NASA/CR—2000-209781

Protocol Architecture Model Report

Chris Dhas
Computer Networks and Software, Springfield, Virginia

January 2000

The NASA STI Program Office . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the Lead Center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA's counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.
- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.
- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.
- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.
- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.
- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that complement the STI Program Office's diverse offerings include creating custom thesauri, building customized data bases, organizing and publishing research results . . . even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at ***http://www.sti.nasa.gov***
- E-mail your question via the Internet to help@sti.nasa.gov
- Fax your question to the NASA Access Help Desk at (301) 621-0134
- Telephone the NASA Access Help Desk at (301) 621-0390
- Write to:
NASA Access Help Desk
NASA Center for AeroSpace Information
7121 Standard Drive
Hanover, MD 21076

NASA/CR—2000-209781

Protocol Architecture Model Report

Chris Dhas
Computer Networks and Software, Springfield, Virginia

Prepared under Contract NAS3–99165, Task 1

National Aeronautics and
Space Administration

Glenn Research Center

January 2000

Available from

NASA Center for Aerospace Information
7121 Standard Drive
Hanover, MD 21076
Price Code: A04

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22100
Price Code: A04

In-Space Internet Node Technology Development Project
Protocol Architecture Model Report

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Section **Page**

List of Figures

List of Tables

1. INTRODUCTION

NASA's Glenn Research Center (GRC) defines and develops advanced technology for high priority national needs in communications technologies for application to aeronautics and space. GRC tasked Computer Networks & Software Inc. (CNS) to examine protocols and architectures for an In-Space Internet Node. CNS has developed a methodology for network reference models to support NASA's four mission areas:

- Earth Science
- Space Science
- Human Exploration and Development of Space (HEDS)
- Aerospace Technology

This report applies the methodology to three space Internet-based communications scenarios for future missions. CNS has conceptualized, designed, and developed space Internet-based communications protocols and architectures for each of the independent scenarios. The scenarios are:

- Scenario 1: Unicast communications between a Low-Earth-Orbit (LEO) spacecraft in-space Internet node and a ground terminal Internet node via a Tracking and Data Relay Satellite (TDRS) transfer.

- Scenario 2: Unicast communications between a Low-Earth-Orbit (LEO) International Space Station and a ground terminal Internet node via a TDRS transfer

- Scenario 3: Multicast Communications (or "Multicasting")
  - 1 Spacecraft to N Ground Receivers
  - N Ground Transmitters to 1 Ground Receiver via a Spacecraft

2. METHODOLOGY FLOWCHART

Developing a protocol architecture is a complex process because of the number of choices available to the designer. The complexity is magnified as each of the design choices is interrelated to several others. Therefore, any methodology that is developed is going to be, at least in part, an artificial structuring of a complex iterative process. An unique protocol architecture methodology does not exist. Figure 1 shows the steps that will be used in this document in developing the protocol architecture for each of the scenarios provided by GRC.

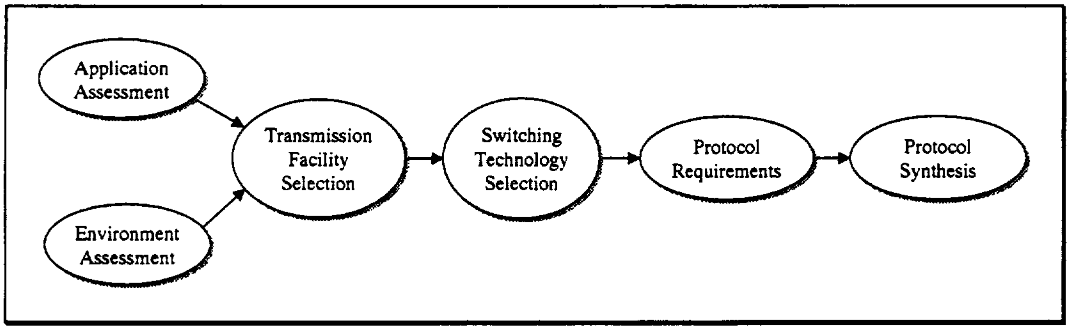

Figure 1. Protocol Architecture Methodology Steps

3. SPACECRAFT APPLICATIONS

The first step in the process is application assessment. It starts with identifying the applications to be supported and their communications related characteristics. A set of applications (Table 1) has been developed to support the protocol architecture development process for the three scenarios. The applications are grouped by categories. The application types within a category are consolidated in Table 2 and their characteristics are aggregated. The three scenarios use the data from Table 2 as a starting point for application requirements. (The definitions of the application characteristics follows Table 2.)

Table 1. NASA Data Application Requirements

Application Category	Types	Transfer Unit (1)	Response Time	Bandwidth Requirements(2)	Precedence	Integrity	Availability	Security	Scalability
Command and Control	Pilot/Controller	Small Async Frequent	1-3 Sec	64 Kbps	High	High	99.999	A+E+C	1-100 Slow
	Mission Coordination	Small Async Frequent	1-3 Sec	64 Kbps	High	High	99.9	A+E	1-1000 Moderate
	Routine	Small Async Frequent	1-3 Min	64 Kbps	Medium	Medium	99.9	E	1-100 Moderate
Telemetry/Navigation	Flight Path Control	Small Async Frequent	1-3 Sec	64 Kbps	High	High	99.999	A+E+C	1-100 Slow
	System Status Monitoring	Medium Sync Continuos	1-3 Min	128 Kbps	Medium	Medium	99.9	NR	1-100 Moderate
	Equipment /Component Monitoring	Medium Async Frequent	1-3 Min	128 Kbps	Medium	Medium	99.9	NR	1-10000 Moderate

Application Category	Types	Transfer Unit (1)	Response Time	Bandwidth Requirements(2)	Precedence	Integrity	Availability	Security	Scalability
Emergency/Flight Critical	Collision Avoidance	Small Async Infrequent	1-3 Sec	64 Kbps	High	High	99.999	NR	1-100 Slow
	"Mayday"	Small Async Infrequent	1-3 Sec	64 Kbps	High	High	99.999	NR	1-100 Slow
Experiment Support/ Mission Pay Load	Data Collection (Real-time)	Large Sync Continuous	10-20 Min	10 Mbps	Medium	Medium	99.95	NR	10-100000 Moderate
	Data Collection (Store and Forward)	Large Async Continuous	> 1 Hr	10 Mbps	Medium	Medium	99.95	NR	10-100000 Moderate
	Interactive	Medium Async Frequent	1-3 Min	1 Mbps	Medium	Medium	99.99	A	1-1000 Moderate
	Process Control	Small Sync Continuous	< 1 Sec	1 Mbps	High	High	99.99	A+E	1-100 Slow

Application Category	Types	Transfer Unit (1)	Response Time	Bandwidth Requirements(2)	Precedence	Integrity	Availability	Security	Scalability
System/Vehicle Maintenance	System Diagnostics	Large Async Medium	10-20 Min	1 Mbps	Medium	Medium	99.9	NR	1-100 Slow
	Event Reports	Small Async Frequent	1-3 Min	128 Kbps	Medium	Medium	99.9	NR	1-1000 Fast
	Testing	Large Async Medium	10-20 Min	1 Mbps	Medium	Medium	99.9	NR	1-100 Fast
	Software Upgrades	Large Async Medium	10-20 Min	10 Mbps	Medium	Medium	99.99	NR	1-1000 Slow

Application Category	Types	Transfer Unit (1)	Response Time	Bandwidth Requirements(2)	Precedence	Integrity	Availability	Security	Scalability
Administrative	Routine Crew	Medium Async Medium	1-3 Min	64 Kbps	Medium	Low	99.9	NR	1-1000 Moderate
	Supply	Medium Async Medium	10-20 Min	128 Kbps	Low	Low	99.9	NR	1-1000 Moderate
	Planning	Medium Async Medium	10-20 Min	128 Kbps	Medium	Low	99.9	A+E	1-1000 Moderate
Entertainment	Video etc.	Large Async Frequent	NA	10 Mbps	Low	Low	99.9	NR	1-1000 Fast

Table 2. NASA Data Applications Category Requirements Summary

Application Category	Transfer Unit	Response Time	Bandwidth Requirements	Precedence	Integrity	Availability	Security	Scalability
Command and Control	Small Async Frequent	1 - 3 Sec	256 Kbps	High	High	99.999	A+E+C	1-100 Slow
Telemetry/Navigation	Medium Sync Continuous	1 - 3 Sec	512 Kbps	Medium	High	99.99	E	1-10000 Moderate
Emergency/Flight Critical	Small Sync Infrequent	1-3 Sec	64 Kbps	High	High	99.999	NR	1-100 Slow
Experiment Support/ Mission Payload	Large Async Continuous	10-20 Min	10 Mbps	Medium	Medium	99.99	NR	10-10000 Moderate
System/Vehicle Maintenance	Large Async Medium	10-20 Min	1 Mbps	Medium	Medium	99.9	NR	1-1000 Fast
Administrative	Medium Async Frequent	1-3 Min	1 Mbps	Low	Low	99.9	NR	1-1000 Moderate
Entertainment	Large Async Frequent	NA	10 Mbps	Low	Low	99.9	NR	1-1000 Fast

Application Table Definitions

The following is the definition of the terms and parameters used to categorize the NASA Applications. The definitions are provided in order of reading left to right across the heading row of Table 1.

Application Category. The requirement for information exchange between the space platform and the earth-based organizations has been decomposed into a set for top level functional groupings. Each category represents a major area of similar functions or processes involved in the interactions requiring the use of a data link to perform the function. The applications may be current or envisioned as future processes. Although voice applications are not included in this analysis, the equivalent interactions done using digital messaging is included (e.g., command and control which is similar to the data link functions of Controller Pilot Data Link Communications of the future FAA Air Traffic Management System).

Type. Used to describe a specific function or process.

Transfer Unit. This parameter describes the size, event timing and the persistence of the data that is transferred over the data communication link. For each type the entry in the column is:

Top = Size
Middle = Event Timing
Bottom = Persistence

Size has been defined as:

Small - The total message (information exchange data) is between 1 to 1,000 Bytes per event.

Medium - The message is between 1,001 to 50,000 bytes

Large - The message is greater than 50,001 bytes and is nominally probably 3 to 5 Megabytes.

Event Timing. This provides an indication of the occurrence of the data to be communicated. The parameter is defined by:

Async (Asynchronous). The event requiring the transmission of data is based upon a demand that occurs at random intervals.

Sync (Synchronous). The event requiring the transmission of data occurs at fixed intervals. This is coupled to precise clock synchronization.

Persistence. This parameter describes, in general terms, the load presented to the data transfer mechanism. Thus, it indicates the attention level that must be given to the data by the transfer mechanism. The persistence (loading) is described by:

Infrequent. The need to communicate data is seldom.

Frequent. It is expected that the need to communicate data is regular but contains periods of inactivity.

Medium. The need to transfer data is less than frequent but more than infrequent.

Continuous. The need to transfer data is continuous without any periods of inactivity.

Response Time. This is the time between the transmission of information and the receipt of a response that action has been taken or the receipt of the information requested by the original transmission. For this analysis, response time is indicated in four levels, which are:

Level 1 = 1 - 3 Seconds.
Level 2 = 1 - 3 Minutes
Level 3 = 10 - 20 Minutes
Level 4 = Greater than one hour

Bandwidth Requirement. The estimated channel bandwidth in terms of bits per second that would accommodate the information transfer.

Precedence. In a mixed application environment where the functions share resources (e.g., the same channel), this is the requirement to give priority to a given data transfer over that of another function. In this case, traffic ranked as high will be handled before that ranked as medium, which in turn is handled before that ranked as low.

Integrity. The integrity level indicates the need for error free data transfer. This is also an estimate of the trust placed in the accuracy of the received data. In general, a rating of high would be equal to an undetected error rate of less than 1 error in 10 gigabits of data. Low would indicate 1 undetected error or less in 100 kilobits.

Availability. The availability is the percent of time that the communication channel must correctly operate and be "available" per unit of time. Thus, an availability of 99.999 means that in one year the channel would be "unavailable" (down) for less than six minutes.

Security. Security is the requirement to protect the privacy of the data and reveal it only to authorized people or processes. The requirement also includes the need to prevent being denied the receipt of the data to due covert actions or the interference of others. The requirement is stated by defining the type of security measures expected to be taken to secure the data transmission. This is defined by:

A = Authentication techniques which provide for confirmation that the true sender and receiver are connected. These may be passwords or certificate style (e.g., PKI) mechanisms.

E = Data Encryption is required to prevent disclosure of the "plain" data content.

C = The taking of active countermeasures may be necessary in other to prevent denial of service (e.g., by the use of anti-jamming encoding schemes or redundant channels).

NR = Not Required. The need for secure communications is not considered necessary for the application type.

Scalability. This factor describes the predicated growth in the required communication to support the application type. The description is in terms of the multiplier (or increase) of bandwidth and in the rate of increase.

For example, in the Application Category of "Command and Control" for the Type "Pilot/Controller", it could be expected that the communications requirement could grow from 1 to support up to 100 small spacecraft. However, this growth rate would be expected to be "slow".

The use of the ratings of slow, moderate and fast corresponds roughly to the following time periods.

Slow = 5 - 10 years
Moderate = 4 - 5 years
Fast = less that 4 years.

Since space communications require long life times, it is expected that the capacity to allow for growth will be a factor in the overall design.

In broad terms, the scalability parameter is an indication of the growth reserve that would be built into the initial communications architecture.

4. SCENARIO 1: LEO SPACECRAFT ↔ TDRS ↔ GROUND TERMINAL

This scenario is for unicast communications between a Low-Earth-Orbit (LEO) spacecraft in-space Internet node and a ground terminal Internet node via TDRS transfer. The types of LEO spacecraft considered are small/unmanned (such as for telecommunications), large/unmanned (such as the Hubble Space Telescope), and large/manned (such as the Space Transportation System). This scenario assumes that the traffic is purely only data communications related.

4.1. NASA Application Types and Characteristics

The existing NASA application categories with the associated application types and their respective characteristics are shown in Table 3. The characteristics form the basis for assessing the protocol functional requirements at each layer in the protocol stack for the applications to be supported. (The Load Factor column in Table 3 is an assessment of the number of times (over the baseline case in Table 2) that the bandwidth should be multiplied to reflect the scenario.) The applications vary from command and control to administrative. The table shows that majority of the applications do not require security. The response time range is from seconds to minutes. The bandwidth requirement range is from 1 Mbps to 10 Mbps. The precedence levels range from high to low. In addition, message integrity ranges from high to low. The availability is spread over 0.999 to 0.99999.

The bandwidth requirement ranges from Kbps to Mbps. It is dominated by Experiment Support/Mission Payload applications. The total daily traffic is found by summing the column defined as the total bandwidth requirements. The peak hour load to be supported by the system is 15% of the total daily traffic. The peak hour load is 1.92 Mbps.

Table 3. Scenario 1: LEO Spacecraft ↔ TDRS ↔ Ground Terminal

Application Category	Transfer Unit	Response Time	Load Factor	Total Bandwidth Requirements	Precedence	Integrity	Availability	Security	Scalability
Command and Control	Small Async Frequent	1 - 3 Sec	1	256 Kbps	High	High	99.999	A+E+C	1-10 Slow
Telemetry/Navigation	Medium Sync Continuous	1 - 3 Sec	1	512 Kbps	Medium	High	99.99	E	1-10 Moderate
Emergency/Flight Critical	Small Sync Infrequent	1-3 Sec	1	64 Kbps	High	High	99.999	NR	1-10 Slow
Experiment Support/ Mission Payload	Large Async Continuous	10-20 Min	1	10 Mbps	Medium	Medium	99.99	NR	10-100 Moderate
System/Vehicle Maintenance	Large Async Medium	10-20 Min	1	1 Mbps	Medium	Medium	99.9	NR	1-10 Fast
Administrative	Medium Async Frequent	1-3 Min	1	1 Mbps	Low	Low	99.9	NR	1-10 Moderate

Application Category	Transfer Unit	Response Time	Load Factor	Total Bandwidth Requirements	Precedence	Integrity	Availability	Security	Scalability
Entertainment	Large Async Frequent	NA	NA	None	Low	Low	99.9	NR	0-10 Fast

4.2. Environment Analysis

The LEO spacecraft to ground terminal via TDRS scenario environment is comprised of a ground segment and a space segment. The ground segment consists of the ground terminal and Terrestrial Internet Nodes (TIN). The TIN infrastructure may be provided by an Internet Service Provider (ISP) or may be based on a private network architecture. It is assumed that nodal interfaces to the network use a Commercial Off-the-Shelf (COTS) Transmission Control Protocol (TCP)/Internet Protocol (IP) (TCP/IP) protocol stack. The protocol architecture of the TIN is not part of the protocol architecture analysis. The space segment consists of an In-Space Internet Node (IIN) communicating to the TIN ground terminal through the TDRS Transfer Node (TN). The scenario is shown in Figure 1.

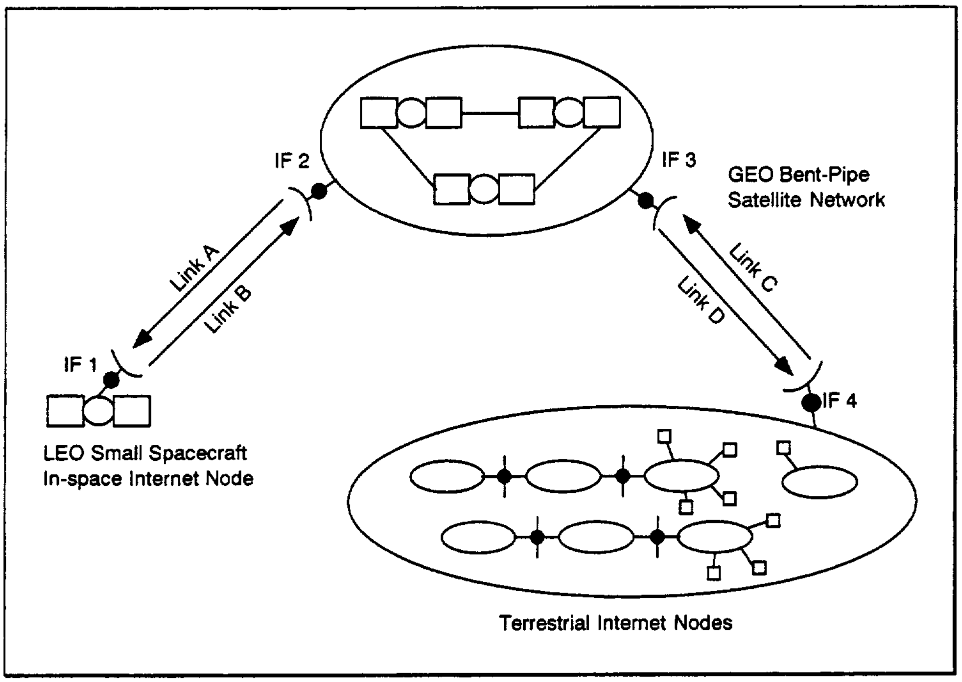

Figure 2. Scenario 1: LEO Spacecraft ↔ TDRS ↔ Ground Terminal

Space communications quality is typically limited by the characteristics of the ground/space link. Limited signal strength and transmission link noise cause data corruption, and standard terrestrial network protocols do not tolerate the inherently long propagation delay (high latency).

In the LEO spacecraft to ground terminal via TDRS scenario, there is continuous ground terminal visibility to the TDRS, with visibility to the LEO spacecraft over approximately 85% of the LEO's orbit (i.e., 10 to 15 minutes). Visibility to the LEO spacecraft is accomplished by acquiring and handing off the link signal among the TDRS constellation satellites. This acquire/handoff process directly impacts the duty cycle as end-to-end connectivity must be re-established after each event. Ideally, the acquire/handoff process would be seamless. However,

the space/space link suboptimality (i.e., link disruption as part of the acquire/handoff process) is considered part of the baseline operational environment for the protocol architecture.
Another aspect of the environment is nodal capacity in terms of bandwidth, processing and storage. For the LEO spacecraft to ground terminal via TDRS scenario, the ground segment is considered to have unlimited flexibility in meeting capacity requirements. The TDRS is limited by transponder bandwidth. The LEO spacecraft's onboard capabilities represent the greatest capacity constraints for the protocol architecture environment.

The Scenario 1 environment is summarized in Table 4.

Table 4. Environmental Assessment

Space segment infrastructure characteristics: • Limited number of end systems in space • Fixed bandwidth • Limited onboard processing and storage capacity
Ground segment infrastructure characteristics: • Modern computing environment • State of the art COTS technologies • Unlimited configuration flexibility
End-to-end communications environment characteristics: • Recurring transmission path disruption (intermittent connectivity) • Weak transmission signals • Noisy transmission path • High latency • Limited bandwidth, processing and storage capacity

4.2.1. Tracking and Data Relay Satellite System Characteristics

The Tracking and Data Relay Satellite (TDRS) system is a constellation of geostationary orbiting satellites effectively providing full-time global coverage by inter-satellite space/space links with the primary ground/space link to the White Sands Ground Terminal (WSGT) at Las Cruces, NM. The TDRS satellites are positioned at 22,300 miles (35,887 kilometers) over the equator in orbital slots approximately 130 degrees apart. The onboard TDRS transponders cover a range of bandwidths:

- TDRS Forward Link: $\leq$ 25 Mbps (K-band), $\leq$ 300 Kbps (S-band)

- TDRS Return Link: $\leq$ 300 Mbps (K-band), $\leq$ 6 Mbps (Single Access S-band), up to 5 users at $\leq$ 3 Mbps each (Advanced TDRS Multiple Access S-band)

4.2.2. Communication and End System Environment

The space node operations environment comprises the ground information infrastructure, with high-speed computing and communications capabilities. The space information infrastructure presents a significantly different environment from the ground systems. In space, there are relatively few end systems and networks and the communications requirements are driven by the extreme mass, power, and volume constraints, together with the delay and expense of developing space-qualified hardware.

The space communications environment is further complicated by the characteristics of the space/ground link. With rare exceptions, connectivity to a space vehicle is intermittent. The duty cycle typically is below 10% due to limited visibility from ground stations and contention among missions for scarce contact time. Limited signal strength and noise make data loss through corruption far more likely than in ground networks, and long propagation times cause terrestrial protocols to operate inefficiently or to fail function at all.

There are several existing protocols that must be supported including:

- Standard protocols to support reliable data transfer
- Evolving multi-node mission configurations that require in-space network routing
- Protocols that provide compatibility and interoperability with the Internet

4.3. Transmission Facility Selection

There are effectively four parts to the transmission facilities for this scenario (Figure 1):

- TDRS to LEO spacecraft forward link (Link A)
- Spacecraft to TDRS return link (Link B)
- Terrestrial Internet nodes to TDRS forward link (Link C)
- TDRS to terrestrial Internet nodes return link (Link D)

Ground segment transmission facilities must accommodate the ground/space link (Link C) and interface to the TIN. The TIN interfaces are assumed to include any protocol conversion and signal handling capabilities necessary to meet the terrestrial network requirements. Typical WSGT to TDRS forward link (Link A) and TDRS to WSGT return link (Link D) ground terminal transmission facilities are considered to be comprised of the antenna subsystems (S-band, Ku-band, Ka-band and C-band) and associated terminal equipment to fully support any protocol architecture requirements.

The TDRS is referred to as a "bent pipe" because it functions only to relay the transmission bit stream. This is a physical layer function of interfacing the mission bit stream (transmitted data) with the transmission medium.

The LEO interfaces (i.e., TDRS to LEO Forward Link and LEO to TDRS Return Link) are at the physical layer for the space/space link. Internally, the data units are interfaced to the onboard systems at the respective levels of the protocol stack. As compared to the ground segment, the LEO IIN capabilities are fixed and inflexible. Therefore, the LEO spacecraft to ground terminal via TDRS scenario transmission facility selection defaults to the onboard LEO IIN transmission systems. The LEO spacecraft is assumed to have, as a minimum, the necessary onboard interfaces (logical and physical) and transmission facilities to satisfy the mission-specific application requirements.

4.4. Switching Technology Selection

The next step in the methodology is the choice of how the various users of the system should share the transmission media. The concept of resource sharing is fundamental to any computer communications system. There are several possible ways of sharing computer and communications resources. Point-to-point communications systems use multiplexing or switching techniques for resource sharing. In the case of multi-point or broadcast communications systems, polling and contention are two alternatives for resource sharing. The LEO spacecraft to ground terminal via TDRS scenario is a point-to-point communications system.

Possible switching technologies that can be used for resource sharing are:

- Circuit (or line) switching
- Message switching
- Packet switching

4.4.1. Circuit Switching

A circuit-switching network provides service by setting up a dedicated physical path between two communicating subscribers. The complete circuit is set up by a special signaling message. The signaling message passes all the way through the network and a return signal informs the source that data transmission may begin. Path setup time is usually on the order of seconds. The entire path remains allocated to the transmission until either the source or destination releases the circuit. Circuit switching is the common method for telephone systems. It is an appropriate method for communication when the two subscribers have identical equipment such as voice telephone instruments and no speed or code matching is necessary. Also, it is appropriate if the users communicates at a fairly constant rate for a long period of time. Circuit switching is inefficient for bursty traffic, which has a high peak-to-average ratio.

