Vol.2013-IOT-22 No.5
2013/8/1

Enhancing Network Reliability by Establishing Redundant Network of Wi-Fi as Disaster Readiness in Soya Regions

BISHNU PRASAD GAUTAM†1†2 SURESH SHRESTHA†2
KATSUMI WASAKI†1

In this research, we conducted a medium scale trace-driven study of redundant networks by setting up a few wireless nodes at 4 distinct network locations, including the access link of Wakkanai City Office and of Wakkanai Hokusei Gakuen University networks of different sizes. This work was targeted to realize the importance of establishing redundant networks in the regional schools of Soya areas thereby providing a by-pass network during natural disasters. The issue of safeguarding networks during disasters is a very important issue. From the network management view point, this issue should be considered during network design phase. However, most of the organizations including schools are not giving much consideration to this issue and networks are highly vulnerable during disaster as these networks are at the risk of single point of failure due to the lack of back up network. In this paper, we are highlighting the importance of redundant network for the academic institutions. We emphasize that redundant networks established over Wi-Fi could be a better option during disaster period. We surveyed the potential of establishing tertiary network of Wi-Fi that can act as a redundant network during the disaster in Soya region of Hokkaido.

1. Introduction

Recent research suggests that Japan is facing the wrath of natural disasters with greater frequency and intensity which are not limited to earthquakes but also floods and storms too [1]. These natural disasters have obviously had great impact on damaging the national economy and the lives of communities thus getting a wider attention from the Government of Japan, humanitarian relief organizations and researchers all over the world and highlighted the need for enhancing the effectiveness of humanitarian relief management [2]. Specifically, after the nuclear disaster at the Fukushima Daiichi Nuclear Power Station, Government of Japan has caused broad concerns regarding energy issues among a broad segment of the public. The positive effect of this disaster lead to the requirement for demand-side management technologies which became a need, and without consuming much time the Japanese government accelerated its demand-side management and energy efficiency project timeline from 2020 to 2015. The issue of energy security and the ICT technologies required for sustainable energy supply has been the impetus for stable networks too. Recent research on Network has emphasized the importance of establishing stable network for business activities in many organizations including schools and Universities. Network is said to be stable and reliable if it satisfies the demand of communications during natural disaster with relatively a high probability. However, in order to establish the stable network, the importance of redundant network through alternative media was almost ignored in the schools and campuses. Most of the time, the network is established over same infrastructure such as fiber optics or over wired network. This paper presents a systematic review of potentiality of establishing redundant network between Wakkanai Hokusei Gakuen University and schools in Soya region with their innovative capacity. We find that the principal benefits of redundant networks as identified in the literature include: risk management; alternate route; back up of network thereby providing a backhaul network for obtaining access to external network. The experiment also illustrates that those schools which do not have alternate network limit their access and ultimately reduce their ability to enter into external network.

This research work identifies several gaps in the literature that need to be filled in. For instance, there is a need for further exploration of the relationship between back up networking and load balancing. Similarly, we need better understanding of back up networks, network configurations, as well as the role of Wi-Fi such as during natural disaster. Based on our experimental research, we present major findings on the benefits and fundamental design issues in redundant network. Some of our key findings are (1) A redundant physical network can be established by using Wi-Fi in a relatively low cost. (2) The backup energy required for tertiary network can be provided from renewable energy resources such as solar power.

(3) The location of AP (Access Point) and its positioning should be considered during design in order to improve the effectiveness of the post-disaster relief operations.

