

11.3.9 Details on the Data Network Management Proposed Solution

11.3.9.1 Current Commonwealth Network

OVERVIEW

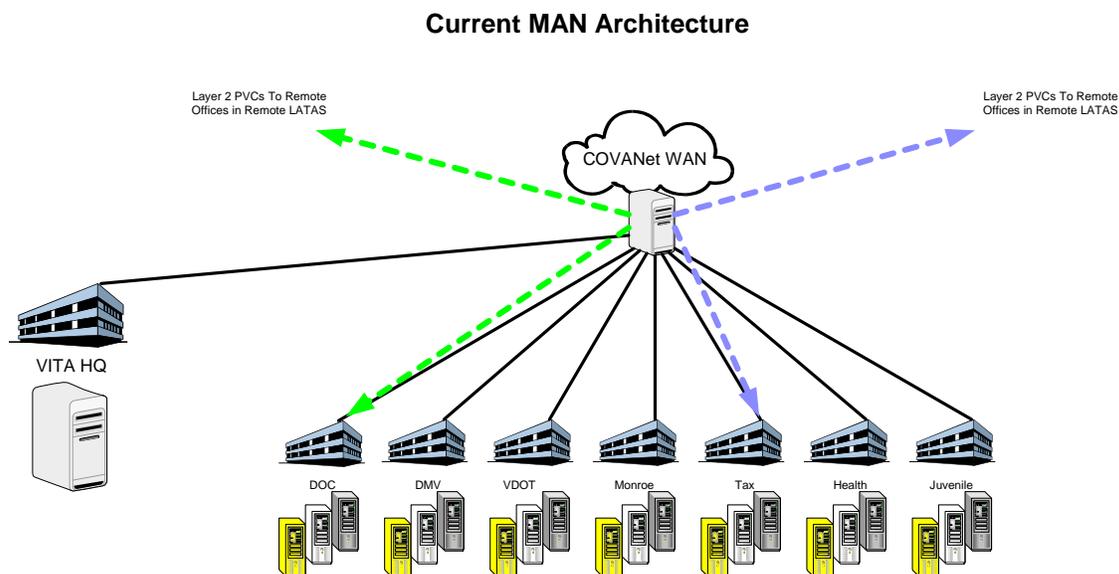
The Commonwealth of Virginia seeks a communications design to better serve its customers including citizens, businesses, other government entities, non-profit organizations, and all who must be licensed, regulated, or receive services. The patchwork of telecommunications systems in government causes delay and a loss of productivity for those who try to access Commonwealth agencies and departments.

As the needs and demands multiply, the Commonwealth needs to address the shortcomings of yesterday's network designs and position itself for a rational, planned evolution into a future network. The next generation optical network must be state of the art and adaptable to future applications.

The Commonwealth of Virginia's current network environment for the majority of the larger agencies consist of independent network deployments primarily designed to support each agency's business requirements. The current network backbone topologies for these agencies are a combination of single or dual homed circuits at various speeds including DS3s, OC3s and T1s. The agencies interconnect through CoVaNet or Network Virginia with MCI and Verizon the major Telco providers. The Commonwealth network backbone architecture is not a conventional Metropolitan Area Network (MAN) residing on a Synchronous Optical Network or SONET ring. The smaller agencies are interconnected through core backbones provided by DGS or VITA.

The Commonwealth's current Wide Area Network (WAN) is disparate where each remote site is provisioned directly to agency headquarters within Metro Richmond. Furthermore, many large agencies have deployed high-speed WAN aggregation points to accommodate remote sites accessing data located within agency headquarters. The level of duplication throughout the Commonwealth WAN is inefficient and is not leveraging common access paths that would reduce overall cost.

The following graphic illustrates the current Commonwealth network layout



11.3.9.2 Future Vision

The proposed architecture addresses the current and future characteristics of the various services and requirements. It provides a converged solution that effectively accommodates the characteristics, and also allows optimization of an efficient and cost-effective infrastructure and operating environment. It positions the Commonwealth of Virginia and our team to effectively manage the new converged network in a manner that is not achievable today.

Providing a comprehensive solution requires a vision of product integration and system expansion to meet diverse system requirements in an efficient and manageable environment. The next generation network will lead to central management of network services. One centralized entity will be responsible for the end-to-end operations and management of the network. The managed services may include routing, switching, backbone network transport, VPN, MPLS, Firewalls, Intrusion Detection Systems (IDS), Internet, voice and video. The services are managed across different planes including; infrastructure, configuration management, change management, billing management, security, SLA management, inventory, backup, and business continuance. The services will be monitored from a central Network Operations Center (NOC), with the capability of being managed in a redundant manner from an auxiliary site for fail-over, disaster recovery, or load sharing scenarios. The central service management entity will manage services and security policies with direct input from the agencies. The requirement of a centrally managed environment is the result of consistent and well-documented policies being followed across the Commonwealth network infrastructure that allows for ease of management, quality, quick problem determination, and lower costs.

Element management is a key component to the overall solution. The management tools implemented must provide end-to-end monitoring and provisioning capabilities of optical transport products. The management portfolio should be integrated with the existing management tools.

Among the primary goals of the converged solution are promoting the evolution of the existing network infrastructure. It will also allow the enabling of new services that will provide the Commonwealth of Virginia with increased efficiencies in the ability to accelerate new service offerings to various agencies. This will bolster both new and existing revenue streams, while realizing the economics associated with a truly converged network.

The need for multiple service capabilities requires that the foundation of the network to be built on an optical transport platform featuring near-instantaneous restoration around failures for the mission critical applications, yet allow for the upper layers to provide protection so that the network is not overbuilt with multiple protection schemes, the ability to transport a wide variety of protocols and bit rates, and the ability to scale economically. Our comprehensive recommended architecture would provide both technical and business merits to the issues of addressing total cost, quality, and service. The architecture of the network can be divided into three major categories: Transport solution, Switching/Routing, and Security.

11.3.9.2.1 Deploy fault tolerant optical Metropolitan Area Network in Phased Approach

The Commonwealth's next generation optical network architecture includes multi-layer switching platforms to comprehensively address the Commonwealth's network requirements. The use of optical transports, Layer 2/ Layer 3 switching and Multi Protocol Label Switching will provide a superior cost-effective solution for multiple bandwidth requirements.

The new network design will position the Commonwealth to meet its future network growth requirements with simple, low cost implementations. In this time of challenging state budgets, this network offers a low cost solution to the demanding and increasingly high-tech needs of the Commonwealth.

A primary driver of the Commonwealth network project is to enable the agencies, boards, and commissions of the Commonwealth to perform at maximum efficiency. As the Internet Age matures, citizens increasingly expect to communicate with government and to conduct business electronically and from a convenient location. Companies want to save time by applying for permits without having to stand in line. Commonwealth agencies need to be able to share information rapidly and accurately. And in a time when public safety and security is critical, reliability of communications cannot be compromised. The network needs to be always “on”, reliable, ready and secure.

The applications that support the services provided by the Commonwealth must be transported seamlessly and smoothly. The implementation, operation, and management of the network must focus on the elimination of risk and the provision of alternate routing paths and the automated fail-over of critical elements in order that the Commonwealth be positioned at all times to perform its functions.

Many Commonwealth agencies need increased bandwidth now or will need it soon. Commonwealth agencies need the ability to implement new bandwidth to new or existing locations to meet emergency service requirements. In order to be cost-efficient, the new network cannot be designed and built to bring huge bandwidth to every street address within the Commonwealth, and yet the network must provide the capability to bring huge bandwidth to selected locations as needed and within acceptable time frames. The ability to install and/or grow bandwidth as needed, cost-efficiently, is a key business driver for the network. Additionally, the network will need to be able to add new customers with incremental adjustments or additions without requiring replacement of expensive units.

