4.0 GCCS ARCHITECTURE OVERVIEW

As mentioned in the discussion on the COE, GCCS follows the TAFIM and the principles of the Technical Reference Model (TRM). The TRM was devised to allow DoD to exploit the benefits of open systems and new commercial technologies. Benefits include:

- Improved use productivity
- Improved development efficiency
- Improved portability and scalability
- Improved interoperability
- Greater vendor independence
- Reduced life-cycle costs
- Improved security
- Improved management.

In the past, custom systems were developed for specific hardware platforms, and software was generally proprietary. Systems tended to be functionally redundant, non-portable, and non-interoperable. The TRM supports modular software applications and promotes software re-use.

The *TAFIM Volume 3, Architecture Concepts and Design Guidance* states: "The objective computing environment is a distributed computing environment based on open systems principles and public standards." The computer model for such a distributed processing environment is the client/server model in which servers at processing nodes provide services over a network.

GCCS uses a three-tier client/server architecture. Client/server architectures were initially single-tiered, mainframe-based in which each application had its own data in its own files with little sharing. Two-tiered architectures were developed to meet the need to separate data from applications, which provided the data that could be shared. Multi-tiered architectures are extensions evolved from two-tiered models. The three-tiered model further separates the user interface (called the presentation layer) from the rest of the application and the already separated data (as in a two-tiered model). Thus the application functional code can be treated as a library of routines, can be put on the network and accessed remotely, and can become re-usable. Elements of the architecture can be more readily rewritten and replaced. This is particularly valuable for dealing with migration of legacy systems as GCCS must do at IOC.

The client/server model provides a flexible framework for designing and maintaining distributed processing applications and many variations in system architecture are possible. Section 4 discusses the specific hardware and software architecture used in GCCS Version 2.1 at IOC.

4.1 Generic Hardware Configuration

There are potentially many variations in the site configurations due to differing site needs. This section briefly identifies the family of various hardware components in use at IOC and their purpose in the system. The following sections discuss the technical parameters of the system hardware platforms, summarize the various possible site configurations, the expected connections made between sites, and present typical software configurations at the various types of sites.

The hardware components and a generic configuration used to implement the GCCS three-tiered architecture are shown in Figure 4-1. Specific equipment requirements for Version 2.1 are shown in Subsections 4.1.1

through 4.1.14. The GCCS distributed computing environment uses interconnected heterogeneous and interoperable computers. The servers are connected at a site via an FDDI high-speed LAN. The servers are Portable Operating System Interface (POSIX)-compliant, meaning they will support the designed system with standard UNIX interfaces (Sun Solaris 2.3 or Hewlett-Packard HP-UX-9.0.1 for GCCS Version 2.1).[1] A communications server can provide interconnection with remote site connections and other GCCS entities via access to a WAN. Clients are shown generically but the current clients identified for GCCS are Sun SPARC 5s, Sun SPARC 10s, Sun SPARC 20s, TAC-3s, TAC-4s (in the future), Macintosh IIfxs, and a variety of DOS-based platforms. Hardware requirements for each platform vary according to user requirements.

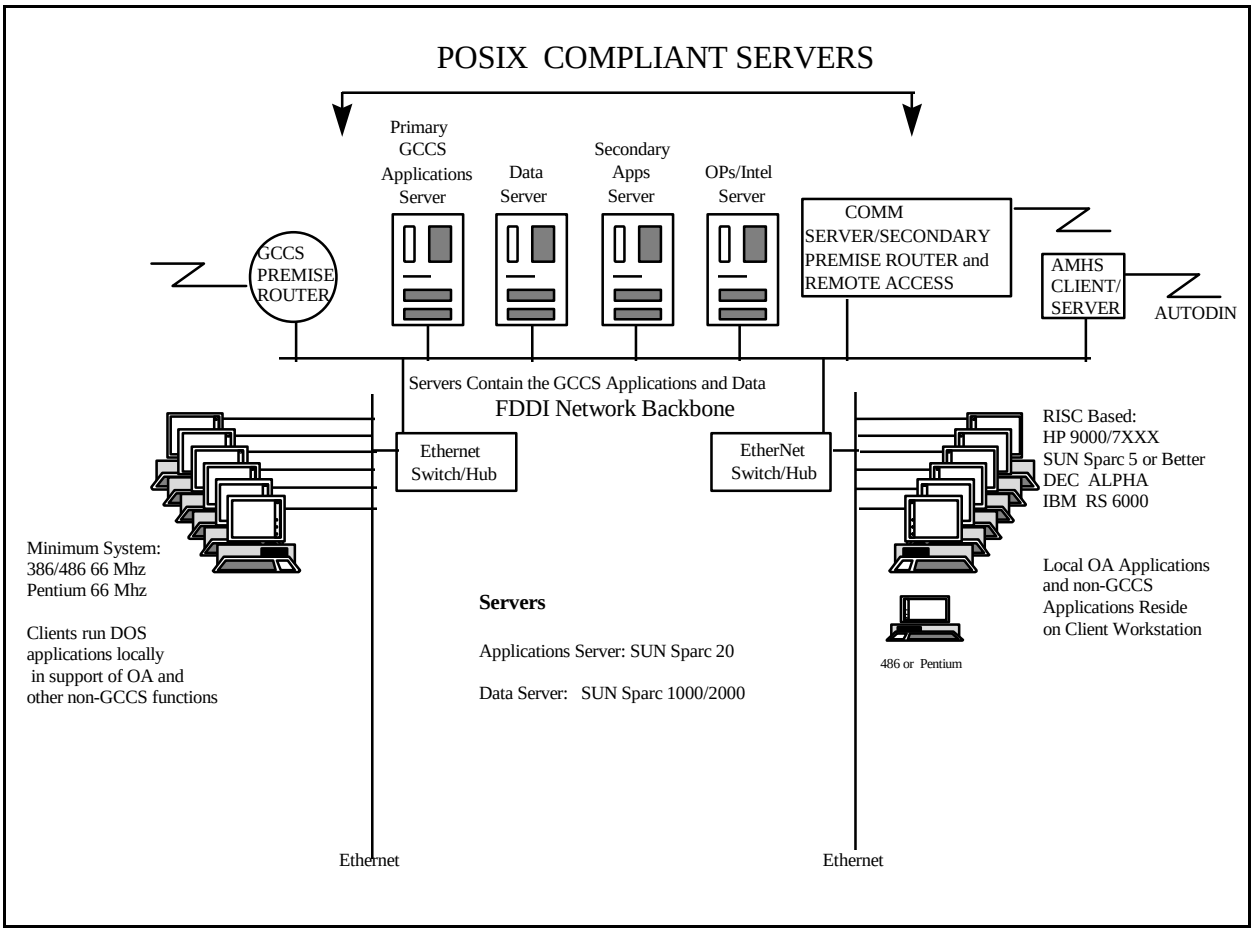

Figure 4-1. Generic Hardware Configuration

GCCS places strong emphasis on software and reduced hardware dependency. The GCCS software is designed for the two chosen operating systems and the hardware platform must be able to support one of these operating systems to run the GCCS suite of software. However, a platform running a different operating system can still be used as a GCCS client. The client could run a standard X-Terminal/X-Windows application software package to reach a GCCS application server. The client would then have all the functionality of a Sun or HP-based client.

---

[1] The POSIX Open System Environment provided a strong foundation for the Technical Reference Model.

Finally, it should be remembered in the three-tiered GCCS architecture, the presentation tier (user interface), the server-tier (functional), and the data-storage-tier are logically separated but may actually reside on one, two, or more different platforms. The presentation-tier will include mission-specific joint, service, and command-unique applications in addition to standard and COTS user interface elements such as X-Windows or Motif. The server-tier includes functions (server-resident applications for mission applications, office automation, systems management, etc), and the components upon which these functions reside. The data-storage-tier, linked to existing systems and applications, includes data storage and database management systems. The following Subsections discuss the GCCS Version 2.1-specific aspects of the generic configuration.

4.1.1 Site Hardware Configuration. Each of the GCCS sites will have a core set of hardware for the GCCS software. Figure 4-2 shows a general hardware configuration for GCCS Version 2.1 (not all sites will have all the components shown). While some of the hardware directly correlates to the three-tiered client/server architecture, other components are used to provide the GCCS communications infrastructure within each site. The *GCCS Systems and Network Management CONOPS*, Version 1.6 provides excellent hardware and functional descriptions of the various general components shown in Figure 4-2. Those descriptions are repeated here but readers should consult that document for detailed information on the operation of GCCS as a networked system.