4.4.2. Message Switching

In message switching, a single path is selected for internodal transmission of a given message. The message is a logical data unit that travels from the source node to the next node in the path and incrementally through intermediate nodes to the destination. Each node in the path assembles and stores the entire message before forwarding it to the next node. This store-and-forward process introduces queuing delays at any node when a path or the next node is too busy to handle the message transmission. Such systems have been built to optimize the use of network lines and to remove the burden of communications responsibility from the user. Speed and code conversion can be performed in such networks. Examples of message-switched networks include Telex, AUTODIN I and the SITA airline system. Throughput delays in message-switched systems built in the last decade are usually on the order of many minutes.

4.4.3. Packet Switching

The final switching technology is packet switching. It is similar to message switching except that secondary storage is not used in the network. Messages are split into smaller units called packets, which are routed independently on a store-and-forward basis through the network. Thus, many packets of the same message may be in transmission simultaneously. This is one of the main advantages of packet switching. Packet switching is the most dynamic switching technique since it makes effective use of circuit bandwidth.

There are various packet mode methods such as Ethernet, Token ring, FDDI, and ATM for Local Area Network (LAN) environments. Technologies such as X.25, Frame Relay, SMDS and ATM are used in Metropolitan and Wide Area Network (MAN and WAN) environments. A simplified comparison can be made among circuit, message, and packet switching. It is worthwhile to note that all of such comparisons are dependent on technology and that there is nothing implicit in the functions performed by these switching methods which makes one superior to the other. That is, a message switching system with high-speed lines can outperform a slow-speed packet-switching system. Table 5 presents a comparison of these switching techniques.

Table 5. Comparison of Switching Techniques

Attribute	Circuit Switching	Message Switching	Packet Switching
Physical connection	Yes	No	No
Real time	Yes	No	Yes
Data storage	No	Yes	Temporary
Blocking with overload	Yes	No	Yes
Delays with overhead	No	Yes	Yes
Error control	No	Yes	Partial
Speed/code conversion	No	Yes	Yes
Delayed delivery	No	Yes	Possible
Multiple address	No	Yes	Possible

By comparing various aspects of the three switching technologies presented above, it is clear that packet switching provides a number of advantages over the other two technologies. In addition, the technology trend is such that more and more applications are being supported by packet mode technologies because of the inherent capability to dynamically share bandwidth and the flexibility in offering services compared to both circuit mode and message mode switch technologies.

The popularity of the Internet and the associated technologies are providing additional incentives to move audio and video services to packet mode switching. The next generation satellite based systems such as Iridium and Teledesic are using packet mode switching technology to support a full spectrum of services. Therefore, we recommend packet mode switching technology as the appropriate technology for the LEO spacecraft to ground terminal via TDRS scenario architecture.

4.5. Protocol Requirements Analysis

Table 6 shows the protocol functions that could be used by the applications in this scenario. Each column except the first column represents the application and its characteristics. Column 1 lists protocol functions using the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) protocol architecture as a guide. It is well known that OSI protocol architecture is ideally suited for protocol analysis purpose, even though the implementation of the model is not popular due to the significant amount of overhead required.

In this analysis we have included both connection oriented and connectionless protocol layers. The application, presentation, and session layers provide connection-oriented service only. A close look at the protocol functions required by the various applications reveals that all of the applications use only the connection establishment and connection release functions of the presentation and the session layers.

In addition, it is better to allow the applications or application layer protocols to provide the syntax transformation currently supported by presentation layer. This approach has two advantages. First the applications are free to choose the best encoding scheme. This eliminates the overhead associated with and the need for the presentation layer. In addition, the need to set up yet another connection at the presentation layer is also eliminated

A similar argument can be made to remove the session layer from the architecture. In the OSI architectural model, the session layer provides some of the functions required by the application layer entities. This creates a situation where the application service elements have to bypass the presentation layer to get the service from the session layer. Therefore, it is better to move these functions to the application layer and merge them with the application service elements.

Note that the merging of the presentation layer and session layer functions in the application layer eliminates the overhead due to these two layers and the need to set up a connection.

Table 7 presents the results of the analysis. In this table the functions related to the presentation and session layers are added to application layer and those that are not required are eliminated. In addition, the connection oriented network layer functions are also removed. As we can see from the table, the connection oriented network layer provides functions similar to that supported by the transport layer. Added to that, a connection oriented network layer protocol requires connection setup and release mechanisms that add to the overhead. In our opinion, there is no need to provide the same function at two different layers. Providing these functions at the transport layer provides an end-to-end capability. Therefore, the connection oriented network layer functions are also removed from the protocol architecture. Table 7 forms the basis for the conceptual protocol architecture.

The following protocol requirements have been identified from the protocol requirements analysis step:

- An application level protocol optimized towards the up-loading of spacecraft commands and software, and the downloading of collections of telemetry data.
- An underlying transport protocol optimized to provide reliable end-to-end delivery of spacecraft command and telemetry messages between end systems that are communicating over a network containing one or more potentially unreliable space data transmission paths.
- A data protection mechanism that provides the end-to-end security and integrity of such message exchange.
- A scaleable protocol that supports connectionless routing of messages through networks containing space data links.
- A data link protocol that takes a given physical link and transforms it to a link that can support the above requirements by compensating for the inherent shortcomings of the underlying physical medium.
- High performance channel coding to virtually eliminate the undetected bit errors in the space link.
- Flexible protocol architecture to take advantage of future high level of spacecraft automation.
- Routing of data dynamically through changing in-space network topologies.

Table 6. Scenario 1 Applications

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative		
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning
Application Layer Functions																			
Applications identifications	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Application context required	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Presentation context required																			
Presentation service requirements																			
requirements																			
Turn management	X	X	X	X							X	X							
Synchronization																X			
Recovery from temporary																			
Synchronous operation					X				X			X							
Asynchronous operation	X	X	X	X		X	X	X		X	X		X	X	X	X	X	X	X
Real time	X	X	X	X	X		X	X	X			X							
User Authentication	X	X		X							X	X							X
Linked operation																			
Presentation Layer Functions																			
Presentation connection	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Negotiation of syntax for presenting application data																			
Syntax transformation including data compression																			
Data transfer by utilizing the services of the lower layers	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative		
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning
Dialogue control																			
Session Layer Functions																			
Connection establishment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Connection release	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Connection abort																			
Activity management																			
Major and minor synchronization																			
Symmetric synchronization																			
Resynchronization																			
Exception																			
Negotiated release																			
Abort services																			
Data transfer by utilizing the services of the lower layers	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Transport Layer Functions - Reliable Transport Required																			
Precedence	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
Segmentation					X	X			X	X	X	X	X	X	X	X	X	X	X
Graceful closing	X	X	X	X			X	X			X	X	X	X	X	X			X
Flow control	X	X	X	X					X	X		X	X	X	X	X	X	X	X
Integrity	X	X	X	X			X	X	X	X	X	X	X	X	X	X			
Duplicate control	X	X	X	X							X	X	X	X	X	X			
Multiplexing	X	X	X	X							X			X					
Sequence control	X	X	X	X							X	X	X	X	X	X	X	X	X
Blocking	X	X	X	X							X			X					
Error detection	X	X	X	X			X	X	X	X	X	X	X	X	X	X			
Error recovery	X	X	X	X			X	X	X	X	X	X	X	X	X	X			

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative		
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning
Expedited data transfer	X	X	X	X							X								
Transport Layer Functions - Reliable Transport Not Required																			
Segmentation					X	X			X	X	X	X	X	X	X	X	X	X	X
Data transfer					X	X													
Network Layer Functions - Connection-Oriented																			
Connection establishment and its maintenance																			
Multiplexing of connections																			
Re-initialization or reset of connections																			
Addressing, routing and relaying	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Normal and expedited data transfer																			
Sequencing and flow control, segmentation and re-assembly					X	X			X	X	X	X	X		X	X	X	X	X
Error detection, notification and possibly recovery	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
Network Layer Functions - Connectionless																			
Addressing, routing and transfer of data	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection and notification	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
Access control	X	X		X							X	X							X

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative		
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning
Source authentication	X	X		X							X	X							X
Confidentiality	X	X	X	X								X							X
Possible segmentation					X	X			X	X	X	X	X		X	X	X	X	X
Multicasting					X	X	X	X	X	X			X	X	X				
Data Link Layer Functions - Connection-Oriented																			
Connection establishment and release	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Splitting of data link connections																			
Delimiting and synchronization of protocol-data-units	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection and recovery	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
Flow control and sequenced delivery	X	X	X	X															
Data Link Layer Functions - Connectionless																			
Data transfer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection	X	X	X	X			X	X	X	X	X	X	X	X	X	X			

Table 7. Scenario 1 Protocol Stack

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative		
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning
Application Layer Functions																			
Applications identifications	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Application context required	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Turn management	X	X	X	X							X	X							
Synchronization																X			
Synchronous operation					X				X			X							
Asynchronous operation	X	X	X	X		X	X	X		X	X		X	X	X	X	X	X	X
Real time	X	X	X	X	X		X	X	X			X							
User Authentication	X	X		X							X	X							X
Transport Layer Functions - Reliable Transport Required																			
Precedence	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
Segmentation					X	X			X	X	X	X	X	X	X	X	X	X	X
Graceful closing	X	X	X	X			X	X			X	X	X	X	X	X			X
Flow control	X	X	X	X					X	X		X	X	X	X	X	X	X	X
Integrity	X	X	X	X			X	X	X	X	X	X	X	X	X	X			
Duplicate control	X	X	X	X							X	X	X	X	X	X			
Multiplexing	X	X	X	X							X			X					
Sequence control	X	X	X	X							X	X	X	X	X	X	X	X	X
Blocking	X	X	X	X							X			X					
Error detection	X	X	X	X			X	X	X	X	X	X	X	X	X	X			
Error recovery	X	X	X	X			X	X	X	X	X	X	X	X	X	X			
Expedited data transfer	X	X	X	X							X								
Transport Layer Functions - Reliable Transport Not Required																			
Segmentation					X	X			X	X	X	X	X	X	X	X	X	X	X
Data transfer					X	X													

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative		
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning
Network Layer Functions - Connectionless																			
Addressing, routing and transfer of data	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection and notification	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
Access control	X	X		X							X	X							X
Source authentication	X	X		X							X	X							X
Confidentiality	X	X	X	X								X							X
Possible segmentation					X	X			X	X	X	X	X		X	X	X	X	X
Multicasting					X	X	X	X	X	X			X	X	X				
Data Link Layer Functions - Connection-Oriented																			
Connection establishment and release	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Delimiting and synchronization of protocol-data-units	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection and recovery	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
Flow control and sequenced delivery	X	X	X	X															
Data Link Layer Functions - Connectionless																			
Data transfer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection	X	X	X	X			X	X	X	X	X	X	X	X	X	X			

4.5.1. Operational Constraints

Ideally, the requirements identified above would be met through use of off-the-shelf technology that has been proven in ground-based systems. Unfortunately, space missions must be carried out under conditions that vary significantly from those in the ground environment. Therefore, the operational constraints encountered in space communications listed below should be taken into account in developing the conceptual protocol architecture. These are:

- Round-trip delays much greater than those seen in ground networks.
- Intermittent connectivity, as a result of orbital position, earth rotation, and availability of ground station support.
- Variation in the format and performance characteristics of the space links used in space missions.
- Changes in the routing path from contact to contact because of the use of multiple ground stations or changes of the relative positions of multiple spacecraft.
- Noise characteristics on space links that (despite sophisticated error correction codes) produce more frequent data loss than on ground links.
- The asymmetry in the bandwidth available for the spacecraft to TDRS link and the TDRS to ground terminal link needs to be taken into account. This asymmetry may affect the features of protocols that support end-to-end communications.

4.6. Protocol Synthesis

Protocol architectures are not developed in a vacuum. In general, it is an evolutionary process. The state of the technology, the operating environment, and the application requirements are the driving factors in the development of a conceptual protocol architecture. The evolution of the TCP/IP protocol architecture is a perfect example of this phenomena. As new applications are developed and fielded, the protocol architecture is enhanced to meet the additional requirements, or new protocols are developed. Therefore, it is worthwhile to identify the technology trends before synthesizing the conceptual protocol architecture.

4.6.1. Technology Trends

The robustness of the Internet has redefined the direction of computer communications networking. The deployment of popular applications and the need to support these applications more efficiently has led to development of new application level protocols as well as research into enhancing the TCP/IP protocol architecture. Data related traffic has already overtaken voice traffic being carried by present day networks and is growing at a much faster rate than voice traffic. This is validated by the transition taking place in the telecommunication industry to develop an integrated backbone network to carry voice, video and data. In addition, there are a number of initiatives in the standards world by various technology forums plus international and national standards bodies to enhance existing protocols or to develop new protocols. Therefore, one has to take into account these technology trends in developing a protocol architecture.

4.6.2. Trends in Standards

There are international, national and industry forums to develop standards so that communication between end systems can take place in an efficient way. Although these groups share a common goal (open communication among end systems), achieving common ground has been elusive. Recently, these groups have gone from a state of holy war to peaceful coexistence, which has benefited the user community.

The architects of the OSI protocol reference model have identified various drawbacks in the OSI model since its initial implementation. Since 1983, experts have claimed that the organization of the OSI upper layers (Application, Presentation, and Session) as described in the OSI reference model is a mess and needs to be restructured. Also, network architectures, such as the Aeronautical Telecommunication Network (ATN) which use the OSI protocol architecture for air to ground communications, have devised methods to bypass the presentation and session layers. They have done this to reduce the overhead and eliminate unnecessary functions present in these two layers.

Recently, ISO extended the application layer structure to allow a single control function to supervise a set of application service elements. Also, they have revisited the entire upper layer architecture. They now essentially allow implementations to slice the upper layers vertically and ultimately collapse the upper layers into a single, object-oriented service layer. The extended application layer structure (XALS) and revised OSI upper layer architecture are under study in the ISO defined application service object (ASO). The ASO will contain multiple application service elements, some formed by grouping session functional units into application service elements. The result is the elimination of the session layer.

The existing presentation layer functionality will be subsumed within a new association control service element, which will offer an association data service. As a result, the presentation layer will be removed from the OSI reference mode as well. This allows the ASO association control service element to directly interface with the OSI transport layer. These developments in a sense align the OSI architecture more closely with the TCP/IP protocol architecture. It also reduces the overhead and protocol complexity.

The ISO transport protocol TP4 and the TCP are not only functionally equivalent but operationally similar as well. A 1985 study performed jointly by the U.S. Defense Communications Agency and the National Academy of Science concluded that TP4 and TCP are functionally equivalent and essentially provide similar services. Table 8 compares the functions provided by these protocols.

Table 8. Comparison of TP4 and TCP Functions

Function	TP4	TCP
Data transfer	Blocks	Streams
Flow control	Segments	Octets
Error detection	Checksum	Checksum
Error correction	Retransmission	Retransmission
Addressing	Variable TSAP	16-bit
Interrupt service	Expedited data	Urgent data
Security	Variable in TP	Not available
Precedence	16 bits in TP	Not available
Connection termination	Nongraceful	Graceful

At the network layer ISO supports the Connectionless Network Protocol (CLNP) and the TCP/IP protocol architecture supports the Internet Protocol (IP). The CLNP and IP are functionally identical and both are best effort delivery network protocols. The major difference between the two is that CLNP accommodates variable length addresses, whereas IP supports fixed 32 bit addresses. (Version 6 of the Internet Protocol (IPv6) supports a larger address space.) Table 9 compares the functions of CLNP with those of IP.

4.6.2.1. Why an Internet-Based Network Architecture

In a heterogeneous network environment, the networking technologies used by various organization range from COTS LANs to dialup networks. This means there are many different types of subnetworks that must be connected together. As no one has control over what the subnetwork will look like, the network layer (Internetwork) protocol has to be designed to work with whatever may be the type of subnetwork available. Therefore, the practical approach is to define one protocol that assumes minimal subnetwork functionality and place it firmly on the top of every subnetwork access protocol. This network architecture model treats every subnetwork and data link service as providing a basic data pipe. Each pipe should support a service data unit large enough to accommodate the header of the network layer protocol and a reasonable amount of user data. This is the IP or OSI connectionless network protocol model of networking. As the subnetwork technology changes, there is just one more subnetwork with which the network layer must interface.

Table 9. Comparison of CLNP and IP Functions

Function	CLNP	IP
Version identification	1 octet	4 bits
Header length	1 octet, represented in octets	4 bits, represented in 32 bit words
Quality of service	QoS maintenance option	Type of service
Segment/fragment length	16 bits, in octets	16 bits, in octets
Total length	16 bits, in octets	Not present
Data unit identification	16 bits	16 bits
Flags	Don't segment, more segments, suppress error report	Don't fragment, more fragments
Segment/fragment offset	16 bits, represented in octets (value always multiple of 8)	13 bits, represented in units of 8 octets
Lifetime, time to live	1 octet, represented in 500 millisecond units	1 octet, represented in 1-second units
Higher layer protocol	Not present	Protocol identifier
Lifetime control	500 millisecond units	1-second units
Addressing	Variable length	32-bit fixed
Options	• Security • Priority • Complete source routing • Partial source routing • Record route • Padding • Not present • Reason for discard (Error PDU only)	• Security • Precedence bits in TOS • Strict source route • Loose source route • Record route • Padding • Timestamp

4.6.2.2. Why a TCP/IP Protocol Architecture

Although ISO's TP4 and the TCP transport protocols are functionally identical, TP4 is not widely implemented. There is limited practical knowledge about the protocol in the real world environment. On the other hand, TCP provides an excellent base of technology for extension. It is a highly robust protocol, widely distributed, and is freely available. Hundreds of individuals worldwide work to ensure that TCP continues to meet the needs of the Internet community. Therefore, TCP is cost effective to implement, and provides additional functionality that may be needed in the future.

In addition, the ISO's CLNP and IP are functionally similar in providing a connectionless network layer service to the transport layer. Here again, CLNP has not been deployed widely and has not been tested thoroughly in an operational environment. Therefore, it is recommended that the TCP/IP protocol architecture forms the starting point for the LEO spacecraft to ground terminal via TDRS scenario protocol architecture.

4.7. Scenario Unique Requirements

Although functionally equivalent to terrestrial networks, space communications networks often have performance and operational considerations that prevent direct use of existing commercial protocols. Protocols used in terrestrial networks assume that: connectivity is maintained; data loss due to corruption is rare; balanced bi-directional links are available; and most data loss is due to congestion. Further, vendors of commercial communications products that implement these protocols use these assumptions to maximize performance and economy in this environment. This results in the treatment of retransmission, recovery, and time-outs inappropriate for space operations. For the majority of space nodes, the space environment makes performance of these protocols unacceptable.

To meet the above constraints, protocols are required to provide interoperability across the spectrum of space nodes and between space data systems and the COTS based ground network environment. They have to provide a set of options and protocol data unit formats that can be scaled to satisfy the communications needs of both complex and simple nodes.

The protocol architecture should provide reliable stream or file transfers over existing and new link layers plus dynamic networking for multiple space node environments. Given the link characteristics and intermittent connectivity encountered over the space link, better performance is achieved by using a balance of upper-layer, confirmed, end-to-end services supported by link level error correction that avoids excessive retransmission.

4.8. Recommended Protocol Architecture

The goal of the LEO spacecraft to ground terminal via TDRS scenario protocol architecture is not only to support applications but also to lower the lifecycle costs by reducing development and operations costs in space communications systems. In addition, the protocol architecture should be able to extend Internet connectivity into space. The rationale for this approach is that both the data systems and the personnel (designers, operators, and users) associated with space missions are already using Internet protocols. The communications services that they need in space are very similar to those they have in ground networks. The easiest, lowest risk, and most direct way to achieve this goal is to adapt the protocols that are used on the ground.

Although the Internet protocols provide an excellent basis for space communications protocol development, the space environment presents a number of constraints that are seldom encountered in the design of terrestrial data communications networks. There are physical, operational, and resource differences. The physical differences include:

- Space link delays ranging from milliseconds to hours.
- Potentially noisy space data links.
- Limited space link bandwidth.
- Variation in sub-network types from simple busses to local and wide area networks.
- Interruptions in the end-to-end data path that can vary from bits lost and link interruptions.

The operational differences include:

- Inherently sporadic nature of contact between space and ground.
- Maximum latency requirement due to "Teleoperations" activities.

The resource differences include:

- Limited onboard processing power.
- Limited onboard program memory.
- Limited onboard data buffering.
- Asymmetry in bandwidth between forward and return links.

Except for a very narrow range of operational conditions, the current off-the-shelf Internet protocols do not satisfy the requirements encountered in the space mission environment. Therefore, the strategy is to: use COTS-supported standards wherever possible; capitalize on established user interface familiarity; and minimize software development costs. This approach allows one to take advantage of the hundreds of thousands of hours of operational experience that the Internet protocols have accrued.

4.9. NASA Conceptual Protocol Architecture

The suite of NASA space protocols should provide flexibility and optional features that allow designers to tailor a communications protocol suite to meet specific requirements and constraints without extensive software development. It should allow specific layers or protocols within layers to be included or omitted to create an optimal profile. This calls for a layered protocol architecture.

The LEO spacecraft to ground terminal via TDRS scenario architecture is shown in Figure 3.

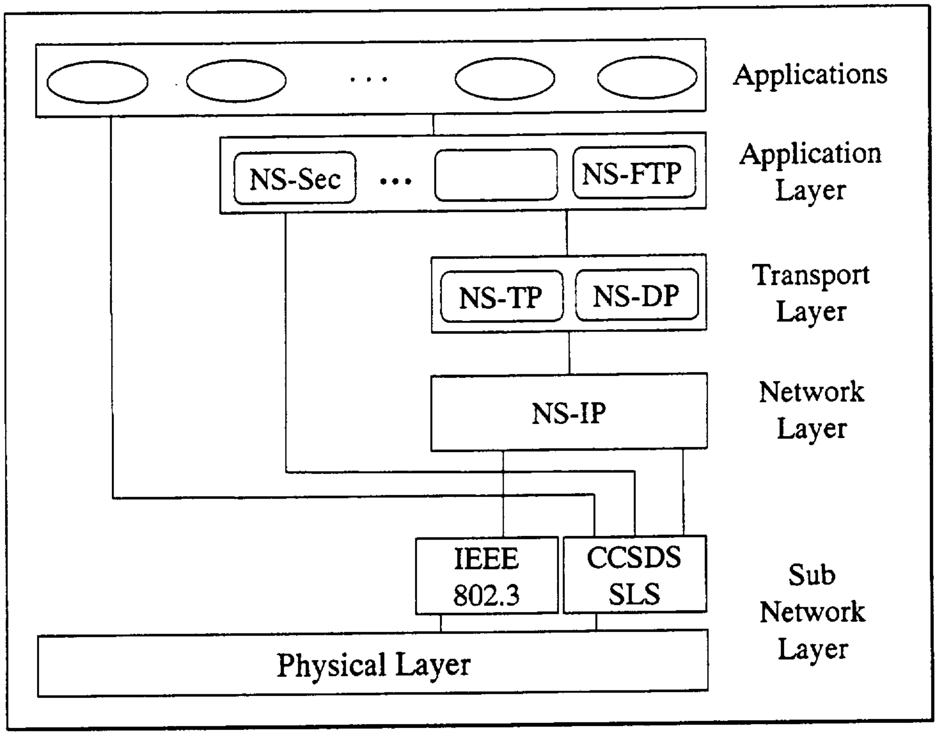

Figure 3. Recommended LEO Spacecraft ↔ TDRS ↔ Ground Terminal Architecture

Figure 3 shows the NASA Space (NS) conceptual protocol architecture. As mentioned before, this scenario supports data only applications. In addition, there is a need to provide bit efficient protocols to support these data applications. The conceptual protocol architecture consists of an application layer supported by the transport layer. The application layer protocols consists of NASA Space File Transfer Protocol (NS-FTP) and the NASA Space Security Protocol (NS-Sec). This protocol architecture is very flexible. It is easy to add more application layer protocols as requirements for such protocol arise.

The transport layer supports a reliable end-to-end protocol called NS-TP. The NS-TP supports functions that are similar to TCP and ISO TP4. In order to meet the space based communications requirements, modifications need to be made to this protocol. Some of the issues are identified in the transport layer section.

The space based applications presented in Table 7 require a connectionless transport protocol as well. The NASA Space Datagram Protocol (NS-DP) provides support for this service. NS-DP supports a minimum capability. It is similar to the ISO Connectionless transport protocol and TCP/IP's User Datagram Protocol.

The NS transport layer interfaces to the connectionless NS-IP protocol. The functions supported by the NS-IP are similar to those of ISO's CLNP and TCP/IP's IP protocols. But in order to operate efficiently in a space based communications environment, a number of enhancements are identified.

For data only application the connectionless NS-IP interfaces to the existing CCSDS space link subnetwork (SLS) subnetwork layer. The user has the option of interfacing to Ethernet (IEEE 802.3) link layer protocols within the spacecraft.

4.9.1. NASA Space System File Transfer Protocol (NS-FTP) Functions

The Internet File Transfer Protocol (FTP) in the TCP/IP architecture supports a rich set of file transfer capabilities. Compared to the ISO's FTAM, FTP is a widely used and stable protocol. The amount of FTP overhead needed is significantly less than required for FTAM. Therefore, FTP is well suited for the bandwidth limited space based network environment. Table 10 shows the functions supported by the FTP.

