed in the *Cost Estimation* section.

2.9.3 Network Emulation Facility

As discussed in section 6, a Network Emulation Facility will be required to permit the development and maintenance of the Network Layer functions for the Network. These functions primarily relate to Routing and Relaying and Network Addressing. This facility will also permit the final testing of prototype protocol stacks to the Network Service specification, and prototype subnetwork types, prior to their operational testing within the main Network. The facility will also provide a training facility for Network staff, and thus should include samples of all equipment used in the Network.

Certain components should be allocated to the Emulation Facility. Equipment spares held for maintenance purposes may also be used by the facility subject to preemption should Network equipment require replacement. The facility cost estimated below considers equipment permanently allocated to the facility only, it does not include maintenance spares. Note also that support equipment for the Technical Centre staff and test equipment is costed elsewhere.

Special equipment for the Emulation Facility includes transmission link simulation devices and test jigs to facilitate the attachment of trial equipment.

Figure 11: Typical Physical Architecture for Network

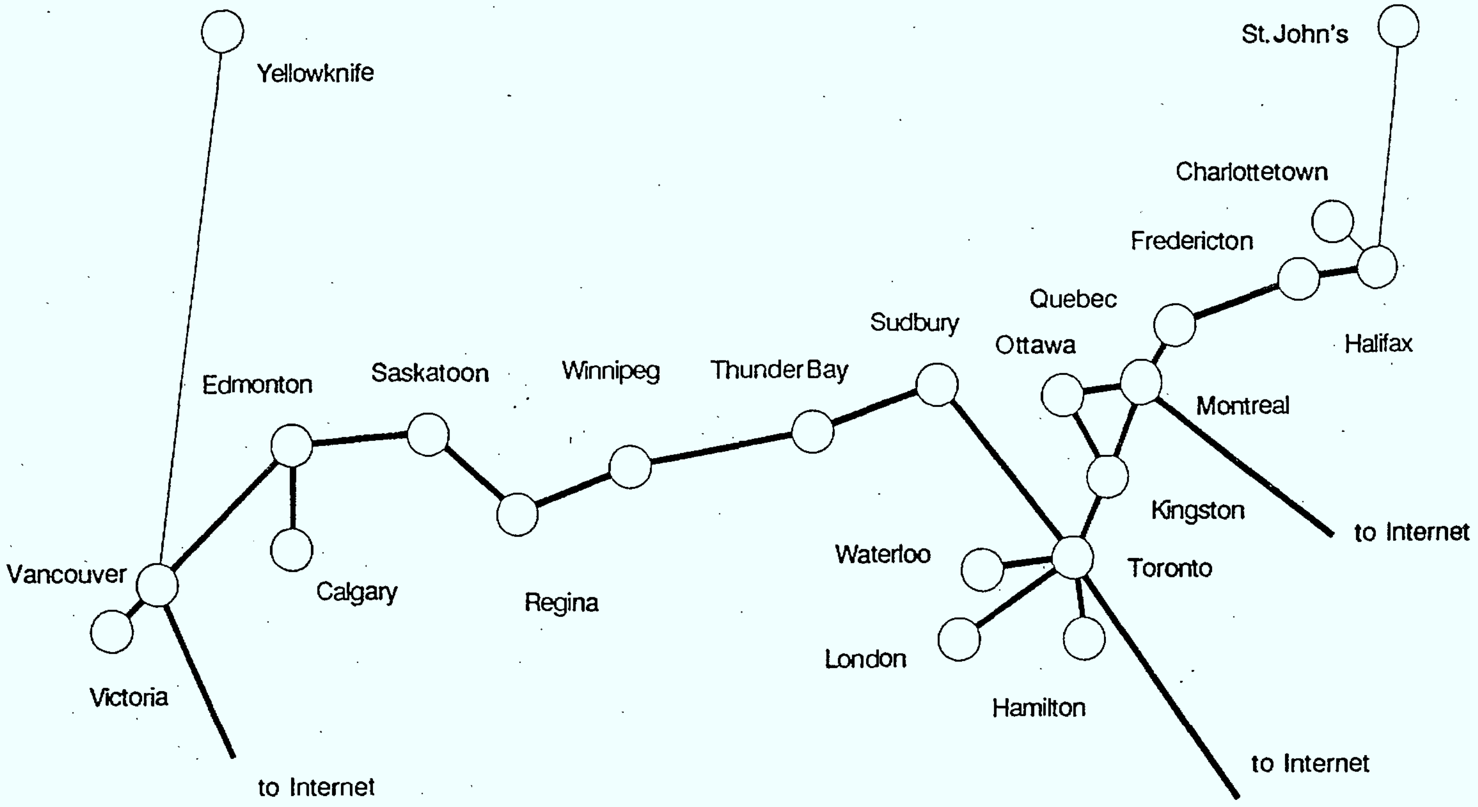

FIGURE 11: TYPICAL PHYSICAL ARCHITECTURE FOR NETWORK

Quantity	Capability	Description	Unit Cost	Total Cost
2	1	Small Router	25,000	50,000
1	2	Large Router	35,000	35,000
1	3	Local LAN	15,000	15,000
1	4	Network Service	50,000	50,000
1	5	Gateway	20,000	20,000
1	6	Local Access	20,000	20,000
–	–	Test Jig(s)	30,000	30,000
3	–	Link Simulators	10,000	30,000
				250,000

2.10 CONCLUSIONS AND RECOMMENDATIONS

This section has developed logical and physical architectures for the Network. Capital costs for the node equipment and Network Emulation Facility have been estimated.

The major conclusions are that the Network:

Must have a logical architecture suitable for the interconnection of multiple subnetworks so that growth and flexibility options are maintained.

The Network will be capable of supporting both ISO and traditional protocols, and of supporting a smooth migration path to the newer ISO protocols. The availability and maturity of ISO IP Routers will be critical to the final design's implementation schedule.

Protocol selections above the Network Layer may be made independently by each community of user (acknowledging, however, that the ISO protocols are preferred).

A Network Emulation facility will be required to support the development of Network Layer protocols off–line to the Network.

Protocol selections at and below the Network Layer will be selected to meet the requirements of the subnetworking technology used. Any research and development carried out on these technologies will use purpose–built facilities separate from the Network. Later operational testing may be carried out in conjunction with the Network.

The Network must promote the normalization of standards at the top of the

Network Layer by agreeing upon a Network Service definition, a Naming and Network Addressing scheme, and Routing and Relaying functions, following the ISO recommendations.

Cost estimates for small nodes, large nodes and large nodes with service capabilities, are $100,000, 150,000 and 200,000, respectively.

A Network Emulation facility is required which will increase the Technical Centre cost by approximately $250,000.

An example physical network architecture consisting of 21 nodes is presented. Note that the complete estimation of Network costs, including cost for leased services, personnel costs, etc., are provided elsewhere in the *Cost Estimation* section.

3. DATA TRANSMISSION SERVICES

3.1 SUMMARY

This section addresses data transmission as a service offered by a common carrier. The section is a survey of existing service offerings from regulated Canadian carriers which are relevant to the definition of a High Speed Network for Research and Development.

The surveyed offerings include Datalink, Dataroute, Datapac, Megaroute and Megastream from Bell Canada, the equivalent Mach III services from CN/CP and Anikom 1000, 500 and 200 from Telesat Canada.

The section highlights the tariffs under which the services are offered and surveys the services as inputs to the physical design and costing of the Network.

3.2 INTRODUCTION

This section discusses existing carrier services which may impact the physical design and economic analysis associated with the High Speed National Network for Research and Development (the Network).

The Network is viewed as an assembly of Subnetworks, including the High Speed Subnetwork which is the emphasis of this Study. The High Speed Subnetwork will consist of transmission links and other physical components which will bind together the existing and future Subnetworks.

Network users will access the Network through a Subnetwork, of which the High Speed Subnetwork is but one[1]. Regional Subnetworks as well as Local Subnetworks, many of which currently exist, represent the typical point of access for the individual user or device.

This section is a survey of available public service offerings from the carriers which could be used for the physical design of the transmission link component of the High Speed Subnetwork or which could be used for low speed access to the Network.

The focus of the discussion on services which are relevant to the design of the backbone is cost while the focus of the discussion related to access services is mainly their availability.

3.3 RELEVANCE TO STUDY

Public service offerings from the carriers represent the most economical vehicle for the provision of the High Speed Subnetwork's transmission links. Carrier offerings will form the basis of the analysis of the economic feasibility and physical design of the link channels

[1] See the issue paper on Network Addressing, Directory and Routing for a discussion of the Network and Subnetworks.

component of the High Speed Subnetwork. The link channel component of the High Speed Subnetwork may represent up to 50% of the cost of operating the Network.[2]

In addition, ubiquitous access to the Network will be heavily dependent on the availability of existing carrier offerings. This is particularly true for low speed access to the Network from locations remote from the Network's end nodes.

3.4 BACKGROUND

3.4.1 Assumptions

This section assumes that full tariff rates will be paid for offerings available under a carrier's General Tariffs (GT's). Special Facility Tariffs (SFT's), which can be priced and negotiated separately with a carrier and do not represent a general public offering, are considered beyond the scope of this section. The opportunities associated with the development of specially priced SFT's or other arrangements with the carriers are discussed in a separate report on regulatory considerations.[3]

3.4.2 The Carriers

There are three main carrier groups in Canada who can provide services on a national basis: Telecom Canada, CN/CP and Telesat Canada. Telecom Canada is an association of telephone companies while CN/CP and Telesat are companies in their own right. In general, Telecom Canada offerings are available on a national basis through the provincial telephone company.

In terms of rate relationships and offerings, CN/CP services are very closely aligned to the equivalent Telecom Canada offering and are generally offered at a 5% discount. Telesat offerings are somewhat different in that they have been developed for applications particularly suited to the use of satellite technology.

For the purposes of this section, terrestrial service offerings will be surveyed through the offerings of Bell Canada, the largest Telecom Canada member, with additional information provided on the equivalent CN/CP offering as appropriate. Telesat offerings will be discussed separately.

3.4.3 Revised Rates

Bell Canada and the British Columbia Telephone Company (BC Tel) filed applications with the CRTC on 25 January and 1 February 1990 respectively for the approval of tariff revisions for their competitive network services which include Megaroute, Megastream, Dataroute, and Datapac [1][2].

[2] This has been the experience reported by existing regional R&D networks in Canada.

[3] See the Regulatory Report #2.

Bell and BC Tel are proposing a revised discount structure in which discount levels would be based on the duration of customer's contract and the monthly billing amount. The average reductions for the digital private line services associated with the application are:

* Megastream:	DS–0 service reduced by an average 20%.
* Megaroute:	DS–1 service reduced by an average 50%.
* Dataroute 56:	56 Kbps service (data only) reduced by an average 70%.

It is anticipated that the rates which were applied for will be approved before the Network implementation. For the purposes of this section, tariff rates will be discussed in light of the recent applications. This section assumes that the proposed changes in rates and offerings will be approved[4]. Bell Canada's proposed tariff pages have been used as the basis of the costing examples in this section.

The applications also addressed the introduction of rates for DS–3 channels. DS–3 service is not currently available from the carriers as a public offering however the current applications suggest that it is reasonable to expect DS–3 service to be available within the year.

3.5 HIGH SPEED SUBNETWORK LINK COMPONENT: SERVICES

3.5.1 Introduction

The transmission links of the High Speed Subnetwork will be procured through available service offerings from the carriers. This section reviews offerings which can provide DS–3, DS–1 or DS–0 (including 56 Kbps) capability on the links as follows:

- Inter–Office Digital Channels (Bell)
- Megaroute (Bell)
- Megastream (Bell)
- Dataroute (Bell)
- Mach III (CN/CP)
- Anikom 1000 (Telesat)
- Anikom 500 (Telesat)

The tariff on Inter–Office Digital Channels is used as the basis for the rating of the Inter–exchange portion of Megaroute and Megastream, as detailed in the following sections.

3.5.2 Inter-Office Digital Channels

Digital channels (DS–0, DS–1 and DS–3) are furnished between Bell Canada wire centres and/or rate centres [3][5]. Bell determines the exchanges where service will be provided.

[4] A decision from the CRTC is not anticipated until July of this year at the earliest.

[5] Trans Canada offerings are not available in the current application, however it is reasonable to expect that such an offering would be available within two years.

Intra–exchange channels (DS–1 or DS–3) are available between wire centres within an exchange, and Inter–exchange channels (DS–0, DS–1 or DS–3) are available between rate centres in adjoining or non–adjoining exchanges.

Proposed rates for Inter–Office digital channels in non–adjoining exchanges, which are used in the rating of other services to be discussed later in this section, are outlined in Table I.

Table I: Bell Canada Rates for Inter–Office Digital Channels, Non Adjoining Exchanges

Distance (miles)	DS–O Channels		DS–1 Channels		DS–3 Channels	
	Base Charge ($)	Charge per Mile ($)	Base Charge ($)	Charge per Mile ($)	Base Charge ($)	Charge per Mile ($)
1–25	–	17.50	–	210.00	–	1,890.00
26–50	125.00	12.50	1,500.00	150.00	13,500.00	1,350.00
51–100	285.00	9.30	3,425.00	111.50	30,800.00	1,004.00
101–200	840.00	3.75	10,075.00	45.00	90,700.00	405.00
201–500	1,170.00	2.10	14,035.00	25.20	126,300.00	227.00
501–1000	1,470.00	1.50	17,635.00	18.00	158,800.00	162.00
+ 1000	2,470.00	0.50	29,635.00	6.00	266,800.00	54.00

3.5.3 Customer Volume Pricing Plan

Under the Customer Volume pricing Plan (CVPP), customers may contract for a minimum monthly billing commitment (MMBC) for their services in return for a discount based on the amount of the commitment [4]. The MMBC is based on the monthly rates for the eligible services which are the inter–exchange and link components of Megaroute and Megastream.

The discount schedule is as outlined in Table II.

Table II: Customer Volume Pricing Plan (CVPP)

Monthly Billing Commitment ($)	Discount (%)					
	1 Year	2 Years	3 Years	4 Years	5 Years	10 Years
2,500	8	11	14	17	20	26
10,000	10	13	16	19	22	28
25,000	12	15	18	21	24	30
50,000	14	17	20	23	26	35
100,000	15	19	23	27	31	40
200,000	15	22	26	30	35	45
500,000	15	22	30	35	40	50
1,000,000	15	22	35	40	45	60

3.5.4 Megaroute Service

Megaroute service is offered by Telecom Canada for the digital transmission of information at 1.544 Mbps (DS–1) between two points in the same exchange or between exchanges or at 64 Kbps (DS–0) between exchanges [5]. Portions of the service are offered on a monthly basis , or on a one to five year minimum contract period. Inter–exchange channels of Megaroute service are also offered under the Customer Volume Pricing Plan.

3.5.4.1 Megaroute Service Components

The service includes the following components:

- * Access: This provides a jack–ended 1.544 Mbps interface and digital local loop form the customer premises to the serving wire centre in the exchange.
- * Link: This provides the Central Office equipment required to connect Accesses in the same wire centre, or to connect an access to a channel.
- * Channel: This provides the digital facility between wire centres.

3.5.4.2 Megaroute Rates and Charges

The rates and charges are on a monthly basis and relate to the Access, Link and Channel service components, as appropriate.

Rates and charges for the service are summarised in Table III and are subject to the discounts of the CVPP.

Table III: Megaroute Service, Summary of Rates and Charges

Item	Monthly Rate($)			Single Payment ($)	Service Charge ($)
	DS–0	DS–1	DS–3		
Intra–Exchange Service					
Construction	–	–	–	9,000	–
Access[6]	–	550	SFT	–	300
Link, each Wire Centre,	–	35	200	–	50/250
Channelizing, each Rate Centre[7]	–	135	–	–	125
Channel, each 400 metres	–	30	500	–	–
Inter–Exchange					
IX Link, each Rate Centre	30	300	3000		40/550 / 1500
Channels, Adjoining Exchanges, each mile	5	120	[8]	–	–
Channels, Non–Adjoining Exchanges	Rates per Table I.			–	–

3.5.4.3 Example Megaroute Network Costs

Tables IV and V outline the link transmission costs of an example 21 node national network using the rates and charges of Table III and applying the Customer Volume Pricing Plan of Table II as applicable on a 3 year contract term. This costing scenario is similar to that which will be required in the determination of costs for the Network.

Table IV approximates access, construction and link charges by assuming uniform access profiles at all nodes of one service point and a 4 Km local channel. Inter–exchange link charges of the example network are also included in Table IV.

[6] Reduced monthly rates for DS–1 Access are available based on the MCP (see the proposed tariff). Unchannelized DS–3 Access may be provided via an SFT. DS–0 access is not available.

[7] Required when a DS–1 Access must be connected to a DS–0 channels.

[8] Rates for DS–3 Channels between adjoining exchanges are per Table I.

Table IV: Example Megaroute Costs, Intra–Exchange and IX Link Charges

Item		Monthly Rate ($)	Single Payment($)	Service Charge ($)
<u>Intra–Exchange Charges</u>				
Construction, each node		–	9,000	–
Access, each node		460	–	300
Channel (4 Km), each node		300	–	–
Intra–Exchange Total, 1 node		760.00	9,000.00	300.00
Intra-Exchange Total, 21 nodes		**15,960.00**	**189,000.00**	**6,300.00**
<u>IX Link Charges</u>				
<u>Location</u>	<u># of Links</u>			
Victoria	1	300		550
Vancouver	2	600		1,100
Edmonton	3	900		1,650
Calgary	1	300		550
Saskatoon	2	600		1,100
Regina	2	600		1,100
Winnipeg	2	600		1,100
Thunder Bay	2	600		550
Sudbury,	2	600		1,100
Toronto	4	1,200		2,200
Waterloo	1	300		550
London	1	300		550
Hamilton	1	300		550
Kingston	3	900		1,650
Ottawa	2	600		1,100
Montreal	2	600		1,100

Table IV: Example Megaroute Costs, Intra–Exchange and IX Link Charges				
Item		Monthly Rate ($)	Single Payment($)	Service Charge ($)
Quebec	2	600		1,100
Fredericton	2	600		1,100
Halifax	1	300		550
Charlotteto wn	1	300		550
St–John's	1	300		550
IX Link Total, 21 nodes		**11,400.00**		**20,350.00**

Table V provides the inter–exchange channel charges associated with the example network. The CVPP discount is applied in Table V, and includes the discount associated with the IX link costs in Table IV.

Table V: Example Megaroute Costs, Inter–Exchange Channel Charges				
Route	Mileage	Monthly Charge ($)		
		DS–0	DS–1	DS–3
Victoria–Vancouver	62	862	10,338	93,048
Vancouver–Edmonton	514	2,241	26,887	242,068
Edmonton– Calgary	174	1,493	17,905	161,170
Edmonton–Saskatoon	329	1,861	22,326	200,983
Saskatoon–Regina	145	1,384	16,600	149,425
Regina–Winnipeg	334	1,871	22,452	202,118
Winnipeg–Thunder Bay	373	1,953	23,435	210,971
Thunder Bay–Sudbury	409	2,029	24,342	219,143
Sudbury–Toronto	212	1,615	19,377	174,424
Toronto–London	104	1,230	14,755	132,820
Toronto–Hamilton	37	588	7,050	63,450
Toronto–Waterloo	58	824	9,892	89,032
Toronto–Kingston	149	1,399	16,780	151,045

Table V: Example Megaroute Costs, Inter–Exchange Channel Charges

Route	Mileage	Monthly Charge ($)		
		DS–0	DS–1	DS–3
Kingston–Ottawa	90	1,122	13,460	121,160
Ottawa–Montreal	103	1,226	14,710	132,415
Kingston–Montreal	181	1,519	18,220	164,005
Montreal–Quebec	144	1,380	16,555	149,020
Quebec–Fredericton	226	1,645	19,730	177,602
Fredericton–Halifax	175	1,496	17,950	161,575
Halifax–St–John's	558	2,307	27,679	249,196
Halifax–Charlottetown	114	1,268	15,205	136,870
IX Channel Total, 21 nodes		31,313	375,647	3,381,537
Total Subject to Discount[9]		37,013	387,047	3,495,537
Discount[10]		6,662	100,632	1,223,438
Grand Total Inter-Exchange including IX Link, 21 nodes		**30,351**	**286,415**	**2,272,099**

3.5.5 Megastream Service

Megastream service is furnished for the transmission of voice, data and image information over digital channels in multiples of 64Kbps (DS–0)[6]. The service is not provided in all exchanges and is provided at the carrier's discretion within and between exchanges. Multipoint and multidrop configurations are not available. Portions of the service are offered on one to five year minimum contract periods. The inter–exchange channels of the service are also offered under the CVPP (See Tables I and II).

This service and its CN/CP equivalent may be appropriate for the provision of thin route links to the High Speed backbone.

[9] Total subject to discount includes the IX Link portion of Table IV.

[10] Discount assumes a three year commitment.

3.5.5.1 Megastream Service Components

The service may consist of up to five components:

Terminating Equipment: This provides the customer with the interface to the network at the individual circuit level and the ability to process line signals onto the DS–1 Access.

Access: This provides a DS–1 access channel to the serving wire centre in the exchange.

Link: This provides the Central Office equipment required to inter–connect Access channels with Megastream inter–exchange facilities.

Network: Channel charges apply in increments of DS–0 channels, and provide for transmission facilities between rate centres.

Network Management and Control System: Provides for network management and control capability at the customer location

3.5.5.2 Megastream Rates and Charges

The rates and charges are on a monthly basis and relate to Station (Terminating Equipment), Access, Link, Network and Network Management and Control charges.

The rates and charges associated with the service are similar to Megaroute for the access and link components with the DS–0 inter–exchange channels rated per Table I. Network management and control charges are optional.

3.5.6 Mach III Services

Mach III service is a service available from CN/CP which is equivalent to the Telecom Canada Megaroute and Megastream offerings [7]. The service is available in point–to–point applications in multiples of 64Kbps or 1.544 Mbps channels. The service components are very similar to the Telecom offerings with rates which are roughly 5% lower.[11]

3.5.7 Anikom 1000

Anikom 1000 is a service available from Telesat Canada which provides T1 or half T–1 capacity on the Ku band (14/12 GHz) satellite [8]. The service is comprised of the earth station at a designated location provided by the customer and the 14/12 GHz space segment.

[11] This paper assumes that CN/CP will maintain this rate relationship, i.e. 5% lower.

3.5.7.1 Anikom 1000 Rates and Charges

The monthly rates for the service inclusive of earth stations at both ends of a link and the space segment are outlined in Table VI.[12] Civil works, in addition to the rates in Table VI, are estimated at $25,000 per site.

Table VI: Anikom 1000 Rates

Transmission Speed	Monthly Rates ($)		
	Minimum Operating Term		
	One Year	Three Years	Five Years
1.544 Mbps	31,875	28,500	27,000
772 Kbps	Approximately half the 1.544 Mbps rate		

3.5.8 Anikom 500

Anikom 500 is a digital transmission service available from Telesat Canada at speeds ranging from 56 to 512 Kbps [9]. The service is available on a point to point or multi–point configuration. the service is comprised of one remote earth station at a designated location and the required 14/12 GHz space segment capacity. The operating term is one three or five years.

3.5.8.1 Anikom 500 Rates and Charges

The monthly rates for a three year operating term for each service used to provide a point–to–point configuration or a multipoint configuration are as shown in Table VII.

[12] The listed rates reflect a recent tariff filing by Telesat which has yet to be approved.

Table VII: Anikom 500 Rates

Transmission Speed	Monthly Rates ($)		
	Minimum Operating Term		
Kilobits per Second	One Year	Three Years	Five Years
56/64	2,095	1,885	1,775
128	3,765	3,385	3,195
192	6,205	5,585	5,275
256	6,915	6,225	5,875
320	10,250	9,225	8,705
384	13,030	11,725	11,605
448	15,810	14,225	13,425
512	17,475	15,725	14,84

3.5.9 Dataroute Service

Dataroute service is furnished for the digital transmission of data [13]. The service may be obtained for speeds up to 56Kbps and has a number of associated channel deriving arrangements. For the purposes of this section, the focus will be on the rates associated with 56Kbps capability.

3.5.9.1 Dataroute (56Kbps) Rates and Charges

In addition to a Dataroute Access Arrangement charges of $350 per month and a $250 service charge for each service point, the rates identified in Table VIII apply.

Table VIII: Dataroute (56 Kbps) Rates

Rate Distance	Base Charge ($)	Charge per Mile ($)
1–25	–	42.72
26–50	756	12.48
51–100	915	9.3
101–200	1470	3.75
201–500	1800	2.10
501–1000	2100	1.50
Over 1000	3100	0.50

3.6 NETWORK ACCESS COMPONENT: SERVICES

3.6.1 Introduction

As was noted earlier, there is a requirement to provide for low speed ubiquitous access to the Network in order to attract small users. This section provides a survey of public service offerings which could satisfy this requirement.

3.6.2 Message Toll Service

Dial access to a Network interface could be made available through the Public Switched Telephone Network (PSTN). For a user, the cost of access to the Network interface point is simply the cost of Message Toll Service (MTS). This is particularly suited to remote users (remote from an end node) who wish low speed access on an relatively infrequent basis.

3.6.3 Datapac

Datapac service provides for the use of a Public Data Network (PDN), called the Datapac network, for the transmission of packets of data [10]. An equivalent service is also available from CN/CP. This service is provided to customers located within or outside Datapac Serving Areas (DP.S.A.). The DP.S.A.'s are classified in three grades for the application of rates and charges: Direct Access, Extended Access to Dataroute Serving Areas and Extended Access to non Dataroute Serving Areas.
There are a number of arrangements associated with the service:

Datapac 3000: Synchronous access with Data Terminal Equipment (DTE) which conforms to the X.25 network access protocol. Public dial access at 2400 bps or dedicated access ranging from 1200 to 19,200 bps with the highest speed only available within a DP.S.A..

Datapac 3101: Asynchronous access for ASCII terminals up to 2400 bps.

Datapac 3201: Asynchronous polled device access up to 1200 bps .

Datapac 3303: Synchronous polled access.

Datapac 3304: Synchronous BSC (polled) EBCDIC access up to 9600 bps.

Datapac 3305: Synchronous BSC (contention mode) access up to 4800 bps.

The ubiquitous nature of the service makes it a good candidate for access to end nodes on the Network.

3.6.4 Anikom 200

Anikom 200 service is an interactive data service available from Telesat Canada using Very Small Aperture Terminal (VSAT) technology [11]. The service is available in two options. Option 210 is configured for a single customer.

Option 210 service is available at speeds from 2.4 to 19.2 Kbps and 56 Kbps with each speed being capable of supporting a single protocol. The service is available in one month, one year, three year and five year terms. Under a three year term, the service ranges in price from $700 per month for a 2.4 Kbps service to $5,800 per month for 56 Kbps service.

The Anikom 200 VSAT may be equipped with up to 15 data ports , and must be obtained separately through Telesat.

3.6.5 Datalink Service

Datalink is a point to point digital circuit switched service, which provides synchronous data transmission at speeds of 2400, 4800 and 9600 bps [12]. The service is provided on the basis of a fixed monthly access rate in addition to network usage charges which are both distance and time sensitive. This service may be too expensive to use as a low speed Network access arrangement. For example, a 9600 bps access is $350 per month, in addition to usage charges which would vary from $0.20 to $0.78 per minute depending on the rate distance.

3.7 CONCLUSIONS AND RECOMMENDATIONS

This section has outlined the services available for the link transmission component of the High Speed Subnetwork as well as the services which could provide low speed and remote access to the Network.

The most likely candidates to satisfy the link requirement are the Telecom Canada Megaroute offering as well as the CN/CP Mach III service. The Telesat Anikom 1000 would be a good candidate for the provision of a parallel high Speed Subnetwork based on satellite technology. Thin route backbone links could also be satisfied with Megaroute at the DS–0 speeds or the equivalent or Mach III service. Dataroute (56Kbps) may be appropriate for certain locations which are not served by the Megaroute/Megastream offerings. Anikom 500 could be the satellite equivalent.

Low speed access from remote locations could use Anikom 200 service, in addition to Datapac and dial up service on the PSTN. Suitable interconnection to public carrier services at the Network end nodes could provide low speed ubiquitous access for small users.

It is recommended that the costing of the High Speed Subnetwork use rates which reflect the recent carrier applications to the CRTC.

3.8 REFERENCES

1. CRTC Telecom Public Notice 1990–11, Bell Canada – Restructuring of Rates for Competitive Network Services, Ottawa, 1 February 1990.

2. CRTC Telecom Public Notice 1990–15, British Columbia Telephone Company – Restructuring of Rates for Competitive Network Services, Ottawa, 9 February 1990.

3. Bell Canada General Tariff (Proposed), CRTC 6716, Item 5060, Inter–Office Digital Channels, Issued 1990 01 25.

4. Bell Canada General Tariff (Proposed), CRTC 6716, Item 5050, Customer Volume Pricing Plan, Issued 1990 01 25.

5. Bell Canada General Tariff (Proposed), CRTC 6716, Item 5060, Megaroute Service, Issued 1985 05 15.

6. Bell Canada General Tariff (Proposed), CRTC 6716, Item 5030, Megastream Service, Issued 1990 01 25.

7. CN/CP General Tariff, CRTC 4001, Part XIV, Mach III Services, Issued 1988 10 14.

8. Telesat Canada General Tariff, CRTC 8015, Item 4.0, Anikom 1000 Service, Approved December 5, 1986.

9. Telesat Canada General Tariff, CRTC 8017, Item 4.0, Anikom 500 Service, Approved August 28, 1987.

10. Bell Canada General Tariff, CRTC 6716, Item 4700, Datapac Service, Issued 1989 08 01.

11. Telesat Canada General Tariff, CRTC 8018, Item 4.0, Anikom 200 Service, Approved April 5, 1988.

12. Bell Canada General Tariff (Proposed), CRTC 6716, Item 4685, Datalink Service, Issued 1990 01 25.

13. Bell Canada General Tariff (Proposed), CRTC 6716, Item 4680, Dataroute Service, Issued 1990 01 25.

4. THE IMPACT OF ISDN

4.1 SUMMARY

This section initially reviews ISDN technology and then exposes ISDN issues which may impact the Network. The section does not restrict itself to a technology view but attempts to expose economic as well as implementation matters. The section proposes that although current narrowband ISDN is not consistent with the objectives of the Network associated with the transportation of large amounts of data at high speeds, it should nonetheless be viewed as a key technology associated with other aspects of the Network's development. The section recommends that a specific ISDN strategy be developed for the Network which recognises:

- That BISDN will probably supplant private leased line alternatives as the most economic basis for the provision of the Network by the end of this decade.
- That narrowband ISDN is an important technology for the carriers and that support for the Network initiative could be fostered through the development and eventual provision of an appropriate Network ISDN interface.
- That information technology researchers will need to access ISDN technology.
- That certain users with a less developed research infrastructure may require an economical low speed Network access such as narrowband ISDN.

4.2 INTRODUCTION

The Integrated Services Digital Network (ISDN) represents an enabling technology sponsored by common carriers which promises to integrate a user's communications requirements (voice, data, video) over a high speed digital network with access provided through one simple universal interface. In the 1970's, ISDN was a vision of the Public Switched Telephone Network (PSTN) of the future. The vision anticipated the inefficiency and cost associated with building separate voice and data networks given the emerging benefits of digitization. At that time ISDN grew from the benefits which the telecommunications carriers foresaw for the management and design of their own networks.

In the 80's the technology began to be deployed. Field and market trials as well a custom, though mainly private, implementations developed throughout the decade. The decade also saw the development of a new view of the evolution of the technology. The earlier vision, which could be termed narrowband ISDN, foresaw speeds up to approximately 1.5 Mbps. The new vision foresaw the development of a Broadband ISDN (BISDN) with access speeds in the 100's of Mbps range. This newer vision was closely linked with the development of fibre based technologies as well as the perceived limited bandwidth capability of the narrowband version for certain applications.

ISDN is a key technology in the development of the public telecommunications network of the future. A preliminary assessment of the impact of the technology on a High Speed Network for Research and Development (the Network) is required and is the purpose of this section.

4.3 RELEVANCE TO THE STUDY

Two of the major objectives of the Network are (1) to provide a high speed communications capability to researchers at reasonable cost and (2) to provide access to key communications technologies to a subset of these researchers whose main interests lie in information technology research.

In terms of providing a high speed communications capability at reasonable cost, two issues must be addressed. One, there is the question of the design of the backbone network itself and two there is the question of user access to that backbone. It is quite clear that narrowband ISDN which is currently limited to T1 speeds cannot meet the objectives of the backbone requirement which will most likely evolve beyond T1 very quickly. Narrowband ISDN may however be a suitable as a ubiquitous low speed access by certain users.

BISDN may however be a serious contender in the provision of the backbone capability by the end of the decade. The fact that BISDN would be offered on the public network suggests potential cost savings relative to private leased line type of networking alternatives.

On the matter of providing access to key communication technologies, the Network must be sensitive to the importance of ISDN as a technology for the provision of public telecommunications services. The technology is important to the carriers and the development of such programs as Vision 2000 suggest that research will be carried during this decade on personal communications using public infrastructures. These communications will most likely include voice, video and data transmission. ISDN will necessarily be a key ingredient to this strategy. Both the narrowband and broadband versions will likely require access by information technology researchers. The Network must therefore make provision for access by researchers to both the narrowband and broadband varieties as they develop.

The objectives of this section are therefore (1) to provide a brief review of the current state of the technology including an estimate on the availability and pricing of both narrowband ISDN and BISDN and (2) to develop in more detail the issues involved in developing a Network ISDN strategy.

4.4 ISDN: THE TECHNOLOGY

4.4.1 The ISDN Concept and Architecture

The ISDN concept is that of a network, in general evolving from telephony Integrated Digital Network (IDN), that provides end–to–end digital connectivity to support a wide range of services, including voice and non–voice services, to which users have access by a limited set of standard multi–purpose user–network interfaces.

As can be seen from the definition, ISDN has both a technology aspect and service aspect. The technology aspect is currently defined in terms of two types of integrated ISDN access: the Basic Rate Interface (BRI) and the Primary Rate Interface (PRI). BRI refers to access to a 144 Kbps digital stream which is organized into two 64 Kbit/s bearer or B channels and one 16 Kbit/s signalling, called data or D channel. Figure 1 illustrates the ISDN Architecture Model.

