CA1
EA
92S23
ENG
DOCS

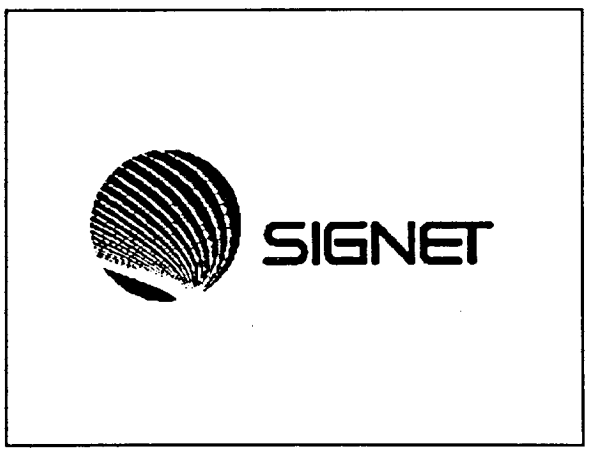
. bz 646730(E) 8

EXTERNAL AFFAIRS & INTERNATIONAL TRADE CANADA

SECURE INTEGRATED GLOBAL NETWORK (SIGNET)

Internetwork Architecture Requirements & Design

Peer Group Review Document



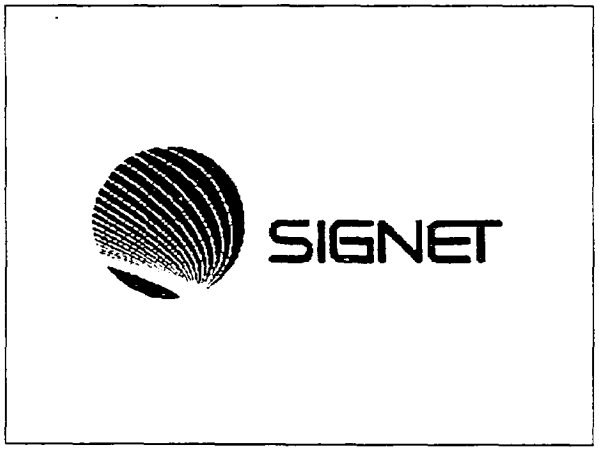
R. Anderson
T. Farrow
R. Watt
October 21, 1992

EXTERNAL AFFAIRS & INTERNATIONAL TRADE CANADA

SECURE INTEGRATED GLOBAL NETWORK (SIGNET)

Internetwork Architecture Requirements & Design

Peer Group Review Document



R. Anderson
T. Farrow
R. Watt
October 21, 1992

43-2710-705
b2646720

TABLE OF CONTENTS

EXECUTIVE SUMMARY

a. The purpose of the SIGNET Internetwork Architecture Peer Review Document is to provide an opportunity for peer EAITC groups to comment on the current view of the SIGNET Internetwork Architecture.

b. The information contained herein is applicable to the local and wide area network communications aspects of SIGNET, also known as the internetwork component of SIGNET (refer to Figure 1.1). The SIGNET Internetwork provides the facilities that enable SIGNET end-systems (PCs, file and application servers, and corporate systems host computers) to communicate locally or around the world. The SIGNET Internetwork also provides communications services to external computing facilities (other government departments, information services, etc.) as required and appropriate. Within EAITC sites, the internetwork communications will be provided via 'Ethernet' Local Area Networks (LANs); between EAITC sites, the internetwork communications will be provided via MITNET. The reader is referred to Appendix 3 for a pictorial overview of the SIGNET architecture.

c. The SIGNET Internetwork is premised upon a suite of international standards selected from Treasury Board of Canada Information Technology Standards (TBITS - ISO Standards), International Telecommunications Standards (CCITT), Institute of Electrical and Electronics Engineers (IEEE), and the Internet Activities Board (IAB). The SIGNET Internetwork is being positioned to enable evolution to a homogeneous TBITS environment in conjunction with the international standards community, the Treasury Board, and positive experience within the international networking community.

d. To enable finalizing the SIGNET Internetwork design, MITNET personnel, the SIGNET Platform team, and EAITC application developers are requested to perform a review of this document and provide corrections to assumptions or estimates, important information which is possibly overlooked, or an indication that the Internetwork Architecture design is judged to be on track.

SIGNET Performance

a. The item with the greatest remaining uncertainty and greatest potential to impact the relative success of SIGNET in the minds of the end users is the performance of applications which require real time interaction across the SIGNET Wide Area Internetwork. Such applications must take into account the utilization of available bandwidth, delay, and availability of the SIGNET wide area internetwork.

b. Preliminary analyses of expected availability of the mission access links, delay (particularly in the Pacific Rim which is serviced out of Ottawa), and limited bandwidth, weight the applications / data architecture in favour of localizing transaction or real time oriented services into the local subnetworks (missions). On the other hand, operations concerns, such as hardware / software costs and data replication, weight the applications / data architecture in favour of regionalizing data bases and implementing transaction oriented services across the wide area subnetwork.

c. Application simulations in the SIM Centre are required to determine SIGNET based applications' sensitivities to the throughput and delay characteristics of SIGNET, particularly real time remote access or remote client / server based applications. The internetwork development program is soon entering the important phase of simulating EAITC applications on a SIM Centre internetwork based upon the target SIGNET internetwork architecture. Close cooperation with MITNET is enabling a realistic wide area network test bed. However, the usefulness of the simulation results is dependent upon realistic assumptions on representative usage cross sections of applications and volumes of data flow; review of the estimates and assumptions contained herein by EAITC applications developers is required.

d. Based upon the outcome of the simulations, recommendations for an optimum architecture for SIGNET based applications will be provided.

SIGNET Internetwork Design Milestones

a. The major milestones in the SIGNET Internetwork development process are:

1) Definition of SIGNET Internetwork requirements for the purpose of identifying network element requirements. The major network elements are routers, multi-port bridges, ethernet concentrators, and terminal servers.

Status: Complete
April 1992

2) Completion of the SIGNET Network Element Request for Proposal.

Status: Complete
June 1992

3) Completion of target model for the overall SIGNET Internetwork.

Status: Complete
August 1992

4) Closing of the vendor proposal period for the SIGNET Network Element Request for Proposal.

   Status: Closed
   September 17, 1992

5) Completion of SIGNET Internetwork management requirements definition.

   Status: In progress.
   Target October 31, 1992

6) Completion of vendor proposal technical evaluations and award of the standing offer for SIGNET network elements.

   Status: Evaluations in progress.
   November 30, 1992

7) Establishment of SIM Centre internetwork based upon target model for the production SIGNET internetwork.

   Status: Preliminary implementation complete. Completion of full implementation pending provision of a complete set of routers.
   Target October 31, 1992

8) Completion of design of off SIGNET communications services.

   Status: Preliminary designs in progress.
   Target November 15, 1992

9) Completion of SIGNET Internetwork management systems procurement and preliminary implementation in SIM Centre.

   Status: Pending completion of 10).
   Target November 30, 1992

10) Completion of SIM Centre simulation of wide area and local area subnetwork performance with respect to proposed applications and data architecture.

   Status: Pending completion of 7) and implementation of EAITC applications in SIM Centre for test purposes.
   Target December 15, 1992

11) Completion of computer and mathematical modeling of SIGNET Internetwork performance and availability based upon the target model.

   Status: Preliminary models completed March 1992; availability model expanded August 1992. Final completion pending vendor availability data required as part of Network Element RFP. Both availability and performance models will be fine tuned as additional data is acquired.
   This milestone is not on critical path.

12) Completion of the designs of the wide area and local area subnetwork components of the SIGNET Internetwork.

Status: Preliminary designs completed August 1992. Acceptance of final design pending outcome of 10).
Target January 15, 1993

13) Completion of initial deployment of SIGNET Internetwork including portions of EAITC Headquarters, at least one internetwork regional node, at least one mission, important off SIGNET communications services, and management systems.

Status: Target March-April 1993

b. The SIGNET Internetwork development program is proceeding well. The activities of the coming three to four months, including evaluation of the network element RFP, applications simulation in the SIM Centre, and implementation of the monitoring and control capability will put EAITC into a solid position to begin deployment of the SIGNET Internetwork in early 1993 with confidence.

1. INTRODUCTION

a. External Affairs and International Trade Canada (EAITC) have undertaken a program to deploy an international distributed computing and communications environment to service their operations in Canada and around the world.

b. This document defines the requirements and design for the internetwork component of SIGNET. The internetwork component comprises the ISO Opens Systems Interconnect (OSI) physical, data link, and network layers. For the purpose of comprehending the role of the internetwork and the allocation of responsibility for the various components of the internetwork, the physical and data link layers may be combined and termed the subnetwork components of SIGNET. Two important types of subnetworks are identified:

   i. Subnetworks which service the local environment. These subnetworks are traditionally known as Local Area Networks or LANs. From the perspective of the intended users or clients of SIGNET, SIGNET will have global connectivity and hence the term Local Area Network is not appropriate. Therefore for the purposes of the design of the SIGNET internetwork architecture, the general term subnetwork is used. The SIGNET internetwork requirements address the LANs in detail.

   ii. Subnetworks which service the wide area. These subnetworks are traditionally known as Wide Area Networks or WANs. EAITC has deployed a sophisticated wide area network known as MITNET. For the purpose of SIGNET, MITNET is viewed as a subnetwork across which the SIGNET internetwork traffic will traverse. MITNET services will be utilized by SIGNET as required. The detailed design of MITNET is outside the scope of SIGNET; from the perspective of MITNET, SIGNET is a client. In regions of the world where MITNET does not offer a service and a requirement for SIGNET presence is identified, the wide area connectivity will be designed as part of the SIGNET internetwork design.

c. From the perspective of the end user, SIGNET is required to provide any-to-any connectivity from desktop to desktop. Therefore, SIGNET is a single network.

d. From the perspective of the SIGNET designers, SIGNET is a cohesive internetwork which utilizes local and wide area subnetworks to provide the required connectivity. Members of the SIGNET design team whose primary purpose is to develop the end user services view SIGNET as a single network resource with a common interface definition. Members of the SIGNET design team whose primary purpose is to deploy the global connectivity view SIGNET as a network layer, which provides a common interface for end user services, operating over two primary types of subnetworks. A great deal of co-operation and synergy amongst the members of the design team is required to ensure the network layer interface will meet the requirements of the end users. Furthermore, it is important to recognize that security and management will transcend all 'layers' of SIGNET. Figure 1.1 illustrates the overall arhcitecture of SIGNET from the perspective of the designers. The shaded areas are the components of SIGNET relevant to the Internetwork design.

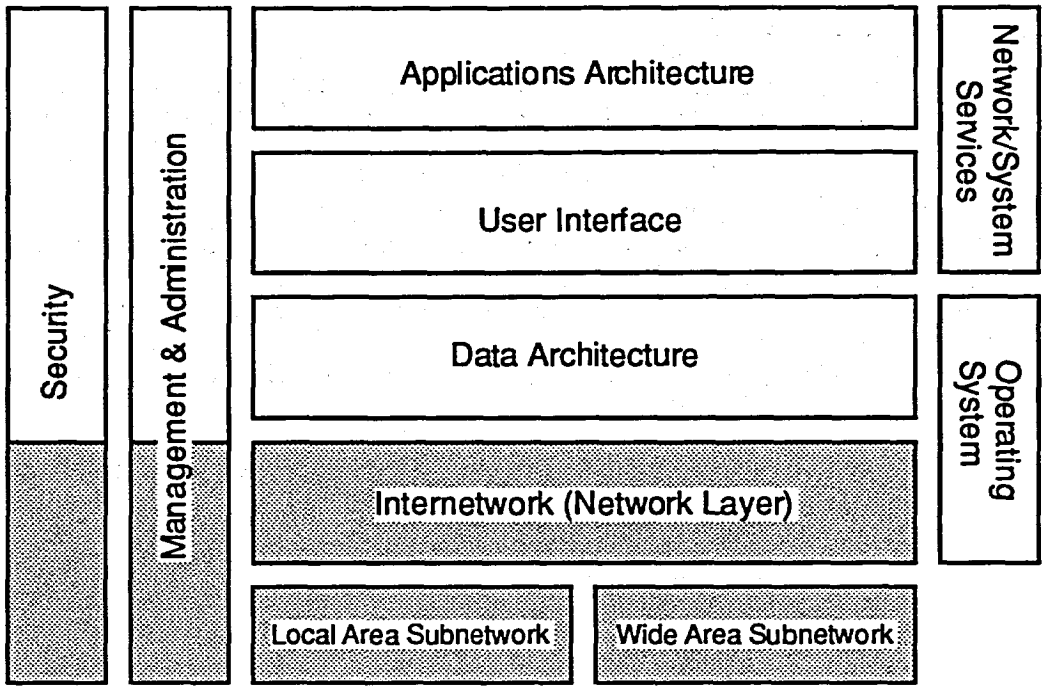


Figure 1.1: SIGNET Architecture

e. The following sections of this document address the SIGNET Internetwork:

Interoperability
Performance
Availability
Scalability
Security
Architecture
  Addressing
  Naming
  Interior Gateway Protocol
  Mission Node Design
  Frame Relay Subnetwork

2. INTERNETWORK INTEROPERABILITY

a. An important requirement for SIGNET is the ability to provide any-to-any connectivity between computing systems supplied by multiple vendors. The statement "interoperability in a multi-vendor environment" is frequently used to describe such a requirement. For the purpose of the SIGNET Internetwork, the required interoperability is applicable to the physical, data link, network, and transport layers. It is of related importance that the mechanism implemented to provide interoperability within the internetwork component of SIGNET enables user interaction / access with applications operating on various computers within SIGNET.

b. The Treasury Board of Canada 'Treasury Board Information Technology Standards' [6] (TBITS) provide the guidance for establishing standards within the SIGNET Internetwork which will enable interoperability. It is an EAITC objective that SIGNET comply with TBITS where practicable today and evolve towards a homogeneous TBITS compliant internetwork as warranted by costs and demonstrated positive implementation experience in other international networks comparable in scope to SIGNET.

c. The initial deployment of SIGNET will utilize a hybrid of proven standards to achieve the required reliable and cost effective interoperability. TBITs standards, augmented with recent ISO and IEEE standards, are selected for the physical, data link, and upper layers (Open Systems Interconnect Reference Model (OSI RM) Layer 1, Layer 2, and Layers 5 through 7). The Internet Activities Board standards are selected for the network and transport layers (OSI RM Layers 3 and 4). For the purpose of the interface into MITNET, the EAITC wide area network, International Telegraph and Telephone Consultative Committee (CCITT) and American National Standards Institute (ANSI) standards are selected.

d. The SIGNET Internetwork will be initially deployed as a hybrid technical environment based upon proven solutions which comply to strategic components of TBITS, ISO, CCITT, ANSI, and IAB standards. The SIGNET Internetwork will evolve towards a pure TBITS environment as warranted by the maturity and cost effectiveness of such an environment offered in the commercial market place.

e. As a vehicle for migration to TBITS network layer standards, the successful router vendor will be required to support TBITS 6.3 "COSAC - Profile for Local Area Networks, LAN" supplemented with associated ISO Intermediate System to Intermediate System routing protocols.

2.1 Internet Activities Board Internet Protocol (IP) Standards

2.1.1 Internet Protocol (IP) Routing Service

1) The routing service must conform to the Internet Activities Board (IAB) Request for Comments 1009, "Requirements for Internet Gateways".

2) External Affairs is required to obtain a network address (Class B) from the Internet Network Information Centre.

2.1.2 Proxy ARP (Address Resolution Protocol)

1) The routing service must support Proxy ARP as defined in IAB RFC 1027, "Using ARP to implement transparent subnet gateways". Enabling/Disabling of Proxy ARP must be under administrative control.

2.1.3 IP Sub-Netting

1) The routing service must support IP sub-netting as defined in IAB RFC 950, "Internet standard subnetting procedure".

2.1.4 Interior Gateway Protocol

1) The routing service must, as a minimum, support the Open Shortest Path First (OSPF) Interior Gateway Protocol (IGP) as defined in IAB RFC 1247, "OSPF Version 2".

2.1.5 Exterior Gateway Protocol

1) The routing service must support the Exterior Gateway Protocol as defined in IAB RFC 904, "Exterior Gateway Protocol Formal Specification".

2) Support for the Exterior Gateway Protocol is required to enable External Affairs to interconnect with other autonomous networks. Interconnection with other autonomous networks requires further security considerations.

