Space Communications Protocol Standards Overview

Robert Durst
The MITRE Corporation
(703) 883-7535
durst@mitre.org

6 April 1998

SCPS Project: A Joint DoD/NASA Effort

- Motivation
  - Help mitigate the resource constraints (e.g., dollars, personnel) on government programs
  - Foster cooperation and interoperability across mission, agency, and national boundaries
- Goals
  - Determine feasibility of standardizing end-to-end data communications across civil and military space systems
  - For cases where standardization is feasible, establish *common* standards
- Means
  - Form the Space Communications Protocol Standards (SCPS) Technical Working Group (TWG) to fulfill the above goals

Project Background

- AIAA-brokered introductions between NASA and USSPACECOM in the Fall of 1991
- 1992 - NASA/DOD meetings, NASA participation in GPALS TIM
- 1993-1994 SCPS Phase 1 - Exploration and Definition
  - Investigate requirements and protocol capabilities
- 1995-1997 SCPS Phase 2 - Development
  - Specification, implementation, and test
- 1998 -> SCPS Phase 3 - Deployment
  - Roll-out and standards finalization

Driver: Changing Mission Environments

- Reduction in budgets, reduction in size of individual missions
- Increased reliance on cooperation/interoperability across mission, agency, and national boundaries
- Pressure to reduce operations budgets through shared infrastructure and increased automation
- Strong pressure to use COTS technology

Related Activities

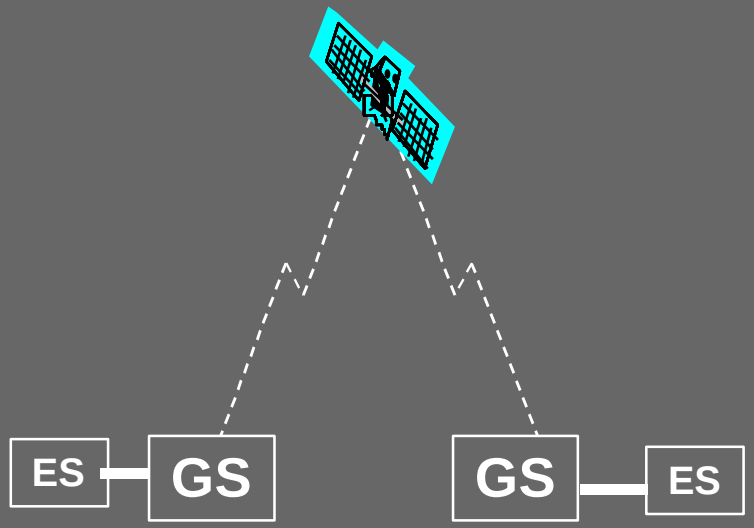
- Mission Operations Control Architecture
  - A family of industrially-derived application-layer protocols for standard command and control of both spacecraft and their supporting ground networks
  - Layered on top of SCPS protocols
- Efficient modulation techniques
  - Attempting to accommodate demands for greatly increased data rates coupled with government RF spectrum encroachment
  - Part of an overall efficiency thrust involving spectrum, communications protocols and applications
  - Layered below SCPS protocols -- SCPS a major factor in achieving efficient communications

Operating Environments

- SCPS protocols were *originally* conceived for communication in which a spacecraft served as one endpoint of the communication
- Original requirements included cross-linked satellite systems, such as Brilliant Eyes, Teledesic, etc.
- Striking similarities were noted between the constraints that satellites face and those of mobile/wireless tactical communication -- solutions applicable to those environments as well
- Immediate utility to SATCOM environments
- Following slides illustrate these environments

