

## 16a. Wide Area Data Network - Intranet

### 16a.1 INTRODUCTION

Motorola will provide a scalable intranet solution to support the enterprise data requirements of the Commonwealth of Virginia's State Police (VSP), Department of Mines, Minerals, and Energy (DMME), Department of Emergency Management, and Department of Environmental Quality (DEQ). Its growth potential is limited by the bandwidth accommodations of the STARS microwave network (see section 5 Microwave). In addition, Motorola will provide the wide area intranet as a foundation for the use by all the Commonwealth agencies. This Wide Area Network (WAN) solution utilizes the transport facilities of the STARS microwave network and is designed to interconnect existing VSP LANs, VSP Land Mobile Radio (LMR) network components, and the Virginia Crime Information Network (VCIN). Any site not co-located with a STARS Microwave node will employ a Motorola approved, Commonwealth provided dedicated leased line or wireless technology equivalent (see Canopy System Description) to connect that site to an appropriate Microwave node.

To complete the intranet solution Motorola has included security measures based on computer networking standards, availability management applications, and network monitoring solutions. Additionally, this design will include tools to enhance productivity, such as a centralized document management system, and dynamic network address management.

#### 16a.1.1. The Intranet solution consists of three main components:

- Wide Area Network – to support wide area networking infrastructure and allow the Commonwealth agencies to access information securely throughout the Commonwealth.
- Data Center Solution – to store STARS project data that can be accessible via the Intranet; as well as provide the foundation for hosting other Commonwealth agency data in the future. The Data Center was designed with high availability in mind; therefore, a disaster recovery design has been included.
- Software Management Solution – to support system management and network fault monitoring.

Motorola will procure implement and provide technical support during the warranty period for a working Intranet. This includes hardware, software, databases, programming and transport media and other services as described herein.

All traffic on the intranet will be encrypted via Cisco IOS IP-SEC 3DES tunnels on the routers. However, when AES encryption becomes available Motorola will submit a new design and additional costs to modify the intranet to use this encryption scheme. All dial-up users will use Virtual Private Network (VPN) software to access the trusted network.

#### **16a.1.1.1. Performance Objectives**

The purpose of this section is to define the design, integration, and testing of a statewide public safety, secure, wide-area data network (Intranet). This network will serve the Commonwealth by providing a hierarchical data network structure, where every participating network site terminates into the nearest Division office. From there the Division offices will connect to the Control Center over bandwidth defined under section Class III Service connections.

The Control Centers are built upon a fully redundant core switches. These switches are connected to each of the core routers that interface to the Division offices. Dual connections to the core routers provide the additional redundancy needed for continued operations should either of the core routers fail.

To ensure privacy on the closed network IPSEC tunnels will be used to encrypt the data as it moves from one site to another. The IPSEC tunnels will be implemented between each point-to-point link in the router.

Dial-up users will require both Virtual Private Network (VPN) Software on their workstation and an ACE device (see Two-Factor Authentication – The RSA SecurID/ACE System section) that dynamically generates secure tokens.

The VPN software is used to create a private secured and encrypted tunnel from the workstation to a VPN Gateway that is connected to the trusted network. The user's ACE card is synchronized to the VPN server gateway. This VPN Gateway then authenticates and logs the user into a session on the trusted network.

The routers for each VSP site listed in Appendix 4 table “Wireless Lan/Wide Area Network” will have a Fast Ethernet port for connection to the local VSP-LAN. The intranet design is based on the Internet Engineering Task Force (IETF) Transmission Control Protocol/Internet Protocol (TCP/IP).

### **16a.1.1.2. Data Repository**

The Wide Area Network design includes a data repository such as for project information, project documents, other documentation, photographs, and reports. Five (5) Terabytes of storage in the SPHQ Primary Control Center and five (5) terabytes of storage in the SPHQ Backup Control Center make up the ten (10) Terabytes (TB) of redundant storage.

The repository will serve as a distribution center for radio, mobile data, microwave operations and maintenance manuals, and system as-built drawings. The repository will also be used to host fixed and mobile equipment inventory data, maintenance records, alarm reports, and WAN configuration management files. In addition, it will serve as a secure location for radio personality profiles used statewide by Commonwealth maintenance personnel.

This repository uses Quest Software's Vista Plus application as the repository manager with an Oracle database implementation on two SUN servers. Each is attached to 5TB of SUN disk storage that is loosely clustered between the primary and backup sites. Vista Plus is a very comprehensive package that will handle documents, photographs, scanned images and data from many different sources. The data, documents and images are accessible for viewing from Microsoft's Internet Explorer web browser.

The Vista Plus is capable of controlling access via a user ID and password mechanism. Vista Plus electronically distributes data via internal networks and email based on security user settings. This software provides reports to multiple users online, who can search and view information electronically.

Finally, Vista Plus contains tools for report viewing, searching, extracting, printing, saving, and archiving. These tools include:

TransVue™: Electronic documents saved in virtually any format can be stored in the same electronic folder as their related reports with TransVue Capture. TransVue Client allows viewing of over 225 electronic document file formats without having the native application installed on the desktop.

SmartAlarms®: Vista Plus provides automatic notification (via email, Vista Plus messages, print-outs, and more) of report availability and changes with SmartAlarms.

Report Index Hyperlinking™: Vista Plus automatically links reports by index values so you can easily drill down and view related report information and make quicker, more accurate business decisions.

Bundling and Bursting: An easy way to automatically group reports together and distribute them electronically to the people who need them.

### **16a.1.1.3. System Management Server**

The network design provides access to a distribution server by which system software updates are pushed to mobile computer clients.

This design consists of Microsoft's "Systems Management Server" (SMS) to push upgrades, packages, and refreshes to mobile computing workstations. This function will be performed when the mobile terminals are brought into any of the eight Radio Maintenance facilities or within suitable range of properly equipped Wireless Local Area Network (WLAN) access points (refer to WLAN System Description). An SMS client will be installed on the Motorola supplied mobile terminal. The system is initially designed to provide service for 5000 mobile computer users.

### **16a.1.1.4. Intranet Access**

The intranet design makes extensive use of the STARS Microwave Network where it is available. For those sites that do not have a Microwave node on site a Motorola approved, Commonwealth provided dedicated leased line or wireless technology equivalent (see Canopy System Description) will be used to connect that site to the appropriate site that has an entrance into the Microwave network. Note, the intranet has been configured to replace the leased data lines used by the State Police among State Police Headquarters (SPHQ), division headquarters, and area offices.

The VSP internal data (approximately 1,300 computers) will be transported by the intranet. Refer to Figures 16A-1 through 16A-10 for a description of the VSP Data Network. The intranet has been designed as a closed network and therefore will not provide internet access.

This WAN has been explicitly configured for intranet operations only. If the Commonwealth should desire Internet connections, Motorola will provide a quote for additional services, equipment, warranty and training upon receiving a formal written request from the STARS Project Manager. In addition, Motorola will provide data relevant to impacts on the Project Schedule.

Further, any Internet connections will be provided only upon the specific approval of the STARS Project Manager. Internet functionality will require a separate design and review by the Commonwealth to ensure that security and access control policies meet the Commonwealth's Standard Operating Procedures.

### **16a.1.1.5. System Layout**

Motorola has supplied a block diagram of the backbone infrastructure, as designed, as well as designs for each of the Division offices and the two control centers. The diagrams can be found in the subsequent pages.