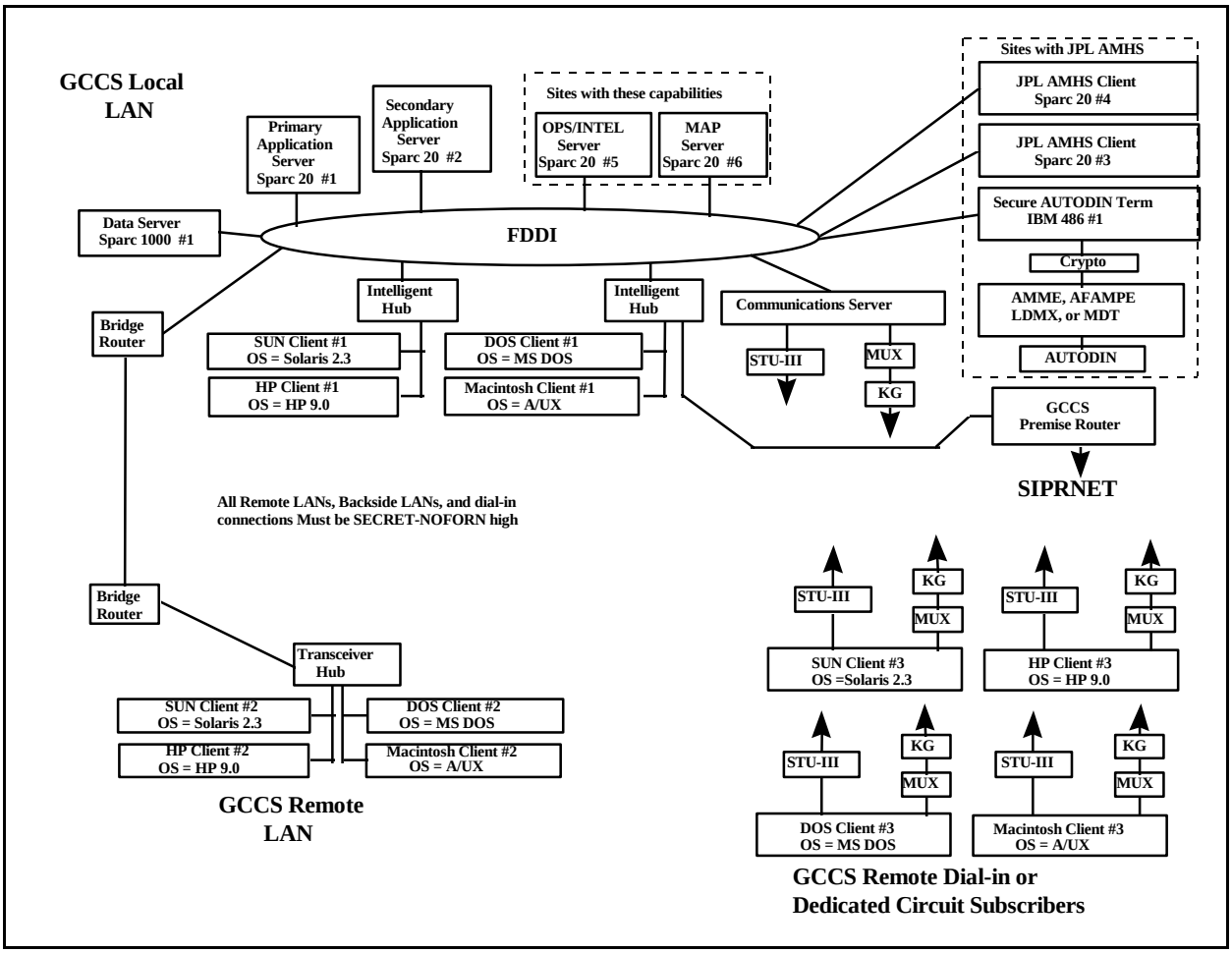

Figure 4-2. GCCS Version 2.1 General Hardware Configuration

4.1.2 Data Server. Represents the third-tier (the data-storage-tier) in the software model. The typical data server is a Sun SPARC 1000 with at least 32 Gigabytes (GB) of mirrored storage from a RAID Array and 512 Megabytes (MBs) of random access memory (RAM). Some of the GCCS sites will have a Sun SPARC 2000 instead of the SPARC 1000 for their data storage device. Variances in disk capacity and RAM size will exist within GCCS as a whole. Also, some sites may have more than one data server installed.

4.1.3 Application Servers. These are initially Sun SPARC 20s with most servers having 4 GBs of hard disc storage and 224 MBs of RAM. They are the second-tier and the server-tier in the software model. Initially, each IOC site will have two application servers. It is possible there will be more servers depending on the size and complexity of the site. The application servers are sized to support 5 concurrent X-Windows sessions or 20 TELNET sessions. Individual differences in application servers will cause these numbers to fluctuate.

4.1.4 OPS/INTEL Server. A select few of the GCCS sites have been identified to receive an additional Sun SPARC 20 after IOC to serve in this capacity. The device has 4 GBs of hard disc storage and 224 MBs of RAM.

4.1.5 MAP Server. Some GCCS sites will have the need to store a large volume of maps at their location.

A Sun SPARC 20 is identified to be this server and will be fielded after IOC. The hard disk size and amount of RAM required in this device is still being determined.

4.1.6 Automated Message Handling System (AMHS). The system being used is the one produced by the Jet Propulsion Laboratory (JPL) for the Army. The system is uniquely identified as the JPL AMHS, GCCS Configuration. In actuality, three configurations will exist for the AMHS suite of equipment based on the hardware utilized for AMHS functionality.

The first configuration consists of two Sun SPARC 20s. One serves as the AMHS server while the other is the AMHS dedicated client. The dedicated SPARC 20 client workstation represents the one used by the operator responsible for the AMHS. It should be noted that any of the GCCS workstations can be loaded with the AMHS client software.

The second configuration consists of a single SPARC 20 and utilizes separate file systems on the database server to complete the AMHS functionality. The final configuration uses only the SPARC 1000 or 2000 data server with no dedicated SPARC 20s. Instead, the entire AMHS functionality resides on the database server. The next device in the AMHS suite is the Secure AUTODIN Terminal (SAT), which contains a specialized communications card for interfacing with the AUTODIN message system. The SAT computer is an Intel 486-based computer operating with the Microsoft (MS) DOS. The next component in the AMHS suite is the cryptographic devices feeding data to the SAT. A large variety of cryptographic devices are used with each being site specific.

The next device in the AMHS suite is one of seven different components (AMME, AFAMPE, LDMX, MDT, ASC, CSP, and AGMS), which are an integral part of the AUTODIN feed to ensure 100 percent message delivery.

Finally, there is a 4800 bits per second (bps) AUTODIN circuit feed. There are a wide variety of AMHS configurations. Each configuration has to undergo certification testing by DMS certified testers. One stipulation of AMHS certification is that the GCCS LAN, all remote LANs, all backside LANs, all remote dial-in subscribes, and all dedicated circuit subscribers must be protected at the Secret classification level. Otherwise certification will be denied at that GCCS site.

4.1.7 GCCS Premise Router. The premise router is part of the GCCS site's LAN infrastructure. This represents the gateway out to the SIPRNET WAN. The majority of GCCS premise routers in use are manufactured by Cisco. Some of the models used at the GCCS sites are the Cisco 3000s, the AGS+s, and the 7000s. The premise routers were supplied by DISA, but they are owned and operated by the individual GCCS sites. As such, it is highly possible that the existing premise routers may be swapped out in the future by some GCCS sites to install a larger capacity router to accommodate their specific mission needs. This will be especially true where the GCCS site has a large campus environment (many buildings linked together by routers or bridges) to support. Replacement routers used by the sites will not necessarily be from the Cisco product line; however, the replacement routers must be compatible with the existing infrastructure.

4.1.8 Communications Server (CS). The CS is part of the site's LAN infrastructure. The devices initially being provided by DISA but owned and operated by the GCCS sites are the CISCO 2511-CSs. These CSs have two serial ports, one Ethernet port, and 16 asynchronous dial-in ports. The CSs will serve two types of users:

- Users who dial into the GCCS site using a Secure Telephone Unit - III (STU-III) to gain access

to the GCCS infrastructure.

- Users who are connected to the GCCS site via low-speed dedicated multiplexer circuits.

Authentication and access control will be performed at the CS location. Authentication control will be performed by separate accounts and passwords required by the CS operating software. Access control will be by the STU-III devices or link encryptors. The CS is considered an access point to the general DoD Secret-level LAN/WAN infrastructure and must be protected as such.

4.1.9 STU-IIIs. The STU-III devices connected to the CSs must be new generation STU-IIIs to accommodate the bandwidth requirements of the GCCS applications. It is recommended that GCCS sites use the AT&T Model 1910 STU-III. This particular device has a 14.4 kbps modem engine and obtains throughput speeds of 38.4 kbps using internally supplied compression algorithms. Built-in error correction algorithms should also be activated to overcome poor quality telephone lines. Access control will be provided by the Secure Access Control System (SACS), which is part of the AT&T Model 1910 STU-III operating software. The SACS feature operates on an Access Control List (ACL) feature for authenticating valid STU-III connections. It is the responsibility of the GCCS site to provide STU-IIIs and telephone lines to support their dial-in requirements.

4.1.10 MUX and Crypto. The next set of devices are the multiplexers and cryptographic equipment used to support the dedicated circuit remote subscribers. This group of users is a carryover from the slow-speed dedicated connections that existed within the WWMCCS community. A majority of these connections are 2.4 and 4.8 kbps in the WWMCCS environment. The vast majority of GCCS applications will not run over circuits this slow. A minimum speed of 32 kbps is recommended for dedicated circuits in the GCCS environment. It may be cost effective for remote GCCS users to migrate from the dedicated multiplexer circuit basis to a dial-in basis using STU-III technology, provided their mission needs can still be met.

4.1.11 Fiber Distributed Data Interface (FDDI). FDDI is high-speed LAN technology used to interconnect all of the major components of the GCCS site. This includes the data and application servers, and the intelligent hubs. In some cases the premise router may be connected to the FDDI ring instead of being connected to the intelligent hub as shown in Figure 4-2. DISA is providing the FDDI equipment to the initial primary GCCS sites.

4.1.12 Intelligent Hubs. Intelligent hubs are LAN infrastructure devices that allow the FDDI LAN to be connected to the site's normal Ethernet LANs. They provide the translation function of the LAN speeds and protocols. It is important to note that individual LAN infrastructures will vary greatly from site to site. DISA provided intelligent hubs during the initial equipment deployment.

