SECTION 4. COMMUNICATIONS PROTOCOLS

4.1 COMMUNICATIONS OVERVIEW

The workstations for the EOF-resident instrumenters (IWSs) will be connected to ECS and among themselves using Ethernet. Upgrades to provide higher capacity to some instrumenters' teams may be implemented if necessary (for instance, upgrade to CDDI). The communications among the IWSs may use either TCP/IP or DECNET. Additionally, TCP/IP will be routed to Internet and DECNET to SPAN. Communications between the ECS and the IWSs will take place using a subset of TCP/IP services and protocol as illustrated in Figure 4-1. Internet connections from remote instrumenters will be routed through NASA GSFC. All instrumenters, resident or not, may access ECS through FTP and SMTP. The IWSs may additionally use sockets, NTP, X11 and rlogin to access various resources on ECS.

4.1.1 FILE TRANSFER

FTP is used to support file transfers between the ECS and all instrumenters' teams (resident or remote). As described in the following paragraphs, four different methods may be used to exchange files between the ECS and the instrumenters. The method selected depends on the type of data exchanged.

1) Files that ECS needs to send to specific instrumenters' teams (i.e., command validation reports).
ECS maintains a list of designated computer addresses where each type of file is to be forwarded, typically two addresses per instrument team. As soon as a file becomes available, ECS initiates an FTP session with the computers designated to receive that type of file for that particular instrument, and writes the file to that computer. ECS must maintain a list of Internet addressees for all the instrumenters' teams. ECS must also have an account on each of these instrumenters' computers and maintain a list of current account names and passwords. In the case where ECS would be unable to connect to any of the receiving computers, the SOC will notify the addressees via E-mail, and ECS will keep the files for a certain period of time for possible manual retransmission by the SOC.

2) Files generated by ECS and retrieved by the instrumenters when needed (i.e., Activity Plan).
These files are deposited by ECS on specific system directories. Read access is available to instrument teams and members of the scientific community with a valid FTP account: the ECS system administrator will maintain a list of these valid account and passwords. Anonymous FTP is not allowed.

3) Commanding files generated by the instrumenters. The transfer of these files (delayed command files and background-queue files) requires the use of a SecureID card. The instrumenters initiate these FTPs and write the files to specified ECS systems directories. When performing the FTP, the originating instrumenter must be in possession of a SecureID card and enter the proper numeric code. These FTPs must also be done on a specific port number different from the default FTP port number.

4) Other files generated by the instrumenters (e.g., input to the summary data or input to the activity plan). These FTPs will be initiated by the instrumenters and performed using account name and password on the default port number. The instrumenters write their files to specified ECS

systems directories. The ECS system administrator maintains a list of authorized computers and account information.

	FTP RFC-959	SMTP RFC-821	X 11	SOCKET I/F	NTP RFC-123
Communication Protocols	TCP RFC-793				UDP RFC-768
and Application Level	IP/ICMP RFC-791 RFC-792				
Services	ETHERNET Link Level RFC-826 RFC-894				

Physical Interface	ETHERNET IEEE 802.3

Note: The Requests for Comment (RFCs) listed above are the specifications for the various protocols for Internet. The full listing of each RFC is available via anonymous FTP on various Internet computers (i.e., NIC.DN.MIL).

Figure 4.1. SOHO/ECS Communication Architecture

4.1.2 E-MAIL

SMTP mail utility will be used to exchange non-time-critical information between ECS and the instrumenters. ECS must obtain and maintain a list of Internet addresses and user-names where to send mail. Similarly, ECS must supply the instrumenters with the ECS Internet address, user-name and password.

4.1.3 XWINDOWS

X11 will be used by the IWSs (i.e., EOF-resident) to view ECS displays such as the commanding status window or telemetry distribution monitoring display. ECS will make 'C' language software available to the instrumenters to allow the display of these Motif windows.