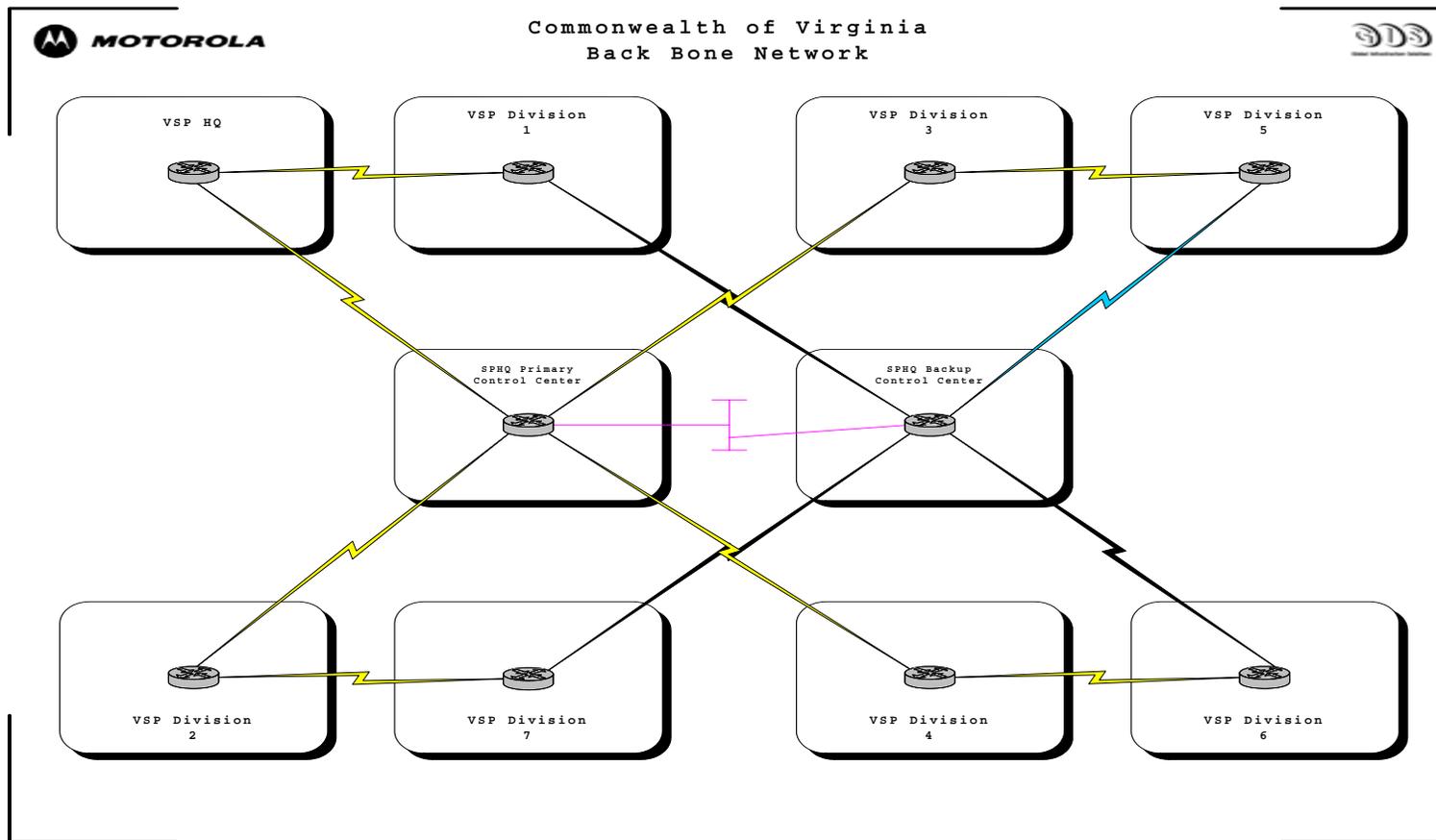


Figure 16A-1 WAN System Block Diagram

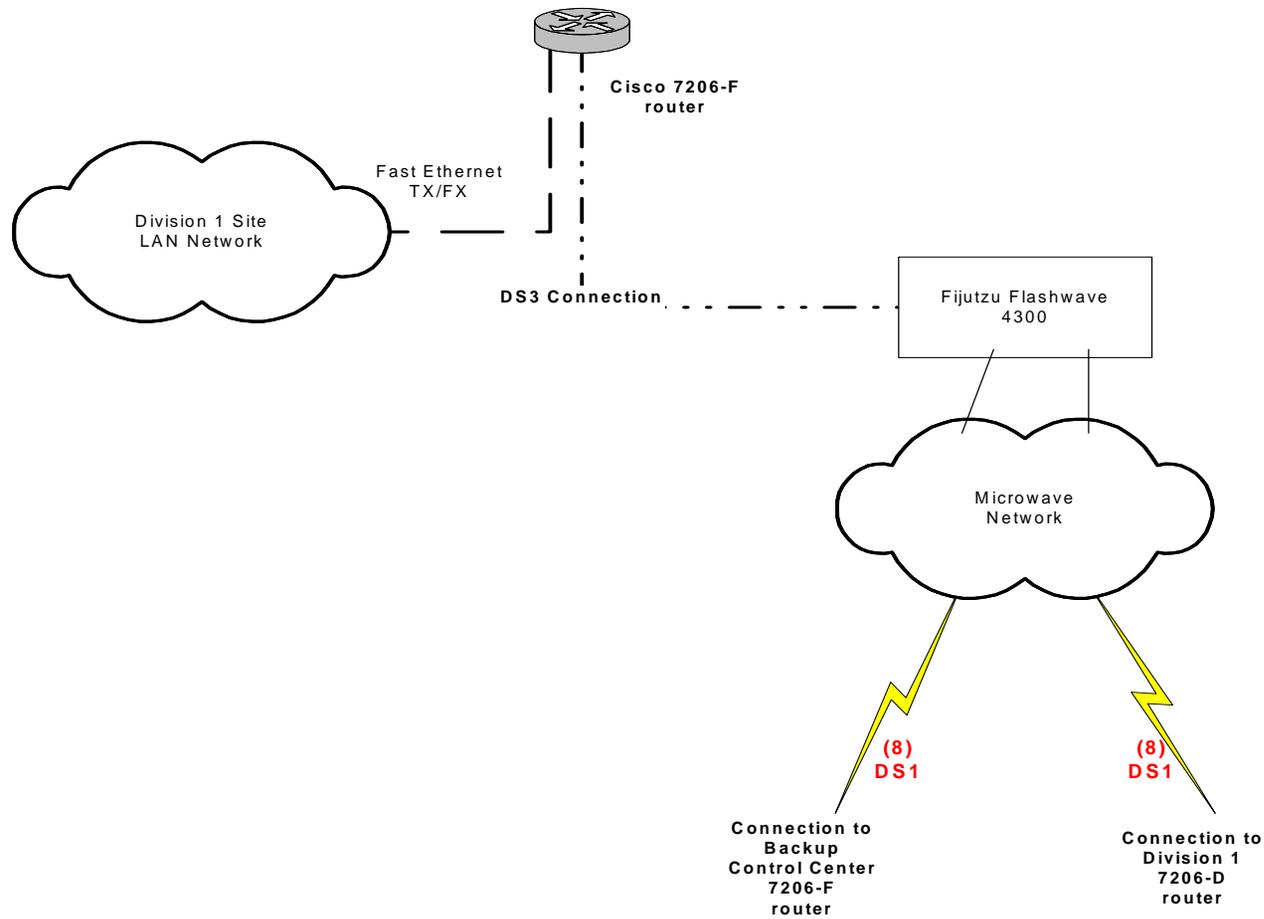


Figure 16A-2. WAN VSP Headquarters Block Diagram

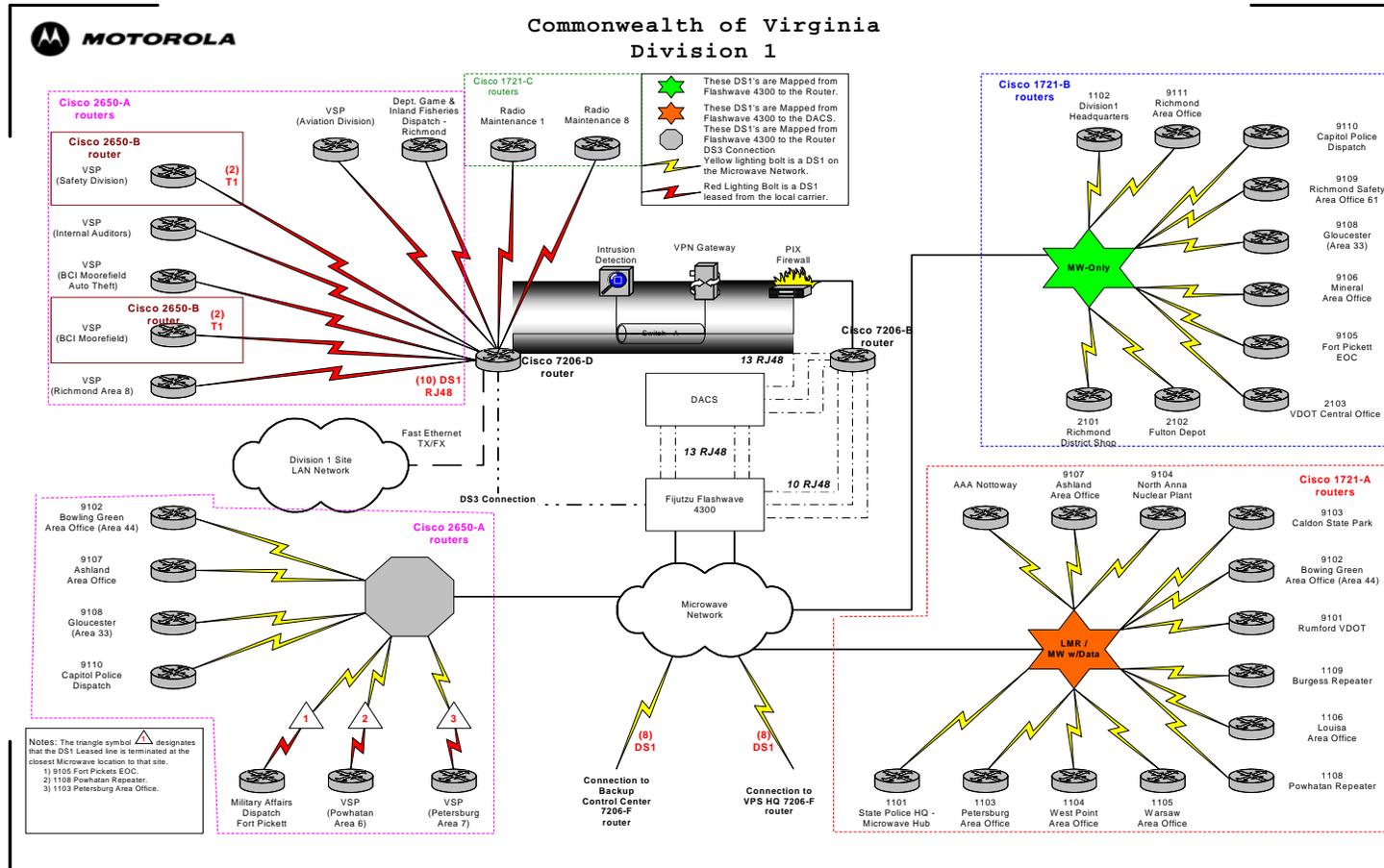


Figure 16A-3. WAN Division 1 Block Diagram

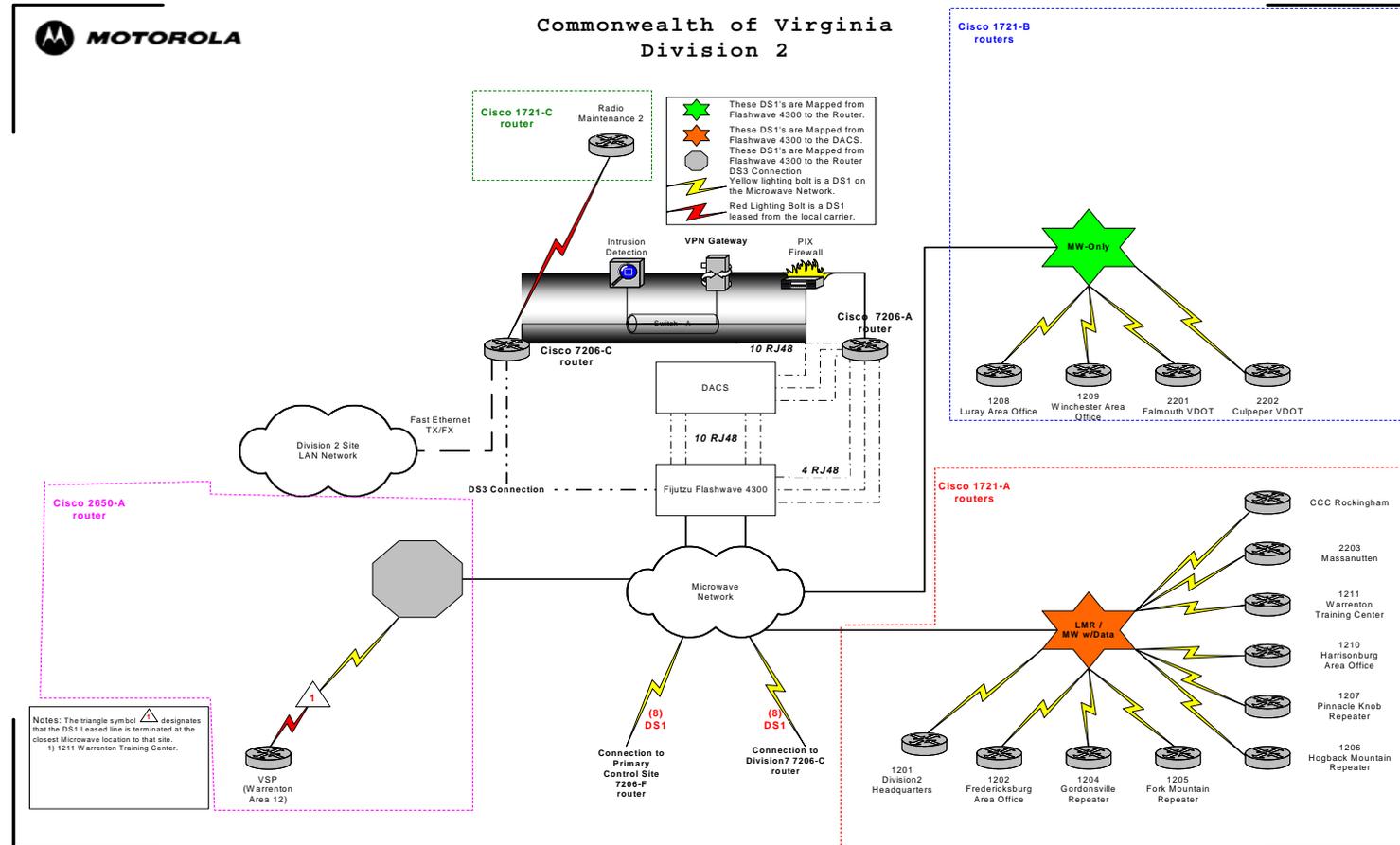


Figure 16A-4. WAN Division 2 Block Diagram

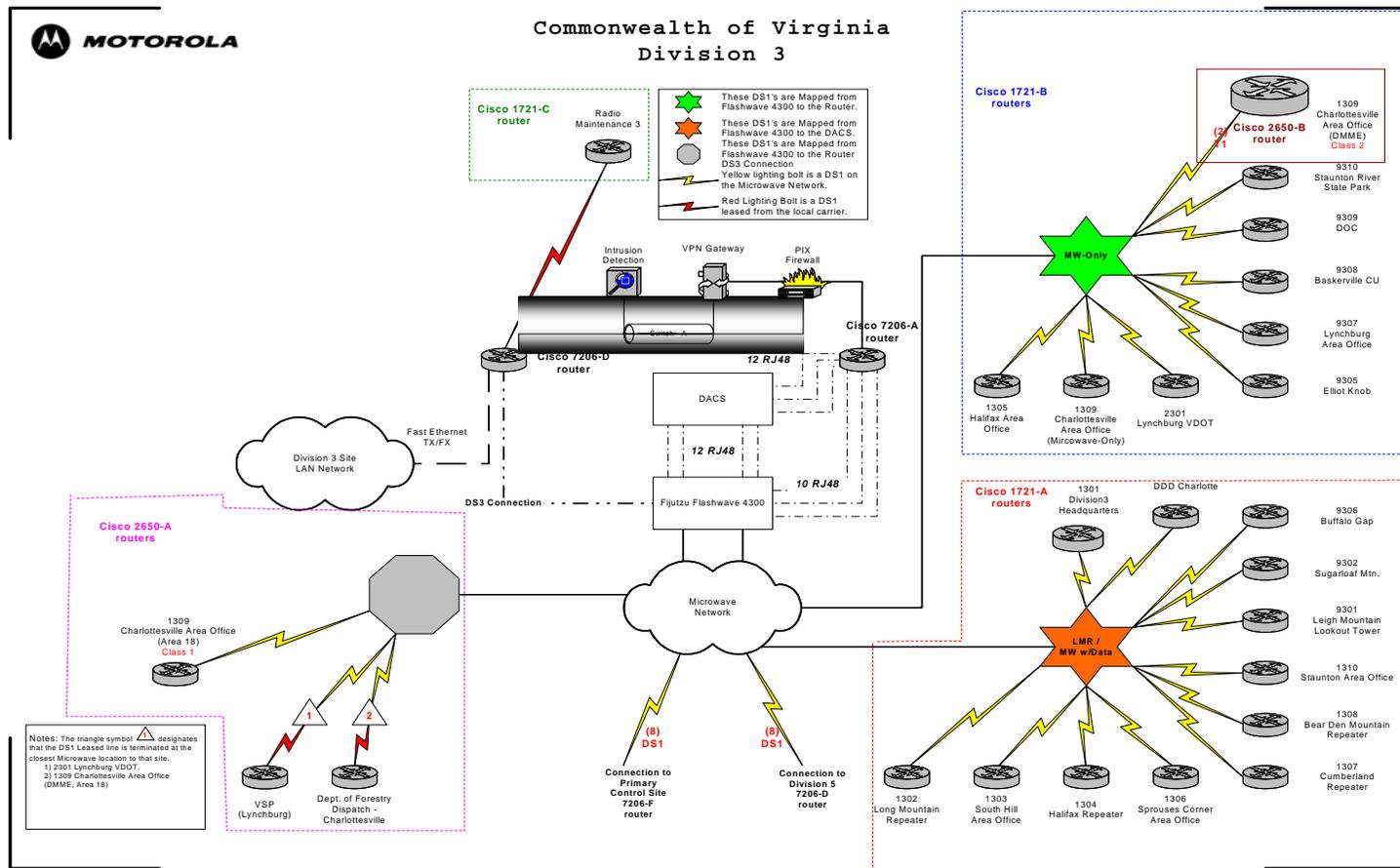


Figure 16A-5. WAN Division 3 Block Diagram

