Experimentation of Emergency Detour Route to Enhance Unstable Networks in Wakkanai, Hokkaido

BISHNU PRASAD GAUTAM[1,†2,a)] KATSUMI WASAKI[2,b)] DAMBAR PUN[2 c)]

Computer Networks often disrupted by number of reasons. The most powerful disruption might occur during natural disasters. For example, we witnessed that many wired networks and servers of the telecommunication companies were disrupted and damaged by the tsunami in Japan. Therefore, it is very essential that Networks must be safeguarded against disasters. In this study, we surveyed the potential for establishing redundant Wi-Fi networks in schools in the Soya region of Hokkaido, to proactively create a bypass network that can be used if a natural disaster occurs. During emergency situations such as earthquakes, tsunamis, and floods, traditional disaster response may not be able to provide adequate communication services to emergency-management teams. We design a model network consisting wired and wireless links and conducted a simulation. Accordingly, we conducted a medium-scale trace-driven study of redundant networks to determine how to decrease disaster risk. We set up wireless nodes at four network locations of different sizes, including the access link between the Wakkanai city office and Wakkanai Hokusei Gakuen University networks. By proactively establishing a redundant wireless network as a detour emergency route using our approach, an organization can reduce disaster risk without consuming much time during disasters.

1. Introduction

Disaster risk reduction (DRR) is a strategic approach to reducing the risk of hazards and panic in a society during disasters, both natural and man-made. DRR aims to identify, assess, and reduce the risks of disaster, as well as reduce socioeconomic vulnerabilities to disaster. DRR should not be performed in isolation. Rather, it should be an integral part of disaster response, such that the government, private-public organizations, and other stakeholders can coordinate their response. DRR is a much broader and deeper approach than conventional risk management.

Research suggests that natural disasters have recently assailed Japan with greater frequency and intensity than in the past. Such natural disasters include not only earthquakes, but also floods and storms [1]. These disasters have harmed the national economy and the lives of people living in affected communities and have drawn the attention of the Japanese government, of humanitarian relief organizations, and of researchers all over the world. The disasters highlight the need to improve humanitarian relief management [2]. Specifically, after the nuclear disaster at the Fukushima Daiichi Nuclear Power Station, the Japanese government has expressed concern regarding energy issues affecting a broad segment of the public. The government also responded quickly by accelerating its demand-side management and energy-efficiency project timeline from 2020 to 2015.

Information and communication technology is also being explored as a way to make energy supply more sustainable and networks more stable. Recent research on networks has emphasized the importance of network stability for business activities in organizations such as schools and universities. Note also that over time, changes can affect both the vulnerability of a computer network and the type, causes, nature, and intensity of the hazards that it faces. Redundant Wi-Fi networks are a good option if a disaster occurs for the geographic location such as in Wakkanai. For example, in an emergency situation, community expect faster response from the rescue management team. In order to pursue faster response, emergency communication systems cannot take hours to deploy. Rapid and easy deployment of communication system is the key point during disaster. Our study investigates the establishment of backup links in order to provide a network that can be re-established during disasters as an emergency detour route more rapidly and easily.

1.1 Methodological Background

Researchers often use modeling and simulation techniques to verify their research data. However, modeling a proactive DRR approach using emergency network routes presented a number of difficult methodological problems. The social and political parameters required for DRR simulation are very difficult to simulate, the simulation process is difficult to represent and trace, there is no standard simulation model, and current literature about DRR for computer networks does not include a sufficiently iterative process for formulating the problem. Therefore, simulation alone is unlikely comply with strategic scientific guidelines or yield sufficiently rigorous results.

Because simulation data would be unreliable, we conducted an experiment to test our strategy in the field directly on real networks, as the part of a trace-driven approach. We first conducted a preliminary survey of the site. Then we tested the links between nodes and identified vulnerable sites. Based on the test, we proposed redundant networks that would maintain the survivability of the network during natural disasters. On the basis of our proposed design, we did a simulation experiment. We began the survey after performing two types of analysis:

1. Vulnerability and survivability analysis
2. Risk-reduction analysis

These two types of analysis allowed us to assess overall risk for different networks by identifying the single points of failure that are most likely to fail in a natural disaster and which of those single points of failure will most affect network assets and the survival of communication.

1 Interdisciplinary Graduate School of Science and Technology, Shinshu University.
2 Wakkanai Hokusei Gakuen University.
a) bishnu35@gamail.com, gautam@wakhok.ac.jp
b) wasaki@cs.shinshu-u.ac.jp
c) dambarmail@gmail.com

1.2 Experimental Strategy and Discussion

A network is said to be stable and reliable if it satisfies the demands of communications not only in normal situations but also in the majority of natural disasters. However, the importance of a redundant network that uses alternative media for a stable network has largely been ignored in schools and on campuses. At our research site, the network is generally maintained over a single infrastructure, such as a fiber-optic or wired network. This paper systematically reviews the potential for establishing a redundant network between Wakkanai Hokusei Gakuen University and schools in the Soya region. The principal benefits of redundant networks, as identified in networking literature, include risk management, alternate routes, and the ability to back up a network in order to provide a backhaul network for obtaining access to an external network. In our experiment, we found that schools without alternate networks had limited access, which ultimately reduced their ability to enter into external networks.

