Medical Grade Network Design and Operation

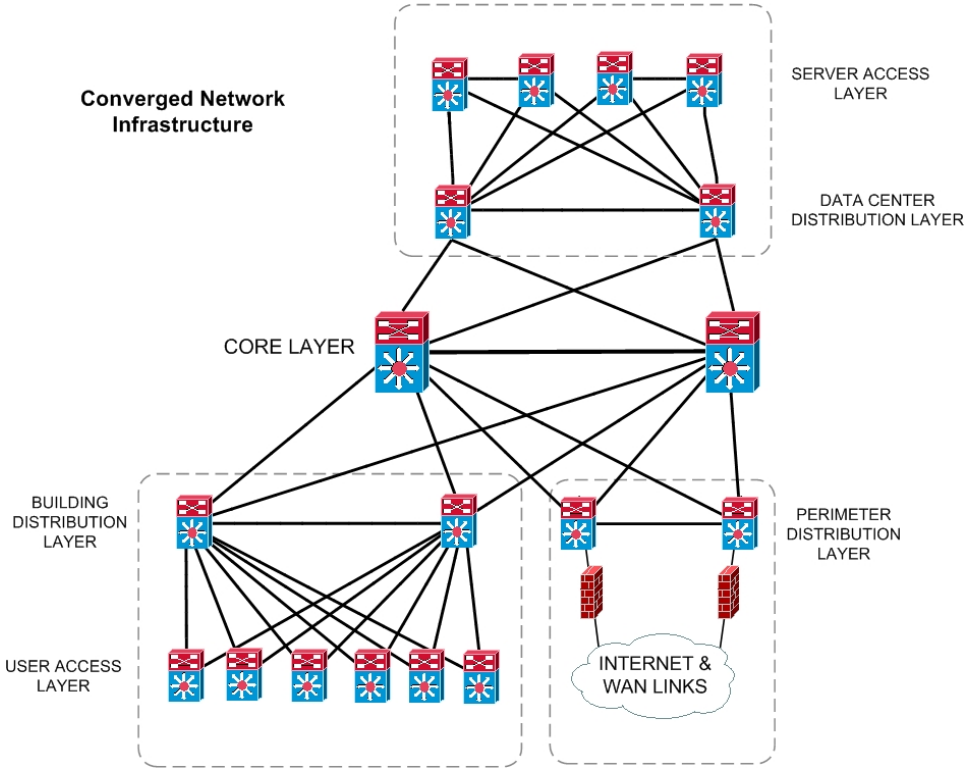
Chesapeake NetCraftsmen has been supporting our health care customers with designs and implementations of 'Medical Grade Networks'. In this whitepaper we will describe medical grade network design and discuss some of the problems that we find in real networks.

Background

Most health care organizations have an existing network infrastructure - often there are *several* physically separate networks, supporting clinical data, non-clinical data, voice, research, educational equipment, and departmental staff. For several reasons (manageability, efficiency, costs), there is a desire to converge these separate networks into one physical infrastructure, while still providing the isolation, security, and responsiveness needed by the organization.