The current network environment is not conducive to support a converged network infrastructure, which would allow the Commonwealth to offer advanced network services. Addressing this barrier, to create the true converged communications system requires secure, predictable and efficient services for a wide range of diverse applications on a common network. Our proposed network architecture will address the Commonwealth’s objectives to improve services for citizens; control costs and provides new services.

The Commonwealth of Virginia currently has what is termed as a distributed network model with point-to-point circuits provisioned across the Commonwealth. This type of network architecture is difficult to manage and deployment of new services, in a planned fashion across dissimilar networks, becomes cumbersome. By adopting a converged network architecture model focused on access control, proactive monitoring, and dynamic response capabilities, the proposed infrastructure will support new network services such as Voice and Video over IP. Our proposed converged network builds a foundation that support future applications and agency business requirements.

Virginia’s future network architecture in the broadest sense of the term sets the expectation of predictability in a system. When considering how to deliver a converged network to support Data/Video/Voice along with the rest of the business applications currently in use or soon to be implemented, a logical approach to the functions of that network can be used to define its capabilities. While the basic network designs of the past worked well enough for non-real-time data such as e-mail and Web traffic, the increasing threat of viruses and worms, along with the introduction of real-time applications to the network such as VoIP and Video on Demand, require fast, smart and efficient systems.

There are three keys to a converged network:

- Ability to control access,
- Ability of the network to offer protection to the devices and applications in use
- Incorporate consolidated high-bandwidth dynamic response architecture.

By adopting a converged architecture model of networking with security-centric thinking, and by focusing on access control, proactive protection, and dynamic response capabilities, the proposed

architecture supports new services like Voice and Video on a converged network while building a foundation equally applicable to future application or service.

Currently, the Commonwealth agencies are provided communications services via a number of different networks and contracts. In order to improve the networking capabilities of all entities, the Commonwealth Network project is designed to aggregate technical, service, and maintenance requirements to maximize performance.

In the current environment of multiple networks and service providers, resources are expended in an inefficient fashion, with costly duplication of effort and staffing. The new Commonwealth network will enable the technologies that allow for integration of communications functions, and leverage the Commonwealth's various communications resources to increase overall efficiency. Concentrating network operations in a centralized environment will enable Commonwealth wide efficiencies.

To properly prepare for a network initiative of this scale and complexity, an analysis of current traffic and trending is paramount for future network design. The data acquired through Due Diligence provided tremendous insight for network topologies throughout various agencies, however detailed network usage statistics were not accessible. Prior to consolidation activities concerning network MAN and WAN, data will be collected to establish baseline and future bandwidth requirements. The bandwidth requirements will be analyzed to accurately project hardware components necessary to architect the Commonwealth MAN and WAN. Any required fiber infrastructure for the core backbone will concurrently be engineered and deployed in parallel as data is captured.

11.3.9.3 Key Network Objectives

The proposed Data Networking solution is designed to meet the following key objectives:

- Create highly reliable and available network that provides flexible and scalable connectivity Commonwealth-wide
- Consolidate the wide range of disparate links and networks currently supporting Commonwealth agencies to achieve operational efficiencies and simplified management
- Standardize and simplify the service offerings for better alignment with agency needs, provide ease of administration and decrease operational cost
- Take advantage of current technology to improve functionality, throughput and performance, to support emerging applications, and to meet or exceed required service levels
- Leverage skills and knowledge of current VITA Data Network staff by effectively integrating them with the future Network Operations Center and support organization

In addition to the above key objectives the following added benefits would be achieved:

- Rapid Deployment of new services
- Effective network aggregation for communication needs
- Preparedness for communications convergence
- Proactive to user needs

The first phase in migrating the Commonwealth Network is to deploy a Metropolitan Area Network, which will serve as the core network backbone for each agency.

11.3.9.4 Build Metropolitan Area Network

An optical backbone will be deployed within the Metro-Richmond downtown area to support each of the key objectives stated in the previous section and to provide adequate bandwidth in preparation for the consolidation of targeted data services. The Commonwealth MAN will function as the core backbone for most agency connectivity requirements and provide the foundation for all telecommunications services.

An analysis of the current high-speed links supporting agencies within Metro-Richmond has provided us with insight for determining locations for MAN access points. The table below illustrates a preliminary list of agencies and their respective locations. Additional assessments after commencement will be necessary to validate these locations.

	Agency Name	REMOTE CITY	REMOTE STREET
1	BOARD OF ACCOUNTANCY	RICHMOND	3600 WEST BROAD STREET
2	CHARLES CITY CO.	CHARLES CITY	10702 COURTHOUSE ROAD
3	CHARLES CITY CO.	CHARLES CITY	10900 COURTHOUSE ROAD
4	COMM. SVCS. BD., DISTRICT 19	PETERSBURG	20 W. BANK ST., SUITE 2
5	DEPARTMENT OF EMERGENCY MANAGEMENT	RICHMOND	10501 TRADE COURT
6	DEPARTMENT OF ENVIRONMENTAL QUALITY	GLEN ALLEN	4949-A COX ROAD
7	DEPARTMENT OF ENVIRONMENTAL QUALITY	RICHMOND	629 EAST MAIN ST., 2ND FLOOR, COMPUT
8	DEPARTMENT OF ENVIRONMENTAL QUALITY	GLEN ALLEN	4949-A COX ROAD
9	DEPARTMENT OF FIRE PROGRAMS	RICHMOND	101 N 14TH ST., 18TH FL.
10	DEPARTMENT OF HEALTH	RICHMOND	109 GOVERNOR ST.,
11	DEPARTMENT OF HEALTH	RICHMOND	1601 WILLOW LAWN DRIVE
12	DEPARTMENT OF JUVENILE JUSTICE	RICHMOND	700 E. FRANKLIN ST. 5TH FL SERVER R
13	DEPARTMENT OF JUVENILE JUSTICE	CHESTERFIELD	9500 COURTHOUSE RD. CIRCUIT COURT B
14	DEPARTMENT OF MOTOR VEHICLES	RICHMOND	2300 WEST BROAD STREET 2ND FLOOR
15	DEPARTMENT OF REHABILITATIVE SERVICES	RICHMOND	8004 FRANKLIN FARMS DR., LEE BLDG
16	DEPARTMENT OF SOCIAL SERVICES	RICHMOND	7 NORTH 8TH STREET
17	DEPARTMENT OF SOCIAL SERVICES	CHARLES CITY	10600 COURTHOUSE ROAD
18	DEPARTMENT OF SOCIAL SERVICES	CHESTERFIELD	9501 LUCY CORR DRIVE
19	DEPARTMENT OF STATE POLICE	RICHMOND	7700 MIDLOTHIAN TRNPK.
20	DEPARTMENT OF STATE POLICE	RICHMOND	900 EAST MAIN STREET, COMPUTER ROOM
21	DEPARTMENT OF TAXATION	RICHMOND	2220 WEST BROAD ST
22	DEPARTMENT OF TAXATION	RICHMOND	DS3 FOR TAX DEPARTMENT
23	DEPARTMENT OF TRANSPORTATION	RICHMOND	1221 E. BROAD ST.
24	DEPARTMENT OF TRANSPORTATION	CHESTER	2201 WEST HUNDRED ROAD
25	DEPARTMENT OF TRANSPORTATION	MIDLOTHIAN	3301 SPEEKS ROAD
26	DEPARTMENT OF TRANSPORTATION	PETERSBURG	4608 BOYDTON PLANK ROAD
27	DEPARTMENT OF TRANSPORTATION	ASHLAND	523 N. WASHINGTON HIGHWAY
28	DEPARTMENT OF TRANSPORTATION	SANDSTON	6020 ELKO TRACT ROAD
29	DEPARTMENT OF TRANSPORTATION	RICHMOND	800 E. LEIGH STREET 3RD FLOOR
30	DEPARTMENT OF TRANSPORTATION	COLONIAL HEIGHTS	PINE FOREST DRIVE
31	DEPT OF ALCOHOLIC BEVERAGE CONTROL	RICHMOND	2901 HERMITAGE RD.
32	DEPT OF MEDICAL ASSISTANCE SERVICES	RICHMOND	4300 COX ROAD, 1ST FLOOR, DATA CENTE
33	DEPT OF MEDICAL ASSISTANCE SERVICES	RICHMOND	600 E. BROAD ST., SUITE 1300
34	MENTAL HEALTH/RETARD & SUBS ABUSE SERVS	RICHMOND	1220 BANK STREET UPPER BASEMENT CO
35	PUBLIC DEFENDER COMMISSION	RICHMOND	701 E. FRANKLIN ST., SUITE 1416
36	RADFORD UNIVERSITY	RICHMOND	110 S. 7TH ST.
37	STATE BOARD OF ELECTIONS	RICHMOND	9TH ST. OFC. BLDG. RM. 101
38	STATE CORPORATION COMMISSION	RICHMOND	1300 E. MAIN ST., 7TH FL.
39	SUPREME COURT	RICHMOND	100 N. 9TH ST., 3RD FL.
40	SUPREME COURT	RICHMOND	400 NORTH NINTH STREET, 2ND FLR, CL
41	VA INFO PROVIDERS NETWORK OF VITA	RICHMOND	1111 E. MAIN ST., SUITE 901
42	VA WORKERS' COMPENSATION COMMISSION	RICHMOND	1000 DMV DR., INFORMATION SYSTEMS,
43	VCU ACADEMIC DIVISION	RICHMOND	1101 EAST MARSHALL STREET, SANGER H
44	VIRGINIA EMPLOYMENT COMMISSION	RICHMOND	703 E. MAIN ST., 2ND FL., ROOM 203
45	VIRGINIA INFORMATION TECHNOLOGIES AGENCY	RICHMOND	202 NORTH 9TH STREET
46	VIRGINIA RETIREMENT SYSTEM	RICHMOND	1200 EAST MAIN ST.
47	VIRGINIA STATE BAR	RICHMOND	707 E. MAIN ST., SUITE 1500

