CCSDS

The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

SPACE COMMUNICATIONS CROSS SUPPORT— ARCHITECTURE DESCRIPTION DOCUMENT

INFORMATIONAL REPORT

CCSDS 901.0-G-1

GREEN BOOK
November 2013

The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

SPACE COMMUNICATIONS CROSS SUPPORT— ARCHITECTURE DESCRIPTION DOCUMENT

INFORMATIONAL REPORT

CCSDS 901.0-G-1

GREEN BOOK
November 2013

AUTHORITY

Issue:	Informational Report, Issue 1
Date:	November 2013
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and reflects the consensus of technical panel experts from CCSDS Member Agencies. The procedure for review and authorization of CCSDS Reports is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3).

This document is published and maintained by:

CCSDS Secretariat
Space Communications and Navigation Office, 7L70
Space Operations Mission Directorate
NASA Headquarters
Washington, DC 20546-0001, USA

FOREWORD

This Report has been prepared by CCSDS for use in developing space communications cross support systems. The space communications cross support architecture described herein is intended to provide CCSDS Agencies with descriptions of recommended practices for the development of systems that provide single-hop and internetworking cross support services for space missions of other CCSDS Agencies.

This Report provides a common framework for describing space communications cross support systems and provides descriptions of practices for developing interoperable space communications and internetworking cross support services and systems. The architecture described in this document was developed based on the Cross Support Reference Model (reference [1]) and the Reference Architecture for Space Data Systems (reference [2]) developed by CCSDS. It defines in technical language an approach for developing systems that are aligned with the Interagency Operations Advisory Group (IOAG) Space Internetworking Strategy Group (SISG) Operations Concept for a Solar System Internetwork (SSI) (reference [3]).

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Report is therefore subject to CCSDS document management and change control procedures, which are defined in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 901.0-G-1	Space Communications Cross Support—Architecture Description Document, Informational Report, Issue 1	November 2013	Original issue

CONTENTS

CONTENTS (continued)

CONTENTS (continued)

CONTENTS (continued)

CONTENTS (continued)

1 INTRODUCTION

1.1 PURPOSE

The purpose of this Informational Report is to describe the CCSDS-recommended configurations for secure space communications cross support architectures. This architecture is to be used as a common framework when CCSDS Agencies 1) provide and use space communications cross support services, and 2) develop systems that provide interoperable space communications cross support services. These space communications cross support services include both elements on the ground and elements in space. These services are of two general types: space Data Link Layer services and internetworking services. Space data link services are used to provide end-to-end links connecting a Mission Operations Center (MOC) to the spacecraft it controls. Internetworking services are used to provide between a MOC and its spacecraft end-to-end Network Layer services that involve routing and internetworking using one or more space and ground assets.

This Space Communications Cross Support Architecture Description Document (SCCS-ADD) provides descriptive information; its companion Space Communications Cross Support Architecture Requirements Document (SCCS-ARD) (reference [4]) provides the normative specifications and definitions.

1.2 SCOPE

This document describes space communications cross support architecture in terms of the following:

- all elements, on ground and in space, that are involved in space communications;
- descriptions of concepts that characterize space communications cross support services;
- descriptions of system elements and components that provide secure space communications cross support services;
- a set of examples of possible protocol configurations;
- a set of examples of end-to-end system configurations to provide secure interoperable space communications services.

This document does not specify:

- the details of how to implement systems that provide space communications cross support services;
- explicit technologies needed to implement space communications cross support services;
- mission operations except for those involved in planning, scheduling, and executing space communications;
- spacecraft onboard cross support, except for space communication services.

This document contains descriptive materials and examples of different viable configurations. Any agency that wants to either use or provide single-hop cross support or space internetworking services should implement interoperable services and interfaces as defined in the companion Recommended Practice document (reference [4]), and as specified in the referenced CCSDS standards (see 1.6 and tables in section 6).

This document contains references to other CCSDS technical engineering and architectural recommendations which describe how systems doing space communications cross support should be engineered, deployed, organized, and operated to provide interoperable space communications cross support services. While this document does not specify detailed internal implementation approaches, which are a private matter, it does discuss recommended protocols, behavior, service interfaces, and end-to-end architectures.

Some of the standards that are described in this document, especially those relating to the SSI, are still in development. They are included here so the reader gets a clear understanding of how they fit into an overall architecture and why and how these new standards are different from existing ones. The protocol-related parts of this document make liberal reference to the layers defined in the Open Systems Interconnection (OSI) Basic Reference Model (reference [5]). (See 6.2 for a discussion of the OSI stack and the functions associated with each layer.)

The technical scope of single-hop cross support is the provision of Data Link Layer (Layer 2) data communications services across the Solar System in support of space mission users, using the *interoperable infrastructure of one or more space agencies*. Services above the Data Link Layer, such as CCSDS File Delivery Protocol (CFDP), Cross-Support File Service (CXFS), or Delta-Differential One-way Range (Delta-DOR), may also be provided.

The technical scope of the SSI is the provision of internetworked (Layer 3) data communications services across the Solar System in support of space mission users, using the confederated and interoperable infrastructure of multiple space agencies to achieve a level of service that individual agencies would otherwise be unlikely to achieve. The SSI protocols may also provide advantages to ‘single-hop’ missions. For example, the automated data forwarding feature of the SSI insulates the various systems from having to know the state of the communications path that is not local to them.

The temporal scope of this document covers current, single-hop, secure interoperable cross support installations, future deployments of an interoperable and evolving networked infrastructure, and the transition strategies to evolve from current typical agency deployments to a future SSI state. Included in this discussion are mission-driven considerations, such as use of hybrid science/routing missions, as well as identification of optional configurations that are considered acceptable because they are in line with the transition strategies defined in this document.

Any agency that wishes to participate as a peer in the SSI should implement interoperable services and interfaces at least up to the Network Layer, along with related support services, as described in this document and specified in the relevant CCSDS and Internet standards. Agencies that provide SSI services will need to establish peering agreements with their ‘neighbors’. These are described in more detail in 2.9.4. Agencies that are not yet ready to adopt the SSI themselves, but wish to offer compliant cross support services that can support

SSI services, may also take advantage of this document for guidance on developing Data Link Layer services that will both meet their immediate needs and also interoperate with SSI-enabled missions.

1.3 RATIONALE

CCSDS has developed a body of space communications recommendations that specify protocols and related services for specific types of functionality at a single layer of the OSI stack, and how to format and exchange a specific type of information. In order to build end-to-end space communications systems that will interoperate, systems designers need to understand how to select, configure, and deploy different kinds of system elements that implement a complete stack of protocols in each element and how these are assembled to deliver end-to-end services. Single-hop communications configurations often require cross support, where one space agency develops the spacecraft and the corresponding MOC, and another agency provides the ground-to-space communications assets. This is the typical cross support configuration used today. Multi-hop communications configurations may require that space assets developed by one agency offer cross support to space elements developed by another agency, with both being supported by ground communications assets from another agency.

Since cross support among agencies has become the norm, and since future agency collaborative missions require elements developed by different agencies, at different times, to interoperate as a network, agreed-upon interoperable standards and architectures must be adopted in an end-to-end sense. As the only international body that defines standards to link space communication service providers with space missions, CCSDS is defining a recommended standard architecture for space communications cross support services, so that interoperable cross support between agencies can be defined and operated more efficiently and effectively for single-hop and multi-hop mission configurations.

Fundamental to the SSI concept is that all full participants in the confederation must expose standard and agreed-upon cross support services at the Network Layer of the OSI communications stack, while observing common network management strategies and governance mechanisms. Agencies that only provide single-hop Data Link Layer services may still participate in the SSI if they provide compliant services at that layer.

This document addresses end-to-end interoperability for both single space link configurations (called ABA configurations—see 1.5.1) and solar system internetworking configurations (called SSI configurations—see 1.5.1).

1.4 DOCUMENT STRUCTURE

This document consists of several sections plus annexes.

- Section 1 presents the purpose, scope, and rationale of this document and lists the definitions, conventions, and references used throughout the document.

- Section 2 provides context and an overview of the space communications cross support architecture.
- Section 3 provides a cross support overview of the ABA and SSI technical architectures.
- Section 4 defines a service view of ABA and SSI configurations from user and provider perspectives.
- Section 5 defines a physical view of spacecraft and ground system functional elements that make up the deployed ABA and SSI configurations.
- Section 6 defines a communications view and provides a set of example application profile ‘stack’ protocol views of the ABA and SSI.
- Section 7 provides an end-to-end deployment view and a set of example end-to-end views.
- Annexes provide an acronym list and background information related to this document.

Each of sections 4 through 7 includes a descriptive introduction, and extended descriptive subsections that provide explanations and examples.

1.5 DEFINITIONS AND CONVENTIONS

1.5.1 TERMS

For the purposes of this document, the following definitions apply. The normative set of definitions is to be found in reference [4]. They are repeated here for convenience. Many of these terms are derived from other sources. Primary sources of definitions are references [1], [2], [6], [5], [7], [8], [9], and [10].

NOTE – Many other terms that pertain to specific items are defined in the appropriate sections. A list of acronyms can be found at annex A.

ABA: A ‘single-hop’ space communications configuration that involves only a single direct to/from Earth space link. Term derives from the notion of an Agency ‘A’ using the ground station of an Agency ‘B’ to communicate between its MOC and its spacecraft, hence ABA.

ABCBA: A multi-hop space communications configuration that involves multiple space and ground elements and one or more direct to/from Earth space links or space-space links. ABCBA configurations nominally include elements from three or more agencies.

Application Layer services: OSI Layer 7 services provided to user applications, such as file or message transfer.

Application Layer: OSI Layer (Layer 7) containing all those functions that imply communication between open systems that are not already performed by the lower layers.

BCH code: A parameterized error-correcting code used for uplink commanding.

building block: The set of nodes, with specific defined characteristics, that are used to describe end-to-end system configurations in this document.

Coding and Synchronization sublayer: CCSDS-defined sublayer (of the OSI Data Link Layer) that provides error detection and correction for the space Data Link Layer protocols to deal with noisy, low signal-to-noise ratio, space link physical channel characteristics.

cross support service element, CSSE: A physical element involved in providing one or more cross support services (including functions for managing services).

cross support service system, CSSS: A set of CSSEs or user elements that are managed by a single authority with a single set of management policies. These may be user or provider systems.

cross support service: A function provided by one space agency to support operations of a space mission of another space agency.

Cross Support Transfer Service, CSTS: A set of cross support services, based on a common framework, that provides reliable, access-controlled transfer of spaceflight mission-related data between ground CSSEs and terrestrial user elements. A CSTS is qualified by the kind of data it transfers (e.g., telemetry frames, tracking data). (See also SLE definition.)

cross support: An agreement between two or more organizations to exploit the technical capability of interoperability for mutual advantage, such as one organization offering support services to another in order to enhance or enable some aspect of a space mission.

data delivery services: CSTS and space link extension services used to deliver data between an Earth-Space Link Terminal (ESLT) and the ground user elements that use it.

Data Link Layer: The OSI Layer (Layer 2, also just *Link Layer*) that provides functional and procedural means for the establishment, maintenance, and release of data link connections among Network Layer entities (where they are used) and for the transfer of data link service data units. CCSDS defines two sublayers in the Data Link Layer of the OSI Model: a Protocol sublayer and a Coding and Synchronization sublayer (see).

data store: Staging for data in transit on the network.

Earth routing node: A physical element, located on the ground, that has responsibility for operating and managing one or more space routing nodes. It may, or may not, directly participate in routing DTN traffic.

Earth Space Link Terminal (ESLT): The CSSE that provides space communication services between the Earth User Node and the Space User Node. It includes the ground station control and management systems. The ESLT has space link protocol interfaces and supports terrestrial SLE and CSTS interfaces. The ESLT also has a service management interface that is controlled by the UE that is responsible for managing the space link.

Earth user access: A port that provides access to a space link user on the 'ground' (i.e., Earth or another planetary surface).

Earth User Node: A physical element, located on the ground, that uses a cross support service provided by a CSSS.

Earth-space terminal access: A port that provides access to a space link terminal on Earth.

element management, EM: A set of functions that manage elements and interact with provision management for purposes of ascertaining element resource availability, configuration and execution of element resources, and reporting status of those resources. User elements also have internal element management functions.

emergency communication services: Specialized services for delivering emergency, 'last-hop', or primitive 'brain stem' commanding to a spacecraft.

encapsulation: A function that wraps a PDU in another PDU in order to transfer it to its destination.

forward data: Data sent from a ground element to a space element.

forwarding: The act of transferring data from its source towards its destination, which may be in space or on the ground.

functional resource: The functions or capabilities that are provided by physical resources (e.g., transmitters and receivers) of a CSSE, but not those physical resources themselves. A functional resource is a logical construct not necessarily linked to any single system component.

gateway: A function that provides protocol translation between two different, but compatible, protocols at the same OSI Layer, e.g., IP to BP.

governance: Decision making that defines expectations, grants power, or verifies performance. It consists either of a separate process, or of a specific part of management or leadership processes. Governance relates to consistent management, cohesive policies, processes, and decision rights for a given area of responsibility.

in-space: Extraterrestrial. In this usage, in-space communications includes Earth-to-space, space-to-space, space-to-planetary surface, planetary surface-to-surface, etc.

interface binding signature: A 'signature' that results from a service user and service provider implementing the proper stack of interface protocols in order to bind to service elements. This signature may involve Transmission Control Protocol/Internet Protocol

(TCP/IP), Hypertext Transfer Protocol (HTTP), or some set of CCSDS space-communication protocols.

internetwork: A ‘network of networks’, where two or more distinct computer networks are connected together using routing devices that allow traffic to flow back and forth between the networks.

internetworking: Practice of connecting two or more distinct computer networks or network segments together to form an internetwork (often shortened to *internet*), using devices which operate at OSI Layer 3 (Network Layer) to connect them together to allow traffic to flow back and forth between them.

interoperability: A property of protocols or systems whereby elements adopt a commonly defined and implemented set of protocols, data, and behaviors.

Network Layer processing: OSI Layer 3 processing that includes any needed routing, forwarding, and management functions.

Network Layer: OSI Layer 3, which provides the means to establish, maintain, and terminate network connections between open systems and provides transport entities independence from routing and relay considerations.

network management: Real-time control of space communication service functions.

network: One or more computers or other processing elements that are owned by a single organization, communicating using a single OSI Layer 3 protocol.

node: A space data system physical entity operating in a physical environment. A node is a configuration of engineering objects forming a single unit for the purpose of location in space, and embodying a set of processing, storage and communication functions. A node has some well-understood, possibly rapidly moving location, and it may be composed of two or more (sub-)nodes.

peering: Voluntary interconnection of administratively separate networks. Peering at the Network Layer includes SSI CSSEs’ carrying each other’s user traffic and also exchanging routing, accessibility, and other network management information.

physical channel: A stream of bits transferred over a space link in a single direction.

Physical Layer: OSI Layer 1, which provides for the transparent transmission of bit streams between data-link entities across physical connections and the mechanical, electrical, functional and procedural means to activate, maintain, and deactivate physical connections.

planet-space terminal access: A port that provides access to a space link terminal on a planetary body.

protocol data unit, PDU: A unit of data which is specified in a protocol of a given layer and which consists of protocol-control information, addressing information, and possibly user data for that layer.

protocol sublayer: CCSDS-defined sublayer (of the OSI Data Link Layer) that specifies methods of transferring data units provided by the higher layer over a space link using data units known as Transfer Frames.

provider system: A CSSS that provides services to a user CSSS. A provider CSSS may also be a user of other CSSS services.

provision management, PM: A set of functions of a CSSS, related to the acquisition and management of services provided by that CSSS to other CSSSes. PM interacts with the utilization management of user CSSSes to negotiate provision of services to their respective CSSSes.

Proximity link: A communications link between an element in space and another nearby element in space or on the surface of a planetary body (<1 second Round-Trip Light Time [RTLT]).

relaying: A managed process for forwarding frame or packet data that involves no decision making

return data: Data sent from a space element to a ground element.

router: A device that forwards Network Layer PDUs between computer networks, creating an Internetwork. A router is connected to two or more data links from different subnetworks and uses address information in the PDU and information in its routing table or routing policy to direct the PDU to the next subnetwork.

routing: The process of selecting paths from origins to destinations in a network.

service management: 1) The set of functions exposed by PM to utilization management for the purposes of acquiring and managing the services provided by the provider CSSS to the user CSSS. These functions include planning, scheduling, and managing the configuration of space communication service functions. 2) The specification for exchanging service management information.

service provider: The role played by a physical, functional, or organizational entity that provides a cross support service for a service user. (A single entity may play the roles of service provider and service user at the same time.)

service user: The role played by a physical, functional, or organizational entity that uses a cross support service provided by a service provider. (A single entity may play the roles of service provider and service user at the same time.)

signal-to-noise ratio, SNR: A measure that compares the level of a desired signal to the level of background noise. The principal signal degradations in space communications are due to the loss of signal energy with distance, and to the thermal noise in the receiving system.

Solar System Internetwork, SSI: A carefully coordinated and managed confederation of independent space communications networks, each often owned and administered by a different space agency.

space asset access: A port that provides access to spaceborne assets offering functions such as routing or relaying.

space communications protocol: A communications protocol designed to be used over a space link or in a network that contains one or multiple space links.

space link access: A port that provides access to a space link.

space link application services: Specialized services offering direct access to the space Link Layer, such as VC service, insert zone.

space link extension, SLE: A set of specific cross support services that provide reliable, access-controlled transfer of spaceflight mission-related data between ground cross support services and user elements. Each specific SLE service is defined separately for the kind of data it transfers (e.g., telemetry frames, telecommand, Command Link Transmission Units [CLTUs], operational control field). (See also CSTS definition.)

space link interface: The interface of a CSSE that uses space link protocols.

space Link Layer processing: Processing at OSI Layers 1 and 2 for space communications, including any needed framing, coding, and modulation.

space link: A communications link between a spacecraft and its associated ground system or between two spacecraft. A space link consists of one or more physical channels in one or both directions.

space routing node: A physical element located in space that provides space internetworking services.

space user access: A port that provides access for an end-user node.

Space User Node: A physical element located in space that uses a cross support service provided by a CSSS.

store and forward, S&F: The process of holding data (store) until a path is available to send it to its destination (forward).

supported agency: A space agency that uses cross support services.

supporting agency: A space agency that provides cross support services.

terrestrial Link Layer processing: OSI Layers 1 and 2 processing for ground communications, including any needed framing, coding, and modulation.

terrestrial-link interface: The interface of a CSSE that uses terrestrial link (and networking) protocols.

tracking data: Any of the following: pointing information, raw or validated tone, Pseudo-Noise ranging results, correlated Delta-DOR data.

Transport Layer: OSI Layer 4, which has end-to-end significance, where the ends are defined as transport entities having transport associations. The Transport Layer provides transparent transfer of data between applications and relieves them from any concern with subnetwork topologies or the detailed way in which transfer of data is achieved.

user applications: OSI Layer 8 functions that use other communications services.

user element, UE: A physical element involved in using one or more cross support services (including functions for managing services). In some configurations a user element may act as a CSSE.

utilization management, UM: A set of functions of a CSSS or user system, related to the acquisition and management of services provided to that CSSS or user system by other CSSSes.

virtual channel, VC: A capability to logically split a single physical or master channel into multiple virtual ones.

WAN access: A port that provides access to a wide-area network.

wide area network, WAN: A set of routers and associated links that provides Network Layer connectivity among two or more terrestrial or planetary surface nodes. The routers may support either IP or DTN or both Network Layer functions.

NOTE – The terms ‘forward’ and ‘return’ are used in this document even for SSI, and they are associated with ‘forwarding’ commands or requests, and ‘returning’ of data. However, for SSI nodes, these ‘directions’ are relative to the sender and receiver, not just to communications to/from the Earth. A forward request could be from a user node on a planetary surface to another user node elsewhere on either that same planet, or to one in orbit around the planet. Elsewhere in this document are used the terms *sending* for outbound connections and *receiving* for inbound connections. In the general case, intermediate routing nodes will also do staging of data, route selection, and forwarding of these data when a path is available in the proper direction.

1.5.2 CONVENTIONS

For the purposes of this document, the graphical conventions shown in figure 1-1 are used. They are derived from the Reference Architecture for Space Data Systems (RASDS) (reference [2]).

There are several different types of objects depicted in the diagrams in this document; they may be color coded according to the key to identify their different nature and/or associated functionality.

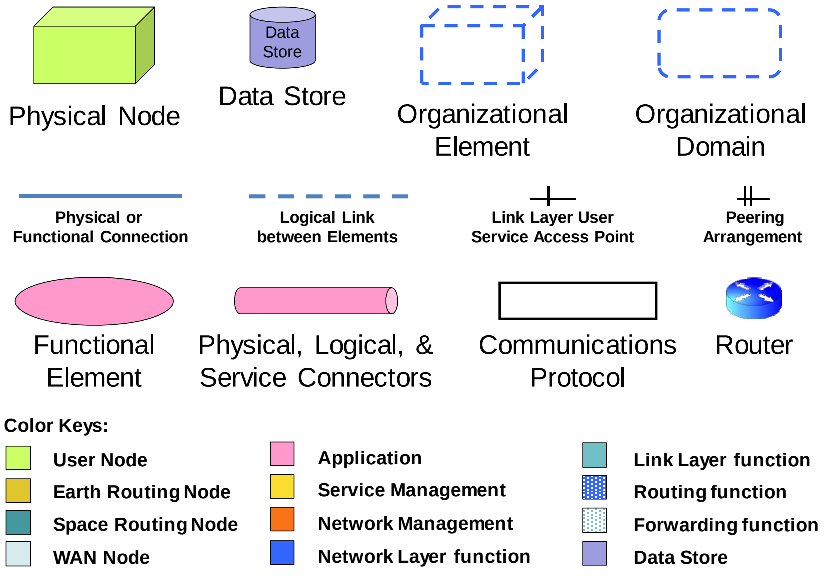


Figure 1-1: Graphical Conventions

NOTES

1 Physical nodes (system elements) are depicted with solid three-dimensional boxes.

2 Data stores are shown as a cylinder.

3 Organizations are depicted with dashed three-dimensional boxes. Organizational domains are depicted with rounded, dashed, two-dimensional boxes.

4 Physical or functional connections are depicted with solid lines.

5 Logical links between elements are depicted with dashed lines.

6 Functional elements (aside from communications protocols) are depicted with ovals. Not all are application layer functions.

7 Service connections are depicted as pipes.

8 Communications protocols are depicted with two-dimensional boxes.

1.6 REFERENCES

The following documents are CCSDS, Internet, or other international standards referenced in this Report. At the time of publication, the editions indicated were valid. All of the documents in this section that have CCSDS Blue or Magenta book numbers, or that have RFC, ISO, or other numbers are formal specifications that are valid as of the time of publication. Users of this Report should be aware that in order to provide adequate guidance for the future, some of the documents that are referenced are still under development (CCSDS Red Books, White Books) or are otherwise in draft form, and these are so marked. There is, of course, a finite chance that some of these standards, when finalized, will not have exactly the features that are described here. In addition to the documents explicitly referenced in the text, there are some other standards referenced in tables that may not be included here.

[1] *Cross Support Reference Model—Part 1: Space Link Extension Services*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 910.4-B-2. Washington, D.C.: CCSDS, October 2005.

[2] *Reference Architecture for Space Data Systems*. Issue 1. Recommendation for Space Data System Practices (Magenta Book), CCSDS 311.0-M-1. Washington, D.C.: CCSDS, September 2008.

[3] *Operations Concept for a Solar System Internetwork (SSI)*. IOAG.T.RC.001.V1. Washington, DC: IOAG, 15 October 2010.

[4] *Space Communications Cross Support—Architecture Requirements Document*. Proposed Recommendation for Space Data System Practices, CCSDS 901.1, proposed.

[5] *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*. 2nd ed. International Standard, ISO/IEC 7498-1:1994. Geneva: ISO, 1994.

[6] *Solar System Internetwork (SSI) Issue Investigation and Resolution*. IOAG.T.SP.001.V1. Washington, DC: IOAG, 1 August 2010.

[7] *Security Architecture for Space Data Systems*. Issue 1. Recommendation for Space Data System Practices (Magenta Book), CCSDS 351.0-M-1. Washington, D.C.: CCSDS, November 2012.

[8] *Cross Support Transfer Service—Specification Framework*. Issue 1. Draft Recommendation for Space Data System Standards (Red Book), CCSDS 921.1-R-1. Washington, D.C.: CCSDS, August 2010.

[9] *Solar System Internetwork (SSI) Architecture*. Draft Report Concerning Space Data System Standards, CCSDS 730.1-G, forthcoming.

[10] *Overview of Space Communications Protocols*. Issue 2. Report Concerning Space Data System Standards (Green Book), CCSDS 130.0-G-2. Washington, D.C.: CCSDS, December 2007.

[11] *TC Synchronization and Channel Coding*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 231.0-B-2. Washington, D.C.: CCSDS, September 2010.

[12] *AOS Space Data Link Protocol*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 732.0-B-2. Washington, D.C.: CCSDS, July 2006.

[13] *TM Space Data Link Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 132.0-B-1. Washington, D.C.: CCSDS, September 2003.

[14] *Space Communication Cross Support—Service Management—Service Specification*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 910.11-B-1. Washington, D.C.: CCSDS, August 2009.

[15] *Information Technology—Open Distributed Processing—Reference Model: Architecture*. International Standard, ISO/IEC 10746-3:1996. Geneva: ISO, 1996.

[16] *Concept for Next Generation Space Communications Cross Support Service Management*. Proposed CCSDS Informational Report, forthcoming.

[17] *IOAG Service Catalog #1*. Washington, DC: IOAG, March 2010.

[18] J. Hawkinson and T. Bates. *Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*. RFC 1930. Reston, Virginia: ISOC, March 1996.

[19] *Mars Mission Protocol Profiles—Purpose and Rationale*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 740.0-G-1. Washington, D.C.: CCSDS, July 2008.

[20] *IOAG Service Catalog #2*. IOAG.T.SC2.2011.V1.0. Washington, DC: IOAG, February 2011.

[21] S. Burleigh. “Contact Graph Routing.” *NASA Tech Briefs* (23 September 2011).

[22] *CCSDS Cryptographic Algorithms*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 352.0-B-1. Washington, D.C.: CCSDS, November 2012.

[23] *Radio Frequency and Modulation Systems—Part 1: Earth Stations and Spacecraft*. Issue 22. Recommendation for Space Data System Standards (Blue Book), CCSDS 401.0-B-22. Washington, D.C.: CCSDS, January 2013.

[24] *TM Synchronization and Channel Coding*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 131.0-B-2. Washington, D.C.: CCSDS, August 2011.

[25] *Bandwidth-Efficient Modulations: Summary of Definition, Implementation, and Performance*. Issue 2. Report Concerning Space Data System Standards (Green Book), CCSDS 413.0-G-2. Washington, D.C.: CCSDS, October 2009.

[26] *Space Packet Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 133.0-B-1. Washington, D.C.: CCSDS, September 2003.

[27] *Encapsulation Service*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 133.1-B-2. Washington, D.C.: CCSDS, October 2009.

[28] *Aircraft Internal Time Division Command/Response Multiplex Data Bus*. Military Standard, MIL-STD-1553B. Washington, DC: U.S. Department of Defense, 21 September 1978.

[29] *Space Engineering—SpaceWire—Links, Nodes, Routers and Networks*. ECSS-E-ST-50-12C. Noordwijk, The Netherlands: ESA Requirements and Standards Division, 31 July 2008.

[30] *Proximity-1 Space Link Protocol—Data Link Layer*. Issue 4. Recommendation for Space Data System Standards (Blue Book), CCSDS 211.0-B-4. Washington, D.C.: CCSDS, July 2006.

[31] *Proximity-1 Space Link Protocol—Physical Layer*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 211.1-B-3. Washington, D.C.: CCSDS, March 2006.

[32] *Proximity-1 Space Link Protocol—Coding and Synchronization Sublayer*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 211.2-B-1. Washington, D.C.: CCSDS, April 2003.

[33] *TC Space Data Link Protocol*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 232.0-B-2. Washington, D.C.: CCSDS, September 2010.

[34] *TM Space Data Link Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 132.0-B-1. Washington, D.C.: CCSDS, September 2003.

[35] *CCSDS File Delivery Protocol (CFDP)*. Issue 4. Recommendation for Space Data System Standards (Blue Book), CCSDS 727.0-B-4. Washington, D.C.: CCSDS, January 2007.

[36] *Asynchronous Message Service*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 735.1-B-1. Washington, D.C.: CCSDS, September 2011.

[37] K. Scott and S. Burleigh. *Bundle Protocol Specification*. RFC 5050. Reston, Virginia: ISOC, November 2007.

[38] M. Ramadas, S. Burleigh, and S. Farrell. *Licklider Transmission Protocol—Specification*. RFC 5326. Reston, Virginia: ISOC, September 2008.

[39] S. Symington, et al. *Bundle Security Protocol Specification*. RFC 6257. Reston, Virginia: ISOC, May 2011.

[40] E. Birrane and V. Ramachandran. *Delay Tolerant Network Management Protocol*. Proposed Internet-Draft. Reston, Virginia: ISOC, forthcoming.

[41] J. Postel. *Internet Protocol*. STD 5. Reston, Virginia: ISOC, September 1981.

[42] J. Postel. *Transmission Control Protocol*. STD 7. Reston, Virginia: ISOC, September 1981.

[43] J. Postel and J. Reynolds. *File Transfer Protocol*. STD 9. Reston, Virginia: ISOC, October 1985.

[44] S. Kent and K. Seo. *Security Architecture for the Internet Protocol*. RFC 4301. Reston, Virginia: ISOC, December 2005.

[45] *Space Link Extension—Forward CLTU Service Specification*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 912.1-B-3. Washington, D.C.: CCSDS, July 2010.

[46] *Space Link Extension Forward Frame*. CCSDS White Paper, forthcoming.

[47] *Space Link Extension—Return All Frames Service Specification*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 911.1-B-3. Washington, D.C.: CCSDS, January 2010.

[48] *Space Link Extension—Return Channel Frames Service Specification*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 911.2-B-2. Washington, D.C.: CCSDS, January 2010.

[49] *Space Link Extension—Return Operational Control Fields Service Specification*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 911.5-B-2. Washington, D.C.: CCSDS, January 2010.

[50] *Return Unframed Telemetry Cross Support Transfer Service*. Proposed CCSDS Draft, forthcoming.

[51] *Tracking Data Cross Support Transfer Service*. Proposed CCSDS Draft, forthcoming.

[52] *Cross Support Transfer Service—Transfer File*. Proposed CCSDS Draft, forthcoming.

[53] *Cross Support Transfer Service—Monitored Data*. Proposed CCSDS Draft, forthcoming.

[54] *Cross Support Transfer Service—Service Control*. Proposed CCSDS Draft, forthcoming.

[55] *XML Specification for Navigation Data Messages*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 505.0-B-1. Washington, D.C.: CCSDS, December 2010.

[56] *Space Link Extension—Enhanced Forward CLTU Service Specification*. Issue 1. Research and Development for Space Data System Standards (Orange Book), CCSDS 912.11-O-1. Washington, D.C.: CCSDS, July 2012.

[57] *Space Data Link Security Protocol*. Issue 3. Draft Recommendation for Space Data System Standards (Red Book), CCSDS 355.0-R-3. Washington, D.C.: CCSDS, October 2013.

[58] *Symmetric Key Management*. Proposed CCSDS Draft, forthcoming.

[59] S. Kent. *IP Encapsulating Security Payload (ESP)*. RFC 4303. Reston, Virginia: ISOC, December 2005.

[60] E. Rescorla. *HTTP Over TLS*. RFC 2818. Reston, Virginia: ISOC, May 2000.

[61] R. Fielding, et al. *Hypertext Transfer Protocol -- HTTP/1.1*. RFC 2616. Reston, Virginia: ISOC, June 1999.

[62] M. Horowitz and S. Lunt. *FTP Security Extensions*. RFC 2228. Reston, Virginia: ISOC, October 1997.

[63] *CCSDS Guide for Secure System Interconnection*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 350.4-G-1. Washington, D.C.: CCSDS, November 2007.

[64] *Recommendations on a Strategy for Space Internetworking*. Report of the Interagency Operations Advisory Group Space Internetworking Strategy Group, IOAG.T.RC.002.V1. Washington, DC: IOAG, 15 November 2008.

[65] *Functional Resources for Cross Support Services*. Draft Technical Note, CSSA-CSS_FRs-TN-0.01. N.p.: n.p., April 2013.

[66] *CCSDS Bundle Protocol Specification*. Issue 2. Draft Recommendation for Space Data System Standards (Red Book), CCSDS 734.2-R-2. Washington, D.C.: CCSDS, October 2013.

[67] *Streamlined Bundle Security Protocol for CCSDS*. Proposed CCSDS Draft, forthcoming.

2 SPACE COMMUNICATIONS CROSS SUPPORT ARCHITECTURE

2.1 BACKGROUND

Cross support is an activity of one space agency providing resources to support the operations of a space mission of another space agency. To reduce the cost of developing systems for operating space missions, multi-agency cross support arrangements have been used by many space missions. To date, most cross support has been one agency using the ground-based communications assets of another agency. This has already shifted to where agencies are providing cross support for in-space relaying of data, but these technical and operational arrangements, to date, have been mission-specific and rather ad hoc and idiosyncratic.

To facilitate space communications cross support, CCSDS developed standard protocols to transfer telecommands (references [11] and [12]) and telemetry (references [34] and [12]) over space links, which can ensure Link Layer interoperability between space elements and ground elements belonging to different agencies. CCSDS also developed standard SLE services (references [1] and [8]) to transfer telecommand and telemetry data on the ground (for example, between a ground station and a spacecraft control center) and service management (reference [14]) as the standard means to request cross support services. By using these CCSDS protocols and services, interoperability between elements of different agencies can be guaranteed to some extent at the Link Layer, but coordination and negotiation for cross support is still done in mission-specific, labor-intensive ways. Space communications cross support and interoperability at higher protocol layers than the space data link, such as internetworking cross support in space, will require some new protocols and new approaches to mission design if space internetworking is to become a reality.

The SCCS communications architecture reference model described in this document establishes a common framework that provides a basis for developing, providing, and using space communications cross support services. This is done by defining a set of common concepts, common protocols and configurations, and common processes and terminology. This architecture is intended to 1) facilitate development of interoperable end-to-end space communications cross support systems, 2) describe characteristics of space communications cross support services, and 3) provide examples of protocol stacks for ground and space, including Data Link and Network Layers.

2.2 ROLE OF THIS ARCHITECTURE DESCRIPTION DOCUMENT

This SCCS-ADD Green Book provides the top-level description of the architecture elements of space communications cross support as shown in figure 2-1. The descriptions in each section start by 1) addressing the needs of simple, single-hop missions that form the bulk of current cross support configurations (ABA configurations), 2) describing what is required to achieve a fully internetworked ‘end game’: a secure, interoperable SSI, and also 3) providing specific descriptions of how to architect the building blocks for these missions. This ADD provides examples of how to architect the building blocks for the ABA systems in a way that can directly serve existing mission modes, the future SSI, and also transitional states between them. This is especially important since these transitional configurations, when correctly constructed, will directly support the future SSI as well as offer useful services for missions and agencies that do not need to adopt the full SSI functionality. Within each section of this document, this SCCS-ADD addresses each of these operational configurations, along with any transitional information. The intent is to permit users who only require single-hop services to be able to readily find the information they need, while also providing guidance for those who are interested in progressing toward the full SSI.

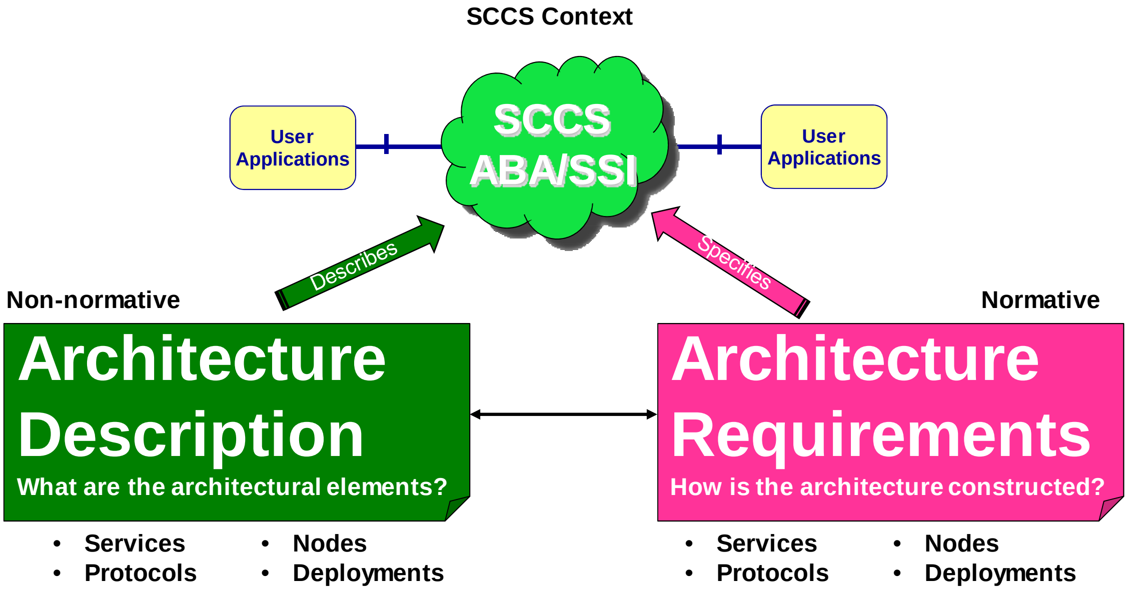


Figure 2-1: Roles of the SCCS Architecture Documents

The companion document, the SCCS-ARD Magenta Book (reference [4]), provides concrete guidance and normative subsections that define the required elements, attributes, and behaviors for service interfaces, functional allocations at nodes, protocol stacks, and end-to-end configurations for both ABA and SSI deployments.

Single-hop cross support has been in use for more than 20 years, largely because of the significant cost of developing ground-communications infrastructure capable of performing near-Earth and deep-space communications. Sharing use of expensive assets has been proven to be cost effective for these ABA mission configurations. For much the same reason, space agencies who are developing missions to do surface and orbital observations of remote planets and moons are adopting architectures that permit shared use of communications assets. In these cases, some assets are in space and require cross support among space assets as well as ground assets. The SSI was conceived as a way to address cross support in space; it is a conceptual extension of the Internet on the ground. While not all missions require this sort of service, those that do will benefit enormously from standardization.

The SSI is intended to be developed in an evolutionary fashion from elements that are produced on a mission-by-mission basis, using ground-system infrastructure elements that are owned by different agencies which will also evolve over time. The approach described in this Report is one that will support evolution from the current practice (which is most typically a single-spacecraft-to-single-space-link approach), to one that increasingly uses a routing spacecraft to forward files from one spacecraft to another, to the full-fledged SSI.

This SCCS-ADD describes the multi-agency, interoperable, secure technical architecture for space communications cross support, including single-hop and internetworked configurations. For single-hop configurations, it describes how service users (MOCs) may use the assets of service providers (ground tracking stations) to communicate with their space assets. For the *end state*, it describes how the SSI may be built and organized (including transitional arrangements). This SCCS-ADD describes 1) the service elements from both end-user and service provider perspectives, 2) the physical elements and building blocks of the SSI, 3) the communications protocols that permit them to operate in end-to-end delivery of service, and 4) the underlying organizational principles. Section 7 provides some examples of specific end-to-end configurations for single-hop missions, for SSI missions, and for transitional strategies in getting from the present ABA operational state to the future SSI one; this includes mixed-mode states describing how SSI-compliant and non-SSI-compliant missions may interoperate in a limited fashion.

2.3 STRUCTURE OF THE ADD: FOUR VIEWS OF SYSTEM ARCHITECTURE

2.3.1 GENERAL

Large-scale system architectures are complex and must be considered from different perspectives, including both technical and operational views. An architecture that provides multi-agency space communications cross support services and uses service systems or elements, has many technical and organizational aspects to it. To help make each of these aspects clear, this ADD uses multiple views to describe space communications cross support services and systems, each focusing on different aspects associated with these services and systems.

The views used in this architecture are:

a) a service view;

b) a physical view;

c) a communications view;

d) an end-to-end deployment view.

These views were defined based on four of the six viewpoints of the RASDS (reference [2]), which were themselves defined based on the five viewpoints of the Reference Model of Open Distributed Processing (reference [15]). Those documents contain more background on this approach of using distinct viewpoints to describe system architectures.

2.3.2 SERVICE VIEW

The service view is discussed in section 4 and is used to describe services provided by CSSSes/CSSEs and their behavioral and interface characteristics. Specifically, it addresses the topics of:

- functional characteristics of services;
- performance characteristics of services;
- means for locating and binding to services;
- methods and/or standards for using services;
- methods and/or standards for managing services.

2.3.3 PHYSICAL VIEW

The physical view is addressed in section 5 and describes the physical configuration of CSSSes/CSSEs and their physical characteristics. Specifically, it addresses the topics of:

- physical location;
- topology and connectivity;
- allocated functionality;
- physical media for access.

2.3.4 COMMUNICATIONS VIEW

The communications view, which is covered in section 6, describes communications protocols used for accessing services provided by CSSSes/CSSEs. Specifically, it addresses the topics of:

- communications protocols;
- suitable ‘building block’ stacks of communications protocols;
- examples of simple assemblies of these communications protocol building blocks.

2.3.5 END-TO-END VIEW

The end-to-end view is discussed in section 7 and describes how to configure the communications protocol building blocks to construct a set of representative mission communications configurations. Specifically, it provides a set of examples covering the following:

- ABA configurations;
- transitional configurations;
- SSI configurations;
- specific examples of mixed ABA and SSI configurations.

The companion Recommended Practice document, the SCCS-ARD (reference [4]), provides a set of normative recommendations for offered service interfaces, CSSE node configurations, suitable building blocks, and end-to-end protocol and system configurations for cross support.

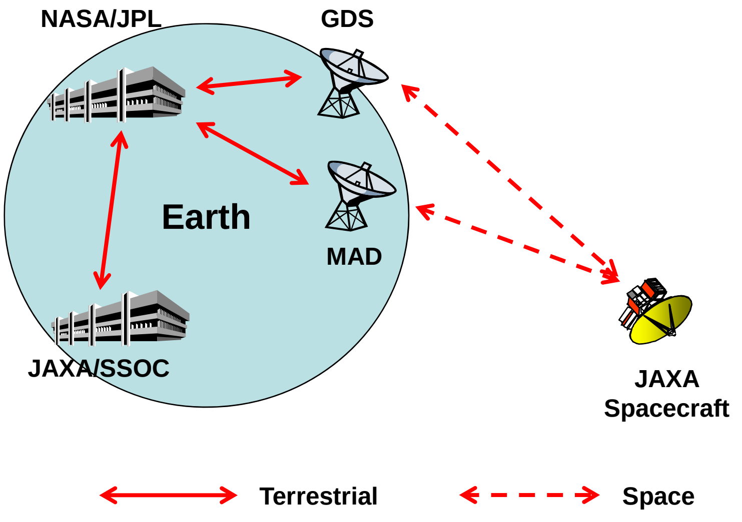
2.4 GENERAL DESCRIPTION OF CONTEXT

The SCCS architecture was developed based on the CCSDS Cross Support Reference Model (reference [1]), the draft SCCS-ARD (reference [4]), and the IOAG SISG SSI studies (references [11] and [12]). The model specified in reference [1] provides an architectural model for SLE services provided by ground stations. The SCCS architecture extends this terrestrial model in order to cover cross support services provided by other elements, such as orbiting spacecraft and elements on the surface of other planets.

NOTE – The term ‘planet’ is used in a general sense throughout this document in reference to any natural celestial object, such as the Earth, Moon, other planets and asteroids.

The IOAG SSI operational concept and studies describe agreed-upon technical means for evolving current cross support to provide SSI services. In order to make clear all of the different aspects of these distributed multi-agency systems, the RASDS specified in reference [2] is used as the conceptual framework for presenting this architecture from several different technical and organizational perspectives.

Figure 2-2 shows a typical current single-hop cross support physical configuration. Space communications cross support can occur across all of the red lines shown in this figure. The SCCS-ADD is intended to provide a common framework applicable to all of the space communications cross support services that are provided and used across all of these red lines. It is assumed that a space communications cross support service is always used by a pair of user nodes (one in space and the other on the ground), where other assets participate in providing the end-to-end services.



JPL = Jet Propulsion Laboratory
GDS = Deep Space Network (DSN) Goldstone Deep Space Communications Complex
MAD = DSN Madrid Deep Space Communications Complex
SSOC = Science Operations Center

Figure 2-2: Basic ABA Space Mission Cross Support Configuration

In figure 2-2, a JAXA SSOC uses one of two DSN ground stations in order to communicate to its spacecraft. Each of the ground stations is used one at a time, and each end-to-end link is an example of an ABA configuration. JAXA must make prior arrangements for services with the DSN, establish a Service-Level Agreement (SLA), and identify mission communication support configurations. The JAXA SSOC has responsibility for scheduling and configuring the link using standard service management interfaces, and it then uses standard Link Layer data transfer service interfaces to send data to and from the spacecraft. The DSN installations may have full SSI capabilities, but in this scenario only the Link Layer services are being used.

Figure 2-3 shows a possible future physical configuration of SSI space missions. Space communications cross support might, in the future, also happen on all of the dashed red lines in this diagram, but here many of these are directly between assets in space. The SSI segments of this SCCS-ADD are intended to provide a common framework applicable to all of these space communications services. In many of these configurations, any given element may be both a service user and a service provider. For instance, the ESA lander is just a service user, but the ESA relay is both a service user (of the DSN ground tracking stations) and a service provider (to the ESA lander).

