

5. One-VA Enterprise Architecture – The Designer’s and Builder’s Views: Distributed Systems Architecture

This chapter defines the logical and physical distributed systems architecture of the target One-VA Enterprise Architecture from a top-level perspective. From that top-level view the next level of detail is defined for both the baseline and target distributed systems architecture of key elements of the One-VA EA. These elements include the Telecommunications, Cyber Security and Data Processing Center infrastructure components of the One-VA EA along with applications components aimed at line of business capabilities.

This chapter presents the combined views of the designer and builder of rows 3 and 4 of the Zachman Framework. Row 3 of the Zachman Framework is titled Designer. It describes VA’s enterprise-wide logical information systems from the perspective of individual VA PMs. It is constrained by VA line and staff managers’ views in Row 2, driven by VA’s Information Technology Board (ITB), and integrated by the VA Chief Enterprise Architect as the steward of rows 1 and 2. In completing row 3 of the Framework, VA will identify and prioritize candidate projects from the Secretary’s Strategic Plan and the Under Secretaries’ and Assistant Secretaries’ Business Plans as expressed in the Information Technology Board’s Plan. High-priority projects will be selected for initiation in FY 2004. These projects will be developed through Milestone’s 0 and 1 of the Capital Planning Process. Only artifacts necessary to address these milestones will be required at this stage. The project manager in consultation with the Chief Enterprise Architect will keep them integrated and consistent with business needs. These artifacts will define detailed functional and technical requirements baselines.

Row 4 of the Zachman Framework is titled Builder. It describes VA’s information systems from the perspective of Information Technology and is the responsibility of the VA PMs. It is constrained by the VA PMs’ detailed functional and technical requirements baselines view and driven by industry “best-practices” as documented in the VA TRM and Standards Profile. VA PMs will initiate the development of artifacts in row 4 in the form of a technical design baseline in preparation for Milestone 2 and complete them for Milestone 3.

This section covers the combined views of the designer and builder of rows 3 and 4 of the Zachman Framework.

5.1 Overview

The Secretary’s Strategic Plan is the key driver for the One-VA Enterprise Architecture. As the Secretary’s strategic goals drive the business model presented in sections 3 and 4, his enabling goal (E-1) is the key driver for this section, Distributed System Architecture.

VA Goal 5 (E-1): Provide One-VA world-class service to veterans and their families through the effective management of people, technology, processes, and financial resources.

The CIO’s Information Technology goals that follow ensure that the Secretary’s goals, especially the enabling goal, will be supported with innovative, disciplined and practical application of information technology.

- IT Goal 1:** Implement One-VA Enterprise Architecture.
IT Goal 2: Implement a One-VA data network.
IT Goal 3: Secure the One-VA enterprise against Cyber Attack.
IT Goal 4: Establish a disciplined, non-bureaucratic project management structure.
IT Goal 5: Establish effective metrics to measure performance.
IT Goal 6: Implement an effective Command and Control, COOP and COG infrastructure.
IT Goal 7: Shape the VA IT workforce to support the target One-VA EA.

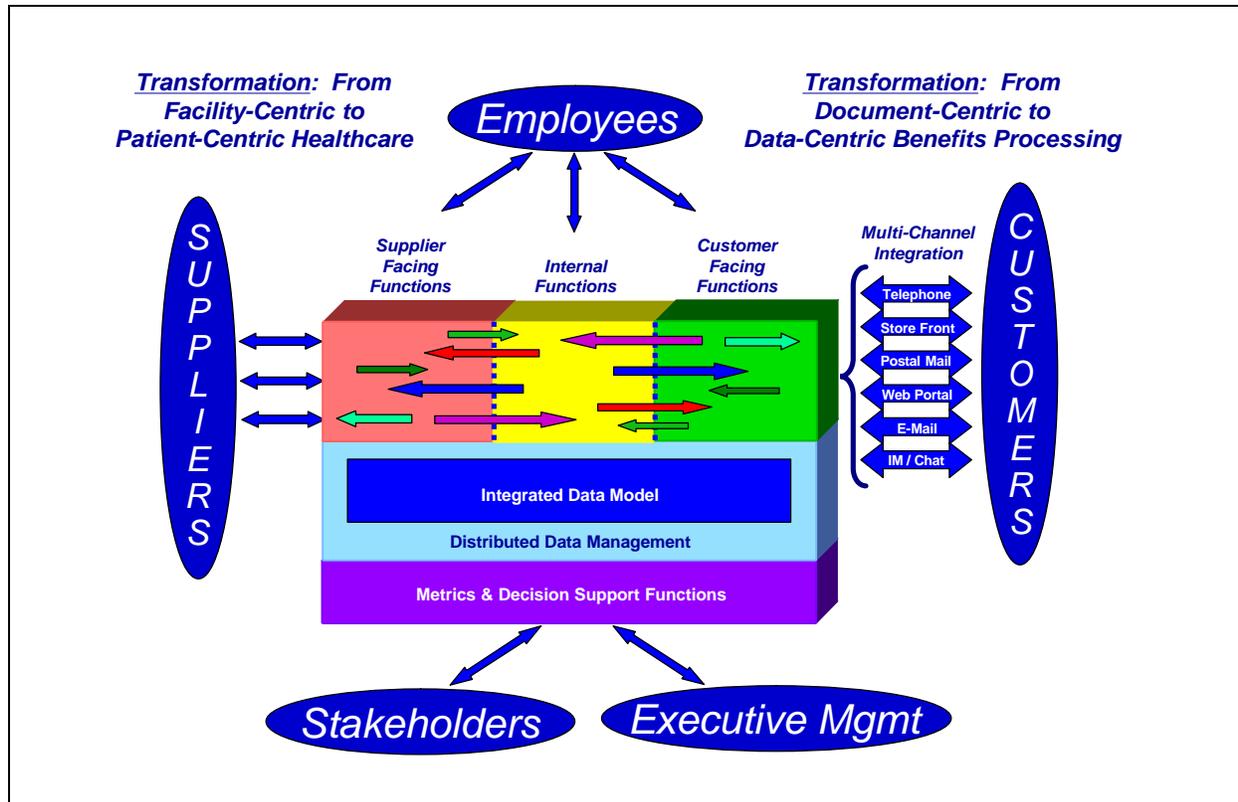


Figure 5.1 Logical model for the applications layer of the target One-VA Enterprise Architecture.

Figure 5.1 presents a logical view of the applications layer model for the target One-VA EA. Maintaining a Veteran-focused perspective requires a fundamental level of integration across business lines when it comes to both processes and corporate data. At the core of the logical model of Figure 5.1 therefore is an integrated data model aimed at catalyzing Veteran-centered integration of corporate information. Since the Department is national in scale and supports a population of over 26 million Veterans, a robust distributed data management capability is required to maintain synchronization of the corporate information across the enterprise and to manage concurrency issues. Front office and back office functions are organized into customer facing functions, internal functions (to include Enterprise Resource Planning (ERP) and vertical line of business specific functions), and supplier facing functions. While these functions are depicted in Figure 5.1 with distinct boundaries, the reality is that the boundaries are soft boundaries. The focus of this One-VA EA is on processes integration and data integration to

maintain a Veteran-focused perspective. In general, the processes across the Department will span the regions of customer facing, internal and supplier facing functions as depicted by the arrows spanning these regions. Particularly when dealing with Veteran customers, it is also important to integrate across all available channels of communications to include postal mail, traditional storefront operations, telephone call center, the Internet and the World Wide Web, and even electronic messaging. Additionally, metrics and decision support functions support executive management and stakeholders.

The One-VA to-be vision is to focus on delivery of services to the veteran. This requires that VA move from facility-centric to patient-centric healthcare and from document-centric to data-centric benefit delivery.

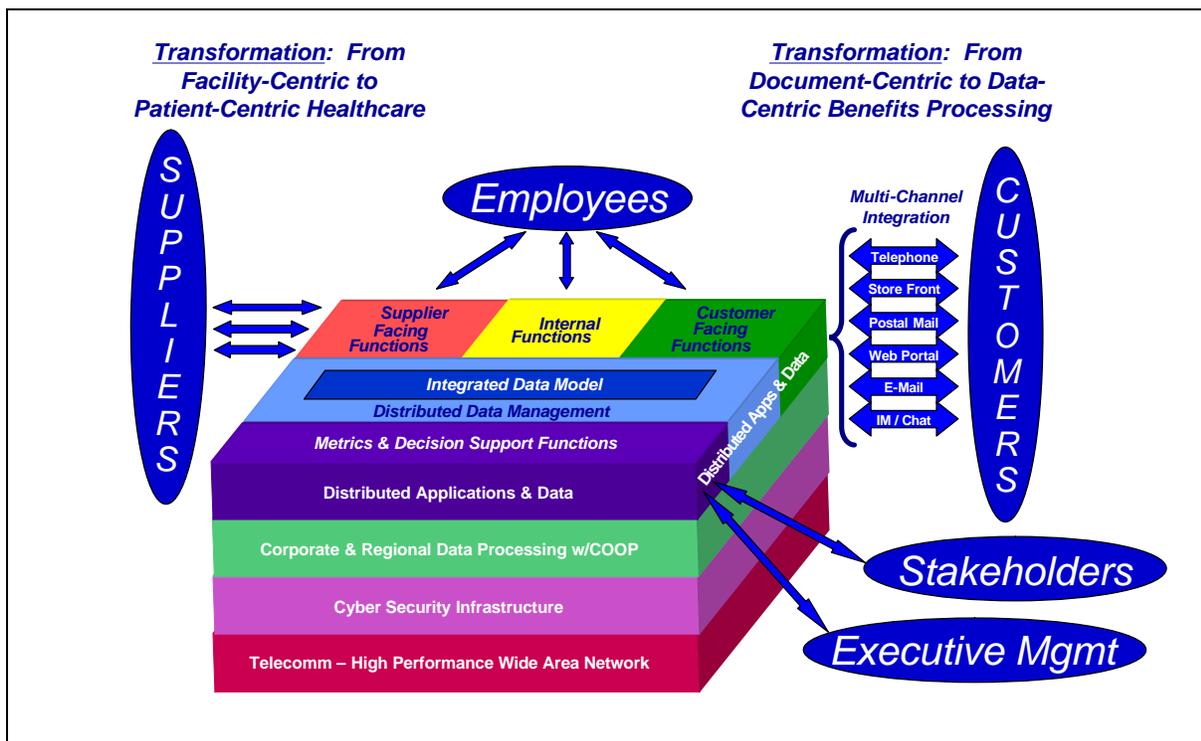


Figure 5.2 Logical model for the overall target One-VA Enterprise Architecture.

The applications layer logical model presented in Figure 5.1 does not stand alone. Below this applications layer, other infrastructure is required to enable it on a national scale across a large organization. Figure 5.2 depicts the distributed infrastructure that supports the target architecture at the applications layer. The primary elements of infrastructure as presented in Figure 5.2 are as follows:

Telecommunications Infrastructure: Voice, video and data telecommunications infrastructure to support distributed operations and integrated processes and corporate information.

Cyber Security Infrastructure: Information Assurance (IA) infrastructure and capabilities to secure the enterprise from both external and internal attack.

Corporate and Regional Data Centers with Continuity Of Operations (COOP):

Corporate processing support the applications layer model depicted in Figure 5.1 with inherent capability to electronically vault information and support business continuity in the face of natural or man made disasters. Additionally, regional processing centers support office automation and line of business specific capabilities.

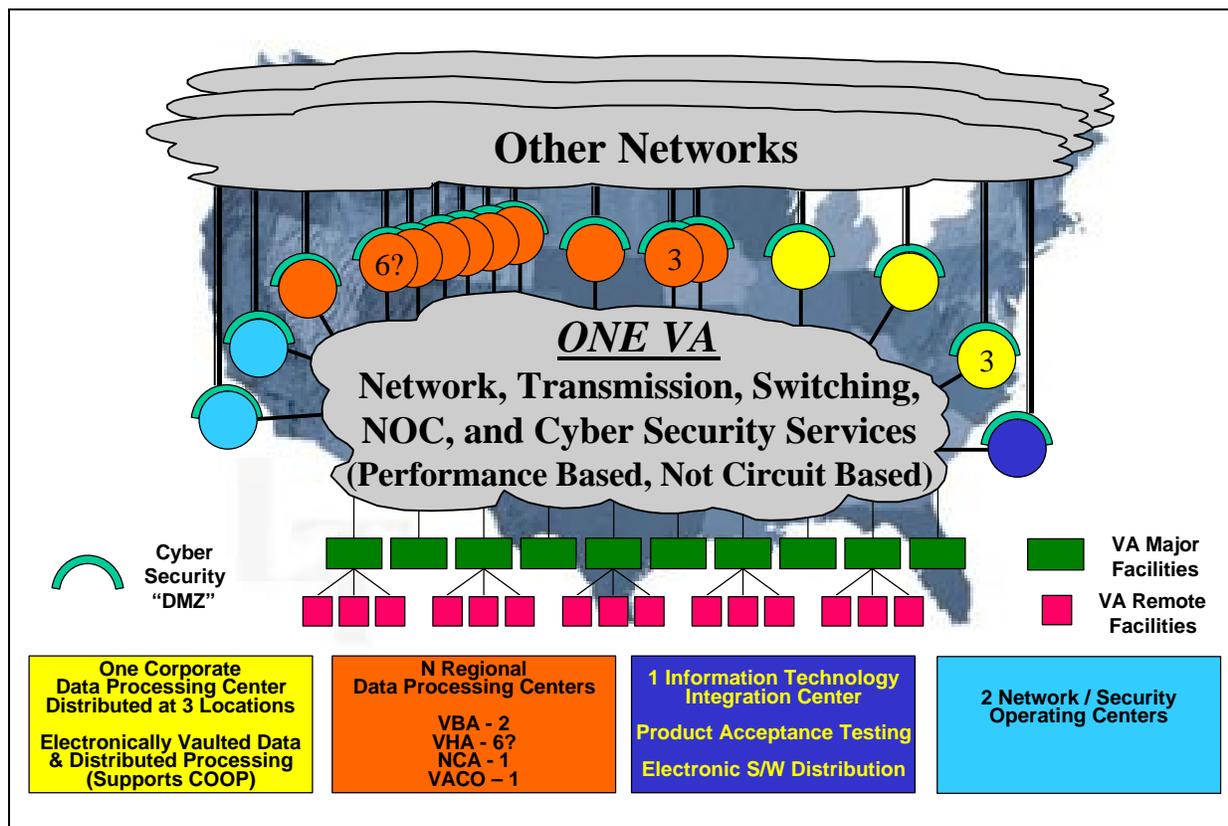


Figure 5.3 The physical architecture model for the target One-VA Enterprise Architecture.

Figure 5.3 presents a physical perspective for this very same One-VA EA. At the core of the illustration is the One-VA telecommunications network to interconnect all major facilities across the Department, and a primary and secondary Network Operations Center (NOC) to provide 24 hour monitoring and operations of the network. It also depicts the Corporate Data Centers and Regional Data Centers that support the integrated corporate information and processes as well as line of business specific processing and office automation. Next the Cyber Security perimeter defense mechanisms and gateways to the Internet and other networks are depicted at the Corporate and Regional Data Centers along with a primary and secondary Security Operations Center to provide 24 hour monitoring of perimeter and internal boundary protections and intrusion detection sensors and to react in real time to incidents. Figure 5.3 also depicts a future Information Technology Integration Center (ITIC) to support integration, test and evaluation, and Cyber Security certification and accreditation processes.

The following sections provide the next level of detail for the elements of the logical and physical models depicted above from both the baseline (as-is) and target (to-be) perspective. Section 5.2 presents the telecommunications infrastructure for the One-VA data network. Section 5.3 presents the Cyber Security infrastructure. Section 5.4 presents the corporate and regional data center infrastructure and inherent COOP capabilities. Finally Section 5.5 presents the applications layer.

5.2 Telecommunications Data Network Infrastructure

A robust, high performance, cost effective and assured telecommunications infrastructure is key to achieving the target One-VA EA and meeting strategic objectives across the Department. This section describes the baseline and target architectures for the telecommunications infrastructure.