The Commonwealth MAN will be built in phases to accommodate current agency requirements as well as support future initiatives such as data consolidation.

The initial phase will establish a core network backbone infrastructure with high-speed Ethernet Links. Verizon's Transparent LAN Services, TLS is a fiber-based network service that uses a high-speed backbone to provide an Ethernet LAN interconnection at native LAN speeds of 10Mbps, 100Mbps and Gigabit Switched Ethernet. Verizon's TLS service is a turnkey solution that is specifically tailored to meet LAN and MAN interconnection requirements without the expense of any new customer premises equipment.

TLS Benefits include:

- **No additional Customer Premise Equipment investment.** Agencies may connect to the MAN directly through an Ethernet switch.
- **Standard customer interface.** The service delivers an interface conforming to Ethernet 802.3z (Gigabit Ethernet), Ethernet 802.3u (Fast Ethernet) and Ethernet 802.3 (10M Ethernet).
- **Protection of data and privacy.** Specialized screening software helps ensure secure transmission of sensitive data.
- **Resilient circuit configurations.** In the event of a failover, Verizon's Protected Access Line feature can quickly and seamlessly transfer your data to a back-up circuit.
- **Scalability.** Adding new locations to the network is non-intrusive with no interruption in your current service. Additionally the expansion from 10 to 100 MBS does not require port changes, Gigabit service requires an interface upgrade or switching to an existing CPE's gigabit port.
- **Cost savings.** Switched Ethernet Service offers a monthly flat fee structure and no per-use charges for maximum convenience, efficiency and affordability.

11.3.9.4.1 Phase I Agency MAN Migration

The phased approach to architect the MAN infrastructure will coincide with the consolidation of Data Services. The core backbone design is inherently scalable and flexible to allow for modification of bandwidth requirements. The initial phase of the MAN will coincide to support data consolidation initiatives. The MAN will evolve to provide the backbone for all telecommunication services for the Commonwealth.

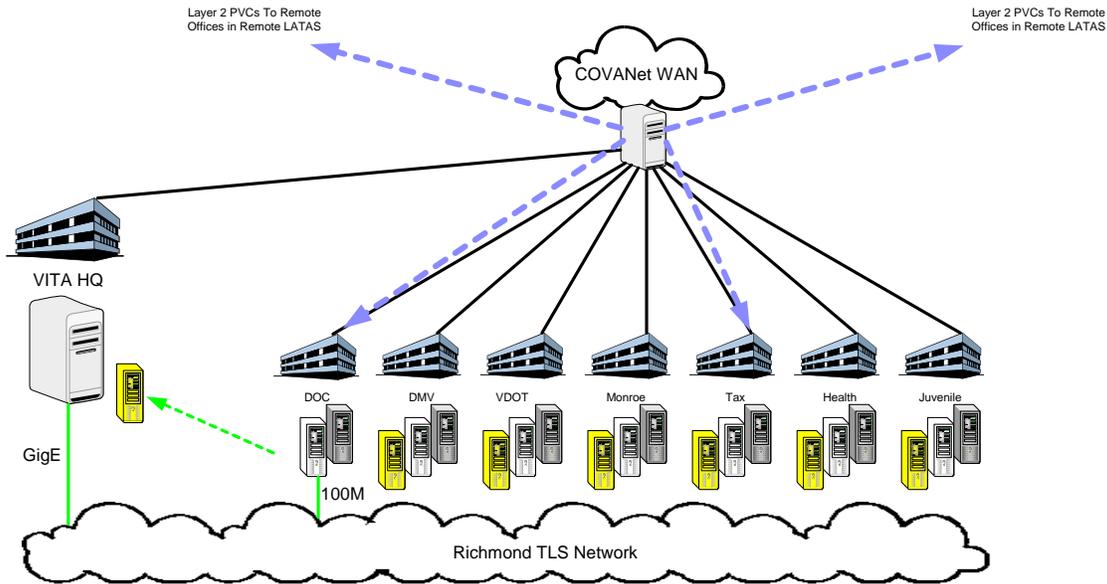
The Migration team has initially identified E-Mail services for Commonwealth Agencies to be consolidated. The schedule and details as (**defined in section 11.3.7**) will directly correlate with the MAN rollout. The network access points established for the MAN will precede the agency cutovers by approximately 30 days to assure MAN connectivity is functional. Current high-speed links for larger agencies will remain to support remote sites, the transition of those circuits will occur during future phases.

MAN connectivity will be established and tested to designated agencies and VITA Richmond Plaza to accommodate E-Mail server consolidation. Agency access points with bandwidth allocations of 10 and 100 MB and 1 Gigabit will be interconnected with Richmond Plaza. Verizon's TLS Service is very flexible and may be upgraded or downsized according to bandwidth demands.

The following graphic below depicts an example of an agency cutover to the Verizon TLS Service while maintaining current COVANET connections to agency WAN. VITA Richmond Plaza will maintain Email servers prior to the Commonwealth's state of the art new Data Center and also will interconnect to the TLS MAN.

