E-SCHOOL IMPLEMENTATION USING RADIUS SERVER AND AUTHENTICATION MECHANISM

Maria Seraphina Astriani[1]; Satrio Pradono[2]

[1]Computer Engineering Department, Faculty of Engineering, Binus University
Jl. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
[2]Computer Science Department, School of Computer Science, Binus International
Jl. Hang Lekir I No. 6, Kebayoran Baru, Jakarta 12120

ABSTRACT

Nowadays a lot of school would like to be a digital school or e-school. They may face lot of problems due to the sudden transition from conventional school to digitalized school. Some major problems are both lacks of human resources or man power and the basic knowledge about technology itself. Based on survey, the most common problem faced by most school is insecure wireless network. Even though they already installed advanced hardware, network security is still be the basic problem. No security mechanism such as encryption and authentication is the most common problem that may cause their network very vulnerable with any possible threat. After doing the research, Radius Server (both for authentication server and monitoring system) can help solve the problem.

***Keywords**: e-school, wireless, radius server, authentication*

ABSTRAK

Saat ini banyak sekolah ingin menjadi sekolah digital atau e-school. Mereka dapat menghadapi banyak masalah karena transisi yang secara tiba-tiba dari sekolah konvensional ke sekolah digital. Beberapa masalah utama adalah tidak memiliki sumber daya manusia atau tenaga dan pengetahuan dasar tentang teknologi itu sendiri. Berdasarkan survei, masalah paling umum yang dihadapi oleh sebagian besar sekolah adalah jaringan nirkabel yang tidak aman. Meskipun sudah memasang hardware yang canggih, keamanan jaringan masih menjadi masalah dasar. Tidak adanya mekanisme keamanan seperti enkripsi dan otentikasi adalah masalah yang paling umum yang dapat menyebabkan jaringan keamanan sangat rentan. Setelah melakukan penelitian, Server Radius (baik untuk server otentikasi dan sistem monitoring) dapat membantu memecahkan masalah tersebut.

***Kata kunci:** e-school, jaringan nirkabel, server radius, otentikasi*

INTRODUCTION

Today Information and Communication Technology (ICT) is used in almost all facets of society. As IT undergoes rapid changes, Rowley, Lujan, and Dolence (1997) pointed out that focused attention must be applied to stimulating innovations in pedagogy, research, and management through computer usage.

Education institution realized that IT has important roles for supporting the business. Implementing proper IT will increase their productivity, work effectiveness, and expense costs. They want their IT not a cost center, but become a business enabler in the company (Astriani, et al.,2010). Digital school or "e-school" can be focused to reach this goal. However, without a good methodology this transition process (a conventional school to a digitalize school) may face a lot of problems. Some major problems are both lacks of human resources or man power and the basic knowledge about technology itself. Based on survey, the most common problem faced by most school is insecure wireless network.

Z School comprises of Kindergarten, Primary School, Junior High School and Senior High School. They have several units or buildings, which are: Kindergarten Unit, Primary School Unit, Junior High School Units, Senior High School Unit, Institution Unit, and Multifunctional Unit. These Units use a combination of ADSL connection for internet connection and Fiber Optic for Local Area Network. Typically, the first floor of a Unit uses UTP cable and the 2nd and 3rd floor uses wireless LAN. Both connections are connected to the Fiber Optic switch, which go to the Institutional Unit and then are connected to the ADSL router.

There are some problems on their network structure such as unsecured WLAN connection (no authentication) and no connection monitoring. Unsecured WLAN connection (no authentication) may cause a condition where network does not need any authentication to connect and use the wireless connection. This means, everyone can connect to the internet without any more authentications. Furthermore, the administrator cannot control if any hacker get to the system and gain access to confidential files. Meanwhile, no connection monitoring can not allow the administrator to monitor any activities on the system. Without monitoring, administrator cannot know any details of the connection (who made the connection, starting time, ending time, connection duration, and IP address) made on the network/internet. Based on the research, Z School needs a guideline for using Radius Server and authentication mechanism to solve the network security problem.

METHOD

Here are several steps to implement the guideline for Radius Server and authentication mechanism (Figure 1).

