Week 2: Patton-Fuller Network  
Nate Bachmeier  
May 10, 2014  
NTC 362: Fundamentals of Networking  
University of Phoenix  
Facilitator: John Buono

**Contents**

[Section I 3](#_Toc389063207)

[Patton-Fuller Community Hospital 3](#_Toc389063208)

[Evaluate the Current Network Topology 3](#_Toc389063209)

[Deliverables 3](#_Toc389063210)

[Convert the Administration Network to a WLAN 3](#_Toc389063211)

[Install VoIP in the Hospital 4](#_Toc389063212)

[Design a High-Speed WAN 5](#_Toc389063213)

[Section II 7](#_Toc389063214)

[Importance of Communication Protocols 7](#_Toc389063215)

[The Solutions 7](#_Toc389063216)

[Translating this to Networking 8](#_Toc389063217)

[Identify Protocols for the Hospital 8](#_Toc389063218)

[Authentication and Authorization Protocols 9](#_Toc389063219)

[Intranet Routing 9](#_Toc389063220)

[Wireless Communication 10](#_Toc389063221)

[Virtual Private Networking 10](#_Toc389063222)

[Purpose of Traffic Analysis 10](#_Toc389063223)

[Performance Considerations 11](#_Toc389063224)

[Terms: Latency, Response Time, and Jitter 11](#_Toc389063225)

[Impact of Data Rates across the Ecosystem 11](#_Toc389063226)

[Options for Improved Availability 12](#_Toc389063227)

[Section III 12](#_Toc389063228)

[Identify Hardware and Software to Protect the Network 12](#_Toc389063229)

[Network Access Protection (NAP) 13](#_Toc389063230)

[Web Application Firewalls 13](#_Toc389063231)

[Virtual Local Area Networks 14](#_Toc389063232)

[Distinguish Between Area Networks 14](#_Toc389063233)

[Building Blocks of a Network 14](#_Toc389063234)

[Hub 14](#_Toc389063235)

[Switch 15](#_Toc389063236)

[Router 15](#_Toc389063237)

[Conclusions 15](#_Toc389063238)

[References 17](#_Toc389063239)

# Section I

## Patton-Fuller Community Hospital

Patton-Fuller Community Hospital (or simply “the Hospital”), is currently evaluating an expansion of their network infrastructure to include VoIP technologies, provide WAN access to various staff, and gain dedicated connectivity with three local hospitals. To accomplish this goal they will only accept solutions that are based on industry standards and compatible with the Apple OSX platform.

## Evaluate the Current Network Topology

In December of 2012, the Hospital renovated their network to logically partition into two subnets. The first subnet isolates the departments that run the business, such as human resource, finance and IT infrastructure. A second subnet exists to manage terminals for doctors and nurses and various medical equipment.

The connectivity of the existing solution is sufficient for a large load, as both subnets are operating on Gigabyte connections. Routing to other areas of the data center takes place on an OC-1 line providing 51Mbit/sec. A VPN router is also already present and Internet facing.

## Deliverables

### Convert the Administration Network to a WLAN

A frequent request from the administration teams is the ability to access corporate resources, outside of their office using laptops and smart phones. To enable this scenario a Wireless Local Area Network (WLAN) needs to be installed and configured.

One concern with deploying wireless technologies in a hospital or any other business is the security risk that it will introduce to the environment. For example say the Finance department has business policy limiting which machines are allowed access to their physical subnet. If a WAP was installed into their department and connected directly to an open Ethernet port; it could provide a method to bypass that policy and allow other devices access (Conklin, White, Williams, Davis, & Cothren, 2012).

To address this concern and all related issues, the first step to deploying the WLAN is to deploy IP Sec. IP Sec is a technology that provides encryption and authentication of network traffic (Morimoto, 2010). It is based on numerous standards and can be made to work with most commercial grade Wireless equipment. For simplicity the IP Sec solution can be connected directly to the existing RADIUS server, reducing the administration overhead (Hernandez, 2012). Leveraging the Internet Security Association and Key Management Protocol (ISAKMP), the certificates can be easily deployed to the Macintosh devices.