This research identifies several gaps in the literature that need to be filled. For instance, the relationship between backup networking and load balancing must be explored further. Similarly, we need more research on backup networks, network configurations, and the role of Wi-Fi during natural disasters. Based on our experimental research, we present major findings of the benefits and fundamental design issues in redundant networks. Some of our key findings are as follows:

1. A redundant physical network can be established using Wi-Fi at a relatively low cost.
2. The backup energy required for a tertiary network can be provided from renewable energy resources, such as solar or wind power in Soya regions.
3. Access points should be carefully positioned during network design, in order to improve the effectiveness of post-disaster relief operations.
4. The Soya region is an appropriate area for deploying Wi-Fi networks as an emergency detour route during a disaster.

2. Motivation

2.1 Issues and Objectives

Disasters, by their very nature, destroy existing network infrastructure. Disasters can also lead to data overloading and saturation, which also destroy networks. The use of mobile ad hoc networks and the distribution of antennas in disaster areas

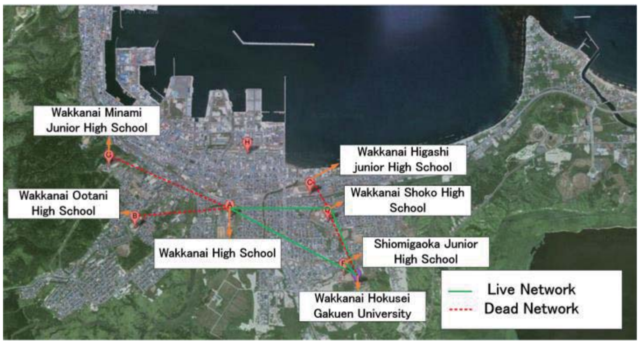

Fig 1: Geographical Location of Schools in Wakkanai Region

can often address these problems. Although networks can be re-established in disaster areas, doing so 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 disaster areas to coordination points [3],[4],[5].

These approaches are all post-disaster measures. In contrast, our approach is a pre-disaster measure that provides more robust management by establishing redundant physical links using Wi-Fi technology. The use of a redundant Wi-Fi network can make network failures easier to identify, but accurate prediction and location of network failures is still a complicated and time-consuming tasks. There are a number of network troubleshooting tools and methods, but they require further research. Better communication infrastructure design can make infrastructure more reliable, reduce the time and money required to manage it, and improve the strategy for managing it. The objective of this research is to identify the need for communication at the distribution-network level, the substation level, the distributed-source level, and the end-user level, and suggest steps to improve communication at these levels. However, we mostly work at the network level to measure the reliability and sustainability of network solutions. Fig. 1 shows the geographical locations of schools in the Soya region. Most schools networks are connected by single links, making them vulnerable at these single points of failure. Network Problems during Disaster

In a disaster, the needs of local residents exceed the response capabilities of the community and community organizations. Risks to be considered include those from natural hazards, neighbors, building environments, political and social unrest, and risks connected with IT and data security [2], [3].

The Fukushima nuclear disaster graphically illustrates the difficulty of protecting the network during a disaster. There may be no alternative way to re-establish a network after it goes down in a disaster. One potential solution is to establish a hastily formed network (HFN). An HFN is a portable IP-based network that is deployed in the immediate aftermath of a disaster, when normal communications infrastructure has been degraded or destroyed [6],[7],[8],[9],[10]. However, significant human resources are required to deploy an HFN, and those can be difficult to find during disasters.

2.2 Importance of Redundancy

Generally, redundancy implies the existence of a backup system that allows service to continue after a main system fails. Redundancy can be provided for systems such as networks, hardware systems, power systems, and locations. In this paper, we describe network redundancy, particularly network-path redundancy, and its importance. Not only campus networks, but any network that requires high availability and survivability or needs to fulfill important operations can benefit from network-path redundancy. Network-path redundancy can provide alternative paths for networks with outdated switches and cables. If a switch or cable breaks, or if an outdated network device is no longer able to provide services, a redundant system ensures continuity and avoids disruption of critical communication and data flow. The Soya regional network that links Wakkanai Hokusei Gakuen University with city high schools, secondary schools, and primary schools in the Soya region are all connected with fiber optics. However, these networks have single points of failure if they are cut off from the wireless networks provided by Wakkanai Hokusei Gakuen University. In our research, we found that most of these schools have no redundant network path.

Unless these schools implement redundant network topologies, they will be unable to provide stable services to users.