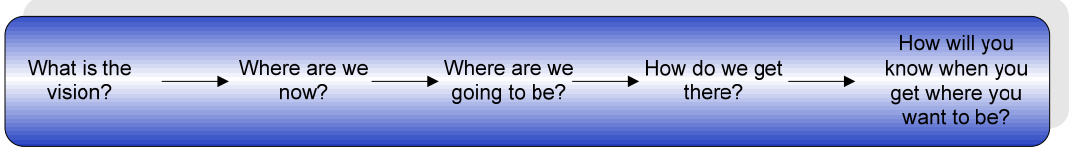


Figure 1. Methodology (Novell, 2007).

What is the Vision?

Before we jump to any solution and conclusion, we do need to define our vision. Our responsibility is to understand the current IT situation related with security. What kind of wireless security do we need? Is it the best wireless security that we can use in our school? Do we have any competent staffs? Those questions are to be asked when you want to define your wireless internet security vision (Astriani and Pradono, 2011).

Most school does not have decent wireless security system, because sometimes, they don't have any knowledge or expertise in that area. What most schools do are they are using a standard wireless security offered by any wireless devices.

Z school is one of the education institutions that has a goal to be a digitalize school. To achieve its goal, currently Z school already implements an advance networking peripherals, such as: fiber optic connection, ADSL connection, wireless connection, etc. Moreover, to improve the wireless networking security and enhance the monitoring system, Z school agreed to use Radius server based on EAP-TLS as an authentication mechanism. By implementing the Radius server, the wireless network in Z school will be secure (Bauer, 2005).

Where are We Now?

In this step, we need to analyze any threats to the network based on daily, weekly, or monthly network monitoring software to capture all the activities in the network. We also need to analyze their current network topology and make a conclusion based on it.

Mainly, the network topology of Z school network is using a Wireless, FO and ADSL and connection. The second and third floor computer is using wireless connection to the AP, the AP itself is connected using UTP cable to the FO switch in the first floor. The first floor computer is connected directly to the FO switch computer using UTP cable. From each unit, the FO switches connected to the Institutional Unit FO switch and then connected to the PC router. PC router itself connected to the ADSL router, to make Z school network can connect to the internet using ADSL internet connection. Z school has 36 AP installed, here are the details: Kindergarten Unit – 0 access point, Primary School Unit – 5 access points, Junior High School Units – 12 access points, Senior High School Unit – 15 access points, Institution Unit – 3 access points, and Multifunctional Unit – 1 access point. So, currently the network in Z school uses a combination of WLAN, FO, and ADSL connection. During this project, Z school is adding another internet connection, which is wireless internet connection. Now, FO switch in the Institutional Unit is connected to the router, and the router is connected to the wireless radio (Figure 2).

The network topology that Z school has is good enough for a big education institution. Z school just needs a clear direction to make it more secure, efficient, and effective. Generally, computer network in such big institution should have a great authentication mechanism, web server, and file server and mail server. After made a presentation and discussed with the people in Z school, their main priority is for securing the wireless LAN connection. After the discussion, they agreed to build a Radius server for the authentication for their wireless connection. Radius is the simplest and best ways for them to secure their wireless network.

