NASA/TM—2006-214058

Taking the Politics Out of Satellite and Space-Based Communications Protocols

William D. Ivancic
Glenn Research Center, Cleveland, Ohio

April 2006

NASA STI Program . . . 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 plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and 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 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 also include creating custom thesauri, building customized databases, organizing and publishing research results.

For more information about the NASA STI program, 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 STI Help Desk at 301–621–0134

- Telephone the NASA STI Help Desk at 301–621–0390

- Write to:
  NASA STI Help Desk
  NASA Center for AeroSpace Information
  7121 Standard Drive
  Hanover, MD 21076–1320

NASA/TM—2006-214058

Taking the Politics Out of Satellite and Space-Based Communications Protocols

William D. Ivancic
Glenn Research Center, Cleveland, Ohio

Prepared for
GLOBECOM 2005
sponsored by the Institute of Electrical and Electronics Engineers
St. Louis, Missouri, November 28–December 2, 2005

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

April 2006

Level of Review: This material has been technically reviewed by technical management.

Available from

NASA Center for Aerospace Information
7121 Standard Drive
Hanover, MD 21076–1320

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161

Available electronically at http://gltrs.grc.nasa.gov

Taking the Politics Out of Satellite and Space-Based Communications Protocols

William D. Ivancic
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

Abstract

After many years of studies, experimentation, and deployment, large amounts of misinformation and misconceptions remain regarding applicability of various communications protocols for use in satellite and space-based networks. This paper attempts to remove much of the politics, misconceptions, and misinformation that have plagued space-based communications protocol development and deployment. This paper provides a common vocabulary for communications; a general discussion of the requirements for various communication environments; an evaluation of tradeoffs between circuit and packet-switching technologies, and the pros and cons of various link, network, transport, application, and security protocols. Included is the applicability of protocol enhancing proxies to NASA, Department of Defense (DOD), and commercial space communication systems.

Introduction

NASA is developing a new Space Communications and Navigation Architecture enabling NASA's Exploration and Science programs to be executed between 2010 and 2030 (ref. 1). NASA has long recognized that efficient, high-quality communication is an essential enabler for all space activities. NASA's Space Exploration Initiative will require communication technology development efforts and protocols that fit into an evolving, dynamic space communication architecture. These communication protocols must match the needs of the emerging exploration program as it matures.

Space-based communications networks are often thought of as having unique characteristics that require special consideration. There is a measure of truth to this, but, only when applied appropriately. Volume, mass, and power are at a premium in space—as well as on Earth, for mobile and ad hoc communication. Intermittent connectivity is a common mode of operations for planetary relays—as it is for many military operations. Delay and latency have to be considered for space-based protocols—as they must be for terrestrial protocols, where delays via low-bandwidth, highly processed links may be in the order of seconds (ref. 2). Deep-space communication has extremely long delays in the order of hours—terrestrially we use e-mail and text messaging and are not terribly concerned about the delay so long as the message gets through eventually. Reliability and redundancy are of major concern, as they are in aeronautical, military, and commercial networks. Finally, space hardware must withstand radiation effects; this one is relatively unique to space, though also present in military and high-altitude applications. Thus, although space-based networks have many interesting and complex characteristics, these characteristics are not necessarily unique, and potential solutions often already exist.

After many years of studies, there is still an amazing amount of misinformation and a number of misconceptions regarding communications protocols in satellite and space-based networks. This paper attempts to provide an unbiased presentation of what one needs to consider when determining what protocols to use—particularly for space-based networks. First, we develop a common vocabulary for communications (link, circuit, packet, frame, etc.). Next, we identify the major protocol suites. This is followed by a general discussion of tradeoffs between circuit and packet-switching technologies and the pros and cons of various link, network, transport, application, and security protocols. Included is a discussion of the applicability of protocol enhancing proxies. NASA, Department of Defense (DOD), and commercial space communication systems are addressed. We then explore the characteristics of various communication environments (surface, near planetary, and deep space).

Vocabulary

Many times information is misconstrued or misunderstood because the communicating parties are not using a common definition—unbeknownst to them. This is easily understood once one begins to look at the overlap of definitions. This overlap may be due to ones point of reference or area of expertise (e.g., radio communications, telecommunications, or networking profession). For example, the following definitions for channel, link, and circuit were taken from the Alliance for Telecommunications Industry Solutions (ATIS) (ref. 3). Note the ambiguity.

Circuit

1. The complete path between two terminals over which one- or two-way communications may be provided.

2. An electronic path between two or more points capable of providing a number of channels.
3. A fully operative communications path established in the normal circuit layout and currently used for message, wide-area telephone service (WATS) access, teletypewriter exchange service (TWX), or private line services.

Channel

1. A connection between initiating and terminating nodes of a circuit.
2. A single path provided by a transmission medium via either (a) physical separation, such as by multipair cable or (b) electrical separation, such as by frequency- or time-division multiplexing.
3. A path for conveying electrical or electromagnetic signals, usually distinguished from other parallel paths.
4. Used in conjunction with a predetermined letter, number, or codeword to reference a specific radiofrequency (RF).

Link

1. The communications facilities between adjacent nodes of a network.
2. A portion of a circuit connected in tandem with, that is, in series with, other portions.
3. A radio path between two points, called a radio link.
4. A conceptual circuit, that is, logical circuit, between two users of a network that enables the users to communicate, even when different physical paths are used.

Note 1: In all cases, the type of link, such as data link, downlink, duplex link, fiber-optic link, line-of-sight link, point-to-point link, radio link, and satellite link, should be identified. Note 2: A link may be simplex, half-duplex, or duplex.