Table 10. TCP/IP FTP Functions

FTP Functions
RETRIEVE
STORE
STORE UNIQUE
APPEND (with create)
ALLOCATE
RESTART
RENAME FROM
RENAME TO
ABORT
DELETE
REMOVE DIRECTORY
MAKE DIRECTORY
PRINT WORKING DIRECTORY
LIST
NAME LIST
SITE PARAMETERS
SYSTEM
STATUS
HELP

As the Internet File Transfer Protocol (FTP) provides a rich set of functions, the NS-FTP should use FTP as a starter set to define the file transfer functions and then add functions required to operate in the bandwidth limited space operations environment. Like FTP, NS-FTP should use two transport connections between host systems - a control connection to exchange control information, and a data transfer connection to move data file. Data is transferred from a storage device in the sending host to a storage device in the receiving host.

Both contact time and bandwidth are scarce resources in space operations. To operate in the resource restricted space environment, NS-FTP should provide enhanced error recovery and restart capabilities. Interruptions in file transfers could be restarted from the point of interruption instead of starting over. This is a common feature supported by many Web-related download applications.

NS-FTP should also provide the capability to read or update part of a file on a remote system rather than the entire file. This avoids the transfer of a large amount of data when only a small part of the file is affected. Other NS-FTP extensions to FTP should provide integrity checks to recover from errors in file transfer or update operations. Finally, to conserve bandwidth and contact time, NS-FTP should suppress text messages between the end systems involved in file operations.

It is suggested that the application layer file transfer protocol support the following functions:

- Transfers of command and data files to the spacecraft.
- Transfers of application software to the spacecraft.
- Transfers of science or mission data to the ground without special processing to reorder or merge data sets.
- Limited management of files onboard the spacecraft (delete, rename, and directory services).
- Automatic restart of transfers after an interruption.
- Read portions of files resident onboard the spacecraft.
- Make updates/changes to files onboard the spacecraft without sending a complete replacement for the file to make minor modifications.

4.9.2. Security Protocol

In the NASA networking environment, network security is an important function. There are a number of security related protocols available from standards bodies. The Secure Data Network (SDNS) "SP3" protocol, the ISO Network Layer Security Protocol (NLSP), the Integrated Network Layer Security Protocol (I-NLSP), and the Internet Engineering Task Force's (IETF)

Internet Protocol Security (IPSEC) all provide data confidentiality, data integrity, authorization, and access control. However, they have far greater overhead than is acceptable over space links.

The NS-Sec data protection protocol should provide the capability to control access to network resources. Only those users (or processes acting on behalf of users) with authorization should be granted access to network resources. The NS-Sec data protection protocol should provide the capability to verify the identity of the end system that originated network communications. The NS-Sec data protection protocol should provide an optional capability to digitally sign a message to indicate that the message was actually sent by the user (or process acting on behalf of the user) claiming to send it. The NS-Sec data protection protocol should provide the capability to ensure that the data sent is exactly the same as the data received. It should provide assurance that any unauthorized modification of the data will be detected while the data is in transit across the network.

There are two issues related to the security protocol environment. One is the amount of overhead required and the other is where the security protocol should be placed. The SCPS-SP protocol has solved the problem associated with overhead. But it is placed in between the transport and network layers to support end-to-end security. This means that all applications whether they need security or not are forced to incur additional overhead.

Therefore, it is suggested that the security protocol be moved to the application layer and only those applications that require security need incur this additional overhead. It is recommended that SCPS-SP be adopted as the NASA space security protocol.

4.9.3. Transport Layer Protocol

NS-TP provides end-to-end full and minimal reliability services. The full reliability service is provided by enhanced TCP. It supports end-to-end data transfer of a sequence of data units with full reliability (complete, correct, in sequence, and no duplication). It uses sequence checking to assure the sequence order and avoid duplication. It incorporates acknowledgments and retransmission requests to provide completeness. This protocol closes connections without loss of data.

The minimal reliability service is provided by the NASA Space Datagram Protocol (NS-DP). It is a connectionless transport protocol and sends data in datagrams. It transfers data with minimal reliability (correct, possibly incomplete, and possibly out of sequence). It does not support sequence numbering, acknowledgment of receipt, or retransmissions.

The NS-TP is based on the Transmission Control Protocol (TCP). Enhancements are identified to improve performance in the space environment. Unmodified TCP performs poorly in communications scenarios with a large bandwidth-delay product and cannot operate efficiently with the unbalanced links typical of space-ground communications. The suggested extensions to the base protocols are intended to address the performance issues.

4.10. Differences Between Communications Environments

TCP provides an excellent base of technology for adding extensions. It is a highly robust protocol, widely distributed, and is freely available. TCP is optimized to provide service in the terrestrial environment. There are significant differences between the terrestrial and space environments that affect a communication protocol's performance. Table 11 presents a summary of the main factors that affect TCP performance when operating in space environments.

Table 11. Factors Affecting TCP Performance in Spacecraft Environments

Factor	Terrestrial Environment	Spacecraft Environment
Bit error rate	$< 10^{-9}$	10^{-5} to 10^{-12}
Round trip delay	Millisecond to second	Seconds to hours
Continuity of Connectivity	Continuous	Intermittent: 10% (LEO) to 90% (TDRS) per orbit
Forward and reverse links	1:1 (equivalent rates)	10:1 to 2000:1 Some have down link only
CPU capacity	Unrestricted	Possibly low
Communication goals	• Fair access over time • High aggregate throughput over time • High reliability	• High throughput during contact • Maximum link utilization
Primary source of data loss	Congestion	• Congestion • Corruption • Link outage

4.10.1. Bit-Error Rates

The error performance of typical terrestrial networks has improved to a point that it is no longer considered as a typical source of data loss. With sufficient channel coding and application of radiated power, some satellite links can approach the error performance of the terrestrial environment. Reed-Solomon error control has proven to be of great benefit in space links. Both hardware and software solutions to perform Reed-Solomon corrections in real time are available. For a link speed of 5 Mbps or less, software solutions have been shown to be adequate. Recent advancements in microprocessor speeds may enable a software solution for processing data at higher rates. A software solution for high-rate Reed-Solomon processing is preferable to a hardware solution in that a software solution would reduce system lifecycle costs and maximize system portability. In the future, the bit error may play a less significant roll in the performance of the transport layer.

4.10.2. Round Trip Delay

Round trip delays in the terrestrial communication environment are typically in the tens of milliseconds to low hundreds of milliseconds. In the spacecraft communication environment, round trip times of 500 milliseconds are the minimum that one expects when communicating through a geostationary satellite. Deep space communications can increase round trip delays to hours.

Long round-trip delays limit the usefulness and effectiveness of TCP's feedback from the remote communication endpoint. This causes problems when the protocol needs to react to changes in the network, but does not receive feedback about the changes until long after they have occurred. Note that long delays are not exclusively a result of speed-of-light propagation times. Low data transmission rates add delay to a network, as can half-duplex operations. Finally, queuing in intermediate systems is a source of delay.

4.10.3. Continuity of Connectivity

Topology changes are infrequent in a terrestrial communications environment. However, space based systems have predictable (possibly highly dynamic) connectivity characteristics. Low earth orbiting satellites typically have connectivity through a single ground station 10% of the time or less. Changes to the number of ground stations or the satellite's orbit can improve this, but even NASA's TDRS system offers only about 90% coverage.

4.10.4. Forward and Reverse Link Capacity

In the terrestrial communication environment, communication links are typically full duplex with the same data rate in both directions. This is not the case in space environments. It is not unusual to have large differences in forward and reverse link capacities. Ratios of 1000:1 are not unusual. This degree of asymmetry causes problems for TCP, which uses a stream of acknowledgments for transmitting data packets. Thus, very low capacity acknowledgment channels limit the transmission rate of data packets.

4.10.5. CPU and Memory Capacity

In the terrestrial communications environment, the availability of computing resources is essentially unrestricted. This is not the case in spacecraft where power, weight, and volume are all precious commodities. The amount of computational resources available to any subsystem in a spacecraft must be traded-off against the benefits of applying that resource elsewhere. Therefore, it is important to be aware of these constraints. The loss of data due to bit-errors has a disproportionately bad effect on TCP's performance because TCP interprets any loss as an indication of network congestion. The appropriate response to network congestion is to reduce the offered load to the network. TCP's congestion response reduces the offered load by half, then builds back slowly over several subsequent round trips. The effect of this response to bit-errors is to significantly under utilize the communication channel.

4.10.6. Primary Source of Data Loss

The primary source of loss in terrestrial networks is congestion, and TCP is optimized to control congestion. The space communication environment is a mixed-loss environment, with losses occurring due to three causes: bit-errors, topology changes (link outages), and congestion. To treat all losses as congestion results in unnecessary reductions in offered load. The increased round trip times in these environments delays the restoration of full-rate transmission.

4.11. Network Layer

From Table 7, the functional requirements for network services for the transfer of data between end points within a space data communications system are:

- Support for multiple routing options
- Packet lifetime support with auto discard
- Support for precedence handling
- Provide efficient operation in constrained-bandwidth environments
- Separate reporting of congestion and corruption

The ability to route data from source to destination is one of the important functions essentially provided by all the network layer protocols that operate at the network layer of the OSI Basic Reference Model. The routing protocol used to a certain extent determines the amount of overhead required to accomplish this task. In addition, the bandwidth available in both transmission directions has an effect on the performance of the network protocol. This constraint results in a requirement to operate with high bit-efficiency. Bit-efficiency quantifies the fraction of transmitted bits that are user data. Improving bit-efficiency may be accomplished in two ways: by increasing the amount of user data per unit of protocol control information (i.e., header information), or by decreasing the amount of protocol control information per unit of user data.

The first approach (making packets longer) is simple, but does not work well in environments that are prone to bit-errors. It also does not work well when the user's data does not lend itself to aggregation. The second approach (reducing the protocol header overhead) is the approach commonly used to obtain high bit-efficiency. Several requirements derive from the need to operate in bandwidth constrained environments: multicasting, support for address translation, and precedence-based data handling. All address bandwidth-related constraints and are described in subsequent paragraphs.

Multicasting is a technique for improving network-wide bit-efficiency. The technique of multicasting allows addressing of data to a group of destination systems. Rather than sending an unique copy of the data to each remote system, data is sent to the group address. Intermediate systems replicate the multicast packet only as necessary in order to reach all of the destination systems in the multicast group.

Header compression can enhance bit-efficiency in networks that can be characterized as having few source-destination pairs that account for most of the network's traffic. In IPv6, these are identified as flows. For these flows, the source and destination addresses can be replaced by an identifier. This is similar to the SCPS managed connection.

Precedence improves operations in bandwidth-constrained environments in two ways. First, it controls the order of service, which reduces queuing delay and variations in queuing delay for high precedence traffic. Second, precedence controls the order of packet discarding when congestion occurs. If packet discarding is required, low precedence packets are discarded before higher precedence ones.

Packet lifetime control provides protection against transient routing loops. A transient routing loop is formed when routing tables in the network are not synchronized. This condition can occur as a result of using certain routing protocols. While a routing loop is in existence, the links forming the loop may become progressively more congested. Packet lifetime control ensures that data packets do not remain in the network indefinitely. They are discarded once they have exceeded their "lifetime." This mechanism combined with either automated or manual means to update the routing tables provides control over routing loops.

Signaling of network conditions to upper-layer protocols is required to allow those protocols to become aware of and to adapt to changing conditions within the network. Signals that may be passed to the upper-layer protocols include indications of network congestion, network corruption, and link outages. This requires the network to identify the conditions at points in the network that may be remote from the end systems that host the upper-layer protocols. It also requires the network propagate network-internal signals to the affected end systems for delivery to the upper-layer protocols.

4.11.1. Shortcomings of Using IP in Space Networks

The Internet Protocol (IP) is a highly capable, widely used protocol. Table 12 identifies IP capabilities and the issues associated with using it in a space based network environment. Most of the issues are related to the limited bandwidth available in the space environment.

IP supports routing methods that forward data from source to destination. In general, IP does not provide any explicit support for operating in bandwidth limited environments. IP headers are a minimum of 20 octets in length, and may be made longer with the addition of options. IP provides support for multicasting, but has no mechanism for shortening its headers.

Table 12. Support of SCPS Network Requirements by IP

Protocol Function	IP
Routing	Yes
Support for bandwidth limited environment	No
Multicast support	Yes
Priority	Yes
Header compression	Yes – not supported in COTS
Priority	Partial
Packet life time control	yes
Signaling to support upper layer	Partial

The IP header contains a field to carry eight levels of precedence. However, COTS products typically do not make use of the field. In particular, high precedence packets would not benefit from a reduced probability of discard in congested routers, nor would they receive any reduced queuing delays in routers. The capabilities in IP for packet lifetime control are adequate for most environments.

With respect to signaling of network conditions, some IP implementations provide partial support. The Internet Control Message Protocol (ICMP) (the companion protocol to IP that handles such signaling) has the ability to generate congestion signals. However, research in this area has resulted in specifications such as Random Early Detection (RED). However, RED is not widely deployed nor is its Explicit Congestion Notification (ECN) option. There is no signaling provided to indicate loss, whether due to corruption or to link outage.

4.11.2. Suggested Enhancements to IP

All the issues identified above are in one way or another related to using the limited bandwidth more efficiently. One way to accomplish this goal is to not transmit unnecessary header elements. This design decision increases the processing to format and parse headers in favor of reducing the number of bits that are transmitted.

Network protocols typically route data from source to destination by selecting the "next hop" router based on the destination address. There are many routing methods by which the next hop router is selected. One method is to use routing tables that may be statically or dynamically configured to selects the next hop router. The routing methods reduce the complexity and overhead associated with routing but sacrifice the adaptive route selection capability.

In a space based networking environment, it is possible to reduce header overhead by performing header compression and address translation as suggested by the SCPS-network protocol. SCPS-NP's method of using a single address to represent an address pair is called a managed connection. In this method an IP source-destination pair may be translated into three alternate managed connection addresses:

- An extended path address which represents the two addresses with a single four-octet address;
- A pair of basic end system addresses which represents the two four-octet addresses with a pair of corresponding one-octet addresses; or
- A basic path address which represents the pair of four-octet addresses with a single one-octet address.

SCPS-NP uses address translation tables that are configured statically to translate addresses. The translation tables are identical throughout the network. In addition, address translation can be used to support multicasting, and to identify multicast (group) addresses.

4.12. Subnetwork Layer

The next layer in the NASA space protocol architecture is the subnetwork layer. The subnetwork is mostly technology dependent. It can range from Ethernet to ATM depending on the environment and the state of the technology. As new subnetwork technologies are developed, they can be easily incorporated into the protocol architecture. Similarly, existing space-based subnetworks can interface to the network layer. Although it is possible to interface any of the existing subnetwork technologies to the network layer, we present only the existing Space Link Subnetwork (SLS) as an example.

4.12.1. Space Link Subnetwork

To share the limited bandwidth of the space-to-ground link, a CCSDS recommendation for Advanced Orbiting Systems has developed the concept of a CCSDC virtual channel for the space link subnetwork. The virtual channel facility allows one physical space channel to be shared among multiple higher-layer traffic streams, each of which may have different service requirements. A single physical space channel may therefore be divided into several separate logical data channels, each known as a "Virtual Channel" (VC). Each VC is individually identified and supports a single "Grade of Service."

To facilitate simple, reliable, and robust synchronization procedures, fixed-length protocol data units are used to transmit data through the weak-signal, noisy space channels. The protocol data units are each associated with one particular VC and are known as "Virtual Channel Data Units" or VCDUs. A service option internal to the VCDU can also produce a protocol data unit known as a "Coded Virtual Channel Data Unit", or CVCDU. Each VCDU and CVCDU contains a header and trailer (which provide space link protocol control information) and a fixed-length data field within which higher-layer service data units are carried. The SLS supports six different types of services: encapsulation, multiplexing, bitstream, virtual channel access, virtual channel data unit, and insert.

The encapsulation service provides a facility whereby variable-length, octet-aligned service data units which are not formatted as CCSDS Packets may be transferred across the SLS. The transfer is asynchronous and sequence preserving.

The multiplexing service provides a facility whereby variable-length, delimited, octet-aligned service data units, which conform to the Version-1 CCSDS Packet format, may be multiplexed together for transfer across the SLS on the same VC. The transfer is asynchronous and sequence preserving.

The bitstream service provides a facility whereby serial strings of bits, whose internal structure and boundaries are unknown may be transferred across the SLS. The transfer is sequence preserving and may be either "asynchronous" or "isochronous." An isochronous transfer from service interface to service interface is provided with a specified maximum delay and a specified maximum jitter at the service interface. High-rate video data may use the isochronous bitstream service.

The virtual channel access service provides a facility whereby a project organization may transfer private service data units (which are sized to exactly load the fixed-length data field of one dedicated VCDU and whose internal structure is unknown) across the SLS. The transfer can be either asynchronous or isochronous and is sequence preserving.

The physical channel function creates one dedicated space data transmission path. A continuous stream of data bits is accepted at the sending side, modulated, serially transmitted through the physical space medium, demodulated, bit synchronized, and delivered through the receiving interface.

The insert service provides a facility whereby private octet-aligned service data units may be transferred isochronously across the SLS in a mode which efficiently uses the space channel transmission resources at relatively low data rates.

4.12.2. Virtual Channel Function

At the sending side, the virtual channel function accepts service data units from higher-layer functions. It then builds them into the space link protocol data units (VCDUs or CVCDUs) and applies error control required by different grades of service, commutates the VCDUs/CVCDUs into an appropriate sequence, and submits them as a serial stream to the physical Channel function for transmission through one physical channel.

At the receiving side the serial stream is synchronized to find the boundaries between VCDUs/CVCDUs, which are then passed through error control procedures and decommutated. The higher-layer service data units are then extracted and passed back through the receiving service interface.

During transmission through the physical channel, each VCDU or CVCDU is carried synchronously within one "Channel Access Data Unit" (CADU). The CADUs provide fixed-length "channel access slots" which occur at precise time intervals that are synchronized with the transmitted bit rate, and whose boundaries are delimited using "synchronization markers." The commutated sequence of VCDUs/CVCDUs is transmitted so that all of the synchronous channel access slots are occupied. In situations where no valid higher-layer data are ready for release, a VCDU/CVCDU containing "fill" data is commutated into the transmitted sequence. The continuous and contiguous stream of CADUs, known as a "Physical Channel Access Protocol Data Unit," is transferred through the physical channel.

Service data units associated with the encapsulation, multiplexing, bitstream or virtual channel access services are placed into a "Data Unit Zone" within the data field of the VCDU or CVCDU.

5. SCENARIO 2: SPACE STATION ↔ TDRS ↔ GROUND TERMINAL

This scenario is for unicast communications between a LEO International Space Station (ISS) and a ground terminal via a TDRS transfer node. The ground terminal is assumed to be part of the terrestrial Internet infrastructure. The terrestrial infrastructure may be provided by a carrier or may be based on private network architectures. The ISS to ground terminal via TDRS scenario supports multimedia applications in addition to the applications supported by the LEO spacecraft to ground terminal via TDRS scenario. It is assumed that multimedia traffic forms a significant portion of the traffic in this scenario.

5.1. NASA Application Types and Characteristics

The existing NASA application categories with the associated application types and their respective characteristics are shown in Table 13. The characteristics form the basis for assessing the protocol functional requirements at each layer in the protocol stack for the applications to be supported. Thee applications vary from command and control to entertainment. The table shows that majority of the applications do not require security. The response time range from seconds to minutes. The precedence levels range from high to low. In addition, message integrity ranges from again from high to low. The availability is spread over .999 to .99999.

The bandwidth requirement ranges from 1 Mbps to 100 Mbps, a wide range. The high traffic is mainly due to multimedia and Experiment Support/Mission Payload applications. The total daily traffic is found by summing the column defined as the total bandwidth requirements. The peak hour load to be supported by the system is 15% of the total daily traffic. The peak hour load is 24.01 Mbps.

Table 13. Scenario 2: ISS ↔ TDRS ↔ Ground Terminal

Application Category	Transfer Unit	Response Time	Load Factor	Total Bandwidth Requirements	Precedence	Integrity	Availability	Security	Scalability
Command and Control	Small Async Frequent	1 - 3 Sec	4	1 Mbps	High	High	99.999	A+E+C	4-10 Slow
Telemetry/Navigation	Medium Sync Continuous	1 - 3 Sec	10	5 Mbps	Medium	High	99.99	E	10-100 Moderate
Emergency/Flight Critical	Small Sync Infrequent	1-3 Sec	1	64 Kbps	High	High	99.999	NR	1-10 Slow
Experiment Support/ Mission Payload	Large Async Continuous	10-20 Min	100	100 Mbps	Medium	Medium	99.99	NR	100-1000 Moderate
System/Vehicle Maintenance	Large Async Medium	10-20 Min	10	10 Mbps	Medium	Medium	99.9	NR	10-50 Fast
Administrative	Medium Async Frequent	1-3 Min	4	4 Mbps	Low	Low	99.9	NR	1-10 Moderate

Application Category	Transfer Unit	Response Time	Load Factor	Total Bandwidth Requirements	Precedence	Integrity	Availability	Security	Scalability
Entertainment	Large Async Frequent	NA	4	40 Mbps	Low	Low	99.9	NR	1-100 Fast

5.2. Environment Analysis

The ISS to ground terminal via TDRS scenario environment consists of a ground segment and a space segment. Figure 4 shows the block diagram of the networking environment. The terrestrial Internet nodes are assumed to be part of the terrestrial Internet infrastructure. The terrestrial infrastructure may be provided by a carrier or may be based on a private network architecture. It is assumed that these nodes interface to the network using a COTS TCP/IP protocol stack. The protocol architecture of the terrestrial Internet nodes is not part of the protocol architecture analysis.

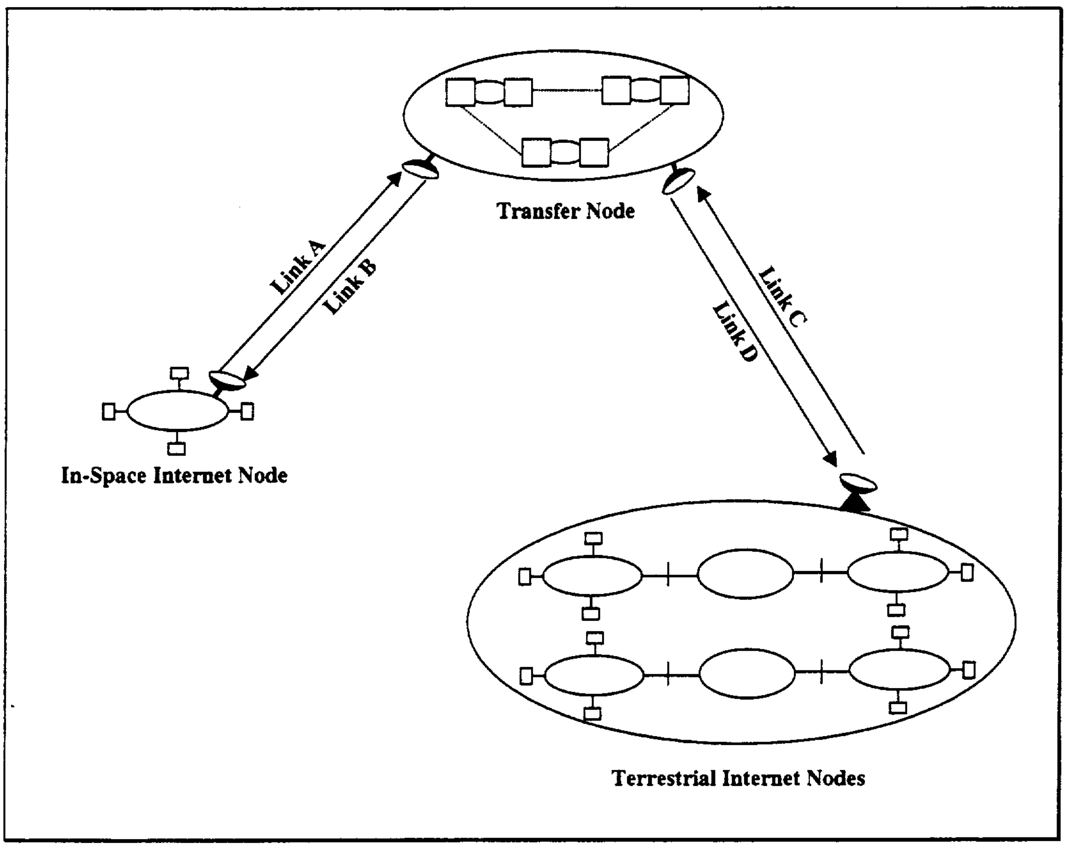

Figure 4. Scenario 2: Space Station ↔ TDRS ↔ Ground Terminal

It is assumed that ISS consists of an intra-network that supports communications functions that meet the internal requirements of the space station. The capability of the ISS may range from on-board communication and on-board data handling resources, including those with limited on-board computer and memory resources, as well as those with multiple, high-capacity on-board computers with extensive data storage. The ISS communicates with the TDRS via the paths identified as Link A and Link B. The links that support communication between the TDRS and the ground terminals are marked as Link C and Link D.

5.2.1. TDRS Characteristics

The TDRS characteristics are discussed in Section 4.2.1.

5.2.2. Communication and End System Environment

The space node operations environment comprises the ground information infrastructure, with high-speed computing and communications capabilities. The space information infrastructure presents a significantly different environment from the ground systems. In space, there are relatively few end systems and networks and the communications requirements are driven by the extreme mass, power, and volume constraints, together with the delay and expense of developing space-qualified hardware.

The space communications environment is further complicated by the characteristics of the space/ground link. With rare exceptions, connectivity to a space vehicle is intermittent. The duty cycle usually below 10% due to limited visibility from ground stations and contention among missions for scarce contact time. Limited signal strength and noise make data loss through corruption far more likely than in ground networks. Long propagation times cause terrestrial protocols to operate inefficiently or fail to function at all.