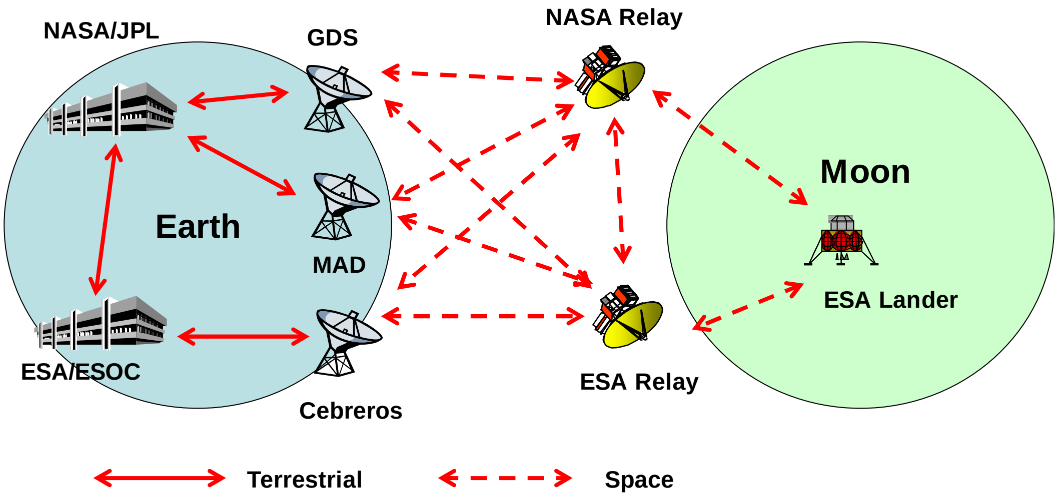


Figure 2-3: Possible SSI Space Mission Cross Support Example

Much more complicated configurations may be conceived, but they all share the same basic functions and sets of pair-wise configurations and interactions.

2.5 BASIC CROSS SUPPORT CONCEPTS

2.5.1 GENERAL

This SCCS-ADD describes how to create a multi-agency SCCS communications architecture by:

a) describing the evolving set of standard services that the infrastructure provides to mission users, i.e., flight programs and projects;

b) describing the physical configuration and evolution of a space communications and navigation infrastructure supported by multiple agencies;

c) identifying standards and interfaces that will be used by the SSI elements to interoperate in the provision of services to the users;

d) identifying standards that will be used by missions to interface with these services, both in space and on the ground;

e) describing transitional strategies to evolve from current deployments to the future SSI state.

2.5.2 DEFINITION OF CROSS SUPPORT

Cross support is a function in which one space agency provides resources to support the operations of a space mission of another space agency. In the context of this document, this includes a ground tracking station (acting as a service provider) being used to communicate with a Space User Node (acting as a service user) by a MOC (the Earth User Node acting as a service user).

A cross support service provider is an organizational entity that can enter into contractual SLAs with a service user to provide service. In general, these services are at the link level, meaning they are specified in terms of carrying data at the Link Layer, from a ground-user asset to a space-user asset, with various throughput, latency, and availability characteristics.

In SSI configurations, cross support also may include a space service element (acting as a service provider) being used to communicate with a Space User Node (acting as a service user). Both of these are instances of cross support. At a minimum, cross support must happen at the Link Layer, but it may also happen at higher layers in the protocol stack.

2.6 RELATIONSHIP BETWEEN SCCS AND OTHER CROSS SUPPORT SERVICE DOCUMENTS

The terminology in the SCCS is derived in part from other cross support service documents, such as the Cross Support Reference Model (CSRM) (reference [1]) and the Service Management Blue Book (reference [14]). Because the SSI configuration introduces some new user/provider relationships, and also places cross support elements in space, some new terminology has been required.

This SCCS-ADD has introduced the terms *cross support service element*, *user element*, and *cross support service system* instead of the more limited complex and mission data operation system terms used in the CSRM. These CSRM terms are still relevant for ABA cross support configurations, but do not scale for the SSI.

The CSRM concept of *complex management* has been replaced here by *provision management*, which is defined as a set of functions of a CSSS, related to the acquisition and management of services provided by that CSSS to other CSSSes. PM interacts with the UMs of user CSSSes to negotiate the provision of services to their respective CSSSes.

The concept of *service management* has been extended to mean the set of functions exposed by PM to UM for the purposes of acquiring and managing the services provided by the provider CSSS to the user CSSS. Similarly, the concept of *utilization management* has been extended to mean a set of functions of a CSSS or user system, related to the acquisition and management of services provided to that CSSS or user system by other CSSSes.

The term *element management* has been introduced to describe functions that manage element resource availability, configuration and execution of element resources, and reporting status of those resources. Elements that perform all or part of the services provided to user CSSSes have EM, and UEs also have EM.

This SCCS-ADD also introduces the concept of nodes and different node types to describe specialized CSSEs, UEs, and their functional configurations and protocol bindings. The CCSDS CSTS (reference [8]) and next-generation service management book (reference [16]) introduce the term *functional resource*, which is defined as the functions or capabilities that are provided by physical resources (e.g., transmitters and receivers) of a CSSE, but not those physical resources themselves. A functional resource is a logical construct not necessarily linked to any single system component. Service management manages the functional resources that compose a CSSE. EM manages the elements inside a CSSE or UE that provide services or support user communications functions.

2.7 CROSS SUPPORT SERVICE SYSTEM ELEMENTS

2.7.1 OVERVIEW

In this architecture, a CSSE is defined to be a physical element that is involved in providing one or more space communications cross support services, possibly together with some other CSSEs. The nodes that are CSSEs play the service provider role and are implemented by different service provider systems. CSSEs functioning together can provide communications and/or navigation services for any space mission element of any space agency provided that the UE conforms to the technical interface specifications and management policies specified for the CSSE.

These service-providing elements are also referred to as ‘building blocks’ because they can be assembled in various ways to provide deployed CSSS services.

A UE is defined to be a physical element that is involved in using one or more space communications cross support services provided by one or more CSSEs. The nodes that are UEs play the service user role and are implemented by different service user systems. A UE may be adapted to also provide services; when this is done they are then functioning as a CSSE.

A CSSS is defined to be a set of CSSEs or UEs that are managed by a single authority with a single set of management policies. These may be provider or user systems.

2.7.2 CROSS SUPPORT SERVICE ELEMENT

2.7.2.1 General

A CSSE may be a landed element on the surface of a heavenly body (e.g., the Earth, the Moon, Mars, Jupiter), an element orbiting around a heavenly body (e.g., a relaying satellite), or an element in cruise through space (e.g., data management systems onboard spacecraft). Table 2-1 shows the types and nominal locations of the different CSSEs described in this document.

Table 2-1: Cross Support Service Elements and Nominal Locations

CSSE Type	Earth	Space/ Orbit	Space/ Planet
Earth Space Link Terminal (ESLT)	X		
Earth Routing Node	X		
Space Routing Node		X	
Planet-Space Link Terminal (PSLT)			X
Earth/Planet Wide Area Network (WAN) Routing Node	X		X

A CSSE may include a single ground station, multiple ground stations, or a large complex consisting of many subsystems. The internal implementation of a CSSE is not visible to its users. What is visible to the users are:

– services (functions) provided for users;

– methods for using and managing the services;

– means for locating and binding to the services;

– physical location or trajectory of the CSSE.

NOTE – For purposes of this document, the Earth is treated separately from the other planets, and the term ‘planet’ is extended to mean any other Solar System body (moon, asteroid, comet) that has missions and associated communications assets.

2.7.2.2 Cross Support Service Element Nodes and Functions

Figure 2-4 abstractly shows how each of the service elements (CSSEs) in any of these deployed systems has an identified set of interfaces and some well-documented behaviors. Each service element has one or more service interfaces (shown here as a solid line) where the services provided by the element are accessible. The visible behavior of a service element is defined at the interfaces. While the internal functions that produce this behavior may be identified, the means used to implement these functions is opaque to the users. The types of services and their operational concepts are described in more detail in section 4. There is a process for locating and connecting to these service interfaces that may involve use of a catalog, a human-mediated process, or some active and automated process of discovery, or the location and access to these service interfaces may be hardwired into the application that uses them.

Each service element also has some sort of service management interface (shown as a red line here) through which the behavior of the service may be securely configured, monitored, and controlled. This interface may be accessible externally to the users, it may be accessible only from within the system, or the necessary control data values may be programmed directly into the service element, accessible only by changing the program and recompiling it. While this last option is a fairly static way of configuring the service elements, it may be suitable in some situations.

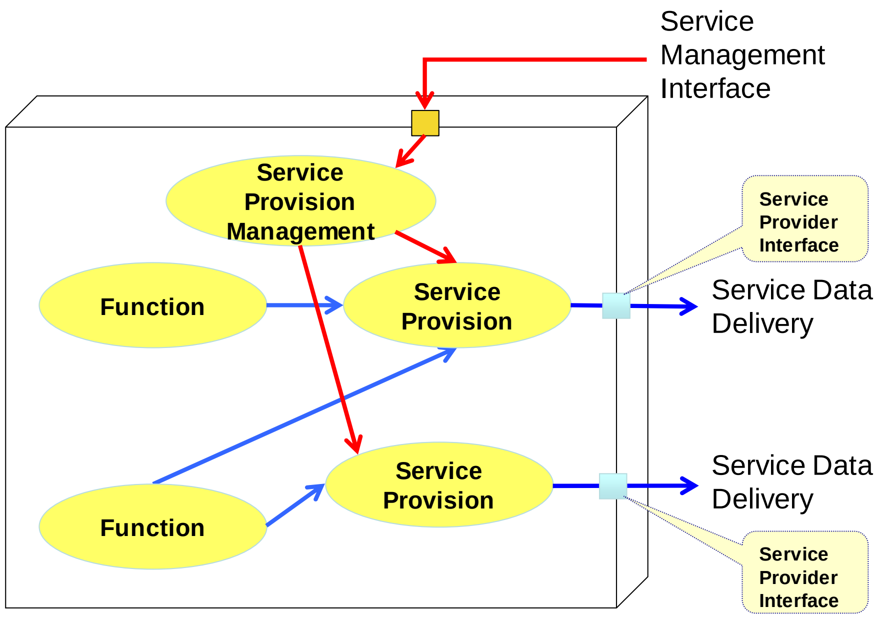


Figure 2-4: Generic CSSE and Interfaces

For ESLTs, the service management interface connects to the entity that does PM; it plans, schedules, and manages the control and service production equipment.

Each of the service and management interfaces has a defined interface binding, which is the technical means by which a user of the service locates, accesses, configures, and utilizes the service itself. This binding includes not just the address of the platform that hosts the service element and the address of the port for the service, it also includes a description of the stack of protocols that the service expects to respond to. The details of interface binding are discussed in more detail in section 4.

2.7.3 USER ELEMENT

2.7.3.1 General

A UE may be a MOC, a landed element on the surface of a heavenly body (e.g., the Earth, the Moon, Mars, Jupiter), an element orbiting around a heavenly body (e.g., a science satellite), or an element in cruise through space. Table 2-2 shows the types and nominal locations of the different UEs described in this document.

Table 2-2: User Elements and Nominal Locations

UE Type	Earth	Space/ Orbit	Space/ Planet
Earth User Node	X		
Space User Node		Varies	Varies
Planet User Node			X
Earth Routing Node	X		

NOTE – The Earth routing node is included in the UE table because acts like a user of the ESLT Link Layer services and operates as a UE for purposes of controlling the space routing node.

A UE may include a single computer or a large complex consisting of many subsystems. The internal implementation of a UE is not visible to provider systems. What is visible to the provider systems are:

- services required by the UE;
- descriptions of the UE and its interfaces, configurations, and operating constraints;
- requests for locating and binding to the services;
- service requests made by users;
- physical location or trajectory of the UE.

2.7.3.2 User Element Nodes and Functions

The UE has a parallel construction to the CSSE, except that it has service user interfaces, service client functions, and a UM function that interacts with the service management of the CSSE.

Figure 2-5 abstractly shows how each of the UEs in any of these deployed systems has an identified set of interfaces and some well-documented behaviors. Each UE has one or more service-client interfaces (shown here as a solid line), where the services provided by the CSSEs are accessed. The visible behavior of a UE is defined at the interfaces. The UE uses a process for locating and connecting to the CSSE service interfaces that may involve use of a catalog, a human-mediated process, or some active and automated process of discovery. Alternatively, the location and access to these service interfaces may be hardwired into the UE.

Each UE has a UM function that accesses the service management interface of the provider system. Through this interface the behavior of the service may be configured, monitored, and controlled.

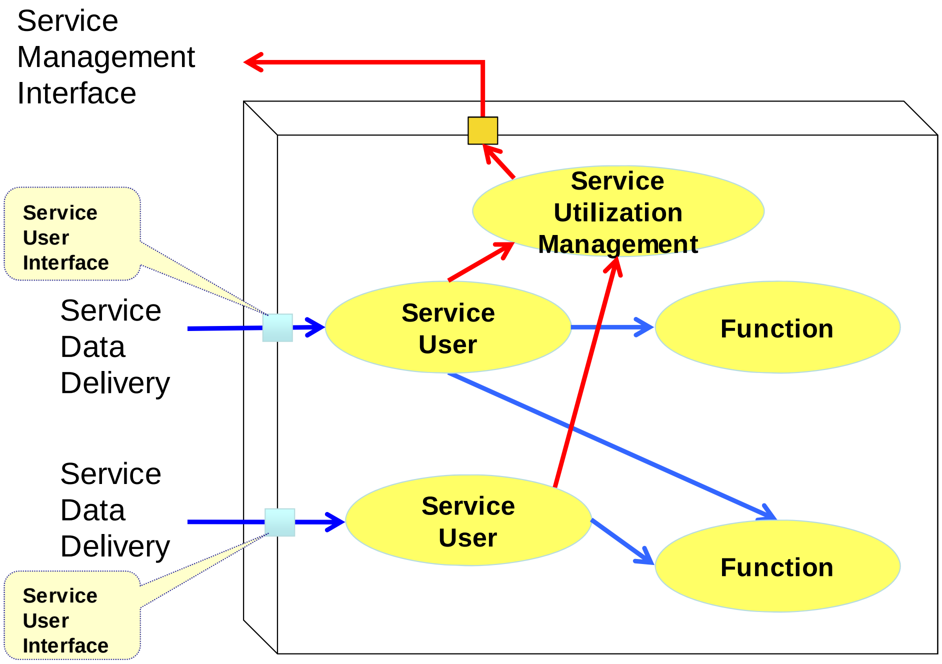


Figure 2-5: Generic UE and Interfaces

2.7.4 CROSS SUPPORT SERVICE SYSTEMS

A CSSS is defined to be a set of CSSEs that are managed by a single authority with a single set of management policies. A CSSS may be a service provider, a service user, or both. Table 2-3 shows some examples of service provider CSSSes and CSSEs contained in them.

Table 2-3: Examples of Provider Cross Support Service Systems and Related Elements

CSSS	CSSEs
Deep Space Network	Deep Space Stations, Network Control Center
Near-Earth Network	Tracking Stations, Network Control Center
Space Network	Data Relay Satellites, Ground Terminals
Lunar Network	Lunar Relay Satellites
Mars Network	Mars Relay Satellites

Users of the service provider CSSSes are service user CSSSes, typically described as a MOC, spacecraft, lander, rover, or other mission element in space. These elements use space communications cross support services to accomplish their mission objectives. Table 2-4 describes some examples of service user CSSSes and the UEs contained in them.

Table 2-4: Examples of User Cross Support Service Systems and Related User Elements

CSSS	UEs
Mission Ground System	MOC, MCC, Instrument CC, Science Center
Spacecraft	Orbiter, Lander, Rover, Hybrid Science/Routing Orbiter

2.8 BASIC SYSTEM-ELEMENT CONFIGURATIONS

2.8.1 ABA SERVICE ELEMENTS

2.8.1.1 Simple ABA Configuration

For the usual space communications cross support service, there is a service UE in space and another service UE on the ground. The ESLT in figure 2-6 is a specialized instance of the generic CSSE shown in figure 2-4. Figure 2-6 shows the basic ABA configuration, with a CSSE of one agency (B) (the ABA ESLT) providing services to the Earth and Space User Nodes of another agency (A). The interface of the CSSE with the service user is called the *service provider interface*. In this case, there is a terrestrial service provider interface to the Earth User Node and a space link service provider interface to the Space User Node.

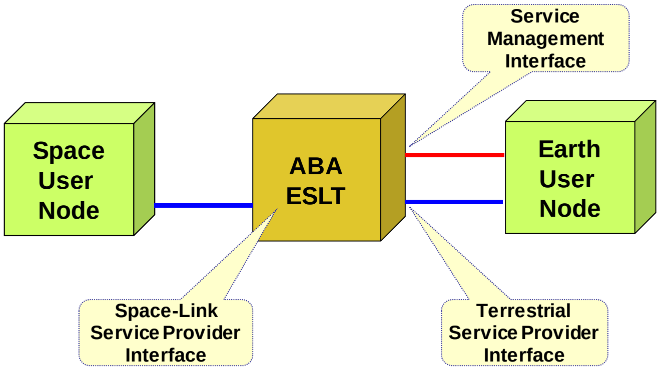


Figure 2-6: Basic ABA Configuration

The Earth and Space User Nodes shown in figure 2-6 are instances of the UE similar to that shown in figure 2-5. Within the Earth User Node, there will be a *UM element*, which manages, controls, and/or monitors the service provided by a CSSE. The UM element may be within the Earth User Node, but it can be separate, and it may be connected either directly to the interface on the CSSE that permits service management, or to another CSSE that supports the service remotely. The interface of the CSSE with the UM element is called the *service management interface*. (See definitions in 2.7.2.2.)

In an ABA configuration, a user's primary interfaces to the service provider are the Link Layer services request and service delivery interfaces either on the ground or in space. The service user produces encoded space link frames for delivery and receives decoded space link frames. The activities within the service provider and the details of the service production are opaque to the service user, but a certain amount of monitor data and reporting is provided to allow the service user to determine the state of communications.

Figure 2-7 shows a simple overview of the two operational domains, the service user organization that does utilization management and the service provider organization that does provision management. There is also a third connection shown, labeled 'Element Management'. In this example, EM is typically done by the Earth User Node by securely sending commands to the Space User Node, i.e., the user MOC on the ground commands and controls the activities onboard the spacecraft. In the general case, all of the elements of each CSSS are managed, usually by some local management and control element. Elsewhere in this document EM will be referenced in the specific context of CSSE management as defined in 2.7.2.2.

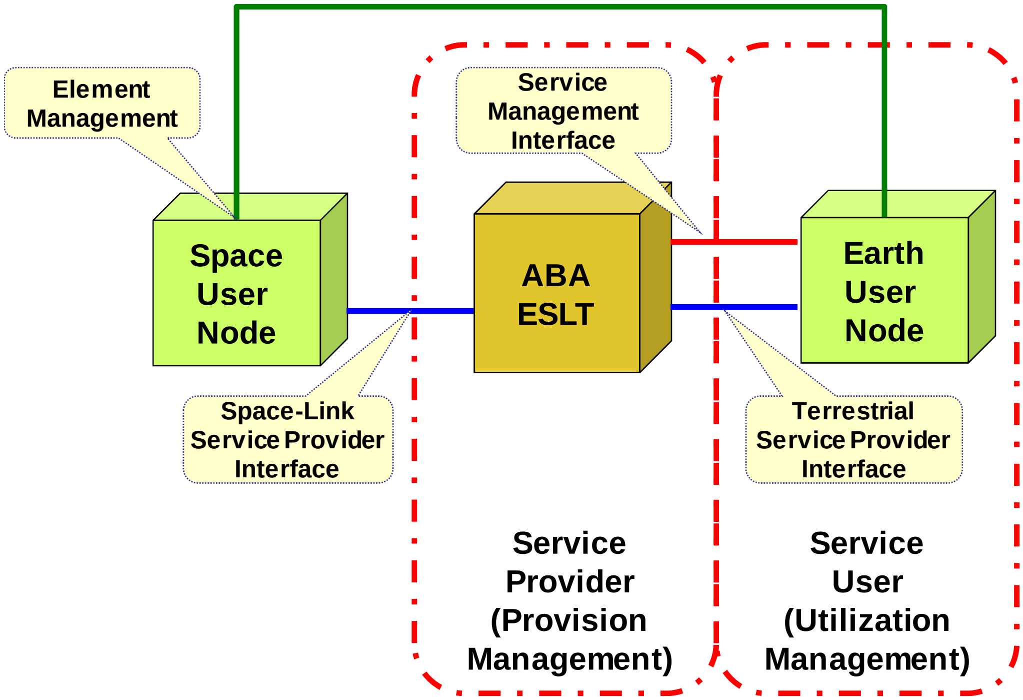


Figure 2-7: ABA Configuration Showing Management Interactions

2.8.1.2 ABA Enterprise Overview

The space communications cross support ABA architecture is composed of a set of interconnected elements that, working together, provide end-to-end communications services for mission users (user nodes). These elements are as follows:

a) The basic service element building block that supports ABA configurations is:

   – ESLTs (e.g., ground stations);

b) and ESLTs support:

   – user nodes (in space and on Earth, including other planet surfaces).

Figure 2-8 shows an ABA enterprise overview, where the space communications cross support building blocks for a generic ABA configuration are shown an abstract set of facilities, distributed across the Earth and some remote planetary body, with no implied agency ownership. Organizational boundaries for the typical service user UM and service provider provision management elements are shown enclosed in dashed red lines. These space communications cross support elements might all be owned by one agency, but more typically they will be owned by different agencies and will provide cross support services to each other. The user nodes must implement an agreed-upon minimum set of standard Link Layer and cross support protocols, and the space communications cross support building-block elements must provide the agreed-upon set of standard Link Layer cross support services. There are procedures for establishing service agreements, for requesting services, for delivering data, and for reporting on the state of service delivery.

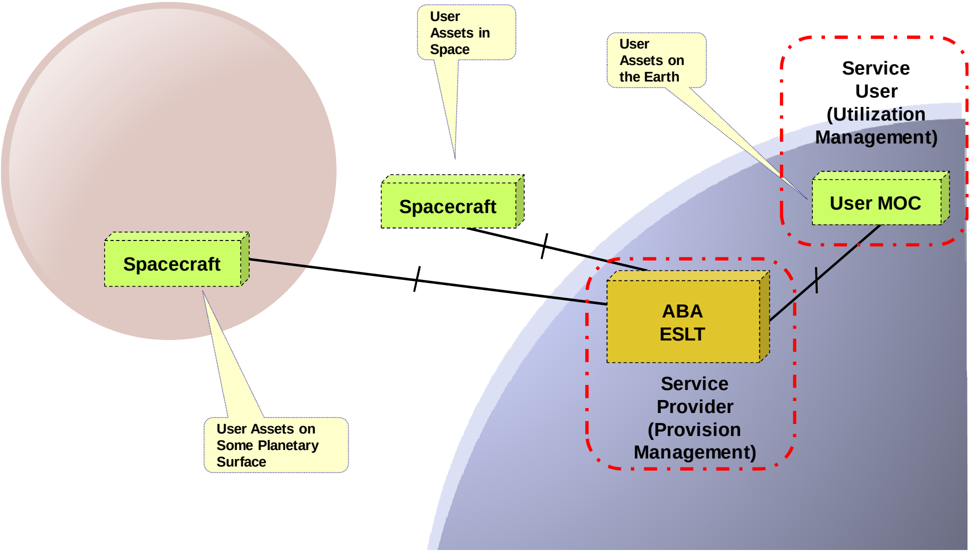


Figure 2-8: ABA Enterprise Overview

2.8.2 SSI SERVICE ELEMENTS

2.8.2.1 Core SSI Configuration

In the SSI, there are cases in which a Space User Node and an Earth User Node are supported by two or more CSSEs. Figure 2-9 shows such an example, in which a Space User Node (a spacecraft) and an Earth User Node (e.g., a spacecraft mission control center) are supported by a space routing node (a relay satellite), the ESLT (a communications ground station), and a terrestrial WAN connection. The WAN is really an infrastructure element, and aside from providing Internet Protocol (IP) or Bundle Protocol (BP) network connectivity, it has no special role in the SSI. The MOC for the space routing node also participates, since it is responsible for managing and configuring the space routing node and for managing the space link to the node that is provided by the CSSE, but it is not necessarily on the direct data path from Earth User Node to Space User Node.

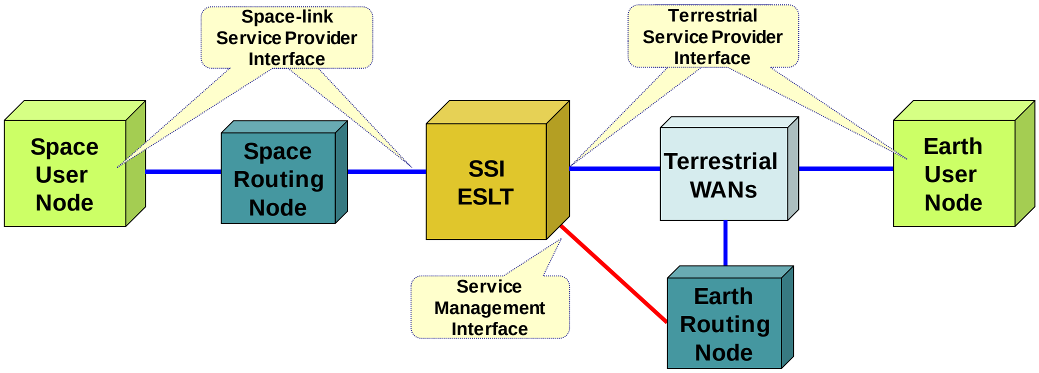


Figure 2-9: SSI Core Configuration

In this document these SSI configurations are also referred to as *ABCBA* style configurations. The notion is that the Earth User Node and the Space User Node both belong to the same agency (A), the space routing node and its MOC may belong to a different agency (B), and the ESLT may belong to yet a different agency (C). So Earth User Node *A*, gets support from the space routing node MOC *B*, connects to ESLT *C*, and then to space routing node *B*, which connects to Space User Node *A*, hence *ABCBA*. Of course, configurations are possible where all of the ABCBA elements may be owned by one agency. The terrestrial WAN may belong to either agency or be a public Internet. In practice the data may not flow directly through the space routing node MOC, but this element is certainly involved in managing the transfer and in controlling the space routing node. Much more complex SSI deployment configurations are possible, but this core SSI ABCBA configuration serves to introduce most of the necessary concepts for any SSI deployment.

2.8.2.2 SSI Enterprise Overview

The space communications cross support SSI architecture is composed of a set of interconnected elements that, working together, provide secure end-to-end communications services for mission users (user nodes):

a) The set of basic service-element building blocks that support the SSI configurations are:

   - ESLTs (e.g., ground stations);
   - Earth routing nodes;
   - space routing nodes;
   - PSLTs;
   - terrestrial WANs;
   - planetary WANs.

b) The UEs are:

   - user nodes (in space and on Earth, including other planet surfaces).

Figure 2-10 shows the SSI enterprise overview, where space communications cross support building blocks for SSI configurations are shown as an abstract set of facilities, distributed across the Earth and some remote planetary body, with no implied ownership. Boundaries for the typical service user (UM) and service provider (PM) elements are shown enclosed in dashed red lines, and include Earth and space elements. User nodes are treated separately from SSI building blocks, because they have different configurations and do not offer services to other nodes, as SSI building blocks must. All of these SSI elements might be owned by one agency, but more typically they will be owned by different agencies and will provide cross support services to each other.

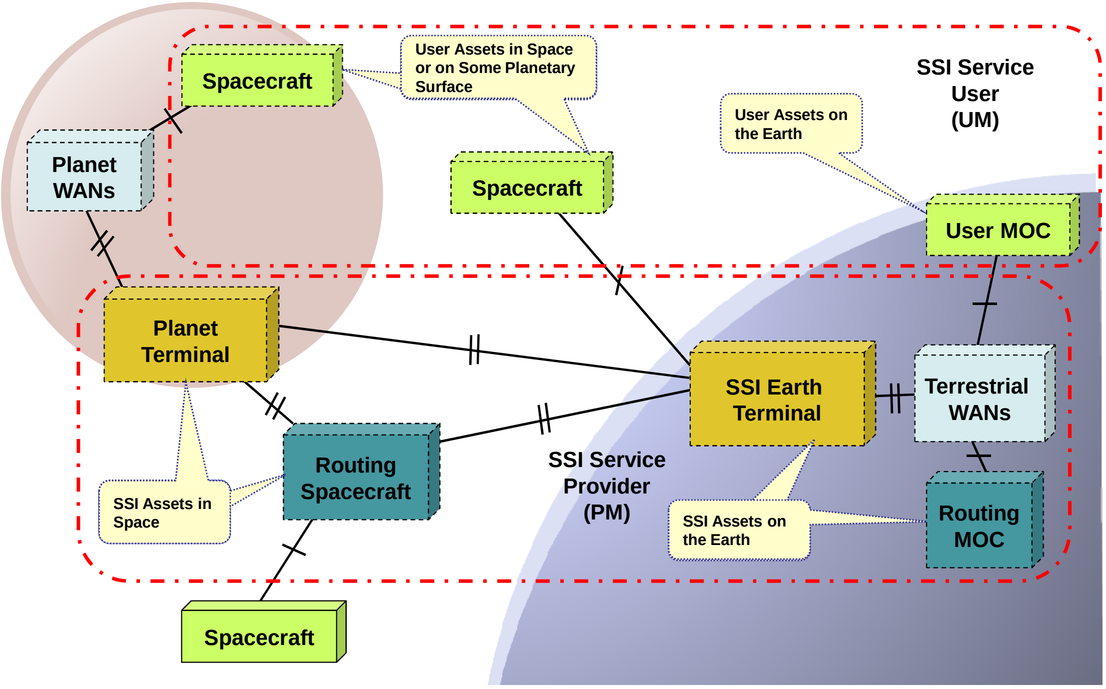


Figure 2-10: SSI Enterprise Overview

Any of the user nodes, or other SSI elements, may communicate with any other, and these communications are expected to use the services of one or more of the SSI building blocks. Just as in the terrestrial Internet, the user nodes must implement an agreed-upon minimum set of standard protocols, and the SSI building-block elements must provide the agreed-upon set of standard services. There are procedures for creating service agreements, and as with the Internet, there are procedures for hooking up a new user node to the SSI, for requesting services, and for inserting a new SSI building-block element into the network.

With each agency having very different mission sets and science or organizational goals, one of the biggest challenges for the SSI is how to coordinate and ensure interoperability of separately funded developments within each agency in order to initiate and evolve the SSI.

2.9 NETWORK TERMINOLOGY

2.9.1 DEFINITION OF A NETWORK

A network consists of one or more computers or other processing elements (such as a spacecraft, data storage device, or other service-providing element) that are owned by a single organization, communicating using a single Layer 3 (Network Layer) protocol (see reference [5]) such as BP or IP. These elements may communicate directly or may be connected via one or more routers that implement the Network Layer protocol and other support protocols for routing and management of the network. The underlying links from each element to another, or to the router, may differ, but the Network Layer protocol is common across the network.

2.9.2 DEFINITION OF AN INTERNETWORK

Internetworking involves connecting two or more distinct computer networks, usually in separate management domains, together to form an internetwork (often shortened to *internet*), using routing devices that operate at Layer 3. These routing devices allow traffic to flow back and forth between the networks in a manner that is independent of how each network is implemented, and they guide traffic to its destination, routing data along a suitable path (among several different paths usually available) across the complete Internetwork. An Internetwork is therefore constructed as *a network of networks*. Internetworks may also use protocols at the boundaries of each network to manage flow from one management domain to another.

2.9.3 DEFINITION OF THE SOLAR SYSTEM INTERNETWORK

The SSI (figure 2-11) consists of a loose confederation of independent space communications networks, each often owned and administered by a different space agency. End users of the SSI are given access to internetworked data communications services by the *Solar System Internet Service Provider (SSI-SP)* with which they have established an SLA. ‘Loose confederation’ means there is no pre-agreed, planned development timeline for the full set of interoperable multi-agency assets that comprise the SSI; rather, the timeline is developed as assets are deployed by different agencies. The loose confederation is still carefully coordinated and managed.

The participation of all assets in the SSI, from initiation until end of life, is carefully planned and managed; there is little that is 'loose' about it except for the lack of a complete, pre-agreed schedule for development and deployment. 'Confederation' means that all agencies that choose to participate, each of which is free to act independently, voluntarily come together to collectively form what is effectively a single infrastructure. They do this by adhering to the operating guidelines, standards, protocols, and service interfaces agreed to by the confederation. Each of these independent participating networks is an SSI-SP which may consist of ground (and planet) communications assets, dedicated routing assets, and/or hybrid science/routing assets. The SSI as a whole provides services to user missions.

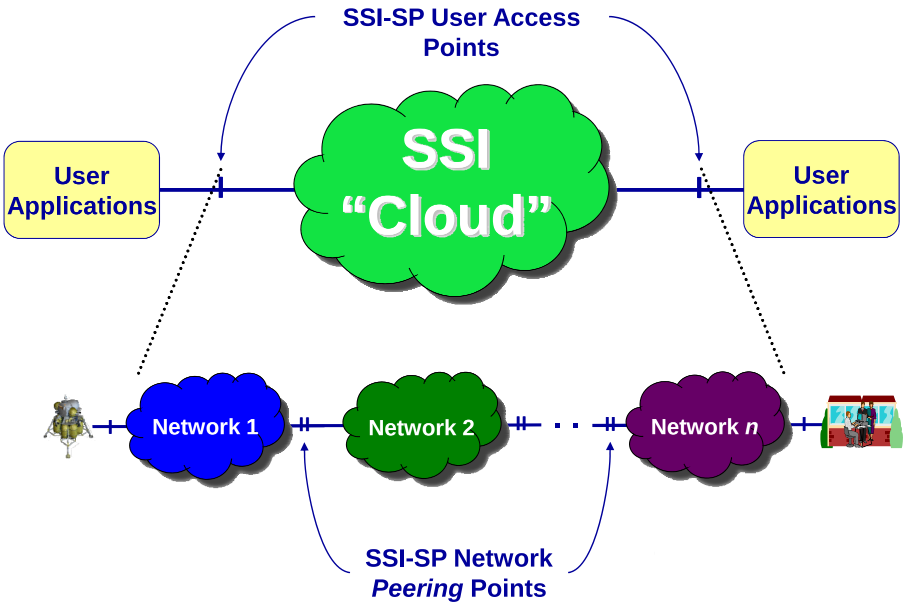


Figure 2-11: The SSI

NOTES

1 Applications are identified using Network Layer addresses.

2 All application communications go through the Network Layer.

3 To applications, there is no difference between a 1-hop, a 2-hop, or a 5-hop network path.

2.9.4 DEFINITION OF AN SSI INTERNET SERVICE PROVIDER

An SSI-SP is an organizational entity that can enter into contractual SLAs with a user to provide SSI services. In general, these are services at the actual user level, meaning they are specified in terms of carrying data end-to-end with various throughput, latency, and availability Quality of Service (QoS) characteristics. A single SSI-SP can only guarantee QoS if it is the only service provider. Where more than one SSI-SP is involved, the SSI architecture (reference [9]) envisions an SSI Coordinating Function that extends existing inter-agency coordination mechanisms to perform SSI network planning and management functions that require coordination across multiple SSI-SPs, reconciling user schedule requests with provider contact plans. The result of SSI network provider coordination is a Composite Contact Plan (CCP) that establishes the temporal windows and communications capabilities (e.g., bandwidth) of all individual node-to-node links in the SSI.

Participating networks reciprocally provide access to each other's users via a process known as *peering*. To be eligible to participate in confederated SSI operations, each participating network must offer peering services at the Network Layer, which includes carrying each other's user traffic and also exchanging routing, accessibility, and other network management information. Peering Agreements (PAs) are negotiated between SSI-SPs to enable them to support users across their boundaries. PAs typically include definitions of interfaces between provider organizations in the different authorities.

NOTE – While an SLA is an agreement between a user organization and a provider organization, a PA is an agreement between the controlling authorities of two provider organizations.

To qualify to be a component of the SSI, each agency's participating network must offer a native Network Layer routing service based on:

- the IP of the Internet Protocol Suite (IPS);
- the BP of the Delay-Tolerant Networking (DTN) suite;
- both of the above protocols and the required gateway functions.

If an agency's space communications infrastructure does NOT offer at least one of these native Network Layer-routing services, that agency may not be a participant in the SSI unless it is embedded in the infrastructure of another agency that does. While an SSI-compliant infrastructure must offer at least one of the routing services, internal to each component network, heterogeneous Physical Layer and Link Layer protocols may operate. For the SSI to operate, it does not just need routing protocols, it requires routers, network management, underlying Link Layer protocols, and Physical Layer compatibility as well. Reference [9] also describes other SSI provider coordination methods, including the exchange of Provider Contact Plans (PCP) and Authority Schedule Requests (ASR) that are processed to create the CCP.

2.9.5 DEFINITION OF THE SSI APPLICATION TYPES

One of the advantages of a networking protocol is that it frees applications from having to understand in detail the underlying physical network topology. Network applications specify with whom they want to communicate using some sort of identifier, such as a BP endpoint identifier or an IP network address, without regard to where the endpoints are located. To an application, it does not matter if the destination is on the same spacecraft, one hop away across a space link, or several hops away separated by a heterogeneous combination of wired and wireless links. To achieve this independence, it is assumed that *all communications* use the Network Layer, regardless of the number of links in the path. This means that from an application and networking perspective, there is very little difference between a 1-hop path, a 2-hop path, or a 5-hop path.

User applications may be *delay aware* or *delay unaware*. Table 2-5 compares the two types of applications. The effective limit for delay unaware applications is roughly 1–2 seconds RTLT, constrained by the assumptions built into the underlying IPS. Delay is related to distance, but the issue here is whether applications are designed to be aware of delays, or if they assume no delay (delay unaware). Properly designed applications will survive the delays they are designed for (which may be many 10s of hours). Applications designed assuming no delays will be unpleasantly ‘surprised’ when they try to operate in an environment where there are delays of even a few seconds or minutes.

Table 2-5: Comparison of Delay-Aware and Delay-Unaware User Applications

	Delay Aware	Delay Unaware
Immediate replies to requests expected?	No	Yes
Acknowledgement from peer applications or other network services expected?	No	Yes
Delay/disruption tolerant?	Yes	No
Response to delay/disruption	Deterministic or configured and anticipated	May treat a delay as a network failure, attempt to retry a communication, or abandon it as an error
End-to-end routing type used	Generally use BP	May use IP
Best network(s) to use	DTN (or hybrid DTN/IP joined by protocol-translating gateways)	Continuously connected IP
Is approach recommended for space internetworking?	Yes. Operates well regardless of delays and/or disconnections	May be used in configurations where there is continuous connectivity and short RTLT (typically <<2 sec)

2.10 TRANSITIONAL STRATEGIES: ABA TO SSI

The accepted CCSDS standards (i.e., Blue Books) available today mainly address single lower-layer protocols and services and do not tend to address end-to-end services. At the time of writing this SCCS-ADD and its companion SCCS-ARD (reference [4]), several of the interfaces to provide fully interoperable ABA Link Layer services are just now being defined, and not all the existing ones are implemented by the majority of space agencies. Included in this set of services are all of the new CSTS-based services for radiometric data transfer and unframed telemetry, as well as the services for monitor data and service control. Standardized cross support file-transfer services are also in discussion, and all of these are needed to provide fully interoperable ABA configuration services. In the absence of agreed-upon interoperability standards, the existing service providers have defined their own local standards, which, while they work, are not interoperable and place a burden on any user organization that needs to integrate with services offered by different providers.

The service management protocols used to request and configure all of these new services and some existing ones (e.g., radiometric tracking, ranging, and Delta-DOR) are also evolving. At present, the service management specification only supports basic command and telemetry. Beyond service management there are not yet agreed-upon standards for service catalogs or for service agreements and service planning, which are the necessary preconditions for cross support services. Currently, these are all done ‘by management’ or bi-lateral agreements, outside of any agreed-upon standards, and are typically very ‘hands-on.’ In order to transition from the current situation to one where users of ABA services are offered common and consistent service interfaces, both for service PM and service UM, these new service interfaces and protocols must be fully defined and widely implemented.

Once this is accomplished, the needs of ABA missions will be met, but it will not solve the needs of missions that require relay operations. At present, relaying is done by the user missions themselves, and no two missions do it in quite the same way. There are no agreed-to standards for relaying, aside perhaps from Class 3 and 4 CFDP, which have seen little implementation. The general approach to ‘relaying’ that has the greatest potential for long-term success is adopting the SSI approach, but some of the standards required to achieve the SSI are still in development; therefore the set of CCSDS standards needs to grow to provide full coverage of both these additional ABA services and also the SSI architecture. These future standards must support current ABA missions, enable the future SSI, and also provide useful services that support current operations while building future capabilities for the SSI.

Space agencies that offer either ABA or SSI services are expected to document their services in an online, accessible service catalog. The catalog will document the service providing system capabilities, provided services and interfaces, protocols that are supported, and the means for establishing agreements for service. The catalogs are expected to include all the agreed-to standard services, but may also include other, specialized, network-specific services. The service agreement documents the agreement between the service user and the service provider. This agreement covers the period of service, mission characteristics, specific capabilities to be used, and other details required to establish the what, when, and how of services. The agreement and detailed mission configuration information are used to define the specific system and equipment parameters to provide the correct services.

Space missions are normally reluctant to adopt new standards before the standards are fully specified and validated. A few agencies may be able/willing to start implementing new standards while all of the formal specifications are still in progress, but others will prefer to see the complete final suite before they initiate implementation. In addition, even when all of the new ABA and SSI architecture and standards are fully defined, it cannot be expected that all agencies will be able to implement the migration at once because of the long development times for space projects and ground infrastructure enhancements. Therefore, at some point in time, an unbalanced situation with respect to assets in space and on the ground will exist. To be able to perform space communication cross support in such a landscape, where older systems will coexist with newer ones, a transitional strategy must be defined to bridge from the current ABA configurations, to intermediate states, to the final SSI architecture.

The transitional strategy assumed in this SCCS-ADD addresses the following considerations:

- definition of extended services at the link level to meet current and future needs;
- backward compatibility with legacy missions;
- migration to operations based on files as basic end-to-end data exchange structures;
- provision of data-forwarding capabilities, offering end-to-end services by implementing hop-by-hop relaying;
- addition of new capabilities for hardware/emergency commanding and return of Link Layer data;
- implementation of a ‘learning’ phase towards fully automated internetworking;
- adaptation to operations based on delay awareness/unawareness;
- provision of cross support capabilities from an ABA infrastructure to more advanced agencies already migrated to SSI;
- testing and validation of the internetworking concept before adopting it in its final configuration.

Following this strategy, participating agencies will be able to implement their ABA services in ways that support current missions and also open a path to the future. They will be able to join the transitional phase without directly offering either of the native Network Layer routing services shown in figure 2-11. They will be able to implement these ‘transitional’ Link Layer services based on CCSDS Physical Layer and Link Layer protocols, interoperable cross support protocols, and using specific agreements for ground network management and service access.

Because there are not yet well-established standards for such cross support interactions, there may be many possible interim configurations, and they may differ in many details; many ad-hoc interim approaches have already been implemented. This SCCS-ADD describes how to approach the general problem, and its companion SCCS-ARD (reference [4]) provides some specific recommendations for services, protocol stacks, and end-to-end deployments, but there is no attempt to be complete nor to cover all possible system and deployment configurations.

2.11 SCCS ARCHITECTURE: ASSUMPTIONS, GOALS, AND CHALLENGES

2.11.1 GENERAL

The goal of the SCCS architecture is to unambiguously define the technical and organizational structures needed to create and securely operate both ABA and SSI configurations. The ABA configurations are the means for providing cross support for missions operating on a single-hop space link. An ABA cross support service provider gives a single mission access to Link Layer communications services.

The SSI configurations are the means for supporting multiple spacecraft at the same time, using a loose, but carefully coordinated and managed, confederation of independent space communications networks, each often owned and administered by a different space agency. An SSI-SP gives end users of the SSI access to secure, internetworked data communications services.

If both service delivery and interoperability interfaces are to be achieved, each must be defined for both the users and service providers.

Protocols must be used that will allow elements built by different organizations, at different times, to interoperate. The ABA cross support architecture must be implemented in a way that provides Link Layer services for single missions. In order to support a transition to an SSI architecture, when this is needed, the architecture must be implemented so as to be capable of supporting ABA missions and also of providing secure internetworking services to SSI missions. Ground cross support elements may provide these services when they are first deployed, or they may add them later and be capable of evolving over time as new elements are added and old ones are retired. This SCCS architecture must be prescriptive enough to be unambiguously interpreted and implemented. It must simultaneously be 1) extensible to permit new applications and upper-layer protocols to be grafted on, and 2) flexible at the underlying physical communications layers so that evolution at this layer does not disturb the operation of the space communications cross support configuration as a whole.

2.11.2 ASSUMPTIONS

2.11.2.1 ABA Configuration Assumptions

The major architectural assumptions underlying the space communications cross support for ABA configurations are as follows:

a) the ABA elements will typically be owned and administered by different space agencies;

b) the ABA services are to provide space link services to end-user missions;

c) elements providing ABA services will be deployed on Earth, and in space or on remote planetary surfaces;

d) the ABA services must be capable of providing a stable platform for secure single-hop operations, but they may also permit deployment of upper-level protocols;

e) the ABA may use dedicated Link Layer services elements, but it should also permit use of service elements that support ad-hoc relay and internetworking services;

f) the ABA elements may have operational, resource, and/or visibility constraints due to other requirements and will typically not be available on a 24-hour basis;

g) the ABA services must provide emergency commanding services in order to handle off-nominal spacecraft situations.

2.11.2.2 SSI Configuration Assumptions

The major architectural assumptions underlying the space communications cross support for SSI configurations are as follows:

a) SSI is a loose confederation of independent space communications networks;

b) the SSI elements typically will be owned and administered by different space agencies;

c) the SSI is to provide secure space internetworking services to end-user missions;

d) elements of the SSI will be deployed on Earth, on remote planetary surfaces, and in space;

e) the SSI must be capable of providing a stable platform for secure networked operations and also permit evolution of upper-level services and lower-level physical protocols;

f) the SSI may contain dedicated service elements, but it must also permit use of hybrid service elements that support science, exploration, or other operational goals in addition to SSI communications services;

g) SSI elements may have operational, resource, and/or visibility constraints due to other requirements and will typically not be available on a 24-hour basis;

h) the SSI must provide secure emergency commanding and telemetry services in order to handle off-nominal spacecraft situations.

2.11.3 GOALS

2.11.3.1 Architecture Change Goals

The architecture change goals are as follows:

a) create an evolving international communications infrastructure that supports the science observation and exploration goals of the collective set of space agencies;

b) evolve the existing ABA cross support services to provide a more complete range of single-hop functionality and interoperable interfaces;

c) define new services such that they completely support ABA configurations and also provide a transitional path to SSI services;

d) evolve the current operational approaches to one that provides SSI services in any operational domain where such services will be of benefit;

e) create an infrastructure that permits any connected mission element to communicate in a timely and secure way with any other permitted mission element.