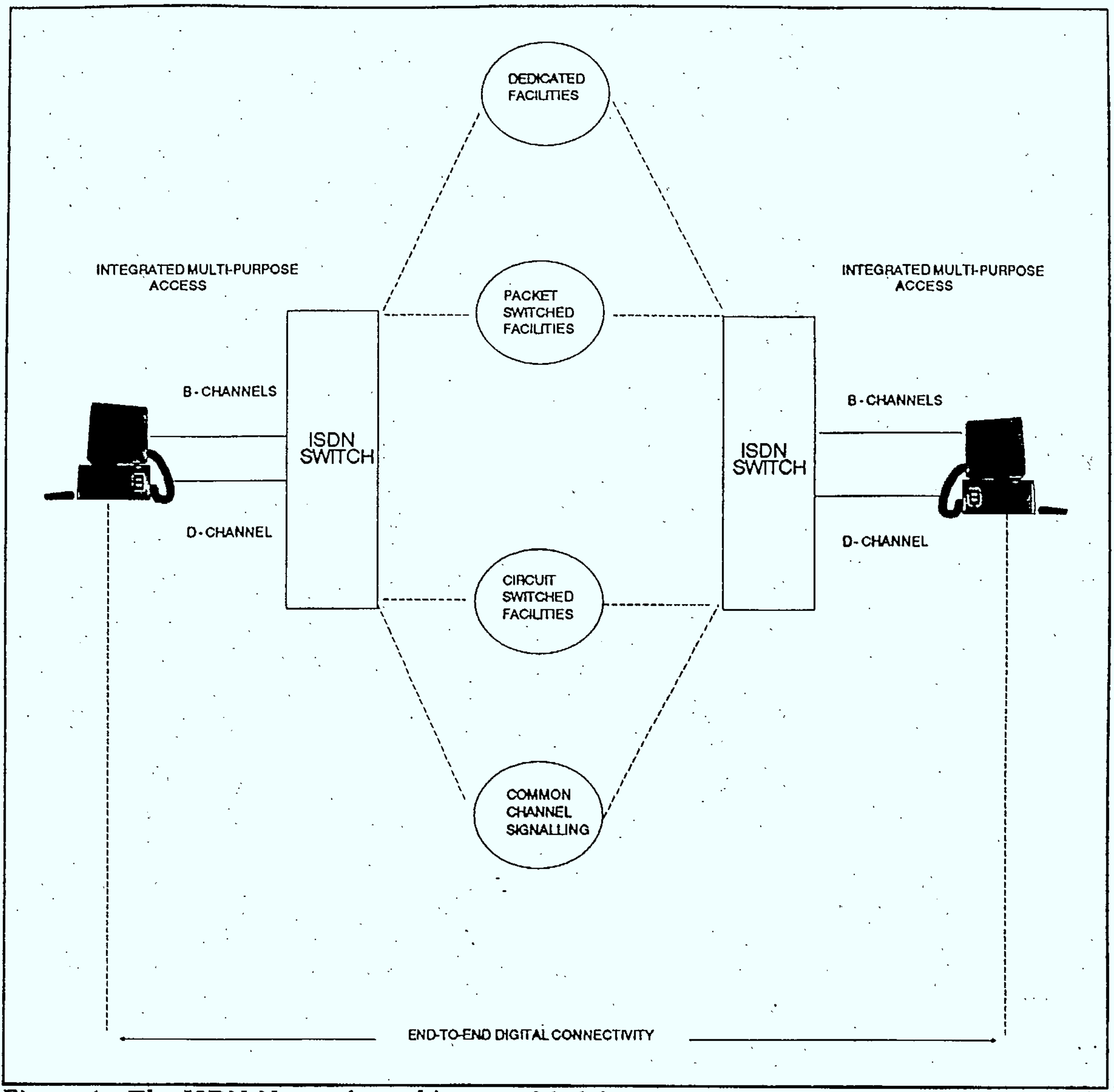
DEDICATED FACILITIES
INTEGRATED MULTI-PURPOSE ACCESS
PACKET SWITCHED FACILITIES
INTEGRATED MULTI-PURPOSE ACCESS
B-CHANNELS
ISDN SWITCH
ISDN SWITCH
B-CHANNELS
D-CHANNEL
D-CHANNEL
CIRCUIT SWITCHED FACILITIES
COMMON CHANNEL SIGNALLING
END-TO-END DIGITAL CONNECTIVITY

Figure 1: The ISDN Network Architecture Model

In North America the PRI access refers to a 1.544 Mbit/s digital stream and is organized into twenty–three 64 Kbit/s B channels and one 64 kbit/s D channel. Twenty–four 64 Kbps channels are equivalent to one T1 channel which is a terrestrial carrier system providing 24 voice channels over a 1.544 Mbps line. In Europe, the PRI has a 2.048 Mbps bandwidth and is referred to as 30B+D. Although there is a difference in the bandwidth of the North American and European PRI, the B and D channels are nonetheless directly compatible. PRI access also offers allocatable higher–speed H channels or mixtures of H and B channels. Both the PRI and BRI accesses may be termed narrow band ISDN. They are summarised in Table I.

Interface	Gross Bit Rate	Structure
BRI	192 Kbps	2B + D16
PRI	1.544 Mbps	23B + D64 3H0 + D64 H11

Note: B = 64 Kbps, H0 = 384 Kbps, H11 = 1.536 Mbps

Table I: Narrowband ISDN Channels

As a service concept, ISDN categorises telecommunications services as either Bearer Services or Teleservices. Bearer Services refer to access by the user to different parts of the high speed digital stream. The Bearer Service provides the underlying transport connections and network functions which permit end–to–end information transfer between two ISDN customer interfaces. Examples of Bearer Services include circuit mode digital (64kbps), circuit mode voice (64kbps) and packet mode data (16kbps). Higher speed ISDN Bearer Services have yet to be fully defined, however one would expect to see an unrestricted high speed digital transmission service as well as a high speed packet service.

Teleservices are higher level services which provide the full capability for communication between users including terminal equipment functions. Teleservices are built upon bearer services. Examples of Teleservices include telephony, videotext and message services. Higher speed Teleservices would likely include high speed file transfer, database retrieval services, directory services, imaging services such as facsimile as well television distribution.

The need for services requiring higher bit rates than catered for in the narrowband portfolio was recognised in the mid 80's. This need led to the development of the BISDN concept. BISDN is still at the level of discussion within standards bodies such as the CCITT, T1 and CEPT in Europe. The literature suggests that the service will be closely aligned to the emerging Synchronous Optical NETwork (SONET) standards and will rely on new high speed packet switching technologies such as Asynchronous Transfer Mode (ATM) being available in carrier networks. BISDN access speeds currently being discussed are in the 150 Mbps range [HAND 89].

4.4.2 ISDN Interface Reference Points

The ISDN architecture is based on the specification of services provided to applications through customer premises terminal equipment (CPE). CPE might include personal workstations or host computers in either a standalone or Local Area Network (LAN) environment. As noted earlier, these services are categorised as Bearer Services or Teleservices. Figure 2 illustrates the ISDN Functional Reference Model for the Configuration of CPE.

ISDN identifies two communication contexts or planes. The User Plane and the Control Plane. The User Plane relates to user information transfer while the Control Plane relates to signalling information between the user's terminal equipment and the network in order to establish a Bearer Service. All signalling information is passed over the D channel.

Both the User and Control planes share the same physical channel interface, either BRI or PRI access. In the Control Plane, signalling is provided across an interface between the user and the network termed NT1 when functions broadly equivalent to Layer 1 (physical) of the OSI reference model are supported or NT2 when additional higher layer protocols are also supported. The NT1 device performs functions such as signal conversion, and the maintenance of electrical parameters. The NT2 is a device responsible for connecting user equipment to the ISDN and typically performs multiplexing and switching functions. PBX's and LAN gateways would be examples of NT2's.

In the User Plane, service is provided at Layer 2 or higher, depending upon the nature of the service, with user information exchanged through the circuit switched, semi–permanent or permanent B or H channels. New packet mode Bearer Services are expected to extend this to the D channel.

As illustrated in Figure 2, reference points are defined relative to CPE. The S and T reference points are located on the terminal side of the NT1 with the U reference point located on the network side. The S and T reference points define the operation of a user's terminal equipment relative to the network while the U reference point defines the interface to the carrier's switching node.

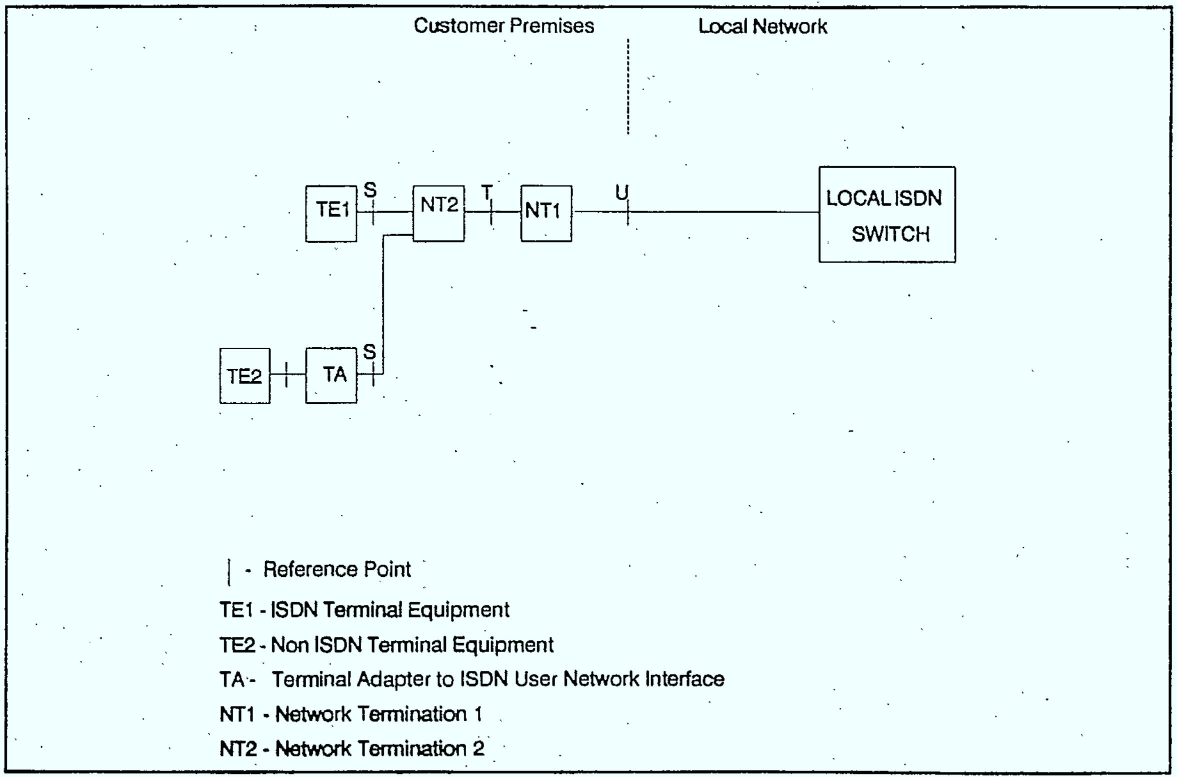
Customer Premises
Local Network
TE1
S
NT2
T
NT1
U
LOCAL ISDN SWITCH
TE2
TA
S
| - Reference Point
TE1 - ISDN Terminal Equipment
TE2 - Non ISDN Terminal Equipment
TA - Terminal Adapter to ISDN User Network Interface
NT1 - Network Termination 1
NT2 - Network Termination 2

Figure 2: ISDN Functional Reference Model

The TE1 is any ISDN terminal equipment which has an ISDN physical Layer interface to an ISDN network termination (either NT1 or NT2) and is capable of ISDN signalling for service access. A standalone ISDN workstation or host computer would fall into this category.

The TE2 is any equipment which is equipped with a non–ISDN physical interface such as V.24 or X.21 and which accesses ISDN Bearer Services through a Terminal Adapter (TA). The TA provides the TE2 with the necessary physical interface and signalling capabilities.

4.4.3 ISDN Standards

The CCITT has fully defined standards for the interfaces at the S and T reference points for both BRI and PRI access. A standard for the U interface has not been addressed by the CCITT, since in Europe it is assumed that he carrier will own the NT1. However one is being developed in the United States where NT1 ownership will most likely be competitive.

Committee T1 of the Exchange Carriers Standards Association in the U.S. has standardised a U interface for BRI access on copper pairs[1] and is developing one for PRI access based on the existing T–1 Extended Superframe Format (ESF). It is expected that competitive pressures will force the development of similar standards in Canada as the technology is deployed. Earlier this year the Department of Communication's ISDN Advisory Committee recommended that Steering Committee on Telecommunications (SCOT) of the Canadian Standards Association (CSA) develop a Canadian standard for the U interface [COMM 89]. It is expected that the next version of CS–03 will address this matter.

Optical Carrier Level	Electrical Equivalent	Line Rate (Mbps)
VT1.5	DS–1 (1.544 Mbps)	1.728
OC–1	STS–1 DS–3 (44.73 Mbps)	51.84
OC–3	STS–3	155.52
OC–12	STS–12	622.08
OC–48	STS–48	2488.32

Table II: Sonet Interfaces

[1] The U interface for BRI access on copper pairs is based on Echo Cancelling Hybrid technology and 2B1Q transmission coding (ECH–2B1Q). See AT&T ISDN Basic Rate Interface Specification, Part II–B, AT&T Technical Reference, Publication 801–802–100, June 1988.

It is also anticipated that equivalent standards will develop in both Canada and the U.S. for ISDN interfaces on fibre optic media. The SONET standards being developed by the CCITT are intended to provide a non–proprietary standard for high–speed network operations, permitting multi–vendor internetworking. Although SONET was originally conceived to provide a standard optical transmission path for inter–office trunks in the carrier network, it quickly became the favoured candidate for a high capacity BISDN medium. It is being suggested that SONET should be able to provide a 155.52 Mbps user interface in the near future [MILL 89]. Table II summarises the various SONET interfaces.

The 155.52 Mbps interface is called STS–3/OC–3 because it is three times the basic SONET rate of 51.84. OC is the photonic interface and STS is the electrical equivalent. SONET transmission equipment will interleave STS's to form a synchronous high speed signal. This permits access to lower speed signals without multistage multiplexing and demultiplexing. The low speed signals are mapped into sub–STS–1 signals called Virtual Tributaries (VT's).

Phase 1 of the SONET standard was adopted in March 1988, and Phase 2 is scheduled for completion in February 1990. It is anticipated that this standard will be used in the definition of a U interface for fibre media.

4.4.4 Private/Public ISDN's and Internetworking

ISDN may be implemented on either public or private networks. In the case of the public version it could take a number of forms which are roughly equivalent to current public service offerings. Current offerings include, for example, trunk service for Private Branch Exchanges (PBX's), Individual Business Line (IBL) or Information System Access Line (ISAL) service for the single line business customer and Centrex service for the customer who wishes the additional capability of internal intercommunication within his organisation. It is anticipated that ISDN as a public service will be offered in a similar manner.

For the Centrex customer this would mean a number of BRI accesses provided by the carrier which would provide for a private voice and data network internal to the customer's organization as well as access to the public wide area ISDN. For subscriber's with ISDN PBX's on their own premises, an NT2 in ISDN terms, a PRI access would provide digital trunking to the carrier's Central Office (CO). The customer could therefore exchange voice and data information between local TE1's through the PBX or communicate with remote TE1's on the public network. For the single line customer, a BRI would provide integrated voice data access to the public network for a digital phone/PC combination. All of these applications provide access to the public network.

Private ISDN's refer to custom networking applications where the facilities and infrastructure of the carrier networks may be used but where the participants on the network form a closed private group, e.g. non–public. The networking of customer owned ISDN PBX's through the leasing of interconnecting channels from the carriers is such an example. Another example, termed Virtual Private Networks (VPN's), refers to the use of the public network where separation from the public network's services is done through the setting up of a logical topology in the ISDN switch.

The CCITT has recognised the need for internetworking between a public ISDN and other networks including a dedicated private network. These are in a set of ISDN Internetworking Recommendations, the I.500 series.

4.4.5 Price and Availability

The availability of narrowband ISDN is closely tied to the perceived market for the service by the carriers. The network infrastructure and equipment is already in place to provide the narrowband version of the service and is not an issue. The issue is more closely tied to the penetration of the service into the marketplace.

A recent study on the matter commissioned by the DOC suggests that penetration over the next five years will be extremely difficult [CSRC 89]. The report strongly suggests that initial penetration will be through Centrex and that this penetration will have more to do with Centrex than ISDN. Existing data networks and accesses are considered quite adequate. Integration is not a burning issue. Commercial service of basic rate for Centrex III and primary rate for PBX's is currently forecast by the end of 1991. It is anticipated that narrowband ISDN will not exhibit significant penetration into the single line market until the late 90's.

Statements from some manufacturers and market analysts talk of the availability of pockets of carrier provided BISDN in the U.S. as early as 1993. These forecasts are considered rather optimistic in terms of the Canadian environment. Although equipments and technologies have been recently announced which could form the basis of BISDN delivery, for example Northern's Fiberworld, their introduction into the public network in Canada under the current regulatory regime is another issue altogether. Field trials of these products in the Canadian public network are scheduled this year, however large investments in earlier generation digital switching technology which will most likely need significant upgrading to address this service are relatively recent.

The carriers have historically introduced new technologies of similar significance and impact over many years and are currently committed to the introduction of narrowband ISDN. Short of a significant change in the monopoly status of the dominant carriers in the near future, there is no reason to expect that this trend would change. In addition, standards have yet to be developed for the provision of the service. More realistically, BISDN availability on the public network should be expected no earlier than the end of the decade.

Recent statements from Bell Canada suggest that tariffs for both Centrex BRI access and PBX PRI access will be filed late this year [CHAG 89]. For access from the customer's premises to the switching centre, there would be a flat monthly charge in addition to usage and link charges associated with the service accessed, for example Datapac. Monthly flat rates that have been discussed include $50 per line for Centrex BRI and $1500 for PBX PRI.

4.5 ISDN AND THE NETWORK: ISSUES

4.5.1 Introduction

As was noted earlier at the outset, two of the major objectives of the Network are (1) to provide a high speed communications capability to researchers at reasonable cost and (2) to provide access to key communications technologies to a subset of these researchers whose main interests lie in information technology research. The development of an ISDN strategy for the Network must recognise the importance of these objectives. It is also apparent that ISDN is more than just a technology. It is the wave of the future in the provision of public telecommunications services. The feasibility study must therefore develop an ISDN strategy for the Network which recognises this fact. This part of the section will attempt to raise certain issues associated with the development of such a strategy.

4.5.2 The ISDN Architecture and the Network

Certain aspects of the narrowband ISDN architecture limit its usefulness in the context of the envisioned Network. The architecture is based on the notion of circuit switched 64 Kbps channels. This contrasts with the connectionless mode of operation associated with high speed LAN's. B channels in the ISDN are allocated to voice and clear data exchanges with the channel allocation controlled through the D channel. A slower speed packet bearer service is available over the D channel. This architectural approach is not consistent with the Network's view of an architecture associated with a high speed research network. The requirements of high speed bursty traffic go against the notion of a circuit switched approach.

It is also apparent that narrowband ISDN did not envision the proliferation of high speed LAN's. The architecture is more closely aligned to stand–alone terminals than LAN stations. For example there is no provision for a TE1 to access an 802 LAN. COBB 89 provides a thorough discussion of this aspect. This fact is somewhat limiting in that most Network interconnects will probably be through local high speed networks.

If there is a requirement for LAN stations to access an ISDN, we are therefore left with the option of developing an ISDN Interface for the LAN proper. For terminals which are not interconnected through a LAN but which are standalone, the question of access to the Network via an ISDN also centres on the availability of an ISDN interface somewhere on the Network.

The next question to address is whether there is a need to provide such an ISDN interface. Before addressing this issue a few words on BISDN. Indications are that the BISDN will not evolve using the channelized approach of narrowband ISDN. Sonet and the evolving BISDN will most likely use more dynamic bandwidth allocation techniques which are based on Asynchronous Transfer Mode (ATM).[2] We can therefore foresee the possibility of a compatible architecture developing on the public network. However this is not foreseen before the end of the decade.

4.5.3 The Need for an ISDN Interface

Narrowband ISDN may be relevant in the evaluation of user access options to the Network. As noted earlier, it is anticipated that narrowband ISDN service will be available in early 1992 in the form of Centrex BRI and PBX PRI.

Under the Centrex BRI configuration the user has a number of 2B + D connections (a minimum of 2 and most likely a few hundred)[3] from individual users on campus to a local

[2] Current suggestions are that Sonet will be using a STM/ATM hybrid in order to accommodate present day services [MILL 89].

[3] A recent tariff filing by Bell Canada would offer Centrex III service to as few as two locals. See CRTC Public Notice 1990–14, Ottawa, 9 February 1990.

carrier switch. In addition to public and intercom voice, the service provides the user with a 64 Kbps clear channel data capability for both internal communications and access to remote systems. The internal capability does not measure up to current LAN speeds and would certainly be considered unacceptable in a research environment. However access to remote systems at 64 Kbps is certainly an improvement over 9600 bps or 19.2 Kbps data access using either the PSTN or PDN. But certainly not as part of a Centrex configuration. More likely as part of a PBX PRI.

The PBX PRI is relevant if the user already has an investment in a PBX which is easily upgradable to ISDN PBX. There may be many academic institutions which fall into this category and who only require low speed access. I'm thinking here of community colleges or smaller universities who may want access but who do not have a high bandwidth requirement. Provincial support of the Network initiative may well be contingent on such access. Recent cost figures suggest that upgrading an existing SL–1 for PRI access would be in the $15,000 range [ANGU 89]. PRI access in chunks of 23B+D channels could provide for both public interconnection as well as interconnection to the Network via dedicated 64 Kbps data channels. It is not clear whether the carriers will be initially providing the higher speed H channels.

Under this PBX PRI scenario, the Network need only provide one physical ISDN interface to the carrier's ISDN. Access to the interface could be in the form of Private Virtual Service (PVS) using the carrier's public facilities. We have mentioned that this alternative may be attractive to certain users. It may also be attractive to carriers in terms of service development and to certain manufacturers in terms of product development.

The Network must also be sensitive to the importance of ISDN as a technology for the provision of public telecommunications services. The development of such programs as Vision 2000 suggest that important research will be carried during this decade on personal communications using public infrastructures. ISDN will necessarily be a key ingredient to this strategy. Both the narrowband and broadband versions will likely require access by certain researchers. The Network should therefore make provision for eventual use of both the narrowband and broadband varieties. The development of a Network ISDN interface for dedicated data channels is not inconsistent with this requirement. However, it may not be sufficient to satisfy research in the voice aspects of the service. This item should be investigated further with certain key players such as BNR. It is not clear whether there is a requirement for this type of capability.

4.5.4 The Impact of BISDN on the Study

In the longer term, the Study may wish to consider the possibility of BISDN availability for both access and the backbone. Its significance to the Study at this stage is mainly in terms of projecting the long term costs of the Network. The BISDN scenario is only considered feasible at the end of the decade.

With BISDN, a PVS could be provided directly by the carrier for the complete backbone network as well as selected high speed user accesses. Network costs under such a scenario are difficult to predict. User costs for emerging high speed Metropolitan Area Network (MAN) services such as Switched–Multi Megabit Data Service (SMDS) from the BOC's in the U.S. may provide a clue as to their magnitude. Early availability SMDS ('91/'92) is currently being described in terms of T1 and T3 access [MCRO 89]. This suggests that access prices well within the current tariff suggestions of PBX PRI e.g. $1500 per access per month with additional usage sensitive charges based on service use.

A BISDN scenario is also important in the development of a vision of the Network at the beginning of the next century. As strategies associated with Network migration are developed and the benefits of information technology research are discussed, BISDN will probably surface as a key Network technology of the future.

4.5 CONCLUSIONS AND RECOMMENDATIONS

This section has proposed that although current narrowband ISDN is not consistent with the objectives of the Network associated with the transportation of large amounts of data at high speeds, it should nonetheless be viewed as a key technology associated with other aspects of the Network's development.

The section highlights that a specific ISDN strategy be developed for the Network which recognises

(1) That BISDN will probably supplant private leased line alternatives as the most economic basis for the provision of the Network by the end of this decade.

(2) That narrowband ISDN is an important technology to the carriers and that any implementation should address this fact through the development and eventual provision of an appropriate narrowband ISDN interface. In addition to providing IT researchers access to a key technology, carrier support is developed for the Network initiative.

(3) That certain users with a smaller bandwidth requirement may opt for a low speed ubiquitous access such as narrowband ISDN and that these users may well represent an important constituency related to support of the program.

It is proposed that the ISDN strategy for the Network be developed with the carriers and certain key manufacturers in order to expose in more detail the uses which they would make of such an interface, if it were available, and the current status of a product to satisfy the requirement.

4.6 LIST OF ACRONYMS

ATM	Asynchronous Transfer Mode, a switching technique
B channel	Bearer Channel in ISDN
BISDN	Broadband ISDN
BRI	Basic Rate Interface in ISDN
CCITT	Comite Consultatif International Telegraphique et Telephonique
Centrex	A Common Carrier service
CO	Central Office
CPE	Customer Premise Equipment

CSA	Canadian Standards Association
D channel	Data Channel used for signalling in ISDN
ESF	Extended Superframe Format, format of a T1 bitstream
H channel	Higher speed channel (>64 Kbps) in ISDN
IBL	Individual Business Line
IDN	Integrated Digital Network in ISDN
ISAL	Information System Access Line, a Bell Canada tariff for a data IBL
ISDN	Integrated Service Digital Network
LAN	Local Area Network
NT1	Network Termination 1 in the ISDN reference model
NT2	Network Termination 2 in the ISDN reference model
OC	Optical Carrier
OSI	Open Systems Interconnection
PBX	Private Branch Exchange
PRI	Primary Rate Interface in ISDN
PSTN	Public Switched Telephone Network
SCOT	Steering Committee on Telecommunications
SONET	Synchronous Optical Network
STS	Electrical equivalent to OC in SONET
T1	A digital transmission system operating at 1.544 Mbps
T1	A committee of the American National Standards Institute
TA	Terminal Adapter in the ISDN reference model
TE1	Terminal Equipment 1, ISDN compatible
TE2	Terminal Equipment 2, not ISDN compatible
V.24	A Physical layer standard
VPN	Virtual Private Network
VT	Virtual Tributary in SONET
X.21	A Physical layer standard

4.7 REFERENCES

1. [COMM 89] Communications Canada, ISDN Canada, Report on ISDN Implementation in Canada, March 1989.

2. [ROBE 87] Roberts, M, ISDN in University Networks, IEEE Communications Magazine, vol 25 n 12, 1987 pp36–39.

3. [CHAG 89] Chagnon, P, ISDN: Graceful Evolution to the Future, Engineering Dimensions, Sept/Oct, 1989 pp25–27.

4. [ANGU 89] Angus, I, Bell Canada Tariffs ISDN for Private SL–1 Networks, Telemanagement, vol 7 n70, 1989 pp4–6.

5. [HAND 89] Handel, R, Evolution of ISDN Towards Broadband ISDN, IEEE Network, January 1989 pp7–13.

6. [CSRC 89] Communications Sciences Research Corporation, Preliminary Study of Economics, Markets, and Potential Demand for ISDN Services, Report prepared for the Department of Communications, July 1989.

7. [MILL 89] Miller, T, Sonet and BISDN: A Marriage of Technologies, Telephony, May 15 1989 pp32–38.

8. [COBB 89] Cobb, A, Prospective ISDN Applications for Academic Networks, York University, April 3 1989.

9. [MCRO 89] McRoberts, J, Schnitzer, R, Switched Multi–megabit Data Service: broadband data for the 90's, Blenheim Online Publications, 1989 pp187–196.

5. CONFORMANCE AND PROTOCOL TEST

5.1 SUMMARY

Conformance and testing issues are important for the Network from two viewpoints: the Network must ensure that new equipment to be added does not impair ongoing operation, and secondly the Network may provide facilities to support the provision of testing services to its clients. Both of these viewpoints stem from the Network's objective to facilitate the development of information technology products and services for domestic and international markets. To meet the needs of the international market, the Network must follow the conformance and certification procedures which are being developed internationally.

5.2 INTRODUCTION

Conformance and Testing issued are considered under two categories. Firstly, equipment must be tested prior to being attached to the Network if this equipment could disrupt the operation of the Network. Secondly, the Network may be used to provide testing facilities as a service to users.

The prior testing of products and services will be an essential process associated with procurement and network management. Testing not only includes the use of tests explicitly designed to determine an equipment's compliance to a given standard, it must also include interoperability testing, performance testing, and other testing normally associated with the purchase of equipment and services. These latter aspects of acceptance testing will not be considered further in this section since they are normal activities associated with procurement and are not unique to the Network application.

The provision of testing services over the Network will require more attention than other services offered by the Network since the injection of test information, if not correctly controlled, might interfere with normal Network traffic. Such testing will be restricted to certain layers of the OSI model and will also require special arrangements to be made with the test service supplier.

5.3 RELEVANCE TO STUDY

The Network is expected to support the R & D user by providing user friendly access to services and, at the same time, to serve as a basis for the development of information technology equipment and services. These potentially conflicting objectives must be resolved by the careful management of the introduction of new equipment. This equipment will need to be tested for conformance to applicable standards to ensure that their introduction does not impair the ongoing operation of the Network.

To facilitate the development of products and services to the ISO standards, it will be appropriate to support ISO testing services over the Network. Since this support may require special technical provisions in the Network, they are considered in this section.

5.4 BACKGROUND

The ultimate objective of conformance and testing programs is the provision of a guarantee to a purchaser that the cited equipment or service is compliant with the referenced standards and that it will interoperate correctly with other conforming implementations.

It is generally accepted that the complexity of the OSI standards will make full interoperability testing difficult if not impossible. However, a growing body of internationally recognized test procedures is becoming available that will minimize incompatibility by providing a uniform approach to *conformance* testing. Such *conformance* testing is directed towards the verification of compliance to the relevant international standards. Since such testing can never completely explore the full range of interactions that could occur between specific implementations of these standards, they cannot be expected to completely guarantee interoperability. Thus, in addition to *conformance* testing, *ad-hoc interoperability* tests are used to augment the testing. Although not formal, these ad-hoc tests are considered an essential adjunct to a testing program.

The High Speed Network will require testing for new equipment prior to attachment to the Network and is expected to offer testing services to facilitate the development of products and services for the international market.

5.5 TESTING OF NETWORK EQUIPMENT

New equipment to be attached to the network must not disturb the ongoing "operational" role of the network. Some of this new equipment may be experimental equipment which may be highly suspect. Several categories of new equipment might be considered, from fully certified commercial equipment to highly experimental equipment. While Network Management will control the attachment of such equipment, it will be necessary to provide a mechanism for conformance testing. Conformance testing may involve the complete certification of the equipment for day to day operational use or may merely certify that the equipment is "benign".

It will be important to not unduly restrict the attachment of experimental equipment so that information technology research may be facilitated. This objective must be balanced with the need to protect the operation of the Network.

The *Network Architecture and Migration Plan* section has proposed that the Network will consist of an assembly of subnetworks internetworked through the use of the ISO Internet Protocol. Using this model, subnetworks are isolated from other subnetworks by the ISO Router equipment. Applications and protocol elements above the Network Layer are individually addressed by their Network Address as discussed in the *Network Addressing, Directory and Routing* section, and the *Network Security and Access Control* section recommends that closed user groups based on Network Addresses be defined for certain user groups.

This architecture will facilitate the following approach to conformance and protocol testing:

1. For transmission and subnetwork equipment related to the lower three layers of the OSI model, testing must be carried out by the administration of the

subnetwork to ensure that the new equipment does not affect the ongoing operation of the subnetwork. Thus, for example, the introduction of a new T1 line must follow testing to the constraints imposed by the wide area network equipment.

2. Only restricted testing of selected components of the Network Layer will be feasible in the on–line portion of the Network. Other components will need to be tested off–line. The *Network Architecture and Migration Plan* section recommends that a Network Emulation Facility be provided to support such testing.

3. For protocol implementations above the Network Layer, these must be tested to the requirements of the respective end system protocol stack, and this may be facilitated by the ISO testing service to be discussed in the next section. A closed user group address on the Network would permit such testing to be carried out without affecting an operational implementation of the same protocol stack. For example, the testing of an X.400 Electronic Mail implementation would be carried out using a unique remote Network Address which has been allocated to the X.400 test function.

5.6 CONFORMANCE TEST SERVICES

The Canadian Interest Group on Open Systems (CIGOS) proposed test centre is a significant initiative which is relevant to this issue, as are equivalent initiatives by the Corporation for Open Systems (COS) in the US. International efforts are attempting to normalize conformance testing procedures.

5.6.1 OSI Conformance Testing Methodology

Conformance testing procedures are being defined by the International Standards Organization (ISO) and the International Telegraph and Telephone Consultative Committee (CCITT) to complement the standards and recommendations issued by these organizations. ISO DIS 9646 *OSI Conformance Testing Methodology and Framework* describes the methods which are expected to be used internationally to validate conforming implementations of OSI standards. While in its early stages of development, the standard provides guidance for the development of testing approaches. By following an internationally accepted approach, the efforts required to develop testing programs are minimized by the international sharing of expertise and test components. Such sharing is possible since the output of international standardization efforts are made available without restriction.

This methodology identifies four main phases in a conformance test plan:

> The first phase requires that the standards developers themselves include provisions in their standard to facilitate the identification of options and parameters to be tested. These provisions include the definition of a pro–forma document structure to be filled in by each implementer of the standard to show the options and parameters implemented.

The second phase requires the development of *abstract test suites* which provide an implementation independent definition of the test suites required to verify compliance. These suites are subject to international review and are expected to produce repeatable results irrespective of their detailed implementation.

The third phase involves the development of *executable tests* and *test systems* which together perform the abstract test cases developed in the previous phase. This represents the first potentially commercial phase of the testing framework.

The final phase involves the actual provision of the testing service itself and the evaluation of specific implementations for conformance. This is generally a commercial phase, roughly corresponding to the traditional activity of equipment test laboratories.

5.6.2 Certification Methodology

Since OSI products are expected to be offered for international sale, it is important that international and national certification procedures are put in place to avoid non–tariff trade barriers. As was indicated in the previous section, international efforts within ISO and CCITT are taking place in an attempt to establish the **technical** basis for a common set of international testing procedures.

The other required component of this international cooperation will be the establishment of **certification** procedures so that the execution of the technical evaluation may be validated and the equipment tested labelled with an internationally approved mark.

In Canada, the obtaining of a certification mark involves two organizations each of which is accredited by the Standards Council of Canada (SCC). The SCC's National Standards System defines *Accredited Test Organizations* and *Accredited Certification Organizations*[1], although one or both of these functions may be held by a single organization. The Canadian Standards Association, for example, is accredited as both a certification organization and a test laboratory. The SCC will in general issue an accreditation to any test laboratory for any regime (including test regimes defined in foreign countries), this accreditation only applies to the methods and traceability of the test laboratory execution of the regime. The Standards Council has a separate procedure for the accreditation of Certification Organizations and there are currently six such organizations in Canada, for example, CSA and UCL[2].

The SCC is Canada's international voice in this area, and it will be expected that the international certification of Canadian products will follow a process which is traceable to this organization.

[1] Of course, the SCC also accredits *Accredited Standards Writing Organizations*, and these are responsible for the approval of standards for Canadian use.

[2] Underwriters Laboratory of Canada.

5.6.3 International Initiatives

Testing procedures are being established in Europe, the United States and in Japan.

In Europe, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Conference of Postal and Telecommunications Administrations (CEPT) have established their working relationships in the OSI testing area. They have established a formal European Conformance Testing Services (CTS) programme for conformance testing services within the Economic Community. These agreements include the provision of funding to establish testing centres.

In the United Kingdom (for UK Government standards) the Central Computer and Telecommunications Agency (CCTA) identify a number of cooperative testing organizations that may fulfil their objectives and identify the CTS programme as the harmonizing initiative.

In the United States, there is some concern over the European activities since there is no facility for US input and there is a great potential for the exclusion of US products from the European market. Recent initiatives by the National Institute of Standards and Technology (NIST), and especially its National Center for Standards and Certification Information (NCSCI) might be interpreted as a response to the European initiatives. Conformance testing for the US Government, the Corporation for Open Systems (COS), and the Manufacturing Automation Protocol/Technical Office Protocol (MAP/TOP) groups seem to be coming together in the US with the issue of a *North American OSI Testing Proposal* on September 21, 1989. Although this document mentions the Canadian Standards Association (CSA), it is not clear to what extent Canadian input is being accommodated.

In Japan, the Ministry of International Trade and Industry has established the Interoperability Database System which was contracted to an industrial consortium called the Interoperability Technology Association for Information Processing (INTAP). A test centre operated by INTAP is expected to offer conformance testing services in Japan.

5.6.4 Canadian Initiatives

The main focus for OSI testing in Canada has resided in the Canadian Interest Group on Open Systems (CIGOS). In September 1989, this group issued a business plan which proposed the establishment of a non–profit organization managed by its members, CIGOS, the Canadian Standards Association (CSA), government and others. It was proposed that this organization would enter into agreements with other similar organizations in other countries to gain access to internationally developed test suites, and would eventually contribute its own suites to the international community.

The Canadian government is drafting a Canadian Open System Application Criteria profile for testing[3].

Basic to the drive in Canada to develop an indigenous test facility is the need to maintain a Canadian capability to test domestic products and to ensure that any unique Canadian

[3] An early draft of this Treasury Board paper provided input to this issue paper.

requirements are fully addressed in the development of international test suites. The absence of such an organization is considered by many as contributing to the exclusion of Canada from full participation in this very important forum.

5.6.5 Protocol Testing as a Network Service

Certain protocol testing services might be reasonably offered to the Network's clients. Considering the complexity of such a service, and the level of client interactions that will be required, it is assumed in this section that the service will be offered by a third party, e.g. by the organization resulting from the CIGOS proposal. All of the services offered by this organization may not be available via the Network, in general it is expected that only the testing of upper layer protocols will be conveniently supported over the Network. In addition to these upper layer testing services, the Network would be capable of supporting the prepatory, documentation and general communication components of a test and certification program for all aspects of a proposed product.

The Network Emulation Facility will be capable of supporting limited testing for Network Layer protocols, e.g. the evolving Routing Exchange Protocols. Certain testing of these protocols may be difficult to supply by third parties without a minimal network configuration.

The Network may also facilitate the international exchange of information, and potentially the exchange of testing services, by its interconnection to foreign networks. The ability to access international testing service (either by Canadian or foreign users) may facilitate the international development and coordination of OSI conformance and certification procedures.

For testing of protocol implementations at the Transport Layer and above, separate Network Address domains may be assigned to the test service supplier. This supplier would attach the protocol test machine to the Network and this machine would respond to information addressed to it from the client. The source address of incoming information would be used to ensure that the service is being accessed by the recognized client. Testing of protocol implementations generally requires access both to the top and bottom of the layer(s) to be tested. It is expected that the test service supplier will define the required service access points to permit such testing to be carried out. Of course, the general communications capabilities of the Network may also, and simultaneously, be used to provide real–time communications between the client and the test facility staff.