2.3 Problem Analysis of Existing Networks

In order to build a network that can provide stable services during disasters, one must include redundant links in the design methodology. As Fig. 2 and Fig. 3 demonstrate, very few schools have tertiary links to Wakkanai Hokusei Gakuen University. The common weakness of regional schools in the Soya region is that their networks have been built without consideration for the importance of redundancy. Site priorities and the location of key services contribute to fault-tolerant design, in which resilience is built into the network infrastructure and services and resources spread over a wide geographical area [5]. The common weakness of these regional school networks is that none of the schools has analyzed the risk posed by single points of failure. Fig. 2 shows the most common network topology at the schools. The weaknesses of the topology are as follows:

It does not have a proper network-management system—there is no proper tool for configuration management, performance management, security management, and traffic management.

The topology lacks backup communication that can be used during a disaster.

The topology lacks a data and network recovery strategy.

Furthermore, from a fault-tolerance point of view, the present configuration of the school networks has a number of weaknesses. Ideally, there should be no single point of failure; however, the common topology has two single points of failure:

One core switch connects all sub-core switches. If the core switch fails, most of the school network will fail with it.

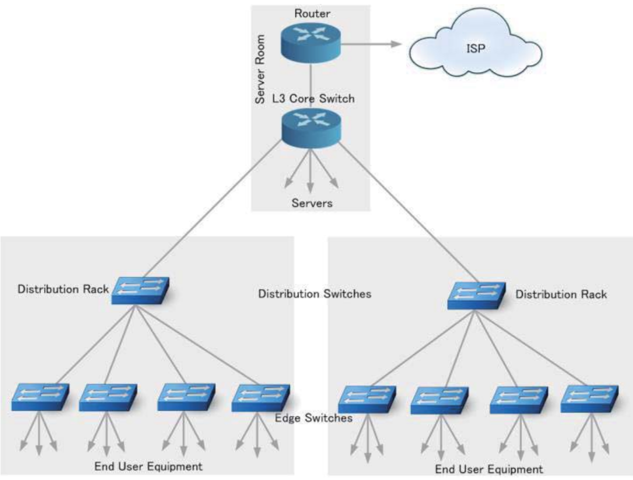

Fig 2: General Network Topology at Schools in the Soya Region

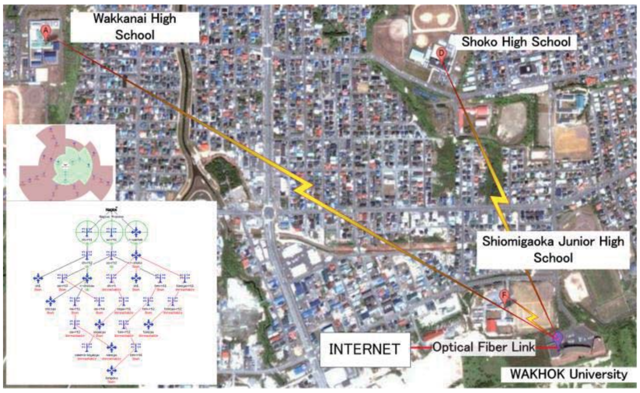

Fig3: Active Links

The topology has only one outgoing route to the ISP. If this connection fails, the school network will lose Internet services.

3. Related Work

The field of wireless networks has been the subject of extensive research [2],[6],[10],[15],[16],[19]. However, little of that research directly analyzes how Wi-Fi networks can be utilized as redundant networks during disasters—most of the research discusses the general-purpose use of Wi-Fi networks. For example, Kanayama and Takizawa first conducted research on the use of Wi-Fi in Wakkanai city in 1998 [11], and they continue to conduct Wi-Fi research in the Wakkanai area [12],[13],[14]. Their research concerned the construction and improvement of communication networks, but did not address the design of redundant networks to reduce network problems during disasters. Nor can we find other reliable documentation or practical research describing the implementation of redundant networks in the Soya region. Nonetheless, the studies of Kanayama and Takizawa provide substantial lessons for our future research.

Research has also been done on the use of wireless networks in disaster situations [15],[17],[18]. However, most of the studies do not concern the use of Wi-Fi networks as redundant networks for DRR. In contrast, our work clearly shows the potential for using a Wi-Fi network as an alternative route for a network in a disaster situation. The research is of value not only to academic intuitions, but also local governments.

This study can also contribute reliable guideline materials for the future development of networks in these localities. The physical network topology suggested by this study uses Wi-Fi to provide a high level of reliability and survivability. The study shows how schools in Wakkanai city can deploy Wi-Fi to optimize network design in order to provide reliability and survivability, without need for a further survey.

4. Proactive DRR measures that enhance network survivability

DRR measures are proactive disaster mitigation measures, which are meant to eliminate or reduce the impact of hazards before a disaster occurs. Generally, DRR activities should incorporate assessment of the evolving risk environment. Some typical examples of DRR measures include hazard mapping.

The enforcement of building and other civil engineering codes Flood, tsunami, and earthquake mapping.These DRR activities reduce the harm that disasters incur on societies. This paper focuses more specifically on reduction measures that can be applied in computer networks. We describe those measures in the following sections.