5.2.1 Baseline VA Data Network Telecommunications Infrastructure

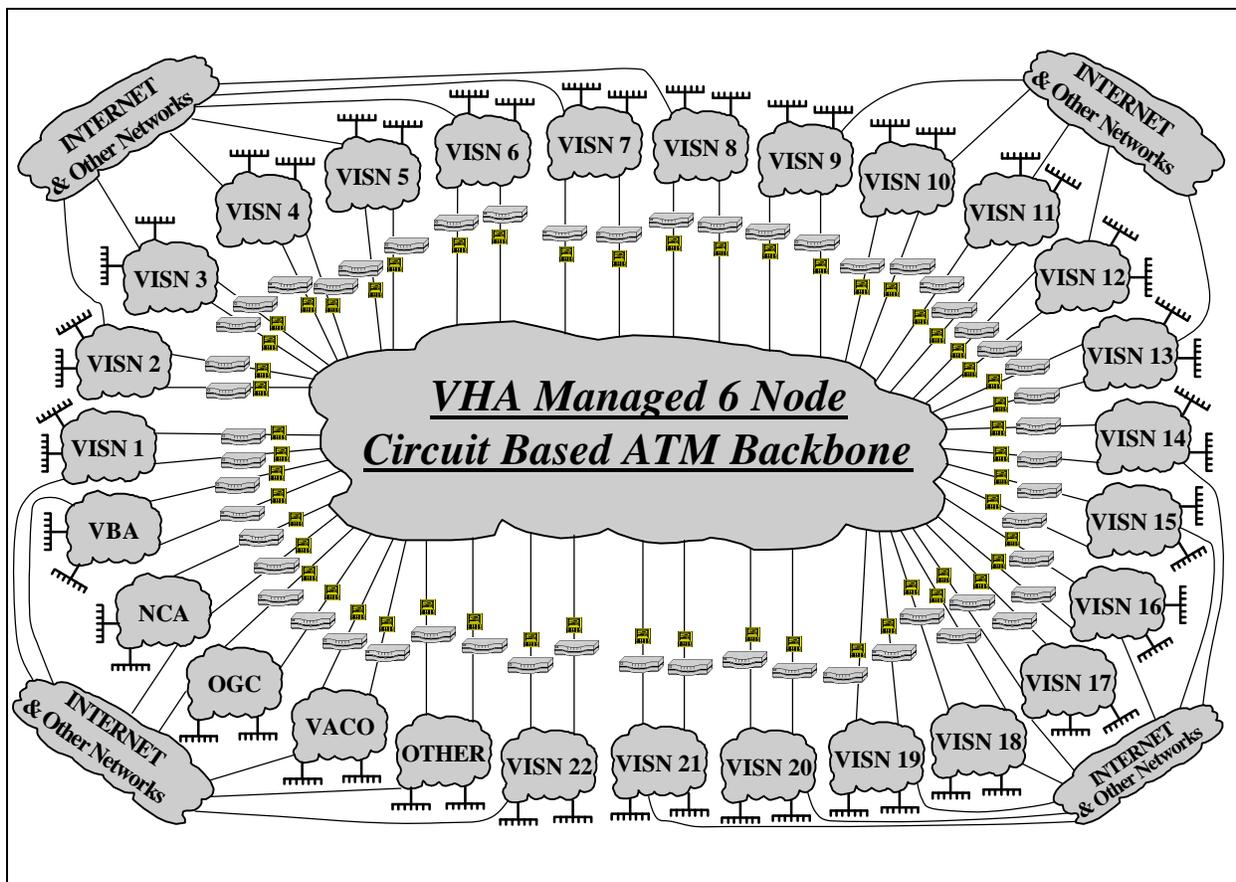


Figure 5.4 Baseline telecommunications data network architecture across existing VA networks.

VA's as-is data network environment is a loose federation of independently owned and operated data networks. Each of these independent networks is also product based and consists of leased circuits, procured switchgear and other equipment, and third party contract management and operations services. VHA manages a six node circuit-based ATM backbone on behalf of all of VA as an interconnection service. This is illustrated in Figure 5.4. As can be seen in the figure,

there are twenty-two different VHA Veterans Integrated Service Networks (VISNs) deployed on a regional basis connected to the ATM backbone via routers. There are also separate networks for VBA, NCA, VACO, OGC and multiple other organizational, regional or functionally focused independent networks. Overall there are a total of more than 30 independent, separately managed and operated data networks across the Department. Each of these regional, organizational or functionally focused networks then services local area networks (LANs) and campus networks at major and remote facilities across the Department. These networks evolved independently over time so that they are now a costly life cycle support issue for the Department. Additionally, there is no Department-wide perspective for end-to-end performance of this loose federation of independent networks or for visibility into the current state of the networks.

Figure 5.4 also illustrates the plethora of backside interconnections on a local or regional basis to external data networks such as the worldwide Internet or other data networks. This environment is problematic at best from a cyber security perspective. It is shown here for completeness. Further discussion of the cyber security architecture and environment is provided in Section 5.4.

5.2.2 Target VA Data Network Telecommunications Infrastructure

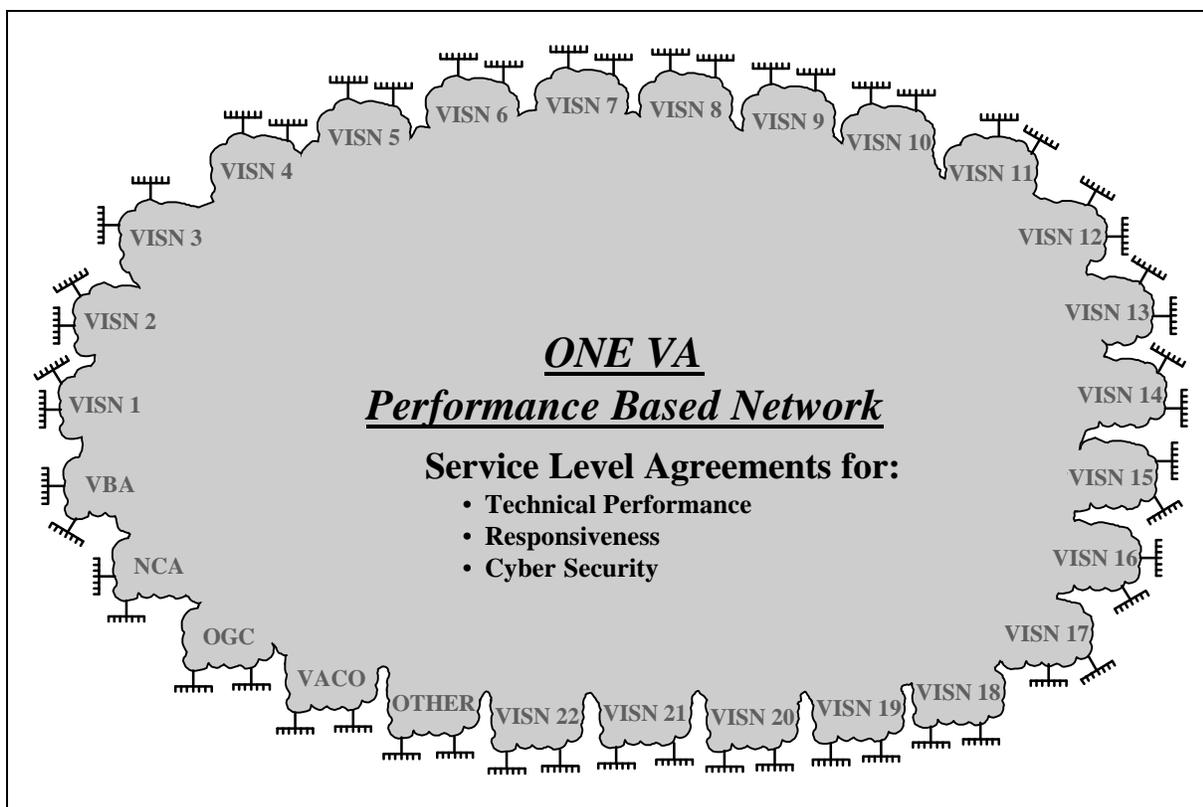


Figure 5.5 Target One-VA performance based telecommunications data network architecture.

The target architecture for the One-VA telecommunications data network infrastructure is a fundamental shift from the baseline architecture depicted in Figure 5.4. Figure 5.5 illustrates the potential target architecture for the Department as an integrated, performance based service with

service delivery points at all major facilities instead of a loose federation of independently owned and operated regionally, organizationally or functionally focused networks. (This is referred to as the “potential” architecture only to reflect the fact that in some geographic regions the nature of the telecommunications market and / or the disposition of VA facilities may result in a decision to retain some element of a regional network and move the service delivery points to the edge of that regional network instead of to the facility or campus level.) The objective of this architectural model is to buy a service from the telecommunications service provider on an end-to-end basis and to specify that service in terms of Service Level Agreements (SLAs) for technical performance, responsiveness (to both routine change orders and emergent incidents or service disruptions) and Cyber Security assurance.

The Telecommunications Modernization Project (TMP) has been established in VA to evolve the Department’s data network infrastructure from the baseline state of Figure 5.4 to the target state of Figure 5.5. TMP has developed a four phase strategy for accomplishing that evolution beginning with the VHA core network depicted in Figure 5.4 and proceeding outward to the over 30 attached regional, organizational or functional networks. Phase one transfers functional responsibility for the operation of the core network from the VHA to the telecommunications service provider. Phases two and three optimize the core network to serve the Department wide data network load. Phase four evolves to a service-based model for procurement of the telecommunications service and to SLAs to specify performance on an end-to-end basis across all service delivery points. Phase four then also extends the core network outwards wherever appropriate moving the SDPs outward to individual major facilities or campuses as depicted in the top level physical infrastructure of Figure 5.3. The TMP project is currently executing this strategy.

While the focus of the discussion surrounding the target or “To Be” network architecture has focused on data since it is the near term most significant effort, this is not to imply an exclusive focus on data only. As this integrated network infrastructure evolves it is a natural evolution to expand service delivery capability to include a converged set of voice and video services. Indeed, even in the early phases of TMP, planning for toll bypass is underway to route long distance telephone calls that both originate and terminate within the Department over the WAN as an alternative to commercial long distance. The strategically most significant near term element of telecommunications modernization however is an integrated, high performance, low cost assured wide area data network as a mandatory infrastructure enabler for other integration and convergence efforts.

5.3 Cyber Security Infrastructure

Securing the enterprise against either external or internal cyber attack is key to achieving the target One-VA EA and meeting strategic objectives across the Department. This section describes the baseline and target distributed systems architectures for major elements of the One-VA Enterprise Cyber Security infrastructure.

5.3.1 Baseline VA Cyber Security Infrastructure and Environment

During the earlier discussion of the baseline telecommunications data network infrastructure accompanying Figure 5.4, the subject of the cyber security environment and infrastructure first arose. Figure 5.6 is another depiction of the cyber security environment within the context of the target physical architecture drawing of Figure 5.3. In today’s baseline environment, in excess of

200 documented gateways to external networks exist on a local, regional and national basis. In all likelihood, other undocumented gateways exist as well. Beyond network gateways, over 2,000 Remote Access Service (RAS) access points also exist to support dial up access by a large group of users. The sheer number of access points in terms of RAS services and network gateways is a cause for concern in first defining the enterprise network perimeter, second securing the enterprise network perimeter, third monitoring the enterprise for indications of intrusion or misuse, and fourth reacting to detections of intrusion or misuse. Reacting in real time requires enterprise wide real time cyber security situation awareness. Real time cyber security awareness requires in turn a uniform deployment of robust intrusion detection sensors, a real time monitoring capability and a command and control structure; all targets for implementation on a 24 hour a day basis in a Security Operations Center (SOC). None of these attributes or capabilities exist in the baseline cyber security architecture and environment depicted in Figure 5.6.

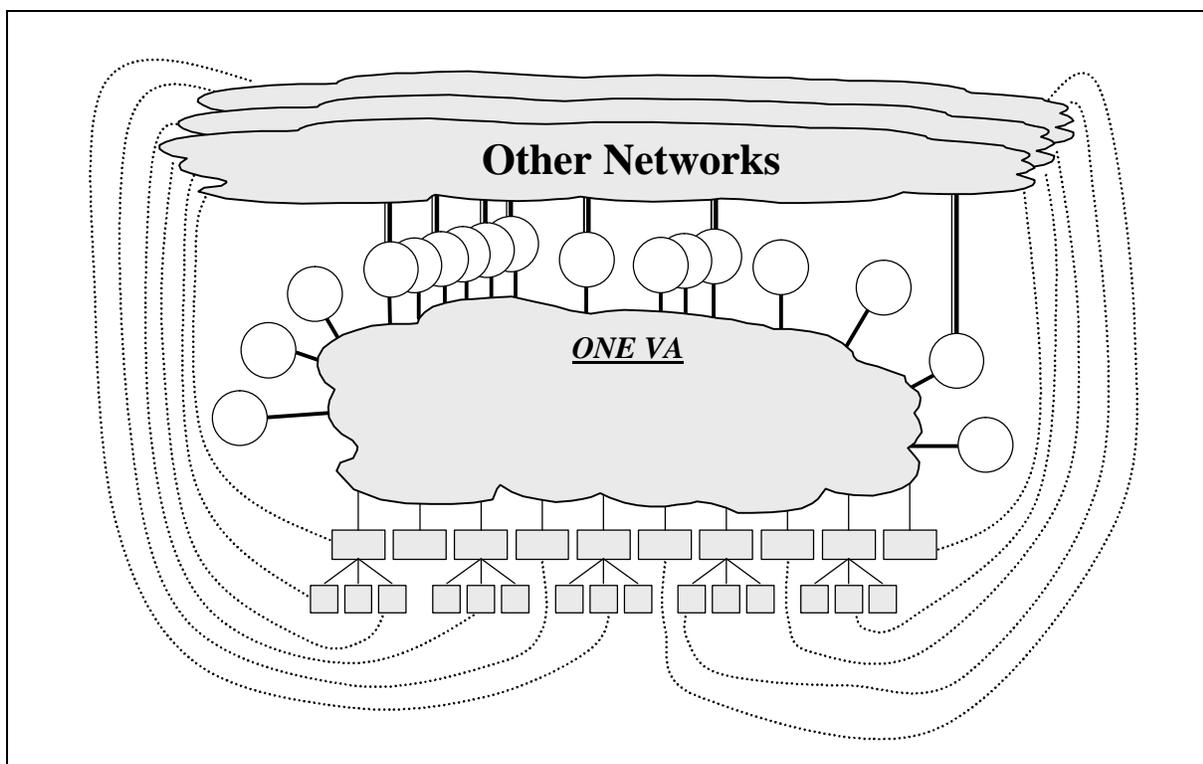


Figure 5.6 Baseline cyber security infrastructure and environment across the Department.

5.3.2 Target VA Cyber Security Infrastructure and Environment

The target cyber security architecture and environment is depicted in Figure 5.7. It shows the establishment of a controlled and modest number of high performance gateways to external networks at the Corporate Data Centers, and, if required, at Regional Data Centers, and the elimination of back side local gateways. These controlled corporate and regional gateways will implement uniform and robust perimeter defenses, and both host based and network based Intrusion Detection Systems (IDSs). Figure 5.7 also depicts the establishment of a 24 hour Security Operations Center (SOC) to monitor and control the cyber security infrastructure across the enterprise, to maintain a real time situation awareness of the cyber security posture of the

enterprise and to react in real time to detections of intrusion or misuse. In establishing this real time capability, the SOC will obtain a feed from the NOC of the network level current status across the enterprise to ensure the ability to segregate outages caused by physical or logical network failures from those that may be caused by a cyber security intrusion or denial of service attack.

The “De-Militarized Zones” (DMZs) established to control and monitor traffic entering or leaving the network are depicted in Figure 5.8. As can be seen from this illustration, the corporate or regional data centers will be segregated into multiple regions to host externally facing functions and internally facing functions and corporate data respectively. Figure 5.8 also presents the establishment of consolidated RAS services at these corporate and regional data centers to consolidate, monitor and control all remote access to the enterprise, and to provide Virtual Private Network services. These VPN services will be employed to enable RAS services across external networks by enabling a cryptographic tunnel from a remote client to the corporate intranet at gateway location, or also to enable trusted interface channels with external organizations such as other governmental entities (e.g. the Department of Defense, the Internal Revenue Service, the Social Security Administration) or with suppliers in a Supply Chain Management (SCM) environment.

