Report progressive hospital

Business

There are also 30 Community Clinics which access the Hospital’s network using Telecom’s Frame Relay service.

CCHB has approximately 15000 users and 200 servers. 1 Local Area Network 1 Network setup within each site: Equipment: At each of the two CCHB sites, there are two Core Switches. These areCiscoCatalyst 6500 switches incorporating Route Switch Modules (RSMs) for Layer 3 switching. Appendix A) The core switches are high end components, offering scalable switching bandwidth up to 256 Gbps. They are chassis based and accept cards to support different media.

CCHB use a number of different card types, including 1Gbps fiber, 100Mbps fiber, 10Mbps fiber, 100Mbps UTP. At each site, the second core switch is cascaded off the first. Building Switches are then cascaded off the Core Switches. These Building Switches are a variety of Cisco Catalyst Switches, including models 4000, 4500, 5000 and 5500. (Appendix B) Servers are Compaq Proliant, running Windows operating system, or Sun Servers running UNIX.

The UNIX machines are used for specific applications, usually involving an Oracle database. Management and maintenance of the Sun Servers is outsourced to EDS (New Zealand office of an international IT consultancy). Each site has a secure server room, which requires card and pin code for access. Inside the room, four rows of approximately 200 rack-mounted servers are positioned on top of a false floor where all cabling runs, protected by H2O sensors. These sensors detect minute water quantities.

On the ceiling are smoke detectors, and three air conditioning units circulate and regulate the air.

Building switch rooms and building hub rooms are also secured through keyed access. Topology: Each hospital building houses a building switch, and from this, 12-port hubs are cascaded (as many as required to service the building). The ports on the hubs are connected with UTP cable to RJ45 connection sockets for each individual workstation, modality, printer, etc. There are over 4000 ports supported across the entire organisation. Servers connect directly to the Core Switches (diagram 1) and are located at either Remuera or City Centre depending on where most users of the particular server are based.

Media: The servers are connected to the switches using 1Gbps fiber or 100Mbps UTP. The clients connect to the hubs using 100Mbps or 10Mbps. Protocols: The organisation uses TCP/IP exclusively for its LAN. Ethernet and Gigabit Ethernet are the Layer 2 protocols in use to support this. [pic] Diagram1: Logical Network Diagram Remuera / City Centre.

2 Wireless LAN: A small section of the City Centre site has been configured for a Wireless LAN, with Access Points positioned throughout the defined area. The size of the WLAN area is limited by the number of Access Points available for use.

The WLAN has a number of limitations and specific issues, including the need for UPS devices, potential for interference with hospital equipment, increased security issues regarding network access and virus introduction, and the overall additional costs of supporting a wireless LAN. 3 3. Routing

Incorporation of the Route Switch Module in the Cisco switches means that the switches can provide both Layer 2 (switching) and Layer 3 (routing) functionality.

The Core Switches act as the routers for the site, handling traffic flows within and between the sites.

When traffic needs to cross from one VLAN to another, the Core Switch (using the RSM) routes this traffic. Traffic between the Core Switches, and between the Core and Building Switches is trunked using Cisco’s proprietary frame tagging technique, ISL (InterSwitch Link), rather than the IEEE802. 1q standard. 4 4.

IP Addressing CCHB uses private IP addressing (10. 0. 0. 0) and a Proxy / NAT Server for Internet access. This helps improve the speed at which users can access pages on the Internet because visited pages are cached at the server for faster future retrieval.

The use of a NAT server hides the internal addressing, which protects against ‘ smurf’ attacks.

5 5. VLANS The switches have been configured to implement Ethernet VLANs (some for security reasons, some to reduce network traffic). The Cisco Catalyst 6500 switch is capable of supporting up to 256 VLANs on a single RSM. The CCHB currently has 6 VLANs implemented: ? Oncology system ? PACS system (radiology images) ? Patient monitoring system ? Wireless network ? Auckland City Hospital ? Other (general) users Each VLAN has its own IP range / subnet. [pic] [pic] 3 6.

Virtual Private Networks

Approved users can access the Hospital network from their home PC via VPN. A Cisco VPN Concentrator, a dedicated piece of hardware (Appendix C) is used at the Hospital end and the Cisco VPN Client software is installed on the user’s home PC. The VPN is created using IPSec over L2TP. A RADIUS Server is used to authenticate users who access the Hospital network this way (Appendix D). The RADIUS server has User Groups implemented which map to the Active Directory User Groups.