High Level Converged Network Infrastructure Design

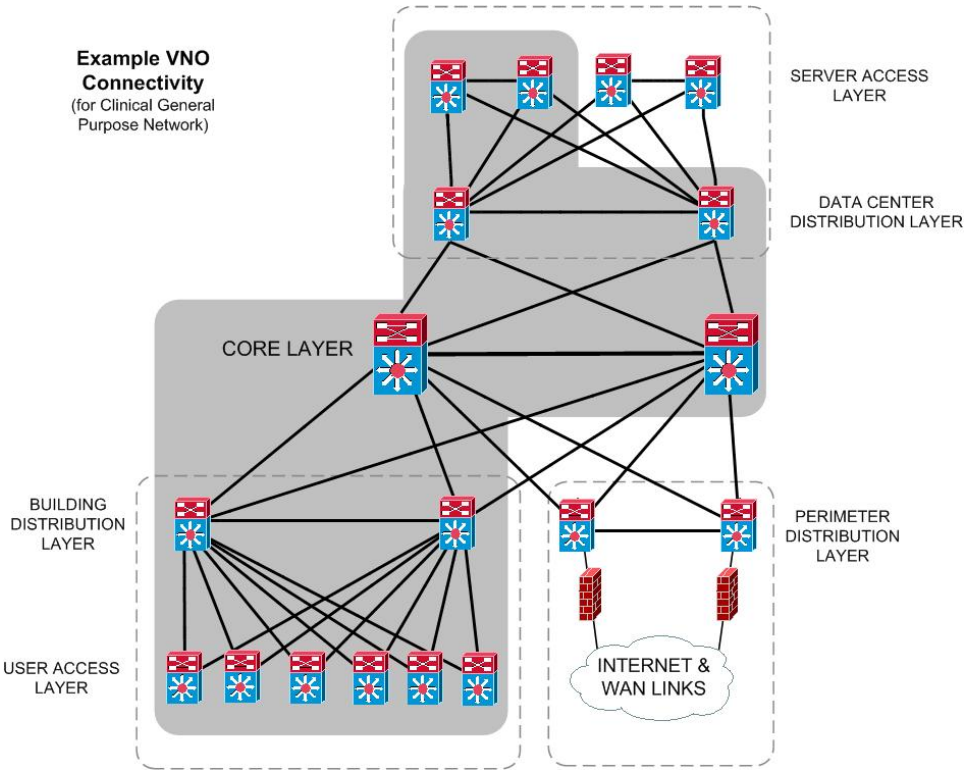
Our design of the converged network infrastructure for a health care organization is based on the hierarchical, three-layer model: core, distribution, and access layers. This hierarchy establishes the foundation and connectivity for the entire network, as shown below. It is a resilient network that is easy to understand and easy to troubleshoot.



Within each layer are redundant modules that serve a specific role in that layer. The hierarchy allows changes or upgrades to be performed at one layer in the hierarchy without disruption or significant changes to the other layers. End-do-end connectivity

uses the ISO network model's network layer (also called the routing layer or Layer 3), which provides network stability, fault isolation, fast response to failures, and maximizes redundant path utilization. Large Layer 2 switching domains are avoided, because of their inherent susceptibility to operational failures. (For example, a large Layer 2 network that failed and caused a four-day network-wide failure at the CareGroup Healthcare System in Boston is described here: http://www.cio.com.au/article/65115/all_systems_down/).

We overlay the network infrastructure foundation with multiple virtual networks to create the connectivity and the isolation previously provided by the separate physical networks. These virtual networks we call Virtual Network Overlays (VNO). By using VNOs, separate logical networks can be built to support clinical, voice, research, and guest users/devices while maintaining appropriate isolation from each other. Connectivity between VNOs is controlled at clearly identified connection points where security and connectivity policies control access into each VNO. The gray area in the figure below illustrates the domain of the Clinical General Purpose VNO across a healthcare network.



Along with Layer 3 routing, we recommend a structured addressing plan based on IPv4, augmented with groundwork for implementation of IPv6. The structured IP addressing plan incorporates stability and security features, making it easy to implement Network Admission Control for network sign-on and easy identification of IP telephony endpoints.

The network Quality of Service (QoS) design is developed to support delay sensitive network applications and to improve application performance. It provides end-to-end differentiated service levels, ensuring that applications like Voice over IP (VoIP), clinical

systems, and telemedicine receive preferential treatment over bulk data applications like email, system backups, and back-office applications. The generalized QoS design, as shown in the figure below, is flexible, easily extending to support new services, and is based a Cisco QoS model.