2.2 Treasury Board Information Technology Standards

2.2.1 COSAC Profile for Local Area Networks

1) Treasury Board of Canada Information Technology Standard TBITS/NCTTI - 6.3; "COSAC - Profile for Local Area Networks, LAN"

   a) Section 5.1.1 - Connectionless Mode Network Layer - Shall support.
   b) Section 5.1.2 - Connection Mode Network Layer - Shall NOT support.
   c) Section 5.1.3.2.1 - IS-IS Routing - Refer to ISO Standards in Section 3.3 herein.
   d) Section 5.1.4 - Addressing - Shall implement NSAP addresses as defined in Canadian Standard Z243.110.2.
   e) Section 5.3 - MAC Sublayer - The MAC sublayer shall be Carrier Sense Multiple Access with Collision Detection only; Token Access method shall NOT be implemented.
   f) Section 5.4 - The Physical Layer for the CSMA/CD MAC shall also support IEEE Standard 802.3i (Supplement to ISO/IEC 8802-3); "System Considerations for Multisegment 10 Mb/s Baseband Networks (Section 13) Twisted-Pair Medium Attachment Unit

(MAU) and Baseband Medium Type 10BaseT (Section 14)" OR g) following.

g) Section 5.4.1 - Baseband - Shall support AUI interface; 50 ohm co-ax cable and transceivers NOT required OR f) preceding.
h) Section 5.4.2 - Broadband - NOT required.
i) Section 5.4.3 - Token Ring - NOT required.
j) Section 5.4.4 - Token Bus - NOT required.

2.3 International Standards Organization Standards

a. In addition to the TBITS Standards indicated in Section 2.2, the following ISO Standards are required.

2.3.1 ISO CLNP Routing Service

1) The routing service must support International Standards Organization ISO 8473, " Information processing systems - Data communications - Protocol for providing the connectionless-mode network service".

2.3.2 ISO End System to Intermediate System Routing

1) The routing service must support International Standards Organization ISO 9542, "Information processing systems - Telecommunications and information exchange between systems - End system to Intermediate system routeing[1] exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)".

2.3.3 ISO Intermediate System to Intermediate System

1) The routing service must be capable of supporting ISO 10589 "Information processing systems - Telecommunications and information exchange between systems - Intermediate system to intermediate system routeing protocol".

2.3.4 ISO Inter-Domain Routing

1) Upon adoption of ISO 10747 as an international standard, the routing service must be capable of supporting ISO 10747, "Information Technology - Telecommunications and information exchange between systems - Protocol for exchange of inter-domain routeing information among intermediate systems to support forwarding of ISO 8473 PDUs".

[1] Proper spelling of 'routeing' in formal ISO titles. The convention used herein: the spelling routeing is used for formal ISO titles; the spelling routing is used for non ISO titles and reference to the function of routing.

2.4 Subnetwork Interoperability Requirements

2.4.1 Local Area Subnetworks

1) The External Affairs Local Area Subnetworks are required to conform to the IEEE Standard 802.3i-1990 specification and the related portions of the ISO/IEC 8802-3 : 1990 specification.

2) The Local Area Subnetwork interface is required to also support a fiber optic interface which conforms to Section 9.9 of ISO/IEC 8802-3 (Fiber Optic Inter Repeater Link)

3) The Data Link Layer Interface into the Local Area Subnetworks is required to conform to ISO/IEC 8802-2 using LLC Type 1, with, as a minimum IEEE 802 Subnetwork Access Protocol for managing Ethernet 'Type' protocol stack pointers.

4) The Data Link Layer Interface into the Network Layer is required to conform to the Internet Activities Board Request For Comments (RFC) 1042, "A Standard for the Transmission of IP Datagrams over IEEE 802 [ISO 8802-2] Networks".

2.4.2 Wide Area Subnetworks

MITNET Interface

1) The wide area network interface must be capable of supporting EIA/TIA RS-232 electrical / ISO-2110 mechanical and CCITT X.27/V.11 electrical / ISO-4903 mechanical interfaces. The wide area network interface should also support EIA/TIA RS-423 and CCITT V.35 interfaces.

2) The wide area network interface must support rates ranging from 9.6 Kbits/sec to 1.536 Mbit/s.

3) The wide area network interface must support an interface American National Standards Institute (ANSI) T1S1 Frame Relay compliant networks.

Other WAN Interfaces

1) For the purpose of supporting existing CIDA communications capabilities a 3270 Gateway service must be available between SIGNET and the CIDA host located in Hull. Currently the service is supported via international X.25 networks on a per mission basis. It is an objective of the SIGNET internetwork design to consolidate the gateway function into EAITC headquarters in Ottawa, accessible from the missions via native SIGNET protocols, thus eliminating the dependency on international X.25 networks. To minimize the impact on the CIDA host, priority will be on implementing an X.25 gateway in EAITC HQ accessible via the SIGNET Internetwork.

2) Supply and Services Canada On-Line Pay is accessed via 3270 sessions from EAITC headquarters in Ottawa. It is an objective to provide access to On-Line Pay to SIGNET workstations; priority will be on implementing a 3270 gateway in EAITC HQ accessible via the SIGNET Internetwork.

2.5 Support for Existing EAITC Networks / Systems / Applications

1) SIGNET is required to interface into existing FINEX, Mission FINEX, and CAIPS (Computer Assisted Immigration Processing System) environments. These systems are VAX based and utilize dedicated bandwidth in the wide area (as applicable). It is an objective to consolidate the wide area network bandwidth into SIGNET and provide support for Mission FINEX and CAIPS via native SIGNET protocols.

2) SIGNET is required to interface into the existing COSICs environment providing security requirements are met.

2.6 Support for General Connectivity Off SIGNET

1) There is a requirement to provide connectivity between SIGNET and outside services, such as News Services, Compuserve, and Dun & Bradstreet . To provide access to off SIGNET services, some type of dial in/out service supporting both public switched telephone network and X.25/28 capabilities is required.

2) There is a requirement to provide connectivity between SIGNET and Federal Government and National electronic mail / message systems including the Government Telecommunications Agency (GTA) services, GEMDES and Senior Executive Network (SEN), and INET 2000 (Envoy). It is most likely that this service will interface directly into the SIGNET electronic mail system, via X.400 MTA - MTA over X.25.

3) There may be a requirement to provide network layer connectivity between SIGNET, other government departments, and CA*net (National IP Backbone).

4) "Connectivity to remote systems (that is, client server applications) over the enterprise network is a longer-term requirement. Immediate connectivity to CIDA hosts using X.25 gateways must be provided when SIGNET implementation occurs for missions with that requirement."[SIGNET Tactical Plan]

5) "There is a minor requirement for access to host computers outside the Department using 3270 terminal emulations. ... gateway for local users, along with standard emulation software." (DSS On line pay) [SIGNET Tactical Plan] .

2.7 Directory Services

2.7.1 Name Services

1) In typical IP network environments, best exemplified by the Internet, Domain Name Services (DNS) (IAB RFC 1035), provides a distributed hierarchical directory service with global uniqueness. The naming structure is defined by DNS; an example for External Affairs may be RWATT@MSS.EAITC.CA. In a homogeneous IP environment, External Affairs would be required to establish a Domain Name Service with DNS name syntax. However, the electronic messaging service is a major client of a name service. In the event that an X.400 based message service is selected, the requirement may be weighted in favour of the CCITT X.500 directory services.

2.7.2 Address Resolution Services

1) An address resolution service is required to provide a mapping between data link layer addresses (i.e.. 8802-3 addresses) and the network layer addresses (i.e.. IP addresses).

3. INTERNETWORK PERFORMANCE

3.1 General

a. The object of this section is to model and predict the required minimum bandwidth per some number of average users and the impact of wide area network communication delays on transaction oriented applications (i.e.. remote terminal or remote client server). The prediction will bound the magnitude of bandwidth required to support information transfer or store and forward oriented applications (i.e.. e-mail) and indicate possible problematic application performance due to communications delays between terminals and remote hosts or between clients and remote servers. Note that communication delays in general consist of physical propagation delays, due to distance and available bandwidth, and communications path utilization due to information transfers, multiple simultaneous remote terminal or client server sessions, and network management related information communications.

b. It is imperative that application loads be actually modeled and tested within the SIM Centre. The SIM Centre internetwork will be modeled after the target SIGNET internetwork including HQ, regional, and mission components and therefore enable a higher degree of confidence to be obtained regarding application performance.

c. The throughput and response capability of the local area subnetworks will exceed the requirements of all existing corporate applications / services. Furthermore, any pressures on increasing local bandwidth can be readily addressed with proper network tailoring techniques and/or utilizing higher throughput network elements or local subnetwork technologies.

d. The wide area subnetwork poses the greatest challenge to supporting communications due to the limited bandwidth and relatively long propagation delays characteristic within the wide area subnetwork. Therefore, the focus within this section is on the wide area subnetwork.

e. The approach to implementing the optimum solution will have to take into consideration the specifics of delay, expected traffic volumes, and availability on at least a per region basis, and perhaps on a per mission basis where experience has shown unreliable and poor quality service in "the last mile". In general, a hybrid approach will lead to the optimum balance between quality service perception from the end users and maintainability of centralized information and human resources.

3.2 Wide Area Subnetwork Performance

3.2.1 Throughput Considerations

a. The available low aggregate bandwidth provisioned to the missions for SIGNET may inhibit the use of regionalized general client/server and terminal/host implementations. The following analysis indicates that 19.2 kbit/s links should be adequate to support the typical mission in terms of information transfer. Delay sensitive applications may be problematic depending upon the required performance as expected by the application users. It is recommended that wide

area transaction oriented services be evaluated within the SIGNET Simulation Centre across a 19.2 kbit/s test circuit with an expected cross section of messaging/transfer load added simultaneously. Consideration of standardized deployment of wide area transaction oriented services should only be given in the event that the simulation yields positive results. A final decision to deploy wide area transaction oriented services must also take into account the availability of the wide area subnetwork (Section 4.0).

b. Table 3.1 and the following calculations summarize the model upon which the throughput oriented recommendations are based. The reader is referred to Appendix I for analysis details.

Application	Remote Volume (kbytes) per 100 Persons per Day	
Electronic Messaging (No Attach)	2695	
CATS (Message Archival)	2695	
CATS (File Archival)	108	
File Transfer / Message Attach	4313	
NOCAMS	105	
WIN Exports	263	
CAIPS	263	
Mission FINEX	53	
CIDA Decentralization	263	
Total Daily Volume	10758	kbytes

Table 3.1: Traffic Volume Estimates

Using a typical model of two busy hours per day, one in the morning, and one in the afternoon, and assuming that during a busy hour 25% of all daily traffic is transferred, for a total of one half the daily traffic within two hours, and further assuming that 5% of the busy hour traffic is transferred during the busy minute yields the required busy minute aggregate throughput, or required bandwidth, to be:

Bandwidth = (10758 kbytes*.25*.05*8000 bits/kbyte) / 60 secs = 18 kbits/s per 100 users

At 18 kbits/s a user would be able to transfer this document, which is relatively image intensive and is approximately 580 Kbytes in size, in approximately 5 minutes.

c. Note the sensitivity of the bandwidth as a function of the busy hour and busy minute volume assumptions; increasing the busy minute assumption from 5%, which is 3 times greater than the average volume per minute during the busy hour, to 10% causes the required aggregate bandwidth to increase to 36 kbits/s; simultaneously increasing the busy hours assumption to 33% has a net effect of increasing the required aggregate bandwidth to 48 kbits/s. A variance of the busy minute assumption from 5% to 10%, combined with a variance of the busy hours assumption from 25% to say 33% may be considered as reasonable variances indicating that a fixed aggregate bandwidth on the order of 19.2 kbits/s per 100 users should be viewed as potentially constraining under the volume assumptions for a typical cross section of 100 users assumed herein.

d. With respect to terminal and/or interactive transaction oriented traffic, the response time of a screen request, when scrolling through a document for example, or a search request on a data base must be considered in addition to aggregate throughput considerations. The screen on which this particular page was typed contained about 1000 characters or 1000 bytes under the basic assumption of 1 byte per character. Under the scenario where a user wishes to scroll through a document, it is reasonable to assume that the user's expectation would be to have the screen scroll by in no more than 2 seconds. Therefore, without considering protocol overhead the required throughput to meet the users expectation is:

Bandwidth = 1000 bytes * 8 bits/byte / 2 secs = 4 kbits / sec

e. In the absence of a block mode capability and under the further assumption of 4 bytes of overhead per character, which is typical of header compressed Telnet transactions, the required bandwidth becomes 16 kbits/s.

3.2.2 Delay Considerations

a. Delay impacts the performance of interactive applications such as remote terminal sessions or remote client / server based applications. The purpose of the following analysis is to provide an early determination of whether, given the expected bandwidth available, and the global expanse of SIGNET, there may be a concern with the general deployment of applications which require the end user to interact across the wide area network in real time.

b. The estimated wide area subnetwork delay components are provided in Table 3.2. The reader is referred to Appendix I for analysis details.

Network Component	Round Trip Delay Contribution	
	19.2 kbit/s	64 kbit/s
Equipment	35 ms	15 ms
Transmission Media	10 ms / 1000 km	

Table 3.2: Network Component Delay Contributions

c. Example total round trip delays are provided in Table 3.3. To put the delays into perspective, experience in large internetworks has shown that when round trip delays begin to exceed on the order of 150 ms, the users of transaction oriented applications, such as terminal emulation sessions, begin to notice a performance degradation. As the round trip delay increases beyond 150 ms, the degradation of performance increases rapidly with 500 ms round trip delays becoming counter productive and frustrating to the user.

End Points	Distance (km)	Total Round Trip Delay (ms)	
		19.2 kbit/s	64 kbit/s
Ottawa-Tokyo	13,000	165	145
Ottawa-London	7,500	110	90
Ottawa-Washington	750	42	12
Paris - Rome	1,200	47	17

Note: The table entries assume a zero length message and do not include computer processing time.

Table 3.3: Example Total Round Trip Delays

d. With respect to client/server based computing, transactions per second is used as a useful measurement of capability. Table 3.4 presents the maximum possible transactions per second, assuming a zero length request and a 128 byte response, between the end-points given in Table 3.3. The message lengths for 19.2 kbits/s and 64 kbits/s transmission rates are approximately 55 ms and 16 ms respectively. Table 3.4 is included for the purpose of informing interested persons as to what sort of data base interaction can be expected; no interpretation of the impact of the numbers in Table 3.4 is made herein.

End Points	Maximum Transactions Per Second Per Session	
	19.2 kbit/s	64 kbit/s
Ottawa-Tokyo	5	6
Ottawa-London	6	9
Ottawa-Washington	10	26
Paris - Rome	10	23

Note: The transactions per second assume a zero length request, a 128 byte response, and do not include computer processing time.

Table 3.4: Example Maximum Transactions per Second

e. To help the reader understand the impact of delays on the order of 100 ms to several hundred ms, the following example is based upon an application with which most readers will have some intuitive understanding. The application is simply one of the round trip delay requirements assuming data entry to a remote host with 'host echo'.

The intent of this example is to translate delay in ms into something which may be intuitively understood thus building an appreciation of whether some round trip delay, say 250 ms, is cause for futher consideration or is acceptable for the application of interest.

A competent data entry person will typically attain peak rates of 450 characters per minute. To achieve this remotely, the data entry person requires an instantaneous minimum response time of:

Response Time = 1 / (450 characters/min * 1 min / 60 sec) < 135 ms

The data entry person requires a round trip response time of less than 135 ms per key stroke. From Table 3.3, degradation in the service would be noticed once the separation between host and terminal begin to exceed approximately 7500 kms, **assuming no delay associated with the remote application** computing and **no competition for bandwidth** across the communication path.

Performance will degrade as additional users or processes (eg. Messaging) use the facilities concurrently. The envisioned SIGNET wide area subnetwork will, to a limited extent, support real time access for users. However, simulation of EAITC applications is required to identify the limits on simultaneous use of wide area subnetwork facilities by multiple users and processes.

3.2.3 General Recommendations for Mission Wide Area Service

a. The previous analysis bounds the throughput and delay requirements to be on the order of a minimum of 19.2 kbit/s per 100 users with round trip delays no greater than on the order of 150 - 250 ms. The round trip delays will be impacted by the degree of utilization of the available bandwidth due to simultaneous loading. Although it is possible to extend the model herein to include cross impacts of utilization on delay sensitive applications, the results will be of nominal value. The best way to garner a better information is to perform actual simulations of the typical application cross section within the SIM Centre.

b. In the absence of the results of simulations, a guiding recommendation is made to assist the SIGNET planners.