There are several existing protocols that must be supported including, standard protocols to support reliable data transfer, evolving multi-node mission configurations that require in-space network routing, and protocols that provide compatibility and interoperability with the Internet.

5.3. Transmission Facility Selection

There are effectively four parts to the transmission facilities for this scenario (Figure 4):

- Space station to TDRS forward link (Link A)
- TDRS to space station return link (Link B)
- Terrestrial Internet nodes to TDRS forward link (Link C)
- TDRS to terrestrial Internet nodes return link (Link D)

The space station interfaces (i.e., Link A and Link B) are at the physical layer for the space/space link. Internally, the data units are interfaced to the onboard systems at the respective levels of the protocol stack. As compared to the ground segment, the space station capabilities are fixed and inflexible. Therefore, the transmission facility selection defaults to the space station transmission systems. The space station is assumed to have the necessary onboard interfaces (logical and physical) and transmission facilities to satisfy mission-specific application requirements.

The TDRS is a "bent pipe" because it functions only to relay the transmission bit stream. This is a physical layer function of interfacing the mission bit stream (transmitted data) with the transmission medium.

The ground segment transmission facilities must accommodate the ground/space link (Link C) as well as interface to the terrestrial Internet node. The terrestrial Internet node interfaces are assumed to include any protocol conversion and signal handling capabilities necessary to meet the terrestrial network requirements. Typical ground node to TDRS forward link (Link C) and TDRS to ground station return link (Link D) ground terminal transmission facilities are considered to be comprised of the antenna subsystems (S-band, Ku-band, Ka-band and C-band) and associated terminal equipment to fully support any protocol architecture requirements.

5.4. Switching Technology Selection

The material presented here is almost identical to that presented in section 4.4. for the first scenario. It is repeated here to make this scenario complete.

The next step in the methodology is the choice of how the various users of the system should share the transmission media. The concept of resource sharing is fundamental to any computer communications system. There are several possible ways of sharing computer and communications resources. Point-to-point communications systems use multiplexing or switching techniques for resource sharing. In the case of multi-point or broadcast communications systems, polling and contention are two alternatives for resource sharing. The space station to ground terminal via TDRS scenario is a point-to-point communications system.

Possible switching technologies that can be used for resource sharing are:

- Circuit (or line) switching
- Message switching
- Packet switching

5.4.1. Circuit Switching

A circuit-switching network provides service by setting up a dedicated physical path between two communicating subscribers. The complete circuit is set up by a special signaling message. The signaling message passes all the way through the network and a return signal informs the source that data transmission may begin. Path setup time is usually on the order of seconds. The entire path remains allocated to the transmission until either the source or destination releases the circuit. Circuit switching is the common method for telephone systems. It is an appropriate method for communication when the two subscribers have identical equipment such as voice telephone instruments and no speed or code matching is necessary. Also, it is appropriate if the users communicates at a fairly constant rate for a long period of time. Circuit switching is inefficient for bursty traffic, which has a high peak-to-average ratio.

5.4.2. Message Switching

In message switching, a single path is selected for internodal transmission of a given message. The message is a logical data unit that travels from the source node to the next node in the path and incrementally through intermediate nodes to the destination. Each node in the path assembles and stores the entire message before forwarding it to the next node. This store-and-forward process introduces queuing delays at any node when a path or the next node is too busy to handle the message transmission. Such systems have been built to optimize the use of network lines and to remove the burden of communications responsibility from the user. Speed and code conversion can be performed in such networks. Examples of message-switched networks include Telex, AUTODIN I and the SITA airline system. Throughput delays in message-switched systems built in the last decade are usually on the order of many minutes.

5.4.3. Packet Switching

The final switching technology is packet switching. It is similar to message switching except that secondary storage is not used in the network. Messages are split into smaller units called packets, which are routed independently on a store-and-forward basis through the network. Thus, many packets of the same message may be in transmission simultaneously. This is one of the main advantages of packet switching. Packet switching is the most dynamic switching technique since it makes effective use of circuit bandwidth.

There are various packet mode methods such as Ethernet, Token ring, FDDI, and ATM for Local Area Network (LAN) environments. Technologies such as X.25, Frame Relay, SMDS and ATM are used in Metropolitan and Wide Area Network (MAN and WAN) environments. A simplified comparison can be made among circuit, message, and packet switching. It is worthwhile to note that all of such comparisons are dependent on technology and that there is nothing implicit in the functions performed by these switching methods which makes one superior to the other. That is, a message switching system with high-speed lines can outperform a slow-speed packet-switching system. Table 14 presents a comparison of these switching techniques.

By comparing various aspects of the three switching technologies, it is clear that packet switching provides a number of advantages over the other two technologies. In addition, the technology trend is such that more and more applications are being supported by packet mode technologies because of the inherent capability to dynamically share bandwidth and the flexibility in offering services compared to both circuit mode and message mode switch technologies.

The popularity of the Internet and the associated technologies are providing additional incentives to move audio and video services to packet mode switching. The next generation satellite based systems such as Iridium and Teledesic are using packet mode switching technology to support a full spectrum of services. Therefore, we recommend that packet mode switching technology as the appropriate technology for this architecture.

Table 14. Comparison of Switching Techniques

Attribute	Circuit Switching	Message Switching	Packet Switching
Physical connection	Yes	No	No
Real time	Yes	No	Yes
Data storage	No	Yes	Temporary
Blocking with overload	Yes	No	Yes
Delays with overhead	No	Yes	Yes
Error control	No	Yes	Partial
Speed/code conversion	No	Yes	Yes
Delayed delivery	No	Yes	Possible
Multiple address	No	Yes	Possible

5.5. Protocol Requirements Analysis

Tables 15 and 16 show the applications and protocol functions for the space station to ground terminal via TDRS scenario. Each column except the first column represents the application and its characteristics. Column 1 lists the protocol functions as identified in the ISO OSI protocol architecture reference model as a guide. It is well known that OSI protocol architecture is ideally suited for protocol analysis purpose, even though the implementation of the model is not popular due to the significant amount of overhead required.

In this analysis we have included both connection oriented and connectionless protocol layers. The application, presentation and session layers provide connection-oriented service only. A close look at the protocol functions required by the various applications reveals that all of the applications use only the connection establishment and connection release functions of the presentation and the session layers.

In addition, it is better to allow the applications or application layers protocols to provide the syntax transformation usually supported by presentation layer. This approach has two advantages. First the applications are free to choose the best encoding scheme. This eliminates the overhead associated with and the need for the presentation layer. In addition, the need to set up yet another connection at the presentation layer is eliminated.

A similar argument can be made to remove the session layer from the architecture. In the OSI architectural model, the session layer provides some of the functions required by the application layer entities. This creates a situation where the application service elements have to bypass the presentation layer to get the service from the session layer. Therefore, it is better to move these functions to the application layer and merge them with the application service elements.

Note that the merging of the presentation layer and session layer functions in the application layer eliminates the overhead due to these two layers and the need to set up a connection.

Table 16 presents the results of the analysis. In this table the functions related to the presentation and session layers are added to application layer and those that are not required are eliminated. In addition, the connection oriented network layer functions are also removed. As we can see from the Table, the connection oriented network layer provides functions similar to those supported by the transport layer. Added to that, a connection oriented network layer protocol requires connection setup and release mechanisms that add to the overhead. In our opinion, there is no need to provide the same function at two different layers. Providing these functions at the transport layer provides an end-to-end capability. Therefore, the connection oriented network layer functions are also removed from the protocol architecture. Table 16 forms the basis for the conceptual protocol architecture.

The following protocol requirements have been identified from the protocol requirements analysis step:

- An application level protocol optimized towards the up-loading of space station commands and software, and the downloading of collections of telemetry data.
- An underlying transport protocol optimized to provide reliable end-to-end delivery of space station command and telemetry messages between end systems that are communicating over a network containing one or more potentially unreliable space data transmission paths.
- A data protection mechanism that provides the end-to-end security and integrity of such message exchange.
- A scaleable protocol that supports both connectionless routing of messages through networks containing space data links.
- A data link protocol that takes a given physical link and transforms it to a link that can support the above requirements by compensating for the inherent shortcomings of the underlying physical medium.
- High performance channel coding to virtually eliminate the undetected bit errors in the space link.
- Flexible protocol architecture to take advantage of future high level of space station automation.
- Routing of data dynamically through changing in-space network topologies.
- Multimedia support.

Table 15. Scenario 2 Applications

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative			Entertainment
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning	Video etc.
Application Layer Functions																				
Applications identifications	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Application context required	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Presentation context required																				
Presentation service requirements																				
Session service requirements																				
Turn management	X	X	X	X							X	X								
Synchronization																X				
Recovery from temporary loss of presentation connection																				
Synchronous operation					X				X			X								
Asynchronous operation	X	X	X	X		X	X	X		X	X		X	X	X	X	X	X	X	X
Real time	X	X	X	X	X		X	X	X			X								
User Authentication	X	X		X							X	X							X	
Linked operation																				
Presentation Layer Functions																				
Presentation connection establishment, and its termination with its peer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Negotiation of syntax for																				

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative			Entertainment
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning	Video etc.
Syntax transformation including data compression																				
Data transfer by utilizing the services of the lower layers	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Dialogue control																				
Session Layer Functions																				
Connection establishment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Connection release	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Connection abort																				
Activity management																				
Major and minor synchronization																				
Symmetric synchronization																				
Resynchronization																				
Exception																				
Negotiated release																				
Abort services																				
Data transfer by utilizing the services of the lower layers	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Transport Layer Functions - Reliable Transport Required																				
Precedence	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	
Segmentation					X	X			X	X	X	X	X	X	X	X	X	X	X	X
Graceful closing	X	X	X	X			X	X			X	X	X	X	X	X			X	
Flow control	X	X	X	X					X	X		X	X	X	X	X	X	X	X	X
Integrity	X	X	X	X			X	X	X	X	X	X	X	X	X	X				
Duplicate control	X	X	X	X							X	X	X	X	X	X				

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative			Entertainment
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning	Video etc.
Multiplexing	X	X	X	X							X			X						
Sequence control	X	X	X	X							X	X	X	X	X	X	X	X	X	
Blocking	X	X	X	X							X			X						
Error detection	X	X	X	X			X	X	X	X	X	X	X	X	X	X				
Error recovery	X	X	X	X			X	X	X	X	X	X	X	X	X	X				
Expedited data transfer	X	X	X	X							X									
Transport Layer Functions - Reliable Transport Not Required																				
Segmentation					X	X			X	X	X	X	X	X	X	X	X	X	X	X
Data transfer					X	X														
Network Layer Functions - Connection-Oriented																				
Connection establishment and its maintenance																				
Multiplexing of connections																				
Re-initialization or reset of connections																				
Addressing, routing and relaying	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Normal and expedited data transfer																				
Sequencing and flow control, segmentation and re-assembly					X	X			X	X	X	X	X		X	X	X	X	X	X
Error detection, notification and possibly recovery	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative			Entertainment
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning	Video etc.
Network Layer Functions - Connectionless																				
Addressing, routing and transfer of data	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection and notification	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
Access control	X	X		X							X	X							X	
Source authentication	X	X		X							X	X							X	
Confidentiality	X	X	X	X								X							X	
Possible segmentation					X	X			X	X	X	X	X		X	X	X	X	X	X
Multicasting					X	X	X	X	X	X			X	X	X					
Data Link Layer Functions - Connection-Oriented																				
Connection establishment and release	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Splitting of data link connections																				
Delimiting and synchronization of protocol-data-units	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection and recovery	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
Flow control and sequenced delivery	X	X	X	X																
Data Link Layer Functions - Connectionless																				
Data transfer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection	X	X	X	X			X	X	X	X	X	X	X	X	X	X				

Table 16. Scenario 2 Protocol Stack

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative			Entertainment
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning	Video etc.
Application Layer Functions																				
Applications identifications	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Application context required	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Turn management	X	X	X	X							X	X								
Synchronization																X				
Synchronous operation					X				X			X								
Asynchronous operation	X	X	X	X		X	X	X		X	X		X	X	X	X	X	X	X	X
Real time	X	X	X	X	X		X	X	X			X								
User Authentication	X	X		X							X	X							X	
Transport Layer Functions - Reliable Transport Required																				
Precedence	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	
Segmentation					X	X			X	X	X	X	X	X	X	X	X	X	X	X
Graceful closing	X	X	X	X			X	X			X	X	X	X	X	X			X	
Flow control	X	X	X	X					X	X		X	X	X	X	X	X	X	X	X
Integrity	X	X	X	X			X	X	X	X	X	X	X	X	X	X				
Duplicate control	X	X	X	X							X	X	X	X	X	X				
Multiplexing	X	X	X	X							X			X						
Sequence control	X	X	X	X							X	X	X	X	X	X	X	X	X	
Blocking	X	X	X	X							X			X						
Error detection	X	X	X	X			X	X	X	X	X	X	X	X	X	X				
Error recovery	X	X	X	X			X	X	X	X	X	X	X	X	X	X				
Expedited data transfer	X	X	X	X							X									
Transport Layer Functions - Reliable Transport Not Required																				
Segmentation					X	X			X	X	X	X	X	X	X	X	X	X	X	X
Data transfer					X	X														

Application Category	Command and Control			Telemetry/Navigation			Emergency/ Flight Critical		Experiment Support/ Mission Pay Load				System/Vehicle Maintenance				Administrative			Entertainment
Characteristics/Types	Pilot/Controller	Mission Coordination	Routine	Flight Path Control	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	Interactive	Process Control	System Diagnostics	Event Reports	Testing	Software Upgrades	Routine Crew	Supply	Planning	Video etc.
Network Layer Functions - Connectionless																				
Addressing, routing and transfer of data	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection and notification	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
Access control	X	X		X							X	X							X	
Source authentication	X	X		X							X	X							X	
Confidentiality	X	X	X	X								X							X	
Possible segmentation					X	X			X	X	X	X	X		X	X	X	X	X	X
Multicasting					X	X	X	X	X	X			X	X	X					
Data Link Layer Functions - Connection-Oriented																				
Connection establishment and release	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Delimiting and synchronization of protocol-data-units	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection and recovery	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
Flow control and sequenced delivery	X	X	X	X																
Data Link Layer Functions - Connectionless																				
Data transfer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Error detection	X	X	X	X			X	X	X	X	X	X	X	X	X	X				

5.5.1. Operational Constraints

Ideally, the requirements identified above would be met through use of off-the-shelf technology that has been proven in ground-based systems. Unfortunately, space missions must be carried out under conditions that vary significantly from those in ground data systems. Therefore, the operational constraints encountered in space communications listed below should be taken into account in developing the conceptual protocol architecture.

- Round-trip delays much greater than those seen in ground networks.
- Intermittent connectivity, as a result of orbital position, earth rotation, and availability of ground station support.
- Variation in the format and performance characteristics of the space links used in space missions.
- Changes in the routing path from contact to contact because of use of multiple ground stations or changes of the relative positions of multiple spacecraft.
- Noise characteristics on space links that (despite sophisticated error correction codes) produce more frequent data loss than on ground links.
- The asymmetry in the bandwidth available for the space station to TDRS link and the TDRS to ground terminal link needs to be taken into account. This asymmetry may affect the features of protocols that support end-to-end communications.

5.6. Protocol Synthesis

The material presented here is almost identical to that presented in section 4.6. for the first scenario. It is repeated here to make this scenario complete.

Protocol architectures are not developed in a vacuum. In general, it is an evolutionary process. The state of the technology, the operating environment, and the application requirement are the driving factors in the development of a conceptual protocol architecture. The evolution of the TCP/IP protocol architecture is a perfect example of this phenomena. As new applications are developed and fielded, the protocol architecture is enhanced to meet the additional requirements, or new protocols are developed. Therefore, it is worthwhile to identify the technology trends before synthesizing the conceptual protocol architecture.

5.6.1. Technology Trends

The robustness of the Internet has redefined the direction of computer communications networking. The deployment of popular applications and the need to support these applications more efficiently has led to development of new application level protocols as well as research into enhancing the TCP/IP protocol architecture. Data related traffic has already overtaken voice traffic being carried by present day networks and is growing at a much faster rate than voice traffic. This is validated by the transition taking place in the telecommunication industry to develop an integrated backbone network to carry voice, video and data. In addition, there are a number of initiatives in the standards world by various technology forums, international and national standards bodies to enhance existing protocols or to develop new protocols. Therefore, one has to take into account these technology trends in developing protocol architecture.

5.6.2. Trends in Standards

There are international, national and industry forums to develop standards so that communication between end systems can take place in an efficient way. Although these groups share a common goal (open communication among end systems), achieving common ground has been elusive. Recently, these groups have gone from a state of holy war to peaceful coexistence, which has benefited the user community.

The architects of the OSI protocol reference model have identified various drawbacks in the OSI model since its initial implementation. Since 1983, experts have claimed that the organization of the OSI upper layers (Application, Presentation, and Session) as described in the OSI reference model is a mess and needs to be restructured. Also, network architectures, such as the Aeronautical Telecommunication Network (ATN) which use the ISO protocol architecture for air to ground communications, have devised methods to bypass the presentation and session layers. They have done this to reduce the overhead and eliminate unnecessary functions present in these two layers.

Recently, ISO extended the application layer structure to allow a single control function to supervise a set of application service elements. Also, they have revisited the entire upper layer architecture. They now essentially allow implementations to slice the upper layers vertically and ultimately collapse the upper layers into a single, object-oriented service layer. The extended application layer structure (XALS) and revised OSI upper layer architecture are under study in the ISO defined application service object (ASO). The ASO will contain multiple application service elements, some formed by grouping session functional units into application service elements. The result is the elimination of the session layer.

The existing presentation layer functionality will be subsumed within a new association control service element, which will offer an association data service. As a result, the presentation layer will be removed from the OSI reference mode as well. This allows the ASO association control service element to directly interface with the OSI transport layer. These developments in a sense align the OSI architecture more closely with the TCP/IP protocol architecture. It also reduces the overhead and protocol complexity.

The ISO transport protocol TP4 and the TCP are not only functionally equivalent but operationally similar as well. A 1985 study performed jointly by the U.S. Defense Communications Agency and National Academy of Science concluded that TP4 and TCP are functionally equivalent and essentially provide similar services. Table 17 compares the functions provided by these two protocols.

Table 17. Comparison of TP4 and TCP Functions

Function	TP4	TCP
Data transfer	Blocks	Streams
Flow control	Segments	Octets
Error detection	Checksum	Checksum
Error correction	Retransmission	Retransmission
Addressing	Variable TSAP	16-bit
Interrupt service	Expedited data	Urgent data
Security	Variable in TP	Not available
Precedence	16 bits in TP	Not available
Connection termination	Nongraceful	Graceful

At the network layer ISO supports the Connectionless Network Protocol (CLNP) and the TCP/IP protocol architecture supports the Internet Protocol (IP). The CLNP and IP are functionally identical and both are best effort delivery network protocols. The major difference between the two is that CLNP accommodates variable length addresses, whereas IP supports fixed 32 bit addresses. (IPv6 supports a larger address space.) Table 18 compares the functions of CLNP to those of IP.

Table 18. Comparison of CLNP and IP Functions

Function	CLNP	IP
Version identification	1 octet	4 bits
Header length	1 octet, represented in octets	4 bits, represented in 32 bit words
Quality of service	QoS maintenance option	Type of service
Segment/fragment length	16 bits, in octets	16 bits, in octets
Total length	16 bits, in octets	Not present
Data unit identification	16 bits	16 bits
Flags	Don't segment, more segments, suppress error report	Don't fragment, more fragments
Segment/fragment offset	16 bits, represented in octets (value always multiple of 8)	13 bits, represented in units of 8 octets
Lifetime, time to live	1 octet, represented in 500 millisecond units	1 octet, represented in 1-second units
Higher layer protocol	Not present	Protocol identifier
Lifetime control	500 millisecond units	1-second units
Addressing	Variable length	32-bit fixed
Options	• Security • Priority • Complete source routing • Partial source routing • Record route • Padding • Not present • Reason for discard (Error PDU only)	• Security • Precedence bits in TOS • Strict source route • Loose source route • Record route • Padding • Timestamp

5.6.3. TCP/IP and ATM in a Satellite Environment

There is active interest in using satellite systems to support both TCP/IP and ATM networking technologies. NASA is actively involved in studying and testing the performance of the TCP protocol and testing the QoS parameters of the ATM technology using the ACTS satellite. The slow start, congestion avoidance, fast retransmit, fast recovery, and support of large windows and delayed acknowledgement are some of the TCP parameters that are being investigated.

Based on industry demands, the Communications and Interoperability Section (CIS) of TIA's Satellite Communications Division has started the ATM satellite standardization process. It has defined a set of satellite-based ATM network architectures for future physical layer specification. The network architectures cover both on-board switching and transparent satellites. The ATM technology offers a number of attractive features such as explicit rate based traffic management, QoS based routing, signaling, and switching which dynamically allocates bandwidth.

In addition, COMSAT has developed ATM products such as COMSAT Link Enhancer (ALE-2000) and COMSAT Link Accelerator (CLA-2000/ATM) that provide essentially an error-free satellite link in a bandwidth efficient manner at fractional T-1 and DS3 rates. The ALE-2000 supports efficient bandwidth utilization and fiber-like link quality. It significantly improves the performance of applications operating over satellite networks by inserting Reed-Soloman forward error correction into the data stream in addition to interleaving. This product incorporates features to improve link quality and application throughput, such as rate adaptation, adaptive forward error correction, interleaving, ATM cell header compression, and lossless ATM cell payload compression. Satellite based system such as Iridium, Teledesic, and Astrolink are using or planning to use an ATM based architecture for their systems.

NASA's ACTS system has already proven that it is possible to design and operate a high bandwidth satellite system. With advances in technology, it is a matter of time before high bandwidth system can be developed at lower cost.

5.6.3.1. Why Internet-Based Network Architecture

In a heterogeneous network environment, the networking technologies used by various organization range from COTS LANs to dialup networks. This means there are many different types of subnetworks that must be connected together. As no one has control over what the subnetwork will look like, the network layer (Internetwork) protocol has to be designed to work with whatever may be the type of subnetwork available. Therefore, the practical approach is to define one protocol that assumes minimal subnetwork functionality and place it firmly on the top of every subnetwork access protocol. This network architecture model treats every subnetwork and data link service as providing a basic data pipe. Each pipe should support a service data unit large enough to accommodate the header of the network layer protocol and a reasonable amount of user data. This is the IP or OSI connectionless network protocol model of networking. As the subnetwork technology changes, there is just one more subnetwork with which the network layer must interface.

5.6.3.2. Why TCP/IP Protocol Architecture

Although ISO's TP4 and the TCP transport protocols are functionally identical, TP4 is not widely implemented. There is limited practical knowledge about the protocol in the real world environment. On the other hand, TCP provides an excellent base of technology for extension. It is a highly robust protocol, widely distributed, and is freely available. Hundreds of individuals worldwide work to ensure that TCP continues to meet the needs of the Internet community. Therefore, TCP is cost effective to implement, and provides additional functionality that may be needed in the future.

In addition, the ISO's CLNP and IP are functionally similar in providing a connectionless network layer service to the transport layer. Here again, CLNP has not been deployed widely and has not been tested thoroughly in an operational environment. Therefore, it is recommended that the TCP/IP protocol architecture forms the starting point for the space station to ground terminal via TDRS scenario protocol architecture.

5.7. Scenario Unique Requirements

Although functionally equivalent to terrestrial networks, space communications networks often have performance and operational considerations that prevent direct use of existing commercial protocols. Protocols used in terrestrial networks assume that: connectivity is maintained; data loss due to corruption is rare; balanced bi-directional links are available; and most data loss is due to congestion. Further, vendors of commercial communications products that implement these protocols use these assumptions to maximize performance and economy in this environment. This results in the treatment of retransmission, recovery, and time-outs inappropriate for space operations. For the large majority of space nodes, the space environment makes performance of these protocols unacceptable.

To meet the above constraints protocols are required to provide interoperability across the spectrum of space nodes and between space data systems and the COTS based ground network environment. They have to provide a set of options and protocol data unit formats that can be scaled to satisfy the communication needs of both complex and simple nodes.

The protocol architecture should provide reliable stream or file transfers over existing and new link layer plus dynamic networking for multiple space node environments. Given the link characteristics and intermittent connectivity encountered over the space link, better performance is achieved by using a balance of upper-layer, confirmed, end-to-end services supported by link level error correction that avoids excessive retransmission. In addition, the architecture must be able to support multimedia applications.

5.8. Recommended Protocol Architecture

The goal of the protocol architecture is not only to support applications but also to lower the lifecycle costs by reducing development and operations costs in space communications systems. In addition, the protocol architecture should be able to extend Internet connectivity into space. The rationale for this approach is that both the data systems and the personnel (designers, operators, and users) associated with space missions are already using Internet protocols. The communications services that they need in space are very similar to those they have in ground networks. The easiest, lowest risk, and most direct way to achieve this goal is to adapt the protocols that are used on the ground.

Although the Internet protocols provide an excellent basis for space communications protocol development, the space environment presents a number of constraints that are seldom encountered in the design of terrestrial data communications networks. There are physical, operational, and resource differences. The physical differences include:

- Space link delays ranging from milliseconds to hours.
- Potentially noisy space data links.
- Limited space link bandwidth.
- Variation in sub-network types from simple busses to local and wide area networks.
- Interruptions in the end-to-end data path that can vary from bits lost, and link interruptions.