It is proposed that the testing service would be developed and supported by the Network's staff in the same manner as other third party services to be offered over the Network.

5.6.6 Ad–hoc Interoperability Testing

As indicated previously, conformance testing cannot be expected to fully test an implementation. Ad–hoc interoperability testing is considered a valuable adjunct to a formalized testing plan. The availability of OSI implementations on the Network will facilitate the execution of ad–hoc interoperability tests. The successful operation of systems on the Network will provide potential purchasers both in Canada and abroad with additional assurance of the correctness of a supplier's implementation of the OSI protocols.

5.7 CONCLUSIONS AND RECOMMENDATIONS

Testing and Conformance procedures will be required for new equipment and services to be incorporated into the Network and these procedures may also be offered as a third party service over the Network. To facilitate access to international markets, product testing should follow international initiatives for conformance and certified testing.

Equipment to be introduced into the network will require testing to ensure that it will not interfere with ongoing operation. Although under the control of Network Management, these requirements must be sufficiently flexible that the experimental needs of Network users are not unduly constrained. Testing of equipment prior to attachment to the on–line portion of the Network will be accomodated by the Network Emulation Facility discussed in the *Network Architecture and Migration* plan section.

Testing and Conformance of implementations of the lower layers of the OSI model are recommended to be performed off–line to the Network, to meet the specific requirements of the relevant subnetwork technology.

The testing of implementations of the upper layers of the OSI model may be carried out over the Network as long as suitable Network Address domains are created for this purpose.

The ability of the Network to support ad–hoc interoperability tests with a variety of systems will enhance the suppliers ability to supply and demonstrate conforming implementations.

5.8 LIST OF ACRONYMS

CCITT	The International Telegraph and Telephone Consultative Committee
CCTA	Central Computer and Telecommunications Agency (agency of UK Treasury)
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEPT	European Conference of Postal and Telecommunications Administrations
CIGOS	Canadian Interest Group on Open Systems
COS	Corporation for Open Systems
COSAC	Canadian Open System Applications Criteria
CSA	Canadian Standards Association
CTS	Conformance Testing Services (Europe)
ECMA	European Computer Manufacturers Association
EIA	Electronic Industries Association (USA)
INTAP	Interoperability Technology Association for Information Processing (Japan)
ISO	International Organization for Standardization
MAP	Manufacturing Automation Protocol
NCSCI	National Center for Standards and Certification Information (USA)
NIST	National Institute for Standards and Technology (USA)
OSI	Open System Interconnection (model)
SCC	Standards Council of Canada
TOP	Technical Office Protocol
UCL	Underwriters Laboratory of Canada

6. NETWORK MANAGEMENT AND TECHNICAL CENTRE

6.1 SUMMARY

This section discusses the requirements for Network Management and for a Technical Centre to promote the Network. The technical requirements of Network Management are summarized and include planning, acquisition, monitoring, control, maintenance and disposal functions. Network Management is also expected to ensure that the policies of the Network's owners are followed and any required billing information acquired. The Technical Centre is expected to assist clients in their use of the network, and will promote the Network.

6.2 INTRODUCTION

This section takes a very general view of the operational technical functions necessary to support the Network. This discussion presents information to be used as input to the Implementation Plan.

To assure the continued performance of the Network it will be necessary to manage, monitor and control the operation of Network components and to control the interface between Network and non–network components. A Technical Centre is also proposed to facilitate the distribution of technical information to users and to operate as a focus for the gathering of user feedback on the ongoing performance of the services provided by the Network. These two functions have been separated in this section since it is believed that Management operations must be performed under the direct mandate of the Network's Owners while the Technical Centre will operate in an advocacy role to promote the exact matching of Network services (including networking research services) to the needs of the Users. In addition, Management operations are generally considered to be a 24 hour a day, 7 day a week operation with priorities of work varying dynamically depending upon the occurrence of network failures or other problems. The Technical Centre will have a more planned work schedule.

6.3 RELEVANCE TO STUDY

The ongoing operation of the Network will require that all equipment be maintained and upgraded as required and that the policies of the Network Owners be implemented as directed. Furthermore, the continued success of the Network will depend upon its ability to satisfy the need of its Users and this will require that these needs be well known and that the information necessary to fully exploit the services currently offered are distributed to all Users. The technical requirements, but not the organizational structures, appropriate to address these functions are discussed in this section.

6.4 NETWORK MANAGEMENT

Network Management, broadly defined, relates to the full 'Life Cycle' maintenance of Network components and leased services. These functions begin with the planning process for new acquisitions to meet an agreed need; the acquisition itself; the monitoring, control, and maintenance of equipment in service; and the disposition of old equipment. Network Management must also acquire, monitor and control the use of leased equipment and services (e.g. transmission services) and must control the interface to client equipment. We have also suggested that the Network Management function should also be responsible for the implementation of the Network Owner's Policies, and this will add additional responsibilities. Network Management must also execute any required billing functions.

This section chooses to interpret Network Maintenance in a very broad manner. The final Implementation Plan may choose to reallocate some of these functions to other groups with different job titles. The entire technical scope is treated here to ensure that these functions are not omitted in the planning process.

6.4.1 Network Planning Function

Network planning will involve the development of strategic plans to manage the development of the Network over both the near and long term. Near term planning would generally deal within a time horizon of one to three years, and would deal with proposals to implement specific Network expansion by the purchase or lease of equipment and services. Long term planning would generally deal beyond the two year horizon, and would deal with more general strategic plans based on a judgement of evolving technologies. Planning must include the development of the communications components of the Network and the Services offered over the Network.

These near and long term planning functions are dealt with here since they both require the technical expertise which is expected to be resident in the Maintenance and Technical Centre staff. The Implementation Plan will need to address the overall planning process in more detail.

6.4.1.1 Near Term Network Planning

Near term planning would involve the monitoring of commercial literature and equipment development programs, and the creation of technical proposals to meet agreed upon changes. This function will result in the creation of recommendations for the purchase of specific equipment and services. These changes would be agreed upon, and the Owners would approve the corresponding expenditures. This planning process would result in the preparation of all required plans, requests for proposal, etc., necessary to implement the proposed changes. If a proposal is of sufficient size, it is expected that specific subgroups would be created which would plan, and eventually manage, the implementation of the change.

The near term plan must be consistent with the Network's budget and long term plan.

6.4.1.2 Long Term Network Planning

Long term planning would deal with more strategic issues relating to the direction of Network development, recommending these directions to the Network Owners based on the monitoring of the underlying technologies and input from clients via the Technical Centre (to be discussed later). These plans would be approved in principal by the Owners and published as statements of future direction. Strategic plans would not result in the purchase of any equipment or services, but they would be used for long term budget planning. Although discussed here under Network Management, the long term plan will best be generated in close cooperation, and possibly with the approval of, the Technical Centre.

There are many models for long term (strategic) planning and the Implementation phase of this study must deal with this in more detail. Of course there are at lease two strategic plans: one is the strategic plan of the Business and the other is the strategic plan of the Network itself. The first is a business plan which evolves over time with the business, the second is a technical plan which evolves over time with the technology. It would probably be a good idea to coordinate the time scales of these two plans so that they will be consistent with one another.

One strategic planning model requires that strategic plans be created at a minimum rate to cover a specific period, for example *a Five Year Plan*. The period of the Network strategic plan should be related to the rate of evolution of the underlying technology and the user requirements and should also have a sufficient period to reassure the employees and users of the Network. For this reason, it might be initially recommended that the Five Year Plan actually cover a ten year period: the second five years being dealt with in a more summary fashion.

6.4.2 Network Acquisition Function

The acquisition of new equipment or services will require technical input to ensure that the products meet the approved requirements. This will include the issue of specific requests for proposal, the evaluation of bids, the technical recommendation for purchase, any technical writing required, the incoming inspection and acceptance of equipment or services, and the arrangements necessary for the installation and commissioning of the equipment or services. It is expected that some acquisitions may follow a standing plan for the purchase of ongoing products or services which are general `consumable' items. This function will operate in conjunction with the business' purchasing agent.

This function would operate closely with the maintenance function (to be discussed below), and the actual installation and commissioning of equipment would be carried out by personnel from the vendor, a third party contractor, or by Maintenance staff.

6.4.3 Monitoring, Control and Maintenance

The operational equipment owned or leased by the Network must be monitored, controlled and maintained. Where third party contracts are being issued, or where equipment or services are being leased, this function must monitor the performance of these other parties and take any actions necessary to resolve difficulties.

Monitoring and control products and services are very popular today. Many product and service vendors are willing to provide products and services to meet this requirement. Many standards exist and are being created to permit global monitoring and control of equipment from central facilities. It should be recognized, however, that this is not a well developed area, and the Network's use of leading edge equipment will generally mean that automated monitoring and control will take a back–seat. This will often mean that human staff on the ground will be required to monitor and control equipment in addition to their maintenance duties.

Maintenance services can also be contracted to third parties. This is a particularly good idea considering the national scope of the proposed Network. Many communications and computer companies will supply maintenance services for third party equipment. A difficulty may arise if the equipment in service is considered by its supplier as being leading edge or in other ways proprietary. It will be important to coordinate the selection of the maintenance service supplier so that this does not become an impediment to the introduction of leading edge equipment or services.

From a technical perspective, the architecture for OSI network management is described in ISO/IEC 7498–4: *Information Processing Systems - Open System Interconnection - Basic Reference Model - Part 4: Management Framework*. Furthermore, the standards ISO/IEC 9595 and 9596 are in draft form which begin to describe protocols to implement standardized OSI network management. Network management must be considered to be in its early phases of development within ISO. There is still considerable question regarding the application of international standards to provide a Network–wide uniform management mechanism. Since the Network will consist of many subnetworks, many operating in different administrative domains, there may be administrative restrictions on the provision of Network–wide management in addition to these technical limitations.

At least in the short term, it will remain the responsibility of the subnetwork owner to manage, or arrange to have managed, his subnetwork. For wide area subnetworks (including the High Speed Subnetwork) this will not only involve the monitoring and control of owned and leased equipment but will also entail the monitoring and potential control of the services provided by the long haul carrier. Thus many types of equipment and service must be monitored and controlled, and the need for a centralized facility with a uniform interface will be highly desirable.

6.4.4 Management of Client Interfaces

The **physical** interface to client equipment is probably best handled by the Maintenance staff since they will probably represent the staff closest to the client's site. Where clients encounter difficulties which are not physical, e.g. logical incompatibilities due to upper layer protocol differences, the first point of contact would likely be the Technical Centre staff. In many cases the Technical Centre staff might be expected to resolve the difficulty. In cases where logical difficulties cannot be resolved by conversations between the Technical Centre and the client, it may be necessary to perform remote monitoring or control operations on the appropriate Network equipment. Monitoring may be permitted by the Technical Centre, but Control would likely be restricted to the Maintenance staff.

It is generally preferred that a single point of contact be defined for clients to call in case of difficulties. It is recommended that this point of contact be in the Technical Centre, and this will be discussed in a following section.

A function that should also be performed by this group is the establishment of `user accounts' if such are required. This may include the allocation of Names and Network Addresses, on an interim basis, as discussed in the *Network Addressing, Directory and Routing* section. The establishment of user accounts may require the appropriate coordination with the Billing Function to be discussed below.

6.4.5 Management of Foreign Interfaces

The interface to foreign networks will need to be managed to ensure these external connections provide the desired level of access but do not impair the ongoing operation of the Network. Foreign networks may be within Canada but managed by a separate administration, or may be networks in foreign countries. Issues relating to foreign networks will include: the establishment and maintenance of interconnection agreements, exchange of information, agreed types of use (including access), billing procedures, regulatory or legal limitations, and technical (protocol) issues. The Technical Centre may also become involved in the distribution of technical information to the users of foreign services.

6.4.6 Management of Services

Services in this context refers to the provision of high level network functions to users. Electronic Mail, Protocol Testing and a Directory Service[1] would be considered examples of Network services. Each service offered by the Network will require functions to ensure that the component is maintained to an adequate level. Like the Network itself, these facilities should be subjected to complete `Life Cycle' management. It is not clear how many services should be offered by the Network itself, and how many would be offered by third parties. The Network Management group may manage its own services, or may contract this to a third party; and, equivalently, third party offerers of services could contract maintenance to the Network Management group. The Technical Centre may provide direct client support for Network services.

6.4.7 Policy Implementation Function

The policies of the Network will be defined by its Owners. Policies will relate to universality of access, permitted use, etc. The Policy Implementation Function must ensure that these policies are followed on a day to day basis, by ensuring that client requests are treated in an appropriate manner. Also included would be the security and policing functions necessary to ensure compliance with policy.

For the Network to influence the development of consistent policies within attached subnetworks, the Policy Implementation Function may formulate strategies and offer access and pricing structures to users which promote the desired policies.

[1] The *Network Addressing, Directory and Routing* issue paper has discussed the Directory Service, which would provide a directory of Network resources.

6.4.8 Billing Functions

The mechanisms that will be required to recover costs (full costs or partial costs) are as yet undetermined. If cost recovery is expected to be related to Network use, it will be necessary to monitor this use and acquire the required billing information. If billing is related to the period of attachment to the Network, it will be necessary to monitor the period during which access is provided. These functions would operate in conjunction with the business' invoicing agent.

6.5 TECHNICAL CENTRE

The Technical Centre is responsible for the distribution of technical information to clients, the promotion of the Network, and the establishment of a strong user community. It is suggested that this function be separated from the Maintenance functions since the Technical Centre will have some conflicting objectives compared to the Maintenance functions. Specifically, the Maintenance function is concerned with the continued smooth operation of the Network. The Technical Centre is concerned with the promotion of the use of the Network's R & D Services and the development of Information Technology products and services using the Network. These concerns may often be in conflict.

The Technical centre will distribute information to the Network's clients, and will generally promote the development of products and services, both to R & D Users and Information Technology developers. It would reproduce or create documents to describe Network use, would arrange for seminars or conferences to promote areas of mutual interest, etc.

The Technical Centre should also have a strong input to the long term planning process, and may also provide advice regarding near term planning.

6.5.1 Client Support

As indicated in the previous section, it is recommended that the Technical Centre provide the first point of contact for a Network client should a difficulty be encountered. For service on the Network not operated by the Network owners, or services offered from a foreign network, client support may be negotiated with the third party service suppliers or foreign network owner. Often the source of a client's difficulty may not be easily identified, thus a minimum level of client support will be required for all services offered over the Network.

The client in this case could be an end user (when the user is directly attached to equipment owned by the Network), a foreign network owner, or a service supplier. It is expected that the Client Interface needs to be maintained using at least two levels of `service'.

The first level would be appropriate to service suppliers or foreign network personnel who are expected to make contact only after a number of sophisticated solutions to the problem have failed. This contact must be prepared to discuss technical issues at a very high level of competence and may require the services of the Maintenance group.

The second level would be appropriate to the more general community of users. It would be expected that difficulties may often be resolved based on previous experience and by reference to existing technical documents. The second level contact would use the first level to resolve the more difficult problems.

6.5.2 Dissemination of Information

A key aim of the Network is to act as a catalyst in the development of information technology products and services. The cooperation necessary to foster this development is based on the availability of international standards. These standards are complex, and are evolving in the international community. Thus it will be important for the Technical Centre to act as a depository of standards and other documents which will promote the development of compatible products and services. Of specific importance will be the role of the Technical Centre in adopting Canadian and international standard profiles for its communications services.

6.5.3 Network Marketing and Service Development

The marketing of the Network may also be supported from the Technical Centre. Such marketing would be directed to the acquisition of new users and new service providers.

6.6 CONCLUSIONS AND RECOMMENDATIONS

This section provides initial input to the Implementation section of the study. It proposes that the Network Management should provide the technical functions of Network Planning (near and long term); Network component acquisition; Network monitoring, control and maintenance; maintenance of interfaces to clients and foreign networks; maintenance of services; policy implementation; and, if required, the acquisition of billing information. A Technical Centre is proposed to provide the direct interface to the user community, to disseminate information to this community, and to promote the Network.

7. NETWORK ADDRESSING, DIRECTORY, AND ROUTING

7.1 SUMMARY

Users and resources on the network will need to be identified using a naming convention which is easy to use, unique and which follows international standards. The network itself, which consists of an interconnected assembly of subnetworks each with their own internal addressing mechanisms, will require the definition of a unique and universal network wide addressing scheme. The translation between names and network addresses will be performed by the Directory function. The network will need to determine the available routes over which a given communication may take place, and this function is the responsibility of the routing function.

7.2 INTRODUCTION

Prior to any communications taking place, it will be necessary for the user to uniquely identify the resource desired. This resource may be an application running on a specific host computer, a human user associated with a particular application (e.g. a mail–box), or a particular end instrument (e.g. a video display). The network must be capable of identifying the end points of the communication and establishing a route over which the communications can take place. From a user's perspective, it is most convenient if the resource is identified by a naming convention which is logical and easy to understand. At the other extreme, the network itself will need to employ addressing mechanisms which are related to the network's topology to specify the communications route. Furthermore, the user and his desired resources may not be fixed to specific network attachment points, so it will be necessary to use a binding mechanism which permits people and applications to move.

For the purpose of this section it will be important to discriminate between the overall Network and the assembly of subnetworks and intermediate processing elements of which it is composed. The High Speed Network, which is the emphasis of this Feasibility Study, is considered to be one[1] of the subnetworks comprising the Network. There is no hierarchical structure implied: subnetworks may be connected together in any way and may physically overlap each other.

The identity of a host machine or instrument which is currently supporting a given resource or user is identified by its **Network Address**[2]. The translation between names which are easily understood by users and the Network Address is performed by the **Directory** function. The Network Address serves to uniquely identify the ends of a communications path, and such end points are within **End Systems**. The path between the End Systems may traverse many **Intermediate Systems** and subnetworks. One of the tasks of the Network is to identify the pathway(s) through the Network which will satisfy the requirements of the intended

[1] or more than one, this will be discussed later in the paper.

[2] All terms in bold in this paragraph are Open System Interconnection (OSI) reference model terms.

communication. The **Routing** function is responsible for the generation and maintenance of such potential pathway information.

Since from the user's perspective the internal physical details of the overall Network will generally be of little interest, the discussions in this section begin by discussing Directory issues. Network Addressing follows. The quality of the path to be established through the Network is an important factor which is discussed next. Finally the Routing functions are presented. These discussions will make explicit mention of the International Organization for Standardization (ISO) approach and the more traditional DARPA Internet approach.

7.3 RELEVANCE TO STUDY

The Network must support the orderly transmission of information (data, voice, video, etc.) between End Systems with a quality of service adequate to the intended task. Since the Network is expected to interconnect current and future End Systems, it will be necessary to define a universal addressing function so that address conflicts may be avoided. The ISO has defined universal naming and addressing methods and it will be necessary to tailor the specific technique used to best fit the Canadian requirements. A Directory function will be required so that users of the network may conveniently identify remote users and End Systems with which they wish to communicate. The Network will interconnect users using a mix of local, regional and other subnetworking links and a pathway between a pair of systems may traverse several subnetworks and pass through zero or more intermediate processing elements. The users will not wish to get involved with this detailed pathway determination, and indeed may not be aware of all of the possible routes between the End Systems. Thus it will be necessary to incorporate an effective routing and relaying capability into the Network. This routing and relaying function must not only operate over the High Speed Subnetwork, but must also accommodate existing and future local and regional subnetworking elements.

7.4 BACKGROUND

Directory, Routing and Relaying functions experienced their major development within the ARPANET (now called the DARPA Internet) [for an overview see Stal87a and Stal87b]. Standards subsequently issued by the International Organization for Standardization (ISO) have extended these concepts, but they differ from the traditional Internet TCP/IP protocols. The Directory, Routing and Relaying functions discussed in this section are based on the standards being developed by the ISO. Reference will be made to the ARPANET Internet protocols (TCP/IP related protocols) where relevant since a migration path from these protocols are expected to be required for the Network.

Strictly speaking there are two kinds of names used to identify objects in the OSI environment: Titles and Addresses (see ISO 7498 AD3). A Title is a name given to an object such as an application process to identify it unambiguously. Titles are expected to identify objects irrespective of their physical location and an object may have more than one Title. The ISO uses Titles in conjunction with other words (including other Titles) to more specifically identify objects. For example, System Titles are names which specifically identify End Systems. Addresses describe the location of an object, for example and End System object. Within this section, **Name** is used to refer to the Title of a user or an end process and the Network Address is used to refer to the location on the Network of the End System (or group of End Systems) supporting the user or process. This represents a simplification of the rigor of the OSI approach and is used here to clarify the current presentation.

7.5 DIRECTORY FUNCTIONS

Directory functions will be required to provide information on the resources and human users available on the Network. Within OSI, Titles (Names) are bound to Addresses by the Directory. A major contributor to the development of this aspect will arise from Working Group 3 of the RARE[3] association in Europe. The CCITT/ISO X.400 message handling protocol and X.500 (ISO 9594) Directory specification should also be considered primary input to the selection of the Naming and Directory functions.

Currently existing academic networks have evolved with differing and sometimes conflicting Naming conventions [Quar90]. Typically the end user or process is identified both by name and supporting host system. For example, a user on the Internet might be identified as follows:

user@host

where the *user* is considered the local name, while *host* represents the domain[4] name of the host system. This particular convention has the unfortunate property of implying the coupling of the Name to its physical location (i.e. attached to *host*). In addition, other existing conventions (e.g. in BitNet networks) exist which conflict syntactically with this Internet convention.

A basic property relating to the provision of Directory services is the objective of providing a universal naming convention which allows users to specify the desired end element without knowing the location or route required to reach it. Other aspects should be considered as well, for example current Naming conventions for the postal system include the provision of work related addressing and personal correspondence addressing. For typical TCP/IP applications, the Directory function is performed by *nameservers* such as the Internet Domain Name System (DNS).

The X.400[5] convention for Names is considered to be a more flexible convention since it includes a name plus attributes. X.400 permits the unambiguous specification of a personal name, organization name, country name, etc.; some of which may be optional and all of which are not necessarily related to the physical location of the Named object.

[3] Reseaux Associes pour la Recherche Europeenne, an association of European research networks and their users.

[4] Domain name is used here rather than host name since many networks differentiate between the physical host supporting the user and the administratively controlled name of one or more hosts any one of which may support the corresponding user. In general `host' should be interpreted in the general sense as being a clearly identifiable system (one machine or many) under the control of a single administration.

[5] The X series of recommendations are standards issued by the CCITT.

The ISO 8824 standard defines rules for naming objects and the X.500 describes a candidate Directory to index them. It is usual to consider Directory entries (Names) to be members of a hierarchical tree structure where the assignment of names is delegated to sub–areas of responsibility. For example, using the ISO 3166 standard for the Canadian country code, a globally unique user Name might be constructed as follows:

CA.ISTC.ITIB.MTO.Williams.D.

This example assumed that Canada has a national level naming authority which allocated the reserved name `ISTC' to Industry Science and Technology Canada, and that ISTC contained a naming authority which delegated the next level to the Information Technologies Industry Branch, etc. Of course, although the unique Name[6] could be assigned in this way, access methods may be provided to search for `Williams, D.' in the Directory should his departmental allegiances not be known. It is noted that this Name does not identify the location of Dr. Williams, the Directory must contain the information necessary to identify the End System (or group of End Systems) which can provide access to this destination.

While it will ultimately be desirable for Canada to implement a universal scheme for assigning Names, it may be necessary to provide an interim solution for the Network. Such an interim method should follow as closely as possible the international standards in this area until the corresponding Canadian policies have been developed. For the interim it may be necessary to permit local mechanisms to perform the Directory function until a global standard function is developed. Since a hierarchical Naming authority tree is unlikely to be established in the near term, it will be appropriate to establish a temporary tree, possibly headed by a Network identifier.

7.6 NETWORK ADDRESSING

Network Addresses uniquely identify the End Systems to the Network. End Systems may be attached to Local Area (sub)Networks (LANs), Metropolitan Area (sub)Networks (MANs), Regional subnetworks or directly to the proposed High Speed Subnetwork. The physical addresses of systems connected to a subnetwork are called **Subnetwork Points of Attachment** (SNPA). These SNPA's need only be unique for each subnetwork (ISO 8648). Network Addresses, on the other hand, must be unique across the entire assembly of subnetworks (that is, across the entire Network). Furthermore, a route between two End Systems (each specified by a Network Address) may flow through many subnetworks and Intermediate Systems, and each leg of such a route will generally involve the use of differing SNPA's.

Thus globally across Canada (and the world) there needs to be a unique Network Addressing convention. Such a convention has been proposed by the ISO (ISO 8348 DAD2), and two major options are available:

Network Addresses prefixed by the Data Country Code (DCC – a specific prefix number) are

[6] This example attempts to identify the human user. In practice if this were an electronic mail application, it would be necessary to identify an application (mail) process which acts as the human user's agent. Thus the Name would need to include a parameter identifying an invocation of a mail process associated with the human user.

provided for assignment by each country. This is followed by another number which specifies the country (Canada has been assigned the number `124' by the ISO). From then on, it is up to an accredited national organization in each country to assign unique values to organizations (possibly in blocks) or individuals. In Canada this responsibility resides with the Canadian Standards Association (CSA).

Network Addresses prefixed by the International Code Designator (ICD – a specific prefix number) are provided for assignment for multi–national organizations (these assignment have been delegated to the British Standards Institution – BSI). This is followed by another number which specifies the multi–national organization (for example, the International Civil Aviation Organization – ICAO – has been assigned the numbers `1001' and `1002' by BSI).

The ISO also defines other Network Address prefixes for other purposes, and some of these purposes allow the specification of Network Addresses which are equal to SNPA's. For example, a Network Address prefix is available to specify that the Network Address is equal to an X.121 format subnetwork address.

The most recent edition of the traditional IP protocol of TCP/IP, uses a 32 bit word[7] to represent the `IP Address'. Although it might be thought that an address space of 2^{32} should be sufficient to address the maximum number of hosts on the Network, the inefficiencies of assigning values will always cause certain values never to be assigned. Thus although the Network Address format of TCP/IP is more efficient (i.e. uses fewer bits) than that of ISO, it is expected that it will not provide the space or flexibility that will be required for much larger Networks. Within the proposed Network architecture it will be necessary to address the coexistence of the TCP/IP Network Address format and that of ISO. It may be possible to allocate suitable prefixes to an ISO format to carry TCP/IP format Network Addresses.

While these methods of assigning Network Addresses to End Systems allows maximum flexibility in the sub–delegation of assignment responsibilities, the format of the fields are of some concern if an efficient routing capability is to be incorporated in the subnetworks[8]. By following a common format for fields, the operation of routing functions may be simplified since each routing point need not know about the unique format of each authorities' assignment methods.

Since each subnetwork only requires the non–ambiguous assignment of SNPA's for correct operation, the role of Network Addresses do not directly impact on their basic operation. However, for routing between subnetworks (including High Speed Subnetworks) and End Systems, a Network Addressing scheme shall be required.

Much as was the case for Naming conventions in the previous section, suitable authorities will be needed to assure the non–ambiguous assignment of Network Addresses. In addition it will be appropriate to follow a particular format for the representation of the addresses since such

[7] This protocol has an additional octet to perform the equivalent function as the Transport selector which within ISO is considered to be part of the Network Address.

[8] Strictly speaking the ISO does not want routing information to be derived directly from the Network Addresses. However, the format of Network Addresses will determine the efficiency with which the routing information may be accessed.

representations will need to be interpreted by the Network's routing functions – and it will be preferred that these functions operate with a single format.

7.7 THE NETWORK SERVICE

A scheme must be put in place to permit the transmission of information (data, voice or video information) between End Systems via the Intermediate Systems and subnetworks which make up the Network. This scheme must accommodate subnetworks with possibly differing subnetwork addressing methods (different SNPA formats), packet sizes, access methods, error control capabilities and other performance features. The overall quality of service offered to the End Systems must be adequate for the intended task. Within OSI, **Quality of Service** is an explicitly defined concept, and includes such qualities as Residual Error Rate, Allowable Delay, Cost, etc. An overall scheme, such as that defined with the OSI model, will be required to ensure that the end to end Quality of Service is maintained. In addition to providing the required qualities of service, the Network must provide specific service types to the user and the most controversial aspect here is that between the provision of connection oriented vs connectionless networking services.

7.7.1 Connection Oriented Networking

A Connectionless service involves the establishment of a connection between the End Systems and this is followed by the transmission of the information. Such methods are common for voice links where a call is first established by dialling the desired End System (telephone set) network address. For voice and video, where a uniform propagation delay through the path is important, this method has the advantage of allowing the reservation of network capacity in advance for the entire period of the connection. For data or other applications where the data flow is highly bursty, this method is less efficient in its use of resources since the network is forced to pre–allocate the maximum required capacity for the period of the call.

Some new network design techniques (*fast circuit switching* or *burst switching* – [HUI89]) are being proposed to reduce this overhead for compressed voice and video applications (which are also bursty) to permit the dynamic allocation of resources upon demand. These latter techniques, however, are not expected to be fully utilize the capacity of the network for data applications with high rate variations.

Connection oriented procedures were highly familiar to the traditional telephone carriers, so it is not surprising that such techniques were carried forward into their initial offering of packet switched data services. The CCITT X.25 standard, probably the most widespread packet switched networking standard in use today, uses the connection oriented approach. After establishing a connection, information contained in packets is transmitted over a common transmission facility with each packet being kept logically separate from all the others by control information stored when the connection was established. In general the internal network operation of X.25 networks is kept invisible to the user, the user only interacts with a local node processing element supplied by the carrier. However, when the route between the end users spans more than one X.25 network the interface between the subnetworks may be exposed and the CCITT X.75 standard was created to define such interconnections.

To preserve the efficiency of packet switched networks, they generally make extensive use of shared facilities with buffering and, since the data loads on such systems are normally highly bursty, the propagation delay for packets in X.25 networks are highly variable and sometimes relatively large. Large and variable delays are generally not acceptable for voice or video unless the basic network infrastructure has sufficient capacity and speed to make worst case delays acceptable.

Within the ISO standards community, an International Standard Profile (ISP)[9] is in the process of being approved for the provision of a Transport Service over a connection oriented Network Layer. This profile is of most interest in Europe, traditional North American preferences are for the Transport Service supported over a connectionless Network Layer as will be discussed in the next section.

7.7.2 Connectionless Networking

The connectionless networking scheme does not use information stored at intermediate points in the network, rather all of the information necessary to route a packet of information between the End Systems is contained within each and every packet. There is no connection establishment phase and each packet of information flows independently through the network. Since more than one path may exist between End Systems, the packets may take different routes and may arrive in a different order than the order in which they were transmitted. If such is possible, facilities are required either in the End Systems or at the last nodes of the network to rearrange this information into the correct order. Connectionless oriented networks may also deliver duplicate packets of information, and are often more prone to the loss of packets. If such rearrangements, duplications or losses are possible, facilities are required either in the End Systems or at the last nodes of the network to rearrange, delete or ask for retransmissions as appropriate.

Connectionless protocols are very popular for use over networks which consist of a large number of subnetworks. In practice certain subnetworks are designed to operate using the connectionless method (e.g. most LAN systems) and it is easiest to use an overall networking scheme with the lowest common denominator. The connectionless method may also simplify subnetwork interconnection devices since they do not need to keep track of each connection, and are additionally more ameniable to parallel processing approaches to attain a higher speed capability.

As in connection oriented packet networks, the propagation delay for individual packets is highly variable and may sometimes be large. However, since each routing component in the array of subnetworks need not know about the End Systems themselves (all information is within each packet), it may be possible to construct highly complex interconnections of subnetworks that can more flexibly respond the changing loads imposed. It is also possible to incorporate more dynamically acting load levelling techniques (sometimes called *Congestion Avoidance Mechanisms*) to reduce overall transmission delays.

[9] ISPs specify a selection of protocols and options within each protocol so that end systems using the same profile should directly interoperate. ISPs were discussed in the *Protocols and Use of Standards* issue paper. This profile, dated November 1989, is being circulated in draft form as ISO/IEC JTC 1/SGFS N 140.

Connectionless protocols are generally referred to as Internet Protocols (IPs). Two major IPs dominate today. The IP of TCP/IP has the longest history and is in common use on existing academic networks. The ISO IP protocol (ISO 8473) is rapidly gaining popularity.

Internet Protocols rely on the fact that each packet completely identifies the end–points of the instance of communications. One of the key parameters of interest when comparing Internet Protocols is the size and efficiency of the data packet format. Since the Internet Protocol must operate in conjunction with a Transport Layer protocol to provide reliable end to end delivery of information (the Transport Layer enhances the capability of the IP by providing error control and sequenced delivery in both TCP/IP and ISO approaches), it is appropriate to address both the packet size and efficiency factors by including the overheads of the corresponding Transport Layer protocol.

One International Standard Profile is being approved internationally to support the Transport Layer class 4 procedure[10] (which is most similar to TCP) over a connectionless Network Layer Service. This profile is expected to be adopted for general use in North America.

7.7.3 High Speed (Sub)Network Access

To this point we have been discussing the overall mechanism for providing transmission over the subnetworks making up the Network. The proposed high speed backbone, in ISO terminology, is just another subnetwork. Within the ISO it is possible to differentiate between the access schemes of subnetworks, thus the transmission technique of the high speed component subnetwork may be optimized for the characteristics of the equipment to be employed. In practice, there may be several access mechanisms for the high speed subnetwork since it may in reality consist of several media types, e.g. land line, satellite; and each may operate optimally with differing mechanisms. The subject of subnetwork access methods suitable for the high speed subnetwork are considered in the *High Speed Transmission Methods, Technology and Networking* section.

7.8 ROUTING AND RELAYING

Routing and Relaying are related to the routing of information between End Systems, Intermediate Systems (including subnetworks). The relaying function is the process of applying route information at each Intermediate System to direct the information onward towards its destination via its next intermediate path segment. The routing function refers to the processes required to establish this route information in each Intermediate System. Within subnetworks, the routing between SNPA's is another matter, generally left up to the subnetwork designer. However, when subnetworks are connected together, the Routing and Relaying functions to be discussed in this section will be required. Furthermore, since the High Speed Subnetwork may in practice consist of several subnetworking technologies (satellite, land line, etc.), the intersubnetworking between them will also require these functions.

[10] Transport class 4 is explained in the *Protocols and Use of Standards* issue paper. This draft ISP is dated July 1989 and is being circulated as ISO/IEC JTC 1/SGFS N136.

Both TCP/IP and ISO Networks include routing functions with varying levels of capability. The general objective is for End Systems to identify themselves to the Network and for the Network to establish the required routing tables and maintain them so that efficient and reliable communications can take place between all End Systems. Early implementations of Networks used Static routing tables which were manually entered by maintenance personnel. Later, protocols were established to automate the establishment and maintenance of routing tables (i.e. the Routing Information Protocol – RIP – for the Internet and the ISO routing exchange protocols).

The ISO has taken a comprehensive approach to Routing. They recognize that while routing within a single administrative domain may be carried out using traditional approaches, routing across different administrative domains may need to be carried out in a `mutually suspicious' manner. This is because one domain may not want the other to know its internal structure and status, and furthermore there may be no means to assure the correctness of information transferred across administrations. For example, a subnetwork (or group of subnetworks) operated by a particular company may not wish to divulge the topology of its internal subnetworks since this might reveal something about the internal organization of the company.

The ISO Internetwork Routing incorporates two main components: routing among End Systems (ESs) and Intermediate Systems (ISs) on the same subnetwork, and routing among the Intermediate Systems that interconnect the subnetworks. For the second components (between Intermediate Systems), there is a further subdivision to discriminate between routing within a single administrative domain and routing between administrations. ISO Routing information exchange protocols (RPs) are being developed to provide dynamic adaptive routing for all three cases: ES–IS Routing (ES–IS), IS–IS Intra–Domain Routing (IS–IS), and Inter–Domain Routing (IDR). IDR enforces `firewalls' between domains and this is expected to be an important factor for the Network so that adequate protection can be included between the interconnected subnetworks.

The ISO ES–IS Routing protocol (ISO 9542) is the simplest of the ISO routing protocols. It provides functions to allow End Systems and Intermediate Systems to identify themselves to their neighbours so that local routing tables can be established. This protocol is relatively well established. The IS–IS and IDR protocols are not as well developed and it may be necessary to use static routing methods in the interim.