4.1 Proposed Community Disaster Ready Network

The primary objective of this research is to provide concrete guidelines for designing networks that can best survive natural disasters. Furthermore, we want to minimize the effects of natural hazards on networks in order to minimize the social and economic disruption caused by the hazards. We want to use effective network design to help control hazards, keeping them from developing into disasters.

During a disaster, regional government generally uses voice radio systems and other broadcasting systems for disaster response. However, disasters can damage wired networks, either destroying them or rendering them unable to maintain the bandwidth and data management required for regional communication. In such situations, backup wireless networks can provide a better alternative.

4.2 Redundant Topology

Network redundancy is the use of backup network links to reduce or eliminate network downtime caused by single points of failure. Redundancy ultimately works like an insurance policy for industrial networks. Redundant connections provide a quick-response backup system, which mitigates the risk of unplanned outages and ensures continuity of operation by allowing instant response to failures along critical data paths [1]. Outages in Wakkanai city can occur not only during winter, but also during natural disasters, which might result in great losses for the region. As experience has shown, Wakkanai city faces many unpredictable outages during winter seasons. Therefore, investment in network redundancy is clearly a smart strategy for making the network resistant to disaster.

Fig. 4 shows our proposed topology, which uses Wi-Fi links to provide network redundancy.

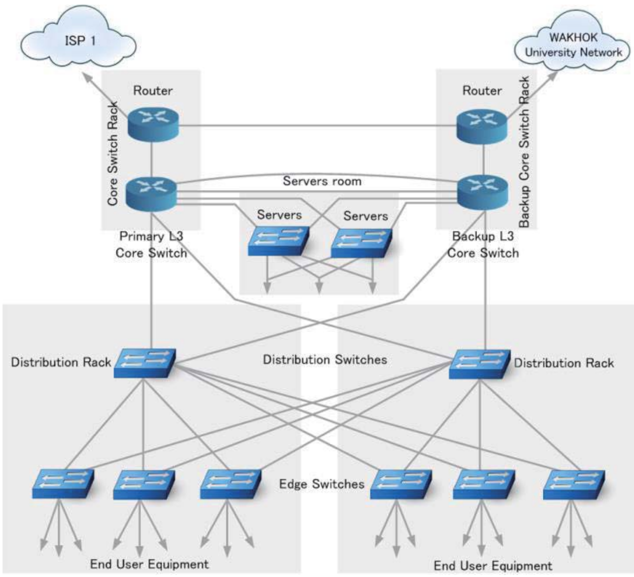

Fig 4: Redundant Network Topology

4.3 Consideration of Data Recovery

Disaster recovery is 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 respond during such situation. The recovery process must improve the efficiency of rescue teams and save as many lives as possible. For a network, the data recovery process includes the restoring of routers, switches, and other devices that make up the network. After a network is recovered, work—either local or remote—can be done to restore data-oriented servers.

Among the activities in a 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 for backing up data rely on a combination of two technologies: RAID [1] and Fiber Channel [2]. Off-site data protection should be organized such that, if a site crashes, the minimum number of server machines must be restarted at another network site to maintain and reactivate the offered services. Indeed, to quickly reactivate services and avoid excessive slowdown of running services, the number of server machines that must be restarted at remote sites should be reduced. Generally, servers are deployed so that if a power outage occurs, the backup power system provides power instantly, obviating the need for a restart. However, in some cases, these backup power systems cannot maintain the power for more than an hour. During our survey, we found that such servers are restarted during power outage and the restart usually resulted in file-system problems and data loss.

4.4 Use of Redundancy Protocols

The use of redundancy protocols to provide a redundant route is crucial when a master router loses its connection to the outside world. In order to provide a stable connection to the LAN without affecting the services in the network, it is recommended to utilize redundancy protocols in a router. A redundant router works as a backup router and must be deployed such that it can receive packets sent by the master router. The network must also be configured so that the interface of the master router is monitored and when it loses its connection with the outside world, the backup router takes over and restores connectivity.

In some cases, two or more routers can be set up to act as the gateway, and a dynamic routing protocol such as routing information protocol (RIP) or open shortest path first (OSPF) is used by hosts to determine the gateway router to use as the next hop in a path to a specific IP destination. However, dynamic routing should not be applied in every situation. When static routing is used, the hosts on the LAN are unable to communicate with hosts in the outside world if the statically configured router fails. Virtual router redundancy protocol

(VRRP) can be used to address this problem. VRRP can stay at the top of different physical routers and can act as the master router. VRRP can provide a stable network, because the physical router can be well monitored and if any interface is down, VRRP can monitor either the interface or the port.

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

Wi-Fi is one of the most popular wireless communication standards used today. It uses a wireless transmission medium (electromagnetic waves) to transmit information such as text, audio, and video content. 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. Wi-Fi can be used for an alternative, redundant network path.

Network-path redundancy entails the use of a backup path to provide stable network services when a network loses its route to the outside world. Wireless devices are good candidates for redundant network paths. A completely redundant system requires redundant switches, redundant communication ports, and redundant device pairs. Complete redundancy can make a network extremely reliable and stable—minimizing data loss and hastening recovery time.

