January 28, 2010

CTN Whitepaper – Project Technical Design and Strategy

Introduction

The California Telehealth Network (CTN) architecture has been designed based upon pre-established strategic, operational, performance and budgetary goals and constraints. Since the establishment of these foundation goals has fundamentally influenced the design, this Whitepaper will begin with a brief discussion of the primary design criteria. It will be followed by a technical description of the resulting network architecture and will conclude with an explanation of how the resulting design fulfills the pre-established foundation goals.

Foundation Design Criteria

Project scope - regional or statewide? During the early inception of the CTN project, it's founding organization, the CTN Advisory Committee considered the issues of project scope and scale. Understanding that the available funding obtained would be the ultimate constraint, two feasible alternatives were considered. The first: build a limited regional network in which the physical infrastructure was primarily purchased outright (fiber links, DWDM, routers, etc.), was operated by the CTN and dedicated to the CTN. Budgetary constraints would certainly limit such a solution to a specific region of the state and encompass perhaps 100 sites or less. The second alternative considered was to extend the network on a statewide basis and strive to encompass a broadly geographically dispersed cadre of Participant sites, with particular emphasis on rural sites. Since constructing a dedicated statewide network de novo would be prohibitively expensive, this alternative would necessarily require capitalizing upon existing telecommunications infrastructure to the maximum extent. After considerable deliberation, the Advisory Committee determined that a statewide project would best serve the clinical and outreach goals that are fundamentally important to its membership.

Operational constraints - limited availability of operational and administrative financial support. The primary source of funding for the project would derive from the FCC Rural Health Care Pilot Program (RHCPP). This program generously subsidizes 85% of telecommunication s costs, but provides no financial support for essential administrative and other operational support. Consequently, a strategy was adopted that endeavored to transfer as much of the administrative and operational responsibilities to vendors, who could legitimately include such costs in their aggregate pricing for the offered telecommunications services and for which they could receive reimbursement under the RHCPP.

In the industry parlance, such services are designated as "managed services." Multiple tiers of managed services are generally available from most large, sophisticated telecommunications vendors. They range on the modest end from equipment installation assistance to very comprehensive "soup-to-nuts" support for the entire panoply of equipment, circuit, and operational support services, including network design, installation, maintenance and monitoring as well as security management services.

Dedicated, Medical Grade Network – the FCC Order for the RHCPP stipulates that funds must be used to construct a "dedicated health care network." A Medical Grade network must comprise certain essential capabilities: 1) End-to-end Quality of Service. Given the rapidly increasing deployment of latency-sensitive telemedicine and telehealth applications such as remote real-time patient encounters and patient monitoring, as well as the growing need for higher bandwidth (e.g.,1080P HD video), it is essential that a medical grade network employ end-to-end explicit Quality of Service, particularly in rural locations where high-capacity circuits may be unavailable or prohibitively expensive. This permits explicit prioritization of clinical traffic, while simultaneously permitting access to lower priority administrative and other non-clinical traffic. 2) Security – HIPAA and other state and federal regulations require that the network meet certain security standards. If traffic transits any public networks (most particularly, the Public Internet), it must be encrypted to ensure the privacy and integrity of the data. Moreover, Virtual Private Network (VPN)-level security must be employed over all links, ideally without the administrative encumbrance of individually establishing individual point-to-point VPN tunnels (any-to-any VPN capability).

Flat Network – a fundamental goal of the CTN Advisory Committee was to establish a network in which each participant was a peer and received identical access and services. The ideal network would involve no obligatory transiting of regional hubs that are responsible for (and also control) access to external networks. The resulting "flat" network would permit entrepreneurial activities to develop without centralized intervention – essentially an "any-to-any" network.