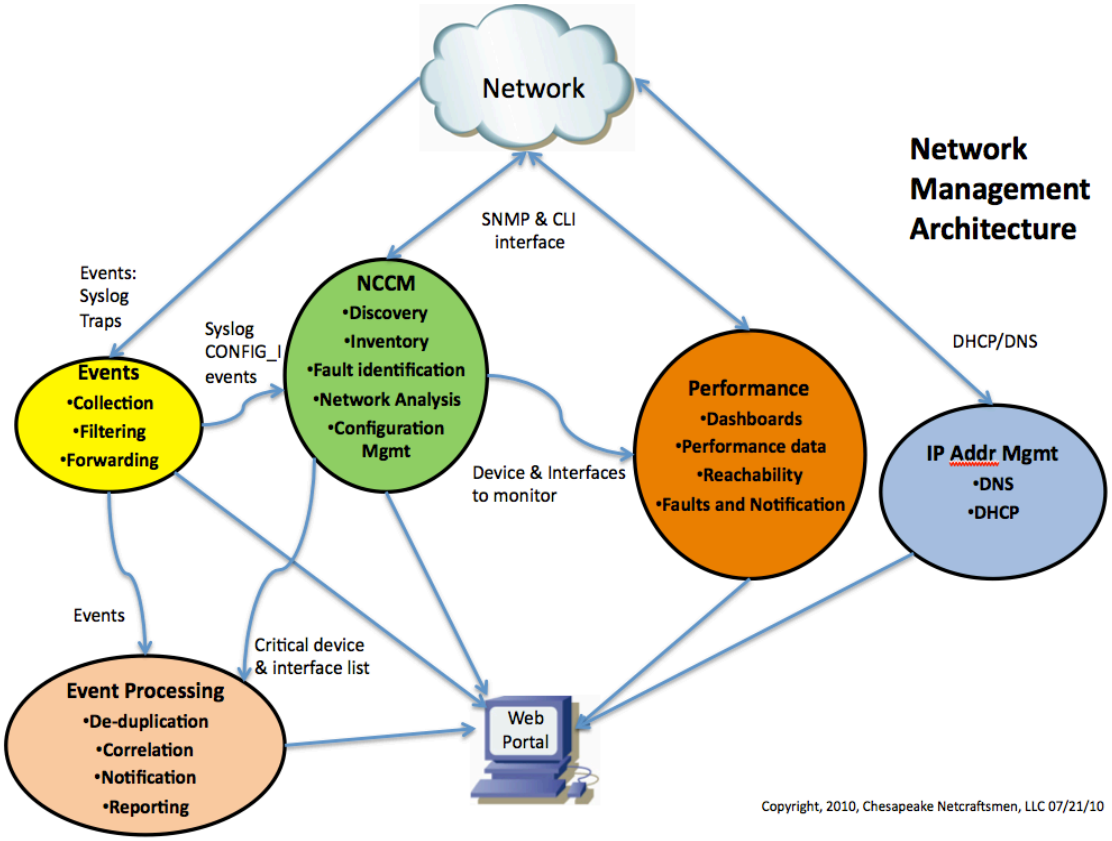
QoS Classes / Applications	Network Priority
Routing & Switching Protocols	Highest Priority
Voice / IP Telephony	Expedited Forwarding
Clinical life-critical	Highest Priority Assured Forwarding
Interactive video	High Priority Video
Streaming video	Low Priority Video
Call signaling	Medium Priority
Premium data	Medium Priority
Transactional data	Low Priority
Bulk data	Low Priority

To implement high availability throughout the network infrastructure, we design with redundant pairs of devices, especially for the core and distribution layer. We find that replicating a standard redundant design, based on pairs, is predictable, easy to implement, scalable, and relatively simple to maintain.

Security is a crucial part of the health care network designs. In addition to standard infrastructure security practices, our designs include a security module to control all communication between the global network and the virtual networks. IPS/IDS devices and firewalls customized with organization specific policies and rules comprise the nucleus of the security module. All traffic that passes between the virtual networks and the global network travels through these network security devices. In addition, the perimeter network is secured to meet appropriate health care policies and regulations.

Network Operations

Once the network is built, network management and operations makes sure that any problems are quickly identified and corrected. We have used the network management architecture containing the functionality shown in the following diagram in multiple organizations. It provides the core functionality that is needed without overwhelming the network operations staff with new tools to learn and use.