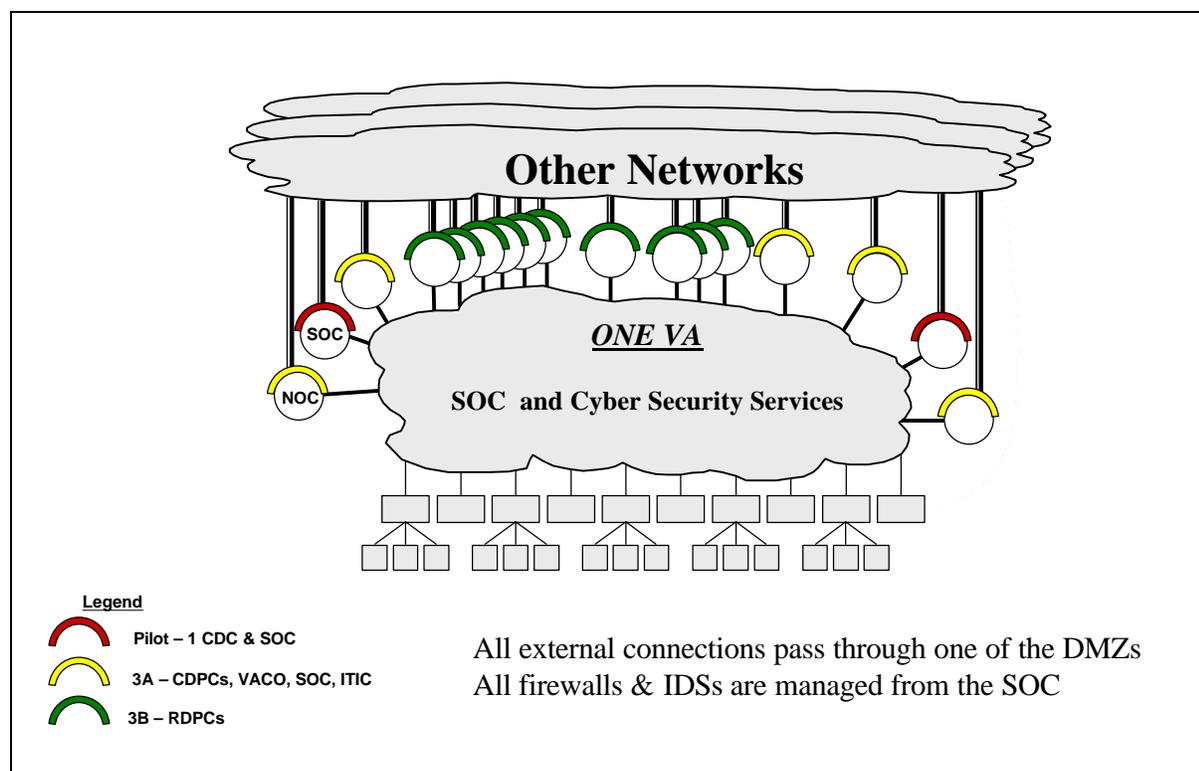


Figure 5.7 Target cyber security infrastructure and environment across the Department.

The Enterprise Cyber Security Infrastructure Project (ECSIP) has been established to implement the target cyber security infrastructure and environment across the enterprise depicted in Figure 5.7. ECSIP has established a strategy for evolution from the baseline state of Figure 5.6 to the target state of Figure 5.7. Elements of that strategy are depicted in Figure 5.7. The strategy

includes piloting an enterprise gateway at a single corporate data center location (Austin, TX.) and piloting the SOC (at the VA facility at Martinsburg W.Va.). This effort will not only prove feasibility but validate the scalability and network performance necessary to support such an approach. In the second phase (labeled by the Milestone 3A limited deployment decision point in Figure 5.7) the validated gateway design will be implemented at the remaining two corporate data center locations (Philadelphia Pa. and the Hines facility in Chicago Il.), along with the backup SOC (location TBD), and potentially at the Information Technology Integration Center and if required at the SOCs themselves. As the pilot and limited deployment of corporate gateway capability is executed, backside gateways on a local and regional basis will be taken down¹ and their traffic rerouted over the intranet to use the corporate gateways. An assessment will be made at that time if additional gateways at regional data centers are required and if so, the project will proceed into a full deployment phase identified by the Milestone 3B decision point in Figure 5.7. ECISP is currently executing this strategy.

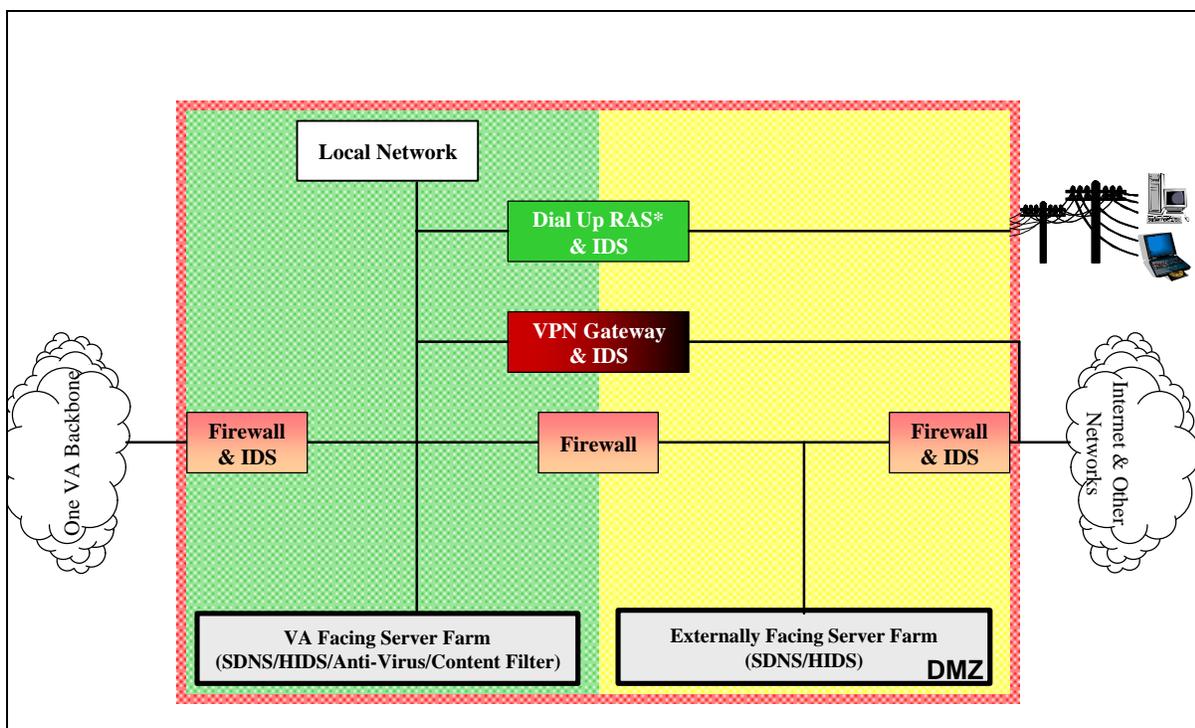


Figure 5.8 Target cyber security architecture for all external network gateway locations and DMZs at either corporate or regional data center locations.

5.4 Corporate and Regional Data Center with COOP Infrastructure

Providing a robust corporate data center environment to host the production environment for the applications layer depicted in Figure 5.1 is key to achieving the target One-VA EA and meeting strategic objectives across the Department. This capability must also inherently provide a data replication capability to support business continuity planning in the face of natural or man made

¹ It is recognized that mission requirements may necessitate the retention of select local gateways to external networks. Any such retained local gateway will require a waiver. It also must conform to the design and implementation established by ECISP, and be centrally monitored and controlled from the SOC.

disasters, and COOP. This section describes the baseline and target distributed systems architectures for major elements of the One-VA Corporate Data Center infrastructure.

5.4.1 Baseline VA Corporate Data Center with COOP Infrastructure

Currently, VA operates a single corporate data center at the Austin Automation Center located in Austin TX. (Other major data centers also exist at Hines and at Philadelphia, but these are administration resources today and not corporate resources.) AAC is an extraordinarily robust production environment supporting many of the lines of business and EBFs and KEFs across the Department. COOP capability is currently provided through an outsourced service. To enable COOP capability incremental daily backups and weekly full backups are made to tape and physically trucked offsite to a secure storage facility remote from the AAC. In the event of an actual disaster, the tapes are to be retrieved, and flown along with AAC staff personnel to a remote site where the outsourced service is hosted and the AAC capability reconstituted on a 72-hour basis or longer.

The tragedy of September 11, 2001 has caused VA to fundamentally rethink its business continuity planning and COOP services, calling into question several elements of the current strategy. Availability of air travel can no longer be assumed. Likewise, availability of trained and experienced personnel to relocate from AAC to the outsourced site can no longer be assumed. Finally, the requirement for restoration of the business processes, currently set at 72 hours for mission critical processes and functions, has been found by the Department Inspector General (IG) to be inadequate and is being re-evaluated.

5.4.2 Target VA Corporate Data Center with COOP Infrastructure

To address business continuity planning and COOP in the post September 11, 2001 environment, VA has decided to establish a single corporate data center distributed across three physical locations; Austin, Hines and Philadelphia. Detachments of AAC are being established collocated with the VBA regional processing centers at Hines and Philadelphia, and allocations of functions and supporting infrastructure are being reassessed. Establishing this capability as a single organizational unit, physically distributed, provides a single management structure and a single responsible and accountable individual to execute the corporate business continuity strategy and COOP.

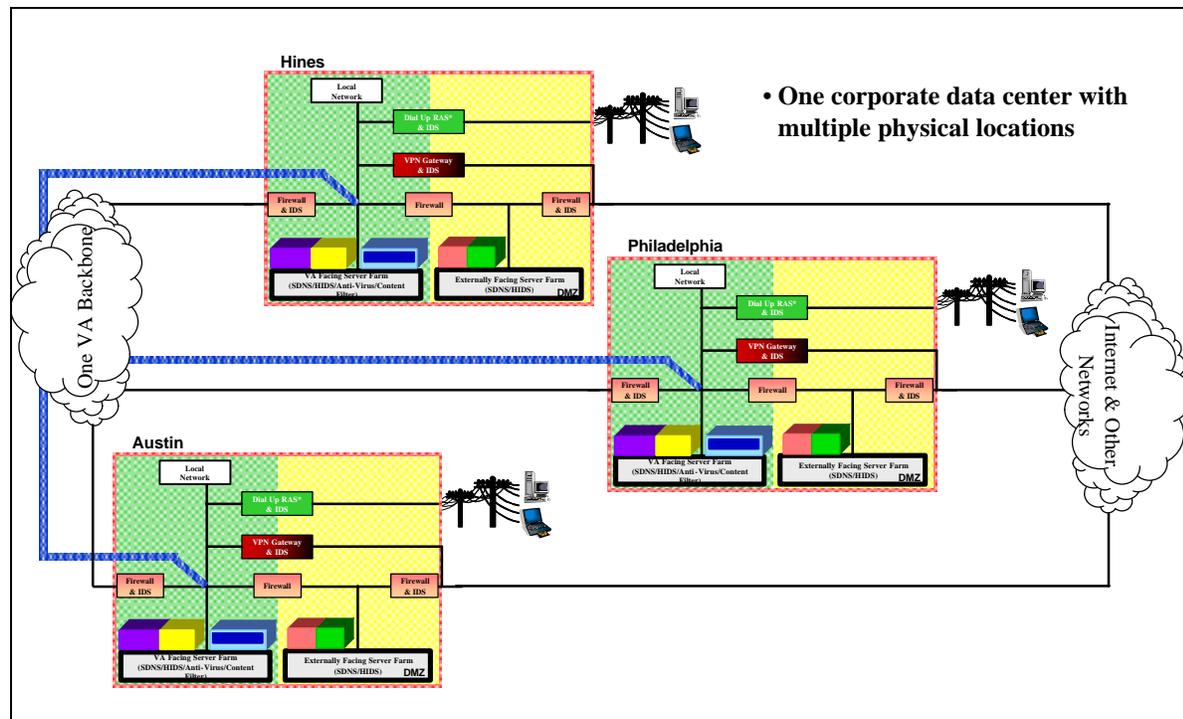


Figure 5.9 Target corporate data center architecture with inherent COOP capability.

From a distributed systems architecture perspective this strategy is depicted in Figure 5.9. The Figure shows the security architecture for the corporate data centers being established by the ECSIP project and superimposes elements from the logical model of the applications layer of Figure 5.1 over the internal and external facing regions of the DMZ. Beyond presenting a single organizational and management structure, it is also important that these three distributed installations appear logically as a single corporate data center. To enable that appearance as a single logical entity, Figure 5.9 depicts a high-speed IP interconnection of the three facilities behind the firewall; basically an extension of the LANs of the three facilities into a single logical extended LAN environment. This interconnection, while provided through the corporate intranet, is unique from all other interconnection services provided by the intranet due to its private connectivity nature, and to its high performance requirements. This logical extension of the LAN at the three widely distributed physical facilities enables electronic vaulting of corporate information in support of applications restart and business process restart after a disaster. It also enables other capabilities such as workload sharing, essential to providing an experienced and trained workforce at each location capable of assuming the production burden in the event of a natural or manmade disaster.

The Corporate Data Center Integration Project is currently being established to execute the integration of a single corporate data center distributed across three locations and the COOP capability described above. It is targeted at a FY 2003 implementation.

5.4.3 Baseline VA Regional Data Center Infrastructure

With few exceptions, VA does not currently employ regional data centers in its distributed systems architecture. The notable exceptions are the VBA centers at Hines and Philadelphia and

the NCA center at Quantico VA. Even with those exceptions, all VBA office automation support, and support for line of business vertical applications is currently provided on a strictly local basis at each of the 57 Regional Offices (ROs) operated by VBA. Likewise within the VHA infrastructure, analogous services are operated locally at 150 hospital locations and to a smaller scale (without local instances of the VistA healthcare applications) at other sites of care as well. Only NCA operates a regional data center model with centralized support for office automation and line of business vertical applications. The general environment with both office automation and line of business or administration specific applications is depicted in Figure 5.10.

Figure 5.10 shows that common services such as mail, file, web and print services, together with administration specific applications, LAN administration and desktop administration are performed locally at a large number of locations across the Department. It also shows the use of administration unique data networks and not the One-VA corporate intranet for data transport services. (Transition to the One-VA corporate data network architecture was addressed previously in Section 5.2.) This environment is problematic from multiple perspectives. It is inefficient from the perspective of hardware resources and software licenses, particularly for server environments. It demands a high skill mix of the local workforce to accomplish not only LAN administration but also system administration and desktop administration. It increases the demands places on local Information Security Officers (ISOs) to properly administer the security requirements for certification and administration of IT systems. Finally, it increases the likelihood of local errors in system administration of the servers and desktops and therefore increases the overall risk level across the Department.

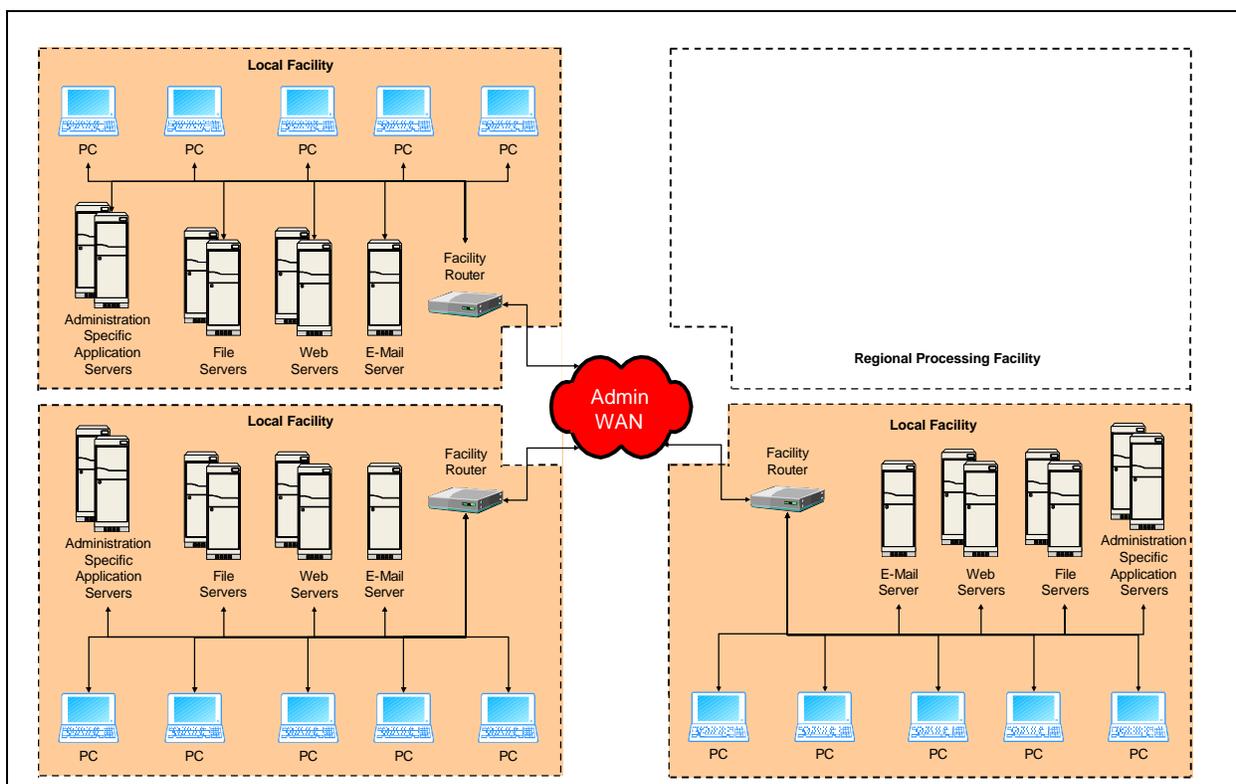


Figure 5.10 Baseline regional data center architecture.