Example Networking Environment

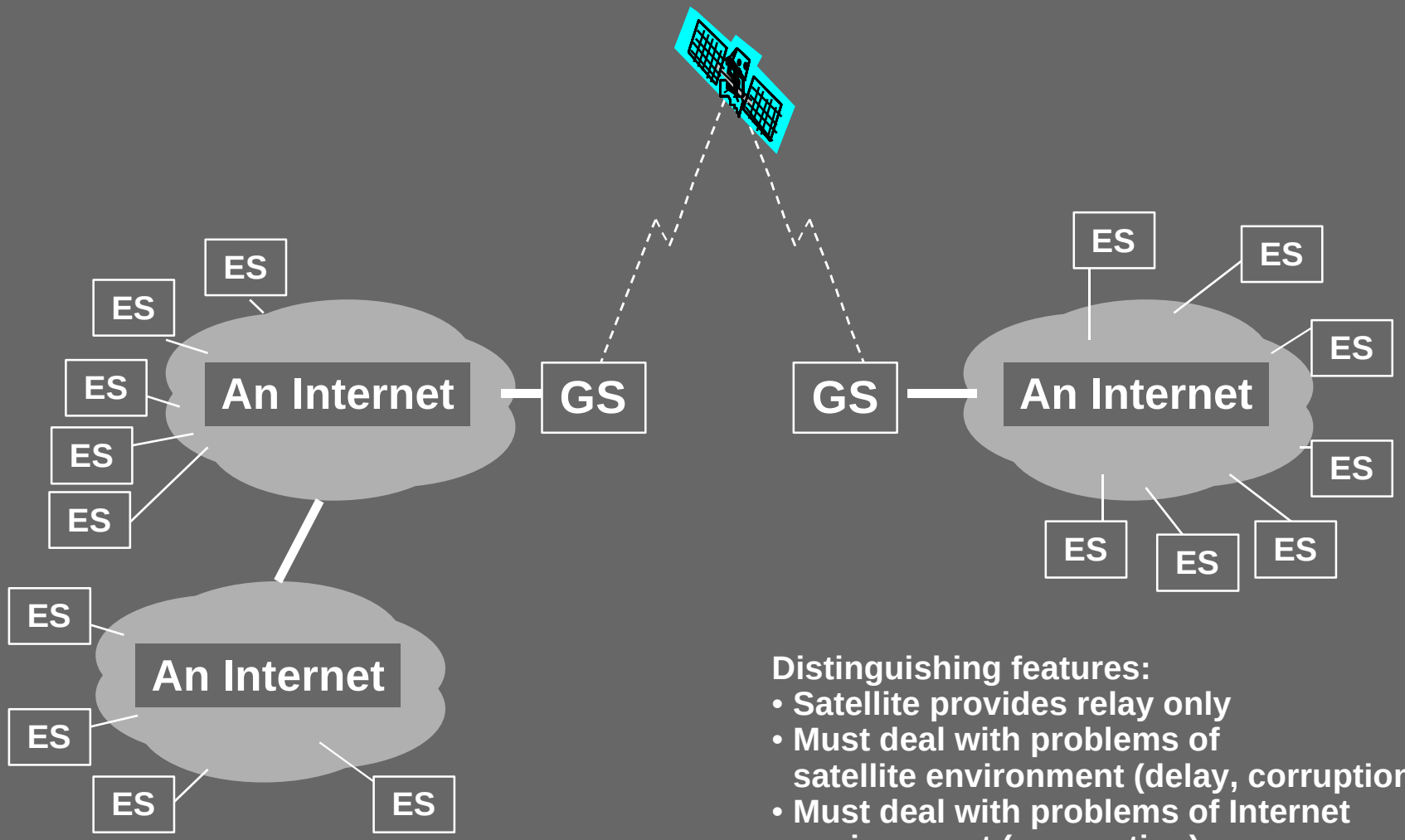
Non-networked SATCOM Environment



Distinguishing features:
- **Satellite provides relay only**
- **End Systems do not contend for access to satellite link (all managed)**

Example Networking Environment

Networked SATCOM Environment

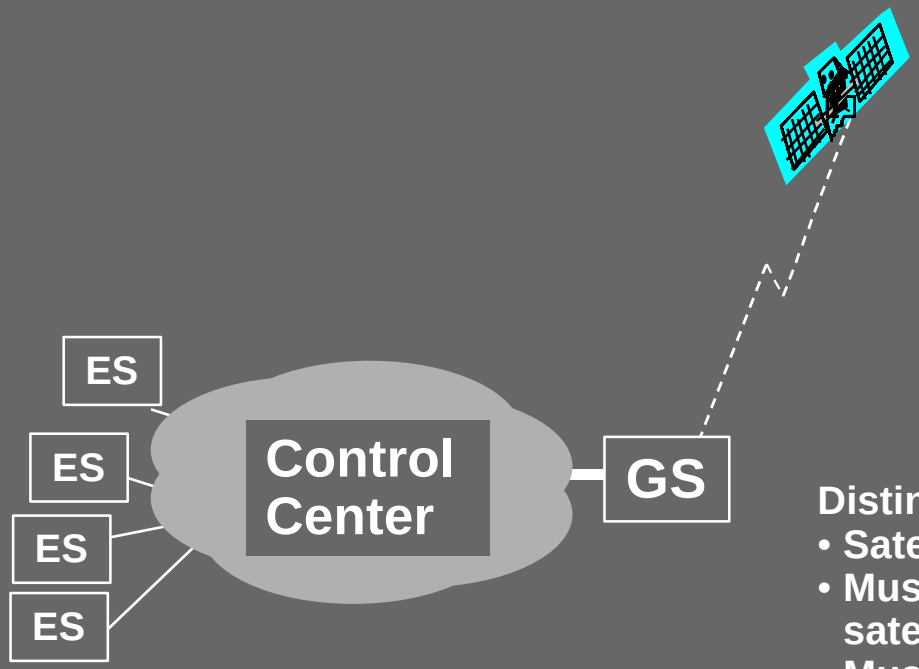


Distinguishing features:

- **Satellite provides relay only**
- **Must deal with problems of satellite environment (delay, corruption)**
- **Must deal with problems of Internet environment (congestion)**

