Advances in Networks
2015; 3(3-1): 23-26
Published online September 16, 2015 (http://www.sciencepublishinggroup.com/j/net)
doi: 10.11648/j.net.s.2015030301.13
ISSN: 2326-9766 (Print); ISSN: 2326-9782 (Online)

Infrastructure Security in a Paediatric Hospital: Architectural Evolution, Virtualization and Network Management Systems

Domenico Cacciari[1, 2], Daniel Zotti[2], Edoardo Sossa[1], Michele Bava[1, 2]

[1]Institute of Maternal and Child Health IRCCS "Burlo Garofolo", Clinical engineering and IT Department, Trieste, Italy
[2]Department of Electronics and Computer Science, University of Trieste, Trieste, Italy

Email address:
cacciari@burlo.trieste.it (D. Cacciari), dada007_87@hotmail.com (D.Zotti), sossa@burlo.trieste.it (E. Sossa), bava@burlo.trieste.it (M. Bava)

To cite this article:
Domenico Cacciari, Daniel Zotti, Edoardo Sossa, Michele Bava. Infrastructure Security in a Paediatric Hospital: Architectural Evolution, Virtualization and Network Management Systems. *Advances in Networks*. Special Issue: Secure Networks and Communications. Vol. 3, No. 3-1, 2015, pp. 23-26. doi: 10.11648/j.net.s.2015030301.13

Abstract: The match of research activity, paediatric healthcare services offered by the IRCCS Burlo and internet access of long-stay patients produces a complex situation regarding IT security, network architecture and management. Often at the most inopportune time computers and other electronic devices quit working so the IT Staff has to ensure the proper functioning of equipment needed by the hospital's activity, the access to the network ensuring both intranet and internet protection and a strong access control to prevent as much as possible any fault or data loss. By the IT staff studies came to light the needs of a network infrastructure built ad hoc for the Burlo environment and a strength and secure server farm able to grant a strong service continuity in order to gear secure and reliable workstations. This paper shows how the IT Staff has reached that, implementing some Network Management System and capitalizing on virtualization capability.

Keywords: Computer Security, Networks, Computer Network Management, Computer Network Security, Protection

1. Introduction

The main problem, inside the hospitals, consists in considering IT security and the whole IT as abstract concepts, until important data get lost or corrupted. Therefore, the budget is never suitable to the IT requirements, particularly in small or medium hospitals, as IRCCS Burlo Garofolo.

For this reason, is very difficult to face IT security threats without an intelligent and efficient resource management.

So opensource softwares have been chosen because, although they initially are tough to use and suitable for expert technical staff, they are free and personalizable for the requirements of each single user and adaptable for the continuously changing needs.

As well as for software the intention was to reduce the costs, using opensource softwares, for the hardware the best solution was the virtualization: in fact it cuts hardware, maintenance and management costs, and also all the costs connected to energy consumption, environmental impact, physical space decrease.

2. Computer Security Through Network Security

Starting from the assumption that it is impossible to find a really secure working environment, it is then fundamental to make a detailed analysis of the risk in order to determinate the possible mistakes and gaps and take measures to reduce the vulnerability.

Nowadays the main problems come mostly from the lacking of technological competences of the users and not from the outside of the network.

Besides that, it must be considered that there are many different situations at the IRCCS Burlo Hospital: sanitary personnel that manage sensitive and personal data of the patients, laboratory technicians who must guarantee 24h analysis and their reliability, administrative personnel, researchers who has to access database and calculating and analyzing tools, long-stay patients who must have the right to access the internet and some services on the intranet,

without risking to compromise the normal hospital's activities.

The studies and the new management of the IT in order to have secure and reliable working environment, have shown [1] that users' awareness and network security are fundamental.

2.1. Network Architecture

In order to realize a functional management, a logical and typological partitioning, based on different type of activity, was implemented.

For each type of activity was created a VLAN: one for the administration, one for the laboratory, different VLANs for operating rooms and intensive care rooms, one for the long-stay patients, etc.

To put in practice this network sectioning, a couple of router CISCO4500 was used as central-node.

Furthermore, a couple of firewall controls the internet access of the entire hospital and even the VLAN for the long-stay patients (only wireless connection using CISCO air-ap113) who must have the internet access without any cognition of the internal network.