The operational differences include:

- Inherently sporadic nature of contact between space and ground.
- Maximum latency requirement due to "Teleoperations" activities.

The resource differences include:

- Limited onboard processing power.
- Limited onboard program memory.
- Limited onboard data buffering.
- Asymmetry in bandwidth between forward and return links.

Except for a very narrow range of operational conditions, the current off-the-shelf, Internet protocols do not satisfy the requirements encountered in the space mission environment. Therefore, the strategy is to: use COTS-supported standards wherever possible; capitalize on established user interface familiarity; and minimize software development costs. This approach allows one to take advantage of the hundreds of thousands of hours of operational experience that the Internet protocols have accrued.

5.9. NASA Conceptual Protocol Architecture

The suite of NASA space protocols should provide flexibility and optional features that allow designers to tailor a communications protocol suite to meet specific requirements and constraints without extensive software development. It should allow specific layers or protocols within layers to be included or omitted to create an optimal profile. This calls for a layered protocol architecture.

The space station to ground terminal via TDRS scenario architecture is shown in Figure 5.

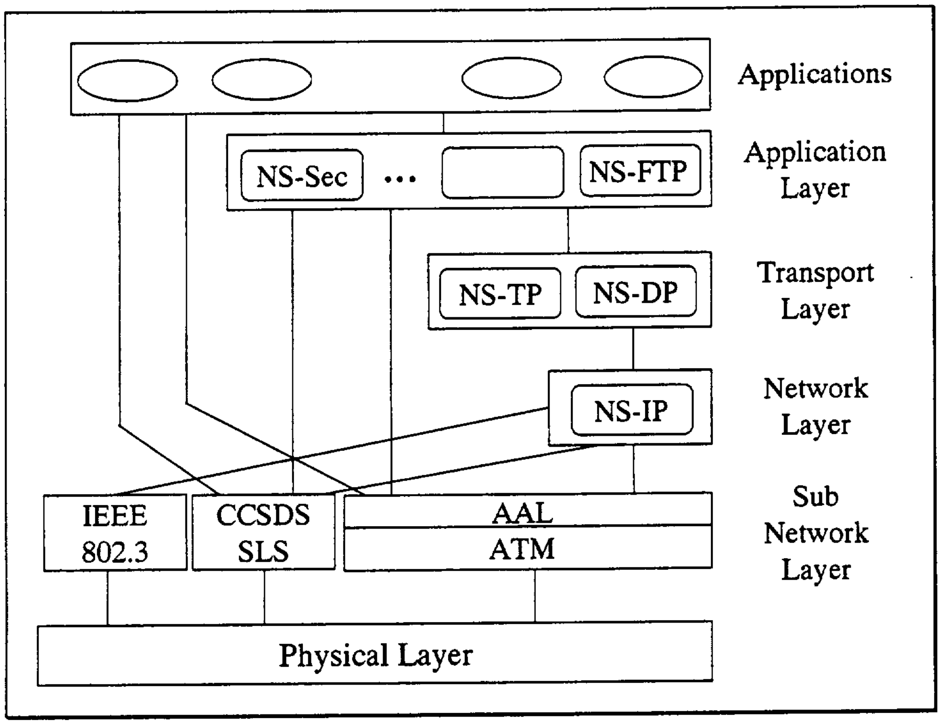

Figure 5. Recommended Space Station ↔ TDRS ↔ Ground Terminal Architecture

Figure 5 shows the NASA Space (NS) conceptual protocol architecture. As mentioned before, this scenario supports data and multimedia applications. In addition, there is a need to provide bit efficient protocols to support these applications. The conceptual protocol architecture consists of an application layer supported by the transport layer. The application layer protocols consists of NASA Space File Transfer Protocol (NS-FTP) and the NASA Space Security Protocol (NS-Sec). This protocol architecture is very flexible. It is easy to add more application layer protocols as requirements for such protocol arise.

The transport layer supports a reliable end-to-end protocol called NS-TP. The NS-TP supports functions that are similar to TCP and ISO TP4. In order to meet the space based communications requirements, modifications need to be made to this protocol. Some of the issues are identified in the transport layer section.

The space based applications presented in Table 15 require a connectionless transport protocol. The NASA Space Datagram Protocol (NS-DP) provides support for this service. NS-DP supports a minimum capability. It is similar to the ISO Connectionless transport protocol and TCP/IP's User Datagram Protocol.

The NS transport layer interfaces to the connectionless NS-IP protocol. The functions supported by NS-IP are similar to those of ISO's CLNP and TCP/IP's IP protocols. But in order to operate efficiently in a space based communications environment, a number of enhancements are identified.

For data only application the connectionless NS-IP interfaces to the existing CCSDS space link subnetwork (SLS) subnetwork layer. The user has the option of interfacing to the Ethernet (IEEE 802.3) link layer protocols within the space station. To support multimedia applications in a integrated fashion, ATM has been selected as an alternate subnetwork layer. Note that the ATM technology is capable of replacing the transport and network layers.

5.9.1. NASA Space System File Transfer Protocol (NS-FTP) Functions

The Internet File Transfer Protocol (FTP) in the TCP/IP architecture supports a rich set of file transfer capabilities. Compared to the ISO's FTAM, FTP is a widely used and stable protocol. The amount of FTP overhead needed is significantly less than required for FTAM. Therefore, FTP ideally suited for the bandwidth limited space based network environment. Table 19 shows the functions supported by the FTP.

As the Internet File Transfer Protocol (FTP) provides a rich functional set, the NS-FTP should use FTP as a starter set to define the file transfer functions and then add functions required to operate in the bandwidth limited space operations environment. Like FTP, NS-FTP should use two transport connections between host systems - a control connection to exchange control information, and a data transfer connection to move data file. Data is transferred from a storage device in the sending host to a storage device in the receiving host.

Both contact time and bandwidth are scarce resources in space operations. To operate in the resource restricted space environment NS-FTP should provide enhanced error recovery and restart capabilities. Interruptions in file transfers could be restarted from the point of interruption instead of starting over. This is a common feature supported by most of the Web-related download applications.

NS-FTP should also provide the capability to read or update part of a file on a remote system rather than the entire file. This avoids the transfer of a large amount of data when only a small part of the file is affected. Other NS-FTP extensions to FTP should provide integrity checks to recover from errors in file transfer or update operations. Finally, to conserve bandwidth and contact time, NS-FTP should suppress text messages between end systems involved in file operations.

Table 19. TCP/IP FTP Functions

FTP Functions
RETRIEVE
STORE
STORE UNIQUE
APPEND (with create)
ALLOCATE
RESTART
RENAME FROM
RENAME TO
ABORT
DELETE
REMOVE DIRECTORY
MAKE DIRECTORY
PRINT WORKING DIRECTORY
LIST
NAME LIST
SITE PARAMETERS
SYSTEM
STATUS
HELP

It is suggested that the application layer file transfer protocol support the following functions:

- Transfers of command and data files to the space station.
- Transfers of application software to the space station.
- Transfers of science or mission data to the ground without special processing to reorder or merge data sets.
- Limited management of files onboard the space station (delete, rename, and directory services).
- Automatic restart of transfers after an interruption.

- Read portions of files resident onboard the space station.
- Make updates/changes to files onboard the space station, without sending a complete replacement for the file to make minor modifications.

5.9.2. Security Protocol

In the NASA networking environment, network security is an important function. There are a number of security related protocols available from standards bodies. The Secure Data Network (SDNS) "SP3" protocol, the ISO Network Layer Security Protocol (NLSP), the Integrated Network Layer Security Protocol (I-NLSP), and the Internet Engineering Task Force's (IETF) Internet Protocol Security (IPSEC) all provide data confidentiality, data integrity, authorization, and access control. However, they have far greater overhead than is acceptable over space links.

The NS-Sec data protection protocol should provide the capability to control access to network resources. Only those users (or processes acting on behalf of users) with authorization should be granted access to network resources. The NS-Sec data protection protocol should provide the capability to verify the identity of the end system that originated network communications. The NS-Sec data protection protocol should provide an optional capability to digitally sign a message to indicate that the message was actually sent by the user (or process acting on behalf of the user) claiming to send it. The NS-Sec data protection protocol should provide the capability to ensure that the data sent is exactly the same as the data received. It should provide assurance that any unauthorized modification of the data will be detected while the data is in transit across the network.

There are two issues related to the security protocol environment. One is the amount of overhead required and the other is the where should the security protocol be placed. The SCPS-SP has solved the problem associated with overhead. But it is placed in between the transport and network layer to support end-to-end security. This means that all applications whether they need security or not are forced to incur additional overhead.

Therefore, it is suggested that the security protocol be moved to the application layer and only those applications that require security need incur this additional overhead. It is recommended that SCPS-SP be adopted as the NASA space security protocol.

5.9.3. Transport Layer Protocol

NS-TP provides end-to-end full and minimal reliability services. The full reliability service is provided by enhanced TCP. It supports end-to-end data transfer of a sequence of data units with full reliability (complete, correct, in sequence, and no duplication). It uses sequence checking to assure the sequence order and avoid duplication. It incorporates acknowledgments and retransmission requests to provide completeness. This protocol closes connections without loss of data.

The minimal reliability service is provided by the NASA Space Datagram Protocol (NS-DP). It is a connectionless transport protocol and sends data in datagrams. It transfers data with minimal reliability (correct, possibly incomplete, possibly out of sequence). It does not support sequence numbering, acknowledgment of receipt, or retransmissions.

The NS-TP is based on the Transmission Control Protocol (TCP). Enhancements are identified to improve performance in the space environment. Unmodified TCP performs poorly in communications scenarios with a large bandwidth-delay product and cannot operate efficiently with the unbalanced links typical of space-ground communications. The suggested extensions to the base protocols are intended to address the performance issues.

5.10. Differences Between Communications Environments

The material presented here is almost identical to the one presented in section 4.10. for the first scenario. It is repeated here to make this scenario complete.

TCP provides an excellent base of technology for adding extensions. It is a highly robust protocol, widely distributed, and is freely available. TCP is optimized to provide service in the terrestrial environment. There are significant differences between the terrestrial and space environments that affect a communication protocol's performance. Table 20 presents a summary of the main factors that affect TCP performance when operating in space environments.

Table 20. Factors Affecting TCP Performance in Spacecraft Environments

Factor	Terrestrial Environment	Spacecraft Environment
Bit error rate	$< 10^{-9}$	10^{-5} to 10^{-12}
Round trip delay	Millisecond to second	Seconds to hours
Continuity of Connectivity	Continuous	Intermittent: 10%(LEO) to 90% (TDRS) per orbit
Forward and reverse links	1:1 (equivalent rates)	10:1 to 2000:1 Some have down link only
CPU capacity	Unrestricted	Possibly low
Communication goals	• Fair access over time • High aggregate throughput over time • High reliability	• High throughput during contact • Maximum link utilization
Primary source of data loss	Congestion	• Congestion • Corruption • Link outage

5.10.1. Bit-Error Rates

The error performance of typical terrestrial networks has improved to a point that it is no longer considered as a typical source of data loss. With sufficient channel coding and application of radiated power, some satellite links can approach the error performance of the terrestrial environment. Reed-Solomon error control has proven to be of great benefit in space links. Both hardware and software solution to perform Reed-Solomon corrections in real time are available. For a link speed of 5 Mbps or less, software solutions have been shown to be adequate. Recent advancements in microprocessor speeds may enable a software solution for processing data at higher rates. A software solution for high-rate Reed-Solomon processing is preferable to a hardware solution in that a software solution would reduce system lifecycle costs and maximize system portability. In the future, the bit error may play a less significant roll in the performance of the transport layer.

5.10.2. Round Trip Delay

Round trip delays in the terrestrial communication environment are typically in the tens of milliseconds to low hundreds of milliseconds. In the space station communications environment, round trip times of 500 milliseconds are the minimum that one expects when communicating through a geostationary satellite. Deep space communications can increase round trip delays to hours.

Long round-trip delays limit the usefulness and effectiveness of TCP's feedback from the remote communication endpoint. This causes problems when the protocol needs to react to changes in the network, but does not receive feedback about the changes until long after they have occurred. Note that long delays are not exclusively a result of speed-of-light propagation times. Low data transmission rates add delay to a network, as can half-duplex operations. Finally, queuing in intermediate systems is a source of delay.

5.10.3. Continuity of Connectivity

Topology changes are infrequent in a terrestrial communications environment. However, space based systems have predictable (possibly highly dynamic) connectivity characteristics. Low earth orbiting satellites typically have connectivity through a single ground station 10% of the time or less. Changes to the number of ground stations or the satellite's orbit can improve this, but even NASA's TDRS system offers only about 90% coverage.

5.10.4. Forward and Reverse Link Capacity

In the terrestrial communication environment, communication links are typically full duplex with the same data rate in both directions. This is not the case in space environments. It is not unusual to have large differences in forward and reverse link capacities. Ratios of 1000:1 are not unusual. This degree of asymmetry causes problems for TCP, which uses a stream of acknowledgments for transmitting data packets. Thus, very low capacity acknowledgment channels limit the transmission rate of data packets.

5.10.5. CPU and Memory Capacity

In the terrestrial communications environment, the availability of computing resources is essentially unrestricted. This is not the case in the space station where power, weight, and volume are all precious commodities. The amount of computational resource available to any subsystem in the space station must be traded-off against the benefits of applying that resource elsewhere. Therefore, it is important to be aware of these constraints. The loss of data due to bit-errors has a disproportionately bad effect on TCP's performance because TCP interprets any loss as an indication of network congestion. The appropriate response to network congestion is to reduce the offered load to the network. TCP's congestion response reduces the offered load by half, then builds back slowly over several subsequent round trips. The effect of this response to bit-errors is to significantly under utilize the communication channel.

5.10.6. Primary Source of Data Loss

The primary source of loss in terrestrial networks is congestion, and TCP is optimized to control congestion. The space communication environment is a mixed-loss environment, with losses occurring due to three causes: bit-errors, topology changes (link outages), and congestion. To treat all losses as congestion results in unnecessary reductions in offered load. The increased round trip times in these environments delays the restoration of full-rate transmission.

5.11. Network Layer

The functional requirements for network services for the transfer of data between end points within a space data communications system are stated below:

- Support for multiple routing options
- Packet lifetime support with auto discard
- Support for precedence handling
- Provide efficient operation in constrained-bandwidth environments
- Separate reporting of congestion and corruption

The ability to route data from source to destination is characteristic of essentially all protocols that operate at the network layer of the OSI Basic Reference Model. Common to all of the prospective environments is that bandwidth may be constrained, either unidirectionally or bidirectionally. This constraint results in a requirement to operate with high bit-efficiency. Bit-efficiency quantifies the fraction of transmitted bits that are user data. Improving bit-efficiency may be accomplished in two ways: by increasing the amount of user data per unit of protocol control information (i.e., header information), or by decreasing the amount of protocol control information per unit of user data.

The first approach (making packets longer) is simple, but does not work well in environments that are prone to bit-errors. It also does not work well when the user's data does not lend itself to aggregation.

The second approach (reducing protocol header overhead) is the approach commonly used to obtain high bit-efficiency. Several requirements derive from the need to operate in bandwidth constrained environments: multicasting, support for address translation, and precedence-based data handling. All address bandwidth-related constraints and are described in subsequent paragraphs.

Multicasting is a technique for improving network-wide bit-efficiency. The technique of multicasting allows addressing of data to a group of destination systems. Rather than sending an unique copy of the data to each remote system, data is sent to the group address. Intermediate systems replicate the multicast packet only as necessary in order to reach all of the destination systems in the multicast group.

Header compression can enhance bit-efficiency in networks that can be characterized as having few source-destination pairs that account for most of the network's traffic. In IPv6, these are identified as flows. For these flows, the source and destination addresses can be replaced by an identifier and this is similar to the SCPS managed connection.

Precedence improves operation in bandwidth-constrained environments in two ways. First, it controls the order of service, which reduces queuing delay and variation in queuing delay for high precedence traffic. Second, precedence controls the order of packet discarding when congestion occurs. If packet discarding is required, low precedence packets are discarded before higher precedence packets.

Packet lifetime control provides protection against transient routing loops. A transient routing loop is formed when routing tables in the network are not synchronized. This condition can occur as a result of using certain routing protocols. While a routing loop is in existence, the links forming the loop may become progressively more congested. Packet lifetime control ensures that data packets do not remain in the network indefinitely. They are discarded once they have exceeded their "lifetime." This mechanism combined with either automated or manual means to update the routing tables provides control over routing loops.

Signaling of network conditions to upper-layer protocols is required to allow those protocols to become aware of and to adapt to changing conditions within the network. Signals that may be passed to the upper-layer protocols include indications of network congestion, network corruption, and link outages. This requires the network to identify the conditions at points in the network that may be remote from the end systems that host the upper-layer protocols. It also requires the network propagate network-internal signals to the affected end systems for delivery to the upper-layer protocols.

5.11.1. Shortcomings of Using IP in Space Networks

The Internet Protocol (IP) is a highly capable, widely used protocol. Table 21 identifies IP capabilities and the issues associated with using it in a space based network environment. Most of these issues are related to the limited bandwidth in the space environment.

Table 21. Support of SCPS Network Requirements by IP

Protocol Function	IP
Routing	Yes
Support for bandwidth limited environment	No
Multicast support	Yes
Priority	Yes
Header compression	Yes – not supported in COTS
Priority	Partial
Packet life time control	yes
Signaling to support upper layer	Partial

IP supports routing method that forward data from source to destination. In general, IP does not provide any explicit support for operating in bandwidth limited environments. IP headers are a minimum of 20 octets in length, and may be made longer with the addition of options. IP provides support for multicasting, but has no mechanism for shortening its headers.

The IP header contains a field to carry eight levels of precedence. However, COTS products typically do not make any use of the field. In particular, high precedence packets would not benefit from a reduced probability of discard in congested routers, nor would they receive any reduced queuing delays in routers. The capabilities in IP for packet lifetime control are adequate for most environments.

With respect to signaling of network conditions, some IP implementations provide partial support. The Internet Control Message Protocol (ICMP) (the companion protocol to IP that handles such signaling) has the ability to generate congestion signals. However, research in this area has resulted in specifications such as Random Early Detection (RED). However, RED is not widely deployed nor is its Explicit Congestion Notification (ECN) option. There is no signaling provided to indicate loss, whether due to corruption or to link outage.

5.11.2. Suggested Enhancements to IP

All the issues identified above are in one way or another limited to using the limited bandwidth more efficiently. One easy way to accomplish this goal is to not transmit unnecessary header elements. This design decision increases the processing to format and parse headers in favor of reducing the number of bits that are transmitted.

Network protocols typically route data from source to destination by selecting the "next hop" router based on the destination address. There are many routing methods by which the next hop router is selected. One of method is to use routing tables that may be statically or dynamically configured to selects the next hop router. The routing methods reduce the complexity and overhead associated with routing but sacrifice the dynamic route selection capability.

In a space based networking environment, it is possible to reduce header overhead by performing header compression and address translation as suggested by the SCPS-network protocol. SCPS-NP's method of using a single address to represent an address pair is called a managed connection. In this method an IP source-destination pair may be translated into three alternate managed connection address:

- An Extended Path Address which represents the two addresses with a single four-octet address;
- A pair of Basic End System Addresses which represents the two four-octet addresses with a pair of corresponding one-octet addresses; or
- A Basic Path Address which represents the pair of four-octet addresses with a single one-octet address.

SCPS-NP uses address translation tables that are configured statically to translate addresses. The translation tables are identical throughout the network. In addition, address translation can be used to support multicasting, and to identify multicast (group) addresses.

5.12. Subnetwork Layer

The next layer in the NASA Space protocol architecture is the subnetwork layer. The subnetwork is mostly technology dependent. It can range from Ethernet to ATM depending on the environment and the state of the technology. As new subnetwork technologies are developed, they can be easily incorporated into the protocol architecture. Similarly, existing space-based subnetworks can interface to the network layer. Even though it is possible to interface any of the existing subnetwork technologies to the network layer, we present only ATM and the existing Space Link Subnetwork (SLS) as examples.

5.12.1. Space Link Subnetwork

To share the limited bandwidth of the space-to-ground link, a CCSDS recommendation for Advanced Orbiting Systems has developed the concept of a CCSDC virtual channel for the space link subnetwork. The virtual channel facility allows one physical space channel to be shared among multiple higher-layer traffic streams, each of which may have different service requirements. A single physical space channel may therefore be divided into several separate logical data channels, each known as a "Virtual Channel" (VC). Each VC is individually identified and supports a single "Grade of Service."

To facilitate simple, reliable, and robust synchronization procedures, fixed-length protocol data units are used to transmit data through the weak-signal, noisy space channels. The protocol data units are each associated with one particular VC and are known as "Virtual Channel Data Units" or VCDUs. A service option internal to the VCDU can also produce a protocol data unit known as a "Coded Virtual Channel Data Unit", or CVCDU. Each VCDU and CVCDU contains a header and trailer (which provide space link protocol control information) and a fixed-length data field within which higher-layer service data units are carried. The SLS supports six different types of services: encapsulation, multiplexing, bitstream, virtual channel access, virtual channel data unit, and insert.

The encapsulation service provides a facility whereby variable-length, octet-aligned service data units which are not formatted as CCSDS Packets may be transferred across the SLS. The transfer is asynchronous and sequence preserving.

The multiplexing service provides a facility whereby variable-length, delimited, octet-aligned service data units, which conform to the Version-1 CCSDS Packet format, may be multiplexed together for transfer across the SLS on the same VC. The transfer is asynchronous and sequence preserving.

The bitstream service provides a facility whereby serial strings of bits, whose internal structure and boundaries are unknown may be transferred across the SLS. The transfer is sequence preserving and may be either "asynchronous" or "isochronous." An isochronous transfer from service interface to service interface is provided with a specified maximum delay and a specified maximum jitter at the service interface. High-rate video data may use the isochronous bitstream service.

The virtual channel access service provides a facility whereby a project organization may transfer private service data units (which are sized to exactly load the fixed-length data field of one dedicated VCDU and whose internal structure is unknown) across the SLS. The transfer can be either asynchronous or isochronous and is sequence preserving.

The physical channel function creates one dedicated space data transmission path. A continuous stream of data bits is accepted at the sending side, modulated, serially transmitted through the physical space medium, demodulated, bit synchronized, and delivered through the receiving interface.

The insert service provides a facility whereby private octet-aligned service data units may be transferred isochronously across the SLS in a mode which efficiently uses the space channel transmission resources at relatively low data rates.

5.12.2. Virtual Channel Function

At the sending side, the virtual channel function accepts service data units from higher-layer functions. It then builds them into the space link protocol data units (VCDUs or CVCDUs) and applies error control required by different grades of service, commutates the VCDUs/CVCDUs into an appropriate sequence, and submits them as a serial stream to the physical Channel function for transmission through one physical channel.

At the receiving side the serial stream is synchronized to find the boundaries between VCDUs/CVCDUs, which are then passed through error control procedures and decommutated. The higher-layer service data units are then extracted and passed back through the receiving service interface.

During transmission through the physical channel, each VCDU or CVCDU is carried synchronously within one "Channel Access Data Unit" (CADU). The CADUs provide fixed-length "channel access slots" which occur at precise time intervals that are synchronized with the transmitted bit rate, and whose boundaries are delimited using "synchronization markers." The commutated sequence of VCDUs/CVCDUs is transmitted so that all of the synchronous channel access slots are occupied. In situations where no valid higher-layer data are ready for release, a VCDU/CVCDU containing "fill" data is commutated into the transmitted sequence. The continuous and contiguous stream of CADUs, known as a "Physical Channel Access Protocol Data Unit," is transferred through the physical channel.

Service data units associated with the encapsulation, multiplexing, bitstream or virtual channel access services are placed into a "Data Unit Zone" within the data field of the VCDU or CVCDU.

5.13. Asynchronous Transfer Mode (ATM) as a Subnetwork

ATM is a packet mode technology that uses fixed size cells consisting of a 5-octet header and a 48-octet information field to transmit information. ATM is both a technology and potentially a service. Sometimes the service is called cell relay. The cell switching technology is highly flexible and can handle both constant bit rate traffic and variable bit rate traffic easily. ATM is a streamlined protocol with minimal error and flow control capabilities. This reduces the number of overhead head fields.

ATM is a connection-oriented technology. Although cell delivery is not guaranteed, the order is. The two important layers of the ATM protocol architecture are the ATM layer and the ATM Adaptation layer (AAL). ATM layer is common to all services and provides cell transfer capabilities and the AAL layer is service dependent. The AAL layer maps higher layer data into ATM cells.

ATM layer uses logical connections referred to as virtual channel connections (VCC). The VCC is the basic unit of switching. A VCC is established between end users to transport data between the users. In addition, ATM provides another layer of switching based on the concept of Virtual Path (VP). A virtual path connection is a bundle of VCCs that have the same end points. ATM supports quality of service, switched and permanent virtual channel connections, cell sequence integrity, traffic parameter negotiation, and usage monitoring. The types of traffic parameters that can be negotiated include average rate, peak rate, burstiness, and peak duration. ATM uses signaling mechanisms to set up and release virtual connections.

To support a wide range of applications, ATM supports real time and non-real time services. Real time services include constant bit rate and real time variable bit rate. Non-real time services include non-real time variable bit rate, available bit rate, and unspecified bit rate.

