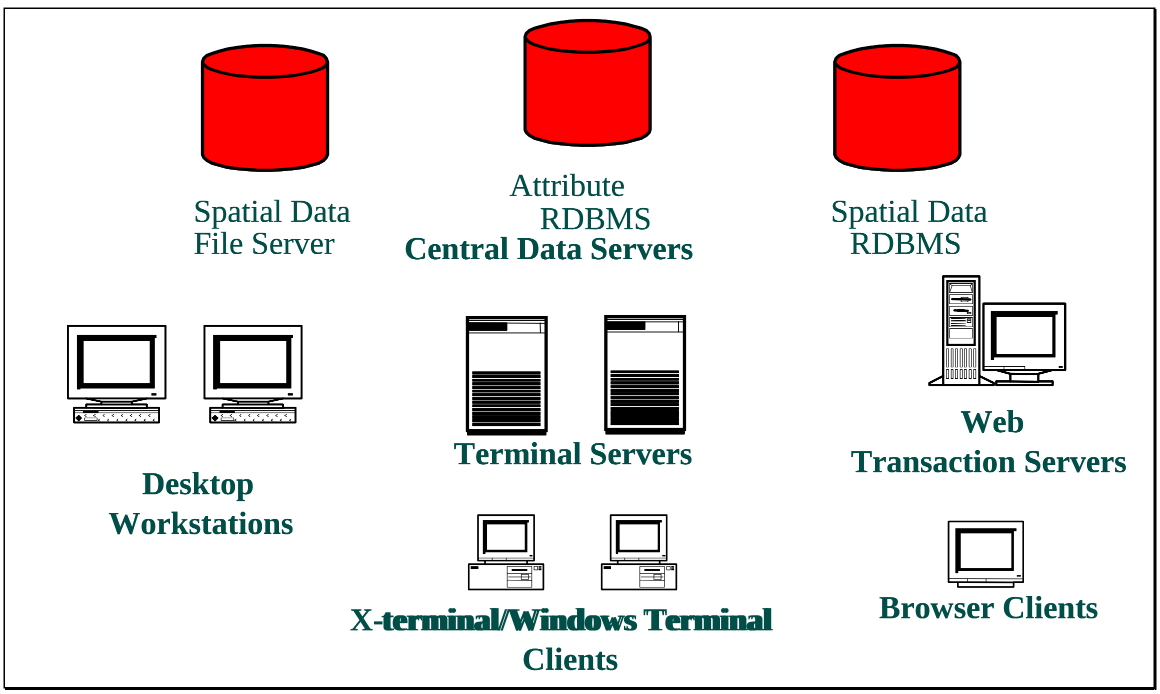
4.0 GIS Product Architecture

This section provides a basis for understanding components involved in distributed GIS applications. Understanding basic application architecture, relationships between commercial products and custom applications, and the component interfaces required to support GIS solutions provides a foundation for understanding distributed GIS design principles.

Enterprise-level GIS applications support a variety of users throughout an organization, all requiring access to shared common spatial and attribute data. System hardware and software environments for distributed GIS applications are supported by multi-tier client/server architecture. An overview of this architecture is presented in Figure 4-1.

Figure 4-1
GIS Multi-Tier Architecture



- **Central Data Servers.** Shared spatial and tabular database management systems provide central data repositories for shared geographic data. These database management systems can be located on separate data servers or on the same central server platform.

- **Application Compute Servers.** GIS applications are supported within the distributed configuration by hardware platforms that execute the GIS functions. In a centralized solution, application compute servers can be UNIX or Microsoft Windows platforms that provide host compute services to a number of GIS clients.

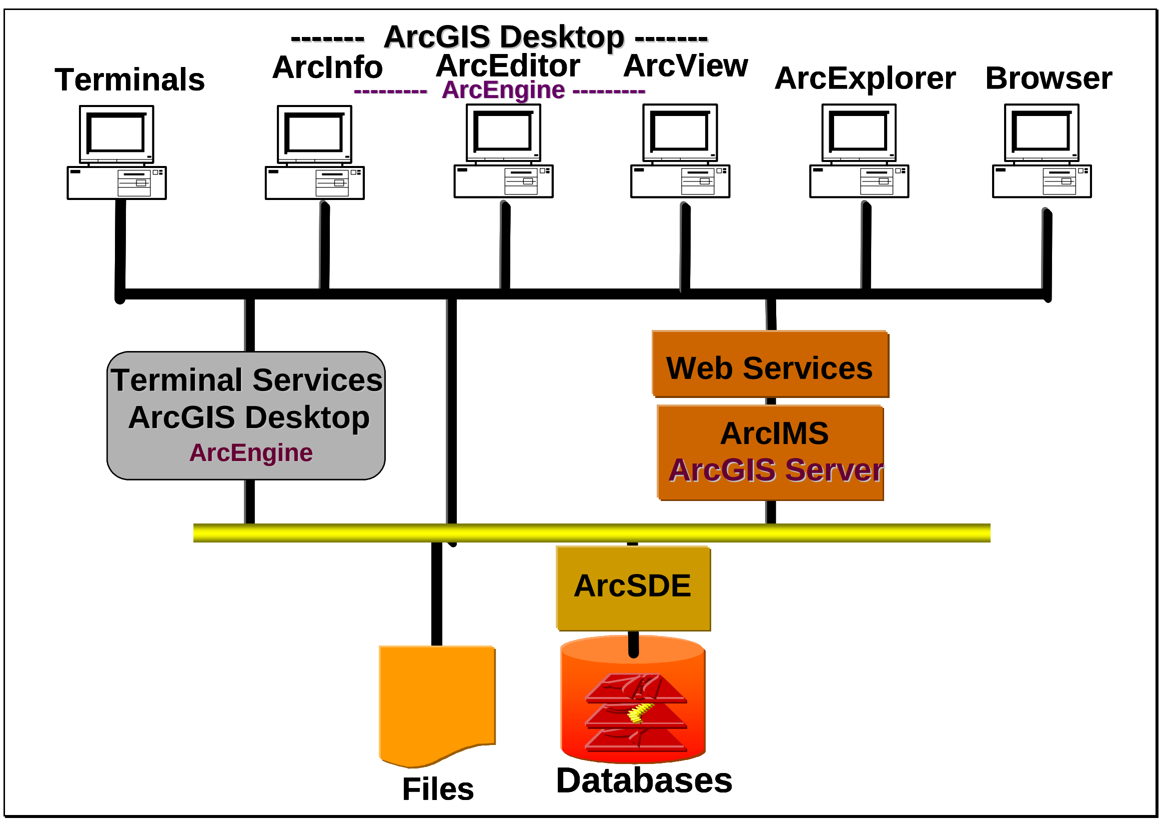
These platforms include terminal servers and Web transaction servers (map servers). In smaller configurations, the application compute server and central data server may be on the same platform.

- **Desktop Workstations.** Display and control of application processes are provided by desktop workstations which, in many cases, are PCs running X-emulation software, Windows terminal clients, or Web browser clients. In many GIS solutions, the client application server and desktop user workstation may be the same platform.

4.1 ArcGIS System Software Architecture

ArcGIS is a collective name representing the combined ESRI GIS technology. This technology includes a mix of ArcGIS desktop applications and ArcGIS server-based services. Figure 4-2 provides an overview of the ArcGIS system environment.

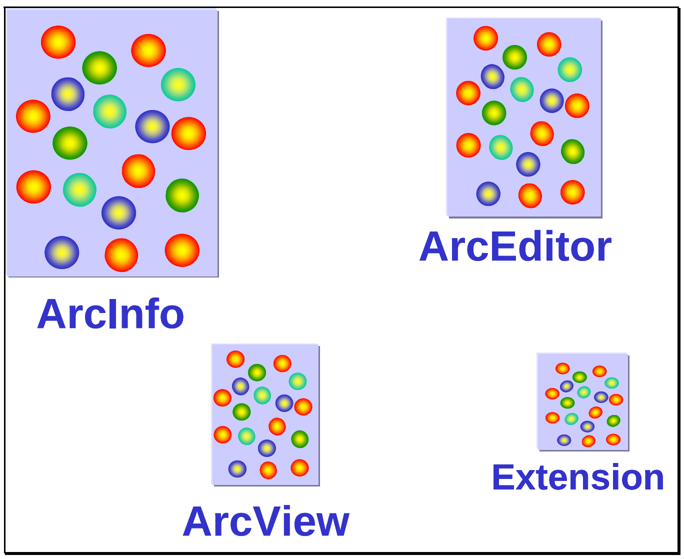
Figure 4-2
ESRI ArcGIS Software



4.2 ArcGIS Desktop Software Architecture

ArcGIS desktop applications include ArcInfo, ArcEditor, and ArcView licensing options. These applications are supported by a common set of ArcObjects developed using COM programming technology. ArcGIS desktop software is supported on the Microsoft Windows operating system. The ArcGIS desktop technology presents an object-oriented, user-friendly interface along with a variety of GIS functionality. Figure 4-3 provides an overview of the ArcGIS desktop software.

Figure 4-3
ArcGIS Desktop Software



The ArcGIS 9 release includes two new ArcObjects developer environments (ArcGIS Engine and ArcGIS Server). ArcGIS Engine supports development of lightweight custom desktop applications, while ArcGIS Server supports development of custom Web geoprocessing services. A complete set of ArcObjects components are exposed for each development environment.

An overview of ESRI commercial GIS software is provided in Figure 4-4. These include GIS applications (UNIX and Windows), data management solutions (GIS file server, ArcStorm, and ArcSDE), and remote access client solutions (Windows terminals and browsers).

Figure 4-4
ESRI Software Environments

- **GIS Applications**
  - GIS for UNIX Product Architecture
  - GIS for Windows Product Architecture
- **Data Management Solutions**
  - GIS File Server (coverages, shapefiles, ArcInfo LIBRARIAN, ArcStorm)
  - Spatial Database Engine (client/server data management)
- **Remote Access Client Solutions**
  - Windows Clients with Microsoft Terminal Servers
  - Browser Clients with ArcIMS
  - Browser Clients with ArcGIS Server
  - GIS Desktop applications with AGS Services

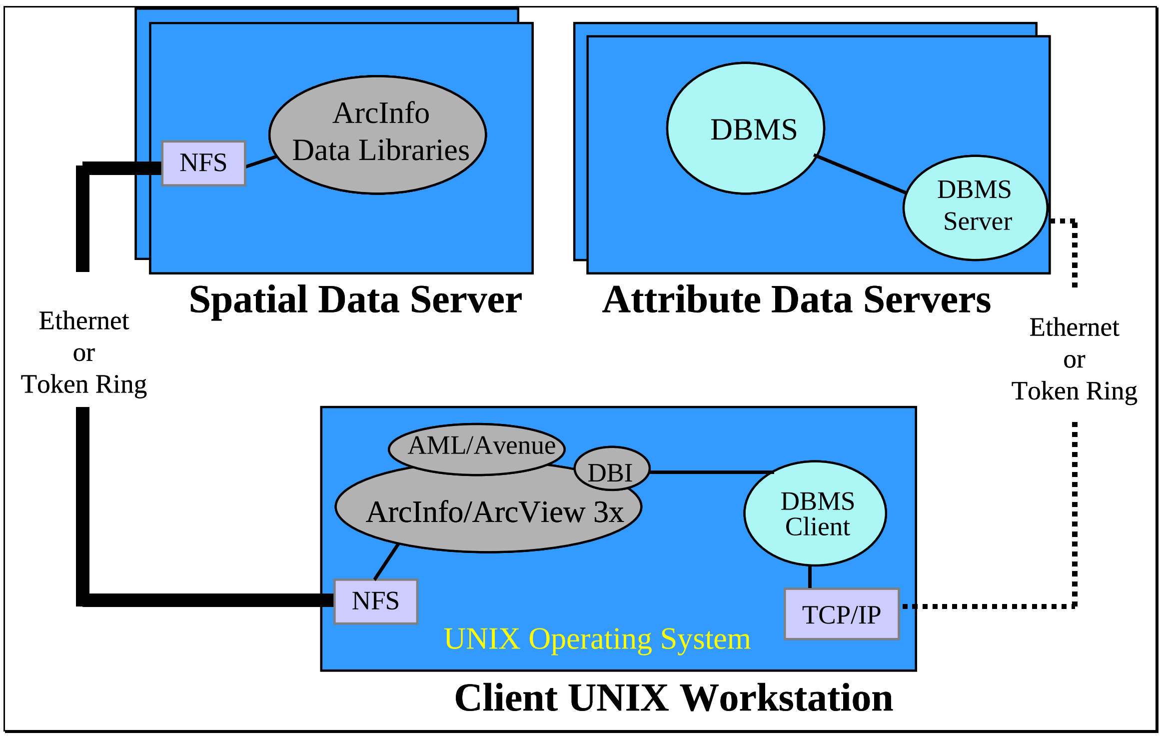
ESRI commercial software performance and associated system interface specifications provide a baseline for system design. Custom GIS application solutions require system resources to support the basic underlying commercial software functions.

