Safeguarding Regional Network from Potential Natural Disaster by Establishing Redundant Network of Wi-Fi

Bishnu Prasad Gautam and Mr. Suresh Shrestha

●要約

災害時にネットワークを保護することは非常に重要な課題である。ネットワーク管理の観点から、この問題は、ネットワークの設計段階で考慮されるべきである。これらのネットワークのほとんどが、バックアップネットワークがないため、シングルポイントフェーラーの危険にさらされている。しかし、高等学校などの教育機関のほとんどがこの問題に考察していないため、そういった組織のネットワークが災害時に脆弱なネットワークであることは明らかである。本稿では、学術機関における冗長ネットワークの重要性を強調している。我々は、Wi-Fi 経由で確立された冗長ネットワークが災害期間にも対応可能なより良いバックアップネットワークとして利用できることを強調している。私たちは北海道の宗谷地域に対して、災害時に利用できる Wi-F を三次ネットワークとして確立する可能性を調査した。

●キーワード

Redundant Network
Redundant Topology
Hastily Formed Network

1. Introduction

Recent research on Network has emphasized the importance of establishing stable network for business activities in any organization including schools and Universities. 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. Until recently, though the indoor wireless networks are well utilized, insights into the potential of redundant network for their backhaul connection through the same have been over-looked. This paper presents a systematic review of potentiality of establishing redundant network between WAKHOK University and schools in Soya region with their innovative capacity. We found that the principal benefits of redundant networks as identified in the literature include: risk management, alternate route, back up of network thereby providing a backhaulnetwork 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 theirability to enter into external network.

Where networks fail, it is due to their lack of backup network, external disruption and lack of infrastructure. This research work identifies several gaps in the literature that need to be filled. For instance, there is a need for further exploration of the relationship between back up networking. Similarly, we need better understanding of back up networks, and network configurations, as well as the role of Wi-Fi such as during natural disaster.Our study highlights the need for interdisciplinary research in these areas.

2. Problem Identification

Though the network failures 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 numbers 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 motivation for this paper is to identify the needs for communication at different levels in the distribution networks, the substation level, distributed source level, and end user slevel. However, our focus would mostly be in network level and identify the reliable solution measure for sustainable and reliable network. In the present scenario of school networks of Soya region, 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.

3. Potential Trouble Scenarios 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 [3]. 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.

4. Importance of Redundancy

Not only the campus networks but any network that requires high availability or need to fulfill important operations get 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 WAKHOK. 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.

5. Common Weaknesses

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. However, the common weakness of regional schools in soya region is that they 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 servicesand resources spread over a wide geography[5]. The common weakness of these regional networks of schools was that none of the schools have analyzed the Single Point of Failure. Furthermore, there was common weakness which is listed as below:

- We could not see a network management system. There was no any 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