These Firewall, two SonicWall NSA5500 in High Availability, were used as content-filter, anti-spyware software, anti-virus with client-av presence check on connected computer and remote accesses with VPN and SSLVPN.

In order to obtain this representation was utilized phpWeatherMap because it allows a general survey of the real situation.

2.2. Network Management

After having created the idea of a useful and functional architecture for the requirements of the IRCCS Burlo Hospital, it was followed a development path.

In the first step, single opensource softwares like php Weather Map (Fig.1) and Cacti, which both allow the monitoring of the state of each node (switches, hosts, servers and servers' services, etc.), and Op Utils of Manage Engines (Figure2) were used.

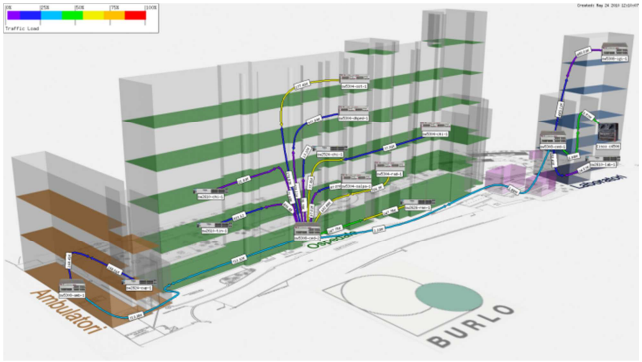

Figure 1. *Burlo 3D Map - phpWeatherMap.The illustration (Figure 1) shows the 3D Hospital Map, where each switch belongs to a dedicated VLAN, that represent all the network apparatus within their network traffic.*

The third software, the only non-free one, not only monitors all network nodes but also, through WUI (Web User Interface), allows to modify in a very simple way the configuration of each single node, through SNMP protocol, to find a solution to any detected problem.