In general, when referring to a circuit, one usually infers reserved capacity between points, where hard state (fixed software configuration) is used to set up that capacity. We talk of circuits being "set up" for use when the state is initialized and "torn down" once done, when that software configuration state is removed from the switching devices. When considering two hosts in a packet-switching network, the term "circuit" is used most frequently to describe a connection between the hosts that behaves as though it is a direct connection even though it may physically be circuitous, a virtual circuit. In this case, the two hosts can communicate as though they have a dedicated connection even though the packets might actually travel across a number of separate links before arriving at their destination.

Virtual circuits are connections between two end points passing over a shared packet-switched network of some type. Two types of virtual circuits exist: permanent virtual circuits (PVCs) and switched "temporary" virtual circuits (SVCs). PVCs are always available, whereas SVCs are set up on demand.

Circuit switching is a process that, on demand, connects two or more end systems and permits the exclusive use the complete path between two terminals over which two-way communication is provided until the connection is released. Here, dedicated capacity is reserved for communication by the endpoints during circuit setup and exists until released. Telephony voice communication at one time was the primary example of dedicated circuit switching; however, packet-switched voice-over Internet protocol (VOIP) is now used throughout much of the telecommunication industry—often with the subscriber unaware of its use.

Packet switching is a technology that explicitly allows the capacity of a link to be shared by numerous users for voice, video, and data services via multiplexing of packets from different sources to different destinations. Quality of Service (QoS) is achieved in such systems by use of traffic shaping, policing at the edge of the network, marking packets with precedence bits, and differentiated services as well as reserving capacity. In general, one can achieve far greater overall link utilization with a multiplexing packet-switched technology than with circuit switching as unused capacity by one service becomes available for use by another.

Traditionally, space-based systems have used separate radio links and separate reserved channels for command and control communications. However, with today's ability to provide priority to packetized communications, one could easily share a single radio link with many services and still obtain the desired QoS with command and control having precedence over other data types.

Packet switching provides much greater flexibility than circuit switching when there is a diversity of traffic types and burstiness of traffic. With circuit switching it is highly advantageous to know the type of data and amounts of data passing over various circuits in order to manage the bandwidth. Circuit-based switching manages capacity via a combination of connection management or other access control (e.g., manual configuration to allocate bandwidth). Packet-based switching manages data throughput via a statistical combination of queue management, traffic policing, and the application of appropriate protocols.

Frames

In communications, a frame is a block of data transmitted as a single entity. Frames can be fixed length or variable length. A frame usually consists of a header and payload. The header provides the necessary information to determine the beginning of a frame (synchronization), the length of the frame, the possible source and destination of the frame, and information on how to handle the payload.

In the early days of space communication, processing power was minimal and use of commutation was common. Data was placed into frame structures via commutation prior

to transmission to the ground. Traditionally, telemetry transmitted from the spacecraft was formatted with a Time Division Multiplexing (TDM) scheme, where data items were multiplexed into a continuous stream of fixed-length frames based on a predefined multiplexing rule. To design and implement a data system for spacecraft, each project was forced to develop a custom system used by that project alone (ref. 4).

One application of framing is to delineate and synchronize data at the media access layer or layer two of the ISO network layer concept. Frames can be fixed sized or vary in size. Ethernet, Hardware Data Link Control (HDLC), Synchronous Optical Network (SONET), High Speed Serial Interface (HSSI), and the American National Standards Institute (ANSI) Asynchronous are common data-link framing techniques found in commercial-off-the-shelf (COTS) network communication equipment interfaces. Satellite modems use a variety of proprietary and standard framing optimized for various media access techniques such as time-division, multiple access (TDMA), frequency-division multiple access (FDMA), code division multiple access (CDMA), and hybrid combinations (e.g., MF–TDMA or multifrequency TDMA). The Consultative Committee for Space Data Systems (CCSDS) protocols specify standard framing formats. For example, CCSDS transfer frames to multiplex telemetry packets and advanced orbiting system (AOS) data into frames for transmission to the ground.

One can argue that framing at the data link may be the point that provides the greatest interoperability challenge between tradition space communications and today's common networking communication—not the transport or application layer. There are two main reasons for this: (1) the natural evolution of space-based systems based on their heritage and (2) optimization for point-to-point communications versus optimization for network communications where flexibility is paramount.

Space-based systems evolved from computationally dumb low-processing-rate systems, and have always had to address radiation requirements and operate in limited powered environments. In addition, traditional space-based systems were point-to-point, space and ground communications—not networked. Hence, systems were designed to optimize processing and power and close the RF link as efficiently as possible. In fact, the framing and coding were even merged to the point where portions of what some consider the physical layer coding are found in the data-link layer (ref. 22 and figs. 1 and 2). Thus, it is difficult to separate some of these layers using CCSDS protocols. As a result, a gateway is required to perform protocol translation when moving between CCSDS framing and COTS frames (HDLC, SONET, HSSI, etc.) (fig. 3).

It is extremely difficult to integrate COTS equipment into CCSDS communication systems as portions of the radio reside in the front-end processor. For example, NASA integrated a special interface card into an IBM PC docking station to complete the CCSDS coding and framing of the radio system in order to run IP into NASA's space shuttle over TDRSS. This device is part of the Orbital Communication Adapter (OCA). If the radio were a complete and separate unit with standard interfaces as shown in figure 1, a COTS router could have been utilized with all the additional features provided by a router such as buffering, debugging tools, and traffic policing (ref. 5).

Communication Protocols

A communication protocol is a set of rules governing the exchange of information between entities. In networking, a protocol is a set of formal rules describing how to transmit data, especially across a network. Low-level protocols define the electrical and physical standards to be observed, bit- and byte-ordering, and the transmission and error detection and correction of the bit stream. High-level protocols deal with the data formatting, including the syntax of messages, the machine-to-machine dialogue, character sets, sequencing of messages, etc.