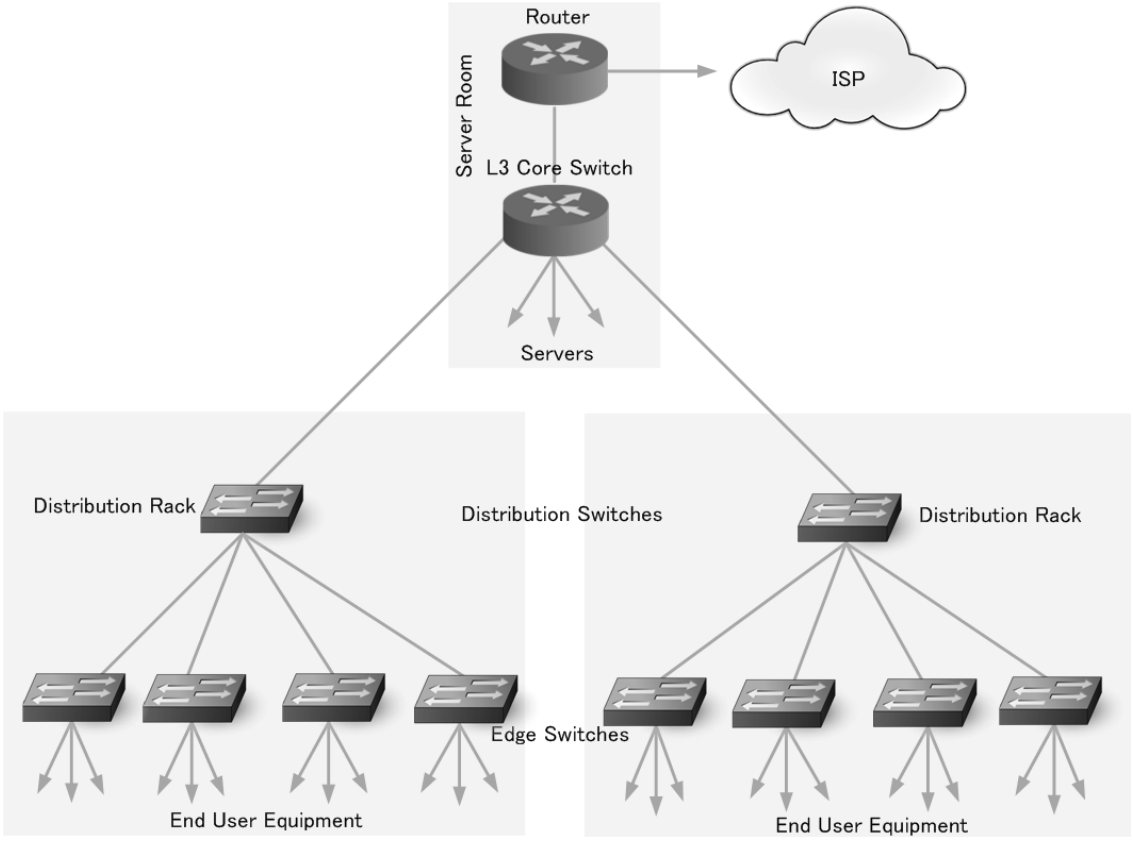

Figure 1: General Network Architecture of Schools at Soya Regions

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 not work.
- Only one outgoing route with ISP. If this connection should fail, all of the school network will out of internet services.

6. Proposed Community Disaster Resistance Network

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.

7. Technical Approach

7.1 Consider 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 has 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. As described in figure 1, the overall network architecture of schools in soya regions is connected with single link. Though the link at most of the time is connected by fiber optics, this network has no alternate link physically.

We have designed the redundant link as shown in figure 2 at which we would like to propose the redundant link of media which can be connected by using Wi-Fi.

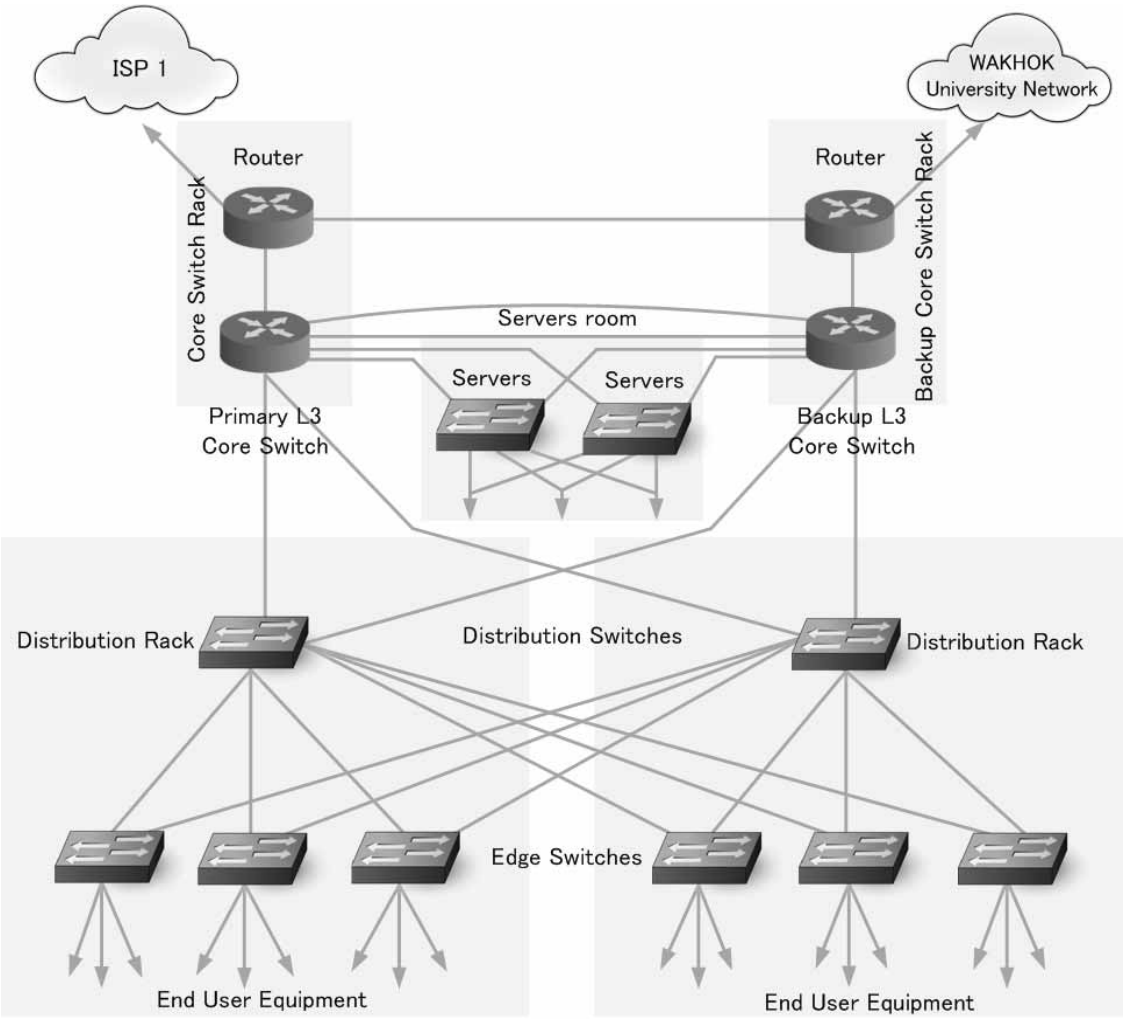

Figure 2: Model Diagram of Redundant Network

7.2 Consider Data Recovery

Disaster recovery refers to the process of restoring data and communication links or business processes. 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 loses.