4.6 Redundant Power Supply

Though power outages are inconvenient and expensive—especially in modern society—extensive electrical outages continue to occur in developed cities, including those in the Soya region. Power outages are disastrous and difficult to mitigate without very expensive backup power systems [8],[9].

Our experience of network administration at Wakkanai Hokusei Gakuen University suggests that we should use redundant power supplies for routers, switches, and servers. Without redundant power supplies, providing a stable network is impossible, even with a redundant network topology. Furthermore, unpredictable power outages hamper hardware devices, due to sudden fluctuations in voltage. A redundant power supply is also a requirement of a fault-tolerant power system. When a network designer considers power availability, the designer should ensure that even if one parallel supply fails, the system continues to provide full power to its power bus [6],[7],[8].

Each power supply source must include a circuit that automatically disconnects the redundant power supply module if it malfunctions. Automatic disconnection functionality is usually provided using isolation (ORing) diodes or MOSFETs placed in series with the output of each parallel supply [8]. If a power supply module short-circuits or shuts down for any reason, the MOSFET switch must be turned off in order to prevent a high impedance state. In addition to having this automatic output "disconnect" feature, each supply module must include a signal and visual indicator that can alert a user or monitoring external system that a specific redundant power supply has failed, so that it can be replaced or repaired [8],[9].

4.7 Adding Redundant Nodes

One fundamental problem of network design is the design of a network with an independent node. This problem arises in designing communication networks that have single-node failures. A network must meet certain link and node connectivity requirements to demonstrate that it can survive failures. We recommend increasing the number of redundant nodes to guarantee that there are at least two nodes that are connected to the outside world. Note that the number of redundant nodes should be increased not for the purpose of increasing link capacity, but rather to improve survivability

5. Simulation scenarios and result

5.1 Simulation Scenarios

This research is a practical oriented research which was performed in the field directly and our main focus was to obtain the results from the field rather than relying solely in simulation results. Nevertheless, we have done a set of experiments by using cisco packet tracer simulation tool with different parameters in order to test the availability of network by introducing redundant path. Packet delay variation (PDV) between the nodes and the end-to-end data delivery delay was also experimented. In order to analyze the scenarios, we have designed different network sizes including changing the number of nodes along with different traffic rate for each set of nodes. In this paper, we present and analyze some of the relevant result that we obtained during our simulation with optimized number of nodes. Specifically, we have focused our observation to find out packet loss and PDV. These data are crucial in order to recommend the construction of redundant network in urban area of Wakkanai during disaster. The detail of simulation parameters used in simulation is indicated in Table I.

TABLE 1: Simulation Parameters

Parameters	IEEE 802.x
Simulation time	1000s per layer
Terrain dimensions	1500,1500 (meters)
Number of nodes	26
Traffic generated	http, icmp, ospf,arp,cdp
MAC protocol	802.11, CDP
Routing protocol	OSPFv2
Loop Detecting Protocol	STP
Number of links (redundant)	2
L2 Switches	Cisco 2950 Series
L3 Switches	Cisco 3560 Series
Packet size	512

5.2 Topology of the Simulated Network

The topology of the simulated networks represents our recommended redundant technology. Our assumptions was that