2. Motivations

2.1 Issues and Objectives

We witnessed that in many cases, existing network infrastructure is destroyed by the very nature of the disaster. Furthermore, Networks at times also can be destroyed due to data overloaded or saturated. This kind of disaster situation often addressed either by utilizing the approach of Mobile Ad hoc Networks (MANET) or by distributing antennas in the disaster area. Although re-establishing the networks in such

†1 Interdisciplinary Graduate School of Science and Technology, Shinshu University
†2 Wakkanai Hokusei Gakuen University

areas is possible, this may not be feasible in large-scale emergencies. Some authors [3] even suggest the use of a wireless opportunistic network based on mobile devices carried by emergency personnel to forward the data created and collected in the disaster area to a coordination point [3],[4], [6], [8]. These approaches are post disaster measures. In contrast our approach is pre-disaster measure and makes it more robust management by establishing redundant physical link through Wi-Fi. Though, Network failures in such situations can be identified relatively more easily, accurate prediction and location of network failures are still complicated and time consuming tasks. In the field of network trouble shootings, there are a number of tools and methods but still there requires further research which are not being saturated in terms of research in computer networks. If the communication infrastructure is improved a more reliable approach could be taken and this would also be a better asset management strategies. The objective of this research paper is to identify and augment the needs for communication at different levels in the distribution networks, the substation level, distributed source level, and end users level. However, our focus would mostly be in network level and identify the reliable solution measure for sustainable and reliable network. The geographical locations of schools in Soya regions are portrayed in figure 1. In the present scenario, we found that most of the schools networks are connected with a single link thereby creating the vulnerability of single point of failure. The major problem of this sort of network of relaying into single point of connection is certainly a high risk scenario for the organization.

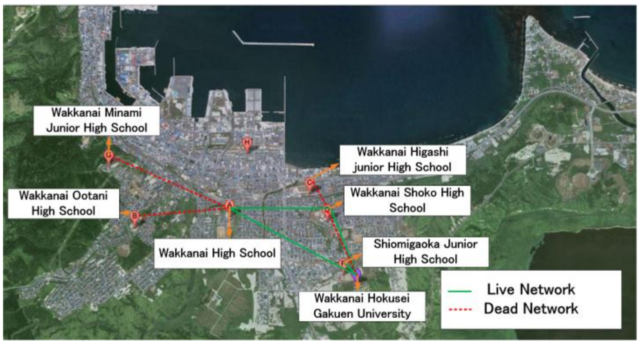

Figure 1: Geographical position of school at Wakkanai-Shi

2.2 Network Trouble during Disaster

Disasters are the situation at which the capacity of local residents exceed the response capabilities of a community and/or the organizations that exist within it. Risks to be considered include those from natural hazards, neighbors, building environment, political or social unrest and risks connected to IT and data security [2].

From the Fukushima nuclear disaster, we can imagine how difficult it is to protect the network during the disaster. The painful situation arises while there is no any alternative way to establish the network from the dead Network. One of the potential alternatives can be establishing Hastily Formed Networks (HFN). HFN are portable IP-based networks which are deployed in the immediate aftermath of a disaster when normal communications infrastructure has been degraded or destroyed [10]. However, HFN networks are also difficult to establish as such networks cannot be deployed without sufficient human resources. We know it is hard to find such human resources during disaster.

2.3 Importance of Redundancy

Generally, redundancy implies that a service should continue during the system failures thereby providing an additional system as a backup. Redundancy covers a wide area of systems , the major of which might include: Network Redundancy, Hardware Redundancy, Power Redundancy and Location Redundancy. In this paper, we explain about the network redundancy specially focusing in Network path redundancy and its importance. Not only the campus networks but any network that requires high availability or need to fulfill important operations gets benefit from network path redundancy. Network path redundancy is beneficial to support network components, such as outdated switches and cables, with alternate path for example if a switch or a cable break, a redundant system ensures continuity and avoids disruption of critical communication and data flow. Soya regional network that links Wakkanai Hokusei Gakuen University with city high schools, secondary and primary schools of Soya regions are all connected with fiber optics however, these networks are vulnerable with single point of failure if these networks are cut-off by wireless networks provided by Wakkanai Hokusei Gakuen University. In our research we found that most of these schools except few of them have no redundant path of network.

Without implementing redundant network topologies, the networks of these schools are unable to provide stable services to the users.