7.9 CONCLUSIONS AND RECOMMENDATIONS

A universal Naming convention will need to be adopted so that the resources and human users on the network may be identified in a manner which is convenient for Network users. A register should be maintained to permit these names to be allocated uniquely. A Directory function will be required to contain these names, to provide information on the resources and human users available on the Network. The ISO provides some guidance on such a Naming convention although no world–wide approach is in place today. An interim approach based on the ISO standards should be considered for the Network. The Directory function may be initially implemented using local procedures until ISO defined automated procedures become standardized.

Similar to the Naming discussed above, a universal Network Addressing scheme will need to be adopted for the Network. Pending the widespread allocation of Network Addresses by supporting organization, it may be necessary to allocate Network Addresses derived from a single authority delegated by the Canadian Standards Association. Provisions for the support of the TCP/IP Network Addressing format should be included.

The High Speed Subnetwork(s) may use their own Subnetwork Point of Attachment (SNPA) approach for internal addressing should this be required, although the use of one of the existing standards in this area would be preferred.

A Network wide scheme to support the specification of Quality of Service should be included so that a range of intended applications may be accommodated in an optimum manner, and this should follow the ISO approach. The provision of a Connection or Connectionless oriented Network Service remains a controversial issue with North America and Europe currently pursuing different paths. Compatibility with the DARPA Internet and some other factors may recommend the use of the Connectionless approach.

Routing and Relaying may be accomplished using static or dynamically routing tables. If dynamic maintenance of routing tables is to be supported, standards being developed by the ISO should be examined. It may be necessary to use interim static routing until the emerging ISO protocols are complete and more experience with them has been obtained.

7.10 REFERENCES

General

[HUI89] Hui, Joseph Y., *Network, Transport, and Switching Integration for Broadband Communications*, IEEE Network, March 1989, pp 40–51.

[Quar90] Quarterman, John S., *The Matrix - Computer Networks and Conferencing Systems Worldwide*, Digital Press, 1990.

[Stal87a] Stallings, William, *Handbook of Computer-Communications Standards - The Open Systems Interconnection (OSI) Model and OSI Related Standards*, Vol 1, 1987.

[Stal87b] Stallings, William, *Handbook of Computer-Communications Standards - Department of Defense (DOD) Standards*, Vol 3, 1987.

CCITT and ISO Standards

ISO 7498, *Information Processing Systems - Open Systems Interconnection - Basic Reference Model.*

ISO 7498 AD3, *Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Addendum 3: Naming Including Addressing.*

ISO 8348 DAD2, *Information Processing Systems - Data Communications - Network Service Definition - Addendum 2: Network Layer Addressing.*

ISO 8473 *Information Processing Systems - Data Communications - Protocol for Providing the Connectionless-Mode Network Service.*

ISO DIS 8648: Information Processing Systems – Data Communications – *Internal Organization of the Network Layer*

ISO 9594 (equal to X.500), *Information Processing Systems - Open Systems Interconnection - The Directory*, Parts 1 through 8, 1988.

CCITT X.25: *Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit*, Fac. VIII.3, 1984.

CCITT X.75: *Terminal and Transit Call Control Procedures and Data Transfer System on International Circuits Between Packet Switched Data Networks*, 1984.

CCITT X.121: *International Numbering Plan for Public Data Networks*, Fac. VIII, 1984.

8. PROTOCOLS & USE OF STANDARDS

8.1 SUMMARY

This section discusses the use of standard protocols to permit uniform access to the proposed Network and to promote the interoperation of systems connected to the Network. The range of standards supported will determine the ease with which users may attach to the Network and will determine the range of applications that may be supported over the Network. The discussion concentrates on the emerging international standards being developed through the International Organization for Standardization (ISO) and the Consultative Committee for Telegraph and Telephone (CCITT) and discusses the support of other traditional end user oriented protocol standards such as TCP/IP. Traditional and developing internal protocols used by carriers to provide wide area networking services are also discussed since these will be important for the construction of the Network and will impact on very high speed access to the Network.

8.2 INTRODUCTION

It is generally accepted that the development and use of internationally approved standards will promote international trade and permit the global interchange of information and provision of services. This international trade will be both in the products which implement the standards and the information that can be transmitted via the compatible international systems. Although the former category of trade is well known, trade in information is a developing category. Canada, with its international reputation for communications technologies, is at the forefront of international standards development and has issued national government directives[1,1] towards the use of these international standards.

The proposed high speed network is expected to support the transfer of data, voice, video and other forms of electronic communications. These communications are expected to take place using an integrated communications network. This section addresses standards from the viewpoint of data standards, it is expected that standards applied to the transfer of voice, video and other communications information when they become available will follow these data standards.

The International Organization for Standardization (ISO), and to some extent the International Consultative Committee for Telegraph and Telephone (CCITT) and the International Electrotechnical Committee (IEC), represent the international organizations responsible for the harmonization of individual national standards in data communications. In addition to these organizations, there are regional assemblies of nations and assemblies of corporations

[1] On April 1, 1987, a new federal government policy on Open Systems Interconnection (OSI) was announced. This policy endorses OSI as a federal Information Technology strategy in preference to any manufacturer–specific or installation–specific architecture and requires departments and agencies to state a clear preference for OSI–based products and services in their procurement. Departments will be required to gradually migrate their systems based on the OSI preference.

who also promote and issue standards. In Europe the CEN/CENELEC group is responsible for harmonizing standards for the European Economic Community. In the United States NIST has been actively promoting the use of standards in both government and industry.

In the shorter term, many existing defacto communication standards are in use. Many of these are manufacturer or application specific. Both IBM and DEC have announced migration paths between their own communications standards and those of ISO. Application specific standards such as that developed in the US for the military are still also in common use, especially in the academic community.

8.3 RELEVANCE TO STUDY

It is proposed that the Network should not constrain the applications, including the communications test and development applications, which it is to support. Applications expecting to make use of the Network must use protocol standards which are either (a) supported by the Network or (b) effectively invisible to the Network. Protocols which are fully supported over the Network will provide maximum convenience for users since effective communications may be carried out with minimum user effort. Users who choose to use protocols which are not supported by the Network will need to ensure that they are invisible to the Network. Certain uses for the Network, e.g. remote protocol testing, will also require that the protocols being tested not impact on the ongoing operation of the Network.

In any event, a minimum level of protocol compatibility will be required for all connections to the Network. Additional protocols required to realize higher level `value added' enhanced communications service may or may not correspond to protocols actively supported by the Network, but rather by remote systems which support these enhanced services.

In addition to the protocols required for the interfacing of user equipment, it will also be necessary to consider the interfacing requirements of any foreign networks.

8.4 BACKGROUND

Wide area networks today are growing with at least four major trends in protocol standards. Beginning with ARPAnet in the United States, TCP/IP[2] networks have the largest following in the academic community. A variety of commercial networking standards have also arisen, for example IBM SNA networks, generally for commercial or government applications. Promoted by the telephone carriers, X.25 networks provide a convenient international networking standard which is still growing in popularity. Finally, international standardization efforts are promoting the use of new ISO based standards for networking which are an extension of X.25 and other standards. While many will argue that the future resides with the developing international standards, the reality is that traditional solutions will remain popular for some time to come and that the future standards still require considerable development both technically and commercially.

[2] Refer to section 8 for an explanation of all acronyms used in this paper.

Although the networking standards themselves differ, there is a generally accepted approach for describing them. These techniques were developed by the ISO and CCITT and are based on the use of the Open System Interconnection (OSI) model. The model itself does not specify standards, it only specifies the way in which standards should be partitioned and described. In some cases it was difficult to describe some traditional standards according to the new OSI model but in general the OSI descriptive approach may be used for all of them.

The OSI approach partitions standards into seven groups (called layers). Each layer progressively `value adds' the capabilities of the layer below until a fairly sophisticated service is constructed which is of direct utility to the user. Many different standards are available for each of the layers, and it will be necessary to rate the compatibility and invisibility of candidate standards within each layer. The appendix provides an overview of each of the seven OSI layers.

A major property of the OSI model is that each layer of protocol is expected to operate independently of both the layers below and above, thus the replacement of one layer's protocol standard with another is expected not to effect the other protocols in use. It should be noted that although this latter statement is true in theory, in many cases some imperfect standards exist which do interact with other standards.

For any given systems to interoperate, it is at least necessary for the same standards to be selected for each layer. In addition, most standards also include options and parameters which if selected improperly will prohibit interoperability. Thus both the standards and the options for each standard must be specified. Since this could be a complex task significantly open to error, the international community has chosen to define Standard Profiles which are application related and aimed at describing specific selections of protocol, option and parameters which when specified together will provide compatible implementations for specific application uses. These Profiles are being specified internationally (International Standard Profiles) and may also be specified by national and industry standardization groups. In Canada, the COSAC documents specify Profiles for specific applications, and the work of MAP and TOP may also be considered an effort to specify industry and application specific Profiles. It would be logical to ultimately specify or reference Profiles as the means to specify compatibility requirements for the High Speed Network.

8.5 NETWORK INTERCONNECTION STANDARDS

Figure 1 provides a logical view of two example end systems interconnected by a network. In the figure, the seven layers of protocols required to support communications are shown in each of the two end systems. Some of these layers are also required to be compatible with the protocols within the network as also shown in the figure. In this example, the horizontal dashed lines indicate that the corresponding layers at each end must be compatible. Some horizontal lines terminate at network equipment, this indicates that the protocols within the end system must be compatible with the corresponding protocol in the network provided equipment. Dashed lines which pass over the network provided equipment and terminate at the other end system indicate that these protocol layers need only be compatible with the end system, thus the network equipment treats these protocols transparently. Although this architecture provides maximum user flexibility in the selection of end system protocols, it provides no guidance on the selection of particular protocols – and of course common agreement on these will be required between the two end systems.

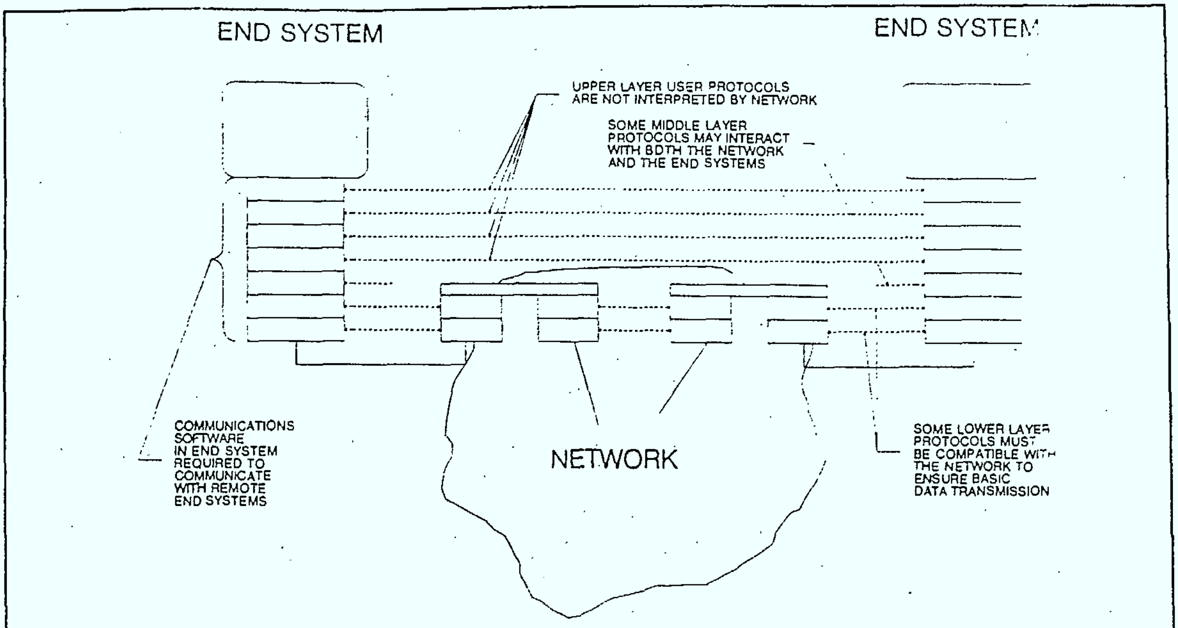
END SYSTEM
END SYSTEM
UPPER LAYER USER PROTOCOLS ARE NOT INTERPRETED BY NETWORK
SOME MIDDLE LAYER PROTOCOLS MAY INTERACT WITH BOTH THE NETWORK AND THE END SYSTEMS
COMMUNICATIONS SOFTWARE IN END SYSTEM REQUIRED TO COMMUNICATE WITH REMOTE END SYSTEMS
NETWORK
SOME LOWER LAYER PROTOCOLS MUST BE COMPATIBLE WITH THE NETWORK TO ENSURE BASIC DATA TRANSMISSION

FIGURE 1: NETWORK INTERCONNECTION WITH MAXIMUM TRANSPARENCY

Figure 1: Nctwork Interconnection with Maximum Transparency

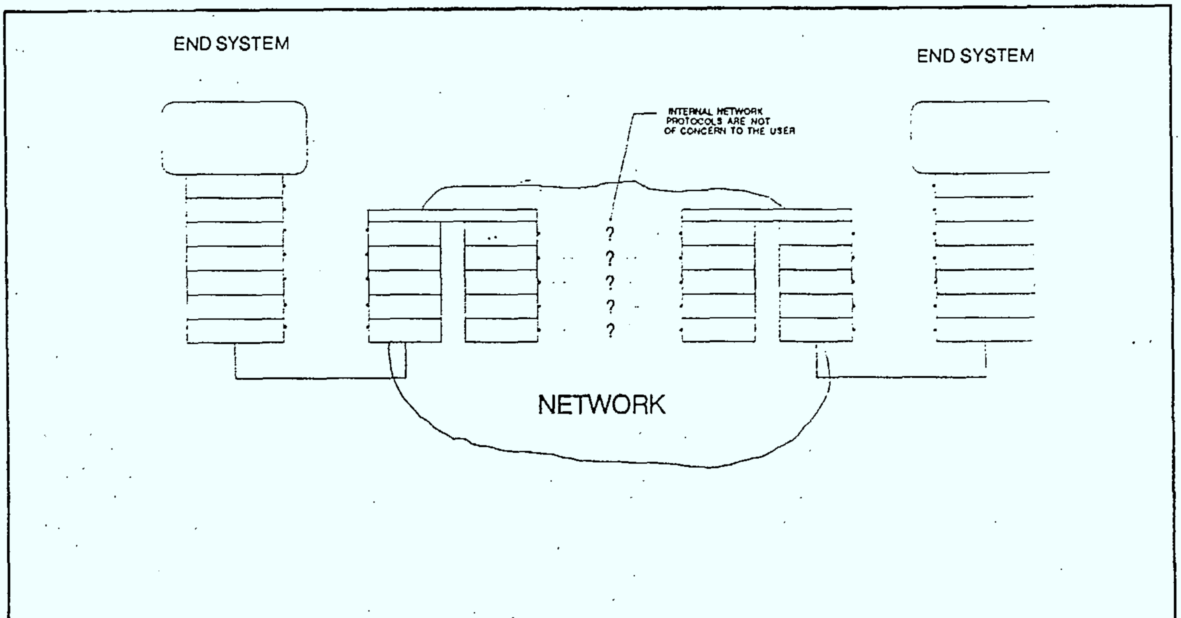

FIGURE 2: NETWORK INTERCONNECTION WITH LARGER NETWORK DEPENDANCY

Figure 2: Network Interconnection with Larger Network Dependency

Figure 2 provides another implementation example where more layers of the end systems are processed by the network equipment. In this example, only the uppermost layer is end–to–end, all others are processed by the network. Thus end user equipment will be required to be compatible to a much higher extent to the requirements of the network itself. On the other hand, since the lower layers interact with network equipment they need not be compatible end to end. Thus, although this example constrains the protocol options available to the end system, it does provide a mechanism for the construction of non–homogeneous end system networks.

Finally, Figure 3 provides a logical architectural example which provides the best of both worlds: the ability to invisibly interconnect the widest range of differing protocol stacks and the ability to perform selective translations between protocol stacks using a suitable intermediate system (this function is often called a gateway function).

The previous figures have indicated methods by which end systems may be interconnected by a single network. In practice, the proposed high speed Network will need to interconnect end systems and other networks. These other networks may be local area networks (LANs) or regional wide area networks (WANs). Such interconnections will require the use of internetworking functions which are also subject to standards.

8.6 APPLICABLE STANDARDS

The Network should satisfy two potentially conflicting requirements: the ability to invisibly interconnect end user protocol stacks with minimum impact, and the ability to provide end users with certain specific protocol stacks a user friendly interconnection.

The first requirement is best met by imposing minimum protocol requirements on the basic Network interconnect point as was shown in Figure 1. The second requirement will be met in situations where the end systems use the same protocol stack or, when they are different, with the provision of gateway interconnect services as was shown in Figure 3.

8.6.1 Conversion Between Protocols

The currently most popular protocol set for academic networks is that which was developed for the US ARPA network. This is generally referred to as TCP/IP but also includes certain other protocols for file access and transfer. Table 1 compares these protocols with those being developed for international use by the ISO. Not shown in the table are certain upper layer protocols used with TCP/IP for UNIX based machines.

A migration to the ISO based protocols is expected in the future since they offer greater functionality to the user and the previous TCP/IP based standards are no longer receiving the level of developmental support which is required to maintain such protocols. In the interim, then, some level of support for the TCP/IP stacks will be required, and a migration path shown towards the ISO based standards. The conversion between TCP and the corresponding ISO Transport Layer protocol class is considered fairly straightforward by some and proposals exist in the literature for such conversion devices[2].

It should also be noted, however, that the conversion between the FTP and ISO FTAM is considered more difficult, and probably not possible to attain unless complex store and

Figure 3: Network Connections Showing Maximum Interworking

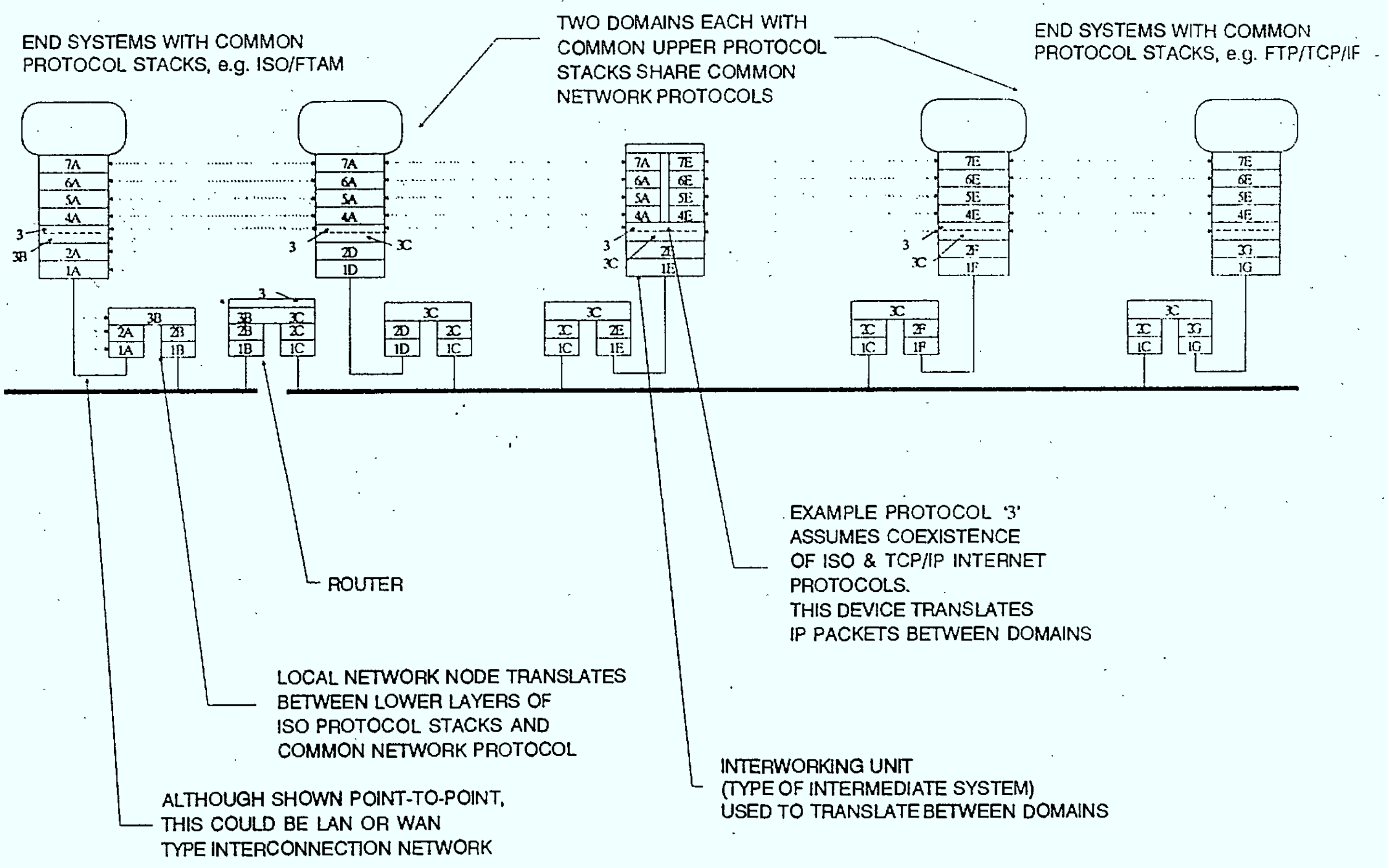
END SYSTEMS WITH COMMON PROTOCOL STACKS, e.g. ISO/FTAM
TWO DOMAINS EACH WITH COMMON UPPER PROTOCOL STACKS SHARE COMMON NETWORK PROTOCOLS
END SYSTEMS WITH COMMON PROTOCOL STACKS, e.g. FTP/TCP/IF
7A
6A
5A
4A
3
3B
2A
1A
2D
1D
3C
7E
6E
5E
4E
2F
1F
3G
1G
2B
1B
2C
1C
2E
1E
ROUTER
EXAMPLE PROTOCOL '3' ASSUMES COEXISTENCE OF ISO & TCP/IP INTERNET PROTOCOLS. THIS DEVICE TRANSLATES IP PACKETS BETWEEN DOMAINS
LOCAL NETWORK NODE TRANSLATES BETWEEN LOWER LAYERS OF ISO PROTOCOL STACKS AND COMMON NETWORK PROTOCOL
INTERWORKING UNIT (TYPE OF INTERMEDIATE SYSTEM) USED TO TRANSLATE BETWEEN DOMAINS
ALTHOUGH SHOWN POINT-TO-POINT, THIS COULD BE LAN OR WAN TYPE INTERCONNECTION NETWORK
C9001f3

FIGURE 3: EXAMPLE NETWORK CONNECTIONS SHOWING MAXIMUM INTERWORKING

Table I: Comparison between Military Standard Protocols and ISO Protocols

MIL-STD-1777 Internet Protocol (IP)	ISO 8473 Protocol for Providing the Connectionless-Mode Network Service
MIL-STD-1778 Transmission Control Protocol(TCP)	ISO 8073 Connection Oriented Transport Protocol Specification
MIL-STD-1780 File Transfer Protocol (FTP)	ISO 8571 File Transfer, Access and Management (FTAM)
MIL-STD-1781 Simple Mail Transfer Protocol (SMTP)	CCITT X.400 Message Handling System (MHS)
MIL-STD-1782 TELENET Protocol	ISO 9041 Virtual Terminal Protocol (VTP)

forward processing gateway devices were to be envisaged. Thus although a conversion between TCP/IP and the ISO protocols may be possible, the actual interoperation of such systems may not be possible due to the lack of conversion between the high layer protocols. In practice, however, the change from FTP and TELENET to the corresponding ISO protocols may not be so difficult for interested end system owners since these protocols are generally implemented in a more accessible manner in the end systems[3].

Some other protocols are in some common use as well, for example UUCP (Unix to Unix copy), and commercial solutions. It is expected that the interim migration solution offered for TCP/IP will be architecturally similar to those available to these users. In these cases, however, the provision of protocol translating equipment and software will be the responsibility of their user community.

8.6.2 Discussion of Specific Protocols

In the following sections, each of the layers, beginning with the Physical Layer will be discussed in turn, with an indication whether or not this layer will impose a requirement on the attached end system or whether or not the requirement will be imposed by the remote end system. In the latter case, some basic support for full interoperability should be recommended (but not mandated) so that users wishing to attach to the Network with minimum effort may carry out work immediately.

[3] This is discussed in some length in [GROE86]. It is suggested that most implementations of TCP/IP protocol stacks allocate the Transport and lower functions (the true TCP/IP functions) to software implemented within the computers operating system while the higher layer functions are often implemented as separate computer modules activated by the particular user's application program. Thus it is considered simpler to convert the latter components than the former.

8.6.2.1 The Physical Layer

The Physical Layer will be visible to all users wishing to install a new interconnection to the Network. The Physical Layer will provide the local physical interconnect to the nearest Network communications device. In general, once installed and operating correctly, the Physical Layer will remain static, not requiring further attention unless a higher data rate interconnect than that initially installed is required. Furthermore, different users of the Network may make use of different Physical Layer interfaces since these interfaces are of local significance only, they do not effect the overall operation of the Network.

For sophisticated access, this interconnect must operate at a minimum of 1.544 Mbps with a migration plan to 45 Mbps. Some low cost interconnects for less demanding users may operate at lower rates (9600 to 64Kbps).

If remote–from–Network–node high capacity transmission is required (e.g. between buildings in a city) then these lines may need to be supplied by the local carrier. For the latter case, interconnects must conform (for the transmission part at least) to the DOC CS–03 Standards for Terminal Equipment and Connection Arrangements[3] at the 1.544 Mbps rate, and higher rates when these standards are issued (new CS–03 standards for higher rates are expected in the near future).

Remote access at rates of 64Kbps and lower (for less demanding users) would be easier to accommodate since international standards in this range are available. For non–ISDN access, traditional standards such as RS–232D, RS–422, RS–423 (equivalent to CCITT V.28, V.11 and V.10) cover the electrical specifications while ISO 2110 (as used in RS–232D), ISO 4903 and RS–530 cover physical connectors.

In certain situations a discrete exposed electrical interface will not be required. For example, if the a Network node processing device were to have direct access (or be combined with) a local user's LAN or WAN node processor then this high speed interconnect would be internal to this equipment.

8.6.2.2 The Data Link Layer

The Data Link Layer will guarantee the error–free transfer of information between the user and the Network node over the Physical Layer discussed in the previous section. Many of the issues discussed in this previous section are also relevant here. The local Data Link Layer protocol is of local significance only and may vary from one interconnect point to another. For convenience it is expected that a similar (or the same) protocol will be used for all high speed interconnect points.

The Data Link Layer is only responsible for the delivery of error free data bits across the interface. Traditional Data Link protocols are candidates for this application, for example the Frame Level part of the X.25 protocol (ISO 7776) would be applicable. A difficulty may exist in operating these traditional Data Link protocols above 1 Mbps since this is not their traditional use and equipment (semiconductor devices) capable of operating at these rates are not readily available[4]. Other newer protocols (e.g. the Data Link Layer of FDDI or one of the ISO 8802 series protocols) may be applicable but these are generally more complicated than is required for a simple full duplex point to point link as used here. Of particular importance when selecting this Data Link Layer protocol is the migration rate to very much higher data rates (to 45 Mbps), and this will place severe constraints on the selection.

As discussed in the previous section, if this interconnection is within a single piece of equipment or a pair of equipments in close proximity, then a variety of local computer interconnect methods are candidates, e.g. SCSI, or even a full LAN interconnect could be used.

8.6.2.3 The Network Layer

The Network Layer is the first layer where interactions with the Network are less easy to define. The Network Layer is nominally responsible for the provision of the `Network Layer Service' to the layer above (the Transport Layer). Two main types of Network Service are generally defined: a *connection oriented service* and a *connectionless service*. A connection oriented service uses an initial call set–up procedure prior to data transmission much like the voice telephone system. Connectionless services allow the direct transfer of information without a call set–up procedure, but each information transfer must contain sufficient additional information to identify the recipients, this is most similar to the traditional mail system. Within the communications industry, considerable discussion occurs regarding the relative merits of each, and in general no consensus exists about whether one or both (or which one) should be supported over any given network. This subject is discussed further in the *Network Architecture and Migration Plan* section. Traditionally connectionless services have been preferentially supported over LANs while connection oriented services have tended to be favoured by WAN suppliers.

The ARPA network in the US and the correspondingly used TCP/IP protocols prefer the use of a connectionless network service. The original ISO approach favoured a connection oriented network layer, although this has subsequently been modified to include the use of connectionless services. The original X.25 standard was entirely oriented around the provision of connection oriented services while later additions allow the optional use of procedures more appropriate to connectionless operations.

In addition to providing the protocol interactions necessary to support these services, the network layer as defined by the OSI model is responsible for uniquely addressing end systems. The network layer must also support all the required routing and relaying functions necessary to route information between the end systems through intermediate network(s) and system(s).

Thus it is clear that the functionality required of the network layer is distributed between the end systems and the network itself. This partitioning makes discussions regarding the network layer difficult. This difficulty was exasperated because it was necessary to fit existing protocols into the new OSI model.

To facilitate the description of the Network Layer, and to facilitate the integration of the CCITT X.25 protocol into the OSI model, the ISO chose to subdivide the Network Layer into three parts. The Sub–Network Independent Convergence Protocol (SNICP) is responsible for providing the connection and/or connectionless service, is responsible for complete network type(s) independent addressing and is responsible for routing between sub–networks. The Sub–Network Access Protocol (SNAcP) is sub–network dependant and provides the network type specific addressing and other functions necessary to share the use of the lower Data Link layer service among multiple transport connections (X.25 PLP is an example of an SNAcP). The Sub–Network Dependant Convergence Protocol (SNDCP) corrects any abnormalities or deficiencies in the services offered by the particular subnetwork type so that the SNICP can be a common protocol for multiple sub–network types.

Traditionally the network layer procedures which are used internally by the carriers in their network have been proprietary and not visible to the user (in Figure 3 for example, the carrier protocols would be those shown as 1C and 2C). The carrier provides interfacing functions within the local node equipment to convert the internal carrier network layer protocols to standardized protocols known to the user, e.g. the X.25 Packet Layer Protocol (X.25 PLP, ISO 8208) which supports network addressing definitions[4] and the multiplexing of multiple transport connections over the same local network node interconnect. Thus in the ISO context when using X.25 to access a WAN, the SNAcP (X.25 PLP) in one end system interacts both with the local node interconnection device and sometimes with the remote end system[5], the ISO defined SNDCP and SNICP protocols[6] currently interact end to end and end to intersubnetworking unit[7].

Many documents discuss Internet Protocols (IPs). The most famous IP protocol is the one used for ARPAnet – the IP part of TCP/IP. This protocol is designed to operate over connectionless network services although it can operate over connection–mode services as well. From the ISO perspective the IP fits within the SNICP of the Network Layer, and the currently proposed ISO SNICP protocol (ISO 8473) is closely modelled on the ARPA IP and is sometimes referred to as ISO IP.

Due to its widespread availability, the X.25 PLP must be considered a prime candidate for access to the Network at data rates below 64kbps. At the present time access at rates below 19.2 kbps would be straightforward in that standards exist and are in common use in Canada. Access at rates above 19.2 will require the use of extensions to current common practice in Canada, although international ISO approved standards are available which are suitable to higher rates. The upper speed limit for the use of this protocol will depend upon a number of factors, access up to 64 kbps is considered technically straightforward and operation to 1

[4] Since this is one network of many potential networks used to interconnect the end systems, so this carrier network is considered a sub–network; and the addressing here is one of several that may be needed to route information completely between the two end systems, thus this subnetwork address is called the `Sub–Network Point of Attachment' (SNPA). The format for this particular SNPA is defined in X.121.

[5] There are components of the X.25 PLP which interact with the local network node and the remote system. For example, the confirmation of packets may be local or end to end depending upon the use of the protocol's `D' bit procedure. Many would argue that such variable interrelationships should be avoided.

[6] The ISO defines protocols to support the ISO defined connection and connectionless Network Layer services using both X.25 and the ISO 8802 series of LAN protocols.

[7] The ISO is in the process of approving protocols relating the support of international addressing techniques and the transmission of the information necessary to support routing functions.

Mbps potentially feasible. Updates to the X.25 procedures are being defined for ISDN, so that this technique is compatible with ISDN access as well. It should be noted, however, that X.25 PLP as currently defined is optimized for the provision of connection oriented operations and this may not be optimum in applications where the connectionless network service is to be supported.

Due to the expected data rate limitations of X.25, high speed access to the Network may not be capable of using this protocol. It has also been indicated that the connection orientation of this protocol may also impede its use.

Options other than X.25 are being developed, for example the `virtual channel' protocols being proposed for Frame Relaying, Asynchronous Transfer Mode (ATM), SONET and others. Some of these are standards which are being contemplated for use within the carrier network. A selection of one of these protocols could minimize the protocol translations necessary in the network node interconnection device and could thus optimize performance and efficiency and particularly may minimize the delay inherent in the resulting communications path.

This section, and the two sections before this one, have not explicitly discussed the selection of standard protocols for use within the carrier network(s) itself. This is because the selection of these protocols are largely independent of the selection of the protocols visible to the user, except with the exceptions discussed in this current section for the Network Layer.

8.6.2.4 The Transport Layer

The Transport Layer is responsible for the orderly and reliable delivery of information between end systems. If the underlying Network Service in use is connection oriented, it is generally assumed that the information will be delivered in order and with high reliability, and thus the extra enhancements that must be provided by the Transport Layer are minimal. For the more basic connectionless Network Service, the Transport Layer must ensure the correct ordering of information and may be required to provide additional error controls.

For the ISO Transport Layer protocols (ISO 8073 and ISO 8602) there are currently five classes of operation and these are identified by number. Transport Protocol Classes 0 through 3 are useful for operation over connection oriented Network Service applications. Transport Class 4 is required for implementing a reliable transport service over an (unreliable) connectionless network service.

The transport protocol of ARPAnet (TCP) assumed a connectionless service and thus corresponds most closely with ISO Transport class 4.

It is expected that the Network itself will not require the use of any specific Transport Layer protocol since the selection of Transport Protocol is theoretically independent of the Network Protocol. However, as implied in the previous paragraphs, any selected Transport Protocol must use only those services which are provided by the selected Network Protocol. In addition, when users interact with a remote end system, they must ensure that the peer level Transport Protocol is the same as the one they choose to use.

To facilitate the attachment of new end systems to the Network who wish to use resources (end systems) already existing on the Network, it will be convenient to define certain default Transport Layer protocols which are recommended for use. This will facilitate interoperability of systems. As indicated in the introduction to this section, the ISO protocols are expected to be the future path and thus the support of the ISO Transport protocol. In North America, Transport Class 4 over a connectionless Network Service is becoming popular for applications requiring reliable transport, and this is discussed further in the *Network Architecture and Migration Plan* section. For the support of traditional academic applications, the interim support of TCP would also be recommended.

8.6.2.5 The Session and Presentation Layers

Both the Session and Presentation Layer standards are only relevant for the ISO protocols. These protocols are expected to be selected on an end–to–end basis and will not interact with Network components. ISO 8327 specifies the ISO Session protocol while ISO 8823 defines the Presentation protocol.

8.6.2.6 The Application Layer

Since a range of user applications will be supported over networks, several Application Layer protocols are required to support these different applications. Table 1 identified three Application Layer protocols typical of TCP/IP implementations and the corresponding ISO standards. The Unix to Unix Copy (UUCP) and IBM RCSC protocols are also Application Layer protocols. Within the ISO, the services to be performed by the Application Layer are divided into common application service elements and specific application service elements. Common elements are provided to establish associations between instances of communications, etc. and specific elements are provided for file transfer, job transfer, message exchange (mail), and remote terminal access. Thus a list of ISO standards are required to specify all of the protocols required to support these various application uses for the communications function.

8.6.2.7 Standard Profiles

Standard profile will ultimately be required to specify the protocols and option required to support a particular application's use of the communications network. These profiles may be drawn from national or international sources. Since the Network may support several 'domains' of interaction, profiles for each domain of interoperation will be required. The production of internationally approved profiles is still in its early stages. At the present time, an international profile for File Transfer is reaching the approval stage, and other international profiles are expected to follow.

8.7 CONCLUSIONS AND RECOMMENDATIONS

This section has proposed that access to the Network should be supported with standardized protocols. The international trend follows standards approved by the International Organization for Standardization (ISO) and related international approval organizations. It is proposed that support for the traditional TCP/IP (and associated methods) should also be supported on an interim basis through the use of gateway devices sited somewhere on the Network.

This section has proposed that from an interfacing viewpoint, two major classes of user will need to be supported: (a) those users wishing to connect to the Network with minimum effort

61

APPENDIX: THE LAYERS OF THE OSI MODEL

There are many excellent reference books which discuss the Open System Interconnection Model as described in the International Organization for Standardization standard ISO 7498. This appendix summarizes the role of each layer in the model to the extent necessary for the current discussion.