Now that a solution exists to secure and restrict the communication, the deployment of wireless infrastructure will be easier to manage. For each department one or more Wireless Access Points can be installed and connected into the existing Local Area Network. Having such a design is desirable as the increased consistency, increases the supportable (Marchewka, 2012).

### Install VoIP in the Hospital

The first step to deploying a Voice over IP system is inventory the current environment, then estimate the increase in traffic (Information Week, 2005). Making sure the added load will not bring down the existing infrastructure is critical to a successful deployment. From previous experience in this industry, I saw running the VoIP on dedicated network hardware was common practice.

Next unless the plan is to only communicate within the Hospital, an upstream provider needs to be selected. The provider will need to support common standards such as SIP termination or IAX/IAX2 protocols (Soares & Blank, 2014).

Once the provider is selected the next step is to provision one or more Private Branch Exchange (PBX) servers. From previous experience, Asterisk is an open source solution that works great for this. It is based on open standards, highly customizable, and has numerous plugins to enable most scenarios. Another PBX that could be considered is Microsoft Communication Server, which could integrate into their existing Exchange infrastructure.

Finally after deploying the PBX, phones need to be installed at each desk and configured to communicate with the PBX. At this point the environment will be ready and working. Deployment of a management solutions on top of the VoIP would be recommended to ease general administration.

### Design a High-Speed WAN

The Hospital employees a few dozen doctors and radiologist that need remote access to the corporate network. Before investing in private lines for these staff members, it will probably be more economical to route their traffic across the public Internet. Only after discovering the bandwidth requirements of local ISPs is insufficient should a more custom solution be reviewed.

According to the data center diagram, VPN routers are already deployed to the environment. These can be repurposed unless the load, security, or regulatory restrictions do not permit this. If that is the case an additional VPN router can be installed with a dedicated connection to the ISP.

Another requirement of the WAN design is that connectivity is required between three local hospitals. To accomplish this the same VPN over the Internet could be considered and after being found insufficient other options reviewed.



Figure 1: Possible Configuration

# Section II

Now that the Hospital has decided on a high level networking architecture, it is time to look at the finer details. Before implementing consideration needs to be taken to which protocols will be utilized, performance requirements, and also placement of networking equipment that will form the actual implementation.

## Importance of Communication Protocols

Imagine that you have randomly selected people and asked them to hold a conversation. Each of these people only speak one language, and no one speaks the same language. To further complicate the issue, some of these people are very old and not very knowledgeable about common lingo. As the conversation progresses, it is just random sounds and no communication is really taking place.

### The Solutions

There are three methods that can be used to fix the language barrier, with the first being teach (or upgrade) everyone a common language. Depending on long this conversation needs to take place, is the scale years or hour, there could be a lot or very little return on investment (ROI).

The second option would be to hire translator which are able to speak more than two languages. These people are able to bridge the communication islands and provide connectivity. However with these extra people comes extra overhead, latency in the translation, and other costs.

The third option would be to replace these five people with five new people, and instead of randomly choose, have a selection bias. Perhaps only English speakers in the 30 to 35 age range are selected.

### Translating this to Networking

The same challenges of getting the people to talk can also be seen with networking equipment to talk. Instead of having languages, such as English and Japanese, they have protocols such as TCP or TLS.

Many of these protocols have different version, which introduces the same problem as using modern lingo with the elderly individuals. In some of those cases the older, slower and less expressive tokens can be sent to enable backward compatibility; however this removes efficiencies in the implementation.

Because of these constraints, it is important to select communication protocols that are common and well supported. Not only do we need to be looking forward, it is often critical to look back. Say the legacy infrastructure is only capable of using XYZ, but the cost of replacing everything is not economical. Then whatever ABC technology selected had better have a method for working with XYZ.