GIS applications are supported by an open systems architecture. This architecture combines a variety of closely integrated commercial products to establish a fully supported system solution. Commercial software supports evolving communication interface standards to enable system integration with minimum customization. The importance of selecting well established software solutions cannot be over-emphasized since all parts of the distributed configuration are critical in supporting overall system performance.

4.3 GIS for UNIX

Primary components supporting distributed ArcInfo for UNIX solutions are identified in Figure 4-5.

Figure 4-5
GIS for UNIX Product Architecture
(UNIX File Server Spatial Data Source)



GIS application functions are executed within the UNIX workstation operating system environment. File-based spatial data management solutions (including spatial coverages, shapefiles, and ArcInfo LIBRARIAN) are supported entirely from the client workstation. The DBMS vendor software operates within the system environment provided by the attribute data server. Network file servers (NFS), provided with the UNIX operating system, mounts files located on the spatial data server to the client workstation, making them appear as if on local disks. Spatial data located on the GIS data server appears as local data to the GIS application.

A Database Integrator module is included with ArcInfo and ArcView that translates communication from the GIS application to the DBMS client module located on the client workstation. DBMS client and server components handle network communication between the client workstation and the DBMS data server using appropriate network communication protocol. ArcInfo AML or other standard programming tools such as Visual Basic, Delphi, PowerBuilder, C, C++, Tcl/Tk, and/or Motif can be used to establish a custom user interface to ArcInfo application environments. Avenue macro language supports customized ArcView application environments.

Communication between GIS workstation applications and spatial data located on a separate file server requires a significant amount of network traffic overhead due to the connection-oriented protocol supporting NFS communications. Single-threaded application processes that function in memory on the client workstation execute program calls against the central database. Each line of code must receive a response over the network connection before the next line of code can be executed. Several transmissions are required to locate each source of required data. This type of communication generates lots of extra network traffic.

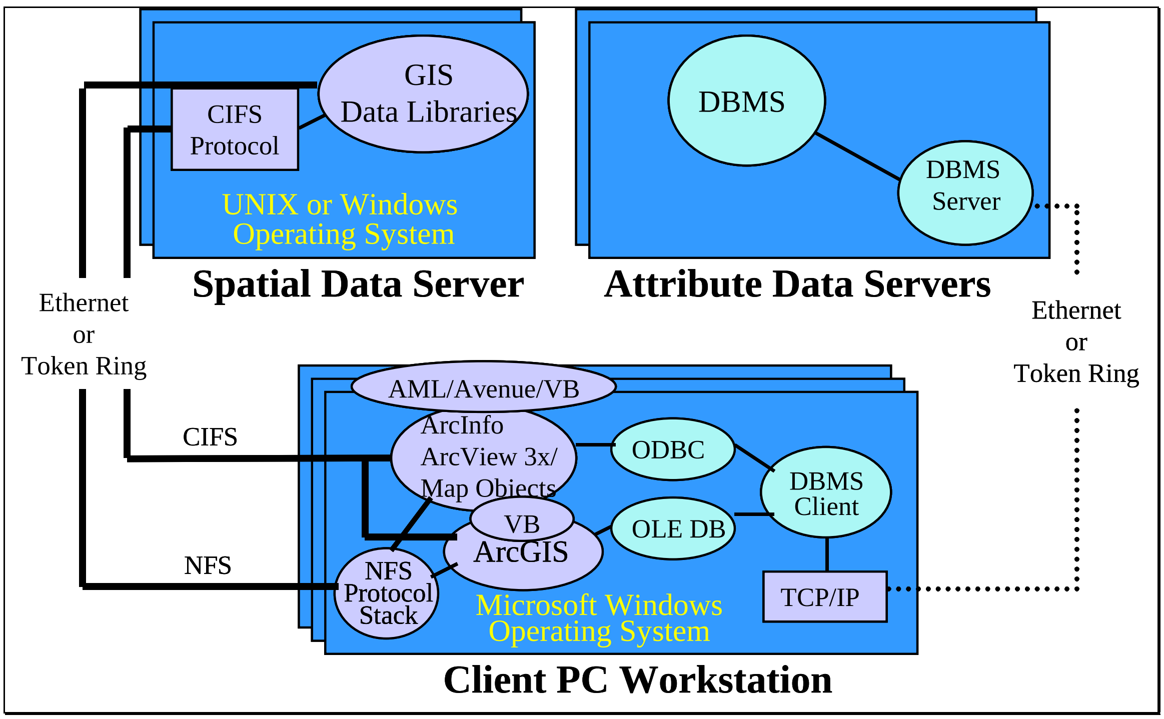
Communication between GIS workstation applications and remote attribute data requires very little network traffic. Queries to the central tabular DBMS are packaged in a single client request and sent as a message to the server for processing. The request is handled by a separate server process, which compiles the answer to the query and sends the response back to the client application for further processing. There are two reasons this is much more efficient than accessing spatial data—one is the use of message-oriented communication protocol (data processing is supported by a local server process); the other reason is the limited size of tabular data files, which are much smaller than spatial graphical files.

All of the ArcInfo functionality represented in the ArcInfo Workstation legacy software has been rewritten and deployed in the ArcGIS desktop software. The modern software takes advantage of object technology to accelerate software development and enhance GIS software functionality. The ArcGIS desktop environment supports a much more friendly user interface and powerful GIS functionality than was possible with the legacy ArcInfo Workstation software.

4.4 GIS for Windows

In 1996, ESRI ported the ArcInfo UNIX workstation application to the Windows platform, positioning ESRI to take advantage of the Microsoft Windows environment and the lower cost of PC hardware. ArcView applications were also deployed on Windows workstations. Critical components supporting distributed GIS for Windows solutions are identified in Figure 4-6.

Figure 4-6
GIS for Windows Product Architecture
(File Server Spatial Data Source)



GIS application executables execute within the operating system environment provided by the Windows platform. Microsoft Common Internet File Services (CIFS) protocols included with Windows operating system support sharing of server disk resources to PC clients. Remote data servers appear as local disk drives to the client Windows workstation, and GIS applications access to spatial data is provided from the client workstation. The GIS Windows applications were developed to an Open Database Connectivity standard (ODBC-compliant) communication interface. The ODBC interface provides access to PC-based attribute data sources including Microsoft SQL Server and Microsoft Access. An ODBC driver must be obtained to complete the interface between GIS applications and each specific attribute database. AMLs developed in the UNIX environment will continue to perform with ArcInfo Workstation for Windows. Avenue scripts supporting custom ArcView UNIX applications are supported by ArcView for Windows software. Desktop clients use an OLE-DB interface to the DBMS client.

Communication between GIS applications and spatial data located on a separate data server (using CIFS protocol) requires network traffic overhead similar to UNIX NFS communications. Accessing remote data sources may take twice as long as accessing the same data on local disk, depending on the data storage technology.

Initially, Windows data servers supported department-level workgroups. Server configurations capable of supporting enterprise-level GIS operations were not available. PC vendors (along with Intel) have made significant progress toward supporting enterprise server requirements. Windows commodity multi-processor servers can be configured for up to eight processors. Microsoft provides a cluster fail-over solution for Windows operating systems that supports server fail-over requirements. Windows 2000 Data Center servers provided by IBM and Unisys support up to 32 processor server environments.

Several solutions are available to support mixed Windows and UNIX environments. Software products are available to enable UNIX platforms to directly share disks to PC clients. Gateway products are available for Novell and Windows servers that support mapping of UNIX server disks to their supported PC workgroups. PC client NFS products are available to support mounting of the UNIX server disk. In all these solutions, the server disk is mapped to the client workstation to allow ArcInfo access to the remote server data as if it was on a local PC drive.

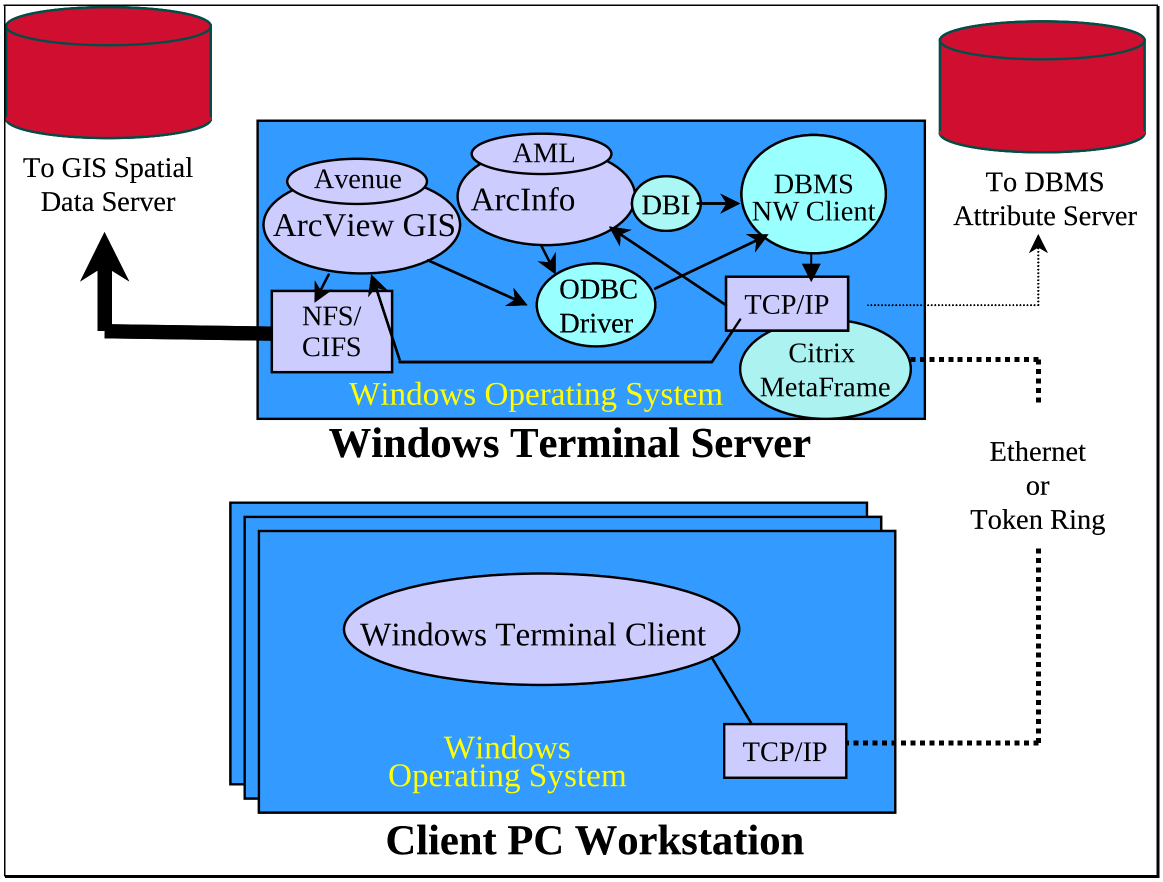
4.5 Microsoft Windows Terminal Server

The Microsoft Windows Terminal Server product establishes a multi-host environment on a Windows server. A Windows Terminal client provides display and control of applications executed on the Windows Terminal Server. Microsoft uses a standard remote desktop protocol (RDP) to support communication between the terminal server and client Windows platforms.