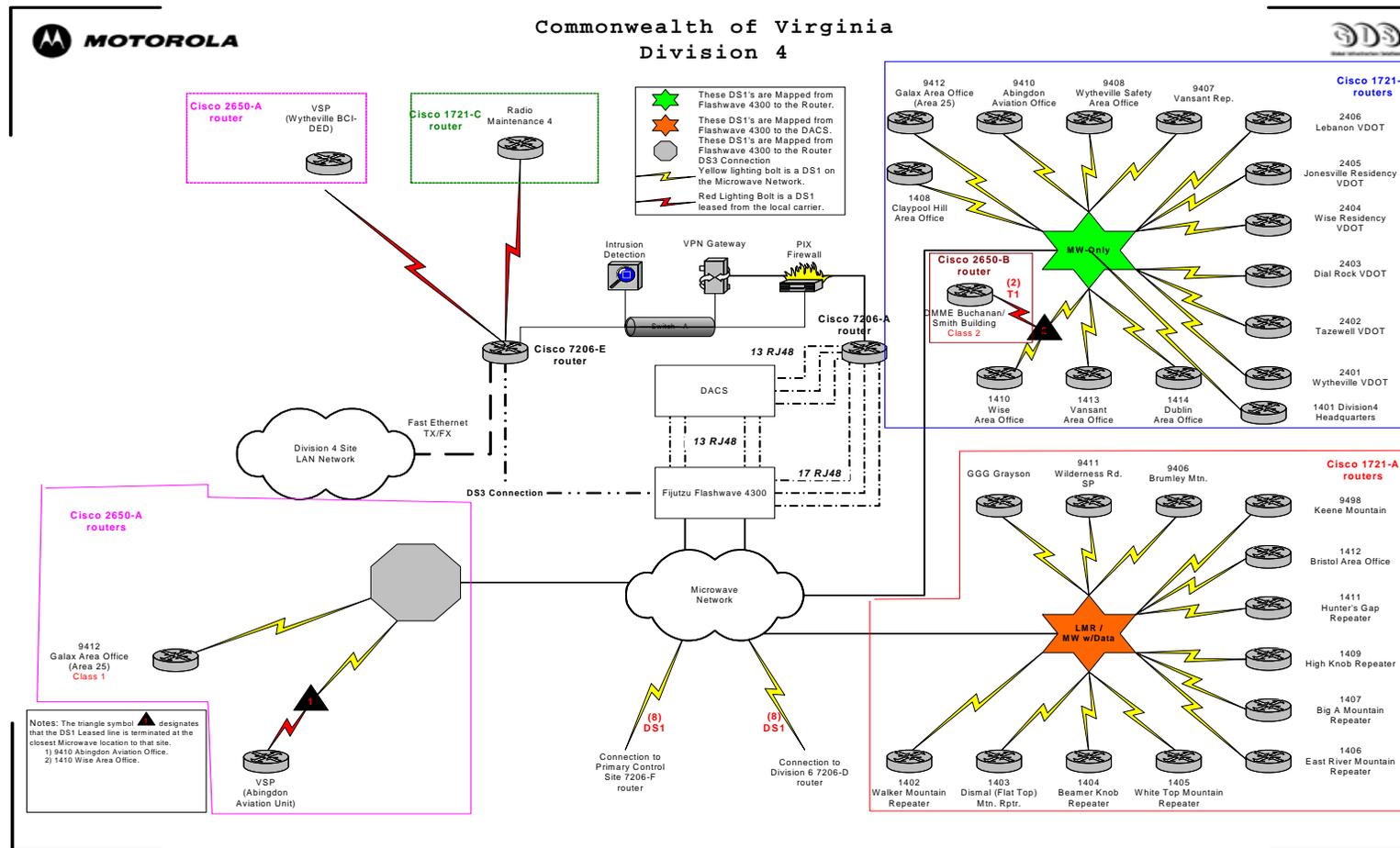


Figure 16A-6. WAN Division 4 Block Diagram

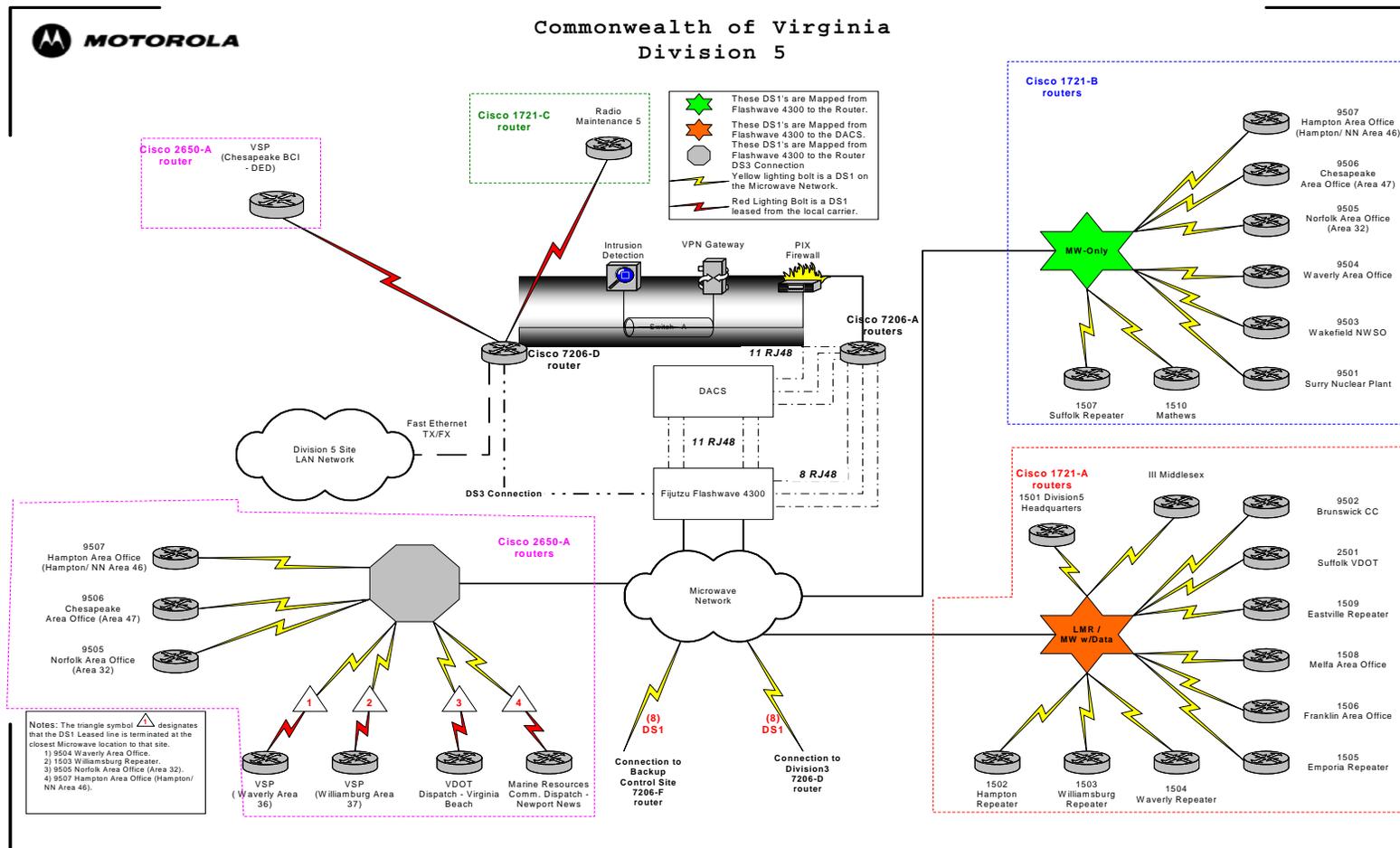


Figure 16A-7. WAN Division 5 Block Diagram

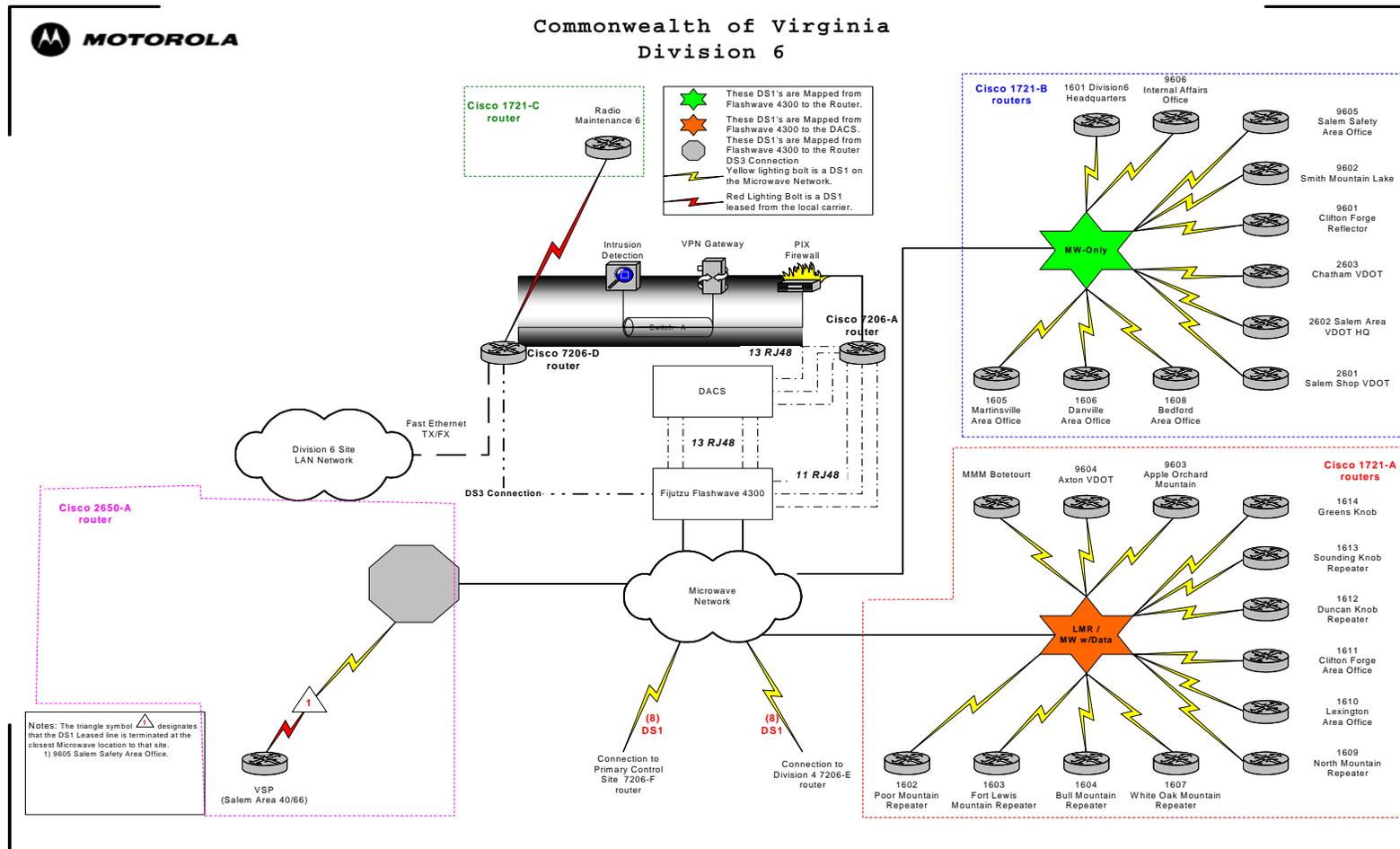


Figure 16A-8. WAN Division 6 Block Diagram

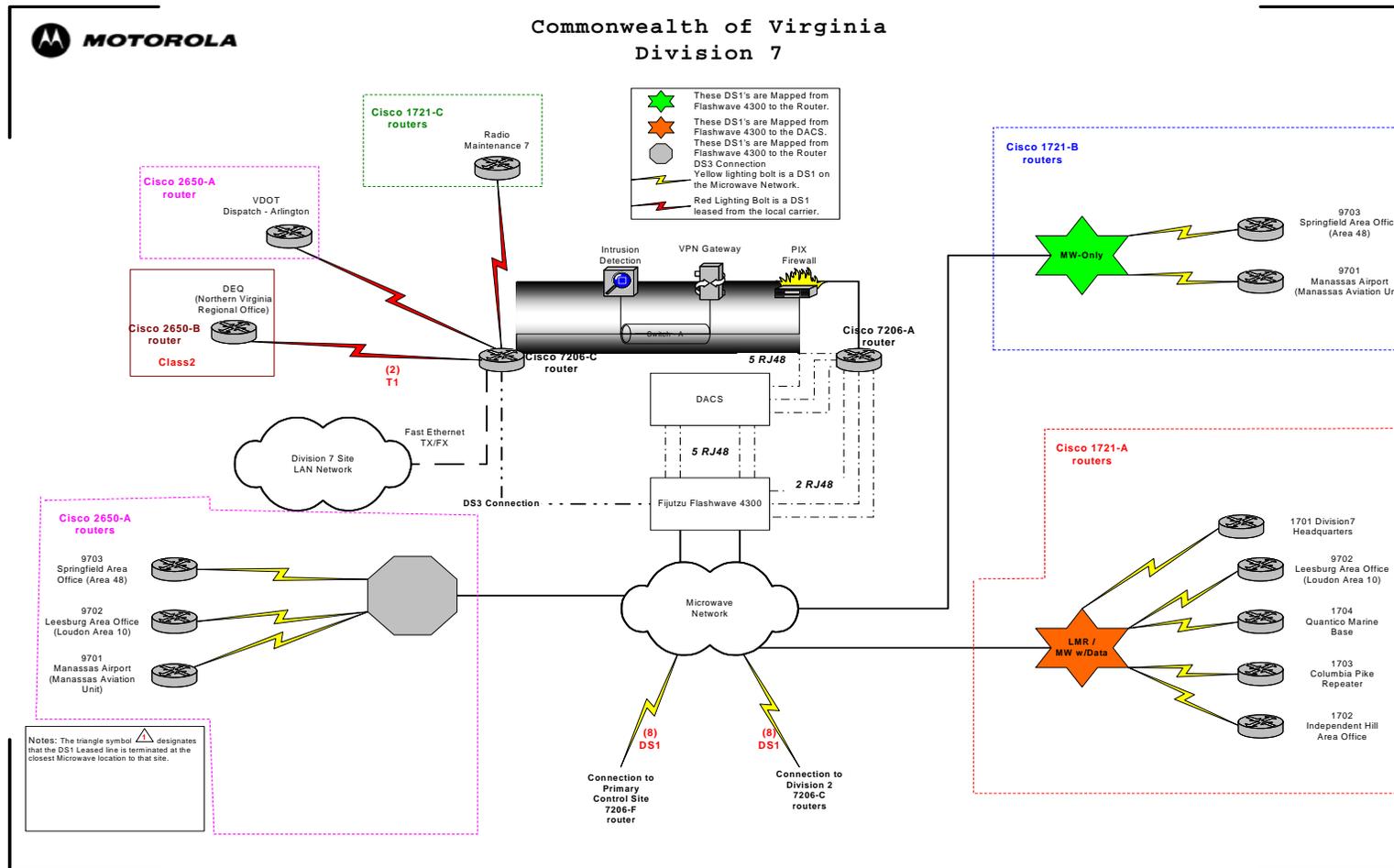


Figure 16A-9 WAN Division 7 Block Diagram

WAN Primary / Backup Control Center Block Diagram