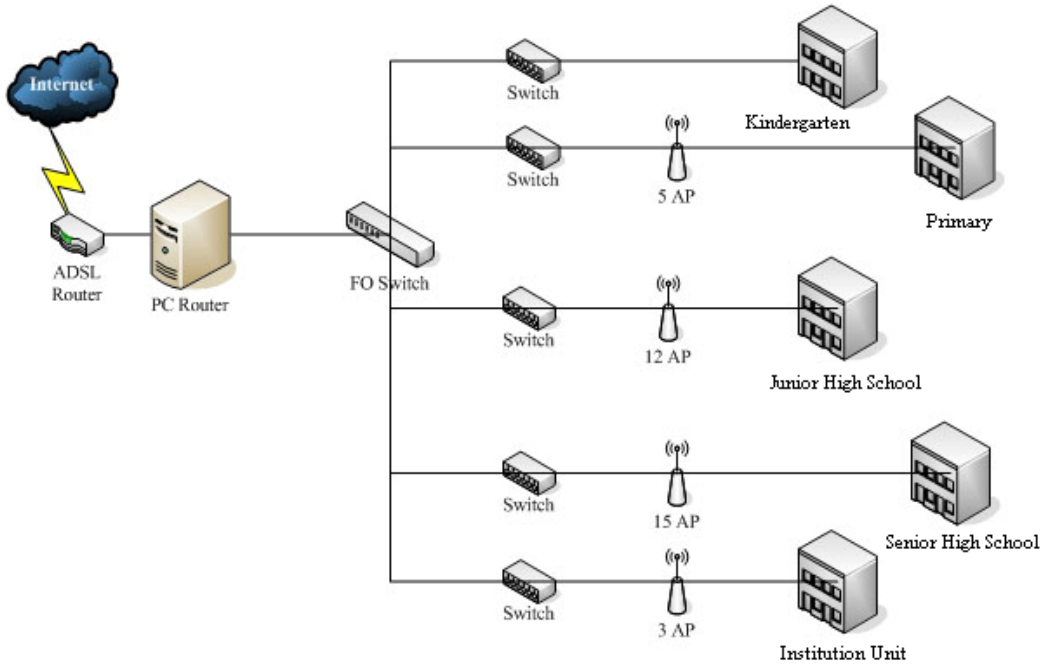


Figure 2. Current topology.

Where are We Going to be?

Implementing Radius server is the main goal. Radius server is an authentication server for a wireless connection. Radius server with EAP-TLS as an authentication mechanism is a server to authenticate valid user by comparing server's and client's digital certificates. Only users with a valid certificate authority (CA) can connect and use school's network (Bauer, 2005).

Radius server will also know when a session begins and ends. Therefore, every user activity can be monitored. The data might also be used for statistical purposes. One main advantage of Radius is its extensibility. Many Radius hardware and software user can configure their Radius to suit their need.

There are some factors why Radius Server is needed in Z school. First of all, security is the most important thing in any computer network, especially a big education institution like Z school. With this radius server, an authentication is needed to connect to the Z school network and use the internet services. Only a user who has certificate can login into Z school network. Second of all, monitoring the network is also important, with Radius Server; we can see how many users are connected to the network at the time.

How Do We Get There?

They need to build Radius Server, and distribute the CA created from the Radius server to all of their clients.

From Figure 4, the number of access points from each unit and the number of the unit is increased, becoming: Kindergarten Unit – 0 access point, Primary School Unit – 5 access points, Junior High School Units – 12 access points, Senior High School Unit – 15 access points, Institution Unit – 3 access points, and Multifunctional Unit – 1 access point.

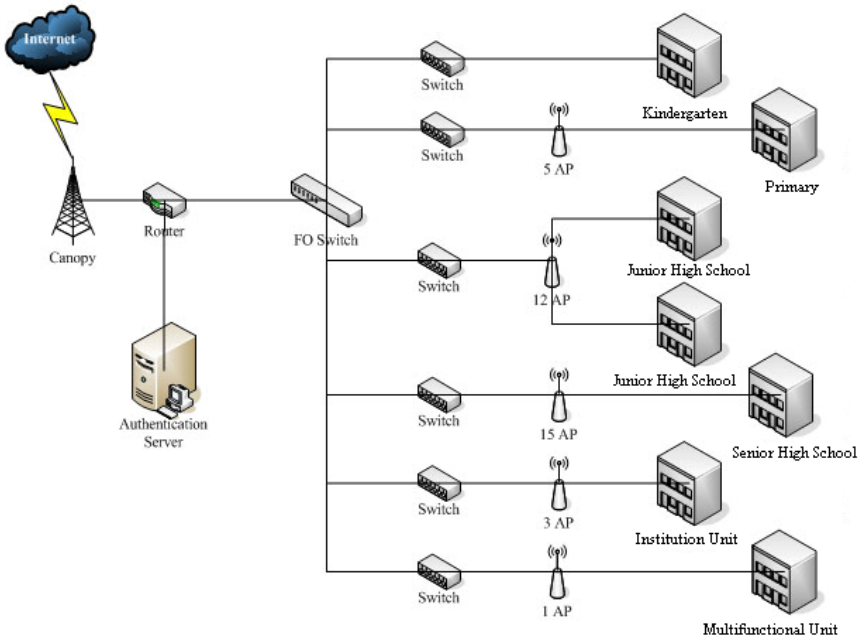


Figure 4. Future topology.

There 36 access points total, throughout the school. Z school wants to concentrates in wireless network security side, so the target are build an authentication server in the network for authentication and using data encryption, and client monitoring. It uses Radius Server for authentication and EAP-TLS as an authentication mechanism. With Radius Server, anyone who trying to connect to the network via access point are required digital certificate installed in their computer. The traffic in the Z school network will be more secure and can be monitored.

