

## **SECTION 2.0: OCSE NETWORK ARCHITECTURE**

## **2.0 OCSE NETWORK ARCHITECTURE**

The Office of Child Support Enforcement (OCSE) Network was designed in 1992 to support communications between remote child support enforcement (CSE) computer systems in 54 locations, including all 50 states, three territories (Virgin Islands, Puerto Rico, and Guam), and the District of Columbia.

In 1998, faced with aging and non-Y2K compliant components, OCSE management decided to completely redesign the network using current technology. The new OCSE Network was designed to provide availability, reliability, redundancy, scalability, and security. The design of the network replaced the old equipment with routers, uninterruptible power supplies (UPS), and modems, which greatly increased the reliability of the network. The wide area network (WAN) now uses frame-relay technology, and the local area network (LAN) at the sites located in Manassas, VA and Baltimore, MD now uses Fast Ethernet (100Mbps) technology. The Transmission Control Protocol/Internet Protocol (TCP/IP) suite is used on the network.

Since this network transports sensitive data, many security features have been incorporated to limit system access. The primary goal of the security features is to protect the Data Exchange Process (DEP). The DEP consists of any resource that allows data to be exchanged between CSE computer systems. Network security and access to the network are discussed in greater detail in Section 2.5.

### **2.1 Description of the OCSE Network Architecture**

The OCSE frame-relay network topology is a hub-and-spoke design, normally referred to as a star topology. This means that there are many outlying sites (remote locations) connected to a central site. The central site is referred to as the hub and the remote locations as spokes, similar to the wheel on a covered wagon. In the case of the OCSE Network there are two hubs, which make the design a dual-star topology. This topology allows connectivity between the two hubs and each remote location, as well as a direct communication path with each other. The hub sites provide a central location for both communications and data processing.

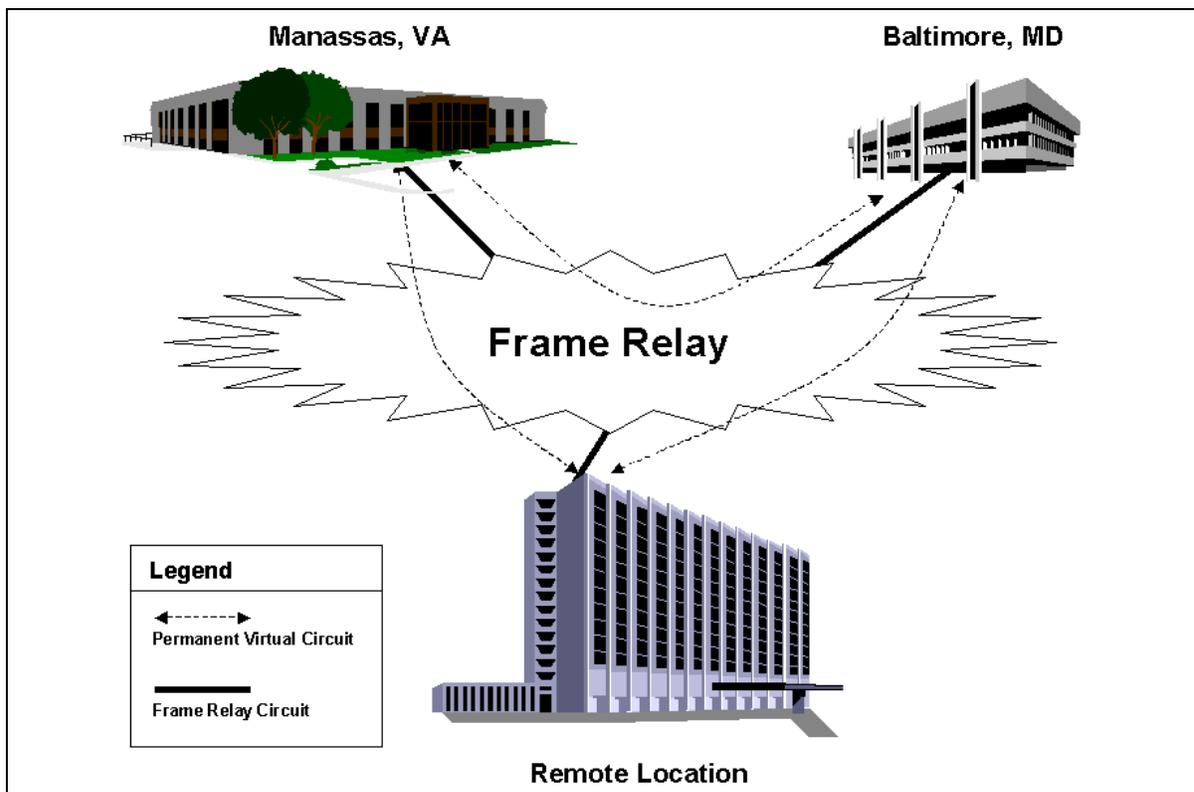
Manassas is the primary hub site and Baltimore is the alternate, or disaster recovery site. The Manassas site, which contains the primary server, runs all of the applications on the OCSE Network. In the event Manassas cannot provide normal data processing services, the Baltimore site automatically performs those actions.

### 2.1.1 PRIMARY METHOD OF COMMUNICATIONS

The primary method of communications between sites is frame-relay services procured under the General Services Administration (GSA) Federal Technology Service contract (FTS2001) for telecommunication services. There are essentially 54 dissimilar networks connected to the OCSE Network with routers. These routers must have the mechanisms to get data efficiently through the network. Routing protocols provide this service, dynamically selecting the best path for data traversing a network. The Open Shortest Path First (OSPF) routing protocol is used on the OCSE Network. This protocol is ideal for stable networks, such as the OCSE Network.

As illustrated in Figure 2-1, each remote location has two communications paths, one to the Manassas hub and the other to the Baltimore hub. The exceptions are Guam and the Virgin Islands, which use analog circuits for their primary communications. The hub sites are connected to all remote locations by frame-relay permanent virtual circuits (PVCs), which are contained within the frame-relay circuit. They are also connected to each other by a frame-relay PVC. The use of redundant data links employed by the OCSE architecture improves the overall network reliability by eliminating a single-link point of failure for communications between the states and the hub sites.

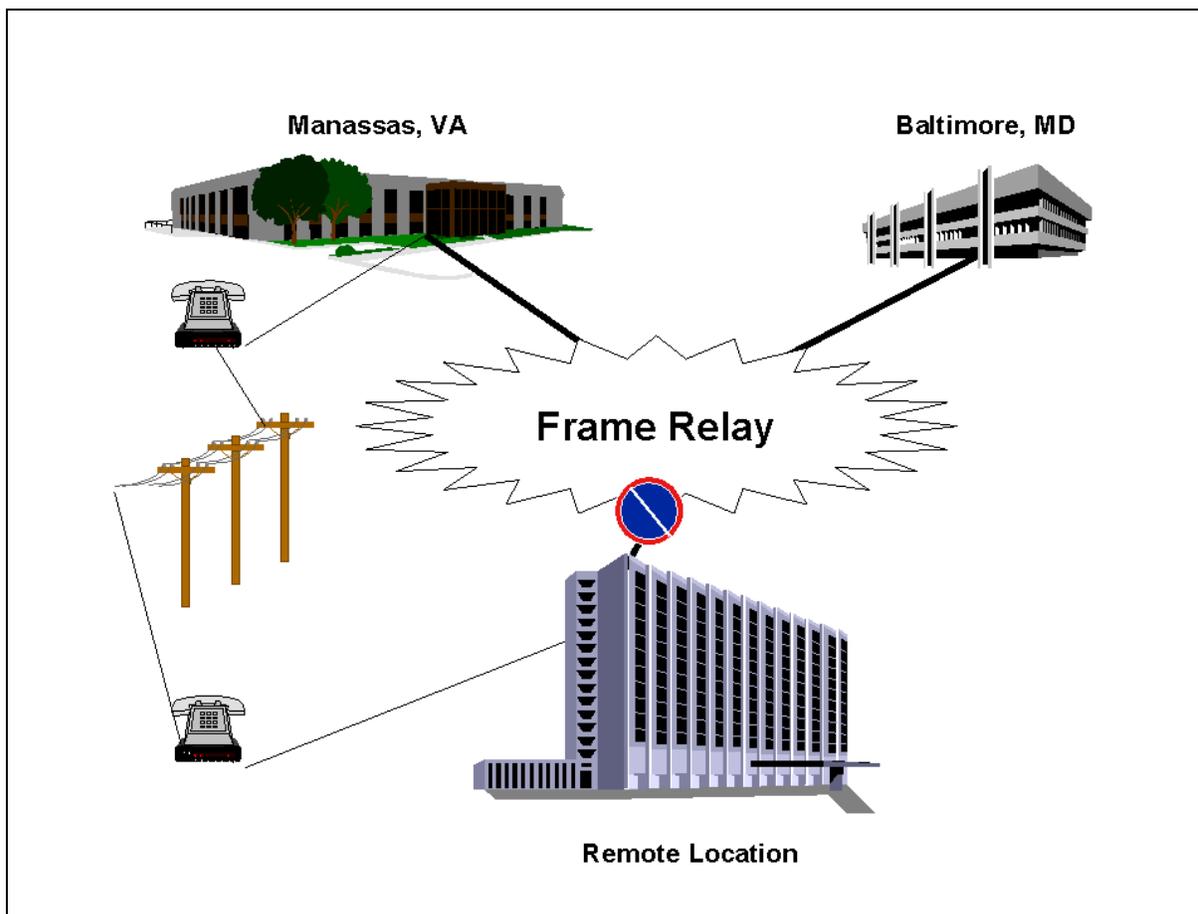
**Figure 2-1: OCSE's Primary Method of Communications**