The AAL layer provides services such as error handling, segmentation and reassembly to enable large blocks of data to be carried in the information field of ATM cells, handling of lost and mis-inserted cell conditions, and flow and timing control. To minimize the number of AAL protocols, four classes of services were defined to cover a broad range of requirements. Four types of AAL protocols were specified ranging from AAL1 to AAL5. Among these, AAL5 is the most popular one to transport bursty data. AAL5 was introduced to reduce protocol processing and transmission overhead and to ensure adaptability to existing transport protocols.

5.13.1. IP over ATM

RFC "1932 IP over ATM", specifies how ATM can be used as a subnetwork in an enterprise wide IP-based network infrastructure. The issues that need to be addressed in such an architecture are:

- Encapsulations below the IP level
- Degree to which a connection oriented lower level is available and used
- Type of address resolution at the IP subnetwork level (static or dynamic)
- Degree to which address resolution is extended beyond the IP subnetwork boundary
- Type of routing (if any) supported above the IP level

In this model the ATM layer acts as a subnetwork and provides the services expected by the IP network layer. Because ATM is connection oriented packet mode technology, there are a number of issues on the ATM side that need to be addressed. In addition, there are a number of alternate ways to interface to the ATM layer (ATM Forums Multiprotocol over ATM). Notice that ATM over IP is an active area of research and is going through the regular standardization process in the ATM Forum and the IETF. Some of the issues that need to be considered are:

- Types of services provided by the ATM Adaptation Layers (AAL) (Quality-of-Service, the connection-mode, etc.)

- Type of virtual circuits used (PVCs versus SVCs).

- Type of support for multicast services.

- Signaling methods

5.13.2. The Classical IP Model

The classical IP model was suggested at the Spring 1993 IETF meeting and retains the classical IP subnetwork architecture. This model simply consists of cascading instances of IP subnetworks with IP-level routers at the IP subnetwork borders. Forwarding IP packets over the classical IP model is straightforward using well established routing techniques and protocols. SVC-based ATM IP subnetworks are simplified in that:

- They limit the number of hosts that must be directly connected at any given time to those that may actually exchange traffic.
- The ATM network is capable of setting up connections between any pair of hosts. Consistent with the standard IP routing algorithm, connectivity to the "outside" world is achieved only through a router, which may provide firewall functionality if so desired.
- The IP subnetwork supports an efficient mechanism for address resolution.

The IP Over ATM Working Group has addressed a number of issues related to the classical IP over ATM model. RFC-1483 addresses methods of encapsulation and multiplexing. Two methods of encapsulation are defined, an LLC/SNAP and a per-VC multiplexing option. RFC-1577 defines an address resolution server to resolve address related issues. The default MTU size is addressed in RFC-1626 and is based on the MTU discovery protocol. To support IP multicasting, the ATM subnetwork must either support point-to-multipoint SVCs or multicast servers, or both. Signaling and QoS related issues are addressed in RFC-1755. These include VC management procedures (when to time-out SVCs, QoS parameters, service classes, explicit setup message formats for various encapsulation methods, node (host or router) to node negotiations, etc.)

5.13.3. Encapsulation Methods

Two additional encapsulation techniques have been discussed within the IP over ATM Working Group, which differ from those given in RFC-1483. These have the characteristic of largely or totally eliminating IP header overhead. These models were discussed in the July 1993 IETF meeting in Amsterdam, but have not been fully defined by the Working Group. The techniques are bit-efficient and, hence, are ideal candidates for satellite based communications environment.

TULIP and TUNIC assume single hop reachability between IP entities. Following name resolution, address resolution, and SVC signaling, an implicit binding is established between entities in the two hosts. In this case full IP headers (in particular source and destination addresses) are not required in each data packet.

The first model is "TCP and UDP over Lightweight IP" (TULIP) in which only the IP protocol field is carried in each packet; everything else being bound at call setup time. In this case the implicit binding is between the IP entities in each end system. Since there is no further routing problem once the binding is established, AAL5 can indicate packet size, fragmentation cannot occur, and ATM signaling will handle exception conditions, the absence of all other IP header fields and of ICMP should not be an issue. Entry to the TULIP mode would occur as the last stage in SVC signaling, by a simple extension to the encapsulation negotiation described in RFC-1755.

TULIP changes nothing in the abstract architecture of the IP model, since each end system or router still has an IP address that is resolved to an ATM address. It simply uses the point-to-point property of VCs to allow the elimination of some per-packet overhead. The use of TULIP could in principle be negotiated on a per-SVC basis or configured on a per-PVC basis.

The second model is "TCP and UDP over a Nonexistent IP Connection" (TUNIC). In this case no network-layer information is carried in each packet; everything being bound at virtual circuit setup time. The implicit binding is between two applications using either TCP or UDP directly over AAL5 on a dedicated VC. If this can be achieved, the IP protocol field has no useful dynamic function. However, in order to achieve binding between two applications, the use of a well-known port number in classical IP or in TULIP mode may be necessary during call setup. This is a subject for further study and would require significant extensions to the use of SVC signaling described in RFC-1755.

TULIP/TUNIC can be presented as being on one end of a continuum opposite the SNAP/LLC encapsulation, with various forms of null encapsulation somewhere in the middle. The continuum is simply a matter of how much is moved from in-stream demultiplexing to call setup demultiplexing. The various encapsulation types are presented in Table 22. Encapsulations such as TULIP and TUNIC make assumptions with regard to the desirability of supporting connection-oriented flow.

Table 22. Summary of Encapsulation Types

Encapsulation	In setup message	Demultiplexing
Demultiplexing	Nothing	Source and destination, source and destination family, protocol, ports
NULL encaps	Protocol family	Source and destination address, protocol, ports
TULIP	Source and destination address, protocol family	Protocol, ports
TUNIC - A	Source and destination address, protocol family protocol	Ports
TUNIC - B	Source and destination address, protocol family protocol, ports	Nothing

6. SCENARIO 3: MULTICASTING

This scenario involves multicast communications. There are two situations. The first involves a spacecraft broadcasting to multiple terrestrial receivers. This is referred to as the 1 to N multicast situation. The other situation involves multiple terrestrial sources communicating with a single ground receiver via the same spacecraft. This is the N to 1 multicast situation.

6.1. NASA Application Types and Characteristics

The existing NASA application categories, with the associated application types and their respective characteristics are shown in Tables 23 and 24. These characteristics form the basis for assessing the protocol functional requirements at each layer in the protocol stack for the applications to be supported. To support the analysis, the number of receivers in the 1 to N situation is assumed to be 200. Likewise, the number of transmitters in the N to 1 situation is assumed to be 200.

The table shows that none of the application in require security. The response time range from seconds to minutes. The bandwidth requirement range from 1 Mbps to 200 Mbps. The precedence levels range from high to medium. In addition, message integrity ranges from high to medium. The availability is spread over 0.999 to 0.99999. For the 1 to N scenario the total daily traffic is found by summing the column defined as the total bandwidth requirements. The peak hour load to be supported by the system 15% of the total daily traffic. The peak hour load is 30.23 Mbps.

For the N to 1 scenario, the peak hour load is 0.08 Mbps.

Table 23. Scenario 3: 1 Spacecraft Transmitter to N=200 Ground Receivers

Application Category	Transfer Unit	Response Time	Load Factor	Total Bandwidth Requirements	Precedence	Integrity	Availability	Security	Scalability
Telemetry/Navigation	Medium Sync Continuous	1 - 3 Sec	1	512 Kbps	Medium	High	99.99	E	1-10 Moderate
Emergency/Flight Critical	Small Sync Infrequent	1-3 Sec	1	64 Kbps	High	High	99.999	NR	1-10 Slow
Experiment Support/ Mission Payload	Large Async Continuous	3-5 Min	200	200 Mbps	Medium	Medium	99.99	A + E	200-1000 Moderate
System/Vehicle Maintenance	Large Async Medium	10-20 Min	1	1 Mbps	Medium	Medium	99.9	NR	1-10 Fast

Table 24. Scenario 3: N=200 Ground Transmitters to 1 Ground Receiver via a Spacecraft

Application Category	Transfer Unit	Response Time	Load Factor	Total Bandwidth Requirements	Precedence	Integrity	Availability	Security	Scalability
Data Collection (Real Time)	Small Async Infrequent	NA	200	512 Kbps	Medium	Medium	99.95	NR	1-1000 Moderate

6.2. Environment Analysis

The multicast environment is characterized by two cases: multicast from a single space-based source to multiple terrestrial receivers (1 to N); and multicast from multiple terrestrial sources to a single terrestrial receiver through a spacecraft (N to 1). The scenarios are shown in Figures 6 and 7.

6.2.1. Communication and End System Environment

The space information infrastructure presents a significantly different environment from the ground systems. In space, there are relatively few end systems and networks and the communications requirements are driven by the extreme mass, power, and volume constraints, together with the delay and expense of developing space-qualified hardware.

The space communications environment is further complicated by the characteristics of the space/ground link. Limited signal strength and noise make data loss through corruption far more likely than in ground networks, and long propagation times cause terrestrial protocols to operate inefficiently or to fail to function at all.

6.3. Transmission Facility Selection

Ground segment transmission facilities must accommodate the ground/space link. The spacecraft is assumed to have its data units interfaced to the onboard systems at the respective levels of the protocol stack. As compared to the ground segment, the spacecraft's capabilities are fixed and inflexible. Therefore, the transmission facility selection defaults to the onboard transmission systems. The IIN spacecraft is assumed to have the necessary onboard interfaces (logical and physical) and transmission facilities to satisfy the mission-specific application requirements.

6.4. Switching Technology Selection

The material presented here is similar to that presented in the first two scenarios. It is repeated here to make this scenario complete.

The next step in the methodology is the choice of how the various users of the system should share the transmission media. The concept of resource sharing is fundamental to any computer communications system. There are several possible ways of sharing computer and communications resources. Point-to-point communications systems use multiplexing or switching techniques for resource sharing. In the case of multi-point or broadcast communications systems, polling and contention are two alternatives for resource sharing. The multicast scenario is a multipoint communications system.

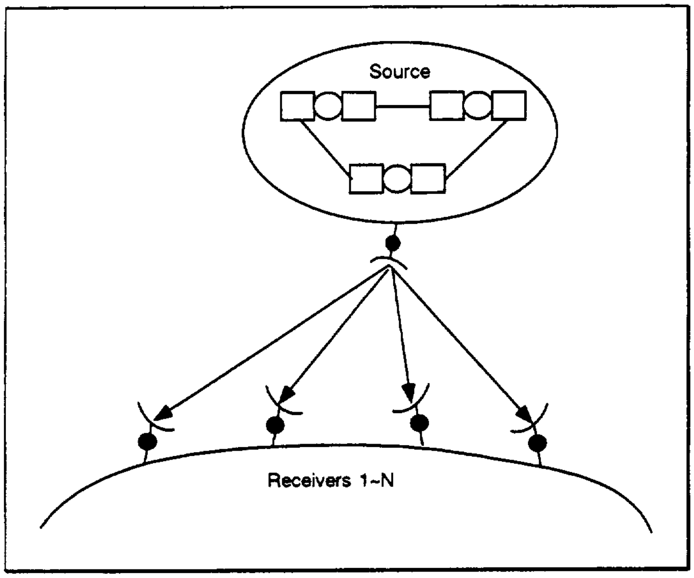

Figure 6. Scenario 3: Single Source, Multiple Receivers (1 to N)

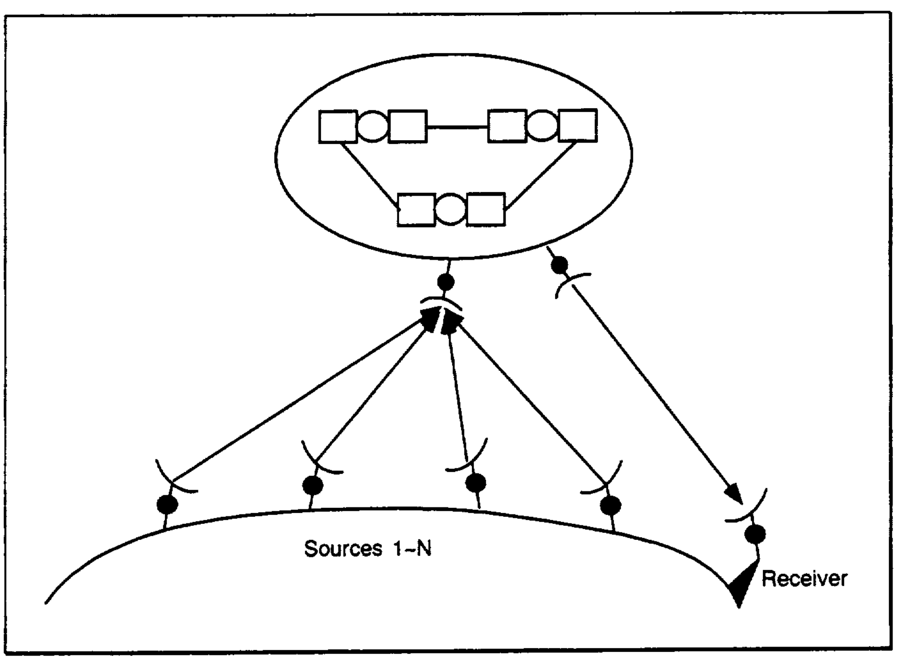

Figure 7. Scenario 3: Multiple Sources, Single Receiver (N to 1)

Possible switching technologies that can be used for resource sharing are:

- Circuit (or line) switching
- Message switching
- Packet switching

6.4.1. Circuit Switching

A circuit-switching network provides service by setting up the dedicated physical path between two communicating subscribers. The complete circuit is set up by a special signaling message. The signaling message passes all the way through the network and a return signal informs the source that data transmission may begin. Path setup time is usually on the order of seconds. The entire path remains allocated to the transmission until either the source or destination releases the circuit. Circuit switching is the common method for telephone systems. It is an appropriate method for communication when the two subscribers have identical equipment such as voice telephone instruments and no speed or code matching is necessary. Also, it is appropriate if the users communicates at a fairly constant rate for a long period of time. Circuit switching is inefficient for bursty traffic, which has a high peak-to-average ratio.

6.4.2. Message Switching

In message switching, a single path is selected for internodal transmission of a given message. The message is a logical data unit that travels from the source node to the next node in the path and incrementally through intermediate nodes to the destination. Each node in the path assembles and stores the entire message before forwarding it to the next node. This store-and-forward process introduces queuing delays at any node when a path or the next node is too busy to handle the message transmission. Such systems have been built to optimize the use of network lines and to remove the burden of communications responsibility from the user. Speed and code conversion can be performed in such networks. Examples of message-switched networks include Telex, AUTODIN I and the SITA airline system. Throughput delays in message-switched systems built in the last decade are usually on the order of many minutes.

6.4.3. Packet Switching

The final switching technology is packet switching. It is similar to message switching except that secondary storage is not used in the network. Messages are split into smaller units called packets, which are routed independently on a store-and-forward basis through the network. Thus, many packets of the same message may be in transmission simultaneously. This is one of the main advantages of packet switching. Packet switching is the most dynamic switching technique since it makes effective use of circuit bandwidth.

There are various packet mode methods such as Ethernet, Token ring, FDDI, and ATM for Local Area Network (LAN) environments. Technologies such as X.25, Frame Relay, SMDS and ATM are used in Metropolitan and Wide Area Network (MAN and WAN) environments. A simplified comparison can be made among circuit, message, and packet switching. It is worthwhile to note that all of such comparisons are dependent on technology and that there is nothing implicit in the functions performed by these switching methods which makes one superior to the other. That is, a message switching system with high-speed lines can outperform a slow-speed packet-switching system. Table 25 presents a comparison of these switching techniques.

Table 25. Comparison of Switching Techniques

Attribute	Circuit Switching	Message Switching	Packet Switching
Physical connection	Yes	No	No
Real time	Yes	No	Yes
Data storage	No	Yes	Temporary
Blocking with overload	Yes	No	Yes
Delays with overhead	No	Yes	Yes
Error control	No	Yes	Partial
Speed/Code conversion	No	Yes	Yes
Delayed delivery	No	Yes	Possible
Multiple address	No	Yes	Possible

By comparing various aspects of the three switching technologies, it is clear that packet switching provides a number of advantages over the other two technologies. In addition, the technology trend is such that more and more applications are being supported by packet mode technologies because of the inherent capability to dynamically share bandwidth and the flexibility in offering services compared to both circuit mode and message mode switch technologies.

The popularity of the Internet and the associated technologies are providing additional incentives to move audio and video services to packet mode switching. The next generation satellite based systems such as Iridium and Teledesic are using packet mode switching technology to support a full spectrum of services. Therefore, we recommend that packet mode switching technology as the appropriate technology for this architecture.

6.5. Protocol Requirements Analysis

Tables 26, 27, 28 and 29 show the applications and protocol functions for the multicast scenarios. Each column except the first column represents the application and its characteristics. Column 1 lists the protocol functions as identified in the ISO OSI protocol architecture reference model as a guide. It is well known that OSI protocol architecture is ideally suited for protocol analysis purpose, even though the implementation of the model is not popular due to the significant amount of overhead required

In this analysis we have included both connection oriented and connectionless protocol layers. The application, presentation and session layers provide connection-oriented service only. A close look at the protocol functions required by the various applications reveals that all of the applications use only the connection establishment and connection release functions of the presentation and the session layers.

In addition, it is better to allow the applications or application layers protocols to provide the syntax transformation usually supported by the presentation layer. This approach has two advantages. First the applications are free to choose the best encoding scheme. This eliminates the overhead associated with and the need for the presentation layer. In addition, the need to set up yet another connection at the presentation layer is eliminated.

A similar argument can be made to remove the session layer from the architecture. In the OSI architecture model, the session layer provides some of the functions required by the application layer entities. This creates a situation where the application service elements have to bypass the presentation layer to get the service from the session layer. Therefore, it is better to move these functions to the application layer and merge them with the application service elements.

Note that the merging of the presentation layer and session layer functions in the application layer eliminates the overhead due to these two layers and the need to set up a connection.

Table 27 and 29 present the results of the analysis. In these tables the functions related to the presentation and session layers are added to application layer and those that are not required are eliminated. In addition, the connection oriented network layer functions are also removed. As we can see from the Tables, the connection oriented network layer provides functions similar to those supported by the transport layer. Added to that, a connection oriented network layer protocol requires connection setup and release mechanisms that add to the overhead. In our opinion, there is no need provide the same function at two different layers. Providing these functions at the transport layer provides an end-to-end capability. Therefore, the connection oriented network layer functions are also removed from the protocol architecture. Tables 24 and 26 form the basis for the conceptual protocol architecture.

Table 26. Multicasting: 1 to N Scenario Applications

Application Category	Telemetry/Navigation		Emergency/ Flight Critical		Experiment Support/ Mission Pay Load		System/Vehicle Maintenance		
Characteristics/Types	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	System Diagnostics	Event Reports	Testing
Application Layer Functions									
Applications identifications	X	X	X	X	X	X	X	X	X
Application context required	X	X	X	X	X	X	X	X	X
Presentation context required									
Presentation service requirements									
Session service requirements									
Turn management									
Synchronization									
Recovery from temporary loss of presentation connection									
Synchronous operation	X				X				
Asynchronous operation		X	X	X		X	X	X	X
Real time	X		X	X					
User Authentication									
Linked operation									
Presentation Layer Functions									
Presentation connection establishment, and its termination with its peer	X	X	X	X	X	X	X	X	X
Negotiation of syntax for presenting application data									
Syntax transformation including data compression									
Data transfer by utilizing the services of the lower layers	X	X	X	X	X	X	X	X	X
Dialogue control									
Session Layer Functions									
Connection establishment	X	X	X	X	X	X	X	X	X
Connection release	X	X	X	X	X	X	X	X	X
Connection abort									
Activity management									

Application Category	Telemetry/Navigation		Emergency/ Flight Critical		Experiment Support/ Mission Pay Load		System/Vehicle Maintenance		
Characteristics/Types	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	System Diagnostics	Event Reports	Testing
Major and minor synchronization									
Symmetric synchronization									
Resynchronization									
Exception									
Negotiated release									
Abort services									
Data transfer by utilizing the services of the lower layers	X	X	X	X	X	X	X	X	X
Transport Layer Functions - Reliable Transport Required									
Precedence	X	X	X	X	X	X	X	X	X
Segmentation	X	X			X	X	X	X	X
Graceful closing			X	X			X	X	X
Flow control					X	X	X	X	X
Integrity			X	X	X	X	X	X	X
Duplicate control							X	X	X
Multiplexing								X	
Sequence control							X	X	X
Blocking								X	
Error detection			X	X	X	X	X	X	X
Error recovery			X	X	X	X	X	X	X
Expedited data transfer									
Transport Layer Functions - Reliable Transport Not Required									
Segmentation	X	X			X	X	X	X	X
Data transfer	X	X							
Network Layer Functions - Connection-Oriented									
Connection establishment and its maintenance									
Multiplexing of connections									
Re-initialization or reset of connections									
Addressing, routing and relaying	X	X	X	X	X	X	X	X	X
Normal and expedited data transfer									

Application Category	Telemetry/Navigation		Emergency/ Flight Critical		Experiment Support/ Mission Pay Load		System/Vehicle Maintenance		
Characteristics/Types	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	System Diagnostics	Event Reports	Testing
Sequencing and flow control, segmentation and re-assembly	X	X			X	X	X		X
Error detection, notification and possibly recovery	X	X	X	X	X	X	X	X	X
Network Layer Functions - Connectionless									
Addressing, routing and transfer of data	X	X	X	X	X	X	X	X	X
Error detection and notification	X	X	X	X	X	X	X	X	X
Access Control									
Source Authentication									
Confidentiality									
Possible segmentation	X	X			X	X	X		X
Multicasting	X	X	X	X	X	X	X	X	X
Data Link Layer Functions - Connection-Oriented									
Connection establishment and release	X	X	X	X	X	X	X	X	X
Splitting of data link connections									
Delimiting and synchronization of protocol-data-units	X	X	X	X	X	X	X	X	X
Error detection and recovery	X	X	X	X	X	X	X	X	X
Flow control and sequenced delivery									
Data Link Layer Functions - Connectionless									
Data transfer	X	X	X	X	X	X	X	X	X
Error detection			X	X	X	X	X	X	X

Table 27. Multicasting: 1 to N Scenario Protocol Stack

Application Category	Telemetry/Navigation		Emergency/ Flight Critical		Experiment Support/ Mission Pay Load		System/Vehicle Maintenance		
Characteristics/Types	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	System Diagnostics	Event Reports	Testing
Application Layer Functions									
Applications identifications	X	X	X	X	X	X	X	X	X
Application context required	X	X	X	X	X	X	X	X	X
Synchronous operation	X				X				
Asynchronous operation		X	X	X		X	X	X	X
Real time	X		X	X	X				
Transport Layer Functions - Reliable Transport Required									
Precedence	X	X	X	X	X	X	X	X	X
Segmentation	X	X			X	X	X	X	X
Graceful closing			X	X			X	X	X
Flow control					X	X	X	X	X
Integrity			X	X	X	X	X	X	X
Duplicate control							X	X	X
Multiplexing								X	
Sequence control							X	X	X
Blocking								X	
Error detection			X	X	X	X	X	X	X
Error recovery			X	X	X	X	X	X	X
Transport Layer Functions - Reliable Transport Not Required									
Segmentation	X	X			X	X	X	X	X
Data transfer	X	X							
Network Layer Functions - Connectionless									
Addressing, routing and transfer of data	X	X	X	X	X	X	X	X	X
Error detection and notification	X	X	X	X	X	X	X	X	X
Possible segmentation	X	X			X	X	X		X
Multicasting	X	X	X	X	X	X	X	X	X

Application Category	Telemetry/Navigation		Emergency/ Flight Critical		Experiment Support/ Mission Pay Load		System/Vehicle Maintenance		
Characteristics/Types	System Status Monitoring	Equipment & Component Monitoring	Collision Avoidance	"Mayday"	Data Collection (Real Time)	Data Collection (Store & Forward)	System Diagnostics	Event Reports	Testing
Data Link Layer Functions - Connection-Oriented									
Connection establishment and release	X	X	X	X	X	X	X	X	X
Delimiting and synchronization of protocol-data-units	X	X	X	X	X	X	X	X	X
Error detection and recovery	X	X	X	X	X	X	X	X	X
Data Link Layer Functions - Connectionless									
Data transfer	X	X	X	X	X	X	X	X	X
Error detection			X	X	X	X	X	X	X

Table 28. Multicasting: N to 1 Scenario Applications

Application Category	Experiment Support/ Mission Pay Load
Characteristics/Types	Data Collection (Real Time)
Application Layer Functions	
Applications identifications	X
Application context required	X
Presentation context required	
Presentation service requirements	
Session service requirements	
Turn management	
Synchronization	
Recovery from temporary loss of presentation connection	
Synchronous operation	X
Asynchronous operation	
Real time	X
User Authentication	
Linked operation	
Presentation Layer Functions	
Presentation connection establishment, and its termination with its peer	X
Negotiation of syntax for presenting application data	
Syntax transformation including data compression	
Data transfer by utilizing the services of the lower layers	X
Dialogue control	
Session Layer Functions	
Connection establishment	X
Connection release	X
Connection abort	
Activity management	
Major and minor synchronization	
Symmetric synchronization	
Resynchronization	
Exception	
Negotiated release	
Abort services	
Data transfer by utilizing the services of the lower layers	X

Application Category	Experiment Support/ Mission Pay Load
Characteristics/Types	Data Collection (Real Time)
Transport Layer Functions - Reliable Transport Required	
Precedence	X
Segmentation	X
Graceful closing	
Flow control	X
Integrity	X
Duplicate control	
Multiplexing	
Sequence control	
Blocking	
Error detection	X
Error recovery	X
Expedited data transfer	
Transport Layer Functions - Reliable Transport Not Required	
Segmentation	X
Data transfer	
Network Layer Functions - Connection-Oriented	
Connection establishment and its maintenance	
Multiplexing of connections	
Re-initialization or reset of connections	
Addressing, routing and relaying	X
Normal and expedited data transfer	
Sequencing and flow control, segmentation and re-assembly	X
Error detection, notification and possibly recovery	X
Network Layer Functions - Connectionless	
Addressing, routing and transfer of data	X
Error detection and notification	X
Access Control	
Source Authentication	
Confidentiality	
Possible segmentation	X
Multicasting	X

Application Category	Experiment Support/ Mission Pay Load
Characteristics/Types	Data Collection (Real Time)
Data Link Layer Functions - Connection-Oriented	
Connection establishment and release	X
Splitting of data link connections	
Delimiting and synchronization of protocol-data-units	X
Error detection and recovery	X
Flow control and sequenced delivery	
Data Link Layer Functions - Connectionless	
Data transfer	X
Error detection	X

Table 29. Multicasting: N to 1 Scenario Protocol Stack

Application Category	Experiment Support/ Mission Pay Load
Characteristics/Types	Data Collection (Real Time)
Application Layer Functions	
Applications identifications	X
Application context required	X
Synchronous operation	X
Real time	X
User Authentication	
Transport Layer Functions - Reliable Transport Required	
Precedence	X
Segmentation	X
Flow control	X
Integrity	X
Error detection	X
Error recovery	X
Expedited data transfer	
Transport Layer Functions - Reliable Transport Not Required	
Segmentation	X
Connectionless Network Layer Functions	
Addressing, routing and transfer of data	X
Error detection and notification	X
Possible segmentation	X
Multicasting	X
Data Link Layer Functions - Connection-Oriented	
Connection establishment and release	X
Delimiting and synchronization of protocol-data-units	X
Error detection and recovery	X
Data Link Layer Functions - Connectionless	
Data transfer	X
Error detection	X

The following protocol requirements have been identified from the protocol requirements analysis step:

- An application level protocol optimized towards the up-loading and downloading of data.
- An underlying transport protocol optimized to provide reliable end-to-end delivery of spacecraft command and telemetry messages between end systems that are communicating over a network containing one or more potentially unreliable space data transmission paths.
- A data protection mechanism that provides the end-to-end integrity of such message exchange.
- A data link protocol that takes a given physical link and transforms it to a link that can support the above requirements by compensating for the inherent shortcomings of the underlying physical medium.
- High performance channel coding to virtually eliminate the undetected bit errors in the space link.
- Flexible protocol architecture to take advantage of future high level of spacecraft automation.
- Routing of data dynamically through changing in-space network topologies.
- Multicast (1 to N, N to 1)

6.5.1. Operational Constraints

Ideally, the requirements identified above would be met through use of off-the-shelf technology that has been proven in ground-based systems. Unfortunately, space missions must be carried out under conditions that vary significantly from those in ground data systems. Therefore, the operational constraints encountered in space communications listed below should be taken into account in developing the conceptual protocol architecture.