2.11.3.2 Architecture Description Document Goals

This ADD Green Book goals are as follows:

a) describe the ABA technical architecture, i.e., the services, protocols, and interfaces, such that new space communications cross support ABA services can be understood;

b) describe the SSI technical architecture, i.e., the services, protocols, and interfaces such that an SSI can be understood;

c) describe the technical architecture such that a smooth transition path from the ABA to the SSI configurations is presented and that both modes are supported in the future;

d) describe how to evolve to the SSI from the ABA via transitional strategies.

2.11.4 CHALLENGES

The major challenges to achieving ABA and SSI end-to-end interoperability are as follows:

a) the space communications cross support elements typically will be owned and administered by different space agencies;

b) the individual space mission development projects are driven by agency science and mission goals, as is appropriate, and cross support is often a secondary (or tertiary) consideration;

c) missions often adopt standard Link Layer protocols, but may utilize local adaptations or specializations that do not, in general, interoperate;

d) missions often develop their own specialized, non-interoperable, protocols above the Link Layer;

e) implementation of the full protocol suite for space internetworking may be costly for early adopters; space internetworking must offer significant mission data return and cost advantages to be seen as a benefit.

3 CROSS SUPPORT OVERVIEW OF ABA AND SSI TECHNICAL ARCHITECTURE

3.1 CROSS SUPPORT BUILDING BLOCKS

3.1.1 OVERVIEW OF BUILDING-BLOCK FUNCTIONS

Each of the space communications cross support building blocks (CSSEs) has an associated set of basic functions that distinguishes the blocks one from another. Any of these building blocks may also incorporate other functionality, but the basic functions must be included to enable interoperability. The sets of functions identified here are suitable for both ABA and SSI configurations, but some of the functions are only required to provide SSI services. The basic sets of functions for each space communications cross support building block are as follows:

a) ESLTs (e.g., ABA and SSI ground stations):
   - route connections between terrestrial elements and space (SSI);
   - provide interface to Radio Frequency (RF) space link;
   - provide services to one (or possibly more) Earth User Nodes;
   - provide full services for Link Layer processing and frame merging (SSI);
   - provide secure access control mechanisms;
   - provide full services for Network Layer processing and routing (SSI);
   - may support last-hop emergency and non-SSI delivery services;
   - have a service management interface for processing requests, and for configuration and reporting;

b) space routing nodes (SSI):
   - provide routing among space elements;
   - provide interfaces to two or more RF space links;
   - provide full services for Link Layer and Network Layer processing and routing;
   - provide security services across their links;
   - must support last-hop emergency and non-SSI delivery services;
   - have an EM interface for configuration and reporting;

c) Earth routing nodes (SSI):
   - operate one or more space routing nodes;

- may provide routing from Earth User Nodes to their ESLT (but this is not required);
- may provide interfaces to one or more Earth User Nodes;
- provide full services for Link Layer and Network Layer processing and routing;
- must support secure essential commanding and telemetry for the space routing nodes that they operate;
- have an EM interface for configuration and reporting;

d) PSLTs (SSI):

- route connections between planet surface elements and space;
- provide interfaces to RF space link, either in situ or long haul;
- provide interfaces to one or more planet ‘terrestrial’ links;
- provide full services, including security, for Link Layer and Network Layer processing and routing;
- may support last-hop emergency and non-SSI delivery services;
- have a service management interface for processing requests, and for configuration and reporting;

e) terrestrial WANs (SSI):

- route connections securely among terrestrial elements (Internet);
- provide interfaces to two or more terrestrial links;
- provide full services for Link Layer and Network Layer processing and routing;
- have an EM interface for configuration and reporting;

f) planetary WANs (SSI):

- route connections securely among terrestrial elements (Internet);
- provide interfaces to two or more planet ‘terrestrial’ links;
- provide full services for Link Layer and Network Layer processing and routing;
- have an EM interface for configuration and reporting.

And these sets of functionalities support user nodes (UEs, in space and on Earth, including other planet surfaces), which in turn:

- are end-user elements, either in space or on some surface;
- provide interfaces to either RF space link or terrestrial link;

- provide basic services for Link Layer processing;
- provide basic services for Network Layer processing (SSI);
- provide basic security services;
- provide at least simple routing to next-hop SSI service point (SSI).

The fully compliant space communications cross support building-block elements are all expected to provide full Network Layer and Link Layer services and to be capable of routing user data from multiple users simultaneously. All of the SSI service elements can also handle requests from non-SSI nodes operating at the Link Layer in ABA style configurations. Using this approach, fully compliant ESLTs can support ABA and SSI configurations at the same time, but an ESLT with only ABA-compliant services cannot directly support SSI missions. The ABA user nodes only need to be able to do the Link Layer services, but they may also implement additional mission-specific protocols above the Link Layer. The SSI user nodes are only expected to be able to do the minimum necessary Network Layer functions in order to hand off their data to the next hop, which will be an SSI service-building block.

3.2 GENERAL DESCRIPTIONS OF PRESENT ARCHITECTURES

3.2.1 ABA ARCHITECTURES

Most of the current space mission operational and cross support configurations are of the ABA style, where a single spacecraft is operated by a spacecraft MOC, using a ground station that belongs either to the spacecraft agency or is provided as a cross support service by another agency. This basic cross support scenario was shown diagrammatically in figure 2-7; contrast it with the SSI topology shown in figure 2-9.

Figure 3-1 shows a simplified end-to-end view of the system elements involved in a typical ABA scenario: the Space User Node, the ESLT, and the Earth User Node, which is where the MOC is located. In this case, two different user end nodes are shown, one in space, and one on the ground. For these ABA configurations, only Link Layer protocols are used, as is shown in figure 3-1.

Because this particular example assumes that the spacecraft is at some distance from the Earth, perhaps at some remote planet, delay-aware applications must be used above the Link Layer and Physical Layer protocols. Only the Link Layer services provided by the ESLT are used. The end-user nodes, in space and on the ground, may use a variety of user applications, including CFDP, to do standard file processing, or a standard file cross support delivery service (reference [17]) may be provided by the ESLT to transfer files using CFDP.

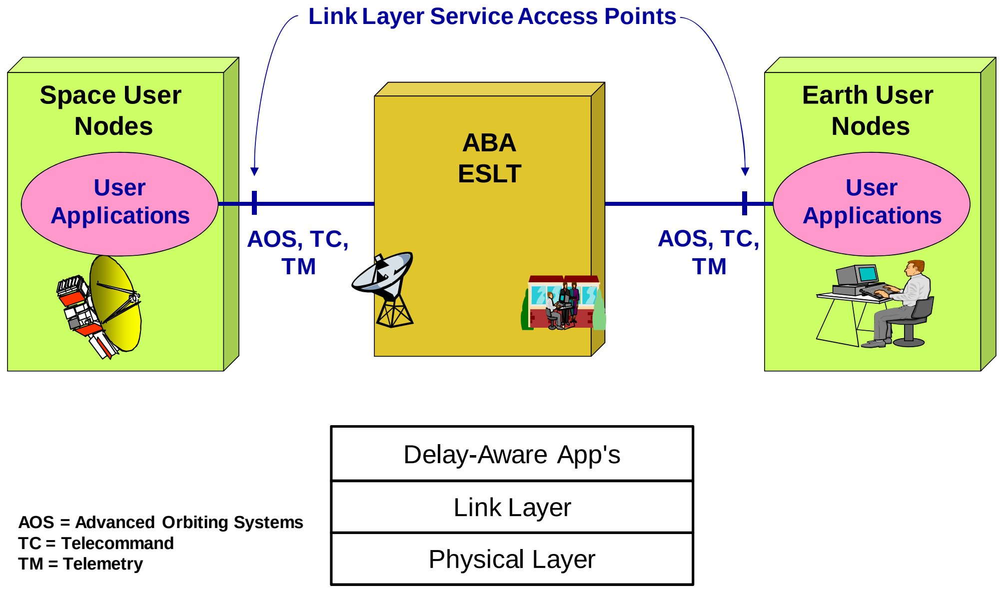


Figure 3-1: Basic ABA End-to-End Configuration and Protocol Stack

Security mechanisms are not explicitly shown in this diagram, but they may be applied at one or more layers:

a) Application Layer security (authentication or encryption) applied to the data by the user application;

b) Link Layer security (authentication or encryption) applied to the data link contents using Space Data Link Security (SDLS).

3.2.2 ABA END-TO-END VIEW

3.2.2.1 General

The end-to-end view shown in figure 3-2 abstractly depicts an ABA configuration as an interconnected set of building blocks that performs Link Layer data transfer service(s). This figure illustrates the specific types of CSSE building-block components and UEs that are used in these configurations and the nominal connectivity among them. ABA building blocks are assembled to provide cross support services to enable an Earth User Node to communicate with its Space User Node. There may be many different types of Space User Nodes and different ESLTs, but the abstract physical topology is essentially the same for all of them.

The ABA ESLT element is depicted as a physical node (a tan 3-D box), and the user nodes—Earth User Node, Space User Node, Circum-Planet Space User Node—are depicted as light green 3-D boxes. Figure 3-2 also illustrates the points at which the ABA service element offers services and the access points at which ABA user nodes connect to the service provider. The UE links are shown with a single hash mark. All of these interfaces require implementations of Link Layer protocols, and the terrestrial link requires implementation of SLE or CSTS cross support and service management protocols.

Each of these physical element types is only required to perform Link Layer data transfer functions, but they may operate higher-level protocols as well. The interfaces between the ESLT and Earth UE are controlled by a *user-provider SLA*.

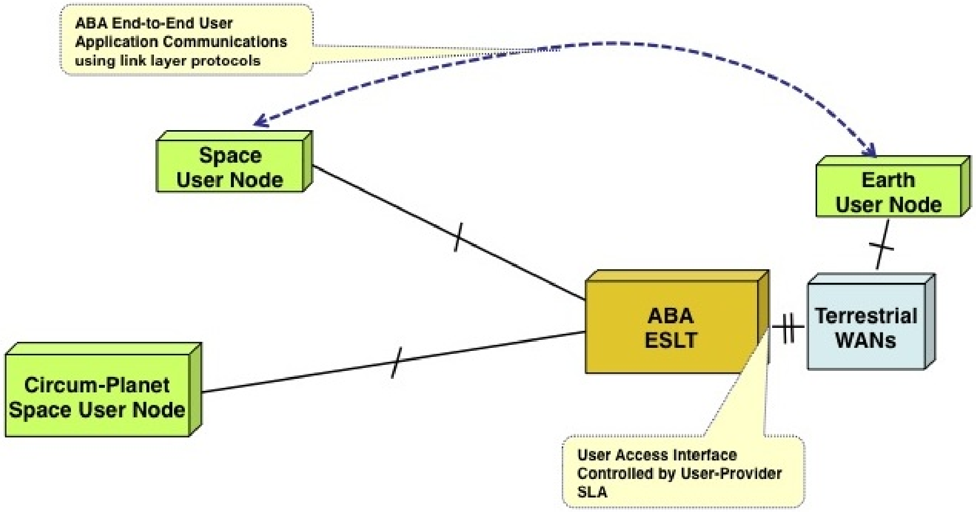


Figure 3-2: End-to-End View of ABA CSSSes and Their Connectivity

3.2.2.2 Role of Link Layer End-point Addresses

All elements in any distributed system require some unambiguous means for identifying, locating, and communicating with them. In some cases these communication paths are direct and immediate; i.e., user A connects directly to service B, using appropriate authentication credentials. For space communications, particularly at the Physical Layer (RF) and Link Layers, where signals are just radiated into space, other means must be provided. The typical means at the Physical Layer is to use an agreed-to frequency band, but at the Link Layer, it is to associate a Spacecraft ID (SCID) with each node in space. All spacecraft have an SCID that is referenced in the Link Layer protocols, and only the spacecraft with the correct SCID is expected to respond to that identifier. For ABA missions that operate at the Link Layer, the SCID is the end-point address.

3.2.3 ABA RELAY ARCHITECTURES

Some ABA missions are now using simple means for relaying data among space missions. Figure 3-3 shows an example of how the elements in figure 3-2 might evolve in order to provide a basic data-relaying capability in space. In this case the Space User Node on the planet’s surface uses the services of a space relay node that acts as a relay. This space relay node is a ‘hybrid’ orbiter, in that its prime mission is to perform science operations, but it also provides a service for relaying data from the Space User Node on the planetary surface, over an in-situ space link, and forwarding it to the user node on Earth. In this case the MOC for the hybrid spacecraft acts as an Earth relay node and performs whatever manipulations are necessary to accept, process, and forward the data to the Earth User Node. The ESLT only provides ABA configuration services and does not do any separate processing of the relay data. All data that flows through the ESLT looks like data sent to and from the space relay node.

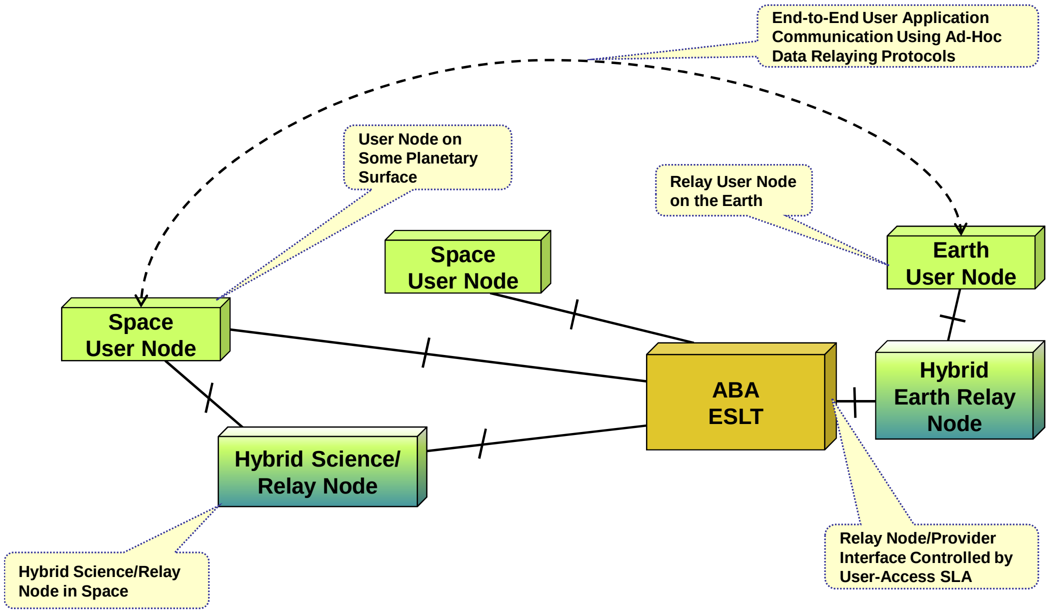


Figure 3-3: Interim ABA-Style Data Relaying Configuration

NOTES

1 An ‘in-situ’ link is a link that is between two elements that are in relatively close proximity. The longest ‘in-situ’ links would be among elements in planetary orbits.

2 A ‘long-haul’ link, such as that between the ESLT and any of the space assets, is a link that is between two elements that are at planetary distances, such as Earth to Mars.

The ABA configuration may be used to support data relaying services, but in such configurations it is the responsibility of the Earth User Node, acting as a relay service provider, to perform those services. There are two reasons for this: 1) the forward Link Layer services—Forward-Command Link Transmission Unit (F-CLTU)—may only be connected to one Earth User Node at a time, and 2) there are no formally defined, cross-supported, interoperable, Link Layer relay services. The missions that provide these relay services use various combinations of Link Layer and Application Layer (space packet protocol and file) services, but these tend to be privately defined, and not generally interoperable, protocol configurations. (These configurations work for the missions that implement them, but because there are no formally agreed-upon ways to do this, they are not interoperable in any general sense.)

In these configurations the Earth User Node MOC, acting as a relay service provider, must accept, in some mutually agreed-to form, using some mutually agreed-to protocol, data to be relayed from the ground relay user. The MOC then combines the data destined for its space user asset, with data destined for the space relay user, so that it can send the combined data in a single data stream to its space user asset using some sort of packaging and marking methods that are local to that mission. The space user asset, acting as a space relay service provider, must strip out the data destined for the space relay user, store it onboard, and then process and forward it, at the requested time, in the agreed manner, to the space relay user asset.

To describe these current configurations in even general terms would require a separate document, and the configurations that are in use have been so diverse that such a document would only be of historical significance. A discussion of some of these earliest two-hop, data-forwarding architectures is provided in *Mars Mission Protocol Profiles—Purpose and Rationale* (reference [19]). Some additional details on current protocol architectures are also provided in the sections on transitional strategies.

3.3 GENERAL DESCRIPTIONS OF FUTURE SSI ARCHITECTURES

3.3.1 SSI ARCHITECTURE

Future space missions that would benefit from internetworking services will use operational and cross support configurations of the SSI style, where a user spacecraft is operated by its spacecraft MOC using SSI cross support services provided by another agency or agencies. This SSI cross support scenario was shown diagrammatically in figure 2-9.

Figure 3-4 shows a simplified end-to-end view of the system elements involved in a typical SSI scenario: the Space User Node, the SSI ‘cloud’, and the Earth User Node, which is where the MOC is located. This figure shows all of the participating networks as the ‘SSI Cloud’ along with the required networking protocol stack. Protocols will be addressed in more depth in sections 6 and 7.

The end-to-end networking services offered by the SSI are implemented using a variety of Link Layer underlying protocols. The user applications communicate by invoking delay-aware or delay-unaware data transfer applications that deliver bundles, messages, files, or other Application Layer data using the underlying internetworking services. From the UE point of view, it is the ‘SSI cloud’ that is providing the network data delivery services. Of course, there may be one or more actual CSSEs involved in this, potentially involving an SSI ESLT, a space routing node and its MOC, and possibly other CSSEs as well.

Security mechanisms are not explicitly shown in this diagram, but they may be applied at one or more layers:

a) Application Layer security (authentication or encryption) applied to the data by the user application;

b) Network Layer encryption applied either within an IP stack (Internet Protocol Security [IPsec]) or within the DTN stack (Bundle Security Protocol [BSP]).

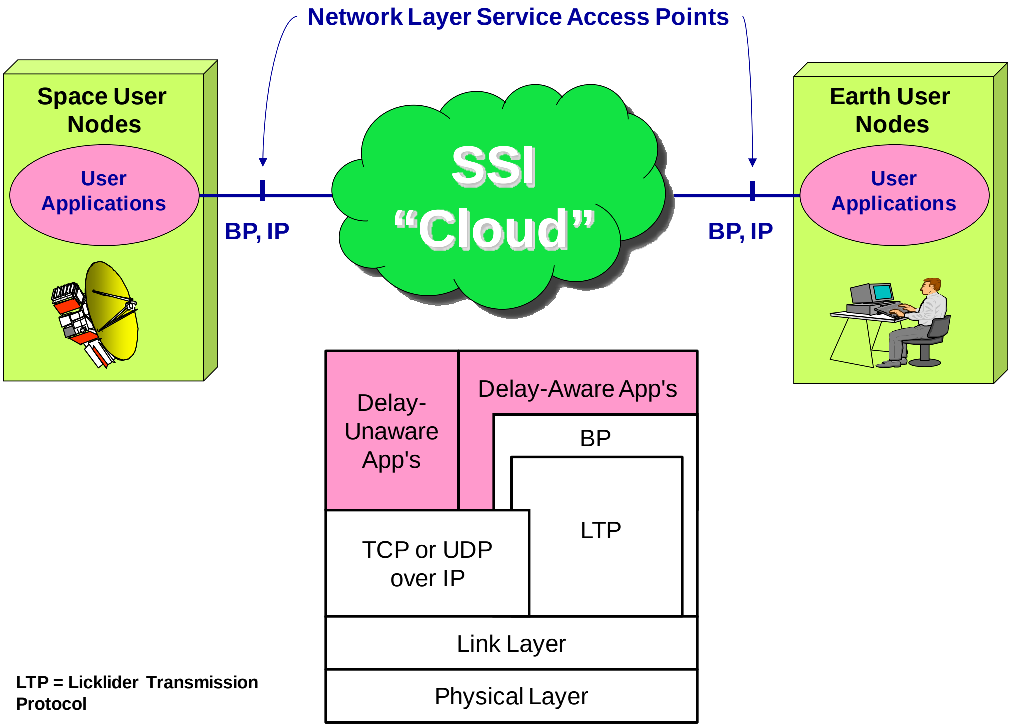


Figure 3-4: Basic SSI End-to-End Configuration and Protocol Stack

This example supports situations where the spacecraft is at some distance from the Earth (delay-aware) and situations where it is near Earth (delay-unaware). If the spacecraft is away from the Earth, perhaps at some distant planet, delay-aware applications must be used above the BP Network Layer and Physical Layer protocols. If the spacecraft is near the Earth, perhaps in High Earth Orbit (HEO) or Low Earth Orbit (LEO), delay-unaware applications may be used above the IP Network Layer and Physical Layer protocols. Any ESLT that is used must support the SSI services. The end-user nodes, in space and on the ground, may use a variety of user applications, including CFDP or Asynchronous Message Service (AMS) configured to run on top of the SSI stack.

3.3.2 SSI END-TO-END VIEW

3.3.2.1 General

The end-to-end view shown in figure 3-5 abstractly depicts the insides of the SSI 'cloud' as an interconnected configuration of federated *participating networks* that perform Network Layer routing service(s). This figure illustrates many of the specific types of building-block components that constitute these networks and the nominal connectivity among them.

The SSI elements are depicted as physical nodes, ESLT/PSLT (tan) or space routing node (aqua) 3-D boxes, and the Earth and Space User Nodes are depicted as light green 3-D boxes. Figure 3-5 also indicates, by double hash-marks, the points at which peer SSI service elements connect and the access points at which SSI user nodes connect to the SSI. The user-node interfaces are shown with a single hash mark, indicating that these need not implement the full suite of SSI protocols. The peering interfaces among SSI service-providing elements require full implementation of SSI protocols, including routing information and management data exchanges. These interfaces also imply there are agreements among the organizations that own and operate these elements to work together as part of an SSI federation to provide interoperable services and to carry one another's, and other SSI users', data traffic.

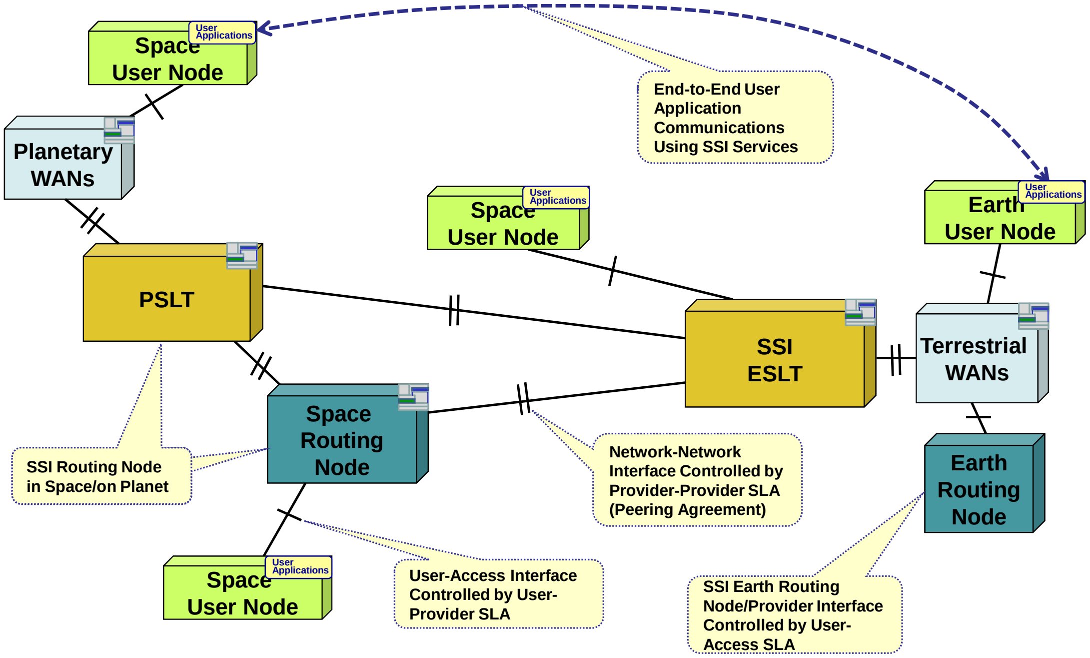


Figure 3-5: End-to-End View of SSI CSSSes and Their Connectivity

Each of the CSSE building blocks can be described as an SSI *participating network* in the sense that 1) it performs a Network Layer routing function, and 2) it may operate as its own Autonomous System (AS). In Internet terms, an AS is a collection of connected routing capabilities under the control of one or more agencies that presents a common, clearly defined routing policy to the SSI as a whole.[1] As with the previous figure, in this figure, the interfaces between tan and light green 3-D boxes are controlled by user-provider SLAs. The peering points between SSI elements (tan and aqua 3-D boxes in the diagram) are controlled by provider-provider SLAs. Terrestrial and planet-surface WANs are also shown as light blue boxes. The WANs consist of one or more routers and links which provide Network Layer (IP, DTN, or both) connectivity and routing services. These and any onboard local area networks (LANs) are essential for connectivity, but only play a supporting role and are treated as infrastructure in this document.

---

[1] RFC 1930 (Internet Best Common Practice 6), 'Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)' (reference [18]) defines an AS in terms of IP. While the sense of the definition in RFC 1930 is correct, routing in the SSI is not limited to IP, but rather includes BP as well. The definition of AS presented here acknowledges that difference in routing flexibility.

3.3.2.2 Role of Link Layer Services in the SSI

In SSI configurations, each CSSE must also connect to other CSSEs, at least at the Link Layer, but there must also be connections at the Network Layer (Layer 3) in order to provide interoperable, end-to-end, Network Layer services. In the SSI, the Earth routing node that controls the space routing node that provides network services in space is defined as the ‘owner’ of that space link; it plans, schedules, and configures the ESLT using service management and CSTS services, and also configures and controls the space routing node. The ESLT, in its turn, performs the necessary functions to create and sustain the secure space link to the space routing node. In this way the Earth routing node that acts as the user MOC for the space routing node can directly control that spacecraft, just as in ABA configurations. This permits the space routing node, and any Network Layer element onboard, to be securely controlled, managed, and restarted by its Earth routing rode MOC in the event of any anomalous conditions without requiring any Network Layer services to be operational.

3.3.2.3 Role of ESLT in the SSI

In SSI configurations, the ESLT provides direct Link Layer services to only the Earth routing node MOC, but the services offered by the SSI ESLT include Link Layer and Network Layer services. In order to offer SSI services, the required forward cross support service in the ESLT is CSTS Forward-Frame (F-Frame), which requires that the service user produce data frames (either telecommand or AOS) that will then be merged, encoded, and modulated on the link. In addition to placing coding and modulation in the ESLT, the F-Frame service can also merge frames from multiple sources. In order to support SSI services for more than one user, the ESLT must also implement a compliant, secure SSI router, running either IP and IPsec or DTN protocols (BP, BSP, or both, in the general case). The SSI router accepts data from multiple users, does either throughput (IP) or store-and-forward (DTN) routing functions, and the output of the router is then placed in frames, merged with all other data using separate VCs, encoded, and modulated by the ground station.

The forward-link frames may carry various kinds of data, and the data in the SSI frames is visible to the service provider, at least down to the DTN bundle or IP datagram level unless it is otherwise secured at the Network Layer. The contents of secured Network Layer data structures are opaque, but the headers remain visible to permit routing. On the return link, some of the VCs may be returned using the Return Channel Frames (RCF) service, but other VCs will be stripped out after decoding, extracted from frames, and sent to the SSI router for delivery to multiple users.

The SSI configuration requires use of the RCF service in addition to the integrated SSI router functions. The return service must be the RCF service in order to permit SSI traffic in separate VCs to be discriminated from non-SSI traffic. Both of these services can also fully support ABA configurations, so there is a natural transition from ABA to SSI when these services are adopted.

3.3.3 TRANSITIONAL SSI RELAY ARCHITECTURES

It is entirely possible to design the sort of ABA mission configurations and deployments shown in figure 3-3 to use the standard services and protocols defined for the SSI. Even though these protocols can support much more complex topologies, they are entirely suitable for use in these relatively simple configurations. A potential motivation for such an approach might be one where a single spacecraft has large data products to downlink that require communications services from more than one ESLT. Adopting the SSI protocols should simplify reliable data delivery at some initial cost in implementation.

A minimalist transitional approach that the SISG studied is to implement the SSI protocols in the Earth relay node and space relay node and just continue to use the ABA ESLT configuration. The Earth and Space User Nodes can also adopt the most basic SSI protocol set, permitting more automated delivery of data and simpler operations without requiring ESLT upgrades.

The SISG-recommended approach is to upgrade the ESLT to include full SSI functionality and then adapt the Earth relay node and the space relay node to provide full SSI routing services. This can work with the sort of hybrid science/SSI mission that is shown doing routing services. These elements then provide the simplest backbone configuration for SSI services. What is required next is to either adapt the end-user nodes in space and on ground to also include basic SSI end-node capabilities, or to use the last-hop and first-hop services to communicate with them as non-SSI nodes. The former approach is preferable, but the latter will work and may be required as a transition path for many existing missions. This transitional approach is described in more detail in section 4.

The strongest multi-agency motivation for taking the recommended transitional approach is that it is the best way to deploy an interoperable collection of elements that can evolve to support the full SSI services. In the absence of this approach, the alternative will be to continue to handcraft, mission by mission, the interfaces and functions for doing simple data relaying. While this works, and it may be a lower-cost approach when viewed on a mission-by-mission basis, in the long run it is more costly for each agency, and for all of the agencies as a whole, because these specialized, one-of-a-kind interfaces and protocols are continuously being invented, developed, and operated.

3.4 SERVICE AGREEMENTS AND ACCESS ARRANGEMENTS

There are some distinct differences between how services are contracted for, agreed upon, and provided in a typical current CSSS and how they are expected to work in the future. The following lists identify some of the key distinctions between these two different operational eras.

a) In present CSSS arrangements:

   – service agreements are most often arbitrarily structured text documents;

- service catalogs only exist for some service providing systems and are locally defined;
- service provision is only by point-to-point arrangement;
- service interfaces are defined by specific Interface Control Documents (ICDs) on a case-by-case basis;
- there is a variety of service management and service request interfaces provided; most are bi-lateral and few use internationally agreed standards;
- there is a variety of different service types; many of these are nonstandard and mission-specific;
- there is a variety of monitor-and-control services and interfaces provided; none use internationally agreed standards;
- addressing and interface binding arrangements are bi-lateral and may be highly nonstandard.

b) In expected future CSSS arrangements:

- service agreements are standardized, structured, parsable documents;
- service catalogs exist for all service providing systems and contain standard (and specialized) service definitions;
- service provision is both a point-to-point and multi-point, multi-party, arrangement;
- services and service interfaces use CCSDS standards;
- standard CCSDS-compliant service management and service request interfaces are provided;
- there are a variety of different service types, including link, file, and Network Layer services, all using CCSDS standard protocols and optional security mechanisms; specialized services may still be provided;
- there are monitor-and-control services and interfaces using internationally agreed standards based on the CSTS framework;
- addressing and interface binding arrangements are standardized and use well-known registries like SANA.

4 SERVICE VIEW

4.1 OVERVIEW

4.1.1 GENERAL

This service view of the SCCS architecture describes space communications cross support services that are provided by CSSSes and those systems' behavioral and access characteristics. This view describes service interfaces (space and ground), methods for using services, and cross-supported behavior for planning, scheduling, configuring, requesting, delivering, and reporting on services. The service view also addresses the means for locating and binding to services at service access points, including an initial discussion of the roles that protocols play in the binding process. These service interfaces and binding methods are a first compliance point for the architecture.

This service view of the architecture was developed based on the CSRM (reference [1]), but extends it in such a way that it can be applicable to services provided at places other than ground stations, such as onboard communication/data systems and spacecraft control centers. In the CSRM, processing of space link protocols by the service provider (which is assumed to be a ground station) is treated as production of a service on the terrestrial interface to the user (see 4.2.2 in reference [1]). This architecture, however, assumes that production of a service and processing of communications protocols may occur on any of the interfaces of any CSSE, so that services can be defined independently of the location of the service provider.

There are two sets of services described in this section: those suitable for ABA configurations, and those that can also support SSI configurations. The ABA services are primarily the single link services identified in IOAG Service Catalog 1 (reference [17]). The services in Catalog 1 support the single-hop ABA mission configurations. The services defined in Catalog 2 (reference [20]) are described next as they provide the underpinnings for the SSI upper-layer space internetworking services (ABCBA configurations). This ADD assumes that the SLE (reference [1]) and CSTS (reference [8]) protocols will be used to define the Link Layer services interfaces for all ESLTs operated by any space agencies or other, possibly commercial, service providers.

4.1.2 OVERVIEW OF SPACE COMMUNICATIONS CROSS SUPPORT STANDARD SERVICES

ABA configurations will be used where only single-hop, point-to-point, Link Layer services are required to support single-hop missions that do not need the added functionality of the SSI. The ABA configurations will also be used within the SSI as the means for the space routing node MOC to control its space routing node. While it is possible to do some of the necessary housekeeping and management functions over the SSI protocols, in general it is assumed that these will remain as Link Layer command and control functions. The ABA, Link Layer services include the following:

a) forward data delivery services;

b) return data delivery services;

c) radiometric services.

The SSI-specific service suite exposed to the users includes:

a) forward internetworking services;

b) return internetworking services;

c) position and timing services.

4.1.3 OVERVIEW OF SERVICE MANAGEMENT AND NETWORK CONTROL

To provide space communication services, it is necessary to provide the users with service management interfaces that permit them to plan, schedule, request, configure, and monitor the operations of the underlying Link Layer service-providing elements. For the basic ABA link configurations, the following set of service management and network communication asset control functions is used. The service management functions are the primary ones that are exposed to users; the network control functions are usually internal to the service provider and not specified by CCSDS.

a) The service management functions include:
   - service planning;
   - service request scheduling;
   - service visibility and controllability;
   - service reporting and accountability.

b) The network communication asset control functions include:
   - network scheduling;
   - network asset configuration and control (including security);
   - network asset monitoring.

4.2 ABA SERVICES

4.2.1 OVERVIEW OF ABA SERVICE CONFIGURATION

Utilizing ABA services is analogous to a user with a dial-up telephone modem using the services provided by their local phone company (telco or Public Telephone & Telegraph [PTT]). The user must establish a contract for services with the service provider, and can then, as needed, establish a connection using the service. The major difference for space communication services is the requirement to schedule most of the underlying space communication links ahead of time, when the ground assets are available and when the spacecraft is in view and ready to communicate. There is also much more choreography involved in space communication, but in many ways the Link Layer services are similar to terrestrial services, and the link contents are opaque to the service provider. For successful communications to the mission, it is also necessary to design services and applications with an awareness of the time delays, antenna pointing, and disconnection that are driven by the physics of the mission and spacecraft operations environment.

Returning to the terrestrial PTT analogy, the ABA service is similar to a PTT in that:

- the ABA service provider may require a contract of some sort for connecting to its service;
- other ABA service providers may be used if they offer comparable services and interfaces;
- the only required standard end-to-end layer is the Link Layer protocol. Application service, i.e., file or message delivery, may be standardized end-to-end, but this is not required;
- the space link production functions are opaque to the user and operate the same regardless of which provider delivers the service;
- the interface between the Earth User Node and the service provider must be standardized and compatible at the Link Layer. The same is true of the interface between the service provider and the Space User Node;
- there will be some stated level of service commitment, including level of service, completeness, and user conditions about delivery latency and throughput;
- users may apply their own data authentication and/or encryption, but this is opaque to the service provider.

4.2.2 ABA SERVICE USER VIEW

From the point of view of an SCCS ABA user, the service provider’s visible interfaces are the service management interfaces and data delivery service interfaces on the ground and the data delivery interfaces in space.

As shown in figure 4-1 an Earth User Node will access two different, but related, kinds of interfaces to use cross support services: one is the service management that is used for planning, configuring, and requesting services; the other is the data delivery service interfaces. The service management interfaces are based upon CCSDS service management standards, and the data delivery service interfaces are based upon CCSDS CSTS and SLE services.

There may be different upper-layer services, such as end-to-end file and message transfer, that can run on top of the ABA Link Layer protocols. These upper-layer services can take advantage of the encapsulation and path services provide by the Link Layer. The encapsulation and path services do not use addressing and do no routing; any path selection is done 'by management', prior agreement, and static configuration.

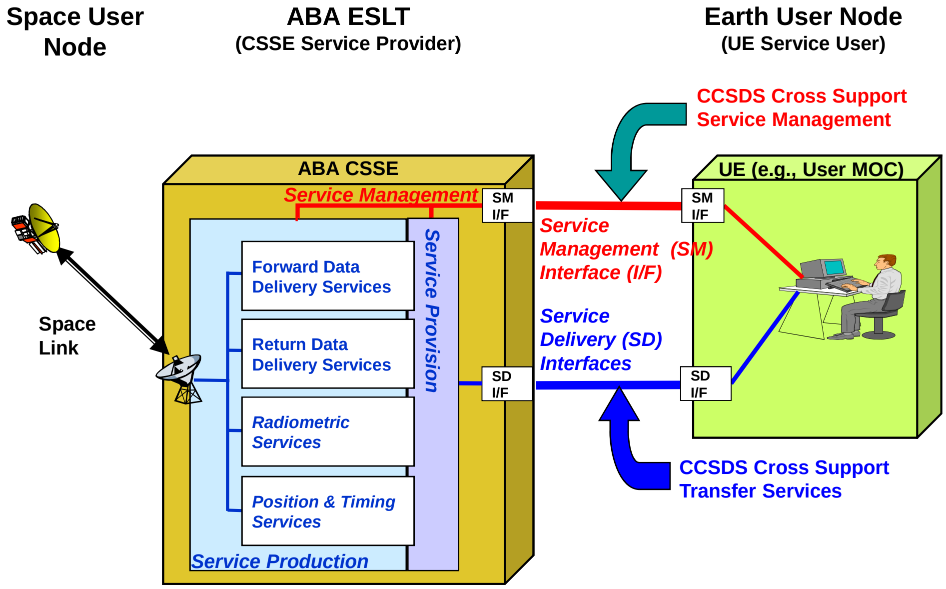


Figure 4-1: ABA Service View

4.2.3 REPERTOIRE OF ABA STANDARD DATA DELIVERY SERVICES

The space communications cross support services can be grouped into two types, related to the operational configuration in which they will be used: single link services (ABA configuration), and SSI services (ABCBA configurations, and others). The ABA standard services are described here.

The ABA configurations will be used where only single-hop, point-to-point, Link Layer services are required to support single-hop missions. These Link Layer functions also correspond to the IOAG Service Catalog 1 (reference [17]). All accesses to ABA service provider facilities, for planning, scheduling, service invocation and execution, are secured at the interfaces; only authorized users are permitted access. Users may apply Application Layer or Link Layer authentication and encryption as required, but this is opaque to the service providers.

The ABA Link Layer services include the following:

a) forward data delivery services:

  - F-CLTU service—delivery of CLTUs to a mission user node (typically in space);
  - forward transfer frame service—delivery of CCSDS AOS or telecommand frames to a mission user node (typically in space);

  - may offer a forward-file service—delivery of files to a Space User Node using CFDP.

b) return data delivery services:

  - Return All Frames (RAF) service—delivery to a mission user node of transfer frames received from another mission user node (typically in space);
  - RCF service—delivery to a mission user node of transfer frames of selected VCs received from another mission user node (typically in space);
  - may offer Return Unframed Telemetry (RUFT) service—delivery to a mission user node of unframed data from another mission user node (typically in space);
  - may offer return file service—delivery to a mission user node of files received using CFDP from a Space User Node;
  - may offer Return Operational Control Field (ROCF)—delivery to a mission user node control field data derived from the space link;

c) radiometric services:

  - raw radiometric data—delivery of tracking data provided in near real-time with little or no processing;
  - validated radiometric data—delivery of tracking data that has been processed for validation and error correction;
  - Delta-DOR—delivery of Delta-DOR data that has been processed to the level of radiometric observables.

NOTE – The ABA configurations will also be used within the SSI as the means for the space routing node MOC to control its space routing node. While it is possible to do some of the necessary housekeeping and management functions over the SSI protocols, in general it is assumed that these will remain as Link Layer command and control functions.

4.2.4 ABA SERVICE REQUEST PROCESSING

Figure 4-2 shows how service planning and data delivery for the space links is configured and managed. These links must be established and operational before any traffic may flow. In the Earth user MOC (UE) the planning, scheduling, configuration, and services request functions collectively are considered UM. The service interface that supports UM is called the *service management interface*. On the service provider side, service management requests are processed by PM, which interacts with the user to schedule and control the network. Within the CSSE, EM has responsibility for configuring, controlling, and monitoring the service production elements that do service execution and delivery.

Planning is necessary for any of these services. This planning involves review of service catalog offerings, estimating link and view period parameters, negotiating service agreements, planning and allocating resources, and performing loading analyses. For Link Layer services, which will be required between each of the communicating assets, RF and link compatibility studies will also have to be performed. Link-layer service planning also includes asset demand assessment, prioritization of user Link Layer services instances, and development of network element service schedules.

The service management interface provides the following services to the user:

a) service package, which requests and manages spacecraft space link session times and execution of the SLE and CSTS transfer services;

b) communication configuration profile, which specifies and manages the information about the space link and ground station configuration;

c) trajectory prediction, which specifies the transfer and updating of spacecraft trajectory data;

d) service agreement, which specifies the information that needs to be agreed upon before a cross support service can be established.

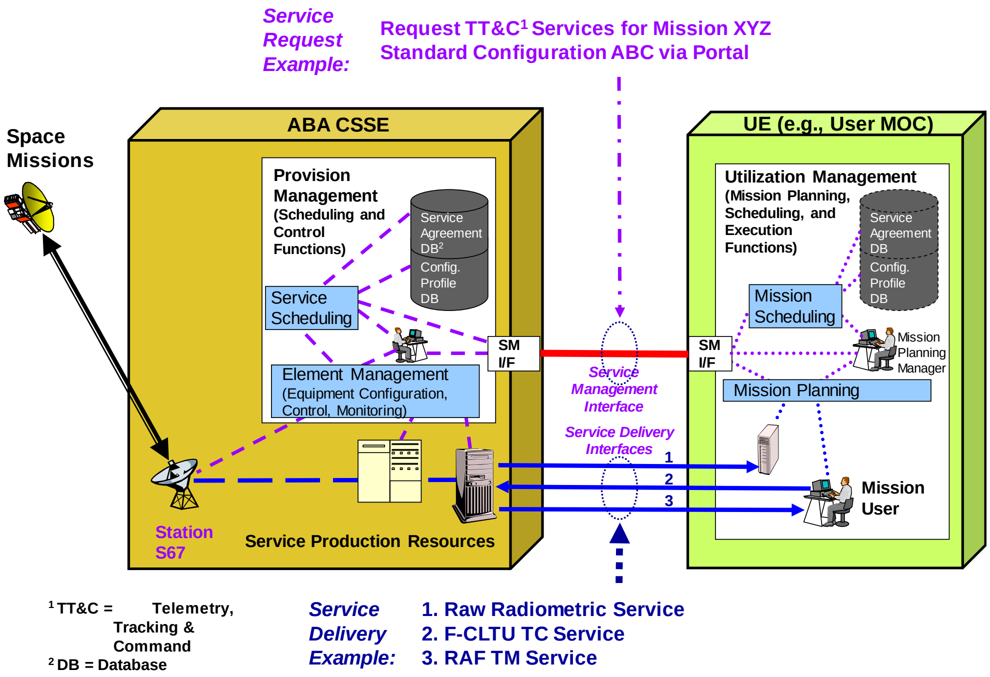


Figure 4-2: Service Request and Delivery for Underlying SLE/CSTS Services

For ABA configurations, requests for Link Layer services are handled between the Link Layer services provider (ESLT) and the MOC for the user node in space. The user MOC uses service management requests to plan and schedule the link in accordance with the contract established with the service provider. It also uses service management requests to provide the necessary trajectory (and other) predictions so that the ground station knows where to point the antenna and how to apply Doppler corrections. It then requests space link instances, making reference to one of the pre-established spacecraft and ground station communication configurations. If necessary in real-time, it may also use a service control interface to request configuration changes to the link (e.g., bit rate, mod index) of the service provider. Once the space link is up and properly configured, data can flow, usually bi-directionally, between the Space User Node and the Earth User Node.

It is also possible to 'time share' a single ESLT and space link among two or more spacecraft that are operating in the same vicinity, such as at Mars. In this case, called *Multiple Spacecraft Per Aperture* (MSPA), a single ESLT will simultaneously support downlinks from more than one spacecraft using frequency diversity. Using current standards, in the forward direction, the ESLT can only communicate with one of the spacecraft at a time, so this service must be managed. In this configuration, there may be more than one return service operating from a single ESLT at the same time, sending telemetry to different MOCs, but there will be only one forward service, with ownership of the uplink alternating among the MOCs needing to command their spacecraft (this is effectively time-division sharing).

4.2.5 ABA SERVICE PROVIDER VIEW

From the ABA service provider perspective, user service management requests, contact plans, and trajectory information are used to plan the delivery of data services and to control when and where there will be Link Layer communication contacts to support mission ground-to-space data delivery. A service agreement is used to establish the period during which services will be offered, and the spacecraft communications configurations are predefined according to what the mission can do and what the service provider can support. Service Requests (SR) are sent to the provider using the service management interface.

During network scheduling, the scheduled contacts will be based on availability of ground communications assets and by mission priorities as established between the user, the rest of the user community, and the service providers. As part of the PM functions, any antenna pointing, view period, and radiometric predictions will be calculated. EM uses the SR and configuration profiles to assign the necessary equipment and configure it for service. At the time of service delivery the data will be transferred on the ground using standard SLE and CSTS forward, return, and radiometric delivery services, and in space using standard Link Layer services. The service provider will transfer operational status, control, and reporting information in-band over the service delivery interfaces. By using CSTS monitor and control interfaces, monitor data from the services and requests to change service parameters may be transferred 'out-of-band' between the service provider and service user (see figure 4-3).

While all ABA Earth User Nodes are located on the Earth, the ABA Space User Node may be on the surface of another planetary body, or in space, either free flying or in orbit around another planet or 'hub' location, such as a Lagrange Point. Once the communications links have been established, Link Layer traffic can flow. The details of any upper-layer protocols that may be utilized by the mission are opaque to the service provider.