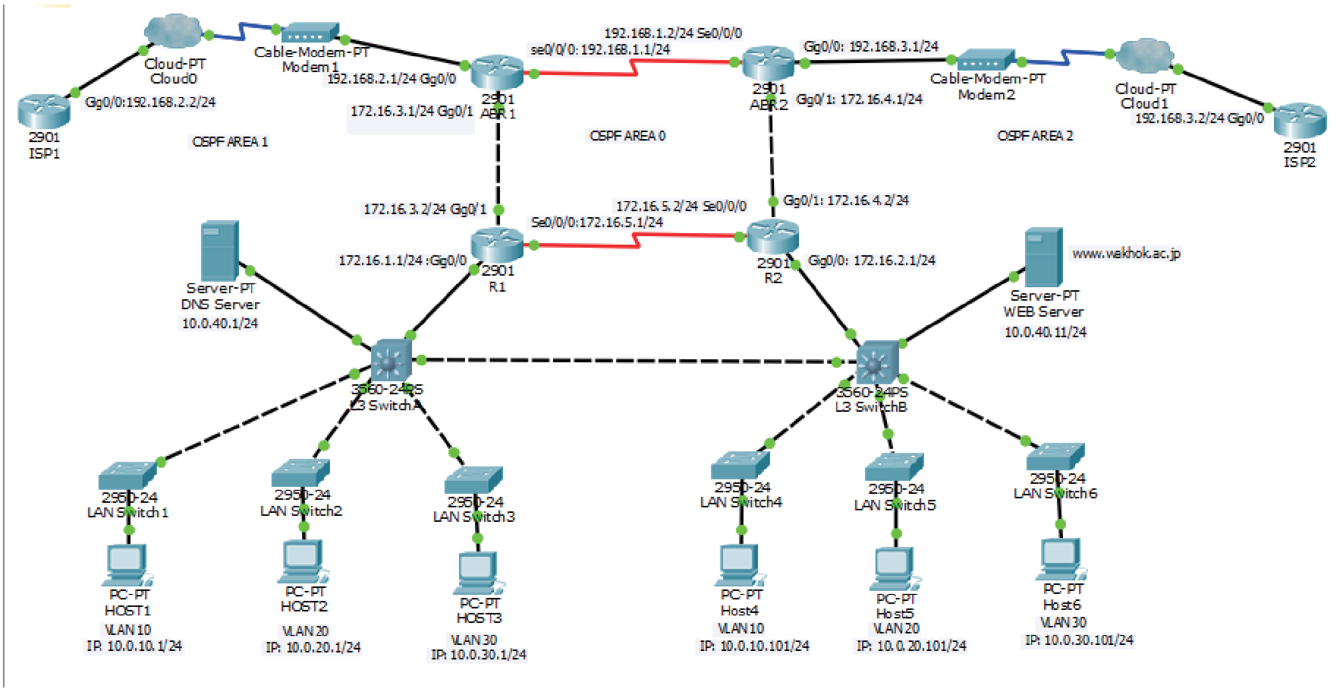

Figure 5: Simulated Topology

we might require at least 3 layers such as core, distribution and access layer. Each layer has maintained the redundant link and node. The simulation scenario is designed as shown in Fig. 5. Accordingly, we optimized the numbers of simulation nodes to 3 nodes at access layer, 2 nodes at distribution layer and 2 nodes at core layer. However, in the real scenario, this can cover larger areas as described in the section 6.

5.3 Packet Delay Variation (Jitter)

While packets are transmitted from source to destination, some packets might reach in different time. Packet delays varies due to different reasons occurred in network. This variation of delay is known as PDV (Packet Delay Variation). Packets transmit from source to destination will reach the destination with different delays time. In our experiments, the end to end delay occurred for the first 2 packets only. This is happened as the ARP required to collect MAC address from peripheral host for the first or second round trip. We observed that jitter has no relation with redundant links. However, the issue of jitter may arise while the number of hosts are increased. Our observations

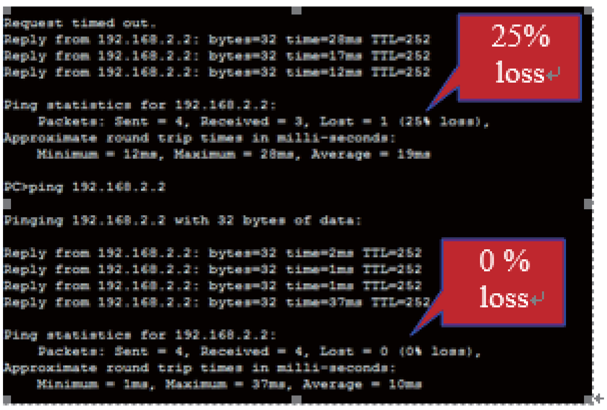

Figure 6: End to End Delay Experiment

prove that redundant networks with the combination of wired and wireless, robustness of networks would increase. We have tested the simulation by simultaneously stopping redundant link of R1 and R2. Connectivity was tested by stopping redundant node in each layers. The packets were sent from source host to destination and got successful to alternate the route as per our assumption.

6. Case Study of Wakkanai

Considering the importance of an alternate path, we experimented with the use of a Wi-Fi backhaul router. Fig. 5 shows the photographs of our equipment and experimental set up. We first surveyed the existing networks and network coverage. As shown in Fig. 9 and Fig. 10, there were only a few active links between Wakkanai Hokusei Gakuen University and the regional school networks. The green areas depict active network coverage and the red areas depict dead networks.

6.1 Scenario of Field Experiment

In order to re-identify the access points and network coverage, we conducted a new survey. We tested connections using the traditional method of locating the two ends. We used a mirror at both ends and reflected the sunlight to identify the direction of the point-to-point connections required for the two ends. The red rounded object in Fig. 8 is the mirror that we used to reflect the sunlight and notify our counterparts about our relative positions. We then mounted the wireless device parallel to the direction of the mirror reflection. We also agreed on where to place radio receivers and where to place transmitters. A person with a receiver then rotated and moved the device to receive the signal from the transmitter device.

Fig 7:　Wi-Fi Experiment near Wakkanai Memorial Tower

After a few attempts, we were able to receive the signal from the wireless access point, which was mounted in the university. This scenario is shown in the Fig. 11. After receiving the signal, we were able to establish a connection between the university and "100-Year Memorial Tower" of Wakkanai.

If the transmitter device were located anywhere other than the 100-Year Memorial Tower, receiving devices would have great difficulty receiving the signal from it. Our experiment suggests that a transmitter device at the tower can cover almost 80% of Wakkanai city with a Wi-Fi signal.