## Identify Protocols for the Hospital

There are five general types of protocols that the Hospital will need to implement in their solution. They are: Authentication/Authorization, Wireless, VPN, Intranet routing, and other general or encapsulation protocols.

Another abstract way to think about the protocol selection is through the OSI model, which defines seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application**Invalid source specified.**. The idea of OSI is that given enough layers of encapsulation it is possible to move data across media.

### Authentication and Authorization Protocols

If the Internet was designed today, it would have started with defining authentication and authorization protocols across the network**Invalid source specified.**. This way confidentiality, availability and integrity of the system can be ensured **Invalid source specified.**. If they are not then the solution is not viable for a business solution (Conklin, White, Williams, Davis, & Cothren, 2012).

The Hospital needs a solution that will integrate across their heterogeneous server infrastructure, but also with their predominately OSX client base. A common and well supported option is Kerberos, created by MIT. In addition to being a “safe bet” long term, it is also easy to deploy across the environment**Invalid source specified.**.

Kerberos provides a central authentication solution, where machines and devices can request a ticket. The ticket uses digital signatures to ensure it is not tampered, and can be handed to other devices as a proof of identity**Invalid source specified.**. Once identity is known then authorization policy can be applied to the requesting user’s actions**Invalid source specified.**.

### Intranet Routing

Now that the safety of the system can be ensured, the next step is to decide on internal routing protocols that are needed. Open possible solution would be Open Shortest Path First (OSPF), which is “a link-state routing protocol […] used for interior routing**Invalid source specified.**.” Wikipedia went on to say, it is widely supported across commercial hardware and is one of the most widely used interior gateway protocols.

### Wireless Communication

Extending the intranet Local Area Network (LAN) will be several Wireless Access Points and other Wireless equipment. Users will need a method to communicate from their device to this hardware. The recommended protocol would be 802.11n which offers high speed communication and is backward compatible with older yet common wireless technologies such as 802.11g.

### Virtual Private Networking

As suggested in the Section I, the existing VPN network could be extended to provide remote access to the staff. The VPN should communicate over L2TP/IPSec, which is a newer and more secure protocol**Invalid source specified.**.

### Purpose of Traffic Analysis

After the network has been implemented and deployed, the operational teams will need insight into what is occurring across their property. The request for insight will come from the needs of ensuring Service Level Agreement (SLA), detecting compromised devices, and ensure business requirements are taking place.

An example of a service agreement might be that patient files need to be accessible from the Intensive Care Unit within 2 seconds. If the next work is becoming too congested delays can be introduced. Depending on the scenario these delays could result in loss of life, or doctors unable to make informed decisions.

Another usage is to detect malware and malicious users attempting to compromise the environment. For instance a sudden surge in traffic at to the authentication machine may indicate a brute force password attack. A second common example would be a surge of outbound SMTP mail from a single host. If it’s not an email server, but sending like one then it is probably compromised.

Third type is to ensure business policy is taking place and being followed as expected. For instance the organization might not allow p2p music downloading applications on their network. Having employees not following this can result in fine or bad press. To catch people doing this, traffic inspection can look at the related ports.

## Performance Considerations

### Terms: Latency, Response Time, and Jitter

Latency is the length of time delay between the packets SYN message and the sender replying with an associated AWK message. Response time is the time it takes to send and receive the entire series of packets that make up a single message. A jitter is variance in response times between two comparable messages.

### Impact of Data Rates across the Ecosystem

When a person on their laptop connects to a WLAN, connected to the LAN, to the router, to the aggregation switch, to the edge router, to the ISP, to the world – each hop will move data at different speeds. The response time will primarily be limited to the transmission speed of the slowest link.

If there is a lot of variance between the speeds of two points, additional systems can be put in place to improve the experience. An example might be a high speed aggregation switch which downloads, compresses and then streams the content. The latency has not decreased but the size has reducing the response time. Another option is to invest in higher bandwidth hardware.