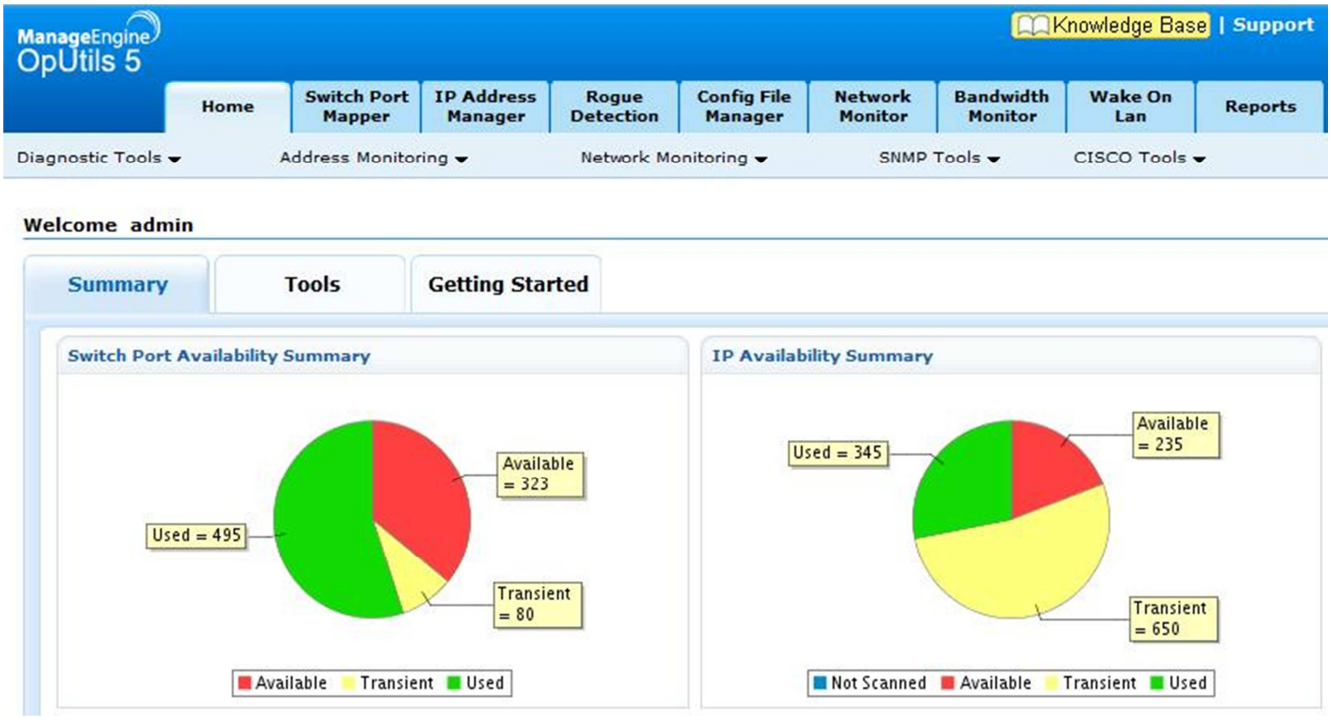

Figure 2. *Switch port and IP utilization graphs - OpUtils.*

Through this initial path IT Technicians were compelled to control many different source of information.

In the second step, in order to simplify this working method, the SANET software (Security Architecture

NETwork) was implemented; it is a network management system for experts which integrates in one single software the functionalities of Cacti and phpWetherMap (Fig.3 and Fig.4).