Extensible, Expandable Architecture – the Advisory Committee envisioned that the CTN could expand considerably as the potential for telehealth applications become more widely realized. Indeed, the originally established complement of 300 sites has increased to over 850 sites statewide in one year! Consequently, the network must be capable of efficiently and transparently expanding, both in geographic scope as well as number of participant sites. Moreover, it must also be inherently extensible, permitting convenient addition of new services and increasing of bandwidth at any individual segment without requiring extensive physical or logical restructuring of the network.

Technical Design

In order to effectuate the multiple pre-established foundation design goals, the CTN has adopted the following network architectural design. Key design points are itemized below:

1. The CTN will consist of an Contractor-provided, MPLS-routed, IP addressed, VPN, composed of approximately 850 individual sites interconnected over a high performance statewide backbone (*see Figure 1*). Multi-Protocol Label Switching (MPLS) is a state-of-the art network routing protocol that provides superior end-to-end routing performance.
2. The network will be procured as a Managed Service – CTN will not construct any "last mile", "middle mile" or Core routing/transport infrastructure. Consequently, CTN will not directly purchase, lease, or install any of the following physical infrastructure components:
    a. Conduit and Fiber spans.
    b. Routers, switches or other network electronics.
    c. Computers and software related to monitoring network activity

d. Security systems, including Firewalls, Intrusion Detection or Prevention Systems hardware and software.

3. Comprehensive Support. All physical infrastructure, detailed architectural design, IP addressing scheme, all communication/routing equipment acquisition, and provisioning, installation, maintenance and repair, establishment of peering points with external networks, will be obtained as a comprehensive managed service.
4. Prime Contractor – since the project spans the entire state, the aggregate facilities and services from multiple regional telecommunications providers (ILEC's and CLEC's) will be required. In order to simplify the administrative oversight as well as to centralize performance responsibilities, the CTN is requiring that a single highly-qualified contractor serve as Prime Contractor, who will assume overall financial and operational responsibility for all subcontractors and services, including the multiple regional ILEC's and CLECS that will provide local/regional connectivity to the CTN core network (provided by the Prime Contractor) .
5. Customer Edge (CE) to Provider Edge (PE) connections. The minimum bandwidth CE-PE connection provided will be standard DS1 service at 1.5 megabit per second (1.5Mb/s). It is anticipated that approximately 100 critical access hospitals will receive available fractional DS3 service, initially at 10 Mb/sec. Additional high volume clinics may also receive 10 Mb/sec service, depending upon budgetary constraints. Where available the CE-PE circuits will be landline circuits provided by ILEC or CLEC in the local service area. Extensive surveys to date have confirmed that all of the current roster of 850+ Participant sites that have been approved by USAC for participation in the CTN have ILEC/CLEC landline DS1 service available. CE-PE circuit distance spans range from one to over 200 miles, with an average of approximately 15 miles.
6. Preferential Fixed-Rate Pricing. CTN has negotiated mileage-independent in-franchise and out-of-franchise rates for CE-PE circuits, so-called "postalized rates."
7. "Hard to Reach" Sites – CTN anticipates that a small number of future sites may not have the minimum DS1 landline service available. These sites will be provided with satellite service, or other alternative connection modality. The Contractor will provide direct interconnection between a satellite-connected site and the CTN VPN (no intervening Public Internet link), thus preserving the essential medical-grade security and privacy.
8. Provider Edge and Core routing and transport services will be provided by the Prime Contractor. The selected Prime Contractor supports statewide/national/international MPLS VPN managed services within California and has extensive statewide Core routing backbone and regional distribution infrastructure to support their voice and data communications services. The vendor's currently available fiber-based backbone infrastructure provides multi-gigabit capacity sufficient to support medical-grade communications from all CTN sites.
9. Expandable IP addressing – The CTN will be a 100% digital, IP-based network – no analog links will be employed. In an IP-based network, each "node" on the network (e.g., PC, telemedicine equipment, etc.) will be assigned an Internet Protocol (IP) address that will be used to transport and route communications to/from the device. CTN will implement a private address paradigm internally ("Class A", 10.x.x.x IPv4 address space), with suitable network address translation (NAT) services at interconnection points with external networks, such as CENIC. The NAT services convert the internal IP addresses used within the CTN into Internet-routable addresses,

thus permitting network devices within the CTN to freely communicate with external sites, including sites that are only accessible through the Public Internet. Use of Class A private addressing will permit vast expansion of the CTN without jeopardizing the availability of IP addresses.

