



Position Paper

How to achieve a clinical-grade network deployment

Many facets of the clinical-grade network are reviewed in Nortel's previous paper: Clinical-grade — A foundation for healthcare communications networks.

This paper presents the complicated analysis and deployment aspects associated with successfully deploying a clinical-grade network, utilizing Nortel's product portfolio as primary examples. One of the key aspects of a clinical-grade network is the consideration of use within the point of care (POC) context. The point of care is where the caregiver (physician, nurse, technician, orderly) happens to be when they need to make a decision regarding a given patient.

Being able to describe a set of environmental requirements is the first step to accomplishing this goal. The bottom line is how to successfully deploy the equipment and services required to meet the end goal of building a clinical-grade network.

User perceived down time

As healthcare institutions move towards an electronic environment, it becomes crucial to have access to information at the point of care. Downtime in other industries may mean loss of face in front of customers or loss of money, but in healthcare it could lead to loss of life or delayed patient care. Downtime of services in healthcare is unacceptable.

The design considerations need to make a distinction between:

- › Users being able to access services or accomplish tasks utilizing their standard processes
- › Users needing to utilize alternative processes to accomplish a task

Operationally the goal is to have standard processes and actions utilized well over 99 percent of the time. Only in extreme cases of multiple systemic failures should non-standard processes be required.

This design consideration is not focused upon single device or service failure but a systemic goal at the end-user interface



The key elements that we will discuss in context of clinical-grade network deployment are:

- 1 Eliminate user perceived down time
- 2 Guarantees of confidentiality, integrity and accountability of data
- 3 Guarantee of accuracy of information transfer within specified time limits
- 4 Respect of Service Level Agreements
- 5 Convergence of systems, applications and usage
- 6 Manageability of the environment
- 7 Interoperability
- 8 Usability



or application. Just as the respiratory, circulatory or integumentary systems do not fail due to a single elemental trauma, clinical-grade networks do not fail due to issues caused by a single network element. A common term for these design considerations is ‘business assurance’ or ‘business continuity’.

Reductions in efficiency of given systems may occur due to single elements failing; however, the goal that standard operations for the given task are maintained can be accomplished with today’s technologies.

Today’s Ethernet and Internet Protocol (IP) systems involve three interrelated levels of services or functionality.

Layer one is the physical layer. Protection of this level of service requires having more than one way in and out of a given location to the service being utilized. This is analogous to the way architects design emergency exits into buildings. If one direction is blocked, allow for exit in an alternate direction. This method is utilized within Nortel’s optical transport systems and Ethernet Switching systems. With protected rings, diverse physical routing and, specifically, Optical Ethernet capabilities, more than one physical path is allowed to carry the same data to remove the single delivery path challenge.

When we move to layer two or the data layer, the concern is delivering Ethernet packets of data from a device to one or more other devices. Protections at this layer include techniques similar to those utilized at the physical layer: provision of multiple delivery paths to a given data packet. Intelligence within network devices and appropriate physical design enable such technologies as Split Multi-Link Trunking (SMLT) to provide active and non-intrusive delivery of data to its

intended destination, leaving the end user to their primary tasks regarding patient care.

As we move up into layer three or the IP layer, active and autonomic controls are leveraged within the routing systems of the various network elements. Services such as Equal Cost Multiple Path Routing (ECMP), Virtual Router Redundancy Protocol (VRRP) and designs that allow for N-1 resiliency services all reduce the potential for the end user being aware of any elemental failure within the overall clinical-grade network.

Deploying services such as Routed SMLT allows for active utilization of all data paths during a healthy network state with no wasted or idle resources. Should the system move into a failure state, services are still delivered within a defined prioritization scheme determined by the criticality of given services. All services can be maintained and it is a matter of definition as to which services receive preferential treatment at the N-1 failure state.

The flexibility and resiliency of the Nortel offerings within network devices and services allow network engineers to define a highly reliable and recoverable system upon which clinical-grade networks provide services to end users.

Guarantees of confidentiality, integrity and accountability of data

Patients’ and regulators’ expectations of confidentiality add to the clinical-grade network’s requirement to support guarantees of confidentiality, integrity and accountability of data.

Clinical-grade networks implement best practices associated with confidentiality, integrity and access (CIA) around the

data being generated. This has to be accomplished in line with the healthcare institution's control policies, regulatory requirements and the risk management practices placed upon staff regarding recording and handling electronic health information.

Confidentiality controls may take many forms from controlling what authentication is required for access to full encryption of data from the capture point to the record storage facility. All are elements of confidentiality maintenance.