The EAP-TLS authentication process (Figure 5 and 6) is as follows: (1) client sends an EAP Start message to the access point; (2) access point replies with an EAP Request Identity message; (3) client sends NAI, which is username, to the access point in an EAP Response message; (4) access point forwards the NAI to the RADIUS server encapsulated in a RADIUS Access Request message; (5) radius server will respond to the client with its digital certificate; (6) client will validate the RADIUS server's digital certificate; (7) client will reply to the RADIUS server with its digital certificate; (8) radius server will validate the client's credentials against the client digital certificate; (9) client and radius server derive encryption keys; (10) radius server sends the access point a radius accept message, including client's WEP key, indicating successful authentication; (11) access point sends client an EAP Success message. The access point sends the broadcast key and key length to the client, encrypted with client's WEP key.

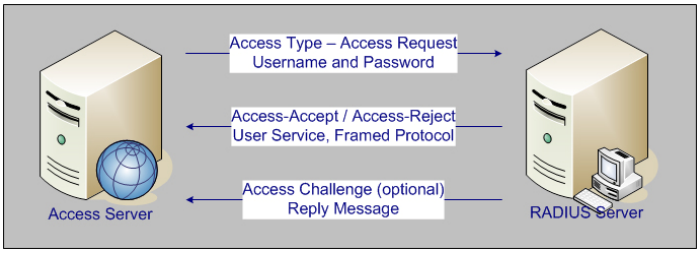


Figure 5. Radius authentication and authorization sequence.

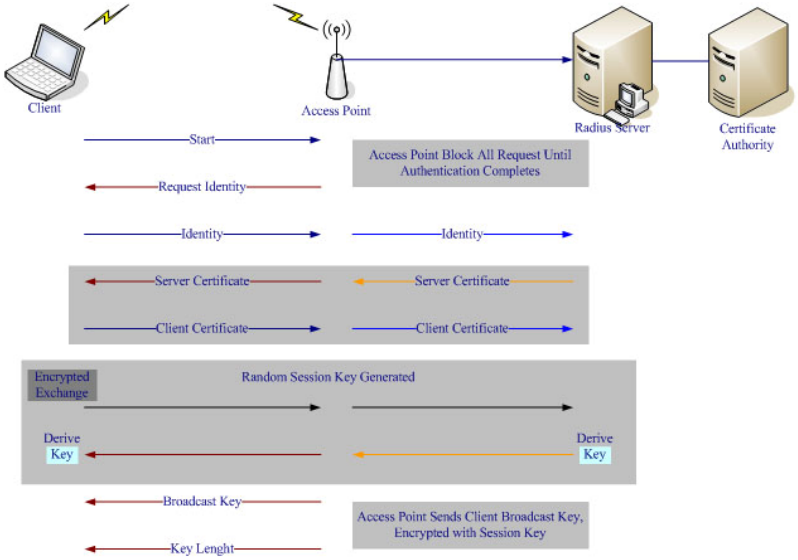


Figure 6. EAP TLS mechanism.

How Will You Know When You Get Where You Want to Be?

This step need a checklist about what should be done from this project, and that checklist should be their project monitoring tools.