## 2.1.2 ALTERNATE METHOD OF COMMUNICATIONS

The OCSE Network has an alternate method of communications between the remote and hub sites using analog communications. Analog communications are activated when both the primary (Manassas) and secondary (Baltimore) frame-relay PVC links fail and there is traffic destined for remote locations. The Cisco AS5300 Access Server automatically initiates a dial-on-demand routing (DDR) session to the affected router through analog telephone lines and modems. This method of communications is activated only for the duration of the data transfer, then disconnected until communications need to be reestablished. Analog communications are the primary communications method for Virgin Islands and Guam. Figure 2-2 illustrates the use of analog communications in the event that frame relay is not available.

**Figure 2-2: OCSE's Alternate Method of Communications**



### **2.1.3 REMOTE LOCATION NETWORK ARCHITECTURE**

OCSE recognizes that network topologies differ from site to site; therefore the network is designed to support various topologies. OCSE provides remote locations with the following equipment:

- a modem for connectivity to the Public Switched Telephone Network (PSTN);
- a UPS to prevent equipment from going down during short-term power outages;
- a router for communications over the WAN and communications to their local network; and
- a Data Service Unit (DSU) for connectivity to the frame-relay network, furnished by the FTS2001 network provider.

There are five options available for connecting to the OCSE Network:

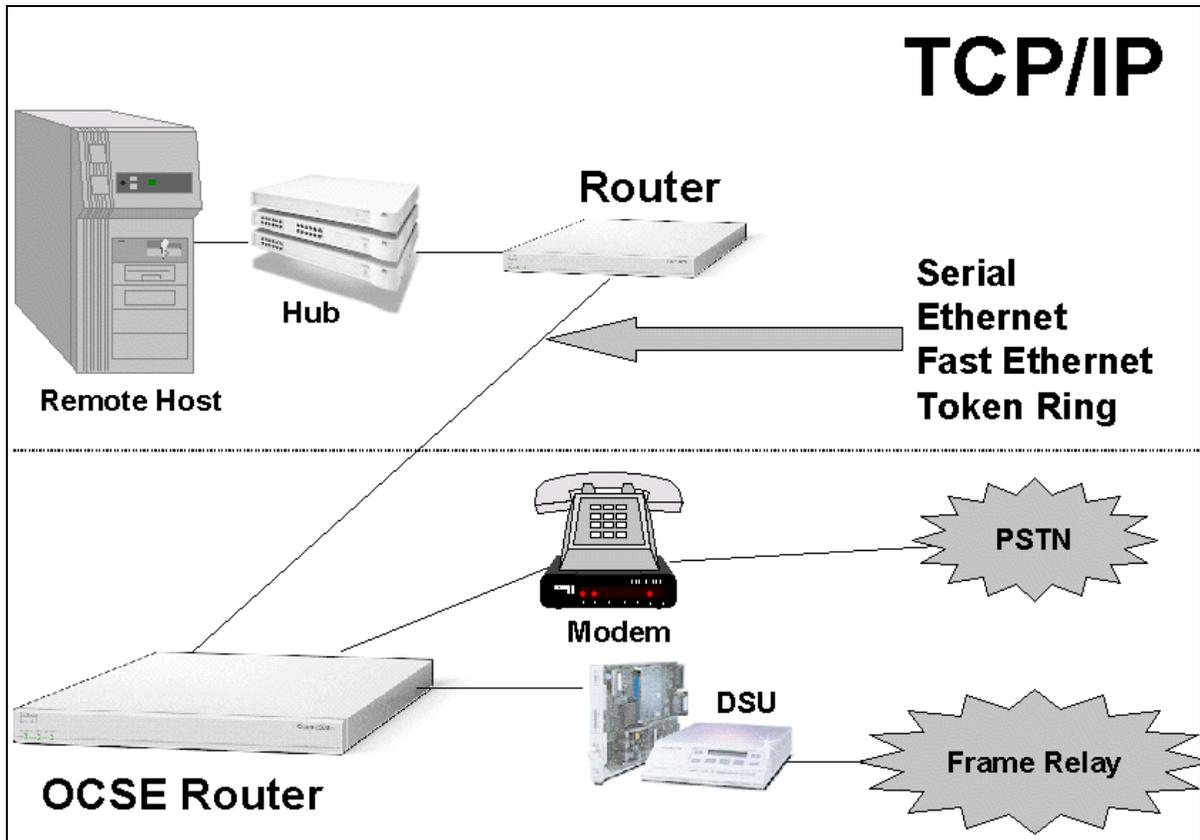
- Router-to-Router;
- Router-to-Firewall;
- Router-to-FTP Server;
- Router-to-Hub (or switch); and
- Router-to-Host.

Each is illustrated in detail in the examples that follow.

### 2.1.3.1 Router-to-Router (Option #1)

Figure 2-3 reflects the Router-to-Router option available to remote locations for connecting to the OCSE Network. Connections to the OCSE router using this option can be made using a serial, Ethernet, Fast Ethernet, or Token Ring interface.

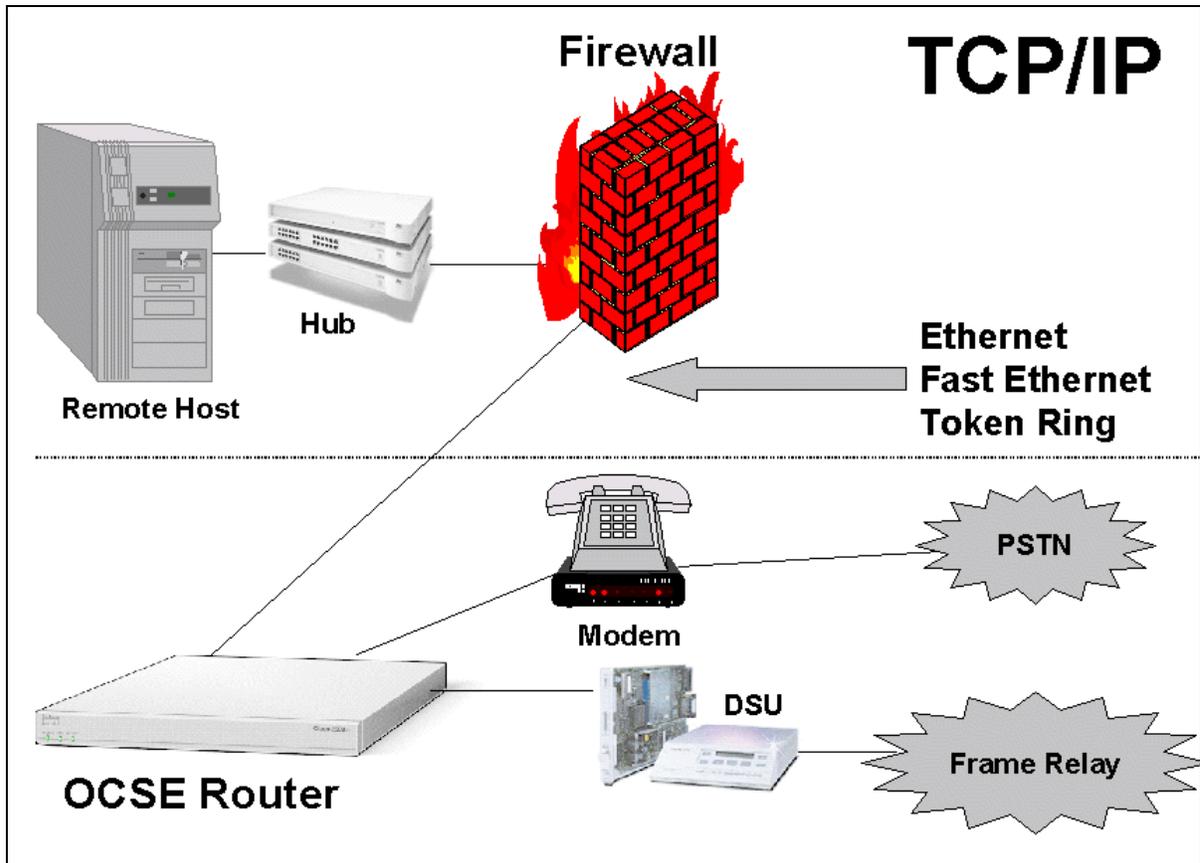
**Figure 2-3: Router-to-Router Connectivity (Option #1)**