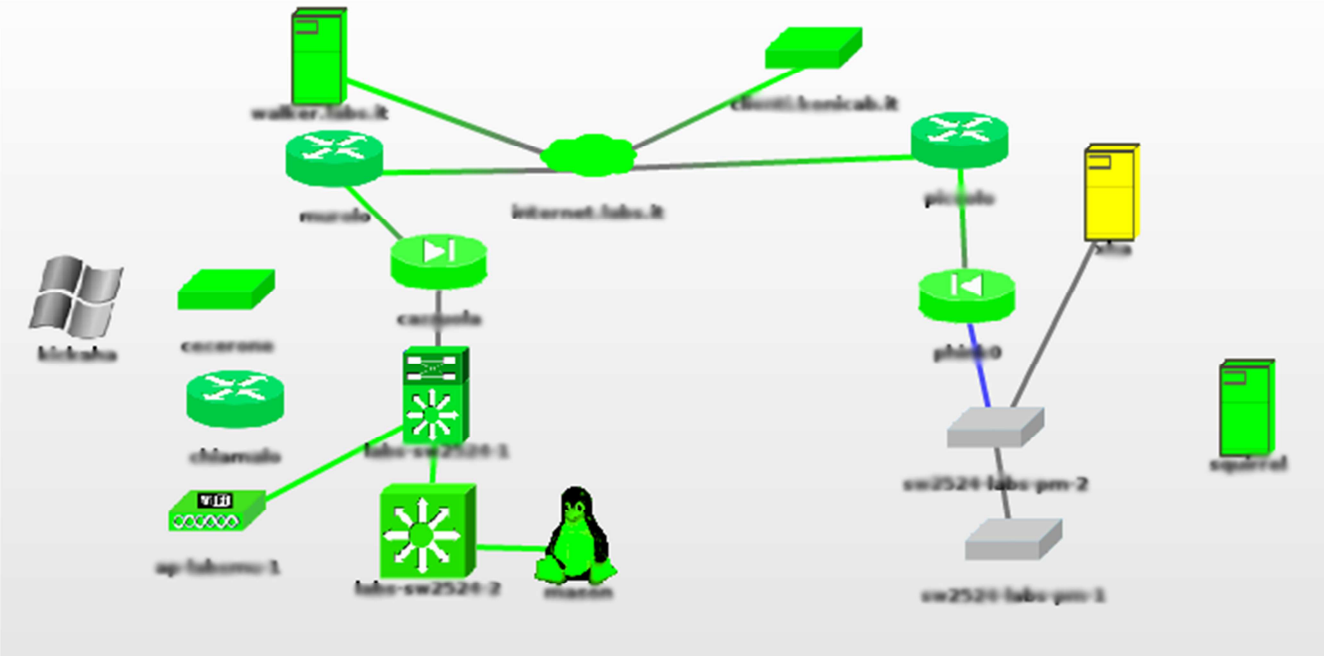

Figure 3. *Nodes map with nodes status - SANET.*

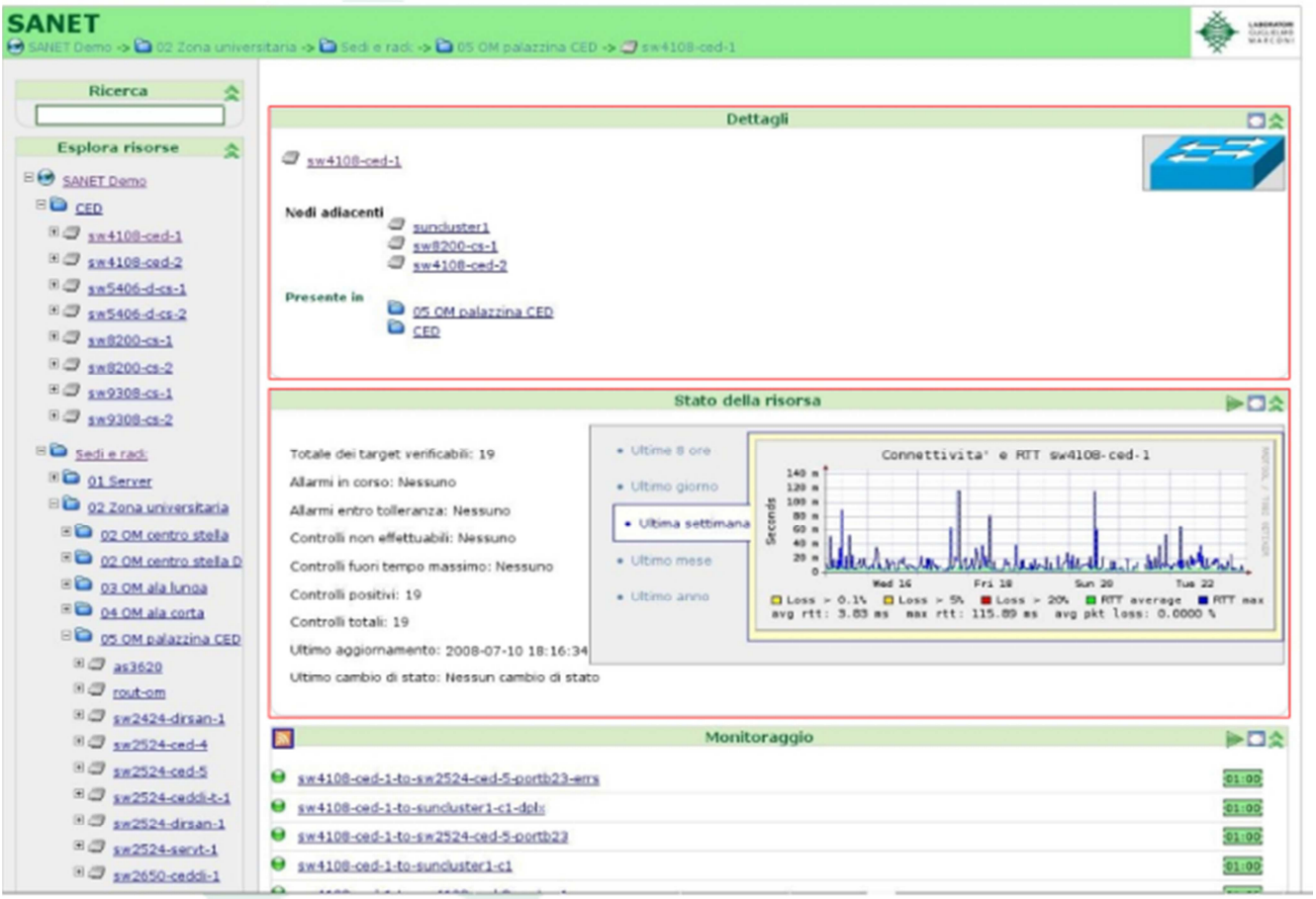

Figure 4. *Node details - SANET.*

It has a more user-friendly WUI because each user visualises just the resources that he/she is qualified to

manage, collecting in one single page (Fig.4) the information related to state, connectivity and accessibility of the interested nodes.