Guidelines for the required minimum aggregate bandwidth of a SIGNET Wide Area subnetwork access are:

1) Under the scenario of <u>no transaction oriented applications</u> across the wide area subnetwork:

Minimum Aggregate Bandwidth = 19.2 kbit/s per 100 persons

Not to be less than 9.6 kbit/s.

2) Under the scenario of <u>transaction oriented applications</u> across the wide area subnetwork:

Limit transactions to mission - regional service. Do not provide global transaction service (i.e.. Tokyo to Ottawa)

Minimum Aggregate Bandwidth = 19.2 Kbit/s + 19.2 Kbit/s per 100 personnel

3.3 Local Area Subnetwork Requirements

a. The minimum SIGNET local area subnetwork service level will support a data link layer aggregate throughput of approximately 3.5 Mbit/s continuous and 6 Mbit/s peak. The SIGNET local area subnetwork traffic requirement is less than 2.0 Mbit/s continuous.

b. The minimum service level supports a data link layer round trip response time of less than 1ms.

3.4 Inter-Regional Link Bandwidth Recommendations (PRELIMINARY)

a. Table 3.5 summarizes the recommended inter-regional node bandwidth requirements. The reader is referred to Appendix I for details.

Link	Bandwidth (kbits/s)	DS-0s
London - Ottawa	256	4
Paris - Ottawa	192	3
Paris - London	192	3
San Francisco - Ottawa	256	4
Washington - Ottawa	128	2
New York - Ottawa	64	1

Table 3.5: Inter Regional Node SIGNET Bandwidth

NOTE: PRELIMINARY VIEW

b. The consolidation of mission traffic on the regional links primarily serves the purpose of maximizing bandwidth efficiency. In the cases of Paris, Washington, and London, a further benefit is realized by providing the larger missions with greater bandwidth than otherwise would be afforded.

c. A limitation on consolidating the bandwidth is that the point of consolidation requires a router unless a frame relay service is provided on MITNet. In the case of San Francisco, there is currently no qualified staff on site. MITNet operations for the Pacific Rim is handled out of Ottawa.

d. The use of a frame relay service within the wide area subnetwork, which will readily enable the consolidation of bandwidth, is to be evaluated in conjunction with MITNET personnel.

4. INTERNETWORK AVAILABILITY

4.1 Availability Objectives

The availability objectives and data presented herein are preliminary. Further refinement to the analysis is pending the awarding of the network element RFP and refinement of the availability data for the underlying MITNET service. The current availability is based upon an assumption of a 24 hour MTTR for remote sites which will also be reviewed pending the awarding of the Network Element RFP. Note that the OBJECTIVES DO NOT INCORPORATE THE AVAILABILITY OF END SYSTEMS (eg. file servers, user workstations).

a. Availability is defined with respect to a user of the internetwork services where a user may be a person or process. The SIGNET service is defined to be unavailable when any user cannot access any desired resource anywhere in SIGNET. The SIGNET Internetwork Service is defined to be unavailable when the outage to the user is due to an outage in the internetwork and not by an outage in the end systems involved in the desired service.

b. The SIGNET Internetwork Service Availability objective is separated into two components:

   1) The two end systems are within the same local subnetwork environment with no traversal of the wide area subnetwork required.

   2) The two end systems are in different local subnetworks and a traversal of the wide area subnetwork is required.

c. The accuracy of the following availability analysis is, of course, dependent upon accurate estimations of the reliability of the various components of SIGNET including devices, such as concentrators and routers, as well as services, such as MITNET and power. The numbers presented in this version are based upon estimates, founded in experience with other networks, and data provided by MITNET personnel for the underlying MITNET services. The Network Element Request for Proposal requires bidders to provide reliability data for the products bid. **The SIGNET Internetwork Availability analysis will be refined using vendor provided reliability data upon awarding of the network element contract.**

d. The SIGNET Internetwork Service availability objective is:

1)	Overall:	97.5%
2)	Local Subnetwork Traversal Only	97.8%
3)	Wide Area Subnetwork Traversal	96.5%

END SYSTEMS NOT INCLUDED

The objective is established by considering realistic values for component reliability, input on the expected availability of the wide area subnetwork service, and the complexity of the network. The availability objective has been established in the absence of input requirements from the user community.

e. The corresponding expected maximum annual outages are:

1)	Overall:	220 hrs
2)	Local Subnetwork Traversal Only	190 hrs
3)	Wide Area Subnetwork Traversal	300 hrs

END SYSTEMS NOT INCLUDED

The annual outage is the outage experienced by an individual user where the user is a person or process requiring access across the internetwork. All users of SIGNET will experience on average annual outages as per the above list. The analysis does not investigate the expected number of affected persons or processes given a particular failure in the network.

f. The Internetwork Service availability objective is established using estimates for device and underlying service availability and objectives for Mean Time To Repair. Detailed data is contained in Appendix 2. For the purpose of the objectives presented above, the availability table under Sparing Consideration in Appendix 2 is used.

g. The overall availability and outage are based on a 70 / 30 weighted average for the local / wide area internetwork service access by a user. The ratio is chosen to allow for a portion of the user's activity to be dependent upon the real time availability of the wide area subnetwork.

4.2 Availability Analysis

a. Availability is defined as the ratio of the time the SIGNET Internetwork Service is operational, as viewed from the end user, to the total elapsed time and is given by:

$$\text{Availability} = \frac{\text{MTTF}}{\text{MTBF}}$$

and

$$\text{MTBF} = \text{MTTF} + \text{MTTR}$$

where

MTTF = Mean Time To Failure
MTTR = Mean Time To Repair
MTBF = Mean Time Between Failures

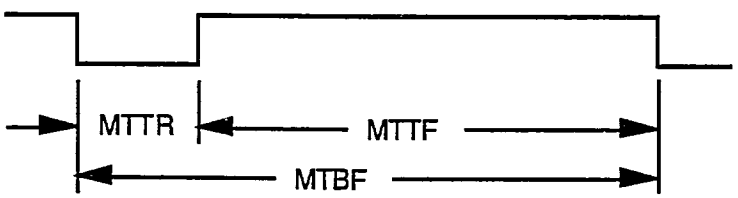


Figure 4.1: Availability Mean Cycle

b. The MTTF is a function of complexity of the component, the quality of manufacturing, the harshness of the operating environment, the degree of redundancy, and the degree of preventative maintenance. The Mean Time to Repair is a function of the time to detection and diagnosis of the failure, availability of qualified repair technicians, complexity of the component exchange, the proximity of spares to the failure site, and the volume of spares available.

c. The SIGNET Internetwork Service availability analysis is based upon the following model, illustrated in Figures 5.2 and 5.3:

$A_l = A_c^4 * A_b^2 * A_{rl} * A_w^8 * A_{pm}$

$A_r = A_c^4 * A_b^2 * A_{rl} * A_{rc}^2 * A_{mc} * A_{ml} * A_w^8 * A_{ws}^4 * A_{pm} * A_{ph}$

$A_{eus} = 0.7 * A_l + 0.3 * A_r + 0$

where

A = Availability of

l	Local Subnetwork Internetwork Service
r	Wide Area Subnetwork Internetwork Service
c	Concentrator
b	Bridge
rl	Mission router
rc	SIGNET core router
w	series path wiring/cabling
ws	Router to MITNET node serial cable
kg	encryption device
mc	MITNET Core
ml	MITNET Mission Link
pm	Mission power
ph	Headquarters power
eus	End User Service

d. The value of zero is added to the formula for the overall availability, A_{eus}, for completeness. The zero term represents the probability that a user does not wish to use the network at some particular time; in the case where a user is a person, the user will not require access to the network upwards of 75% of the time due to evenings, weekends, and vacation absence. In the case where the user is a process, the process may be automated to run at any time, thereby requiring a higher degree of availability in the network. Detailed data and calculations are contained in Appendix 2.

e. A significant factor in the overall internetwork architecture is the link between the MITNET regional node and the mission. Initial discussions with the MITNET personnel led to the use of a Mean-Time-To-Failure of 1 month with a Mean-Time-To-Repair of 6 hours for the region to mission access links. Further

consideration has indicated that this high degree of outage is applicable to only a few of the mission sites; a more appropriate outage estimate is under review and will be incorporated into the final analysis, pending revised input from MITNET personnel.

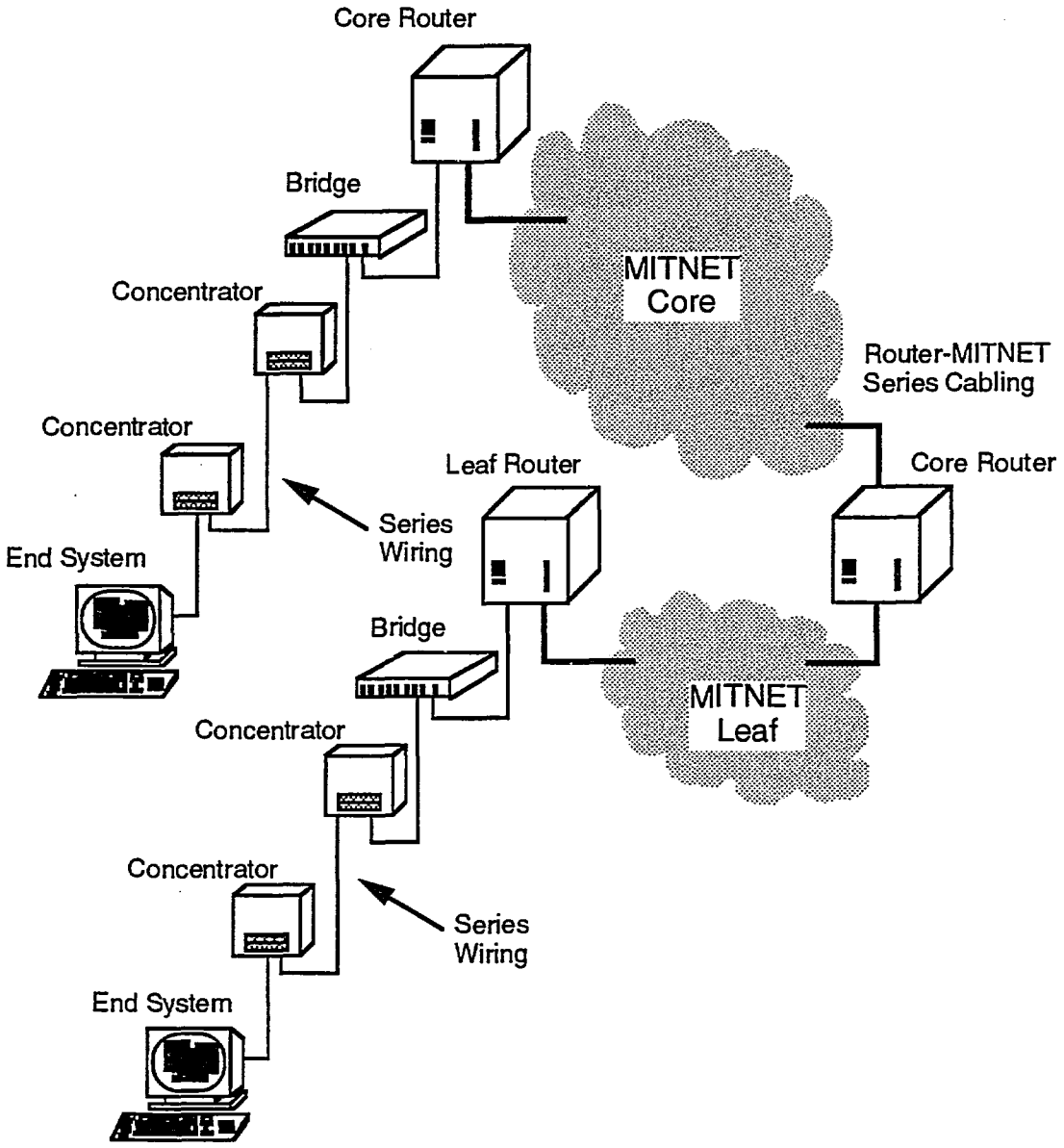


Figure 4.2: Wide Area Subnetwork Model

4.3 Impact of the Internetwork Availability on the General Architecture

The Impact on the General SIGNET Architecture will be reviewed pending awarding of the Network Element RFP. The current availability is based upon an assumption of a 24 hour MTTR for remote sites which will be reviewed pending actual failure rate data.

a. The contrast in the expected availability of the local subnetwork vs the availability of the wide area subnetwork indicates that the probability of success of SIGNET, as perceived by the end user, is enhanced by the degree of localization of the data and applications which the user will require "real time" access to.

b. A quasi-worst case scenario whereby all user internetwork access requires traversal of the wide area subnetwork would result in the users not having access on the order of 25 hours per month (300 hrs/yr / 12 mths/yr). Furthermore, the model does not account for a signal degradation case whereby the network is actually up but the signal bit error rate causes frequent retransmissions. Telecommunications companies' signal quality objectives in North America and are such that no significant problem exists; the same can not be said in general for other regions in the world. Hence, dependency upon real time access across the wide area subnetwork may lessen the success of the network from the users perspective.

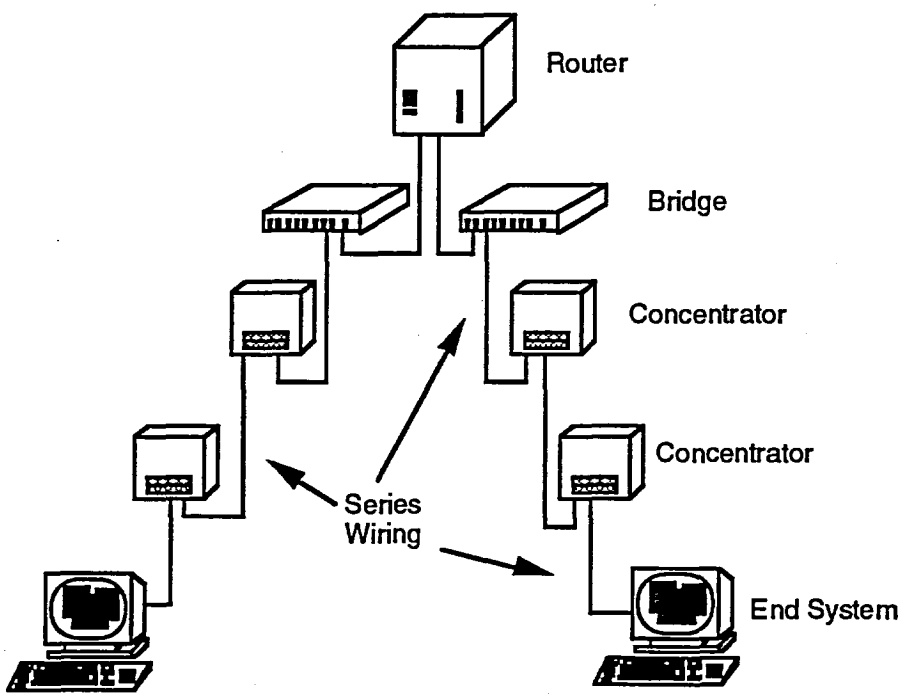


Figure 4.3: Local Subnetwork Model

c. A best case scenario whereby all user internetwork access requires traversal of the local area subnetwork only would result in the users not having access on the order of 16 hours per month (190 hrs/yr / 12 mths/yr). Note that in this scenario, information transfers across the wide area subnetwork would be performed on a non-real time basis using appropriate store and forward mechanisms.

d. The implications of implementing application/data architectures which require wide area subnetwork access vs those which do not require wide area subnetwork access are significant when consideration is given to the requirement for hardware and data replication and maintenance of same. Hence, although the expected poor availability performance of the mission access links weight the data architecture in

favour of localizing all transaction oriented services into the missions, the operations implications weight the data architecture in favour of regionalizing data bases and implementing transaction oriented services across the wide area subnetwork.

e. The approach to implementing the optimum solution will have to take into consideration the specifics of delay, expected traffic volumes, and availability on at least a per region basis, and perhaps on a per mission basis where experience has shown unreliable and poor quality service in "the last mile". In general, a hybrid approach will lead to the optimum balance between quality service perception from the end users and maintainability of centralized information and human resources.