5.4.4 Target VA Regional Data Center Infrastructure

To deal with the issues cited in Section 5.4.3 above, VA is formulating a regional data center initiative. Whereas the corporate data center will focus attention primarily on corporate applications production processing, the regional data centers will focus primarily on office automation services and administration or line of business unique production processing best served by a regional infrastructure model. One of the objectives of the regional data center initiative is to remove server infrastructure from local facilities wherever possible and appropriate and consolidate it at regional processing facilities. Where not possible or appropriate to remove server infrastructure from local facilities, this initiative seeks to remotely manage server assets that remain local. Finally, this initiative seeks to remotely manage local desktops retaining onsite (level three) help desk support locally. In order to successfully achieve the regionalization of server assets, several conditions must be met. Clear and realistic performance requirements on an end-to-end basis must be established for the application in question (including the provision of local contingency backup mechanisms in the event of WAN failure if required). Service Level Agreements (SLAs) must be established to define the agreed to level of service. An appropriate regionalization construct must be established for major applications to determine the appropriate number and distribution of regional processing centers. Finally, the regionalization must be able to demonstrate FTEE and cost savings. It is recognized that even with these criteria met, there may be mitigating factors such as critical mission resilience or the manner in which some legacy applications were built that may prevent regionalization of server infrastructure. Decisions to regionalize, retain as local but manage remotely, or retain as local with local management (Status quo) will be made on an application by application basis with due consideration of mission requirements including availability.

A notional distributed systems architecture for this approach is depicted in Figure 5.11, which shows servers supporting both office automation functions as well as administration specific applications in the regional data centers vice the local facilities. It is referred to as a notional architecture since the extent of the ability to remotely serve administration specific applications in both the baseline state and the target state remains to be established. Figure 5.11 shows all office automation services and all administration specific line of business unique applications served from a data center environment. It also shows reuse of the ECSIP security infrastructure model for the regional data centers if gateways to external networks or RAS services prove to be required on a regional basis. While not obvious from the illustration, this approach also enables remote administration of all desktop clients from the regional data centers as well. This has the effect of greatly reducing the local demands for highly skilled workforce to accomplish system administration, security administration and ISO functions.

It is also anticipated that these regional data centers (and the corporate data centers) will host a consolidated, Department wide help desk service and manage disposition of trouble calls across lower level help desk functions to include telecommunications, cyber security, application or domain specific functions and local facility level help desk services.

COOP capability must also be provided in regional data centers in support of business continuity in the face of natural or manmade disasters, just as with the corporate data centers. VA's current plan is to employ a scaled version of the same architecture presented in Section 5.2 above (and

discussed in the context of the corporate data centers) with regional data center facilities providing COOP services for one another.

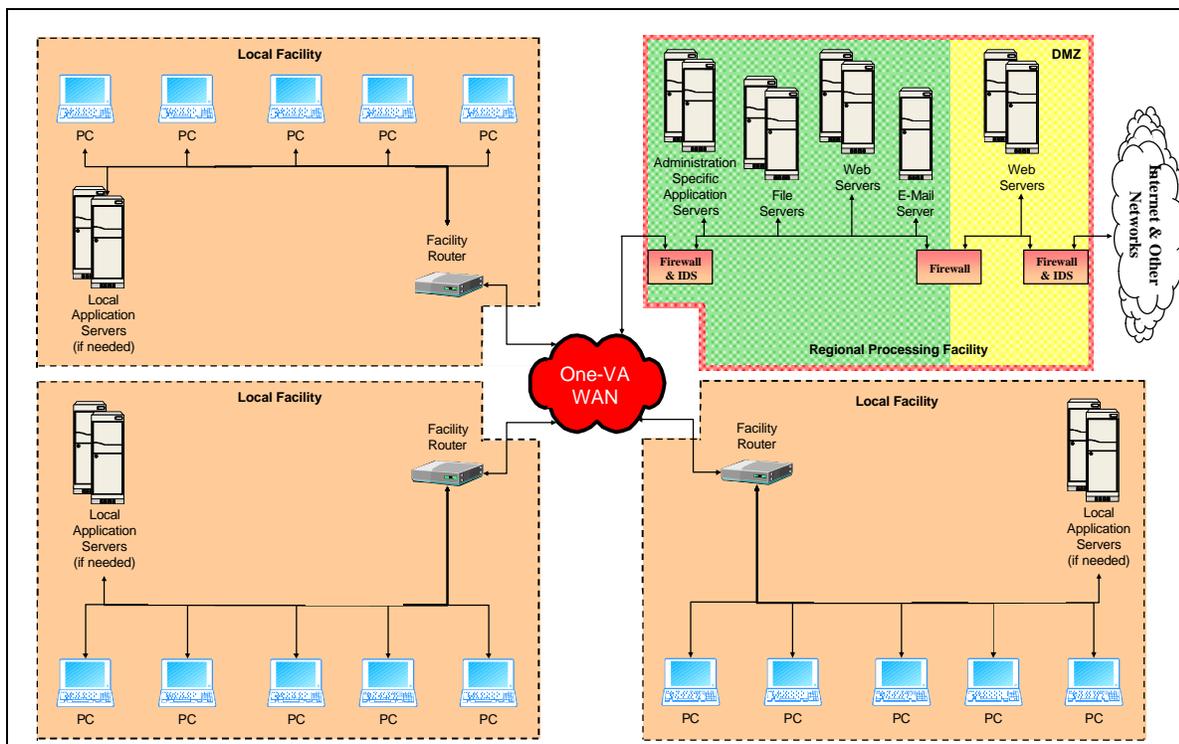


Figure 5.11 Target regional data center architecture.

5.5 Applications Layer Infrastructure and Distributed Systems Architecture

The following sections provide a top-level perspective on the distributed systems architecture across the Department from the perspective of the administrations; VBA, VHA and NCA. In each case a baseline “as is” distributed systems architecture at the top level is identified and specific, key applications are mapped to the EBFs that they support (with the exception of the Medical Education and Medical Research EBFs which do not currently maintain any significant dedicated distributed systems infrastructure). In addition to these baseline distributed systems applications architectures, preliminary target or “to be” distributed systems architectures are provided where they have been sufficiently developed.

5.5.1 Baseline VBA Applications Layer Infrastructure and Distributed Systems Architecture

Figure 5.12 through Figure 5.18 graphically illustrate the baseline (as-is) applications layer infrastructure and distributed systems architecture for VBA systems. It has evolved within the administration on a highly vertical basis. Figure 5.12 presents the overall environment with VBA components installed at the AAC corporate data center, at administration data centers located at Hines and Philadelphia, and at 57 regional offices nationwide. It also distinguishes between some components identified as legacy and others identified as modern in the context of near term modernization efforts being undertaken by VBA; particularly those aimed at transitioning off of the legacy and no longer supported Honeywell Bull environment. In this

context however, the label of “modern” does not refer to the One-VA EA target architecture in support of the transformation from document centric to data centric benefits claims processing. Figure 5.13 through Figure 5.17 then overlay the specific applications used to support individual business lines in the baseline architecture. Figure 5.13 depicts the baseline architecture in support of the Compensation and Pension EBFs. Figure 5.14 depicts the baseline architecture in support of the Education EBF. Figure 5.15 depicts the baseline architecture in support of the Vocational Rehabilitation and Employment EBF. Figure 5.16 depicts the baseline architecture in support of the Loan Guaranty EBF. Figure 5.17 depicts the baseline architecture in support of the Insurance EBF. Finally Figure 5.18 depicts other applications in the baseline VBA architecture that support multiple EBFs and KEFs.

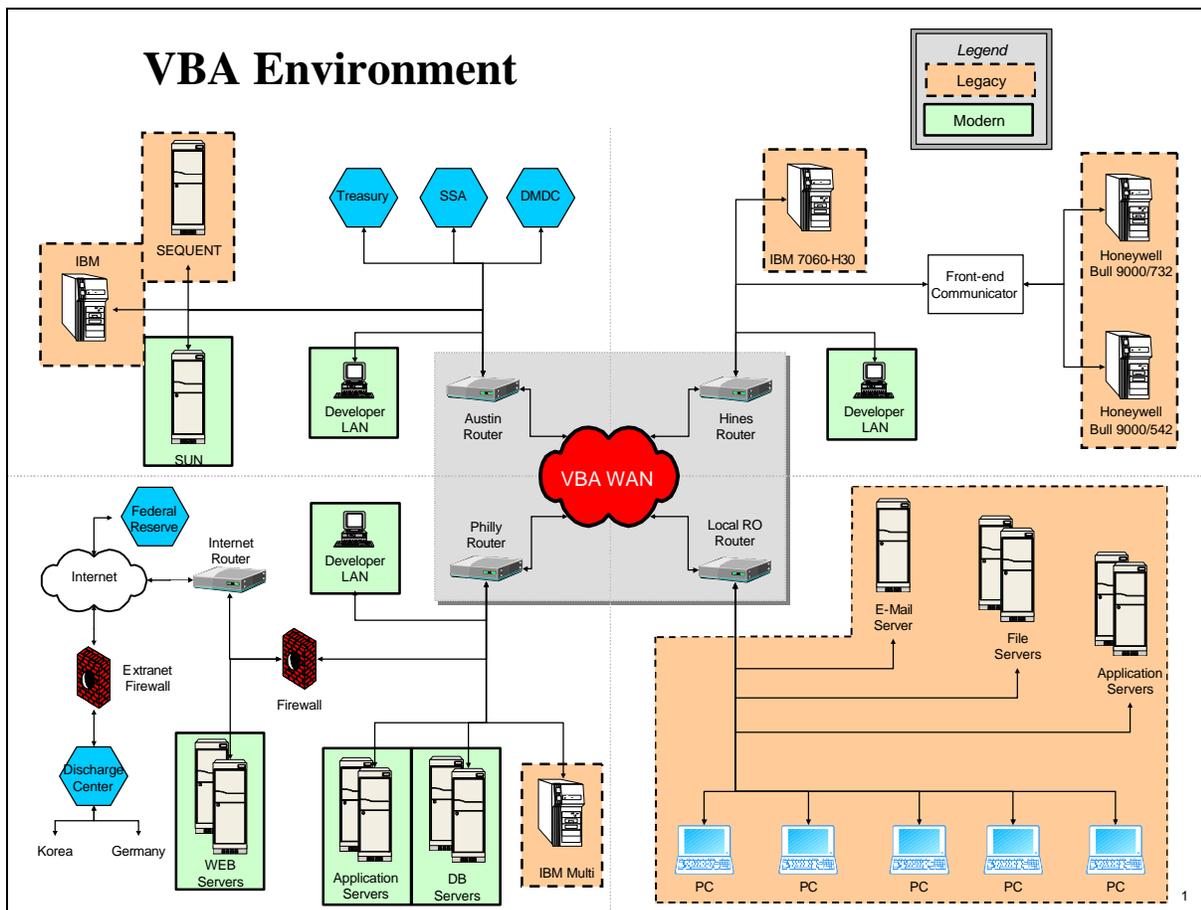


Figure 5.12 Baseline overall VBA architecture and environment.

VBA WAN Environment

- Four routers
 - Austin
 - Chicago Hines
 - Philadelphia
 - Local PO router
- Austin router
 - External Interfaces
 - Treasury

- Social Security Administration
- DMDC
- Servers
 - Legacy Sequent
 - Legacy IBM
 - Modern Sun
 - Modern Development LAN
- Chicago Hines Router
- Direct Connect
 - Legacy IBM 7060 H30
 - Modern Development LAN
- Front-End Communicator
 - Legacy Honeywell Bull 9000/732
 - Legacy Honeywell Bull 9000/542
- Philadelphia Router
- Direct Connect
 - Modern Development LAN
 - Legacy IBM Multi
 - Modern Application Servers
 - Modern Database Servers
- Behind Firewall
 - Internet Router
 - Internet to Federal Reserve
 - Modern Web Servers
 - Behind Extranet Firewall
 - Discharge Centers in Germany and Korea
- Local PO Router
 - Legacy Email Server
 - Legacy File Servers
 - Legacy Application Servers
 - Various Legacy Desktops

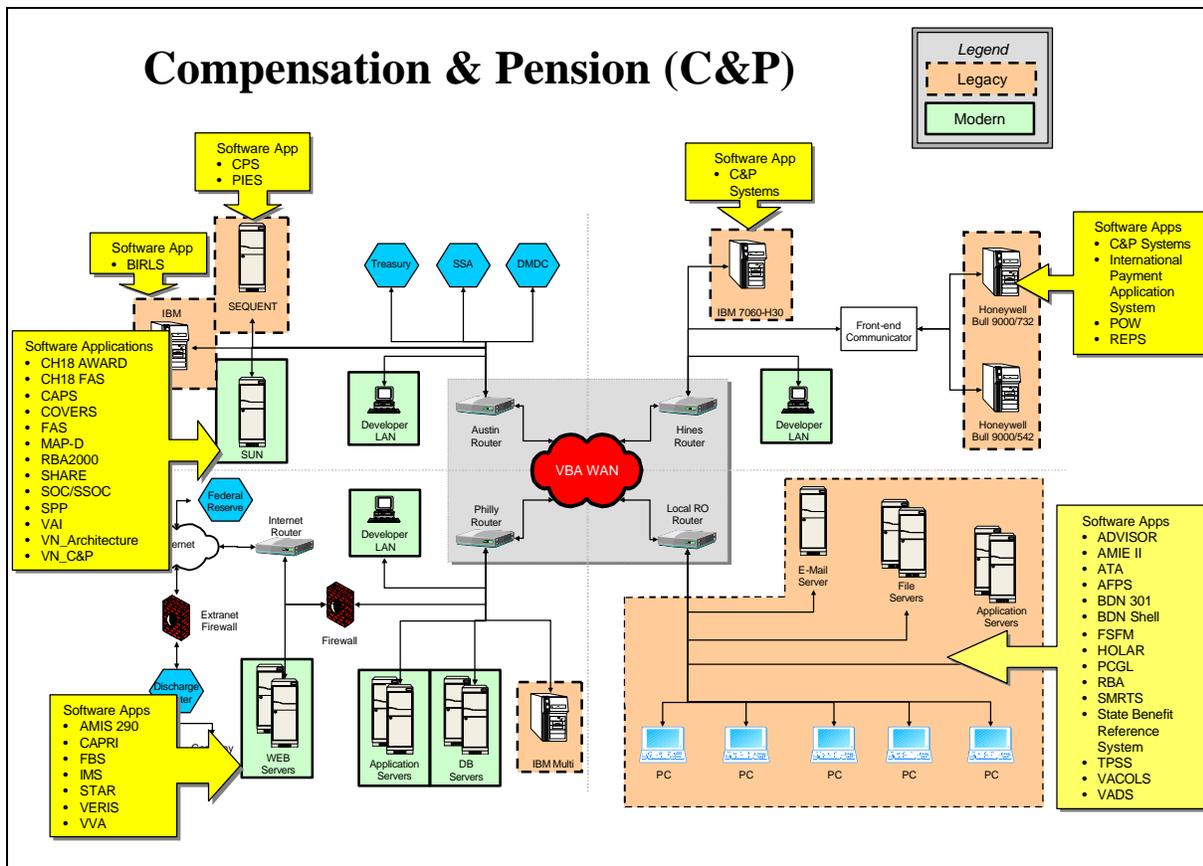


Figure 5.13 Baseline VBA architecture and environment in support of the Compensation and Pension EBFs.