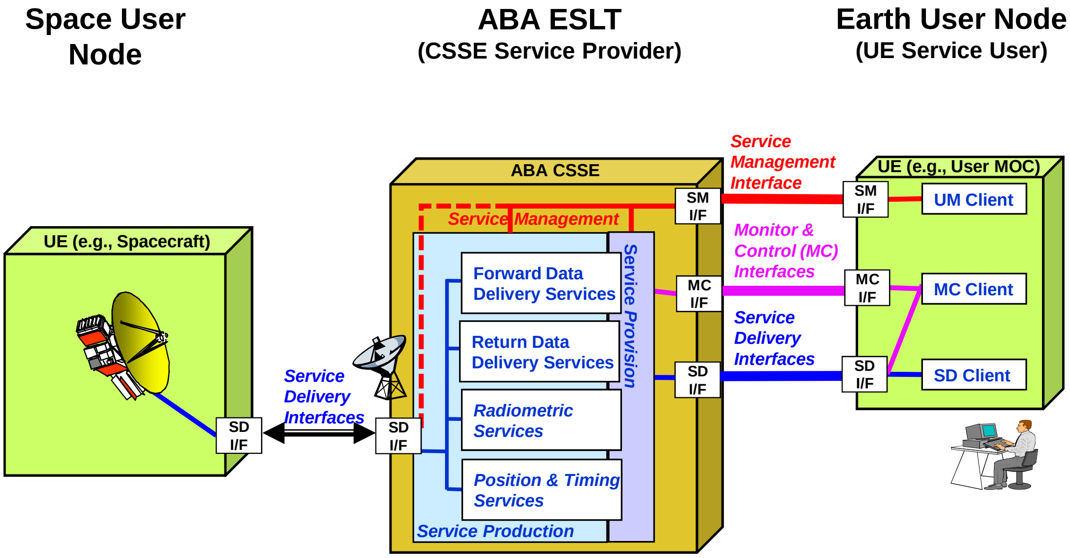


Figure 4-3: ABA Run-Time Service Provider Interfaces

4.3 SSI SERVICES

4.3.1 OVERVIEW OF SSI SERVICE CONFIGURATION

Services in the SSI configuration use many of the underlying ABA capabilities to establish the space links, but the SSI networking services are similar to those offered by an Internet Service Provider (ISP), instead of simple telco link services. The major difference for the SSI is the continuing need to schedule and choreograph the underlying space communication links over which SSI traffic flows. As with ABA services, in SSI configurations, there is also the need to design services and applications with an awareness of the time delays and disconnection that are driven by physics. In the SSI there is a distinction between the service user nodes, of which there may be several, and the service provider nodes. The SSI service provider’s primary views of the network are the service request and delivery interfaces on the ground and the service provider interfaces in space. These will be discussed separately.

What the SSI service user sees is an SSI-compliant network service router interface, essentially a space SSI-SP. This may be implemented by software in a computer local to the user or in a separate local router. Between the SSI service user’s local router and the destination, there may be network services provided by other SSI-SPs, but these should be transparent to the end user (aside from delays due to physics and availability of communications contacts). This is very similar to the Internet, where all users need to be concerned with, as they hook up a laptop in some random WiFi hotspot, is the local ISP that provides that end-user connection service. All of the other transcontinental or transoceanic ISPs, transport services, circuits, security, and routers are invisible to the users unless they probe for them or they fail.

All accesses to SSI service provider facilities—for planning, scheduling, service invocation and execution—are secured at the interfaces; only authorized users are permitted access. Network Layer security services may be provided, using Internet (IPsec) or SSI (BSP) protocols. Furthermore, users may apply Application Layer authentication and encryption as required, but this is opaque to the service providers.

The SSI is in other ways similar to the terrestrial Internet, in that:

- the ‘first-hop’ SSI-SP will typically require a contract (service agreement) for connecting to its service;
- the services of other SSI-SPs are usually provided on a ‘peering’ basis and usually do not need any sort of direct contract for service;
- the only required standard end-to-end layer is the network protocol. Application services (i.e., file or message delivery) are supported and may be standardized end-to-end, but this is not required;
- the end-to-end services should be transparent to the user and operate the same regardless of which intermediate nodes actually provide service;
- the interface between any two neighboring SSI nodes (nodes between which there is a Data Link Layer connection) must be compatible from the Physical through the Data Link Layers, as well as the Network Layer. There is no requirement for the Link Layers to be the consistent end-to-end;
- there will be some stated SSI service commitment, including level of service and completeness, but there will also be stated expectations about latency.

In contrast to the SSI service users, the SSI service providers are responsible for the SSI routers, routing updates, establishing PAs, and for managing the network assets, but they are also responsible for managing the terrestrial and space links that support SSI traffic flows. In this regard, the service providing nodes must operate a lot like ABA nodes at the Link Layer, and SSI nodes at the Network Layer. SSI service-providing nodes coordinate among themselves in order to provide SSI services for the user. (See 2.9.4 for more on peering.) Once all these SSI services are operating properly, they may be used to carry SSI user data or management data among all SSI operating nodes.

4.3.2 SSI STANDARD SERVICES

The SSI infrastructure adds a new category of internationally standardized services for its space internetworking users. The primary role of the SSI is to provide fully interoperable space internetworking and routing services, i.e., networking (OSI Layer 3) and end-to-end transport (OSI Layer 4). These new services are inserted beneath the Application Layer services (such as file or message transfer) and above the Link Layer services. In addition to the underlying ABA services and the associated service management and control functions, the SSI requires new network management services. The SSI-specific service suite exposed to the users includes:

a) forward data delivery services:

  - forward internetworking service for DTN—routing of BP internetworking data units from a mission user node (typically on the ground) to another mission user node in space, possibly via intermediate routing nodes;
  - forward internetworking service for IP—routing of IP internetworking data units from a mission user node (typically on the ground) to another mission user node in space, possibly via intermediate routing nodes;
  - forward last-hop delivery service—a standardized last-hop delivery service in the forward direction to support ‘essential commanding,’ legacy (non-networked) mission commanding, and Proximity link-time distribution;

b) return data delivery services:

  - return internetworking service for DTN—routing of BP internetworking data units from a mission user node (typically in space) to another mission user node on the ground, possibly via intermediate routing nodes;
  - return internetworking service for IP—routing of IP internetworking data units from a mission user node (typically in space) to another mission user node on the ground, possibly via intermediate routing nodes;
  - return last-hop delivery service—a standardized last-hop delivery service in the return direction to support ‘essential’ telemetry, legacy (non-networked) mission telemetry, open-loop recording (Entry, Descent, and Landing [EDL] and emergency), Proximity link tracking and time data return;

c) radiometric services:

  - no new service is added, but open-loop recording and Proximity link radiometric data may also be returned from the last-hop service;

d) position and timing services:

  - time synchronization service—allows aligning clocks to a common timescale, such as Universal Time Coordinated (UTC), but it requires that both clock correlation and time transfer be performed. Time synchronization in space may also require knowledge of orbital dynamics and relativistic effects. This is a TBD Application Layer service built using lower-level time stamps and time exchange mechanisms;
  - position service—provides information about the positions of relay and possibly user assets for planning and pointing purposes. This is a TBD application layer service built using radiometric & tracking observables.

NOTE – The SSI end-to-end Network Layer services directly support a variety of end-to-end standardized application services that are available to users. Because these application services—file transfer (CFDP), message delivery (AMS), and mission operations services—are built upon the Network Layer, they need not concern themselves with the underlying details or routing, fragmentation, and network management.

4.3.3 SSI SERVICE REQUEST PROCESSING

For SSI configurations, the SSI Earth User MOC (UE) must establish a service agreement for the SSI services that the provider organization(s) will provide to the user organization. Service agreements will take into account the resource constraints of the provider organization(s) and the aggregate anticipated needs of its users. This is a part of SSI UM, which also includes user schedule requests.

For SSI services, any ESLT service management requests occur between the ESLT and the MOC that controls the next hop destination, which may either be a space routing node or some other SSI routing asset such as a PSLT. Only the project that ‘owns’ the link to the next-hop SSI node may configure and manage the link, but once the link is operational, SSI traffic will flow as priority and capacity allow.

The space routing node MOC uses the SSI ESLT in an ABA configuration to control the link to the space routing node, sending commands to control space router operations, and receiving engineering telemetry to assess, state, and report on any anomalous conditions. This link will also be used to transmit any necessary routing information and updates to the routing node, and possibly on to other assets in the SSI.

In addition to the basic Link Layer services interfaces that provide essential telemetry and commanding of the space routing node, there is also a set of network control services that is used by the SSI service providers to schedule, configure, control, monitor, and coordinate the operation of the SSI itself. These are introduced in the following sections.

As shown in figure 4-4, service-request scheduling for space internetworking includes identification of priority and high-volume service requests so that they may be assessed and accommodated if possible. The scheduling of these service requests will also involve contact planning for data forwarding. As with ABA services, SSI Network Layer service requests also include assessment of demand for lower-layer link assets, prioritization of user Link Layer services instances, and creation of network-element service schedules. These calculations all feed into operations schedules and routing table updates for the relay assets and into routing table updates for the SSI user nodes.

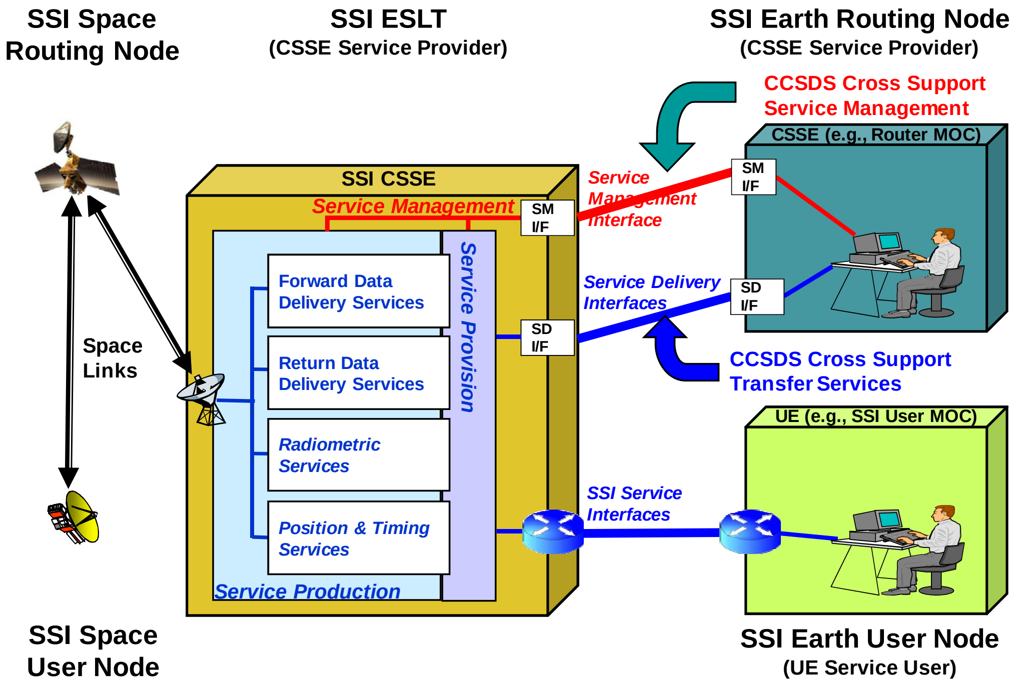


Figure 4-4: SSI Service Request and Delivery

4.3.4 SSI SERVICE USER VIEW

The SSI service user arranges for services by submitting user schedule requests to the provider organization that has agreed to provide services. The service provider, once it has gathered all of the user service requests (from multiple users) for some period of operation will negotiate schedule adjustments with the individual user organizations, based upon the availability of the SSI provider resources. The SSI service provider then distributes the provider contact plan to user organizations so they may plan their user contacts accordingly.

Service delivery for space internetworking is accomplished by the user sending Network Layer data (and any Application Layer data they contain), along with appropriate routing and addressing information, to the nearest routing/forwarding node. For IP traffic, this will be forwarded immediately, obeying the IP routing and connectivity rules. For DTN/BP traffic, the data may be forwarded immediately if a path is available, or they may be staged in intermediate storage until a suitable route is available. These routing elements are shown as ‘blue hockey pucks’ in figure 4-5 and they will typically exist at all intermediate relay nodes in the system.

Only the DTN relay elements provide ‘store and forward’ functions. These relay elements are likely to support only one protocol suite or the other, but some nodes may support both protocols.

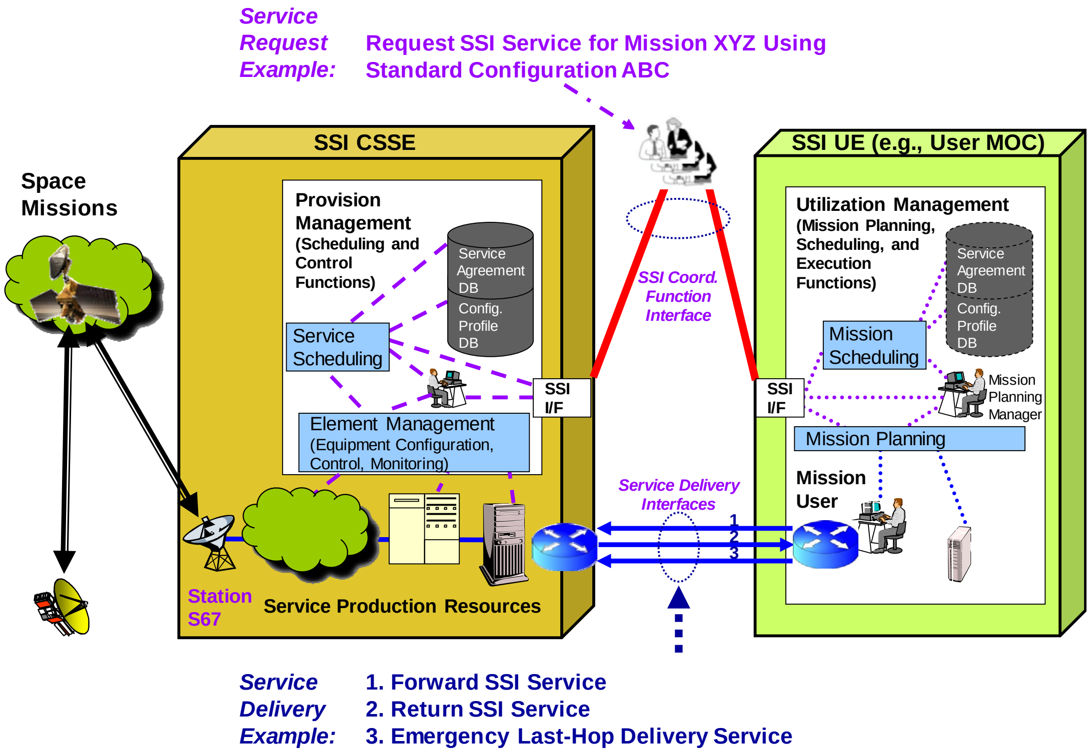


Figure 4-5: SSI Run-Time Service Provider Interfaces

NOTE – A tenet of DTN is that it will deliver data even in a disrupted or delayed environment. A dedicated, full-time, fixed link to the Moon or Mars would be a great asset to have available, but it is a) expensive, and b) not needed unless there are mission requirements for immediate delivery of all data.

The SSI Earth-user data will flow to the next hop destination once the link is established. In the typical compliant deployment, this transfer will not involve the Earth routing node at all; typically there will be continuous connectivity between the Earth User Node and the ESLT, so data can sent by the Earth User Node can be immediately forwarded across this link. Once the link to the space routing node is running, data can be transmitted by the ESLT node across the space link. Routing of data at intermediate nodes is automatically handled by the DTN protocols. Optionally, the DTN BSP can be used to provide hop-by-hop or end-to-end DTN security.

Similar services are provided for delivery of data across all links of this end-to-end path. In the initial SSI deployments, it is expected that all of the planning and scheduling for space links as well as ground links will be done on Earth to ensure there is adequate capacity and coordination. Over time, additional space internetworking service management functionality may be defined to permit autonomous scheduling of network contacts, more dynamic requesting of data transfers, or signaled requests for dynamically assigned bandwidth.

In the SSI, UE nodes do not need to concern themselves with directly scheduling the space links; this is the province of the SSI service providers. The service users may wish to know what the schedules are in order to estimate the time of data delivery, but the only link they need to actually configure and control, in some fashion, is the link between their Space User Node and its nearest SSI access point. Scheduling of the future SSI is the province of the SSI Coordinating Function (reference [9]).

NOTE – The SSI provides priority delivery flags and may offer some sort of delivery estimates and/or guarantees. It should also offer user feedback on delivery success and status, but the means to do this is still To Be Determined (TBD).

There will be different upper-layer services, such as end-to-end file and message transfer, that will run on top of the SSI Network Layer protocols. These upper-layer services can take advantage of the end-to-end transfer, routing, forwarding, security, and reliability services provided by the internetworking layer. In order for the federated SSI to work, all of these services and protocols must be standardized internationally so that transfer initiated via any SSI access point and transported by any SSI-SP, will be properly routed through other SSI elements until it reaches its final destination, which may be many ‘hops’ away.

NOTE – All of the interoperable SSI services and protocols must be standardized, just as all of the Internet specification documents—Requests for Comment (RFCs)—are standardized. This does not mean that users must standardize their mission operations or agency-specific protocols that run on top of the SSI, but this is permitted.

4.3.5 SSI SERVICE PROVIDER VIEW

From the SSI service provider perspective, user schedule requests are negotiated with the users and then are used to develop provider contact plans that are used to plan the delivery of data services. These contact plans are also used to develop routing information that defines when and where there will be communication contacts to support internetworked data delivery. The negotiations for service may include more than one service provider organization, and in the future are expected to involve an SSI Coordination Council to perform SSI network planning and management functions that require coordination across multiple providers.

The routing information may be completely static, programmed into the SSI nodes, or use ‘contact graph routing’ (reference [21]) that allows routes to be calculated based on priority of data and availability of ground communications assets, space links, and node capacity. Regardless of the means used, SSI service nodes will transfer routing information and other control-and-reporting information as part of a peer-to-peer network control process. These are done as ‘in-band’ transfers between peer service nodes in the SSI; these arrangements are established using pre-agreed peering agreements between agencies and missions (see figure 4-6).

NOTE – While not every specific standard mentioned in this architecture is finalized at this time, those that are not are either in process or under discussion in current CCSDS working groups. For example, Contact Graph Routing (CGR) is being defined at the time of writing this document; the other SSI control and reporting management functions will be defined in the future.

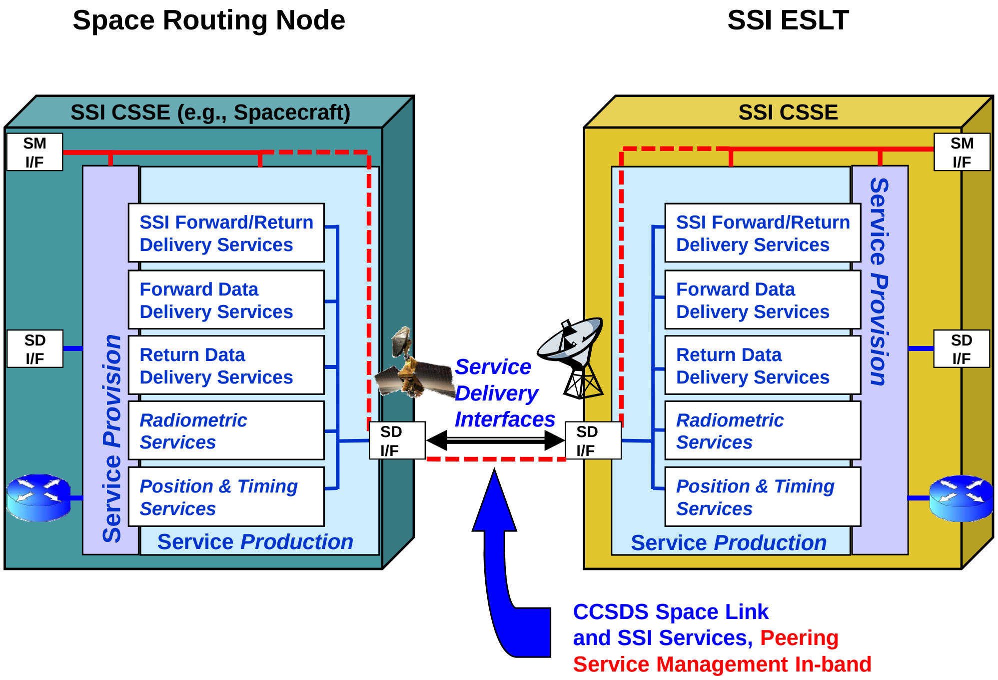


Figure 4-6: SSI Service Provider Peer-to-Peer Run-Time Service Interfaces

The SSI CSSEs may be on the Earth, on the surface of another planetary body, or in space, either free-flying or in orbit around another planet or ‘hub’ location, such as a Lagrange Point. Once the peering agreements are in place and a coordinated contact plan has been distributed, the SSI is ready to support user traffic. CSSEs will all have some sort of internal EM function that is used to configure the service delivery equipment. They will also use network management to manage any routing table updates that are necessary.

Internally, the SSI Earth routing node CSSEs use essentially the same ABA-style service request and service delivery interface to construct the space link between the space routing node and the Earth routing node that manages it. In the SSI, a conformant ESLT that provides the ground communications service will also support the SSI Network Layer protocols and the means to merge multiple streams of data onto a single space link. Once the link is established to the space routing node, any data destined for end nodes that can use that path will flow at the Network Layer. SSI service nodes forwarding DTN/BP traffic should have some storage available to store data until a suitable route is available, but may route data immediately if a path is available. It should be noted that SSI service nodes are not *required* to store data unless they assume responsibility for the reliable forwarding of such data.

NOTE – The SSI ESLT will provide what is in essence an ABA service to the Earth routing node (so it can directly control the relay spacecraft without needing SSI to be operational) and an SSI service to that relay spacecraft (possibly) and to all other spacecraft to which the relay provides services.

The delivery of data from some intermediate node to the SSI Space User Node is similar to the initial hop, except that the link is likely to be a space link of some sort and there is not any explicit service management interface. In figure 4-7, the space-user end node is assumed to be operating as an SSI node, with the basic network functions described in section 3 in place. The SSI service node in this figure is shown as a space routing node, but it could equally well be a PSLT on the surface of a remote planetary body.

NOTE – There is not yet any defined means of signaling service requests and link configurations to remote intermediate nodes. A protocol to do this may be needed, and the CGR may become the means to distribute this information.

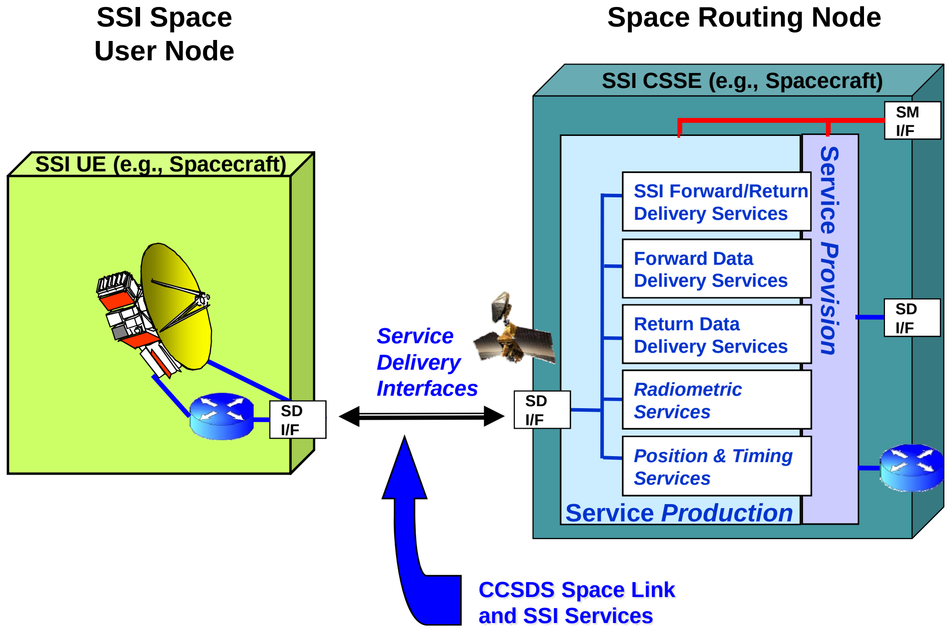


Figure 4-7: SSI Service Provider Run-Time End-User Service Interfaces

4.4 SSI LAST-HOP SERVICE

In some cases, the space-user end node may not be fully SSI compliant, in which case it will only be running Link Layer services and transmitting frames, packets, or some other primitive Link Layer data structures. In these cases the space-user end node may still be served by an SSI intermediate node as long as that SSI node implements the last-hop data delivery service. This same last-hop service also provides the necessary low-level, Link Layer command transmission functionality to do an emergency ‘reboot’ of an SSI node that is in need of a restart.

The SSI will implement a standardized last-hop delivery service in the forward direction to support ‘essential commanding’, legacy (non-networked) mission commanding, and Proximity link time distribution. As with other spacecraft commanding functions, these may be secured using authentication, encryption, or Link Layer security. A standard, file-based ‘delivery package’ structure is defined as the means for the user to transmit both the data to be delivered and the instructions about how to deliver it in a consistent way. A corresponding first-hop service is defined to return essential telemetry, radiometric data, and data from open-loop recording equipment from SSI or non-SSI nodes.

NOTE – These are new services that are intended to provide the ‘hooks’ for non-SSI missions into the SSI framework. They are further described in the following paragraphs.

These services are designed to operate over SSI networked end-to-end services, and they will enable a ground-user MOC to transfer data to its spacecraft (Space User Node) via multi-hop relaying of the file through a sequence of SSI nodes. The penultimate node then provides this last-hop service. A *delivery-agent* application resides in this service node and provides the actual data delivery to the last node. The last hop from the service node to the end node does not rely on SSI-networked services. (See 6.5.3 for more details on how this delivery agent and the associated protocols are to operate.)

NOTE – While the exact standards for providing this capability are TBD, and no such CCSDS standards presently exist, the IOAG SISG *SSI Issue Investigation and Resolution* document (reference [6]) has provided a viable approach that is referenced here. As the SSI is deployed, and more end nodes support the SSI protocol suite, it will be essential to provide such a capability in order to recover from spacecraft emergencies and to support non-SSI end nodes; it is the equivalent of a remote ‘reset’ button for SSI assets. This is future work for CCSDS. These emergency communications functions will need to be implemented in any node that provides service to either ABA end-user nodes or other SSI nodes that will need to be ‘rebooted’. There is a corresponding first-hop service that returns essential telemetry from an SSI node or a non-SSI ABA node, and that can also process and return other data such as radiometric observables from a Proximity link, time-exchange information, or open-loop recordings acquired during an EDL pass.

4.5 DEPENDENCE OF SERVICES ON PROTOCOLS

The definition of service interfaces is independent of the communications protocols used to access the services. For example, an end-to-end service to deliver files or frames may use different communications protocols depending on where the CSSE and the UEs are located. The service behavior is also defined separately from the protocols that are used to bind to the service interface, but both must be defined in an unambiguous way for interoperability. Protocols are treated separately in section 6, but figure 4-8 introduces the concepts of how service elements and protocol stacks are related.

In figure 4-8 the ovals represent service elements, i.e., either service users or service providers. The 'tubes' that are shown represent the service interfaces, which are defined by one or more *service protocols* such as SLE or CSTS. These interfaces are where the behavior of the service itself is visible. In order for the service user to access the service provider, it must first identify where the service is located and what address it is using. This service address may be the name of a system and an IP (or other) address and port number, or some other unambiguous identifying information such as a Uniform Resource Locator (URL). This information may be programmed into the service elements, stated in some form as user-entered parameters, or looked up in a service registry.

NOTE – The details of services addresses are an implementation issue; however, it is not addressed here since it may be handled differently for different service types. It is also evolving.

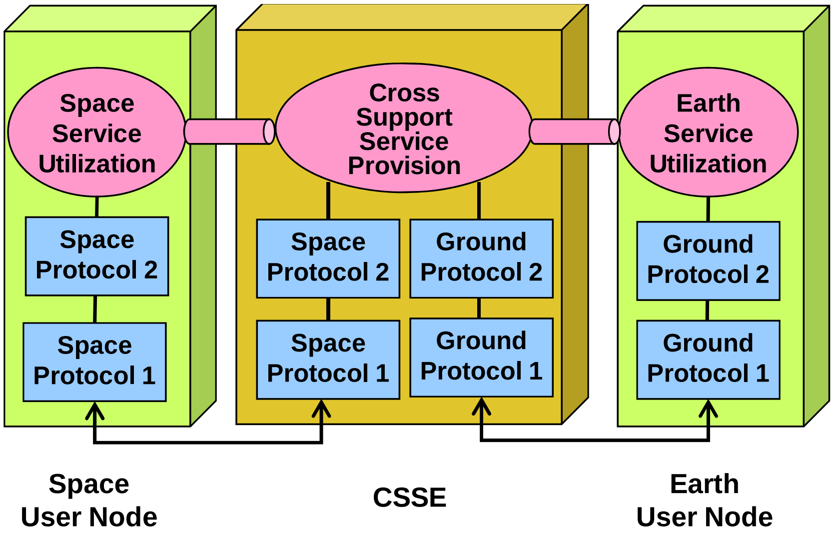


Figure 4-8: Relationship between Service Interfaces and Protocols

In order to bind to the service element, the service user and service provider must implement the proper stack of interface protocols; this is the *interface binding signature*. This signature may involve TCP/IP, HTTP, or some set of CCSDS space-communication protocols. These underlying protocols are shown as blue rectangles in figure 4-8. They may consist of a simple Link Layer and Physical Layer pair, or they may involve internetworking layers and even other higher-layer protocols. The binding information may be predefined or it may be discovered at run-time. This is an implementation detail, but the later the binding information is defined, the more flexible (and complicated) the design.

In most cases, in addition to the binding at a single service-element interface, the selection of specific communications protocols in the whole end-to-end stack is determined by the location of the CSSE or the exact nature of the link. For example, CSSEs at ground stations will always use space link protocols on the space-link interface. A CSSE that is an orbiter around another planet will typically use two different space protocols, a long-haul protocol like AOS on the space link back to Earth, and an in-situ protocol like Proximity-1 on the link to the planet surface. End-to-end, the protocols used at the Application Layer in an ABA configuration are unlikely to be the same, but there will be some common data structures, possibly just the space packet or a file structure. Similarly, in a typical interoperable SSI internetworking architecture, there will be at least one layer that is consistent end-to-end, such as DTN or IP.

While the links between all elements in these service viewpoint diagrams are shown as just simple links, in reality there is a potentially complex stack of protocols providing the service and flowing the data. Section 6 contains more descriptions of the communication protocol configurations at specific interfaces, and section 7 contains descriptions of end-to-end configurations.

4.6 SECURITY CONCEPTS FOR SERVICE VIEW

The system elements that provide user services will typically be secured in a number of ways, both physically and logically. The following security methods are likely to be employed in the implementation of service systems:

- operational staff will be required to login to the operational systems;
- operational staff will have assigned roles and access controls, as appropriate;
- all service interfaces will be secured and require some sort of access credentials;
- users will be required to login to the system management interfaces in order to plan and schedule services;
- users will be required to login to the system management interfaces in order to request, monitor, and control services;
- users will be required to login to the service execution interfaces in order to send and receive data;
- different users may have different roles and access credentials;
- users will be required to establish a service contract with the service provider before services may be accessed.

More details about service security interfaces and appropriate authentication approaches can be found in the security sections of the SLE and CSTS documentation (references [1] and [8]), and the Security Architecture and Cryptographic Algorithms documents (references [7] and [22]).

Physical security is addressed in section 5; other types of communications link security, such as link encryption, are addressed in section 6.

5 PHYSICAL VIEW

5.1 GENERAL

The physical elements (nodes) of a deployed CSSS embody a set of functions that implement the behavior exhibited by the CSSEs and UEs that compose the system. The external interfaces of these functions are the services described in section 4. The physical view is used to describe 1) the expected physical configuration of CSSSes/CSSEs/UEs and their physical characteristics, 2) the allocation of functionality to these different physical elements, and 3) an overview of possible topology and connectivity of the physical elements (including UEs) that support specific space missions.

A physical element may be an element on the surface of a heavenly body (e.g., the Earth, the Moon, or Mars), an element orbiting around a heavenly body, or an element in cruise through space. Examples of physical elements are orbiting spacecraft (deep-space and near-Earth), landed elements on the Moon or Mars, data management systems onboard spacecraft, ground stations, control centers, and computers at control centers. The physical elements that are CSSEs are referred to as building blocks, since they are used to build end-to-end systems configurations.

Space communications cross support involves several types of physical elements, ranging from individual hardware elements such as antennas, receivers, and computers, to large or complex elements such as tracking stations, control centers, and spacecraft. In this ADD the internal details of physical elements are described only where they are necessary for explaining how cross support services are provided. For example, a tracking station provides cross support services for the Space and Earth User Nodes it supports, but knowledge of the internal implementation of the tracking station is not necessary for using the service.

In this section, only the tracking station as a whole and its essential functions are shown as the CSSE, and the implementation details of the internal components of the tracking station are not shown. These details would be shown in some other architecture descriptions, such as the implementation description for the antenna itself. In other documents, such as Service Management (reference [14]) the term ‘functional resources’ is used to describe these lower level functional implementation details. (See Functional Resources for Cross Support Services, reference [65], for a description of Functional Resources.) Each of these essential functions is typically implemented by more than one functional resource.

5.2 ABA PHYSICAL ELEMENTS

5.2.1 OVERVIEW

This section defines the ABA CSSE and UE nodes and the descriptions of the functions they are expected to implement. A generic physical model of an ABA building block is presented, followed by the CSSEs and UEs that are used to compose ABA end-to-end systems.

5.2.2 GENERIC ABA BUILDING BLOCK

Figure 5-1 provides a view of the interfaces and functions that may reside in any given node in an ABA configuration. This is a generic diagram for ABA nodes; not all nodes will necessarily include all of these functions. Specializations of this generic ABA node for particular purposes will be presented later in this section.

The ABA node type only includes Link Layer processing functions, service management functions, and may include one or more applications. Instead of a routing function, which typically includes decision making, these nodes only include a managed function to do data forwarding along a predefined path, usually identified by Link Layer tag fields. No explicit addressing is provided by these Link Layer tags, only a path ID that must be managed by the users and service providers in order to control data flows. There may also be a data store associated with this node type to hold data until the next link along the preprogrammed path is available.

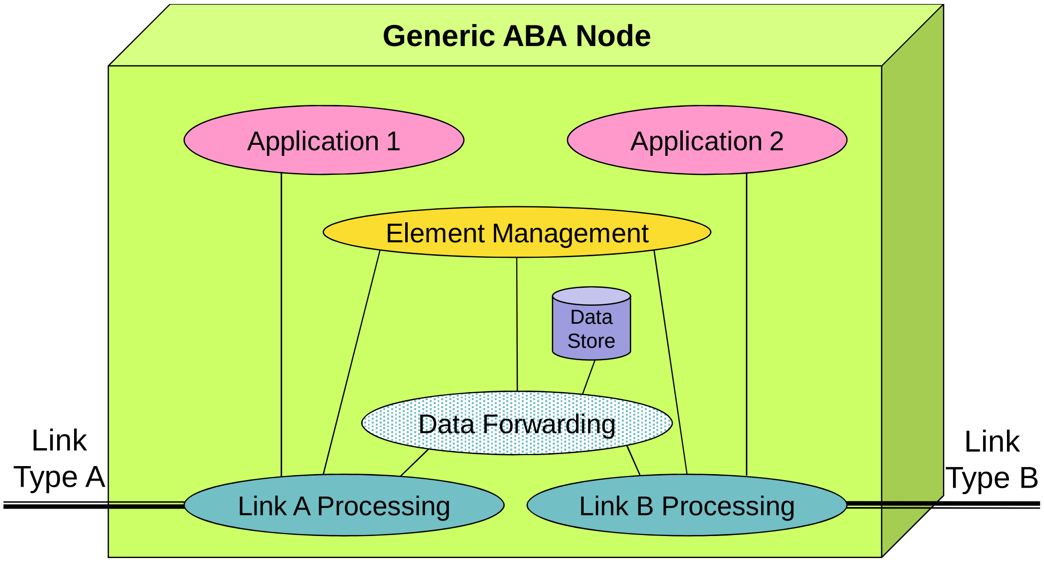


Figure 5-1: Generic ABA Building Block and Functions

NOTE – The decision making happens in the service management and data forwarding functions. This diagram is intentionally simplified and symmetric, and it is notionally also bi-directional.

The three major elements in an ABA configuration are a service provider node and two service user nodes, one on the ground and (typically) one in space. There is no expectation that the ABA Space User Node can perform any services for other nodes.

NOTE – Some ABA missions are constructed using one or more space and ground nodes that define and use private protocols to communicate. In some cases these protocols are used to relay data from one spacecraft node to another, and to forward data to and from the Earth. Since these configurations tend to be unique to each mission, there is usually no attempt to standardize them and they are not described further here.

5.2.3 ABA-SPECIFIC CSSE BUILDING BLOCKS

This section briefly describes each specialized ABA CSSE, its role, and how it interconnects with the other element types. It also describes the functions allocated to each of these nodes, since these functions are what determine their behavior.

A typical ABA configuration involves an Earth User Node (the MOC) communicating with the Space User Node using the Link Layer services of an ESLT. The ESLT may offer full SSI service functionality, but in this instance only the Link Layer services are considered.

Table 5-1 shows the ABA node type, its interfaces, and associated functions. The grayed-out functions are not required for ABA, but may be present. This table provides an overview the ABA CSSE node, the kinds of interfaces it supports (links), and the key functions it implements (link control). For ABA configurations there is only one CSSE type.

Table 5-1: ABA CSSE Node Type, Interfaces, and Functions

CSSE/ Building Block	Terrestrial Links	Space Links	Proximity Links	Space Link Control	Routing
ABA ESLT	X	X		X	N/A

The ABA node shown in table 5-1 only communicates at the Link Layer; it does not include any Network Layer routing functions. These nodes can communicate directly to space UEs using standard Link Layer services and to Earth UEs using terrestrial services (SLE, CSTS, and service management).

As shown in figure 5-2, the ABA ESLT provides Link Layer connections over a space link so that standard space link frames are transmitted between the MOC and ABA user nodes in space. The ESLT provides one of two services, both of which involve pointing of directional antennas, selection of appropriate spacecraft identification and communication attributes, and may involve cryptographic operations that are specific to the target spacecraft and applied by the MOC:

a) Using F-CLTU, the ESLT accepts CLTUs (frames that are already encoded and possibly encrypted), then modulates the RF, and radiates it toward the end user node in space. This service accepts inputs from only one source; no multiplexing is possible.

b) Using F-Frame, the ESLT accepts telecommand or AOS frames destined for space and encodes and multiplexes them into the frame stream in the space link, encodes and modulates the RF, and radiates it toward the end user node in space.

On the return side, the ESLT 1) receives and demodulates RF signals from Space User Nodes, 2) frame syncs, decodes, and extracts frames from the link, and 3) de-multiplexes the frames destined for user MOC nodes. The SLE service options are RAF or RCF, which may send subsets of the data to different users. These services are identified in the SLA that specifies the services provided to a particular mission by the SSI.

The ABA ESLT has terrestrial interfaces that use suitable link protocols and support SLE and CSTS traffic (shown as ‘SLE Tunnel’). The ESLT also has a service management interface that is controlled by the UE that is responsible for managing the space link. The ABA ESLT does simple managed data forwarding controlled by the VC IDs that are part of the Link Layer protocols. On the forward path, data may be radiated immediately (online), or at some proximate fixed time (release time), or it may be stored in the ESLT until it is time to be radiated (forward offline service). On the return path, it either may be returned online, or stored and returned offline if the user MOC is not ready at the time the data is received on the ground.

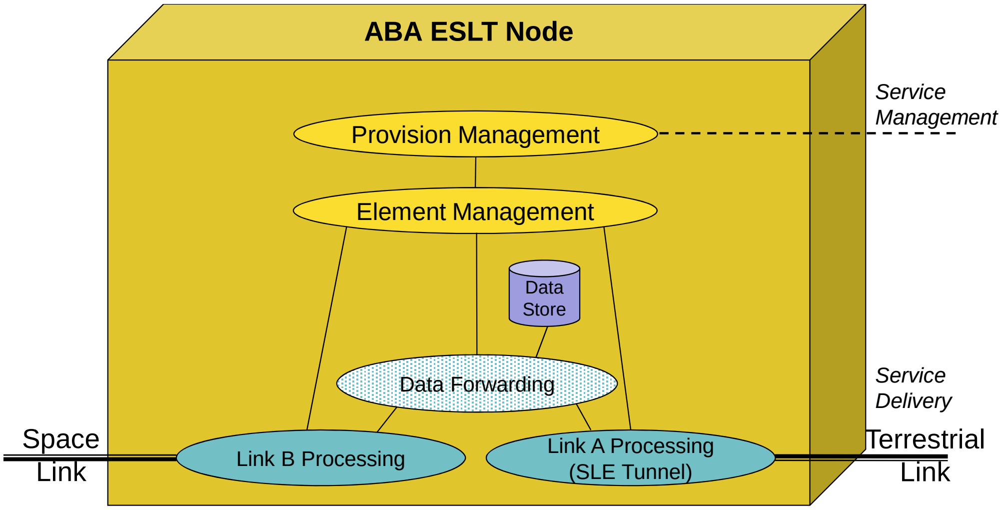


Figure 5-2: ABA ESLT Node

5.2.4 ABA-SPECIFIC USER ELEMENT NODE TYPES

5.2.4.1 Overview

This section briefly describes each specialized ABA UE type, its role, and how it interconnects with the other element types. It also describes the functions allocated to each of these nodes, since these functions are what determine their behavior. There are two basic node types described in table 5-2, Earth User Nodes and Space User Nodes.

Table 5-2: ABA UE Node Types, Interfaces, and Functions

CSSE/ Building Block	Terrestrial Links	Space Links	Proximity Links	Space Link Control	Routing
Earth User Node	X				N/A
Space User Node		X	X		N/A

5.2.4.2 ABA Earth User Node

The ABA Earth User Node, as shown in figure 5-3 uses only Link Layer services and does simple, preprogrammed, managed, data-forwarding functions. Since this user node is the MOC for the spacecraft at the other end of the link, it has responsibility for requesting, configuring, controlling, and monitoring the space link via the service management interfaces. Only one application is shown, but in practice there may be many different applications, each with its own application protocols running on top of the space Link Layer services. These may use space packets or other means (e.g., CFDP file-delivery protocol encapsulated in space packets) to structure and transfer data. Details of these Application Layer services and associated protocols are not shown here.

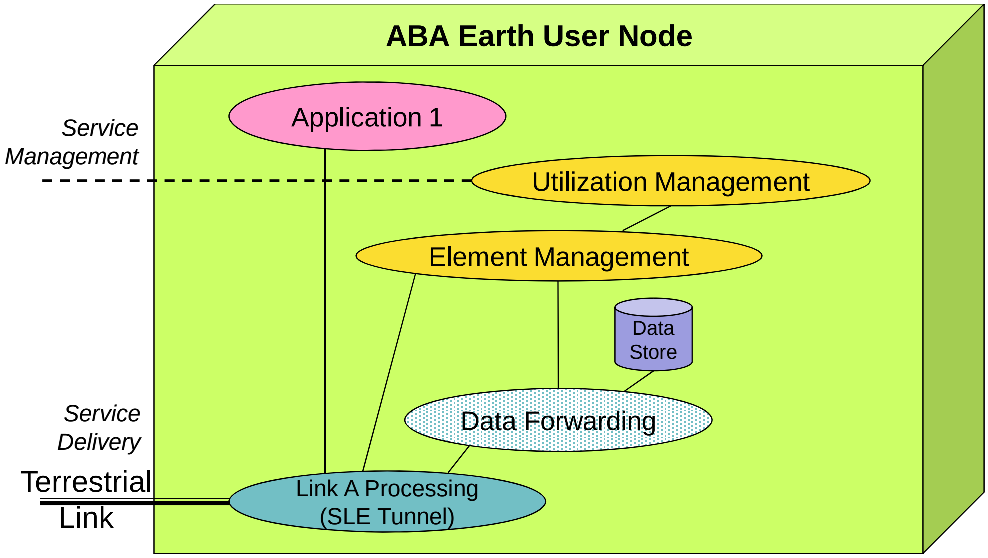


Figure 5-3: ABA Earth User Node

5.2.4.3 ABA Space User Node

The ABA Space User Node, as shown in figure 5-4, is configured much like the Earth User Node, with Link Layer processing and related data forwarding that is usually preprogrammed. It also includes what is effectively an EM function, but this is typically a function commanded by the spacecraft MOC and obeys no current standard protocols nor interfaces.

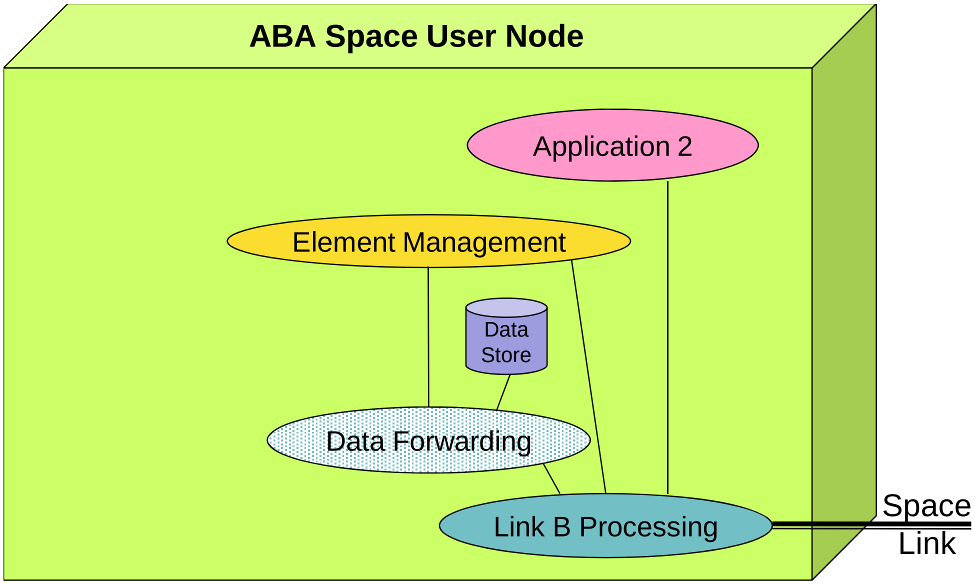


Figure 5-4: ABA Space User Node

As mentioned earlier, even in these ABA configurations, it is possible to arrange for a certain level of multi-spacecraft interoperability. This may be done by 'piggy-back' spacecraft that communicate over a local bus, by using private 'proximity' links, by flying a cluster of spacecraft that share a main link back to Earth, or in spacecraft configurations like the International Space Station (ISS). For cross support purposes these are all treated like ABA configurations, the relaying is internal to the missions until the 'piggy-back' missions separate.