4.1.13 Backside Routers and Bridge. Backside routers and bridges will vary from site to site. In most cases, a GCCS site will not exist within a single building or facility nor contain a single LAN segment. It is highly likely there will be multiple buildings within a close geographical area to form a campus environment. This campus environment will consist of a group of individual LANs interconnected by additional routers or bridges to form the site. The additional routers or bridges are not limited to interconnecting those sites within close geographical proximity. They could also be used to link GCCS Remote LANs that are separated by large distances. The existence of these campus environments and GCCS Remote LANs is one of the primary, driving factors for performing network management within the GCCS environment.

4.1.14 Clients. The clients are the users of the GCCS software. Clients are hardware used for user (operator) interface and represent the presentation layer. Platforms can vary, but current clients identified for GCCS are Sun SPARC 5s, Sun SPARC 10s, Sun SPARC 20s, TAC-3s, TAC- 4s (in the future), Macintosh IIfxs, and a variety of DOS-based platforms.

The specific hardware requirements for each of the primary equipments in GCCS Version 2.1 are summarized in Tables 4-1 through 4-5.

Table 4-1. SPARCserver 1000 Hardware Requirements

Item Description	Quantity	Size	Comments
Memory	1	1 GB	C1 Configuration
	1	768 MB	C2 Configuration
	1	480 MB	C3 Configuration
Disk	1	35.7 GB	C1 Configuration
	1	31.5 GB	C2 and C3 Configuration
Processors	6		
SCSI Controllers	4		
Monitor	1		
Keyboard	1		
Mouse	1		
SPARCPrinter	1		
Tape Drive	1	8 mm	
CD-ROM Drive	1		
Ethernet Transceiver	1		

Table 4-2. SPARCserver 2000 Hardware Requirements

Item Description	Quantity	Size	Comments
Memory	1	1.92 GB	
Disk	1	35.7 GB	
Processors	6		
SCSI Controllers	4		
Monitor	1		
Keyboard	1		
Mouse	1		
SPARCPrinter	1		
Tape Drive	1	8 mm	
CD-ROM Drive	1		
Ethernet Transceiver	1		

Table 4-3. SPARCstation 20 Hardware Requirements

Item Description	Quantity	Size	Comments
Memory	1	224 MB	
Disk	1	2.1 GB	Internal
	1	2.1 GB	Internal
Processors	1		
Monitor	1		
Keyboard	1		
Mouse	1		
SPARCPrinter	1		
Tape Drive	1	8 mm	
CD-ROM Drive	1		
Ethernet Transceiver	1		

Table 4-4. JFAST 486 Workstation Hardware Requirements

Item Description	Quantity	Size	Comments
Memory	1	16 MB	
Disk	1	1 GB	Internal
Processors	1		486DX2/66
Monitor	1	20 Inch	SVGA
Keyboard	1		
SPARCPrinter	1		
SCSI Tape Backup	1	250 MB	Wangtek
Tigersafe board	1		TS2K
Ethernet Card	1		

Table 4-5. PC-XTerminal Workstation Hardware Requirements

Item Description	Quantity	Size	Comments
Memory	1	8 MB	
Disk	1	500 MB	Internal
Processors	1		486DX2/66
Monitor	1	15/17 Inch	SVGA
Video Adapter	1	1 MB	
Keyboard	1		
Mouse	1		
Ethernet Card	1		

4.2 GCCS Site Hardware and Software Configurations

There are three main types of sites for GCCS Version 2.1: GCCS Core Database Sites, Non-Core Database Sites, and Remote User Sites. The specific hardware and software configurations for each type of site are presented in this section.

4.2.1 GCCS Core Database Sites. Fifteen (15) sites have been designated as operational GCCS Core Database Sites. These sites' hardware configurations are shown in Figure 4-3. These are the only sites that will be configured with and will maintain the S&M Database (also called the JOPES CORE Database), GSORTS Oracle Server and GSORTS World Data, MEPES Database, JEPES Database Server, LOGSAFE Database Server, PDR Database Server, RDA Server, and the ESI Flat File Allocate. These sites are:

ACC	PACAF	USEUCOM
AMC	USACOM	USFK (Taegu)
FORSCOM	USAFE	USSOCOM
HQDA	USARPAC	USSOUTHCOM
NMCC	USCENTCOM	USTRANSCOM

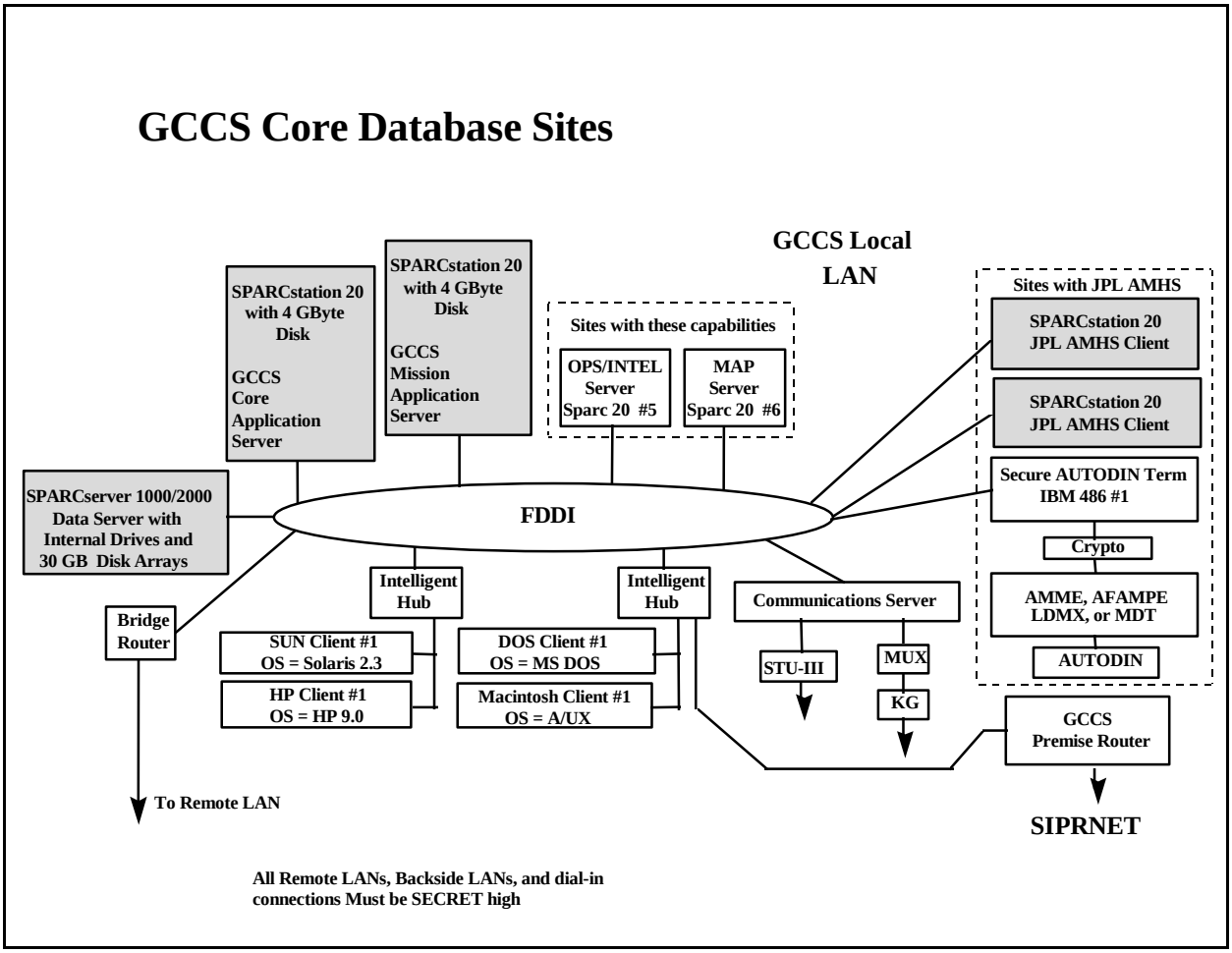

Figure 4-3. Hardware for GCCS Core Database Sites at IOC

4.2.2 Non-Core Database IOC Sites. Non-Core Database sites will connect to one of the GCCS Core Database sites as a source of information. The following sites will not have the GCCS Core Database:

AFMC	MARFORPAC	USCENTAF
ANMCC	MSC	USFK (Yongsan)
CNO	MTMC	USNAVCENT - Rear
HQUSAF	PACFLT	USNAVEUR
HQUSMC	USARCENT	USPACOM
JTO	USAREUR	USSPACECOM
LANTFLT	USASOC	USSTRATCOM
MARFORLANT		

These sites will have the hardware configurations shown in Figure 4-4 for GCCS Core software.