Citrix provides a MetaFrame extension product that provides a more efficient independent computing architecture (ICA) communication protocol to support communication between the terminal server and client Windows platform. The ICA protocol requires less than 28 Kbps bandwidth (rendering vector data information products) to support full Windows display and control of GIS applications supported on a Windows Terminal Server. The MetaFrame product also includes client software for UNIX, Macintosh, and embedded Web client applications.

Figure 4-7 provides an overview of the Windows Terminal Server communication architecture.

Figure 4-7
Windows Terminal Server Product Architecture

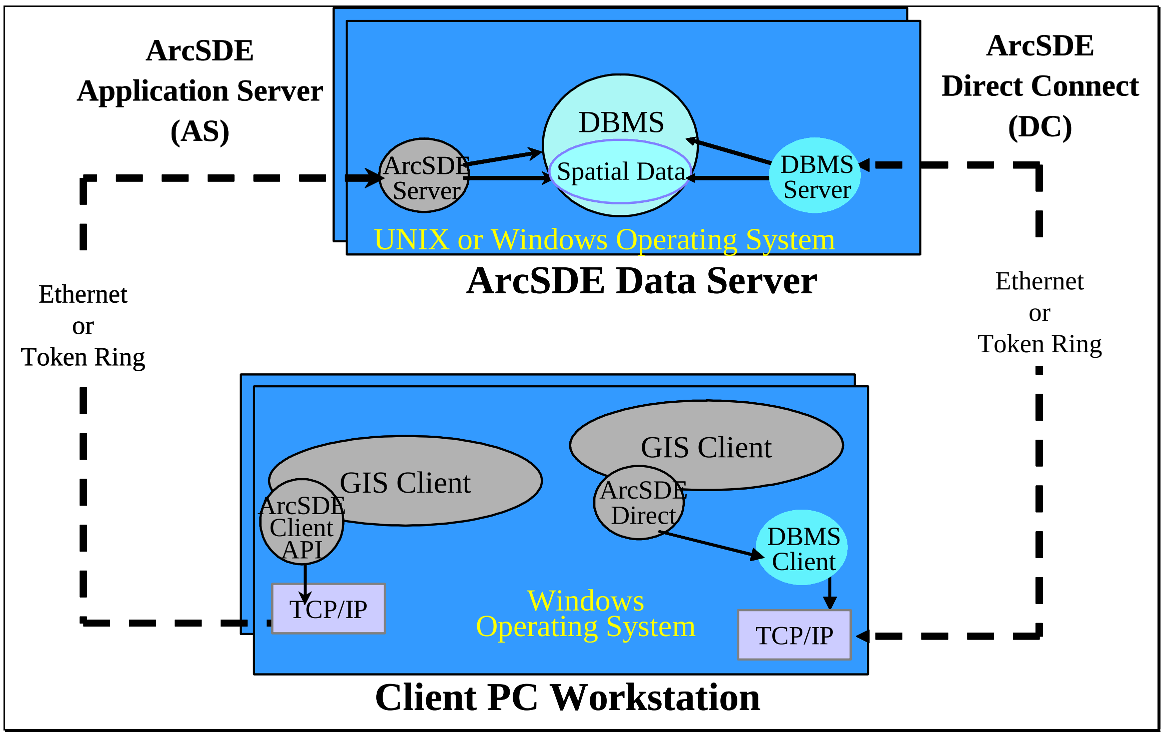


The Windows Terminal client communicates with the Windows Terminal Server through a compressed message-oriented communication protocol. The Windows environment display must be provided over the network to the client workstation, which requires much less data than that required for spatial data processing by the terminal server or a workstation client. The terminal display traffic requirements are very small, supporting full server application performance over 28-Kbps modem dial-up connections (displays with an image backdrop may require more bandwidth).

4.6 Spatial Database Engine (ArcSDE)

Spatial Database Engine supports storage of spatial data within standard commercial DBMS applications. Integration of GIS spatial data with the enterprise-level DBMS environment provides a powerful enterprise-level data storage solution for large data stores and/or solutions supporting a high number of GIS clients. A variety of data performance and administration tools are provided with the associated DBMS solutions. Critical components associated with ArcSDE communication architecture are identified in Figure 4-8.

Figure 4-8
ArcSDE Data Server Product Architecture



The ArcSDE solution combines spatial and attribute data into a single GIS database. Query processing is supported by the ArcSDE DBMS server. A transaction request is prepared by the GIS application client and sent to the ArcSDE server for processing. The ArcSDE server process completes the transaction query and returns the response back to the client for processing. There is no requirement in this configuration to map the data server disk to the GIS client. Application processes located on the ArcSDE data server process all spatial and attribute data requests received from the GIS client application.

ArcInfo, ArcView, MapObjects, ArcGIS Engine, ArcIMS, and ArcGIS Server applications include ArcSDE client APIs that support direct access to central SDE server data. Also, both ArcSDE and ArcInfo support direct conversion of ArcInfo coverages to ArcSDE layers. An additional ArcSDE CAD Client API is available to support storage of MicroStation and AutoCAD data in ArcSDE.

ArcSDE 8 supports the traditional georelational database and a new geodatabase-relational data model. This version also introduces the concept of a versioned database and supports native data maintenance operations from the desktop ArcInfo 8 platform in the form of a versioned database.

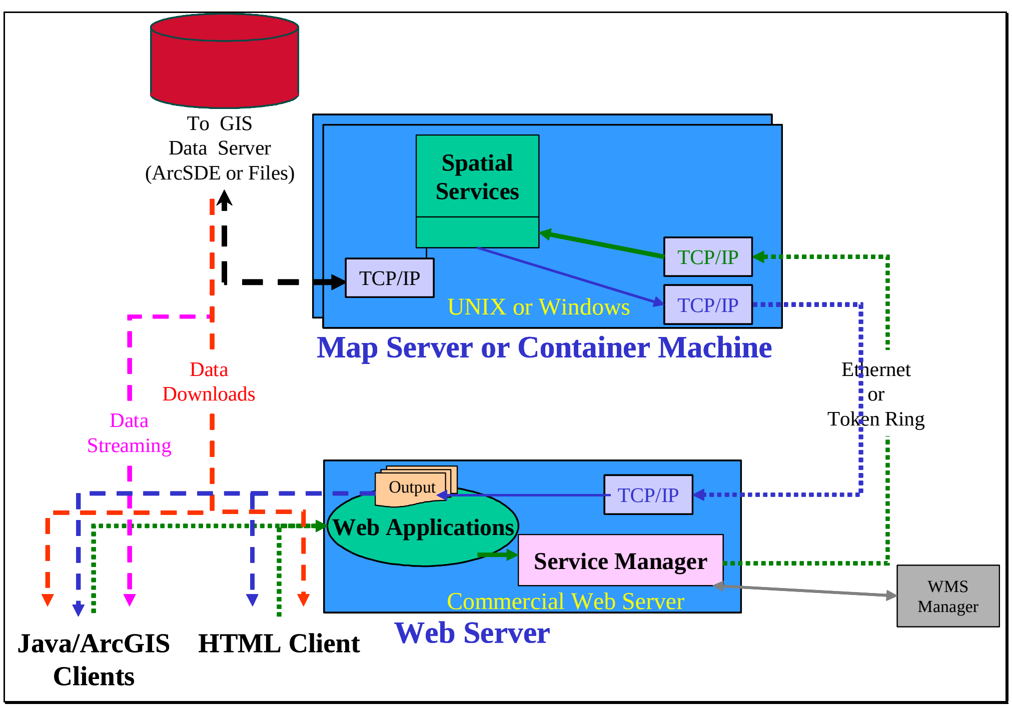
Standard DBMS client/server communications can be used with ArcSDE but are not required for ArcSDE queries. When used, they can provide standard access to attribute data through the DBMS client communication interface.

The ArcGIS 8.1 release includes a direct connect ArcSDE client access option for Microsoft SQL2000 and Oracle database solutions. The ArcSDE Direct option for Oracle will connect to the Oracle network client. The Oracle network client will communicate ArcSDE query calls to the server. The ArcSDE Direct option for SQL2000 will support direct communications to the server. Query processing will be supported by the DBMS functions on the server platform. To upgrade existing ArcSDE client applications, the ArcSDE Direct Connect API is available for download. A mix of direct connect and ArcSDE server connect clients can be supported in the same geodatabase environment.

4.7 Web Mapping and Network Services (ArcIMS and ArcGIS Server)

Web mapping services provide a modern approach to serving map products and services over the Internet. The ArcGIS Desktop architecture presented earlier in this section represents tightly coupled client/server processes that demand stable high bandwidth communications over relatively short distances. Web communications are supported using a transaction based HyperText Transfer Protocol (HTTP), which optimizes communications over long distances and less stable communication environments. Critical components associated with the Web services communication architecture are identified in Figure 4-9.

Figure 4-9
Web Services Architecture



Web services are published on the Web server. Web server clients are presented a catalog of published services. Web applications consume map services and render a client presentation layer to support the published application workflow. Client and Web server are loosely connected, where each client communication represents a complete transaction. Transactions are processed by the appropriate Web-based GIS server and returned to the client.

ESRI Web GIS services are supported by ArcIMS and ArcGIS Server software. ArcIMS includes several service engines that support efficient deployment of map services on the Web. ArcGIS Server provides an ArcObjects software-based server development environment for deploying GIS server-based ArcGIS applications and services. ArcGIS Server can be deployed in a Web architecture or as a LAN/WAN network service for desktop clients. ArcGIS Server will also be used to deploy "smart client" technology with the ArcGIS 9.2 release. Smart clients are loosely connected, lightweight handheld or desktop computers that support persistent data cache and disconnected GIS client operations. Client application deployment and data synchronization are managed by ArcGIS Server parent services.

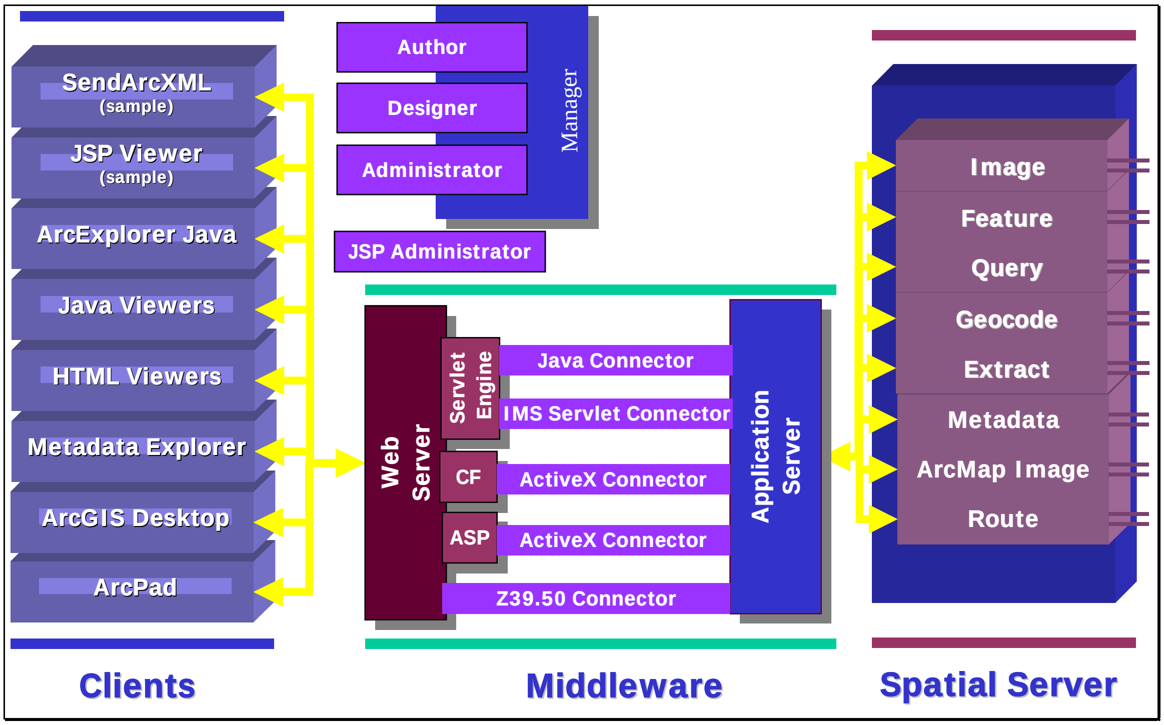
In the following general architecture discussions, GIS server will be used as a general term to represent ESRI ArcIMS or ArcGIS Server technology.