Example Networking Environment

Non-crosslinked TT&C Environment

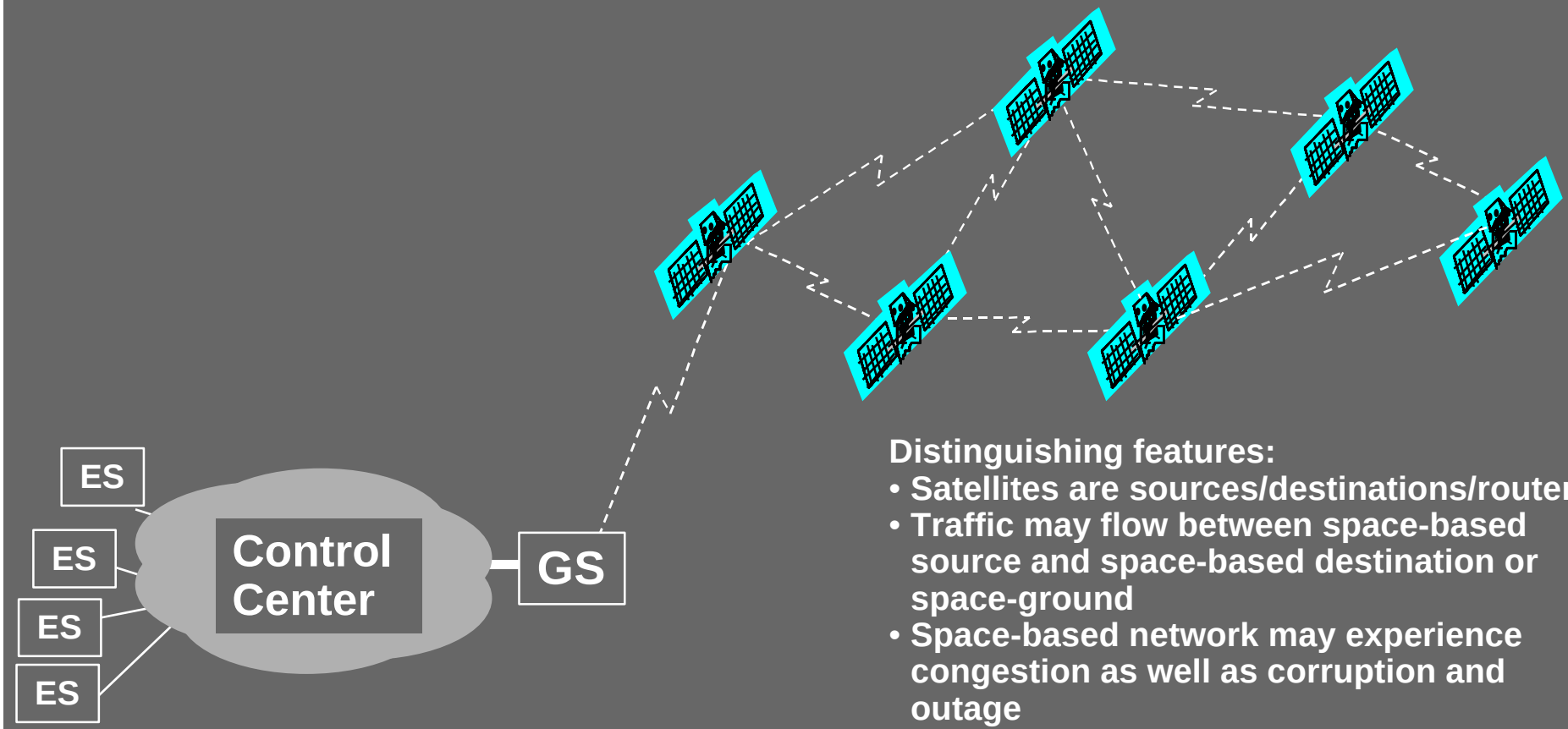


Distinguishing features:

- **Satellite is source/destination of data**
- **Must deal with problems of satellite environment (delay, corruption)**
- **Must deal with problems of Internet environment (congestion)**
- **Note: TT&C term used loosely -- equally applicable to mission/payload data and control**