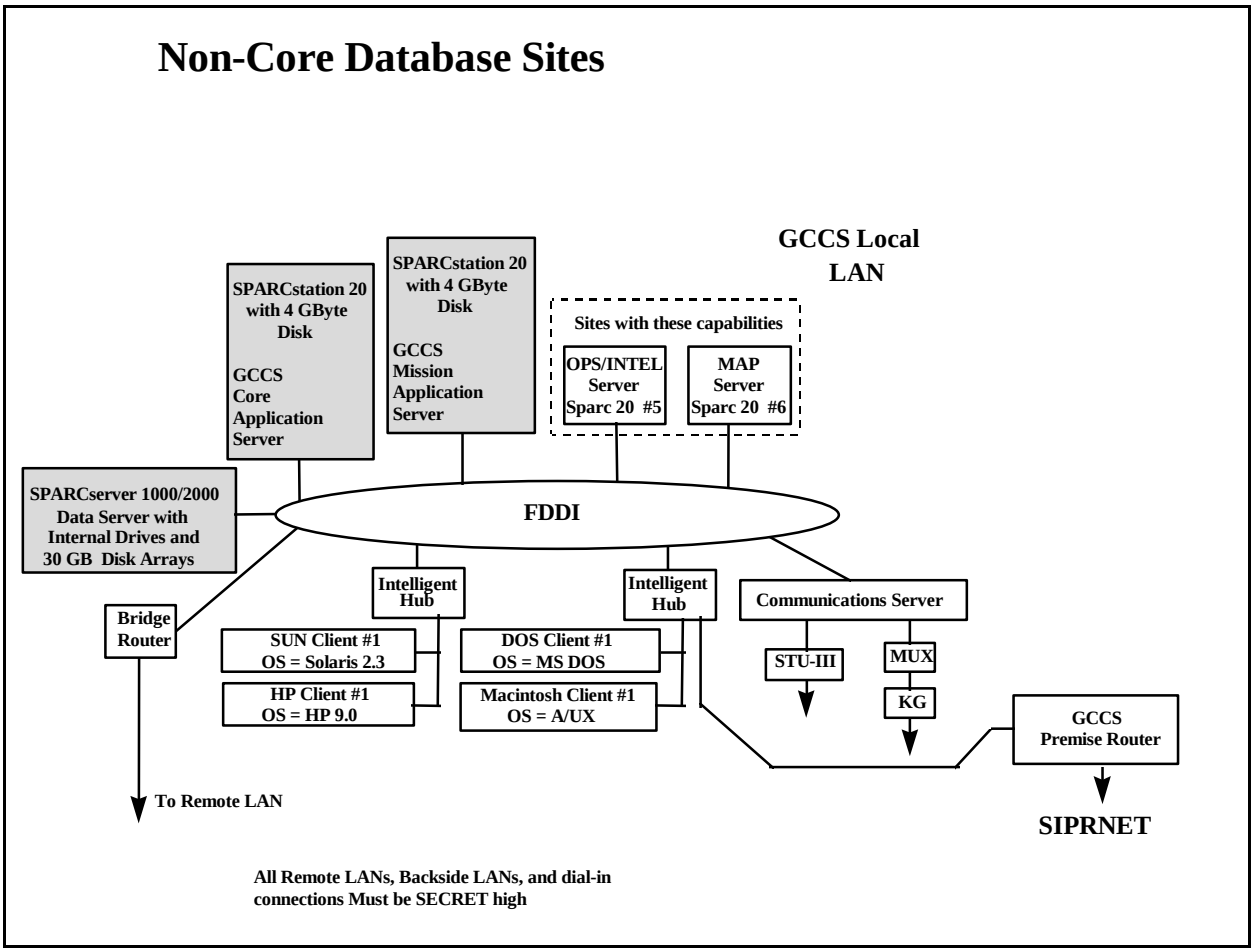

Figure 4-4. Non-Core Database Sites

4.2.3 Remote User Sites. Remote sites are those that have at least one SPARC 20 workstation and connect to one of the IOC GCCS sites for application access. These sites do not require Sybase to run the EM as a Desktop. The minimum hardware configuration at these sites is one client connecting to a SPARCstation 20 with 4-GB or more (designated as GCCS Core Applications Server) via remote

communications links.

4.3 Site Software Configuration

GCCS is a client/server system consisting of a SPARCserver 1000/2000 database server and at least two SPARCstation 20 application servers. The database server at all JOPES Core Database sites uses mirrored 30-GB disk arrays (30-GB as primary, 30-GB as back-up) to hold the JOPES Core Database. The database server software consists of the Oracle COTS product and a database server software segment for each application utilizing the Oracle database. The two SPARCstation 20 application servers are designated as the "GCCS Core Application Server" and "Mission Application Server." The GCCS Core Application Server holds the GCCS Core software, while the Mission Application Server holds other mission application software segments. The final configuration of the Mission Application Server will be determined by the mission requirements of the site. The software configurations required for GCCS Version 2.1 functionality will vary depending on the site.

The term application server can be confusing since these servers are actually used to hold software application "clients." Users at site workstations can run client applications one of three ways:

- Use their workstation as an X-Terminal and view the application at their workstation while the application is actually running on the application server.

- Install the application client software segment on their workstation and run client/server connecting to the database server and effectively bypassing the application server.

- Use the UNIX Network File System (NFS) feature to run an application client software segment on their workstation (in RAM memory) by downloading the application across the LAN from the disk drive of the application server. The application server is in effect a "disk drive" for the workstation.

Configuring workstations is site-specific and Site SAs will meet the site mission operational requirements using different techniques, which are driven by site hardware and network considerations.

The following sections describe the software configurations at the various sites. The information in the figures should be considered representative of the IOC configurations and not exact. They show the recommended loading of the various software segments but there will be some variations by site. Many software segments are not shown although they are important, such as the EM needed for the GCCS Desktop, or the Network management segments. Some applications are not shown. For example, RFA is only used at the NMCC, JFAST is loaded on a high-end IBM DOS compatible PC, and GTN is only at USTRANSCOM (but accessible from other sites). Regardless of actual hardware and software configuration, all GCCS components are controlled through the CM process described in Section 9. Users can ask the appropriate GCCS site personnel (see Section 6) about specific configurations at their sites.

4.3.1 Software Configuration for the GCCS Core Database Sites. GCCS Core Database sites are the data repositories for all shared GCCS system-wide information. These sites are provided two additional SPARCstation 20s for the purposes of implementing AMHS. The GCCS functional software configurations for GCCS Core Database sites are shown in Figure 4-5.

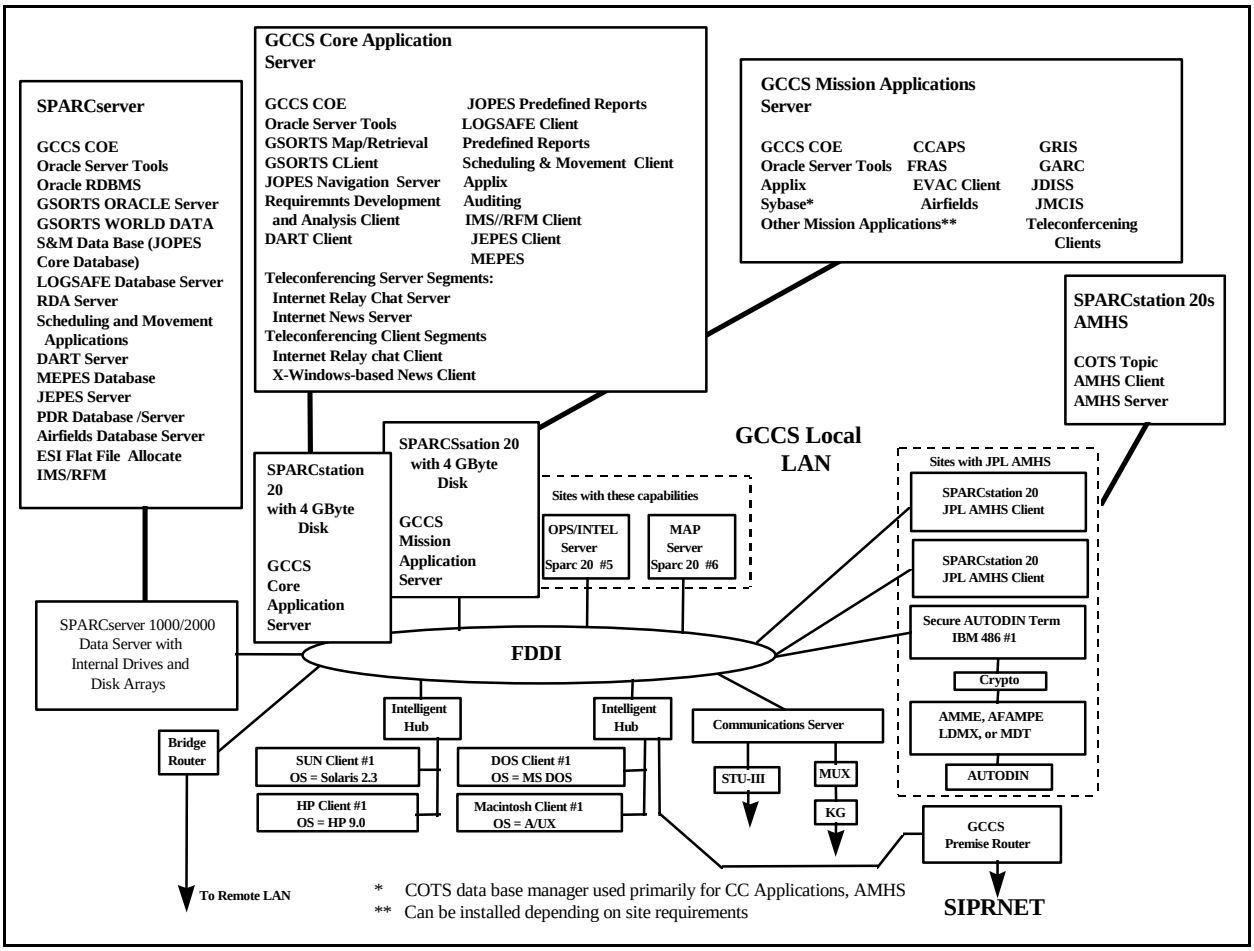

Figure 4-5. Software Configuration for GCCS Core Database Sites

4.3.2 Software Configuration for the Non-Core Database Sites. Non-Core Database sites are required to connect to one of the GCCS Core Database sites to obtain system-wide information. These sites will have the COTS Oracle product installed and this product may be used for local or site-specific data. AMHS is installed on the SPARCserver 1000/2000. The software configuration at these sites is shown in Figure 4-6.