- **ArcIMS Architecture.** ArcIMS includes a Java Web servlet that supports Web map-publishing services. The standard product includes an ArcIMS manager and map development wizards that support design and authoring of most standard map products without special programming. ArcIMS also includes a Java client that supports standard Web products, data streaming, and data downloads. The Java client also supports integration of local vector data with map images obtained from the Web. ArcIMS Web services can also be used as a data source for ArcGIS desktop clients.

  The map server platform supports the primary ArcIMS Web services. Map services are developed by the ArcIMS Manager design and authoring tools producing templates on the application server that manage the map service and performance as a service queue. Additional programming tools (ColdFusion [CF] and Active Server Pages [ASP]) can be used on the Web server to develop custom user workflow presentations.

Figure 4-10 provides an overview of the ArcIMS 4 component architecture.

Figure 4-10
ArcIMS 4 Architecture

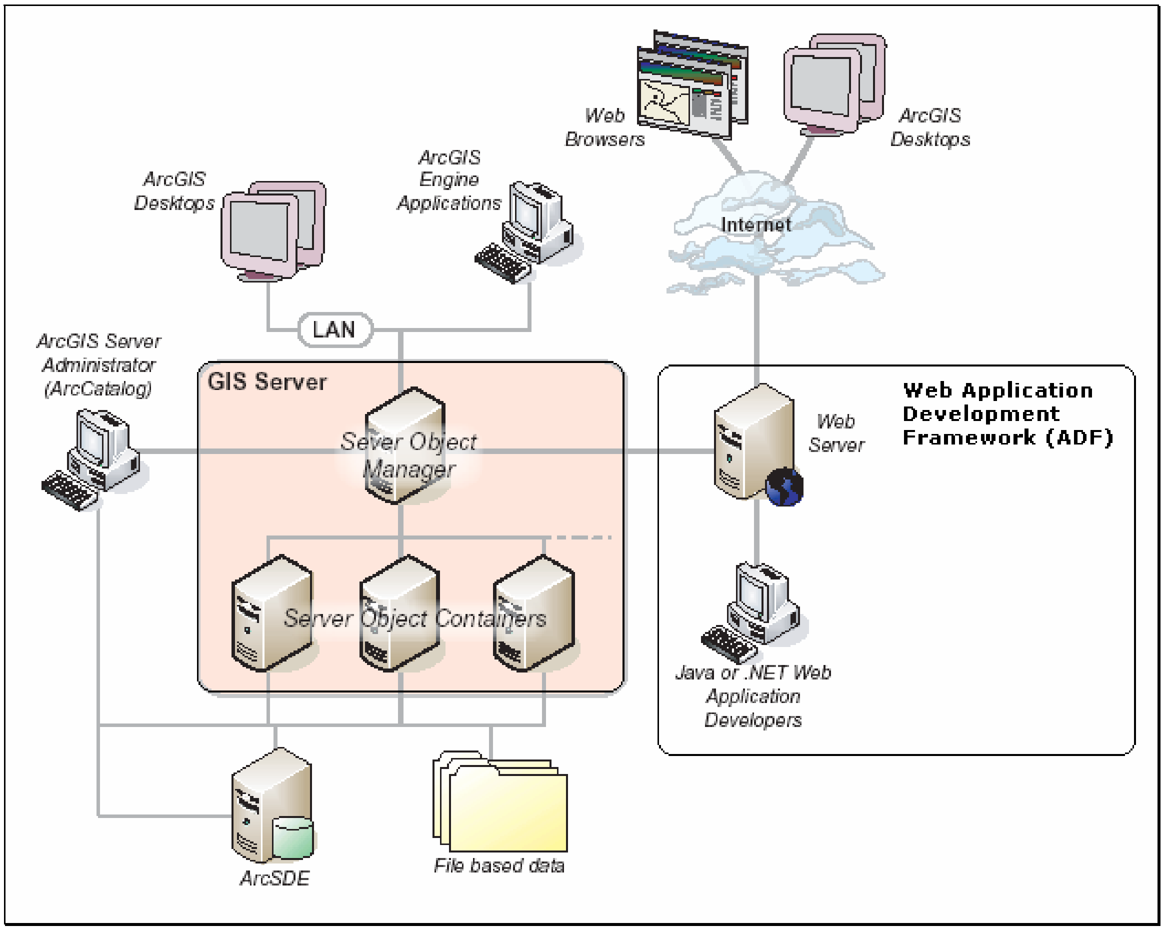


- **ArcGIS Server Architecture.** ArcGIS Server is a set of objects, applications, and services that make it possible to run ArcObjects components on a server platform environment. Server objects are managed and run within the GIS server. Server applications make use of server objects and may also use other ArcObjects components that are installed on the GIS server.

  The Web server hosts server applications and Web services written using the ArcGIS Server application programming interface (API). These Web services and Web applications can be written using the ArcGIS Server Application Development Framework (ADF), which is available for both .NET and Java developers.

Figure 4-11 provides an overview of the ArcGIS Server component architecture.

Figure 4-11
ArcGIS Server Environment

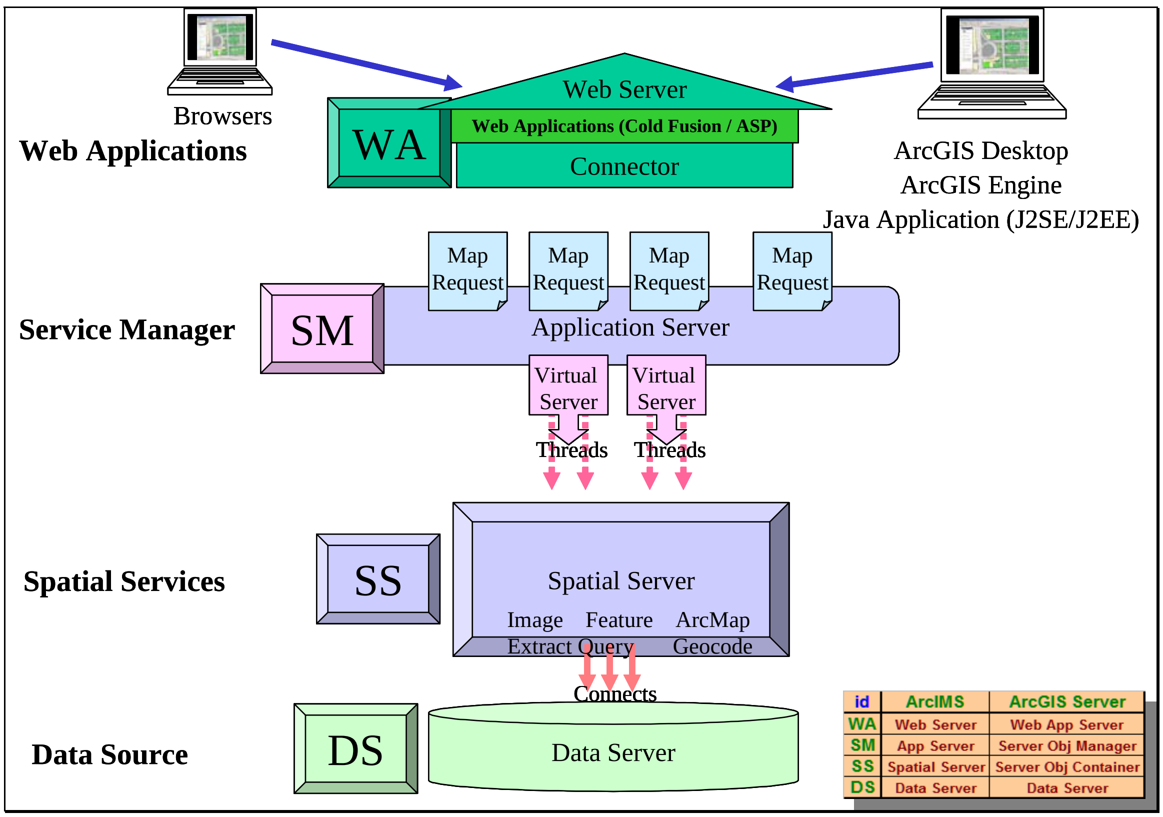


4.7.1 Web GIS Server Platform Configuration Strategies

The software architecture components for ArcIMS and ArcGIS Server have different names and functionality, although in a logical sense they perform similar functional roles and are supported by similar platform configuration strategies. Location of the various software components and the software configuration can directly impact the Web site peak transaction capacity, service reliability, and overall output performance.

Figure 4-12 provides an overview of the ArcIMS component architecture and the associated software configuration groups. The ArcIMS server architecture includes four potential configuration groups identified as Web applications (WA), service manager (SM), spatial services (SS), and data source (DS).

Figure 4-12
ArcIMS Component Architecture



The ArcIMS configuration groups include the following:

- **ArcIMS Web Applications (WA).** The Web server components support communications between the ArcIMS map services and the Web client. Web applications can be included to manage and enhance user workflow and client display presentation. Connectors on the Web server translate Web HTTP traffic and/or Web application program calls to communication understood by the ArcIMS Web services.

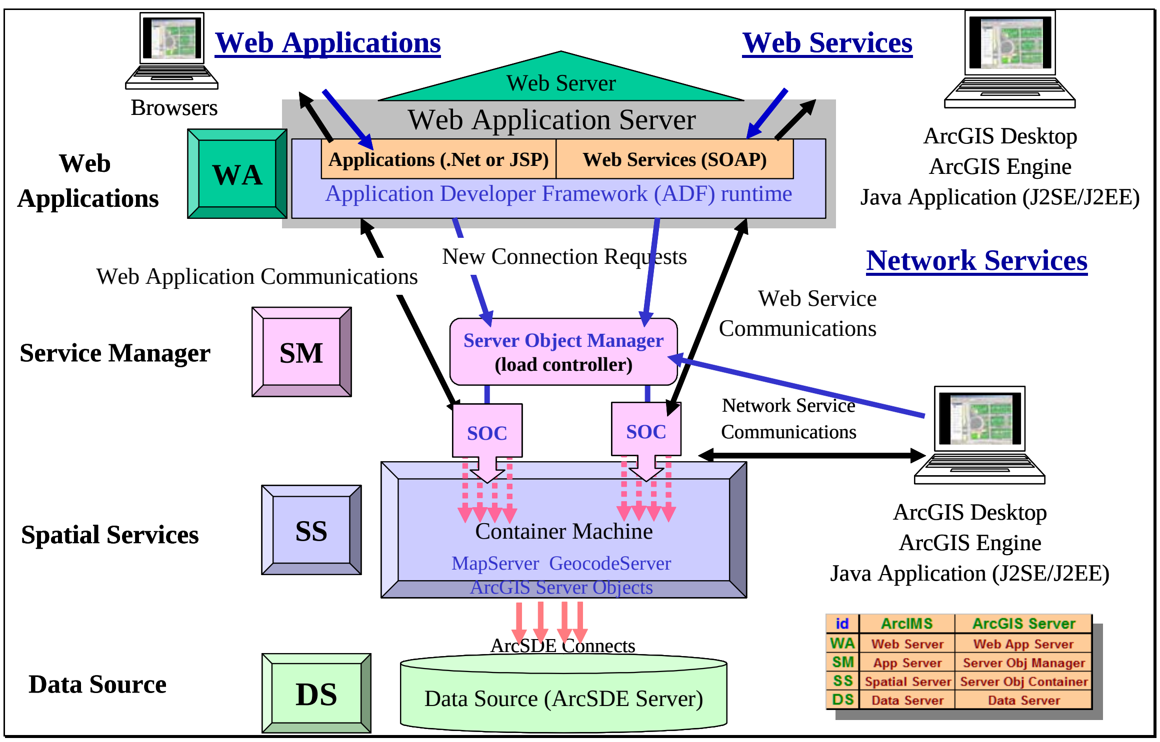
- **ArcIMS Service Manager (SM).** The ArcIMS application server component provides a service management role that supports the inbound map service request queues (virtual servers) and configured connects to the ArcIMS public service engines (Image, ArcMap, Feature, Extract). Inbound requests are routed to available service instances for processing. A relatively small amount of processing is required to support the application server functions.