Example Networking Environment

Crosslinked TT&C Environment

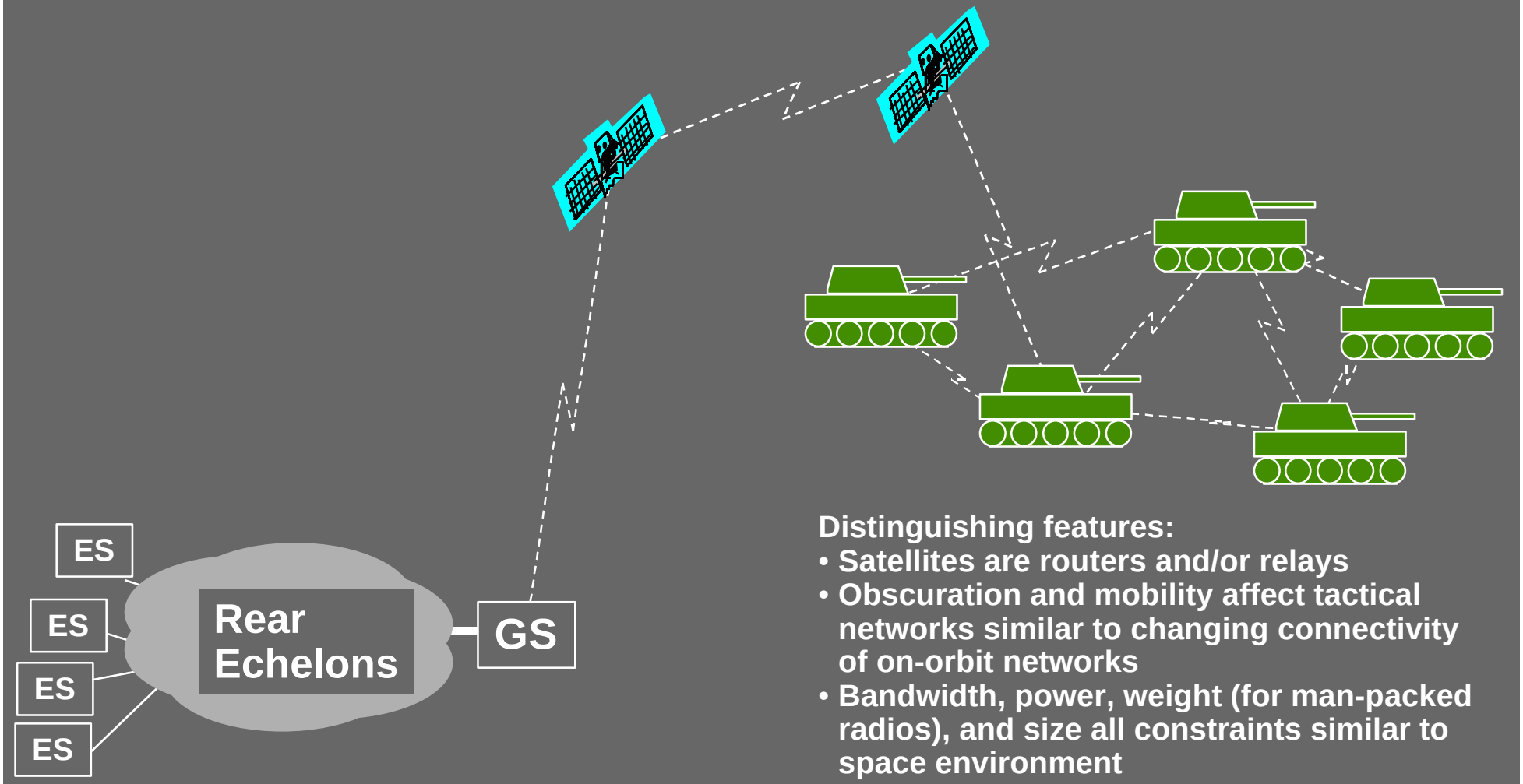


Distinguishing features:

- **Satellites are sources/destinations/routers**
- **Traffic may flow between space-based source and space-based destination or space-ground**
- **Space-based network may experience congestion as well as corruption and outage**

