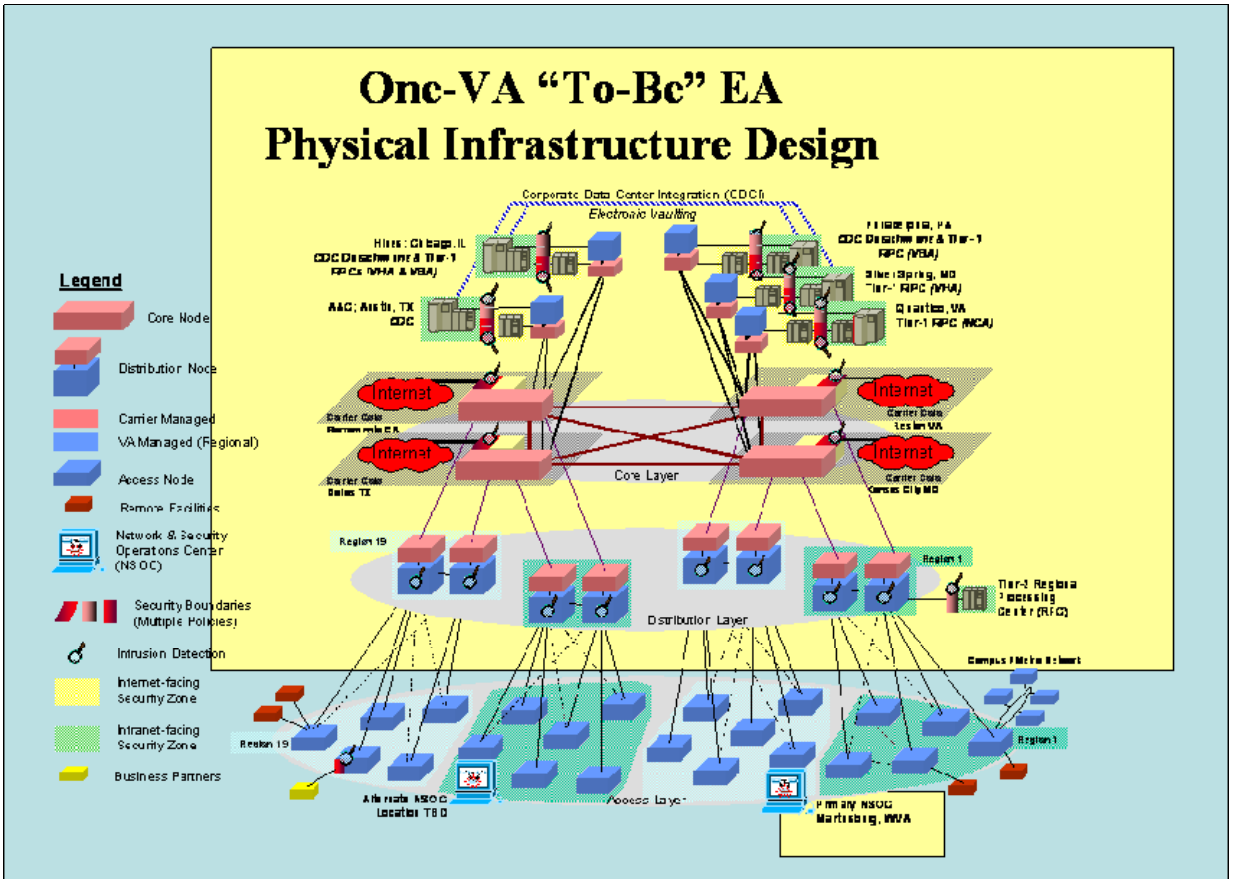
Veterans Affairs Backbone

The US Department of Veterans Affairs has begun a move to the next generation of IP communications with the gradual transition to Internet Protocol version six (IPv6). Per this endeavor, a common understanding must be established in defining the components of the network infrastructure in order to successfully take these steps. The initial transition for the agency will encompass the Intranet Backbone. This document will provide a definition for the Veterans Affairs network Backbone

From the perspective of the Enterprise, the Backbone spans the facilities, services and network devices needed for the functioning of data communication across the Veterans Affairs communities. This transport network from a TMP perspective uses the terms Core, Distribution, and Access layers to define network elements. In this case the Enterprise Backbone would span all network components contained in the Core, Distribution, and secure Enterprise Internet Gateways (ECSIP). This definition is better depicted in the illustration below:



****Note: Area in yellow only depicts two of the nineteen regions and four of the six Data Centers****

Items identified within the yellow highlighted area, are the elements defined as the VA Backbone which provide the transport for all remote offices and facilities which comprise the remainder of the Veterans network infrastructure (displayed in blue). An excerpt from the TMP architecture documentation describes the foundation of this definition