### Options for Improved Availability

Hardware consists of electronic parts that mechanically move, and emit enough heat that they burn up without cooling solutions. It is not surprising that over enough time the device will fail. If the hardware doesn’t fail first the buggy software that drives the software will.

To improve availability monitoring solutions can be put in place to make sure all equipment is operating within an expected use scenarios. This will solve part of the problem the rest comes from the redundancy. Removing any single points of failure and providing mess networking can help address these concerns.

# Section III

Patton-Fuller is redesigning their network to include remote access via VPN to various staff members and WLAN support within the building. Now that the system has been designed and implemented, the next phase is to choose hardware and security solutions.

## Identify Hardware and Software to Protect the Network

The Hospital’s network will contain lots of Personally Identifiable Information (PII), which is a high value target for hackers and other attackers. To keep it safe and secure hardware and software solutions need to be added to the environment.

### Network Access Protection (NAP)

According to the Security Intelligence Report, it is becoming the norm for attackers to begin launching exploits within ten to thirty days of the patch being released (Microsoft, 2013, p. 5). Given the significant risk presented here, the first step would be to ensure a good patch management story is in place.

On solution is called Network Access Protection (NAP), which has a server component and a client side State Health Validator (SHV). After installation the clients will contact the DHCP server to get routing information. The DHCP server will reply with a challenge that various patches need to be installed or other business policy is being followed. The SHV will compute a response and give it back to the DHCP server (Microsoft, 2014).

If the response is valid, the device is given full access to the network. Otherwise the device is quarantined such that it can only communicate with the software updating and deployment infrastructure. After applying all the patches, the SHV will send another request for routing information and finally be allowed to join the rest of the network.

### Web Application Firewalls

Having a good patch management story prevents vulnerabilities that are publicly known and fixed. The next set of risk comes from known unknown vulnerabilities in the supporting systems of the Network Operating System (NOS). For instance there might be a SQL injection vulnerability in the website that no one has discovered yet.

To mitigate this risk Web Application Firewalls (WAF) can be installed at critical junction points throughout the network. As traffic flows through the WAF deep packet inspection is performed to find signs of malicious intent. If the traffic is classified as malicious it can be audited and dropped, before reaching the protected system (ex: web server) (Wikipedia, 2014).

### Virtual Local Area Networks

Another protection that can be applied is the deployment of Virtual Local Area Network (VLAN), which “providing a layer-2 network that is partitioned to create multiple distinct broadcast domains (Wikipedia, 2014).” This allows multiple networks to exist within the same physical network.

Once the network is partitioned it would be possible to define trust zones such as the web server can talk to the database server, but a person in radiology could not directly talk to the database server. Preventing unexpected traffic from being routable can significantly reduce attack space and increase the complexity of exploit.

## Distinguish Between Area Networks

There are a lot of achromous for area networks such as LAN, PAN, MAN, WAN, WLAN, etc. They each act more or less the same with the differences being seen in the scope of the network and the protocols used by them.

If the network is very small, such as around a single person; then it is a Personal Area Network. As the network gets larger it will encompass a handful of devices and become a Local Area Network. Growing out over an entire city is a Metropolitan Network. As the network spans multiple cities or long distances then it becomes a Wide Area Network.

## Building Blocks of a Network

### Hub

A hub is a simple device that accepts multiple connections and funnels them into a single upstream connection. The responses back from the upstream are then broadcasted to all ports. This enables scenarios such as easy auditing of network traffic or two computers sharing a single cable modem.

### Switch

Similar to hub is a switch which takes traffic from many locations and aggregate it for an upstream connection. This helps make traffic patterns more efficient and removes the need to have thousands of ports on our edge routers. Unlike a hub the responses are only sent to a specific port instead of a broadcast.

### Router

A router is a hardware device that takes data from one network and moves it to another network. For instance your edge router moves the traffic to the upstream ISP’s network. Another key feature of routers is they often implement firewalls and Network Address Translation (NAT) services. Both are useful to defense in depth strategies.