- **ArcIMS Spatial Services (SS).** The map server platform hosts the ArcIMS spatial servers. The spatial servers include the ArcIMS service engines (Image, Feature, Extract, Query, ArcMap Image, Geocode, and Route) that service the map requests. ArcIMS monitor is another term used for spatial server in the ArcIMS documentation.

- **Data Source (DS).** The data server (GIS data source) is where the GIS data is stored. An ArcSDE data source supports the query processing functions. Standard GIS image or file data sources are also represented at this level.

Figure 4-13 provides an overview of the ArcGIS Server component architecture and the associated software functional locations. The ArcGIS Server architecture includes four configuration groups of software identified as Web applications (WA), service manager (SM), spatial services (SS), and data source (DS).

Figure 4-13
ArcGIS Server Component Architecture



The ArcGIS Server configuration groups include the following:

- **ArcGIS Server Web Applications (WA).** The ArcGIS Server WA components include a commercial Web server supporting communications with the Web clients and a developer environment for .NET or Java Web applications or Web service catalogs.

- **ArcGIS Server Service Manager (SM).** The ArcGIS Server Service Object Manager (SOM) performs a service management role that controls service object deployment and initial application assignment to deployed server object containers. The SOM performs as a parent process controlling service load balancing and managing published service configurations.

- **ArcGIS Server Spatial Services (SS).** The container machines (one or more depending on peak transaction requirements) host the Server Object Containers (SOCs) that are managed by the SOM. Each service configuration is supported by dedicated SOCs. The objects hosted within each SOC are ArcObjects components that are installed on the container machine.

- **Data Source (DS).** The data server (GIS data source) is where the GIS data is stored. An ArcSDE data source supports the query processing functions. Standard GIS image or file data sources are also represented at this level.

Services available on ArcGIS Server can be exposed for use by Intranet LAN or WAN application clients. Application service assignment can be provided with direct access to the SOM without using the Web server interface.

A minimum Web services site can be configured with as few as one platform or as many as six or more platforms, depending on performance capacity and availability requirements. ArcIMS and ArcGIS Server configuration strategies are similar, and criteria for establishing the proper configuration strategy apply to both technologies.

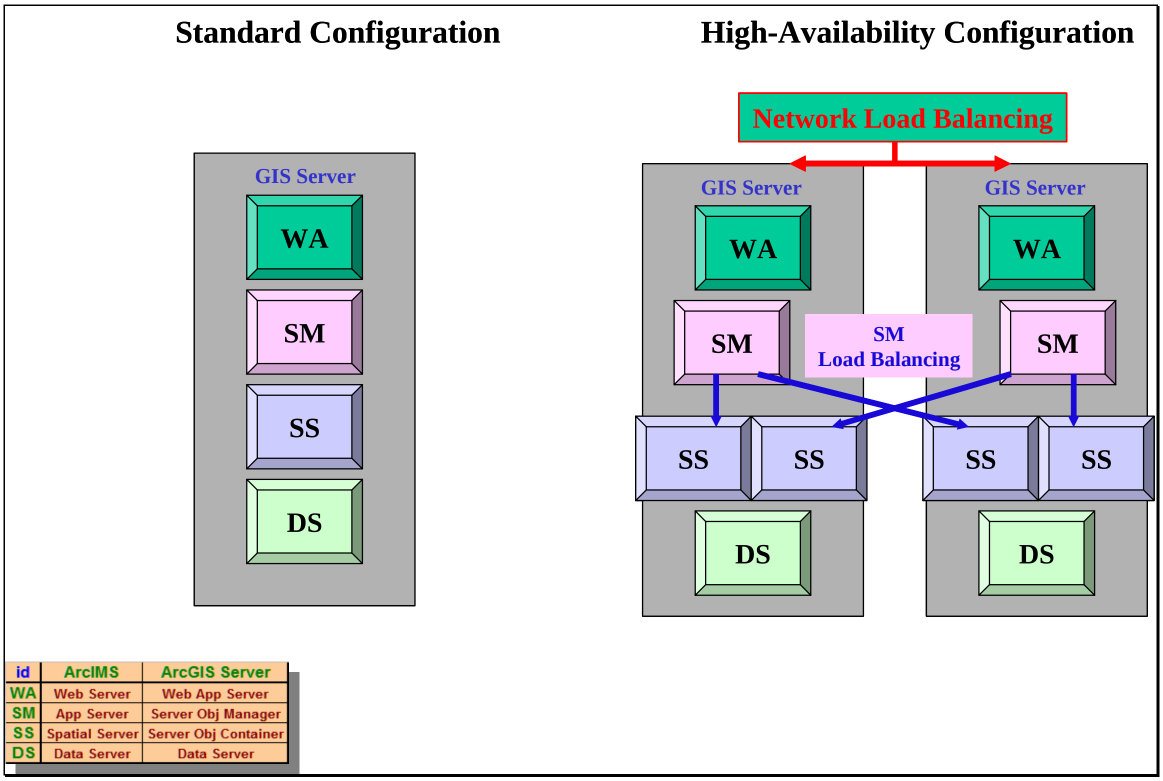
Platform deployment alternatives are presented in the following sections grouped as single-tier, two-tier, and three-tier configurations. Simple configurations are easier to maintain and support. More complex configurations have higher capacity and system availability requirements. High availability Web server configurations are normally deployed when supporting production operations.

ESRI uses a server CPU-based licensing strategy for both ArcIMS and ArcGIS Server. Licensing requirements are based on the number of CPUs on the ArcIMS map servers or the ArcGIS Server container machines, platforms that support the primary GIS services.

4.7.1.1 Single-Tier Platform Configuration

Figure 4-14 provides an overview of some example single-tier platform configurations. Single-tier configurations provide one or two platforms capable of supporting all the Web services components. Most initial customer deployments can be supported by a single-tier architecture.

Figure 4-14
Single-Tier Platform Configuration



- **Standard Configuration.** A complete Web services site can be configured on a single hardware platform. This configuration is appropriate for map service development, sites with a limited number of service requests, and initial prototype deployments.

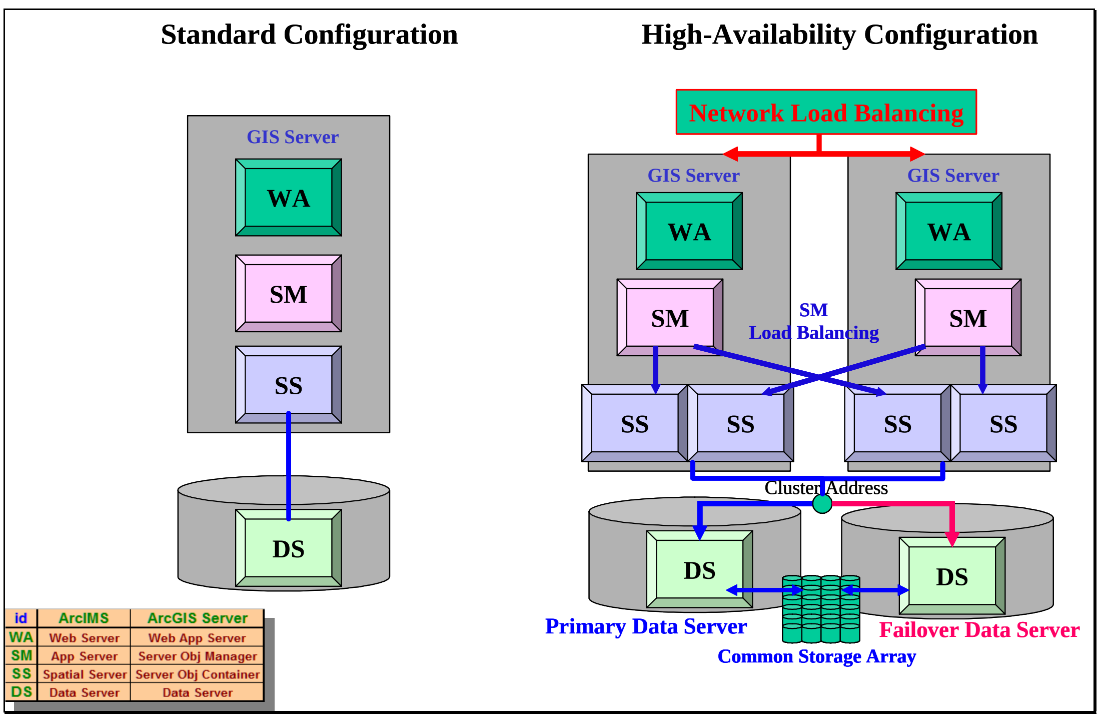
- **High-Availability Configuration.** Most GIS server production operations require redundant server solutions, configured so the site remains operational in the event of a single platform failure. This configuration will continue to support production operations during single platform maintenance and upgrade and while configuring and publishing new services. This configuration includes (1) network load balancing to route the traffic to each of the servers during normal operations and only to the active server if one of the servers fails; (2) service manager (SM) load balancing to distribute spatial services (SS) processing load between the two platforms to avoid having requests back up on one server when extra processing resources are available on the other server (separate SS containers are required on each platform to support this configuration); and (3) data servers that require a complete copy of the data.

4.7.1.2 Two-Tier Platform Configuration

There are several different options for supporting a two-tier platform architecture. The two-tier options support different Web services components on the two layers of physical platform environments.

The two-tier architecture in Figure 4-15 includes the GIS server and data server platforms. The Web server and GIS server components are located on the GIS server platform, and the data server is located on a separate data server platform. This is a popular initial configuration for sites with large volumes of data resources or existing data servers. A single copy of the data can support multiple server components in conjunction with other enterprise GIS data clients.

Figure 4-15
Two-Tier Platform Configuration
(Separate Data Servers)



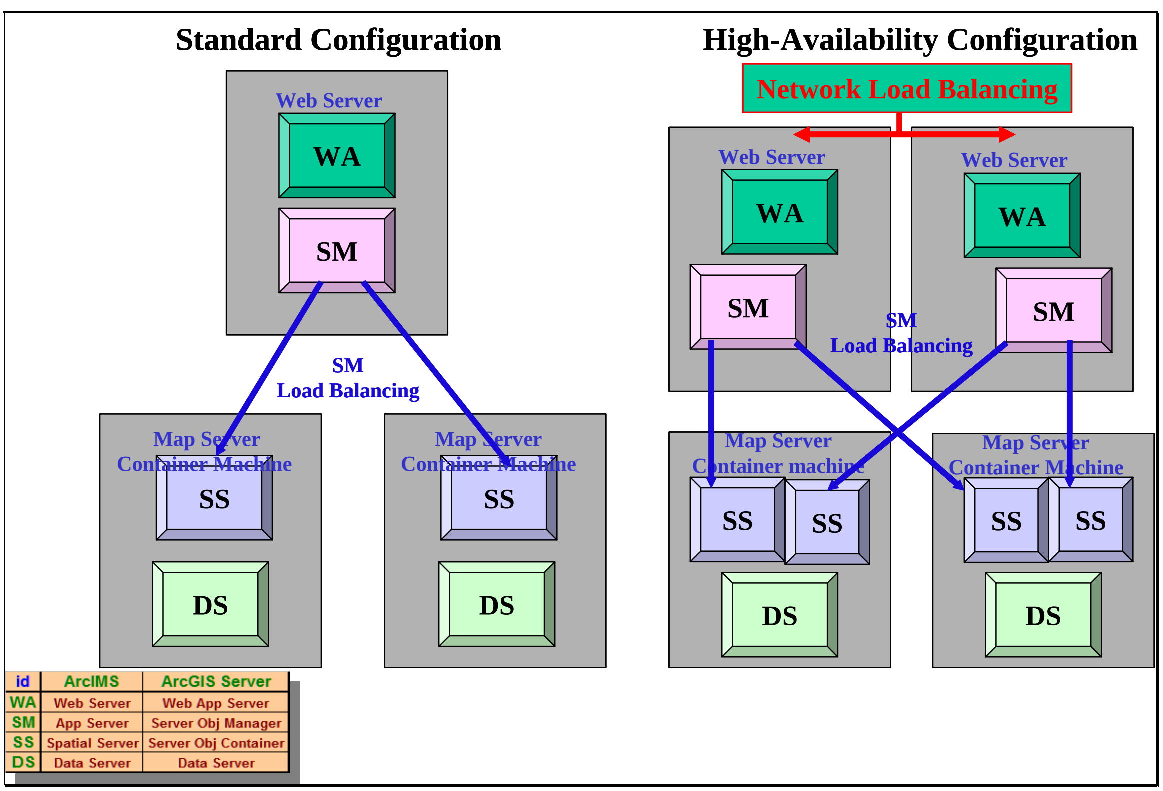
id	ArcIMS	ArcGIS Server
WA	Web Server	Web App Server
SM	App Server	Server Obj Manager
SS	Spatial Server	Server Obj Container
DS	Data Server	Data Server

- **Standard Configuration.** The standard configuration includes one GIS server platform with a separate single data server platform. The Web server is installed on the GIS server platform.