Figure 1 showed the seven layers of the model and these are discussed briefly below.

When transmitting information between two end systems with zero or more intermediate systems, the layers of the OSI model may be considered to fulfil the required functionality in three parts: The Physical and Data Link Layers are responsible for getting messages from one node to the next node (for example, between an end system and its adjacent intermediate system). The Network Layer is responsible for finding the best route between the end systems by using potentially different routes and the Transport Layer is responsible for getting the information across correctly and in the right order. Finally the Session, Presentation and Application Layers are 'end system' specific and are responsible for the provision of consistent services (i.e. services of the same kind and format) tailored to the specific application programs.

All interconnections, whether they be point–to–point without and intervening intermediate system or whether they be multi–hop through multiple sub–networks, all require the same capabilities and thus require communications capabilities which may be categorized using the seven layer model.

The **Physical Layer** considers all of those aspects of communications relating to the translation of a logical signal internal to the end system into an 'exposed' electrical or optical, etc. energy signal which may be transmitted over distance using the defined transmission medium. It includes all of the encoding and modulation aspects and defines the physical connector required. Standards which are grouped under the Physical Layer include connector definitions, electrical voltage/current definitions, radio modulation definitions, wire specifications, optical component specifications, etc.

The **Data Link Layer** considers all aspects relating to the packaging of information into their most elemental (for the medium) package, the addition of error control information, and all other functions required to realize reliable communications over the wire, optic, etc. Physical Layer defined medium. Standards grouped under the Physical Layer may include sub–networking addressing (physical addressing), cyclic redundancy code specifications, and in the case of multi–access media, media access control protocols.

The **Network Layer** considers all aspects relating to the routing of messages between end systems irrespective of whether the systems are on the same, or an interconnected, sub–network, and regardless of the distance between them. The process of routing involves the derivation of individual sub–network addresses for each hop of the transmission from an overall address provided for the end system. Thus the Network Layer is intimately involved with maintenance of a Directory for end systems and the correspondence between a Directory entry and a sequence of sub–network addresses.

The **Transport Layer** considers all aspects relating to ensuring a reliable and efficient and network independent end–to–end data transfer. It may detect and correct errors and re–order the information received such that it is delivered in the same order as transmitted.

The **Session Layer** is the first of the three application–oriented layers. It encompasses all protocols responsible for setting up and managing dialogues between end systems. Protocols in this group include those required to choose the type of dialogue required, to transfer user and control information over the session connection, to transfer synchronization and resynchronization signals and to re–establish the status of the session connection after resynchronization.

The **Presentation Layer** considers all aspects relating to the setting up of `transfer syntaxes' and to provide translation between transfer syntaxes. This involves the definition of the information to be transferred and it representation in an unambiguous bit–level format for transmission over the network.

The **Application Layer** considers all aspects relating to the interface to the user's processes. Since there are many types of user process that must be accommodated (e.g. file transfer, electronic mail), there must be many Application Layer protocols to provide the services required of each.

so that they can quickly access the Network in support of their work, and (b) those users wishing to utilize the network for experimentation and testing who require that the Network be as transparent as possible to their equipment. To maximimize the Network's utility to the latter and to make the widest range of end system protocol selections possible, it was proposed that the Network interfacing nodes should minimize the amount of protocol processing that they perform. With respect to the OSI model, this means that the local Network interfacing devices should have a minimum number of protocol layers.

This section has provided a brief overview of the OSI reference model which should be used to organize the description of the relevant standards. The Network will impose interfacing constraints at least at the two lower layers of the model, and may additionally require specifications at the third layer. Existing ISO and other popular standards at these layers were discussed with respect to their applicability at these layers, and it was noted that a current gap exists for appropriate protocols at the Network Layer. Higher layer protocols are expected to follow the emerging ISO approved standards but interim support will be required for traditional standards such as TCP/IP and UUCP. A method for the support of other standards in addition to these is possible by the inclusion of suitable additional gateway devices.

In the future it will be usefull to examine the impact of the protocols used by the wide area carrying mechanisms to ensure that the overheads of the Network interfacing equipment have a minimum impact. This area will be very important when higher network speeds are contenplated.

8.8 REFERENCES

1.[TBIT89] Treasury Board of Canada, *Canadian Open System Application Criteria (COSAC) Overview*, Treasury Board Information Technology Standard Number 6.1, June 1989.

2.[GROE86] Groenbaek, I, *Conversion Between the TCP and ISO Transport Protocols as a Method of Achieving Interoperability Between Data Communication Systems*, IEEE Journal on Selected Areas in Communications, vol SAC–4, n2, March 1986 pp288–296.

3.[DOC88] *Standard for Terminal Equipment, and Connection Arrangements Systems, Network Protection Devices*, Communications Canada, CS–03, Issue 6a, Jan 1988.

4.[TERA88] Terada, Y., *High Speed, Broadband Communications and OSI*, Computer Standards & Interfaces, vol 7 n 1–2 (special issue), 1988 pp23–28.

8.9 LIST OF ACRONYMS

CCITT	–	International Telegraph and Telephone Consultative Committee
COSAC	–	Canadian Open System Application Criteria
DEC	–	Digital Equipment Corporation
DOC	–	Department of Communications (Canada)
FTAM	–	File Transfer, Access, and Management (ISO)
FTP	–	File Transfer Protocol (MIL–STD–1780)
IBM	–	International Business Machines
IEC	–	International Electrotechnical Commission
IP	–	Internet Protocol
ISDN	–	Integrated Services Digital Network
ISO	–	International Organization for Standardization
LAN	–	Local Area Network
MAP	–	(General Motors) Manufacturing Automation Protocol
NBS	–	National Bureau of Standards (now called NIST)
NIST	–	(United States) National Institute of Standards and Technology
OSI	–	Open System Interconnection (model)
PLP	–	Packet Level Protocol (as per X.25)
SNAcP	–	Subnetwork Access Protocol
SNDCP	–	Subnetwork Dependent Convergence Protocol
SNICP	–	Subnetwork Independent Convergence Protocol
TCP/IP	–	Transmission Control Protocol/Internet Protocol
TOP	–	(Boeing) Technical Office Protocol
UUCP	–	Unix to Unix Copy
WAN	–	Wide Area Network

9. LOW COST ACCESS METHODS

9.1 SUMMARY

This section describes the network access possibilities and methods of achieving them. For the purpose of this study, access to the network means connection to one of its nodes, that is, a designated switching host. This connectivity could be either through fixed and permanent links or temporary and ad–hoc arrangements. The main focus of this section is to look at the situations where individual user access is required on a short term and irregular basis and within a low cost budget. The subject of access for a group of users normally connected to a LAN is treated in a separate section on "High Speed Transmission Methods, Technology and Networking", [14]. A number of commercial services through which access can be arranged are described. These services have different technical and cost characteristics and therefore not all are suitable for all applications. Examples of costs and rate structures are outlined for each product. In conclusion, some typical applications of each product is highlighted.

9.2 INTRODUCTION

Traditionally, the normal access method to a computer facility has been through dial–up and fixed link modems using the Public Switched Telephone Network (PSTN). This method of accessing computers is still wide spread. It has however advanced in the past two decades from a low speed error prone facility to relatively high speeds (as high as 64Kbps) and reliable arrangement. In addition to the access using modems and PSTN, there are a number of public and private data networks utilizing a variety of transmission and transport technologies. These facilities can also be used to gain access to a processing node and are discussed in the following sections.

9.3 RELEVANCE TO THE STUDY

Convenient access to a national network is essential because it can significantly increase the utilization of what might constitute an expensive network facility. It is essential to meet the needs of widest community of users including small and/or irregular users where the access method must meet the cost/requirements trade off of their application. In order to minimize fixed costs associated with a WANs basic structure, one should attempt at maximizing the convenience of temporary and occasional access. Therefore, low cost access, if available, maximizes the use of the network and reduces the need for a large number of nodes, their costly interconnections and hence make it more cost effective to operate such network.

9.4 BACKGROUND

The past few decades have witnessed a proliferation of networking concepts and technologies. As computer technology advances so does the need for information transfer and exchange. This has resulted in the establishment of many public and private WANs in Canada and mostly in USA. Most of these networks have been instigated by the needs for information exchange in commercially non–competitive environments such as Universities and other public research establishments (e.g. all R&D networks). The need for data transfer within such communities has led to the current investigation looking at the feasibility of a Canadian national high speed network primarily for research and development. This study looks at the current and future requirements of such network in terms of, user population, data load and capacity, applications, technologies and transition or migration strategies. In addition, the study focuses on the economical and utilization aspects of this network.

There have been a number of similar initiatives in Canada. One of these is the NRnet. NRnet provides an initial operating speed of 56Kbps with future expansion to 1.5Mbps. This study will be based on the NRnet initiative and will examine the feasibility of a network with greater bandwidth and functionality. As part of this study, a number of technical sections have been produced, of which this is one.

9.5 ACCESS METHODS

Interconnection to a network can be achieved using a number of different connection mechanism and access methods. Networks in R&D environment, because of their potential wide area of application and location, are likely to utilize a variety of access methods. Access could be on the basis of a permanent link or temporary and on demand connections for remote and mobile users. Examples of such cases could be categorized based on the user location relative to the nearest node, or the nearest user facility which has access to a node, and availability of communication facilities. These are:

1. Metropolitan Access (MA) – Access from within a metropolitan area where public and private telephone and data networks are widely available; e.g. access from a user's home or a location other than his permanent work area;

2. Remote Access (RA) – Access from a remote location where the only means of communication is through public telephone network; e.g. remote rural areas or on–site expedition locations;

3. Isolated Access (IA) – Access from an isolated area where no means of wired communication would be available; e.g. arctic expedition and research sites in isolated parts of the country.

Often, users of a network are permanently connected to a local network node. A local network node can be defined as a switching host to which a user has a direct permanent access, either by a direct short local link or through a local gateway. However, in many situations this is not the case and some users find it necessary to gain access to the network from locations different from those they have existing access to the network. Similarly, there are occasional users who would use the network on an ad–hoc basis and therefore do not posses an existing permanent link to the network. Typical reasons for such access to the network under conditions described above are:

1. Research and investigation taking place in remote areas for the purpose of data collection and information gathering;

2. Access to databases kept at a base location by researchers gathered at a remote location;

3. Access to the network facilities by occasional users who do not have a permanent link to a node;

4. Access to the network by mobile services for the purpose of carrying out their mission (e.g. mobile libraries)

Under all of these circumstances, a convenient and economical method of access would be required. There are a number of commercial services offered by, mostly, telephone companies and private organizations (less so in Canada). In addition, there are organizations who are willing to provide access to occasional users through their already connected facilities. Examples of these would be Universities, research establishments and companies with significant amount of interest in R&D activities. In the following sections we will describe the existing commercial facilities available in Canada.

9.5.1 PSTN Access

The most commonly used and economical access method is the use of Public Switched Telephone Networks (PSTN) and modems. An individual can gain access to a network node, or a processor which has existing access to the network, by using one of many different types of dial–up modems. Dial–up modems technology has advanced significantly in the past decade. These devices are now capable of speeds, in the electrically noisy environment of PSTN, that were only possible using short RS232 cables. Speeds of 4.8 and 9.6Kbps are now widely available. The cost elements are the pair of modems and the PSTN holding time.

9.5.2 Telecom Canada Datalink

Datalink is a service provided by the member companies of Telecom Canada. It is a circuit switched digital facility that utilizes the digital nodes in the public telephone network. The subscriber loop is a dedicated one and operates using a data transmission system called *Datapath* developed by Northern Telecom. Datapath transmit data at speeds up to 64Kbps. In fact it operates at 64Kbps. The devices that operate at slower speeds, are automatically rate adapted to 64Kbps. Datapath uses Pulse Code Modulation (PCM) together with Time Compression Multiplexing (TCM) at 160Kbps to support a full duplex 64Kbps transmission facility over the subscriber loop. The distance limitation on the loop is about 5Km to the nearest node. Datalink is suitable for applications requiring high speed reliable bulk transfers over long distances in a non–continuous manner.

Currently, Datalink is offered in 63 locations in Canada mostly in Ontario, Quebec and BC. The user access is through an RS232 link operating synchronously at 2.4, 4.8 and 9.6Kbps. This is a half or full duplex link with full code transparency and auto answer facility. Access from outside Datalink serving areas can be arranged via analogue access arrangement.

The rate structure is based on the concept of "pay–as–use" in the form of a monthly usage charge. There is a one time installation charge and, monthly options and access charges which include all equipments costs. The minimum contract period is one month. A summary of the charges are as shown below:

Access Arrangement:

A monthly charge of $145.50 (2.4Kbps) to $370.50 (9.6Kbps) for the link, plus a one off service charge of $125.00 per service point.

Usage Costs:

A two tier usage costs structure based on time, speed and distance applies. Basic rates apply to accumulated time up to 500 minutes and, discounted rates (about 30%) apply for holding times above 500 minutes. The basic rate for the 2.4Kbps service varies, depending on distance, from $0.013 (up to 20 miles) to $0.062 (above 1676 miles) per six–second period. For the 4.8 and 9.6Kbps lines, the corresponding figures are $.02 and $0.087.

More detailed information can be found in reference [2].

9.5.3 Telecom Canada Dataroute

Dataroute is another digital service offered by Telecom Canada members. It provides a dedicated end–to–end fixed circuit with international access. This digital network has been operating since early 70's and now serves over 100 cities across Canada. The service supports synchronous speeds of 1.2 to 56Kbps in any of two–point, multipoint or multidrop configurations with dial access at 1.2, 2.4, and, 4.8Kbps speed rates. Asynchronous access is at 110 to 1200 bits/s with similar configuration options to the synchronous facility. Access from outside Dataroute serving areas can be arranged through analogue access arrangement. The minimum contract period is one month.

The rate structure is based on a number of factors. In Canada, these factors are: speed, distance, transmission type, serving area and duration of service per day (24–hour or day service between 7am and 9pm). For Ontario and Quebec, the monthly rates summary is as follow:

Asynchronous Service:

7am to 9pm (24–hour):

300 bits/s	$0.97($1.075)/mile for 1st 50 miles and down to $0.12($0.13)/mile for distances above 300 miles;
0.6/1.2Kbps	$2.24 ($2.49) to $0.34 ($0.37)(as above);

Synchronous Service:

7am to 9pm (24–hour):

1.2Kbps	$2.45($2.71) to $0.37($0.41)
2.4Kbps	$5.17($5.74) to $0.57($0.64)
4.8Kbps	$7.38($8.20) to $0.79($0.88)
9.6Kbps	$11.02($12.25) to $0.99($1.1)
19.2Kbps	$16.03($17.81) to $1.38($1.54)
56Kbps	$54.85($60.94) to $4.48($4.97)

For TransCanada services, different set of numbers would apply. They are based on longer distances and are generally about 10 to 30% lower than the corresponding figures shown above. However, the larger discounts applies to higher speed links. For example, the monthly rate for the 24–hour synchronous link at 56Kbps is reduced from $60.94 to $42.42 for the first 100 miles(as oppose to the first 50 miles).

The rates for service between serving points in more than two serving areas are calculated differently. Detailed tariff information can be obtained from the operating companies or by consulting the Bell Canada Tariff filed with CRTC "CRTC6716/Part 4/Sec.12" [1].

9.5.4 Telecom Canada Datapac

Datapac is a digital data network utilizing packet switching technology. User data is collected and transmitted in packets which also contain control information. This service is provided to users within or outside the Datapac serving areas. There are currently over 90 serving areas in Ontario and Quebec and over 80 in the rest of the country. Each serving area is classified in accordance with the services they provide. These grades are used for rates identifications. The three different grades are: grade 1 for direct access, 2 for extended access to Dataroute serving areas and, 3 for extended access to non–Dataroute serving areas.

Datapac supports a number of access arrangements and functional options. The current options available include: Closed User Group (CUG), Reverse Charge (RC), Network User Identifier (NUI), Permanent and Switched Virtual Circuits (PVC,SVC), Hunt Group (HG) Call Redirection (CR) and, Call Negotiation (CN). There are five access arrangements as described below:

1. Datapac 3000 – This provides X.25 synchronous access to Datapac network. The Data Terminating Equipment (DTE) must be a packet mode DTE operating in accordance with X.25 protocol. Access can be either through dedicated point–to–point links or via dial–up method. The dedicated access can run at speeds in the 1.2 to 19.2 Kbps, whereas, the dial–up option operates at 2.4Kbps only.

2. Datapac 3101– This provides access for non–packet mode DTEs. It supports most character mode terminals using ASCII character code. The service is offered through RS232 interface at speeds of 110 to 2400 bps operating asynchronously in full duplex mode. Both dedicated and dialed access arrangements are catered for. This service is an implementation of CCITT triple X standards X.3, X.28, and X.29 commonly referred to as Packet Assembler/Disassembler (PAD) standards.

3. Datapac 3201– This is a service to support asynchronous polled devices which use ANSI X3.28 protocol. 3201 is provided either on shared lines or dedicated facilities at the discretion of the operating company (due to possible technical limitations).

4. Datapac 3303 – This supports synchronous polled devices. The supported protocol for this service are: IBM 3270 BSC/SDLC operating at 2.4, 4.8 and. 9.6 Kbps. This service is provided through synchronous PADs and Datapac Access Software (DAS) on dedicated or dialed facilities.

5. Datapac 3304 – This synchronous access arrangement supports IBM BSC multileaving protocol and EBCDIC character set.

6. Datapac 3305 – This is another synchronous access method used for IBM BSC point–to–point configuration (IBM 2780/3780) and EBCDIC character set.

3305 is provided via RS232 at speeds of 2.4 or 4.8Kbps on either a dedicated line or dialed facility.

The cost structure is based on two main components: access and usage. The total cost includes: monthly access charge, PAD usage charges, features charge and, network usage based on the number of packets and call set–ups. A call set–up charge of $0.01 is made for each user initiated instance. The network usage charge is calculated by multiplying the number of data segments (1 segment equals 256 bytes) by the appropriate grade/distance rate. The usage rates vary by distance between the calling and called points and the grade of the serving area. For example, for distances up to 100 miles, grade 1 to grade 1 charge is $0.35 per kilosegment whereas, grade 3 to grade 3 figure is $2.95. Similar figures for distances above 1000 miles are $1.70 and $6.60 respectively. Monthly charges for the optional features are anywhere between $1.35 to over $50.00. Other charges are service specific as indicated below:

1. Datapac 3000 – Monthly rate of $200.00 for 1.2Kbps and $760.00 for 19.2Kbps, both dedicated lines, with a fixed service charge of $250.00 per point. For dial access the charge is $0.04 per minute.

2. Datapac 3101 – Monthly charges vary between $100.00 and $200.00 depending on speed and access method. Also a PAD usage charge of $0.50 per kilosegment is applied.

3. Datapac 3201 – PAD charge of $0.65 per kilosegment plus monthly access charge of $100.00 (for up to 20 miles) to $385.00 (for 400 to 450 miles). These figures are for shared lines, different charges apply to single lines.

4. Datapac 3303 – Monthly rates of $320.00 (within a serving area) and $175.00 (outside a serving area) plus a service charge of $250.00. Also a PAD charge of $0.70 per kilosegment applies.

5. Datapac 3304 – Monthly rate of $205.00 (2.4Kbps) to $460.00 (9.6Kbps) for lines within a serving area and, $103.00 (2.4Kbps) to $230.00 (9.6Kbps) for lines outside a serving area. A service charge of $250.00 and PAD charge of $0.80 per kilosegment is applicable.

6. Datapac 3305 – Monthly rate of $230.00 plus $250.00 service charge for private dial access. $0.10 per minute for public dial access. Monthly rate of $215.00 (2.4Kbps) to $310.00 (4.8Kbps) for lines within a serving area or $108.00 (2.4Kbps) to $155.00 (4.8Kbps) otherwise.

For further details see reference [3].

9.5.5 Telecom Canada Megaplan

Megaplan is a digital network service with three specific products: Digital Channel Servi–ce(DCS), Megaroute and Megastream. Although these are not considered low cost facilities, there may be situations that warrants their use. These are therefore briefly described below.

1. DCS is a point–to–point synchronous facility at 2.4, 4.8, 9.6 or 56Kbps

between two points in the same serving area. There are nine serving areas in Ontario and Quebec (major cities). The rate structure is based on access, link and channel components. The monthly access rates vary from $85.00 per service point, for 2.4Kbps, to $105.00, for 56Kbps, plus a service charge of $150.00. The monthly link charge per serving wire–center varies from $60.00 (2.4Kbps) to $120.00 (56Kbps). The channel cost is $1.25 per 400 meters for service points located in different wire–centers of a serving area.

2. Megaroute is a synchronous point–to–point facility in the same exchange or different ones. It operates at 1.544Kbps in accordance with T1 specification. The service is offered on the basis of 1, 3 or 5 year contracts. The facility can be connected to customers own equipments or carrier provided ones. The rate is structured as DCS. For serving points within the same exchange, the monthly rates for the access portion of the cost is(based on 3–year contract) $480.00 (common equipment) plus $270.00 (access system) plus $310.00 (construction) per service point. The monthly link cost is $40.00 per serving wire–center and, the monthly channel rate is $30.00 per each 400 meters. For service points not in the same exchange, an additional charge of $120.00 per mile, for the first 10 miles, and $250.00 per mile for additional miles is applicable. When service points are between rate centers, the channel portion of the rate consists of a fixed base cost plus a per mile additional cost. For example, two service points one in Ottawa and one in Toronto would have a monthly channel rate of $24200.00 plus 300(miles distance) multiplied by $40.00. A total of $36200.00 per month. Similar calculation for a TransCanada channel between Ottawa and Vancouver (3000 miles) would be $80500.00.

3. Megastream is a digital facility with transmission in multiples of 64Kbps. This is a point–to–point synchronous facility provided within and between exchanges with similar contract period arrangement as Megaroute. There are five components to the rate structure: terminating equipments, access, link, network and others. Charges are comparable to Megaroute with lower total cost corresponding to smaller capacity(1/12).

9.5.6 CNCP Products

CNCP has similar products to Telecom Canada. Their currently tariffed products are: FASPAC (previously called Infoswitch), Infodat and, MACH(III).

FASPAC is a nationwide packet switched data network with about 120 serving areas. This service is available 24 hours a day and seven days a week. FASPAC service is structured similar to Telecom Canada's Datapac offerings. The serving areas are classified in the same fashion to three classes for rates application. CNCP provides a volume discount based on the total dollar amount spent during a one to five year period. The rate structure consists of monthly access and feature charges plus the network usage charges with comparable values to Telecom Canada's rates. FASPAC is targeted at lower–volume users (in comparison with leased digital facilities) and support X.25, X.28 and SDLC protocols at speeds ranging from 110bps to 19.2Kbps.

Infodat is CNCPs' dedicated point–to–point service with about 90 serving areas. The service is provided on both asynchronous and synchronous lines at speeds of 300/600/1200 bps, for asynchronous, and 1.2/2.4/4.8/9.6/19.2/56 Kbps on synchronous lines. This service is comparable to Telecom Canada's Dataroute. Similarly, it offers code transparency, lower speed service derivation, and multi–point configuration. The rate structure is also similar and based on fixed monthly rates plus a speed/distance–related tariff. Examples of monthly charges for 19.2 and 56 Kbps links between a few locations are:

Montreal–Toronto	$2584.00(19.2Kbps)	$8425.00(56Kbps)
Toronto–Vancouver	$4951.00	$17683.00.

MACH(III) is CNCPs' DS–0 and DS–1 services. It is a digital point–to–point facility with capacity in multiples of 64Kbps. The service is available in Canada through CNCP and non–CNCP serving areas. Access is through standard DS–1 interface, lower asynchronous speeds 300/600/1200 bps and, 1.2 to 56Kbps synchronously. The rates structure consists of four components: subscriber site equipment, access, CNCP site equipment and transport. The transport constitute the major part of the total monthly rate (these figures are the same as those used by Telecom Canada as channel rates). Overall, the costs are very similar.

CNCP also offers a satellite–based service called VSAT (based on Telesat's VSAT technology). There is not a specific commercial name for this product. The service provides a full duplex digital transmission of data using 12/14 GHz band. The service is offered at all time subject to availability of facilities. The service is available in two options: bulk rate and volume sensitive. Terminal speeds supported are 1.2 to 19.2Kbps with the maximum channel capacity of 56Kbps. For example, the monthly (bulk rate service) rate for the first two–way 56Kbps channel is $13390.00 (one year contract) and additional channels are provided at reduced rates. For the volume–sensitive option, the total monthly rate is the sum of the monthly charge for each station and a network usage charge. The monthly charge per station is $80.00. The usage charge is based on the number of 128–byte packets and differs for terminals and hosts. For example, the first 25 Kilopackets are charged at $0.90 per kp, for hosts, and $0.75 for terminals. These rates decrease as the number of packets increases.

9.5.7 Telesat services

The pertinent services provided by Telesat Canada are: Anikom 200, Anikom 500, Anikom 1000 and Anikom 600.

Anikom 200 is a VSAT service as described in the previous section. The CNCP service is actually derived from Telesat Canada's Anikom 200. Two options exists: single user service (option 210) and bulk service (option 220). The rate structure for both are based on fixed monthly charges in accordance with each speed (no usage charge as in CNCP volume–based VSAT service). Anikom 200 supports a variety of customer equipment interfaces including RS232 and RS422 with speeds up to 9.6Kbps (asynch.) and 64Kbps (synch.). For the bulk rate service speeds are 128 and 512Kbps synchronously. Additional user protocols supported include X.25 and SDLC. The bulk service can be contracted on a 1, 3 and 5 year basis. The 210 option can be contracted also on a monthly basis. The monthly rates for the month to month contract for the 2.4, 9.6 and 56Kbps (210 option) lines are $875.00, $1500.00 and $7500.00 respectively. The monthly rate for the 128 and 512Kbps from 220 option are $23310.00 and $86580.00 respectively, for the one year contract. For the 220 service, there is also an additional charge ($140.00 to $600.00) per data port per month.

Anikom 500 and 1000 are complementary services and collectively provide full duplex leased service in point–to–point and multipoint star configuration at speeds of 56 to 512Kbps (Anikom 500), 768and 1544Kbps (Anikom 1000). The cost components are monthly service charge and earth station charge. For example, a total monthly charge of $7700.95 for a 64Kbps link, $23175.00 for a 512Kbps link or $30600.00 for a 1.544Mbps T1 link.

Anikom 600 is a transportable earth station operating in the C–band and can support voice and data. The maximum data rate that can be transported is 112Kbps (synchronous only)using high speed data modems. This is a limited service (only 12 in deployment) and would have a monthly charge of about $10,000. It can be contracted, by prior reservation, for a minimum of one month.

9.6 CONCLUSION AND RECOMMENDATION

The issue examined by this section concerns how an individual user can gain access to the network. An individual user may have an existing permanent link to a node of the network either directly or via an intermediate processor in a LAN environment. There are also situations where planned and permanent access to a regular user may not be available due to circumstances controlled by his mission. A user may have to gain access to the network from a temporary location which could be anywhere in the country such as the users' home, a few miles away, or a research post in the remote areas of the arctic. The duration of access may also vary from a few hours or days to a few months or possibly a year. Duration beyond a year may justify the use of more permanent arrangements. Normally, long duration means more individuals and therefore, more traffic that would require higher capacity and longer term facilities.

The preceding sections, described a number of existing commercial facilities that can be utilized. These facilities can be classified into a three of groups:

1. Circuit Switched Access (CSA)– e.g. hybrid PSTN (dial up) and digital Datalink. Normally involves buying or leasing terminating equipments and paying a usage charge based on time, distance and, in the case of Datalink, speed.

2. Packet Switched Access (PSA)– e.g. Datapac and Faspac. These support a variety of user devices and protocols. Costs are based a fixed monthly charge and a usage charge.

3. Dedicated Link Access (DLA)– e.g. Dataroute, Infodat, Megaplan, MACH–(III), CNCP VSAT and, Anikom 200/500/600/1000. These are generally the most costly with complicated cost structures based on fixed monthly rates set by speed and distance (not in the case of satellite–based products) regardless of usage.

CSA facilities, specially dial up access using analog modems, are most appropriate for the purposes of this section. PSTN is widely available and costs are easily understood . Datalink provides a much more reliable and faster facility for bulk transfer over longer distances. Its cost is still mostly usage based and therefore suitable for high speed occasional use. For example, the usage portion of the cost for a 300–mile and 3000–mile 9.6 Kbps links are about

$20.00 and $40.00 per hour. The monthly rate for a 9.6Kbps link is $350.00. This would be an appropriate solution where local processing power is available to a user and the access usage is limited to bulk information exchange.

PSA facilities are equal alternatives to the CSA ones in many cases. The speed goes to a maximum of 19.2Kbps with a variety of supported protocols. PSA facilities are also mostly usage oriented and therefore can be used for low to medium speed access from most populated parts of the country. As an example, the fixed monthly charge for an asynchronous device would be as low as $100.00 (not a major overhead for temporary applications).

DLAs are the most costly options. These are typically log term facilities. Nevertheless, there are situations that they can be applied to meet the needs of this study. One example would be VSAT and mobile satellite earth stations. A VSAT link can support a number of user devices and protocols and offer relatively high speeds and costs. In an isolated area VSAT can be used to provide a short to medium term solution. The monthly cost would be in the order of $1500.00 for a 9.6Kbps link. Alternatively, CNCPs' VSAT product can be used with a low monthly rate of $80.00 plus a usage charge of about $0.50 to $0.90 per 128000 characters. Similarly, transportable earth stations can be used for providing access to isolated users where VSAT range is not adequate. The cost is relatively highe ($10,000.00 per month) but with cost benefit consideration it might be a viable solution for a given application. However, some of the limitations of satellite technology should be noted (as described in [14])prior to any decision to utilize these facilities.

Finally, it is also appropriate to note the potential suitability of ISDN as a low cost access method. As discussed in [14], ISDN has the potential of being available on every residential and commercial premises at some time in the future. An ISDN link can support a number of voice and data devices simultaneously on an on–demand basis. However, until a universally supported service is made available, such facility will have very limited application.

To summarize, there are facilities available to meet a wide spectrum of cost/performance requirements. The following table illustrate the various possibilities available today.

Facility	Cost/Performance	Application
Dial up (PSTN)	Low/Low	For local short distance interactive applications when using low speed modems (up to 4.8Kbps)
Dial up (PSTN)	Low/Med	For short to medium distance bulk transfers when using high speed modems (above 4.8Kbps)
Datalink	Med/Med	For reliable digital occasional bulk transfers over long distances at medium speeds (up to 9.6Kbps)

6ª

Dataroute/Infodat	Med/Med	For reliable high speed (up to 56Kbps) continuous use over long or short distances
Datapac/Faspac	Med/Med	For medium to long distance at low to medium speeds for both interactive and bulk occasional use
Megaplan/MACH(III)	High/High	For high performance, short to long distances, high capacity and continuous use

9.7 REFERENCES

[1] CRTC 6716, Part 4, Sec. 12, Item 4680, Dataroute Tariff.

[2] CRTC 6716, Part 4, Sec. 12, Item 4685, Datalink Tariff.

[3] CRTC 6716, Part 4, Sec. 12, Item 4700, Datapac Tariff.

[4] CRTC 6716, Part 5, Sec. 1, Item 5020, Megaroute Tariff.

[5] CRTC 6716, Part 5, Sec. 1, Item 5030, Megastream Tariff.

[6] CRTC 6716, Part 5, Sec. 1, Item 5040, Megaplex Tariff.

[7] CRTC 4001, Part 14, MACH(III) Tariff.

[8] CRTC 4001, Part 7, Sec. A to J, Infoswitch Tariff.

[9] CRTC 4001, Part 2, Sec. J, Infodat Tariff.

[10] CRTC 4001, Part 16, Sec. A, CNCP VSAT Tariff.

[11] CRTC 8018, Anikom 200 Tariff.

[12] CRTC 8017, Anikom 500 Tariff.

[13] CRTC 8015, Anikom 1000 Tariff.

[14] CGI Report SE–R90.05, "High Speed Transmission Methods, Technology and Networking".

9.8 ACRONYMS

ANSI	American National Standards Institute
BPS	Bits Per Second
BSC	Binary Synchronous Code
CCITT	Consultative Committee on International Telephone and Telecommunication
CN	Call Negotiation
CR	Call Routing
CSA	Circuit Switched Access
CUG	Closed User Group
DAS	Datapac Access Software
DLA	Dedicated Link Access
DTE	Data Terminating equipment
HG	Hunt Group
IA	Isolated Access
KBPS	kilo Bits Per Second
KP	Kilo Packet

LAN	Local Area Network
MA	Metropolitan Access
NUI	Network User Identifier
PAD	Packet Assembler/Disassembler
PCM	Pulse Code Modulation
PSA	Packet Switched Access
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
R&D	Research and Development
RA	Remote Access
RC	Reverse Charge
SDLC	Synchronous Data Link Control
SVC	Switched Virtual Circuit
TCM	Time Compression Multiplexing
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network

10. HIGH SPEED TRANSMISSION METHODS, TECHNOLOGY AND NETWORKING

10.1 SUMMARY

This section addresses the technological aspects of transmission facilities and the methodologies employed in their implementation. In the course of doing so, issues pertinent to the applications of such facilities to Wide Area Networks (WAN) will be highlighted. The emphasis will be on the techniques and technologies involved and their associated merits, limitations and impacts within the context of WAN applications. The subject of commercial data transmission services is not the main focus of this work. The technical discussions are concentrated around the physical and medium access sublayer which characterize a transmission facility.

Specifically, this section addresses three areas in sections 5.1, 5.2 and 5.3. Section 5.1 looks at the current transmission technologies. These existing technologies are classified as terrestrial, using land lines and techniques, and celestial, using space as the medium. The current state of the art in cable and radio systems such as optical cables, satellite and the T–carrier services are discussed in this section. Following that, some emerging transmission technologies and methodologies are described in section 5.2. These emerging technologies are looked at in view of their importance to the future of high speed networking and the possibilities of upgrade requirements at some stage in the future. Topics examined in section 5.2 includes narrowband and broadband ISDN, Fast Packet Switching, Synchronous Optical NETwork (SONET) and Fiber Distributed Data Interface (FDDI). Finally, the section examines the issues associated with the design of high speed WANs utilizing facilities offered by T–carriers and its associated terminating equipments. Networking options using T–carrier technology is described and exemplified with supplementary information on the choice of digital multiplexers and resource managers. The section also looks at the migration issues going from a T1 environment to the higher speed T3 one. This is then followed by a discussion on the role and choice of gateways and routers in a typical high speed wide area network consisting of a number of individual subnetworks.

10.2 INTRODUCTION

Information transmission technologies can be classified in different ways. They can be categorized by the technological factors such as media, capacity, range or underlying protocols. In this paper, the classification, at the highest level, will be based on medium of transmission and further subdivided in terms of other factors as appropriate. Two classes of transmission medium can be defined as:

1. Terrestrial Cable Systems; whereby land cables are used for the transmission of data (e.g. copper and optical fibre)
2. Celestial Radio Systems; whereby space is used as the medium for transmission of data (e.g. ground radios and satellites)

Apart from the choice of medium, there are different techniques involved in the encoding of the information and access to these communication links. Each of these types are further subdivided according to the materials used in the media and their functional, application and operating characteristics. There are basically four fundamental parameters characterizing a transmission facility; bandwidth, delay, speed and integrity or quality of service. Bandwidth and speed are interrelated since bandwidth defines the amount of data transmitted in unit of time and speed is the measure of how fast data can be inserted into a transmission facility. Delay is a measure of latency between the time a piece of data is transmitted and the time it is received. Integrity or the quality of service is a measure of how error–free is the facility. These are significant factors in determining the choice of a transmission facility for a given application and the associated protocols which govern the use of such facility.

One other aspect, not directly related to the electrical transmission of information, is the ability to gain access to the information at a low level with minimum amount of processing overhead. Information transfer methods have recently become an integral component of transmission facilities. These techniques define the methodology used in the transfer of data units in a flexible and application independent manner. These techniques are not specifically geared to, say, voice or data applications and are thus suitable for integrated services. As will be seen later, this plays a significant role in the design of a truly high speed network, where, not only the links operate at high speeds, but also, the infrastructure of the transmission facility significantly contributes to the high speed processing of the received information.

There are also a number of issues associated with the emerging technologies in the field of transmission and high speed networking. Various transmission technologies such as Broadband ISDN, SONET and Fast Packet Switching have a direct bearing in the design of the high speed networks of the future. Similarly, the terminating equipments which will be used to handle these new and different technologies, define some of the constraints that one would be faced with in responding to architectural issues the network evolution. Section 5.3 attempts to address some of these issues.