2.4 Common Weakness of Existing Networks

In order to build a network that can provide stable services during the disaster, it is necessary to think about the potential methodology by which the network can be designed with additional links. There were very few schools as shown in figure 3 which have tertiary links connected with Wakkanai Hokusei Gakuen University. However, the common weakness of regional schools in soya region is that their networks are not aware of the importance about it. Furthermore, it should be considered that the site priorities and location of key services contribute to a fault−tolerant design, with resilience built into the network infrastructure, and services and resources spread over a wide geography [5]. The common weakness of these regional networks of schools was that none of the schools have analyzed about the risk of single point of failure. Figure 2 shows the topological alignment of networks of these schools. The common weakness of their networks is listed as below:

- We could not see a proper network management system. There was no proper tool for configuration management, performance management, security management and traffic management.
- Lack of back up communication during disaster.
- Lack of data and network recovery strategy

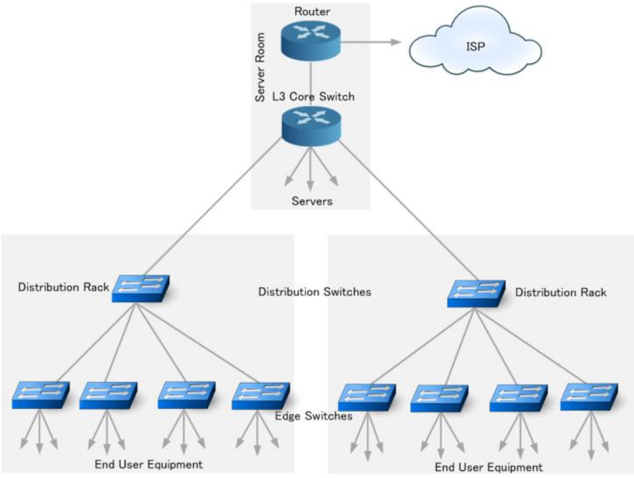

Figure 2: General Network Architecture of Schools at Soya Regions

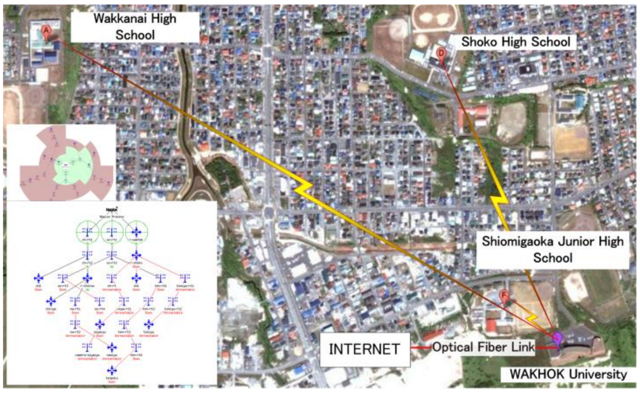

Figure 3: Active Links

Furthermore, from the fault-tolerance point of view, present configuration of school networks has number of weakness. Ideally, there should not be single point of failure; however, the present configuration has following situations.

- There is only one core switch that is connected with sub-core switches. If this should fail, most of the school network will be stopped.
- Only one outgoing route with ISP. If this connection should fail, all of the school network will out of internet services.

3. Proposed Community Disaster Ready Network

Our primary objective of this research is to provide some concrete guidelines while designing the networks that consider natural disasters. Furthermore, we want to minimize the effects of natural hazards on our networks in order to minimize the social, economic disruption caused by these extreme natural events. We want to keep hazards under our control from becoming disasters.

During the disaster, government of any region generally utilizes voice radio systems or broadcasting systems which are considered essential for disaster response. However, due to the disaster most of the wired networks viable to receive the damage and even if those networks are survived they cannot support the bandwidth and data management needs of a regional event where the goal of community involvement is attained. In such situation, the backup network constructed by wireless network can be a better alternative.