Integrity of information within a network must prevent repudiation: has the data been modified from its original form in any way and can this modification be detected and defended within appropriate audit controls? Authentication, authorization and accounting methods along with privacy controls within the network allow for this need to be met. Nortel is a leader in privacy capabilities in our security portfolio of products, combining our own Tunnel Guard and Intelligent Traffic Management elements with partner components like Symantec's Intelligent Network Protection software component.

Access is an evolving element within the security landscape. It used to mean perimeter controls; now, with a very permeable perimeter at best, this control element must be enforceable at the devices connecting to the network. Nortel's Security portfolio encompassing specifically user-based networks and Nortel Secure Network Access systems allows for extremely granular controls within various environments.

At the network element level, Authentication, Authorization and Accounting (AAA) services are linked into enterprise systems for coordinated controls, reporting and administration within a clinical-grade network. Standards-



based services such as RADIUS, Active Directory or other LDAP services, Syslog and other correlation elements all contribute to a systemic control system within the network.

Each network element must have linkage into the administrative elements referred to as AAA. How these linkages are accomplished does not and should not follow a single communication path or protocol. Diversity within these linkage services provides both resiliency and security elements that must be present and accounted for within clinical-grade network designs. Whether utilizing TLS, IPSec, SNMPv3 or SSH as privacy controls within the network infrastructure and administrative elements, variety and diversity allow for more robust designs. Nortel products such as Secure Routers, Ethernet Routing Switches, Ethernet Switches, various security products along with multimedia systems including the BCM, CS 1000, MCS, contact centers and optical and BCS elements all allow for integration with administrative services providing for AAA services to be systematic and avoid silo implementations.

Guarantee of accuracy of information transfer within specified time limits

While many industries are becoming concerned with time-to-decision issues, this need has always been a dynamic in healthcare environments. This drives a need for guarantee of accuracy of information transfer within specified time limits.

While this tenet may conjure up thoughts of more and bigger network connections as far out into the user environments as possible, it also must include controls for performance assurance during sub-optimal conditions.

Building a network hierarchy that only has single high-speed interconnects into and out of a given user grouping leaves a risk of failure of this single path, causing many users' services to be inaccessible. Single points of failure can be avoided by utilizing Nortel's implementation of Resilient Packet Ring (RPR), Split Multi-Link Trunking (SMLT), Routed Split Multi-Link Trunking (RSMLT) as well as Equal Cost Multiple Path (ECMP). These elements each work at various levels within the

network OSI layers one through five and the corresponding IP layers one through three.

RPR and other optical resiliency techniques essentially transmit and receive data through two unique physical interfaces across two unique fiber paths. Thus, if one path fails, the alternate delivery path is able to keep the communications path functional. This virtualization is transparent to upper layer data control and manipulation and allows the systemic up-time required across geographic areas that can justify optical transport.

SMLT functions at OSI layer two and allows for high-speed transport, physical resiliency and virtualization across multiple physical Ethernet paths. This virtualization and physical resiliency allows upper layer protocols to avoid convergence manipulations or failure by maintaining an available transmission and reception functionality over available interfaces and physically resilient data paths. This functionality can be maintained over both copper as well as fiber data paths. This flexibility allows



network architects to design according to the appropriate physical attributes of their environments.

RSMLT and ECMP are techniques that function at OSI layers 3 through 5, effectively utilizing state information and distributing traffic at these layers across the available multiple physical or virtual paths known to the protocol.

With this many options to choose from, all networks should expect to encompass some level of network resiliency. The higher the classification toward mission-critical, the more of these resiliency elements, discussed above, should be in a given design. All of the technologies discussed in this section are interoperable and augment each other versus compete with one another. If the goal is to assure that application traffic always arrives and the network is to become a utility, all of these elements will apply to your environment.

Accuracy begins with consistent delivery of data without loss; it also has several facets.

After we have addressed the basic distribution design elements of the network, architects must address the inevitable risk of a failure within a network environment. Failures at the element level will always be a risk and architectures must encompass this eventuality.

Techniques to control applications by their performance requirements must also be put in place. This is commonly known as network Quality of Service (QoS). The result is to improve end users' Quality of Experience (QoE). Services or applications should perform well in both a normal state as well as when elements are put into a failure state, whatever the reason. Prioritization may not be apparent in a normal operation state if sufficient bandwidth is in

production to prevent any congestion.

In a failure state, there should still be sufficient bandwidth to accommodate the level of applications identified as mission-critical and patient-critical. These choices at the design level require inputs from a wide spectrum of medical staff and their dependency upon technology to enable their services. With a holistic approach to the various dynamics within a healthcare environment, prioritization of both application and service delivery elements will drive the actual QoS features implemented to maintain sufficient QoE at the user level.