4 7. Metropolitan Area Network The dedicated fibre link between the two sites is provided by Telecom and is leased by CCHB. Media:

The link consists of a dedicated fibre cable running from the City Centre site to Telecom’s Mayoral Drive exchange; and another dedicated fibre cable running from the Mayoral Drive exchange out to the Remuera site. Equipment: At the exchange, the two fibre cables are connected to an CCHB dedicated Cisco 3550 switch owned by Telecom. At this stage CCHB are only leasing 200Mbps worth of the 1Gbps capacity.

The rate limiting capability of the Telecom switch enforces this. 5 8. Wide Area Network 1 Community Clinics CCHB has 30 Community Clinics that access the Hospital network via Telecom’s Frame Relay services.

Permanent Virtual Circuits are implemented for each of the clinics, each with a guaranteed bandwidth of 320Kbps (CIR) and a burst rate (PIR) up to 1Mbps. The PVCs join directly to the CCHB LAN through one of four Cisco routers (these are older models, eg 2660s, 4000s).

At the Remuera and City Centre sites, the data is received in 2Mbps trunks (ie each trunk can carry 6 of the 320Kbps connections). The Community Clinic traffic and users are considered to be trusted, and as the Frame Relay technology is considered to be relatively secure, no additional security measures are in place. 2 9. Health Alliance connection

Waitemata, North Shore and Counties Manukau District Health Boards have formed a strategic alliance, called Health Alliance for the purchase of services. IT services are purchased jointly and Telecom have provided dedicated fibre cables from North Shore, Waitakere and Middlemore Hospitals into the Mayoral Drive Exchange.

As with CCHB, the fibre cables are converted to UTP and joined by a dedicated switch. The CCHB Switch and the Health Alliance Switch are co-located (positioned next to each other with a fibre connection from one switch to the other), providing connectivity between the networks.

The Health Alliance traffic is trunked from the Mayoral Drive Switch to the City Centre site where it passes through the DMZ before connecting with the LAN. Control over access between the networks is managed by firewalls and authorization at each site. 6 10. DMZ Each of the two main sites has an external switch that receives all trunked traffic from the Mayoral Drive Exchange.

This switch breaks out internal VLAN traffic, which is directed to the 6500 Core Switch and then appropriately onto the network (depending on VLAN tagging). Other traffic, eg Internet traffic, is routed/switched to a hardware Cisco Firewall (Appendix E).

The Firewall is dualhomed and delivers the Internet traffic to an internal switch on a separate VLAN. The Mail Server, VPN Concentrator, Proxy server and WebServer (hosting hospital website) are all connected to ports on this VLAN, and are all in turn multihomed to the LAN. The individual servers are configured to act as software firewalls for the connections to the LAN: routing is disabled on these servers to ensure traffic cannot pass through from the outside onto the LAN and all services not required are disabled on these devices.

All outgoing traffic is allowed, and all incoming traffic is stopped except for SMTP. This means users can access the Internet (as they create an outgoing connection), but unsolicited traffic from the Internet is blocked. Traffic received from the Health Alliance switch (considered to be untrusted traffic) is switch/routed to the City Centre firewall. All traffic from this source is blocked and then allowed by exception using manual routing rules. [pic] 7 11.

Network Redundancy

The organisation has a failover / fault tolerance system in place to ensure a link between the two sites is maintained in the event of a failure in the dedicated fibre connection. An entirely separate connection between the sites is created using additional routers at each site connected by a 6Mbps microwave link. Cisco Hot Standby Router Protocol is used to monitor the state of the primary connection (fibre link) between the two sites and if this connection fails for any reason, all traffic is diverted to the standby routers and is thus transmitted via the microwave link.

The 6Mbps capacity of the standby link would not be sufficient to provide full services, but would at least allow essential connectivity between the sites to be maintained. Description of Protocols LAN Protocols The site uses TCP/IP exclusively, and Ethernet (IEEE802.

3) and Gigabit Ethernet (IEEE802. 3z) to support this. Speeds include 10Mbps, 100Mbps and 1Gbps. Gigabit Ethernet is for the link between the 2 sites. Network Management Protocols SNMP is the network management protocol used on site, largely because the key managed devices and tools used on site are all SNMP based.