MAN Migration

Phase 1: Enable TLS Ethernet Service to Example Agency Relocate Email Server(s)



11.3.9.4.2 Phase II – Agency MAN Migration

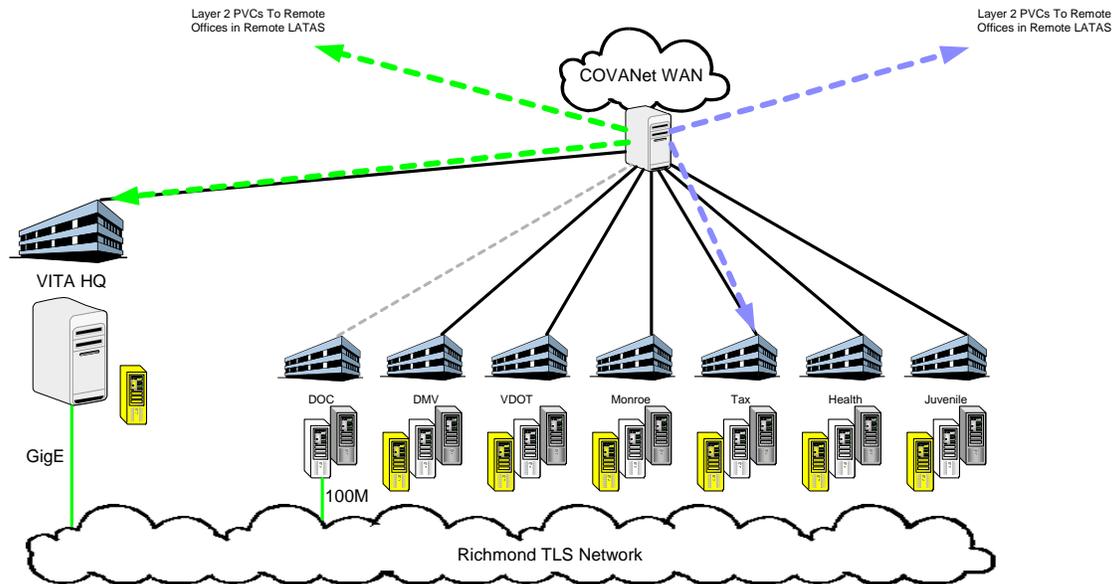
The MAN connectivity will be established for agencies that are slated for initial E-Mail services consolidation and continue to evolve. The data centers for larger agencies currently are interconnected with multiple high-speed circuits to CovaNet to support remote sites. These circuits are the aggregate WAN circuits that currently terminate within agency headquarters. These links will be re-provisioned through the Commonwealth MAN to Richmond Plaza and CovaNet circuits will be phased out. The circuits pertaining to the remote WAN locations will not be altered during this phase.

An analysis of bandwidth allocated to Richmond Plaza will be monitored and increased as the various agencies' links are moved to the Richmond Plaza location. The data traversing the MAN to agency headquarters will increase as agency remote sites are transitioned.

The graphic below depicts an example of the logical cutover for agencies migrating their aggregate WAN circuits and the elimination of the CovaNet circuit at agency's headquarters.

MAN Migration

Phase 2: Re-Provision Agency Headquarters WAN PVCs Remove Agency CovaNet DS3/OC3 Connection



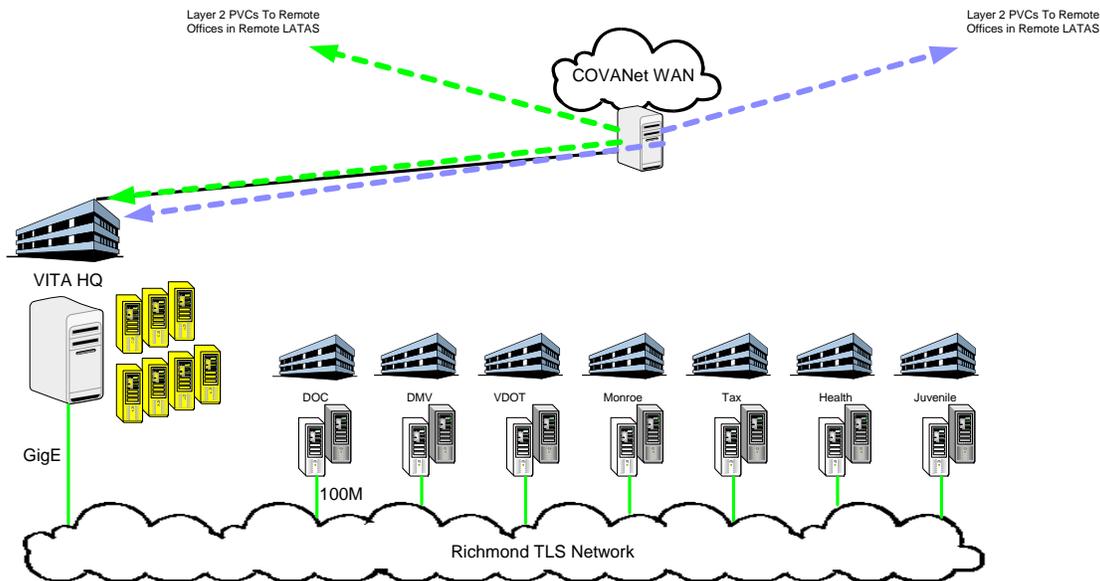
Phase II continued – Agency MAN Migration

The MAN migration progression will evolve to include each agency within the Commonwealth designated for MAN access. The deployment for MAN connectivity to these agencies will precede the agency E-Mail services consolidation schedule as previously mentioned (**more details provided in section 11.3.7**). The initial cutover will prepare the migration team with valuable forecasting insight with regard to bandwidth allocation. The flexible and scalable characteristics inherent within the Commonwealth MAN design will allow for non-intrusive bandwidth modifications from 10 to 100 Mbs.

The graphic below illustrates the remaining agency cutovers to the Commonwealth MAN and the completion of agency E-Mail services consolidation.

MAN Migration

Phase 2 continued: Agencies transitioned to MAN
Email Consolidation Completed



11.3.9.4.3 Phase III – MAN Migration – New Data Center

The Commonwealth MAN will be established and include each of the designated agency locations. The migration team will concurrently identify a location within the Metro Richmond area to host a State-of-the-Art Data Center. The MAN architecture, initially consisted of Verizon TLS Ethernet services, will evolve to include an optical SONET ring that will interconnect Richmond Plaza, the new Commonwealth Data Center and the existing MAN.

The Verizon TLS service will be augmented and provide additional protection and redundancy at MAN locations. A SONET based Resilient Packet Ring (RPR) will be deployed at key points to include the New **Redacted** Data Center, the current VITA Data Center, and two Verizon Central Office TLS switches. RPR is a new standard that was developed in an effort to bring SONET-like abilities to metro Ethernet networks by adding support for a ring topology and fast recovery from fiber cuts and link failures at Layer 2