Example Networking Environment

Tactical Communications Environment

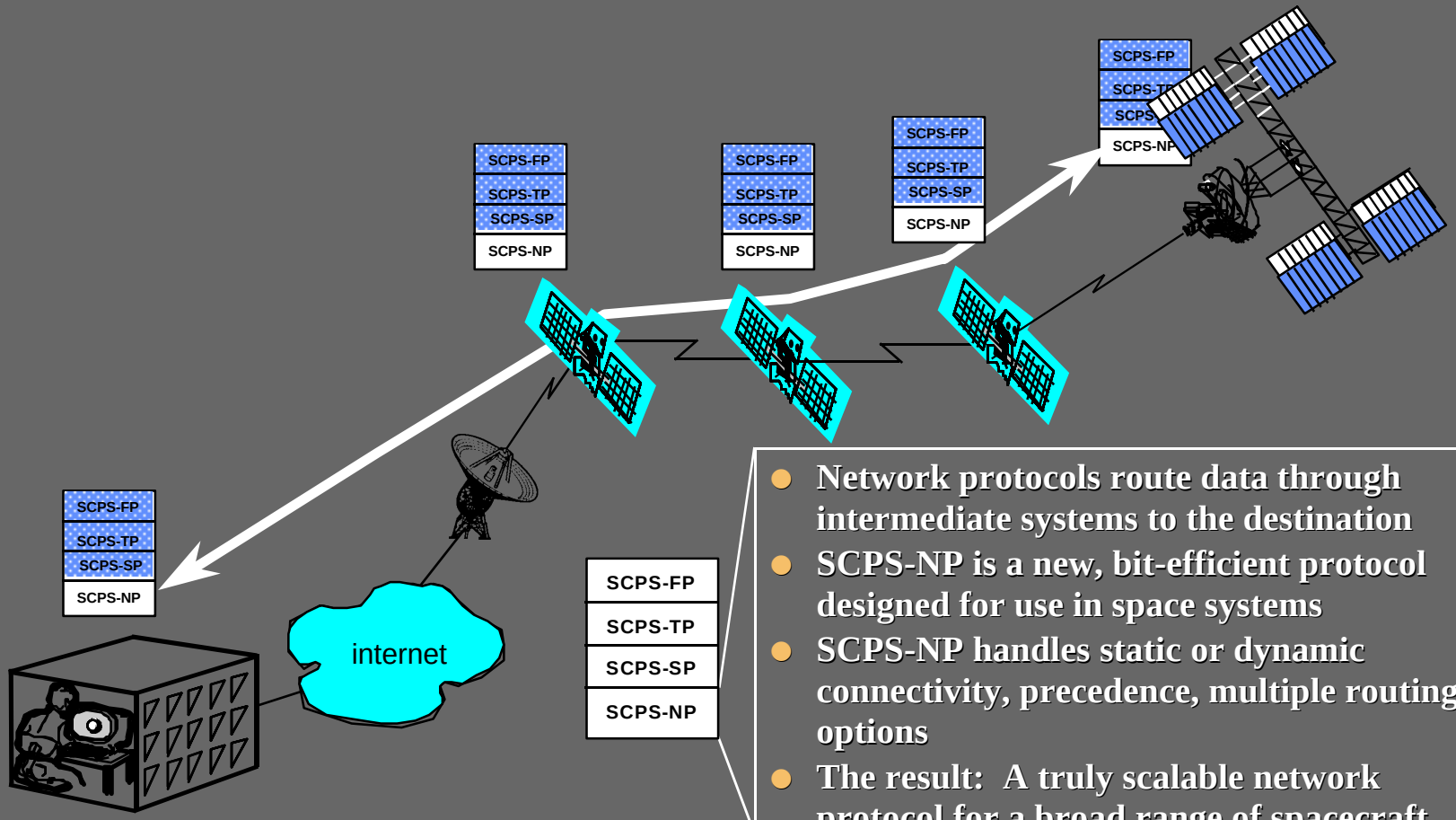


Distinguishing features:

- Satellites are routers and/or relays
- Obscuration and mobility affect tactical networks similar to changing connectivity of on-orbit networks
- Bandwidth, power, weight (for man-packed radios), and size all constraints similar to space environment
- High bit-error environment, potentially high channel access delays

Protocol Overview

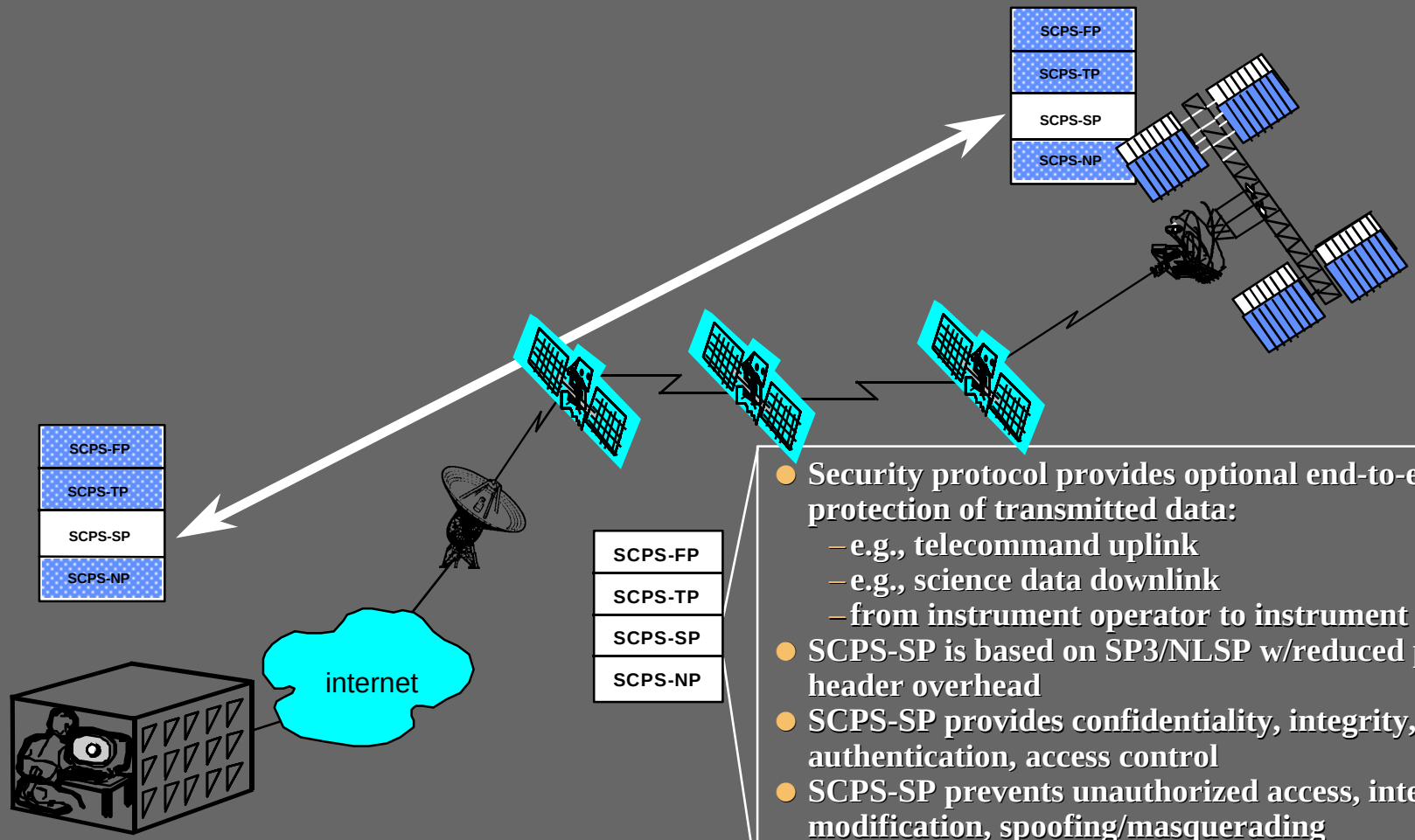
The SCPS Network Protocol (SCPS-NP)