In following with the TMP Network Design Document specifications, each of the Regions and DCs will be dual-homed to the core via ***four distribution layer routers****. The two distribution routers directly connected to the core routers will be managed by Sprint.*

The ASs will also contain a ***pair of VA-managed distribution routers*** *which will connect to the Sprint-managed distribution routers. Since the VA-managed and Sprint-managed routers will be physically co-located, connectivity between them will be implemented using Fast Ethernet. This second pair of distribution layer routers was implemented in order to provide the region full policy control for routing and policies.*

The specific breakdown of Veterans Affairs National Backbone is detailed below:

Core Sites (4) - 4 routers
Corporate Data Centers (6) - 12 routers (6 DC * 2 carrier * 2 VA)
Distribution Sites (19) - 76 Routers (19 Regions*2 carrier*2 VA)
Network Operation Center (2) - 3 routers
Internet Gateways (4) - 6 Routers, 4 Firewalls, 4 VPN Appliances, 6 Intrusion Prevention Systems, 1 Internal DNS, 1 External DNS, 2 Web Caching Appliances, 2 ISA Servers, 2 Web Filters, 2 Web Accelerators, 2 Reverse Proxy Servers

VA Enterprise Backbone Logical Components

Routing/Addressing
Logically, a migration to IPv6 presents the opportunity for a fresh start in terms of address allocation. Future technical discussions will need to be conducted in order to refine specifics of how the Agency will handle distributing the IPv6 allocation. The routing protocols used by the VA Backbone for the most part are already IPv6 compatible. BGP and OSPF (used in the Core of the VA network) are standards based routing protocols and are already capable of running IPv6 natively or with the dual stack approach. EIGRP is the exception and testing is already underway for this routing protocol that is used primarily throughout the VA regions. Assurances have been provided by the hardware vendor (Cisco) that EIGRP will be fully capable for IPv6 in fiscal 2006. Further testing and design of the VA network will be necessary before IPv6 systems will be able to take advantage of IPv6 features such as stateless auto-configuration, encryption, and authentication.

IPv6 DNS
Domain Name Service (DNS) is not only an essential component of VA Intranet traffic, but also VA Internet destined traffic. DNS is something that must be considered before transitioning to IPv6. The current 32-bit name DNS servers cannot handle name-

resolution requests for the 128-bit addresses used by IPv6. To provide a mapping from a domain name to an IPv6 address, as well as an IPv4 address, a new DNS record type of "AAAA," or "quad A," has been defined. The current DNS infrastructure will need to be modified/upgraded or purchased new for IPv6 compatibility. Once the IPv6 DNS is in place, dual-stack hosts can interact interchangeably with IPv6 nodes. If a dual-stack host queries a DNS and receives back a 32-bit address, IPv4 is used; if a 128-bit address is received, then IPv6 is used. The migration down to the host level will not be prominent until after the initial Backbone transition for June 2008. Only limited systems for monitoring, management or IPv6 testing would require such capability during this period.

IPv4/v6 Network Management

Network managing and monitoring devices need to be included within the definition and planning of the Enterprise Backbone. The two National Network Operation Centers use various software/hardware tools and applications to administer the network infrastructure. Network management in a dual-stacked network can continue to be performed with IPv4 or with a new IPv6 address. The management systems, including IT Operations support systems, need to be aware of IPv6 and must run proper Simple Network Management Protocol (SNMP) stacks in order to perform IPv6-based management. These tools will need to be addressed independently with their respective vendors to ensure IPv6 capability during the planning stages of the transition.

Internet Gateways/Security

Transitioning of the VA Backbone will include the devices that comprise the VA National Internet Gateways (formerly ECSIP). Any IPv6 Internet circuit acquired for testing purposes constitutes a live Internet path and needs to be handled in a manner as such. IPv6 Internet connections brought into the VA Enterprise must follow best practices and adherence with all applicable VA mandates on securing such data paths that interconnect, to a level equal to or greater then the current VA Internet Gateway architecture. A recommendation is to create a parallel platform for initial IPv6 Internet testing based on a similar security framework. This test platform would be limited only to IPv6 test traffic initially, followed by a gradual migration of VA production traffic. The current thinking would introduce an Internet connection into the Enterprise for IPv6 testing prior to the full Backbone transition in 2008. From the Internet drop-off point regardless of the selection of service provider and platform, the VA can provision tunnels to/from internal VA endpoints that have a requirement or desire to participate with IPv6 testing.

This definition captures the Enterprise network as a snapshot for this period of time. As the Veteran Affairs network infrastructure continues to evolve up through the June 2008 transition deadline, these changes will need to be incorporated into any future planning moving forward for IPv6.