4. Technical Requirements and Recommended Considerations

4.1 Redundant Topology

Network redundancy is providing a backup network that try to eliminate network downtime caused by a single point of failure which can ultimately work like an insurance policy for industrial networks. Acting as a quick-response backup system, the goal of network redundancy is to mitigate the risk of unplanned outages and ensure continuity of operation by instantly responding to and reducing the effects of a point of failure anywhere along the critical data path [1]. Outage in Wakkanai city can occur not only during winter time, but also can happen during the natural disaster which might bring a great loss to the region. From our past experiences, Wakkanai city faces lots of unpredictable outage during winter seasons. Therefore, it is clear that making the investment in network redundancy is a smart strategy to achieve disaster bearable network.

We have designed the redundant link as shown in figure 4 at which we would like to propose the redundant link of media which can be connected by using Wi-Fi.

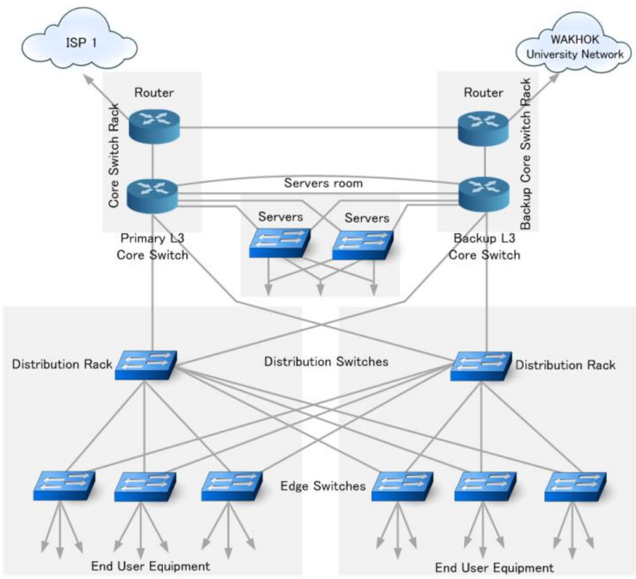

Figure 4: Model Diagram of Redundant Network

4.2 Consider Data Recovery

Disaster Recovery refers to the process of restoring data and communication links or business processes. Recovery from an emergency situation is always a complex task, particularly in mass casualty disasters [1], [2], [3]. In these scenarios, a quick and coordinated response is not possible without establishing a redundant network that could response during such situation. Recovery process must be given to improve the efficiency of rescue teams and save as many lives as possible. In network scenario this process includes the restoring of router, switches and other devices that are contributing to networks. After recovering the networks, restoring processes of data oriented servers can also be accessed locally or remotely. Among the activities comprised in the Disaster Recovery framework, Off-site Data Protection is the process of copying critical data to a physically remote site, where storage resources are available. Today, the most widely used solutions to backup data rely on the combination of two technologies: RAID [1] and Fiber Channel [2]. When a site crashes, we wish to minimize the number of server machines that have to be restarted on another network site to maintain and active the offered services. Indeed, to quickly reactivate the service, and to avoid excessive slowdown of running services, it is important to reduce the number of server machines that must be restarted at remote sites. Generally, the servers are deployed in a way that while there is power outage, the backup power system will provide the power instantly thereby avoiding the situation of restart. However, in some cases, these backup power systems cannot maintain the power for more than an hour. Such servers are restarted during the power outage and most of the time we experienced the file system problem and data losses.

4.3 Applying Redundancy Protocols

Applying redundancy protocols to provide redundant route is crucial while a master router loses its connection to the outside world. In order to provide stable connection to the LAN without affecting the services in the network, it is recommended to utilize redundancy protocols in a router. To address the situation when master router lost the connection with the outside world, redundant router that works as back up router should be deployed which can receive the packets sent by master router. Also, we can set the functionality by which interface of master router can be monitored so that while it lost the connection with outside world, backup router can take over the role of master thereby restoring connectivity with the outside world. Specially, in some cases we can set up two or more routers that can act as the gateway, and a dynamic routing protocol such as RIP or OSPF is used by hosts to determine the gateway router to use as the next hop in order to reach a specific IP destination. However, we do not apply dynamic routing in every situation. Static routing can be an option but if the statically configured router fails, the hosts on the LAN are unable to communicate with hosts with the outside world. To address such situation, we can use virtual router redundancy protocol widely known as VRRP. VRRP can stay at the top of different physical routers and can act as master router. Applying VRRP, we can provide stable network as the physical router can be well monitored and if any interface is down, VRRP can be utilized either to monitor interface or the port.