### 2.1.3.2 Router-to-Firewall (Option #2)

Figure 2-4 reflects the Router-to-Firewall option available to remote locations for connecting to the OCSE Network. Connections to the OCSE router using this option can be made using an Ethernet, Fast Ethernet, or Token Ring interface.

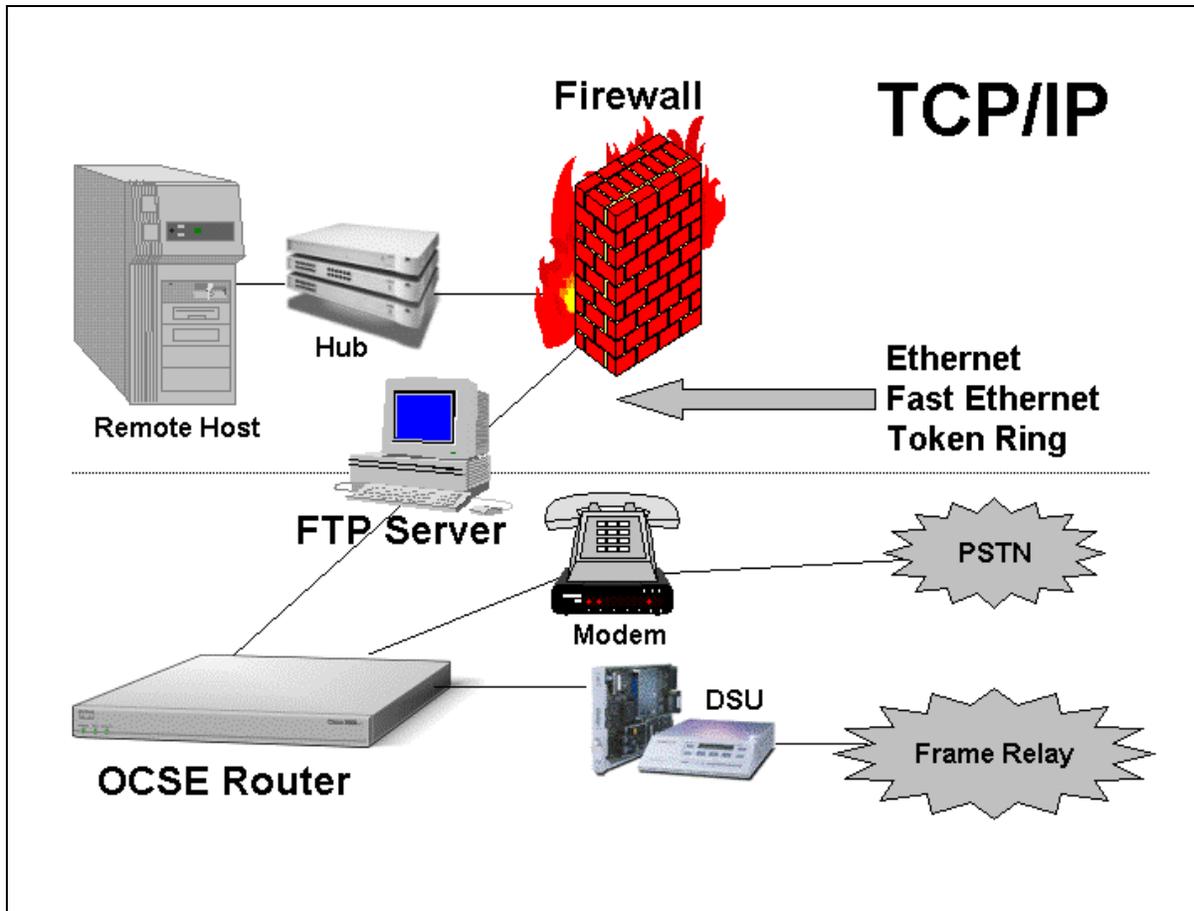
**Figure 2-4: Router-to-Firewall Connectivity (Option #2)**



### 2.1.3.3 Router-to-FTP Server (Option #3)

Figure 2-5 reflects the Router-to-FTP Server option available to remote locations for connecting to the OCSE Network. Connections to the OCSE router using this option can be made using an Ethernet, Fast Ethernet, or Token Ring interface.

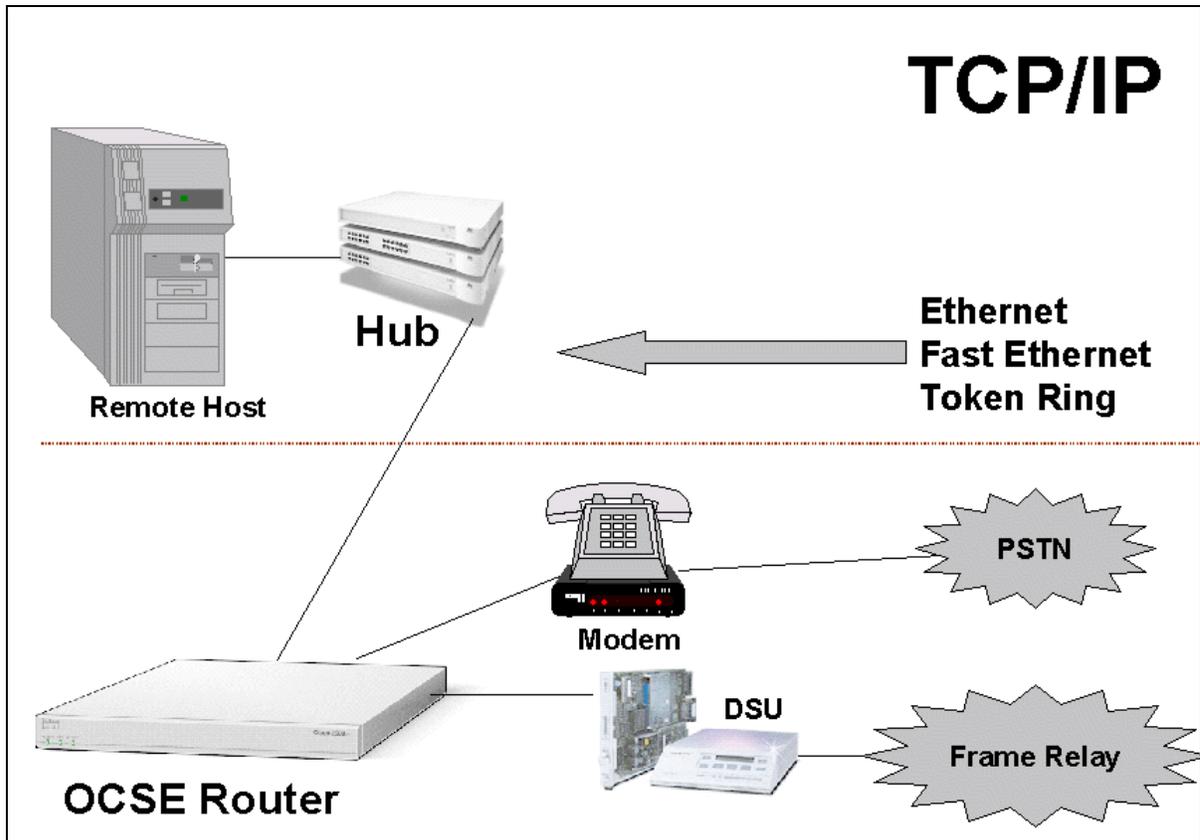
**Figure 2-5: Router-to-FTP Server Connectivity (Option #3)**



### 2.1.3.4 Router-to-Hub (Option #4)

Figure 2-6 reflects the Router-to-Hub option available to remote locations for connecting to the OCSE Network. Connections to the OCSE router using this option can be made using an Ethernet, Fast Ethernet, or Token Ring interface.