After availability and prioritization have been accounted for within the clinical-grade network, distribution of end-user access also contributes to the accuracy of information generated. Accuracy of data creation, by allowing input as close to the originating procedure as feasible, rounds out this tenet. This is where mobility elements such as WLAN, wireless clients and soft clients may be leveraged to integrate multiple modes of communication into the treatment protocol that exists today or may be created in the future.

Mobility has several elements within it. Physical mobility of IP can be enabled with proper distribution of WLAN elements such as the Nortel 2300 Series of Access Points (APs). Physically enabling data input with wireless technology also must encompass securing the airwaves being utilized. This element can be addressed with proper distribution of Nortel Wireless Security Switch (WSS) components. This element controls both authentication and encryption within the WLAN environment, avoiding the risk of data manipulation or exposure via the elements enabling mobility for patient data processing as well as collaboration utilizing patient data.

Enhancing the ability to distribute WLAN elements and other elements that may require additional power installation is a technology known as Power over Ethernet (PoE). A PoE-enabled infrastructure enables flexibility in the deployment of powered elements that also require data connectivity. Many new network elements are coming to market with this option for deployment. Nortel's PoE switching portfolio can enable a clinical-grade network to meet these future demands without repeated replacement of infrastructure elements.

Leveraging common policy enforcement across multiple platforms will be key to successful QoE for end users of information services. Nortel's Enterprise Policy Manager allows for enterprise-wide controls of both QoS and security policies from a single management entity while distributing authority as appropriate. This tool allows for virtualization of controls both from a multi-user access environment as well as logical groupings of administrators into allowed functional groupings.

Respect of Service Level Agreements

Healthcare, being a collaborative environment at the point of care, requires enforceable Service Level Agreements and compliance to enhance patient care in an electronic health record environment. Consultative review of digital patient information (e.g., images, results) now enabled by multimedia data exchanges can improve both time to decision and patient satisfaction within a clinical-grade network.

Similar to the previous discussions of information transfer in a timely manner, enforced Service Level Agreements (SLAs) require defining requirements and then enforcing these definitions within the

deployed technology infrastructure and support systems. Beginning definitions at the application availability or services level will allow for an encompassing definition versus simply defining elemental or network uptime requirements. Once the goal is defined, risks and dependencies need to be identified. In order to deliver an SLA, elements from basic physics and network protocol controls through to application resiliency elements must be accounted for. A systematic analysis of the dependencies and risks can provide a confidence factor that the SLA goals can actually be accomplished within the environment being deployed.

After basic analysis is completed, leveraging features for physical, infrastructure and application controls will allow a clinical-grade network to be deployed for optimal support of the environment.

Nortel provides products such as the Application Switch, Switched Firewall, Secure Multimedia Controller and

Communication Servers along with the variety of infrastructure elements mentioned previously to create an environment that can be controlled to provide SLA services. Coupled with Nortel's Network Management portfolio for the distribution and control of the environment, these collaborative elements allow for mitigation of risks and dependencies to meet many SLA environmental needs.

Convergence of systems, applications and usage

All participants in patient care require access to information, appropriate to the caregiver's roll and EMR module being accessed. Convergence of systems applications and their usage can bring this litany of requests and sources into a manageable systemic flow. Multiple levels of access are inherent to patient interactions appropriate to the caregiver's role (e.g., physician, nurse, scheduler, transport technician). Multiple devices also



are generating a spectrum of inputs to enhance decision-making by staff.

As the adoption of Services Oriented Architecture (SOA) structures become more and more prevalent, it will be necessary to both understand the constructs that this architectural shift requires and enables for convergence on many levels.

Moving toward a single interface for many services, whether physically at the device use level or logically at a user interface level, many services should become clicks on a screen versus discrete devices or applications that must be mastered to change a patient care protocol. As this simplification occurs, more time is available for patient care and consultation.

Back-office application integration and possible homologation with front-end patient care activity is a key to the success of electronic health record implementations and acceptance. Allowing a single patient activity to trigger off the necessary back-office elements required for regulatory, billing and outcomes elements adds to the simplification of patient care.

Convergence of other elements within the network such as AAA, Presence

awareness and location controls will also bring additional levels of operational simplification into play for clinical-grade networks.

Manageability of the environment

Manageability of the environment during implementation and deployment of a clinical-grade network takes advantage of tools and resources for troubleshooting during this phase. These same tools can also be leveraged for continuous improvement goals within healthcare environments.