Software Applications on SEQUENT

- CPS - Claims Processing System
- PIES - Personnel Information Exchange System: A client/server application designed to improve the quality and timeliness of requesting veteran information from outside agencies. Information gained from these requests are used to process claims for: compensation, pension, education, burial and loans.

Software Applications on IBM

- BIRLS - Beneficiary Identification Records Locator System: BIRLS processes on-line inquiry & updates, controls number assignment, different folder-type management, stores inactive compensation, pension & education data, and active/inactive insurance policy numbers.

Software Applications on Modern SUN

- CH18 AWARD
- CH18 FAS
- CAPS - Computerized Accounts Payable: Matches invoices and receivers and sends matched payment documents to FMS for payment to vendor via Treasury.
- COVERS - Control of Veterans Records: An MS Windows-based client/server application using bar code technology to support RO and RMC folder activities, including requests, mail, search and external transfer. The initial release applies to CLAIMS and NOD folders only.

- FAS – Financial Accounting System: FAS focuses on the development of a VETSNET Accounting system. It will support the financial business functionality of the C&P system. It can be used by other VBA benefit programs to provide a single system fully compliant w/ accounting requirements.
- MAP-D: The system provides the ability to perform claims development, case management and customer service for C&P claims. It features requesting and tracking evidence. It provides an overview of claimants and claims, including a letter library.
- RBA2000 - Rating Board Authorization 2000: The VETSNET RBA 2000 application provides the user with the ability to input data related to a claimant and have a rating document produced. The final product is a Word Document, and the data that is input is saved to the corporate database.
- SHARE: Share is a computer application built w/windows based color screens that a Regional Office employee can use to establish claim data. SHARE automatically creates claim data in the BDN & the corp. dbase to support the case mgmt of many types of C&P claims
- SOC/SSOC
- SPP
- VAI - Veterans Assistance Inquiry: VAI is a client/server application built with windows based screens. The application automates the veteran inquiry process from receipt of the inquiry to final resolution.
- VN_Architecture
- VN_C&P - Compensation and Pension

Software Applications on Modern Web Servers

- AMIS 290 - Automated Medical Info System: This application accepts the number of exams completed/returned not done/insufficient exams and the avg. days for completion to calculate the % insufficient & the % not done. It then exports data into a spreadsheet & provides monthly/yearly totals.
- CAPRI - Compensation & Pension Records Interchange: Graphic User Interface (GUI) for VistA AMIE II (Automated Medical Information Exchange files. The software implements a graphical user interface to replace the entire functionality found in the VistA AMIE II application and the functionality of the Patient Information Management System (PIMS) application, which is pertinent to and applicable to the VBA work process.
- FBS - Fiduciary Beneficiary System: Fiduciary and Field Examination (F&FE) personnel at VBA Regional Offices (ROs) nationwide use the FBS system as a database and diary system for incompetent beneficiaries under their charge.
- IMS
- STAR - Statistical Technical Accuracy Review
- VERIS - Veterans Exam Request Info System: VERIS is used by rating specialists at ten regional offices to request disability examinations from a private contractor. VERIS compiles the daily workload into a file & automatically sends it to the contractor on a daily basis. When examination reports.

- VVA

Software Applications on IBM 7060-H30

- C&P Systems - Compensation and Pension

Software Applications on Honeywell Bull 9000/732

- C&P Systems - Compensation and Pension
- International Payment Application System
- POW - Prisoner of War Database: This system tracks the level of service received by former POWs from the VA. Code sheets are converted to e-input and process via COBOL programs to edit input, update the POW master file create a listing of valid transactions/POW master records.
- REPS - Restore Entitlement Program for Survivors

Software Applications on Desktops

- ADVISOR - Advisor Computer-Based Training
- AMIE II - Automated Medical Information Exchange: AMIE II allows medical center staff read access to the BDN system for veterans' eligibility inquiries while regional office staff have electronic access to medical supporting data and streamlined logon capability within the VHA VISTA system.
- ATA - Adjudication Training Academy Database
- AFPS - Automated Folder Processing System: Automates various file maintenance projects as a replacement for those that previously used punched cards produced by the Austin Automation Center. These are XC, R&E, DEA, NOD retirement projects, inactivate claims folder relocation & sequence checking.
- BDN 301
- BDN Shell
- FSFM - File Server File Management: FSFM facilitates the saving of aging Rating Board Automation (RBS) data files on their own drive.
- HOLAR - Hearing Officer Letters and Reports System: database system used to maintain hearing officer schedules and data and permits automatic letter and report generation.
- PCGL - PC Generated Letters: PCGL provides letter generation capabilities to Field Office Veteran Service Center personnel for C&P and Education letters, Loan Guaranty and ORM letters, and allow the C&P personnel to 'scrape' BDN data into a decision notification letter.
- RBA - Rating Board Automation: The RBA application provides the user with the ability to input data related to a claimant and have a rating document produced. The final product is a Word Document, and the data that is input can be saved to the Data Warehouse.
- SMRTS - Service Medical Records Tracking System
- State Benefit Reference System: Comprehensive, ready references on state benefits & services, 50 states, P. Rico, DC, Virgin islands, Philippines + info on VA facility & local resources. Includes instructions to VA employees for certifying various info to assist veterans applying.
- TPSS - Training Performance Support System: This is a training program which is on CD Rom and does not reside on the network system.

- VACOLS - Veterans Appeals Control and Locator System: Access to VACOLS allows RO personnel to view, locate, update and track the status of appeals cases submitted to the Board of Veterans Appeals. VACOLS contains pre-programmed queries and generates reports.
- VADS - Veterans Assistance Discharge System: This system captures data from the DD214 which is used to update the BIRLS database and release letters to recently discharged persons on benefits to which they may be entitled.

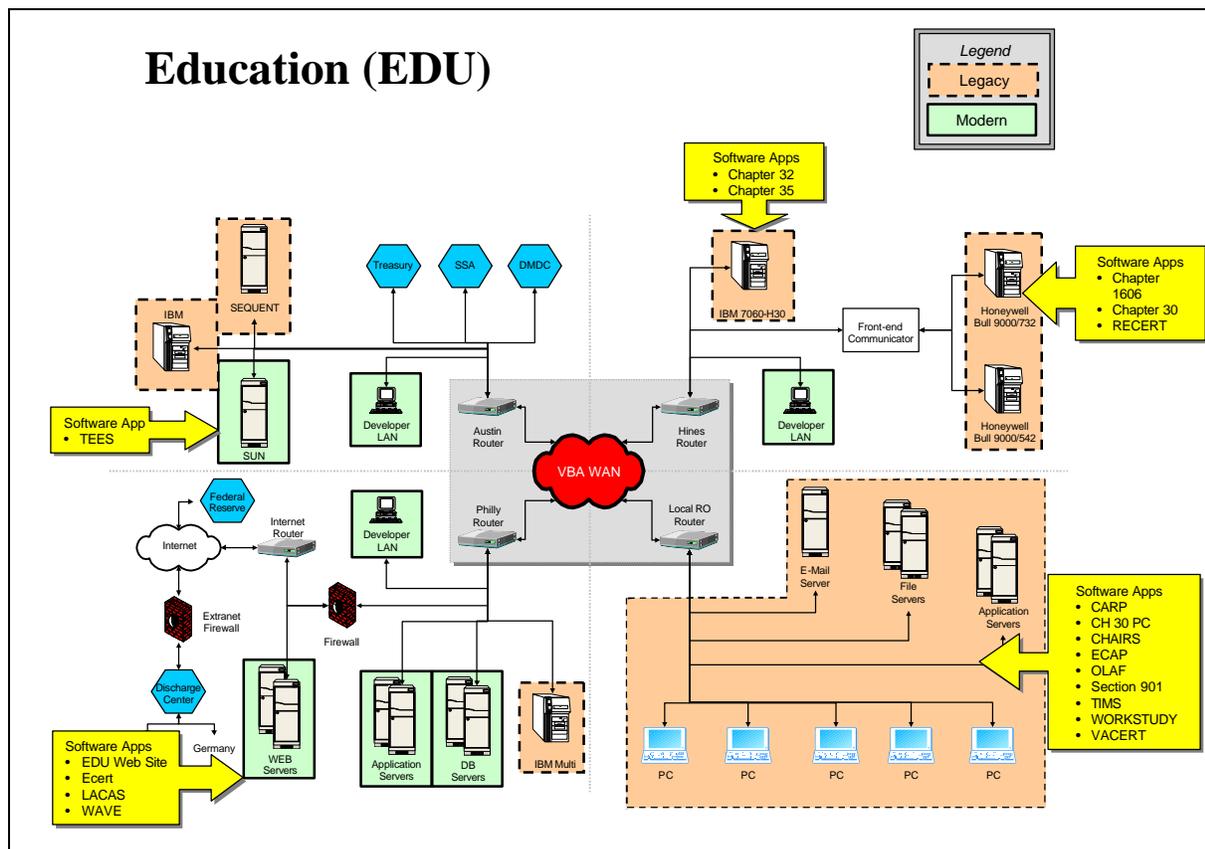


Figure 5.14 Baseline VBA architecture and environment in support of the Education EBF.

Software Applications on Modern SUN

- The Education Expert System (TEES)

Software Applications on Modern Web Server

- EDU Web Site
- Ecert
- LACAS
- WAVE - Web Automated Verification of Enrollment: The WAVE system allows veteran students the ability to verify their monthly enrollment over the Internet rather than returning a form to VA.

Software Applications on IBM 7060-H30

- Chapter 32
- Chapter 35 - Chapter 34/35: Chapter 35 provides up to 45 months of education and training benefits to eligible veterans' dependents. Chapter 35 processing

runs three times a week with no online capabilities. Payments are sent the same day awards are adjudicated or certified.

Software Application on Honeywell Bull 9000/732

- Chapter 1606 - Chapter 1606 assists eligible servicemen to further their post-high school education by providing educational assistance. Batch runs are processed three times a week and "big" pays are processed between the 23rd and 26th day of each month. Payments are sent the same day awards are adjudicated and certified.
- Chapter 30 - Chapter 30 PC Payment System - This system builds payment transactions for the BDN for flight, apprenticeship, on-job-training and correspondence benefits.
- RECERT – Recertification

Software Applications on Desktops

- CARP - Chapter 32 Accounts Receivable: CARP maintains and tracks Chapter 32 accounts receivable debt collection. CARP replaced the manual maintenance of accounts receivable subsidiary cards thus enabling operators to query the database for specific conditions prompting collection letters. The system decreases processing time for collection actions and provides an efficient method of monitoring and management.
- CH 30 PC - Chapter 30 PC Payment System: This system builds payment transactions for the BDN for flight, apprenticeship, on-job-training and correspondence benefits.
- CHAIRS - Chapter 35 Alternate Input Replacement System: CHAIRS is a Windows-based application which performs additional CH35 transactions that cannot be done in BDN. It allows the RPOs and Manila to remotely logon to the Hines BDC to input CH35 transactions.
- ECAP - Enrollment Certification Automated Processing: To attempt to process education awards based upon electronic enrollment certifications and notices of change in student status received from educational institutions using VACert.
- OLAF - On-Line Approval File: Maintains information on educational institutions and the programs of education that are approved for VA education benefits.
- Section 901
- TIMS - The Image Management System: Document imaging and workflow control for all VBA Education Benefits.
- WORKSTUDY
- VACERT

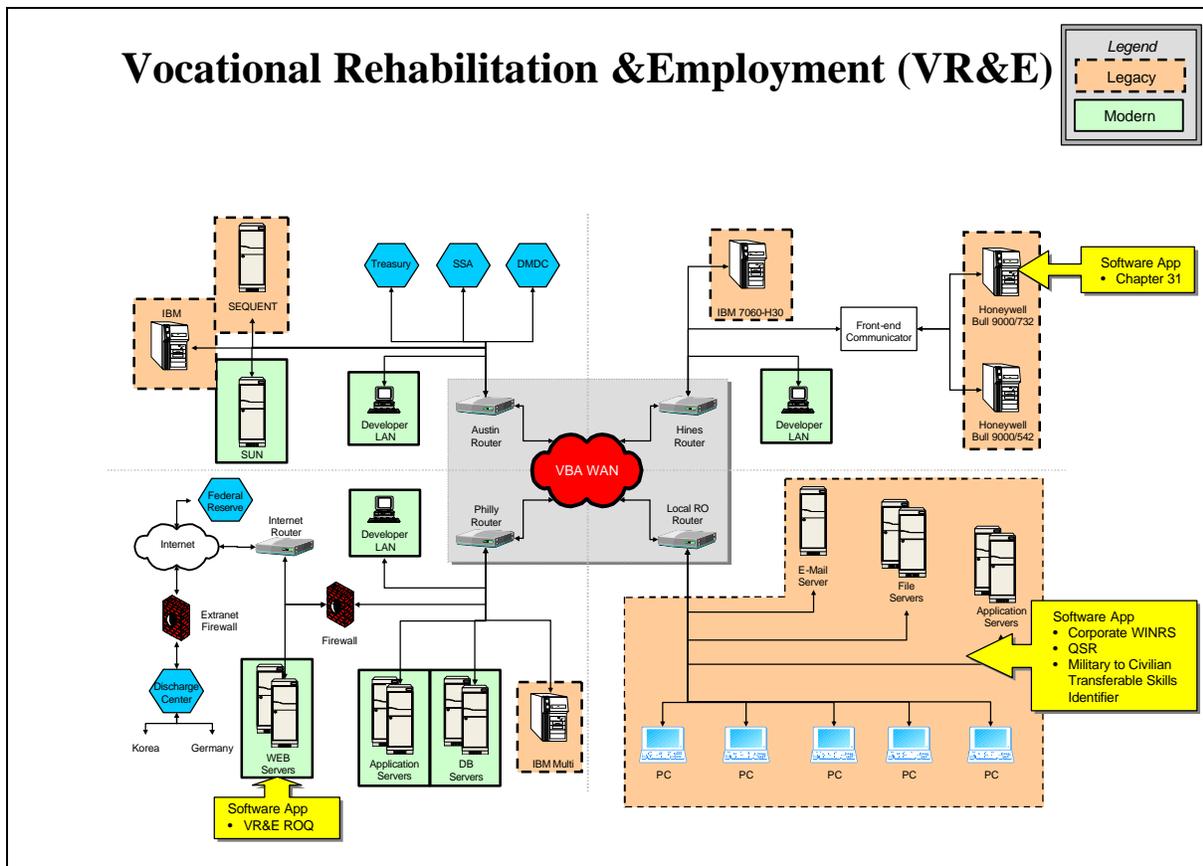


Figure 5.15 Baseline VBA architecture and environment in support of the Vocational Rehabilitation and Employment EBF.

Software Applications on Modern Web Servers

- VR&E ROQ - Vocational Rehabilitation and Employment Review of Quality: The Review of Quality (ROQ) Intranet site captures and collects data to reflect quality of delivery of services to Ch. 31 veterans.

Software Applications on Honeywell Bull 9000/732

- Chapter 31 - The system by which the major vocational rehabilitation and employment benefit, chapter 31 benefit processing is done, including payment, award, and accounting.