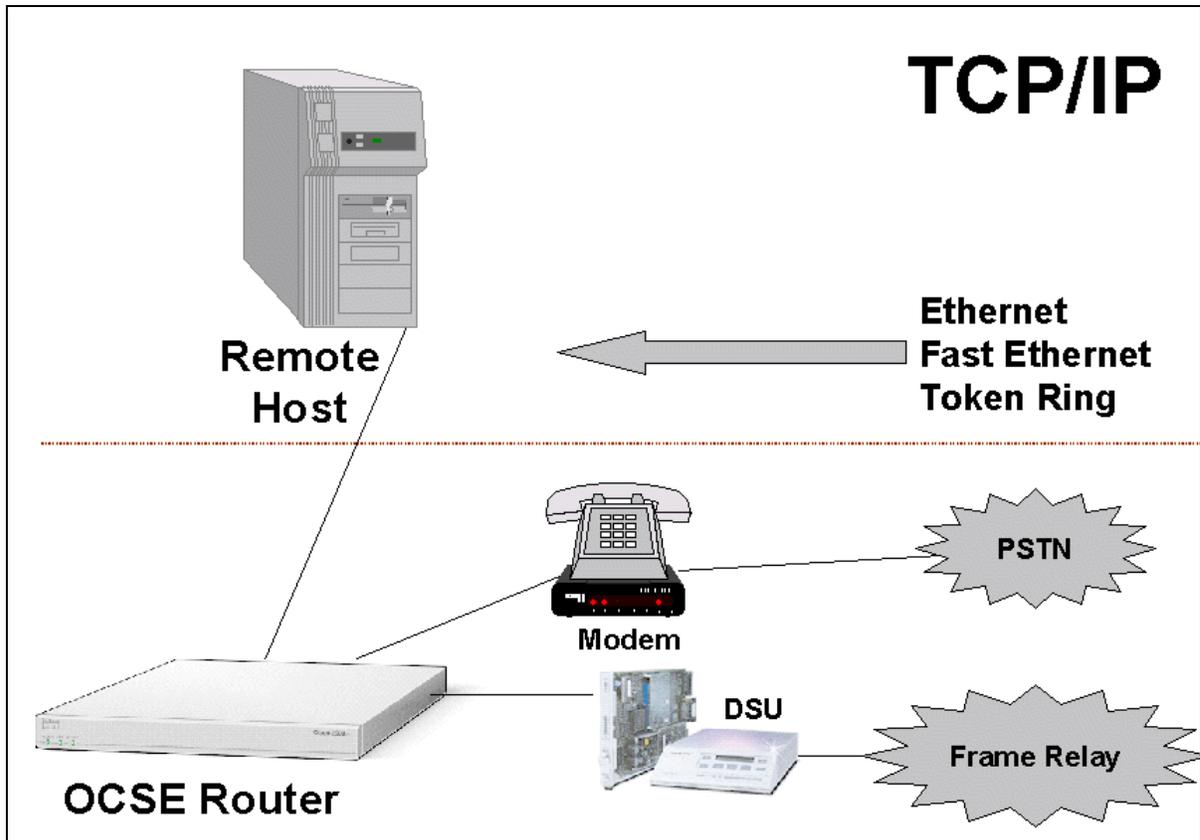
**Figure 2-6: Router-to-Hub Connectivity (Option #4)**



### 2.1.3.5 Router-to-Host (Option #5)

Figure 2-7 reflects the Router-to-Host option available to remote locations for connecting to the OCSE Network. Connections to the OCSE router using this option can be made using an Ethernet, Fast Ethernet, or Token Ring interface.

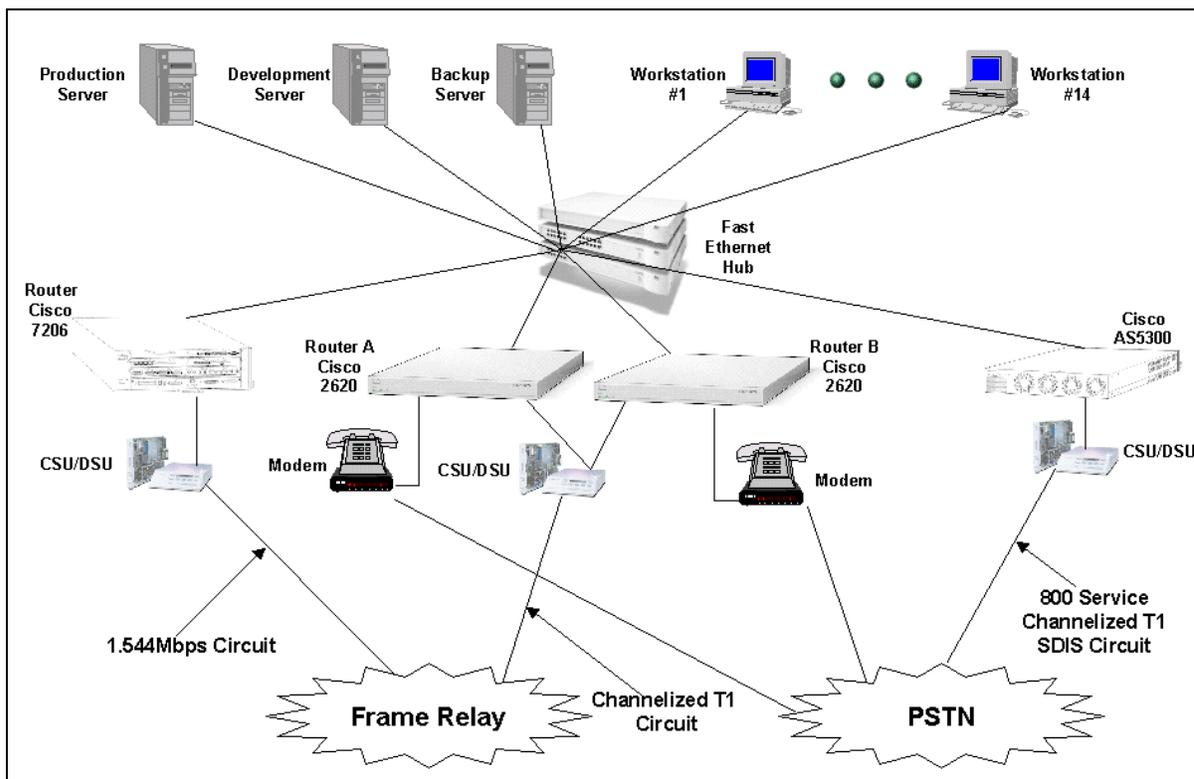
**Figure 2-7: Router-to-Host Connectivity (Option #5)**



## 2.1.4 MANASSAS NETWORK ARCHITECTURE

Figure 2-8 reflects the architecture of the primary processing site located in Manassas.

**Figure 2-8: Manassas Network Architecture**



Of the three servers, the Production server is the primary server for the CSENet 2000 Application Suite. The Development server is used for developing software and performing tests with the state CSE systems. The Backup server is used to run the CSENet software in the event the primary server malfunctions. This server allows for redundancy of server hardware, software, and operating system in Manassas. The Backup server is maintained as a mirror image of the Production server and assumes the Production server's role in the event of a system malfunction.