4.1.4 REMOTE LOGIN

Rlogin will be used by the IWSs to initiate an X11 session. ECS will maintain a list of network addresses and user-names of these IWSs allowed to do remote login.

4.1.5 TIME SERVICES

NTP will be used to supply standard time to the instrumenters. This protocol allows the synchronization of the internal clock of each served computer to a time server computer. No special hardware or software is needed on the instrumenter computers: NTP is part of the suite of software distributed with almost all implementations of TCP/IP. The time server computer provides the Coordinated Universal Time (UTC). Using NTP, the instrumenters can synchronize the system clock of their computers to within 20 milliseconds of UTC. Then, they can obtain UTC by using system utilities to read their system clock. System clocks are generally readable down to milliseconds and sometimes microseconds.

4.1.6 SOCKETS

Sockets are used for the transmission of real-time data streams (primarily, near-real-time commanding and telemetry distribution) between the IWSs and the ECS. The IWSs will serve the necessary sockets and ECS will connect to them when data need to be transferred (for instance, at the beginning of a pass when real-time telemetry is received by ECS or when the NRT throughput mode is enabled). ECS has reserved a group of port numbers for the sockets to be served by the IWSs (see Table 4.1 below).

- For telemetry data, 4 sockets are available to each IWS, one of these being reserved for the transmission of MDI-M data. This could allow a given IWS to receive telemetry simultaneously on up to 3 separate sockets for non-MDI data, and a fourth socket for MDI-M data. It is envisioned that operationally, an IWS will not use more than one or two sockets at one time. However, this is provided to allow separate processes to run and accept different types of telemetry on a single IWS. ECS will maintain a list of 'default IWS-socket pairs' which are the sockets over which telemetry is expected to be distributed during a real-time pass. At the beginning of the pass, ECS will attempt to initiate a session with each of these 'default IWS-socket pairs'. Additional connections may be requested at any time via the SOC.

- For commanding data, 11 sockets are available to each IWS, each socket corresponding to one instrument. Each IWS will use the port socket(s) it needs to command the instrument(s) it intends to command. ECS will maintain a list of 'default IWS-instrument pairs'. When the throughput mode is enabled, ECS attempts to initiate a session with each 'default IWS-instrument pair'. It is expected that an IWS will not serve a socket for an instrument it is not authorized to command or an instrument it will not command during the current NRT session.

Table 4.1 Port number assignments for NRT sockets.

FUNCTION		**PORT NUMBER**
Telemetry	Connection	
	First	20100
	Second	20101
	Third	20102
	Fourth	20103
Commanding	Instrument	
	CDS	20200
	CELIAS	20201
	CEPAC	20202
	EIT	20203
	GOLF	20204
	LASCO	20205
	MDI	20206
	SUMER	20207
	SWAN	20208
	UVCS	20209
	VIRGO	20210

4.2 ECS HARDWARE CONFIGURATION

The current ECS hardware configuration is illustrated in figure 4.2. It is only included in this document for informational purpose and may be modified during the life of the mission. The ECS hosts are RS/6000 workstations running AIX. The hardware configuration has been in part dictated by the interface with MODNET an by security considerations. The description of specific security measures, policies and procedures are not within the scope of this ICD. The following section outlines the main characteristics of the security implementation within the ECS.

1) The filtering capability of the routers will be utilized to limit external access to the EOF. Only packets with specific combinations of source address, destination address and IP port number or DECNET packet type will be allowed to pass.

2) Only specific services (e.g., E-mail, or FTP) on specific ECS hosts will be available to external users. The ECS itself will support only TCP/IP. The use of the SecureID card is required for FTP of commanding data.

3) Host protection measures will remain the primary security measures. They vary from host to host, depending on the capabilities of the various operating systems. It is recommended that remote logins not be allowed on a given IWS while this IWS supports an active near-real-time commanding session.