7.3 Consider 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 takeover the role of master thereby restoring connectivity with the outsideworld. 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.

7.4 Consider 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 fastrecovery time.

7.5 Consider Redundant Power Supply

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.

8. Experiment and Demonstration

Considering the importance of alternate path, we have surveyed whether it is possible to connect our backhaul router with Wi-Fi. Figure No. 3 and 4 portrayed the experimented scenario of Wi-Fi connection in the field.

Figure 3: Wi-Fi Experiment nearby Wakkanai Memorial Tower

First of all, the connection was tested through utilizing traditional way. We used mirror on the both sides and reflect the sun light to identify the direction of the point to point connections. Figure 3 at the right side with red rounded object is mirror by which we tried to reflect the sun light to notify our counterparts so that he or she will recognize the direction of our location. After identifying the direction, we mounted the wireless device parallelly to the direction of mirror reflection. 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 Nen Memorial Tower ”of Wakkanai. Our experiment suggest that this point can cover almost 80% of the areas of Wakkanai-city from which we can receive the Wi-Fi signal.

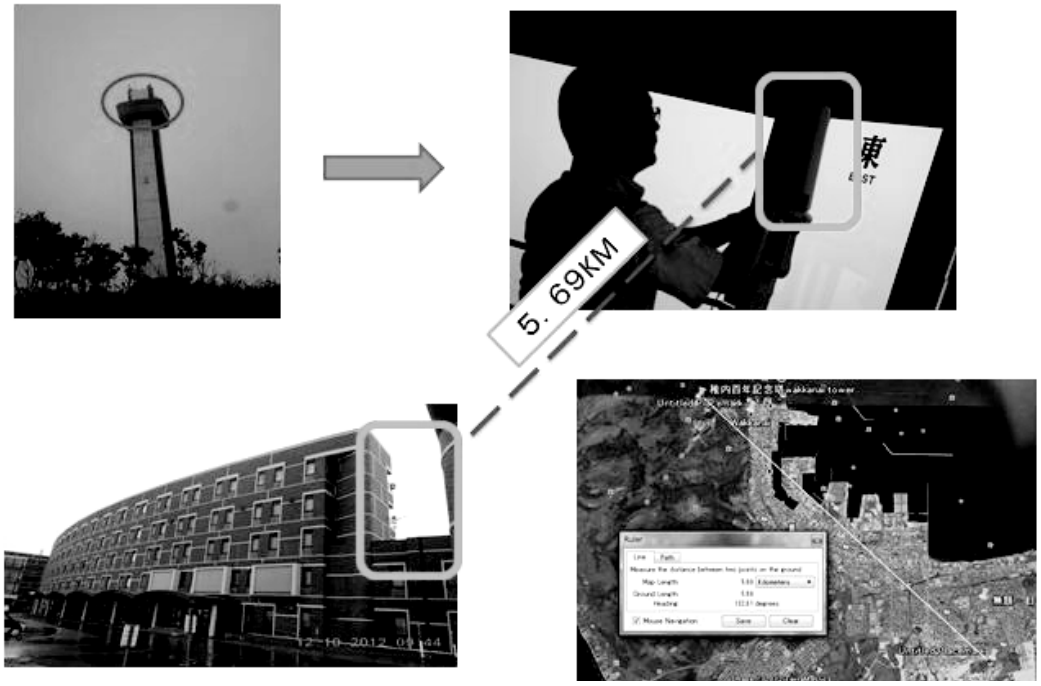

Figure 4: Connection Established Between Different Points

9. Future Works

In this research, we observed that most of the schools in soya regions are connected with single links. Most of the links were connected with fiber optics and stable internet services are provided, however, these networks are vulnerable of 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 the 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.

10. Conclusions

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 trouble shooting tools, and practices that can help safeguard the networks. We have presented some considerations that should be given while constructing the stable networks. Computer networks in any university or schools can utilize the lessons learned by the computer networks and telecommunications industries and safeguard the networks before the safety and reliability of the computer networks are compromised.

● References

1．Robert J. Shimonski, *The Importance of Network Redundancy* http://www.windowsnetworking.com/articles-tutorials/netgeneral/Importance-Network-Redundancy.html, Date Accessed: 2013/01/26

2．Disaster Preparedness and Recovery Plan, URL: http://www.cof.org/files/Documents/Community_Foundations/DisasterPlan/DisasterPlan.pdf, Date Accessed: 2013/01/27

3．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

4．Jim Geier, Desiginging and Deployeing 802.11n Wireless Networks, Cisco Press

5．Cisco － Disaster Recovery: Best Practices White Paper, URL: http://www.williamsdatamanagement.com/pdfs/Cisco%20Disaster%20Recovery%20PDF.pdf

● Abstract

The issue of safeguarding networks during disaster is very important issues. From the network management view point, this issue should be considered during network design phases. 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.