4.4 Internetwork Device Repair Rates and Sparing Levels

a. The availability of SIGNET is affected by the Mean Time to Repair of a failure and in turn by the ready access to spare components. Determination of spare levels takes into account the rate of failure of components in the network, the rate at which the failure can be resolved, and the availability objective for the particular component. The availability equations, Section 4.2 paragraph a., may be re-stated as:

$$\text{Availability} = \frac{\mu}{\lambda + \mu}$$

where

$\lambda = 1 / \text{MTTF}$

$\mu = 1 / \text{MTTR}$

which are the failure rates and repair rates of components of interest respectively.

b. Given a population of n components, the effective failure rate in the population is $n\lambda$. Given a repair rate of μ to resolve a failure, the required sparing level, m, can be determined from:

$$m = \frac{A\,n\,\lambda}{\mu\,(1-A)}$$

where

A = availability objective for the component.

c. As an example, consider a population of 120 mission routers. The Mean Time to Failure is stated by the manufacturer to be 36 months which equates to a failure rate of one failure per 26,280 hours. Given the general dispersive geography of the missions, the spares are to be located in such a fashion that the Mean Time to Repair is 24 hours. Finally the overall availability of SIGNET requires that the

availability of the mission routers be 99.75%, equivalent to an average outage of just under 2 hours per month. From this, the required number of spares is calculated to be 44 or a required sparing level of approximately 33%. If the MTTR is reduced to 4 hours, the required number of spares becomes 15 or 13%. Note that the spares may be located at a vendors site, but must be available such that a failure may be resolved within 24 hours.

d. It may not be intuitive why reducing the Mean Time to Repair reduces the required sparing level when the failure rate remains constant. Consider that the repair exercise requires qualified personnel, a replacement component, and possibly travel; with a long mean time to repair, the probability of suffering simultaneous failures increases and therefore simultaneous repair actions will need to be supported.

e. Estimated spare levels for the SIGNET Internetwork components are provided in Appendix 2 under Sparing Considerations. **Final analysis of sparing will be completed subsequent to the network element RFP award. The final sparing analysis will be completed on a per region basis plus head quarters.**

f. The option of providing alternate back up facilities to reduce the impact of a single failure, and therefore reduce the required number of spares, is under evaluation.

5. INTERNETWORK SCALABILITY

5.1 General

a. SIGNET is required to provide services to sites ranging in size from several hundred to less than 100.

b. The internetwork scalability requirement is segregated into a local subnetwork technology scalability requirement and a routing technology scalability requirement.

5.1.1 Local Subnetwork Technology Scalability

1) The technology utilized to provide the local subnetwork service must be capable of supporting numbers of connections ranging from less than 10 through to greater than 100.

2) A logical limitation may exist on the maximum size of a local subnetwork if the subnetwork design is tailored to personnel logical function. A natural limitation exists at on the order of 100 to 150 connections per subnetwork for operations purposes.

5.1.2 Routing Technology Scalability

1) The technology utilized to support the routing service is required to support both the large number of small to medium sized mission sites, medium to large sites, and (most likely) concentration sites (possibly co-exist with major MITNet nodes (ie. London , Paris , Washington etc.)

6. INTERNETWORK SECURITY

6.1 Background

a. The SIGNET Designated Network is designed to process data designated up to, and including, "Protected A ... The SIGNET Designated Network will operate in "system-high" mode."[2]

"A system is considered to be operating in the system high mode when all of the following statements are satisfied concerning the users with access to the system, network, its peripherals, remote equipment, or hosts:

- Each user has the appropriate level of personnel screening for all information on the system or network.
- Each user has formal access approval for, and has signed a nondisclosure agreement for all information stored and/or processed on the system or network.
- All users have a need-to-know for some of the information contained within the system or network."

b. The designated LAN will not carry information with a classification greater than Protected A.

c. No connection shall be permitted with external systems unless appropriate safeguards, which have been approved by the departmental security authorities, are in place.

6.2 Implications on SIGNET Internetwork

6.2.1 Local Area Subnetworks

a. The local subnetworks, or LANs, will be physically located wholly within the "system high" operating environment. There are no security requirements which yield security specifications directly impacting the local subnetwork related hardware or software, where local subnetwork connectivity is defined to be provided at the physical layer interface (i.e.. RJ-45 10BaseT jack) in the vicinity of the computing end system and does not include any system related interfaces such as Network Interface Cards.

b. Note that the planned physical / data link layer LAN equipment employs a physical layer broadcast protocol mechanism[2]. The implication is such that all physical layer interfaces into the LAN receive all information transmitted onto the LAN.

c. The physical layer star topology of the planned LAN technology allows operations based policy to limit the threat of unauthorized

[2] Carrier Sense Multiple Access / Collision Detection (CSMA/CD)

access into the LAN by means of physically servicing only the physical layer interfaces which are providing connectivity to authorized end systems (PCs, servers, etc.). All other non-used physical layer interfaces are not connected back to the centralized LAN equipment.

d. Furthermore, the planned local subnetwork architecture (i.e.. physical, data link, and network layers) enables the implementation of LAN equipments employing special security related mechanisms. For example, there are commercially available 10BaseT hub products which overwrite the data field of all packets not destined for the end system connected to a particular port.[3]

6.2.2 Wide Area Subnetwork

a. In general, the wide area subnetwork connectivity will utilize the services of MITNet. All information transmitted across the wide area subnetwork normally undergoes encryption/decryption using government approved encryption devices on MITNET. MITNET is currently evaluating bulk encryption technologies which will reduce the general requirement for encryption on a per input circuit basis.

b. A decision has been made to not use KG encryption devices for SIGNET input circuits.

c. No additional security related requirements are assigned to the wide area subnetwork.

6.2.3 Internetwork Elements Security

a. All network elements deployed into SIGNET must employ adequate access security to allow access to device configuration and monitoring to authorized personnel only. Authorized personnel should be limited to the organizations responsible for the operations and maintenance of the SIGNET internetwork.

6.2.4 Access External to the SIGNET Local/Wide Subnetworks

a. Access external to the SIGNET local/wide area subnetworks may be provisioned in at least three forms:

1) Point-to-point connections, either dedicated or switched and through the public telephone network (eg. Bell Canada network), between External Affairs devices and devices operated by other departments or service corporations. For example, connections between External Affairs and Employment and Immigration for exchanging CAIPs related information; service contracts with SHL Systemhouse for FINEX; and an X.400 MTA - MTA gateway between SIGNET and the GTA e-mail services.

[3]Such a capability is not a requirement for the concentrators in the Network Element RFP.

2) A continuous network layer interface between External Affairs and other like networks. For example, the Government Telecommunications Agency is currently investigating offering a Government of Canada backbone service for government department networks.

3) General dial in / dial out capabilities through the public switched telephone network. For example, External Affairs personnel would be able to "dial in" to the External Affairs network when off site. Commercially available PSTN communications server technology enables dial in/dial out services to be generally available to SIGNET users. An example is access to Dun & Bradstreet data base services. Dial access control may be integrated with External Affairs PBXs or Centrex services.

b. The security requirements relating to each of the three scenarios:

1) The point to point connections to other government departments or service corporations may be considered to operate in the "system high" state. A requirement for encryption/decryption may be applicable on a per link basis.

2) External Affairs should not consider interconnecting SIGNET with other internetworks at this time. In the event that External Affairs requires connectivity to a general service internetwork, GTA offered or otherwise, a secure router function would be required at the interface.

3) Dial In/Out Requirements are:

i. The general use of dedicated modems and communications software on per PC basis should not be allowed on SIGNET.

ii. For the purpose of access from External Affairs to dial up services, such as Dun & Bradstreet services, the communications servers should be implemented with dial out capability only.

iii. For the purpose of general dial in / dial out capabilities, if required, communications servers should be implemented as a shared resource available at various points within SIGNET; the communications servers must employ an authentication mechanism for access. Dial in security would be further backed up with access controls on all networked end systems.

7. SIGNET INTERNETWORK ARCHITECTURE - DESIGN

a. This following portion of the document details the design of the SIGNET Internetwork. The SIGNET Internetwork design is premised upon meeting the SIGNET Internetwork Requirements. In areas where the requirements may not be finalized, the design is subject to change. However, no major alterations to the significant aspects of the design are anticipated.

b. The focus of the following sections, particularly routing and addressing related sections, is on the Internet Activities Board Internet Protocol suite. Note that the requirements for procurement of the routers include the support of Treasury Board Information Technology Standards (TBITS) Layer 3 (ISO) related standards. Design details for TBITS Layer 3 related aspects of SIGNET will be completed in a later phase of the evolution of SIGNET.

8. SIGNET ADDRESSING

8.1 IP Network Addressing

a. TCP/IP requires every individual host to be provided a unique 32-bit internet protocol address which will be utilized by all IP network communications to and from this station. These addresses are divided into both a network identifier portion, upon which routing decisions are based, and a host portion which uniquely identifies a host on any given network.

b. Currently assigned to EAITC by the Internet Architecture Board (IAB) Network Information Center (NIC) are two Class B network address 158.128.0.0 and 160.106.0.0 respectively. Class B networks are capable of providing addressing for intermediate size networks which have between 256 and 65,536 hosts.

c. IP Addresses are divided into two sections, the network portion as assigned by the NIC, and a host portion which is under the control of the organization's network administrators. SIGNET's class B address 160.106.0.0 network/host portion is broken down as follows.

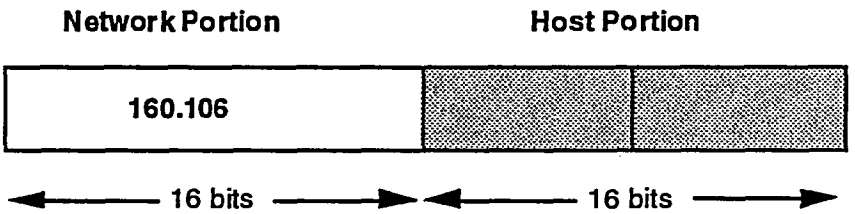


Figure 8.1: IP Address Network/Host Portion

d. Each Internet Protocol (IP) network address has a third component termed the subnet address. The subnet address portion allows the local network administrator to segment portions of their address space, via the host portion, to uniquely identify separate physical networks within the local network administrators control. An example of a 160.106 subnet/host configuration with a 12 bit subnet address is shown below. The number of bits reserved for the subnet portion is set by the network administrator via a subnet mask.

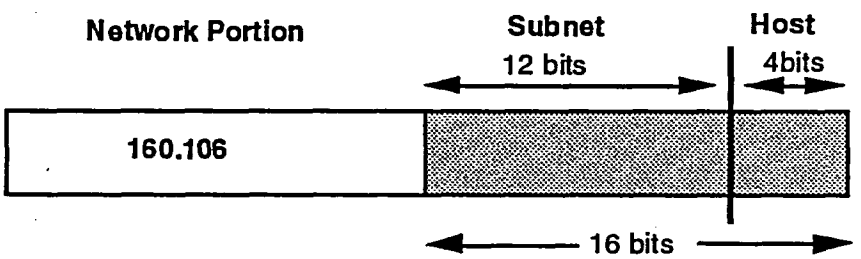


Figure 8.2: IP Address Network/Subnet/Host Portion

8.2 IP Subnet Addressing

a. SIGNET has four major network addressing categories. Each category has a different set of characteristics based upon the number of sites within SIGNET and the number of end systems within a particular site. This breakdown of sites/end-systems is as follows:

i. *Missions* which will have typically under 128 end systems on their respective Local Area Networks. These missions will have a small number of network devices, less than 128, but will account for the majority of sites within the SIGNET enterprise network. SIGNET will consist, in part, of approximately 125 of these missions.

ii. *Regional missions* such as London, Washington etc. will have larger number of end systems per site, though less than 300. These end systems may/may not be on one logical subnet but the current subnetting plan will allow these sites to have all of their hosts on one subnet if required. The number of regional mission sites will be limited to be less than 10.

iii. *Serial interfaces*, on point-to-point connections, will need an IP addresses associated with them as well. There will be at least one serial connection through MITNET for each instance of the following:

- Headquarters - Region,
- Region - Region, and
- Region - Mission

SIGNET, upon completion, will be well over 125 point-to-point subnets with only a router at either end connected to each subnet. Assigning a subnet mask which allows 256 hosts per subnet would be a waste of address space as typically only 2 hosts will reside per serial subnet.

iv. *Headquarters* - Ottawa based with several buildings containing approximately 3000 end systems. A typical scenario will be several hundred hosts per connected subnet with 10 to 20 subnets within the Ottawa area.

8.3 SIGNET Addressing Alternatives

a. Based upon the scenarios discussed in Section 8.2, the following number of subnets/hosts combinations are required for the SIGNET project.

Area	Approx. # Subnets	Hosts/Subnet
Missions/Annexes	150	128
Serial Links	150	15
Regions	10	300
Headquarters	20	512

Table 8.1: Subnet/Host Combinations Required

b. Maintaining one subnetting scheme across the entire enterprise network requires an addressing scheme that provides the minimum requirements of:

- at least 300 subnets across the entire enterprise network, and
- able to accommodate large networks of over 300 hosts.

Implementing a common subnet mask solution, with the current SIGNET Class B address structure, would require 9 bits of addressing for the host, leaving only 7 bits for subnetting. These 7 bits allow 2^7 or 128 subnets, not enough to meet SIGNET requirements.

c. Even by utilizing SIGNET's 2nd Class B address for headquarters use only, thereby eliminating the need for the first Class B network address to support 512 hosts per subnet, would require over 300 subnets each supporting 300 hosts. Using enough bits to meet the subnet requirements leaves too few addresses to satisfy the minimum number of hosts.

d. In order to provide a large enough addressing space for the EAITC enterprise network the following alternative solutions are considered:

i. Split all subnets of 300 or more hosts into subnets of < 128 hosts, then use 9 bit subnet mask to have 2^9 subnets of 2^7 hosts. This would require all subnets within headquarters to contain less than 128 end systems and managed devices.

ii. Assign part of the Headquarters Network address space to be used in Regions/Missions i.e. Pacific Rim would utilize subnet space out of 158.128. Then break subnets into 2^7 subnets of 2^9 hosts and use both network addresses to meet the minimum number of subnets needed.

iii. Use variable subnet mask to ensure best application of address space for Region/Missions depending on whether they are being used for larger region, mission or the serial link.

e. Solution (i) forces a logical network topology due to network addressing. Where it is feasible that remote regions will have their subnets reduced to less than 128 nodes, an addressing solution should not force this configuration. Only 126 host addresses are available, due to the restriction of not using all 0's or 1's for the host portion of the addresses. Use of this solution requires use of both Class B network addresses, one for headquarters LANs and the other for the remaining network.

f. Solution (ii) creates a waste of address space. Subnets with small number of hosts and devices will have a subnet addressing scheme which supports 512 host addresses. As part of solution (ii) the network administrator must also track which part of the Headquarters' address space is being utilized in which missions and regions. Use of this solution requires use of both Class B network addresses, one for headquarters LANs and the other for the remaining network.

g. Solution (iii) has the ability with OSPF and variable subnet masks to apply a finer granularity of subnetting depending upon the use of the subnets. With (iii) the

network administrator must take greater care to ensure that the subnet mask being used is correct for the attached subnet.

h. Address efficiency can be measured in the amount of actual hosts addresses that can be utilized within the network space available. In the case of SIGNET it is not practical to implement the entire addressing requirements with one fixed partition between the host and subnet portions as required by alternative (i) and (ii). A solution for one of the addressing requirements yields a waste in the address space for the remaining areas.

i. Variable subnet masking is the solution for the SIGNET Enterprise Network. This solution allows **one Class B network address, 160.106,** to be used within the EAITC SIGNET network.

8.4 Variable Subnet Masking

a. Subnet masks provide the network administrator a method of distinguishing which part of the IP network address are to be used for the host address portion and which portion will be used for the network and subnet portion. Subnet masks are specified by using a 1 in every bit position that is to be used for the network/subnet portion.

b. The 160.106 network portion of the address is fixed from the Internet Architecture Board's Network Information Center as SIGNET's Class B address. This leaves the remaining 2 octets (16 bits) to use for a subnet and host portion. This can be represented as follows:

160.106.xxxx xxxx.xxxx xxxx

c. The first three bits immediately following the fixed network portion indicate a type of subnet mask to follow (shown below by t's). The subsequent subnet mask allows the necessary flexibility to accommodate various numbers of subnet and host combinations. The following are SIGNET subnet types and their typical applications within SIGNET.

160.106.tttx xxxx.xxxx xxxx

1ss - *mission,* by utilizing the 2nd and 3rd bits of the type field as part of the subnet mask the number of subnets and hosts that can be accommodated will be increased.

01x - *headquarters and large region subnets,* this type will have an associated subnet mask to allow for large number of IP addresses per subnet to meet the headquarters and large regions requirements for many host addresses per subnet.