Software Applications on Desktops

- Corporate WINRS - A re-engineering and enhancement of the LAN-based WINRS application. Finance functions have been added for monitoring and making payments incurred under the Voc. Rehab Program. It is a comprehensive case-management system.
- QSR - Quarterly Statistical Report: Provides statistical data on various workload indices for each quarter of the FY & an annual report, from each VR&E Division. Data is collected & a report is sent to each Division at the end of each quarter of the FY & an annual report at the end of FY.
- Military to Civilian Transferable Skills Identifier

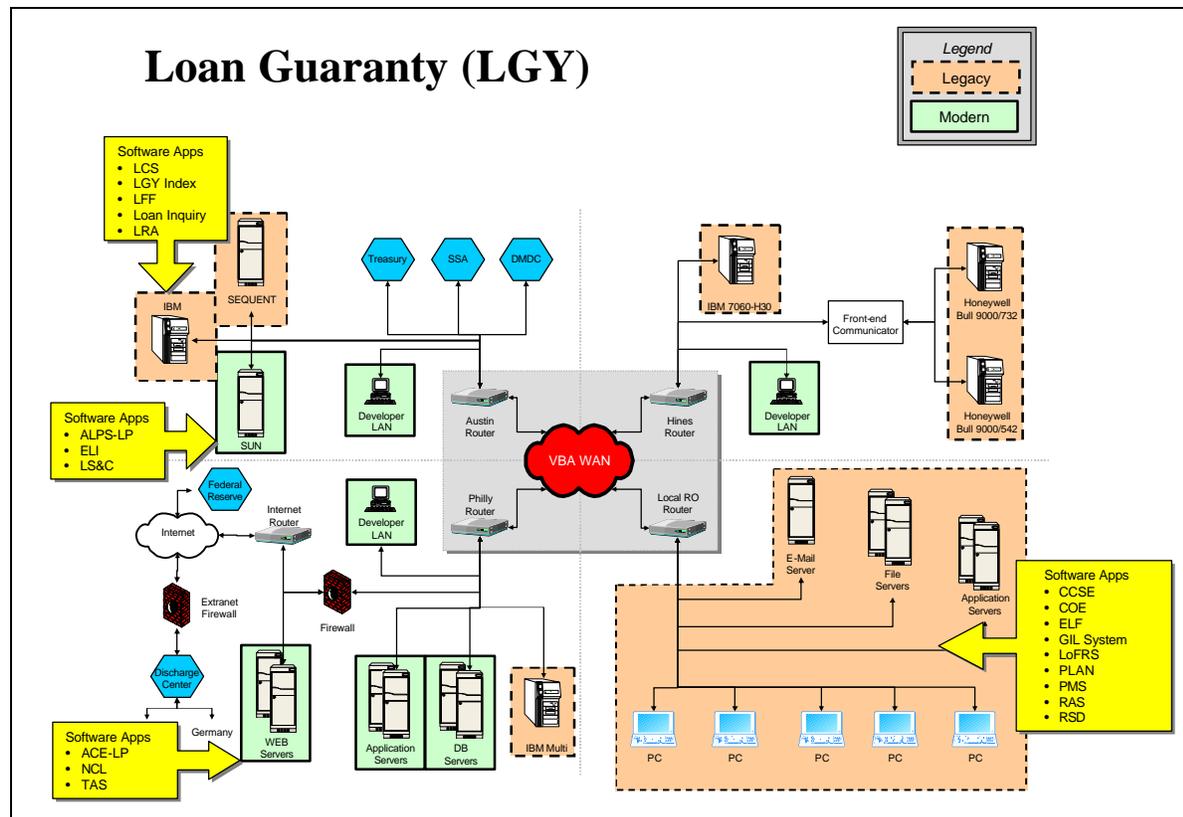


Figure 5.16 Baseline VBA architecture and environment in support of the Loan Guaranty EBF.

Software Applications on IBM

- LCS
- LGY Index - Loan Guaranty Index
- LFF - Lock Box for Funding Fee: The LFF replacement system will provide for automated linkages to electronically submitted applications for guaranty, electronic receipts, automated linkages to VBA accounting systems and improved operational support capabilities. The current LFF generates hard copy receipts, which are mailed to the lender, who in turn submits the receipts back to VA with the loan application and guaranty package. The LFF replacement system will eliminate hard copy receipts and their handling and will improve the loan origination process.
- Loan Inquiry
- LRA - Loan Guaranty Rapid Access: RAS is an online inquiry system used to determine the conditions of batch system master records - currently used with PMS only.

Software Applications on Modern SUN

- ALPS-LP - Automated Loan Production System/Loan Processing: ALPS-LP is a case mgmt tracking system for VA Home Loan processing at VA Regional Loan Centers. ALPS is a client/server, GUI-based application updating VBA's Oracle Corporate database.
- ELI - Expanded Lender Information: The ELI system provides VACO and ROs with a complete record of both approved & unapproved lenders. This includes

info about areas of operations, staff appraisal reviewers (SARS), underwriters, corporate/managing officers, agents & their functions, approved states & regional underwriters.

- LS&C - Loan Service and Claims: LS&C provides case management for defaulted VA home loans, and automated support for claims against guaranty & property acquisition processing. The system provides VACO & ROs w/a complete record of cured defaults/liquidated/refunded VA home loans and repurchased home loans.

Software Applications on Modern Web Servers

- ACE-LP
- NCL - National Control Listing: NCL provides an online list of builders, lenders and other mortgage industry related companies and individuals barred from participation in the VA Loan Guaranty Program.
- TAS – The Appraisal System

Software Applications on Desktops

- CCSE - Centralized Code Sheet Elimination: An on-line data entry and edit of LGY related code sheets.
- COE - Certificate of Eligibility: COE supports determination of eligibility for Loan Guaranty benefits, prints and records appropriate forms and letters, and provides reporting capability.
- ELF
- GIL System - Guaranteed/Insured Loans
- LoFRS - Loan Guaranty Folder Retirement System: LoFRS provides automated support for loan folder retirement processes. It consists of PC and handheld components.
- PLAN - Property Management Local Application Network: A comprehensive on-line system to automate daily functions related to property management.
- PMS
- RAS - Loan Guaranty Local Access to Rapid Access System: Provides access to LGY Target Inquiry Screens via the BDN or SNA.
- RSD - Report System Distribution

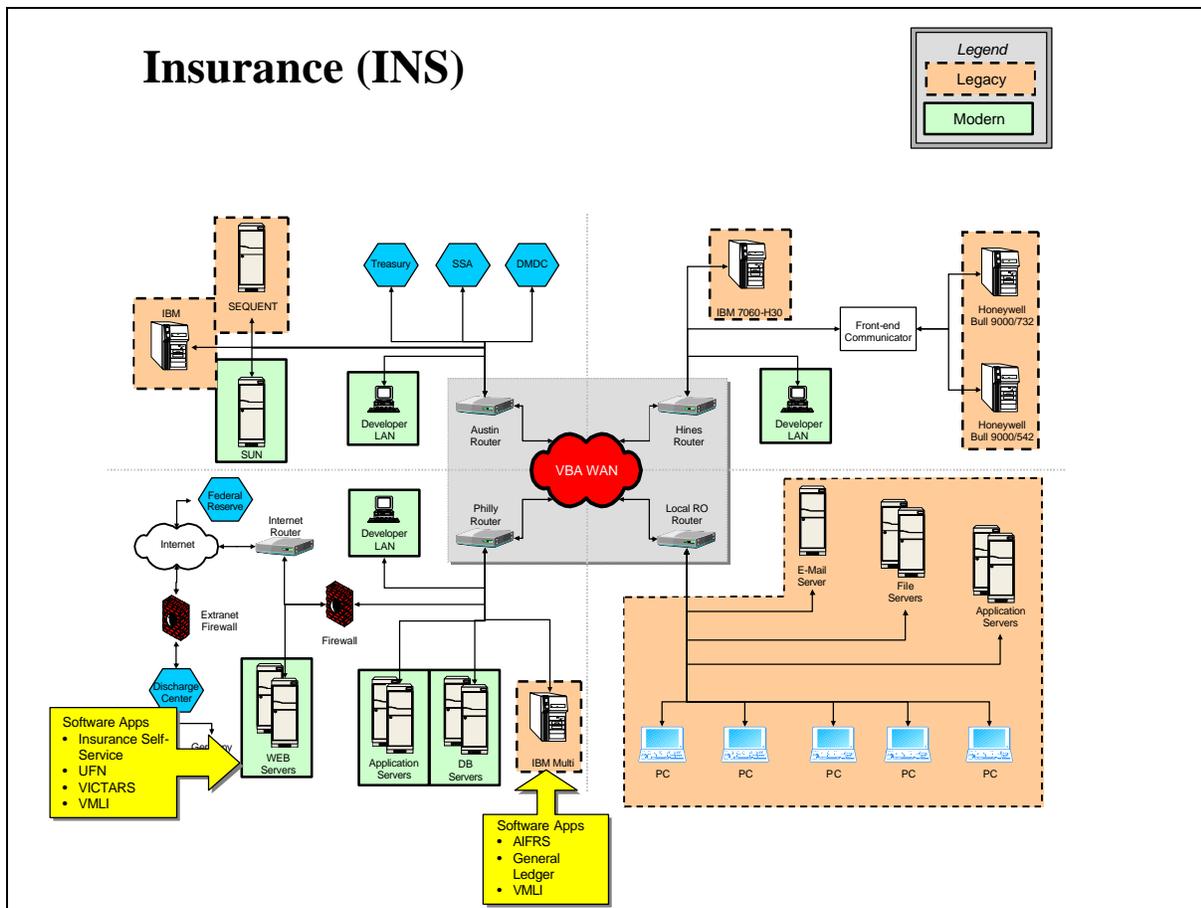


Figure 5.17 Baseline VBA architecture and environment in support of the Insurance EBF.

Software Applications on Modern Web Servers

- Insurance Self-Service
- UFN
- VICTARS - Veterans Insurance Claims Tracking and Response System
- VMLI - Veterans Mortgage Life Insurance: Began in 1971, and is issued to severely disabled veterans who have received grants for Specially Adapted Housing from VA. Designed to provide financial protection to cover eligible veterans' home mortgages in the event of death. Is a mortgage insurance.

Software Applications on IBM Multi

- AIFRS - Automated Insurance Folder Processing System: According to GISRA survey, no longer used.
- General Ledger
- VMLI - Veterans Mortgage Life Insurance: Began in 1971, and is issued to severely disabled veterans who have received grants for Specially Adapted Housing from VA. Designed to provide financial protection to cover eligible veterans' home mortgages in the event of death. Is a mortgage insurance.

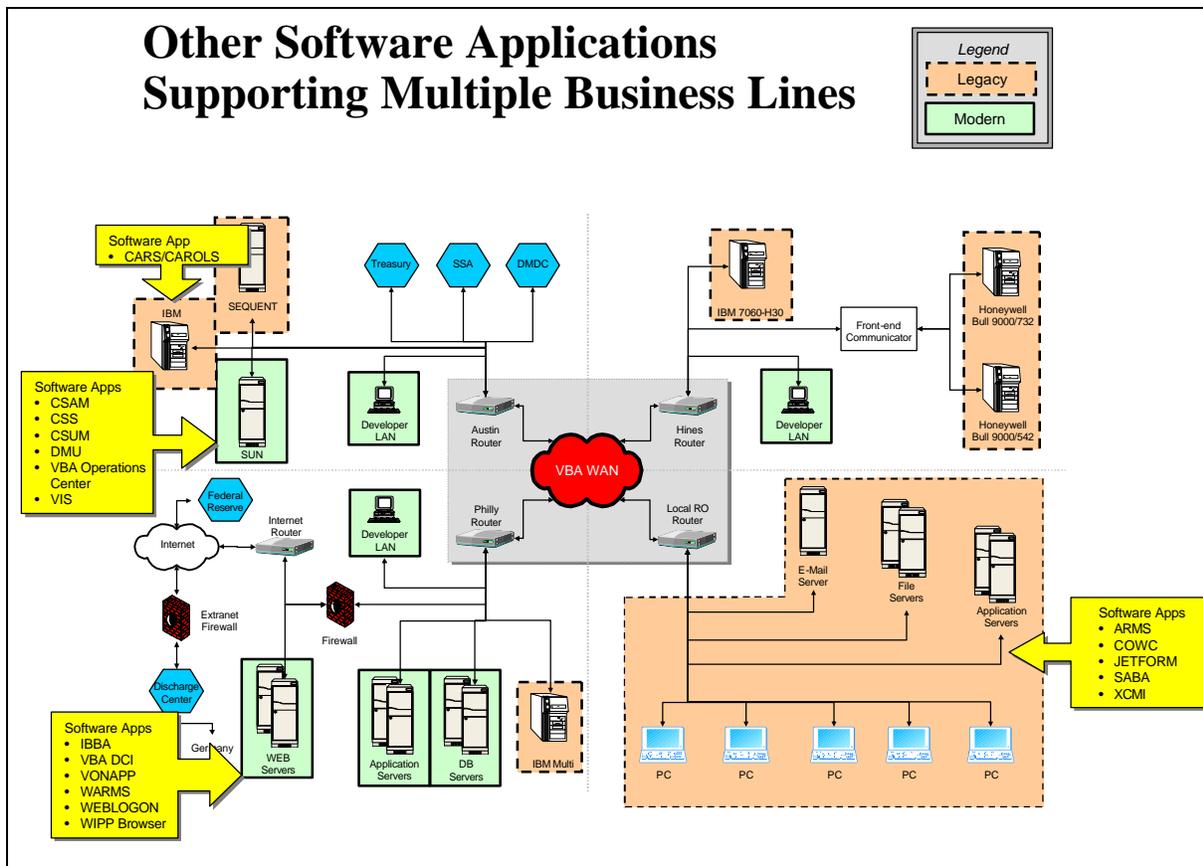


Figure 5.18 Baseline VBA architecture and environment for applications which support multiple EBFs and KEFs.

VBA supports and maintains a number of applications that are used to support operations in several different business lines across the VA enterprise and in some cases, in other Federal agencies. Figure 5.18 shows where these applications reside in the architecture. The applications include:

- Centralized Accounts Receivable System (CARS)/Centralized Accounts Receivable Online System (CAROLS), a legacy debt management application, in support of VA, the US Treasury, Social Security Administration (SSA), and Debt Management Centers (DMC).
- The following applications operating on Unix equipment:
 - CSAM
 - Common Security Services (CSS), a security application used by Security Officers to manage employee access to corporate applications, business functions, and "sensitive" records.
 - Common Security User Manager (CSUM), a security module used to control access privileges for users on the Benefits Delivery Network (BDN).
 - DMU
 - Vendor Inquiry System (VIS) enables VA's vendors to make online inquiries to determine status of their payments and to request information on previous payments made.
 - Other miscellaneous applications supporting the VBA Operations Center
- The following applications running on Web servers to allow Web-based access:

- Intranet BDN/BIRLS Access (IBBA)
- VBA Data Collection Instrument (DCI)
- Veteran's Online Application (VONAPP), an official VA website designed to allow individuals to apply for benefits through the Internet. VONAPP will allow veterans, and in the future, dependents and other VA claimants, electronic access to file applications online.
- Web Automated Reference Materials System (WARMS), a system for online searching various VA directives, pamphlets, manuals, guides, etc. This is particularly useful for veterans looking for information on whether or not they may qualify for a particular benefit.
- WEBLOGON
- Work In Progress Program (WIPP) Browser, an interface to allow viewing Benefits Delivery Center (BDC) work flow
- The following applications running in Regional Operations Centers:
 - Automated Reference Materials System (ARMS), an application that provides search capability to VBA publications, directives, manuals, circulars, etc.
 - Committee on Waivers and Compromises (COWC), a database system used to assist the committee on waivers and compromises and their staff to manage and report on activity at the Regional Offices.
 - JETFORM – a forms management application
 - Saba, an employee management system.
 - XCFI

5.5.2 Target VBA Applications Layer Infrastructure and Distributed Systems Architecture

Beyond the near term modernization efforts identified in the above discussion of Section 5.5.1 aimed at retirement of the aging Honeywell/Bull systems, the Department has established a strategic objective to transform the current benefits processing processes from a highly document (both paper and scanned paper) centric approach to a data centric approach. The target applications layer and distributed systems architecture to support this objective will be cast within the context of the overall One-VA target architecture for the applications layer and associated infrastructure layers as discussed in Sections 5.1, 5.2.2, 5.3.2, 5.4.2 and 5.4.4 earlier in this chapter. Beyond that however, it is premature at this time to identify how that transformation initiative will affect the applications layer distributed systems architecture across the enterprise. Therefore, the target distributed systems architecture for related implementations will be provided in later versions of this One-VA EA as the associated projects proceed into execution.

5.5.3 Baseline VHA Applications Layer Infrastructure and Distributed Systems Architecture

Figure 5.19 graphically illustrates the baseline (as-is) applications layer infrastructure and distributed systems architecture for VHA systems in support of the Medical Care EBF. Like the VBA applications architecture discussed in Section 5.5.1, this VHA infrastructure has evolved within the administration on a highly vertical basis. It reflects the distribution of applications across administration sponsored national facilities, six administration sponsored regional data

centers, 150 local major installations of the legacy VistA system at VA Medical Centers and smaller installations at smaller field locations such as Community Based Outpatient Clinics (CBOCs). Like the VBA drawing it also reflects use of an administration specific data network infrastructure with interfaces to other VA wide area data network infrastructure.