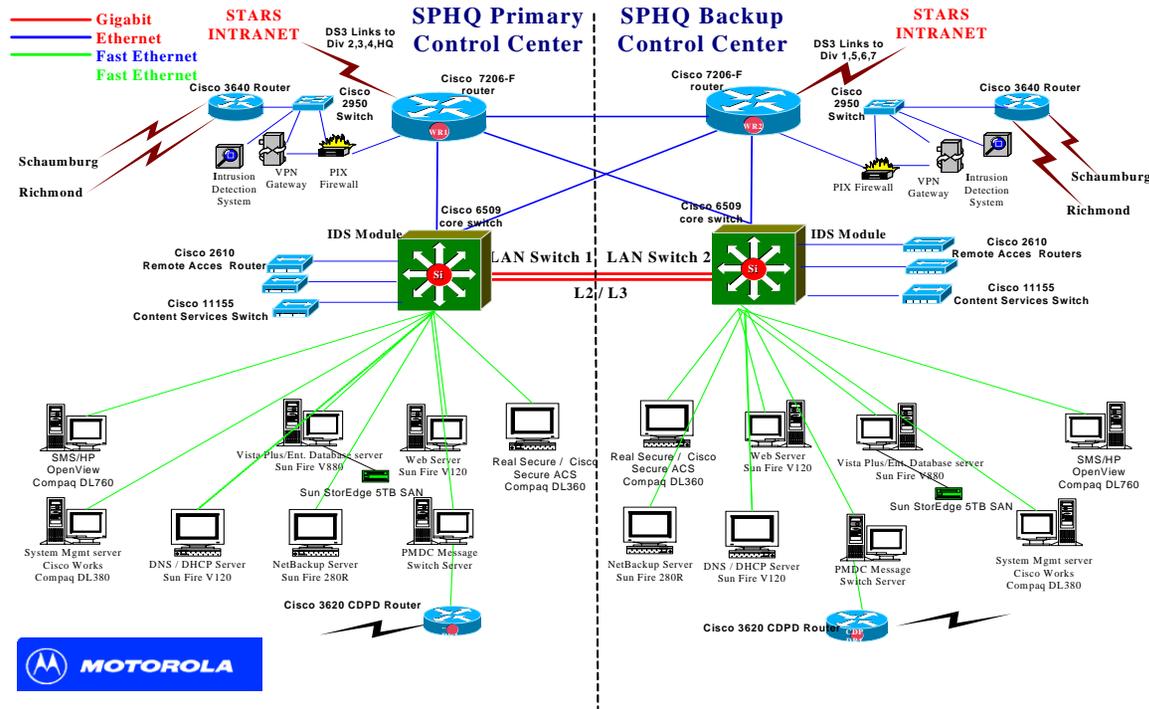


Figure 16A-10. WAN Control Center Diagram

#### **16a.1.1.6. Implementation and Migration**

The implementation of the intranet is described in the System Integration Statement of Work section.

The Computer Aided Dispatch (CAD) switch resides on the VSP Internal network (100.15.x.x). The STARS Intranet will be connected to this network. This CAD interface is not available for other agency users. Mobile users will be able to connect to their internal agency databases and servers and will be prevented from connecting to servers for which they are not authorized access.

#### **16a.1.1.7. Agencies Connections**

The following agencies, as identified in Appendix 4 matrix “Wireless LAN/Wide Area Network” will have operational intranet access provided as part of the first four divisions of this project.