In addition to redundant hardware, all data on the Production server is archived on removable media (tape) once daily. The backup software has the ability to restore single files, multiple files, directories, drives, and volumes. Archived data can be restored to any server in the event of a serious malfunction. The current data retention period is 90 days.

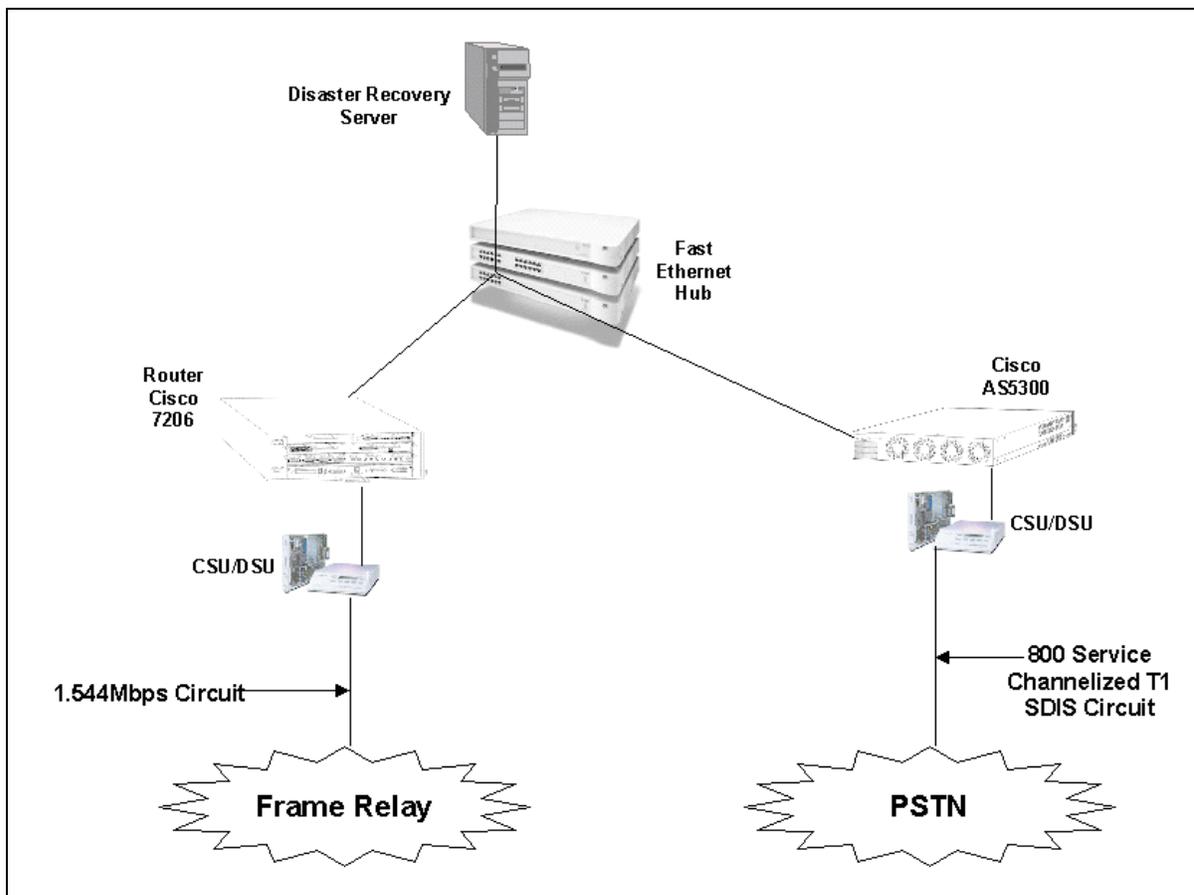
The CSENet workstations in Manassas are used for software development, database administration, system administration, network administration, tape-backup administration, and testing.

A Cisco 7206 router is the primary communications gateway for the servers. The Cisco 2620 Router A is used as the primary communications gateway for the majority of workstations. Router B is used to simulate communications to remote CSE systems and to test router configurations before they are implemented on remote routers. A Channel Service Unit/Data Service Unit (CSU/DSU) is used for digital transmission of data over wide area networks. The Cisco AS5300 is the analog communications gateway and is used as an alternate method of communications.

### 2.1.5 BALTIMORE NETWORK ARCHITECTURE

Baltimore, MD is the disaster recovery site for applications that reside on the network. If something catastrophic happens to the Manassas site, the Baltimore hub takes over as the primary processing site, ensuring the continuous operations of the Data Exchange Process. The disaster recovery site has the same equipment configuration as the primary processing site, except for the Cisco 2620 routers and the workstations. The network architecture for the Baltimore hub is shown in Figure 2-9.

**Figure 2-9: Baltimore Network Architecture**

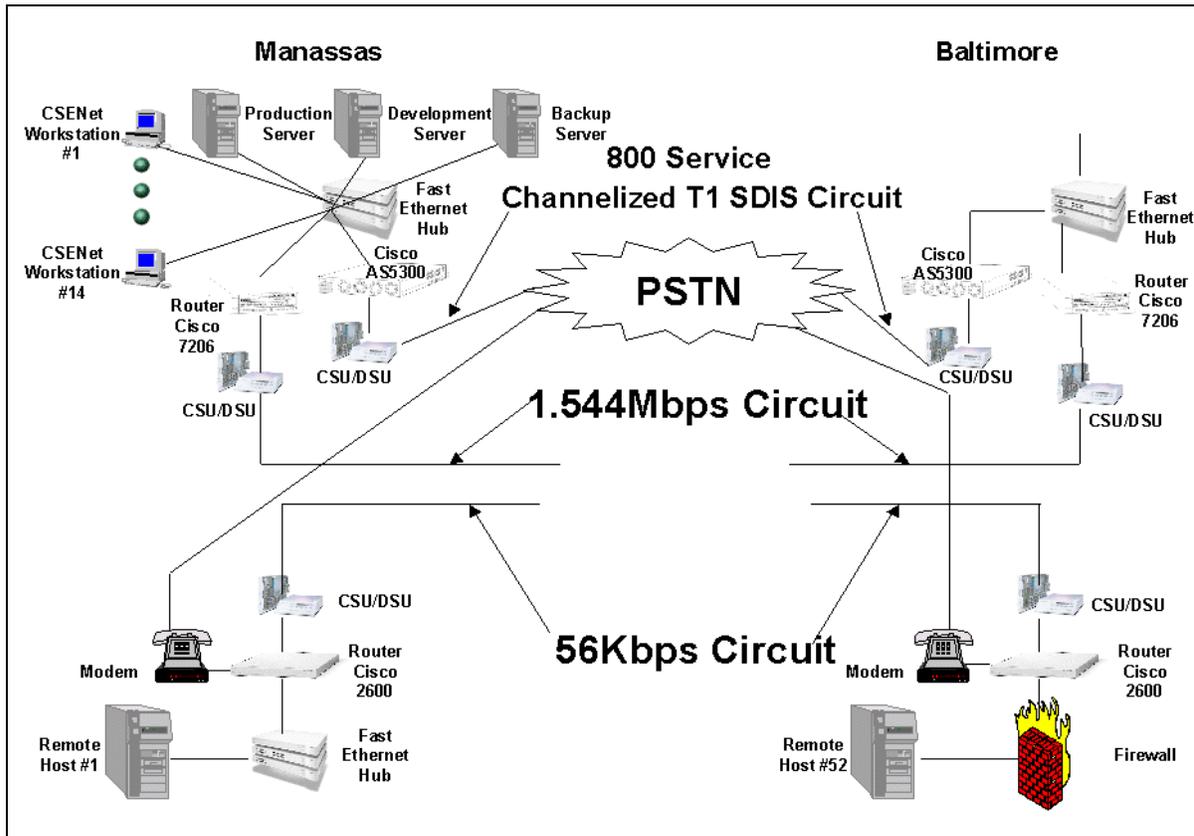


Continuous operation of applications from Baltimore is automated and therefore transparent to remote locations. Further, states are not required to make any system configuration changes to support processing from the Baltimore site.

### 2.1.6 OCSE NETWORK TOPOLOGY

Figure 2-10 reflects the topology of the entire OCSE Network. This figure takes all the components discussed previously and displays them in one diagram.