It is possible for an ABA end node to be communicated to by an SSI node, using the 'emergency' communication or 'first-hop' processing described in 6.5.3.2. This involves delivering a file, plus delivering metadata to the last-hop SSI node, which would then process and deliver the file contents in a way that the ABA end node can understand.

5.3 SSI PHYSICAL ELEMENTS

5.3.1 OVERVIEW

This section defines the SSI CSSE and UE nodes and the descriptions of the functions they are expected to implement. A generic physical model of an SSI building block is presented, followed by the CSSEs and UEs that are used to compose SSI end-to-end systems.

5.3.2 GENERIC SSI BUILDING BLOCK

Figure 5-5 provides a view of most of the typical interfaces and functions that may reside in any given SSI node. This is a generic diagram, and not all nodes will necessarily include all of these functions. Specializations of this generic node for particular purposes will be presented later in this section. Some SSI nodes may include additional functions, such as the last-hop service, security, or science functions that may be co-hosted on a hybrid science/SSI spacecraft. User nodes will typically include fewer functions.

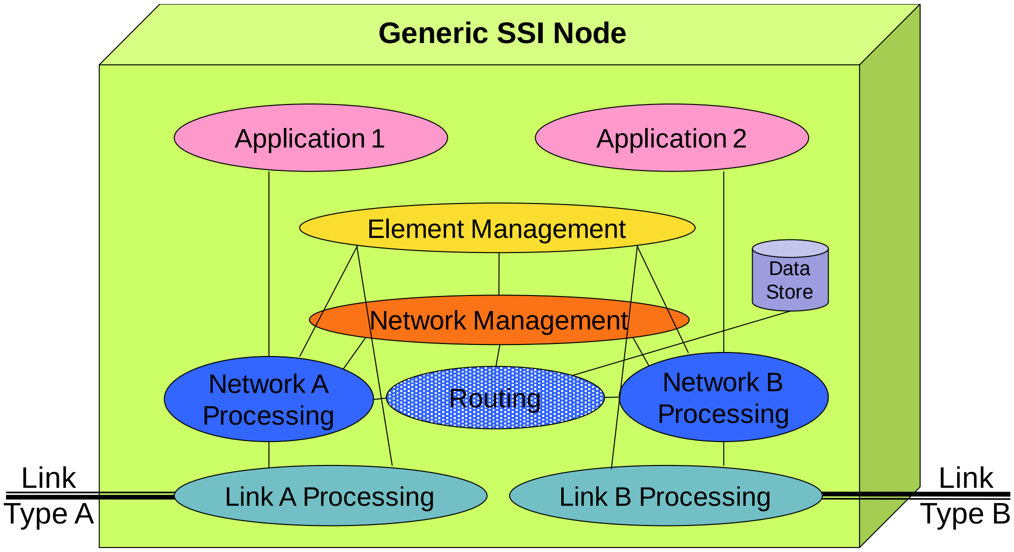


Figure 5-5: Generic SSI Building Block and Functions

NOTE – As with ABA, decision making is inside the service management, but it is also in the network management and routing. The data store could be symmetric, but as long as there is a data store somewhere inside this node, that is sufficient. The service is notionally two-way, bi-directional.

The SSI CSSE nodes specifically include Network Layer processing functions and the associated routing, network-management, and security functions. Like the ABA node type, it also includes Link Layer processing functions, EM functions, and may include one or more applications.

Instead of a simple, managed, data-forwarding function, SSI CSSE nodes include network processing and explicit routing functions, which typically will include decision making. SSI PDUs include explicit source and destination addresses, and these are used, along with contact plans, to make routing decisions essentially in real time. There typically will be a data store associated with this node type to hold data until the next link is available to transport data toward its destination.

Generally, the Link Layer interfaces on SSI nodes may use either terrestrial protocols (e.g., Ethernet, WiFi), space protocols (e.g., telecommand, telemetry, AOS, Proximity-1), or a combination of more than one of these types. The specific link configuration will depend upon where the CSSE is deployed and the services it is to provide.

Only those autonomous systems that provide either DTN (BP) or IP routing functionality are fully compliant SSI building-block types. Purely Physical Layer space relays (such as the NASA Tracking and Data Routing Satellites [TDRS]) are considered to be just Physical Layer (Layer 1) data pass-through subcomponents of another SSI building block (such as an ESLT). They effectively function as a remotely operated ground station aperture that is located in space.

The other major SSI node type is the UEs: the Space User Nodes and Earth User Nodes; however, these user nodes are not considered SSI building blocks in that they do not necessarily implement all of the necessary routing, forwarding, and management functions to provide service to other nodes. It is not possible to construct an SSI using just user nodes.

All accesses to SSI service provider facilities for planning, scheduling, and service invocation are secured at the interfaces; only authorized users are permitted access. Users may also apply Application Layer or Network Layer authentication and encryption as required, but this is opaque to the service providers.

5.3.3 SSI-SPECIFIC CSSE BUILDING BLOCKS

5.3.3.1 Overview

The following subsections briefly describe each specialized SSI CSSE physical node, its role, and how it interconnects with the other CSSEs and user nodes. Each of these building blocks provides a nominal set of interfaces, either over a space link (typically RF) or over some sort of terrestrial link, or both. They also provide required functionality such as 1) Network Layer processing (routing, forwarding, gateway, and security functions), 2) store-and-forward data handling, 3) Link Layer processing, 4) RF transmit/receive functions, and 5) service management, network control, and routing exchange/peering functions. They may also implement last-hop essential commanding and emergency mode functions and first-hop data return functions.

Table 5-3 provides an overview of the SSI CSSE node types, their interfaces, and their functions. Not all nodes will support all functions and interfaces, but each SSI building block will at least support DTN or IP (or both) Network Layer functions.

Table 5-3: SSI CSSE Node Types, Interfaces, and Functions

CSSE/Building Block	Terrestrial Links	Space Links	Proximity Links	Space Link Control	Routing
ESLT	X	X		X	X
Earth Routing Node	X			X	X
Space Routing Node		X	X	X	X
PSLT		X	X	X	X
Earth WAN Routing Node	X				X
Planet WAN Routing Node	X				X
Hybrid Science/Routing Node		X	X	Varies	X

In order to directly control any SSI node, particularly in the case of emergency or ‘back door’ management access, it is assumed that simple Link Layer command delivery and telemetry functions are available that will operate even if the SSI components are not operational. This direct control capability is provided by the specialized last-hop delivery functions. This method permits an SSI node that has a fault to be commanded to 'reboot' using only standard Link Layer functions, and it permits control and rebooting of the SSI routing functions as well. These network management interfaces will be secured. (See 6.5.3.1 for more details on this service.)

5.3.3.2 SSI Earth-Space Link Terminal

The SSI ESLT includes all of the ABA functions described earlier as well as those required to provide SSI services.

An SSI ESLT provides network connections over a space link so that IP and BP traffic is routed between SSI Earth and Space User Nodes, as shown in figure 5-6. The ESLT encapsulates BP bundles and/or IP datagrams destined for space into frames that are multiplexed into the frame stream in the space link, encoded and modulated to RF, and radiated toward the next space routing node in the SSI. The SSI requires full Network Layer functionality to be implemented at the ESLT, including the selection of the next-hop space routing node. This involves pointing of directional antennas, selection of appropriate spacecraft identification attributes and Link Layer configurations, and may involve cryptographic operations that are specific to the target spacecraft.

On the return side, the SSI ESLT receives and demodulates RF signals from Space User Nodes; frame syncs, decodes, and extracts frames from the link; and authenticates, decrypts, de-multiplexes, and de-encapsulates IP datagrams and BP bundles destined for terrestrial SSI nodes. In the case of BP, the ESLT may also act as an intermediary storage point for bundles (forward and/or return) and may assume custody of bundles. The SSI would identify these services in the SLA that specifies the services provided to a particular mission.

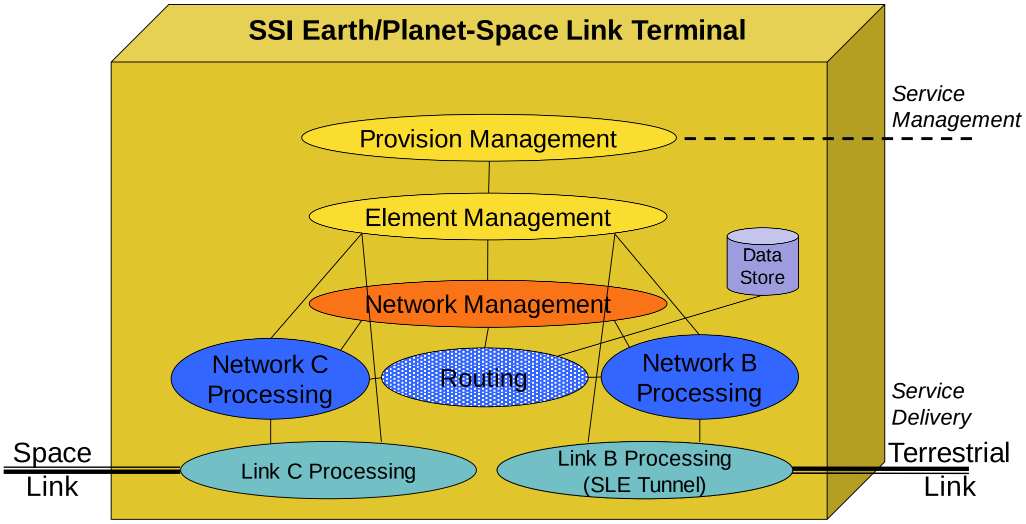


Figure 5-6: Earth/Planet-Space Link Terminal

In the context of the SSI, the ESLT establishes and maintains network connections with space routing nodes, PSLTs, and directly with SSI-compliant user nodes (either user spacecraft or landed assets). The ESLT has terrestrial interfaces that use suitable link protocols and support SLE and CSTS traffic (shown as 'SLE Tunnel') and also SSI traffic. The SSI ESLT also has a service management interface that is typically controlled by the Earth User Node that is responsible for managing the space link to the next-hop space routing node.

Security policies might dictate the use of BSP to provide bundle security or IPsec to provide Network Layer security.

5.3.3.3 SSI Earth Routing Node

Terrestrial SSI traffic may also make use of an SSI Earth routing node (router), shown in figure 5-7, as a means for routing SSI data among other user nodes on the surface of the Earth. In reality, this exact same node type, with either 'terrestrial' or space links, may exist as a routing node in any location remote from Earth where routing functions are required. Any of the user nodes may include all of these SSI network and routing functions, and they may also include Application Layer functions as well. Application functions might include standard file and/or message transfer functions (CFDP and AMS), the CXFS, or a variety of mission operations functions.

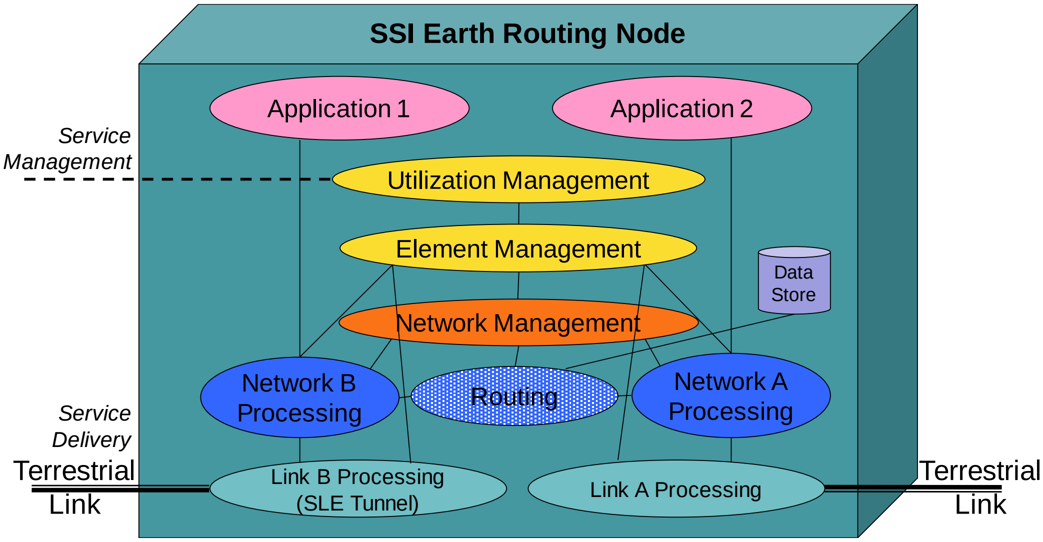


Figure 5-7: Earth Routing Node

Both of the links for the Earth routing node are shown as terrestrial links. If the space routing node MOC also serves as an Earth routing node (not required, but possible), one of the links might use an SLE tunnel to access the SSI ESLT in order to control the space link to the space routing node. The space routing node MOC is expected to always be the node that controls the space link to the space routing node and to manage the operations of that node, but it need not embody all of the other routing-node functions, nor does it necessarily provide SSI routing and other services for other users.

5.3.3.4 SSI Space Routing Node

The SSI space routing node performs routing and storage functions for BP/IP traffic over 'long haul' (i.e., AOS/telemetry/telecommand) space links, proximity space links, or spanning proximity links, as shown in figure 5-8. In the context of the SSI, a space routing node may establish space links with ESLTs, other space routing nodes, PSLTs, and directly with user nodes (either user spacecraft or landed assets). Security policies might dictate the use of BSP to provide bundle security or IPsec to provide Network Layer security.

Because IP requires continuous connectivity from source to destination during any end-to-end transfers, an IP-enabled space routing node must maintain contemporaneous space links with at least two other SSI nodes simultaneously, but may maintain more depending upon the end-to-end path.

A BP-enabled space routing node requires a minimum of a single space link to another SSI node at some time (although there is no requirement to have a space link operational at *all* times), over which stored bundles may be sent and are received for subsequent storage and transfer. If space links with other SSI nodes are available contemporaneously, a routing node may route bundles to their next hops without using intermediate storage. BP-enabled space routing nodes may assume custody of bundles, as controlled by the relevant SLAs in force. Routing policies may be used to manage QoS and autonomous data forwarding when links are available.

In addition to its primary routing functions, a space routing node may also host one or more BP or IP user nodes (e.g., science applications), in which case the routing node not only serves to route/store/forward traffic from other nodes, but is itself a source and/or destination of BP/IP traffic. This is similar to the hybrid science/routing node that is described later in 5.3.4.4.

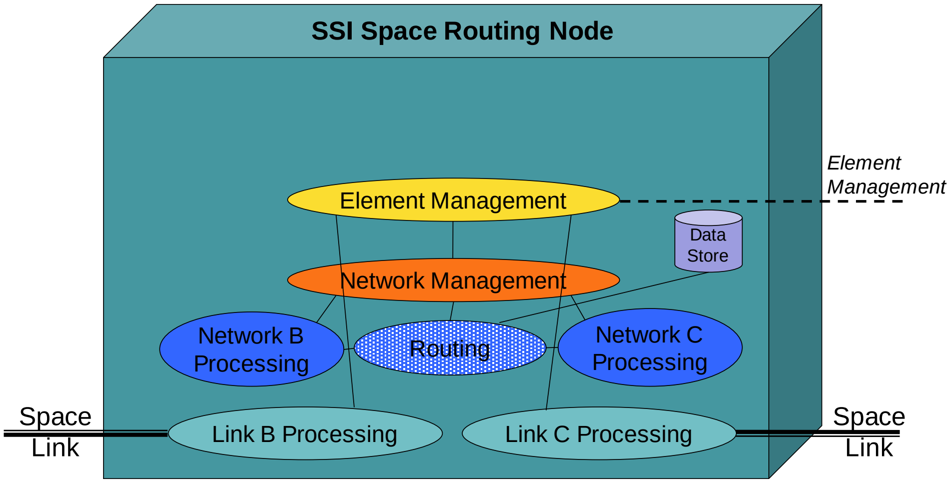


Figure 5-8: Space Routing Node

NOTE – Space routing nodes are only required to have EM and routing functions. They need to provide no other applications except last-hop/first-hop services. (See figure 5-9 for that.)

Space routing nodes should also implement emergency commanding and other last-hop specialized delivery functions, as shown in figure 5-9. These functions will be offered in addition to the normal routing, storage, and data-forwarding functions.

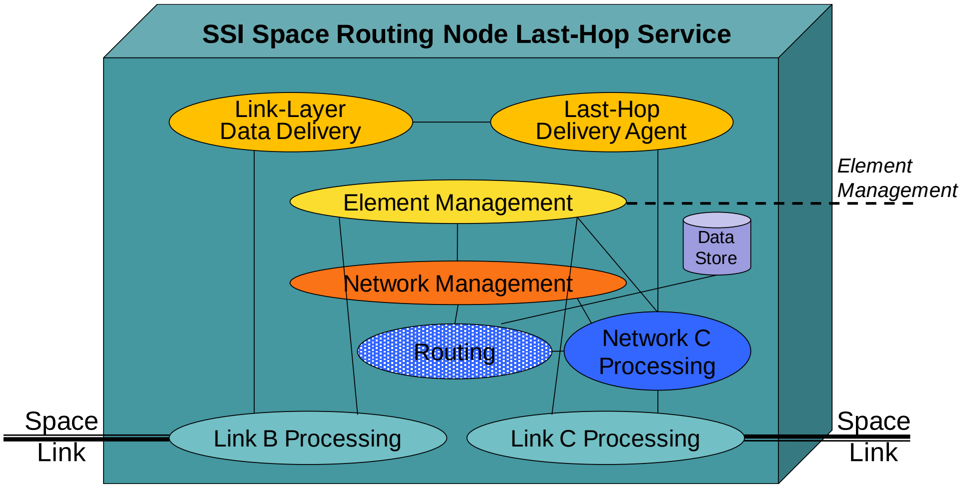


Figure 5-9: Space Routing Node with Last-Hop Service

5.3.3.5 SSI Planet-Space Link Terminal

A PSLT is essentially the same as an ESLT (see figure 5-6). It is located on the surface of some remote planetary body and provides the space link over which BP and IP traffic is routed between a planetary WAN and any other nearby or distant space or terrestrial SSI nodes.

A PSLT provides many of the same functions as the ESLT, in that it 1) encapsulates and multiplexes BP bundles and/or IP datagrams destined for space into a symbol stream that is modulated to RF and radiated toward the next Space User Node in the SSI, and 2) receives and demodulates RF signals from Space User Nodes and de-multiplexes and de-encapsulates IP datagrams and BP bundles destined for terrestrial SSI nodes. In those cases where a single PSLT maintains multiple concurrent space links to different destinations, it will also perform a routing function to place the datagrams/bundles on the appropriate space links; it may also do routing to one or more planetary WAN links. It may also provide SLE/CSTS services to local users and Network Layer security services. In the case of BP, the PSLT will also act as an intermediary storage point for bundles and may assume custody of bundles, as controlled by the relevant SLAs in force.

A PSLT may establish and maintain space links with some or all of the following 1) space routing nodes (using proximity protocols or AOS/TC/TM), 2) ESLTs (using AOS/TC/TM), 3) other user nodes on the surface of the planet (using BP or IP over ‘terrestrial’ links deployed on the planet), or 4) directly with Space User Nodes on mission spacecraft. A PSLT could also offer SLE/CSTS service interfaces to ‘local’ users on a remote planet who manage nearby SSI (or ABA) space routing nodes.

5.3.3.6 SSI Earth WAN Routing Node

An SSI Earth WAN consists of one or more routing nodes that provide Network Layer connectivity among terrestrial SSI user nodes and ESLTs. In addition to the transport of ‘data’, the WAN may be used to transport voice and video, which can require specialized handling because of latency and jitter considerations. The WAN provides the connectivity over which DTN bundles/IP packets are exchanged among terrestrial nodes and ESLTs. Routing nodes in a BP-enabled WAN also typically will contain a data store, but this is not always required.

Figure 5-10 shows just one such routing node. In this figure, WAN routing nodes are treated as infrastructure, but it is important to understand the functions that they require. They may be implemented as separate components or the functions could be implemented within a workstation or other component that has adequate processing, interface bandwidth, and storage resources.

These SSI WAN routing nodes are in many senses nearly identical to existing Internet routers, in that they are intended to perform only Network Layer functions in support of user applications, and typically host no applications themselves. SSI BP routing nodes deployed on Earth will include the BP processing and routing functions, associated BP network management functions, optional BP security functions (i.e., BSP), and also will include a data store that is required to support the BP protocols. These nodes may also use the TCP/IP or User Datagram Protocol (UDP)/IP protocols as a ‘virtual link’ protocol under BP. (For a deeper treatment of protocol issues see sections 6 and 7.)

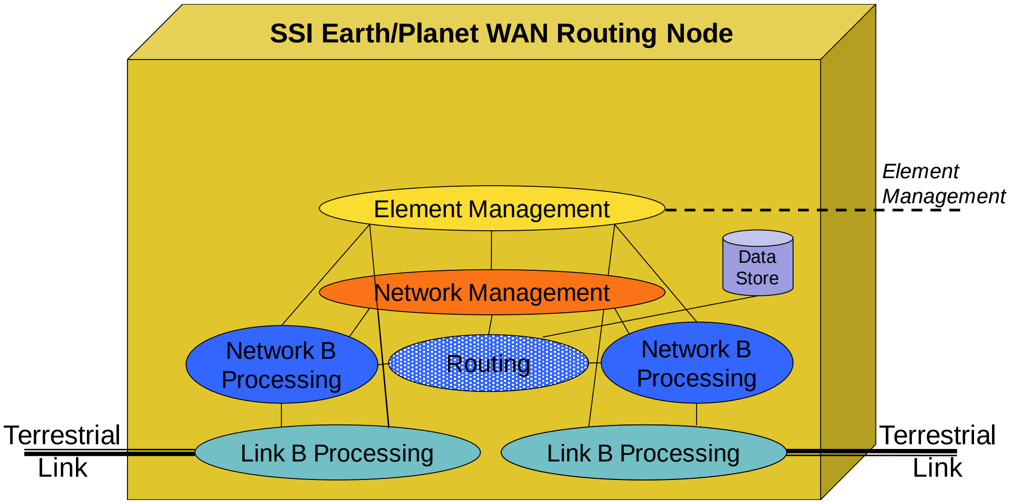


Figure 5-10: Sample Earth/Planet WAN Routing Node

5.3.3.7 SSI Planet WAN Routing Node

An SSI planet WAN is essentially the same as an SSI Earth WAN; i.e., it provides Network Layer connectivity among planet SSI user nodes and PSLTs. In addition to the transport of data, the WAN may be used to transport voice and video (e.g., Voice Over Internet Protocol [VOIP]). Planet WANs may use either IP or BP as the basis for their Network Layer connectivity.

A planet WAN interfaces with planet SSI user nodes and other SSI elements via gateway routers, through which Network Layer traffic enters and leaves the WAN. The planet WAN provides and enforces the provisions of the controlling SLAs regarding QoS for the traffic it transports. Nodes in a BP-enabled planet WAN may also contain a data store, but this is not always required, especially if continuous connectivity to the nodes it serves can be assured.

5.3.4 SSI-SPECIFIC USER NODE TYPES

5.3.4.1 Overview

The following subsections briefly describe each specialized SSI UE physical node, its role, and how it interconnects with the CSSEs. Each of these UEs provides a nominal set of interfaces, either over a space link (typically RF) or over some sort of terrestrial link, or both. They also provide required functionality such as 1) Network Layer processing (routing, forwarding, security, and gateway functions), 2) store-and-forward data handling, 3) Link Layer processing, and 4) RF transmit/receive functions. These interfaces and functions are essentially the same as those described in figure 5-5.

Table 5-4 provides an overview of the specific SSI UE node types, their interfaces, and their functions. A more detailed description of all of these user nodes and their allocated functions follows.

Table 5-4: SSI UE Node Types, Interfaces, and Functions

UE	Terrestrial Links	Space Links	Proximity Links	Space Link Control	Routing
Earth User Node	X				X
Space/Planet User Node			X		X
Hybrid Science/Routing Node		X	X	Varies	X

User nodes that participate fully in the SSI will directly implement a fully functioning version of the Network Layer protocols, but will not necessarily provide the resources nor the full routing, forwarding, security, and management functions to provide services to other nodes. They must, however, implement enough of the routing functionality to be able to identify and route to the next hop node that provides full SSI services.

Any end-user node that does implement routing and forwarding, in addition to other typical user/science functions, could function as a hybrid science/routing node, as described in 5.3.4.4. As such, these hybrid nodes perform both as SSI user nodes and as SSI CSSEs.

5.3.4.2 SSI Earth User Node

An SSI Earth User Node is provided service by the SSI-SP element (or terrestrial WAN) to which it is directly attached, as shown in figure 5-11. The Earth User Node may attach only to a terrestrial (or planetary) WAN, or it may connect to an ESLT. A Space User Node is similar in that it may connect to a planetary WAN, a PSLT, or a space routing node.

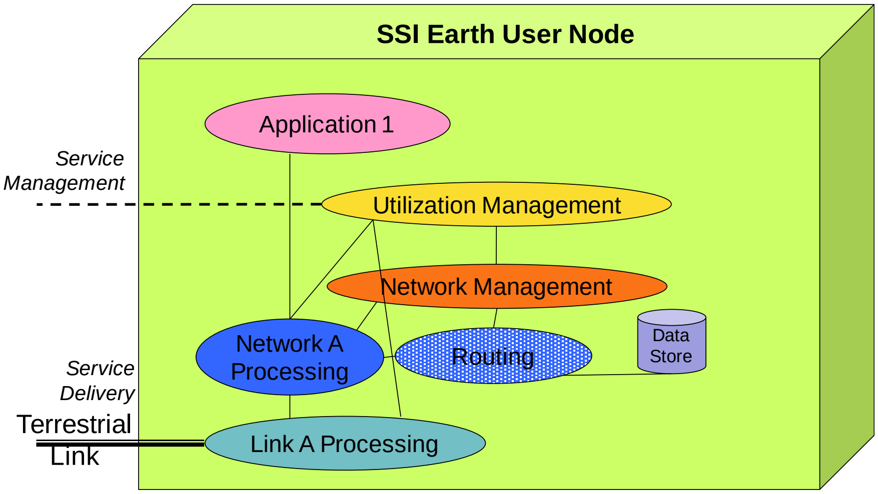


Figure 5-11: Earth User Node

A user node may have one or more SSI-SP access links, but only one is shown in figure 5-11. User nodes are the only types of elements where a user application, or Application Layer service is always expected to appear. User nodes may host many functions in the support of their science goals; however, only those relevant for the SSI are shown. While CSSE nodes *may* host other functions, their primary purpose from the point of view of the SSI is to provide space internetworking services.

5.3.4.3 SSI Space/Planet User Node

Figure 5-12 shows a Space/Planet user node that only has a connection via a space link to some other SSI-SP space-communications asset. This is representative of space assets that primarily communicate either to a space routing node, such as a lander or rover, or to an SSI ESLT or PSLT as described in 5.3.3.5. A variation of this same Space User Node might only have a connection via a terrestrial or planetary WAN. This is representative of a user asset that primarily communicates either via a terrestrial or planetary WAN or to an ESLT/PSLT. The upper-level and internetworking functionality is the same in either case; what changes are the lower-level Physical Layer and Link Layer protocols that are required.

The application function shown in figure 5-12 may be any of a variety of functions that directly utilize the SSI Network Layer protocol, or that bypass that and operate directly on the data at a link level. This may include specialized functions making direct access to the space Link Layer, such as hardware commanding, frame functions, and VC functions.

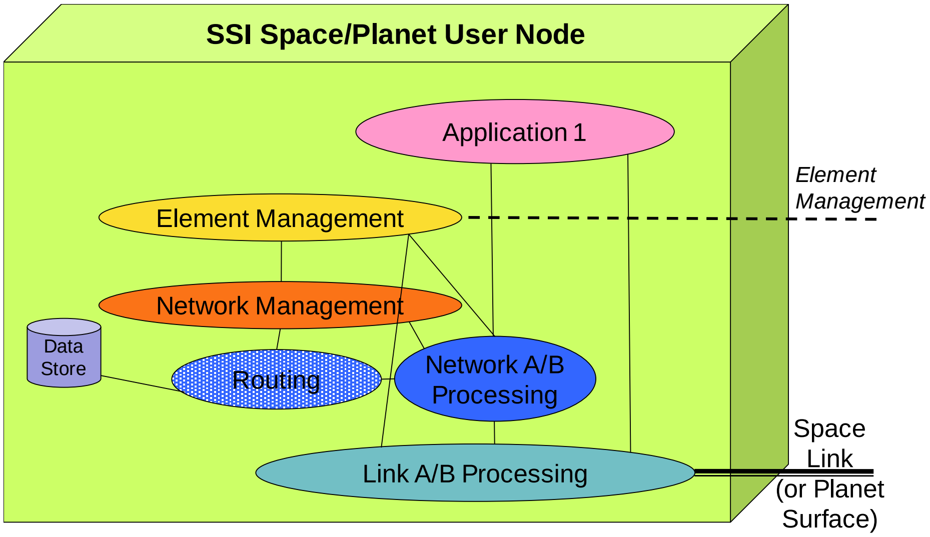


Figure 5-12: Space User Node Connected via a Space or Planet Surface Link

5.3.4.4 SSI Hybrid/Science Routing Node

In the SSI, especially during the early deployment phase, many elements of the system may be hybrid in nature, primarily providing science operations, but also offering SSI routing functionality. Figure 5-13 depicts this by showing all of the functionality already familiar from the space routing node figure (figure 5-8), but also including Application Layer services and user applications.

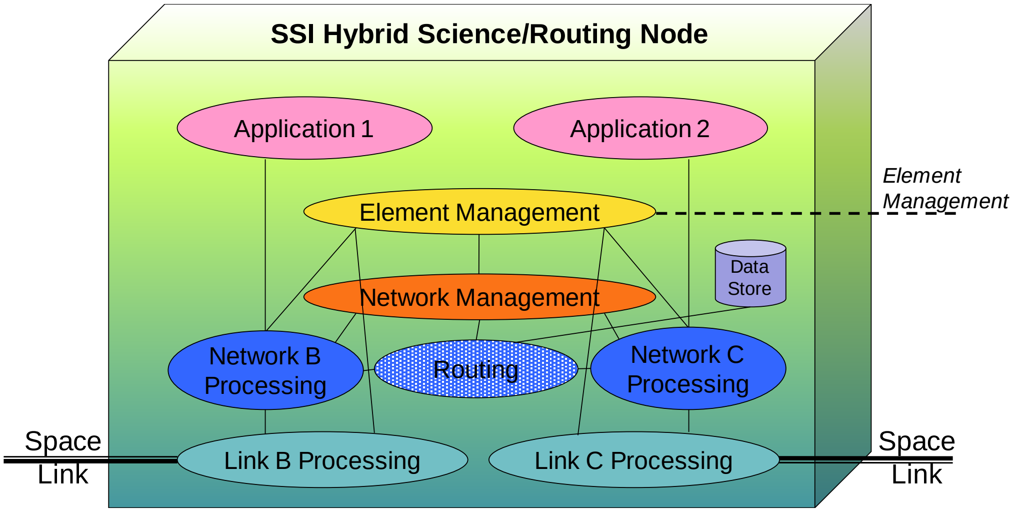


Figure 5-13: Hybrid Science/Routing Node

A hybrid node will often have a primary mission to perform science, but will host SSI routing-node functions as a support activity, with some modest (or significant) allocation of resources. Once their primary science mission is complete, it is also possible for nodes with this configuration to be repurposed to provide SSI routing service as a primary function during the remainder of an extended mission lifetime. In this way the SSI can be built up and extended without requiring dedicated investments in SSI infrastructure.

5.4 SECURITY CONCEPTS FOR PHYSICAL VIEW

The system elements that provide user services typically will be secured physically. The following physical security methods are likely to be employed at service system boundaries:

- operational systems will be within a secure physical perimeter;
- only approved and trained staff will be allowed physical access to operational systems;
- appropriate credentials and vetting will be required to gain access to operational facilities;
- isolated LANs and firewalls are likely to be used to secure the operational systems;
- operational systems may be configured to only be accessible via proxy agents or a ‘demilitarized zone’ (DMZ).

The security documents (references [7] and [22]) provide more details about security and threat analysis. Elements located in space typically will be secured by various encryption algorithms and protocols that will be described in more detail in section 6.

6 COMMUNICATIONS VIEW

6.1 GENERAL

This view describes communications protocols used for accessing space communications cross support services that are provided by CSSSes and CSSEs. Its focus is on the protocol stack details of the communications interfaces that define the binding points between the CSSEs and UEs.

The communications protocols used for accessing a space communications cross support service are determined by the nature of the cross support service, the kinds of interface binding points that are supported, and where the service elements are located. For example, for a space link service to deliver telemetry frames from a Space User Node to an Earth User Node using an ESLT, the CCSDS telemetry or AOS Space Data Link Protocol (reference [34] or [12]), appropriate coding, and one of the CCSDS RF and modulation Recommended Standards (reference [23]) will be used on the space interface (that is, on the link between the Space User Node and the CSSE). The interface that delivers those frames to the Earth User Node will use SLE or CSTS and terrestrial link protocols, and data may flow over a WAN. Because of these different interfaces, the appropriate set of communications protocols must be specified for each interface of each CSSE.

Section 4 (Service View) introduced the notion of an interface binding signature for service elements. This section focuses on how the communication protocols that implement those interfaces are used to transport data among system elements. It focuses particularly on the stacks of protocols that are appropriate in different system deployments and how they support the various offered services. These are presented here as protocol building blocks that are appropriate for different elements and the services they consume or provide. This section introduces some abstract views of end-to-end protocol chains; specific end-to-end recommended protocol deployments will be described in detail in section 7.

This section does not attempt to provide concrete guidance for the selection of specific modulation, coding, or Link Layer standards for any particular application. That is a deep technical subject and there are CCSDS documents that provide excellent overviews. The reader is directed to the Overview of Space Communications Protocols (OSCP) (reference [10]), TM (and TC) Synchronization and Channel Coding (reference [24]), Bandwidth-Efficient Modulations (reference [23]) and the other technical standards to which they refer.

6.2 OSI PROTOCOL STACK AND LAYER DEFINITIONS

6.2.1 GENERAL

Protocol configurations are usually described as a stack of protocols, showing how the functions at the various layers, from Physical Layer through Application Layer, are provided. Figure 6-1 shows an abstract view of the nominal OSI protocol stack as defined within the CCSDS standards suite. As in many terrestrial applications, some of the layers in the full OSI stack have been left out (Session, Presentation), and some new functions derived from the

Physical Layer (radiometric, time) have been added. Not shown explicitly is the further distinction that is usually made for space link communications that separately treats coding and synchronization as the sublayer at the ‘bottom’ of the Link Layer, modulation as the ‘top’ part of the RF Physical Layer signaling, and the relevant RF (or future optical) frequency spectrum (the rest of the Physical Layer). The protocol data types associated with each layer are shown in dashed boxes.

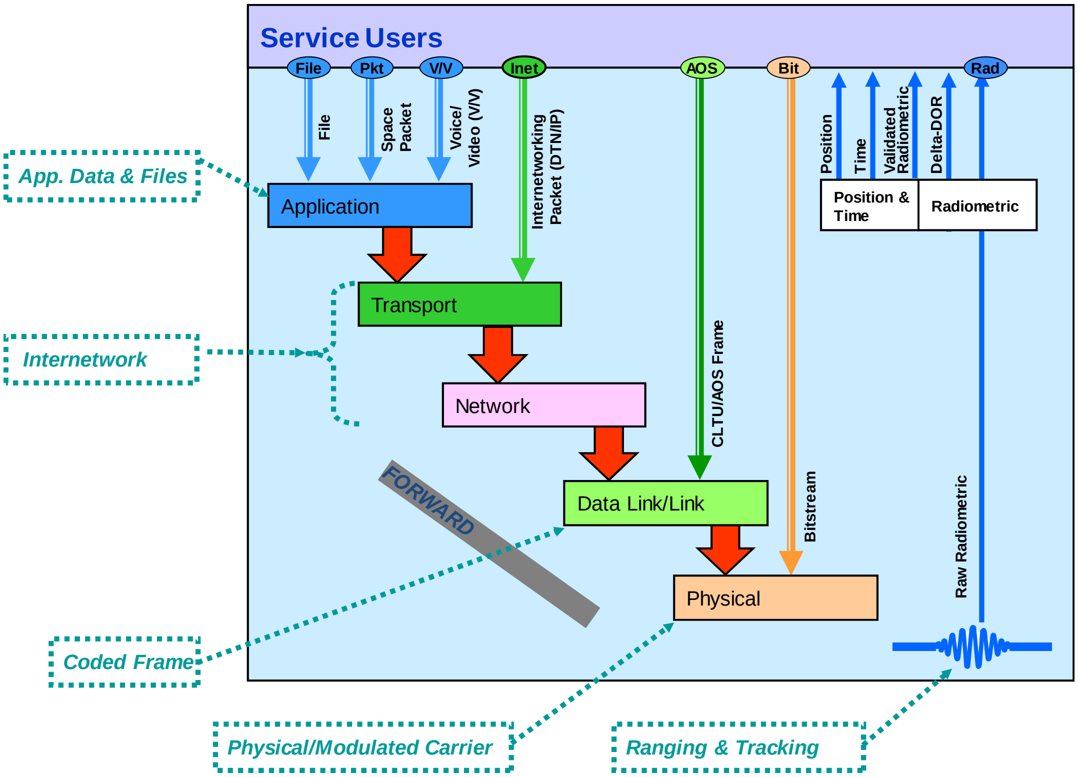


Figure 6-1: OSI Protocol Stack, with Notes Showing Data at Each Layer

The definitions of the layers used throughout this document are derived directly from the OSI Basic Reference Model (reference [5]), modified slightly to align with CCSDS terminology. The Session and Presentation layers are left out, although they do often have an identifiable role within systems. There is also a corresponding ‘return’ stack that is not shown in this figure.

The following subsections define the functions at each layer and then use these to provide protocol stack building-block diagrams showing use of these protocol layers. For the basic ABA Link Layer deployments, there will not be a Transport or Network Layer, as user applications interface directly either to application services (file or message) transfer, or to the Link Layer itself. For the SSI configurations, the Transport and Network Layers will be used to do routing and end-to-end delivery.

6.2.2 APPLICATION LAYER

The Application Layer (Layer 7) contains all those functions that imply communication between open systems that are not already performed by the lower layers. These include functions performed by programs as well as functions performed by human beings. An application entity can be structured internally into Application Layer objects representing groups of functions. The Application Layer may provide security services such as authentication, integrity, and confidentiality either in addition to or as a replacement for any such services provided at lower layers.

6.2.3 TRANSPORT LAYER

All protocols defined in the Transport Layer (Layer 4) have end-to-end significance, where the ends are defined as transport entities. The Transport Layer is relieved of any concern with routing and relaying since the Network Layer provides data transfer from any transport entity to any other across subnetworks. The Transport Layer provides transparent transfer of data between applications and relieves them from any concern with the detailed way in which reliable and cost-effective transfer of data is achieved.

6.2.4 NETWORK LAYER

The Network Layer (Layer 3) provides transport entities independence from routing and relay considerations. It provides the means to establish, maintain, and terminate network connections between open systems containing communicating applications and the functional and procedural means to exchange network service data units between transport entities over network connections. The Network Layer may also provide security services such as authentication, integrity, and confidentiality.

6.2.5 DATA LINK LAYER

6.2.5.1 General

The Data Link Layer (or simply ‘Link Layer’) (Layer 2), provides functional and procedural means for a connectionless or connection-oriented mode for the establishment, maintenance, and release of data link connections among Network Layer entities and for the transfer of data link service data units. A data link connection is built upon one or several physical connections. The Data Link Layer detects and possibly corrects errors that may occur in the Physical Layer (see ‘Coding and Synchronization Sublayer’). The Data Link Layer may also provide security services such as authentication, integrity, and confidentiality.

6.2.5.2 Coding and Synchronization Sublayer

The CCSDS Coding and Synchronization Sublayer (of the Link Layer) specifies methods of synchronization and channel coding for transferring transfer frames over a space link. It provides error detection and correction for the space Data Link Layer protocols and deals with noisy, low SNR, space link physical channel characteristics.

6.2.6 PHYSICAL LAYER

The Physical Layer (Layer 1) provides the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for bit transmission between Data Link Layer entities. The Physical Layer provides for the transparent transmission of bit streams between data link entities across physical connections. The services provided by the Physical Layer are determined by the characteristics of the underlying medium and are too diverse to allow categorization, but the CCSDS includes modulation and ranging as functions of the Physical Layer. The Physical Layer may also provide security services such as authentication, integrity, and confidentiality.

6.3 SPECIFIC PROTOCOLS FOR SERVICE INTERFACE BINDING

6.3.1 GENERAL

In 4.5 a variation of figure 6-2 (see figure 4-8) was used to describe the role of protocols in supporting the binding to external interfaces of services. In this section the focus is on the protocol stacks themselves; the nature of the services and what they do is secondary. Figure 6-2 begins to describe in more detail the actual protocol stacks that provide the communications. One set of communications protocols is used to support interactions between the space user’s service utilization and the ESLT space data link service production, and another set is used between the ESLT cross support service provision and the UE’s service utilization. The logical flow of information is across the dashed line from the Earth to space user applications; the actual flows of application information end-to-end occur along the solid black lines and go through protocol processing and encapsulation at each layer.

Each cross support service uses a set of communications protocols that is determined by the nature of the service, the locations of the physical elements (the CSSE and the Earth and Space User Nodes), and the characteristics of the physical links between the physical elements.

Each service interface used to support a space communications cross support service is characterized by a set of standard communications attributes defined in a service catalog (reference [3]).

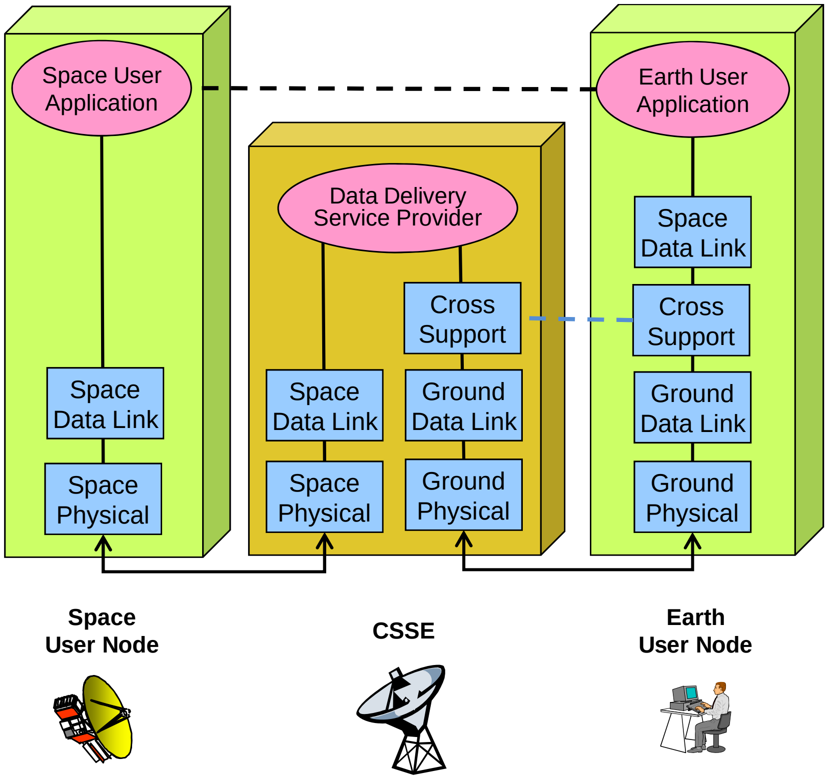


Figure 6-2: Generic Communications Protocols to Support a Service

6.3.2 EXAMPLE COMMUNICATION PROTOCOLS

Table 6-1 lists the most common examples of communications protocols used to support space communications cross support services. CSSSes and CSSEs may use other communications protocols that are not listed in this table.

The ABA Link Layer configurations use only the first four sections of table 6-1; the SSI configurations use one or both of the last two sections and also the Physical Layer through Link Layer protocols specified in the first three sections of the table. For ABA configurations the Application Layer protocols will be implemented directly on the Link Layer, using a ‘shim’ such as Space Packet Protocol (SPP) (reference [26]) or Encapsulation Packet (EP) (reference [25]). For the SSI, the Application Layer protocols will be implemented on top of the Network Layer protocols instead of on the Link Layer protocols.

Table 6-1: Example Communications Protocols

Physical Link Type	Communications Protocol	Reference
Onboard Links	MIL-STD-1553B	MIL-STD-1553B [28]
	SpaceWire	ECSS-E-50-12C [29]
Proximity Links	Proximity-1 Space Link Protocols: Data Link Layer, Physical Layer, Coding and Synchronization Sublayer	CCSDS 211.0-B-4, [30] CCSDS 211.1-B-3, [31] CCSDS 211.2-B-1 [32]
Space-to-Ground Links	Radio Frequency and Modulation Systems	CCSDS 401.0-B-22 [23]
	TC Synchronization and Channel Coding	CCSDS 231.0-B-2 [11]
	TM Synchronization and Channel Coding	CCSDS 131.0-B-1 [24]
	TC Space Data Link Protocol	CCSDS 232.0-B-1 [33]
	TM Space Data Link Protocol	CCSDS 132.0-B-1 [34]
	AOS Space Data Link Protocol	CCSDS 732.0-B-2 [12]
Application Layer Protocols	Space Packet Protocol	CCSDS 133.0-B-1 [26]
	CCSDS File Delivery Protocol	CCSDS 727.0-B-4 [35]
	Asynchronous Message Service	CCSDS 735.1-B-1 [36]
DTN Internetworking Protocols	Bundle Protocol Specification	RFC 5050 [37]
	Licklider Transmission Protocol	RFC 5326 [38]
	Bundle Security Protocol	RFC 6257 [39]
	Contact Graph Routing Protocol	Burleigh, NASA Tech Brief [21]
	Delay Tolerant Network Management Protocol	Birrane, Ramachandran, Proposed Internet Draft [40]
IP Internetworking Protocols	Internet Protocol	STD 5 [41]
	Transmission Control Protocol	STD 7 [42]
	File Transfer Protocol (FTP)	STD 9 [43]
	Security Architecture for the Internet Protocol	RFC 4301 [44]

6.3.3 EXAMPLE CROSS SUPPORT PROTOCOLS

Table 6-2 lists some typical cross support protocols that are used between the Earth User Node and the ESLT CSSE. Other protocols may be used in addition to these.