001 - *smaller headquarter LANs and typical region subnets,* these subnets will typically be used in a region where several subnets are present, or in a smaller headquarters site where the LAN will not contain a large number of hosts.

000 - *serial interface subnet,* used typically for point-to-point addressing of serial links, and small fully-meshed frame relay networks where the number of interfaces per subnet will be small.

8.5 SIGNET Addressing Implementation

8.5.1 Headquarter/Large Region Addressing Structure

a. Headquarters addressing requirements as identified to date will require an addressing scheme capable of supporting:

- Number of Clients 2800
- Number of Servers 14
- Clients per Server 200

b. The servers are connected in pairs with 400 users per 2 servers, and each group of 2 servers represents both one IP subnet and one logical LAN Manager 2.0 domain. These LAN Manager domains will require well over 400 host address per subnet, and in the case of headquarters 8 - 10 subnets. Large regions may have a similar issue whereby over 256 host addresses are required per subnet.

c. Headquarter LANs and larger region subnets have a type of 01 which provides the remaining 14 bits for use in the subnet/host portions.

160.106.01xx xxxx.xxxx xxxx

d. Headquarter LANs and larger region subnets will require less than 512 hosts per subnet therefore 9 bits for the host portion (h's) will be sufficient. i.e.

160.106.01ss sssh.hhhh hhhh

e. This combination generates a subnet mask of 255.255.254.0, and provides 2^5 subnets of 2^9 hosts or 32 subnets of 512 hosts.

8.5.2 Smaller Headquarter/Regional LAN Addressing Structure

a. Smaller Headquarter LANs and Region node subnets have a type of 001 which provides the remaining 13 bits for use in the subnet/host portions.

160.106.001x xxxx.xxxx xxxx

b. Smaller Headquarter LANs and typical region LANs will require less than 256 hosts per subnet therefore 8 bits for the host portion (h's) will be sufficient. i.e.

160.106.001s ssss.hhhh hhhh

c. This combination generates a subnet mask of 255.255.254.0, and provides 2^5 subnets of 2^8 hosts or 32 subnets of 256 hosts.

8.5.3 Mission Addressing Structure

a. Mission node subnets have a type of 1xx which provides the remaining 15 bits to be used for subnet/host portions. i.e.

160.106.1xxx xxxx.xxxx xxxx

b. Missions will require less than 128 hosts therefore 7 bits for the host portion (h's) will be sufficient. i.e.

160.106.1sss ssss.shhh hhhh

c. This yields a subnet mask of 255.255.255.128, and allow 2^8 subnets of 2^7 hosts or 256 subnets of 128 hosts.

d. To determine the next mission subnet address increment the s bits, highest bits first. Therefore the mission subnet allocation will be as follows:

Subnet	Address	Dotted Decimal
1st	**160.106.11**ss ssss.shhh hhhh	160.106.192.0
2nd	**160.106.101**s ssss.shhh hhhh	160.106.160.0
3rd	**160.106.111**s ssss.shhh hhhh	160.106.224.0
4th	**160.106.1001** ssss.shhh hhhh	160.106.144.0
5th	**160.106.1101** ssss.shhh hhhh	160.106.208.0

Table 8.2: Mission Subnet Allocation

e. The first host will be numbered starting from the least significant bit, within the host portion or the h bits. Therefore the first few hosts within the first mission subnet will be as follows:

Host	Address	Dotted Decimal
1st	**160.106.11**ss ssss.shhh hhh1	160.106.192.1
2nd	**160.106.11**ss ssss.shhh hh10	160.106.192.2
3rd	**160.106.11**ss ssss.shhh hh11	160.106.192.3
4th	**160.106.11**ss ssss.shhh h100	160.106.192.4
5th	**160.106.11**ss ssss.shhh h101	160.106.192.5

Table 8.3: Mission Host Address Allocation

8.5.4 Serial Links

a. Serial link subnets have been defined as having type of 000. This provides 13 bits to be used for subnet/host portions.

160.106.000x xxxx.xxxx xxxx

b. Serial links will require less than 15 systems connected to them, typically 2. To ensure some growth for technologies, such as Frame Relay, 4 bits will be used for the host portion (h's). Utilizing 4 bits will allow us to connect 15 hosts to the network. If networks, via Frame Relay require more than 15 nodes per connected sub-network technology a portion of the address space from the mission supply can be used. The serial link address has the following format:

160.106.000s ssss.ssss hhhh

c. This yields a subnet mask of 255.255.255.240 , and allow 2^9 subnets of 2^4 hosts or 512 subnets of 16 hosts.

d. The first IP address will be numbered starting from the least significant bit, within the host portion or the h bits. Therefore the 1st connected interface on the 1st serial subnet is listed below. The non contributing bits to the subnet or host are left as s and h but would be set to 0 in these examples.

Subnet	Interface	Address	Dotted
1st	1st	**160.106.0001** ssss.ssss hhh1	160.106.16.1
1st	2nd	**160.106.0001** ssss.ssss hh10	160.106.16.2
1st	3rd	**160.106.0001** ssss.ssss hh11	160.106.16.3
1st	4th	**160.106.0001** ssss.ssss h100	160.106.16.4
2nd	1st	**160.106.0000** 1sss.ssss hhh1	160.106.8.1
2nd	2nd	**160.106.0000** 1sss.ssss hh10	160.106.8.2

Table 8.4: Serial Subnet and Interface Addresses

8.5.5 Subnet and Host Address Allocation

a. To determine the next subnet address of any particular type increment the s bits, highest bits first. With subnets the bit counting is from left to right.

160.106.ttt1 0000. hhhh hhhh
160.106.ttt0 1000. hhhh hhhh
160.106.ttt1 1000. hhhh hhhh

b. Similarly to determine the next host address within the low order bits increment the h bits, starting at 1 and incrementing up, counting right to left.

160.106.ttts ssss.0000 0001
160.106.ttts ssss.0000 0010
160.106.ttts ssss.0000 0011

c. Using this methodology as the host bits and subnet bits approach the remaining bits can be switched from subnet bits to host bits if more hosts are required or vice versa if more subnets are required. This can be achieved without having to re-address all hosts within the subnet or network.

9. SIGNET INTERNETWORK NAMING STRUCTURE

a. A naming plan and a standard naming syntax is an essential step in any network design regardless of size. The ability to determine a network component, its associated information, and its network connectivity rely on a structured naming base and the appropriate tools to manipulate them. In a network naming structure determining the primary network abstraction unit is essential. In terms of SIGNET this level of abstraction is the LAN Manager Domain or in the internetwork realm an IP Subnet. End users and administrators will view themselves as part of a LAN Manager Domain.

b. Network elements within the LAN Manager Domain are named to provide a finer level of granularity within the LAN Manager Domain. The overall network path of an end user from their desktop machine to a remote network service is not determined by any component name but rather the surrounding tool set which identifies connections between named network entities. In order to provide the appropriate tools the underlying naming structure needs to be in place.

c. SIGNET network tools will need to be in the form of a Database Management Systems (DBMS) and will incorporate the appropriate information of each of the network elements and computer equipment within SIGNET. Network operations personnel will need appropriate interfaces to the DBMS system in order to determine logical network connectivity within SIGNET. These tools should provide features such as network topology diagrams, concentrator utilization counts etc.

9.1 Backbone Naming Architecture

a. A network backbone, or LAN Manager Domain is logically defined as the highest layer of a Local Area Network. In a "tree diagram" of network components it is defined as being the "root of the tree". All network hubs, routers and end stations are connected via this "root". The routers provide interconnection of backbones.

b. An actual physical backbone may be, in the case of a single concentrator network, the concentrator's backplane or, in the case of a high utilization backbone, the backplane bus of a multi-port bridge.

c. The number of backbones per location will vary depending upon whether the site is a mission, region or headquarters. A backbone naming structure must allow for numerous backbones per location, as illustrated in Figure 9.1 for the London regional location. The naming architecture must include labeling of the physical location to enable determination of which location a specific backbone is in. A concise naming structure is essential in order to incorporate any hierarchical naming into the names of backbone connected devices.

d. Each site, region and mission currently has an associated 3-5 letter mnemonic with it. These names such as BONN, LDN can be utilized for the primary backbone name. A simple 2 digit numeric suffix will be used to distinguish between the backbones, i.e. BONN01 and BONN02. These names in turn will be associated with a LAN Manger Domain but for internal tracking purposes will have a layer of abstraction between LAN Manager Domain and IP Subnet Name. i.e.

Subnet Address	Subnet Name	LAN/MAN Domain Name
160.106.192	BONN01	BONN.TRADE

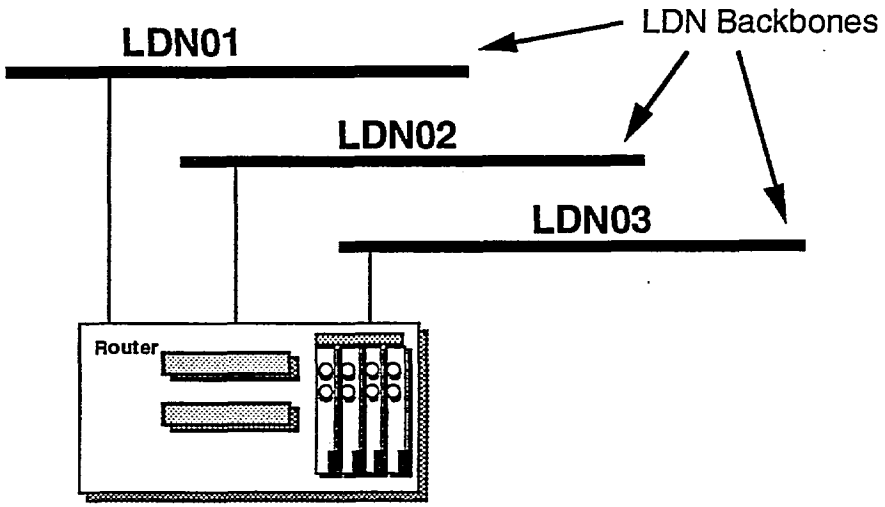


Figure 9.1: Backbone Naming for London Region

9.2 Intermediate Systems - (Routers)

a. Routers are attached to multiple backbones and Wide Area subnetworks. Routers reside in a single physical location, and therefore can have a geographic component within their naming convention. As with backbones, there may be multiple routers per location and the routers require a numeric component within their naming schema. Figure 4 demonstrates the geographic location, R (router) and a 2 digit numeric numbering sequence.

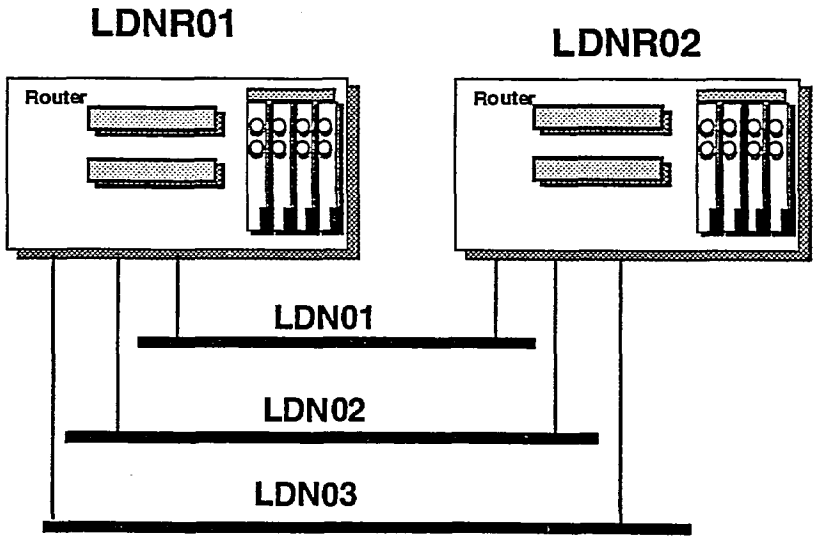


Figure 9.2: Router Naming Scheme

b. Routers have several access points to the network. Each interface has an IP address associated with it. In order to reach a router through a specific interface each interface must have an associated address and name with it. Figure 9.3 demonstrates the naming convention of a router and its associated interface addresses. Figure 9.4 outlines the naming of both the WAN and LAN ethernet ports of a multi-homed router. The convention of appending a w (WAN) and e (Ethernet) has been adopted for port naming.

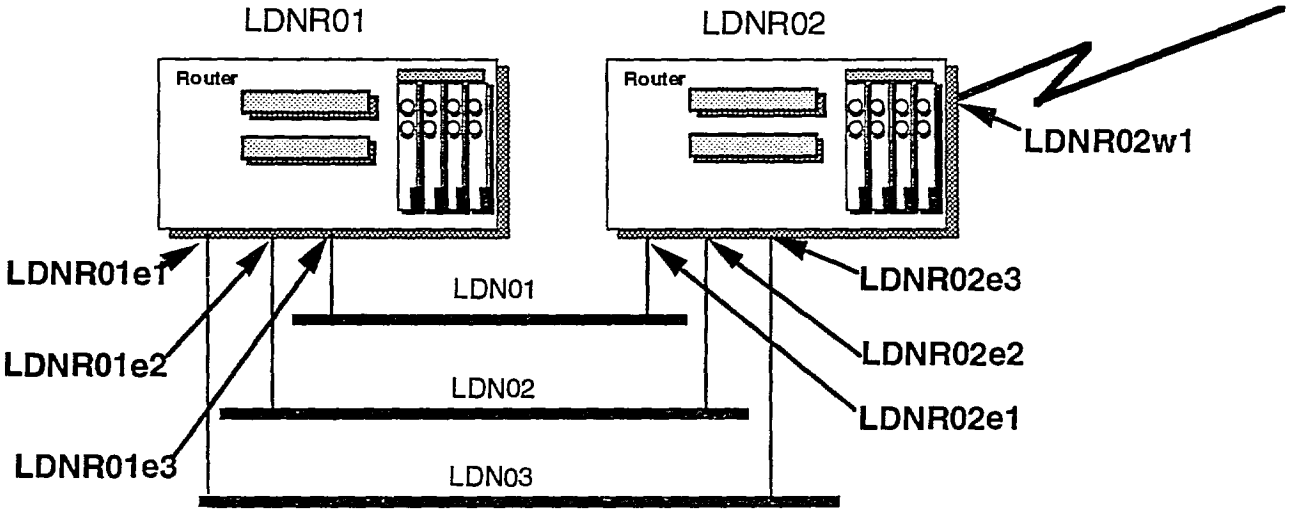


Figure 9.3: Router and Interfaces Naming Architecture

c. In assigning an IP address to routers with multiple Local Area Network interfaces assigning a consistent HOST portion, across Router Interfaces, assists network personnel in their daily operations. Consistent host address allocation is possible by reserving portions of the host address space. Hosts addresses 1 - 9 on all subnets are reserved for router connectivity.

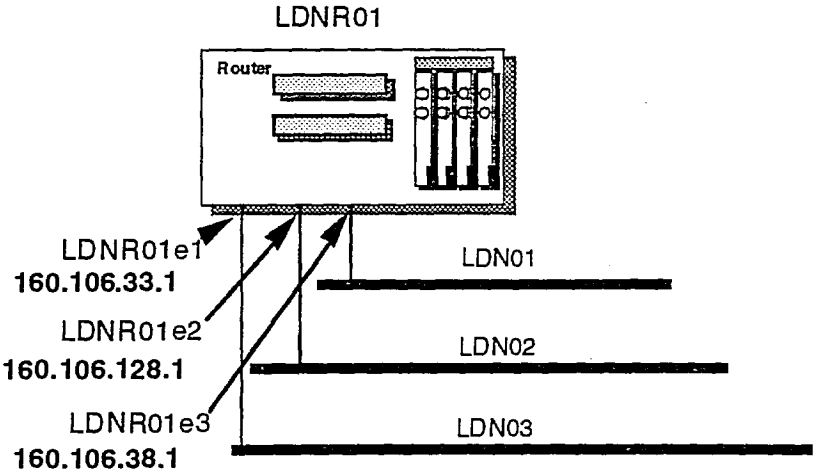


Figure 9.4: Router and Multiple LAN Interfaces

d. To date, IP addresses 1 - 9 have been reserved for Router interfaces, and 10 - 19 for locally attached LAN Manager Servers within the subnet. The end system host address portion should be equal to or greater than 20.