The information provided in this paper is to complement that available in the documentation provided by the service providers and vendors which can be used to determine the transmission facility and associated equipments for a given situation.

To summarize this introductory section, it would be interesting to look at today's transmission options (requirements and capabilities) in the North American market. Table 1 depicts the current and emerging options [Held89]. In the following sections, the features and limitations of these transmission options will be discussed.

Table 1: Transmission Options

Transmission Technology	Transmission Rate
Analogue Modem	
Switched Network	110bps–9.6Kbps
Leased Line	1.2–64Kbps
Dataphone Digital Service(DDS)	
Switched Network	56Kbps
Leased Line	2.4–56Kbps

Local Area Networks	
Appletalk	.25Mbps
Arcnet	2.5Mbps
Ethernet	10Mbps
Token Ring	4/16Mbps
FDDI	100Mbps
IBM 3270 Twisted Wire	2.38Mbps
T1	
North American	1.544Mbps
Europe	2.048Mbps
ISDN	
Narrowband	144/1544Kbps
Broadband	150/800Mbps?

10.3 RELEVANCE TO STUDY

The national high speed network will undoubtedly require a number of different transmission facilities. This is attributed to factors such as, vast geographic area of coverage, need for different access methods, type of application (interactive or bulk data) and differences in the load and capacity requirements. In addition to these requirements, there are issues associated with the choice of a particular transmission facility that would impact higher level functions. Example of such would be the impact of inherent delay in a satellite link on access to a network and, operation of other higher layer protocols which require extensive interaction.

The issue of migration to higher speeds and capacity at a later time necessitates the awareness of emerging technologies in various areas, such as, processors, protocols and transmission facilities of tomorrow. The information in this section provides a mechanism to develop this essential awareness.

10.4 BACKGROUND

The past few decades have witnessed a proliferation of networking concepts and technologies. As computer technology advances so does the need for information transfer and exchange. This has resulted in establishment of many public and private WANs in Canada and mostly in US. Most of these networks have been instigated by the needs for information exchange in commercially non–competitive environments such as Universities and other public research establishments. The need for data transfer within such communities has led to the current investigation looking at the feasibility of a Canadian National High Speed network primarily for the research and development. This study looks at the current and future requirements of such network in terms of, user population, data load and capacity, applications, technologies and transition or migration strategies. In addition, the study focuses on the economical and utilization aspects of this network.

There have been a number of similar initiatives in Canada. One of these is the NRnet. NRnet provides an initial operating speed of 56Kbps with future expansion to 1.5Mbps. This study will be based on the NRnet initiative and will examine the feasibility of a network with greater bandwidth and functionality.

10.5 HIGH SPEED TRANSMISSION TECHNOLOGY AND NETWORKING

Transmission technology encompasses a variety of elements. These are:

1. transmission media;
2. equipment, such as, antennae, receivers, transmitters, repeaters, multiplexers;
3. signal processing methodologies, such as, encoding and signalling techniques;
4. communication protocols;
5. Interfacing devices to other transmission facilities.

The services provided by transmission facilities collectively constitute a "reliable and transparent" transfer of information from one point to another. This includes the internal decision processes that should take place to guide the flow of information through the system (e.g. routing functions etc). However, as we will see, in addition to the reliability and transparency, other factors such as bandwidth, speed and latency must also be examined closely for each application. Furthermore, application of transmission facilities in networking requires a detailed examination of the suitability of such facilities in meeting the objectives of the network design. The following sections examine these issues by looking at the different transmission systems and how they serve various applications.

10.5.1 Current Transmission Technologies

10.5.1.1 Terrestrial Cable Systems

This class of transmission systems use physical cables as the media of transmission. Different types of material may be employed with individual functional and technical characteristics. The three categories are: Twisted Cable Pair, Coaxial and Fibre Optic cables.

Metallic Cable Systems

The most commonly used transmission medium is twisted pairs of copper wires. The diameter of such wires is in the order of 1mm or so. The reason for twisting pairs of wires is to minimize the interference between adjacent wires by reducing the antenna effect associated with parallel pairs of wires. Depending on the size of the wires and the electromagnetic protection and shielding, twisted pairs can provide bandwidths of up to several megabits/second over a few kilometers. The bandwidth and distance characteristics of the twisted pair depends not only on the thickness, EM shielding and electrical balance, but also on the encoding techniques used for the transmission of data.

In the telephony world, cable pairs (two pairs) are used to support many applications ranging from the basic subscriber loop to Digital Signal facilities, DS1 and DS2, operating at 1.544 and 6.312Mbps respectively. A 22–gauge pair of twisted wires can be used to carry a DS–1 signal over distances up to few a hundred Kms (before being multiplexed into the higher level facility DS2) with line and office repeaters located every 1.8Km and 40 Km respectively (40 Km is a powering limitations). Higher capacity facilities such as DS–3 (44.736Mbps) and DS–4

(274.176Mbps) utilize coaxial, fibre optic or radio technologies.

Due to the adequate performance and low cost, twisted cable pairs will be used in many communication applications for many years to come. They are currently used for almost every link between every telephone subscriber and its telephone office. This wide spread use of twisted pairs in the telephony world is of significance to this work since, in conjunction with the telephone facilities, it will provide a primary means of access to data network nodes, either directly or through other means like satellites.

Another commonly used medium is coaxial cable. similar to the twisted pair, coaxial cables can be used for both digital and analogue signals. Because of their construction nature (coaxial vs parallel axial), they offer high bandwidth and very good noise immunity. Again, similar to the cable pair, the bandwidth depends on the construction and length of the cable. Depending on the transmission method, a coaxial link can be either baseband or broadband. In the context of this section, broadband indicates the use of modulated analogue signals for transmission purposes.

Baseband coaxial cables are widely used in Local Area Networks (LAN). They offer a respectable bandwidth for the type of distances involved in a typical LAN. For example, a 1 Km 50 Ohm baseband coaxial cable can provide a 10 Mbits/s bandwidth. Computers can conveniently be connected to an installed backbone of coaxial cable using one of several techniques such as Vampire Taps or T–junctions.

In the telephony world, coaxial cables are used to provide digital communication links of high capacity using baseband technology and regenerative repeaters. For example, thicker coaxial cables can support a DS–4 (T4) circuit with a 274.176Mbps capacity over a distance of 6560 Km with repeater spacing of 1600 to 1800 meters (e.g. LD–4 System of Bell Canada & T4M of US Bell System).

Due to the use of analogue signals, a broadband link can provide bandwidths approaching 500Mbps over distances of up to 100Km. The vast bandwidth of a broadband link is divided into a number of channels. In the CAble TV (CATV) industry (where the broadband coax technology comes from), this division is based on the bandwidth that a single TV channel requires, 6Mhz. This 6Mhz channel can, nevertheless, carry digital data streams of roughly 3Mbps (depending on the terminating equipment, 1 bit of digital data can occupy 1 to 4 Hz of bandwidth) alongside with the analogue television signals.

Contrary to the baseband technology, broadband links require rather sophisticated terminating equipments. These equipments are needed to provide a number of signal processing functions. Additionally, a broadband system requires intermediate equipments to repeat and strengthen the signal. This poses a notable problem when broadband technology is used for duplex computer communication. Existing radio amplifiers used for repeating the signal are only capable of performing this function in one direction. Therefore, a simultaneous duplex communication between two computers would require replacement of the existing amplifiers by the bi–directional ones. Alternatives would be using two coaxial or one Twin Coaxial Cables, one for each direction of the communication, or to utilize two permanent and separate channels within the link for one duplex interaction.

To summarize, baseband communication is relatively simple and inexpensive. It is easy to install and requires uncomplicated interfaces. It can provide a communication facility with a bandwidth in the order of 10Mbps over distances of around 1Km which is adequate for most LAN applications. On the other hand, broadband technology provides much higher bandwidths over longer distances. Multiple channel operation, although in most cases of data transmission is limited to 3Mbps, can facilitate the use of single link for voice, data and video. The price to pay, is the need for critical radio amplifiers and equipments with ongoing maintenance support of high magnitude. The interfacing equipments are more costly than those required for baseband applications (up to an order of magnitude). However, this difference may be significant in certain broadband LAN applications where, in comparison with the total cost, these components constitute a small fraction.

Optical Transmission Systems

Advances in optical technology (fibre and laser) have made it possible to consider fiber optic systems for the future long–haul trunk lines at 1.2 and 2.4 Gbps with repeater spacing of 100 Km. Since 1984, Bell Canada has been installing only fiber optic systems for its trunk lines, and today, the fiber optic transmission system is the preferred choice for delivering T–1 facilities to office buildings in metropolitan areas. Today, many successful installations support the significant optical systems growth estimates we have seen in the past. The Trans–Pacific and Trans–Atlantic undersea fiber optic systems are now operational with a bit rate of 280 Mbps and repeater spacing of 40Km. Also, a repeater–less 140Km link between France and England is installed and operates at 140Mbps. In both examples, the bit rates are expected to be upgraded to 560 Mbps within the next couple of years.

The basic fibre optic transmission system consists of :

1. optical fibre
2. regenerative repeaters
3. optical sources
4. optical detectors
5. optical connectors
6. Wavelength Division Multiplexing (WDM) technique

Fibre optic transmission media offers several advantages over the conventional copper media. These are:

1. electromagnetic immunity
2. transmission security
3. high bandwidth
4. absence of ground loops
5. longer distances with fewer repeaters
6. cost competitiveness with copper or better.

In the past, the major criticism of fibre optic transmission systems have been associated with the complicated nature of their construction, fragility, splicing techniques, and maintenance issues. These are now considered problems of the past and have been overcome by advances in the technology. Another shortcoming of the fibre transmission systems has been related to the slow standardization efforts. This is also changing. The signal transmission formats used in fiber optic systems are primarily the extension of the standard digital transmission T–Carrier hierarchy. However, a new standard, SONET (Synchronous Optical NETwork) has been introduced recently by ANSI to accommodate the need to support high speed digital signals such as those for the digitized NTSC (National Television Standards Committee) TV and Broadband ISDN (see sections 5.2.1 and 5.2.2). Also, a standard matching the need for a high speed LAN, FDDI (Fiber Distributed Data Interface), is becoming popular through the introduction of low cost components (see 5.2.3).

Fiber optic technology has matured to the stage where large scale implementation of fiber–to–the–home might be considered on commercial basis. What remains is the establishment of a coherent national telecommunication policy that might direct the separation of carrier and contents, and clearly define the areas of licensed exclusive operation and free market operation of the various telecommunication services to the users. Once the policy is established, construction of BISDN or fiber–to–the–home could start shortly thereafter. Such a scenario might be realized as early as 1995. Once BISDN is established widely, services supporting bit rates such as T1 and T2 on a centrally switched demand basis can be provided readily.

10.5.1.2 Celestial Radio Systems

Celestial transmission systems rely on the free space as the medium for communication. Radio waves are transmitted through antennae by one station and received by another. Radio transmission systems are used in different forms to support a variety of applications (e.g. cellular system where a mix of radio and land technologies are employed). However, they can be classified into the following two groups:

1. Land Radio Systems – providing point–to–point communication between two stations, situated on the ground, through a series of terrestrial repeaters;
2. Satellite Systems – providing communications between two terrestrial points via a repeater (satellite) situated in the earth's orbit.

The two systems differ in operational characteristics mainly in their propagation and attenuation characteristics and the higher level of complexity and cost associated with the satellite receivers and transmitters. Land radio systems have a typical range of tens of Km between repeaters and are affected by the physical and atmospheric conditions. On the other hand, the only serious environmental factor affecting satellite communication is the atmospheric phenomena (e.g. rain, fog, sun rays etc). The other significant factor affecting the communication between two points utilizing satellite is the inherent delay associated with the signals travelling up to and down from a satellite. Delays of this nature significantly affect some of the underlying principles of protocols used in conjunction with terrestrial cable systems.

Land Radio Systems

Radio communication using microwave transmission in the frequency range of 2 to 40 GHz is used in many applications. For example, LANs situated in different buildings can be joined by gateways communicating via microwave radio links. In many situations it is more cost effective to erect towers for microwave antennae than dig trenches tens of Km long, lay cables, repeaters and close up.

Most radio communication takes place in the 4–6GHz band. This band is also used for satellite communication and is currently overcrowded and highly regulated. Higher frequencies are also assigned and can be used. These higher frequencies are however less useful for long distance communication on land and need more costly and complex earth stations.

Because of the limited range of repeaterless ground radios (up to tens of Km), in many cases repeaters are needed to relay the signals for medium and long haul applications. This poses a notable problem with the routing of packets in a typical Packet Radio Network (PRN). Adjacent repeaters would tend to bounce a packet back and forth without getting it to its destination. Also, packets may end up to live for ever without performing any useful work. There are several routing algorithms in use which resolve some of these design problems. Examples of these are: *hop counting* and *source routing* techniques [Tane88]. Another interesting design issue is associated with collision. When packets collide, in a PRN, the packets from a station with stronger signal are picked up by an FM receiver (capture effect). Under heavy load conditions, stations near the central site might potentially lock out the farther stations . Other issues significant in the design and use of a land radio system are:

1. Radio Frequency– Choice of the frequency directly affects the equipment cost, range and bandwidth. The higher the frequency, the higher the cost and bandwidth.
2. Signal modulation.
3. Number of Hops– determined by the height of towers that can be raised. The higher the tower the longer the range.
4. Choice of Antennae.
5. Repeaters– Provide reception, regeneration, amplification and retransmissions of signals at intermediate points between two stations. The positioning of repeaters are governed by the environmental characteristics of the area, tower heights and the operating frequency.
6. Licensing issues– In a highly crowded frequency band each link must have the approval of the regulatory authorities.

Land radio is suitable for users who need to transfer large volume of data at high speeds between two close fixed points. The fastest growing application of microwave land radio is for the building of private networks. This would be either for joining LANs or building of a Packet Radio Network. However, the licensing issues associated with microwave links should be carefully considered. An alternative, but with more limited range and application, is the use of infrared signals which do not require licensing.

Because of the shorter communication delays, simplicity of equipments and lower costs, ground radio communication has been used to implement a number of Packet Radio Networks. PRNs are attractive in a number of applications. These are:

1. communication with stations situated in areas where telephone system is inadequate or unavailable; e.g. rural areas, remote data acquisitions, such as seismic information, and communication with on site expedition base;
2. communications with mobile stations;
3. applications where stations have a high peak–to–average ratio or low data rate requirements, where, the cost of fixed data lines with unused capacity might prove uneconomical.

Satellites

Satellites provide a significant means of communication due to the following factors:

1. nearly unlimited bandwidth;
2. good coverage and availability of service;
3. distance insensitivity;
4. broadcast capability.

On the negative side, satellite communication has the following limitations:

1. introduces notable delay in start of communication;
2. transmits weak signal because of power limitations;
3. introduces some degree of security risk because of its broadcast nature;
4. signals are susceptible to environmental conditions like rain, fog and sun rays;
5. extreme northern parts of the hemisphere not covered adequately.

Satellites are basically repeaters used for extending the signal range of a radio system. The exception here is that this *repeater* is stationed in the space. The orbital positioning of satellites is significant in all of the factors mentioned above. Point–to–point communication between two ground stations is achieved by one station transmitting its signal to a satellite which in turn retransmit the same signal, in a broadcast fashion, covering a large or selective area. The coverage area of a satellite (footprint) can range anything between 100Km to 1000's of Km in diameter.

Satellite communication has three main components: the space, the signal and the ground equipments. The space component is the aspects of positioning the satellite in the space in a useful position. The signal component deals with the methods of encoding the information so that maximum use is made of the facility. The ground equipments address the construction of earth stations, multiplexing issues and choice of antennae.

The space – satellites are launched and parked in what is known as geosynchronous orbits of the earth. These orbits are located roughly 36000Km above the equator. A satellite stationed in such orbit would appear stationary to an observer on earth. Thus, allowing fixed alignment between the ground stations and the satellite. This large distance between a satellite and an earth station is responsible for the satellite propagation delay, several times larger than any encountered in a terrestrial system. A propagation delay of 3 and 5 micro second per Km is typical for coaxial cable and land radio systems respectively. For a maximum distance between two earth stations of approximately 12000Km allowable by a satellite coverage (roughly 1/3 of the earth surface), the propagation delay is about 50 millisecond, when using ground facilities. In contrast, the up and down time delay for a satellite link is roughly 250 millisecond, five times greater.

The signals – as mentioned before, satellites enjoy a high bandwidth. Today's satellites can have a number of transponders (usually 12 or 24), each of which can transmit simultaneously. The total available bandwidth to a satellite is 500MHz. This allows a 36MHz bandwidth for each of 12 transponders. However, using signal polarization and frequency reuse this bandwidth can be effectively increased. Thus a 24–transponder satellite can offer a bandwidth of 864MHz (coax cable offers 450 MHz). This translates to 132 TV channels, each occupying 6MHz.

Three frequency bands have been assigned for satellite communication; C–band, Ku–band and the lesser used Ka–band. C–band is also used by the ground radio systems; it has a wider coverage, weaker signal, and is less directional. The C–band operates in the 4 and 6GHz bands for the downward and upward signals respectively. The Ku–band and Ka–band use 12/14 GHz and 20/30GHz frequency bands respectively, in a similar fashion to the C–band. The characteristics of the Ku–band is somewhat complementary to those of the C–band. They have smaller footprints, directional tendency and stronger signals. The Ku–band can cover an area equivalent to all the lower provinces of Canada, whereas, the C–band almost doubles the coverage extending to the remote areas of the lower arctic making it ideal for broadcasting. Because of the geosynchronous positioning of the satellites and their area of coverage, upper portions of the arctic would not enjoy the benefits of geosynchronous satellite communication. Ku_band and Ka–band signals also have immunity from interference by ground radio signals since they are strictly for satellite use. Ku–band and Ka–band signals require smaller and less expensive earth stations because of their signal strength. On the other hand, they are highly susceptible to environmental conditions like rain and fog. Ka–band technology is not as widely used as the C and Ku–bands.

Satellites support both analogue and digital signals. All broadcast TV channels and most telephone voice channels use analogue signals. Although, more and more digital voice is used over the satellite links. Nearly all analogue signals are modulated using FM technique. Digital links use Quaternary Phase Shift Keying (QPSK) technique. Phase shift keying has the benefits of making good use of the available bandwidth and resistance to noise. However, these two components vary inversely in relation to one another. That is, more phase change results in better noise resistance and reduced bandwidth.

Multiple access to satellites is made possible by using one of the two multiplexing techniques: Frequency Division Multiple Access (FDMA) or Time Division Multiple Access (TDMA). FDMA is used by stations that operate in analogue mode. The up and down beams frequency of satellites have a usable bandwidth of 500MHz. This usable bandwidth is further divided to support multiple channels. In the case of analogue transmission, a carrier with a frequency in the assigned band is modulated with a , say, voice signal using standard FM techniques. Each transponder's 36 MHz bandwidth can carry a single 50Mbps data stream or 800 64Kbps digital voice channels. With the TDMA, the division is based on time. Each station uses the available bandwidth for a prespecified time slot.

The ground facilities – Earth stations are where the intelligence of satellite communication reside. Satellites are just radio repeaters in the space and their sole function is to maintain a correct orbit, receive and, retransmit earth signals. By contrast, the functions performed by an earth station include: reception, transmission, multiplexing, modulation, error control, framing and, access control. For modulation and multiplexing signals, earth stations use QPSK modems and standard T–carrier multiplexers. Additional equipments required are antennae and some frequency conversion devices. Antennae in satellite communication are significant for a number of reasons. Their size and construction dictate a number of factors including: costs, bandwidth, area of coverage and quality of communication. Parabolic antennae, most commonly used for satellite communication, vary from 30 meters down to 1.8 meters (inversely proportional to signal strength) with a cost ranging from a few millions of dollars to a few hundred. The larger the antennae the better is its reception and satellite aiming. With the advent of higher power satellites, more sensitive on–board receivers and, stronger signals, use of smaller and smaller antennae has become possible in the Ku–band range. In addition to antennae, ground stations also include frequency converters to change the signal frequency from Intermediate Frequency (IF), commonly used for radio communication, to microwave frequencies of the satellite channels.

Protocols and other satellite communications issues

The operational characteristics of satellites have a significant effect on the use of higher layer protocols. The most important of which is the inherent delay in the reception of data. Protocols that rely on numerous handshaking and acknowledgment techniques are least efficient in a satellite environment (typically byte–oriented and polling protocols such as IBM–BSC). The best results are obtained with using bit–oriented protocols like HDLC and SDLC. Windowing techniques used in these types of protocols allow a high amount of data being transferred before the sender receive its acknowledgement. Thus, hiding the effect of the 250 ms delay in natural pauses of interactions. The propagation delay in satellite links has also an effect on the higher layer protocols. Higher layer protocols that require retransmissions of unacknowledged packets must have time–outs sufficiently longer than twice the 250 ms propagation delay time to allow normal operation.

Generally, bit–oriented protocols such as HDLC and SDLC are recommended to use large window sizes, packet sizes and, time–out values. For example, Telesat Canada, recommends an average frame size of greater than 1000 bits with a window size of 7 and 8 for SDLC and HDLC respectively. The acknowledgement times are also to be increased by 600ms to a minimum of 1000ms. HDLC LAPBE (Extended LAPB), which differs from LAPB in its window size being extended from 8 to 128, allows an even larger window sizes to be used. Similar treatment should be applied to higher layer protocols. According to [Mur/88] and [Skem88] the optimum window size for modulo 128 protocols can be calculated using the following formula :

Window Size=[Delay(Sec)*Link_Speed(bps)]/[Frame_Size(bits)].

With asynchronous protocols, the general recommendations are to avoid remote host echoing, character by character transmission and to attempt concentrating asynchronous lines to a higher rate synchronous one.

Satellite links are best utilized under full capacity. Anything less than that would waste valuable power source and the unused spare capacity leads to higher tariffs. Most of today's applications are in the areas of bulk data transfer and T–carrier services. An untapped area of application is interactive communication. Again, the reason for this lack of application is the delay problem in satellite communication and sporadic nature of interactive computing. One way of eliminating this phenomenon is using a *demand assignment* scheme. This scheme would allow the transponders to turn off when not in use.

An example of implementing interactive communication is the system deployed at the University of Hawaii, (ALOHA). This is a ground packet radio system. It uses fixed length short packets. Every station is allowed to transmit at any time. If a collision occurs, the sending station will not receive an acknowledgement and then would retransmit. [Tane88] calculates the efficiency of pure ALOHA to be around 18%, a discouraging figure. A modified scheme known as slotted ALOHA doubles this figure to about 36% by dividing the time scale into a number of equal time slots and having a station signal the beginning of each slot. Under this scheme, no station can transmit until the beginning of the next time slot is signalled. There has been further refinement to the ALOHA protocol to the extend that the operation has become very much like CSMA/CD used on Ethernet.

The adaption of ALOHA within the context of satellites, would require that a station sending data can also listen for its own echo coming back from the satellite after half the up–down. This approach would avoid the need for positive acknowledgements. However, collision detection is still not possible within the framework of satellite communication. Difficulties with collision detection and efficiency figures indicate a necessity to move towards more deterministic protocols in satellite applications.

VSAT and MSAT Networks

Advances in satellite technology such as large scale integration, better power amplifiers, low–cost frequency converters and digital signal processing , has made it possible to provide lower cost and more practical satellite based facilities. One of these is the Very Small Aperture Terminal (VSAT) networks. These networks are based on current Ku–band satellite technology and have all the characteristics described above with the exception of lower cost and better user interfacing facilities. VSAT networks are based on the star network topology. Typically, users supported by a VSAT access a central hub which provides data processing facilities. The communication between a VSAT and a central hub is via a satellite. VSAT–to–VSAT communication is through the central hub and a satellite and thus involves four hops (a serious limitation). The key feature of the VSAT network application is its ability to provide a wide area distributed network at low cost. VSAT antennae are relatively small (1.2 to 1.8 meters) and the associated ground equipments very practical in size and cost. However, smaller antennae means lower bandwidth. Mobile SATellite (MSAT) is the mobile version of VSAT where stations are typically on the move. First MSAT service in Canada is expected to be offered by Telesat Canada in the early 90's (1993?). More information on MSAT and related issues can be found in [Murt88].

Existing VSAT networks support a number of widely used user interfaces and protocols. In Canada, Telesat's VSAT network ANIKOM–200 supports standard asynchronous and synchronous interfaces at 9.6 and 64Kbps respectively. It also supports protocols such as SNA/SDLC, X.25 and 3270BSC. Remote LANs can utilize VSAT technology for gaining access to a network node that is connected to a VSAT serving hub. This could be potentially quite appropriate in the context of a national network in Canada.

Currently offered VSATs provide a bandwidth of up to 512Kbps in Canada. This is sufficient for meeting the requirements associated with today's applications. However, several issues need to be addressed to support future requirements. VSATs should be able to provide voice, data, and video capabilities with acceptable propagation delays and yet more affordable VSATs. As mentioned before, VSATs capabilities are still limited by their use of power starved satellites and intermediate ground hub. A number of these limitations can be overcome by using the concept of multiple beam satellite antennae, on–board processing and switching and advance access techniques. Today, these are topics of research and development and no doubt they will soon become a reality [Nade88], [Chit88], [Stra88].

10.5.1.3 T-Carrier Technology

This section addresses the concept of digital transmission facility commonly referred to as the T–carrier facility. The reason this topic was not included in the previous sections is because the T–carrier is a data transmission facility that utilizes any of the technologies described in earlier sections. A T–carrier service can be provided over a pair of twisted cables, coax, fibre optic, or satellite media. Also, T–carrier facilities are significantly important in the framework of this study and therefore require a more detailed examination.

The T–carrier is basically a point–to–point digital transmission facility. Depending on its classification, it can carry the equivalent of 24, 96, 672 or 4032 digital Voice Frequency (VF) channels in North America. In terms of bandwidths, these numbers translate to 1.544, 6.312, 44.736 and 274.176 MHz of data capacity respectively. The T–carrier terms used for these services are T1, T2, T3 and T4 respectively.

Fractional T1 facilities are available and serve as an alternative for those who don't yet have the load to fill a T1 channel. Various carriers have products with 64Kbits increments or multiples thereof. Because of the complexity of the tariffs, there has been vast amount of arguments as to the cost effectiveness of FT1 facility. Depending on the location, distance, the carrier, and the product it can work either way. It may be more cost effective to underuse a T1 than fully use a 1/2 T1.

Most T–carrier services are currently based on copper and optical fibre media. However, many celestial service providers offer T–carrier products. In terms of the North American digital hierarchy standards, these facilities utilize the corresponding Digital Signals standards DS1, DS–2, DS–3 and DS–4 as shown below:

Digital Signal(DS) Designation	Hierarchy Level	Rate	T–Carrier Designation	Efficiency
DS–A	A	56Kbps		100%
DS–0	0	64Kbps		100%
DS–1	1	1.544Mbps	T1	99%
DS–2	2	6.312Mbps	T2	97%
DS–3	3	44.736Mbps	T3	96%
DS–4	4	274.176Mbps	T4	92%

T–carriers significance to this project stems from a number of factors;

1. They are widely available services in the North American telecommunication market (although not as cost effectively in Canada).
2. They provide the speed, capacity, and a convenient growth path to higher capacities specially with the advents of Fractional T1 (FT1).
3. They provide a relatively high quality of service.
4. They are used as the basis of many other services, e.g. ISDN.
5. They have been used by telephone companies for many years (and since late 70's by US Government) and thus have a proven record.

The key issues associated with the use of T–carrier facilities are: the terminating equipments, the cost, the ability to utilize the entire bandwidth and the underlying transfer technologies. Practically speaking, if one has the load to fill the bandwidth of a T–carrier facility, then it can be quite cost effective. To achieve this seemingly easy but actually not such common occurrence, a host of equipments and techniques are deployed for use with T–carrier facilities. Channel Service Unit (CSU), Channel Bank(CB), Transcoders, Digital Cross–Connect System(DCS, DSX or sometimes referred to as DACS for AT&Ts' Digital Access and Cross–connect System), Digital Multiplexers (DM) and a whole host of signalling, coding , framing and multiplexing techniques are good examples of this flourishing phenomenon. T1 and T3 are the two most widely used and talked about facilities. They are also the ones that provide the transmission speeds of interest to this study. Therefore, we will concentrate on these in the following sections.

Digital Signals Format

T1 uses bipolar coding for the information signal. In bipolar coding scheme, a pair of adjacent pulses with opposite polarities represent a binary 1 and the absence of pulses represent a binary 0. The technical characteristics of the DS–1 signal can be listed as:

1. 1,544,000 clock intervals/second;
2. 24 digital voice channels grouped to form a 192–bit frame;
3. one extra bit added to each frame for synchronization, 193rd bit;
4. 12 193–bit frames form a multiframe, in normal T1 frame format, and 24 frames in the Extended Super Frame (ESF) format used for providing 64Kbps clear channel DS–0 service;
5. CRC–6 error detection scheme (with extended frames) to indicate occurrence of an error;
6. minimum of 12.5% of bits must be 1's on average to maintain synchronization;
7. a better than 1 in 1000,000 error rate 95% of the time with 1.6Km repeater spacing
8. maximum distance of 80Km to switching node due to timing jitter introduced by too many repeaters.

The 193rd synchronization bit accounts for 8Kbits of T1s' bandwidth. With the advances in technology this requirement has been reduced to 2Kbits without any loss of functionality. The remaining 6Kbits are used for error and performance monitoring as well as facility management and reconfiguration.

The Pulse Code Modulation (PCM) bytes from each of the 24 channels are byte–interleaved, starting from Ch1 and ending with Ch24, to form the 192–bit DS–1 frame. This sequence is preserved throughout the transmission and bits are received in the same order. DS–2 and DS–3 are derived from bit–interleaving a number of DS–1 and DS–2 frames respectively (DS–3 can also be formed by multiplexing 28 DS–1 signals). However, the resulting frames do not have the same multiples of bits per frames as the number of tributary signals. The reason for this is the introduction of multitude of framing, signalling and control bits added at each stage of the multiplexing. A direct consequence of this is the degree of complexity introduced in the higher layers of the hierarchy and associated equipments which interpret these signals. For example, a terminating equipment must constantly examine a multiframe to establish the occurrence of a framing pattern delivered by the 193rd bit of each frame in the DS–1 signal. Similar function has to be performed for higher layer signal framing in addition to bit–stuffing/destuffing functions necessary for slower signals before and after they are interleaved and separated respectively. The exact nature of the bit patterns and function is beyond the scope of this section. However, detailed information on the format and operation of Digital Signals is given in the Telecom Canada's "Digital Network Notes" and CCITT recommendations G.700 to G.956 referenced in this document [CCIT88], [Tele83].

The T1 facilities offered in Canada are at their infancy. Telecom Canada's products are called Megaroute and Megastream. Megaroute is a full T1 facility whereas Megastream provides fractional capacity in increments of 64Kbits. CNCP offers MACH(III) as their T1 product and Telesat's T1 product is ANIKOM 1000 which provides full T1 via satellite in the Ku–band covering all lower provinces of Canada.

10.5.2 Emerging Transmission Technologies

The technologies described in the previous sections of this document form the basis of the future facilities and services. To arrive at these future technologies, existing capabilities are complemented, extended or modified to create a new or an integrated facility. In this section, we will examine some of these evolving technologies that could impact our networking design within the next decade.

10.5.2.1 Integrated Services Digital Network

The Integrated Services Digital Network (ISDN) provides a totally digital communication facility that can be used for private networks. ISDN is a network based on the various transmission technologies described in the previous sections. Today, ISDN technology provides prototype communication capabilities for voice, data, and video image transmission. In the future, ISDN can bring much higher capacity and greater bandwidth to every one of today's telephone subscribers through Broadband ISDN. The advantages of fully operational ISDN as a communication facility are notable. ISDN is not just a point–to–point transmission link. It is a Wide Area Network and has all the advantages associated with a carrier operated network, such as, network management, maintenance, supervision and installation. The following sections examine the technologies involved in the narrowband and broadband ISDN and their application potential as the future networks backbone.

Narrowband ISDN (NISDN)

Key elements of NISDN (commonly referred to as just ISDN) are the switching, signalling, terminals and the transmission structures. ISDN provides a digital access point to a subscriber with a transmission interface supporting a total bandwidth equivalent to three or twenty four DS0 circuits. This transmission structure is formulated in terms of channels referred to as B and D. The B channels are purely for user data, whereas, the D channel is primarily used for signalling and control purposes with potential for carrying user data. ISDNs Basic Rate Access(BRA) offers two B and one D channels (2B+D). The Primary Rate Access(PRA) offers 23B+D. Each B channel carries 64Kbps of data and the D channel supports 16Kbps, for BRA, and 64Kbps for PRA. BRA is offered on twisted pairs, whereas, PRA can be found on any of the twisted pair, coax or fibre optic media.

In terms of the OSI reference model, ISDNs B channels perform layer 1 and D channels perform layers 1, 2 and 3 functions. The B channels utilize technologies used for T–carrier facilities whereas, the D channels use a modified X.25 technology (HDLC LAPD with multiple logical links), for Layer 2, and Digital Access Signalling System (DASS) for signalling and control.

The components of ISDN are Terminal Equipments (TE1 & TE2), Terminal Adapters (TA) and Network Terminators (NT1 & NT2). NT1 is a device directly connecting to the 2–wire network interface (U interface) and converts it to an 8–wire ISDN interface (S/T interface).

TE1 is an ISDN terminal device that can be connected to NT1 at the S/T point (e.g. digital phones & ISDN data terminals). Non–ISDN devices connect at the S/T interface point via a TA (the interface between a TE2 and TA is defined by the R reference point). An additional device, NT2, is used to perform higher layers (2 & 3) functions such as, layers 2 & 3 protocol handling, multiplexing, switching and maintenance functions.

The interface reference points U, S, T, and R are defined by CCITT I–Series standards 1988 [CCI/88]. Briefly, The U interface for the BRA (PRA) is a 2–wire (4–wire) interface between an ISDN node and an NT1 carrying 2B+D (23B+D) channels in the North American market. For the BRA, S/T interfaces are 8–wire points carrying 2B+D or 144Kbps in a point–to–point or multi–point configurations. With PRA, S and T points are 4–wire interfaces operating at 2B+D (144Kbps) and 23B+D (1.544Mbps) respectively. The T point for PRA configuration is between NT1 and NT2. Finally, an R interface defines a variety of interfaces ranging from 2–wire to 25–wire RS232 [Tele87].

ISDN can be used in a number of applications with differing degrees of satisfaction. As a transmission facility, it can be used for telephony with enhanced services based on the ability of the network Common Channel Signalling System No. 7 (CCS7) to convey Caller ID (CID). ISDN can be used for LAN implementations and interconnections. However, there are serious doubts as to its suitability for graphics information, specially high resolution graphics, and full motion video. For example, a full black and white EGA screen contains 224Kbits of information. To transfer a single screen at 64Kbps in a B–channel would require about 7 seconds. The same number for a VGA and super extended VGA would be 19 and 43 seconds respectively [Held89]. Therefore, depending on the data transfer application, the B–channel could become a bottleneck when interactive high contents data is to be transferred.

The problems with ISDN escalate by a number of other factors. The most important of all is the fact that ISDN is of limited use unless it becomes universal. Becoming universal requires introduction of new devices, switching equipments and installation facilities for 600 million worldwide subscribers. Not an easy task. The technology employed by ISDN is mature. However, its implementation is limited to a number of island trial efforts. Today, the only respectable, but nowhere near complete, nationwide implementations are in Australia and the UK. The main reason for this is the vast amount of investment in the current telephone systems and enormous obstacles associated with migration to out–of–band signalling system, CCS7. Without CCS7, or more importantly, without universal CCS7, ISDN is of limited value.

As we will see in the next section, some of the technical limitation may be overcome with the advent of broadband ISDN. However, that in itself, aggravates the long wait already endured by at least another few years.

Broadband ISDN (BISDN)

The limitations of the narrowband ISDN has been known since the conception of the I–series standards in 1984. It is clear that NISDN is inadequate for motion picture and tele–services such as TV distribution etc. This has lead to the concept of BISDN and its associated technologies (CCITT draft recommendation I.121). BISDN is envisaged to be provided on fibre optic cable operating at speeds above 100Mbps and employing transmission protocols like Asynchronous Transfer Mode (ATM). Since ATM has been declared by I.121 as the target method for BISDN, we will look at it briefly in a subsequent section.