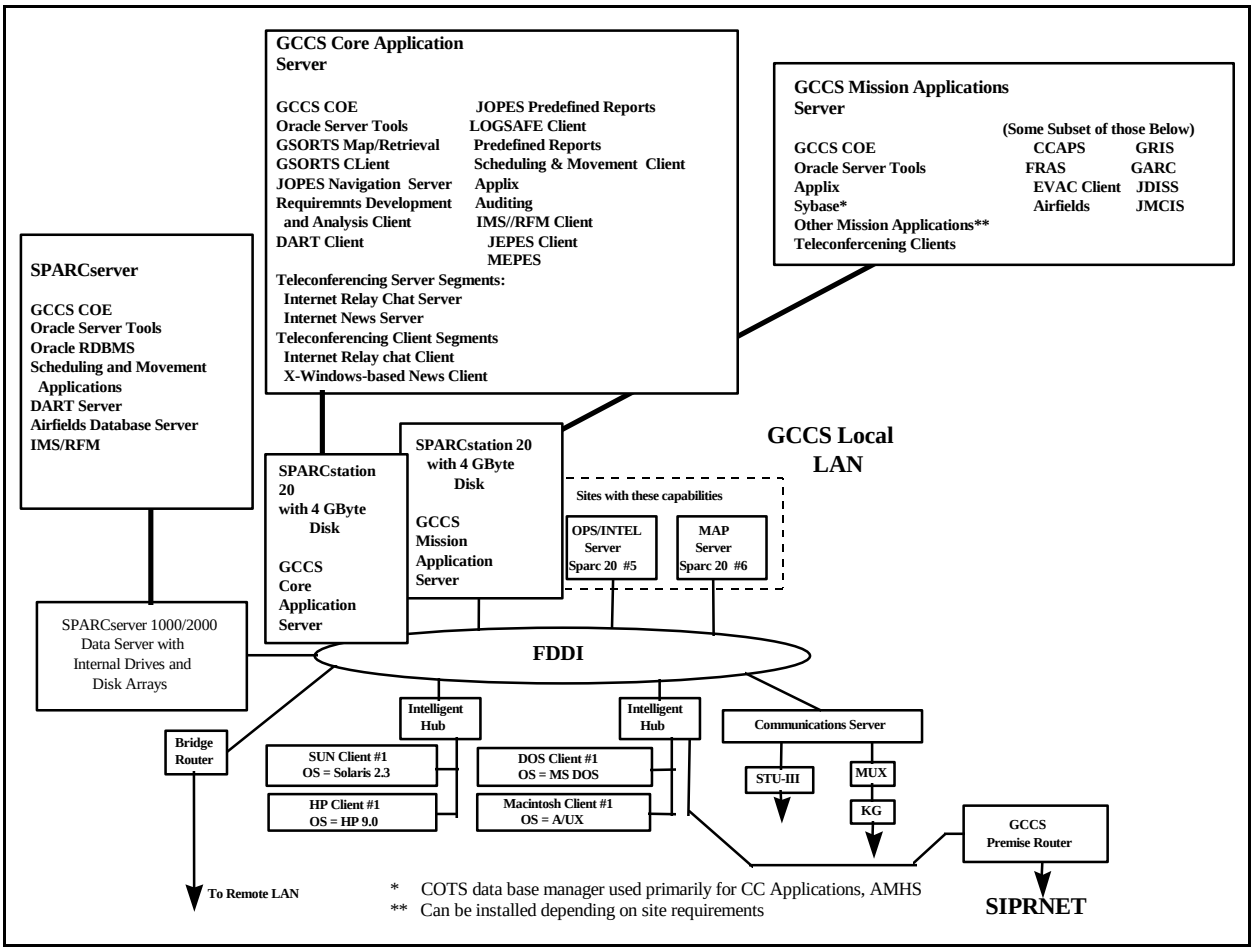

Figure 4-6. Software Configuration Non-Core Database Sites

4.3.3 Software Configuration for the Remote User Sites. These sites each have one client workstation (SPARCS, PC, TAX-X, etc). and connect to one of the Non-Core Database sites or a GCCS Core Database site for applications/data. These sites do not require Sybase to run the EM as a Desktop.

4.4 GCCS IOC Topology

The concept of operations (CONOPs) for GCCS is for the 15 GCCS Core Database sites to provide planning information to all other sites in the network. The inter-relationship of the GCCS Core Database sites and the Non-Core Database sites is shown in Figure 4-7. Each of the Non-Core Database sites is connected at IOC to a GCCS Core Database site as a primary source of information. Figure 4-7 reflects the IOC topology (JTO not shown). Also, each of the 15 GCCS Core Database sites (except HQDA) will serve as a back-up database site for another site, so that each GCCS Core Database site has two designated back-up sites. The primary/back-up designations are shown in Table 4-6.

Responsibility for shifting from the primary to back-up database site is a local site responsibility. If GCCS users experience problems indicating a need to use the back-up site and the local site has not already taken action to switch from the primary database site to the back-up database site, the local TDBM and FDBM should be corrected. The necessary switch procedures should already be pre-arranged. The local site GCCS

System Administrator GSA and GDBA (TDBM and FDBM) will ascertain conditions and in coordination with the site security officer, contact the back-up database site and arrange for the shift. Additional information can be found in Section 6.2.8.

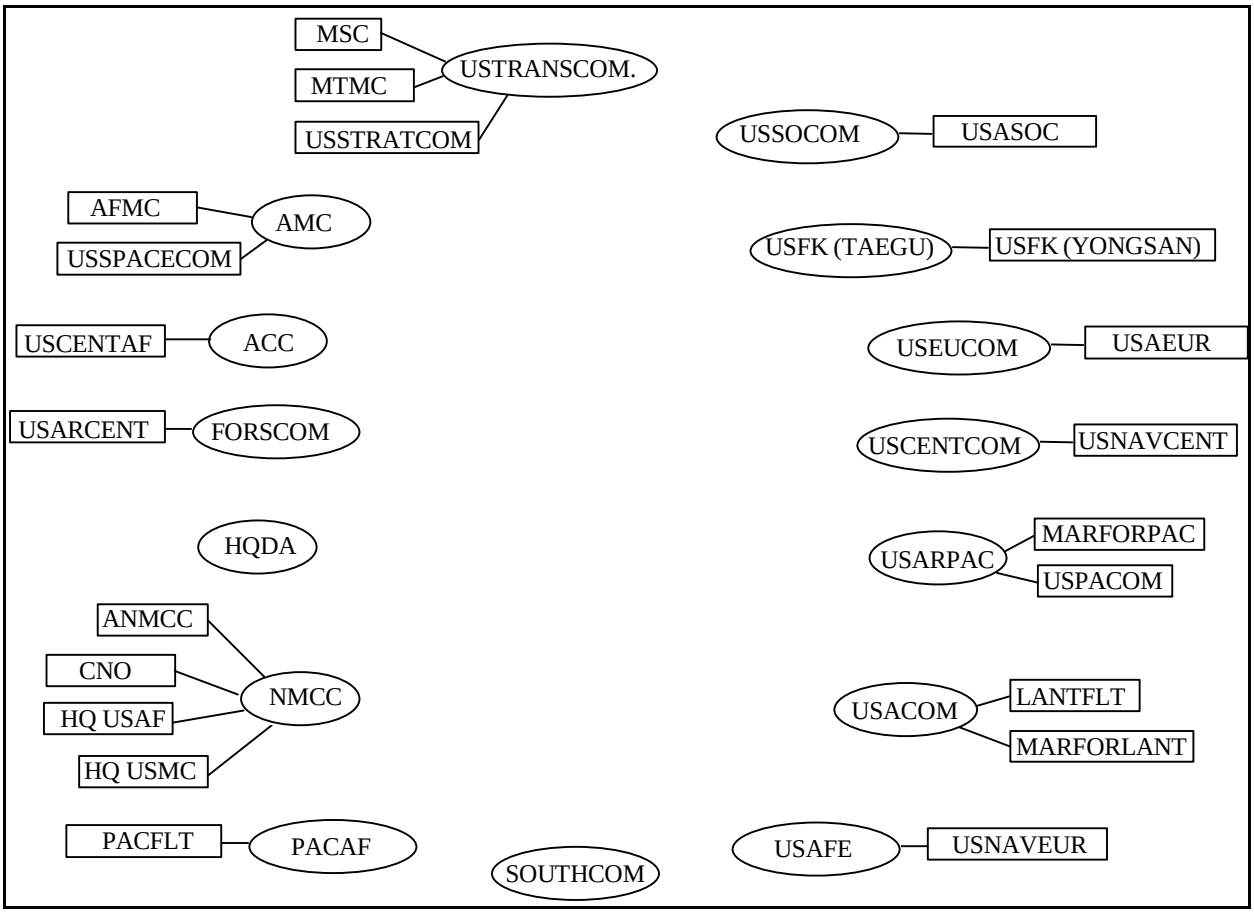

Figure 4-7. GCCS Version 2.1 (IOC) Topology

Table 4-6. Back-up Sites for GCCS IOC Sites

GGCS IOC Site*	Back-Up Site	GGCS IOC Site*	Back-Up Site
ACC	USACOM/AMC	PACAF	USARPAC/AMC
AMC	USTRANSCOM/ USSOCOM	USACOM	ACC/NMCC
FORSCOM	AMC/USSOUTHCOM	USCENTCOM	USSOCOM/ACC
HQDA	NMCC/FORSCOM	USARPAC	PACAF/AMC
USEUCOM	USAFE/FORSCOM	USSOCOM	USCENTCOM/ACC
USFK (Taegu)	USARPAC/PACAF	USSOUTHCOM	USSOCOM/FORSCOM