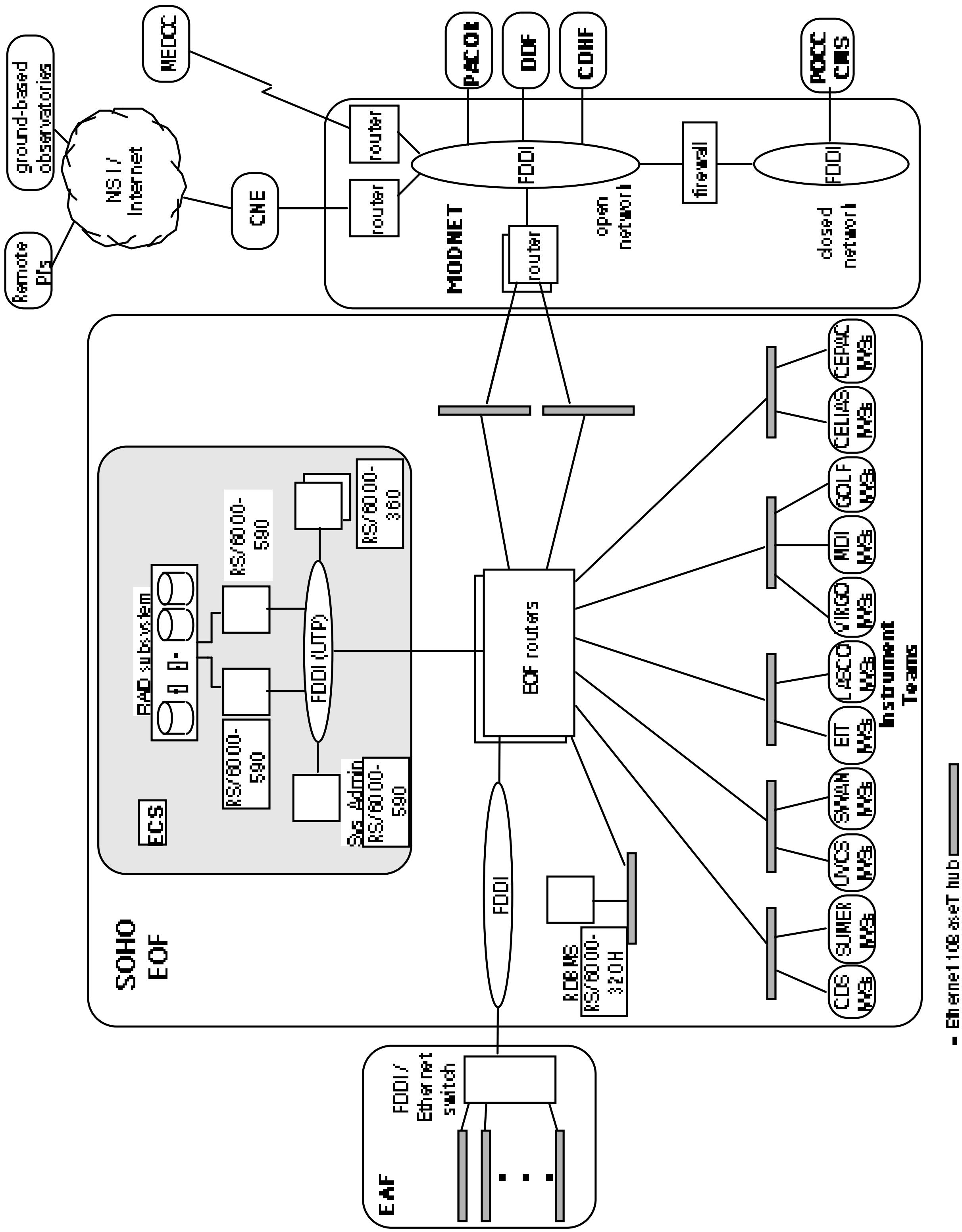

Figure 4.2. SOHO/EOF Hardware Architecture