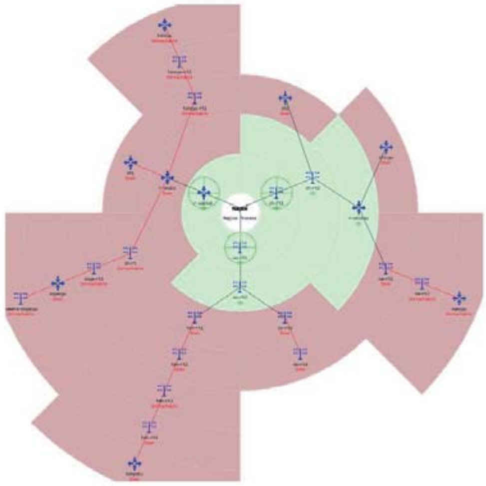

Fig 8: Active Network Coverage

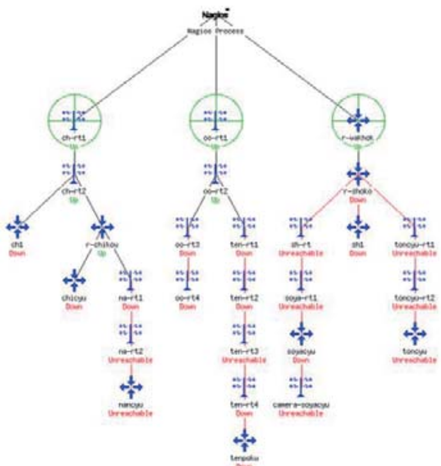

Fig 9: Active Network in Tree Structure

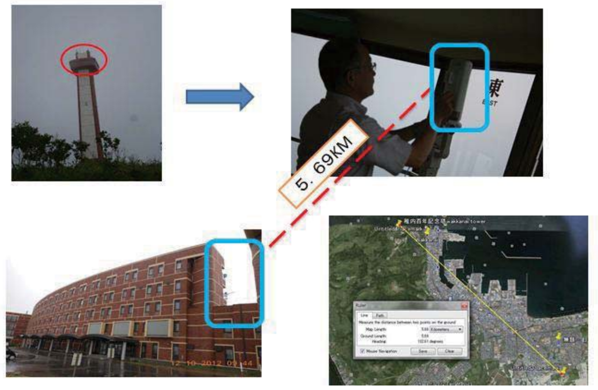

Fig 10: Link Surveys for Different Points

6.2 Discussion

We found that almost every school in the Soya region has a single point of failure in its network. This situation is common to schools in Japan. Only two schools have two connected networks: one provided by Wakkanai Hokusei Gakuen University and the other provided by an ISP. The rest of the networks have only a single connection. A network with a single link has a single point of failure and will fail if that link breaks. Bad weather causes frequent link failures on networks in Wakkanai city, so multi-hop wireless networks with redundant nodes are an important alternative. Redundant nodes are often introduced in mesh networks, and these redundant nodes can maintain network availability and survivability.

Redundant nodes do not increase network bandwidth, but rather increase the network reliability by providing failover links when a link in the shortest path fails. This paper includes a basic topology that can be used to identify the optimal topology of redundant nodes for a given school network. To help network designers choose the optimal topology, we provide a method by which they can calculate the additional network reliability that will result from adding a redundant node to a given topology.

7. Future Work and Conclusion

In this research, we observed that most of the schools in the Soya region connect to the outside world using a single physical link. Only two schools are connected with two links—one to the university and one to an outside ISP. Although most of the links are connected with fiber optics and stable internet services are provided, these networks are vulnerable to network outages during natural disasters. Our future work will include the actual installation of redundant links. However, to be able to implement the tertiary links, we will require funding support either from local government or from the MEXT (Ministry of Education, Culture, Sports, Science and Technology) of Japan.

We believe that disaster-response and disaster-ready networks are crucial for saving communities from unexpected damage. Disaster-response networks are typically connected to sensor networks that can detect disastrous events before they occur, in order to warn communities to find shelter and to take other appropriate measure [3]. However, network failures can severely hamper the ability of sensor networks to gather useful information in a timely manner. For example, networks aimed at monitoring fast-moving destructive physical phenomena, such as earthquakes and floods, must be designed to be disaster ready. During disasters, large-scale geographically correlated failures often occur. In addition, individuals use the network to try to contact each other and to request help, which leads to serious network congestion and exacerbates failures or even ties up channels entirely. This paper provides guidance for designing topologies with redundancy in the Soya region. Although designed for the Soya region, the topology can be used for designing redundant networks at any other institution. In our research, we determined that most Soya schools can get a backhaul link from Wakkanai Hokusei Gakuen University. In addition to helping a network meet hierarchical network design guidelines, redundancy can also allow a network to provide high availability and reliability, even during disasters. By "reliable" we mean that even if a network failure occurs, a network has connectivity through non-failed links. Thus, our focus is on the availability and reliability of network services when a disaster occurs, considering several measures of risk and operating on the assumption that link failures are independent.