**Figure 2-10: OCSE Network Architecture**



## 2.2 Network Reliability

Reliability is an important factor when designing any network. One key design feature of the OCSE Network that helps to ensure reliability is redundancy. There are many built-in mechanisms to automatically allow data to be transmitted, even when there is a problem on the network.

These redundant mechanisms include:

- multiple frame-relay paths to states;
- backup connectivity through analog communications;
- dual processing sites; and
- backup processing at the Manassas site.

Effective use of the TCP/IP protocol suite on the OCSE Network also facilitates network reliability. Further, a proactive network monitoring program also adds to the reliability of the system.

### 2.2.1 OPEN-STANDARD PROTOCOLS

A protocol is a set of rules governing the exchange of data between computing devices. The computer and telecommunications industries have established hundreds of standard communications protocols, referred to as open-standard protocols. The use of open-standard protocols, as opposed to proprietary protocols, ensures that data can be exchanged seamlessly without regard to manufacturer.

The OCSE Network uses industry-based open-standard protocols exclusively. For example, TCP/IP, an open-standard protocol, is used to support the communications of all the current applications running on the network. TCP/IP is widely available for most computer operating systems today and is the de facto standard for most data communications networks, including the Internet. TCP provides reliability for the TCP/IP suite of protocols.

The CSENet suite uses one application protocol for file transfer, File Transfer Protocol (FTP), a protocol that uses TCP/IP for communication with IBM mainframe computers. FTP is used in the OCSE environment to transfer or copy files between the OCSE servers and the remote hosts. It is one of the protocols in the TCP/IP protocol suite and operates on the Process/Application layer, as shown in Chart 2-1. The protocols in **bold text** are used in the file transfer process, using the FTP application. The OCSE Network has the ability to transfer data using other methods; however, remote locations are encouraged to use FTP.

<b>CHART 2-1: THE DoD REFERENCE MODEL</b>				
<b>Layer</b>	<b>Protocol</b>			
Process/Application	FTP	Telnet	TFTP	SNMP
	<b>TN3270E</b>	SMTP	NFS	X windows
Host-to-Host	<b>TCP</b>		UDP	
Internet	ICMP	BootP	ARP	RARP
	<b>IP</b>			
Network Access	Ethernet	Fast Ethernet	Token Ring	Frame Relay

## **2.2.2 NETWORK MONITORING**

It is necessary to implement network and systems management to effectively administer and maintain a network. Software tools were developed to monitor the health of the network so that as potential problems develop, they can be addressed promptly. This monitoring consists of periodically executing a program that has the ability to check connectivity between:

- the hub networks and remote networks;
- the hub servers and remote CSE servers; and
- servers and workstations on the local area networks located in Manassas and Baltimore.

A number of Production and Disaster Recovery server resources are also monitored, such as memory, CPU, and disk utilization, to preclude any problems stemming from insufficient computing resources. The output of the program generates a report that is analyzed twice daily. Any network abnormalities identified in the reports are immediately investigated and appropriate corrective action is taken.

## **2.3 Network Capability**

The OCSE Network has the ability to accommodate data, voice, and video services to states, territories, and the District of Columbia. The service being used under the current configuration is data. In the event that our mission requirements change to necessitate inclusion of voice or video, either service can be easily implemented.

### **2.3.1 CURRENT UTILIZATION OF THE NETWORK**

It is essential to assess network utilization in order to optimize network performance. There are a number of network-management tools that obtain and record current network utilization. The Multi Router Traffic Grapher (MRTG) is one of the network management tools used in the OCSE Network. This tool monitors traffic on the WAN and provides statistics on a near real-time basis. This information is used to set up a baseline for normal operating conditions. In addition, it can be used to troubleshoot network problems by comparing the baseline to current network conditions. Finally, the tool can be used for determining additional bandwidth requirements on active frame-relay links.

### **2.3.2 DATA COMPRESSION TECHNOLOGY**

Because of its nature, bandwidth over the WAN is typically considerably less than the bandwidth of a typical LAN. Data compression is one mechanism used to optimize the data throughput over data links. This technology can be applied in a WAN environment to increase data throughput by reducing the payload, thereby allowing more data to be transmitted over a link. Additionally, data compression allows improved application performance and service availability for end users without having to upgrade the circuit. Tests have shown that the data transmission rates over a data link using compression can increase throughput by over 350%.

### **2.3.3 HARDWARE DESIGN**

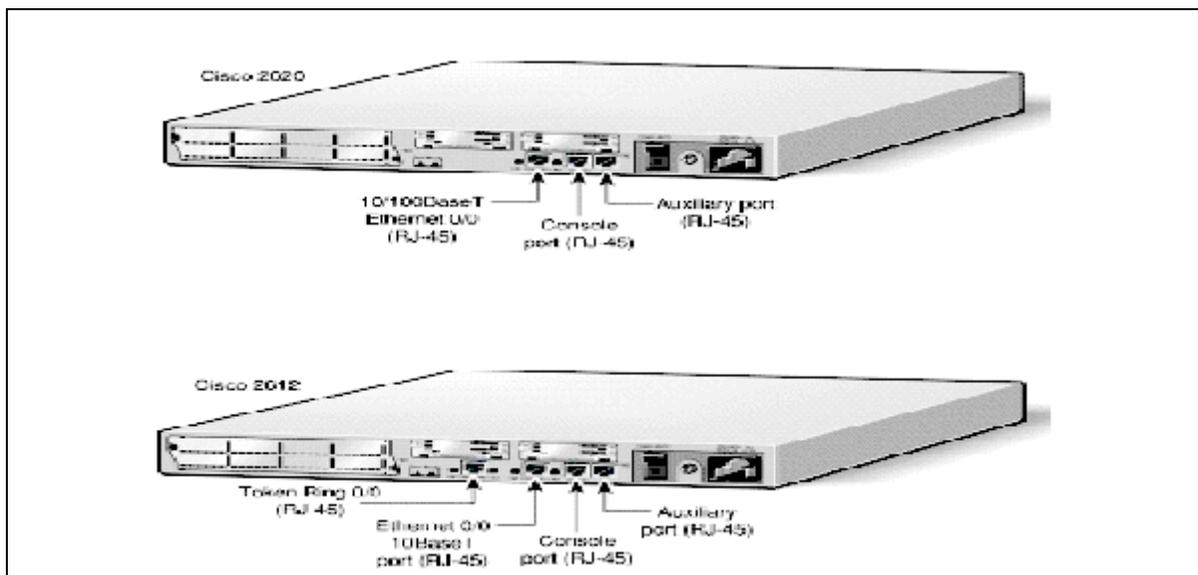
In designing the OCSE Network infrastructure, hardware components were scrutinized in order to produce an adaptable and scalable network. The modular design of hardware incorporated in the network architecture, such as the Cisco routers and Compaq servers, provides a flexible platform to customize components according to specific requirements. Modular-designed devices are superior to fixed-configuration devices because they simplify and expedite repair, upgrade easily, and normally allow for interchanging components without disrupting service (e.g., hot-swapping). The network components discussed in this section are the Cisco routers and the OCSE servers. There are three types of Cisco routers used in OCSE Network environment:

- Cisco 2600 series router;
- Cisco 7206 router; and
- Cisco AS5300 Access Server.

### 2.3.3.1 Cisco 2600 Series Router

The Cisco 2600 series router was selected for use in remote locations. The Cisco 2620 model is installed in all remote locations that have an Ethernet, Fast Ethernet, or serial network environment; the 2612 model is installed in the Token Ring network environment. All of the 2600 series routers have at least one 2-port WAN interface card installed for connection to the network. (Remote locations using a serial interface to connect to their LAN have two 2-port WAN interface cards installed.) Figure 2-11 shows the rear view of the Cisco 2620 and 2612 routers.

**Figure 2-11: Cisco 2620 – 2612 Router**



The Cisco 2600 series router provides the following features:

- two 2-port adapter slots;
- access control list security;
- analog and digital access services;
- multi-service voice/data integration;
- virtual private network (VPN) access; and
- routing with bandwidth management.

### **2.3.3.2 Cisco 7206 Router**

Since the hub sites are the central points for all network traffic, identical Cisco 7206 routers are installed at each to handle the heavy traffic generated on the network. An additional router is installed for backup at the Manassas site.