10. No Internet Transit – CTN requires that no segment of CE-PE, PE-Core, or interconnection with external networks transit the Public Internet. This restriction will isolate CTN from performance variability due to Internet problems and eliminate the need to employ encryption technologies within the CTN to protect sensitive health care transactions.
11. Explicit Quality of Service – CTN will internally employ " End-to-end delineated Quality of Service" (QOS) capability. It is important to note that explicit, delineated QOS does not simply imply that the network will provide "quality" in the sense of reliability consistency and bandwidth performance, although these characteristic are certainly important requirements. Any network, no matter the bandwidth available can become congested – overwhelmed with the volume of traffic to the extent that sessions are interrupted and data lost. The Explicit QOS employed within the CTN provides the capability to "tag" high priority traffic (e.g., telemedicine or patient monitoring sessions) with a numerical priority flag. As the QOS-tagged packets traverse the network, each routing/switching device recognizes the priority tag and preferentially processes and forwards the packets. This capability is viewed as particularly important in providing reliable performance for latency-sensitive real-time telemedicine and remote patient monitoring activities. Initially one QOS level will be implemented, although a minimum of four levels are available from the Contractor for the requested MPLS-based VPN services. The Contractor will be required to appropriately process QOS tags at the interface with all external networks, so that explicit QOS tags are preserved across these interfaces. (NOTE: most external networks do not currently support the delineated QOS capability which is considered an "advanced" feature).
12. Any-to-any Private IP VPN - CTN will employ any-to-any VPN capability, providing VPN security over any site-to-site link internally within the network. This architecture will eliminate the need for establishment of labor-intensive point-to-point VPN tunnels. Where a high level of security is required for connections to sites external to CTN, some of which may transit the Public Internet, an additional level of encryption security (IPSec) can be implemented.
13. External Networks – CTN will provide access to Internet 2, National LambdaRail and the public Internet. Connection will occur via a direct connection to California's Regional Optical Network, CENIC. This connection will also provide high-bandwidth connection to every major academic medical center within the state (UC's, Stanford, USC, etc.), as well as access to a very large contingent of K-12 , community college and state university institutions that participate in CENIC. Initial design calls for a single 100 Mb/s connection. Depending upon budgetary constraints, a second 100Mb/s link may be installed for load-sharing and redundancy.
14. Project Management – Prime contractor will provide comprehensive project management services and will bear full responsibility for undertaking at least three independent implementation initiatives throughout the state (North, Central and South) and must complete the entire project within a maximum timeframe of three years. Based upon vendor representations, the actual implementation period may be as short as one year.

15. Detailed Project Specifications available – a detailed technical description of the proposed network is presented in a previously posted CTN RFP, available at the USAC RHCPP Web site: http://www.ucdmc.ucdavis.edu/ctn/rfpmain.html

Advantages of Network Architecture

1. Capitalizes on existing infrastructure and resources – leveraging existing physical network infrastructure available from telecommunications carriers, as well as maximizing the use of pre-existing design, implementation , management and support resources will : 1) make it feasible to construct a large, statewide network on a very accelerated schedule with a minimum of operational and administrative resources; 2) will leverage well-proven routing and transport technologies that are increasingly being adopted by top-tier financial, governmental and industrial organizations.