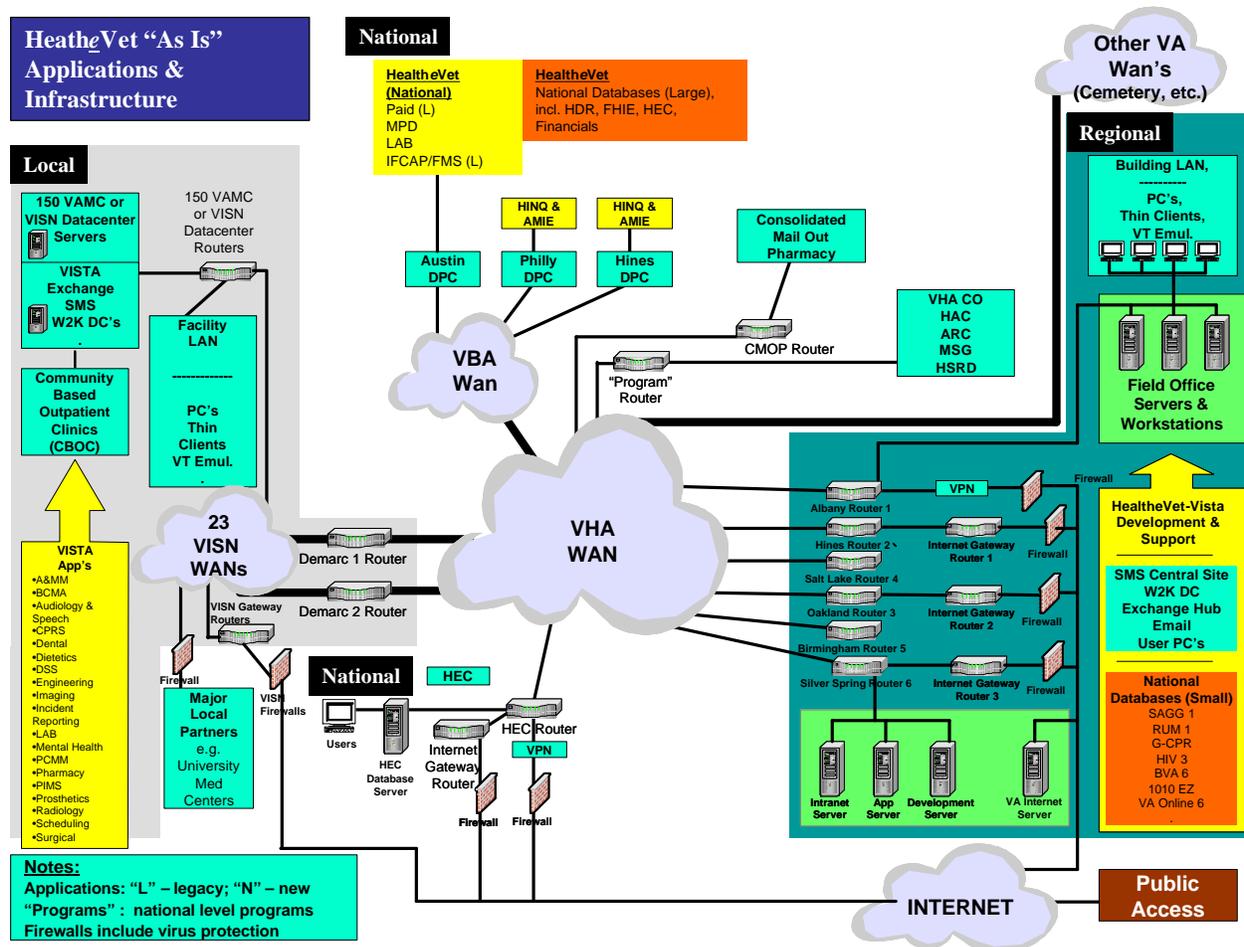


Figure 5.19 Baseline VHA architecture and environment for the Medical Care EBF.

The VHA network structure, shown in Figure 5.19, is an extensive Wide Area Network (WAN) that can be described as encompassing National, Regional, and Local WAN structures. These are all interconnected to the VHA-managed ATM backbone shown in Figure 5.19, and depicted in Figure 5.19 as the “cloud” labeled VHA National WAN. Figure 5.19 shows that the National WAN interconnects three major Data Processing Centers (DPCs), listed below:

- Austin
- Philadelphia
- Chicago Hines

Through routers shown in the diagram, the VHA National WAN also connects to

- a Consolidated Mail Out Pharmacy (CMOP)
- other VA WANs (NCA, VBA, etc.)
- other groups at the VHA Central Office (CO): Health Administration Center (HAC), Allocation Resource Center (ARC), Management Science Group (MSG), and Health Services Research and Development (HSRD).

- Health Eligibility Center (HEC) which hosts the HEC database server.

The VHA National WAN connects to regional offices through six routers at the following locations:

- Albany – which serves as the Health_eVet-VistA development and support site. Albany also serves as an SMS central site and hosts the following National small databases:
 - SAGG 1
 - RUM 1
 - G-CPR
 - HIV 3
 - BVA 6
 - 1010 EZ
 - VA Online 6
- Chicago Hines
- Oakland
- Salt Lake
- Birmingham
- Silver Spring – which hosts the VA Internet server, applications servers, and development servers.

Each of these field offices include VPNs behind firewalls that provide connection to the VA Internet Server and to the public Internet.

The local environments are the 23 VISN WANs, which also include access to the public Internet. The VISNs use firewalls for security protection, and provide two-way access to major local partners, such as University Medical Centers. Community-Based Outpatient Clinics (CBOCs) are connected to the VISN WANs through a total of 150 VAMC or VISN Data center routers. The CBOCs host or provide access to a number of VISTA applications.

5.5.4 Target VHA Applications Layer Infrastructure and Distributed Systems Architecture

Figure 5.20 graphically illustrates the top-level target (to be) applications layer infrastructure and distributed systems architecture for VHA systems supporting the Medical Care EBF. It reflects a planned shift in many applications from a local level to either a national or regional level at regional or corporate data centers. Implicit in this distributed systems architecture is support for the strategic goal of shifting from facility centric health care where patient records are dependent on the facility where a patient is seen, to patient centric where a longitudinal health care record is maintained for each patient independent of the health care facility at which the patient is seen. This distribution of applications and distributed systems architecture should be regarded as preliminary at this time however since analysis and design efforts are still underway in key projects such as the Health Data Repository (HDR) discussed in chapter four of this version of the One-VA EA.

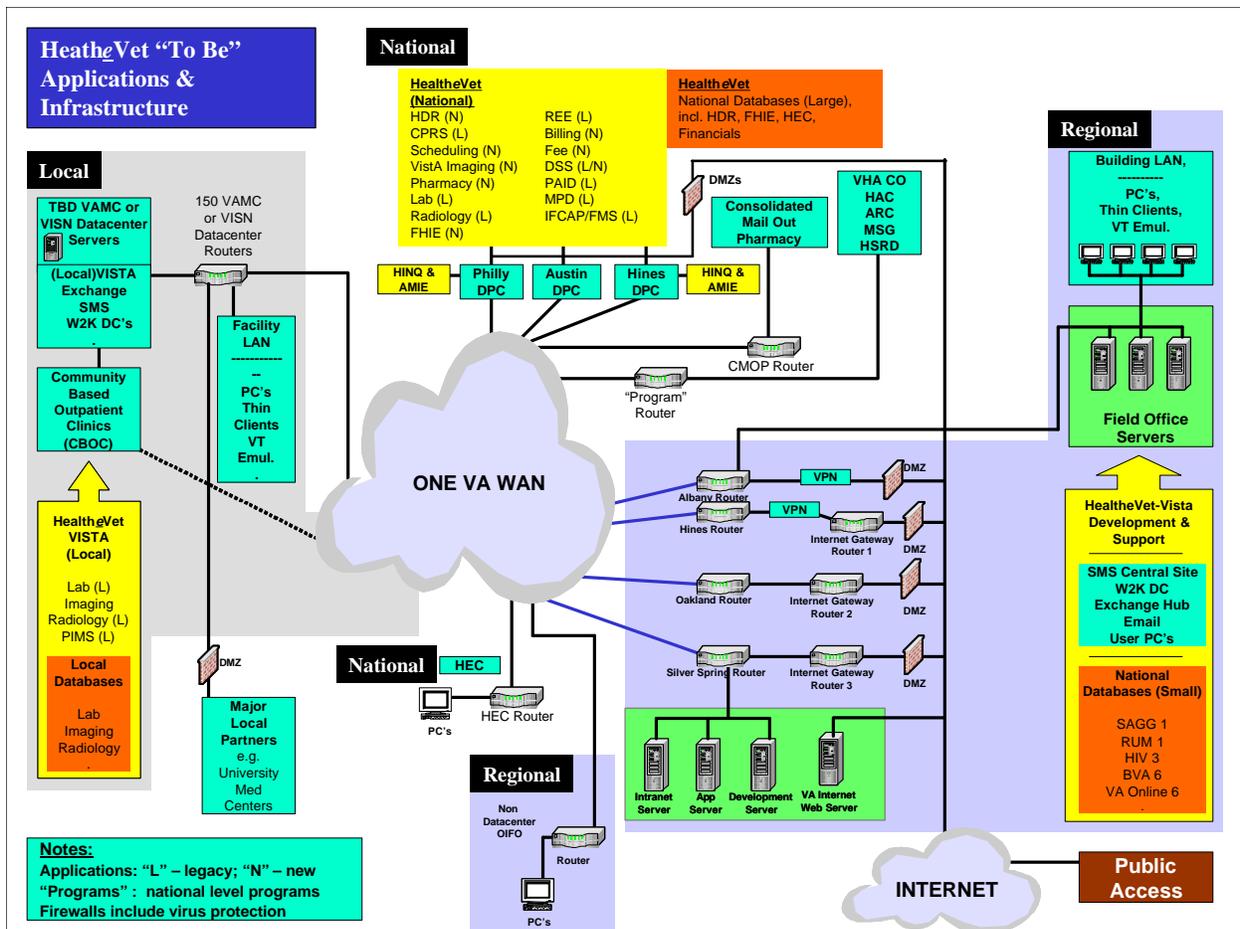


Figure 5.20 Target VHA architecture and environment for support of the Medical Care EBF.

- Austin – the National HealtheVet is located here with the following applications
 - PAID – Personnel and Accounting Integrated Data: The Enhanced Time and Attendance System (ETA) automates time and attendance for employees, timekeepers, payroll and supervisors.
 - MPD – Minimal Patient Dataset: The Minimal Patient Dataset (MPD) software enables personnel to search for treatment dates, treatment locations, and the types of care a patient has received throughout the VA health care system.
 - LAB – Laboratory: The Laboratory module supports the following areas: General Laboratory, Microbiology, Histology, Cytology, Surgical Pathology, Electron Microscopy, Blood Donors, and Blood Bank.
 - IFCAP/FMS – Integrated Funds Distribution, Control Point Activity, Accounting and Procurement: VA employees use IFCAP to fund budgets, order goods and services, maintain records of available funds, determine the status of a request compare vendors and items to determine the best purchase, record the receipt of items into the warehouse, and pay vendors.
 and the following large National databases
 - HDR – Health Data Repository: (TBD)
 - FHIE

- HEC - Health Eligibility Center: HEC inserts veteran specific data provided by Health Eligibility Reports into electronic forms/letters to print and mail to veterans.
- Financials
- Philadelphia – hosts the following applications
 - HINQ - Hospital Inquiry: The Hospital Inquiry (HINQ) module provides the capability to request and obtain veteran eligibility data via the VA national telecommunications network.
 - AMIE - Automated Medical Information Exchange: Used to share information with VBA.
- Chicago Hines – hosts the same applications as at Philadelphia.

Through routers shown in the diagram, the VHA National WAN also connects to

- a Consolidated Mail Out Pharmacy (CMOP)
- to other VA WANs (NCA, VBA, etc.)
- other groups at the VHA Central Office (CO): Health Administration Center (HAC), Allocation Resource Center (ARC), Management Science Group (MSG), and Health Services Research and Development (HSRD).
- HEC which hosts the HEC database server.

The CBOCs host or provide access to a number of VISTA applications, including the following:

- A&MM
- BCMA - Pharmacy - Bar Code Medication Administration: The Bar Code Medication Administration software will enable users to electronically document medications at the bedside or other points of care. Bar code technology will be utilized with real-time Ethernet connectivity, via Intel x86 based, Windows 95/98 devices (notebooks or PCs) to improve the accuracy of medication administration.
- Audiology & Speech – QUASAR - Quality Audiology and Speech Analysis and Reporting: Provides support for the Audiology and Speech Pathology Service. The package is used to enter, edit, and retrieve data for each episode of care.
- CPRS - Computerized Patient Record System: Comprehensive patient record. Enables clinicians to enter review and continuously update all order-related information connected to any patient.
- Dental: The Dentistry module is a menu-based system incorporating features necessary for the maintenance of medical center dental records.
- Dietetics: The Dietetics software integrates the automation of many Clinical Nutrition and Food Management functions.
- DSS - Decision Support System Extracts: Decision Support System (DSS) provides a means of exporting data from selected VistA modules to DSS resident in the Austin Automation Center (AAC).
- Engineering: Provides for management of the information needed to effectively discharge key operational responsibilities normally assigned to VA engineering organizations such as: Equipment Mgmt, Work Control, Space/Facility Management, Project Planning and Submission, and Project Tracking.
- IS - Imaging: VistA Imaging provides for the capture and management of clinical images, scanned documents, electrocardiogram (EKG) waveforms and other non-textual data files.

- Incident Reporting: The Incident Reporting module supports VHA policy by compiling data on patient incidents. It organizes the data into defined categories for reporting and tracking at medical facility level and also for transmission to the National Quality Assurance Database for review and tracking by Headquarters.
- LAB - Laboratory: The Laboratory module supports the following areas: General Laboratory, Microbiology, Histology, Cytology, Surgical Pathology, Electron Microscopy, Blood Donors, and Blood Bank.
- Mental Health: The Mental Health module provides computer support for both clinical & administrative patient care activities.
- PCMM - Primary Care Management Module: To develop a national strategy and plan for implementing Practice Profiling nationwide.
- Pharmacy:
 - Controlled Substances Pharmacy Drug Accountability Package: This system works towards perpetual inventory for each medical facility pharmacy by tracking all drugs through pharmacy locations.
 - The Controlled Substances (CS) software package is one segment of the Veterans Health Information Systems and Technology Architecture (VistA) being installed at VAMCs. The CS software will monitor and track the receipt, inventory, and dispensing of controlled substances. Automation of the narcotic inventory process will permit pharmacists & inspectors to perform vault inventories utilizing portable barcode readers. Monthly (or more frequent) inspections can be conducted by mgmt w/ discrepancies in stock levels automatically identified.
- PIMS – Patient Information Management System: Applicable to the VBA work process
- Prosthetics: Provides improved control and auditing of expenditures, maintains a record of prosthetic devices provided to each veteran, and allows for the rapid generation of management reports.
- RNM – Radiology/Nuclear Medicine: Automates the entire range of diagnostic functions performed in imaging departments.
- Scheduling: The Scheduling module automates all aspects of the outpatient appointment process including ability to check-in/check-out patients, clinic set up and maintenance, enrollment/scheduling/discharge of patients to and from various clinics, and the generation of managerial reports, statistical reports, patient letters, and workload reporting.
- Surgical: Designed to be used by surgeons, surgical residents, anesthetists, operating room nurses, and other surgical staff. This module integrates booking surgical cases and tracking clinical patient data to provide a variety of administrative and clinical reports.

5.5.5 Baseline NCA Applications Layer Infrastructure and Distributed Systems Architecture

Figure 5.21 graphically illustrates the baseline (as-is) overall infrastructure for NCA in support of the Memorials and Burial EBF. Figure 5.22 overlays the distributed systems applications layer architecture in support of the Memorials and Burial EBF. Like the VBA and VHA infrastructure and applications architecture discussed in Section 5.5.1 and 5.5.3, this NCA infrastructure has evolved within the administration on a highly vertical basis. Unlike the other administration specific architectures however it reflects a strong centralization of both Unix and Windows services at the NCA ‘regional’ data center located at Quantico Virginia. This includes both office automation server infrastructure as well as administration specific vertical

applications. Only desktop administration occur on a local basis at the NCA field locations across the nation. In that sense this baseline distributed systems architecture within NCA is significantly closer to the target regional processing model discussed previously in Section 5.5.4 of the One-VA EA. The only significant evolution that is required is away from the administration specific WAN and cyber security infrastructure identified in Figure 5.21 to the corporate telecommunications infrastructure and cyber security infrastructure discussed earlier in this chapter in Sections 5.5.2 and 5.3.2.