Hot Standby Router Protocol Hot Standby Router Protocol is used to provide network redundancy, ensuring connectivity between the two main sites in the event of failure of the main fiber connection. L2TP CCHB use L2TP to create a Virtual Private Network connection between users' home PCs and the CCHB network, over the Internet. IPSec While L2TP ensures the transfer of unsupported data across the Internet, it does so in clear text. IPSec is used to encrypt the data prior to encapsulation to provide authentication, confidentiality and integrity.

WEP Wired Equivalent Privacy is an encryption algorithm defined in the IEEE802.

11 standard for encrypting data on wireless LANs. It has several weaknesses that result in wireless LANs being considered as security risks. The main weakness of WEP is the way in which data is encrypted and the fact that a hacker can use a ' sniffer' to crack the encryption key. Frame Relay Frame Relay is the Wide Area Network protocol used by CCHB to implement

Permanent Virtual Circuits between the main sites and their Community Clinics. 13. Network Management Software All servers managed by the Network Operations team are Compaq servers.

A server tool, Compaq Insight Manager, is used to maintain a view of the server states. This view uses colours to indicate the status of each server and allows the Network Operations staff to drill down to individual servers to view a number of elements including network and disk state information, eg statistics on CPU usage, and disk health. WhatsUp Gold and CiscoView are used to keep track of the network operations.

CiscoView provides a view of the current state of any given switch, with the ability to drill down and access detailed performance information regarding the traffic active on the switch. Cisco provides WhatsUp Gold bundled with CiscoView for use as a network mapping and monitoring tool, which has been used at CCHB to map the Core and Building Switches. Compaq Insight Manager, WhatsUp Gold and CiscoView all run on a management PC in the Network Operations area at CCHB.

3 monitors are connected to the PC to allow concurrent viewing of the 3 main screens: the server states, the switch states, and the core link between the sites. 14. Performance Management ensuring the network is operating as efficiently as possible IPClarity A 3rd party service provider, IPClarity, provide a performance monitoring service. The company provide a hardware device (called a ‘ DataSink’) which is connected to the CCHB network. This ‘ box’ polls devices on the network to gather information about their state.

The DataSink can auto-discover SNMP capable devices on the network and can include these in the monitoring if configured to do so.

The polling results are forwarded to the IPClarity central database where they are compiled and made available in the form of web-based reports and alerts. The CCHB Network Operations staff can access realtime information to see current and recent statistics on many variables. The service can provide reporting on: CPU performance, up/down status, latency from the DataSink to the device, availability, free memory, and buffer utilisation. IPClarity is a fully managed service, provided and managed offsite and accessed via a web interface.

Reporting can be carried out on live data or historical data.

Filter reporting can allow the site to identify any potential bottlenecks or trouble points (eg list the 10 most error-prone ports) and therefore allow opportunity for better optimisation of the network. CCHB has access to the last week’s worth of data in online, realtime reports to view any recent trends. The service can provide up to a year’s worth of data for live reporting and data is stored for 3 years. The IPClarity service includes threshold alert functionality, where thresholds can be configured and alerts raised if the threshold is exceeded. Alerts can be sent using SMS (short messaging service), or email, or simply logged.

Additional configuration options allow the site to specify the period for which the level is sustained before alerting; a period of time or counter in which not to raise the same alert again, or request not to be notified again unless it drops back to a pre-defined level. However, CCHB do not make use of the

alert functionality – the Network Operations Manager believes that they hear of bottlenecks, issues, etc from users just as quickly as they would from alert reporting. CCHB has 24 hour network support, so any queries are directed to the on-site or on-call staff.

The Internet is widely used by staff members, with a few key websites particularly popular. The Network Operations team use Latency Testing provided by the IPClarity service to monitor the latency on some popular websites, to help ascertain whether any speed problems are internal network issues. This is done using a ping and HTTP request.

The XTRA DNS router (closest point), NZ Herald (reliable NZ site) and Recruitsoft (US site popular with hospital staff) are all monitored. Compaq Insight Manager Performance monitoring of CPU, PCI and EISA bus utilization in the Compaq Servers is possible with Compaq Insight Manager.

It allows the setting of thresholds on parameters such as CPU, bus and disk partition usage for performance monitoring. However, CCHB don’t use the Performance Monitoring functionality of the software. They do use the drilldown capability of the software to view individual details for a server in a Fault Management capacity.