- Round-trip delays much greater than those seen in ground networks.
- Intermittent connectivity, as a result of orbital position, earth rotation, or availability of ground station support.
- Changes in the routing path from contact to contact, because of use of multiple ground stations.
- Noise characteristics on space links that (despite sophisticated error correction codes) produce more frequent data loss than on ground links.

6.6. Protocol Synthesis

The material presented here is similar to that presented in sections 4.6 and 5.6 for the first two scenarios. It is repeated here to make this scenario complete.

Protocol architectures are not developed in a vacuum. In general, it is an evolutionary process. The state of the technology, operating environment, and the application requirement are the driving factors in the development of a conceptual protocol architecture. The evolution of the TCP/IP protocol architecture is a perfect example of this phenomena. As new applications are developed and fielded, the protocol architecture is enhanced to meet the additional requirements or new protocols are developed. Therefore, it is worthwhile to identify the technology trends before synthesizing the conceptual protocol architecture.

6.6.1. Technology Trends

The robustness of the Internet has redefined the direction of computer communications networking. The deployment of popular applications and the need to support these applications more efficiently has led to development of new application level protocols as well as research into enhancing the TCP/IP protocol architecture. Data related traffic has already overtaken voice traffic being carried by present day networks and is growing at a much faster rate than voice traffic. This is validated by the transition that is taking place in the telecommunication industry to develop an integrated backbone network to carry voice, video and data. In addition, there are a number of initiatives in the standards world by various technology forums, international and national standards bodies to enhance existing protocols or to develop new protocols. Therefore, one has to take into account these technology trends is developing protocol architecture.

6.6.2. Trends in Standards

There are international, national and industry forums to develop standards so that communication between end systems can take place in an efficient way. Although these groups share a common goal (open communication among end systems), achieving common ground has been elusive. Recently, these groups have gone from a state of holy war to peaceful coexistence, which has benefited the user community.

The architects of the OSI protocol reference model have identified various drawbacks in the OSI model since its initial implementation. Since 1983, experts have claimed that the organization of the OSI upper layers (Application, Presentation, and Session) as described in the OSI reference model is a mess and needs to be restructured. Also, network architectures, such as the Aeronautical Telecommunication Network (ATN) which use the ISO protocol architecture for air to ground communications, have devised methods to bypass the presentation and session layers. They have done this to reduce the overhead and eliminate unnecessary functions present in these two layers.

Recently, ISO extended the application layer structure to allow a single control function to supervise a set of application service elements. Also, they have revisited the entire upper layer architecture. They now essentially allow implementations to slice the upper layers vertically and ultimately collapse the upper layers into a single, object-oriented service layer. The extended application layer structure (XALS) and revised OSI upper layer architecture are under study in the ISO defined application service object (ASO). The ASO will contain multiple application service elements, some formed by grouping session functional units into application service elements. The result is the elimination of the session layer.

The existing presentation layer functionality will be subsumed within a new association control service element, which will offer an association data service. As a result, the presentation layer will be removed from the OSI reference mode as well. This allows the ASO association control service element to directly interface with the OSI transport layer. These developments in a sense align the OSI architecture more closely with the TCP/IP protocol architecture. It also reduces the overhead and protocol complexity.

The ISO transport protocol TP4 and the TCP are not only functionally equivalent but operationally similar as well. A 1985 study performed jointly by the U.S. Defense Communications Agency and National Academy of Science concluded that TP4 and TCP are functionally equivalent and essentially provide similar services. Table 30 compares the functions provided by these two protocols.

Table 30. Comparison of TP4 and TCP Functions

Function	TP4	TCP
Data transfer	Blocks	Streams
Flow control	Segments	Octets
Error detection	Checksum	Checksum
Error correction	Retransmission	Retransmission
Addressing	Variable TSAP	16-bit
Interrupt service	Expedited data	Urgent data
Security	Variable in TP	Not available
Precedence	16 bits in TP	Not available
Connection termination	Nongraceful	Graceful

At the network layer ISO supports Connectionless Network Protocol (CLNP) and the TCP/IP protocol architecture supports the Internet Protocol (IP). The CLNP and IP are functionally identical and both are best effort delivery network protocols. The major difference between the two is that CLNP accommodates variable length addresses, whereas IP supports fixed 32 bit addresses. (IPv6 supports larger address space.) Table 31 compares the functions of CLNP to those of IP.

Table 31. Comparison of CLNP and IP Functions

Function	CLNP	IP
Version identification	1 octet	4 bits
Header length	1 octet, represented in octets	4 bits, represented in 32 bit words
Quality of service	QoS maintenance option	Type of service
Segment/fragment length	16 bits, in octets	16 bits, in octets
Total length	16 bits, in octets	Not present
Data unit identification	16 bits	16 bits
Flags	Don't segment, more segments, suppress error report	Don't fragment, more fragments
Segment/fragment offset	16 bits, represented in octets (value always multiple of 8)	13 bits, represented in units of 8 octets
Lifetime, time to live	1 octet, represented in 500 millisecond units	1 octet, represented in 1-second units
Higher layer protocol	Not present	Protocol identifier
Lifetime control	500 millisecond units	1-second units
Addressing	Variable length	32-bit fixed
Options	• Security • Priority • Complete source routing • Partial source routing • Record route • Padding • Not present • Reason for discard (Error PDU only)	• Security • Precedence bits in TOS • Strict source route • Loose source route • Record route • Padding • Timestamp

6.6.2.1. Why an Internet-Based Network Architecture

In a heterogeneous network environment, the networking technologies used by various organization range from COTS LANs to dialup networks. This means there are many different types of subnetworks that must be connected together. As no one has control over what the subnetwork will look like, the network layer (Internetwork) protocol has to be designed to work with whatever may be the type of subnetwork available. Therefore, the practical approach is to define one protocol that assumes minimal subnetwork functionality and place it firmly on the top of every subnetwork access protocol. This network architecture model treats every subnetwork and data link service as providing a basic data pipe. Each pipe should support a service data unit large enough to accommodate the header of the network layer protocol and a reasonable amount of user data. This is the IP or OSI connectionless network protocol model of networking. As the subnetwork technology changes, there is just one more subnetwork with which the network layer must interface.

6.6.2.2. Why a TCP/IP Protocol Architecture

Although ISO's TP4 and the TCP transport protocols are functionally identical, TP4 is not widely implemented. There is limited practical knowledge about the protocol in the real world environment. On the other hand, TCP provides an excellent base of technology for extension. It is a highly robust protocol, widely distributed, and is freely available. Hundreds of individuals worldwide work to ensure that TCP continues to meet the needs of the Internet community. Therefore, TCP is cost effective to implement, and provides additional functionality that may be needed in the future.

In addition, the ISO's CLNP and IP are functionally similar in providing a connectionless network layer service to the transport layer. Here again, CLNP has not been deployed widely and has not been tested thoroughly in an operational environment. Therefore, it is recommended that TCP/IP protocol architecture form the starting point for multicast protocol architectures.

6.7. Scenario Unique Requirements

Although functionally equivalent to terrestrial networks, space communications networks often have performance and operational considerations that prevent direct use of existing commercial protocols. Protocols used in terrestrial networks assume that: connectivity is maintained; data loss due to corruption is rare; balanced bi-directional links are available; and most data loss is due to congestion. Further, vendors of commercial communications products that implement these protocols use these assumptions to maximize performance and economy in this environment. This results in the treatment of retransmission, recovery, and time-outs inappropriate for space operations. For the majority of space nodes, the space environment makes performance of these protocols unacceptable.

To meet the above constraints protocols are required to provide interoperability across the spectrum of space nodes and between space data systems and the COTS based ground network environment. They have to provide a set of options and protocol data unit formats that can be scaled to satisfy the communication needs of both complex and simple nodes.

The protocol architecture should provide reliable stream or file transfers over existing and new link layers and dynamic networking for multiple space node environments. Given the link characteristics and intermittent connectivity encountered over the space link, better performance is achieved by using a balance of upper-layer, confirmed, end-to-end services supported by link level error correction that avoids excessive retransmission. In addition, the architecture has to support an efficient multicast environment.

6.8. Recommended Protocol Architecture

The goal of the protocol architecture is not only to support applications but also to lower the lifecycle costs by reducing development and operations costs in space communications systems. In addition, the protocol architecture should be able to extend Internet connectivity into space. The rationale for this approach is that both the data systems and the personnel (designers, operators, and users) associated with space missions are already using Internet protocols. The communications services that they need in space are very similar to those they have in ground networks. The easiest, lowest risk, and most direct way to achieve this goal was to adapt the protocols that are used on the ground. This architecture is shown in Figure 8.

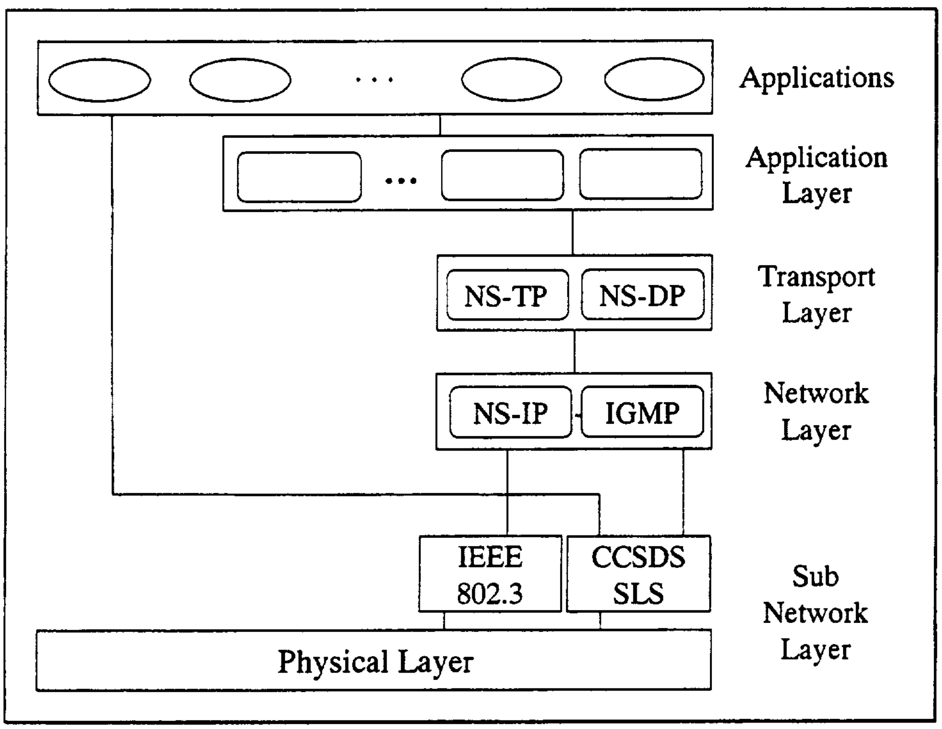

Figure 8. Recommended 1 to N Protocol Architecture

Although the Internet protocols provide an excellent basis for space communications protocol development, the space environment presents a number of constraints that are seldom encountered in the design of terrestrial data communications networks. These are physical, operational, and resource differences. The physical differences include:

- Space link delays ranging from milliseconds to hours.
- Potentially noisy space data links.
- Limited space link bandwidth.

- Variation in sub-network types from simple busses to local and wide area networks.

- Interruptions in the end-to-end data path that can vary from bits lost, and link interruptions.

The operational differences include:

- Inherently sporadic nature of contact between space and ground.
- Maximum latency requirement due to "Teleoperations" activities.

The resource differences include:

- Limited onboard processing power.
- Limited onboard program memory.
- Limited onboard data buffering.

Except for a very narrow range of operational conditions, the current off-the-shelf, Internet protocols do not satisfy the requirements encountered in the space mission environment. Therefore, the strategy is to: use COTS-supported standards wherever possible; capitalize on established user interface familiarity; and minimize software development costs. This approach allows one to take advantage of the hundreds of thousands of hours of operational experience that the Internet protocols have accrued.

6.9. NASA Conceptual Protocol Architecture

The suite of NASA space protocols should provide flexibility and optional features that allow designers to tailor a communications protocol suite to meet specific requirements and constraints without extensive software development. It should allow specific layers, or protocols within layers, to be included or omitted to create an optimal profile. This calls for a layered protocol architecture.

6.9.1. Transport Layer Protocol

NS-TP provides end-to-end full and minimal reliability services. The full reliability service is provided by enhanced TCP. It supports end-to-end data transfer of a sequence of data units with full reliability (complete, correct, in sequence, and no duplication). It uses sequence checking to assure the sequence order and avoid duplication. It incorporates acknowledgments and retransmission requests to provide completeness. This protocol closes connections without loss of data.

The minimal reliability service is provided by the NASA Space Datagram Protocol (NS-DP). It is a connectionless transport protocol and sends data in datagrams. It transfers data with minimal reliability (correct, possibly incomplete, and possibly out of sequence). It does not support sequence numbering, acknowledgment of receipt, or retransmissions.

The NS-TP is based on the Transmission Control Protocol (TCP). Enhancements are identified to improve performance in the space environment. Unmodified TCP performs poorly in communications scenarios with a large bandwidth-delay product and cannot operate efficiently with the unbalanced links typical of space-ground communications. The suggested extensions to the base protocols are intended to address the performance issues.

6.10. Differences Between Communications Environments

The material presented here is almost identical to that presented in the first two scenarios. It is repeated here to make this scenario complete.

TCP provides an excellent base of technology for adding extensions. It is a highly robust protocol, widely distributed, and is freely available. TCP is optimized to provide service in the terrestrial environment. There are significant differences between the terrestrial and space environments that affect a communication protocol's performance. Table 32 presents a summary of the main factors that affect TCP performance when operating in space environments.

Table 32. Factors Affecting TCP Performance in Spacecraft Environments

Factor	Terrestrial Environment	Spacecraft Environment
Bit error rate	$< 10^{-9}$	10^{-5} to 10^{-12}
Round trip delay	Millisecond to second	Seconds to hours
Continuity of Connectivity	Continuous	Intermittent: 10% (LEO) to 90% (TDRS) per orbit
Forward and reverse links	1:1 (equivalent rates)	10:1 to 2000:1 Some have down link only
CPU capacity	Unrestricted	Possibly low
Communication goals	• Fair access over time • High aggregate throughput over time • High reliability	• High throughput during contact • Maximum link utilization
Primary source of data loss	Congestion	• Congestion • Corruption • Link outage

6.10.1. Bit-Error Rates

The error performance of typical terrestrial networks has improved to a point that it is no longer considered as a typical source of data loss. With sufficient channel coding and application of radiated power, some satellite links can approach the error performance of the terrestrial environment. Reed-Solomon error control has proven to be of great benefit in space links. Both hardware and software solutions to perform Reed-Solomon corrections in real time are available. For a link speed of 5 Mbps or less, software solutions have been shown to be adequate. Recent advancements in microprocessor speeds may enable a software solution for processing data at higher rates. A software solution for high-rate Reed-Solomon processing is preferable to a hardware solution in that a software solution would reduce system lifecycle costs and maximize system portability. In the future, the bit error may play a less significant roll in the performance of the transport layer.

6.10.2. Round Trip Delay

Round trip delays in the terrestrial communication environment are typically in the tens of milliseconds to low hundreds of milliseconds. In the spacecraft communication environment, round trip times of 500 milliseconds are the minimum that one expects when communicating through a geostationary satellite. Deep space communications can increase round trip delays to hours.

Long round-trip delays limit the usefulness and effectiveness of TCP's feedback from the remote communication endpoint. This causes problems when the protocol needs to react to changes in the network, but does not receive feedback about the changes until long after they have occurred. Note that long delays are not exclusively a result of speed-of-light propagation times. Low data transmission rates add delay to a network, as can half-duplex operations. Finally, queuing in intermediate systems is a source of delay.

6.10.3. Continuity of Connectivity

Topology changes are infrequent in a terrestrial communications environment. However, space based systems have predictable (possibly highly dynamic) connectivity characteristics. Low earth orbiting satellites typically have connectivity through a single ground station 10% of the time or less. Changes to the number of ground stations or the satellite's orbit can improve this, but even NASA's TDRS system offers only about 90% coverage..

6.10.4. CPU and Memory Capacity

In the terrestrial communications environment, the availability of computing resources is essentially unrestricted. This is not the case in spacecraft where power, weight, and volume are all precious commodities. The amount of computational resources available to any subsystem in a spacecraft must be traded-off against the benefits of applying that resource elsewhere. Therefore, it is important to be aware of these constraints. The loss of data due to bit-errors has a disproportionately bad effect on TCP's performance because TCP interprets any loss as an indication of network congestion. The appropriate response to network congestion is to reduce the offered load to the network. TCP's congestion response reduces the offered load by half, then builds back slowly over several subsequent round trips. The effect of this response to bit-errors is to significantly under utilize the communication channel.

6.10.5. Primary Source of Data Loss

The primary source of loss in terrestrial networks is congestion, and TCP is optimized to control congestion. The space communication environment are mixed-loss environments, with losses occurring due to all three causes: bit-errors, topology changes (link outages), and congestion. To treat all losses as congestion results in unnecessary reductions in offered load. The increased round trip times in these environments delays the restoration of full-rate transmission.

6.11. Network Layer

The functional requirements for network services for the transfer of data between end points within a space data communications system are stated below:

- Support for multicasting
- Support for multiple routing options
- Packet lifetime support with auto discard
- Support for precedence handling
- Provide efficient operation in constrained-bandwidth environments
- Separate reporting of congestion and corruption

The ability to route data from source to destination is characteristic of essentially all protocols that operate at the network layer of the OSI Basic Reference Model. Common to all of the prospective environments is that bandwidth may be constrained, either unidirectionally or bidirectionally. This constraint results in a requirement to operate with high bit-efficiency. Bit-efficiency quantifies the fraction of transmitted bits that are user data. Improving bit-efficiency may be accomplished in two ways: by increasing the amount of user data per unit of protocol control information (i.e., header information), or by decreasing the amount of protocol control information per unit of user data.

The first approach (making packets longer) is simple, but does not work well in environments that are prone to bit-errors. It also does not work well when the user's data does not lend itself to aggregation.

The second approach (reducing the protocol header overhead) is the approach commonly used to obtain high bit-efficiency. Several requirements derive from the need to operate in bandwidth constrained environments: multicasting, support for address translation, and precedence-based data handling. All address bandwidth-related constraints and are described in subsequent paragraphs.

Multicasting is a technique for improving network-wide bit-efficiency. The technique of multicasting allows addressing of data to a group of destination systems. Rather than sending an unique copy of the data to each remote system, data is sent to the group address. Intermediate systems replicate the multicast packet only as necessary in order to reach all of the destination systems in the multicast group.

Header compression can enhance bit-efficiency in networks that can be characterized as having few source-destination pairs that account for most of the network's traffic. In IPv6, these are identified as flows. For these flows, the source and destination addresses can be replaced by an identifier. This is similar to the SCPS managed connection.

Precedence improves operations in bandwidth-constrained environments in two ways. First, it controls the order of service, which reduces queuing delay and variations in queuing delay for high precedence traffic. Second, precedence controls the order of packet discarding when congestion occurs. If packet discarding is required, low precedence packets are discarded before higher precedence ones.

Packet lifetime control provides protection against transient routing loops. A transient routing loop is formed when routing tables in the network are not synchronized. This condition can occur as a result of using certain routing protocols. While a routing loop is in existence, the links forming the loop may become progressively more congested. Packet lifetime control ensures that data packets do not remain in the network indefinitely. They are discarded once they have exceeded their "lifetime." This mechanism combined with either automated or manual means to update the routing tables provides control over routing loops.

Signaling of network conditions to upper-layer protocols is required to allow those protocols to become aware of and to adapt to changing conditions within the network. Signals that may be passed to the upper-layer protocols include indications of network congestion, network corruption, and link outages. This requires the network to identify the conditions at points in the network that may be remote from the end systems that host the upper-layer protocols. It also requires the network propagate network-internal signals to the affected end systems for delivery to the upper-layer protocols.

6.11.1. Shortcomings of Using IP in Space Networks

The Internet Protocol (IP) is a highly capable, widely used protocol. Table 33 identifies IP capabilities and the issues associated with using it in a space based network environment. Most of these issues are related to the limited bandwidth in space environment.

Table 33. Support of SCPS Network Requirements by IP

Protocol Function	IP
Routing	Yes
Support for bandwidth limited environment	No
Multicast support	Yes
Priority	Yes
Header compression	Yes – not supported in COTS
Priority	Partial
Packet life time control	yes
Signaling to support upper layer	Partial

IP supports routing methods that forward data from source to destination. In general, IP does not provide any explicit support for operating in bandwidth limited environments. IP headers are a minimum of 20 octets in length, and may be made longer with the addition of options. IP provides support for multicasting, but has no mechanism for shortening its headers.

The IP header contains a field to carry eight levels of precedence. However, COTS products typically do not make use of the field. In particular, high precedence packets would not benefit from a reduced probability of discard in congested routers, nor would they receive any reduced queuing delays in routers. The capabilities in IP for packet lifetime control are adequate for most environments.

With respect to signaling of network conditions, some IP implementations provide partial support. The Internet Control Message Protocol (ICMP) (the companion protocol to IP that handles such signaling) has the ability to generate congestion signals. However, research in this area has resulted in specifications such as Random Early Detection (RED). However, RED is not widely deployed nor is its Explicit Congestion Notification (ECN) option. There is no signaling provided to indicate loss, whether due to corruption or to link outage.

6.11.2. Suggested Enhancements to IP

All the issues identified above are in one way or another related to using the limited bandwidth more efficiently. One way to accomplish this goal is to not transmit unnecessary header elements. This design decision increases the processing to format and parse headers in favor of reducing the number of bits that are transmitted.

Network protocols typically route data from source to destination by selecting the "next hop" router based on the destination address. There are many routing methods by which the next hop router is selected. One of method is to use routing tables that may be statically or dynamically configured to selects the next hop router. The routing methods reduce the complexity and overhead associated with the routing but sacrifice the dynamic route selection capability.

In a space based networking environment, it is possible to reduce header overhead by performing header compression and address translation as suggested by the SCPS-network protocol. SCPS-NP's method of using a single address to represent an address pair is called a managed connection. In this method an IP source-destination pair may be translated into three alternate managed connection address:

- An Extended Path Address which represents the two addresses with a single four-octet address;

- A pair of Basic End System Addresses which represents the two four-octet addresses with a pair of corresponding one-octet addresses; or

- A Basic Path Address which represents the pair of four-octet addresses with a single one-octet address.