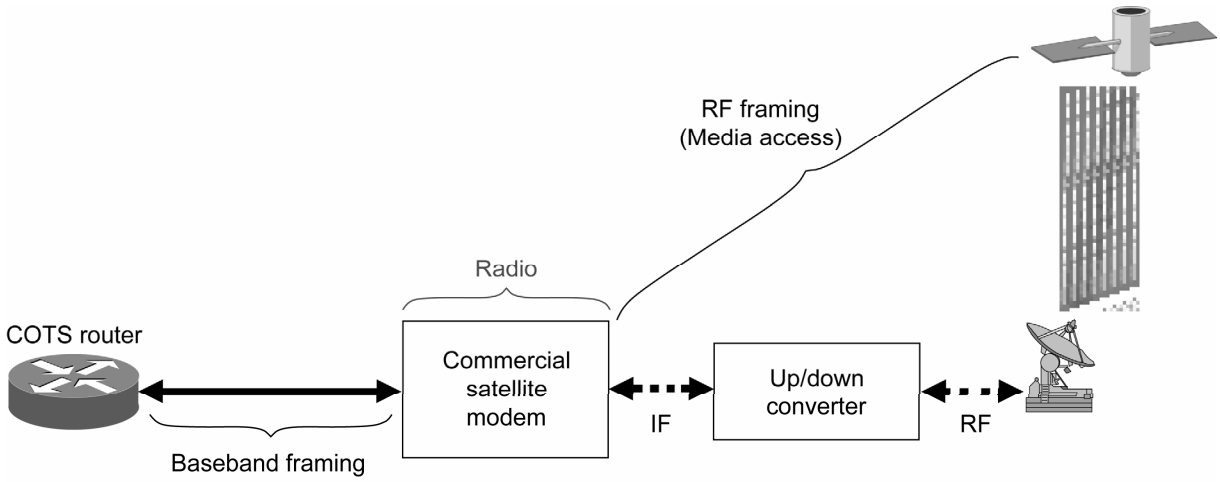

Figure 1.—COTS satellite radio.

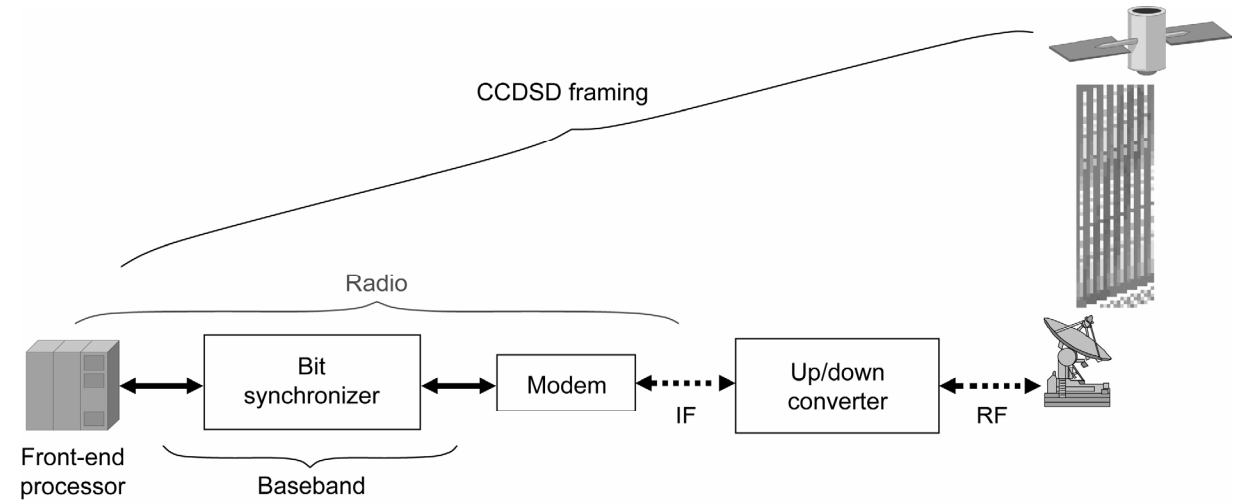

Figure 2.—CCDSD satellite radio.