4.4 Network Path Redundancy through Alternative Media such as Wi-Fi

Wi-Fi known as wireless fidelity is one of the most popular wireless communication standards used today. It uses wireless (Electromagnetic waves) transmission medium in order to transmit information such as text audio videos pictures etc. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards", since most modern WLANs are based on these standards. We can utilize Wi-Fi in order to create the alternative path thereby providing redundant path of Network.

Network path redundancy that entails a backup path while the networks lost the route to outside world is an alternative way of providing stable network services. In order to provide redundant network path through alternate media, the good candidate can be wireless. In order to construct a completely redundant system, there is the requirement of redundant switches, redundant communication ports, and redundant device pairs. Complete redundancy can form an extremely reliable network that minimizes data loss stable network and has fast recovery time.

4.5 Redundant Power Supply

Though, power outages are inconvenient and expensive, especially in modern society, extensive electrical outages are still occurring in recent years and in developed cities including Soya regions. Power outages are disastrous and difficult to mitigate without very expensive backup power systems [8], [9].

Our past experience indicates that we should avail the redundant power supply for the routers, switches and servers too. Without having redundant power supply, it will impossible to provide stable network even if we have redundant network topology. Furthermore, unpredictable outage of power supply will hamper the hardware devices due to sudden fluctuations in voltage. Furthermore, the reason behind recommending a redundant power supply is that fault-tolerant power system is not possible without constructing such type of system. While considering power availability, we have to make sure that even if one of the paralleled supplies should fail, the system will continue to provide full power to its power bus [6],[7],[8].

Additional consideration should be put on that each supply must include a circuit that can automatically disconnect while the module of redundant power supply goes malfunction. Typically this automatic disconnect is accomplished by having Isolation (ORing) Diodes or MOSFETs placed in series with the output of each paralleled supply [8]. In the event one of the supplies develops a short circuit on its output or shuts down for any reason, the MOSFET switch must be turned off in order to prevent from high impedance state. In addition to having this automatic output "disconnect" feature, each supply must include a signal and visual indicator which can be used to alert the user or the monitoring external system that a specific redundant power supply has failed, so it can replaced and repaired in the future [8],[9].

5. Summary of a Field Experiment

Considering the importance of alternate path, we have surveyed whether it is possible to connect our backhaul router with Wi-Fi. Figure No. 5 and 8 portrayed the experimented scenario of Wi-Fi connection in the field.

Figure 5: Wi-Fi Experiment nearby Wakkanai Memorial Tower

First of all, we surveyed the existing networks and their coverage. As shown in figures 6 and 7 there were only few school networks which has active links between Wakkanai Hokusei Gakuen University and the regional schools. As shown in those figures, the green areas signify the active network coverage, whereas the red coverage signifies the dead networks. In order to re-identify the access points and network coverage, we began a new survey. The connection was tested through utilizing traditional way of locating the two ends. We used mirror on the both sides and reflect the sun light to identify the direction of the point to point connections required for two ends. Figure 5 at the right side with red rounded object is mirror by which we tried to reflect the sun light to notify our counterparts about our position so that he or she will recognize the direction of our location. After identifying the direction, we mounted the wireless device parallel to the direction of mirror reflection. In such experiments, it is important to decide the receiver and transmitter role of the radio device.

Accordingly, person carrying receiver can rotate or move the device in order to receive the signal from transmitter device. After doing few attempts, we were able to receive the signal from the wireless AP which was mounted in the University. After receiving the signal, we were able to establish the connection between University and “100 Year Memorial Tower” of Wakkanai.