- Department of Environmental Quality (DEQ)
- Department of Mines, Minerals, and Energy (DMME)
- Virginia State Police (VSP)
- Department of Emergency Management

#### **16a.1.1.8. Service Classifications**

Three (3) classifications of service are established based on the facilities and organizational demands placed on the specific office. The service classifications are further defined below:

##### ***16a.1.1.8.1. Class I Service***

This class of service will include a firewall, router, and Channel Service Unit/Data Service Unit (CSU/DSU) in addition to the Intranet interconnect equipment. Where microwave equipment is used as the Intranet connect media, this class of service receives the basic level of microwave service. The VSP offices are served by the microwave network where available and specified in the microwave system section; other requesting agencies may be connected by other means. Class I offices are served by no more than a full DS1 bandwidth.

#### ***16a.1.1.8.2. Class II Service***

This level of service adds Intranet service to an existing network through the inclusion of firewall functionality and a router. Where microwave equipment is used as the Intranet connect media, this class of service receives multiple DS1 microwave service.

The VSP offices are served by the microwave network where available and specified in the microwave system section; other requesting agencies may be connected by other means. Class II offices are served by no more than 2 DS1s worth of bandwidth.

#### ***16a.1.1.8.3. Class III Service***

This service is restricted to the Virginia State Police (VSP) Division Headquarters, the SPHQ Primary Control Center and the SPHQ Backup Control Center. This service provides the major interconnection point for each VSP division and mobile computer terminals (MCTs). All mobile data to and from the MCTs shall be handled at these locations. Class III offices are served by more than 2 DS1s. However, the initial Class III implementation is designed with 4 DS1s of bandwidth.

#### **16a.1.1.9. Number of Users**

The intranet's capacity can grow and accommodate users up to the amount of bandwidth allocated to the network by the microwave infrastructure.

### **16a.1.2. System Design**

#### **16a.1.2.1. System Components**

The Servers' hardware and software (HW and SW) in the SPHQ Primary Control Center are connected to a set of redundant servers in the SPHQ Backup Control Center via select lighted strands within a dark fiber bundle. The database (DB) servers are clustered across this link using SUN Cluster 3.0 software. The DNS servers and web servers are load balanced between the sites. All systems will failover or be redirected to this backup system should the primary DNS server fail.

### **16a.1.2.2. LAN Technology**

Motorola is providing IEEE 802.3u 100 Mbps Fast Ethernet ports on the remote routers for connection to the Commonwealth's existing LAN environments. In the Control centers the same port types are being supplied to support the server infrastructure. Motorola is not providing a quote for the build out of any existing LAN environments and therefore cannot control the collision rate or overall performance of the local ("off-intranet") LAN environment.

### **16a.1.2.3. Operating System Software**

The operating system is designed for a multi-user environment and high reliability and availability in an environment where information security is critical. The operating system contains features to safeguard information contained within the system or information as it passes through the system. The operating system will function on a strict need-to-know basis where information and resources are only made available to authenticated users.

The operating system will be the current approved software version at the time of order. It will include all manufacturer issued patches, service packs and interim releases. The operating system manufacturer will have expressed the intention to continue supporting the operating system version purchased.

Since this will be a system installed over time, Motorola assures the Commonwealth that patches, service packs and interim releases are consistently applied for each portion of the system as it is brought on-line. This may include updating operating equipment. Where operating equipment is updated, Motorola will make every reasonable effort to ensure the redundant equipment is fully operable during the change over. A minimum of one (1) week "burn-in time" should elapse before applying operating system changes to redundant equipment.

There are two types of system servers in this proposal – UNIX and NT based. All UNIX hosts will be running SUN Solaris. All NT systems will be running Microsoft Windows Server. The manufacturers of these software operating systems regularly release patches and updates to enhance the availability, performance and usability of their software and primarily to fix problems. These patches are provided at no additional cost for users with current maintenance coverage. Along with Motorola's SMS implementation to provide software refreshes across the network and the current products being used, OS currency will be maintainable, manageable and fairly unobtrusive.

#### **16a.1.2.4. Communication Protocol**

The communication protocol used will be Transmission Control Protocol running on top of Internet Protocol (TCP/IP).

#### **16a.1.2.5. Software Development**

Motorola will provide the interface software necessary to display information from terrestrial databases to the user community.

The Repository Management software – Vista Plus is all browser-based for viewing of data and reports. All of the system and network management and monitoring systems are also browser-based for viewing and monitoring purposes.

#### **16a.1.2.6. Upgrades**

Given the expected evolution in technology during the life cycle of the wide area data network, Motorola's design allows for renewal and replacements. Please see the appropriate Warranty Service Plan or Maintenance Service Plan for details.

#### **16a.1.2.7. Maintenance and Renewal**

The wide area data network has been designed to provide highly reliable service to the Commonwealth. Please see the appropriate Warranty Service Plan or Maintenance Service Plan for details regarding support of this network.

#### **16a.1.2.8. System Redundancy**

Motorola will provide a fully redundant Database system at the SPHQ Primary Control Center. The Sun Cluster software will provide the cluster environment. In the event of a service failure on the primary node the Database and the associated Applications will be restarted on the secondary node. Availability is achieved by using scripts that monitor application service health on individual cluster nodes. The system provides redundant storage arrays (RAID-5) with each of the Database/Document Management servers to ensure data integrity. The Veritas Volume Replicator mirrors data to the backup control site maximizing data continuity.

A disaster at the SPHQ Primary Control Center would mean that the Database and the Document Management environments would failover to the SPHQ Backup Control Center, which would now function as a Disaster Recovery (DR) environment.

### **16a.1.2.9. Back-up**

Back-up capability will be provided. This system has the capability to completely save all data on the system without causing any interruption to the use of the system. The back-up system will use a system of incremental and complete backups conducted hourly, daily, weekly, and monthly to assure that:

- At no time will an equipment failure result in the loss of more than four hours of data,
- A complete back-up will be created each month

The system performance is not impaired by redundant back-ups.

The Backup infrastructure includes two (2) servers – one at each of the Data Centers.

The Veritas NetBackup DataCenter software provides complete data protection for the Commonwealth environment. Veritas Backup agents will be installed on the Database/Document Management Servers at the Data Centers. Policies will be implemented to configure full backups to occur monthly, with incremental backups occurring on a nightly basis.

The L180 Tape Library has been selected keeping in mind that the Backup infrastructure at each of the Data Centers would need to be able to backup the entire Data Center. The Sun StorEdge L180 tape library is a 180-cartridge automated tape library that offers enterprises a storage solution of up to 6.96 terabytes.

It is recommended that the Commonwealth consider offsite storage of backup tapes as an optional item. Otherwise backups will be stored at the SPHQ Primary site.

Motorola is providing three (3) layers of protection to the Commonwealth data. First, the data is stored on the disk using RAID5, which allows recovery of single bit errors – on the fly as the data is written. Second, the Repository systems are clustered across the primary/secondary campus, so an injured system will failover to its complement without losing data. Finally, the data is backed up using the automated tape library on a scheduled basis reducing potential data loss to a four hour window.

All of the intranet network equipment configurations are stored in the server environment and will be backed up using the procedures previously outlined.

### 16a.1.2.10. Audit Trail

The system design includes provisions for an audit trail of intranet protocol transactions. The audit trail will report the following data:

- Time and date stamp
- Logged on name and user identification

The audit trail will be available for review and processing by the administrator. Tools for converting this information into user friendly data are included. Motorola will work with the Commonwealth to define the format and detail of information to be tracked.

### 16a.1.2.11. System Security Design

The system includes the security measures and elements described below:

### 16a.1.2.12. Identification and Authentication

Prior to allowing access to the server or any data hosted on the server, the software will require at a minimum, user identification and a password.

Different levels of access are allowed depending on the user identification. The System Administrator can set access levels for individual users, add additional access levels, and monitor the usage of each assigned access. Initial access levels are:

<u>ACCESS LEVEL</u>	<u>TYPICAL ACTIVITIES ALLOWED</u>
Administrator	Establish user accounts, add or delete software, change, edit and delete virus protection, broadcast software updates change encryption keys, read usage logs
User	Need-to-know read, edit and/or delete files based on permission levels granted by the administrator.
Guest	All guest accounts will be permanently disabled from all devices that require passwords. Motorola will individually verify and document this for each password-protected device, including but not limited to any servers, firewalls, routers and switches.

Any Motorola specific or used passwords will be removed at the completion of the installation process. This includes software installation passwords. Authorization to access the wide area data network resides with the STARS Project Manager.

The Database/Document Management servers in the primary facility will utilize the Trusted Solaris (UNIX) operating system (OS) environment. The Trusted Solaris Operating Environment extends the capabilities of the Solaris Operating Environment to provide superior safeguards against internal and external threats far beyond the protection commonly found in standard operating systems.

The Oracle Database application itself is secured with its own user access and password protection system.

Motorola will run an internal security audit of the system before turning it over to the Commonwealth. Motorola will work closely with the Commonwealth Account Administrator(s) to ensure accessibility and denial of access procedures are in place as well as procedures to terminate accounts and access when appropriate.