- Network protocols route data through intermediate systems to the destination
- SCPS-NP is a new, bit-efficient protocol designed for use in space systems
- SCPS-NP handles static or dynamic connectivity, precedence, multiple routing options
- The result: A truly scalable network protocol for a broad range of spacecraft

MITRE

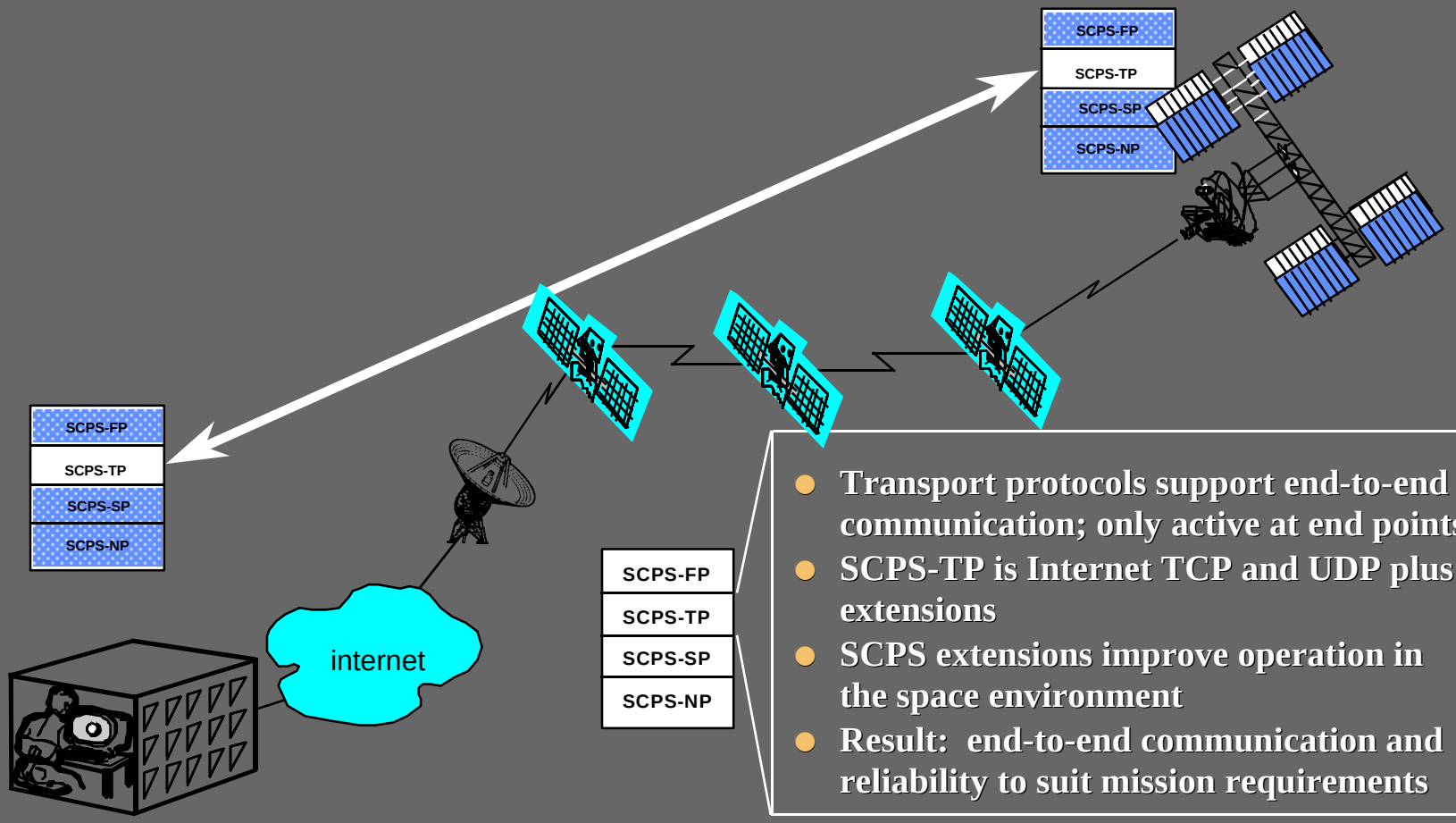
The SCPS Security Protocol (SCPS-SP)