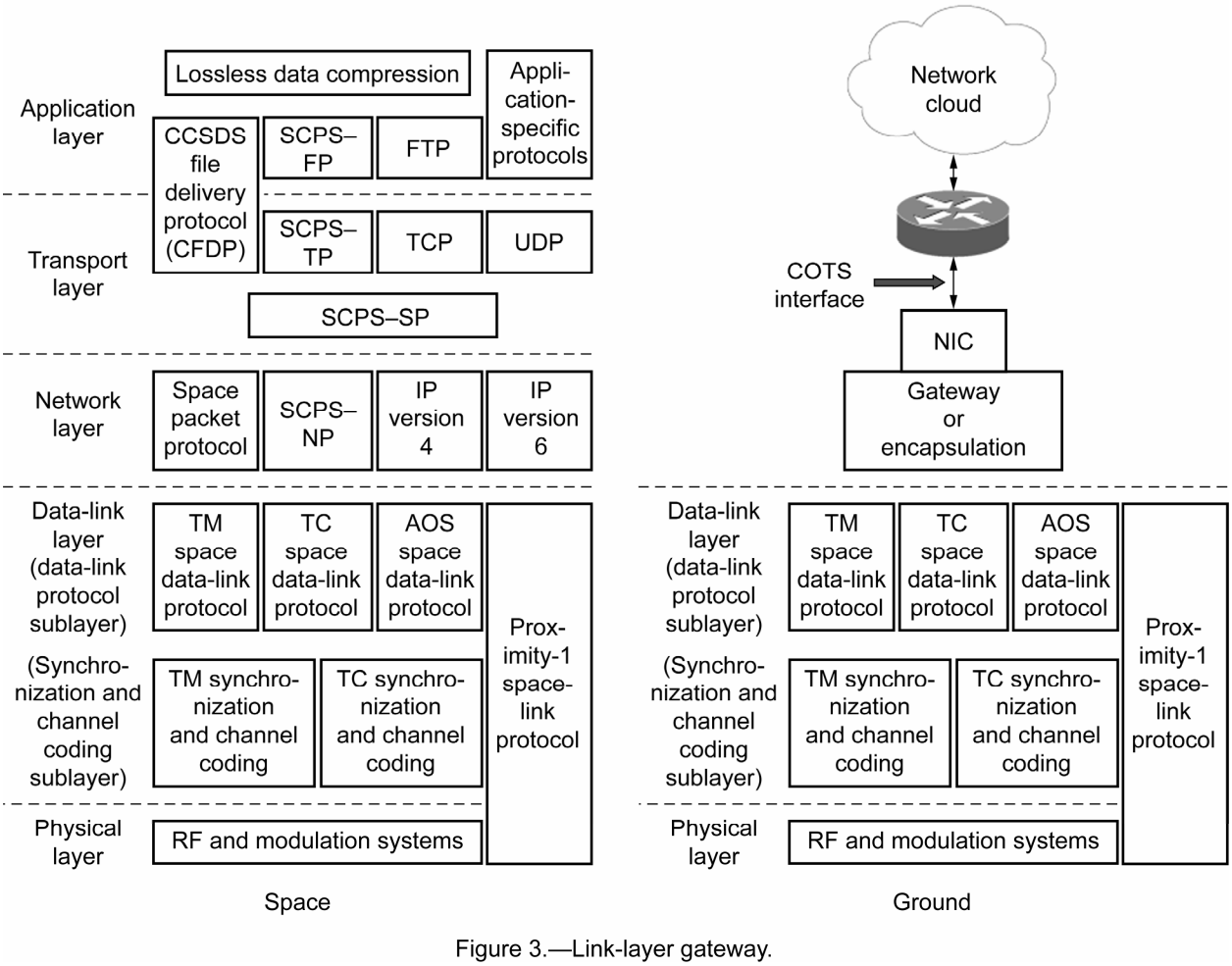

Figure 3.—Link-layer gateway.

Protocols are the tools of network communication. There are hundreds of communications protocols, each with its own purpose—just like physical tools. Often one can choose from a number of protocols to get a specific job done albeit, one may work better for the specific job than another. However, the "best" protocol may be determined by factors other than simply performance. For example, one may choose a protocol that is readily available and gets the job done over a protocol that is optimal with regard to performance—particularly if the inefficiencies of the protocol are of little concern compared to the costs of design, testing, and implementation. One may also weigh flexibility as of greater importance than efficiency. Most certainly, one size does not fit all cases.

There are a number of organizations that work on protocols concentrating on various layers of the seven-layer ISO/OSI network model and four-layer transmission control protocol/Internet protocol (TCP/IP) network model (ref. 6). The International Electronic and Electrical Engineers (IEEE), the International Telecommunication Union (ITU), ANSI, the International Standards Organization (ISO), the Internet Engineering Task Force (IETF), and the Consultative Committee for Space Data System (CCSDS) are just a handful of organizations that work to develop specifications (refs. 7 to 10). When considering communications and networking, the ITU is most prevalent in RF spectrum and modulation and coding, whereas the IEEE and ANSI activities are most prevalent in the physical and media access (radio systems and hardware specifications). CCSDS was formed in 1982 by the major space agencies of the world to provide a forum for discussion of common problems in the development and operation of space data systems. The IETF's focus is on the network, transport, and application layers of the IP suite. The IETF does not specify standards at the lower layers. Other bodies, such as the multiprotocol label switching (MPLS) forum and asynchronous transfer mode (ATM) forum, promulgate standards for their protocols and technologies.

Layering protocols as in the ISO and TCP models permits one to develop various protocols for each layer. This allows for a divide-and-conquer engineering approach to solving network communication problems and provides tremendous flexibility. However, one does not have to use a layered approach. By merging layers, one can often improve the overall efficiency of a system (size, mass, power, and processing) at the expense of flexibility. Merging layers sometimes can simplify the design and reduce the overall processing requirements. Most of the first space missions merged layers as the entire communication systems was well defined and overall efficiency was of far greater importance than system flexibility. As we move from point designs to space-based networks, flexibility becomes paramount.

CCSDS Protocols

CCSDS protocols encompass all aspects of the communication network from modulation and coding up through application development. The following is just a small sample of the range of existing protocols that have been developed (ref. 4).

Telemetry Channel Coding—establishes a common framework and provides a common basis for the coding schemes used on spacecraft telemetry streams.

Packet Telemetry—establishes a common framework and provides a common basis for the data structures of spacecraft telemetry streams.

TM Synchronization and Channel Coding—specifications for synchronization and channel coding to be used on synchronous data channels.

Proximity-1 Space Link Protocol: Physical Layer—defines the Proximity-1 Space Link Protocol Physical Layer. The specification for the channel connection process, provision for frequency bands and assignments, hailing channel, polarization, modulation, data rates, and performance requirements.

CCSDS File Delivery Protocol (CFDP)—defines a protocol suitable for the transmission of files to and from spacecraft data storage and capable of operating in a wide variety of mission configurations.

Space Communications Protocol Specification (SCPS) Recommendations—defines a protocol suite that is parallel in function to the protocols of the Earth-based Internet (FTP/TCP/IP). The SCPS protocols (security, network, transport, and file handling) have been optimized to overcome problems associated with using IPs in space.