Table 6-2: Example Cross Support Protocols

Cross Support Link Type	Cross Support Protocol	Reference
Space Link Extension Forward	SLE F-CLTU	CCSDS 912.1-B-3 [45]
	CSTS F-Frame	CCSDS White Paper [46]
Space Link Extension Return	SLE Return All Frames	CCSDS 911.1-B-3 [47]
	SLE Return Channel Frames	CCSDS 911.2-B-2 [48]
	SLE Return Operational Control Fields	CCSDS 911.5-B-2 [49]
	Return Unframed Telemetry CSTS	CCSDS White Book [50]
Application Layer Protocols	Tracking Data CSTS	CCSDS White Book [51]
	CSTS Transfer File	CCSDS White Paper [52]
	Monitored Data—CSTS	CCSDS White Book [53]
	Service Control CSTS	CCSDS White Book [54]
Service Management	SCCS Service Management	CCSDS 910.11-B-1 [14]
	XML Specification for Navigation Data Messages	CCSDS 505.0-B-1 [55]
	Functional Resources for Cross Support Services	CSSA-CSS_FRs_TN-0.01 [65]

NOTE – All documents with a specific assigned numbers are existing published standards at the time of writing, but several others are currently in development as White Papers (concept papers) or White Books (early drafts of standards). Check the ccsds.org website for the current versions of any of these items.

6.4 BASIC END-TO-END PROTOCOL OPERATION

6.4.1 ABA PROTOCOL OPERATIONS

ABA protocol stacks are intended to provide end-to-end flows of Link Layer data and the application data they carry. The usual communications stack transports space link frames constructed by the user MOC to the Space User Node using an ESLT that provides space communications and cross support services. The space link itself will typically use CCSDS telecommand, telemetry, and/or AOS protocols, along with a variety of underlying coding, modulation, ranging, and frequency choices. Standard references (see the protocol list in table 6-1) should be consulted for the details of all of these, the supporting protocols, and applicable combinations. Supporting lower-layer protocols may include ranging, MSPA, and security. Applicable upper-layer protocols may include file delivery (CFDP), SPPs or encapsulation packets (EPs) and path IDs, or private applications protocols that run over space link frames or packets.

NOTE – The coding, modulation, and Physical Layer (frequency) choices are below the level that this document will address. Consult the OSCP (reference [10]) and other related references (references [23] and [25]) and for this discussion.

A nominal end-to-end set of nodes and typical protocol layering for the ABA configuration is shown in figure 6-3. There are several points to note about this figure:

a) Although the ABA configurations support applications, the applications themselves and the protocols they use to communicate are outside the scope of the ABA space link cross support. Current telemetry and telecommand applications, as well as more complicated applications such as file or message transfer (e.g., CFDP or AMS) can be implemented on top of any ABA space Link Layer.

b) User applications exist only at the ‘ends’ of communication and rely on the ESLT for data communications. No user-specific capabilities are implemented in the ESLT, although some ESLTs may offer file-delivery capabilities.

c) User-Application Layers are implemented on top of Data Link and Physical Layers, and the lower layers must be standardized for interoperability. There is a firm requirement for elements at each end of the link to use the same protocols, but each hop may use different link protocols.

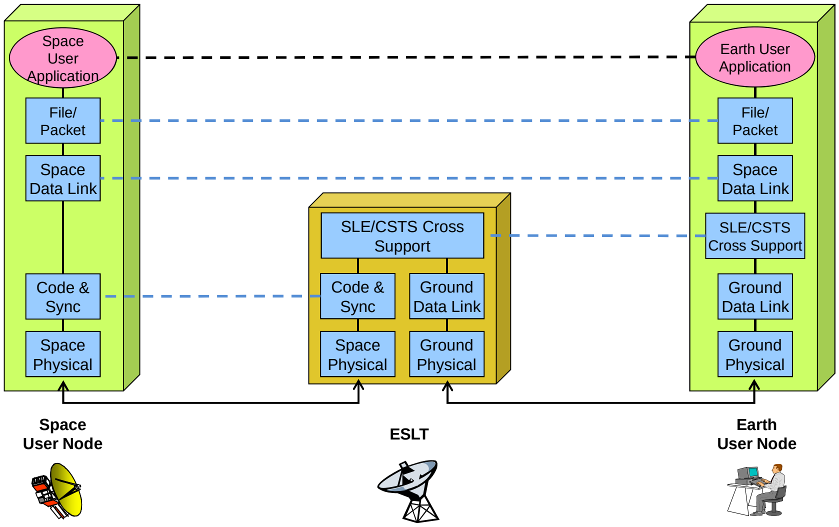


Figure 6-3: Typical ABA Protocol Layering

The current SLE services are asymmetric in that the forward path contains a single stream of encoded space link frames produced by the Earth User Node, but the ESLT space link provider does the decoding of the return path. The stream sent to the users contains either all of the space link frames or just a subset of those frames. A new CSTS F-Frame service is in development that will make this space link ‘tunnel’ service symmetric, accepting space link frames from the user and encoding them in the ground station. This new service will permit AOS synchronous links to be used in the forward direction and will also permit data from more than one source to be multiplexed. The current F-CLTU offers no such services. This new F-Frame service is also completely applicable for SSI configurations.

NOTE – There is an existing experimental specification, the *Space Link Extension—Enhanced Forward CLTU Service Specification*, CCSDS 912.11-O-1 (reference [56]), that provides a forward service for both AOS and TC frames and can do encoding in the ground station. This is an available precursor to the CSTS F-Frame service listed in table 6-2 for those networks that require an AOS forward service.

Figure 6-4 shows the protocol stack that permits the UM function in the Earth User Node to communicate with the PM function in the ESLT. The protocol stack uses the service management protocol, which defines eXtensible Markup Language (XML)-formatted messages and interaction patterns, on top of a secure HTTP protocol that itself uses standard terrestrial Internet and data link connections. This is shown as a shared link with the cross support data delivery services. In reality it may be a separate link.

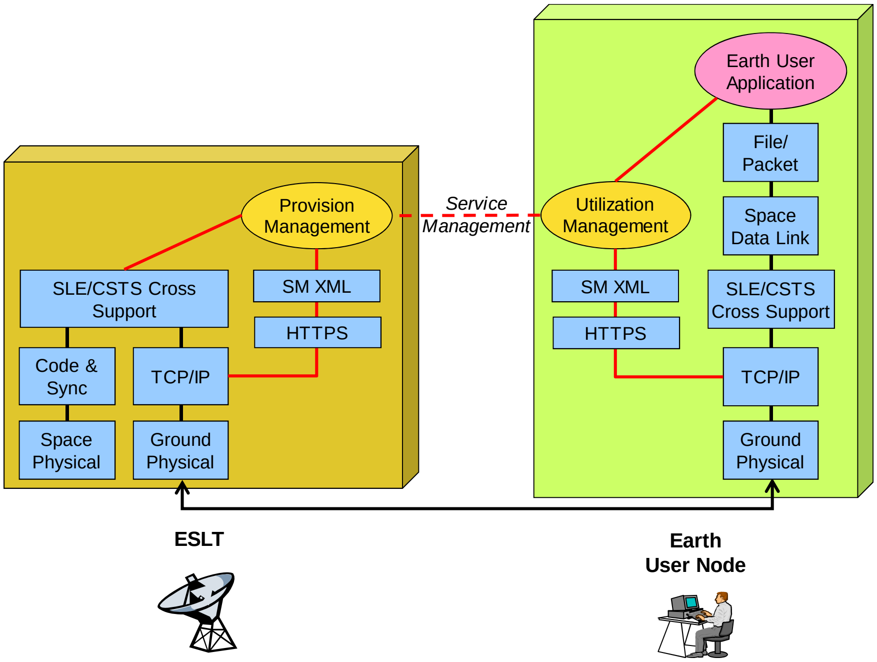


Figure 6-4: ABA Service Management Protocol Layering

6.4.2 SSI PROTOCOL OPERATIONS

The SSI protocol stacks use exactly the same Link Layer protocols described for the ABA configurations, but add Network and Transport Layer protocols. Where the ESLT explicitly offers SSI services, these protocols will all be implemented in the ground station. There are two Network Layer protocols currently envisioned for the SSI: the *CCSDS Bundle Protocol Specification* (reference [66]) (and when required *Streamlined Bundle Security Protocol for CCSDS*, reference [67]), and the IP as specified by STD 5 (reference [41]) (and when required RFC 4301, reference [44]). IP is appropriate for fully connected environments with short transmission delays and continuous connectivity, regardless of the number and types of links in network paths. DTN is applicable for all space internetworking applications. Because of this it is preferentially used in this section.

NOTE – The Internet Protocol Suite (IPS) actually defines a whole range of protocols to accomplish reliable transfer, routing, management, and ISP peering, but the full description of this is beyond the scope of this document; external references can be consulted for IP and its supporting protocols.

DTN also uses a suite of protocols, including routing, security, and management, and the primary Network Layer protocol is BP. BP is required for use in environments where it may not be possible to form and maintain fully connected paths and where long delays and disconnections are the norm, but it may be used in any space communications deployment requiring a Network Layer service. The supporting protocols in both suites are generally omitted from the diagrams in this section for clarity, but both primary network protocols include protocols for routing, management, reliable data delivery, signaling, reporting, and security.

The basic SSI protocol layering and end-to-end configuration for the SSI is adapted from the OSI standard model, as shown in figure 6-5. There are several points to make about this figure:

a) While the SSI supports applications, the applications themselves and the protocols they use to communicate are outside the scope of the SSI. Current telemetry and telecommand applications, as well as more complicated applications such as file or message transfer, e.g., the CFDP (reference [35]) or AMS (reference [36]), can be implemented on top of either SSI Network Layer.

b) User applications exist only at the ‘ends’ of the communication path and rely on the network for data communications. No user-specific functions are implemented ‘in the middle’ of the network.

c) Network Layers are implemented on top of Data Link and Physical Layers; for interoperability there is a need to standardize the lower layers between successive subnets. There is no requirement for the same Data Link Layer to be used end-to-end.

None of the diagrams in this subsection makes direct reference to SLE or CSTS protocols; the focus is entirely upon the Network Layer protocols, but SLE and CSTS do have a fundamental role. Section 7 addresses the full details of these end-to-end configurations and the roles that SLE/CSTS play.

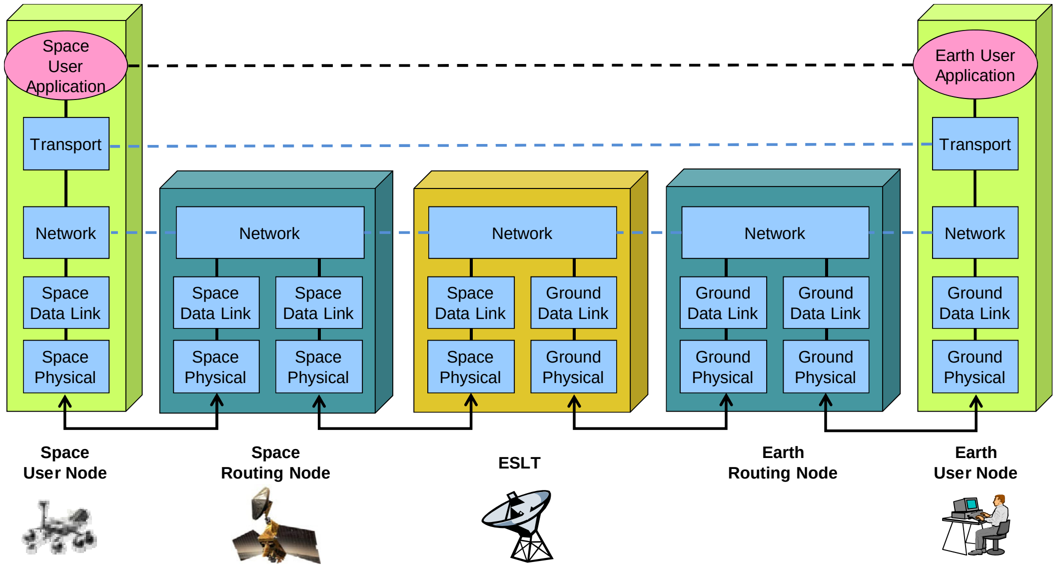


Figure 6-5: Basic SSI Protocol Layering

The basic SSI end-to-end configuration consists of a series of nodes, each of which implements either the DTN protocol stack, the IP stack (where that can operate properly), or both. In most of these diagrams the focus is upon DTN, since that is the most general case and will work whether there is delay and disruption or not. On some subnets, such as on terrestrial or other planetary surfaces where there is continuous connectivity, the DTN protocol stack may actually operate over an underlying IP-based Network Layer, as shown later in figure 6-6. This is called an *overlay network configuration* and IP, in this case, is effectively acting as a reliable Link Layer for BP. Different Link Layer protocols may be used as needed on any given hop.

The ESLT is shown as implementing only the ground protocols up to the Network Layer. The Earth routing node shown may be at the MOC for the space routing node (orbiter) or at some other location. It is important to understand that the MOC for the space routing node is still responsible for establishing and operating the space link to that space routing node by requesting services from the ESLT to configure the space link. If contemporaneous links are available, these data may flow immediately to the Space User Node, or they may be staged on the space routing node until a link to a suitable next-hop destination becomes available.

6.4.3 SSI NETWORKED COMMUNICATIONS

Each of the CSSE and UE nodes in figure 6-5 actually implements several protocol layers, and these are the interoperability points in the SSI architecture. Each of these interface points between nodes requires that compatible protocols be implemented at all layers on both sides of the link. While the bulk of the new work to define the SSI will focus on the upper (Network and Transport) layers, the CCSDS already has a set of Recommended Standards for the lower layers; this document describes the recommended protocols and configurations for each protocol layer at each of the interoperability points.

6.4.4 EXAMPLE END-TO-END SSI PROTOCOL DIAGRAMS

6.4.4.1 Example SSI IP-based End-to-End Protocol Diagram

Figure 6-6 is a representation of a protocol lay-down for IP-based SSI communications. Here the IP network protocol is invoked at each ‘hop’ to do routing and to forward IP datagrams between the endpoints. A transport protocol (either TCP or UDP in the figure) provides de-multiplexing to applications and (in the case of TCP) end-to-end reliability. IPsec may be used to provide optional Network Layer security. In this configuration, all communications use IP; applications use IP addresses and do not deal in Ethernet addresses or SCID (although the SCID is used on the space segment as a Link Layer destination address—see 3.2.2.2).

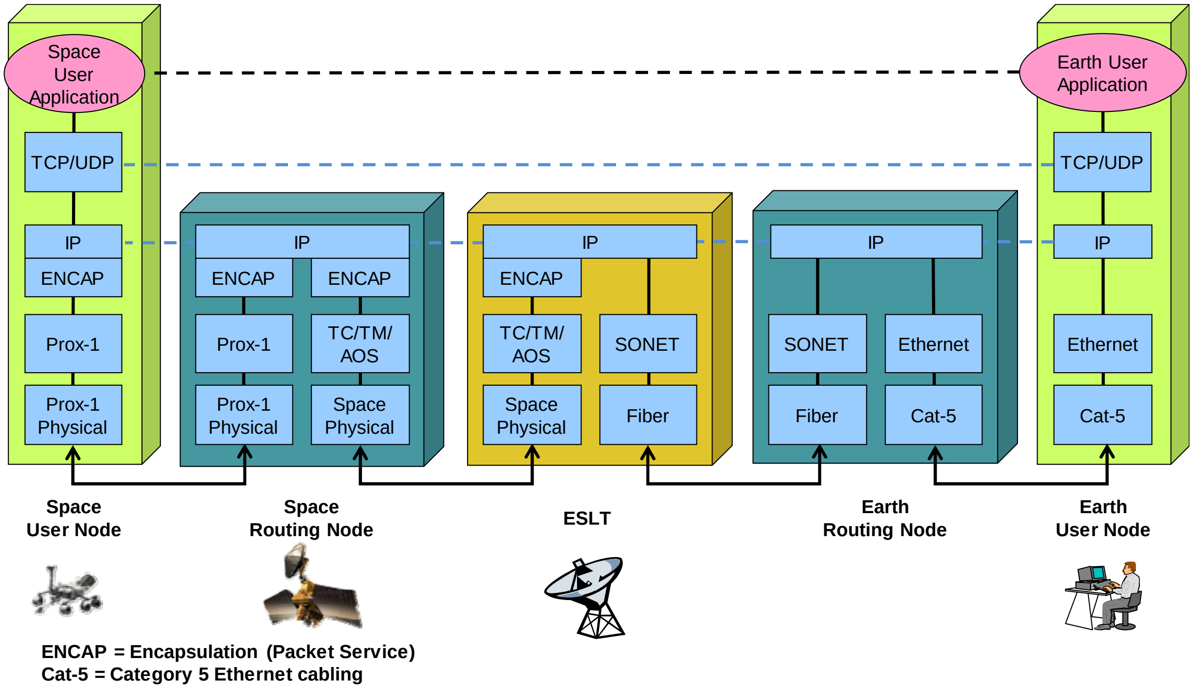


Figure 6-6: Protocol Layering for IP-based SSI Communications

6.4.4.2 Example SSI BP-based End-to-End Protocol Diagram

Figure 6-7 shows the protocol lay-down for a BP-based communication within the SSI. Here BP provides the Network Layer services, optional BSP security services, and runs over a number of different underlying Link Layer protocols. In space, this Link Layer is implemented using CCSDS encapsulation packet as a shim above the CCSDS space link protocols; on Earth TCP/IP or UDP are used as a virtual reliable link under BP. All Application Layer communications use BP, and thus the only change between a scenario with a single spacecraft and one with multiple relays is the addition of more hops, and possibly more/different protocols underneath BP to support each of the different links. Nothing changes from the applications’ points of view.

In the SSI Earth user application, data is converted into BP bundles, and the DTN protocols provide the end-to-end routing and delivery of bundles. The application data may be files or messages (as in AMS), or may be other application-specific data objects encapsulated in bundles. The files themselves may contain packets or other sorts of data structures. In all of these circumstances, the assumption is that only DTN and supporting protocols are used end-to-end, i.e., from the Earth User Node to the Space User Node.

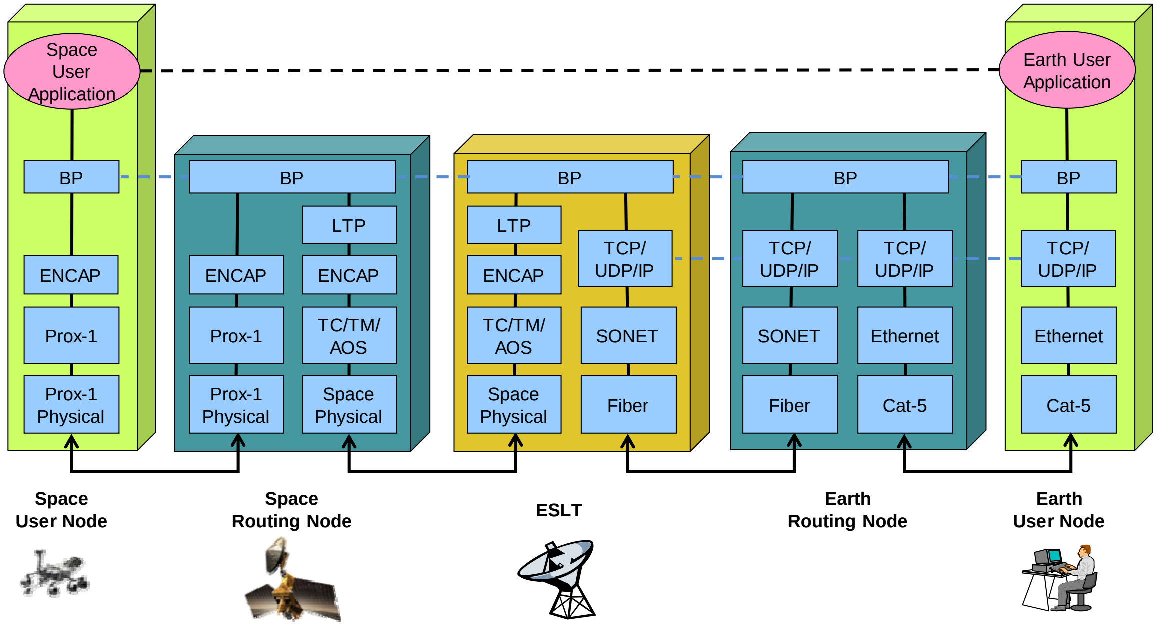


Figure 6-7: Protocol Layering for BP-based SSI Communications

6.5 PROTOCOL BUILDING BLOCKS

6.5.1 ABA CONFIGURATION PROTOCOL BUILDING BLOCKS

6.5.1.1 Overview

This section introduces ABA protocol building blocks, and each of the following diagrams presents one or more ABA protocol building blocks. Each diagram describes an appropriate stack of protocols for use in specific Link Layer configurations. Some of them are suitable only for ABA configurations, but some are also suitable for SSI configurations. Section 7 shows how to configure these protocol building blocks to meet the needs of specific end-to-end configurations.

6.5.1.2 ABA Service Provider Stacks

Figure 6-8 shows two different pairs of forward and return stacks for the service provider. The left-hand (a/b) pair shows forward and return stacks using current SLE F-CLTU and RAF services. These are primarily suitable for ABA configurations and single link mission designs. RCF (d) can also be used in this configuration. The right-hand (c/d) pair shows forward and return stacks using F-Frame and RCF. These both permit multiplexing of different frames to/from different sources, based upon the frame VC identifiers. This is a basic capability that can support ABA configurations with symmetrical frame services and is required to support SSI traffic or SSI traffic combined with single link, frame-level service on a different VC.

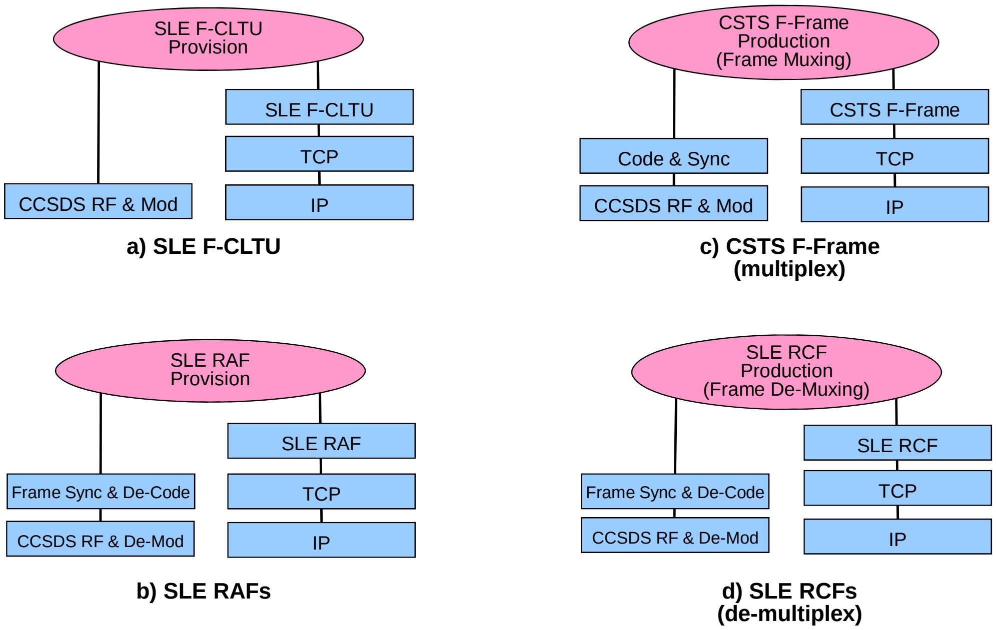
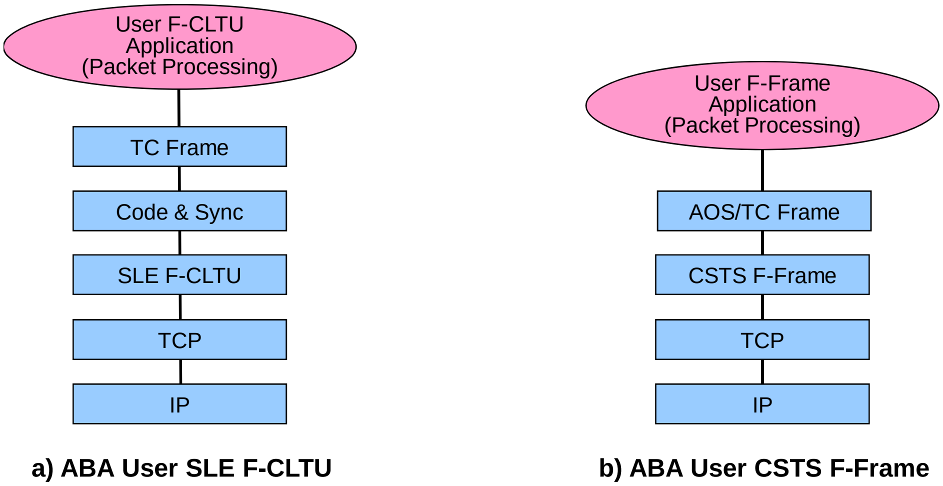


Figure 6-8: Generalized Service Provider Protocol Stack Building Blocks

6.5.1.3 ABA Service User Forward-Frame Stacks

Figure 6-9 shows two different styles of service user ABA F-Frame stacks. In either of these, any processing of packet data or higher-level protocols like CFDP is the user’s responsibility. The left-hand (a) figure shows a ground-user forward stack using current SLE F-CLTU service. It should be noted that the user is responsible for implementing the protocols for producing data frames (typically TC, but could be AOS), encoding the data, attaching the sync marker, and assembling CLTUs that are ready for modulation and radiation. This is primarily suitable for ABA configurations and single link mission designs. The right-hand (b) figure shows the ground-user forward stack that uses the CSTS F-Frame service. In this case the user just has to implement the protocol to provide frames (AOS or TC) and send them to the F-Frame service, which does any frame multiplexing, the frame encoding, and the rest of the modulation and radiation services. This configuration works with service provider options shown in figure 6-8(c), and can be used to support either ABA or SSI traffic.



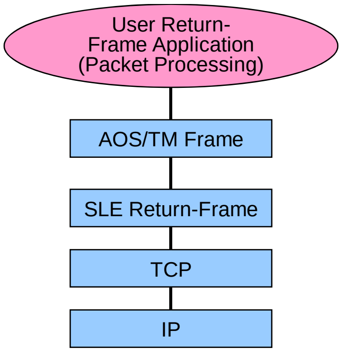
a) ABA User SLE F-CLTU

b) ABA User CSTS F-Frame

Figure 6-9: ABA Service User F-Frame Building Blocks

6.5.1.4 ABA Service User Return-Frame Stack

Figure 6-10 shows the corresponding ABA user SLE return-frame configuration. This can be used with either RAF or RCF services, the difference being whether the one user site gets all of the frames or just selected subchannels. In all of these forward or return configurations, data in packets (SP or EP) must be merged for delivery or extracted for processing by the ground user.



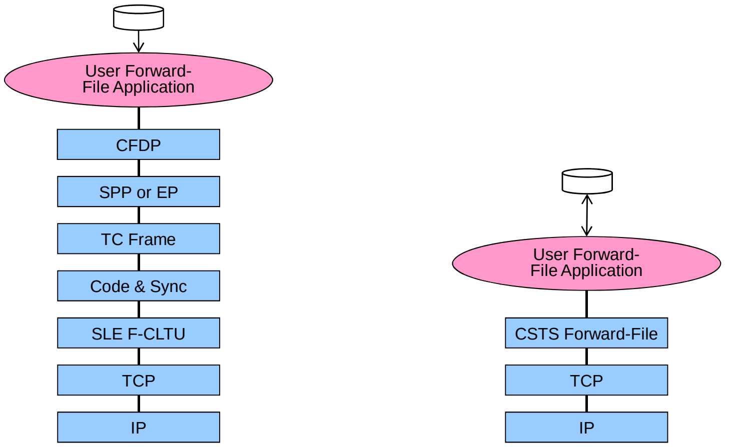
ABA User SLE Return-Frame

Figure 6-10: ABA Service User Protocol Return-Frame Building Block

6.5.1.5 ABA Service User Forward-File Stacks

Figure 6-11 shows two styles of service user forward-file stacks. The left-hand (a) figure shows a ground-user forward-file stack using the CFDP protocol and SLE F-CLTU service. It should be noted that the user is responsible for implementing CFDP to process the file, and that protocol agent puts CFDP PDUs into SPs or EPs, then uses the protocols to create TC (or AOS) frames, does encoding, attaches the sync marker, and assembles CLTUs that are ready for modulation and radiation. This is primarily suitable for ABA configurations and single link mission designs. The right-hand (b) figure shows a ground-user forward stack that uses the CSTS forward-file service. In this case, the user provides the file and implements the CSTS forward-file service to send the file to the service provider. The service provider then accepts the file, invokes CFDP, and does all required frame processing, multiplexing, encoding, and the rest of the modulation and radiation services. (See figure 6-13(a) for the ABA service provider forward-file stack diagram.)

The approach shown in figure 6-11(b) trades service user simplicity for added complexity for the service provider. However, where the service providers do offer these services, or higher-level SSI services, the burden on all of the users will be reduced.



a) ABA User CFDP File Delivery over SPP and SLE F-CLTU

b) ABA User CSTS Forward-File (Requires CSTS Forward-File in Service Provider)

Figure 6-11: ABA Service User Forward-File Building Blocks

6.5.2 SSI CONFIGURATION PROTOCOL BUILDING BLOCKS

6.5.2.1 General

In order to provide fully compliant SSI services, the service provider organizations must implement the additional Network Layer and support protocols in the ESLT. Similarly, any space routing nodes, PSLT, and WAN nodes must implement specific services and protocols in order to interoperably support SSI services.

It should be noted that while figures 6-9 and 6-10 are described as being used for ABA mission configurations, where a single-user mission ground-user MOC uses a space link to communicate with its space user asset, this same protocol-stack building block may also appear as part of an SSI configuration. In the SSI case, the space relay MOC may use the protocol stack shown in figure 6-9(b) to form the forward link to the space relay node, and may use the one shown in figure 6-10.

6.5.2.2 SSI Service Provider Space/Ground Stacks

Figure 6-12 shows a related pair of SSI protocol stacks: 6-12(a) shows the protocol stack that must be implemented in the ground node, typically in the ESLT or service provider ground station, and 6-12(b) is to be implemented in a space routing node that connects a long-haul space link with a local proximity link.

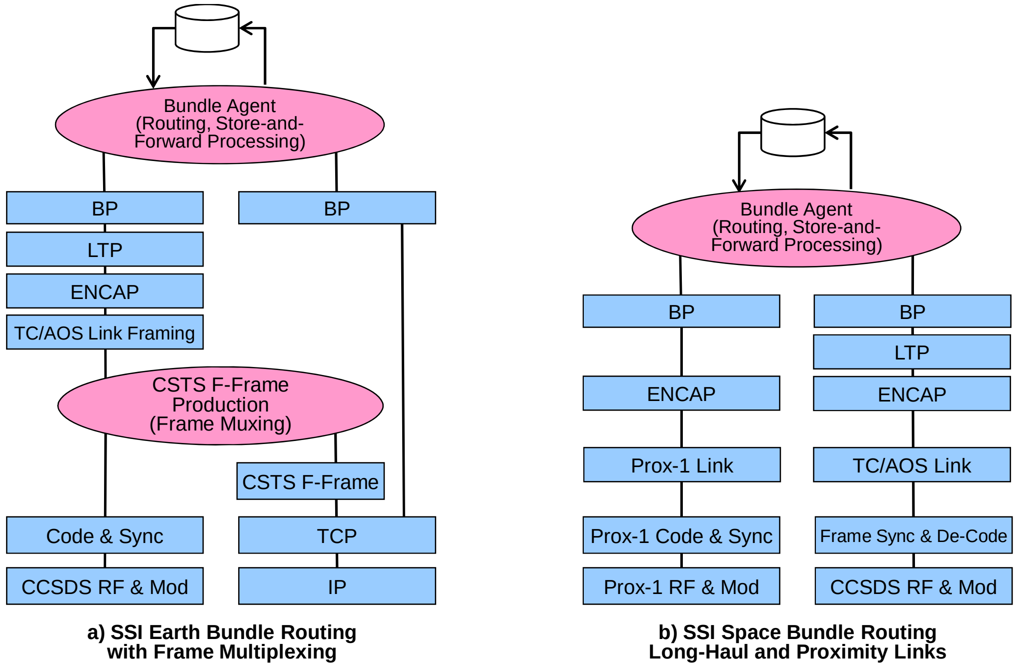


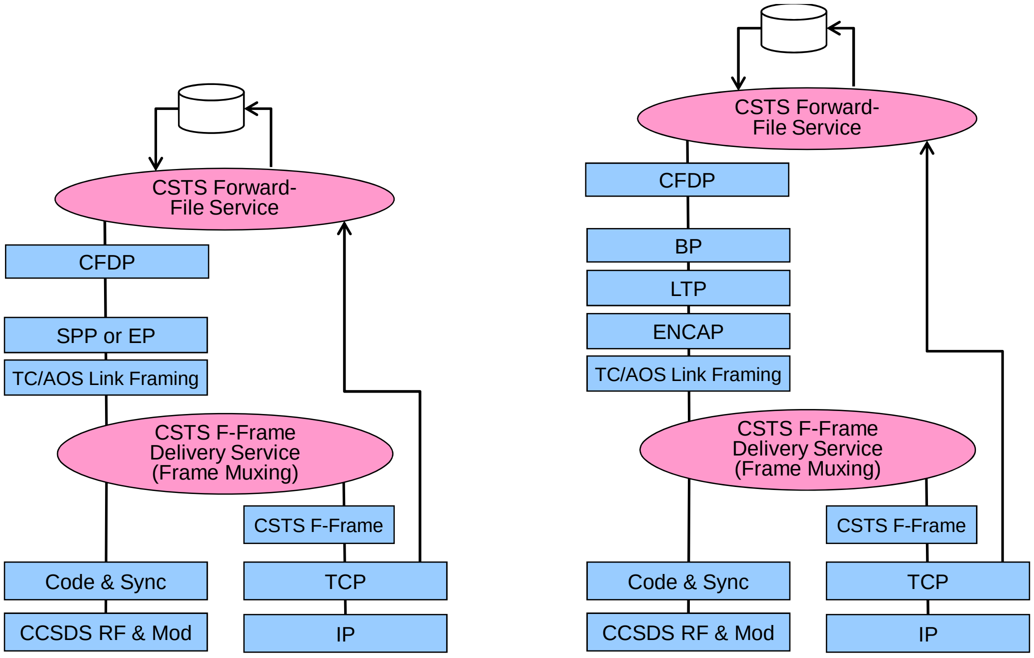
Figure 6-12: SSI Service Provider Space and Ground Building Blocks

Figure 6-12(a) shows the configuration in the service provider. This uses the new F-Frame service that multiplexes frames and then performs encoding and modulation within the ESLT. On top of the Link Layer part of the stack is a layer of BP elements, including the bundle agent, which is a protocol entity that handles routing and store-and-forward functions for BP. It should be noted that this protocol is accessed directly from TCP/IP on the terrestrial side; it does not depend upon the CSTS or SLE services. The output of the bundle agent goes into BP again, and then into the Licklider Transmission Protocol (LTP), which ensures reliable delivery of bundles over long-haul space links. LTP uses encapsulation and AOS or telecommand Link Layer and framing protocols, and the output of this stack is fed into the multiplexing function of the CSTS F-Frame. In this way, frame streams from BP (or IP) associated with one VC may be merged with frame streams from other sources (and VCs). This merged output is encoded and transmitted over the RF link. BSP may be used to provide bundle security services.

In figure 6-12(b) the protocol stack configuration for a space-bundle routing node is shown. This could be implemented in a PSLT or in a space relay node. For the long-haul space link, this is where the LTP-reliable transmission is terminated. There is also a bundle agent shown in this stack, and routing and store-and-forward functions are implemented. Data on the forward path is shown flowing on a Proximity-1 link, which would be typical of a space relay node deployment, but if this were a PSLT, data could also be flowed over an adapted terrestrial link protocol, like Ethernet or WiFi 802.11. Frame-level de-multiplexing is not shown explicitly, but the space link might contain streams from multiple VCs, and some could be processed as shown, while others are sent to different frame and/or packet-level protocol functions. These are not shown here.

6.5.2.3 ABA/SSI Service Provider Forward-File Stacks

Figure 6-13 shows the ABA and SSI service provider protocol stacks implemented in the ESLT. These use the CSTS forward-file and forward-frame service, and a protocol stack that produces frames for merging into the forward stream. The advantage of this configuration is that with two simple options it can support ABA users, SSI BP (or IP), CFDP, and basic F-Frame services. The ABA user side of this was presented in figure 6-11(b).



a) ABA CSTS Forward-File Service Provider Using CFDP File Delivery over SPP and CSTS F-Frame

b) SSI CSTS Forward-File Service Provider Using CFDP File Delivery over BP and CSTS F-Frame

Figure 6-13: Service Provider SSI Forward-File Building Blocks

6.5.2.4 SSI Service User CFDP Stack

Figure 6-14 shows the SSI service user protocol stack that uses the CFDP protocol for file delivery, and then uses the BP protocol stack to produce frames for merging into the forward stream. The bundles flow over TCP/IP terrestrially and then get processed as shown in figure 6-12(b) as part of the BP traffic managed by the bundle agent in the ESLT. In the case of CFDP implemented over BP, a simplifying assumption is made that all of the reliability, data management, and routing functionality may be stripped out of the implementation, leaving only the CFDP Class 1 or 2 file delivery and accountability functions. Any other upper-layer protocols, such as AMS, may also be layered directly over the BP protocols in the service user node. BSP and/or IPsec may be used to provide security services as required.

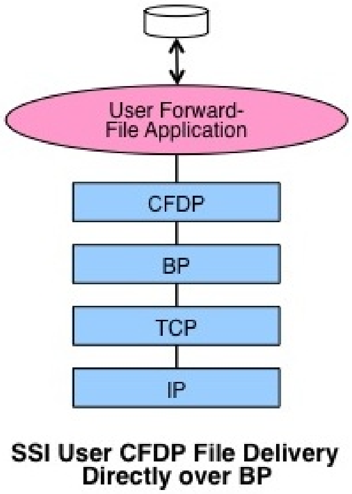


Figure 6-14: Service User CFDP over BP Building Block

6.5.3 SSI LAST-HOP AND FIRST-HOP SERVICE

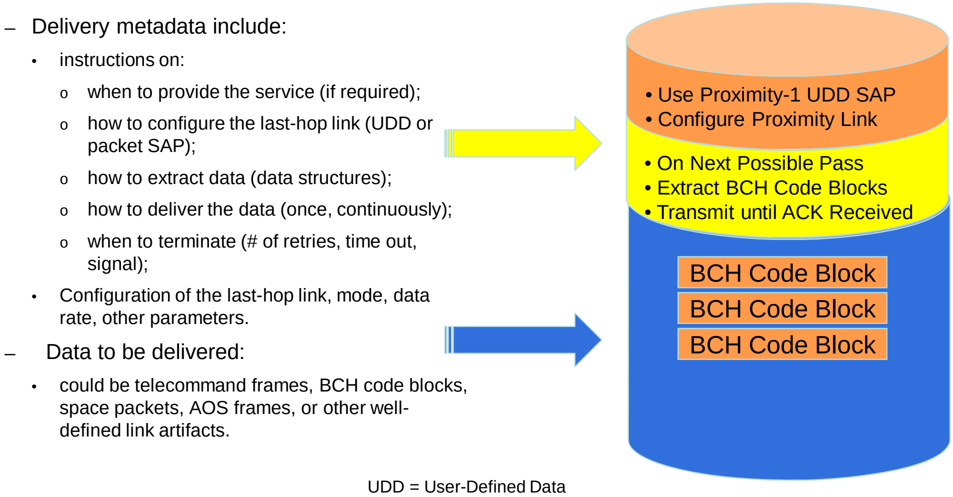
6.5.3.1 SSI Last-Hop and First-Hop Service Description

The last-hop and first-hop services are defined for the SSI as the means recover from spacecraft emergencies and to support non-SSI end nodes. These emergency communications functions will need to be implemented in any node that provides service to either ABA end-user nodes or other SSI nodes that will need to be 'rebooted'. There is a corresponding first-hop service that returns essential telemetry from an SSI node or a non-SSI ABA node, and it can also process and return other data such as radiometric observables from a proximity link, time-exchange information, or open-loop recordings acquired during an EDL pass.

For these specialized delivery functions, a *delivery agent* (the last-hop application), using normal file delivery processes, accepts a specially constructed file that includes required delivery instructions and metadata. The metadata will include delivery instructions for the delivery agent, including the destination spacecraft, pass(es) for delivery, delivery process to be used, and any retry instructions. The delivery agent uses the metadata to drive the process of extracting the low-level PDUs from the file and sending them to the destination, in the prescribed way, at the requested time. The instructions may include requests to send multiple times or to resend on successive passes, and could even include a request to look for some reply/signature on the return path. Spacecraft command data may be secured as needed using authentication of encryption applied by the MOC.

6.5.3.2 SSI Last-Hop and First-Hop Delivery Package

The relayed file, or *delivery package*, is transmitted from the ground user to the last-hop service node and contains all the information the delivery agent needs to satisfy the request (see figure 6-15). It does this by interpreting the delivery instructions (e.g., timing, link configuration, etc.) to understand what is required to transmit the data over the last hop. The forward delivery agent then extracts data according to the instructions, configures the last-hop node to deliver those data, and sends the data (using whatever format and process was requested) over the link to the end node.



– Delivery metadata include:
  - instructions on:
    - when to provide the service (if required);
    - how to configure the last-hop link (UDD or packet SAP);
    - how to extract data (data structures);
    - how to deliver the data (once, continuously);
    - when to terminate (# of retries, time out, signal);
  - Configuration of the last-hop link, mode, data rate, other parameters.

– Data to be delivered:
  - could be telecommand frames, BCH code blocks, space packets, AOS frames, or other well-defined link artifacts.

UDD = User-Defined Data
SAP = Service Access Point
BCH = Bose, Chaudhuri, Hocquenghem

Figure 6-15: Last-Hop Delivery Package Structure

In the forward direction, the data to be transmitted may be any of several possible forms of command data. In the return direction, the service operates a little differently, in that the delivery package that is sent to the first-hop service node contains just the necessary request and link configuration information. In the return direction, the returned package includes any data that are returned, along with the report on the status of the request.

6.5.3.3 SSI Last-Hop and First-Hop Data Exchanges

Figure 6-16 shows the kinds of data exchanges that will take place among the CSSEs and UEs to support the forward and return last-hop services.

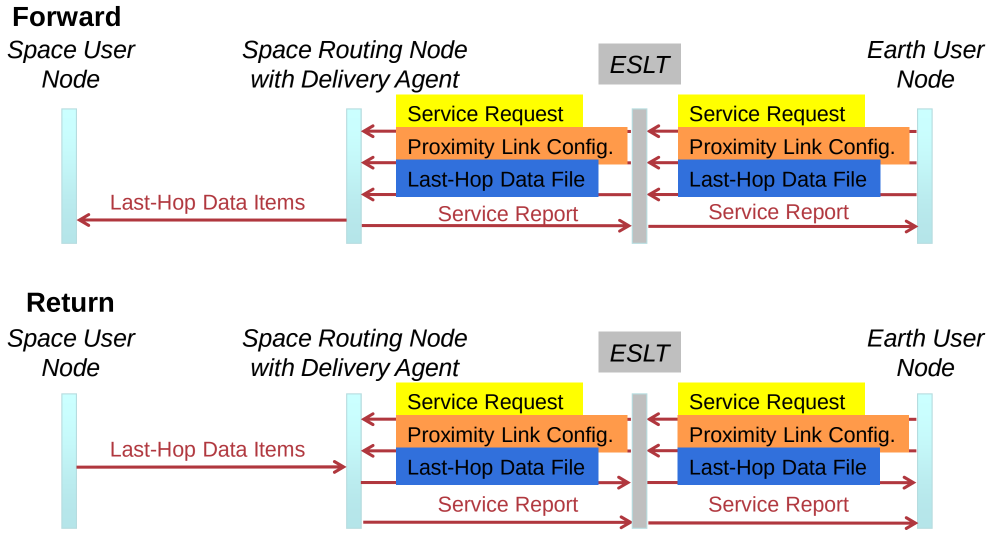


Figure 6-16: Data Exchanges for Forward Last-Hop and Return First-Hop Service

Figure 6-17 shows a generic 'forward' view of how the SSI last-hop delivery agent end-to-end protocols are configured. (For more details on the end-to-end configuration refer to 7.3.3.)