Based on the typical services that BISDN is expected to support, one can arrive at the bandwidths of 150Mbps and 800Mbps, say, for BBRA and BPRA (Broadband BRA & PRA). The 150Mbps rate is probably more cast in concrete than the higher rate. On the down side, ATM is very immature technology. Many issues still are undefined (e.g. cell size, delay, recovery and jitter) and the suitability of ATM for all services is also questionable. To illustrate, consider the problem of possible delay and asynchronous arrival cells of a channel that contains voice data. It is conceivable that a delay of 5 to 10 ms can occur in processing the cells associated with a speech. The impact of this effect not only introduces delays at the receiving end but can also cause unacceptable delay in local echoing. Another issue is related to the proposed choice of connection–oriented ATM. This makes gateway functions more complex in applications involving connectionless networks[Scaf88], [Ride89], [Hand89], [Minz89].

10.5.2.2 Synchronous Optical NETwork

Synchronous Optical NETwork (SONET) became ANSI standard at the end of 1989. It defines the optical signals used between the equipments carrying digital signals over fibre optic medium. It also defines a synchronous frame structure for the multiplexed digital traffic. SONET is interesting because it is the first optical standard for WAN transmission. SONET provides the "missing link" between the various telco's equipments. Major telephone equipment vendors (Northern Telecom's Fiberworld) have already launched implementation efforts for SONET.

SONET was created as the result of high demands for higher speed links in support of services such as High Definition TV, BISDN and full motion picture. These needs formulated the requirements for a family of optical digital signal interfaces that offered the following characteristics:

1. A base rate of 50Mbps to support DS–3 electrical signals at 44.736Mbps;
2. Simple multiplexing formats for ease of access to the payload;
3. Support for transport of higher rate payloads in multiples of 50Mbps;
4. Enough overhead capacity to fully support facility maintenance.

As the result of the above requirements, SONET offers a basic building block called Synchronous Transport Signal–Level 1 (STS–1). STS–1 has a bit rate of 51.84Mbps synchronized with a network synchronization source. The frame structure is a two dimensional matrix of 9 rows and 90 columns called an envelop. Each cell contains an 8–bit byte of information. Therefore, each envelop contains 810 bytes or 6480 bits (in comparison with 4760 bits for DS–3). The bits in the envelop are transmitted and received from top row to bottom and from left to right in a 125 microseconds period. Cells in the first three columns and nine rows are used for overhead purposes. The remaining bytes are used for the payload including 9–byte path information. This scheme simplifies access to the payload and allows multiplexing of information at a high speed frame level as oppose to TDM which is limited to byte level multiplexing. The advantage of this is significant as far as the data network design is concerned. It makes it possible to quickly examine frames for processing or routing purposes, whereas, with the TDM, a large number of bytes from a large number of channels should be looked at before any processing can take place.

The corresponding optical signal hierarchy for SONET is referred to as Optical Carrier–Level n (OC–n). That is, OC–1 is the corresponding optical signal for STS–1 and so on.

One significant aspect of SONET is the way it handles control information. In contrast with the TDM pattern matching and distributed control bits formats used for the Digital Signals, the SONET frame is divided into specific payload and control parts. The control parts is further subdivided to separate information types so that various communication equipments have an easier time in locating and processing pertinent information. Within the first three columns of each STS–1 frame one finds control bytes for frame alignment, STS–1 identification, error handling, and a pointer system for the location of the payload within the frame. The pointer system is an innovative concept that can be used for multiplexing synchronization and frame alignment functions. Current terminating equipments require a 125 microsecond buffer to handle these functions – causing an undesirable consequence of signal delay and impairment. The pointers allow the payload to be positioned anywhere in the STS–1 frame and thus provide the necessary flexibility for synchronization (see [Ball89] for details).

SONET has a linear multiplexing hierarchy. N STS–1 frames, when multiplexed, result in an STS–N frame of 9 rows and N*90 columns with the same overhead bytes as its tributary frame. STS–N is created by byte interleaving of the N STS–1s frame after they are aligned. All the overhead bytes in the first STS–1 are used together with some of the overhead bytes in the subsequent STS–1. When converted to optical signal, an STS–N produces an OC–N optical signal.

SONET can support all North American signals up to and including DS–3. It was due to become ANSI standard at the end of 1989. Further standardization efforts will define the data communication channel protocol within the next few years. Today, the SONET activities are limited to a number of field trials carried out by some vendors R&D labs (BNR and BellCORE). CCITT and ANSI working groups have been working towards defining a Broadband ISDN service delivered by an STS–3 signal of 150Mbps.

10.5.2.3 Fibre Distributed Data Interface

Fibre Distributed Data Interface (FDDI) is a high performance fibre optic LAN based on Token Ring networking architecture. It operates at a bit rate of 100Mbps over a maximum distance of 200Km with 1000 stations. FDDI(II) is modified FDDI to support synchronous circuit switched PCM data.

FDDI is based on the concept of double counter rotating rings. These characteristics allow the two rings to be joined to form a single ring should a failure at one point of the two rings occur. However, not all stations need to be attached to both rings. Two types of stations are defined. Class A and class B stations. The cheaper class B stations connect to one ring only.

FDDI consists of a Physical (PHY) and a Data Link control (DCL) layers. Station Management (SMT) functions are performed throughout various layers. The PHY maps into OSI layer 1 and MAC sublayer maps into the lower portion of the Layer 2 (ie. Link Layer). The upper portion is defined by the Logical Link Control sublayer. SMT functions are not limited to a specific layer (non–OSI).

FDDI uses a coding scheme called "4 out of 5" as oppose to the popular Manchester code. A 5–bit code can represent 32 entities called "symbols" (0's, 1's and others). 16 of these entities are used for data representation, 8 for control and the rest are unused. The reason for selecting this coding scheme is to minimize the overhead to about 25% as oppose to 50% that would have been required with Manchester encoding.

The operation is based on a start–up and a data transfer phases. At start–up, each station establishes links with its neighbors on both rings. Once this is complete each node activates its by–pass relay to establish a three node configuration. This procedure continues until all links are established and the ring is configured. For normal data transfer phase, the access method is modeled on 802.5 standard. The station wishing to communicate captures a travelling token. Then it transmit a frame and remove it when it returns to that station.

The physical layer of the FDDI(I) is modified by the emerging standards for FDDI(II) to accommodate voice applications. To achieve this, a master station generates a synchronous frame every 125 microseconds. Each frame has a preamble byte, 10 channel header bytes filled with FDDI symbols, 16 bytes of non–circuit–switched data, and 96 bytes (time slots) used for circuit–switched data (note 96=4*24 where 24 is the # of channels in a T1 circuit). Each frame takes up 6.144 Mbits of the FDDI capacity. The total 100Mbits is divided into 16 of these frames. That is, a maximum of 16*96=1536 voice channels . The time slots are requested, acquired and kept on demand. This way the unassigned portion of the bandwidth of the network is basically used on an on–demand–basis.

FDDI is relevant to this work both from the point of view of an optical transmission technology and the fact that as a LAN technology it may be found in some of the environment from which access to the high speed network is required. FDDI can be used for voice, data, graphics and compressed video applications with networks spanning a geographical area somewhere between that covered by traditional LANs and WANs. FDDI is also suitable for use as a backbone linking LANs in a campus environment. Today, there are notable advances in optical technologies in general and FDDI in specific. Chip sets are now available from Advanced Micro Devices and others which implement FDDI protocols. FDDI choice of connector problem and special bypass switches are now resolved. Companies such as Fibronics have FDDI system products incorporating higher OSI layers.

10.5.2.4 Fast Packet Switching Methods

Fast Packet Switching (FPS) is one of the key elements in the framework of this study. FPS methods play a significant role towards a true high speed network. Without FPS, we might have networks of interconnected nodes by the means of high speed, or even super high speed links, degraded by orders of magnitude by enormous bottlenecks imposed by the lack of processing power and protocol efficiency. High speed links used in telephony applications, and available today, were designed for circuit–switched TDM applications of the telephony world. Bandwidth efficiency, automatic routing and processing power limitations of computer systems with multitudes of protocol layers involved in today's applications (e.g. voice, data, video) were not considered. These are the issues that have led to the emerging concepts such as SONET, Synchronous and Asynchronous Transfer Modes (ATM & STM), HDLC(LAP–D), Frame Relaying (FR) and generally FPS techniques. In the sequel, we will briefly look at these emerging techniques.

Generally speaking FPS is an architecture which combines the benefits of traditional packet switching concept, such as, bandwidth efficiency and automatic routing, with the advantages of circuit switches, such as, protocol transparency and low delays. FPS is to be used to carry all types of data, such as, voice, signalling, data and pictures. In traditional TDM, devices pre–allocate bandwidth to channels regardless of the actual need of a channel for data transfer. If a channel has no data to transfer, that portion of the bandwidth is wasted. With FPS, bandwidth is used and assigned based on needs. This method of allocating bandwidth to various sources on demand and at the packet level means that the actual multiplexing function is done by interleaving packets as oppose to bytes or bits. Each packet has a fixed length and contain its own source and destination addresses and therefore can be self–routed through the network independently. Also, each packet contains the data from one channel only. Figure 5.1 illustrate the basic differences between FPS and TDM formats.

A major difference between FPS and traditional packet switched systems is that with FPS the overhead is kept to absolute minimum. Thus, functions like error recovery and packet sequencing are not performed. Some of these functions, such as sequencing, are in fact not required because of the high speed and reliable characteristics of circuit switching. Thus, FPS nodes are only concerned with transporting and routing packets within a fixed time.

In a FPS system, two sets of functions are performed by two components, Packet Assembler/Disassembler (PAD) and Trunking subsystem. PAD interfaces with data generating and sinking devices such as, telephones, terminals, and video devices, and performing the necessary PAD functions before submitting to the Trunking subsystem. The trunking subsystem receives packets from the PAD subsystem and transfers them through the network. On the receiving, PADs monitor the incoming packets for selection of those addressed to them. PADs are protocol insensitive and create exactly the same format packets for all the devices they may terminate.

Some specific FPS techniques have been talked about and are being implemented by various carrier companies to meet the demands of future applications. Asynchronous Transfer Mode (ATM) is an example of these.

ATM is a multiplexing and switching function performed at the bottom two layers of the OSI model. ATM provides a transfer mechanism based on bandwidth demand. Information is put into fixed length packets called *cells*. Each cell is filled as the data for it becomes available and is provided by the terminal equipment. Thus, resulting in an asynchronous departure and arrival of cells. As oppose to the synchronous TDM method that requires a framing synchronization field prior to transmission of information for "n" consecutive channels, ATM has a header for each cell and each cell can contain information from any channel that has its data ready. ATM essentially has all the features of FPS architecture. ATM is currently the most likely candidate for the future BISDN application to be used as the payload for the SONET frame described earlier.

Another FPS protocol is the new HDLC–LAPD protocol used for the ISDN D–channels. The main difference between LAPD and LAP or LAPB is its ability to handle multiplexed data and multiple logical channels. LAPD effectively lowers the level of multiplexing function from layer 3 to layer 2 of the OSI model. LAPD contains a set of basic functions and a set of optional functions. The basic functions are error detection, multiplexing and switching. The optional functions are additional error control and flow control. As we discussed previously, these latter functions are kept out of the domain of FPS and are left to the higher layer local elements to handle. Protocols such as LAPD, when performing basic relaying functions are referred to as Frame Relaying(FR) protocols. The associated switching systems are called frame–relay switches. In these switches, the frame relaying functions are most likely to be implemented in the hardware. This is attributed to the simplification of protocol handling and the elimination of the need for complex state machines in the network nodes.

In conclusion, FPS and FR offer simplicity, high capacity, bandwidth efficiency, automatic and alternate routing capabilities. Since the switching nodes are not the terminal points for layer 2 or 3 protocols, there is no mechanism for controlling the flow, using such primitives as RR/RNR used by X.25. Therefore, at peak traffic periods lost frames and degraded service may be encountered. To eliminate such degradation problems, efficient control strategies are needed. [Chen88] outlines some of the issues associated with frame relaying techniques proposed for the ISDN application.

10.5.3 High Speed Wide Area Networking

With the availability of T–carrier facilities as communication services in the early 80's, initial simple point–to–point applications evolved to multi–point ones and then to full scale wide area networking with specific applications. Each point–to–point application required no switching or routing capabilities. As the network evolution progressed, the need for multiple paths for alternate routing became evident. Further expansion into the world of high speed networking raised the issues associated with cross connection of circuits. A host of equipments and technologies are involved in addressing the needs of high speed networking of today where, voice, data and image information is meant to be handled by the infrastructure. To illustrate the issues associated with high speed networking and the use of T–carrier products, it would be appropriate to give a general description of the equipments used for networking with T–carriers.

Figure 5.2 illustrate the North American Digital Signal (DS) hierarchy in terms of the signals and equipments commonly referred to.

The commonly used equipments used in conjunction with T–carrier lines are Channel Banks (CB), Digital Multiplexers (DM) and Digital Cross–Connect (DSX, DCS or sometimes called Digital Access & Cross–Connect–DACS after AT&T product range). The numbers used after the letters represent the hierarchical levels to which an equipment interfaces . For example, DM–23 is a Digital Multiplexer that multiplexes level 2 signals (7 DS–2 signals) into a level 3 signal (DS–3).

Channel Banks (CB) – Channel Banks are used to multiplex 24 voice frequency channels into one DS–1 circuit. Channel Banks are commonly referred to as D–series after D–series channel banks produced by AT&T (first model was D–1 introduced in 1962 and D–4 in 1977 with latest being D–5 introduced in the early 80's). Channel banks are unconfigurable hardware devices with very limited diagnostics and intelligence. They are the simplest level of multiplexing device available for T–1 applications.

Digital Multiplexers (DM) – These are new generation of multiplexing devices produced for multiplexing signals at different levels of the hierarchy. They are intelligent devices with continually expanding capabilities and features. DMs can multiplex information from different sources, such as, voice, data and video channels. They can operate in point–to–point as simple multiplexers or as a component of a network performing a multitude of functions, such as, switching, routing, diagnostics and, management. DMs perform the multiplexing function by bit or byte–interleaving data coming from various channels and performing the reverse process at the opposite end.

On the carrier side, DMs support T1 (and some T3) for the North American market. On the user side, they support a number of interfaces such as RS232, RS449, X.21 for the data side together with a number of voice related interfaces. DMs supporting voice channels offer a number of multiplexing techniques and voice encoding algorithms to reduce the bandwidth requirements of voice channels to 32, 16 or even 8Kbps as oppose to the traditional 64Kbps.

Digital Cross-Connect (DSX) – DSXs perform the switching function for the digital channels on a programmable basis. A circuit coming in on one path can be switched to a circuit going out on a second path (a path is a T1 facility). DSXs terminate only T1 lines and have no means of terminating DS–0 circuits. That is, DSXs must be used in conjunction with CBs or DMs. However, DSX functionality is incorporated in some of the more recent digital multiplexers as an integral feature.

Channel Service Unit(CSU) – CSUs are carrier network terminating equipments that are used to provide isolation between the carrier network and the network terminating equipments on the user side. CSUs primary function is to ensure that high quality signal is received from and transmitted to the carrier network. A secondary function is to provide some diagnostics capability for line fault isolation. CSUs may not be required for optical or satellite links where the likelihood of network damage is limited. CSU functions are usually incorporated in DMs. CSU functionality is subject to regulatory certification. Most DMs incorporate an integral CSU.

Transcoders – Traditionally, transcoders are used to encode two incoming PCM–based DS–1 voice circuits into one ADPCM–based DS–1 circuit while maintaining the standard format of the DS–1 frame. Other bit reduction techniques, such as Continuously Variable Slope Data Modulation (CVSDM), can also be used within transcoders for higher compression characteristics.

10.5.3.1 Networking With T-Carrier Terminating Equipments

T1 networking can be implemented using a number of different options. The underlying principles of T1 networking options can be categorized into three groups:

1. Modification of the structure of a transit T–carrier path, passing through a location, by termination of some circuits and addition of new ones (Drop & Insert method). This is done by using multiplexers back to back or Drop/Insert multiplexers with two T1 paths at the center as shown in Figure 5.3;

2. Interchanging time slots between a number of T–carrier paths connected to a node; that is, ch1 of path 1 being switched to the time slot for ch3 of path 3. This is achieved by using DACS or DMs incorporating DACS function;

3. Alteration of T–carrier frame structure to incorporate a different information transfer envelop format that is easier to switch and route information.

The techniques in 1 and 2 above have been used for voice applications for some time. Similar application of these techniques to integrated voice, data and video networks however is not as widespread (at least not in the true sense of high speed networking). Options 1 and 2 described above rely on a static routing and cross connection configuration. Dynamic addressing and data transfer is not possible. A number of vendors (e.g. Stratacom) are currently in the process of providing DM products that operate on the basis of 3rd method. The principle of the operation is to utilize the 192 bits of information in a T1 ESF and fill it with an envelop containing data from one circuit and its associated source and destination addresses. This kind of technique would allow dynamic routing of data units as discussed earlier in section 5.2.4.

Networking with T–carrier paths heavily depends on the use of digital multiplexers. They play a strategic role in the communication equipment market because of the fact that they interface the user equipments to the T–carrier facilities. To that end, there has been a vast prolification of DMs and vendors constantly enhancing and expanding the capabilities of their products. It is therefore important to look at these products in more detail.

10.5.3.2 Digital Multiplexers

Today, there are at least 100 generic multiplexing products manufactured by over two dozen key vendors. The DM products range from simple point–to–point multiplexers, used for relatively static configurations, to highly advanced resource managers and node processors incorporating a multitude of switching, maintenance and management functions with costs ranging from a few thousands to a few hundreds of thousands. The leading manufacturers in the intelligent DM market are listed below with their phone numbers and estimated market share (when known):

1. Avanti of Newport RI, (401) 849–4660;
2. Racal Milgo of Fort Lauderdale, FL, (305) 846–1601, 31%;
3. Network Equipment Technologies of Redwood City, CA, (415) 366–4400, 28%;
4. Newbridge Networks of Kanata, Ont., (613) 591–6300, 6%;
5. CASE/Datatel of Cherry Hill NJ, (609) 424–4451;
6. Stratacom of Campbell CA, (408) 370–2333, 5.4%;
7. Timeplex of Woodcliff Lake NJ, (201) 391–1111, 18%;
8. Infotron of Cherry Hill, NJ, (609) 424–9400;
9. Coastcom of Concord CA, (415) 825–7500;
10. AT&T Paradyne of Largo, FL (813) 530–2000, 8%.

Multiplexer vendors have been teaming up to meet the challenges of this rapidly growing market. Newbridge and Wellfleet Communication of Bedford MA have signed an agreement to market LAN–TO–T1 bridging products, a significant component for WAN design. Infotron and LICOM both of Virginia have merged so that Infotron can take a leap into the T3 market comfortably covered by LICOM. Network Equipment Technologies, a self claimed leader in the world, combined forces with yet another significant player Tellabs (a key supplier of telephony equipments) to develop a nonblocking DSX with 64 T3 ports for use in private networks which also support SONET. Finally, Stratacom, a self claimed leader in the FPS and FR technologies, combined forces with Telenet Communications Corp. to develop an ISDN FR interface for their joint products scheduled for release in mid 1990. This product is in anticipation of the first commercial FR network (date unknown but possibly in the early 90s).

Digital Multiplexers, acting as nodal processors are of significant importance to this study. They can be cascaded to create a wide area backbone. Because of the importance of the intelligent DMs to this study, we will concentrate in discussing issues of significance with this class of DMs as oppose to more basic models. The key characteristics of intelligent DMs can be grouped into Transmission, Features and Maintenance/Management functions each with sub–items as discussed below:

Transmission Characteristics

No. of T1 line:
Anything from 2 to 96 offered by larger systems (Stratacom, NET).

No. of tandem unit:
Usually high, a few hundred but also some support only a few, e.g. Paradyne 3210.

Types of framing:
Usually most support D4 and extended superframe with B8ZS for 64Kbits clear channel support.

Clocking modes:
This is important to network synchronization issues and most support the four different modes: master, slave, internal & external. Some support internal & external modes only.

Facility type:
Typically refers to support for interfaces to fibre optic, satellite, DS1/T1, DS3/T3 or microwave. All support DS1, some support others but only a few support DS3/T3.

Input I/F:
This refers to the low speed side of the multiplexer. A number of interfaces are supported. All tend to support RS232, RS449, V24 and V35.

No. of input channels:
Usually in the few hundred range with different mix between voice and data. Some go up to 1000 with usually most allocated to voice circuits.

Input channel speeds:
On the data side, almost all support up to 19.2Kbits (asynch.) and up to the T1 rate of 1.544Mbits (synch.). For voice, all support 64Kbit rate and quite a few support reduced rates down to 8Kbits(e.g. Newbridge).

Voice I/F:
All support D3/D4 Channel Bank formats.

Voice modulations:
All support PCM, most support ADPCM and some support CVSD and LPVS.

Multiplexing method:
All support byte interleaving, some support both byte and bit interleaving and few support FSP or FR (e.g. Stratacom).

Traffic types:
All support voice and data, some also support video and a few support image as well (e.g. Timeplex & Racal Milgo)

Features

Dynamic BW allocation:
Almost all support some sort of dynamic BW allocation. Usually predefined and based on time of day, BW is allocated to various channels. e.g. more voice BW during the day and more data BW for bulk transfers at night. Very few support software controlled on demand BW allocation. Only those that support some type of FSP (e.g. Stratacom and NET).

Automatic Alternate Routing:
This refers to the automatic selection and deployment of predefined alternate paths should a path becomes unusable. Most of the high end resource managers and nodal

DMs support this.

Routing:

Two types of routing methods may be employed, static or algorithmic. Some use simple static table look–up methods (faster but inconvenient to manage), some use algorithmic methods such as nearest neighbor and global techniques (slower but automatic).

Channel prioritization:

This is to assign access priorities to various channels. Most support this feature.

Configurability:

How is the multiplexer configured? Centrally, from all nodes or only directly. All support configuration from a central node and most support configuration of parameters from any node.

Drop/Insert:

All support Drop/Insert function.

DACS:

Quite a few support digital cross–connect feature. A few don't.

Password security:

Supported by all top end multiplexers and resource managers.

T3 support:

Every one has a plan to support, but only a few claim to have upgrade capability to T3.

Maintenance/Management

Event recording:

Almost all resource managers have a terminal display and/or print facility for indicating alarms, security breaches, line outages etc.

Diagnostics tests:

Almost all provide local and remote testing as well as self test.

Automatic bad line bypass:

Most do this through the automatic alternate routing capability.

IBM Netview support:

Some support IBM NetView network management architecture.

Other Issues

Price:

Prices for resource managers range from $30,000 (e.g. NET IDNX40) to over $300,000 (e.g. NET IDNX70) with an average of about $100,000.

First Delivery:

Products have been delivered since 1984. Most products in this range, however, started hitting the market early 1987.

10.5.3.3 T3 Migration Issues

T1 DM vendors have started to provide upgrade paths to T3 in response to the market growth. Two major issues can be noted: transmission and equipments.

DS–3/T3 differs from the DS–1/T1 facility in terms of its transmission medium require–

ments. At 45 Mbps, the transmission media of choice would be fibre optic cable or microwave link from the technology point of view, and own or lease from the economical sense. The traditional solution would be to lease these facilities from the T–carrier service providers. This can be done either by direct termination of T3 facility on the user premises or via a mix of T3 facility to the nearest point of presence and existing T1 lines terminating on the user site. The latter method would probably be the initial arrangement in most cases. The alternative to leasing would be owning such facility. The options here are laying fibre cables or installing microwave links. The decision to own is mostly based on economical factors. However, technical issues associated with each option must be considered. Laying and owning fibre optic cable is not always possible unless one has the right of way to do so. In addition, maintenance of such facility can be a formidable task. On the up side, owning a fibre cable facility has significant economical advantages as well as tremendous capacity. Microwave links, in contrast, do not pose the physical cable installation problems but instead face the regulatory issues. Also microwave links do not provide the near limitless bandwidth capacity of the fibre optic cables and are prone to environmental conditions and line of sight limitations.

Once transmission issues have been decided, the next step is the choice of terminating equipments. The simplest way of acquiring T3 facility is by using a DM13 equipment. DM13 collects 28 T1 lines and multiplexes them into a single T3 path. There is a large number of DM13s currently deployed in public networks and their costs are in the $10,000 range. DM13s, however, lack the necessary level of sophistication required for complex voice, data, video and image high speed wide area networks. Their appropriateness is limited to point–to–point applications. DM13s are the T3 equivalent of channel banks used for T1 paths. Similar to T1 equipments, there are high and mid–level equipments. At the high end, one can talk about T3 DACS or DSX3s. DSX3 provide a wider range of functionality which include switching DS–0 and DS–1 circuits which comprise the DS3/T3 facility. DSX3s, currently, are not widely marketed and therefore carry a significantly high price tag. As mentioned before, this situation will be changing very rapidly as more and more vendors respond to the needs for higher capacity by development of new T3 product ranges. The growth of the T3 market (equipment and services) is estimated to reach $1.3 billion in 1994 from a 1988 level of $40 million [Flem89]. At the mid–range, there are Drop/Insert multiplexers for T3 which perform similar functions to their T1 counterparts. The circuits added and dropped here are DS–1/T1 circuits as oppose to DS–0 circuits in the case of T1 counterparts.

As far as emerging technologies are concerned, one must note the emergence of SONET–based multiplexers within the next three to five years. SONET–based devices will offer functionality (as discussed earlier) well beyond what is offered today by the current DM13 devices. Because of the synchronous nature of the SONET architecture, networks based on SONET will enjoy the benefits of DSX3 and DM13 used in the Drop/Insert mode.

10.5.3.4 Gateway Issues

Most accesses to a nationwide high speed network would be via intermediate LANs. Almost entirely all R&D establishments own one or more LANs internetworked by means of bridges, routers or gateways. By experience, 80% of the generated traffic is found to be amongst the local users of a LAN [Mier89]. The other 20% is destined for remote users of a WAN. To this end, it is appropriate to look at some of the issues associated with linking LANs to a WAN.

There are basically three options available in internetworking. First, *bridges, they* can be used to effectively extend a given LANs range at the physical or link layer to form a MAN or WAN (in the case of physical layer extension, the device is called a *repeater* as oppose to a bridge). The second option is to provide a routing capability between the networks at the network layer. This is done by redirecting the network layer data units to the appropriate network through a network *router* (or just simply router). The third approach would entail a higher level of interoperation between two networks. This might take place at the transport layer or higher and involves a multitude of protocol handling and conversion. This class of devices are referred to as *gateways*.

Depending on the individual local circumstances, any of the above devices might be used. However, in most cases, the most appropriate device for linking a LAN to a T–carrier–based WAN would be a bridge or, most likely, a router. There are a number of vendors currently supplying such devices. CISCO Systems of Menlo Park, CA, Wellfleet Communications of Bedford, MA, Proteon Inc. of Westborough MA are key router vendors. Bridges are offered by Crosscomm Corp. of Marlborough, MA and Halley Systems of CA. Their products come with some variation in characteristics and are priced in the $10,000 to $15,000 range for the routers, and $5,000 to $10,000 range for the bridges.

To address some of the performance issues related to bridging between two different speed networks (LANs at 10Mbits and T1 at 1.5Mbits), vendors are incorporating multiple T1 lines and large amount of buffers in their products. They have introduced schemes that filter data units not only by destination address but also by the type of higher layer protocols used (e.g. send frames containing TCP/IP data units on one link and those containing Novells' SPX/IPX on another).

The way T1–LAN bridges work is by intercepting LAN link layer frames and forwarding them to the remote network on one or more T1 interfaces. All characteristics of the frame are preserved so that when the frame is placed on the remote LAN by the remote bridge, it would look to the recipient as if it was generated locally. Since there are no flow control mechanism at the link layer and bridges operate in a connectionless mode, they may become overloaded if insufficient buffer space is available or even when sufficient space exists the frame may be delayed considerably. When buffers are full, incoming new frames are discarded and thus excessive time–outs may be experienced at the source end. Therefore, bridge vendors tend to incorporate high amount of buffer space to minimize the chances of dropping frames. Nevertheless, delayed frames still remain to be a serious limitation.

Routers on the other hand, have more flexibility as the result of their ability to throttle the traffic and operate in a connection–oriented mode. The routers have to understand and operate multiple protocol stacks and convert between them. The limitation with routers tend to be solvable by addition of more processing power and multiple T1 links. Although this reduces the performance problems, it nevertheless, significantly adds to the cost of such units. A router could cost up to three times higher than a bridge.

CISCO Systems, a leading vendor of internetworking products, offers routing products for use between a number of different types of networks. they operate at the network layer, level 3 of the OSI model, and route messages between which may also be dissimilar at the lower layers. The networks/protocols currently supported are:

- X.25/OSI8473 Internet (Connectionless Network Services)
- DDN–X.25/EGP (External Gateway Protocol)
- ARPANet/IP (RFC791 & Mil–Std–1777)
- NSFNet/Hello(RFC891)
- DECnet
- XNSNet/IPX
- UNIX/RIP (Routing Information Protocol).

CISCO routers are advertised to be capable of handling up to 12000 packets per second over media such as Ethernet, Token Ring and T1. CISCO products are made by configuring an appropriate set of Multibus cards in a chassis to arrive at the required configuration for a given application. Therefore pricing very much depends on the application. Typically, CISCO gateways and routers are priced in the range of $13,000.00 to $17,000.00CDN.

Another vendor of router/gateway products is Proteon. Their products are somewhat less expensive but also have less capabilities and lower performance. Proteon has two different routers. They allows up to 8 communications board to be connected and operated at T1 speeds. They also have an Ethernet interface for LAN connections. The price again, depending on the configuration, varies between $10,000.00 and $14,000.00 CDN.

Most of the routers and gateways support one or more T1 interfaces. However, no vendor is currently offering T3 interface capability.

10.6 CONCLUSION AND RECOMMENDATIONS

This paper has looked at transmission techniques and facilities from the point of view of their technical characteristics and limitations. The aim of this paper has been to walk the reader through this technological evolution and outline some of the achievements and limitations. Although every attempts have been made to highlight the areas of relevance to the overall project, further consultation to the referenced material, listed in the following section, is highly recommended. The concept of transmission technology is based on the technological evolution of materials and our better understanding of their intricate characteristics. One of the earliest transmission facilities was a pair of wire which formed a loop and signalled by stopping and starting a current induced by a battery in the loop. This technology was further advanced to twisted pairs, shielded twisted pairs, coaxial and other concentric cables and then to fibre optics. In addition to these terrestrial means of transmitting electromagnetic signals, the radio technology progressed to satellites. All of these advances posed challenges and additional technological needs in other areas of communication technology such as, encoding, protocols, signalling, error handling, digitizing, modulation and frequency managements techniques. Faster and higher capacity facilities have necessitated the needs for better and more efficient deterministic protocols to overcome problems such as those associated with satellite delays, TDM–based circuit switching and the choice of terminating equipments.

In summary, we have examined:

Terrestrial Systems– Widely used and known technology. Metallic systems offer wide range of capacity and reach. Economical in most applications.

Bandwidths of up to 10 Mbps over few Kms in the baseband mode, and approaching 500 Mbps in the broadband mode with distances of an order of magnitude higher. Fiber optic systems with high bandwidth, security and immunity offer a viable alternative. Current installations of optical–based systems have achieved speeds of up to 2.4Gbps over 100Km without repeaters. Conclusion of standardization efforts are making optical systems the preferred choice for future applications.

Celestial Systems– A variety of applications can be implemented using radio–based systems. Packet Radio Networks have come a long way through the use of more sophisticated protocols and engineering techniques. Very suitable for building of private networks in joining close locations with high speed links and in communicating with stations in isolated areas or in mobile environments. However, regulatory issues are not to be underestimated. Satellites introduce another mode of radio communication with very high bandwidth, wide coverage, distance insensitivity and broadcast capability. With using specific techniques to overcome the key satellite handicap, the long propagation delay, many networks use and can be highly based on satellite technology. Examples of these would be T1 facilities and VSAT/MSAT networks using satellite communication.

T–Carrier Facilities– A technology used in telephone systems since the 60s'. They offer a point–to–point channelized digital facility with capacities ranging from 1.5 to 275Mbps. Widely used for networking application with significant amount of voice and data traffic. High costs in Canada and channelized characteristics constrain its ultimate application to on demand capacity assigned networking architectures.

ISDN– Many argue that ISDN has missed its window of opportunity. This may very well be the case for the narrowband ISDN. However, with this knowledge and significant advances in transmission technologies, broadband ISDN could become a success within the next five to ten years. BISDN will have a 150Mbps bandwidth for its BRA and some figure in the 600–800Mbps range for the PRA, adequate to support a variety of voice, data, and image applications.

SONET– As the first optical standard for WANs, standardized in 1989, it defines optical signals between equipments carrying digital signals using fiber optic medium. It has a base rate of 50Mbps and supports digital signals, in multiples of 50Mbps, up to DS–3 (150Mbps) level. Simple frame–level multiplexing formats allow ease of access to the payload; a significant factor in networks designs relying on on–demand capacity assignment protocols and low level routing.

FDDI– As a high speed optic–based standardized LAN protocol could become the preferred choice. Token Ring architecture, operation at 100–Mbps with a 200Km span and up to 1000–station support, are some of its characteristic features. This may be the underlying architecture for subnetworks of the future forming larger WANs.

FPS– The concept of Fast Packet Switching has been receiving substantial amount of attention because of its ability to move the current transmission technology from its fixed channel TDM format to a packet–based architecture capable of providing on–demand capacity assignment function. FPS is significant in addressing the requirements of today's networking applications such as bandwidth efficiency and automatic routing in a heterogeneous application environment. There is ,however, significant amount of work to take place in the standardization arena.

End Equipment– High speed networking requirements based on the availability of high speed facilities have resulted in a flourishing end equipment business. The high speed facilities used in networking applications require sophisticated terminating equipment to handle capacity, manage channel utilization and perform application adaptation. Digital multiplexers in the form of advanced resource managers provide capabilities such as dynamic bandwidth allocation, automatic alternate routing and channel switching using both TDM and FPS architectures with an average price tag of $100,000.

Migration to T3– Most of the high speed WAN designs have relied on the use of T1, 1.5 Mbps links with an understanding that their facilities would migrate to higher capacity ones like the 45Mbps T3 facilities. Pertinent issues are related to the choice of medium, terminating equipments and emerging technologies, none of which has had a near comparable growth as their corresponding T1 counterpart.

Gateways & Routers– WANs are made of LANs and MANs. What makes a WAN is the ability to interconnect and interoperate subnetworks. This task is mostly left to gateways and network routers. Vendors are now offering gateways interconnecting a variety of networks using different protocols and transmission media and technologies. CISCO as a leading vendor, has products that interconnect the networks of today (e.g. ARPANet, NSFNet, DECnet, XNSnet & UNIXnets) to those of tomorrow based on OSI, high speed T–carrier facilities and technologies.

10.7 REFERENCES

[Ball89] Ballart R., Ching Y., "SONET: Now It's the Standard Optical Network", IEEE Communications, March 1989.

[Bell82] Bellamy, J., "Digital Telephony", J. Wiley & Sons, 1982.

[Boeh89] Boehm R., "SONET: The Next Phase", Telecommunications, Sep. 1989.

[Brac88] Brackett J., "Fast Packet Switching: A Tutorial", Telecommunications, Nov. 1988.

[Byrn89] Byrne W.R. etal, "Broadband ISDN Technology and Architecture", IEEE Network, Jan. 1989.

[CCIT88] CCITT Recommendations G700–G772, "General aspects of Digital Transmission Systems; Terminal Equipment, Blue books, 1988.

[CCI/88] CCITT Recommendations I110–I464, Blue Books, 1988.

[Chen89] Chen K. etal, "Analysis and Design of a Highly Reliable Transport Architecture for ISDN Frame–Relay Network", IEEE Journal on Selected Areas in Communications, Oct. 1989.

[Chit88] Chitre M, McCoskey J.S., "VSAT Networks: Architectures, Protocols, and Management", IEEE Communications Magazine, July, 1988.

[Data89] "Datapro Reports On Telecommunication", McGraw–Hill, 1989.

[Flem89] Flemming S, "The Evolution of T3 Networking", Telecommunications, Dec. 1989.

[Flm/89] Flemming S, "Get Ready for T3 Networking", Data Communications, Sep. 1989.

[Focu89] Focus On ISDN, Bell–Northern Research, Jan. 1989.

[Gech89] Gechter J., O'Reily P., "Conceptual Issues for ATM", IEEE Network, Jan. 1989.

[Hand89] Handel R., "Evolution of ISDN Towards Broadband ISDN", IEEE Network, Jan. 1989.

[Held89] Held G., "Is ISDN an obsolete data network?", Data Communication, November 1989.

[High89] "High Speed Network Protocols", IEEE Communications Magazine, June 1989.