SCPS–TP (transport protocol) has been designed to be interoperable with TCP. SCPS–TP has numerous options that can be used by the application or gateway including fully, partially, or unacknowledged service, rate-based transmission, and the ability to remove congestion control when appropriate to increase efficiency across a single link (ref. 11). Note, in order to fully utilize SCPS–TP between hosts, SCPS–TP has to be implemented at both hosts and the applications must be written to take advantage of the desired options. In addition, the applications must understand the characteristics of the end-to-end path in order to call appropriate options such as rate-based transfer. For these reasons, SCPS–TP, or portions of SCPS–TP, have found their greatest deployment in gateways as protocol enhancing proxies rather than in end-system hosts.

Note that SCPS–NP (network protocol) and SCPS–SP (security protocol) DO NOT interoperate with the corresponding TCP/IPs: IPv4, IPv6, and IPsec (IP Security). A gateway (protocol translation function) is required.

Recently, the CCSDS protocol suite has been adopting many of the TCP/IPs by reference. Notice the placement of TCP, UDP, IPv4, and IPv6 in figure 3. Also, there are ongoing efforts to move HDLC framing and segments of frame relay into the CCSDS specifications (ref. 12).

TCP/IP

TCP/IP is a suite of hundreds of network communications protocols dealing with packet formatting, routing, transport, services, and applications.

The IP versions 4 and 6 (IPv4 and IPv6) specify packet formats used for routing packets through an IP network. Numerous routing protocols exist including Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP). Reliable transport protocols include the TCP and Stream Control Transport Protocol (SCTP). Reliable transport protocols tend to be delay sensitive due to the fact that handshaking occurs to ensure data delivery; this behavior is worsened by congestion control algorithms.[1] The User Datagram Protocol (UDP) provides unreliable data delivery and forms the bases for many unreliable protocols such as video streaming. UDP can also be used for application-level reliable protocols. The file transport protocol (FTP) is an application-level protocol ensuring reliable file delivery by using TCP.

TCP is probably the best known and most widely used networking transport protocol to date. TCP's two major features are reliable transport and congestion control. The congestion control feature of TCP enables multiple users with different communication paths of different lengths to share a communication link and associated network in a fair manner. TCP assumes it knows nothing of the link and quickly probes the link to determine capacity by exponentially increasing its transmission rate. To date, in the vast majority of systems, packet loss is due to congestion. Thus, once a packet is lost, TCP assumes congestion and exponentially decreases its transmission rate then linearly probes for capacity from that point on. Thus, TCP is a poor tool for large file transfers over noisy paths—particularly if the path is not shared, which is currently the common mode of operation when communicating between spacecraft and ground. In addition, TCP uses a three-way handshake prior to beginning data transmission. As such, TCP is not a good choice for commanding over extremely long delays such as Earth to Mars. TCP has been used in space links and works well for small file transfers and commanding if the delays and small inefficiencies are not of concern (refs. 13 and 14). TCP performance over various links is very well understood and very well documented (refs. 15 to 21).

UDP is an unreliable transport protocol; packets that arrive are decoded reliably, but the arrival of those packets is not guaranteed. Many reliable and unreliable transport protocols written at the application layer have used UDP as the delivery mechanism for space-based applications. UDP has been used in space as the underlying transport mechanism for blind commanding as well as for the CCSDS file delivery protocol (CFDP), the Saratoga file delivery protocol, and for the multicast dissemination protocol (MDP) (refs. 22 to 25).

[1]Congestion control algorithms enable applications to share link capacity in a fair manner.

Beware of Poor Terminology!

The TCP/IP suite is often referred to as simply TCP or simply IP. This has generated great confusion in the space community as TCP, the transmission control protocol, is not necessarily the transport protocol of choice for communication over long bandwidth-delay links, whereas numerous tools are available from the TCP/IP suite that work well in space and are either delay insensitive or delay tolerant. The phrase "TCP will not work in space" is incorrect in either case. TCP can work in space, but may not perform well as it is designed for shared networks, not optimized for dedicated links. However, it is simply wrong and misleading to imply that the TCP/IP suite will not work in space. Such statements are either made out of ignorance or with the intent to mislead.

Security

Security protocols exist at all layers of the OSI protocol stack. The most common are link, network, transport, and application layers. One may (and probably should depending on one's risk assessment) implement security at multiple layers.

Some security mechanisms require the ability to communicate with certificate servers and key management systems in real time. Such mechanisms are not appropriate for Moon, Mars, and interplanetary communication where access to a remote certificate server is difficult or intermittent.

Link-layer security, using shared keys and perhaps even dynamic key updates, is possible for near-Earth communications. However, the usefulness of dynamic key updates the need for such link-layer security for near-planetary communications—other than Earth—is questionable. Link-layer security often uses shared keys. Shared keys are relatively easy to manage for small networks such as those that would comprise the Space Exploration Initiative.

Both SCPS and IP security protocols (SCPS–SP and IPsec) can be used for space communications. However, one would generally utilize shared static keys to avoid a sophisticated key management infrastructure as well as to alleviate performance problems associated with dynamic key updates over long delays. SCPS–SP is similar to IPsec transport mode (ref. 26). Both SCPS–SP and IPsec can reside between the transport layer and the network layer or in the network layer between network segments. Both protocols provide integrity, confidentiality, and authentication services.

The SCPS–SP operates with the assumption that there exists a Security Association (SA) database that contains pertinent security information, for use between the communicating entities, such as the encipher key, the key expiration, the key length, the encipherment algorithm, and the integrity algorithm. Use of IPsec for space-based applications would require similar types of security databases—as would any other security protocol including bundling.