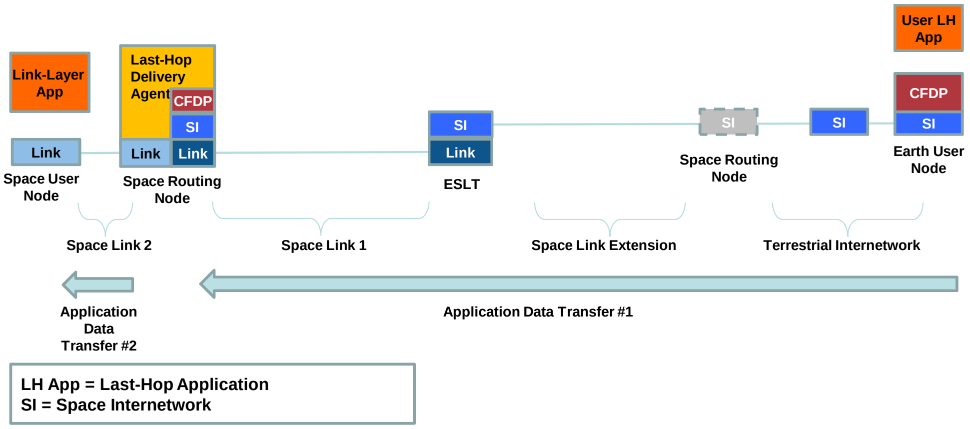
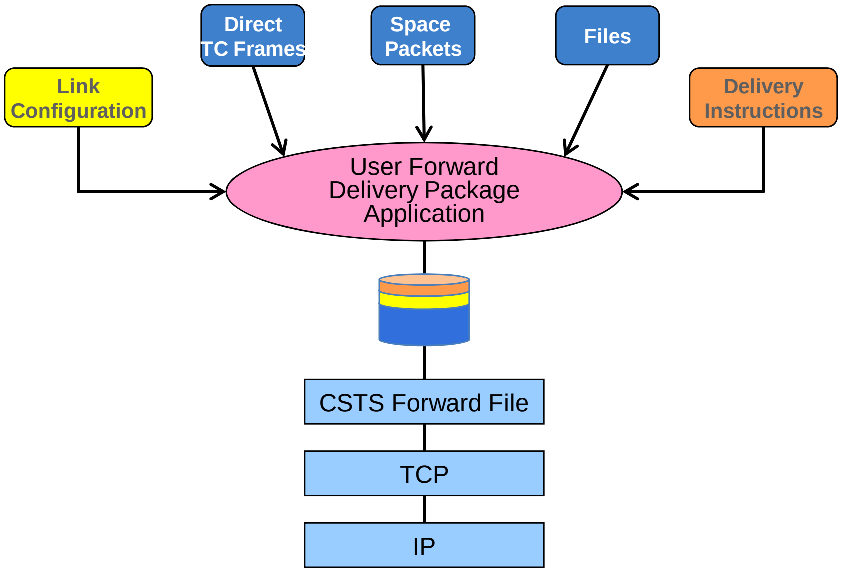


Figure 6-17: End-to-End Generic Protocol for Forward Last-Hop Service

6.5.3.4 SSI Last-Hop and First-Hop Building Blocks

To implement the last-hop and first-hop services, some new protocol elements have to be introduced. Figure 6-18 shows the user application that is required to construct the last-hop delivery package. As shown earlier in figure 6-15, that package is a file that has three separate parts: the delivery instructions (information on when and how to deliver the data [orange], how to configure the link [yellow], and the data itself [blue]). The data may contain a variety of different kinds of Link Layer data structures, such as telecommand frames, packets, BCH code blocks, or whatever specific artifact is required to be delivered across the last-hop link.



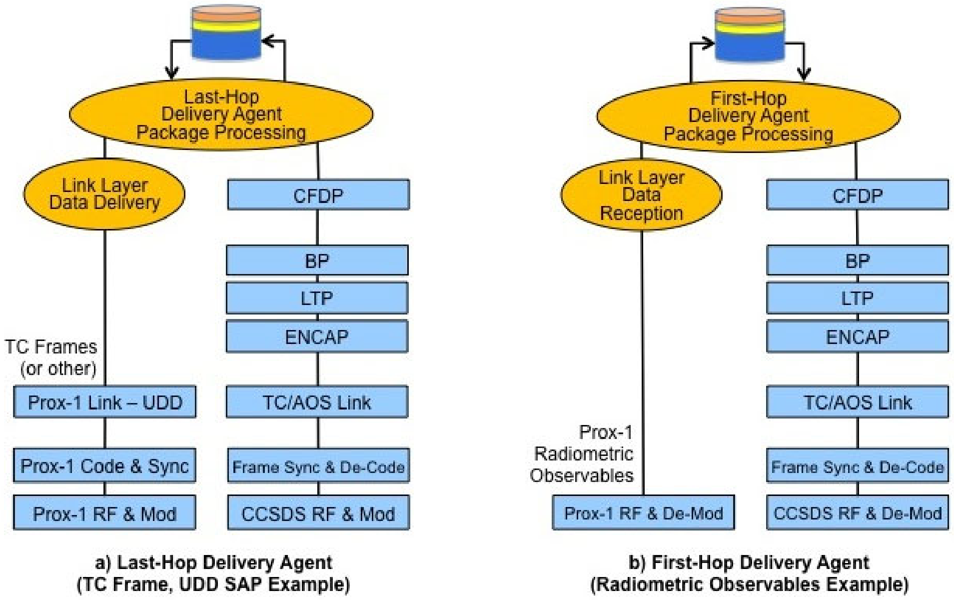
ABA Last-Hop Delivery Package Assembly and CSTS Forward-File Delivery

Figure 6-18: Last-Hop Delivery Package Assembly

The forward delivery package application must construct the package. Normal SSI file-delivery mechanisms are used to transfer the file to the delivery agent residing on the last-hop node. In figure 6-18 the CSTS forward-file service is used (see figure 6-13(a) for the ABA service provider stack). This configuration is appropriate for a non-SSI mission that wishes to use the service to deliver data at the Link Layer to its Space User Node. Alternatively, for SSI missions, the file could have been sent either using CFDP over BP, as shown in figure 6-14, or using CSTS forward-file to an SSI ESLT (figure 6-13(b)).

Figure 6-19 shows the configurations of the last-hop (a) and first-hop (b) services and protocols on a space routing node that implements the delivery agent. The right-hand sides of both of these diagrams look just like normal onboard CFDP-over-BP file delivery; it is the space side of what was shown earlier in figure 6-13. But in figure 6-19, the onboard CFDP delivers the data to the last-hop delivery agent.

The ‘first-hop delivery agent’ is symmetrical. It gets instructions from the ground, but then returns the acquired data in a return delivery package. The return file transfer uses normal SSI protocols unless the final destination is a non-SSI node, in which case some other method such as CSTS file transfer may be used for the final delivery to the Earth User Node.



a) Last-Hop Delivery Agent (TC Frame, UDD SAP Example)

b) First-Hop Delivery Agent (Radiometric Observables Example)

Figure 6-19: Last-Hop and First-Hop SSI Service-Delivery Building Blocks

6.6 NETWORK MANAGEMENT

6.6.1 GENERAL

SSI network management functions include defining those data tracked by the managed devices (DTN bundle agents and routers) in the deployed system, querying the values of those data, defining reporting/configuration behavior, and issuing control directives. Management functions will typically be secured themselves, and may include administrative/security configurations and computed performance measurements.

6.6.2 NETWORK MONITOR AND CONTROL

Monitoring and maintaining the quality of the RF links among the space elements of the SSI is the responsibility of the managers of those elements. Managing these links will have aspects of both service management and network management; service management interactions among the provision managers of linked subnetworks will be used to exchange link-level information regarding their peered link(s), and network management tools will be used by each subnetwork manager to monitor and control that manager’s network’s side of each RF link.

Service management protocols for exchanging RF link monitor data among component network managers have yet to be developed.

The concept of ‘control’ may have to evolve for RF link management, too. In today’s concept of control, the ‘user’ is given limited ‘service control’ over some parameters of the provider network. When two satellites share a space link for the purposes of transferring SSI traffic, the roles of ‘user’ and ‘provider’ become blurred. For example, what are the rules for determining which manager gets to control the peer side of the RF interface on the other component network? Perhaps the model needs to evolve from that of user/provider to peer entities. In any case, the protocols by which component networks coordinate the operation of their peered RF interfaces have yet to be developed.

6.6.3 SSI NETWORK MANAGEMENT PROTOCOL

6.6.3.1 General

Unlike the terrestrial Internet, the SSI contains nodes whose communication links are challenged by potentially large signal propagation delays and/or transmission disruption. These challenged links make timely data exchange difficult or impossible. The DTN Management Protocol (DTNMP) (reference [40]) accomplishes the management function using open-loop, intelligent-push, asynchronous mechanisms that scale to fit the SSI operating environment. DTNMP is one of the key protocols supporting peering and its use is essential to support the SSI confederation. The protocol is designed to implement four desirable properties:

a) the intelligent push of information eliminates the need for round-trip data exchange in the management protocol. This is necessary in open-loop systems where reliable round-trip communication may not exist;

b) smaller messages require smaller periods of viable transmission for communication, incur less retransmission cost, and consume fewer resources when persistently stored en-route in the network;

c) fine-grained data identification allows all data in the system to be explicitly addressed, while flexible data identification allows users to define their own customized, addressed data collections;

d) the DTNMP adopts an identifier approach compatible with the Management Information Base (MIB) format used by typical Internet management protocols such as the Simple Network Management Protocol (SNMP), thus enabling management interfaces between DTNs and other types of networks.

The DTNMP performs the four core network management functions of configuration, performance reporting, control, and administration, as described below.

6.6.3.2 SSI Configuration

The configuration function synchronizes definitions amongst various DTNMP agents and managers in the DTN. Managers must understand what Application Data Models (ADM) are understood by respective agents, and agents must be configured with the types of computed data, reports, and control functions that they must produce, and when. Within the DTNMP, the requirement to operate in an open-loop manner over asynchronous and, at times, unidirectional links, is satisfied by preconfiguring information at agents and managers prior to data exchange.

6.6.3.3 SSI Performance Reporting

Since DTNMP operates asynchronously, performance monitoring has been replaced by performance reporting. There is no expectation of closed-loop control of a managed device across a high-latency link. As such, the best action that a managing device may undertake is collecting reports as received by managed devices and applying controls as appropriate.

Reporting the performance of a managed device involves collecting reports from the managed device and the communicating those reports to appropriate managing devices. Reports contain both data from the ADMs preconfigured on the agent and custom-defined information configured dynamically by managers. In all cases, DTNMP agents ‘push’ their performance reports; there is no defined ‘get’ function. Managers ‘pull’ information by configuring associated agents to perform a push.

6.6.3.4 SSI Control

Part of the ADM for each application supported by an agent includes a list of controls that operate common functions for the application. Managers in the network either directly invoke controls on agents, or configure the invocation of controls on agents predicated by local agent state or time.

6.6.3.5 SSI Administration

The mappings among agents and managers within a network may be complex, especially in networks comprising multiple administrative domains. The administrative management function provides a level of configuration associated with which managers may control which agents, for what types of information. This provides a level of granular logging and security beyond that provided by the protocols carrying the DTNMP messages.

6.7 REMAINING CHALLENGES TO PROTOCOL DEPLOYMENT

6.7.1 GENERAL

The space IP and space DTN suites both have residual challenges that must be taken care of prior to final operational deployment. IP provides a rich body of knowledge and Commercial-Off-The-Shelf (COTS) equipment in scenarios where end-to-end connectivity can be assumed, but this is seldom the case in space, so IP has a constrained operating environment. DTN provides 'IP-like' services in areas where constant end-to-end connectivity cannot be assumed, but applications must be written or adapted to take advantage of it and to deal with the (possibly) delayed and episodic communications environment.

6.7.2 SPACE IP

The following items need further work in order to deploy IP as a network protocol within the SSI:

a) network management: A unified naming scheme for space endpoints needs to be defined;

b) routing: IP assumes continuous and generally bi-directional connectivity among routers. Some experimentation needs to be done to determine the best routing mechanisms for the 'edge' cases of IP applicability, such as unidirectional and periodically connected links.

NOTE – These are primarily operational issues; there is very little specification work that needs to be done, provided that IP is used in regimes that permit it.

6.7.3 SPACE DTN

The following items need further work in order to deploy the DTN suite and BP as a space internetworking protocol within the SSI:

a) endpoint identification: A unified naming scheme for space endpoints needs to be defined. NASA has developed a Compressed Bundle Header Encoding (CBHE) to provide a compatible naming scheme that has been standardized by the Internet Engineering Task Force (IETF);

b) routing: While IP routing is quite mature, BP routing, especially routing that involves making effective use of scheduled contacts, is relatively immature. CGR has been tested on the Deep Impact Network (DINET) experiment and requires continual updates of contact plans. This is an ad-hoc protocol, and there is not yet a standardized approach. Extending CGR to include an automated protocol (controlled by mission policy) to exchange and update schedules would improve performance;

c) network management: Protocols and practices for configuring and managing BP agents are still in development;

d) documentation: Users of the Internet enjoy an enormous body of documentation and experience in configuring, operating, and exploiting the capabilities of the network. Similar documentation for the BP has barely begun.

6.8 SECURITY CONCEPTS FOR PROTOCOL VIEW

6.8.1 GENERAL

Security for the protocol view may be applied at the Physical Layer, Link Layer, Network Layer, or Application Layer. Table 6-3 identifies the current security standards defined for each layer.

Table 6-3: Security Standards

OSI Layer	Security Standards	Reference
Physical Layer	No CCSDS Standards defined; various methods in local use	N/A
Link Layer—Space-to-Ground Links	Space Data Link Security Protocol	CCSDS 355.0-R-3 [57]
	CCSDS Cryptographic Algorithms	CCSDS 352.0-B-1 [22]
	Symmetric Key Management	CCSDS White Book [58]
Network Layer—DTN Internetworking Protocols	Bundle Protocol Specification	RFC 5050 [37]
	Bundle Security Protocol Specification	RFC 6257 [39]
Network Layer—IP Internetworking Protocols	Security Architecture for the Internet Protocol	RFC 4301 [44]
	IP Encapsulating Security Payload	RFC 4303 [59]
Application Layer	HTTP Over TLS	RFC 2818 [60]
	Hypertext Transfer Protocol—HTTP/1.1	RFC 2068 [61]
	FTP Security Extensions	RFC 2228 [62]
	File Transfer Protocol (FTP)	STD 9 [43]

6.8.2 SECURITY FOR ABA SPACE LINK CONFIGURATIONS

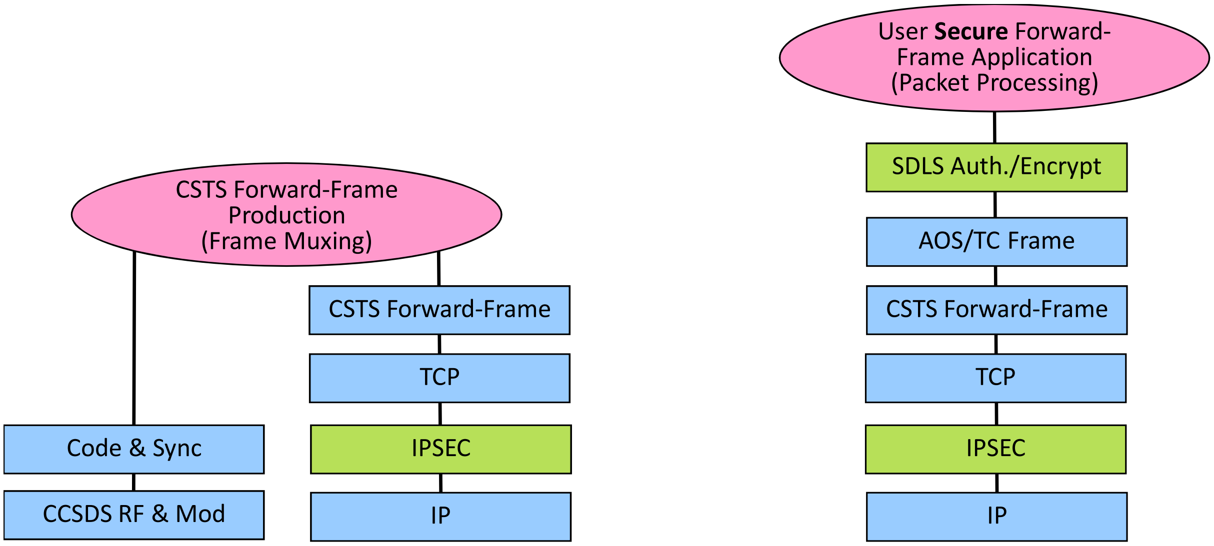
For ABA configurations security is usually applied at the Link Layer, and often this is only in the forward/command direction and not in the return direction. There are two methods in general use:

a) securing the space link by installing OSI Physical Layer encryption devices in the ground station and on the spacecraft (reference [63]);

b) securing the link by using OSI Link Layer security such as SDLS.

Either of these methods works to secure the link. The former is usually provided by hardware and it must be installed and operated at the ESLT. This encrypts the entire data stream, including frame headers and other signaling structures, so it must be removed before decoding can be performed. The latter requires no special processing at the ESLT since the user applies encryption to the data and it affects only the contents of the frame, not the frame headers and other protocol signaling structures.

Figure 6-20 shows two approaches for securing the data in an ABA configuration, shown in green for emphasis in this and following figures. Use of SDLS provides the means to do end-to-end Link Layer security. An ABA user MOC may apply one (or both) of the encryption or authentication algorithms to its command data, load it into an AOS or TC frame inside the SDLS security block, and then use the normal service delivery mechanisms to transmit the data to the user space node, as reflected by the SDLS authentication/encryption layer in figure 6-20(b) (references [22] and [57]). It should be noted that the service provider stack in figure 6-20(a) does not show the presence of the SDLS authentication/encryption layer since that security block is opaque to the CSTS F-Frame service.



a) ABA Secure CSTS Forward-Frame Provider (Multiplex)

b) ABA Secure CSTS Forward-Frame User

Figure 6-20: ABA Secure Forward-Frame Building Blocks

The user spacecraft must also implement the SDLS authentication/encryption functions to process the received data contents of the frame. The presence of the SDLS security mechanism and the options that are selected are not signaled and are set ‘by management’; i.e., they are prearranged. Some means must also be provided to establish and manage the keys used to protect or sign the data and to signal any changes to the spacecraft (reference [58]).

This figure also shows an additional layer of encryption that optionally may be applied at the Network Layer to secure the IP traffic over the Internet. This is IPsec, and it may be employed as a security mechanism where traffic analysis or just terrestrial exposure of the data is a concern. In most configurations, one or another of these two mechanisms might be employed; however, it would be unusual to elect to use both, as shown in these figures.

6.8.3 SECURITY FOR SSI NETWORK CONFIGURATIONS

In SSI configurations, users may also apply encryption directly to their data, and Network Layer security may also be employed. Because an internetworked space architecture allows packets to be forwarded (possibly through multiple hops), and because of the value of both space assets and communication opportunities, care needs to be taken to ensure that only authorized traffic is allowed onto the SSI.

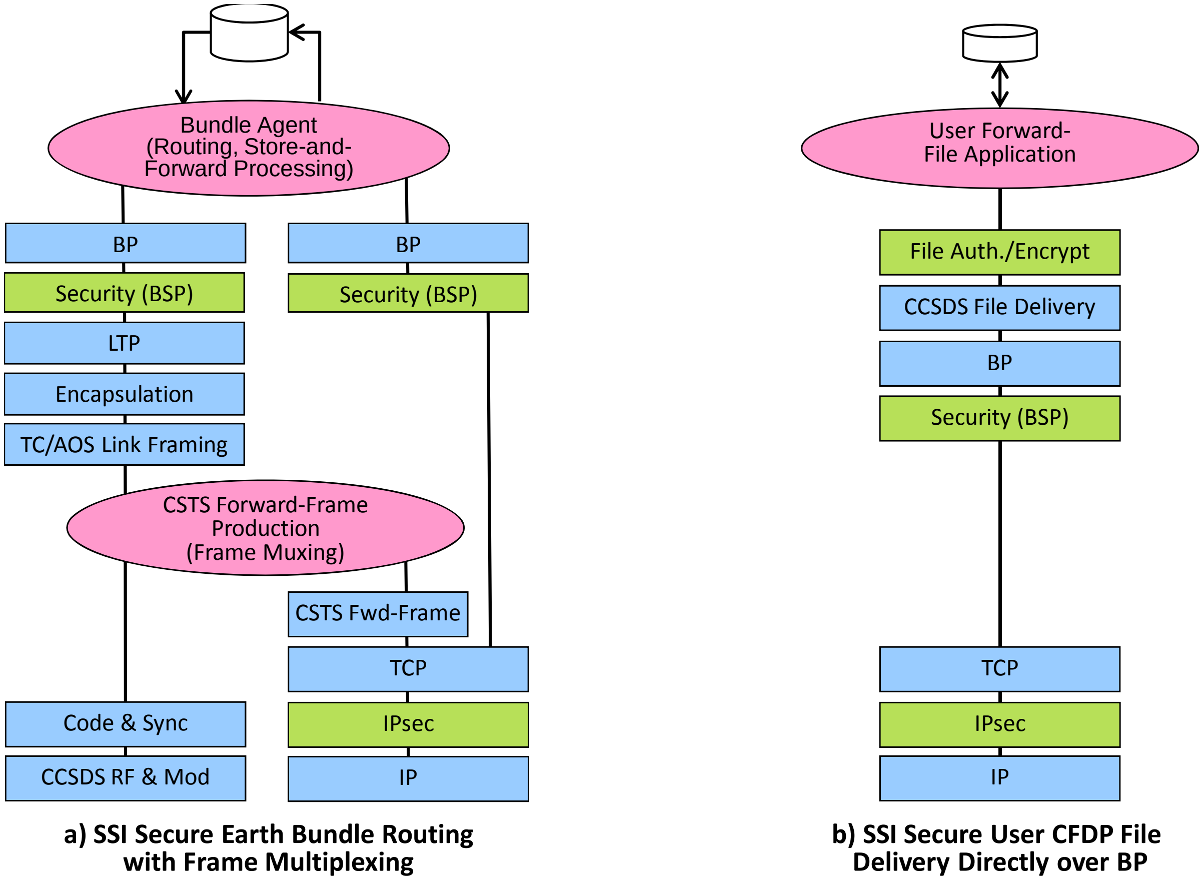
For IP, it is important to realize that using IP in the SSI does not mean connecting the SSI to the Internet at large. The SSI can use a private IP address space that is not routable on the Internet and/or Virtual Private Network (VPN) and can use IPsec protocols on the ground.

Both IP (IPsec) and BP (BSP) include security protocols that provide:

- end-to-end or ‘edge-to-edge’ confidentiality (encryption);
- end-to-end or ‘edge-to-edge’ authentication.

In addition, BP provides a ‘hop-by-hop’ authentication mechanism so that data is authenticated at each router before being forwarded. This provides an additional level of infrastructure protection above end-to-end security, since a malicious intruder who can inject traffic onto a network link cannot cause that traffic to propagate. This would protect constrained resources (e.g., space links) from denial-of-service traffic.

Figure 6-21 shows three alternatives for securing an SSI end-to-end file transfer. The SSI user MOC may apply one of the encryption or authentication algorithms to its command data and load that into a file. The secured file, in and of itself, provides end-to-end data security. That secured file may be transferred using CFDP, loaded into a BP bundle (or IP datagram), and the bundle protocol itself may be secured by the BSP. In figure 6-21(b), BSP is shown as a separate layer when, in fact, part of the BSP security processing is wired directly into the BP itself, and other parts are done after BP has completed its work (as shown). BP/BSP may then use TCP/IP to transmit the data to the ESLT, as shown in figure 6-21(a), and thence to the user space node (references [63] and [36]).



a) SSI Secure Earth Bundle Routing with Frame Multiplexing

b) SSI Secure User CFDP File Delivery Directly over BP

Figure 6-21: SSI Secure Forward-File Building Blocks

The user spacecraft must also implement the symmetrical authentication/encryption functions to process the received data contents of the file and the BSP applied security. The presence of the BP/BSP security mechanisms that are in use are signaled. Some means must also be provided to establish and manage the keys used to protect or sign the data and to signal any changes to the spacecraft.

Like figure 6-20, this figure also shows an additional layer of encryption that optionally may be applied at the Network Layer to secure the IP traffic over the Internet. This is IPsec, and it may be employed as an additional security mechanism. In most configurations one or another of these three mechanisms (file data security, BSP, or IPsec) might be employed; however, it would be unusual to elect to use all three, as shown in these figures.

6.8.4 SECURING ACCESS TO SERVICE PROVIDERS

For all of the terrestrial or space service interfaces, access control and authentication will be applied, usually during connection establishment or binding to the service. The SLE, CSTS, and service management service interfaces include access control mechanisms that will require user authentication. This may use one of the types of credentials described in the cryptographic algorithms document (reference [22]) or other methods as required by the service provider.

Service interfaces that offer web services or file transfer functionality will also be similarly secured. They may also implement stronger security in the form of HTTPS or Secured File Transfer Protocol (SFTP) encrypted interfaces that both authenticate the user and shield the traffic by sending it in an encrypted ‘tunnel’.

7 END-TO-END DEPLOYMENT VIEW

7.1 GENERAL

This section describes end-to-end deployments of system elements, and provides examples of node, service, and protocol deployments for the provision of either ABA or SSI space communications cross support services. Building upon the element-by-element protocol stack views shown in the communications view (section 6), this section presents how these elements are to be assembled to provide end-to-end data delivery.

These deployment examples cover basic ABA deployments, control of space link ‘B’ by mission ‘A’ ground system, and some transitional single-hop ABA configurations that include SSI protocols. This section also describes nominal SSI ABCBA deployments, as well as SSI ABCBA deployments supporting non-SSI relays, transition of non-SSI node to SSI node, last-hop service from SSI routing node, and last-hop service from non-SSI relay node.

Each of these views describes the nominal end-to-end physical node deployments, the end-to-end communication services provided, the ground cross support services provided, the space-ground and space-space services used (if any), and any user or provider node-specific services. These are nominal configurations that provide the basic services that are described. Actual deployments may include more than one service, such as ABA, SSI, or CFDP file service, and also a last-hop service element. Some deployments may include the standard services described here and also agency- or mission-specific ones, such as customized use of Space Packets (SPs) for mission operations-specific functions.

NOTE – There is no direct treatment of mission operations services; they are assumed to use the standard end-to-end frame-, network-, file-, or message-delivery functions. Nor does this section describe any other mission-unique applications or services that may use the underlying frame, file, or internetworking services to deliver their data.

7.2 ABA END-TO-END PROTOCOL VIEWS

7.2.1 BASIC ABA END-TO-END PROTOCOL VIEWS

The simplest end-to-end configuration is the basic ABA forward Link Layer configuration. Figure 7-1 shows just such a simple F-CLTU service, where the Earth User Node sends CCSDS telecommand frames to the Space User Node. This is currently the most commonly deployed forward cross support service.

In figure 7-1 there are two user nodes (the light green Earth User Node on the right, and the Space User Node on the left) using the F-CLTU service in the ESLT. This deployment uses the F-CLTU service, as described in figure 6-8(a), and the Earth and Space User Nodes conform to the figure 6-9(a) configurations.

The features of the configurations shown in figures 7-1 and 7-2 are summarized below.

a) Description of basic ABA end-to-end configuration:

  – these configurations depict the transfer of TC or AOS frames from a single agency (A) Earth User Node (MOC), to the Space User Node, using the space link services of an ESLT provided by agency (B);

  – both agency A and B implement frame-level services, but may also use packets or files inside these frames.

b) End-to-end services provide:

  – forward transfer of encoded space data link frames (CLTUs containing TC/TM/AOS link PDUs) between the control center and its space asset.

c) Ground cross support services provide:

  – forward transfer of frames between the Earth User Node and ESLT using F-CLTU or F-Frame services;

  – encoding and frame merging in the ESLT when F-Frame services are provided.

d) Space-ground CCSDS services provide:

  – forward TM/TC/AOS frame transfer.

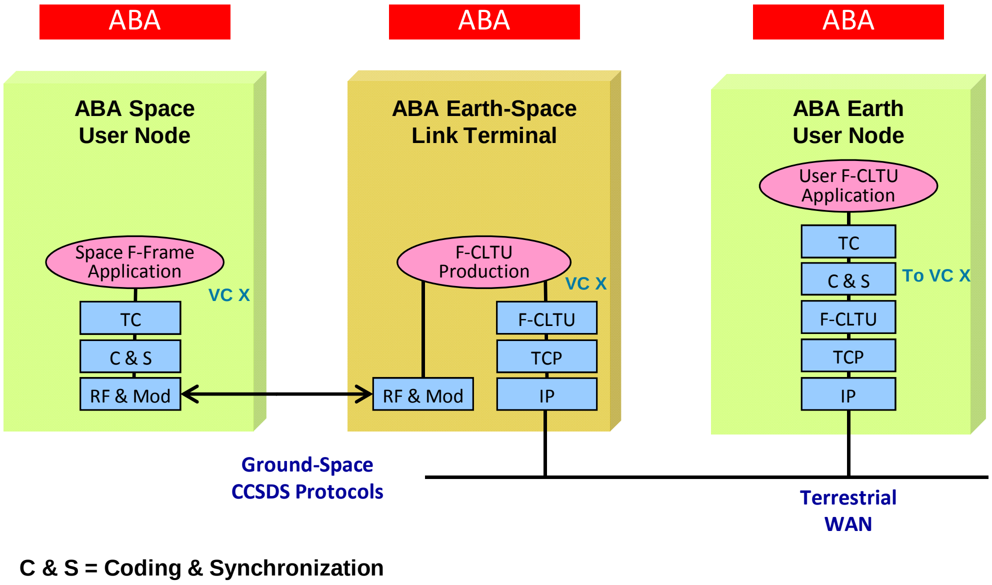


Figure 7-1: Basic ABA End-to-End Forward-CLTU Protocols

This ABA forward configuration could, of course, also adopt a F-Frame approach (figure 7-2), which uses the user node F-Frame configuration shown in figure 6-9(b) and the corresponding ESLT F-Frame configuration shown in figure 6-8(c). The delivery of data to the Space User Node is the same in either case. The advantage of the configuration depicted in figure 7-2 is that this use of F-Frame service in the ESLT can support both ABA and SSI configurations and either traditional TC commanding or AOS forward links. In practice, ESLTs are likely to offer both F-CLTU and F-Frame services.

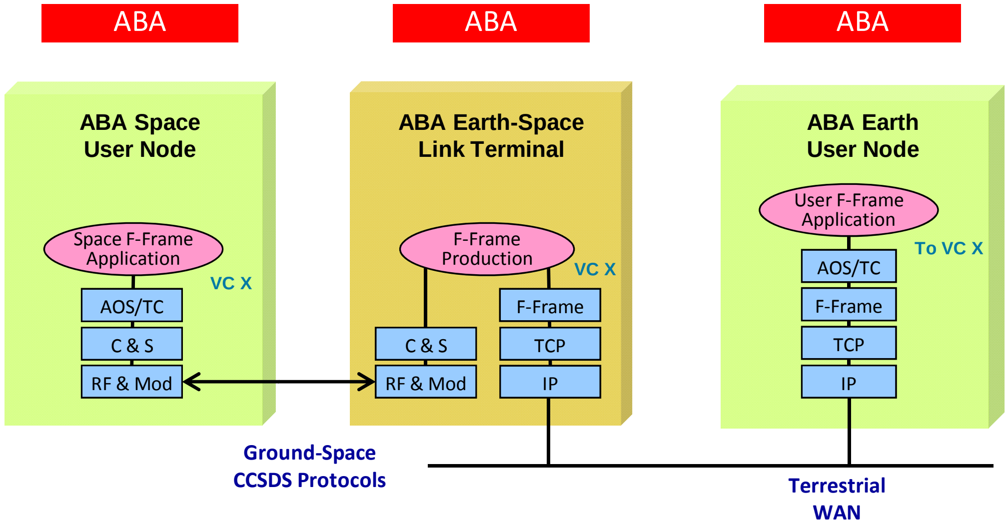


Figure 7-2: Basic ABA End-to-End F-Frame Protocols

7.2.2 ABA END-TO-END PROTOCOL VIEWS WITH USER APPLICATIONS

Figure 7-3 is similar to figure 7-2, but shows use of SPP to send commands in the F-Frames and the use of CFDP and SPP to transmit files. This figure also shows the user commands sent in SPs, and optionally the user-applied CFDP over SPP, in both the Earth User Node and the Space User Node. This deployment shows the file protocol implemented in the ABA Earth User Node, similar to what is described in figure 6-11(a), but it should be noted that the ESLT configuration is the same as figure 6-8(c) configuration.

The following list summarizes the features of configurations shown in figures 7-3 and 7-4.

a) Description of ABA configuration with CFDP end-to-end:

  - this configuration depicts the transfer of files and packets between a single agency (A) Space User Node, and the Earth User Node (MOC), using the space link services of an ESLT provided by agency (B);
  - both agency A and B implement frame-level services, but agency A may also use packets or files inside these frames.

b) End-to-end services provide:

  - bidirectional transfer of space data link frames (TC/TM/AOS link) between the space asset and its control center.

c) Ground cross support services provide:

  - bidirectional transfer of frames between the Earth User Node and ESLT using F-Frame and RAF SLE/CSTS services;
  - encoding and frame merging in the ESLT as part of F-Frame services.

d) Space-ground CCSDS services provide:

  - bidirectional TM/TC/AOS frame transfer.

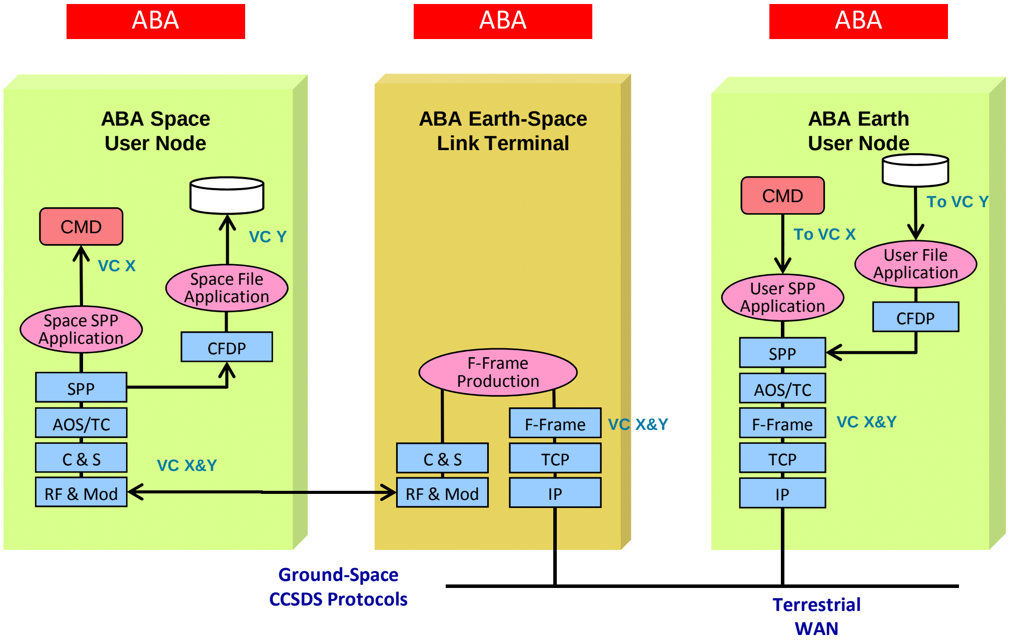


Figure 7-3: ABA End-to-End F-Frame with SPP/CFDP User Protocols

The corresponding ABA end-to-end return configuration is shown in figure 7-4. This deployment uses the RCF service as described in figure 6-8(d). The Earth and Space User Node configurations use variations of the figure 6-10 configuration, but add the optional CFDP protocol as well for file transfers. These diagrams show use of RCF service to permit frame-level data from two different sources, or of two different priorities, to be de-multiplexed in the ESLT and delivered to different destinations. The RAF service could also be used, but then the Earth User Node would have to de-multiplex the separate VCs from the frame stream.

These diagrams all show examples of the use of two different VCs (VC X and VC Y) to separate out the frame traffic containing commands or engineering telemetry from those containing CFDP file PDUs. These configurations may be adapted directly to include additional frame-level telemetry channels or to include multiple packet flows each with their own Application Process Identifier (APID).

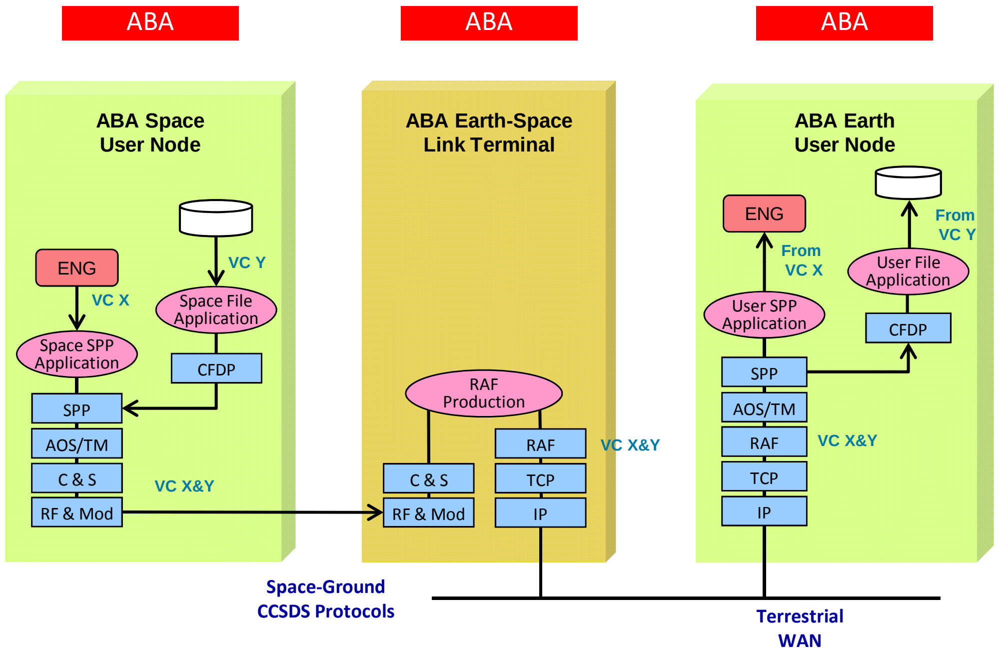


Figure 7-4: ABA End-to-End Return with SPP/CFDP User Protocols

7.2.3 ABA END-TO-END PROTOCOL VIEWS WITH BP DELIVERY

One of the issues that will arise during transition from ABA configurations to a fully supported SSI deployment is to identify just what needs to change in order to move to that configuration, and how the configuration can continue to support ABA missions. Even in some existing ABA configurations, such as ones where a spacecraft has to successively use more than one ground station to downlink a large dataset, adoption of the BP under CFDP may be a distinct advantage. This might particularly be the case for high data volume near Earth missions in LEO or Mid-Earth Orbit (MEO).

Figure 7-5, which is similar to figure 7-3, is intended to describe one possible transition approach. This is still a single-hop, 'ABA' mission configuration, but it includes use of CFDP over BP to transmit files. This deployment shows the file protocol implemented in the ABA Earth User Node, but it uses BP to transfer the data direct to an SSI ESLT over a TCP/IP terrestrial WAN. The ESLT configuration is similar to the figure 6-8(c) configuration used in figure 7-3, but it adds the BP protocols, the bundle agent, and the necessary LTP and frame construction protocols as shown in figure 6-12(b). The ESLT in this configuration provides both legacy ABA space link and space internetworking services, using frame multiplexing in the ground station.

The Space User Node is similarly modified to include the BP protocol stack, and LTP is used to provide reliable data delivery across the long-haul link. More than one VC may be sent at the same time; one can carry BP, while the other carries more normal commands, sent as SPP in this example.

For emphasis in these two diagrams the added BP protocol elements are shaded, and the added data flows are shown in red.

Figure 7-6 is the ABA return diagram that corresponds to the figure 7-5 forward diagram. In this example, engineering data are returned as a stream of SPP, and bulk science data are returned as files using CFDP over BP. Reliable (or best-effort) delivery may be selected in LTP, as needed.

Figures 7-5 and 7-6 also describe the means whereby an SSI space routing node MOC (acting as the Earth User Node in this example) can directly configure and control the space link (ESLT) and use it to transfer Link Layer commands and engineering telemetry to/from the space routing node that it controls. This same core ABA configuration appears at the heart of the ABCBA SSI diagrams.

The following list summarizes the features of configurations shown in figures 7-5 and 7-6.

a) Description of ABA configuration with BP end-to-end delivery added:
   - this configuration depicts the transfer of files and packets between a single agency (A) Space User Node, and the Earth User Node (MOC), using the space link services of an ESLT provided by agency (B);
   - both agency A and B implement frame-level services, but agency A may also use packets or files inside these frames;
   - agency A and agency B both implement the BP services; agency A may use BP to route data to its space asset.

b) End-to-end services provide:
   - bidirectional transfer of space data link frames (TC/TM/AOS link) between the space asset and its control center;
   - secure bidirectional transfer of BP bundles (containing files or other data) between the control center and its space asset (CFDP over BP).

c) Ground cross support services provide:
   - bidirectional transfer of frames between the Earth User Node and ESLT using F-Frame and RAF SLE/CSTS services;
   - encoding and frame merging in the ESLT as part of F-Frame services;
   - bidirectional transfer of bundles between the Earth User Node and the ESLT.

d) Space-ground CCSDS services provide:
   - bidirectional TM/TC/AOS frame transfer;
   - secure bidirectional BP transfers merged with Link Layer.

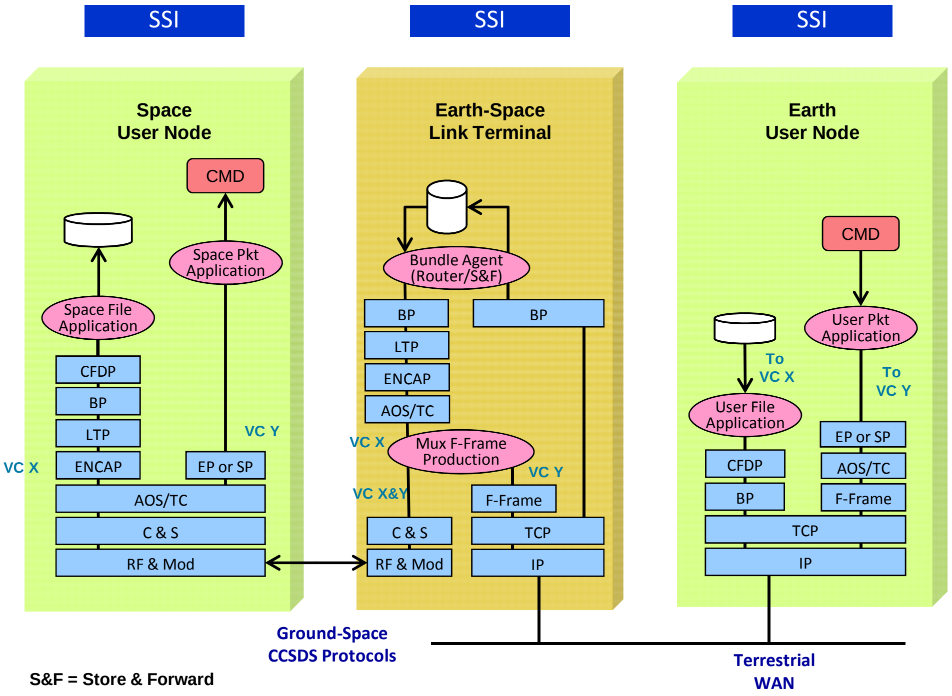


Figure 7-5: Transitional ABA End-to-End Forward Including BP Protocols

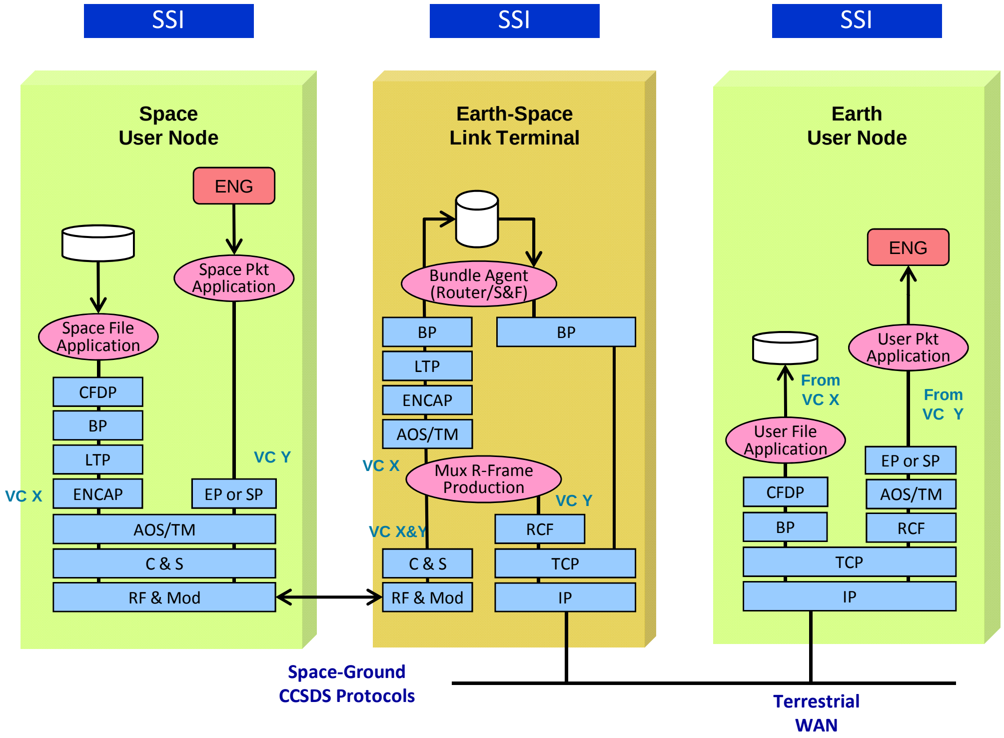


Figure 7-6: Transitional ABA End-to-End Return including BP Protocols

Figure 7-7 is the same mission configuration as is shown in figure 7-5, but in this example the mission is using only the SSI-based protocol stacks to perform all mission command and data transfer functions. The essential commanding and telemetry functions are still present for contingencies, but primary mission operations are all done using SSI protocols, even in this ABA mission configuration. For missions that need to use more than one ground station (ESLT) to downlink large datasets, this may prove to be a highly effective configuration.

The services to support traditional TC/TM commanding are still available within the ESLT F-Frame service, but they are not shown as being used in this figure. The same packet commanding and telemetry services shown in figures 7-5 and 7-6 can still be employed if required.

The following list summarizes the features of the configuration shown in figure 7-7.

a) Description of ABA configuration with BP end-to-end delivery added:
   - this configuration depicts the transfer of files and packets between a single agency (A) Space User Node, and the Earth User Node (MOC), using the space link and SSI services of an ESLT provided by agency (B);
   - both agency A and B implement frame-level services, but agency A is using BP to route data to its space asset.

b) End-to-end services provide:
   - bidirectional transfer of space data link frames (TC/TM/AOS link) between the space asset and its control center;
   - secure bidirectional transfer of BP bundles (containing files or other data) between the control center and its space asset (CFDP over BP).

c) Ground cross support services provide:
   - bidirectional transfer of frames between the Earth User Node and ESLT using F-Frame and RAF SLE/CSTS services;
   - encoding and frame merging in the ESLT as part of F-Frame services;
   - secure bidirectional transfer of bundles between the Earth User Node and the ESLT.

d) Space-ground CCSDS services provide:
   - bidirectional TM/TC/AOS frame transfer;
   - secure bidirectional reliable DTN transfers using BP over LTP merged with Link Layer.