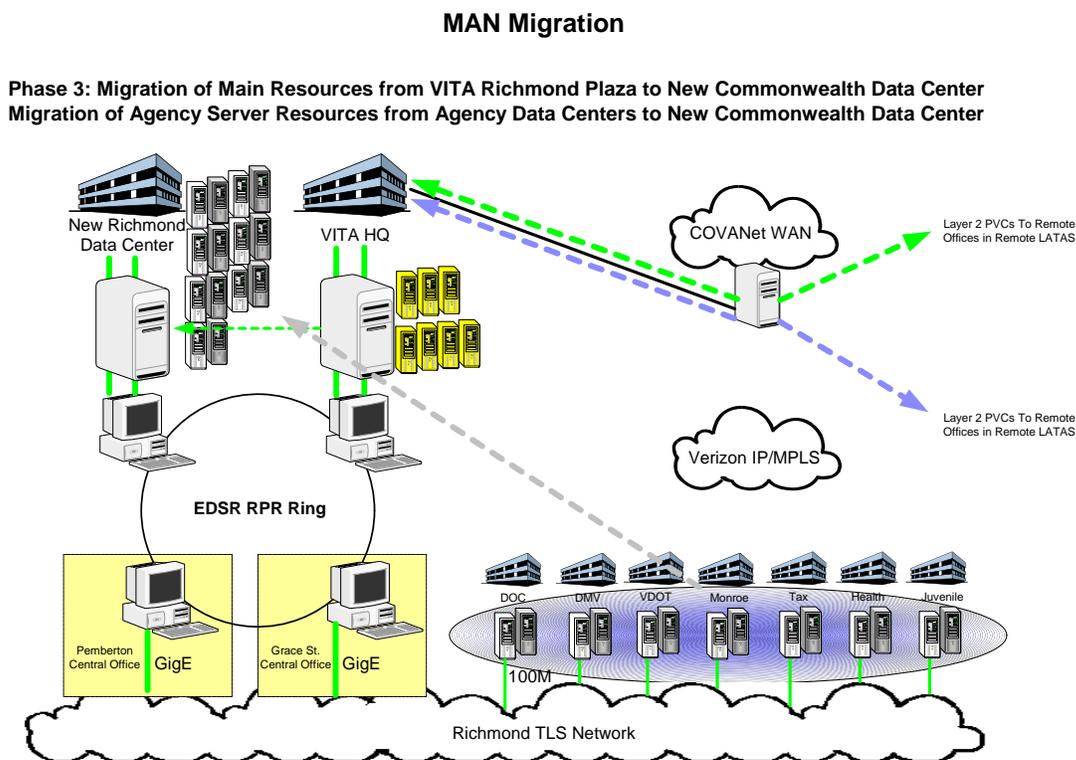
RPR uses Ethernet switching and a dual counter-rotating ring topology to provide SONET-like network resiliency and optimized bandwidth usage while delivering multipoint Ethernet/IP services. RPR maintains its own protection scheme and when a failure is detected, the RPR switching mechanism restores networks in less than 50 milliseconds.

The RPR technology provides the ability to offer voice services over Ethernet in the future. RPR also uses statistical multiplexing so that bandwidth can be oversubscribed, while establishing committed information rate (CIR) and peak-rate thresholds on a per-application basis. This guarantees each enterprise application Quality of Service and the ability to take advantage of the peak rates when bandwidth is available. This offering permits each agency to incur only defined CIR charges regardless of use, while taking advantage of peak or burst rate bandwidth.

This technology may be more widely deployed throughout the Metro Richmond area as additional services warrant expansion. The initial deployment will concentrate on data center consolidation with the flexibility to extend these capabilities to the remote locations, as needed.

The Commonwealth MAN has been built to provide adequate bandwidth for E-Mail consolidation for the initial phases. Additional consolidation initiatives including file and application servers will occur following the establishment of the Commonwealth's new state-of-the-art Data Center. Some agency data centers will continue to host application defined prior to migration. **(Details for this activity located in section 9.0)** The network infrastructure at the agency data centers will be scaled back to reflect the change in agency requirements.

The graphic below illustrates the continued MAN Migration with the introduction of the Commonwealth Data Center, a SONET Ring over RPR technology and additional Data Consolidation:



11.3.9.5 Migration of Wide Area Network

CURRENT WAN OVERVIEW

As previously stated the Commonwealth of Virginia currently has what is termed as a distributed network model with point-to-point circuits provisioned across the Commonwealth. Over time, these types of networks become more difficult to manage. Deployment of new services, in a planned fashion across dissimilar networks, becomes cumbersome. The deployment of a converged network will allow the use of advanced access methods and the collaboration of multimedia devices accessing the same network. In many cases, these devices can't use the traditional network model of provisioning a T1 for every need. By adopting a converged architecture model of networking as well as focusing on access control, proactive monitoring, and dynamic response capabilities, the proposed architecture will support new network

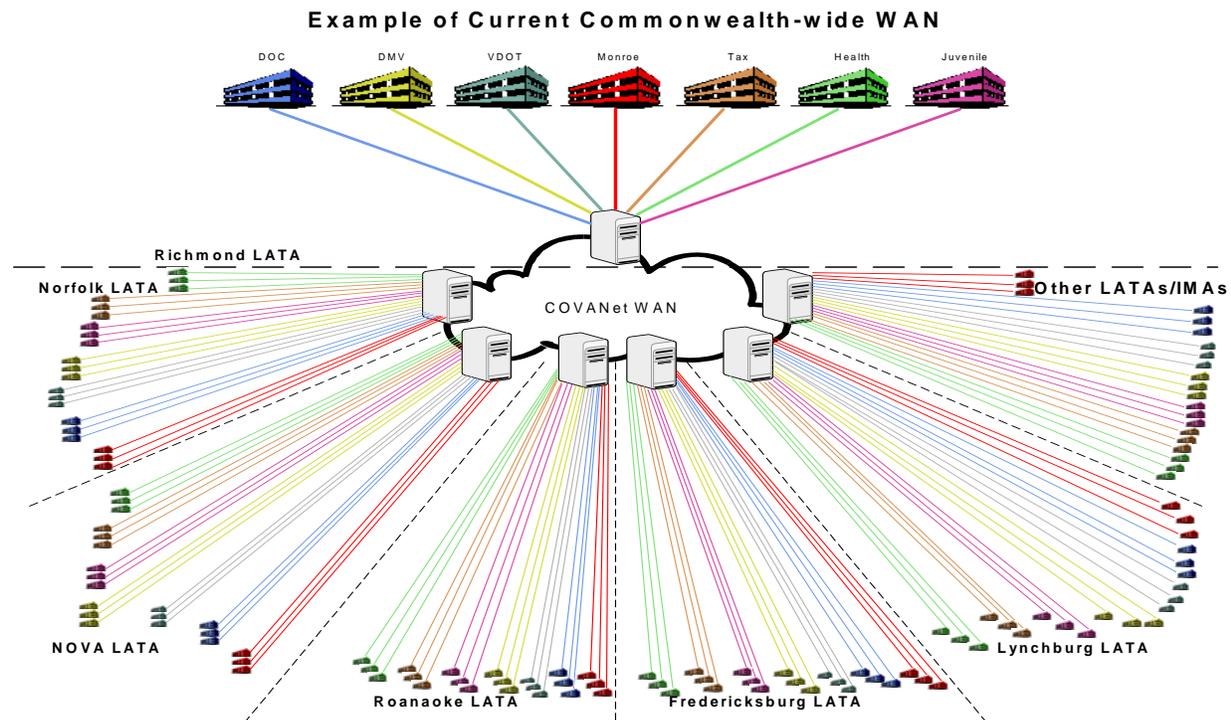
services such as Voice and Video on the converged network while building a foundation that is equally applicable to future applications or service requirements.

The data acquired through the Due Diligence process identified network protocols traversing the Commonwealth MAN and WAN is primarily TCP/IP. There may be some exceptions at agency locations but it is our assumption that MAN related data is TCP/IP with limited Data Link Switching, which is also referred as SNA 'tunneling' under TCP/IP.