For interplanetary Internet, a bundling security mechanism is being devised. This bundling mechanism applies security more at the data and application layers (ref. 27). As with IPsec and SCPS–SP, some type of preplaced static keys and security association database configuration are necessary. This is not necessarily part of the security protocols, but rather, part of protocol configuration.

The United States Government has a National Information Assurance (IA) Policy for all U.S. Space Systems (ref. 28), which mandates various levels of information assurance, particularly with regard to protecting the command and control links. Additional security guidelines are also provided in this administratively controlled document. To summarize this policy, one should highly protect the command and control links and perform a due-diligence risk assessment on all systems to determine the necessary level of protection for those systems.

Gateways

Gateways provide a translation interface between two different protocols at the same layer of the protocol stack. Gateways require maintenance when protocols change—and they do change! In addition, gateways can unintentionally break some protocols as you move data between one protocol with one set of assumptions and semantics and another different protocol with different assumptions and semantics. This may be considered a minor inconvenience on the ground compared with getting two different systems to interoperate. In space-based systems, gateway maintenance is much more difficult. Custom gateways are relatively expensive, as they must completely implement and support more than one protocol at a layer. Gateways are a tool that is best avoided if possible. However, sometimes a gateway is a necessary evil.

Link-Layer Gateways

Figure 3 shows the need for gateway between the CCSDS telemetry, telecommand, or AOS data-link protocols and commercial data-link protocols. This is necessary as large commercial suppliers of networking equipment have indicated that they have no intention of building special interface cards for a small space community. Thus, the space community has to either manage interfaces with special gateways, adopt commercial practices where practical, or has to remain completely separate from other networking worlds, attempting to fund and develop its own brand of networking.

Performance-Enhancing Proxies

Performance-enhancing proxies (PEPs) are used to improve degraded TCP performance caused by characteristics of specific link environments (ref. 29). PEPs may be employed in satellite, wireless wide area network (WAN), and wireless local area network (LAN) environments.[2] For communication through geostationary satellites and for other space links with large bandwidth-delay products, PEPs are deployed as middleware in an attempt to optimize control loops in TCP (fig. 4). In general, PEPs are designed to optimize the TCP. PEPs usually have to be able to examine the transport layer of the protocol. Thus, if IPsec or some other layer-three encryption is implemented, the PEP cannot provide the desired improvement on the encrypted traffic. As such, a PEP must be placed before any network layer encryption function (or device). Great care should be taken to fully understand the type of data being sent through the PEP and the environment it is used in.

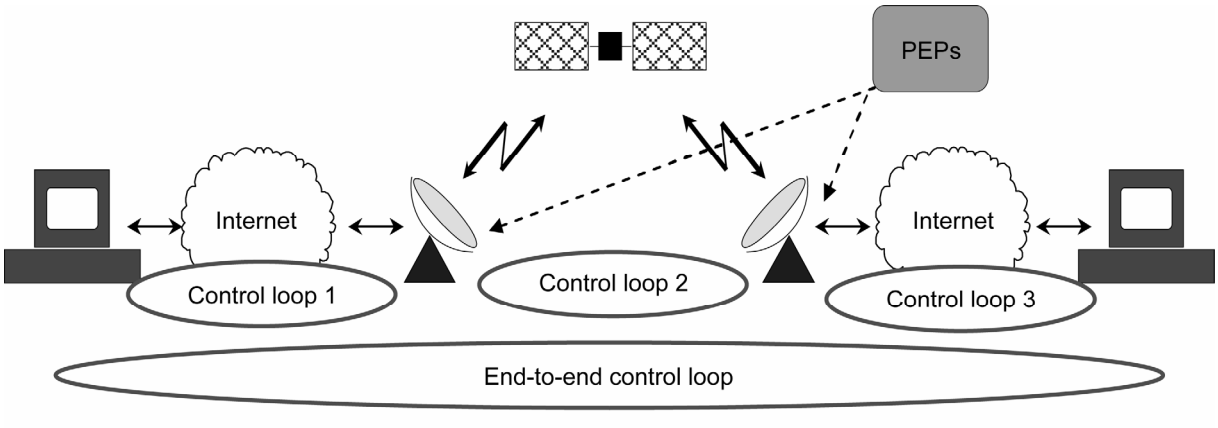

Figure 4.—Performance-enhancing proxy.

[2] Often called “link accelerators” for satellite and wireless applications.

Interplanetary Gateways (Deep Space)

There are obvious incompatibilities between terrestrial networks and interplanetary systems due to different requirements placed on the terrestrial and space-based networks and assumptions about propagation delay and sharing of links (congestion). Work is ongoing in this arena under the Delay Tolerant Network working group (formally the Interplanetary Internet working group (ref. 30)) within the Internet Research Task Force (IRTF). The incompatibilities are due to the nature of the various communication environments depicted in the next section. In order to overcome these incompatibilities, interplanetary gateways are necessary.

Communication Environments

When considering space-based communications there are basically three operating environments: surface, near planetary, and interplanetary. Each has its own characteristics that dictate which protocols are appropriate and inappropriate for the given environment. Obviously, robustness, reliability, and the ability to withstand harsh environments are necessary for the communication equipment. However, this is independent of the actual protocols being deployed.

Surface (Terrestrial)

Systems operating on the surface of a planet have similar, if not identical, operating characteristics to those systems on Earth: delay, power and congestion, connectivity, and mobility. The problem is actually much simpler regarding protocols as security may not be necessary between terrestrial nodes on the surface of the Moon or Mars. Furthermore, congestion may not be an issue for a small number of users.