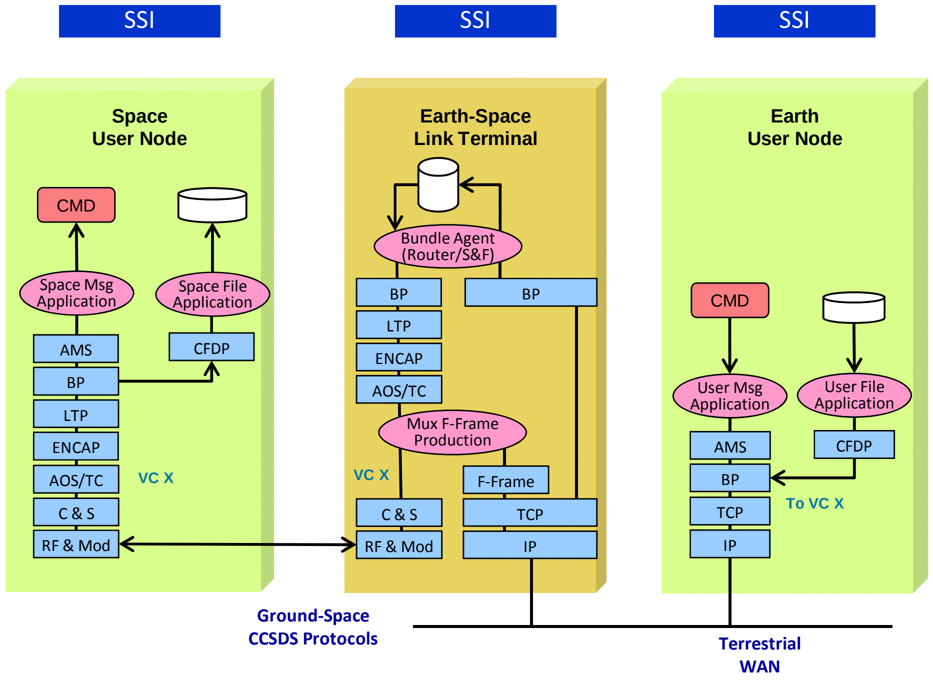


Figure 7-7: Single Link—SSI End-to-End Forward: All DTN

7.3 SSI END-TO-END PROTOCOL VIEWS

7.3.1 CORE SSI END-TO-END ABCBA PROTOCOL VIEWS

Figure 7-8 shows the core SSI end-to-end forward DTN configuration. In this example, there is a light green agency A Earth User Node sending a file to the Space User Node (agency A). This process requires support from a space routing node (agency B) that provides the store-and-forward and data-routing functions for BP traffic. In this example, the space link from Earth to the space routing node is provided by an ESLT operated by agency C. Agency B also manages the space routing node, configures and controls the space link, and uses that same space link to communicate directly with the space routing node to control and monitor its behavior.

The following list summarizes the features of the configurations shown in figures 7-8 and 7-9.

a) Description of SSI ABCBA configuration with BP end-to-end delivery:

   – these configurations depict the transfer of files and packets between an agency (A) Space User Node, and its Earth User Node (MOC), using a space routing node provided by another agency (B) and the space link and SSI services of an ESLT provided by a third agency (C);

   – agencies A, B, and C all implement SSI/DTN services, but agency B may also using frame-level services to control its space routing node asset.

b) End-to-end services provide:
   - bidirectional transfer of space data link frames (TC/TM/AOS link) between the space routing node (B) and its control center (space routing node MOC);
   - secure bidirectional transfer of BP bundles (containing files or other data packets over BP).

c) Ground cross support services provide:
   - bidirectional transfer of frames between the space routing node MOC and ESLT using F-Frame and RAF SLE/CSTS services;
   - frame merging, encoding, and fill insertion in the ESLT as part of F-Frame services.

d) Space-ground CCSDS services provide:
   - bidirectional TM/TC/AOS frame transfers;
   - secure bidirectional reliable DTN transfers using BP over LTP merged into Link Layer.

e) Space-space CCSDS services provide:
   - secure bidirectional reliable DTN using BP over Proximity-1;
   - bidirectional Proximity-1 packet transfer (packet Service Access Point [SAP] of Proximity-1).

In figure 7-8, the Earth User Node and Space User Node exchange data in the form of files, using CFDP and the underlying BP protocols. BP is the end-to-end routing protocol that provides the Network Layer services. The space routing node MOC uses CFDP and BP to communicate to the space routing node, but it also has a frame- and packet-level connection direct to the space routing node for command, control, and tracking functions. This core functionality is exactly as described in figures 7-5 and 7-6. In this example, the forward link to the Space User Node uses the Proximity-1 link protocol, which optionally includes reliable packet delivery, so LTP is not required.

The BP functions on the space routing node may be implemented in a Software-Defined Radio (SDR) that can be programmed to include the Proximity-1 link and DTN functions in one piece of hardware. A similar radio might be used on the Space User Node. There is no requirement to do this sort of implementation, but it is an effective way to deliver a high level of functionality in a single hardware package for space-mission integration. (See figure 7-14 for a concrete example of this approach.)

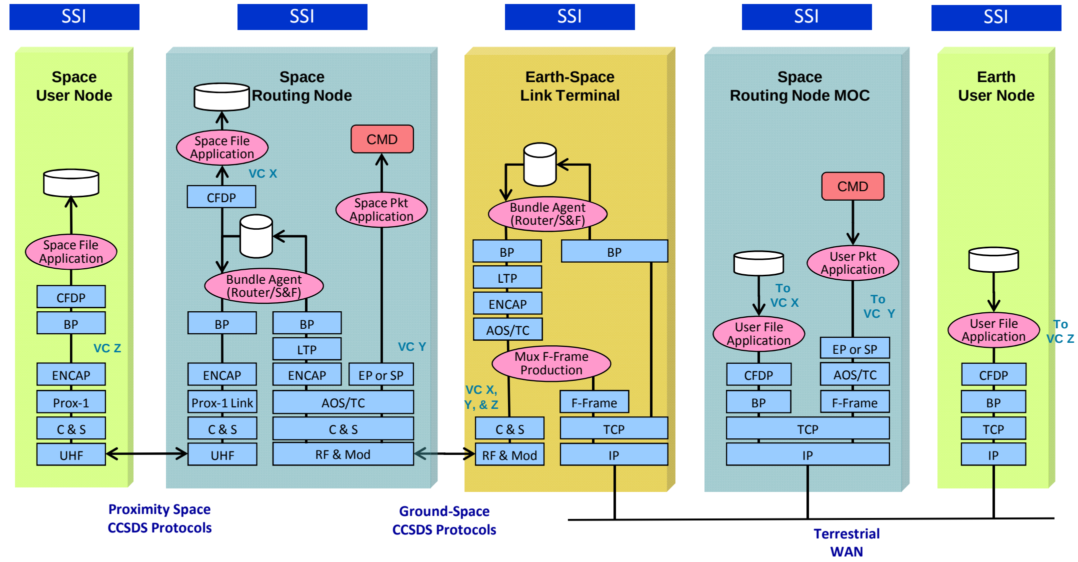


Figure 7-8: SSI End-to-End Forward: All DTN

Figure 7-9 shows the corresponding basic SSI end-to-end DTN return configuration. The Space User Node uses CFDP to transfer a file to the Earth User Node via the space routing node. The ESLT and space routing node MOC provide similar return functions to those described for figure 7-8.

In both of these figures the traffic to/from the Earth User Node travels on the terrestrial WAN direct from the Earth User Node to the ESLT. These data do not need to flow through the space routing node MOC. In order to exercise greater control over the data flow to the space routing node, and depending upon mission policy, it is also possible for the space routing node MOC to implement the DTN Earth routing functions and to require all the data to flow along this path.

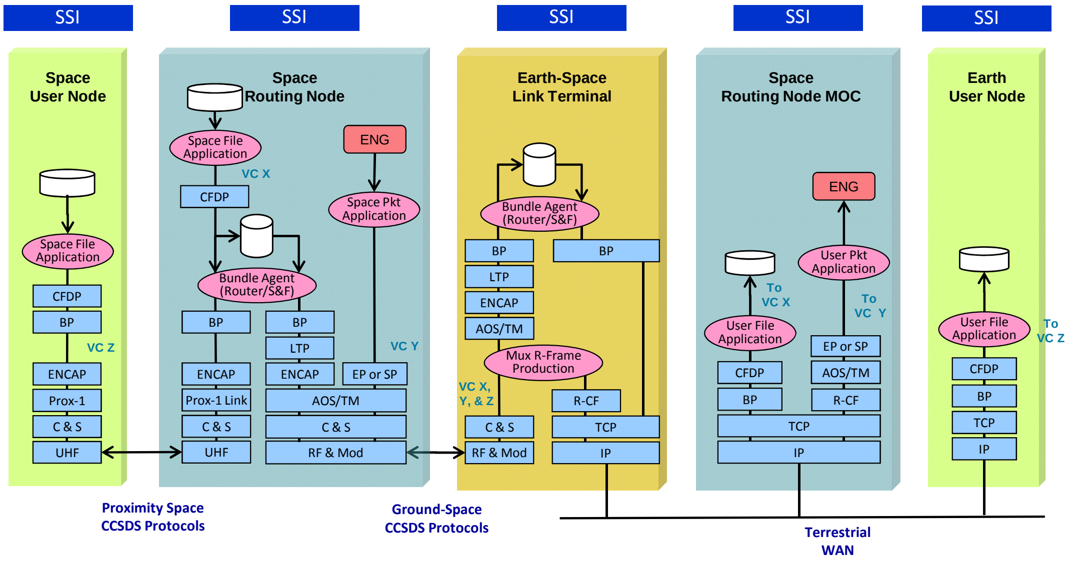


Figure 7-9: SSI End-to-End Return: All DTN

This configuration may be used by hybrid science/routing nodes (figure 7-12) and in the early transition phase, but it is not recommended for future SSI deployments because it imposes higher traffic flows on the space routing node MOC.

7.3.2 SSI PLANETARY SPACE LINK TERMINAL AND WAN PROTOCOL VIEW

Because many different configurations of missions and intermediate nodes are possible, they cannot be presented in any complete or exhaustive fashion. Figure 7-10 is included to show a configuration with one of the other primary SSI CSSEs, a PSLT. For situations where there are a number of assets in orbit around a distant planetary body, or deployed on the surface, there may be a need for a PSLT. This routing node may have one or more of the following: deep space link, Proximity-1 link, WiFi or WiMAX, planetary WAN, or other space or surface links. It may provide routing of data from one node on the surface to another, or from one orbiting asset to another, or from assets on the planet surface to those in orbit around the planet.

Figure 7-10 is a simple extension of the basic configuration shown in figure 7-8; all of the elements that are common to both operate the same and provide the same services. What is added is a PSLT on the planet surface, and this example shows it performing routing to a Space User Node on the planet surface, via some sort of WAN connection (Ethernet in this case). In this example the PSLT does not do Direct-to-Earth (DTE)/Direct-from-Earth (DFE) communications (it could), but is connected via a space routing node using Proximity-1.

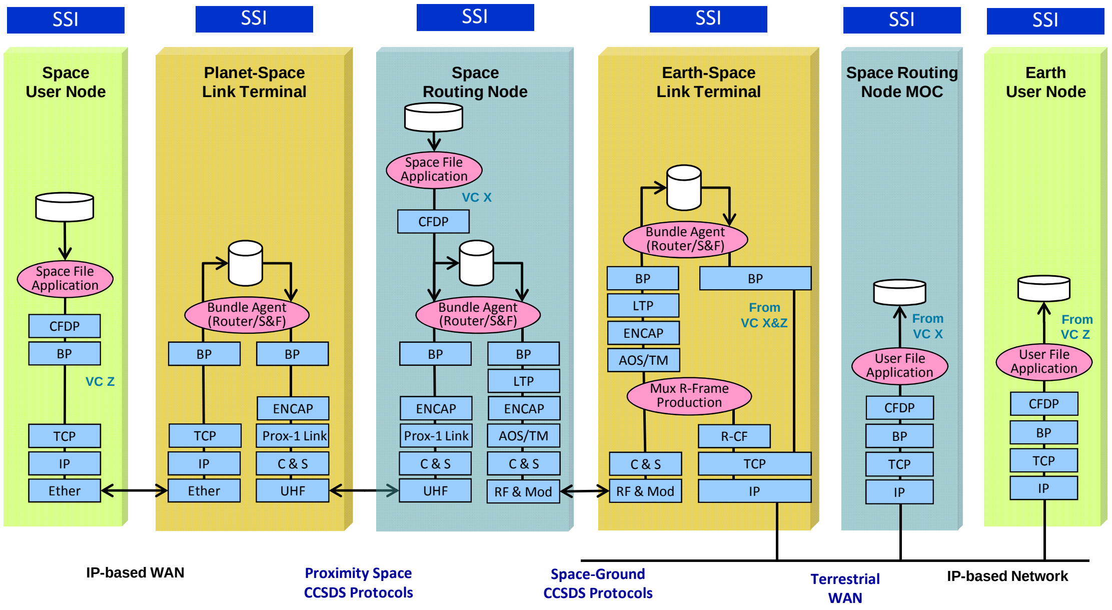


Figure 7-10: SSI End-to-End Forward: All DTN, Showing PSLT

7.3.3 SSI EXTENDED DTN FUNCTIONS: EMERGENCY COMMUNICATIONS AND LAST-HOP DELIVERY

The middle three nodes in the SSI end-to-end configuration shown in figure 7-11 each implement the DTN protocol stack. This configuration provides all of the same services as are present in the core SSI configuration, but it also offers additional services for supporting emergency communications and last-hop delivery to DTN and non-DTN nodes.

The last-hop service on the space relay node implements the last-hop delivery agent. This delivery agent is capable of delivering a variety of different types of commands, in different forms, to the last-hop Space User Node. In this example, that node is an ABA node; it is not a proper part of the SSI itself, but it could equally well be an SSI node that needs to be ‘rebooted’. The Earth User Node must construct this delivery package with the required commands and instructions, and use file-delivery services to send the file to the last-hop delivery agent. Details of this last-hop service and the delivery package have already been described in 4.4 and 6.5.3.1.

Standard SSI services are used to deliver the file from the ABA Earth User Node to the space routing node delivery agent, which performs its duties based on the instructions in the file. In this case, the ABA Earth User Node sends a file containing commands in coded TC blocks, and the delivery agent uses the Proximity-1 packet SAP to deliver these commands to the Space User Node. The file could also have contained SPP packets in telecommand frames, or file-formatted data, and the delivery package could have asked for the Proximity-1 User-Defined Data (Prox UDD) SAP to be used to transmit the data as a bit stream.

Another protocol present in this diagram is the CSTS forward/return file-transfer service. This service is TBD, but it is expected to be a secure file-transfer service that reliably delivers a file and associated delivery metadata. In this case, the Earth User Node uses this service to send the delivery package file to the SSI ESLT, which then uses CFDP to send the file over BP to the delivery agent on the space routing node.

The following list summarizes the features of the configurations shown in figures 7-11, 7-12, and 7-13.

a) Description of SSI ABCBA configuration with first/last-hop delivery:
   - these configurations depict the transfer of a forward or return delivery package between agency (A) Space User Node, and its Earth User Node (MOC), using a space routing node provided by another agency (B) and the space link and SSI services of an ESLT provided by a third agency (C);
   - agencies B and C implement SSI/DTN services;
   - agency A may implement SSI service, or it may only implement ABA services and the first-hop/last-hop delivery package function;
   - agency B implements the first-hop and/or last-hop delivery services to provide emergency commanding or essential telemetry for the agency A space user asset.

b) End-to-end services provide:
   - bidirectional transfer of space data link frames (TC/TM/AOS link) between the space routing node (B) and its control center (space routing node MOC);
   - secure bidirectional transfer of delivery packages (containing frames, files, or other data) between the Earth User Node (A) and its Space User Node asset (delivery package file over BP and delivery agent).

c) Ground cross support services provide:
   - bidirectional transfer of frames between the space routing node MOC and ESLT using F-Frame and RAF SLE/CSTS services;
   - encoding and frame merging in the ESLT as part of F-Frame services;
   - secure bidirectional transfer of files between the Earth User Node and the ESLT (files over forward/return-file service);
   - merging of files into DTN stream for delivery to the space routing node (files over BP).

d) Space-ground CCSDS services provide:
   - bidirectional TM/TC/AOS frame transfers;
   - secure bidirectional reliable DTN transfers using BP over LTP merged into Link Layer.

e) Space-space CCSDS services provide:

   - bidirectional Proximity-1 bit-stream transfer (Prox UDD);
   - bidirectional first-hop/last-hop Link Layer services over Proximity-1 (delivery agent).

f) Node-specific functions include:

   - agency A Earth User Node must provide forward/return delivery package assembly/processing functions;
   - agency B space routing node must handle first-hop/last-hop delivery package processing and delivery agent functions;

Figure 7-11 shows the forward, last-hop, service. This figure shows the transfer of a delivery package of spacecraft commands in the form, in this case, of TC frames that are sent to the space routing node and packaged for delivery to the ABA Space User Node.

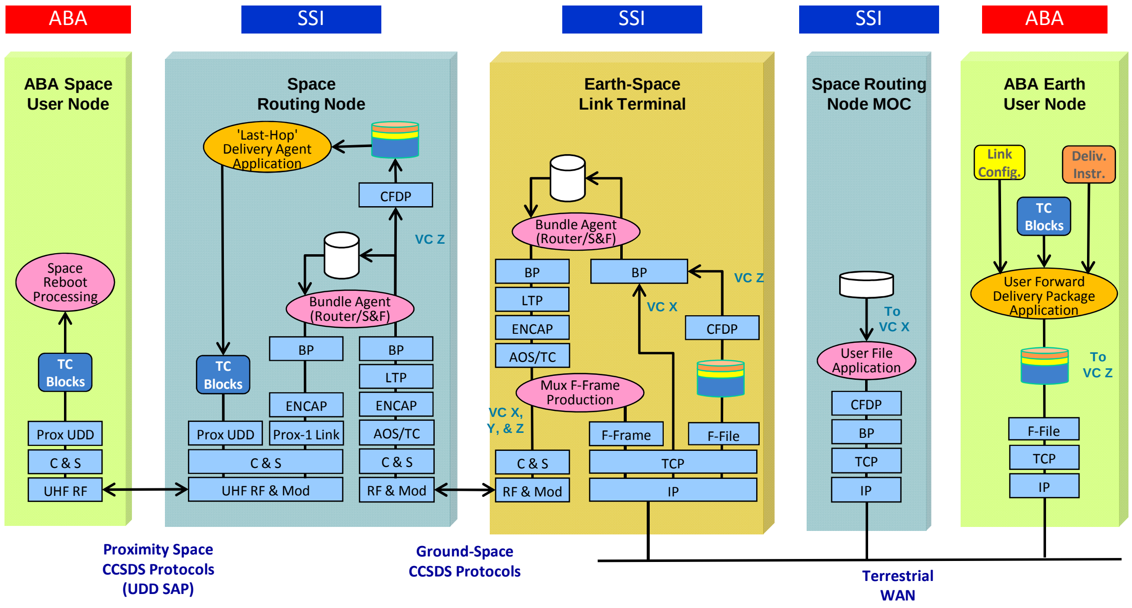


Figure 7-11: SSI End-to-End Forward: DTN Agency Supporting ABA Agency, Including Last-Hop Service and CSTS Forward-File

Figure 7-12 shows the corresponding return first-hop service. This figure shows the return of ‘essential telemetry’ in the form of engineering telemetry data, in space or encapsulation packets, that are acquired on the space routing nodes and packaged for delivery.

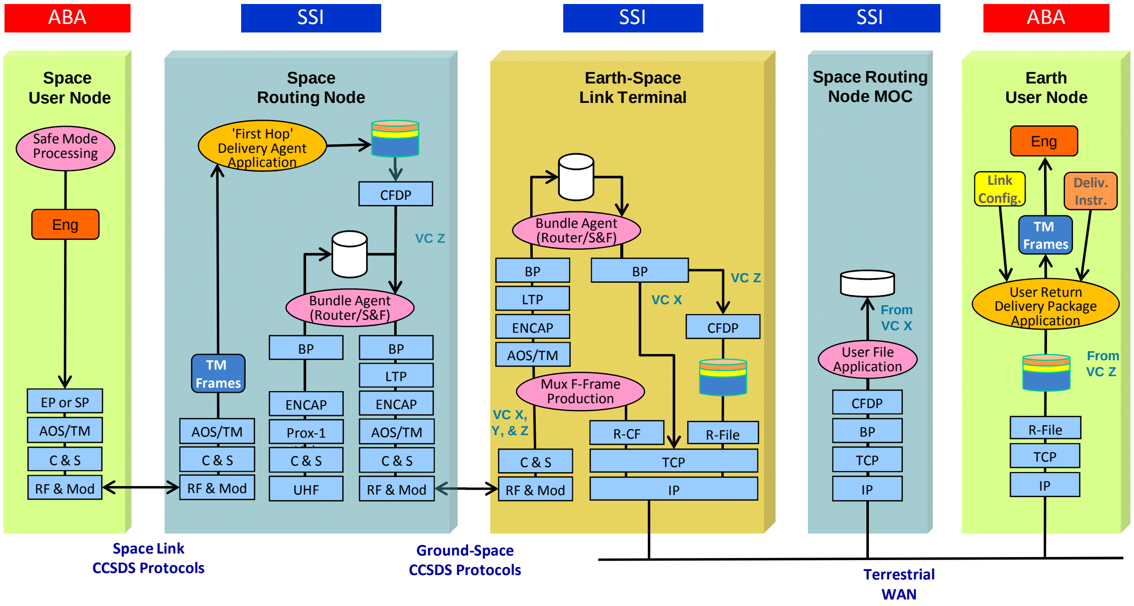


Figure 7-12: SSI End-to-End Return: DTN Agency Supporting ABA Agency, Including First-Hop Service and CSTS Return File

Figure 7-13 shows a different return example that uses the first-hop delivery agent to acquire Open-Loop (O/L) recordings while tracking an Entry, Descent, and Landing (EDL) activity. Such data can be critical to understanding what is going on in a lander during the last few minutes while it plunges toward a planetary surface for a (hopefully gentle) landing.

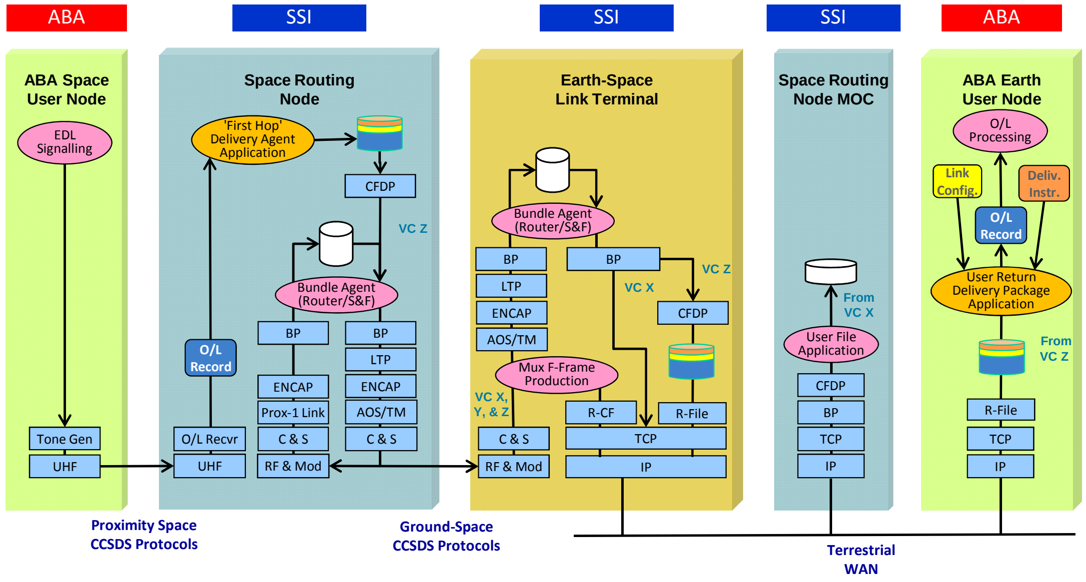


Figure 7-13: SSI End-to-End Return: DTN Agency Supporting ABA Agency, Including Open Loop Recording Using First-Hop Service

7.3.4 SSI TRANSITION: ABA AGENCY SUPPORTING SSI AGENCY

At any point in the deployment of the SSI there will be agencies implementing the SSI protocols and services and also agencies that chose not to. Figure 7-14 represents such a configuration, where an agency that does not natively support DTN agrees to carry a payload on its space routing node that internally hosts DTN services. In this way, at modest impact to the supporting agency, the agency will be in position to provide SSI routing services even though it does not use them itself.

The essential element in this strategy is the presence onboard the ABA space routing node of a capable radio that hosts the necessary SSI services. This example shows a modified Electra radio (which uses SDR technology) that has been provided to the ABA agency that builds and operates the space routing node. In this example, the space routing node MOC is designed to only operate using standard TC/TM protocols and SPs. From the point of view of the space routing node and its MOC, it operates in its normal fashion, but in reality it shares access to the space link (supported by an SSI ESLT) with the SSI Earth User Node. As noted in 7.3.1, the space routing node MOC could also implement an Earth routing node to exercise more control over traffic going to the spacecraft it operates, but that is not shown here.

What really makes this configuration work is that the ABA space routing node incorporates the DTN-enabled SDR, and that the ESLT implements the full SSI-compliant ground-station functions that include frame merging. It is possible to create an ABCBA configuration where the ESLT only implements the standard ABA ground-station configuration, but in that case, the space routing node MOC must be configured to 1) accept DTN traffic to and from the Earth User Node MOC, 2)create encoded frames, and 3) merge these into its own frame stream.

The following list summarizes the features of the configuration shown in figure 7-14.

a) Description of ABA agency supporting DTN agency configuration:

   – this configuration depicts the transfer of DTN traffic between an agency (A) Space User Node, and its Earth User Node (MOC), using an ABA space routing node provided by another agency (B) and the space link and SSI services of an ESLT provided by a third agency (C);

   – agencies A and C implement SSI/DTN services;

   – agency B only implements ABA services in its space routing node MOC;

   – agency B hosts an SSI-compliant radio on its space routing node to provide SSI services for the Agency A space user asset.

b) End-to-end services provide:

   – bidirectional transfer of space data link frames (TC/TM/AOS link) between the space routing node (B) and its control center (space routing node MOC);

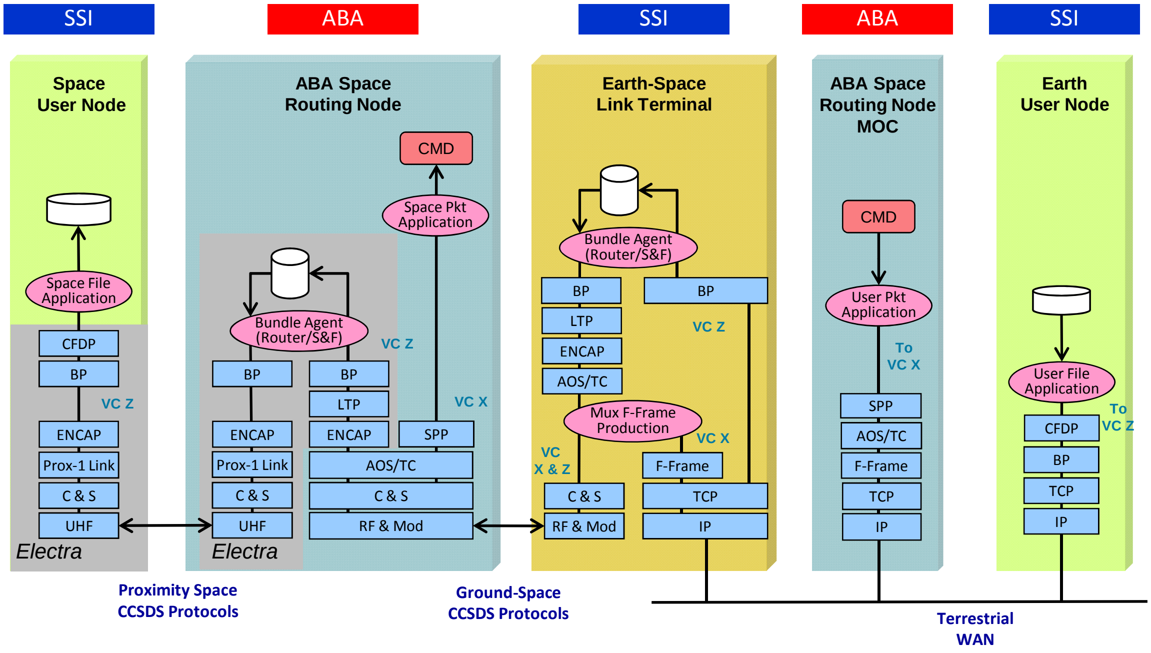


Figure 7-14: SSI End-to-End Forward: ABA Agency Supporting SSI Agency, Integrated Specialized Onboard Relaying Service

- secure bidirectional transfer of DTN bundles (containing frames, files, or other data) between the Earth User Node (A) and its Space User Node asset (DTN over space link).

c) Ground cross support services provide:

- bidirectional transfer of frames between the space routing node MOC and ESLT using F-Frame and RAF SLE/CSTS services;
- encoding and frame merging in the ESLT as part of F-Frame services;
- merging of DTN stream into frames for delivery to the space routing node (TM/TC/AOS frames).

d) Space-ground CCSDS services provide:

- bidirectional TM/TC/AOS frame transfers;
- secure bidirectional reliable DTN transfers using BP over LTP merged into Link Layer.

e) Space-space CCSDS services provide:

- bidirectional Proximity-1 reliable transfer (Prox-1 link);
- bidirectional DTN services over Proximity-1 (SSI-compliant radio).

f) Node-specific functions include:

  - agency B space routing node must host SSI-compliant radio and manage transfer of segregated frame stream.

The SSI ESLT accepts DTN bundles from the Earth User Node, and when it is signaled that the space link is available, it transmits these data to the space relay node. On the space relay node these data are treated just like another TC/TM frame stream (VC Z), but that stream is sent to the Electra radio for processing. The functions described in the Electra could also be implemented in other ways. Internal to the Electra are the normal BP and bundle-agent functions, a CFDP protocol engine, and local, internal storage. The intent of this approach is to make the least impact on ABA design and resources while providing high functionality.

For communications to take place between the space routing node and Space User Node, there may need to be a certain amount of accommodation in ABA space routing node operations, such as scheduling the downlink, orienting the spacecraft, and making sure the necessary power and storage reserves are available to run the downlink. Once that is accomplished, the Electra actually can, given permission, signal the Space User Node on the planet surface, acquire the signal, and run the downlink passes to the surface asset.

One further consideration must be pointed out in this example: the ABA space routing node may also use the SPP port on the Electra to send SPs to its own, ABA-style, Space User Node (not shown). In this way the space routing node actually provides dual services, one path that is SSI-compliant and can support SSI routing and relaying functions, and another that supports its own, private, ABA functions.

7.4 SECURITY CONCEPTS FOR END-TO-END PROTOCOL VIEW

Security for the end-to-end protocol view utilizes all of the security elements described in earlier sections. In addition, this view is where use of end-to-end user encryption will be shown as a means to secure transfers to the final space routing nodes or Space User Nodes. This was described in 6.8. For SSI missions, Network Layer security may also be applied, or users may choose to apply encryption at the Application Layer. This was also described earlier.

Figure 7-15 shows two approaches for securing the data in an ABA end-to-end configuration. These optional stack elements are shown in green. SDLS is used to provide end-to-end Link Layer security for an SPP packet flow. The ABA user node may apply one (or both) of the encryption or authentication algorithms to packet data, load this into an AOS or TC frame inside the SDLS security block, and then use the normal service delivery mechanisms to transmit the data to the user space node, as reflected by the SDLS authentication/encryption layer. It should be noted that the ESLT service provider stack in figure 7-15 does not show the presence of the SDLS authentication/encryption layer, since that security block is opaque to the CSTS F-Frame service.

Alternatively, the User MOC may apply encryption or authentication to a data file (File Secure) and that file may then be merged into the secure forward frame stream. In both of these cases the ABA Space User Node must be prepared to undo the security that has been applied, and some private means for establishing and managing keys must also be implemented. Both of these methods offer end-to-end Link Layer security.

This figure also shows use of IPsec as an additional layer of encryption that optionally may be applied at the Network Layer to secure the IP traffic over the Internet. In most configurations, one or another of these mechanisms might be employed; however, it would be unusual to elect to use all of them, as shown in this figure.

Figure 7-16 shows three separate, optional alternatives for securing an SSI end-to-end data transfer, using DTN and either AMS or CFDP in this example. The SSI Earth User Node may apply one of the encryption or authentication algorithms to its command data and load that into a file. The secured file provides end-to-end data security. That secured file, or AMS messages as in this example, may be transferred in a BP bundle, which itself may be secured by the BSP. On the terrestrial hop, BP/BSP may then use TCP/IP and IPsec to securely transmit the data to the ESLT. The ESLT, which merges data from multiple sources, will reapply BSP security for the ELSE to Space User Node hop. Once the file is securely on the space node, the file security may be removed.

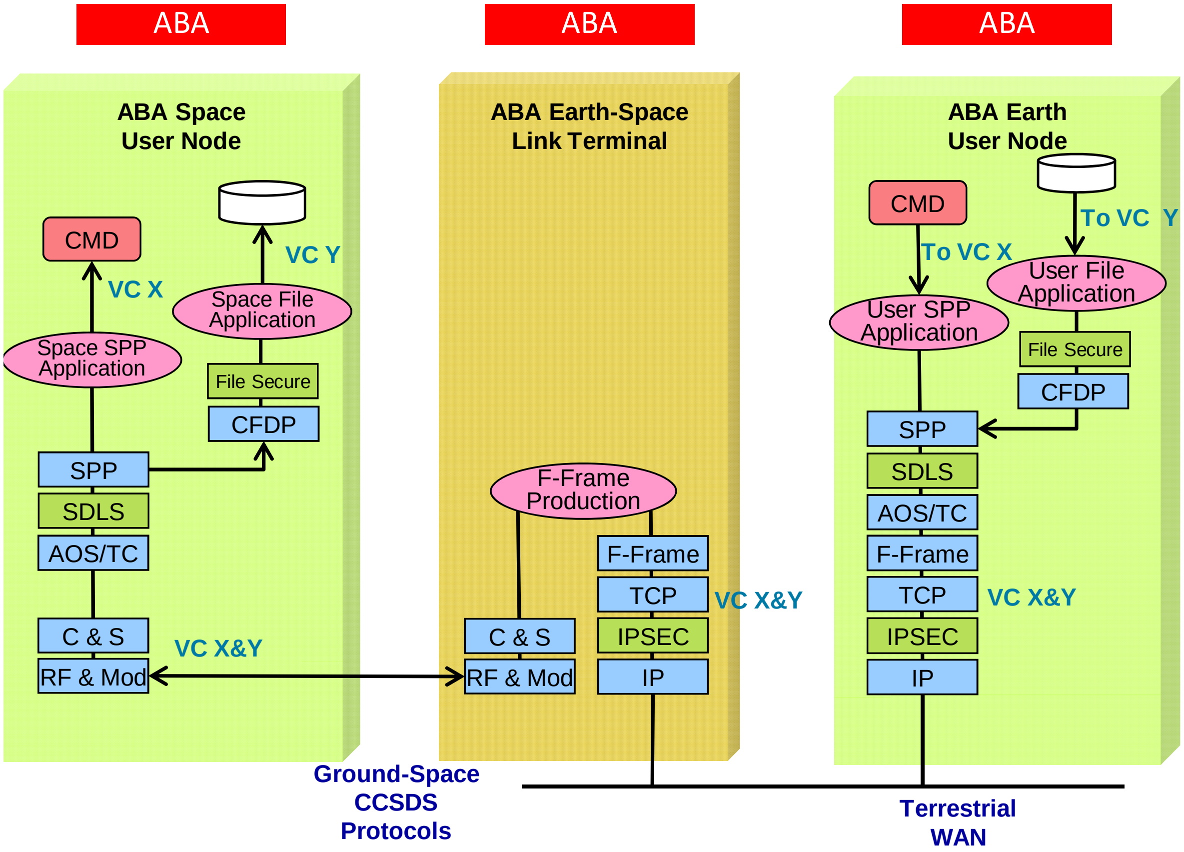


Figure 7-15: ABA Secure End-to-End Forward: ABA Agency Supporting ABA Agency

These same mechanisms work across multiple SSI hops. The final layers of security are only applied and removed in the end nodes.

It will seldom be the case that all of these security measures will be applied in any one deployment, but it is possible. Where terrestrial security is essential, IPsec may be applied, as this masks Internet traffic from any snooping. BSP may be employed end-to-end for command security or where service providers that do not belong to the same agency as the user are involved. If a given Space User Node hosts instruments belonging to different agencies, it might elect to separately secure their command uplinks, or data returns, by use of file-level security.

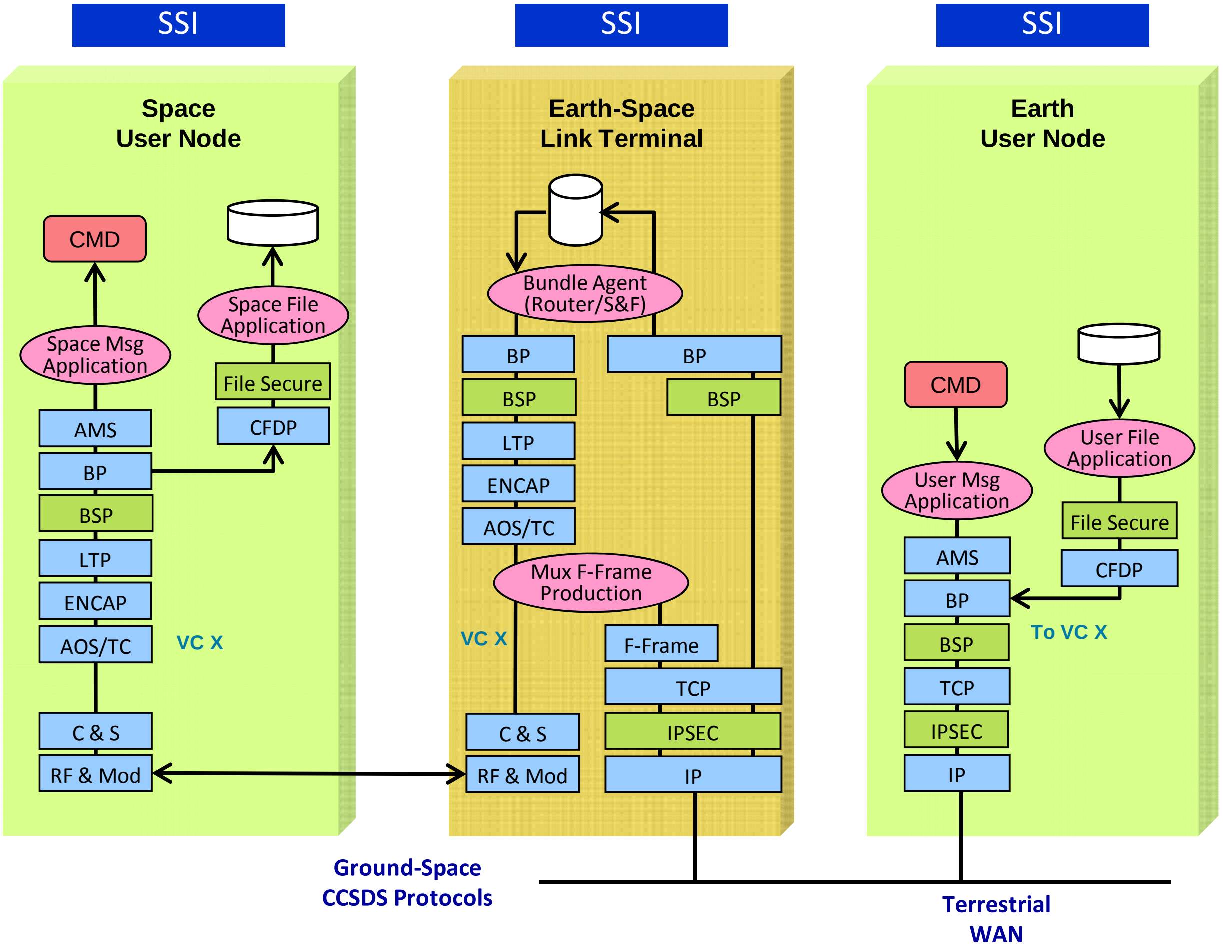


Figure 7-16: SSI Secure End-to-End Forward: SSI Agency Supporting SSI Agency

ANNEX A

ACRONYMS

ADD	Architecture Description Document
ADM	Application Data Models
AMS	Asynchronous Message Service
AOS	Advanced Orbiting Systems
APID	Application Process Identifier
ARD	Architecture Requirements Document
AS	Autonomous System
ASR	Authority Schedule Request
BCH	Bose, Chaudhuri, Hocquenghem
BP	Bundle Protocol
BSP	Bundle Security Protocol
Cat-5	Category 5 Ethernet cabling
CBHE	Compressed Bundle Header Encoding
CCSDS	Consultative Committee for Space Data Systems
CCP	Composite Contact Plan
CFDP	CCSDS File Delivery Protocol
CGR	Contact Graph Routing
CGRP	Contact Graph Routing Protocol
CLTU	Command Link Transmission Unit
CM	Complex Management
COTS	Commercial-Off-The-Shelf
CSRM	Cross Support Reference Model

CSSE	Cross Support Service Element
CSSS	Cross Support Service System
CSTS	Cross Support Transfer Services
CXFS	Cross-Support File Service
DFE	Direct-from-Earth
DINET	Deep Impact Network
DMZ	demilitarized zone
DOR	Differential One-way Range
DSN	Deep Space Network
DTE	Direct-to-Earth
DTN	Delay-Tolerant Networking
EDL	Entry, Descent, and Landing
ENCAP	Encapsulation (Packet Service)
EP	Encapsulation Packet
ESLT	Earth-Space Link Terminal
F-CLTU	Forward-Command Link Transmission Unit
FTP	File Transfer Protocol
GDS	Ground Data System
HEO	High Earth Orbit
HTTP	Hypertext Transfer Protocol
ICD	Interface Control Document
I/F	Interface
IETF	Internet Engineering Task Force
IOAG	Interagency Operations Advisory Group
IOP	Inter-Operability Plenary

IP	Internet Protocol
IPsec	Internet Protocol Security
ISO	International Standards Organization
ISP	Internet service provider
ISS	International Space Station
LAN	Local Area Network
LEO	Low Earth Orbit
LTP	Licklider Transmission Protocol
MAD	DSN Madrid Deep Space Communications Complex (also MDSCC)
MEO	Mid-Earth Orbit
MIB	Management Information Base
MOC	Mission Operations Center
MSPA	Multiple Spacecraft Per Aperture
O/L	Open Loop
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PTT	Public Telephone & Telegraph
PSLT	Planet-Space Link Terminal
QoS	Quality of Service
RAF	Return All Frames
RASDS	Reference Architecture for Space Data Systems
RCF	Return Channel Frames
RFC	Request for Comment
RTLT	Round-Trip Light Time
RUFT	Return Unframed Telemetry

S&F	Store & Forward
SAP	Service Access Point
SCID	Spacecraft Identifier
SCCS	Space Communications Cross Support
SD	Service Delivery
SDR	Software-Defined Radio
SFTP	Secured File Transfer Protocol
SI	Space Internetwork
SISG	Space Internetworking Strategy Group
SLA	Service-Level Agreement
SLE	Space Link Extension
SM	Service Management
SNMP	Simple Network Management Protocol
SP	Space Packet
SPP	Space Packet Protocol
SR	Service Request
SSI	Solar System Internetwork/Internetworking
SSI-SP	Solar System Internet Service Provider
SSOC	Science Operations Center
TBD	To Be Determined
TC	Telecommand (pertains to TC Space Data Link Protocol)
TCP/IP	Transmission Control Protocol/Internet Protocol
TDRS	Tracking and Data Routing Satellites
TM	Telemetry (pertains to TM Space Data Link Protocol)
TT&C	Telemetry, Tracking & Command

UDD	User Defined Data
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
VC	Virtual Channel
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access (4G Wireless, IEEE 802.16)
XML	eXtensible Markup Language

ANNEX B

BACKGROUND

The IOAG chartered a Space Internetworking Strategy Group (SISG) at the IOAG-11 meeting in June, 2007, which resulted in the following resolution:

> The IOAG resolves to form a Space Internetworking Strategy Group to reach international consensus on a recommended approach for transitioning the participating agencies towards a future ‘network centric’ era of space mission operations. The group will focus on the extension of internetworked services across the Solar System, including multi-hop data transfer to and from remote space locations and local networked data interchange within and among the space end systems.

The SISG produced the *Recommendations on a Strategy for Space Internetworking (SISG Phase 1 Report)* (reference [64]), that was accepted at the IOAG-12 meeting (October, 2008) and presented in summary form at the second Inter-Operability Plenary meeting (IOP-2) in December 2008. Resolution #6 from IOP-2 directed that:

> The IOAG’s Space Internetworking Strategy Group (SISG) should formalize a draft Solar System Internetwork (SSI) Operations Concept and candidate architectural definition in time for IOAG-13 and should prepare a mature architectural proposal for review and endorsement at the third Inter-Operability Plenary meeting (IOP-3).

Subsequent to that directive, the SISG formed a set of study teams to develop an IOAG Service Catalog #1 for standard link services (reference [17]), an Operations Concept for the SSI (reference [3]), and an SSI Issue Investigation and Resolution (reference [6]). These documents, taken together, provide management, operational, and high-level technical guidance for the development of specific standards for developing the SSI. The IOAG has subsequently asked CCSDS to accept the task of producing the SSI ADD (IOAG-14 meeting, November, 2010).

This document is part of the response to that request. A more narrowly focused, high-level, SSI Architecture Informational Report (Green Book) is also being produced (reference [9]).