9.3 Concentrators

a. The primary building block of SIGNET's Local Area Networks will be the concentrator. Concentrators provide the necessary connectivity from the user's desk to the backbone and subsequently the SIGNET WAN environment. Due to the various configurations of concentrators, (single 12-port boxes, multiple chassis, several cards per chassis) a naming structure for concentrators should relate to the implementation of the device. A port should be easily identifiable as port 2 on card 3 via its associated name. Closer examination of the concentrator naming schema must be performed upon award of the Network Elements standing offer.

b. In order to meet the distance requirements of the structured cabling, a 2 level hierarchical structure of concentrators will generally be deployed with a primary concentrator providing connectivity to secondary concentrators which in turn provide connectivity to end systems. Some locations, depending on their requirements, will have service via a primary concentrator only.

c. In order to distinguish between a primary and secondary concentrator the prefixes P and S will be used followed by a 3 digit numeric. These 3 digits will provide a counter for incrementing the primary and secondary concentrator counts. This P/S prefix and 3 digit counter will provide a unique naming convention within the SIGNET Enterprise Network. Management of the naming architecture and logical network location will be a necessary function of the network elements inventory tracking system.

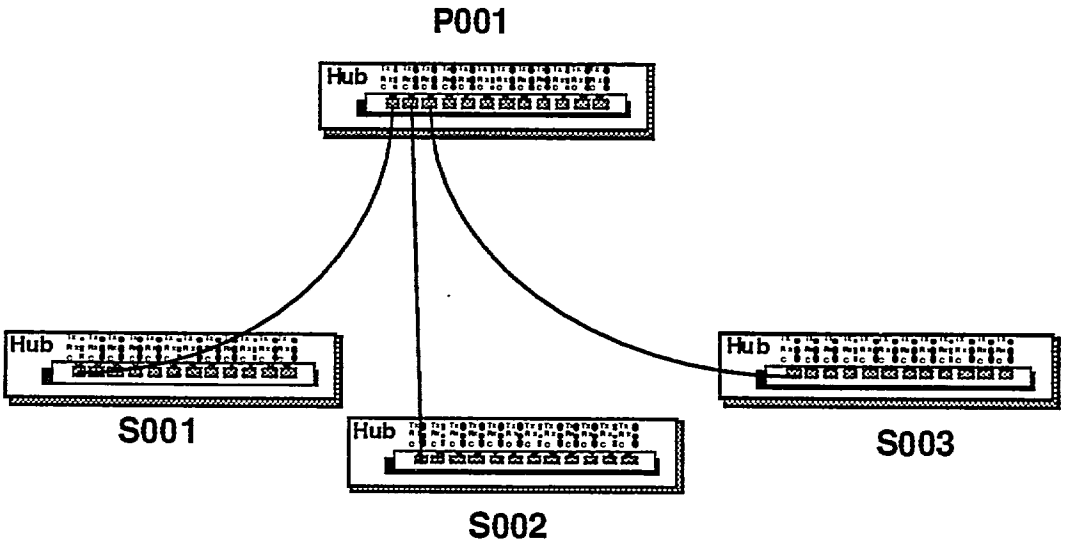


Figure 9.5: Primary/Secondary Concentrator Naming

d. Most managed concentrator devices will have only one IP address associated with it. In the case of multiple IP addresses per managed concentrator the ability to associate an IP address with a specific port may be necessary. An additional numerical suffix, in the case of 12 port hubs, 2 digits, will be necessary. Maintaining consistency with the router naming convention an additional e (for LAN Ethernet) and 2 digit numeric sequence is appended to the name.

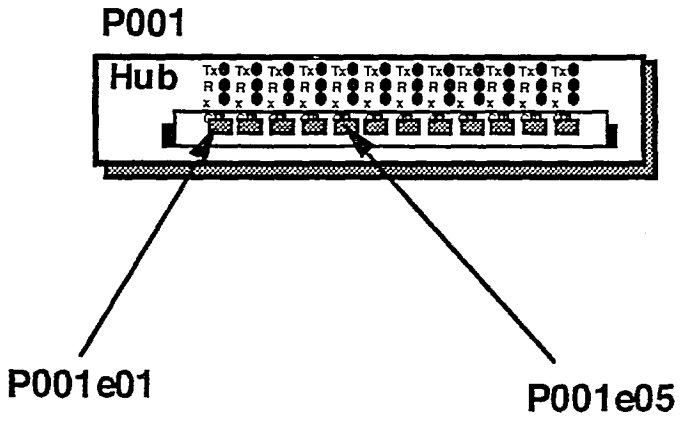


Figure 9.6: Primary Hub with Named Ports

e. To determine network connectivity, vendor reports, hardware addresses, and other pertinent information network personnel will use information tools with the globally unique concentrator name to determine this information.

9.4 Network Equipment

9.4.1 Network Diagnostic Equipment

a. Equipment such as portable Network Analyzers will require numerous IP addresses, one for each subnet that it may be come attached to. This will ensure the ability to use various network utilities such as file transfer to other hosts within SIGNET when attaching the Network Analyzer to different subnets. Maintaining a unique HOST Portion within all subnets in a location, similar to the Router Interfaces, would be advantageous to network personnel.

9.5 Terminal Servers

a. Terminal Servers may require a block of addresses to be allocated by the individual box. The allocation of such IP addresses in this matter is a function of the IP address database management application and not the naming. The naming of a terminal server can simply be the location followed by a T designator and a 2 digit numeric sequence. i.e. LDNT01

9.6 Bridges

a. The following naming convention can be utilized for all types of bridges:

   i. Remote Bridges
   ii. Local 2-port Bridges
   iii. Multi-port Bridges

b. The role of bridges has not yet been finalized within SIGNET. Multi-port bridge deployment within large SIGNET backbones may provide a greater application traffic throughput. It's ability to provide this greater bandwidth is dependent on existing traffic loads and patterns. A more detailed application traffic analysis within the SIMCENTRE would provide some of the details necessary to determine multi-port bridge requirements.

c. A generic naming structure for bridges is included here. A simple structure, similar to the concentrators, provides the necessary functionality. A prefix of B followed by 3 a digit number provides the necessary naming capability with the designator e for LAN ethernet ports and w for WAN ports, if remote bridges are used within SIGNET. Network connectivity and position within the network hierarchy will need is determined via the proper network management tools.

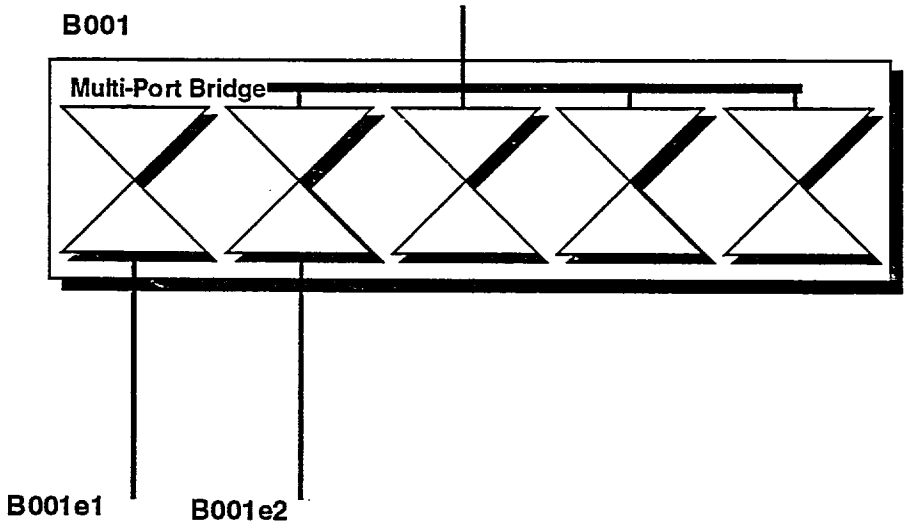


Figure 9.7: Bridge Naming Convention

10. INTERIOR GATEWAY PROTOCOL

a. Interior Gateway Protocols (IGP) allow routers within the autonomous system to share routing information to facilitate end-systems communication within the enterprise network. Industry standard IGPs are limited to Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF). Router vendors who are not utilizing one of these two IGPs will provide a proprietary solution with similar functionality. RIP has major shortcomings for major networks of SIGNET proportions, and while these are currently being addressed in an IAB RIP Version 2 Working Group they will not be commercially available in time for SIGNET deployment. The primary solution for an open, industry standard IGP today is OSPF.

10.1 OSPF Routing Protocol

a. The Open Shortest Path First (OSPF) routing protocol is an Internet Architecture Board (IAB) standard developed by the Internet Engineering Task Force (IETF). OSPF Version 2 is defined by the Network Working Group in Request for Comments (RFC) 1247. John Moy, author of OSPF, has published a draft update to RFC 1247, as of April, 1992. Current versions based on the RFC 1247 will operate within the SIGNET enterprise network. OSPF is commercially available by the major router vendors.

10.2 OSPF Backbone/Area Configuration

a. OSPF provides a method of splitting an entire Autonomous System (AS) into groups called Areas. An OSPF Area is a contiguous collection of hosts and networks within the AS including any routers which have interfaces connecting to the networks.

b. Each OSPF area maintains a copy of the network topology and associated metrics for each network or host within the area. The remaining topology of the AS is not known within the area and connectivity to other areas is through Area Border Routers which are routers connecting more than one area. Area Border Routers maintain multiple sets of tables, one for each area that it is connected to.

c. The utilization of areas within SIGNET AS will:

   i. Reduce "routing update" traffic between routers as area routing tables are summarized before propagating throughout the AS,

   ii. Provide security such that no exterior routes will enter the AS routing tables

d. SIGNET will be broken into an area per regional node router. Each OSPF area and backbone have a unique identifier known as the Area ID. The Area ID is a unique 32 bit area identifier that identifies a collection of networks and router interfaces. In order to maintain uniqueness amongst area ids the IP subnet number used for the regional node to headquarters node subnet can be utilized for that specific region's Area ID. Figure 10.1 demonstrates a typical Area structure with the Area ID equivalent to the "region to HQ" subnet link subnet.

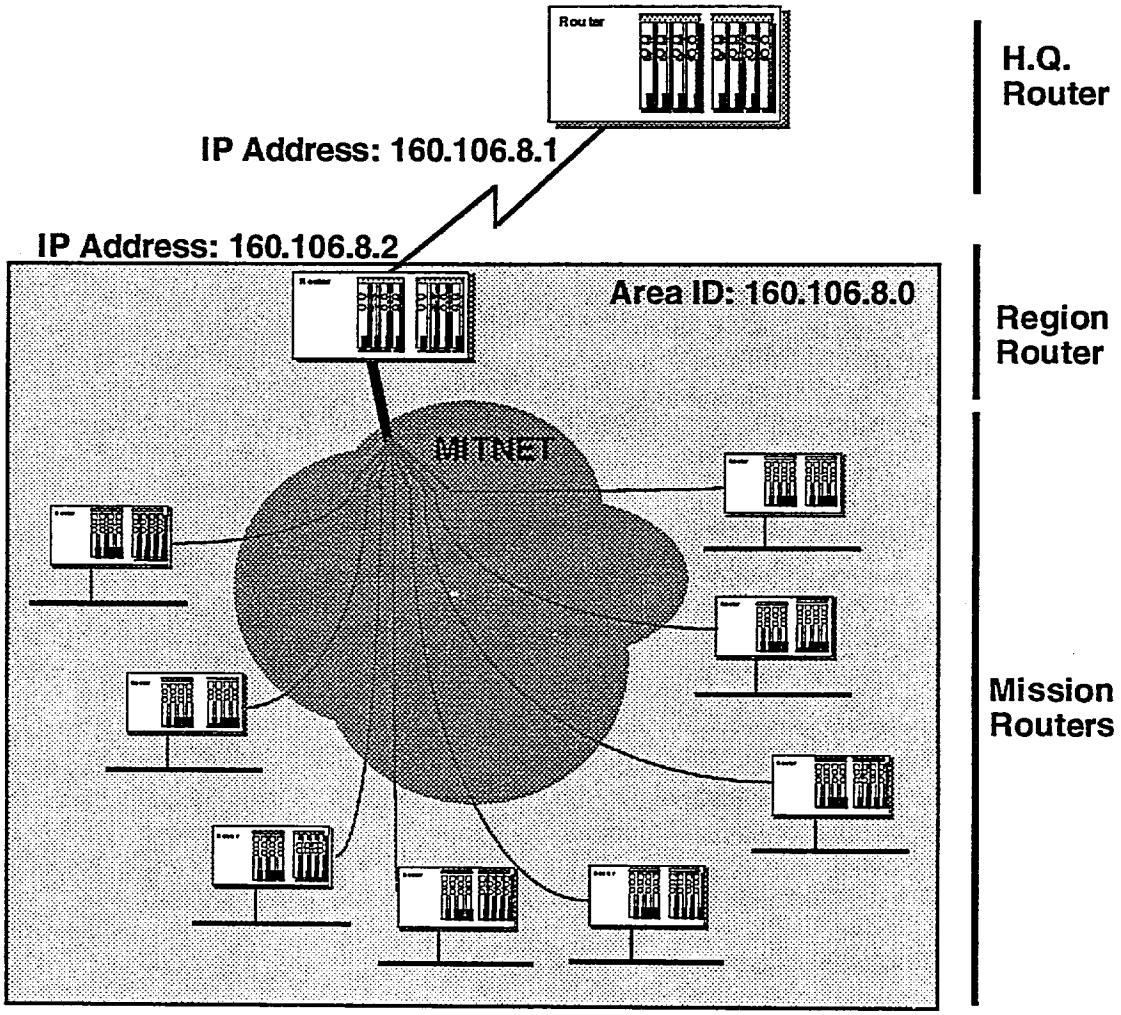


Figure 10.1: Area IDs for SIGNET OSPF Areas

f. Figure 10.2 shows the allocation of several areas and the special backbone Area ID of 0.0.0.0.

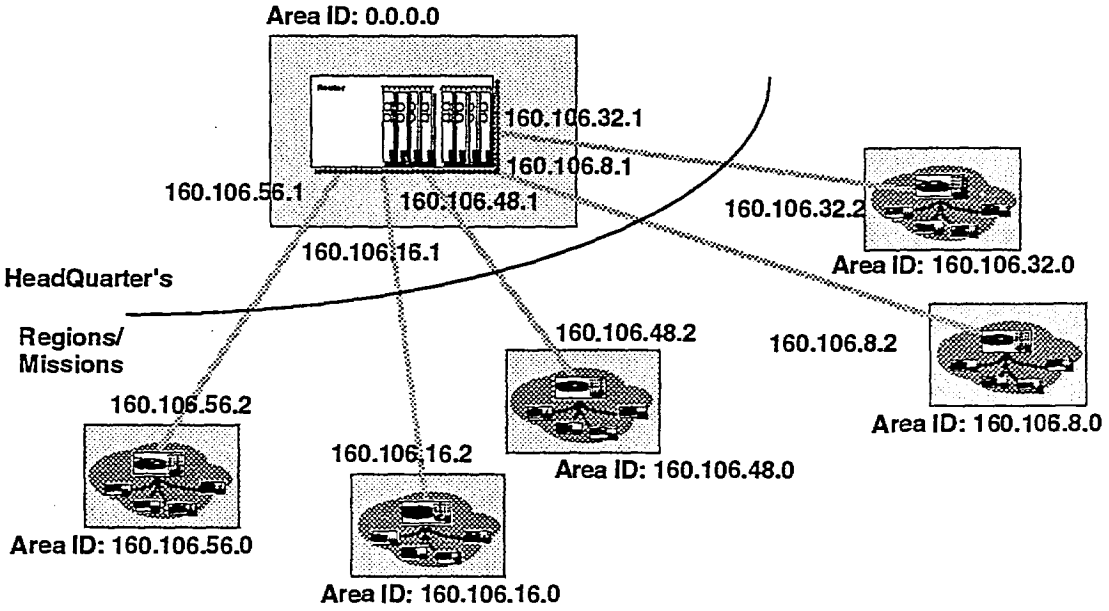


Figure 10.2: OSPF Backbone Area and Regional Area

10.3 OSPF Link Metric

a. The WAN facilities between the region and the mission will be strictly point-to-point and therefore only one path is available. However between regions and headquarters several alternate paths, for redundancy purposes, are available for traffic flow and therefore a least cost metric is useful in determining the proper path.

b. The OSPF routing protocol provides network administrators the facility to associate costs with each router LAN/WAN link. The OSPF routes are determined via a least cost method. Several factors can be used for a costing metric including delay, bandwidth, volume of traffic, or a dollar cost for the leased line. With MITNET provided links the cost metric can be determined as a function of bandwidth to ensure that the higher bandwidth facilities are utilized.

c. Table 10.1 outlines the associated metrics based on the formula assuming a possible implementation of FDDI 100 Mb/s as the highest bandwidth that will be utilized within the SIGNET enterprise network.

$$cost\_metric = \frac{10 \times HBw}{Bw}$$

$HBw \rightarrow$ Highest Bandwidth Feasible (*bits / sec*)

Bw $\rightarrow$ Link Bandwidth (*bits / sec*)

Link Name	Link Speed (bits/sec)	Cost Metric
Serial-SlowSpeed/Dialup	1200	833333
	2400	416667
	4800	208333
	9600	104167
Serial - Region/Mission	19200	52083
Serial - Trunking Lines	56000	17857
	64000	15625
	112000	8929
	128000	7813
	224000	4464
	256000	3906
	448000	2232
	512000	1953
	672000	1488
	768000	1302
Serial - T1	1536000	651
LAN - Token Ring	4000000	250
LAN - Ethernet	10000000	100
LAN - Token Ring	16000000	63
WAN - SMDS	45000000	22
LAN - FDDI	100000000	10

Table 10.1: OSPF Link Metrics

10.4 Security

10.4.1 OSPF Security

a. The OSPF protocol allows for authenticated updates between each communicating router. OSPF provides several layers of security within the routing update datagrams.

b. The OSPF routers can be configured with a simple password to ensure that only SIGNET authorized routers exchange information within the SIGNET Network. The introduction of router passwords provides another level of maintenance and administration within the SIGNET Internetwork.