RESULTS AND DISCUSSION

Graphic User Interface

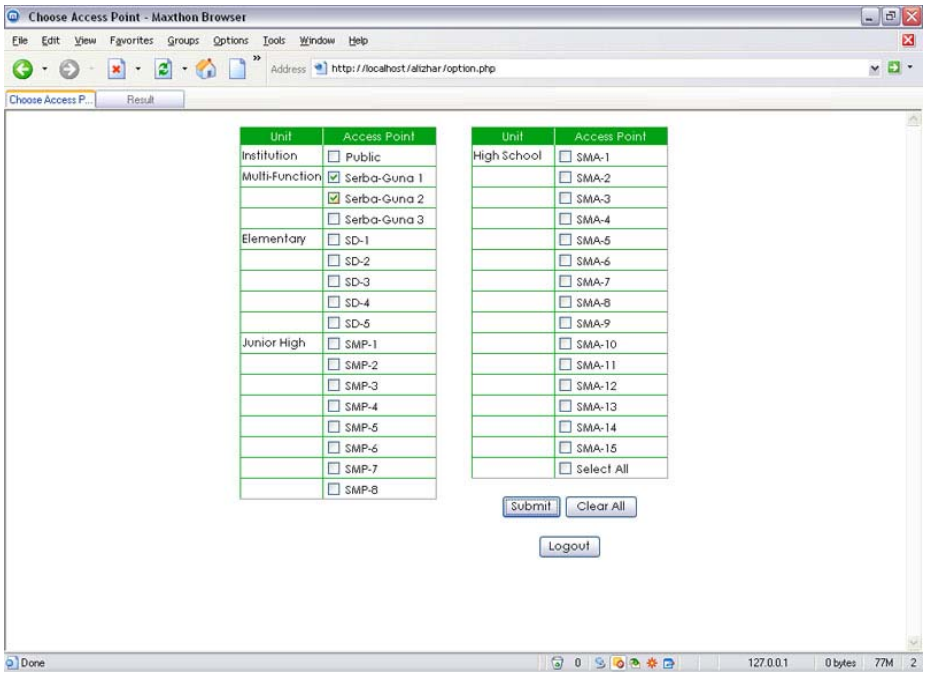
Figure 7 is the website interface for administrator to monitoring the wireless activity from Radius server. There are 6 pages for this monitoring site, they are Index page, Login Failed page, Option page, Result Error page, Result page, and Administrator page.

Certificate Validity

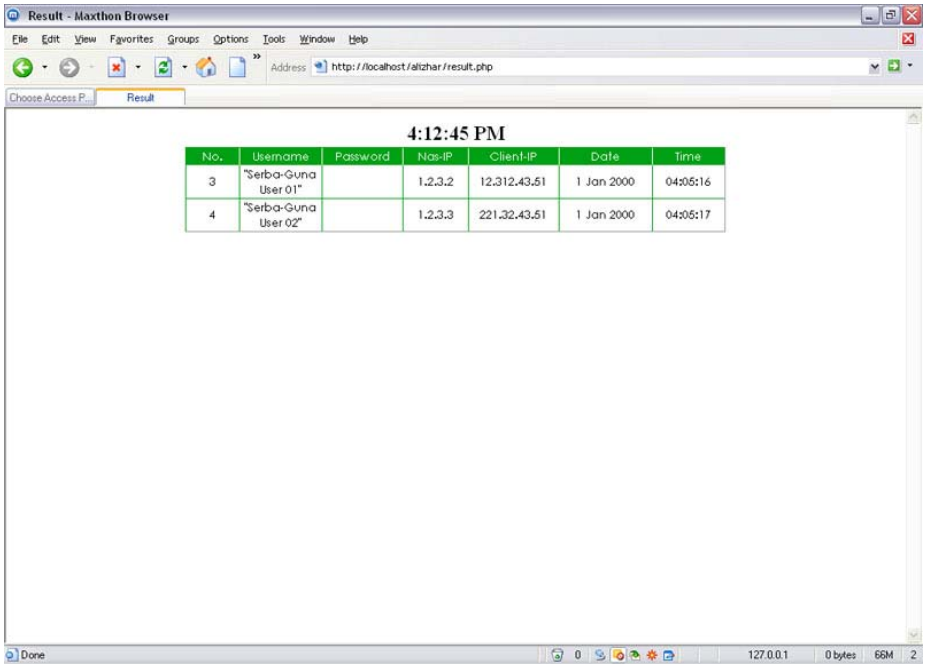
In order to connect to the Z school network, they have to have two valid school digital certificate to install to their computer, as follows:

Root Certificate

Root certificate (Figure 8) is Certificate Authority (CA), which is an entity trusted by every sides involved. The main purpose of CA is to issue a certificate for a user or a computer whose identity has been verified so that users and computers can depend on the authenticity of the certificate yielder identity. Digital certificates might contain data about the yielder's public key, expiration date, and digital signature of certification authority. CAs is used by SSl and PKI, which is a cryptographic security system which uses a public or private key to check and ensure the identity of user/organization. This is done in order to ensure a secure exchange of electronic messages over the World Wide Web.



(a)



(b)

Figure 7. (a) Select AP; (b) result.

Client Certificate

Client certificate (Figure 9) is use to authenticate user with the server. Without using this certificate, the server cannot authenticate the user, and it will appear an authentication failed message.

The server will authenticate user by checking this certificate, if this certificate is match with the server side, then the authentication is success.