Password access to all network equipment is controlled at two levels, read only and full update access. Additional security will be provided by the Cisco Secure product that is user ID and password based. All control of access to all equipment will remain within the Commonwealth.

#### **16a.1.2.13. Password Controls**

Motorola has designed the system to enforce the following password requirements on all devices with password protection (this includes routers, switches, servers and firewalls):

- All passwords will be stored in a one-way encrypted form to assure that they cannot be read by anyone including the system administrator.
- Only the system administrator has the ability to reset passwords.
- All passwords are system unique.
- The system will not allow any indication of the password length or of the number of characters in the password. The cursor will not move as a password is entered into any device.
- The system will require users to change their passwords on a period selected by the system administrator (typically ninety (90) days).
- After three (3) unsuccessful access attempts, the system inactivates that password effectively disabling the account.

All passwords are encrypted during transmission and while stored on the systems. System administrators or personnel, i.e., Customer Service personnel, with system administrator rights are the only individuals authorized to reset passwords.

Additionally, Motorola is providing an ACE card system with an initial count of one hundred (100) ACE card tokens. These tokens have a four year life and will equip dial-up users into the intranet with the additional level of authentication required before being granted access. An ACE PIN is appended to their password and User ID to put further controls on access.

Uniqueness of user ID and password is built into the security and password routines included in the NT and UNIX OS security modules.

#### **16a.1.2.14. User Account Controls**

The system will provide the following functionality concerning user accounts:

- Inactivity time out will be provided. Any account inactive over 30 minutes is logged out.
- Accounts that have not been used for a period established by the administrator are inactivated.

The system administrator will have the ability to immediately suspend or disable any user account.

#### **16a.1.2.15. Firewall and Interconnections**

A firewall will be provided from any interconnection point into the Wide Area Data Network. Each network port interconnecting to another local area network or wide area network will also be protected by a firewall.

Internet connectivity has not been provided as a function of this system design.

#### **16a.1.2.16. Dial-up Access**

Dial-up access by users is supported through secured VPN Client software. One remote dial access server has been provided to facilitate this access.

#### **16a.1.2.17. Access at Microwave Radio Site**

The intranet system includes wide area network access for a user at each microwave only site. The network design also provides an intranet access point at each of the eight field repair locations (Radio Maintenance facilities). Each access point will provide a secure path across the Intranet for authorized persons to retrieve information such as maintenance data, instruction sets, drawings, and other stored knowledge from the Data Repository.

#### **16a.1.2.18. Virus Protection**

All servers, routers, and firewalls will be protected by virus protection software.

During the warranty period, virus protection software will be updated bi-monthly by Motorola. Changing or updating virus protection software requires administrator privileges on the protected device. The ability to update includes revising and or replacing the virus detection engine as well as the virus definition files.

This system will notify network Administrators when a credible threat could potentially degrade the network, software running on the network or Motorola installed systems attached to the network. This warning will list the type of threat (virus, worm, etc.), list the actions that can or will be taken to eliminate or mitigate the threat, and list any software changes that may be required. Notification will not be provided in situations where the threat does not affect any user and where corrective action(s) have already been taken or are completed. The Commonwealth PM will be informed of any threat.

The SMS implementation will be used to push out anti-virus updates.

Internal NT and UNIX servers are protected by Symantec Anti-virus software. Motorola has designed Intrusion Detection systems in various Switch/Firewall configurations on the intranet and on the System Servers in the SPHQ Primary Control Center and SPHQ Backup Control Center. This system monitors intranet data traffic patterns for unusual patterns of activity such as might be caused by a virus.

#### **16a.1.2.19. Security Assessment**

During the warranty period, Motorola will perform a semi-annual security audit of the intranet. This audit will include a complete review of all network equipment and the application of all relevant patches, as well as an orchestrated “hacking” attack to validate security against intrusion. Should this challenge identify problems, Motorola will notify the STARS Project Manager within 6 hours and initiate corrective actions within 12 hours.

#### **16a.1.2.20. Intrusion Detection System**

The STARS Project Manager will be notified of any significant intrusion detection system activity within two hours.

An Intrusion Detection System (IDS) will be implemented inside each firewall access point on the trusted network. These systems will provide unobtrusive, continuous surveillance of the 100Mbps network. They will intercept and respond to known security breach tactics and network abuse before pertinent systems are compromised. Attack recognition, incident response, and intrusion prevention occur immediately, with full customization of signatures and response capabilities. Alarm and response capability includes sending SNMP traps, sending an email, logging events to the database, recording a complete session for playback and forensics, killing a connection, blocking a connection, suspending an account, or disabling an account. Each IDS sensor recognizes hundreds of signatures ranging from Denial of Service (DoS) Attacks, Probing, Service Exploits, etc.

The RealSecure™ Workgroup Manager, which will reside on the trusted network, provides central management for all of the Intrusion Detection Systems as well as a graphical reporting system that can produce a wide variety of predefined and customizable reports.

### **16a.1.2.21. Alarms and Reporting**

The following alarms will be provided and incorporated in the overall alarm system:

- System failure
- Identification of failed system
- Identification of failed sub-system or components
- Which system is in service
- Intrusion alert
- Type of intrusion (which trigger(s) has been activated)
- Time of intrusion
- Account under which the intrusion is reported
- Automated action(s) taken to deter intrusion (if any)
- Current status of intrusion and suspect account
- Firewall reporting
- Date and time of a connection
- User(s) connected
- Thru-put per user, department and agency (for user statistics and charges)
- Performance monitoring tools (automated)
- Set Thresholds – the administrator is expected to have the ability to change threshold limitations.
- Provide Alerts - notify administrators and users when a specified threshold has been reached.
- Provide real time network performance data.
- Show all views on one screen – allow the ability to compare their page fault rate with their disk I/Os, Memory CPU usage with total CPU usage, etc. without manipulating from screen to screen.
- Create reports, graphs and summaries of historical alarm events.
- Data is exportable to Microsoft standard formats.
- Server Alarms / Reporting
- Any unplanned status change including shifting from primary to hot standby.

Through the use of HP OpenView SNMP traps will be sent to the central console. Please see the following link for more information.

<http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps2118/index.html>

### **16a.1.2.22. Interconnection**

The intranet provides the infrastructure that connects mobile and stationary computer users at remote locations to the Division Offices, across N x 64kbps channels depending on the requirements of the site. These channels are carved out of T1 access circuits, which terminate in each remote location. The Division offices are connected to the Primary and Secondary Control Centers through 4T1s of channelized bandwidth that attaches to a 7200 series router.

Within the Control Centers, the router connects to a Cisco 6509 switch that supports connections to the enterprise servers, DNS servers, and the network management and monitoring devices. These switches also support the MDS PDGs and MDS Message Switches (see Mobile Data System section) and act as the interface to the intranet.

### **16a.1.2.23. Intranet Routers**

A variety of network router platforms have been selected to support the intranet infrastructure.

#### ***16a.1.2.23.1. 7206:***

The Cisco 7206 router was selected for use at the 7 Division Headquarters, VPS State HQ, and the Primary and Backup Control Centers. This router is a high performance Multifunction mid-range router in the Cisco Router product line. The Cisco 7206 Router has a 6 slot chassis and has a 1-Gbps midplane which is able to support up to 6 high-speed (greater than 45Mbps speeds) port adapters. The network processor selected is the NPE-400 that is capable delivering 400,000 packets per second (pps) of throughput. The port adapters that will be used are the Fast-Ethernet-TX/FX for 10/100 BaseT connections, Multichannel T1/E1 (w/ Integrated CSU/DSU), and the Multichannel STM-1.

The Multichannel T1/E1 port adapter is a T1 or Fractional T1 network interface. This adapter allows for the mapping of N x DS0 (64 kilobits per seconds (kbps)) per sub interface in the router. This allows for easy reconfiguration of an interface to increase the bandwidth.

The Multichannel STM-1 is designed to provide 256 channel groups to provision circuits down to the DS0 level. This allows for easy reconfiguration of an interface to increase the bandwidth.

#### ***16a.1.2.23.2. Cisco 3640:***

The Cisco 3640 router was selected for the Class I, Class II and Dispatch remote sites. This router is a mid-range small office router that provides approximately 50 to 70 thousand pps throughput. The chassis supports up to four network modules (i.e. Fast Ethernet, Serial).

#### ***16a.1.2.23.3. Cisco 1720***

The Cisco 1720 router was selected for the Land Mobile Radio (LMR), Microwave Only and Microwave Only with Data and the Radio Maintenance sites. This router is for small offices that require a maximum speed of T1 1.544 Megabits per second throughput. The chassis supports up to two network interface cards (i.e. Fast Ethernet, Serial).

#### **16a.1.2.24. Intranet Security**

The intranet as designed is a private network, and will be transported via the STARS microwave system in conjunction with approved leased services. This provides an inherent level of security for the network, however, in view of the sensitivity of data that could traverse the network, Motorola has designed the network with consideration for the extraordinary level of security required. All dial-up access points into the network are protected by two-factor authentication.