- **High-Availability Configuration.** High-availability operations require redundant server solutions, configured so the site remains operational in the event of any single platform failure. This configuration includes (1) network load balancing to route the traffic to each of the GIS servers during normal operations and only to the active GIS server if one of the servers fails; (2) SM load balancing to distribute SS processing load between the two GIS server platforms to avoid having requests back up on one server when extra processing resources are available on the other server (two SS containers are required on each GIS server platform to support this configuration); and (3) two data servers that are clustered and connected to a common storage array data source. The primary data server supports query services during normal operations, and the secondary data server takes over query services when the primary server fails. Data server clustering is not required if availability requirements are satisfied with a single data server.

The two-tier architecture in Figure 4-16 includes Web server and map server platforms. The Web and application server components are located on the Web server platform, and the spatial and data server components are located on the map server platform. A separate copy of the data must be provided on each map server to support this configuration. This configuration is only practical for small data sources.

Figure 4-16
Two-Tier Platform Configuration
(Separate Map Servers)

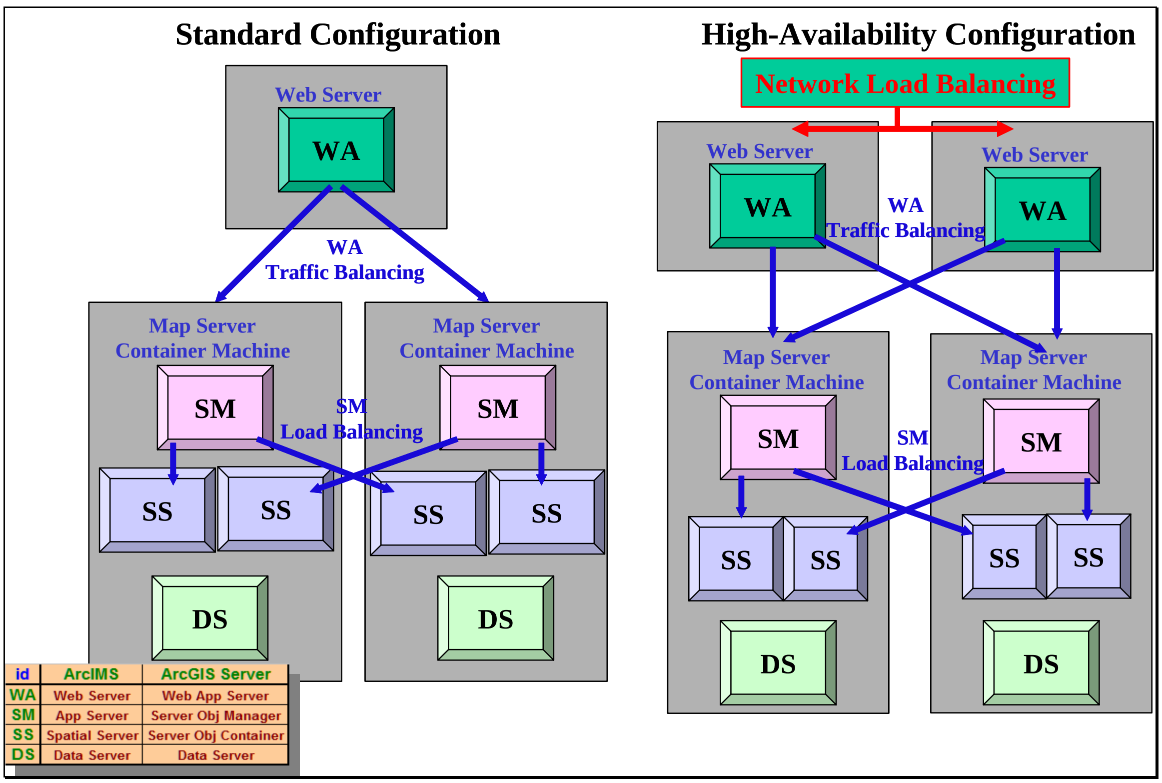


- **Standard Configuration.** The standard configuration includes a single Web server with a separate map server/container machine layer. The map server/container machine layer can be a single platform or can be expanded to support several platforms, depending on the required site capacity. SM load balancing is provided by the GIS server service manager.

- **High-Availability Configuration.** High-availability operations require redundant server solutions, configured so the site remains operational in the event of any single platform failure. This configuration includes (1) network load balancing to route the traffic to each of the Web servers during normal operations and only to the active Web server if one of the servers fails; (2) SM load balancing to distribute SS processing load between the two map server/container machine platforms to avoid having requests back up on one server when extra processing resources are available on the other server (two SS containers are required on each map server/container machine platform to support this configuration); and (3) each map server/container machine that requires a complete copy of the data.

The two-tier architecture in Figure 4-17 includes Web server and map server/container machine platforms. The Web server and GIS server connectors are located on the Web server platform, and the SM, SS, and data server components are located on the map server/container machine platform. A separate copy of the data must be provided on each map server/container machine to support this configuration. This configuration is only practical for small data sources.

Figure 4-17
Two-Tier Platform Configuration
(Separate Web Servers)



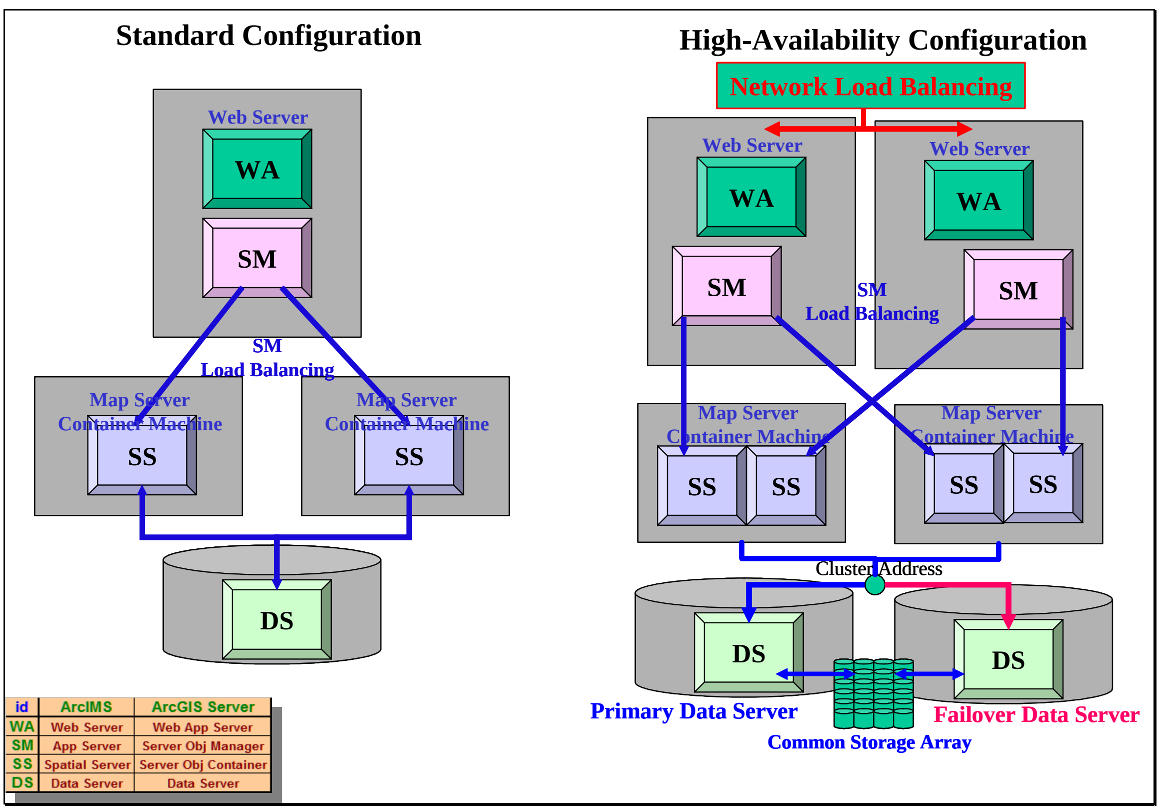
- **Standard Configuration.** The standard configuration includes a single Web server with a separate map server/container machine layer. The map server/container machine layer can be a single platform or can be expanded to support several platforms, depending on the required site capacity. Web application traffic balancing is supported by the GIS server connectors. SM load balancing is provided by the server manager components. Multiple SS containers must be configured on the map servers to support load balancing of multiple platforms. Administration of this architecture becomes increasingly complex as additional map servers/container machines are deployed.

- **High-Availability Configuration.** High-availability operations require redundant server solutions, configured so the site remains operational in the event of any single platform failure. This configuration includes (1) network load balancing to route the traffic to each of the Web servers during normal operations and only to the active Web server if one of the servers fails; (2) SM load balancing to distribute SS processing load between the two map server/container machine platforms to avoid having requests back up on one server when extra processing resources are available on the other server (two SS containers are required on each map server/container machine platform to support this configuration); and (3) each map server/container machine that requires a complete copy of the data. Administration of this architecture becomes increasingly complex as additional map servers/container machines are deployed.

4.7.1.3 Three-Tier Platform Configuration

Figure 4-18 provides an overview of some example three-tier platform configurations. The three-tier configuration includes a Web server, a map server, and a data server tier with the application server located on the Web server.

Figure 4-18
Three-Tier Platform Configuration



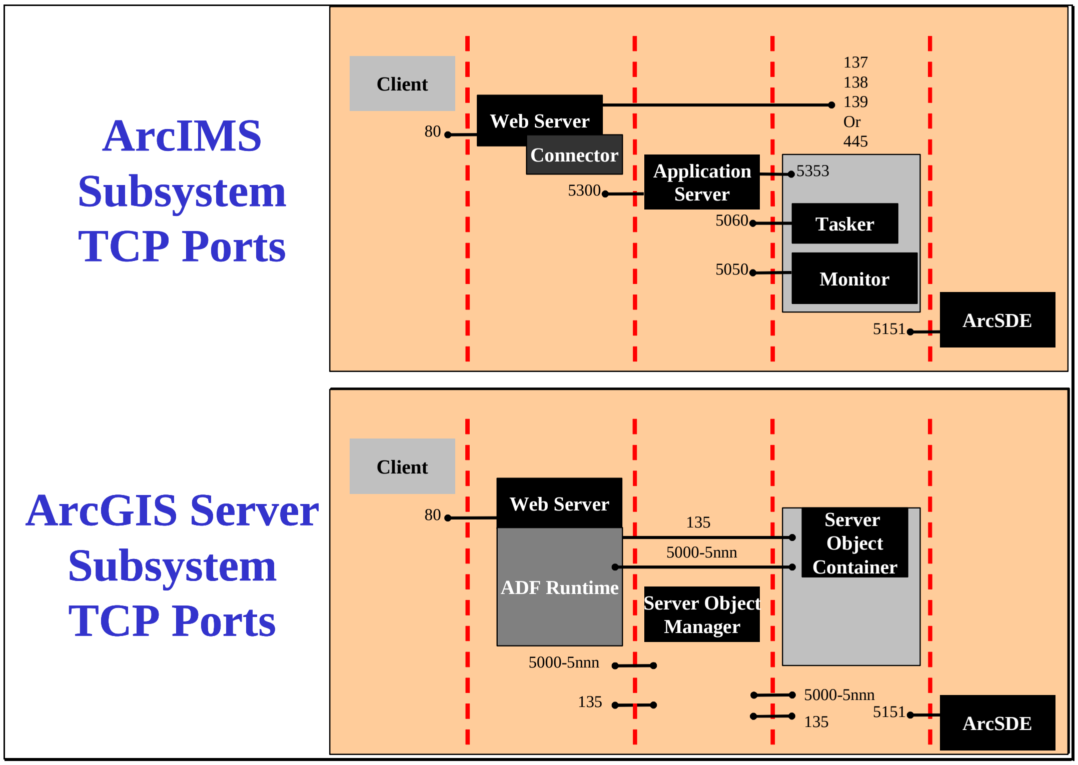
- **Standard Configuration.** The standard three-tier configuration includes a single Web server with a separate map server/container machine and data server tier. The map server/container machine tier can be a single platform or expanded to support several platforms, depending on the required site capacity. SM load balancing is provided by the service manager. Both map servers/container machines use a common data source.