2. Provides an Expandable and Extensible Framework – the MPLS-routed IP VPN provides a flexible framework that can be rapidly expanded without construction of additional physical infrastructure (e.g., regional hubs). Bandwidth at individual facilities can be increased without extensive redesign and upgrade or construction of PE and Core routing facilities. Explicit QOS capabilities permit highly efficient use of existing bandwidth; a very significant advantage in certain rural areas where infrastructure is limited. Secure peer-to-peer , any-to-any intrinsic security will facilitate entrepreneurial activities on a local and regional basis and require no regional or centralized management (e.g., establishment of point-to-point VPN's). The Class A private addressing scheme will as a practical matter, permit limitless expansion of the network without requiring labor-intensive IP address reorganization.

3. Capitalize on Beneficial Pricing – the CTN will exploit very beneficial pricing available, resulting from state government contracts. The State of California Department of Technology Services has established comprehensive contracts with multiple telecommunications carriers to provide a broad array of telecommunications services for state agencies, at very beneficial pricing (CalNet 2 program). These contracts include all circuits, equipment and managed services anticipated for the CTN. Some pricing benefits available include: 1) mileage-independent circuit charges; 2) statewide pricing for managed services (postalized rates). Since the CTN will include many very rural sites, availability of a postalized rate structure will tremendously advantage the ability to cost-effectively connect rural constituencies.

4. Provide Medical Grade Service – the MPLS IP VPN architecture equitably provides "out of the box", ubiquitous availability of security, quality and reliability sufficient to support current and near-future real-time telemedicine and telehealth activities at every Participant Site. 1) any-to-any VPN, 2) explicit QOS, 3) minimum bandwidth (DS1) sufficient for current and emerging telemedicine functionalities (e.g., 1080P HD video).

Fibure 1 - Technical Summary Diagram

The following figure illustrates the high-level organization of the major components of the CTN.

Core Backbone – the core backbone will be provided by the Prime Contractor. It is composed of multiple routing centers located throughout the state, interconnected by a very high-speed, fiber-based backbone infrastructure. Each node in the core is interconnected to at least two other nodes. Each node is equipped with fully redundant "Carrier Class" high performance routers and other electronics. The Core is represented as a cloud, since it functions in such a fashion that failure of a circuit or hardware at any node will result in traffic being automatically rerouted around to an alternative device, or two an adjacent core routing facility.

Provider Edge – The Provider Edge nodes are regional locations where circuits from CTN sites are terminated. They may be separate Regional Hub facilities, or may also serve as a node in the Core Backbone. Each CTN Site will be connection to the closest PE facility.

PE-CE Circuits – Provider Edge to Customer Edge circuits will be provided by a regional telecommunications provider (phone company). In many cases, the Prime Contractor will also provide these circuits, since they also provide phone service in the region. Alternatively, other ILEC's and CLECS who have "Intercarrier Exchange Agreements" with the Prime Contractor will provision these circuits. Circuit speeds will vary between 1.5 and 10 megabits per second (Mb/s).

Redundant Circuits – due to the critical care nature of their services, some sites may merit the installation or redundant PE-CE circuits. Note that each PE-CE circuit terminates at a separate Regional Hub facility. Should one circuit fail (or a catastrophic failure occurs at one Provider Edge facility) the redundant circuit will automatically assume the full load. During normal operation, the two circuits can share the aggregate load through "load sharing" programming.

CE Router – the CTN connection to each site will terminate on a "Customer Edge" router that is located at the local facility. The Prime Contractor will be responsible for comprehensive support of the network, including the CE router. The router will provide an Ethernet connection to which the individual sites can connect a Local Area Network (LAN) to gain access to the CTN. Neither CTN Management nor the Prime Contractor will be responsible for supporting the Site's LAN, or any network-based equipment that may attach to it (PC's, telemedicine devices, printers, etc.).

Security DMZ – all traffic to/from external networks passes through a "De-Militarized Zone." Various security devices, including firewalls, Anti-Virus Systems, Intrusion Prevention Systems, etc., interrogate the traffic and enforce security rules. CTN has the option to contract for these managed services from the Prime Contractor, but is not obligated to do so.

CTN Technical Architecture