The routers contain dual, hot-swappable, load-sharing power supplies for redundancy. The Cisco Internetwork Operating System (IOS) version 12.0 (7) T is currently running on these routers. The input/output (I/O) controller card used is equipped with the optional Fast Ethernet port for connection to the OCSE LAN. Each of the three Cisco 7206 routers has a 4-port serial adapter card installed for connection to the OCSE Network.

There are currently five unused port adapter slots available for upgrading on the 7206 routers. These slots can be used for different interface modules such as asynchronous transfer mode (ATM), digital voice or video, Integrated Services Digital Network (ISDN), or Gigabit Ethernet.

### **2.3.3.3 Cisco AS5300 Access Server**

There are Cisco AS5300 Access Servers installed at each of the hub sites as shown in Figure 2-10. The AS5300 Access Server provides dial-up modem and routing functions in a single modular chassis. Currently the access server in Manassas is configured to automatically initiate dial-backup connection to a Cisco 2600 router in a remote location in the event the frame-relay links go down. The AS5300 Access Server is also the primary communications means for Guam and the Virgin Islands, which are not directly connected to the network.

The access server has 48 internal modems to support dial backup connectivity through the PSTN. There are two Ethernet ports built into the access server, a 10BaseT and a combination 10/100BaseT. The AS5300 Access Server connects to the OCSE LAN through the 10/100BaseT Ethernet/Fast Ethernet port.

### **2.3.3.4 OCSE Server**

The Compaq Proliant 6000 Pentium II Xeon server used in the network architecture is a high-end system. There are currently four Compaq Proliant 6000 servers in the configuration. These servers are designated as Production, Backup, Development, and Disaster Recovery. Each server is equipped with dual 400 MHz Pentium II Xeon processors, 1.152 Gigabit (GB) of memory, three hot-swappable redundant power supplies, eight 18.2 GB SCSI hot-swappable hard drives and a three-channel Smart Array Redundant Array of Independent Disks (RAID) controller.

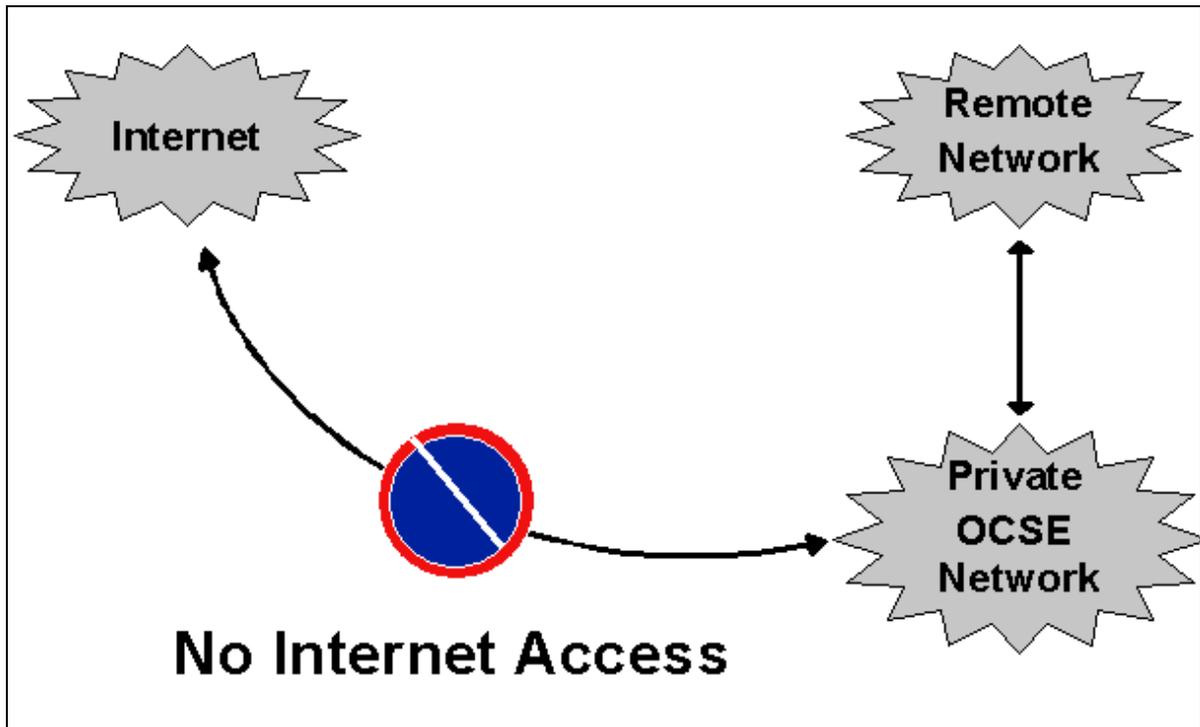
## 2.4 Network Security

A combination of safeguards has been incorporated to address the unique security requirements of the network. A private IP-addressing scheme, Network Address Translation (NAT), access control lists (ACLs), and authentication are mechanisms that are currently protecting the network. Encryption, though not currently being used, is an embedded capability that can also be implemented to protect sensitive CSENet data.

### 2.4.1 PRIVATE IP ADDRESSES

The network architecture is a private frame-relay network. In addition to the physical protection that this topology offers, the IP-addressing scheme used to exchange data over this network is also private. The implementation of private IP addressing is typical for a network that is not connected to a public network, such as the Internet, as shown in Figure 2-12. Private IP addressing provides security because public networks are not configured to route packets containing private IP addresses; they are also configured to drop inbound packets containing private IP addresses.

**Figure 2-12: Secure Private Network**



## **2.4.2 NETWORK ADDRESS TRANSLATION**

Network Address Translation (NAT) is a technology built into the router IOS that conceals internal addresses. It also enables seamless communications over the WAN between OCSE's private network and each of the 54 remote networks. The implementation of NAT on the network provides practical protection because the addresses it conceals are not needed by the remote locations. In this way, NAT does not hamper connectivity or the Data Exchange Process, but rather complements CSENet security.

## **2.4.3 ACCESS CONTROL LISTS**

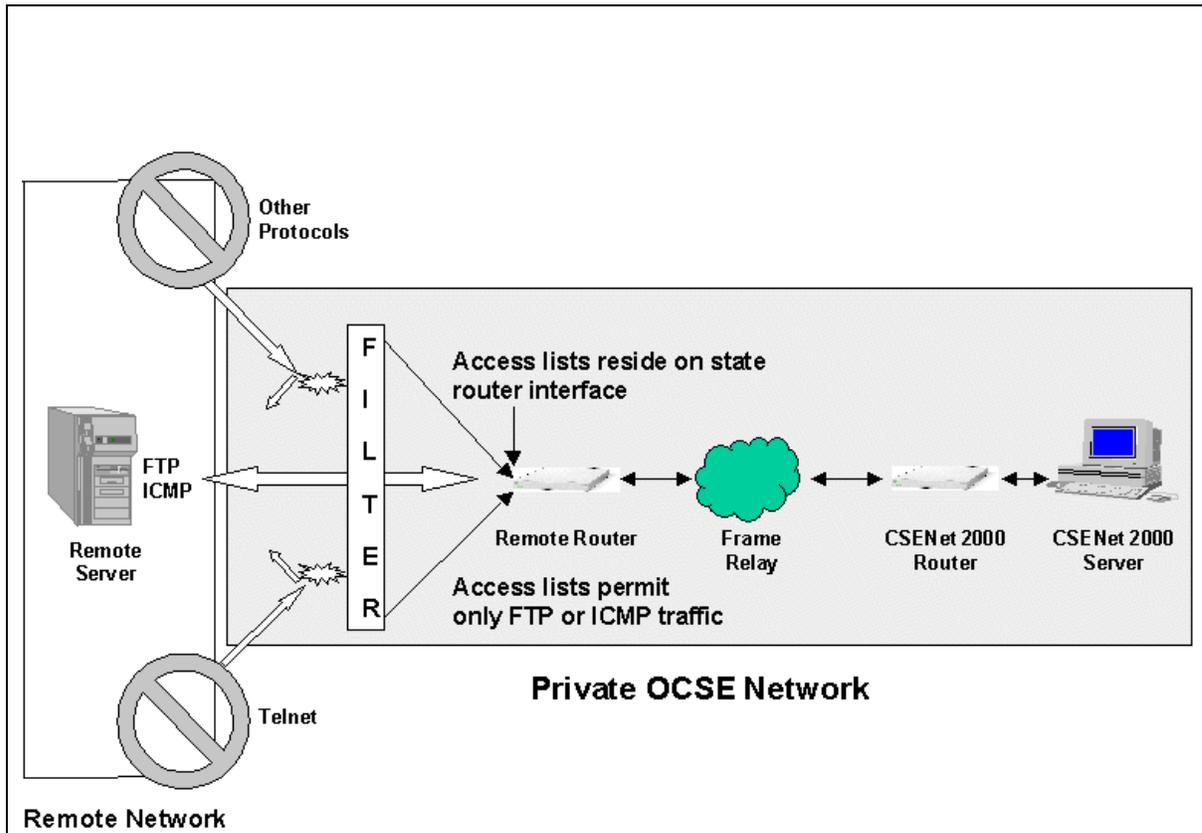
Access control lists are features embedded in the Cisco router IOS used to filter out undesirable traffic. They do this by defining conditions for filtering packets into or out of the router interface. A filter examines specific types of packets that pass through an interface and permits or denies them based on the conditions defined in the ACLs. ACLs protect the OCSE Network by keeping potentially intrusive traffic off of the network.