- **High-Availability Configuration.** This configuration includes two Web servers, two map servers/container machines, and two data servers. This solution includes (1) Network load balancing is provided to route the traffic to each of the Web servers during normal operations and only to the active Web server if one of the servers fails; (2) SM load balancing distributes the SS processing load between the two map server/container machine platforms to avoid having requests back up on one server when extra processing resources are available on the other server (two SS containers are required on each map server/container machine platform to support this configuration); and (3) two data servers that are clustered and connected to a common storage array data source. The primary data server supports query services during normal operations, and the secondary data server takes over query services when the primary server fails.

4.7.2 Web Security Configuration Alternatives

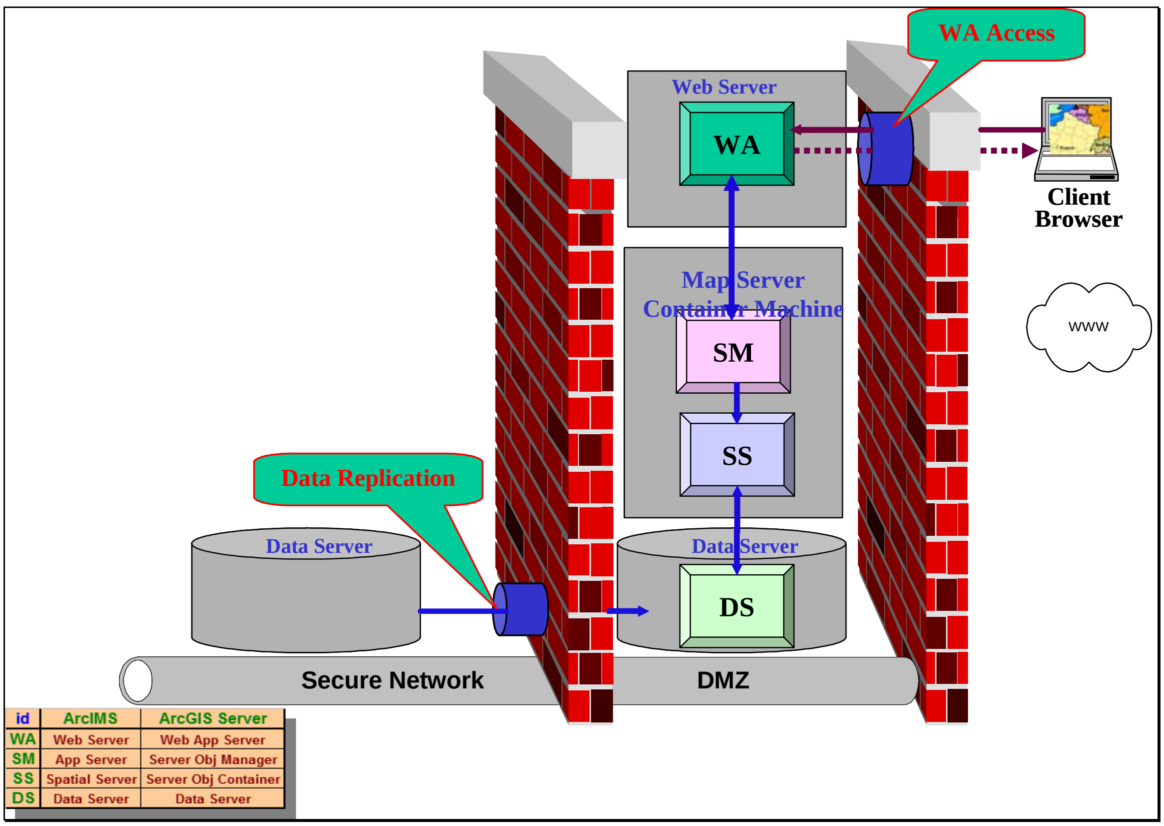
An ESRI white paper, *Security and ArcIMS*, addresses configuration options for secure ArcIMS environments. This paper is available on the ESRI Web site at the following URL: http://www.esri.com/library/whitepapers/pdfs/SecurityArcIMS.pdf. Firewall configurations are provided to support various levels of security. A number of security options are identified here, based on the location of the ArcIMS software components.

Figure 4-19
Firewall Communications



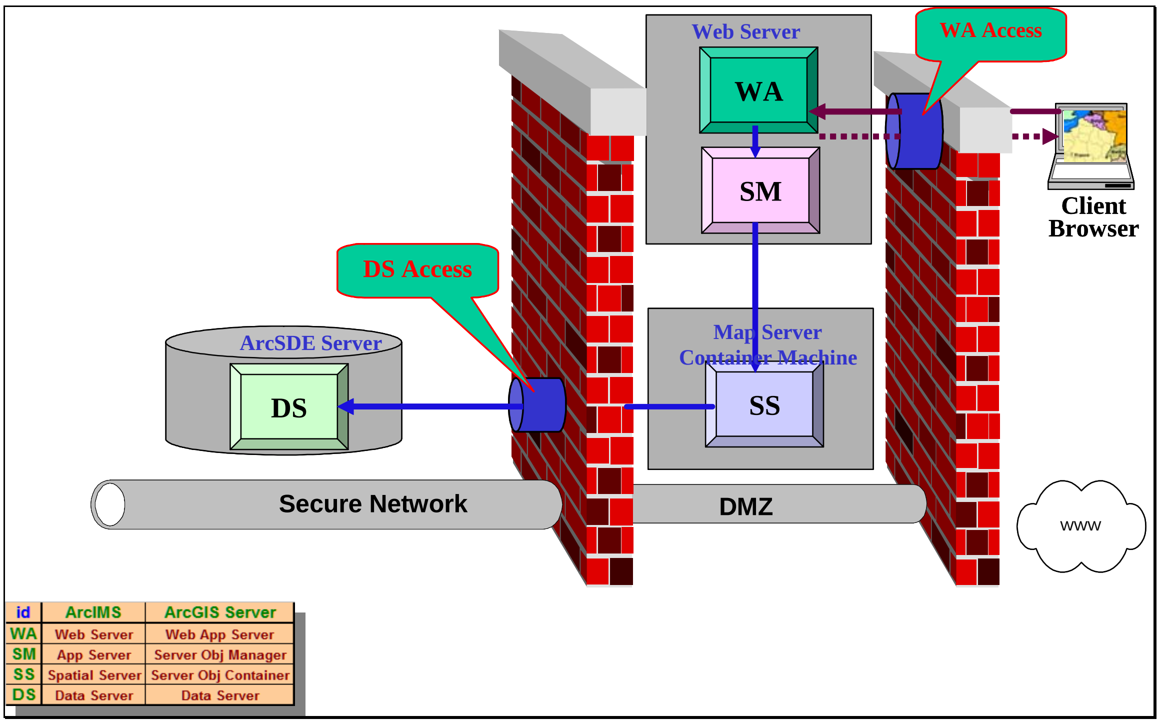
- **All ArcIMS Components in DMZ.** The most secure solution provides physical separation of the secure network from all of the ArcIMS software components. Figure 4-20 shows the Web server, application server, spatial server, and data server are all located outside the secure network firewall within the DMZ. This configuration requires maintenance of duplicate copies of the GIS data. Data must be replicated from the internal GIS data server to the external data server supporting the ArcIMS services.

Figure 4-20
All ArcIMS Components in DMZ



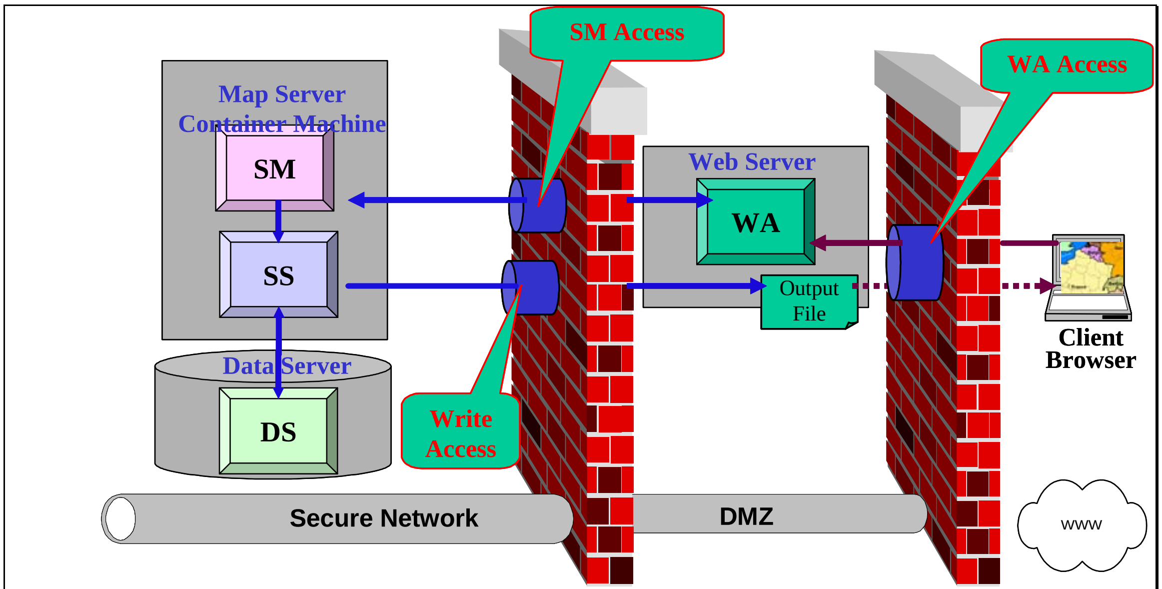
- **All ArcIMS Components in DMZ Except Data Server.** Figure 4-21 shows the Web server, application server, and spatial server located in the DMZ, accessing the internal ArcSDE data server located on the secure network. Port 5151 access through the secure firewall will allow limited access to the ArcSDE DBMS data server. Security is provided through the ArcIMS services and the DBMS security. Firewall prevents traffic from any other source to access the internal secure network.

Figure 4-21
All ArcIMS Components in DMZ Except Data Server



- **Web Server in the DMZ, Remainder of the ArcIMS Components on the Secure Network.** Figure 4-22 shows the Web server located in the DMZ, with the map server and data server located on the secure network. The application server and spatial server must be located on the internal network for this configuration to be acceptable. The output file, located on the Web server, must be shared to the map server. This disk mount will support one-way access from the map server through the firewall to the Web server.