#### **16a.1.2.25. Firewalls - Cisco PIX®**

The PIX Firewall is an integrated hardware/software firewall appliance that will be implemented between each access point to the trusted Intranet and the rest of the untrusted networks. The PIX will be configured to take advantage of its connection-oriented adaptive security algorithm (ASA), to ensure that only IPSEC traffic destined for the VPN Gateway or SNMP traps destined for the internal network management system are allowed to enter the trusted network. The PIX is known for its performance, which can provide 500,000 simultaneous connections and nearly 1.7 Gigabits per second (Gbps) aggregate throughput. The PIX is built on a hardened operating system, which eliminates security risks associated with general purpose operating systems. The multiple PIX Firewalls in each of the divisions are easily managed with Microsoft's Internet Explorer web browser via the PIX Device Manager (PDM). The PDM provides a wide range of informative, real-time, and historical reports that give critical insight into usage trends, performance baselines, and security events.

The firewall will be sized to handle traffic for the defined class of use. All network traffic originating from outside the intranet (i.e. dial-up users) passes through a firewall. Both transport and network layer information is examined as packets access the firewall. The firewall requires secure access to adjust or change any parameter. The firewalls must be located in secured locations at each VSP Division Headquarters compound.

#### **16a.1.2.26. VPN Gateways - Cisco VPN Concentrator**

The Cisco VPN Gateway will be installed on each divisional intranet to provide high-performance IPSEC 3DES encryption and authentication capabilities for roaming users/technicians. Highly configurable VPN groups can allow for detailed individual restrictions and access or access can be easily generalized to many users with the Cisco Management GUI. The GUI also allows the administrator to see multiple levels of statistics like packets in/out and packets encrypted/decrypted. System logging capabilities provide tracking of user "login and logoff" specifics as well as other system and debugging information.

The Cisco VPN Gateway supports multiple client platforms, including Linux, Solaris, all versions of Windows and the Macintosh. The special NAT Transparency Mode allows users to securely connect to the Intranet from behind network translated addresses. The gateway and clients work in conjunction with the SecurID ACE/Server to provide two-factor authentication.

### **16a.1.2.27. Two-Factor Authentication - The RSA SecurID®/ACE System**

The SecurID/ACE System is supplied by RSA. The SecurID/ACE System ensures each user/technician who attempts to access the internal trusted network through the VPN gateway is "who they say they are." This is accomplished by enforcing strong two-factor authentication, which is something the user has, an ACE Authenticator Token, as well as something the user knows, a secret Personal Identification Number (PIN). The tokens are as simple to use as entering a password, but much more secure. Each end user/technician is assigned a unique token which generates a new, unpredictable code every 60 seconds. The user combines this number with a secret PIN to log into the division intranet sites. This method of authentication uses a unique 64-bit symmetric key in each token that is combined with an algorithm to generate this pseudo-random number (PRN). Only the RSA ACE/Server, which resides in the trusted network, knows which PRN is valid at that moment in time for that user/authenticator combination. The SecurID tokens are available in both hardware and software formats.

### **16a.1.2.28. CSS: Content Services Switches**

This product allows geographically disparate data centers to interconnect together globally. By mapping content requests to servers in multiple data centers regardless of their location, we are able to perform global redirection to mirrored sites, global load balancing, and localized personalization. The Cisco CSS 11xxx series switches improve reliability and response time by examining content requests in detail and directing them to the best site and best server at that moment, avoiding busy or overloaded sites and dynamically replicating "hot" content across the network. If one of the servers goes down then these switches will detect the fault and automatically route users to an alternative server where the content is held

### **16a.1.2.29. System Reliability**

Through the use of dynamic routing protocols and the design of a hierarchical network utilizing redundant hardware, the system is designed for the automatic rerouting of traffic and dynamic hardware fail over. Additionally within each of the backbone switches and routers, there is internal redundancy by way of dual power supplies and multiple processors.

### **16a.1.2.30. Interoperability**

Network Management products used within the intranet employ industry standard SNMP to communicate up/down status of network interfaces and queries Cisco's extended MIB to gather performance statistics.

### **16a.1.2.31. Revenue Capacity**

Through the use of IP accounting on selected network components Motorola will provide information on byte counts seen from each of the network interfaces. Through the use of firewall and ACE server logs, we will supply reports on total logged time on the system by user ID. Reports will be provided to the STARS Project Manager, which detail the total logged time on the system by user ID.

### **16a.1.2.32. Training and Support**

System Administrator training and support will be provided to Commonwealth of Virginia personnel. This training will be limited to the administrative aspects of the intranet hardware and system servers.

## **16a.2 Specifications**

### **16a.2.1. Baseline Equipment Specifications**

#### **16a.2.1.1. Message and Data Router**

The routers supplied in this implementation are sized to handle the traffic load specified in the “Class” classification section of this document, and will allow for growth as specified in the Expandability section of this document.

Physical access to routers will be subject to the security of the facilities in which they reside. Software access will be via multi level password process. Administration of user ID’s for access will be controlled by the Commonwealth.

Within the router the only configurable table that will be backed up will be the configuration file. As part of the standard maintenance process the configuration files will be stored and updated from Cisco Works Configuration Manager. At all times the configuration files for all routers and switches will be current on the Cisco Works tool. There will be a second copy of this tool in the network. Both WAN Configuration Management servers will be behind the firewall.

#### **16a.2.1.2. Cabling**

Cabling will meet the requirements of the National Electrical Code and applicable local building codes. Where cable is run in a plenum, the cable will meet NFPA requirements for plenum grade cable. All data Category 5 cabling will meet EIA/TIA specifications for Category 5 – rated to 100 MHz.

### **16a.2.2. Fixed End Equipment and Software**

#### **16a.2.2.1. Servers**

The Servers provided are implemented for the Repository DB, Systems / Network Management, DNS, Web and Backup systems.

#### **16a.2.2.2. Suppression**

Motorola has not provided individual surge protection for the servers but has included Type 1 surge protection for all equipment loads at the SPHQ Primary Control Site and SPHQ Backup Control Site.

### **16a.2.2.3. Uninterruptible Power Supply**

Each server installation shall be provided with an uninterruptible power supply (UPS). The UPS provides power in the event that site power is lost.

- In the event that normal AC power is unavailable for longer than 30 minutes, the UPS will initiate automatic shutdown of the associated network servers.

Motorola has included UPS backup of the power for the entire building (SPHQ Primary Control Site) as described in the Facilities Section of this document. The servers will be fed from this UPS power source to provide protection from loss of power.

### **16a.2.2.4. Network Attached Storage (NAS)**

Two fully redundant network attached storage devices will be provided at the SPHQ. These devices will provide 10 Terabytes (TB) of combined network addressable storage volume (5 TB at SPHQ Primary Control Center and 5 TB at SPHQ Backup Control Center).

The Sun StorEdge T3 fiber-to-fiber architecture provides the basis for a modular network storage concept. The array's design includes hardware RAID controller technology, hot-swap/redundant components and industry-standard Fiber Channel technology. The design provides redundant disk arrays (RAID-5) with each of the database/storage servers.

- Each T3 Rack → (8) T3 Units
- Each T3 Unit → (9) Disk Drives
- Thus, Each Rack → (8)\*(9)\*36GB → 2.52 TB RAW

Two (2) T3 Racks will be set up at the Primary Center and two (2) T3 Racks at the Backup Center (co-located at SPHQ), each site providing a storage capacity of 5.04TB Raw (or 5.0TB RAID-5).

### **16a.2.3. Cutover Plan (Summary Outline)**

Motorola has developed a cutover plan for the orderly overall transfer of the Intranet fixed equipment. This plan will provide for the minimal disruption of essential network services.

Motorola will deploy the wide area network and install servers in accordance with the project schedule detailed in the System Integration section of this document. Meshed network design insulates users from impact of Microwave circuit re-provisioning

Migration from the SPHQ Backup Control Center to the SPHQ Primary Control Center will proceed in the following order:

- SPHQ Backup Control Center brought online
- All locations terminate into SPHQ Backup Control Center router as they come online
- SPHQ Primary Control Center brought online and connected to backup
- Perform connectivity verification
- Outages due to Microwave provisioning will be mitigated by Microwave migration plan.
- Microwave circuits will be re-provisioned
- Identify those circuits that will terminate at Primary Site
- Those circuits which terminate in Primary site will be remapped to the SPHQ Primary Control Center router.
- Move the applicable configurations from the SPHQ Backup Control Center router to the primary router. Test and validate the circuit. Activate the path.

### **16a.2.4. Document**

Included in this document is the following information.

- System block diagram, with connection options available commercially and dedicated the Commonwealth circuits
- Description of operation
- Demonstration of how the system meets % utilization and collision rate numbers
- The implementation and migration plan
- List of equipment, including the server(s)
- Manufacturer guaranteed specifications for each major component
- List all equipment hardware and software
- List the anticipated Intranet performance metrics
- A complete description of the security design, including means to assure transmission security, prevention of external and internal unauthorized access and unauthorized use by otherwise authorized individuals.
- Documentation of the qualification(s) of the network development, maintenance and installation personnel

- Description of the training and technical support to be provided and the period over which this support will be provided
- Description of the measures anticipated for electrical protection including surge suppression and uninterruptible power supplies.
- Description of the means to assure back-ups are made.
- Basic Cutover Plan.

Refer to Appendix 4 for site details

THIS PAGE LEFT BLANK INTENTIONALLY