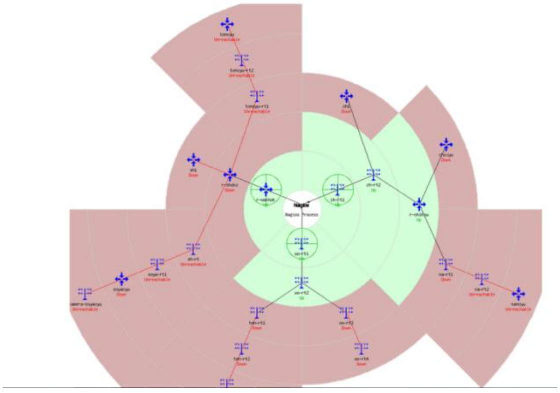

Figure 6: Active Network Coverage

Otherwise, it will be very hard to properly receive the signal from transmitter device. Our experiment suggests that this point can cover almost 80% of the areas of Wakkanai-city from which we can receive the Wi-Fi signal.

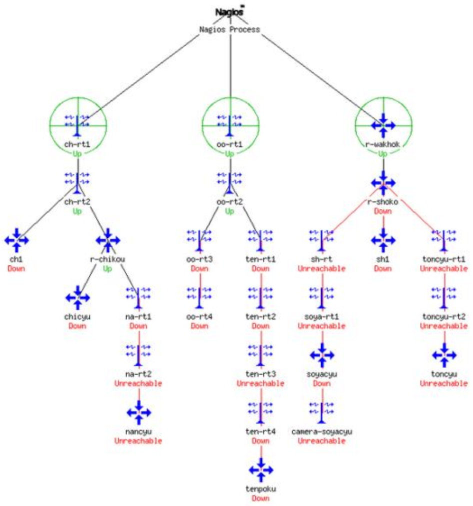

Figure 7: Active Network in Tree Structure

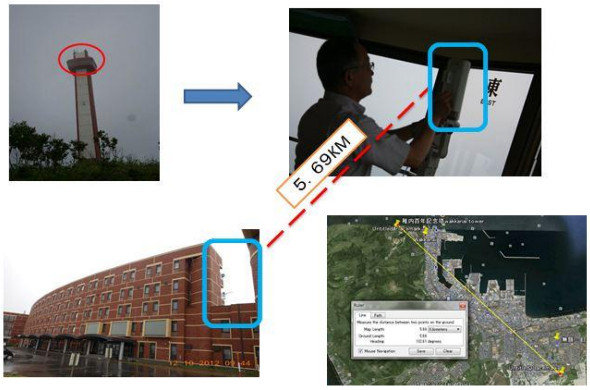

Figure 8: Link Surveys for Different Points

6. Future Works

In this research, we observed that most of the schools in soya regions are connected with single physical link. We found that there were only 2 schools at which the networks were connected with external link. One of which was connected with ISP and the other of which was connected with the link of Wakkanai Hokusei Gakuen University. Though, most of the links were connected with fiber optics and stable internet services are provided, these networks are vulnerable to network outage during natural disasters. In this survey, we were able to identify the vulnerabilities of network outage; however, we are unable to implement the tertiary link for the local schools. This situation arises due to the limitation of our research scope. We were tasked to do the survey and identify line of sight (LOS) spots. Our future work will include implementation of redundant link. We will definitely consider the deployment of wireless technology as tertiary network link for the points which are vulnerable with single point of failures. However, in order to implement the tertiary link, we will require the funding support either from local government or from the Ministry.