The proposed Data Networking solution is designed to meet the following key objectives:

- Consolidate the wide range of disparate links and networks currently supporting Commonwealth agencies to achieve operational efficiencies and simplified management
- Standardize and simplify the service offerings for better alignment with agency needs and ease of administration
- Take advantage of current technology to improve functionality, throughput and performance, to support emerging applications, and to meet or exceed required service levels
- Leverage skills and knowledge of current VITA Data Network staff by effectively integrating them into the new Vendor/Partnership organization

The following graphic illustrates an example of the current WAN network layout displaying multiple point-to-point circuits throughout the Commonwealth for various agencies:



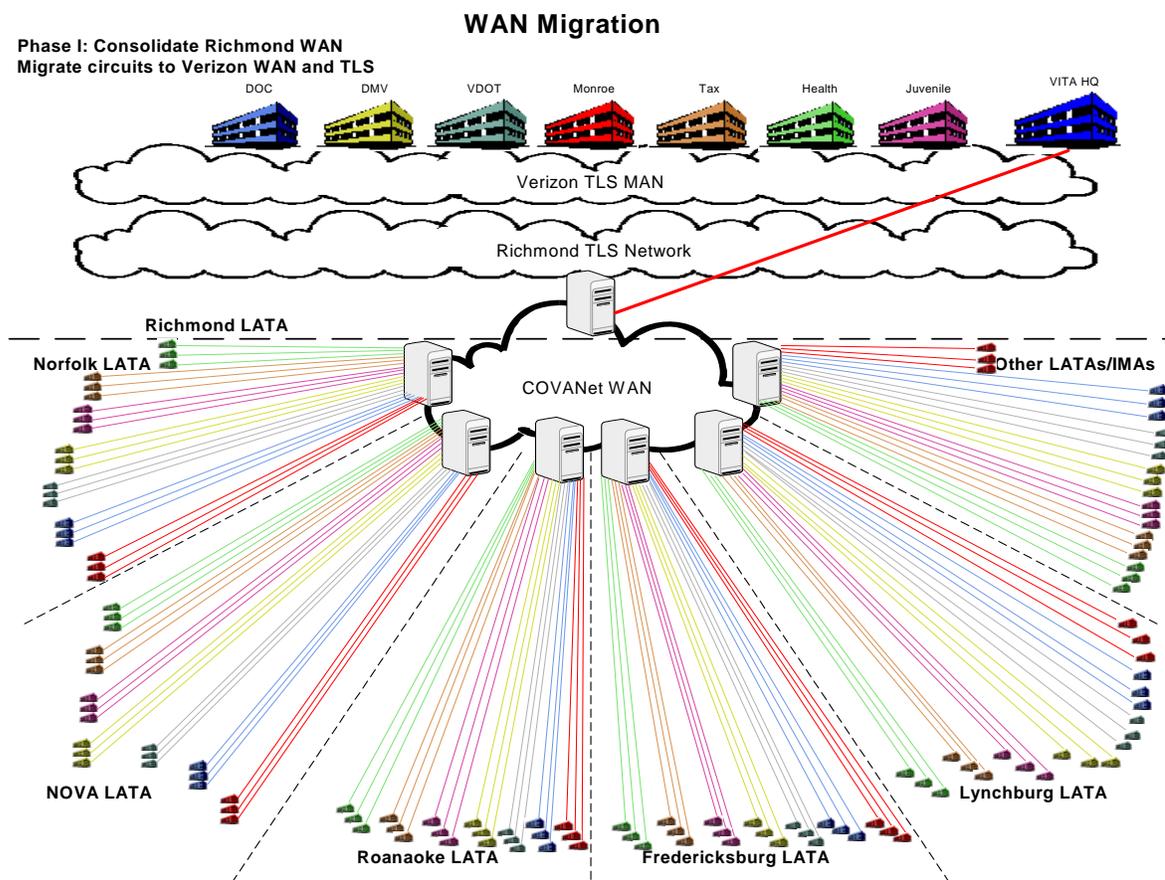
Phase I –WAN Migration

The WAN Migration will eliminate redundancy and overlap that exist in the current state. The inefficiency of multiple circuits routed individually with Point-to-Point connection from remote sites is cost prohibitive and difficult to manage. The diagram below represents the distribution of Points of Presence (POP) throughout the Commonwealth to support network aggregation points. There are multiple

Verizon POPs that will support network service to the customer locations throughout the Commonwealth. The primary goal of this initiative is to leverage local POPs within several Local Access Transport Areas or LATAs, to leverage economies of scale and reduce overall WAN cost.

The initial tasks will focus on identifying Commonwealth agencies circuits within common LATAs that may be candidates for consolidation. This initiative has begun with an analysis of Due Diligence data and a preliminary assessment has been developed based solely on logistics. Following commencement this analysis will be more in-depth to understand potential challenges such as security risks and existing agency mandates. Based on our initial finding we have targeted a reduction of 20 % of the existing WAN, which will result in a cost savings of at least 20 %.

The first phase will concentrate on consolidating the local WAN circuits within the Richmond LATA and migrating them to Verizon TLS services. The following graphic illustrates the first phase of WAN consolidation:

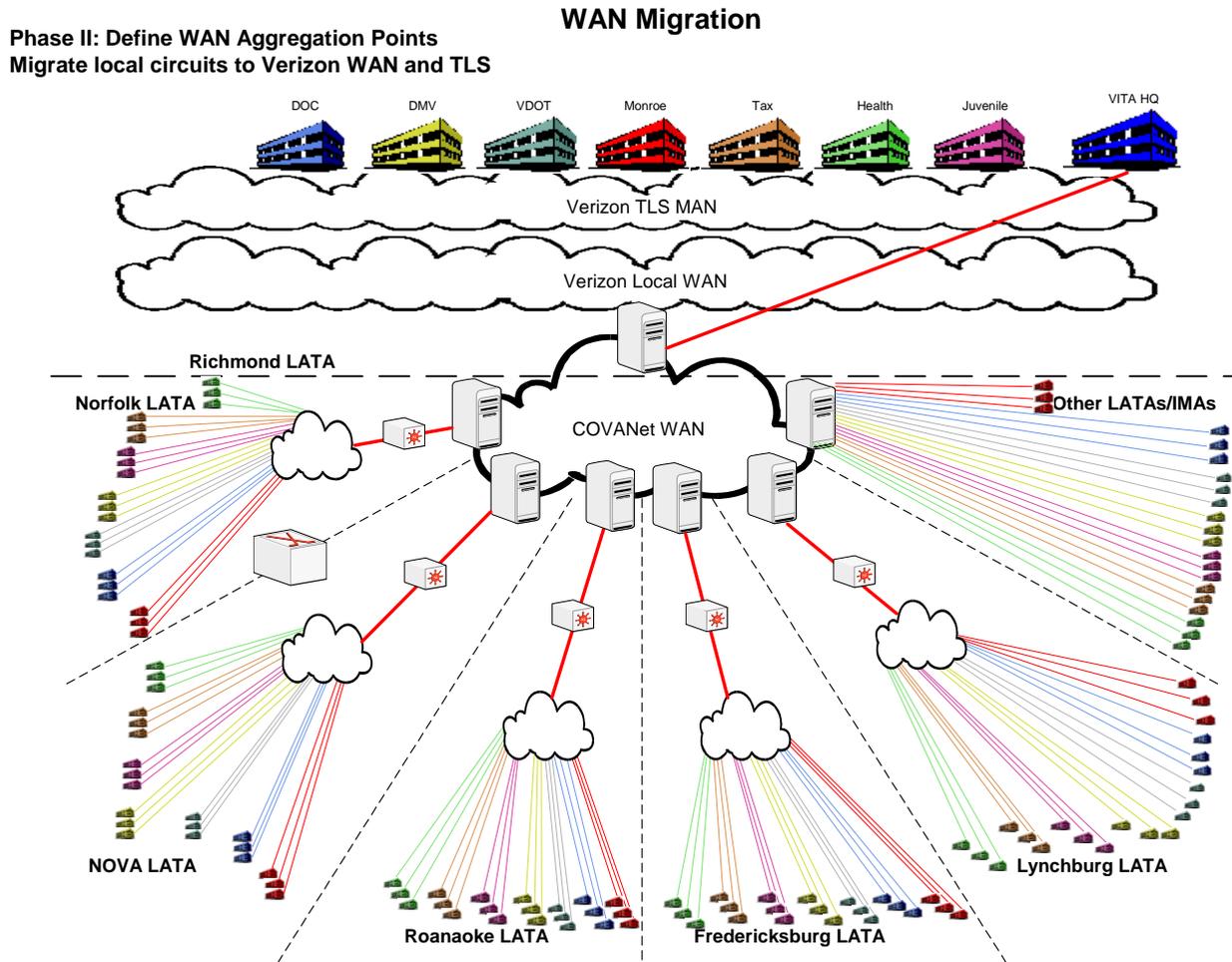


Phase II and III – WAN Migration

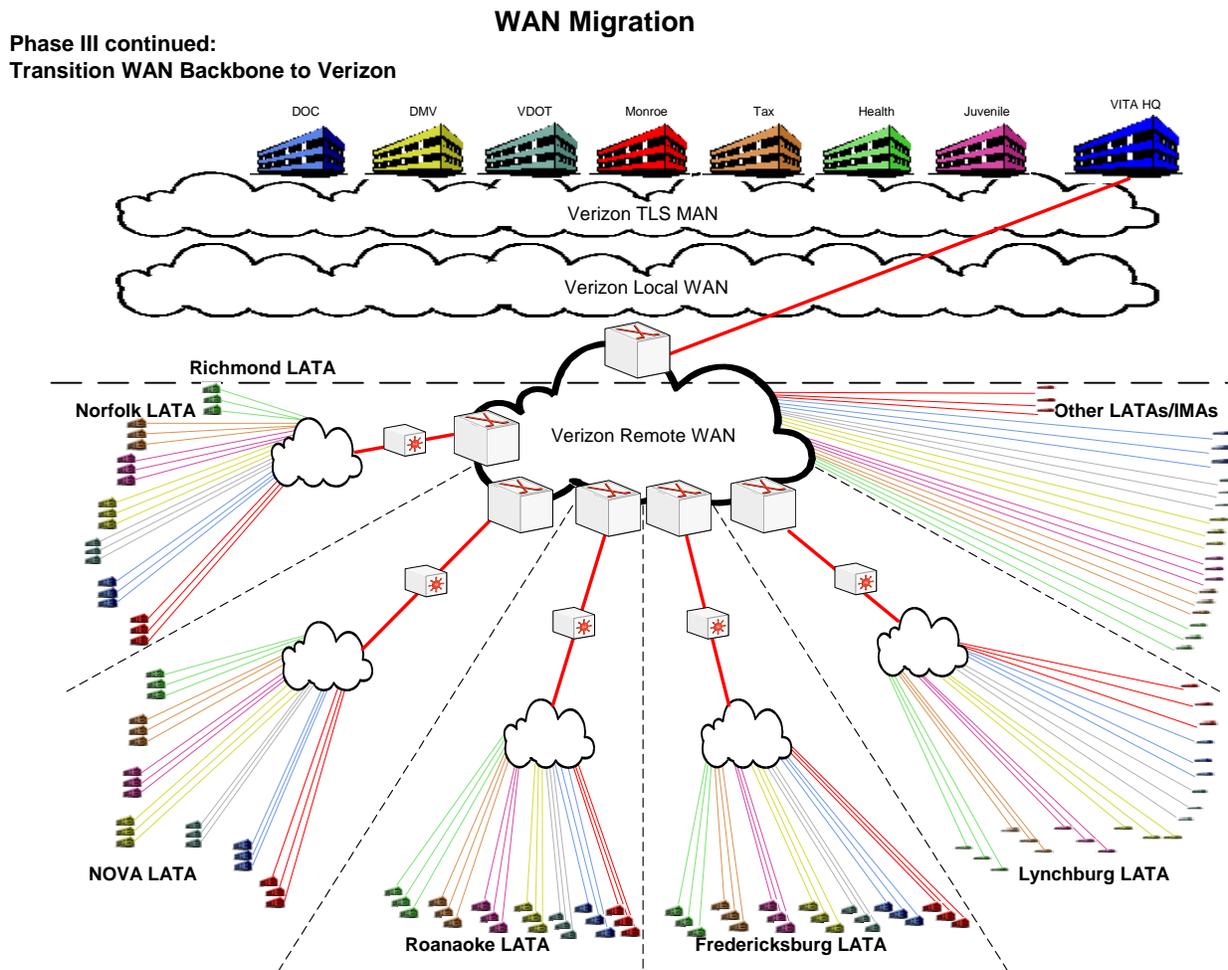
The WAN Migration will evolve to include remote aggregation points defined prior to the transition of the Commonwealth WAN. These sites will be determined through additional due diligence analysis and proper business justification with agency stakeholders. The WAN Migration will continue in an iterative fashion with the identification of aggregation points within various LATAs throughout the Commonwealth. The final phase of the migration will include CovaNet WAN re-provisioned to the new Commonwealth's WAN provided by Verizon. A thorough analysis of the current Commonwealth WAN

environment will be performed prior to any transition to determine the most practical and cost efficient solution for the Commonwealth.

The following graphic illustrates an example of Phase II of the WAN Migration:



The following graphic illustrates an example of Phase III of the WAN Migration:



11.3.9.6 Local Area Networks LANs

CURRENT LAN OVERVIEW

The LAN at remote Commonwealth sites and agency headquarters is a heterogeneous environment consisting of multiple platforms and vendors. The majority of larger agencies have standardized on Cisco Systems and Nortel Networks. The remote sites LANs for the smaller agencies are a mix of Cisco, Nortel and third party vendors, with some outdated equipment lacking maintenance support. The primary LAN media is Ethernet, with some Token Ring.

LAN Migration

The future strategic direction for the LAN architecture for the Commonwealth of Virginia will include a robust switching solution. The approach to achieve this architecture is to provide an infrastructure that is scalable, intelligent, and reliable to meet converged network requirements. Industry leading LAN Switches will be used to provide intelligent connectivity to accommodate for high-speed data access, segregation of traffic, Intranet and Video content distribution networks. The switching solution will

provide superior Quality of Service (QoS) feature sets as well as cater to the multicast routing requirements. Most Layer 2 manufactures provide switches that feature rich, scalable switching solution with modularity. The Switch architecture will support thousands of VLANs, and be designed to segregate traffic and provide for aggregation points throughout the converged networks.

The LAN will also require a ‘refresh strategy’ to address current and future hardware platforms. We have analyzed the data provided during Due Diligence and have developed a preliminary assessment. At the time of commencement this data will require validation. We have selected criteria to assist with determining the lifecycle for current LAN equipment and created a refresh strategy. The antiquated LAN equipment will be targeted immediately after the initial transition period, which is yet to be determined. There may be exceptions to these timelines for legacy LAN equipment such as Token Ring, where application specific protocols or hardware may be adversely affected. Proper analysis of legacy LAN hardware in conjunction with strategic application direction will be major factors in response to these potential circumstances.

Emerging LAN technologies such as wireless LANS will also be included as a service offering. The benefits for these offering are infrastructure cost savings as well as rapid deployment timeframes. Security must be tightly integrated for all wireless solutions and policies as **defined in section 11.3.4**

11.3.9.7 TCP/IP Addressing and DNS

OVERVIEW

The Commonwealth agencies manage their individual TCP/IP addressing requirements and DNS resolution with VITA Central responsible for allocating address pools and core network backbone links. There is redundancy throughout the Commonwealth Network for administrative tasks and hardware deployment.

Migration

The future IP addressing scheme for the Commonwealth network will concentrate initially for core backbone nodes in preparation for the MAN Migration and will not affect remote sites. The MAN Migration will necessitate two autonomous networks until completion. To accomplish this task Border Gateway Routing will be engineered to connect the legacy MAN and future MAN environments. Once this migration is complete the Commonwealth will revert back to one autonomous network.