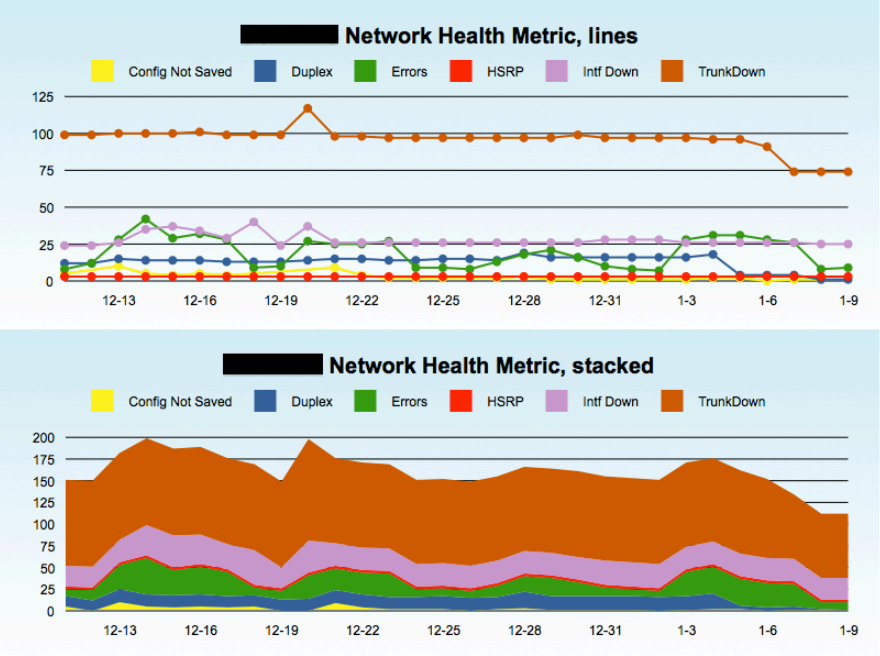


The combination of event processing and performance data collection provides real-time notification of network problems. NCCM (Network Change and Configuration Management) identifies inconsistent configurations that create compliance problems and security holes, in addition to performance problems and errors. IP Address Management tracks devices on the network, so that when a problem is identified, the affected device can be quickly located.

Performance monitoring systems report on high utilization interfaces, identifying hot spots in the network where links are oversubscribed. These same systems also identify interfaces with high numbers of errors, allowing the network staff it correct the problem and increase productivity of anyone using applications whose data transits the interface.

Dashboards that show network health and operational problems are key to identifying and correcting network problems before they impact healthcare applications. A combination of real-time alerts and the network health metrics dashboard, shown in the following diagram, informs the network team of immediate and long-term problems that need to be corrected.

Network Health Metric



- Config Not Saved: Cisco devices whose configuration has been changed and not saved to NVRAM
- Duplex: Duplex mismatches, reported as CDP duplex mismatches, from syslog
- Errors: Interfaces with high error rates, as reported by syslog
- HSRP: HSRP groups containing only a single router, either due to a configuration error, or the failure of the second router or a problem with the communications between routers
- Intf Down: Router interfaces that are in the Up/Down state. Any router interfaces that are 'up/down' are presumed to have failed and need attention
- TrunkDown: Switch trunk ports that are in the Up/Down state. Trunking interfaces that are 'up/down' are presumed to have failed and need attention

Conclusion

The Medical Grade Network has become a critical infrastructure element for healthcare organizations, incorporating significant redundancy and security components. With a few good network management tools, the network team can work proactively to keep the network operating smoothly.

About Chesapeake NetCraftsmen

Chesapeake NetCraftsmen, LLC is an advanced network consulting firm that specializes in high-profile and challenging network consulting jobs. We provide network design and consulting services for many healthcare organizations. NetCraftsmen is a Premier Cisco Partner, with a large number of Cisco specializations. A third of the company staff are Cisco Certified Internetwork Experts (CCIEs).

Chesapeake NetCraftsmen, LLC.
1290 Bay Dale Drive, Suite #312
Arnold, MD 21012
1-888-804-1717
www.NetCraftsmen.net