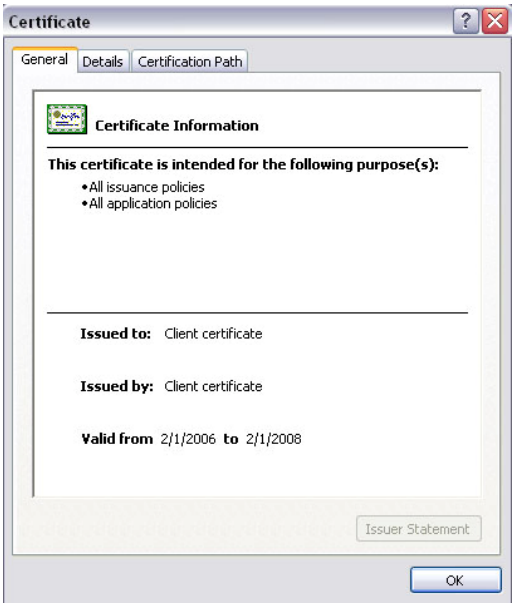


Figure 8. Root certificate.

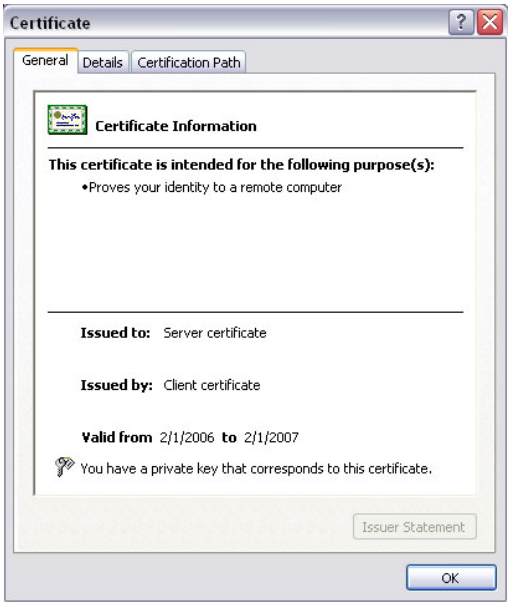


Figure 9. Client certificate.

Summary of Implementation

These are the summary after a few months of analysis and implementation:

Radius Server

The basic importance of Radius server is to increase security and for client authentication. The major improvement from the previous system to the new system is the authentication process. Now, only people who have the authentication can connect to school network. Moreover, it is required for all of the students and staff to give username and password to access the school network. It is an important issues to have an authentication server because Z school is a big education institution with five major buildings from kindergarten to senior high school and one thousands students.

Web Monitoring

The web monitoring that we also built is just a complementary advantage of using Radius server. Basically, by having Radius server installed on the network, Z school can simply do monitoring through the log file. However, since Z school is a large institution, it will be great to make the monitoring GUI-based. The idea is that we manipulate the raw data created by the radius server and get important data to be shown in a GUI-based format (Web application). It is quite important to have a GUI-based monitoring because it is a lot easier for the school administrator to use it. So they do not need to interact with the internal configuration.

CONCLUSION

Without any security method, school network is very vulnerable from hackers attack. Besides, anyone who is inside the wireless range can connect easily without any authentication. Radius server is an authentication server for a wireless connection. Radius server with EAP-TLS as an authentication mechanism is a server for authenticates a valid user with a digital certificate. Only a user with a valid Radius certificate can connect to school computer network and use the internet services. By using Radius server with authentication mechanism, wireless network will be more secure.

REFERENCE

Astriani, M. S., Pradono, S., Saragih, H. (2010). IT blueprint for education institution. *Second International Conference* of *Advances in Computing, Control and Telecommunication Technologies (ACT)*, Jakarta-Indonesia.

Astriani, M.S., Pradono, S. (2011). IT blueprint and school. *WSEAS International Conferences, Jakarta-Indonesia*.

Bauer, M. (2005). *Paranoid Penguin - Securing Your WLAN with WPA and FreeRADIUS, Part III*.

Novell. *A Blueprint for Better Management from the Desktop to the Data Center.* Novell: 2007.

Rowley, D. J., Lujan, H. D., & Dolence, M. G. (1997). *Strategic Change in Colleges and Universities. San Francisco.* CL: Jossey-Bass Publishers.