- Highly scalable IP core addressing – The detailed design will include an IP address plan to support the migration of agencies to a Commonwealth TLS MAN. The address plan for the Core MAN Network, which includes Verizon backbone edge nodes and Customer Premise Equipment (CPE) router interfaces, will be based on an unused Commonwealth of Virginia block of public addresses.
- Agencies retain local IP addressing – Agencies will retain their current LAN IP address plan. Agencies that are currently performing Network Address Translation (NAT) to transverse a public cloud or the Internet will continue to do so. Those agencies that are performing NAT to tie disparate local agencies with overlapping private addresses together will continue to perform NAT or would require changing the IP address scheme.

The Commonwealth will centralize DNS services with local DHCP and internal DNS services – The architecture design for the core network will be integrated with future initiatives such as implementation of Microsoft Active Directory and server consolidation efforts. **Reference Section 11.3.8 for more details**

11.3.9.8 *Internet*

OVERVIEW

The majority of agencies within the Commonwealth independently provide Internet access for their employees and business partners. The current level of redundancy and the absence of an overall Internet security policy may leave the Commonwealth's network vulnerable. Furthermore, many agencies utilize these redundant links to communicate with each other instead of over a common infrastructure. The current environment presents challenges with regard to routing loops and potentially creates 'back doors' into the Commonwealth's network.

Internet Migration

The Commonwealth would benefit from an Internet solution strategically focused on a common architecture. Agencies today have Internet connections with excess capacity and the Commonwealth should leverage this with combined aggregation points. A centralized architecture will allow customers and employees Internet performance that is predictable and reliable with redundant access points interconnected with the Commonwealth MAN.

The Internet migration will also provide a centralized point to focus security resources, which will lower administrative cost. An enterprise security plan and policy is less complicated and easier to control, monitor and enforce with limited points or "back door" connections to the Internet.

In addition to meeting recommended security standards of consolidating Internet access, the practice of eliminating individual agency Internet connections is a key cost savings measure. It is expected that some exceptions will exist for agency mandates and business justifications meriting existing Internet access to remain.

The major benefits for the Internet Migration will be:

- Lower administrative cost
- Elimination of redundancy, reduced circuit cost
- Increased efficiency
- Increased security controls

11.3.9.9 *Remote Access (Virtual Private Networks)*

OVERVIEW

The Commonwealth today provides Remote Access and VPNs within most large agencies. They are managed and administered separately and the hardware is a mix of vendors with Cisco and Nortel being the main providers. There are limited pools of dial-in access for users utilizing analog lines with most employees primarily connecting to Commonwealth resources via Access VPNs. Some agencies provide Extranet VPN connections to business partners, which are separate from the internal network at some agencies such as the Virginia Department of Transportation. Intranet VPNs also are deployed in a few circumstances to connect remote agency locations to agency data centers

Below is a description of various VPN types utilized within the Commonwealth:

- Access VPNs – Provide remote access to an enterprise customer's intranet or extranet over a shared infrastructure. Access VPNs use analog, dial, ISDN, DSL, mobile IP, and cable technologies to securely connect mobile users, telecommuters, and branch offices.

- Intranet VPNs – Link enterprise customer headquarters, remote offices, and branch offices to an internal network over a shared infrastructure using dedicated connections. Intranet VPNs differ from extranet VPNs in that they only allow access to the enterprise customer’s employees.
- Extranet VPNs – Link outside customers, suppliers, partners, or communities of interest to an enterprise customer’s network over a shared infrastructure using dedicated connections. Extranet VPNs differ from intranet VPNs in that they allow access to users outside the enterprise

Remote Access Migration

The Commonwealth Remote Access platform should be aligned with the Internet strategy, which will leverage common infrastructure and provide enhanced security controls. Access VPNs for employees will be centrally located within the new Commonwealth Data Center and provide access to all resources interconnected to the MAN. The VPN architecture will also provide a service offering to agencies that require or request Intranet VPNs to remote sites.

Agency solutions for business partners will remain in place to access resources located within agency data centers. The existing business partner VPNs will require further analysis to justify consolidation. The location of resources and sensitivity of data will be factors in the evaluation.

11.3.9.10 Network Management

The Commonwealth of Virginia does not currently have a centralized network operational center or NOC. Currently some agencies employ outsourced vendor services to manage network resources and other have in-house tools with many agencies not providing Network Management capabilities.

To provide innovation and meet the current and future management and operational challenges presented by the Commonwealth’s large and complex network, the Commonwealth Partners have offered network monitoring services that will provide a comprehensive, state of the art Network Operations Center (NOC) integrated with the overall data center operations in Virginia with tools that meet a wide range of requirements.

The Commonwealth Partners understand the challenges of managing networks, and will offer a leading remote network management solution that is a proactive, reliable and provides a cost-effective approach to meeting design, implementation and on-going management requirements as noted in the SOW.

The operations approach will leverage the current expertise of the Commonwealths’ skilled staff of network professionals, and add our proven processes and industrial strength tools. The primary components of the Network Management services include the following:

- a) 24 x 7 monitoring and fault management,
- b) SNMP based tools,
- c) Interface to Change Management process
- d) Configuration management of network components,
- e) Performance management of network components,
- f) Network documentation, and
- g) Secure Web portal access to network management information and reports.

The services need to include implementation and turn-up monitoring and coordination for all installation services, 24x7x365 network monitoring, rigorous fault identification and resolution processes, change and configuration management processes and performance engineering services.

Further details for this may be referenced in section 11.3.9

11.3.9.11 Network Migration Benefits

- SONET Backbone infrastructure more reliable
 - The technology advances available today with optical equipment include numerous options and provide the robust network backbone required to deliver multiple services over a common infrastructure. Metro Dense Wave Division Multiplexing capabilities in conjunction with routing and switching portfolios provide intelligent switching solutions for efficient handling of network applications through the use of Quality of Service and Multicast feature sets. Integration of Wave Division Multiplexing (WDM), Gigabit Interface for core, distribution, and access levels of internetworking devices allows for flexibility in the optical transport and edge design. In addition, it lowers the total cost of the switching and optical transport solution.
- Inherent fault tolerance, flexibility and scalability
 - The core SONET network consists of two highly reliable networks, each of which is capable of functioning independently of the other with no service impact. The High-Speed TLS service relies on Verizon's Protected Access Line feature, which has failover recovery in the event the primary link is down. At the same time the overall design is tolerant from a device component and unit failure standpoint. Fault tolerance is ensured by a design that incorporates the following: diverse circuit routes, redundant power supplies, diverse internal cable paths, and redundant network switches.
- Disaster Recovery Ready
 - The SONET Ring design and inherent capabilities of this technology will provide the backbone for future Disaster Recovery requirements. The Secondary Data Center will be interconnected to the SONET Ring (**further details provided in section 9.4**)
- Common Infrastructure accommodates Agency data aggregation requirements
 - Commonwealth agencies currently access network services via multiple vendors and contracts. The network migration plan is designed to aggregate technical, service, and maintenance requirements to maximize the operating efficiencies while at the same time strengthening the Agencies and local municipalities negotiating position in procuring equipment and services in the most cost-effective manner.
- Operational cost savings
 - In the current environment of multiple networks and service providers, resources are expended inefficiently with costly duplication of effort and staffing. The network migration will enable the technologies that allow for enterprise-wide integration of communications functions. It will also leverage the Commonwealth's various communications resources through the optimized use of infrastructure, staffing, investments, maintenance, and vendors. Concentrating network operations in a more centralized environment will enable Commonwealth-wide operational efficiencies.
- Enhanced service offerings (converged communications, rapid deployment)
 - Enhanced network and operational controls will be a direct result of the network migration and will extend horizontally across the network. These enhancements and controls will allow for more rapid deployment of services to all the agencies. Future network service deployment can be managed more cost-effectively and in a timely fashion.