ACLs work on the same principal as a firewall using the same filtering mechanisms. Only specified sources and types of traffic (protocols) explicitly called out are allowed to enter the network. They access the network through logical pinholes similar to those applied to a network firewall. All other traffic is implicitly denied.

Any traffic that does not meet the conditions specified in the ACL constitutes a violation of ACL parameters. In the OCSE Network, ACL violations are logged and this activity is analyzed daily. ACLs, which reside on the remote router interface, are used to selectively allow data transfers between only the OCSE server and the remote server. At the same time, the type of traffic allowed between those servers may be only Internet Control Message Protocol (ICMP), which is beneficial for troubleshooting, and File Transfer Protocol (FTP), which is used to transfer CSENet data.

Figure 2-13 shows how ACLs applied to the remote router interface scrutinize all traffic and allow only FTP or ICMP protocols to enter the network.

Figure 2-13: Access Control List Operation



#### 2.4.4 AUTHENTICATION

Authentication is the process of determining whether someone or something is who or what it is declared to be. The most simple form of authentication centers around logon ID and password usage. Knowledge of the password is assumed to guarantee that the user is authentic. The OCSE Network requires this level of authentication when accessing its servers, and a password is required prior to router access through the LAN or WAN.

The network requires users to be authenticated before they gain network access over dial lines. Within the Point-to-Point Protocol (PPP) used for analog connections there are two types of authentication: Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). CHAP is used on the network to allow only the Cisco Access Server to connect over dial lines to a remote router.

## **2.4.5 ENCRYPTION OVER THE WIDE AREA NETWORK CAPABILITY**

Encryption is the encoding of data with the intention that decoding be conducted by authorized individuals only. CSENet routers ship with a standards-based capability to encrypt/decrypt all data. The current IOS version 12.0(7) T is capable of handling 168-bit encryption, which is considered strong encryption. Strong encryption has proven almost impossible for the average PC user to break. If implemented, clear text traffic from the network entering the main router at Manassas, VA or Baltimore, MD would be encrypted for transmission across the frame-relay network and then decrypted at the remote router or vice versa.

## **2.5 Network Configuration and Testing**

Considering that there are 54 separate entities connecting to the OCSE Network, the network is in a constant state of change. It is vital to capture all information regarding changes to the network configuration. A State Profile is used to track unique information for each remote location. The State Profile is maintained at the Manassas site and is updated whenever changes are made to the state network. Section 2.6.1 describes the details of the State Profile.

There are also three separate areas to consider when discussing testing on the OCSE Network based on the network architecture. First, there is the LAN portion of the network in Manassas and Baltimore. Second, there is the WAN, or frame-relay portion. Last, there is the state LAN that also requires a limited degree of testing from the Manassas site. There are three tests used to validate the correct configuration and operation of the OCSE networking equipment:

- Frame-Relay Functionality Test;
- Host Connectivity Test; and
- Dial-backup Connectivity Test.

These tests are performed on an as-required basis only and encompass all three portions of the OCSE Network. As-required testing is conducted for numerous reasons including:

- new equipment installation;
- troubleshooting connectivity problems;
- change of IP addressing;
- change of phone number;
- change of remote equipment; or
- change of remote host.

The results for all tests performed are provided to the remote location.

### **2.5.1 STATE PROFILE NETWORK PARAMETERS**

The Manassas site maintains a database containing information pertaining to each remote location called a State Profile. This profile contains key information regarding the remote network and is used in part to configure and maintain the OCSE communications equipment. Some of this information includes:

- IP addresses and subnet masks;
- LAN interface (Ethernet, Fast Ethernet, Token Ring, or serial);
- analog phone number (for dial backup communications);
- logon parameters (userid, password);
- data set names; and
- points of contact information (technical POC, communications coordinator, etc.).

It is recognized that this information periodically changes for various reasons. Changes to the network configuration parameters, logon parameters, and data set names must be coordinated in advance through the CSENet Service Desk. A sample of a State Profile is shown in Appendix I.

### **2.5.2 FRAME-RELAY FUNCTIONALITY TEST**

This test has three main functions:

- The Ping application verifies connectivity to the remote router over the network.
- The Ping application verifies connectivity to the remote host.
- The local and remote router statistics and configurations are captured.

The results of the test are written to an output file. The test results are validated by successful Ping responses to the remote router and host, and the statistics matching expected results from the remote and local routers.

### **2.5.3 HOST CONNECTIVITY TEST**

This test performs the following functions:

- The Ping application verifies connectivity to the remote router.
- The FTP application verifies proper logon parameters to the remote host.
- The FTP application retrieves a specified data set after the logon.

A successful logon and retrieval of the data set validate the test. The results of the test are written to an output file.

## **2.5.4 DIAL BACKUP CONNECTIVITY TEST**

This test demonstrates fallback communications to remote locations that normally use frame relay and have an analog phone line for fallback data communications. This test performs the following functions:

- Disables both of the frame-relay interfaces for the tested remote location;
- Uses a fallback analog circuit to restore communications to the remote location;
- Ping and Traceroute applications verify connectivity with the remote router over the fallback analog circuit.

The test is validated if the Ping and Traceroute applications can communicate with the remote router over the analog phone line. The test concludes by enabling both of the frame-relay interfaces and terminating the modem connection. The results of the test are written to an output file.

## **2.5.5 SEMI-ANNUAL DIAL BACKUP TEST**

This test also demonstrates fallback communications to remote locations. Test methodology is very similar to the Dial Backup Connectivity Test except the Semi-annual Dial Backup Test checks all remote locations on a specific schedule instead of as required. The test is conducted every six months and the results are provided to OCSE and the remote-location points of contact. The test is validated if the Ping and Traceroute applications can communicate with the remote router and host over the analog phone line.

The Semi-annual Dial Backup Test provides two output reports. The first is a detailed report showing all of the test scripts executed and the recorded results of those scripts. The detailed report is used if there are questions regarding the validity of the test results. The second is a summary report, which shows concise test result information regarding the status of the fallback communications to each remote location. The summary is provided to OCSE and points of contact at remote locations.

## 2.6 New Site Installation

To connect a new site to the OCSE Network, a state should take the following steps:

Contact the CSENet technical representatives or Service Desk at (800) 258-2736. This team will provide information concerning the CSENet suite and the OCSE Network.

1. Provide the State Profile information (Appendix I), and determine if the site is to install the inside wiring between the demarcation point and the OCSE equipment or if this service should be contracted using the GSA FTS2001 contract.
2. With OCSE's approval, a frame-relay circuit will be procured through the FTS2001 contract.
3. Make available an analog phone line for backup communications.
4. Depending on the circumstances, a CSENet engineer may be deployed to install the OCSE equipment.

For questions regarding the network or the CSENet applications, contact the Service Desk at (800) 258-2736. Refer to Section 8: *Technical Support for States* for specific information regarding technical support.

## 2.7 Network Troubleshooting and Maintenance

Equipment provided to remote locations is owned, administered, and maintained by OCSE. Remote locations are responsible for maintaining communications between their remote host and the OCSE router. The state communications coordinator will be notified if communications between the remote host and the remote router cannot be established.