Nortel brings a wealth of experience and tools to clinical-grade network implementations. Management elements that integrate with existing AAA systems as well as augment these systems with front-end and back-office controls allow for reduced Total Cost of Ownership (TCO) to be another positive consideration for clinical-grade network deployments.

Tools such as Nortel's Enterprise Network Management System, Enterprise Telephony Manager, Enterprise Policy Manager and Address Domain Manager allow for comprehensive management of the various aspects of a clinical-grade network. All of these tools also provide integration tools to blend into existing

hierarchies of management systems while adding their own unique capabilities to the Network Manager's arena of controls.

Interoperability

As the healthcare environment moves forward, linkage and correlation requires that the multiple levels of technology creating a clinical-grade network must provide interoperability. Interoperability must be accomplished without degrading other clinical-grade network requirements.

Within the 100+ years of Nortel's existence, there have been many times that standards definition and advocacy have been necessary. This tradition continues with clinical-grade networks. All elements within a clinical-grade network must be standards-based and interoperable to provide for an ecosystem of elements that support the end goal of better patient care and outcomes. This tenet is brought forward to emphasize the importance of working within a collaborative environment, both at the human level and at the infrastructure level. Development of open Application Programming Interfaces (APIs) and supporting common service provisioning and control languages allow Nortel implementations to provide information



upstream and control elements downstream from a given transaction where proper authentication and authorization are available. As Nortel works with a variety of Healthcare Information Management Systems providers, the need to be open and interoperable has always been a requirement of the systems we provide to customers.

Usability

End users are always key to the acceptance and use of any healthcare service and their perceptions of the usability of any portion of the clinical-grade network are critical to realizing expected gains of the system being implemented.

A clinical-grade network focuses upon the end-user experience in providing healthcare services. Many of these elements are controlled at the application level. However, the proper infrastructure is required to enable many improvements in the actual delivery of healthcare services.

For example, presentation of the necessary information while avoiding physical constraints and balancing the proper security controls are all elements that are enhanced with the proper clinical-grade network deployment. The other side of this particular discussion revolves around minimizing extraneous information that is either clinically unnecessary or exposure of the data may be regulatory or procedurally limited.

An additional aspect of usability is the ability to enable users of information technology to control their environment during particular procedures. The default may be to not disturb the caregiver, while during a case with a particular patient the clinician may want to collaborate with a specific colleague. This situational-specific control can be enabled within a Nortel clinical-grade network.

These examples, along with the ability to support models and modes of communication that fit into users' specific needs whether in a medical center, medical

office building, clinic or in transit between these and other facilities, generally enables a higher acceptance rate for successful clinical-grade networks.

As your environment moves toward the need for a clinical-grade network, a final non-technical element needs to be addressed. The Total Cost of Ownership (TCO) must be weighed into the decision of vendor partnerships. Nortel brings a respect for the need to lower the TCO of the companies that we do business with and drives all of the solutions that it brings to market toward the goal of lowering the TCO and fulfilling our vision of Business Made Simple.

In conclusion, communication, collaboration and partnership are all needed to create a successful clinical-grade network. As a technology innovator, Global Services provider and open standards partner, Nortel is ready to assist you with the many facets of a clinical-grade network implementation.

Nortel Services www.nortel.com/services

Nortel Products www.nortel.com/products

Nortel Customer Solutions www.nortel.com/solutions

Nortel Healthcare Information www.nortel.com/healthcare

Tolly report on SMLT and Terabit cluster

http://www.nortel.com/products/02/bstk/switches/baystack_5520/collateral/tollyts205116.pdf

Designing a resilient network - 8600 collateral

http://www.nortel.com/products/01/passport/8600_rss/collateral/nn107680-031804.pdf

In the United States:

Nortel
35 Davis Drive
Research Triangle Park, NC 27709 USA

In Europe:

Nortel
Maidenhead Office Park, Westacott Way
Maidenhead Berkshire SL6 3QH UK

In Canada:

Nortel
195 The West Mall
Toronto, Ontario M9C 5K1 Canada

In Asia:

Nortel
United Square
101 Thomson Road
Singapore 307591
Phone: (65) 6287 2877

In Caribbean and Latin America:

Nortel
1500 Concorde Terrace
Sunrise, FL 33323 USA

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Our next-generation technologies, for both service providers and enterprises, span access and core networks, support multimedia and business-critical applications, and help eliminate today's barriers to efficiency, speed and performance by simplifying networks and connecting people with information. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

For more information, contact your Nortel representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

Nortel, the Nortel logo, Nortel Business Made Simple and the Globemark are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2007 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel assumes no responsibility for any errors that may appear in this document.



> BUSINESS MADE **SIMPLE**