CiscoView CiscoView is partly used for performance management, with the ability to drilldown to view current performance statistics on individual routers (Layer 3 switches), however, CCHB generally make use of CiscoView for Fault Management. 4 15. Hardware Tools

All cabling is outsourced by CCHB and is warranted by the suppliers, so the CCHB network team don’t make any real use of tools such as cable testers, LAN analysers, reflectometers, etc. 5 16. Other Software Utilities PerfMon (to capture and analyse performance statistics) and NetMon (to capture and analyse network packets) are used on occasion if required to investigate a specific problem.

Event Viewer is used to monitor Servers, and the site are investigating the use ofMicrosoftSMS (Systems Management Server) for planning, deploying and managing software applications. Organisation of the Operation and Maintenance functions

The City Centre Health Board network and data communications are a centralised system with a hierarchical structure, and consistent protocols, equipment, and management across the whole network. One central team is responsible for managing all network related activities and they are also responsible for integrating any new network requirements appropriately into the existing framework. For example, in 2003 the Radiology department completed an 18 month long implementation of a new computerised Radiology system (PACS) which manages the production and storage of all radiology images (MRI, CT, X-ray, etc).

The system replaced the hardcopy filing system and is now producing over 20GB worth of images per day which must be created, transported and saved, and be available realtime for retrieval by specialised diagnostic workstations. Rather than implementing a separate LAN to support this new system, the support for the system was incorporated into the existing

infrastructure. This saved on duplication of hardware (media) and ensured full interoperability with other hospital systems. A VLAN was created to separate the significant amounts of data from the rest of the hospital network.

MAN and WAN management is outsourced to Telecom New Zealand Ltd, and remains part of the responsibility of the centralised Network Operations team. Telecom’s LANLink Managed Network Service is used to manage the Mayoral Drive switch and the Frame Relay connections between the Community Clinics and the main sites.

Tasks are spread across the Network Operations team, ensuring a multi-disciplinary team. Documentation is used to assist in ensuring consistency in actions and tracking of activities. The site does not have a specific maintenance plan.

Service Packs and non-critical updates are applied whenever a server is having other work done on it. Critical updates are applied as they are released. Other network maintenance is done on an ‘ as required’ basis.

The site maintains 24 hour support by having Primary and Secondary on-call staff. They are required to respond within 15 minutes. User access to servers, applications, etc on the network is by exception – users start with minimal Internet access (a few approved sites) and a few basic applications.

Any additional access is requested and granted if approved. The integrity of the machines is protected by user awareness and culpability.

With 15000 users and a 20% staff turnover rate, the Network Operations team felt that trying to manage Group Policy and Profiles could prove very time consuming. Instead, CCHB have a user-pays policy. CCHB allow a user one incident where a PC needs significant attention due to careless use of the machine/resources (eg as a result of inappropriate Internet access). Any future incidents cost the user personally, at $500 each.

Any software installation on a client PC is attended to by a Network Operations team member (staff do not have permissions to install software). Backup Systems The site uses Veritas Backup Exec to backup server data, using daily incremental backups.

Two copies are made of each backup and are stored separately in different locations (buildings) from the servers. Data redundancy is also ensured on the servers by using RAID 5 or disk mirroring. 800GB of data is backed up per day on each of the two main sites. 17. The Requirement

Due to the increase in the number of customer base it is envisaged that the existing City Centre hospital is to be extended to cater to an additional 2000 patients and 100 staff members. The areas of expertise in the new facility would be spread across all areas of the medical discipline as in the existing set up at the City Centre and the Remuera sites.

A network needs to be established for the new extension and integrated with the rest of the existing network at the city centre site. The IT manager is expecting the network traffic to increase in proportion to the additional load.

As for the other requirements like performance management and security, these would be at a level no lower than the existing set up. A possibility of change in the existing infrastructure in addition to the media and equipment for the new facility as a consequence of the integration would also need attention. The new extended network design is anticipated to cater to Vo-IP and other requirements well into the next five years.

The senior nursing and medical staff that would be 50% of the total staff members are expected to be connected on an anytime anyplace basis.

The hospital CEO has also recommended that you explore the possibility of video conferencing involving document/radiological/surgical procedure exchange in the new network design. List any assumptions being made for the requirements analysis, the logical design and the final physical design. Assumptions being made should be supported by research for both the standard and specialist applications in a modern medical facility.