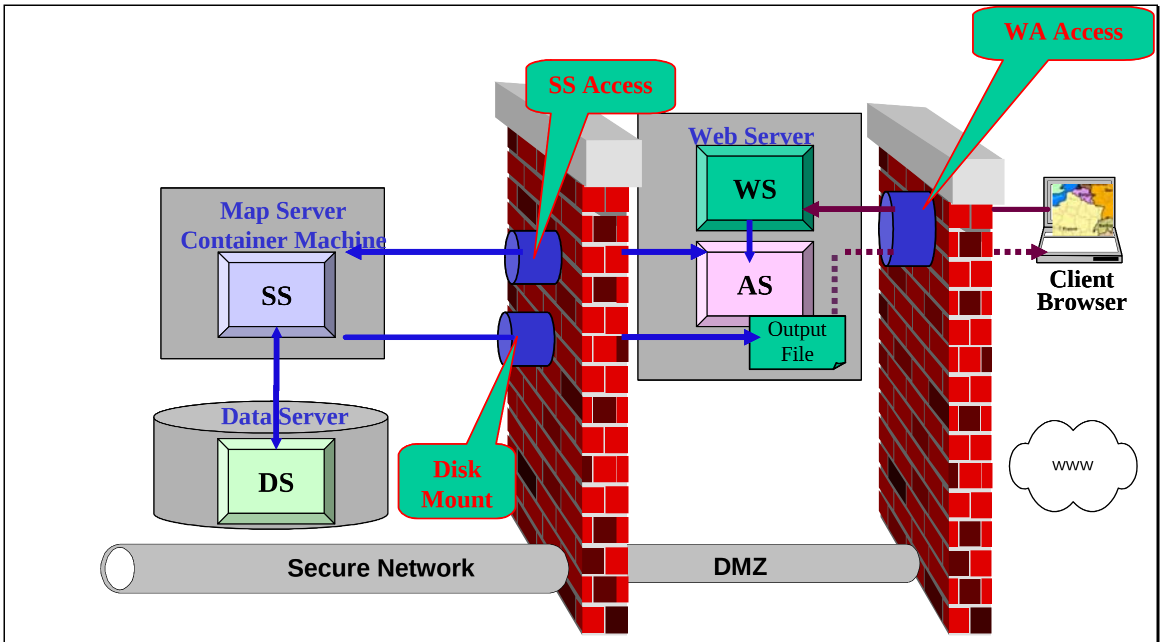
Figure 4-22
Web Server in DMZ, Remainder of Configuration on Secure Network



id	ArcIMS	ArcGIS Server
WA	Web Server	Web App Server
SM	App Server	Server Obj Manager
SS	Spatial Server	Server Obj Container
DS	Data Server	Data Server

- **Web Server and Application Server in the DMZ, Remainder of the ArcIMS Components on the Secure Network.** Figure 4-23 shows the Web server and application server located in the DMZ, with the map server and data server located on the secure network. The output file, located on the Web server, must be shared to the map server. This disk mount will support one-way access from the map server through the firewall to the Web server.

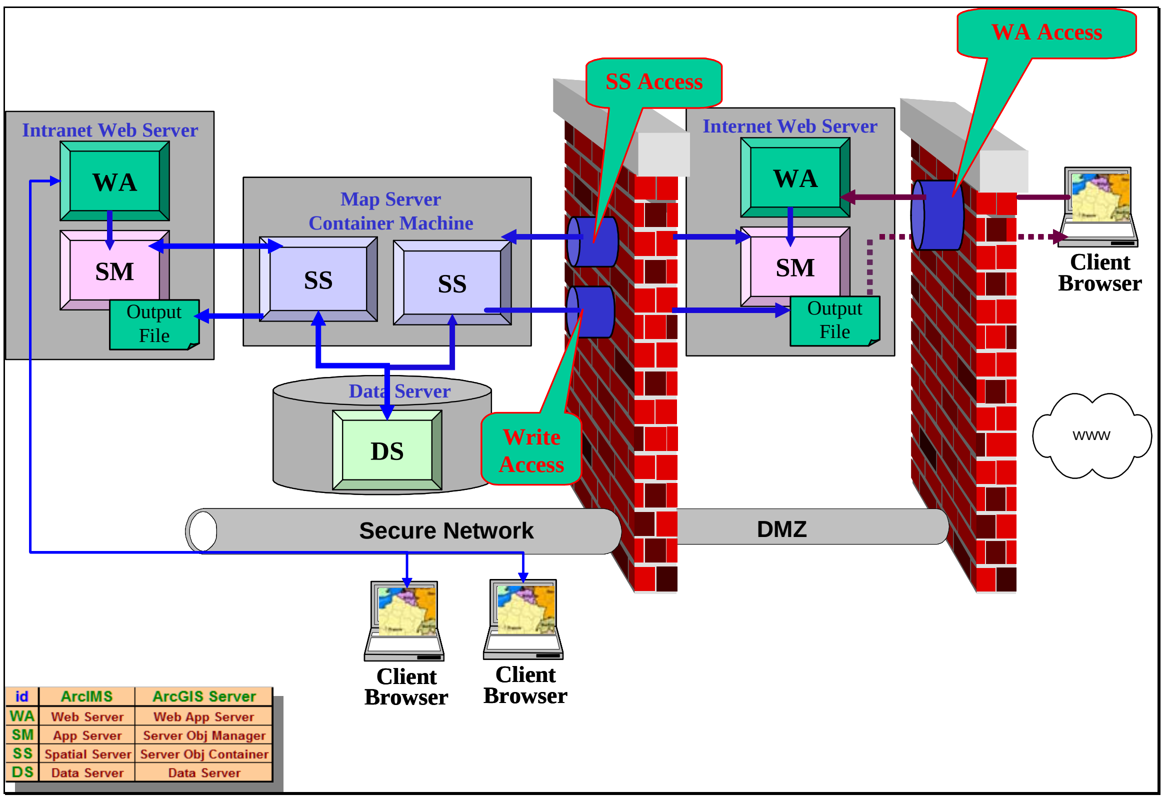
Figure 4-23
Web and Application Server in DMZ, Remainder on Secure Network



id	ArcIMS	ArcGIS Server
WA	Web Server	Web App Server
SM	App Server	Server Obj Manager
SS	Spatial Server	Server Obj Container
DS	Data Server	Data Server

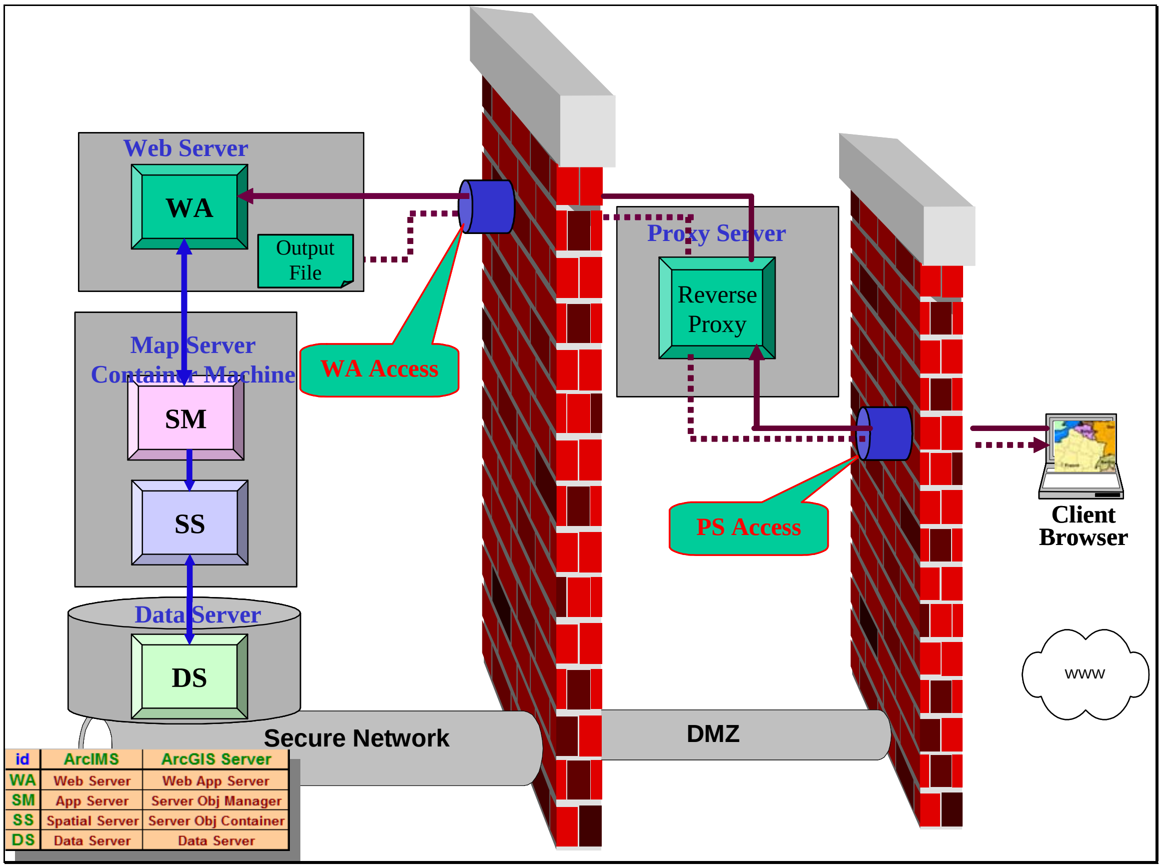
- **Multiple Web Server Configuration.** Figure 4-24 shows a multiple Web server solution, providing separate access security to Intranet and Internet browser clients. This hybrid solution provides shared use of a central map server compute environment while supporting separate user access security requirements. Separate map services can be deployed on the two Web servers, providing secure access to separate user communities from the same ArcIMS site.

Figure 4-24
Multiple Web Server Configuration



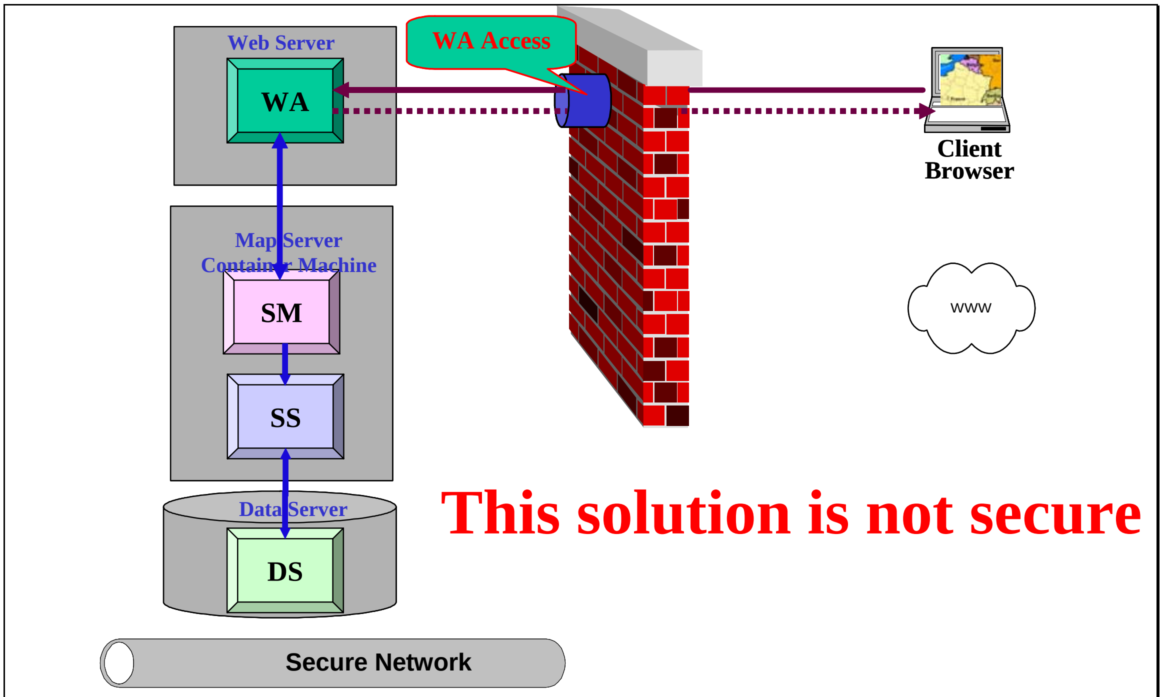
- **Web Services with Proxy Server.** Figure 4-25 shows interface with Intranet Web Server configuration supported by a proxy server. This solution provides private network security through a proxy server and supports the complete Web configuration on the private network. This configuration enables full management of the Web site on the private network.

Figure 4-25
Web Services with Proxy Server



- **All of the ArcIMS Components on the Secure Network.** Figure 4-26 shows the Web server, map server, and data server components all inside the firewall on the secure network. Port 80 must be open to allow HTTP traffic to pass through the firewall. Many organizations are not comfortable with this level of security.

Figure 4-26
All ArcIMS Components on Secure Network



id	ArcIMS	ArcGIS Server
WA	Web Server	Web App Server
SM	App Server	Server Obj Manager
SS	Spatial Server	Server Obj Container
DS	Data Server	Data Server