GGCS IOC Site*	Back-Up Site	GGCS IOC Site*	Back-Up Site
NMCC	USSOCOM/USSOUTHCOM	USTRANSCOM	AMC/FORSCOM
ANMCC	USSOCOM/USSOUTHCOM	MSC	NMCC/AMC
CNO	USACOM/USSOUTHCOM	MTMC	NMCC/AMC
HQ USAF	ACC/USSOUTHCOM	USSTRATCOM	AMC/FORSCOM
HQ USMC	USACOM/USSOUTHCOM		
USAFE	USEUCOM/ACC		
USNAVEUR	USEUCOM/ACOM		

***** Back-up sites for the GCCS Core Database sites also back-up the associated Non-Core Database Sites, which are not listed in this table. However, if the back-up sites for the Non-Core Database sites are different than the back-up for the parent GCCS Core site, then back-up sites are listed individually, as for the NMCC and USTRANSCOM.

4.4.1 Connectivity. GCCS is a global, distributed processing system and thus relies heavily on a mixture of WANs, LANs, and dedicated or dial-up circuits for interconnection and data transport. The SIPRNET, which is part of the Defense Information System Network (DISN), is the primary WAN supporting GCCS, although various service and agency WANs also provide connectivity as needed. Since many GCCS sites may be distributed across facilities such as bases and posts, LANs are often interconnected to the GCCS LAN though bridge (or "backside") routers in a campus environment (see Section 4.1). Many remote users depend on dial-in or dedicated circuit connections to a GCCS site communications server for remote access. This section will discuss the primary WAN, the SIPRNET, and the various methods for achieving remote connectivity.

4.4.1.1 The SIPRNET. The SIPRNET is a world-wide network of backbone routers interconnected by high-speed serial links (mostly 512 kbps interconnections). The SIPRNET supports the TCP/IP protocol service and is planned to eventually support the Government Open Systems Interconnection Profile (GOSIP) service. The SIPRNET serves all DoD Secret-level subscribers and is not dedicated to GCCS users. In fact, GCCS users only comprise about 15 percent of the subscribers to the SIPRNET, unlike the WWMCCS environment in which WWMCCS users have dedicated use of the DSNET2 Top Secret level network. The SIPRNET is growing and the *GCCS System and Network Management CONOPS*, Version 1.6 lists 48 SIPRNET WAN locations which are receiving CISCO routers (CISCO AGS+ or 7000s). Seventeen of these sites serve the IOC GCCS sites (normal configuration) as shown in Figure 4-8. Appendix A of the *GCCS System and Network Management CONOPS* contains more detailed information on the SIPRNET, including topology charts by regions. GCCS users should contact DISA/D32211 at commercial 703-735-8290 or DSN 653-8290 for the most current information concerning the SIPRNET. Additionally, the SIPRNET is supported by the SIPRNET Support Center (SSC) located at Government Systems, Inc., Chantilly, Virginia. It provides general user services via telephone, e-mail and postal mail. Many services, such as the WHOIS, registry of network users, are available through the SSC's automatic mail service, SERVICE *@SSC.SMIL.MIL*. A help desk can be reached Monday through Friday, EST at:

Commercial Toll-Free	1-800-582-2567
International	1-703-802-8202

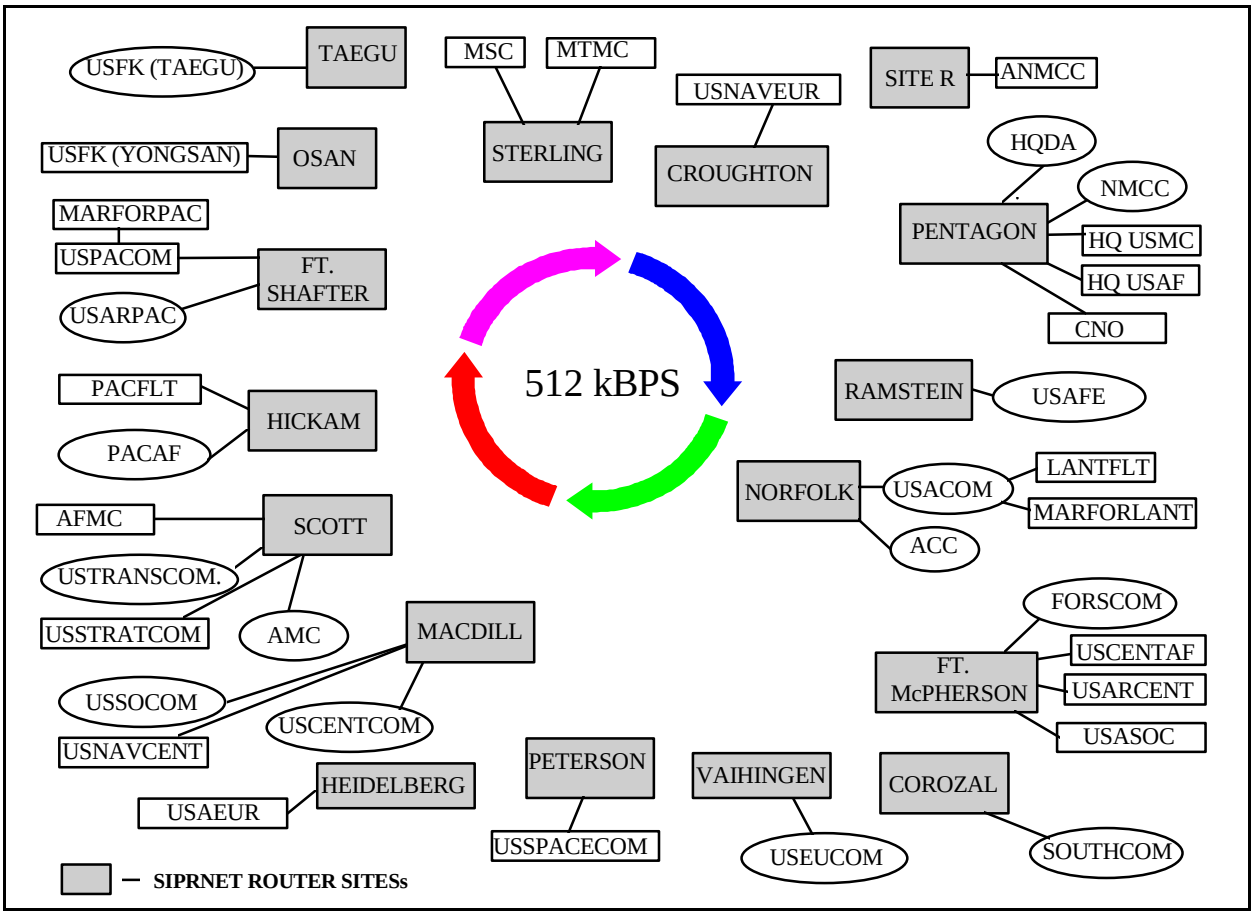

Figure 4-8. SIPRNET Router Site Support to GCCS IOC Sites

General user assistance is also available at *ssc@ssc.smil.mil* (SECRET level). Additional information on the SSC can be obtained from DISA/D32211 at the phone numbers for SIPRNET information provided above. Appendix A contains more information on the SSC.

SIPRNET sites are also being equipped with communications servers, which can be dialed-up by DoD Secret-level subscribers, including GCCS users. These servers are in addition to the GCCS communication servers being provided by the GCCS community (see Section 4.4.1.2).

4.4.1.2 Remote Connectivity. Remote connectivity is available to GCCS users removed from a GCCS site (geographically or in a network sense) via several paths, which provides flexibility to these users. Remote users in this context are those users who will access the target site GCCS LAN, either through a dedicated multiplexer channel or STU-III dial up, into a communications server (remote users are not those users removed from the target site but attached via a backside bridge router directly into the GCCS LAN or connected to the target site via the SIPRNET WAN). Remote users can either access a SIPRNET communications server or a GCCS communications server. Both methods are discussed in the following Subsections based on Figure 4-9.

4.4.1.2.1 Access via SIPRNET Communications Servers. Eighteen SIPRNET WAN sites worldwide are equipped with Cisco 2511(2511-CS) communications servers. (Appendix C of the *GCCS System and Network Management CONOPS* lists the eighteen sites.) The 2511-CS communications servers will serve all SIPRNET users, not just GCCS users. The SIPRNET communications servers will be under the operational control of the Defense Information Infrastructure (DII) Regional Control Centers (RCCs), not the GCCS community. Most of the SIPRNET 2511-CSs will be connected to the SIPRNET WAN via Ethernet connections at 10 Mbps. The 2511-CSs connect to the AT&T STU-III model 1910 for dedicated wireline encryption. The 2511-CS dial-in ports are capable of 112 kbps throughput but are being limited initially to 19.2 kbps to match all makes of DoD user dial-in equipment. Newer STU-IIIs will allow speeds up to 38.4 kbps and subscribers will be allowed this service after initial fielding. The user STU-III connection is shown as link "c." in Figure 4-9 (see the reference for additional information). Some users, including GCCS users could use dedicated circuits for asynchronous connection to the SIPRNET through these communications servers if necessary. Additional information can be obtained from the DISA/D32211 office.