11. MISSION NODE DESIGN

a. Missions will need to implement several different designs to incorporate the various physical layouts. Missions may have annexes associated with them that will require SIGNET interconnection. These annexes may be located such that an extension of the local area subnetwork within the mission compound is feasible, otherwise a separate leased line, provided by the local telephone company, may be required.

b. The network design for these missions needs to be flexible yet maintain some consistency such that network personnel are able to operate across all missions easily. Figures 10.1 and 10.2 demonstrate possible scenarios for missions.

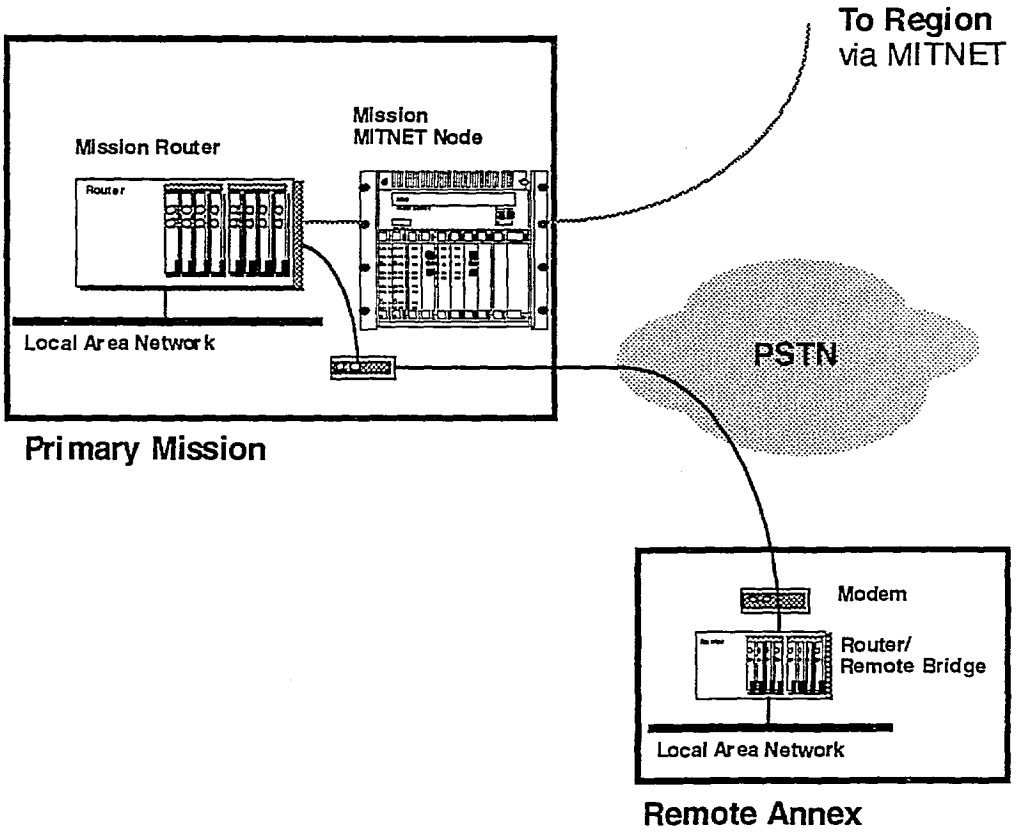


Figure 11.1: Mission Routers and Remote Annex Connection

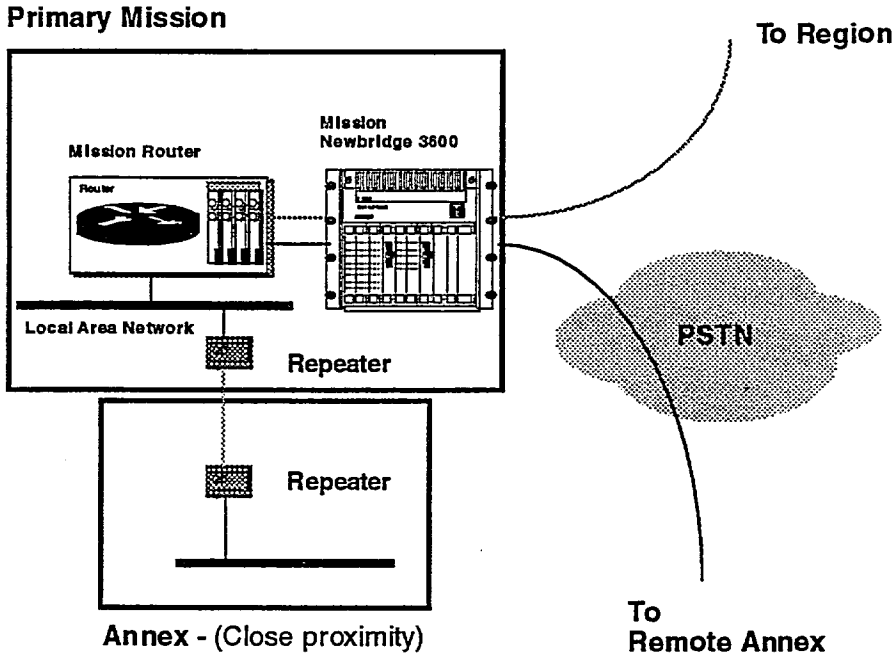


Figure 11.2: Mission Routers and Close Proximity Annex Connection

c. Mission routers will communicate with the region routers via the MITNET Frame Relay Service. The Mission MITNET will not switch the frame relay service but provide a backhauled 19.2 Kbit/s circuit to the region MITNET node. The Frame Relay services is further described in Section 12.0.

11.1 Electrical Specification

a. The region MITNET node and router will be in compliance with the CCITT Recommendation X.21. This recommendation defines the physical characteristics and call control procedures for a general purpose interface between DTE and DCE.

b. The Mission MITNET node and router will be in compliance with the RS-232C/D standards.

c. In the case of a remote annex a PSTN network connection may be needed to implement the desired connectivity. In this case a V.32bis modem with an RS-232C/D connection. Where national PTT standards dictate specific standards then these should be applied.

11.2 Physical Interconnection

a. CCITT Recommendation X.21 defines the mechanical characteristics as being a 15-pin DTE/DCE connector. These characteristics are defined in International Standards Organization (ISO) 4903 document.

12. FRAME RELAY SUBNETWORK TECHNOLOGY

12.1 Permanent Virtual Circuits

a. Utilizing Frame Relay technology as the subnetwork technology will allow the ability to maintain the same number of region/mission connections but reduce the number of physical interfaces on the region router and MITNET equipment.

b. Mission MITNET nodes will not switch the Frame Relay service, via a FRS card, but will backhaul a circuit to the region MITNET node which switch the Frame Relay traffic. Mission routers will run one DLCI/PVC connection back to the region router.

c. The Frame Relay Service (FRS) will be provided with the NewBridge 3600 MainStreet equipment utilizing their FRS card[4]. These card upgrades will be needed for the appropriate region and headquarter MITNET equipment that will be switching the Frame Relay service. Similarly all mission, region and Wide Area Network (WAN) headquarter routers will require a Frame Relay capability.

d. Frame Relay allows us to interconnect several logical Permanent Virtual Circuits (PVCs) over one physical circuit. Current application needs are such that only one logical circuit will be connected from the mission to its respective region router. The region router in turn will have a separate logical connection for every connected mission router, headquarters connection, and one for any other region router that it is connected to.

12.2 IP Subnet Addressing/Frame Relay

a. SIGNET's utilization of Frame Relay will be as a point-to-point subnetwork technology. The current serial link Subnet Addressing Plan allows for the use of up to 15 addresses per serial subnet. During the implementation of the Frame Relay Service if a fully meshed FRS appears, then each node can be a part of one IP subnet.

b. The IP to Data Link Connection Identifier (DLCI) mapping must be a dynamic one performed by the Frame Relay router. Maintaining these entries, in a static fashion, would be yet another administrative process. The process for Inverse ARP over Frame Relay, and IP over Frame Relay are defined in current Request for Comments. RFC 1294 Multiprotocol Interconnect over Frame Relay and RFC 1293 Inverse Address Resolution Protocol define how this Frame Relay service and router interaction is to be performed.

[4] Three NewBridge Frame Relay Service cards have been ordered by MITNET for SIMCENTRE testing purposes.

c. Figure 11.1 shows a region MITNET node with trunking to another region and headquarters. Each of the mission MITNET nodes have a 19.2 Kbit/s circuit backhauled to the region MITNET node providing the FRS.

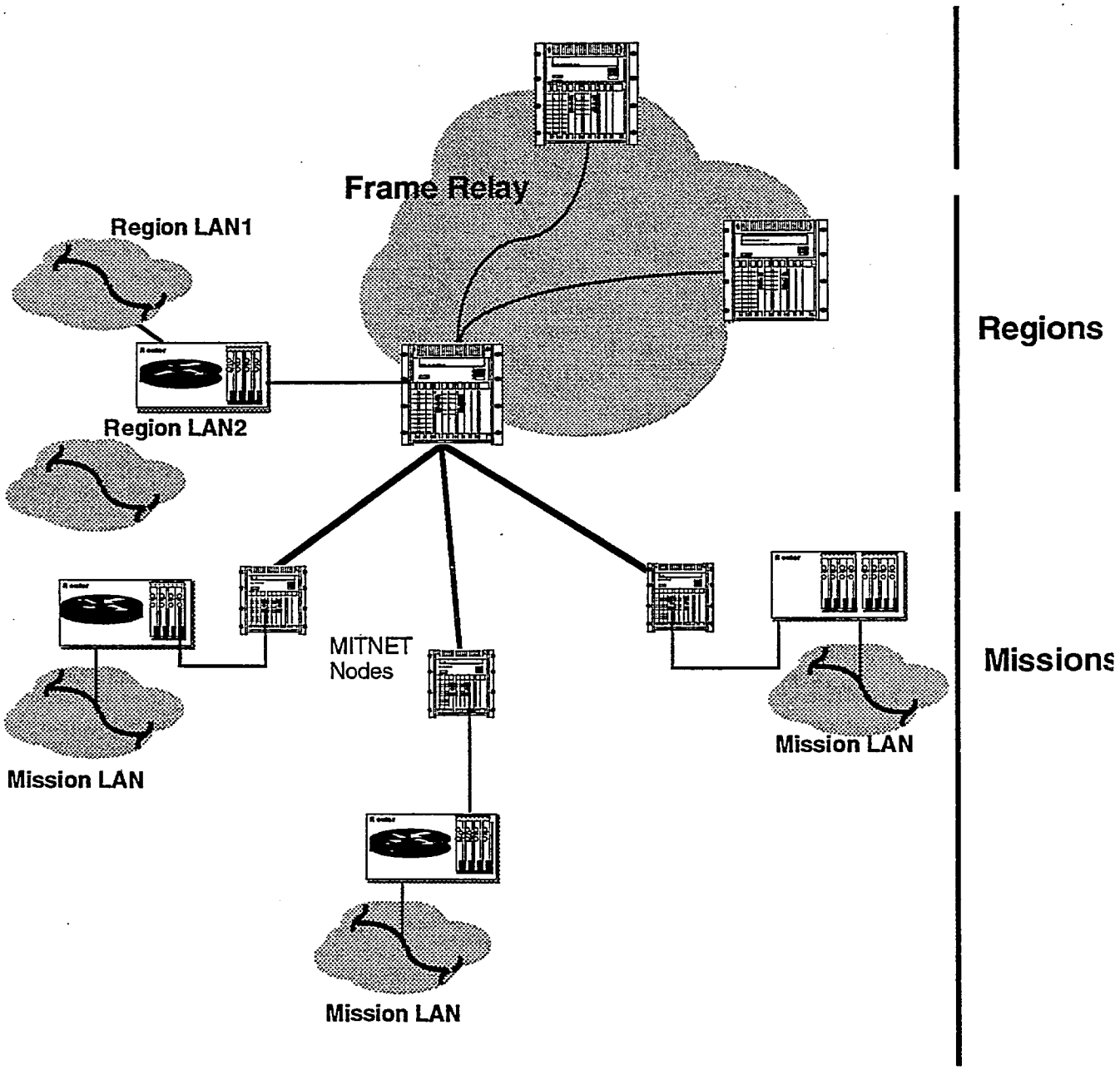


Figure 11.1: Frame Relay Service/MITNET Nodes

13. GENERAL CONNECTIVITY OUTSIDE SIGNET

a. Application investigation is a necessary step within the SIGNET Network Enterprise development to ensure that each application will interoperate over the SIGNET Network.

b. These applications fall into three major categories:

- General Dial-Up Access
- Mainframe Host Connectivity
- Alternative Access

13.1 General Dial-Up Access

a. **Work in Progress.**

13.2 Mainframe Host Connectivity

a. Mainframe host connectivity will be provided via 3270 terminal emulation for those applications.

b. **Work In Progress.**

12.2.1 DSS/SSC On-line Pay Access

12.22 CIDA AIDIS Access

13.3 Alternative Mission Access

a. **Work In Progress**

BIBLIOGRAPHY

[1] External Affairs and International Trade Canada; "SIGNET TACTICAL PLAN"; February 5, 1992

[2] "SIGNET Designated Network; Proposed Implementation Approach; Security"; Glenn Reed (Mike Munroe); Tabled EAITC ; February 21, 1992

[3] External Affairs and International Trade Canada; "Security Requirements For SIGNET Designated LANs"; Version 2.2; January 9, 1992

[4] "SIGNET Designated Network; Draft EDP Security Plan"; Glenn Reed (Mike Munroe); Tabled EAITC ; February 17, 1992

[5] Billinton and Allan; "Reliability Evaluation of Engineering Systems, Concepts and Techniques"; Plenum Press; New York and London; 1983; ISBN 0-306-41296-9

[6] Treasury Board of Canada; Information and Administrative Management; "Information Technology Standards"; Published by Minister of Supply and Services Canada 1991; Available through Canada Communications Group; Ottawa

APPENDIX 1 TRAFFIC ANALYSIS

a. Refer to the following pages.

SIGNET Traffic Estimates
24-Mar-92

The following estimates are averages based per a typical cross section of 100 persons.