- Security protocol provides optional end-to-end protection of transmitted data:
  - e.g., telecommand uplink
  - e.g., science data downlink
  - from instrument operator to instrument
- SCPS-SP is based on SP3/NLSP w/reduced protocol header overhead
- SCPS-SP provides confidentiality, integrity, authentication, access control
- SCPS-SP prevents unauthorized access, interception, modification, spoofing/masquerading
- SCPS-SP is algorithmic independent

SPARTA

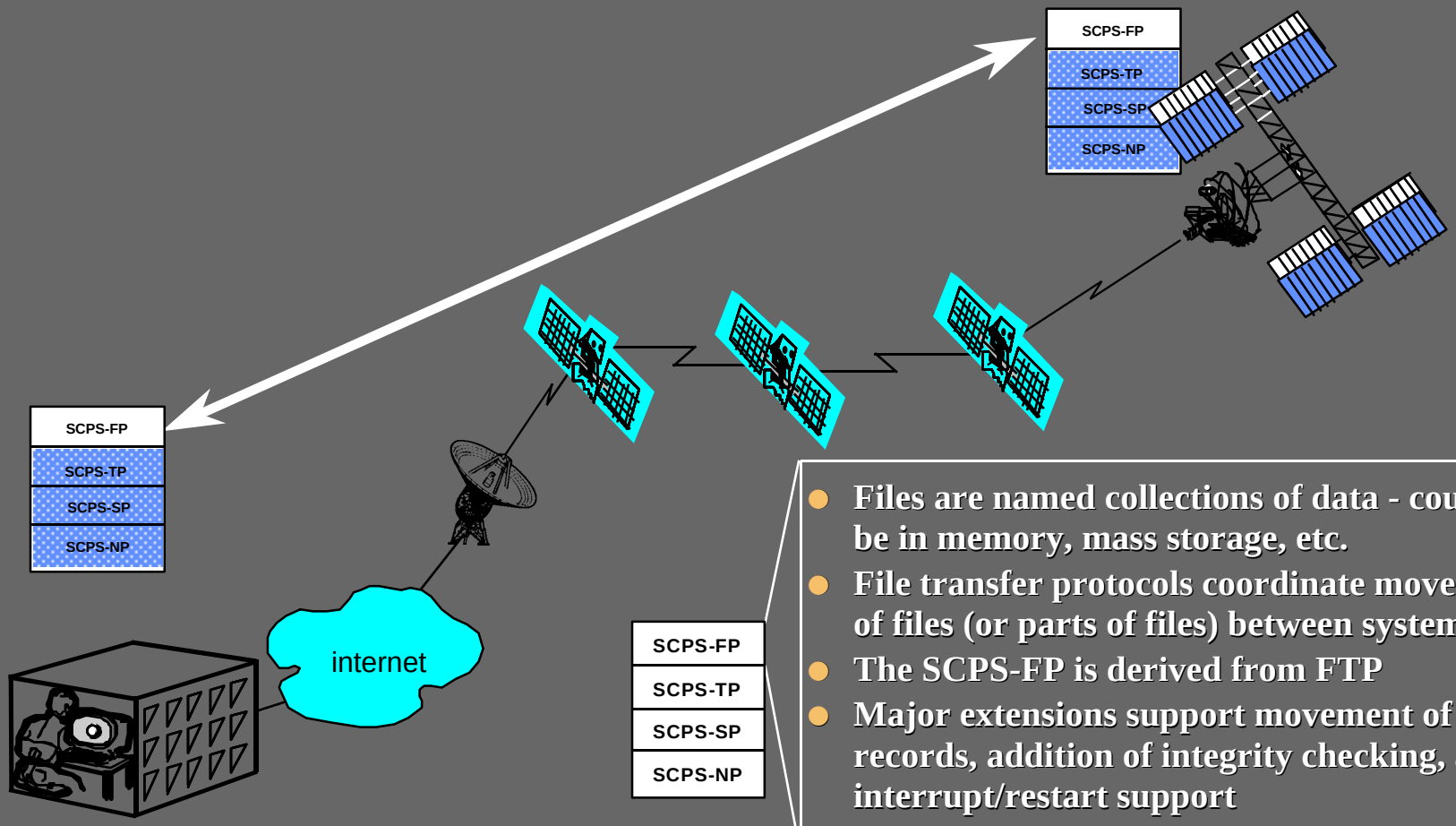
The SCPS Transport Protocol (SCPS-TP)