[Mier89] Mier E.E., "Fractional T1: Carriers carve out bandwidth for users", Data Communication Magazine, November 1989.

[Mie/89] Mier E.E., "Adding to your net worth with T1–to–LAN devices", Data Communications, Sep. 1989.

[Mill88] Miller M.J., Ahmad S.V, "Digital Transmission Systems and Network", Computer Science Press, 1988.

[Minz89] Minzer S.E., "Broadband ISDN and Asynchronous Transfer Mode(ATM)", IEEE Communications, Sep. 1989.

[Murt88] Murthy K.M.S., Sward D.J., "Interworking of VSAT and MSAT systems for end–to–end connectivity", Satellite Integrated Communication Network, Elsevier Science Publication, 1988.

[Mur/88] Murthy K.M.S., Sward D.J., "Wide Area Networking by Interconnecting LANs and MANs via Satellites", Satellite Integrated Communication Network, Elsevier Science Publication, 1988.

[Nade88] Naderi F.M., "Advanced Satellite Concepts For Future Generation VSAT Networks", IEEE Communication Magazine, Sep. 1988.

[Ride89] Rider M.J., "Protocols for ATM access Network", IEEE Network, Jan. 1989.

[Shar89] Sharifi M.H., Garber K., "Economic analysis of Computer Communication networks", IEEE Network Magazine, May 1989.

[Scaf88] Scaffer B., "Synchronous and Asynchronous Transfer Modes in the future Broadband ISDN", IEEE Journal on Selected Areas in Communications, July 1988.

[Skem88] Skemer T, Altken G., "Implementing Network Protocols Over satellite– A user Perspective", Protocols, Standards and Communications Inc., Ottawa, 1988.

[STAN88] Standards for Terminal Equipment and Connection Arrangements Systems, Network Protection Devices, Communications Canada, CS–03 Standards, Jan. 1988.

[Stra88] Stratigos J, Mahindru R, "Packet Switched Architectures and User Protocol Interfaces For VSAT Networks", IEEE Communications Magazine, July, 1988.

[Tane88] Tanenbaum A.S., "Computer Networks", Second Edition, Prentice Hall, 1988.

[Tera88] Terada Y., "High Speed, Broadband Communications and OSI", Computer Standards and Interfaces, July 1988.

[Tele83] Telecom Canada, "Digital Network Notes", Technical Planning and Standards, Network Development and Operation, Telecom Canada, 1983.

[Tele87] Telecom Canada, "ISDN", Second Edition 1987, Service Planning (ISDN), Telecom Canada, 160 Elgin St., Ottawa.

[Wrig89] Wright D.J., To M., "A Characterization of Telecommunication Services in The 1990's", IEEE Journal on Selected Areas in Communications, Sep. 1989.

[Zerb88] Zerbiec T., Cochran R, "Is a private T1 network the right business decision?", Data Communications, July 1988.

10.8 ACRONYMS

AM	Amplitude Modulation
ATM	Asynchronous Transfer Mode
BBRA	Broadband Basic Rate Access
BISDN	Broadband ISDN
BPRA	Broadband Primary Rate Access
BRA	Basic Rate Access
CB	Channel Bank
CID	Caller ID
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CSU	Channel Service Unit
CTV	Cable Television
CVSDM	Contineously Variable Slope Delta Modulation
DACS	Digital Access and Cross–connect System
DASS	Digital Access Signalling System
DCS	Digital Cross–connect System
DSX	Digital System Cross–connection
DM	Digital Multiplexing
DS	Digital Signal
EGA	Enhanced Graphic Adapter
EGP	External Gateway Protocol
ESF	Extended Superframe Format
FDDI	Fibre Distributed Data Interface
FM	Frequency Modulation
FPS	Fast Packet Switching
FR	Frame Relaying
FT1	Fractional T1
HDLC	High–level Data Link Control
HDTV	High Definition TV
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LAP	Link Access Protocol
LAPD	Link Access Protocol D
LDDS	Limited Distance Data Set
LPVS	Linear Predictive with Variable Slope ????
MAN	Metropolitan area Network
MSAT	Mobile SATellite
NISDN	Narrowband ISDN
NTSC	National Television Standards Committee
OC	Optical Carrier
PAD	Packet Assembler/Disassembler
PCM	Pulse Code Modulation
PRA	Primary Rate Access
PRN	Packet Radio Network
QPSK	Quaternary Phase Shift Keying
RNR	Receive Not Ready
RR	Receive Ready
SDLC	Synchronous Data Link Control

SNA	Synchronous Network Architecture
SONET	Synchronous Optical NETwork
STM	Synchronous Transfer Mode
STS	Synchronous Transport Signal
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TE	Terminal Equipment
VGA	Video Graphic Adapter
VSAT	Very Small Aparture Terminal
WAN	Wide Area Network

11. NETWORK SECURITY AND ACCESS CONTROL

11.1 SUMMARY

This section discusses information security issues that should be considered in the planning and specification of the high speed national R&D network. The sensitive information assets of the network are summarized and the potential threats to the confidentiality, integrity and availability of this information are identified. These aspects are then examined to determine the expected security related policies and constraints that will govern the technical and administrative measures needed to appropriately protect information in the network. Security measures are then identified and recommendations made in the areas of personnel, administration, physical facilities, communications and computer processing. Finally, the effect of communications standards and the expected costs are discussed.

11.2 INTRODUCTION

The need for network security in recent years has been fuelled by the growing demand for networking host computers and PCs in order to gain access to increasingly large volumes of vital information. Because of the high connectivity levels, over both wide and local areas, and because of the tremendous growth in computer based databases, information networks are becoming extremely complex. The number of points that are vulnerable to compromise are therefore now much higher and the ability to trace or prevent network violations has become much more difficult.

These factors are also evident for the planned R&D network which is the subject of this study. Not only are the networks large and the information accesses widely dispersed, but the types of organizations participating have operational and environmental characteristics that make them quite distinct from each other. Their views with respect to the security issues are also quite varied. It is therefore one of the goals of this section to put information security into proper perspective for all potential participants and to specify an information security posture for the network that is both suitable and sufficient.

Publicity regarding computer hackers and viruses, while they have been sensationally presented at times, have been largely responsible for raising the general level of concern for the security of information in government, institutional and private sector organizations. For example, in the spring of 1987, the CHAOS computer club in Hamburg, West Germany, located a security flaw in one of the operating systems in NASA's worldwide network of some 1000 computers. These network hackers were able to break into about 20 hosts on the network, browse through files and even plant Trojan Horses allowing others to access databases in the network. Although there was apparently no damage inflicted, other well known breakins, such as the Internet Worm (1988) and the IBM Christmas Tree Exec (1987), have produced damaging results. Such security violations have been reported with increasing frequency over the last few years even though victimized organizations have done their best to avoid the negative publicity that results.

The instigators of such network violations range from disgruntled employees, operators and maintenance staff, to network hackers and electronic thieves. These individuals may crash the computers, read or damage sensitive information or insert software viruses into the system. Unauthorized users may be able to gain access to terminal equipment by simply guessing passwords or break through the access controls and sign–on processors. Dial–in ports on the network or host procedures are particularly vulnerable. Operators and maintenance staff may be in a position to remove or copy information on magnetic media, browse through private files or surreptitiously view transmissions. The software within host processors and network switches may not be sufficiently trusted and could be penetrated by the skilled attacker. Finally, in extreme cases, the professional thief with wiretapping equipment or a sensitive electronic listening device could compromise the system.

The steps taken to protect against such threats must be commensurate with the sensitivity and/or value of the information. Resources are limited and the most cost effective strategies for the situation at hand must be found. Security requirements, however, are rarely fully understood. Therefore this study has taken the approach of outlining the available security options and making recommendations on each issue discussed.

In general terms, the security measures that may be adopted are very broad and range from administrative and physical controls to technology based ones. While this section is devoted to reviewing the factors affecting the choice of technical security measures, related non–technical issues are also addressed as required.

11.3 RELEVANCE TO THE STUDY

The organizations participating in this study will have divergent views and concerns when it comes to the precautions required to respect the confidentiality and integrity of the information being exchanged over the network. Their current practices are driven by the focus and aims of the economic sectors they occupy on the one hand, and on the competitive forces within each of these sectors and the organizations themselves on the other. The natural consequence of this, of course, is that some organizations and sectors will have a better awareness and respect for security then others, and have therefore addressed the security issues more comprehensively than some of their colleagues.

It is doubtful that any of the participants have a global view of the issues generated as a result of bringing such a range of organizations together in the pursuit of such an advanced enterprise as is the objective represented by this feasibility study. This particular section is therefore aimed at identifying the security issues that are of unique concern within the context of a high speed national network for research and development.

11.4 BACKGROUND

At the time of writing, it was only possible to get a preliminary assessment of the security requirements of the project. The known key factors that will affect the security posture to be taken, are as follows:

> The network will be used by government, university and private sector labs or research groups for:
>
> - experimentation (e.g. communications research) and
> - carrying messages and interactive traffic to support information exchange among researchers;
>
> Universities are by nature very open to exchanging research information, their concerns being primarily directed at maintaining the integrity of information and systems;
>
> Industry is interested in co–operative research and in certain cases is concerned with the protection of proprietary information that may be passed to collaborating research organizations;
>
> The Government must diligently respect privacy and proprietary information in its possession as it sets an example for others to follow in this area;
>
> All participants must ensure that this proprietary R&D information and their sensitive non–research oriented information (e.g. corporate databases) are effectively protected against potential compromise through the network;
>
> The technical security measures taken must be compatible with the communications technologies used to construct the network.

11.5 DEFINITIONS

To assist the reader in his review of this document, we have provided the following abbreviated security related definitions in the context of this study.

Confidentiality: Secrecy of information transmitted or stored.

Integrity of Information: Correctness of the information mechanisms may be designed to protect the integrity of information against ambient noise, component failures or intentional manipulation of information.

Integrity of Systems: The stable and well behaved operation of communications and computer systems failures due to hardware faults or software bugs and logic errors can cause integrity violations that may in turn cause information integrity violations.

Availability and Denial of Service: In the security context this has to do with system flooding or outages that cause the networking facilities to fail to deliver services.

Authentication: In this study this term is used to describe the process by which user identities are confirmed by the automated systems through mechanisms such as password checking or card verification.

Access Control: Closely related to authentication this is the process of mediating assess to network resources (e.g. computers, files, applications, communications channels) based on the user's identifier and his permissions (access rights).

11.6 DISCUSSION

11.6.1 Information Assets

While the network is not intended to carry national security data, some of the information associated with the network will nevertheless be sufficiently sensitive that automated and/or manual security measures may need to be taken.

To facilitate the discussion, the following categories are seen to be representative of the information assets that will be either processed by the network or potentially exposed because of the network's existence:

1. experimental traffic;
2. public domain information;
3. open R&D information;
4. proprietary R&D information;

5. corporate information.

In this discussion it is worth mentioning that the information being processed over the network may be in the form of software being transmitted and applied in experiments on the network or software that may be distributed over the network to upgrade the systems comprising the network support processes themselves. Further, network users may wish to import software from public bulletin boards for experimentation purposes. Violation of such software could be as injurious as the theft or modification of sensitive information.

With respect to all categories mentioned above, it is evident that maintenance of the integrity of the information handled by the network is a fundamental requirement. The network and user facilities must be such that the information is not modified or deleted unintentionally. Basic integrity protection should be provided in the face of communications errors and system malfunctions. Users must also be correctly and consistently authenticated by the network when information access is attempted. All network and end user facilities should be sufficiently reliable to provide generally accepted levels of system availability.

11.6.2 Experimental Traffic

Our assessment is that participants will not be concerned with protecting the confidentiality of traffic over the network generated by experimentation. Security services are likely to interfere with the experiments themselves. In any case, security services are not currently available at the high speeds at which much of this experimentation would take place.

Public Domain and Open R&D Information

Open domain databases, public bulletin boards and open R&D information will not require protection over the network beyond the basic need for a reliable communications service. As outlined in the next section, however, public domain software may present a threat in itself that should be taken into consideration by network participants.

Proprietary R&D and Corporate Information

Proprietary R&D and Corporate Information is of particular importance to all participating organizations. Institutions may wish to keep their connections to the R&D network as open as possible so that the community of corporate users may be kept as wide as possible. Corporate databases and local area networks may be closely coupled to the R&D network thereby exposing them to compromises through the network. Participating organizations must therefore determine how much exposure their corporate databases will tolerate if their corporate processors were to be connected to the network.

Assess Damaging Compromise

It can be said that it is desirable to maintain the confidentiality of information for all categories throughout the network and within the end processing sites. The question is always: how much effort can be justified to insure that confidentiality will not be violated? The damage caused by the exposure of information will affect the degree to which confidentiality protection is required. Correct authentication of users will result in adequate confidentiality for most R&D information. Proprietary or Government designated "Protected" R&D information categories, however, may require both enhanced confidentiality and integrity protection. By this we imply mechanisms that protect the confidentiality and integrity of communications and computer processing against determined active attacks. Individual or co–operating organizations should assess the cost of damaging compromise to determine if enhanced confidentiality and integrity protection of such proprietary information is required.

User Groups

A common characteristic of much of the information that will be processed by the network is that groups of users from different organizations may wish to exchange information or experiment among themselves. Such organizations may wish to communicate within closed groups and thereby limit access to exchanged information.

11.6.3 Threats

Security requirements for an information system are usually expressed in terms of a policy (or policies) regarding permitted access to sensitive information, and are closely linked to the threats that may compromise that information.

Threat agents, both from within the organization and external to it, may mount passive and active attacks which could compromise the confidentiality, integrity and availability properties of the information and the network itself. External attacks will be primarily focused on the communications facilities and physically exposed equipments. Such attacks would be mounted by hackers and professional electronic thieves for the most part. Internal attacks will concentrate on breaking through the manual and automated procedures governing access to the processing facilities and resources within these facilities. Typically such threats are from unauthorized employees or authorized users or operators who, accidentally or intentionally, access sensitive information they are not authorized to see.

In a network of co–operating organizations, it is not as evident who the internal and external threats agents are. In any case, it appears that students connected to the research computers represent one of the most significant threats to the network. Because the networks most likely will be connected on a worldwide basis through such networks as the ARPANET, it is clear that the scope for threat sources is very broad indeed. Such network hackers could steal or corrupt R&D information regardless of its value to the organization. This threat is significantly amplified in those cases where network participants attach their corporate machine(s) to the network.

Internal threats by disgruntled employees are likely to be focused on the organization's own computing resources. Measures taken to contain the student threat should also yield protection against such violators should they choose to penetrate the hosts of co–operating organizations.

Given that attacks by wiretappers and electronic eavesdroppers, is passive, the integrity threat to most information in the network from such sources is not considered to be significant.

Such "professionals", however, may be sufficiently motivated to attack certain sensitive R&D information that could be critical to a particular organization's economic well being. It should be kept in mind that in addition to viewing R&D information transmitted over the network, wiretapping could yield passwords which could then be used to log onto host computers through the network.

Computer viruses, dramatized in the press, also represent a significant risk to all those connected to the network. While computer viruses are less likely to infect mainframe computers, PCs are exposed through accesses to public bulletin boards, unreliable suppliers and shareware practices. Both R&D and corporate PCs may be at risk.

Given the range of information security assets handled by the network, the primary threats appear to be as follows:

network hackers at participating sites or worldwide;

viruses introduced through connected PCs.

The professional hacker (in contrast to the nuisance hacker) will focus on the more valuable targets such as R&D information. If corporate information is physically available through the network, it too is vulnerable to both hacker and virus attacks. While the virus threat could compromise the confidentiality of information in some special cases, the primary threat is with respect to system and information integrity.

11.6.4 Security Requirements

Policies and Constraints

Given the above information and threat profiles, it is now possible to formulate the security related policies and constraints required. They will be expressed in terms of information access control requirements to maintain the confidentiality, integrity and availability of information processed by the network. Both network and local issues relating to the participants are addressed.

a. The information network itself must be basic reliable information service that provides adequate integrity and availability service to generally accepted commercial levels. This basic service does not need to be designed to tolerate active wiretapping or other electronically mounted attacks.

b. The network itself should also provide a basic facility for organizing users into closed user groups to limit accesses to groups where a degree of confidentiality is demanded. This basic service is not intended to tolerate active penetration attacks.

c. Participants must assess the risks of exposure for all their sensitive information assets communicated over the network. Should the economic or privacy loss potential be considered to be sufficiently damaging, the organization(s) should consider enhancing the protection afforded over the network or prohibiting the transmission of such information over the network.

d. Enhanced security services should be made available to requesting organizations. These services should protect the confidentiality and integrity of transmitted information appropriate for proprietary and "Protected" information..

e. Because the network cannot be expected to control access to information within each participant's processing facilities, local administrations must take on the responsibility of deciding which of their processors, databases and end user equipments will be connected to the network and what security measures are required to control local accesses.

f. Participants should negotiate bilateral security policies with co–operating organizations whenever there is a vested interest in the confidentiality or integrity handling of proprietary or "Protected" information.

Personnel Security

Personnel security, typically the most critical aspect of any information network implementation, is also the area where most can be gained if personnel are properly vetted. Vetting procedures and records must be processed for all individuals who may come into contact with the system. It will also be important to make all individuals in contact with the system be security aware so that they recognize the importance of good security practices and take their roles and responsibilities, whether in a user role or a support capacity, seriously. The key types of individuals who will need to be considered in the implementation from a security perspective are:

system developers;
system administrators;
security administrators;
operational personnel;
maintenance personnel;
end users.

It will be important to ensure that personnel are vetted to the level of the most sensitive information they are permitted to access. Beyond the actual end user data, this includes directories, logs, user profiles and privileged processes. End users, for example, should not be permitted to access such sensitive elements of the network.

In a networking environment, personnel security is complicated by the need to service, operate and use widely distributed sites. Locally available suppliers and maintenance may be inadequately trusted: Typically, adroit separation of duties, reliability checks and careful supervision will be required to overcome such problems.

Each participant in the project will be responsible for vetting its own support staff. However, a standard will need to be developed to address the personnel security requirements for all staff supporting the administration, maintenance and support of the network interfaces and the network facilities themselves.

Procedural and Operational Security

Procedural and operational security has to do with the organization, and roles and responsibilities, for administering and managing network security. Primary areas of concern are:

access to physical, communications and computer facilities;
development/procurement of systems and components;
installation and checkout of equipment and software;
maintenance and operations;
training (user, maintenance, operations).

It is critical that suitable procedures be put in place and practised to maintain the security and integrity of the operational environment. Security procedures must be well documented and promulgated, specify separate security related duties, keep records of access to media, facilities and equipment, institute good configuration management for equipment and software, carry out ongoing surveillance, inspections and audits, and periodically review all security procedures.

Security related procedures that will be particularly important for the R&D network will be with respect to:

security management;
assured distribution of software and hardware;
remote maintenance and operations.

As already mentioned, viruses and worms may be inadvertently introduced into a network if software is not well managed. In recent years this problem has been exacerbated by the proliferation of PCs and LANs connected to networks. Software purchased from suppliers of doubtful reputation, borrowed from friends, or copied from bulletin boards, may contain harmful or malicious code. In such systems it would be prudent to employ controlled procurement and installation practices to minimize this threat.

Physical Security

Physical security in the context of the R&D network relates to:

access to communications facilities, transmission media and material: Facilities may include patch panels, modems, multiplexers, switching equipment, modems and encryption equipment (if used). Materials could include configuration and maintenance documentation.

access to EDP facilities, storage media and materials: Processors, peripherals, terminals, printers, tapes, disk packs and documentation are all critical items to protect.

Most organizations have adopted physical security standards that call for one or more of the following mechanisms:

security guards;
intrusion alarm systems;
locked buildings, rooms and communications closets.

Depending on the sensitivity and aggregation of the information and facilities, several of these physical protection measures may need to be called up.

Communications Security

Communications security relates to technology based mechanisms designed to preserve the confidentiality, integrity and/or authenticity of communications channels that are open to attack.
Encryption devices employ cryptographic techniques to encipher data bits transmitted over a link or network. If all bits are enciphered, a wire tapper will be "prevented" from reading the data. Encrypted checksums and counters can be employed to prevent insertion, deletion, modification and replay (i.e. integrity compromises). Encrypted source/destination identifiers will yield an authentication service.

The "security grade" of any cryptographic mechanism is largely dependent on the strength of the encryption algorithm used, length of the encryption key, and life of the key itself. "High grade" encryption technology is mandated for protecting national security data and is therefore not applicable to the requirements of the R&D network. "Medium grade" cryptos are recommended by the government for information designated "Protected (very sensitive)" and "Protected (sensitive)" and may be required in some applications, especially those that might involve a government department of agency. "Low grade" commercial devices are advised for less sensitive applications requiring protection such as sensitive proprietary information.

Encryption devices are commonly employed in one of two ways. Link level encryption involves inserting crypto units into all links exposed to external threats. Network level encryption involves inserting crypto units at every access point to the network. Link level encryption protects all of the links and hides the statistics of the channels (important in some military applications for example), but leaves the information in the network nodes unprotected. Network level encryption, on the other hand, protects all information on an end–to–end basis, from one organization's host to another's, and utilizes fewer crypto units. They can therefore be selectively introduced to provide enhanced protection among groups of participants without affecting the rest of the network.

Computer Security

Computer Security, also referred to as EDP security, generally deals with access to sensitive information stored within host processing environments. Software and hardware based logic, controls and monitors access to the host's terminal ports, operating system services, applications, files and database elements.

The aim is to put in place a computing base sufficiently trusted to control access among authorized users of the system. The greater the threat, and therefore the risk of damaging compromise, the more trustworthiness is required of the computing system. In many closed environments, a commercial grade processing environment will be considered to be sufficiently secure. In open systems dealing with very sensitive information, more trusted computer systems are required.

Given that participating organizations will be expected to secure their own facilities adequately, this area is not expected to be an issue. Even according to government guidelines, commercial grade computing environments are considered to be sufficient to control access to systems containing protected information.

The major areas of concern should be with respect to the procedures and practices adopted to support each organization's processing facilities and the processing facilities that will comprise the switches and control points in the network. Good password management practices, in particular, should be enforced throughout the network.

Standards and Compatibility

It is expected that the resultant R&D network will be compatible with the OSI standards, including X.25 and X.400, and that there will also be support for the DoD TCP/IP protocols. It is apparent from the discussion in 5.3.5 that when enhanced security if required at all, will not be needed on the high speed network trunks but rather on the low speed/low cost access lines on an end–to–end basis across the network. Therefore security devices providing confidentiality, integrity and authentication services will be needed that operate at low and medium speeds and are compatible with these protocols. Such devices for X.25 and TCP/IP protocols, however, are only beginning to be available. With respect to X.400, it appears that the related standard will incorporate security mechanisms which will therefore become commercially available within the next five years.

11.6.5 Costs

Given that local security is a participating organization's responsibility, that the high speed trunks will not need enhanced security, and that the basic network service is costed elsewhere, the additional costs that could be considered are the following:

a. For each organization that may require enhanced protection, end–to–end security devices or modules can be estimated to cost about $4000 for every 10,000 bits of bandwidth at each access point to the network.

b. Security management may add about 20% overhead to the network management services of the network and about the same overhead at each participating end point.

It is clear that such costs would escalate network costs dramatically if the whole network were to be protected. This suggests a strategy that introduces security mechanisms only where it can be properly justified through a risk analysis.

11.7 CONCLUSIONS AND RECOMMENDATIONS

This section has outlined the range of information assets in the network and the types of threats that could compromise the information. The major threats to consider are network hackers who may attack the confidentiality and integrity of proprietary and "Protected" R&D information and viruses that may be unknowingly introduced into the network. The cost of introducing security measures for the whole network can be expected to be prohibitive, especially when it appears that not all network sites will require protection. The most significant recommendations of this report are therefore as follows:

a. A thorough security awareness program for all users, administrators and operational personnel is highly recommended;

b. Participating organizations should be responsible for assessing the sensitivity of their information assets and for protecting their proprietary R&D information, local corporate databases and other highly sensitive assets from access through the network. Physical separation of these assets from the R&D network is recommended;

c. The basic network service should be reliable to commercial standards and provide a closed user group facility. Should closed user groups not be supported by the network, network participants could design such controls into their host gateways;

d. Should risk assessment or security policies require enhanced network security, end–to–end security services should be made available. These would be in the form of commercial and government grade encryption that will protect the confidentiality and integrity of sensitive proprietary and "Protected" information over the network. Such devices must be compatible with the access protocols of the network (i.e. X.25 and TCP/IP);

e. The security services provided by X.400 once they become available should be adopted as a standard and the mechanisms be made available to participants with enhanced security needs;

f. Participating organizations should be made aware of the virus threat and should be encouraged to adopt safe software procurement, installation and management practices;

g. Proper personnel, physical and administrative security practices should be instituted for the network sites and should be adopted by all network participants;

h. Special attention should be paid to password selection and management practices to improve the level of authentication service achieved;

i. It is recommended that a security service be provided to participating organizations to assist them in evaluating their security requirements, obtaining the appropriate security services and security training, and managing security operations. This service should make users aware of the risks to which they are exposed through the network.

11.8 REFERENCES

[CSCSTD85] DoD Computer Security Center, "Password Management Guideline", CSC–STD–002–85, 12 April 1985.

[SECSTD90] Treasury Board of Canada, "Security Policy" and Standards", draft received January 1990 (Undated).

[DHS88] Deloitte, Haskins and Sells, "Computer Viruses", Proceedings of an Invitational Symposium, Oct. 10–11, 1988.

11.9 LIST OF ACRONYMS

CCITT	–	International Telegraph and Telephone Consultative Committee
OSI	–	Open System Interconnection
TCP/IP	–	Transmission Control Protocol/Internet Protocol
X.25	–	CCITT standard protocol for network access
X.400	–	CCITT standard message handling service

APPENDIX A: GLOSSARY

Address	The prefix of a coded message that identifies either the sender or receiver of the message. Any group of bits that identifies a network node as a separate, identifiable location.
AM	Amplitude Modulation
ANSI	American National Standards Institute
ARPANET	A wide–area network of packet switching nodes, operated by the U.S. Department of Defense for the support of research.
Asynchronous transmission	A method of transmitting computer data one character at a time. The length of time between characters is variable. Each character establishes a synchronization pattern for the receiver by means of start and stop bits.
ATM	Asynchronous Transfer Mode, a switching technique
B channel	Bearer Channel in ISDN
Bandwidth	The range of frequencies of an electromagnetic energy form measured from the lowest to the highest frequencies. The frequency range of a transmission medium such as the 3,000 Hz bandwidth of a voice–grade communications channel.
BBN	Bolt, Beranek and Newman; the originators of packet switching nodes (PSNs).
BBRA	Broadband Basic Rate Access
BISDN	Broadband ISDN
BPRA	Broadband Primary Rate Access
BPS	(bits per second) The measurement of the rate at which digital information signals are transmitted.
BRA	Basic Rate Access
BRI	Basic Rate Interface in ISDN
Bridge	A device that acts as a connector between similar local area networks. Bridges operate at OSI Level 2, the Data Link Layer.
Broadband link	A transmission channel with a wide frequency range that is divided into separate communication channels.
BSC	Binary Synchronous Code
CB	Channel Bank

CCITT	Comite Consultatif International Telegraphique et Telephonique
CCTA	Central Computer and Telecommunications Agency (agency of UK Treasury)
CD–ROM	Compact Disc Read Only Memory. Computer form of audio compact discs.
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
Centrex	A Common Carrier service
CEPT	European Conference of Postal and Telecommunications Administrations
Channel	A path used for the transmission of electrical signals. One of several independent communication links available on a broadband link.
CID	Caller ID
CIGOS	Canadian Interest Group on Open Systems
CN	Call Negotiation
CO	Central Office
COM	One of the top–level domains. Stands for commercial and includes commercial enterprises.
Common carrier	An organization licensed to provide tele–communications facilities to the public.
Contention	A method of control that determines how the separate nodes of a network can access a shared transmission medium.
COS	Corporation for Open Systems; provides testing services for networking products.
COSAC	Canadian Open System Applications Criteria
CPE	Customer Premise Equipment
CR	Call Routing
CRTC	The Canadian Radio–television and Telecommuni–cations Commission. The agency responsible for regulation of the broadcast industries in Canada and the federally incorporated telecommunications common carriers.
CSA	Canadian Standards Association
CSA	Circuit Switched Access

CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CSU	Channel Service Unit
CTS	Conformance Testing Services (Europe)
CTV	Cable Television
CUG	Closed User Group
CVSDM	Contineously Variable Slope Delta Modulation
D channel	Data Channel used for signalling in ISDN
DACS	Digital Access and Cross–connect System
DAS	Datapac Access Software
DASS	Digital Access Signalling System
Datagram	A self–contained package of data that carries enough addressing and routing information so that it can travel from source to destination without reliance on earlier exchanges between the source or destination and the transporting network.
DCS	Digital Cross–connect System
DEC	Digital Equipment Corporation
DECnet	A proprietary network for Digital Equipment Computers.
Digital signal	A discrete or discontinuous information signal that represents a numerical value; it is separated from other signals by an identifiable period of time.
Distributed processing	The movement of information processing functions from a central computing facility to separate locations equipped with independent systems.
DLA	Dedicated Link Access
DM	Digital Multiplexing
DOC	Department of Communications (Canada)
DS	Digital Signal
DSX	Digital System Cross–connection
DTE	Data Terminating equipment

ECMA	European Computer Manufacturers Association
EDU	One of the top–level domains. Stands for educational and includes educational institutions.
EGA	Enhanced Graphic Adapter
EGP	External Gateway Protocol
EIA	Electronic Industries Association (USA)
ESF	Extended Superframe Format, format of a T1 bitstream
Ethernet	A kind of network cable, or a network which conforms to IEEE standard 802.3.
FAX	Common abbreviation for facsimile; a page transmission service using scanners and copiers.
FDDI	Fibre Distributed Data Interface
FM	Frequency Modulation
FPS	Fast Packet Switching
FR	Frame Relaying
Frame	A self–contained package of data at the link layer.
FT1	Fractional T1
FTAM	File Transfer, Access, and Management (ISO)
FTP	File Transfer Protocol; a user–level protocol and program that you can use to transfer files over the network.
FTP	File Transfer Protocol (MIL–STD–1780)
Gateway	A device that acts as a connector between two logically separate networks. It has interfaces to more than one network and can translate the packets of one network to another, possibly dissimilar, network.
Gigabyte	One thousand million bytes.
GOV	One of the top–level domains. Stands for government and includes government organizations.
H channel	Higher speed channel (>64 Kbps) in ISDN
HDLC	High–level Data Link Control

HDTV	High Definition TV
HG	Hunt Group
IA	Isolated Access
IBL	Individual Business Line
IBM	International Business Machines
IDN	Integrated Digital Network in ISDN
IEC	International Electrotechnical Commission
iNET	A Bell Canada service based on Datapac, that provides Intelligent Network functions.
INTAP	Interoperability Technology Association for Information Processing (Japan)
Internet Protocol Suite	Alternate name for TCP/IP Protocol Suite.
IP	Internet Protocol
ISAL	Information System Access Line, a Bell Canada tariff for a data IBL
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization; responsible for publishing the Open System Interconnection Reference Model.
Kb	Kilobyte: 1 Kb = 1024 bytes (accurately), a thousand bytes (colloquially). Also used as an abbreviation for Kilo–baud.
Kbps	Kilobits per second. A measure of transmission speed.
KP	Kilo Packet
LAN	Local Area Network. A term used to describe the dedicated networks used to link computers and peripherals together within a relatively confined area. The area is usually an office, but may be as large as a building or campus.
LAP	Link Access Protocol
LAPD	Link Access Protocol D
LDDS	Limited Distance Data Set
Leased line	A communications channel reserved for the sole use of the leasing customer. Filtering elements are usually added to leased lines to support high data transmission rates. This process is called conditioning.

Line switching (circuit switching)	A method of completing a direct physical communications path between two communicating devices. This contrasts with message switching where no physical circuit is established.
LPVS	Linear Predictive with Variable Slope
MA	Metropolitan Access
MAN	Metropolitan area Network
MAP	(General Motors) Manufacturing Automation Protocol
Mb	Megabyte: 1 Mb = 1,045,576 bytes (accurately, 1024 x 1024), one million bytes (colloquially, and more usually).
Mbps	Million bits per second. Another measure of higher transmission speed. If one were dealing with computer mainframe channel speeds, one would talk of Mbps and mean Megabytes, not megabits.
Message switching	A communications operation in which messages are received by a switching center and re–transmitted to their ultimate destinations.
MIL	One of the top–level domains. Stands for military and includes military organizations.
MILNET	A wide–area network of packet switching nodes, operated by the U.S. Department of Defense for the operational support of military communication.
Modem	A device that impresses digital signals onto a carrier wave for transmission over an analog transmission path. At the receiving end, the modem converts the analog signals back to digital pulses. Modems are used in pairs, one at each end of an analog communications line used for data communication.
MSAT	Mobile SATellite
Multiplexing	The division of a communication line into two or more separate channels either by separating it into independent frequency bands (frequency division multiplexing), or by assigning the same channel to different users at different times (time division multiplexing).
NBS	National Bureau of Standards (now called NIST)
NCP	Network Control Protocol or Program; the original host–to–host protocol for the ARPANET. In 1983, it was replaced by TCP/IP.
NCSCI	National Center for Standards and Certification Information (USA)

NET	One of the top–level domains. Stands for network and includes network service centers, network informations centers, and other organizations that have a hand in network management.
NISDN	Narrowband ISDN
NIST	(United States) National Institute of Standards and Technology
Node	A network location where communication links begin, end, or intersect. A node can be a user device with a direct attachment to its network, or it can be a communication processor that performs network functions for user devices.
NT1	Network Termination 1 in the ISDN reference model
NT2	Network Termination 2 in the ISDN reference model
NTSC	National Television Standards Committee
NUI	Network User Identifier
OC	Optical Carrier
ORG	One of the top–level domains. Encompasses nonprofit organizations.
OSF	Open Systems Foundation. A grouping of major computer industry companies to promote the adoption of microcomputer standards.
OSI	Open Systems Interconnection. A model of communicating processes established for use in the definition of inter–machine protocols.
Packet	A self–contained package of data at the network layer.
PAD	Packet Assembler/Disassembler
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
PLP	Packet Level Protocol (as per X.25)
PRA	Primary Rate Access
PRI	Primary Rate Interface in ISDN
PRN	Packet Radio Network
Protocols	Communication software that establishes bit, character, or message synchronization between communicating devices; enables devices to recognize and correct errors; and determines how devices can access a network.

PSA	Packet Switched Access
PSN	Packet Switched Network.
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
QPSK	Quaternary Phase Shift Keying
R&D	Research and Development
RA	Remote Access
RC	Reverse Charge
RNR	Receive Not Ready
Router	A hardware and software device that connects hosts on different networks. Routers operate at OSI Level 3, the Network Layer.
RR	Receive Ready
SCC	Standards Council of Canada
SCOT	Steering Committee on Telecommunications
SDLC	Synchronous Data Link Control
Server	A provider of network service.
SNA	Synchronous Network Architecture
SNAcP	Subnetwork Access Protocol
SNDCP	Subnetwork Dependent Convergence Protocol
SNICP	Subnetwork Independent Convergence Protocol
SONET	Synchronous Optical Network
STM	Synchronous Transfer Mode
Store and forward	A data communication technique where switching node accepts messages from a communicating device and stores them until they can be passed on to their destinations.
STS	Synchronous Transport Signal. Electrical equivalent to OC in SONET
SVC	Switched Virtual Circuit

T1 Carrier	A designation of a transmission circuit, referring to its capacity. T1 Carrier has a bandwidth of 1.544 Mbps and T3 Carriers operate at 45 Mbps.
T1	A digital transmission system operating at 1.544 Mbps
TA	Terminal Adapter in the ISDN reference model
TCM	Time Compression Multiplexing
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TE	Terminal Equipment
TE1	Terminal Equipment 1, ISDN compatible
TE2	Terminal Equipment 2, not ISDN compatible
Telcos	An abbreviation used to refer, collectively, to the telephone companies.
TOP	(Boeing) Technical Office Protocol
UCL	Underwriters Laboratory of Canada
User–level protocols	Protocols, such as TELNET, SMTP, and FTP, which allow you to perform operations or applications on the network.
UUCP	Unix to Unix Copy
V.24	A Physical layer standard
VGA	Video Graphic Adapter
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
VT	Virtual Tributary in SONET
WAN	Wide area network; a network that spans great distances.
X.21	A Physical layer standard
X.25	A commercial packet network access protocol that specifies three levels of connections. The X.25 physical level, link level, and packet level correspond to the first three layers of the ISO/OSI model. CCITT standard protocol for network access

X.400	CCITT standard message handling service