All this allows an easier "all-in-one" analysis, permitting to find gaps or problems before it damages the user's activity, both hospital's personnel, and patients. Furthermore, visualizing the likely causes of the different problems in such a detailed and precise way, it is possible to find out the solution easily, in order to get to the bottom of the problem.

In order to guarantee a secure access to the network, besides the monitoring, protocol 802.1x (concerning the wired connection) and WPA AES MSCHAPv2 (concerning the wireless connection) were implemented with a FreeRADIUS server, completely integrated with Active Directory.

The only exception is in the VLAN (just the wireless connection with WPA-PSK) for the long-stay patients, which is similar to an internet point. A captive portal software was adopted, with authentication on radius, which allows the patients to surf the network and to chat freely without interfering and/or having any access to the office automation. However, the network is protected from virus, malware and spam.

2.3. Server Farm Management (Virtualization)

In the third step, given that virtualization is a well-established technology nowadays, it has been used at Burlo Hospital because it perfectly fits the budget and energy saving needs. Moreover, it guarantees more reliability and service continuity, compared to the single separated physical machines.

Other advantages concern purchase costs, hardware maintenance, energy consumption and physical space, and last but not least, the reduction of the refrigeration costs.

Due to the quantity of physical servers for 2010-2011, it has been decided not to buy VMware vSphere licenses, but to limit the choice to VMware ESXi free version, used on 3 Sun Fire X4450 geared with 4 Quad-Core Xeon X7350, 32Gb RAM, 8 SAS Discs of 73Gb 15 krpm. Due to obvious security and reliability reasons, the third machine acts as backup machine.

Once the servers' virtualization is consolidated with a proper infrastructure, the client virtualization can start (thin client + virtual desktop) and it logically allows better security and AAA control (Authentication, Authorization and Accounting).

3. Conclusions

The followed path at Burlo Hospital has been very important because the IT Staff is now aware that the network infrastructure and the server farm must be studied and updated, using the available technologies and developing integration methodologies between them based on the various requirements of the working environment.

However, there must always be particular attention for each workstation, both for its technology updating and for a high level of security and reliability.

It is true that the IT Dept. has decided to guarantee computer security through network security and now it is also true that the network cannot be secure if the nodes aren't secure.

Besides all this, it is also required a constant formative updating of the whole IT Staff, in order to be always ready to face the new technologies and threats.

Furthermore, the IT Staff at Burlo Hospital is planning systems which are based on Artificial Intelligence algorithms that are able to analyse the information produced by the whole hardware and software infrastructure, and then decide which is the best solution to a problem and giving notice to the technician.

Acknowledgements

Thanks to Laboratori Guglielmo Marconi, that have created SANET software and Krizia Bencic for her support.

References

[1] Bava M., Cacciari D.; "Information Security Risk Assessment in Healthcare" – in *Proc. 1st International Conference on Computational Intelligence, Communication Systems and Networks CICSyN 2009*, Indore, India, 23-25 July, pp. 321-326

[2] Pfleeger C., Pfleeger S. *Sicurezza in informatica. Pearson* – Prentice Hall 2004

[3] Erikson J. *L'arte dell'hacking*. Apogeo 2008.

[4] Mortellaro A., Cacciari D., Accardo A., Zangrando R., Bava M.; Sistemi per la gestione della sicurezza informatica delle reti ospedaliere: un protocollo per la valutazione dei rischi e delle vulnerabilità dei dispositivi medici collegati in rete. XIII Convegno Nazionale AIIC (Associazione Italiana Ingegneri Clinici) "Information Technology & Medical Devices", Napoli, 11 – 12 Aprile 2013

[5] Cacciari D., Zotti D., Sossa E., Bava M.; Evoluzione architetturale, virtualizzazione, sistemi di gestione e monitoraggio per la sicurezza informatica di una rete ospedaliera. 11° Congresso nazionale @itim 2011, IRCCS "Rizzoli", Bologna, 29-31 Maggio 2011

[6] Bava M.: Analisi del Rischio per la Sicurezza Informatica in Sanità: l'esperienza dell'IRCCS "Burlo Garofolo", atti del 9° Congresso Nazionale dell' Associazione Italiana di Telemedicina e Informatica Medica, @ITIM 2008, pp. 9-15, Trieste, 14-16 Dicembre 2008