# Conclusions

When building a networking system care and thought needs to go into which communication protocols are being used and implemented. If this is not performed then sections of the network may have issues communicating with other legs.

The selection of the protocols falls into different levels and form the encapsulation model of the OSI system. In this design specific higher level protocols have been called out such as L2TP/IPSec along with some lower level such as OSFP and TCP.

Once the system has been implemented the next challenge is to implement traffic analysis so the health can be monitored and compliance reported. Along with the monitoring data is the need to validate the performance and make sure it is sufficient. If the performance or availability is not sufficient then compression proxies or other hardware can be installed.

Security is a real concern that needs to be handled across the network. This can be addressed by deploying hardware and software solutions such as Network Access Protection (NAP), Web Application Firewalls (WAF), and Virtual Local Area Network (VLAN) technologies.

In addition to selecting the proper security equipment it is also important to select the correctly network building blocks, such as routers and switches. Having the right tool for the job will make the network more efficient and easier to manage.

# References

Conklin, A., White, G., Williams, D., Davis, R., & Cothren, C. (2012). *Principles of Computer Security: CompTIA Security+™ and Beyond (Exam SY0-301), Third Edition.* McGraw-Hill Company.

Hernandez, S. (2012). *Official (ISC)² Guide to the CISSP CBK.*

Information Week. (2005, September 26). *Guide to Deploying VoIP*. Retrieved from Information Week: http://www.informationweek.com/guide-to-deploying-voip/d/d-id/1036414?page\_number=1

Marchewka, J. (2012). *Information Technology Project Management. Providing Measurable Organizational Value, Fourth Edition.* John Wiley & Sons Inc.

Morimoto, R. (2010). *Windows Server 2008 R2 Unleashed, 1e.* Pearson Education, Inc.

Soares, M., & Blank, A. (2014). *How to Setup Asterix@Home*. Retrieved from Mike Soares: http://www.mikesoares.com/guides/asterisk/

Conklin, A., & al, e. (2012). *Principles of Computer Security: CompTIA Security+™ and Beyond (Exam SY0-301), Third Edition.* McGraw-Hill Company.

Davis, D. (2008). *Mac OS X Authentication Case Study*. Retrieved from University of Utah : http://www.macos.utah.edu/documentation/authentication/mac\_os\_x\_authentication/mainColumnParagraphs/00/document/20030501-UofU\_Authentication.pdf

Goleniewski, L., & Jarrett, K. (2007). *Telecommunications Essentials. The Complete Global Source, Second Edition.* Pearson Education.

Microsoft. (2003). *Selecting a VPN Protocol*. Retrieved from TechNet: http://technet.microsoft.com/en-us/library/cc783910(v=WS.10).aspx

Microsoft. (2014). *Microsoft Kerberos*. Retrieved from MDSN: http://msdn.microsoft.com/en-us/library/windows/desktop/aa378747(v=vs.85).aspx

MIT. (2014). *MIT Kerberos Documetation.* Kerberos Consortium.

Parker, D. (2005, August 11). *Understanding UDP Protocol*. Retrieved from Windows Networking: http://www.windowsnetworking.com/articles-tutorials/network-protocols/Understanding-UDP-Protocol.html

Stalling, W. (2008). *Computer Security Principals and Practice.* Pearson Education.

Wikipedia. (2014). *Open Shortest Path First*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/OSPF

Microsoft. (2013). *SIR Volume 16*. Retrieved from http://download.microsoft.com/download/7/2/B/72B5DE91-04F4-42F4-A587-9D08C55E0734/Microsoft\_Security\_Intelligence\_Report\_Volume\_16\_English.pdf

Microsoft. (2014). *Network Access Protection*. Retrieved from MSDN: http://msdn.microsoft.com/en-us/library/windows/desktop/aa369712(v=vs.85).aspx

Wikipedia. (2014). *Application Firewall*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Application\_firewall

Wikipedia. (2014). *VLAN*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/VLAN