- Transport protocols support end-to-end communication; only active at end points
- SCPS-TP is Internet TCP and UDP plus extensions
- SCPS extensions improve operation in the space environment
- Result: end-to-end communication and reliability to suit mission requirements

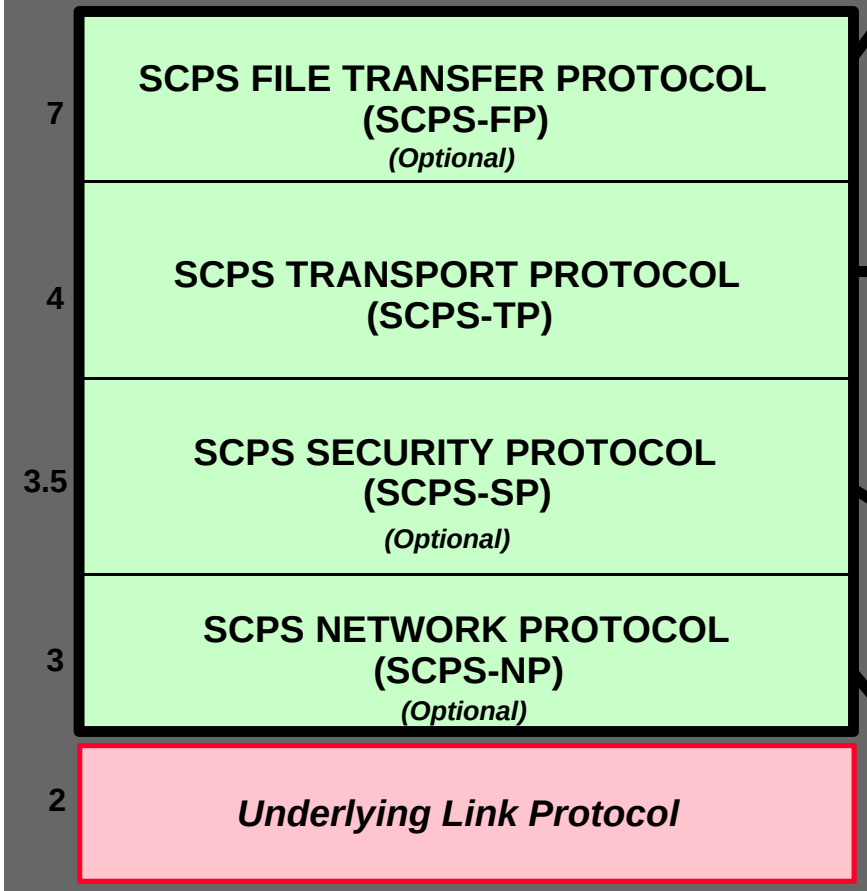
MITRE

The SCPS File Transfer Protocol (SCPS-FP)



- Files are named collections of data - could be in memory, mass storage, etc.
- File transfer protocols coordinate movement of files (or parts of files) between systems
- The SCPS-FP is derived from FTP
- Major extensions support movement of file records, addition of integrity checking, and interrupt/restart support

SCPS Capabilities



Core = Interoperable Internet FTP

Record read & record update;
File & record Integrity;
Automatic restart;
User suspend/resume;
Suppress ASCII reply codes.

Core = Interoperable Internet TCP/UDP

Congestion control appropriate for mixed-loss environments (congestion, corruption, outage);
Selective negative acknowledgment;
Robust header compression;
Window scaling ("long/fat pipes");
Partial Reliability service (BETS);
Delimitation of record boundaries;
Time stamping for high rate sequencing, delay measurement.

Authentication: guarantee of the identity of a source;
Access Control: prevention of unauthorized access;
Integrity: protection against modification;
Confidentiality: protection from disclosure.

Provide both connectionless and managed-connection routing;
Support precedence (priority) based handling;
Offer multiple routing options;
Signal errors to the layer above;
Support packet lifetime control;
Scaleable - tailor capability to need, e.g., high communications efficiency in constrained bandwidth conditions.

SCPS sits on top of existing link capabilities, and augments them