Near Planetary

Near-planetary systems communicating with their corresponding terrestrial systems have similar characteristics to communication between Earth-based satellites and their corresponding ground-based systems. Regarding Earth-based communications, geostationary satellites (GEO) provide round-trip time delays of approximately 500 milliseconds whereas low-Earth-orbiting satellites have delays in the hundreds of milliseconds. GEO (areosync for Mars) provide continuous visibility and connectivity whereas LEO connectivity is on the order of minutes. One should expect similar characteristics for near-planetary systems relative to each planet's orbital dynamics.[3] Thus, solutions that work well for Earth-based space communications should readily apply to other planets.

Interplanetary

Interplanetary communication is quite different than terrestrial or near-planetary communications. The general characteristics are speed-of-light delays, intermittent and unidirectional connectivity, and error-rates characteristic of deep-space communication. One has to take into account when a system will be on and pointed and orbital dynamics in order to point-and-shoot to close the link at the proper time. Feedback is very limited due to an extremely long time delay. Thus, communication methods must be developed that can accommodate such operational environments. Current thoughts are to utilize message switching (ref. 31) and bundling protocols somewhat analogous to e-mail (refs. 32 to 34). Interplanetary time-synchronization is also critical for interplanetary communication (ref. 35).

Summary

This document was generated to help dispel much of the misinformation and misconceptions regarding applicability of various communications protocols for use in satellite and space-based networks. The following key points should go a long way to help one decide on what protocols are appropriate for their particular applications:

- Vocabulary is very important when speaking of networking. Be precise.
- Protocols are simply tools for communication. One size does not fit all.
- Packet-based switching is generally simpler to configure, is more flexible, and often provides better bandwidth utilization than circuit-base switching.
- The operating environment heavily dictates what protocols can be used—particularly delay, bandwidth, and intermittent connectivity.
- Many protocols in the transmission control protocol/Internet protocol (TCP/IP) suite operate well in space. Others, such as TCP or routing protocols are applicable only to surface and some near-planetary applications.
- Consultative Committee for Space Data Systems (CCSDS) protocols have evolved over time as technology and processing power has improved. Originally designed to optimize power and processing on point-to-point links, CCSDS has begun incorporating networking capabilities with the advent of SCPS.
- Neither IPv4 nor IPv6 interoperate with SCPS–NP. A gateway is necessary.

[3]Although not stated, the Moon, Sun, and any celestial body can be considered—each with its own orbital dynamics characteristics.

- Current CCSDS data-link protocols are incompatible with COTS data-link protocols, requiring a data-link gateway for interoperability.
- Many CCSDS protocols—particularly legacy systems—merge layers and thus require application level gateways to operate with COTS protocols such as general IPs. Such merging of layers results in one-off implementation and makes interoperation difficult.[4]
- Great care should be taken when deploying PEPs. Understand their limitations.
- Gateways, including PEPs, must be maintained as protocols change. This can be an expensive proposition.
- Security is difficult anywhere. Sophisticated key management systems are not practical for space-based networks. Thus space-based security architectures should be as simple as policy will allow.

References

1. Schier J., et al.: Space Communication Architecture Supporting Exploration and Science: Plans & Studies for 2010–2030. AIAA–2005–2517, 2005.
2. Ivancic, Will: Internet Trends and the Cost of Connectivity. First BroadSky Workshop, Lacco Ameno, Italy, Nov. 2003. http://roland.grc.nasa.gov/~ivancic/papers_presentations/KaBand_BroadSky_2003.ppt
3. Alliance for Telecommunication Industry Solutions, http://www.atis.org/tg2k/_link.html Accessed Dec. 20, 2005.
4. Overview of Space Link Protocols. CCSDS 130.0–G–1, June 2001.
5. Carreon, P.: Electronic Systems Test Laboratory (ESTL) and Qualification & Utilization of Electronic System Technology (QUEST)—System Engineering Test Report—Space Based Communication System Upgrade. Prepared by NASA Johnson Space Center Code DV2, Dec. 2000. (NASA Internal Document)
6. Unix System Administration Independent Learning. http://www.ussg.iu.edu/usail/network/nfs/layers.html Accessed Dec. 20, 2005.
7. IEEE Standards Association. http://standards.ieee.org/ Accessed Dec. 20, 2005.
8. Standards Activities Overview. http://www.ansi.org/standards_activities/overview/overview.aspx?menuid=3 Accessed Dec. 20, 2005.
9. CCSDS. http://public.ccsds.org/publications/default.aspx Accessed Dec. 20, 2005.
10. Internet Engineering Task Force. http://www.ietf.org/ Accessed Dec. 20, 2005.
11. Space Communications Protocol Specification (SCPS)—Transport Protocol (SCPS–TP). CCSDS 714.0–B–1, Blue Book, issue 1, May 1999.
12. Schnurr, R., et al.: HDLC Link Framing for Future Space Missions. AIAA SpaceOps 2002, P–T5–21. http://www.aiaa.org/Spaceops2002Archive/papers/SpaceOps02-P-T5-21.pdf Accessed Dec. 20, 2005.
13. UoSat-12 Test Results Summary. Presented at the Small Satellite 2000 Conference, July 2000. http://ipinspace.gsfc.nasa.gov/documents Accessed Dec. 20, 2005.
14. Ivancic, William, et al: Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low-Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC). NASA/TM—2005-213556, 2005. http://gltrs.grc.nasa.gov/cgi-bin/GLTRS/browse.pl?2005/TM-2005-213556.html
15. Allman, M.; Glover, D.; and Sanchez, L.: Enhancing TCP Over Satellite Channels Using Standard Mechanisms. IETF RFC 2488, Jan. 1999. http://www.ietf.org/rfc/rfc2488.txt?number=2488 Accessed Dec. 20, 2005.
16. Allman, M.: Ongoing TCP Research Related to Satellites. IETF RFC 2760, Feb. 2000. http://www.ietf.org/rfc/rfc2760.txt?number=2760 Accessed Dec. 20, 2005.
17. Karn, P., et al.: Advice for Internet Subnetwork Designers. IETF RFC 3819, July 2004. http://www.ietf.org/rfc/rfc3819.txt?number=3819 Accessed Dec. 20, 2005.
18. Dawkins, S., et al.: End-to-End Performance Implications of Slow Links. IETF RFC 3150, July 2001. http://www.ietf.org/rfc/rfc3150.txt?number=3150 Accessed Dec. 20, 2005.
19. Dawkins, S., et al.: End-to-End Performance Implications of Links With Errors. IETF RFC 3155, Aug. 2001. http://www.ietf.org/rfc/rfc3155.txt?number=3155 Accessed Dec. 20, 2005.
20. Fairhurst, G.: Advice to Link Designers on Link Automatic Repeat reQuest (ARQ). IETF RFC 3366, Aug. 2002. http://www.ietf.org/rfc/rfc3366.txt?number=3366 Accessed Dec. 20, 2005.
21. Balakrishnan, H., et al.: TCP Performance Implications of Network Path Asymmetry. IETF RFC 3449, Dec. 2002. http://www.ietf.org/rfc/rfc3449.txt?number=3449 Accessed Dec. 20, 2005.