We gave highest priority to issues that render networks vulnerable not only to sudden outages during winter seasons, but also during other natural disasters. We used disaster scenarios from university computer networks and areas such as Fukushima to describe how a disaster may occur and how it can negatively affect organizational computer networks. There are many potential techniques, troubleshooting tools, and practices—at a wide range of prices and levels of complexity—that can be used to safeguard networks. We have presented some considerations to take into account when constructing a stable network. Furthermore, with regard to disaster-preparedness in the Soya region, we recommend providing disaster education and disaster mitigation plans for school networks to school teachers. Education and planning should enhance teacher readiness to act during natural disasters in a way that supports the proposed emergency operation plan. Because natural disasters such as earthquakes can occur without warning, a proper network-management plan for natural disasters is essential.

Reference

1) Japan Disaster Statistics, Natural Disasters from 1980 – 2010, International Disaster Database URL: http://www.preventionweb.net/english/countries/statistics/?cid=87, Date Accessed: 2013/06/11

2) H. Xing, A. L. Miguel, Stochastic network design for disaster preparedness, URL: http://www.optimization-online.org/DB_FILE/2012/12/3705.pdf, Date Accessed: 2013/06/11

3) A. Martin-Campillo, J. Crowcroft, E. Yoneki and R. Martil, Evaluating opportunistic networks in disaster scenarios, URL: http://www.cl.cam.ac.uk/~ey204/pubs/2012_JNCA.pdf, Date Accessed: 2013/6/15

4) CFLT Team: Disaster preparedness and recovery plan, URL: http://www.cof.org/files/Documents/Community_Foundations/DisasterPlan/DisasterPlan.pdf, Date Accessed: 2013/01/27

5) B. N. Catherine, 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: 2013/07/22

6) G. Jim, Designing and Deploying 802.11n Wireless Networks, Cisco Press, 2010

7) Cisco − Disaster Recovery: Best Practices White Paper, URL: http://www.williamsdatamanagement.com/pdfs/Cisco%20Disaster%20Recovery%20PDF.pdf, Date Accessed: 2013/07/22

8) M. Berman, Eliminate system downtime with redundant power supplies, URL: http://www.newark.com/pdfs/techarticles/lambda/ESDRPS.pdf, Date Accessed: 2013/07/26

9) J. Kruckenberg, A. Lippolis, E. Schacht, and C. Seeley, Prioritized backup power system, URL: http://www.ti.com/corp/docs/landing/universityprogram/09_winners/Ohio_State_Kruckenburg.pdf, Date Accessed: 2013/4/15

10) J. Robert, The importance of network redundancy, URL: http://www.windowsnetworking.com/articles-tutorials/netgeneral/Importance-Network-Redundancy.html, Date Accessed: 2013/07/26

11) O. Takizawa and N. Kanayama, Progress of wakkanai experimental community network project, National Institute of Information and Communications Technology, Vol. 50, 2004, URL: http://www.nict.go.jp/publication/shuppan/kihou-journal/kihou-vol50no1.2/kihou-vol50no1.2_0702.pdf, Japanese Version, Date Accessed: 2013/07/28

12) Y. Minami, N. Kanayama, F. Takeshi, Problem of wireless network and the construction of regional, Japanese Version, URL: http://www.crl.wakkanai.ne.jp/draft/wit2001-m.pdf, Date Accessed: 2013/07/28

13) N. Kanayama, K. Sakamoto, Building a regional network for education by using multicast broadcasting, URL: http://takizawa.ne.jp/ipe2001.pdf, Japanese Version, Date Accessed: 2013/07/28

14) O. Takizawa, N. Kanayama, Progress of wakkanai experimental community network project, URL: http://www.nict.go.jp/publication/shuppan/kihou-journal/journal-vol51no1.2/ippan2.pdf, Date Accessed: 2013/07/28

15) S. Ivan, L. Xu, Power-aware localized routing in wireless networks, ieee transaction on parallel and distributed systems, Vol. 12, No. 10, URL: http://www.site.uottawa.ca/~ivan/power-tpds.pdf, Date Accessed: 2013/07/30

16) D. R. Paudel, S. Kazuhiko, B.P. Gautam and D. Shrestha, Design and implementation of partial mesh community wireless network in himalayan region, Proceedings of Third Asian Himalayas Internationl Conference on Internet AH-ICI2012, 2012/11, Kathmandu, Nepal

17) L. Franck, H. Theus, S. Felix, P. Bernhard, 30 Years of Wireless Ad Hoc Networking Research What about Humanitarian and Disaster Relief Solutions? What are we still missing? URL: http://people.ee.ethz.ch/~lfranck/acwr-legendre.pdf, Date Accessed: 2013/08/22

18) Z. Gil, S. Adrian, Energy efficient routing in ad hoc disaster recovery networks, URL: http://www.ieee-infocom.org/2003/papers/17_02.PDF, Date Accessed: 2013/08/25

19) B. P. Gautam, D. R. Paudel and K. Shrestha, A study and site survey in himalayan region for proper utilization of wireless community networks: an assessment of community wireless implementation in heterogeneous topography, WAKHOK Journal, Vol. 11