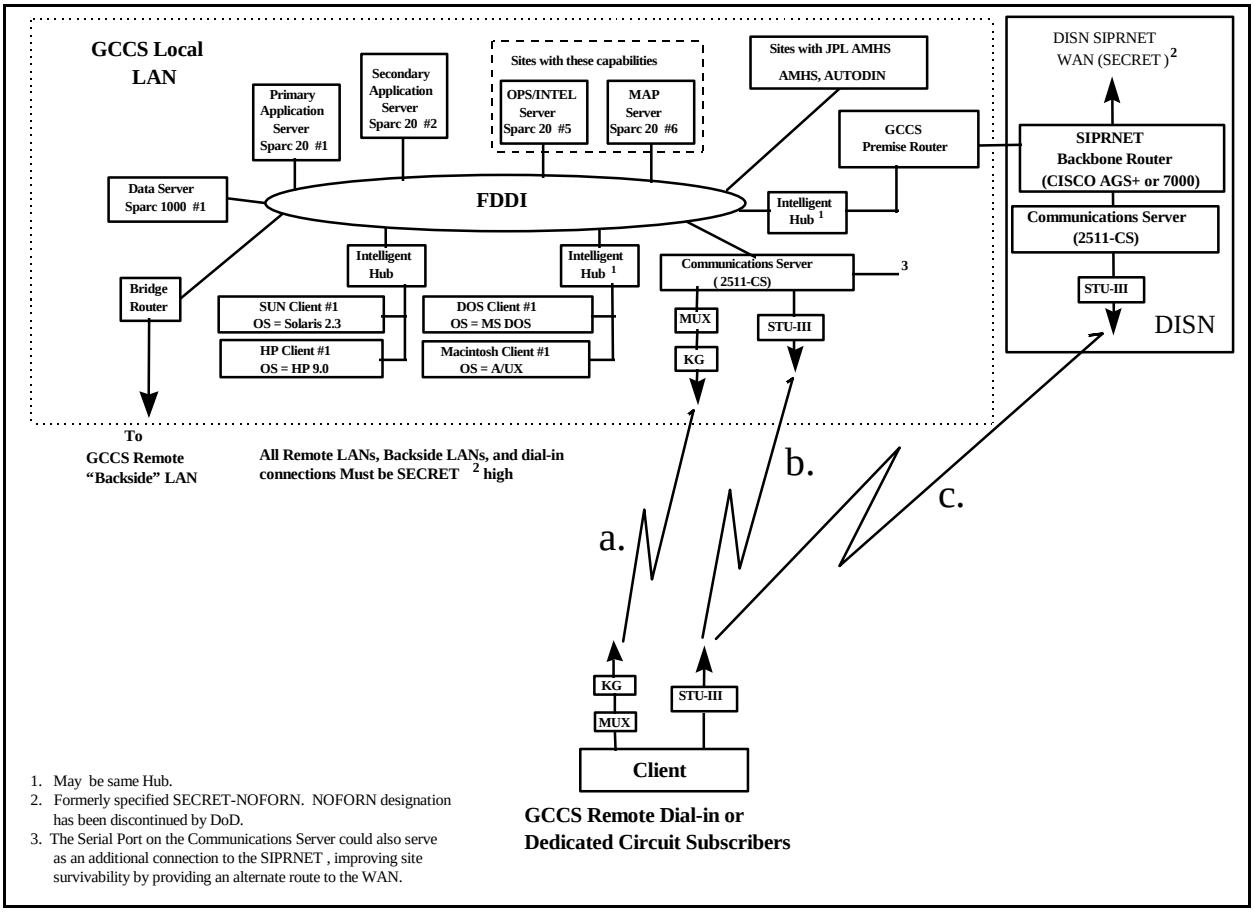

Figure 4-9. Remote Connectivity

4.4.1.2.2 Access via GCCS Communications Server. Appendix D of the *GCCS System and Network Management CONOPS* describes the use of the GCCS communications servers. Eighty-six Cisco 2511 communications servers, different than the SIPRNET assets, are being installed at GCCS sites worldwide. Users can access these servers using dedicated circuits (link "a." in Figure 4-9) or dial-up via STU-IIIs (link

"b." in Figure 4-9). The GCCS 2511-CSs will be under the operational control of the GCCS sites. Overall direction and management will be under the GCCS Management Center (GMC). GCCS users must use the newer generation STU-IIIs capable of compression for a 38.4 throughput rate, such as the AT&T STU-III Model 1910. This is because most GCCS applications will require at least 32 kbps bandwidth to run adequately. Also, each GCCS IOC site will have at least one asynchronous port on a 2511-CS dedicated to remote emergency management access by the GMC, if necessary, to prevent a site from becoming isolated from the GCCS network.

GCCS users must know the correct phone numbers, addresses, and security codes/authentication requirements to maintain connectivity in GCCS. Also, correct codes, account numbers, and permissions must be obtained ahead of time to use GCCS software. Users with questions on the proper procedures must contact their site administrators and communications personnel before attempting to use the system's capabilities. Additional information can be obtained from the GMC and the GCCS Engineering Department.

4.5 Teleconferencing Topology

GCCS Teleconferencing replaces the former WIN Teleconferencing functionality in WWMCCS but with much more capability. Three applications: IRC, Newsgroups (Usenet News), and World Wide Web (WWW) provide the Teleconferencing capability. These applications are described in Section 3.3. IRC is a real-time interactive conferencing tool in which user messages input into the conference are visible to everyone in the conference. However, the messages are non-persistent. This capability is similar to a telephone conference and the old "Comm" functionality in WIN. Usenet News is a version of the Newsgroups used on the Internet. Users run client software called newsreader to download articles from a news server. The articles are almost entirely text without binary graphical files or word processor control characters. Articles current at the time of log on are available. WWW provides the ability to use and the intuitive graphical interface to move large files of any type. This application is not interactive. Rather, an author makes material available on the "web" where other users can use client software (web browsers) to download and print it. Files can be formatted word processor files and binary graphical files such as maps and pictures. The GCCS Teleconferencing applications are from public domain sources and commercial vendors, modified to allow need-to-know features with an access restriction appropriate for GCCS operations on the SIPRNET.

The three Teleconferencing applications use different topologies. The IRC network is a virtual network on the SIPRNET and each link is a virtual link between two servers. Servers are interconnected by primary links, those necessary to connect all servers that are necessary to operate the network properly, with secondary links as back-ups. Initially, there are six hubs as shown in Figure 4-10. These are USACOM, NMCC, USPACOM, USTRANSCOM, USCENTCOM, and USEUCOM. All other servers are connected to exactly one of these six servers at any one point in time.[2]

Due to their central position in the topology, ACOM and TRANSCOM play a critical role in the IRC network. If one of them goes down, the network will be divided into three separate networks (until operators reconfigure the network using secondary links).

---

[2] Organization names have been abbreviated in Figure 4-10 and Table 4-7 for simplicity (e.g., USEUCOM is referred to with the short title EUCOM).