[4]The CCSDS Space Link Extensions (SLE) is designed to help alleviate some of this interoperability problem. However, as with any gateway, all variants of any protocol-pair mapping that must be accomplished, must be implemented. To date, each CCSDS implementation, although based on a standard, is a variant. Thus, implementing widespread interoperable SLE services is a daunting task.

22. Hogie, K.; Criscuolo, E. and Parise, R.: Using Standard Internet Protocols and Applications in Space. Comp., vol. 47, no. 5, 2004, pp. 603–650.
23. Wood, Lloyd: Testing a Router Onboard a Satellite in Space. Proceedings of the End-to-End Challenges of Broadband via Satellite, issue 2005–10808, 2005, pp. 81–85.
24. Jackson, C.: Saratoga File Transfer Protocol. SSTL Internal Technical Document, May 2004.
25. Hogie, K.: LPT/CANDOS IP Space Communication Results. Presented at Goddard Space Flight Center, June 2003. http://ipinspace.gsfc.nasa.gov/documents/CANDOS_MobileIP.ppt Accessed Dec. 20, 2005.
26. Space Communications Protocol Specification (SCPS)—Security Protocol (SCPS–SP). CCSDS 713.5–B–1, Blue Book, issue 1, May 1999
27. Symington S.; Farrell, S.; Weiss, H.: Bundle Security Protocol Specification. draft-irtf-dtnrg-bundle-security-00, June 8, 2005 (work in progress).
28. National Information Assurance (IA) Policy for U.S. Space Systems. Fact Sheet, NSTISSP no. 12, http://www.cnss.gov/Assets/pdf/nstissp_12.pdf Accessed Dec. 20, 2005.
29. Border, J., et al.: Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations. RFC 3135, June 2001. http://www.ietf.org/rfc/rfc3135.txt?number=3135 Accessed Dec. 20, 2005.
30. InterPlaNetary Internet Project. http://www.ipnsig.org/home.htm Accessed Dec. 20, 2005.
31. Fairhurst, Gorry: Message Switching. Jan. 10, 2001. http://www.erg.abdn.ac.uk/users/gorry/course/intro-pages/ms.html Accessed Dec. 20, 2005.
32. Cerf, V.S., et al.: Delay-Tolerant Network Architecture. draft-irtf-dtnrg-arch-03.txt, July 2005 (work in progress).
33. Scott, K.; and Burleigh, S.: Bundle Protocol Specification. draft-irtf-dtnrg-bundle-spec-03.txt, July 2005 (work in progress).
34. Burleigh S.; Ramadas, M.; and Farrell, S.: Licklider Transmission Protocol—Motivation. draft-irtf-dtnrg-ltp-motivation-01.txt, July 2005 (work in progress).
35. Akyildiz, I.F., et al.: InterPlanetary Internet: State-of-the-Art and Research Challenges. Comp. Net., vol. 43, no. 2, 2003, pp. 75–113.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	April 2006	Technical Memorandum

4. TITLE AND SUBTITLE

Taking the Politics Out of Satellite and Space-Based Communications Protocols

5. FUNDING NUMBERS

WBS–591158.04.04.04.03

6. AUTHOR(S)

William D. Ivancic

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

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

8. PERFORMING ORGANIZATION REPORT NUMBER

E–15415

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

National Aeronautics and Space Administration
Washington, DC 20546–0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

NASA TM—2006-214058

11. SUPPLEMENTARY NOTES

Prepared for GLOBECOM 2005 sponsored by the Institute of Electrical and Electronics Engineers, St. Louis, Missouri, November 28–December 2, 2005. Responsible person, William D. Ivancic, organization code RCN, 216–433–3494.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Categories: 62 and 17

Available electronically at http://gltrs.grc.nasa.gov

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

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 words)***

After many years of studies, experimentation, and deployment, large amounts of misinformation and misconceptions remain regarding applicability of various communications protocols for use in satellite and space-based networks. This paper attempts to remove much of the politics, misconceptions, and misinformation that have plagued space-based communications protocol development and deployment. This paper provides a common vocabulary for communications; a general discussion of the requirements for various communication environments; an evaluation of tradeoffs between circuit and packet-switching technologies, and the pros and cons of various link, network, transport, application, and security protocols. Included is the applicability of protocol enhancing proxies to NASA, Department of Defense (DOD), and commercial space communication systems.

14. SUBJECT TERMS

Encryption; Computer networks; Mobile networks; Security

15. NUMBER OF PAGES

16

16. PRICE CODE

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