7. Conclusions

We believe that it is highly crucial to construct a disaster response or disaster ready networks in order to save communities from unexpected damage. Generally, disaster response networks are connected with sensor networks that could potentially detect the events that can onset and warn possibly affected individuals to find shelter, as well as aid first responders through increased situational awareness [3]. However, network failures can severely hamper these networks' ability to gather useful information in a timely manner, especially important for those aimed at monitoring fast-moving destructive physical phenomena such as earthquakes and floods. Such events often result in large scale geographically correlated failures in addition to serious network congestion as individuals contact each other or request help, exacerbating failures or tying up channels entirely. This research document provides topology design guidance for implementing a redundant network in the Soya regions. This topology however can be applied while designing redundant network of any institutions thereby providing the redundant access. In our research we surveyed that most of the schools can get the backhaul link from Wakkanai Hokusei Gakuen University. It is an accompaniment to the hierarchical and redundant network design guides, designing a redundant Network is also for a high availability and reliability even in the case of disaster. Our consideration of Network reliability implies in terms of its connectivity through non-failed links. Thus, our focus is to provide network services during disaster time considering several risk measures and design a post-disaster reliable system under the assumption that link failures are independent. We have highlighted the issues to the high priority level that the network is vulnerable not only in the sudden outage during winter seasons but also during other potential natural disaster. Trouble scenarios, based on similar incidents in the computer networks at the Universities and other areas such as Fukushima are presented to describe how the disaster may unfold and show the negative consequences to organizational computer networks. Fortunately, there are many potential alternatives and techniques, with a wide range of pricing and complexity of troubleshooting tools, and practices that can help safeguard the networks. We have presented some considerations that should be given while constructing stable networks.

Furthermore, with regard to disaster preparedness of Soya regions, we recommend providing school teachers with disaster education and school network disaster mitigation plans. It should aim to enhance readiness and act during natural disaster as according to the proposed emergency operation plan. Proper network management plan during natural disaster is required as natural disasters such as earthquakes often occurs without warning.

References

1. Japan Disaster Statistics, URL: http://www.preventionweb.net/english/countries/statistics/?cid=87 Date Accessed: 2013/06/11
2. Xing Hong, Miguel A. Lejeune, Stochastic Network Design for Disaster Preparedness, URL: http://www.optimization-online.org/DB_FILE/2012/12/3705.pdf Date Accessed: 2013/06/11
3. Abraham Martın-Campilloa, Jon Crowcroft, et.all, Evaluating opportunistic networks in disaster scenarios, URL: http://www.cl.cam.ac.uk/~ey204/pubs/2012_JNCA.pdf Accessed Date: 2013/6/15
4. Disaster Preparedness and Recovery Plan, URL: http://www.cof.org/files/Documents/Community_Foundations/DisasterPlan/DisasterPlan.pdf, Date Accessed: 2013/01/27
5. Catherine Blackadar Nelson, The Evolution of Hastily Formed Networks for Disaster Response, URL: http://www.cisco.com/web/about/doing_business/business_continuity/Paper_124_MSW_USltr_format.pdf , Date Accessed: 2013/01/22
6. Jim Geier, Desiginging and Deployeing 802.11n Wireless Networks, Cisco Press
7. Cisco − Disaster Recovery: Best Practices White Paper, URL: http://www.williamsdatamanagement.com/pdfs/Cisco%20Disaster%20Recovery%20PDF.pdf
8. Mel Berman, Eliminate System Downtime with Redundant Power Supplies URL: http://www.newark.com/pdfs/techarticles/lambda/ESDRPS.pdf, Date Accessed: 2013/01/26
9. John Kruckenberg, Andrew Lippolis et.all, Prioritized Backup Power System URL: http://www.ti.com/corp/docs/landing/universityprogram/09_winners/Ohio_State_Kruckenburg.pdf, Accessed Date: 2013/4/15
10. Robert J. Shimonski , *The Importance of Network Redundancy* URL: http://www.windowsnetworking.com/articles-tutorials/netgeneral/Importance-Network-Redundancy.html, Date Accessed: 2013/01/26

Acknowledgments We would like to thanks to the entire staff of Wakkanai Hokusei Gakuen University, who helped us during our experiments. Special thanks go to Mr. Shitosi Hata who helped us while testing the tertiary link of Wi-Fi at different line of sights in Wakkanai.