Total Number of Persons	100
% of messages Copied to CATS	100%
Protocol Bytes per Packet	40

	% of Person Use	Sessions Per Day Per Person	Sessions Per Day Total	Kbytes Per Session	Kbytes Total	% Remote	Data Remote (kbytes)	Packet Size (Bytes)	Mean Packets	Protocol Overhead (kbytes)	Total Remote (kbytes)	%ofTotal
Electronic Messaging	100%	10	1000	5	5000	50%	2500	512	4883	195	2695	25.1%
CATS (Message Archival)	50%	10	500	5	2500	100%	2500	512	4883	195	2695	25.1%
CATS (File Archival)	20%	0.2	4	25	100	100%	100	512	195	8	108	1.0%
File Transfer / Attach	80%	4	320	25	8000	50%	4000	512	7813	313	4313	40.1%
Facsimile	50%	0	0	20	0	100%	0				0	0.0%
NOCAMS	10%	2	20	4	80	100%	80	128	625	25	105	1.0%
WIN Exports	5%	100	500	4	2000	10%	200	128	1563	63	263	2.4%
CAIPS	5%	100	500	4	2000	10%	200	128	1563	63	263	2.4%
Mission FINEX	5%	10	50	4	200	20%	40	128	313	13	53	0.5%
CIDA Decentralization	5%	10	50	4	200	100%	200	128	1563	63	263	2.4%
				Total	20080		9820		23398		10756	100%

Total	10756
% Busy Hr.	25%
Total Busy Hour	2689
%Busy Minute	5%
Total Busy Minute	134
Throughput	
Kbytes/sec	2.2
kbits/s	18

Terminal Emulation		Characters Per Screen Update (Bytes)	Header Compress	Prot OH/Byte	Local Echo	Total Bytes	Screen Per Min	Bytes Per Min	KBits/Sec	Response Single Sc. (sec)
		1000	yes		4 no	8000	30	240000	32	2
	IP	20								
	TCP	20								

Required Minimum Throughput for Maximum Response Time

		Characters Per Screen Update (Bytes)	Header Compress	Prot OH/Byte	Local Echo	Total Bytes	Maximum Response	Throughput (Kbit/s)
		500	yes		4 no	4000	2	16
	IP	20						
	TCP	20						

Regional to HQ Traffic

Approach: Aggregate all leaf nodes into Ottawa via connected Region node
Assumptions: Under the point to point serial circuit model, the bandwidth available is the sum of the bandwidth available for the individual leaf nodes served.

Regional Node	Sites Served	Total Staff	Expected Volume (KBytes)	Expected Busy Min (KBytes)	Throughput (Kbits/s)
London		339	36462.6	455.8	60.8
	Stockholm	28	3011.7	37.6	5.0
	Helsinki	19	2043.6	25.5	3.4
	Oslo	28	3011.7	37.6	5.0
	Dublin	25	2689.0	33.6	4.5
	The Hague	61	6561.1	82.0	10.9
	Bonn	138	14843.2	185.5	24.7
	Brussels	31	3334.3	41.7	5.6
	NATO	74	7959.4	99.5	13.3
	Hundreds	8		Total	133.2
	n*19.2	153.6			
	Circuit	192		Circuit	192
	#DS-0s	3		#DS-0s	3
	Ratio	144%			144%

Regional Node	Sites Served	Total Staff	Expected Volume (KBytes)	Expected Busy Min (KBytes)	Throughput (Kbits/s)
Paris		216	23232.8	290.4	38.7
	Lisbon	50	5378.0	67.2	9.0
	Geneva	50	5378.0	67.2	9.0
	Vienna	55	5915.8	73.9	9.9
	Madrid	43	4625.1	57.8	7.7
	Berne	35	3764.6	47.1	6.3
	Rome	104	11186.2	139.8	18.6
	POECD	25	2689.0	33.6	4.5
	Hundreds	6		Total	103.6
	n*19.2	115.2			
	Circuit	128		Circuit	128
	#DS-0s	2		#DS-0s	2
	Ratio	124%			124%

Regional Node	Sites Served	Total Staff	Expected Volume (KBytes)	Expected Busy Min (KBytes)	Throughput (Kbits/s)
Washington		335	36032.4	450.4	60.1
	Atlanta	43	4625.1	57.8	7.7
	Boston	43	4625.1	57.8	7.7
	Buffalo	39	4194.8	52.4	7.0
	Chicago	42	4517.5	56.5	7.5
	Cleveland	22	2366.3	29.6	3.9
	Detroit	43	4625.1	57.8	7.7
	Minneapolis	28	3011.7	37.6	5.0
	Hundreds	6		Total	106.7
	n*19.2	115.2			
	Circuit	128		Circuit	128
	#DS-0s	2		#DS-0s	2
	Ratio	120%			120%

Regional Node	Sites Served	Total Staff	Expected Volume (KBytes)	Expected Busy Min (KBytes)	Throughput (Kbits/s)
New York	New York	103	11078.6	138.5	18.5
	Hundreds	2		Total	18.5
	n*19.2	38.4			
	Circuit	64		Circuit	64
	#DS-0s	1		#DS-0s	1
	Ratio	347%			347%

Regional Node	Sites Served	Total Staff	Expected Volume (KBytes)	Expected Busy Min (KBytes)	Throughput (Kbits/s)
San Francisco		31	3334.3	41.7	5.6
	Seattle	43	4625.1	57.8	7.7
	Los Angeles	67	7206.5	90.1	12.0
	Tokyo	180	19360.7	242.0	32.3
	Beijing	112	12046.7	150.6	20.1
	Seoul	65	6991.4	87.4	11.7
	Bangkok	97	10433.3	130.4	17.4
	Manila	130	13982.7	174.8	23.3
	Hong Kong	184	19790.9	247.4	33.0
	Singapore	76	8174.5	102.2	13.6
	Jakarta	91	9787.9	122.3	16.3
	Kuala Lumpur	48	5162.9	64.5	8.6
	Wellington	22	2366.3	29.6	3.9
	Canberra	34	3657.0	45.7	6.1
	Melbourne	8	860.5	10.8	1.4
	Sydney	35	3764.6	47.1	6.3
	Hundreds	13		Total	219.2
	n*19.2	249.6			
	Circuit	256		Circuit	256
	#DS-0s	4		#DS-0s	4
	Ratio	117%			117%

Delay Estimates Ottawa - Tokyo
24/3/92

	19.2 Kbit/s	64 Kbit/s
Total Estimated Round Trip Delay (ms)	**621**	**285**
(Excluding host processing time)		

Link Rate (kbit/s) 19.2

	Data	TCP/IP	HDLC	Total
Test Message	500	40	4	544

Repeater Spacing (km) 40
Repeater Delay (us) 10
Fiber propogation delay (us/km) 5
Propogation Delay = #km*5us/km+#km/40*10us

Ottawa - Washington - San Franciso - Tokyo
Include message length Yes

Link	Distance m	km	Link Speed	Mess Length (ms)	Prop Delay (ms)	One Way	Two Way (ms)
Ottawa - Washington	450	720	19.2	227	4	230	461
Washington - San Francisco	2440	3904	19.2	0	20	20	41
San Franciso - Tokyo	5140	8224	19.2	0	43	43	86
		12848		Add message once			588

Link	Distance m	km	Link Speed	Mess Length (ms)	Prop Delay (ms)	One Way	Two Way (ms)
Ottawa - Washington	450	720	64	68	4	72	144
Washington - San Francisco	2440	3904	64	0	20	20	41
San Franciso - Tokyo	5140	8224	64	0	43	43	86
		12848		Add message once			271

	Throughput (pps)	Switch Delay	Buffer Length (bits)	Transmission Delay 19.2 kbit/s	64 kbit/s
KG			50	3	1
Router core	25000	0.5			
Router leaf	10000	1			
Bridge	15000	0.5			
Concentrator		0.005			
Fiber serial links to KGs		0			
Series Cabling/Connections		0			
Multiplexor (Total Mux / Dmux Buffer Operation)			30	2	0

Network Component	Round Trip Delay Contribution (ms) 19.2 kbit/s	64 kbit/s
Equipment	35	15
Transmission Media	10 ms / 1000 km	

End Points	Distance (km)	Total Round Trip Delay (ms) 19.2 kbit/s	64 kbit/s
Ottawa-Tokyo	13000	165	145
Ottawa-London	7500	110	90
Ottawa-Washin	750	43	23
Paris - Rome	1200	47	27
128 Byte Message Length		53	16

Total Transaction Delays	19.2 kbit/s	64 kbit/s
Ottawa-Tokyo	218	161
Ottawa-London	163	106
Ottawa-Washington	96	39
Paris - Rome	100	43

Network Element Delay

	One Way 19.2 kbit/s	64 kbit/s	Two Way 19.2 kbit/s	64 kbit/s
Dl(ms)	2	2	4	4
Dr(ms)	17	7	33	14

Dl=Dc*4+Db*2+Drl+Dw*8
Dr=Dc*4+Db*2+Drl+Drc*2+Dkg*4+Dmc+Dml+Dw*8+Df*4
Dmc + Dml = Dms*2 (Dms = Mainstreet Mux/Demux Operation)

Maximum Transactions Per Second Per Session
(Host processing not included, no network congestion)

	19.2 kbit/s	64 kbit/s
Ottawa-Tokyo	5	6
Ottawa-London	6	9
Ottawa-Washington	10	26
Paris - Rome	10	23

APPENDIX 2 AVAILABILITY ANALYSIS

a. Refer to the following pages.

SIGNET Internetwork Availability Analysis
21-Aug-92

Definitions

The SIGNET service is defined to be unavailable when any given
user cannot access any desired resource anywhere in SIGNET.
The SIGNET Internetwork service is defined to be unavailable when the outage
perceived by the user is due to an outage in the internetwork.
and not by an outage in the end systems involved in the desired service.
Therefore, the SIGNET Internetwork availability objectives exclude the availability of end systems.
The SIGNET availability objective is divided into two parts:
1) Both end systems are within the same local subnetwork environment with no
traversal of the wide area subnetwork required.
2)The two end systems are in different subnetwork environments with a traversal
of the wide area subnetwork required.

Assumptions

Number of Missions	120		
Hours Per Year	8760	Per Month	730
Minutes Per Year	525600		
Work Week (Hrs)	37.5		
%Usage of network	100%		
% Local Access	70%		
% Remote Access	30%		
Pn	0%		
Pl	70%		
Pr	30%		
Total	100%		
MTTR (hrs)	2		

MITNet Leaf Outage

Base data: 80% of leaf nodes experience an outage of 6 hours per month.
Assume: MTTR = 6 hrs MTTF = 1 month
** Used MTTF of 6 months for following analysis.

	MTTR (hr)	MTTF (m)	Availability	Outage (hrs/yr)	%Repair	Population	Repair Actions Per yr	Repair Actions Per mth	Device Failures	Spares
MITNet Core	4	24	99.9772%	2.0	50%	1	0.5	0		1
MITNet Leaf	6	6	99.8632%	12.0	200%	120	240.0	20		120
Router core	2	24	99.9886%	1.0	50%	6	3.0	0	0	6
Router leaf	2	24	99.9886%	1.0	50%	120	60.0	5	5	120
Bridge	2	24	99.9886%	1.0	50%	20	10.0	1	1	20
Concentrator	2	24	99.9886%	1.0	50%	660	330.0	28	28	660
Router - Mitnet Series Cabling	2	60	99.9954%	0.4	20%	126	25.2	2		126
UTP Series Cabling	2	60	99.9954%	0.4	20%	10000	2000.0	167		10000
Mission Power	1	6	99.9772%	2.0	200%	120	240.0	20		120
HQ Power	0.25	6	99.9943%	0.5	200%	1	2.0	0		1
								242	34	

Calculations (Using Lower Table)

	Availability	Outage (hrs/yr)	(hrs/m)	(min/wk)	MTTF (m)	MTTF (wks)
Local Internetwork Access	97.76%	196.0	16.3	226	0.1	1
Wide Area Internetwork Access	96.69%	289.6	24.1	334	0.1	0
Probability of Success	97.44%	224.1	18.7	259	0.1	0

Al=Ac4*Ab2*Arl*Aw8*Ap
Ar=Ac4*Ab2*Arl*Arc2*Amc*Aml*Aw8*Aws4*Apm*Aph
Ar=Al*Arc2*Akg2*Amc*Aml*Af4

Ps=PlAl+PrAr+Pn

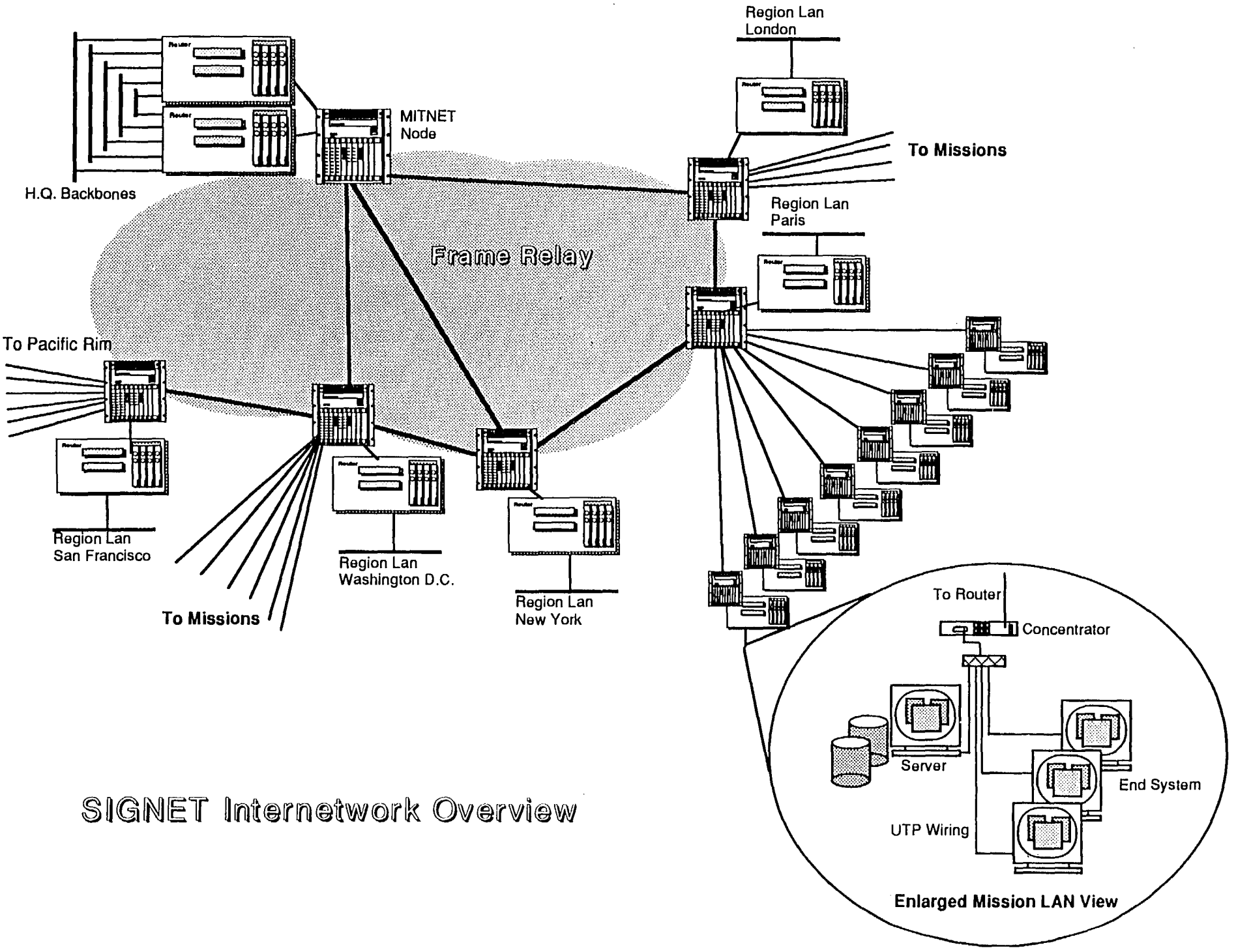
Sparing Considerations

Sparing estimates begin with an availability objective and with known FIT rate, repair rate, and population the sparing level can be determined.

	Objective Outage hrs/mth	Availability	MTTF (mth)	MTTR (hrs)	Population	Spares	% Spares
MITNet Core	0.25	99.97%	60	2	1	N/A	N/A
MITNet Leaf	6	99.18%	4	4	120	N/A	N/A
Router core	0.25	99.97%	24	2	6	2	33%
Router leaf	2	99.73%	36	24	120	40	33%
Bridge	2	99.73%	36	24	20	7	33%
Concentrator	2	99.73%	36	24	660	219	33%
Router - Mitnet Series Cabling	0.25	99.97%	60	2	126	17	13%
UTP Series Cabling	0.25	99.97%	60	2	10000	1333	13%
Mission Power	0.5	99.93%	6	1	120	N/A	N/A
HQ Power	0.25	99.97%	6	0.25	1	N/A	N/A
Generic Device	7.5	98.97%	24	4	100	2	2%

APPENDIX 3 SIGNET NETWORK OVERVIEW

a. Refer to the following page.



SIGNET Internetwork Overview

LIBRARY E A/BIBLIOTHEQUE A E
3 5036 20042366 6

DATE DUE

FEB 2 2005