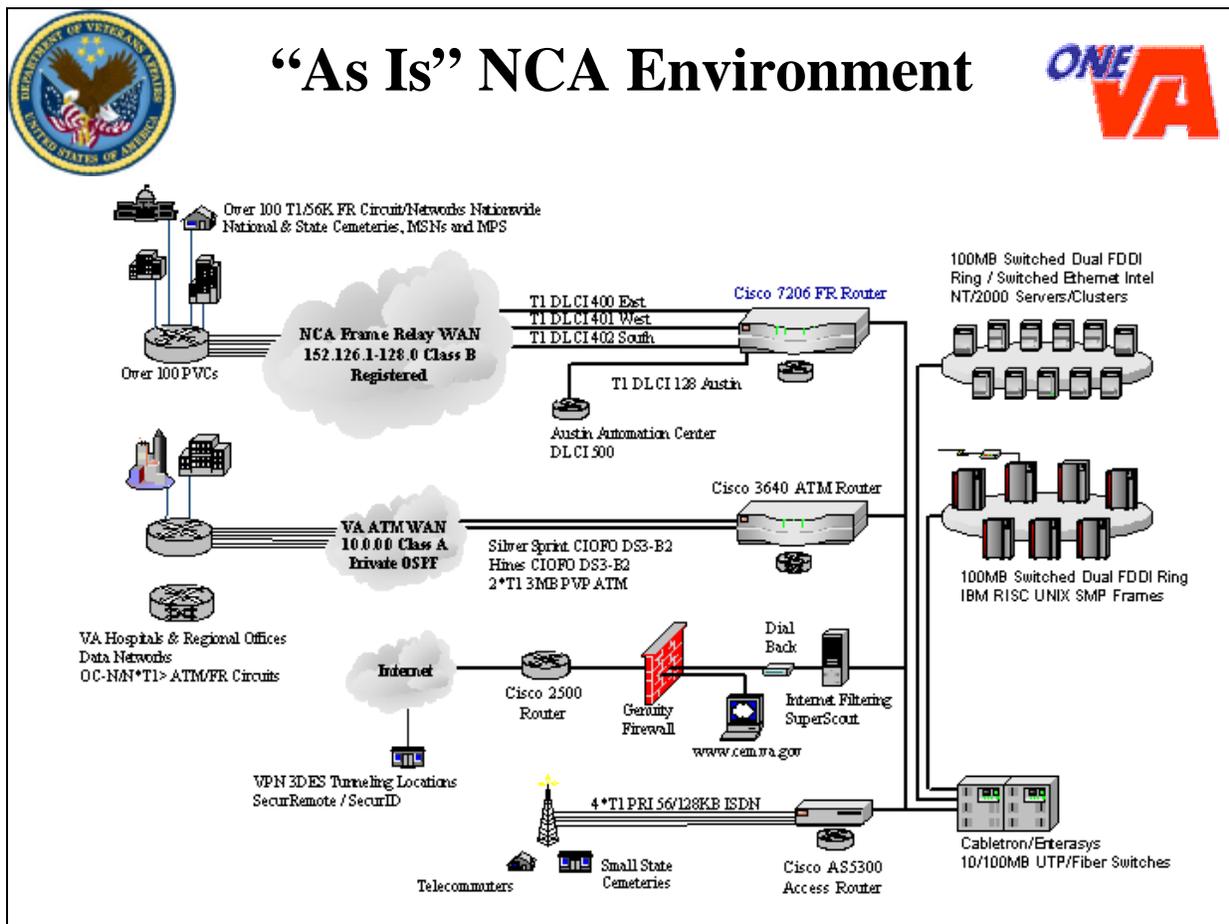


Figure 5.21 Baseline NCA architecture and environment.

The NCA Network & Systems Engineering (NSE) Division is responsible for the design, implementation, security and management of all data networks and systems for the National Cemetery Administration. This division maintains over 1 terabyte of disk storage, supports over 3000 devices and processes over 70 billion bytes of data traffic monthly as we manage our operations 24x7.

Technical Areas of Management

- NCA Data Networks
- IBM RISC SMP Frames
- Intel Based Systems and all Peripheral Devices

- Oracle Databases for NCA Applications
- UNIX/NT/2000 Kernels and Applications
- Network and Systems Administration and Security
- Power Systems

Supports Customers in over 160 Locations Nation Wide

- VA National Cemeteries
- State Veterans Cemeteries
- Memorial Service Networks
- Memorial Program Service Offices
- Centralized Contracting Division
- Veterans Health Administration
- Veterans Benefits Administration
- Austin Automation Center
- Department of Interior
- Department of Army (to include Arlington National Cemetery)

NCA DATA NETWORKS

NCA Frame Relay Class B Wide Area Network (NCA Backbone)

- Approximately 100 T1/56KB router based networks nationwide
- Segmented into four major Frame Relay trunks (East, West, South and Austin) to the Sprint

FTS2001 PDN

- Process approximately 40 billion bytes of data traffic monthly and is managed and monitored locally via HPOpenView, Visual Uptime and CiscoView
- Cisco 7206 and Cisco 7204 serve as the NCA backbone routers for these networks

VA ATM Class A Wide Area Network (NCA Connection to VA Backbone)

- 3MB ATM PVP to Silver Spring and Hines that connects NCA to the VA Class A ATM Network Backbone via OSPF routing
- All data traffic passed to and from NCA to other VA organizations utilize this ATM connection
- Process approximately 10 billion bytes of data traffic monthly and is managed and monitored locally. Signal Corporation and the Sprint Management Service Center manage the external connection
- Cisco 3640 router serves as the VA/NCA backbone router for this network

NCA Internet Gateway (CheckPoint Firewall)

- Internet Service Provider for customers on the NCA Data Network
- All Internet traffic is filtered and logged with SuperScout and UNIX syslog servers
- NCA Firewall is monitored 24x7 by Genuity Site Patrol
- Provide 168bit IPsec 3DES encryption via SecureRemote tunneling from the Internet through the NCA CheckPoint Firewall on inbound connections

- Customers must authenticate with a valid certificate, a valid account and a SecurID card on inbound connections (except web e-mail connections)
- Process approximately 20 billion bytes of data traffic monthly and is managed and monitored locally and by Genuity Site Patrol
- Cisco 2500 series router and Sun Sparc Station running Solaris and CheckPoint Firewall serves as the Internet Gateway

NCA AS5300 56KB/ISDN PRI 800 Dial-In Network

- Four T1 PRI circuits that support up to 96 concurrent 56KB or ISDN connections
- Provide customers, small locations and telecommuters toll free dial-in access to the NCA Data Network via CHAP (Challenge-Handshake Authentication Protocol). This protocol provides 3-way MD5 128bit checksum challenges
- Users establish a PPP (point to point protocol) connection utilizing DHCP and have the same functionality as direct Ethernet connected users
- Process several billion bytes of data monthly and is managed and monitored locally via Cisco TACACS server
- Cisco AS5300 serves as the access router

NCA Data Center Network

- 14 T1 Frame Relay, ATM and PRI Circuits to interconnect over 100 locations
- Dual switched 100mb FDDI Fiber Rings to Production Devices
- Switch 100mb Ethernet to Development / Testing Devices
- 7 Cisco Routers (7000, 4000, 3000 and 2000 series)
- 3 Fiber/Copper Switches
- Future plans are to install an internal PIX firewall to protect against VA vulnerabilities

IBM RISC/INTEL SYSTEMS

Large scale Systems are in full production 19 hours/day from 5:00am to 12:00am.

During non production hours the following is performed; full database exports, full system backups with offsite storage, data extracts and transmissions to other VA and Federal organizations, summary and report generations

IBM R6000 RISC Frames (UNIX)

- IBM 7017/S70 SMP Frame (primary Oracle Database Engine)
- IBM 7015/R50 SMP Frame (Forms Engine / Training)
- IBM 7026/M80 SMP Frame (Scan Engine)
- IBM 7026/6M1 SMP Frame (Web Front End / Forms Engine)
- IBM 7026/6H1 SMP Frame (Development / Testing)
- IBM 7026/F50 SMP Mini (DNS/FTP/Performance/Logs Engine)
- SUN Sparc (Internet Firewall)
- Supports UNIX/Oracle based applications

Intel Based Servers and Desktops (NT/2000/98)

- 20 Intel based servers, primarily Dell 6300 to 8450 series
- Support NT/2000 Server based applications

- Configure and support over 1000 desktop computers and peripheral devices to include; printers, print servers, notebooks, cameras, scanners, CDRWs, PDAs, etc.

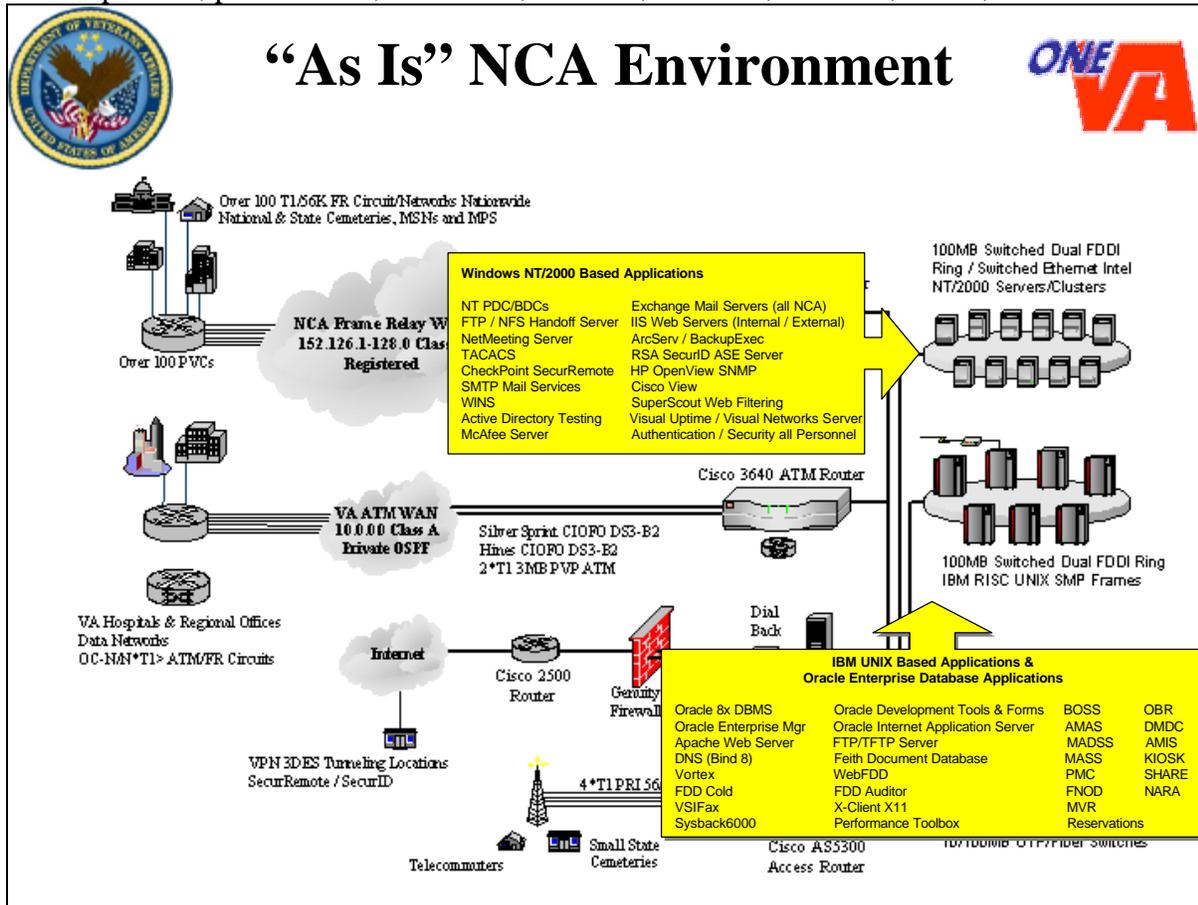


Figure 5.22 Baseline NCA architecture and environment with distributed applications supporting the Memorials and Burial EBF overlaid.

ORACLE DATABASES AND APPLICATIONS

NSE Division maintains 6 Oracle databases and 4.3 million decedent records; 2 repositories for the Oracle applications, 2 development databases, 1 training database and 1 systems management database. Applications for these databases include:

- BOSS – Burial Operations Support System, supports interment related activities at national and state veterans’ cemeteries. Process over 100,000 cases per year
- AMAS – Automated Monument Application System, supports monument ordering and tracking. Process over 330,000 orders per year
- MADSS – Management Application Decision Support System, tracks statistical interment data and handoff
- MASS – Monument Application Scanning System, converts 1330 applications in electronic format for MPS processing
- AGS/GRS – Adjacent Grave Site / Grave Site Reservation
- PMC – Presidential Memorial Certificates (data handoff)
- FNOD – First Notice of Death (data handoff)
- MVR – Master Veteran Record (data handoff)

- OBR – Outer Burial Receptacles, tracks government supplied casket liners
- DMDC – Defense Manpower Data Center, data handoff of deceased veteran information to the Department of Army
- AMIS – Automated Management Information System (data handoff)
- Kiosk Project – Kiosk gravesite locator for National and State Veterans Cemeteries
- Share Project – Data exchange with other federal agencies
- NARA Project – National Archives and Records Administration, file handoff of entire BOSS database for historical records
- Reservations – automates letters to send to veteran or spouse to maintain reservation of burial site

UNIX KERNEL AND APPLICATIONS

- IBM Frames operating under UNIX/AIX 4.3.3 with Lynux libraries
- Anonymous FTP – File Transfer Protocol, allows users to share data files
- DNS (Bind 8)– Domain Name Server, translates names of host computers and devices to IP addresses, BIND (Berkley Internet Name Daemon version 8
- Apache Web Servers – Web server engine
- Oracle 8x DBMS - relational database, java supported
- Oracle Development Tools and Forms - builds internet applications to view, update and add data to the database
- Oracle Internet Application Server – provides the middle tier, internet access between the forms and database
- Oracle Enterprise Manager – centralized console to manage the complete database and application environment
- Feith Document Database – fax solution to accommodate large volumes of transmissions, using an Oracle 8i database. Oracle 8i based engine
- Vortex - automates the handling and searching directories for incoming files and associates this with online applications for MASS (indexing)
- WebFDD - provides the web interface and accesses scanned or faxed images for AMAS/MASS
- FDD Cold – Feith Document Database that handles the Enterprise Report Management and automates indexing of documents
- FDD Auditor – Feith Document Database performance measurement tool
- VSIFax – Inbound Fax Applications for Feith Initiative (MPS)
- X Clients – X Window front end that handles X11 libraries for UNIX based applications
- Sysback6000 – backup management software for IBM Frames
- Performance Toolbox – manages all performance activity on IBM Frames
- Sun Solaris/CheckPoint Firewall – provides Internet security and inbound/outbound connectivity for customers on the NCA data network

NT/2000 KERNEL AND APPLICATIONS

- Visual Uptime – provides network management at the circuit and protocol levels
- McAfee Server – provides virus protection updates automatically to field computers (still in progress)

- NetMeeting – allows customers to collaborate on one desktop over the NCA data network
- Dell Servers operating under Windows NT and Windows 2000 Advanced Server in RAID 5 and Cluster configuration
- NT PDC/BDC – Primary and Backup Domain Controllers. These servers provide the authentication process for all NCA employees and groups the NT based servers onto the CEMMASTER NT Domain
- Exchange Mail Servers – manage all Outlook related activities for NCA to include; internal and external SMTP e-mail, calendars, tasks, etc.
- Internal / External Web Servers – manage the NCA Web Sites (mirrored) at www.cem.va.gov and NCA internal web site at vaww.cem.va.gov. The NCA Home Page (external web server) currently averages over 70,000 visitors per month
- WINS – Windows Internet Name Service translates between Windows based computers and their associated IP address
- ARCServ/BackupExec – backup software for NT/2000 platform
- SuperScout – manages, monitors and logs all Internet activity
- SecurRemote - provides 3DES 168 bit encryption VPN tunneling access into the NCA data network from the Internet
- RSA SecurID – provides an authentication method via token for VPN users
- ASE Server – provides authentication management for SecurID
- TACACS – provides management and a 128 bit CHAP authentication method for toll free dial-in users via PPP over 56KB or ISDN
- HPOpenView – provides SNMP network management of all NCA data networks
- Cisco View – provides statistics and logging on Cisco routers

POWER SYSTEMS

- Three Power Distribution Units run in parallel with 80Kva output to supply continuous filtered power to the NSE Division's Computer Room to include; all network and system devices, climate control units, security systems and lights
- Two Kohler Diesel Generators with 130Kva output to supply power to the Power Distribution Units. A 500 gallon diesel fuel tank feed these generators through a pressure holding tank
- Alert Status – 24x7 monitoring of power equipment to include status of commercial power, generator power, fuel levels, temperature sensors, pumps and basins