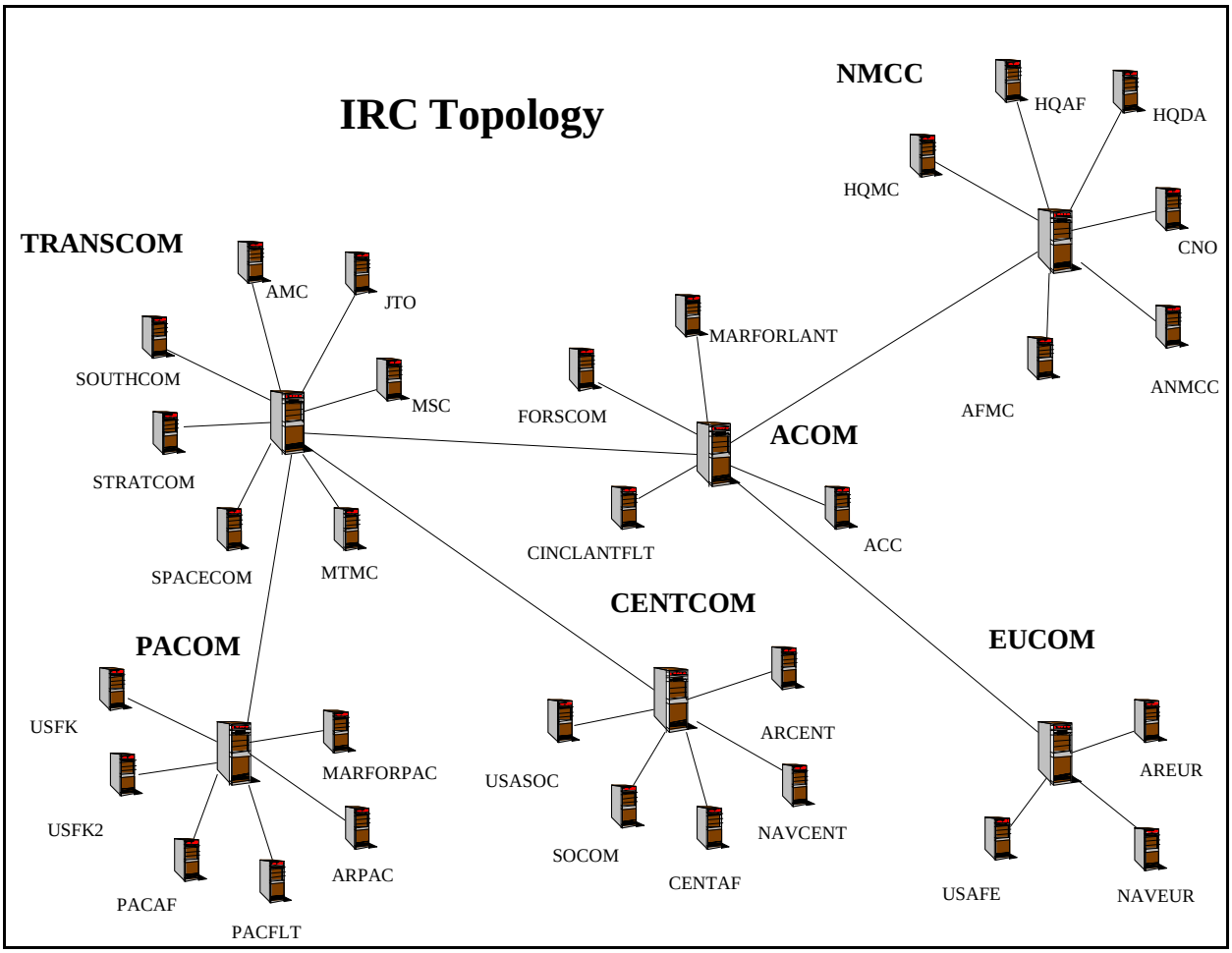

Figure 4-10. Topology of the IRC Network

Newsgroups uses the News Network topology shown in Table 4-7. This is not like the IRC topology since News servers maintain databases of articles received and do not require an acyclic network. There are also six hubs, the same as IRC, but these hubs are multi-connected to each other. News forwards articles in batches with a default for a server to transmit every 10 minutes.

Table 4-7. News Topology

Site #	Site Name	Links
1	ACOM	2,3,4,5,6,10,21,27
2	CINCLANTFLT	1,3,5,7
3	FORSCOM	1,2,4,13,26
4	ACC	1,3,5,22,30
5	MARFORLANT	1,2,4,33

Table 4-7. News Topology (cont).

Site #	Site Name	Links
6	CENTCOM	1,7,8,9,10,14,29,30,33
7	ARCENT	2,6,8,9,27
8	NAVCENT	6,7,9,21
9	CENTAF	6,7,8,32
10	EUCOM	1,6,11,12,13,27
11	USAFE	10,12,13,34
12	AREUR	10,11,13
13	NAVEUR	3,10,11,12,24
14	PACOM	6,15,16,17,18,19,20,21
15	PACAF	14,16,20
16	PACFLT	14,15,17,36
17	ARPAC	14,16,18
18	USFK	14,17,19,23
19	USFK2	14,18,20
20	MARFORPAC	14,15,19,26,32
21	TRANSCOM	1,8,14,22,23,24,25,26,31,32
22	AMC	4,21,23,25,35
23	JTO	18,21,22,24,31
24	MSC	13,21,23,25
25	MTMC	21,22,24
26	SPACECOM	3,20,21
27	NMCC	1,7,10,28,33,34,35,36,37
28	ANMCC	27,29,31
29	SOCOM	6,28,30
30	USASOC	4,6,29
31	STRATCOM	21,23,28

Table 4-7. News Topology (cont).

Site #	Site Name	Links
32	SOUTHCOM	9,20,21
33	CNO	5,6,27,34,37
34	HQDA	11,27,33,35
35	HQAF	22,27,34,36
36	HQMC	27,35,37,16
37	AFMC	27,33,36

For the WWW, the Web operates on an entirely different principle than do IRC or News so the architecture is different than either IRC or News. IRC and News are "active" services i.e., servers transmit information to the client/users who select what they will or will not receive. The Web, on the other hand, is a passive information supplier. The Web user directs browser software to connect to specific Web servers to retrieve documents of interest. Instead of servers communicating with each other and clients communicating with one local server, WWW servers are autonomous and clients must directly access the server that has the information the client needs.

The following information is taken from the SUM for easy reference. Two server packages are being provided for GCCS. Netsite is a commercially available Web server produced by Netscape Communications Corporation. Httpd is a public-domain server available from NCSA. Both support restricting user access to documents based either upon user ID + password or upon the location of the user (the specific PC from which the user is connected).

The browser software for GCCS is Netscape (produced by Netscape Communications) or Mosaic. Netscape can display files in a wide variety of formats including HTML, the workhorse of the Web, text, and gif (graphics). It also has the ability to execute other programs for displaying files that are in other formats such as *postscript*, *jpeg*, *mpeg*, *wav*, etc.

The use of Netscape as the client and Netsite as the server provides a level of privacy that is currently unavailable using any other combination of Web browser and server. The data passed between these two programs may be encrypted. The encryption mechanism is <u>not</u> supported by the National Security Agency, but nevertheless, provides enhanced privacy to the user. See Figure 4-11 for the basic Web architecture.

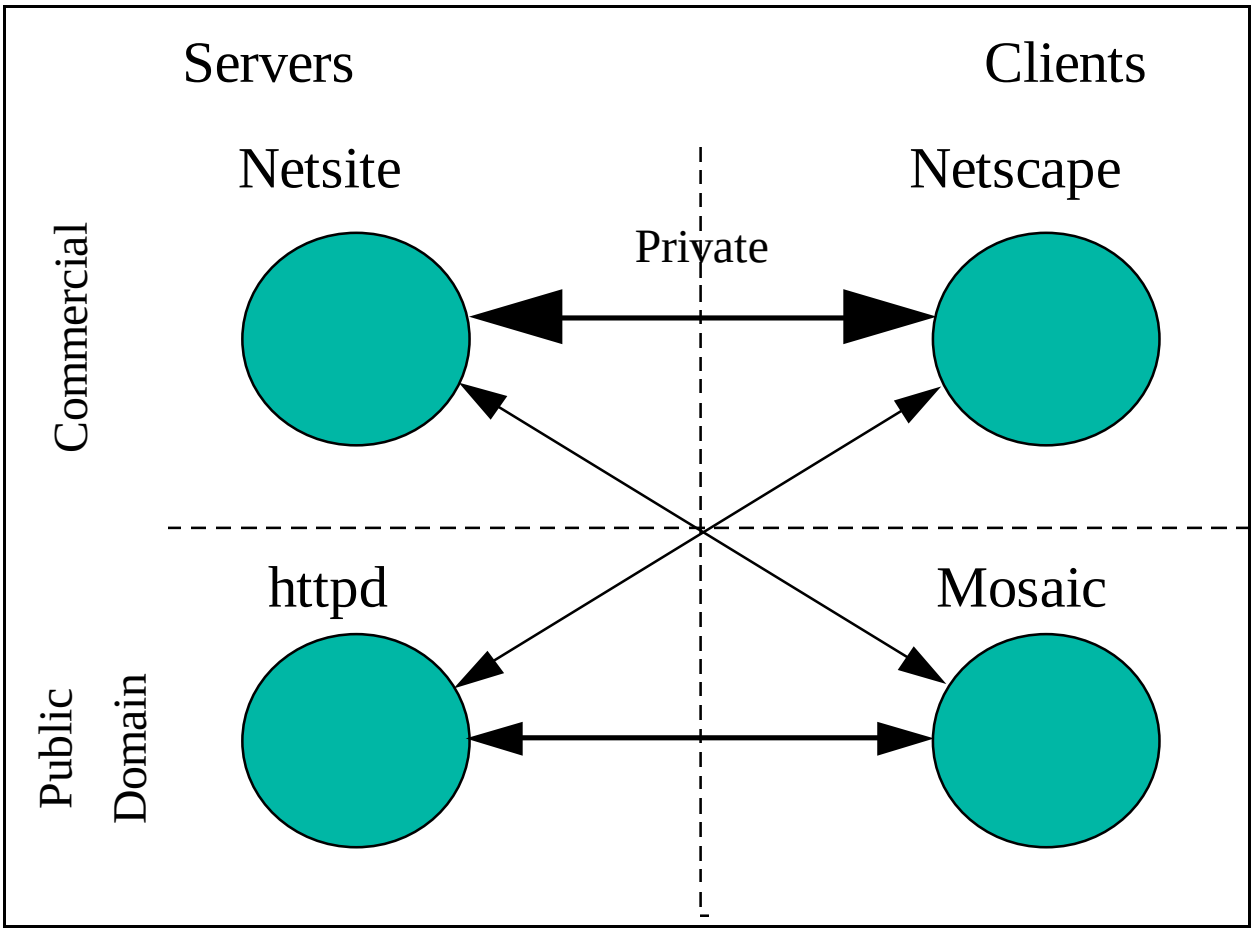

Figure 4-11. World Wide Web Architecture

Users can find additional background information on GCCS Teleconferencing in the *GCCS System Administration Manual, Change 1 added*, Section 4. The GCCS Site SAs play important roles in establishing client/server configurations within the topologies. Teleconferencing users can find instructions in the *GCCS Teleconferencing User's Manual*. GCCS users should review the applicable portions of both references to better understand GCCS Teleconferencing and the user's responsibilities, especially in regard to security.