SCPS-NP uses address translation tables that are configured statically to translate addresses. The translation tables are identical throughout the network. In addition, address translation can be used to support multicasting, and identifies multicast (group) addresses.

6.11.3. IP Multicasting

IP multicasting is the transmission of an IP datagram to a "host group", a set of zero or more hosts identified by a single IP destination address. A multicast datagram is delivered to all members of its destination host group with the same "best-efforts" reliability as regular unicast IP datagrams. The membership of a host group is dynamic; that is, hosts may join and leave groups at any time. There is no restriction on the location or number of members in a host group. A host may be a member of more than one group at a time. A host need not be a member of a group to send datagrams to it.

A host group may be permanent or transient. A permanent group has a well-known, administratively assigned IP address. It is the address, not the membership of the group, that is permanent. A permanent group may have any number of members, even zero. The IP multicast addresses that are not reserved for permanent groups are available for dynamic assignment to transient groups that exist only as long as they have members.

Forwarding of IP multicast datagrams is handled by "multicast routers" which may be co-resident with, or separate from, Internet gateways. A host transmits an IP multicast datagram as a local network multicast that reaches all immediate-neighboring members of the destination host group. If the datagram has an IP time-to-live greater than 1, the multicast router(s) attached to the local network takes responsibility for forwarding it towards all other networks that have members of the destination group. For the other member networks that are reachable within the

IP time-to-live, an attached multicast router completes delivery by transmitting the datagram as a local multicast.

IP multicasting allows a host to join and leave host groups, as well as send IP datagrams to host groups. It requires implementation of the Internet Group Management Protocol (IGMP) and extension of the IP and local network service interfaces within the host. Host groups are identified by class D IP addresses; i.e., those with "1110" as their high-order four bits. Class E IP addresses; i.e., those with "1111" as their high-order four bits, are reserved for future addressing modes.

In Internet standard "dotted decimal" notation, host group addresses range from 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is guaranteed not to be assigned to any group, and 224.0.0.1 is assigned to the permanent group of all IP hosts (including gateways). This is used to address all multicast hosts on the directly connected network. There is no multicast address (or any other IP address) for all hosts on the total Internet. The addresses of other well-known, permanent groups are to be published in "Assigned Numbers".

The multicast extensions to a host IP implementation are specified in terms of the layered model. In this model, IGMP is implemented within the IP module, and the mapping of IP addresses to local network addresses is considered to be the responsibility of local network modules. To provide multicasting, a host IP implementation must support the transmission and reception of multicast IP datagrams. The IP module must also be extended to implement the IGMP protocol. IGMP is used to keep neighboring multicast routers informed of the host group memberships present on a particular local network. To support IGMP, every host must join the "all-hosts" group (address 224.0.0.1) on each network interface at initialization time and must remain a member for as long as the host is active.

IGMP is used by IP hosts to report their host group memberships to any immediate-neighboring multicast routers. IGMP is an asymmetric protocol and is specified here from the point of view of a host, rather than a multicast router. IGMP is a integral part of IP. It is required to be implemented by all hosts for IP multicasting. IGMP messages are encapsulated in IP datagrams, with an IP protocol number of 2.

Multicast routers send Host Membership Query messages (called Queries) to discover which host groups have members on their attached local networks. Queries are addressed to the all-hosts group (address 224.0.0.1), and carry an IP time-to-live of 1. Hosts respond to a Query by generating Host Membership Reports (called Reports). The Reports indicate each host group to which they belong on the network interface from which the Query was received. In order to avoid an "implosion" of concurrent Reports and to reduce the total number of Reports transmitted, two techniques are used:

- A Report is generated for the corresponding host group when a randomly-chosen timer expires. This spreads the reporting over an interval instead of all occurring at once.

- Normally only one Report is generated for each group present on the network. It is generated by the member host whose delay timer expires first.

A host should confirm that a received Report has the same IP host group address in its IP destination field and its IGMP group address field, to ensure that the host's own Report is not cancelled by an erroneous received Report. A host should quietly discard any IGMP message of type other than Host Membership Query or Host Membership Report.

Multicast routers send Queries periodically to refresh their knowledge of memberships present on a particular network. If no Reports are received for a particular group after some number of Queries, the routers assume that that group has no local members and that they need not forward remotely-originated multicasts for that group onto the local network. Queries are normally sent infrequently (no more than once a minute) so as to keep the IGMP overhead on the hosts and networks very low. However, when a multicast router starts up, it may issue several closely-spaced Queries in order to quickly build up its knowledge of local memberships.

When a host joins a new group, it should immediately transmit a Report for that group, rather than waiting for a Query in case it is the first member of that group on the network. To cover the possibility of the initial Report being lost or damaged, it is recommended that it be repeated once or twice after short delays. Note that on a network with no multicast routers present, the only IGMP traffic is the one or more Reports sent whenever a host joins a new group.

6.12. Subnetwork Layer

The next layer in the NASA space protocol architecture is the subnetwork layer. The subnetwork is mostly technology dependent. It can range from Ethernet to ATM depending on the environment and the state of the technology. As new subnetwork technologies are developed, they can be easily incorporated into the protocol architecture. Similarly, existing space-based subnetworks can interface to the network layer. Although it is possible to interface any of the existing subnetwork technologies to the network layer, we present only the existing Space Link Subnetwork (SLS) as an example..

6.12.1. Space Link Subnetwork

To share the limited bandwidth of the space-to-ground link, a CCSDS recommendation for Advanced Orbiting Systems has developed the concept of a CCSDC virtual channel for the space link subnetwork. The virtual channel facility allows one physical space channel to be shared among multiple higher-layer traffic streams, each of which may have different service requirements. A single physical space channel may therefore be divided into several separate logical data channels, each known as a "Virtual Channel" (VC). Each VC is individually identified and supports a single "Grade of Service."

To facilitate simple, reliable, and robust synchronization procedures, fixed-length protocol data units are used to transmit data through the weak-signal, noisy space channels. The protocol data units are each associated with one particular VC and are known as "Virtual Channel Data Units" or VCDUs. A service option internal to the VCDU can also produce a protocol data unit known as a "Coded Virtual Channel Data Unit", or CVCDU. Each VCDU and CVCDU contains a header and trailer (which provide space link protocol control information) and a fixed-length data field within which higher-layer service data units are carried. The SLS supports six different types of services: encapsulation, multiplexing, bitstream, virtual channel access, virtual channel data unit, and insert.

The encapsulation service provides a facility whereby variable-length, octet-aligned service data units which are not formatted as CCSDS Packets may be transferred across the SLS. The transfer is asynchronous and sequence preserving.

The multiplexing service provides a facility whereby variable-length, delimited, octet-aligned service data units, which conform to the Version-1 CCSDS Packet format, may be multiplexed together for transfer across the SLS on the same VC. The transfer is asynchronous and sequence preserving.

The bitstream service provides a facility whereby serial strings of bits, whose internal structure and boundaries are unknown may be transferred across the SLS. The transfer is sequence preserving and may be either "asynchronous" or "isochronous." An isochronous transfer from service interface to service interface is provided with a specified maximum delay and a specified maximum jitter at the service interface. High-rate video data may use the isochronous bitstream service.

The virtual channel access service provides a facility whereby a project organization may transfer private service data units (which are sized to exactly load the fixed-length data field of one dedicated VCDU and whose internal structure is unknown) across the SLS. The transfer can be either asynchronous or isochronous and is sequence preserving.

The physical channel function creates one dedicated space data transmission path. A continuous stream of data bits is accepted at the sending side, modulated, serially transmitted through the physical space medium, demodulated, bit synchronized, and delivered through the receiving interface.

The insert service provides a facility whereby private octet-aligned service data units may be transferred isochronously across the SLS in a mode which efficiently uses the space channel transmission resources at relatively low data rates.

6.12.2. Virtual Channel Function

At the sending side, the virtual channel function accepts service data units from higher-layer functions. It then builds them into the space link protocol data units (VCDUs or CVCDUs) and applies error control required by different grades of service, commutates the VCDUs/CVCDUs into an appropriate sequence, and submits them as a serial stream to the physical Channel function for transmission through one physical channel.

At the receiving side the serial stream is synchronized to find the boundaries between VCDUs/CVCDUs, which are then passed through error control procedures and decommutated. The higher-layer service data units are then extracted and passed back through the receiving service interface.

During transmission through the physical channel, each VCDU or CVCDU is carried synchronously within one "Channel Access Data Unit" (CADU). The CADUs provide fixed-length "channel access slots" which occur at precise time intervals that are synchronized with the transmitted bit rate, and whose boundaries are delimited using "synchronization markers." The commutated sequence of VCDUs/CVCDUs is transmitted so that all of the synchronous channel access slots are occupied. In situations where no valid higher-layer data are ready for release, a VCDU/CVCDU containing "fill" data is commutated into the transmitted sequence. The continuous and contiguous stream of CADUs, known as a "Physical Channel Access Protocol Data Unit," is transferred through the physical channel.

Service data units associated with the encapsulation, multiplexing, bitstream or virtual channel access services are placed into a "Data Unit Zone" within the data field of the VCDU or CVCDU.

6.13. Multiple Access

In the N to 1 multicast scenario, multiple earth terminals communicate with the spacecraft which collects and forwards the information to one earth receiving terminal. Assuming that the multiple earth stations are communicating with the space station simultaneously, what is needed on the up link a multiple access protocol. The multiple access protocol exploits the satellite's geometric advantage. Although there are many specific implementations of multiple access systems, there are only three fundamental system types. They are: frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA).

6.13.1. Frequency Division Multiple Access

These systems channelize a transponder using multiple carriers. The bandwidth associated with each carrier can be as small as required. FDMA can use either analog or digital transmission in either continuous or burst mode. The two generic types of FDMA are the multiple channel per carrier (MCPC) and single-channel-per-carrier (SCPC).

6.13.2. Time Division Multiple Access (TDMA)

TDMA is characterized by the use of a single digitally modulated carrier per transponder, where the bandwidth associated with the carrier is typically the full transponder bandwidth. This maximizes the attainable bit rate for that transponder. The bit rate of the carrier is timeshared between a number of earth stations such that the sum of the traffic information rate (plus overhead) between individual earth stations can never exceed the rate of the carrier. However, each earth station must transmit its information data burst at the agreed rate of the carrier in preassigned recurring time slots. Clearly, timing requirements that must be met in such a system are crucially stringent, particularly because the space station is always slightly moving in an undulating fashion. Although the primary advantage of TDMA is realized in the single-carrier-per-transponder arrangement, there are cases where the TDMA bandwidth may be a fraction of the transponder's.

6.13.3. Code-Division Multiple Access

CDMA also uses a digitally modulated carrier. However, earth stations transmit simultaneously at an agreed on high rate, with each source message coded uniquely so that only the intended destination with the proper decoder can retrieve the message. The carrier rate is many times the individual source rate, and typically occupies the entire transponder bandwidth.

6.13.4. N to 1 Architecture

The protocol architecture for multiple access is shown in Figure 9. It is assumed that the spacecraft supports other applications in addition to multiple access. The multiple access capability is supported by the Media Access Control (MAC) protocol.

6.13.4.1. NASA Space System File Transfer Protocol (NS-FTP) Functions

The Internet File Transfer Protocol (FTP) in the TCP/IP architecture supports a rich set of file transfer capabilities. Compared to the ISO's FTAM, FTP is a widely used and stable protocol. The amount of FTP overhead needed is significantly less than required for FTAM. Therefore, FTP is well suited for the bandwidth limited space based network environment.

As the Internet File Transfer Protocol (FTP) provides a rich set of functions, the NS-FTP should use FTP as a starter set to define the file transfer functions and then add functions required to operate in the bandwidth limited space operations environment. Like FTP, NS-FTP should use two transport connections between host systems - a control connection to exchange control information, and a data transfer connection to move data file. Data is transferred from a storage device in the sending host to a storage device in the receiving host.

Both contact time and bandwidth are scarce resources in space operations. To operate in the resource restricted space environment NS-FTP should provide enhanced error recovery and restart capabilities. Interruptions in file transfers could be restarted from the point of interruption instead of starting over. This is a common feature supported by many of the Web-relate download applications.

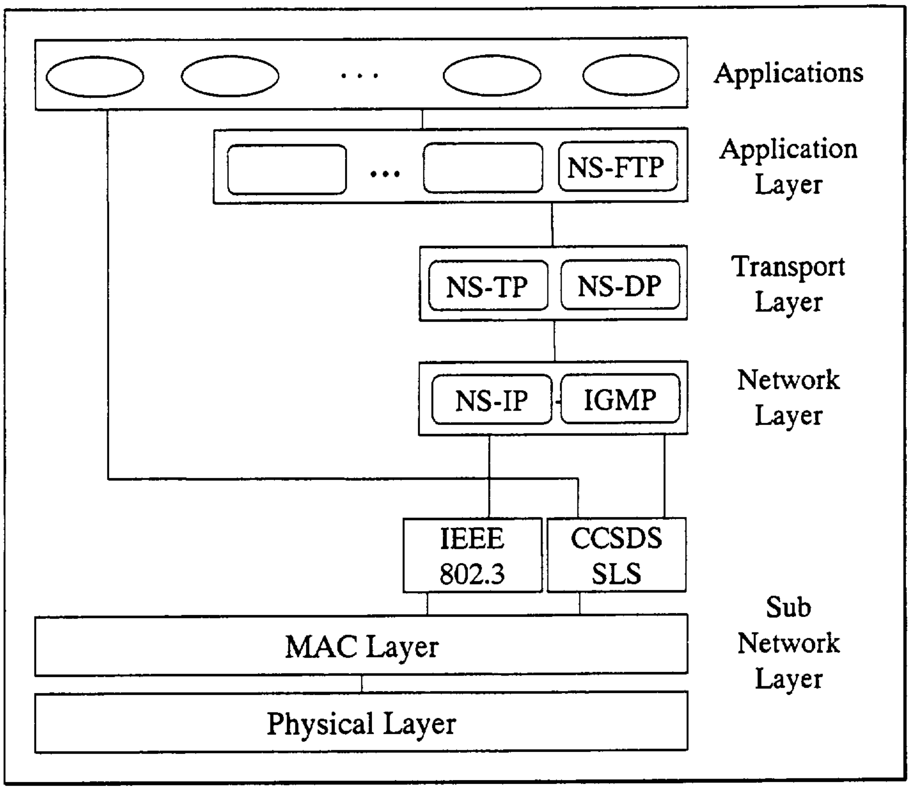

Figure 9. Recommended N to 1 Protocol Architecture

NS-FTP should also provide the capability to read or update part of a file on a remote system rather than the entire file. This avoids the transfer of a large amount of data when only a small part of the file is affected. Other NS-FTP extensions to FTP should provide integrity checks to recover from errors in file transfer or update operations. Finally, to conserve bandwidth and contact time, NS-FTP should suppress text messages between end systems involved in file operations.

It is suggested that the application layer file transfer protocol support the following functions:

- Transfers of science or mission data to ground without special processing to reorder or merge data sets.
- Limited management of files onboard spacecraft (delete, rename, and directory services).
- Automatic restart of transfers after an interruption.

6.13.5. System Engineering Considerations

A system designer is always faced with selecting the proper multiple access technique to meet the requirements of the communications services to be provided. In deciding which technique best fits the application, a number of factors must be considered. The factors that are normally used to evaluate the effectiveness of a multiple access technique for a particular application are:

Capacity: The capacity of the multiple access system is usually defined in terms of the number of voice or data channels of a specified quality that can be supported using the power and bandwidth of a single transponder. In selecting a system, the highest capacity system is the most desirable. However, the system network requirements may lead to the choice of a system providing less total capacity.

Power and bandwidth: Power and bandwidth are the fundamental resources of the satellite link. The power and bandwidth available in a satellite communication system are directly reflected in its cost. To use the available power and bandwidth efficiently, a multiple access system should be designed so that it is simultaneously bandwidth and power limited.

Interconnectivity: The network topology for various communications services dictates the interconnectivity requirements. Simple point-to-point networks can often be served economically by other wide-band transmission techniques, such as fiber optics. However, in a multi-node topology, the ability of a multiple access techniques to provide interconnectivity among many users at various data rates and quality levels often makes satellites the most cost effective method.

Adaptability to growth: Since the investment in multiple access equipment can be a significant portion of the ground system cost, the designers must consider the ability of the technique chosen to adapt to traffic growth and changes in the traffic patterns.

Accommodation of multiple services: Modern approaches to telecommunications rely heavily on digital techniques and multi-service transmission. The use of an integrated service environment implies that multiple services such as voice, data, image and video applications share the same transmission facilities. Multiple access system should be designed to accommodate integrated services.

Terrestrial Interface: Interconnecting with existing terrestrial facilities that provide the last mile between the earth station and the user is extremely important to the overall economic and technical effectiveness of the multiple access system. As more digital interconnection become available, it becomes more attractive to employ all digital techniques.

Communication security: Although in the past most considerations of communication security have been relegated to the military applications, modern commercial satellite communications systems must now face the problem of protecting confidential corporate and government data in a satellite communications environment that is vulnerable to unauthorized reception.

Cost effectiveness: The cost per channel of implementing multiple access is an important consideration for system engineers. Because of the dramatic development and continuously decreasing cost of digital technology, their economic desirability continues to increase. However, analog techniques are still more cost effective in certain circumstances.

7. REFERENCES

1. Advanced Orbiting Systems, Networks and Data Links, Blue Book, CCSDS 701.0-B-2, Oct 1989.

2. ATM Forum PNNI Working Group, af-pnni-0055.000, Private Network-Network Interface Specification Version 1.0, Mar 1996.

3. ATM Forum, ATM User-Network Interface Specification, Prentice Hall, Sep 1993

4. ATM signaling support for IP over ATM, RFC –1755 (Perez, M., Liaw, F., Grossman, D., Mankin, A., and A. Hoffman), Jan 1995.

5. Bhasin, K. B., et al., Enhancing End-to-End Performance of Information Services Over Ka-Band Global Satellite Networks, NASA/TM-97-206297, Dec 1997.

6. CCSDS SCPS-710-0-G-0.4 1-4 SCPS Network Protocol, Red Book, CCSDS SCPS-713.0-0-R-1, Issue 1, Apr 1997.

7. Charalambous, P. C. et al., Performance Evaluation of TCP Extensions on ATM over High Bandwidth Delay Product Networks, IEEE Communications Magazine, Jul 1999.

8. Chitre, P. and Yegenoglu, F., Next-Generation Satellite Networks: Architecture and Implementations, IEEE Communications Magazine, Mar 1999.

9. Classical IP and ARP over ATM, RFC 1577 (Laubach, M.), Jan 1994.

10. Comer, D. E., Internetworking with TCP/IP, Vol. I: Principles, Protocols and Architecture, Prentice Hall, 1991.

11. Cuevas, E. G., The Development of Performance and Availability Standards for Satellite ATM Networks, IEEE Communications Magazine, Jul 1999.

12. Default IP MTU for use over ATM AAL5, RFC -626 (Atkinson, R.), May 1994.

13. Directed ARP, RFC-1433 (Garrett, J., Hagan, J., and J. Wong), Mar 1993.

14. Durst, R. C., et al., TCP extensions for Space Communications, Proc. ACM Mobicomm'97, Nov 1996.

15. File Transfer Protocol (FTP), RFC-959, (Postel, J. B., and Reynolds, J. K., Ed.), Oct 1985.

16. Ghani, N., and Dixit, S., TCP/IP Enhancements for Satellite Networks, IEEE Communications Magazine, Jul 1999.

17. Goyal, R. et al., Traffic Management for TCP/IP over Satellite ATM Networks, IEEE Communications Magazine, Mar 1999.

18. Hoe, J. C., Improving the Start-up Behavior of a Congestion Control Scheme for TCP, Proc. ACM SIGCOMM'97, Aug 1996.

19. Information Technology - Open Systems Interconnection—Basic Reference Model: The Basic Model. International Standard, ISO/IEC 7498-1, 1994.

20. Internet Engineering Task Force, Internet Protocol, (Postel, J. B., Ed.), Request for Comments (RFC) 791, Sep 1981.

21. Internet Engineering Task Force, Postel, J. B.; and Reynolds, J. K., File Transfer Protocol (FTP), Request for Comments (RFC) 959, (Postel, J. B., and Reynolds, J. K.; Ed.), Oct 1985.

22. Internet Engineering Task Force, TCP Extensions for High Performance, RFC 1323. (Jacobson, V.; Braden; R, Borman,.. D.; Ed.), May 1992.

23. IP over ATM: A Framework Document, RFC 1932 (Cole, Shur & Villamizar), Apr 1996.

24. Ivancic, W. D., et al., NASA's Broadband Satellite Networking Research, IEEE Communications Magazine, Jul 1999.

25. Keshav, S., A Control-Theoretic Approach to Flow Control. Proc. ACM SIGCOMM'91, Sep 1991.

26. Liu, Z., et al., Evaluation of TCP Vegas: Emulation and Experiments, Proc. ACM SIGCOMM'95, Aug 1995.

27. Mathis, M., et al., TCP Selective Acknowledgement Options, RFC 2018, Oct 1996.

28. Mathis, M., Mahdavi, J., Forward Acknowledgement: Refining TCP Congestion Control, Proc. ACM SIGCOMM'96, Aug 1996.

29. Mertzanis, I. et al., Protocol Architecture for Satellite ATM Broadband Networks, IEEE Communications Magazine, Mar 1999.

30. Multiprotocol Encapsulation over ATM Adaptation Layer 5, RFC-1483 (Heinanen, J.), Jul 1993.

31. NBMA Address Resolution Protocol (NARP), RFC –1735 (Heinanen, J., and R. Govindan), Dec 1994.

32. Packet Telemetry, Blue Book, CCSDS 102.0-B-3, Issue 3, Nov 1992.

33. Partridge, C., and Shepard, T. J., TCP/IP Performance Over Satellite Links, IEEE Network, Sep/Oct 1997.

34. Path MTU Discovery, RFC-1191 (Mogul, J., and S. Deering), Nov 1990.

35. SCPS File Protocol, Red Book, CCSDS SCPS-717.0-0-R-1, Issue 1, Apr 1997, or later issue.

36. SCPS Security Protocol, Red Book, CCSDS SCPS-713.0-0-R-1, Issue 1, Apr 1997, or later issue.

37. SCPS Transport Protocol, Red Book, CCSDS SCPS-713.5.0-0-R-1, Issue 1, Apr 1997.

38. TCP Extensions for High Performance, RFC -1323. (Jacobson, V., Braden, R, Borman, D., Ed.), May 1992.

39. TCP Selective Acknowledgement Options, RFC-2018, (Mathis, M., et al.), Oct 1996.

40. TCP Selective Acknowledgement Options, RFC-2018, (Mathis, M., et al.), Oct 1996.

41. Telecommand - Part 1 Channel Service, Blue Book, CCSDS 201.0-B-1, Jan 1987.

42. Telecommand - Part 2 Data Routing Service, Blue Book, CCSDS 202.0-B-2, Jan 1987.

43. Telemetry Channel Coding, Blue Book, CCSDS 101.0-B-3, May 1992.

44. Zhang, Y., et al., Satellite Communications in the Global Internet-Issues, Pitfalls, and Potential, Proc. INET'97, 1997.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	January 2000	Final Contractor Report

4. TITLE AND SUBTITLE

Protocol Architecture Model Report

5. FUNDING NUMBERS

WU–632–50–51–00
NAS3–99165
Task 1

6. AUTHOR(S)

Chris Dhas

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Computer Networks and Software, Inc.
7405 Alban Station Ct.
Springfield, Virginia 22150

8. PERFORMING ORGANIZATION REPORT NUMBER

E–12065

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
John H. Glenn Research Center at Lewis Field
Cleveland, Ohio 44135–3191

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

NASA CR—2000-209781

11. SUPPLEMENTARY NOTES

Project Manager, Thomas Wallett, Communications Technology Division, NASA Glenn Research Center, organization code 5610, (216) 433–3673.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Category: 32 Distribution: Nonstandard

This publication is available from the NASA Center for AeroSpace Information, (301) 621–0390.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

NASA's Glenn Research Center (GRC) defines and develops advanced technology for high priority national needs in communications technologies for application to aeronautics and space. GRC tasked Computer Networks and Software Inc. (CNS) to examine protocols and architectures for an In-Space Internet Node. CNS has developed a methodology for network reference models to support NASA's four mission areas: Earth Science, Space Science, Human Exploration and Development of Space (HEDS), Aerospace Technology. This report applies the methodology to three space Internet-based communications scenarios for future missions. CNS has conceptualized, designed, and developed space Internet-based communications protocols and architectures for each of the independent scenarios. The scenarios are: Scenario 1: Unicast communications between a Low-Earth-Orbit (LEO) spacecraft inspace Internet node and a ground terminal Internet node via a Tracking and Data Relay Satellite (TDRS) transfer; Scenario 2: Unicast communications between a Low-Earth-Orbit (LEO) International Space Station and a ground terminal Internet node via a TDRS transfer; Scenario 3: Multicast Communications (or "Multicasting"), 1 Spacecraft to N Ground Receivers, N Ground Transmitters to 1 Ground Receiver via a Spacecraft

14. SUBJECT TERMS

Protocol; Architecture

15. NUMBER OF PAGES

72

16. PRICE CODE

A04

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	