Operational Management Using Wake-on-LAN

Yeongkwun Kim
School of Computer Sciences
Western Illinois University
Macomb IL, USA
email:Y-Kim2@wiu.edu

Injoo Kim
Department of Computer &
Information Science
East-West University
Chicago IL, USA
email: injoo@eastwest.edu

Abstract **- Remote access is a valuable way to access network resources. Wake-on-LAN (WoL) is a well-known technology commonly used for external remote access. In this work, we implement an operational supporting system to perform key operations such as security checks including virus scanning, software modifications/updates, amongst others. Such functions are all dependent on WoL to access remote systems.**

Keywords-operational management; virus scan; remote login; WoL.

I. INTRODUCTION

The WoL (Wake-on-LAN) has widespread use as a networking protocol that enables clients to wake up all computer systems remotely [1]. It allows administrators to perform system maintenance even if the user has turned off the computer. Appropriately applied, it is valuable for administrative activities such as security patch delivery and framework maintenance as well as for diminishing overall energy utilization. Since it permits administrators to turn on computers remotely, turning off computers while they are not being used does not have any negative effects on system management. It might be particularly helpful for academic institutions or organizations/companies with huge networks to have the option to turn on computers remotely, where the option to turn on all computers within a reasonable timeframe is not viable. WoL is an independent platform, requiring explicit adjustments of the hardware and software to operate appropriately. Most desktop hardware and operating systems such as Microsoft Windows, Mac OS X, and Linux support WoL. In this paper, we present the preliminary findings of our implementation of the operational support system based on the WoL. The rest of this paper is organized as follows. Section II describes related work, Section III describes the WoL, and Section IV addresses the network setup. Section V draws the conclusion and briefly indicates future work.

II. RELATED WORK

Stefanovic et al. [1] used WoL to save time on business processes by turning on and having computers ready for employees when they arrive. Depending on the working hours of each employee, they measured how much the machines used the network. Although they did make use of remote access, they did show that it was possible to turn on users' computers depending on the working hours of each employee. This provides important foundation for possible improvements that can be made by enabling remote access.

III. WAKE-ON-LAN

WoL [2]-[4] is implemented utilizing an extraordinary network message called a magic packet. A magic packet has the MAC address of the destination computer. The listening computer waits for a magic packet routed to it and afterward initiates the system wake-up. The magic packet is sent on the data link or layer 2 in the OSI (Open System Interconnection) model and communicated to all NICs (Network Interface Cards) utilizing the network broadcast address. In order for WoL to function properly, the MAC address of the destination computer is required. The MAC (Medium Access Control) address can be distinguished on a nearby local network by utilizing simple commands, such as, ipconfig/ ifconfig. It is difficult to track down the MAC addresses of a group of PCs in a huge network by hand. Thus, we send the magic packets to the destination by providing the MAC address. The magic packet basically contains the destination computer's MAC address 255 (FF FF FF FF FF FF) that will be sent to the destination computer. The magic packet will be only checked for the MAC address and a complete protocol stack will not parse it. So, it can be sent as any network and transport-layer protocol. A link-oriented transport-layer protocol like TCP (Transmission Control Protocol) is not appropriate for this purpose because it requires a functioning connection to be formed before sending client information.

IV. NETWORK SETUP

We set up our network topology to simulate a multi-hop cross-subnet network with two arrangements of virtual PCs, each having their subnet. Furthermore, the router-to-router association is likewise viewed as its own subnet, making it a multi-hop network. Since network routing is done point to point, the number of routers does not matter, and thus we can

 ISBN: 978-1-68558-037-7

include more hops or subnets without influencing the results. The network topology model was created utilizing GNS3 (Graphical Network Simulator-3) [5]. Table 1 shows subnet masks & IP configuration. Figure 1 shows the model network configuration.

TABLE 1. SUBNET MASK AND IP CONFIGURATION

	Router1	Router2	PC1	PC 2	PC 3	Windows server	Kali linux server
Interface0	10.1.1.1	20.1.1.1	10.0.0.6	20.0.0.7	20.0.0.8	10.1.1.118	20.1.1.50
Interface1	2.1.1.1	2.1.1.2	N/A	N/A	N/A	N/A	N/A

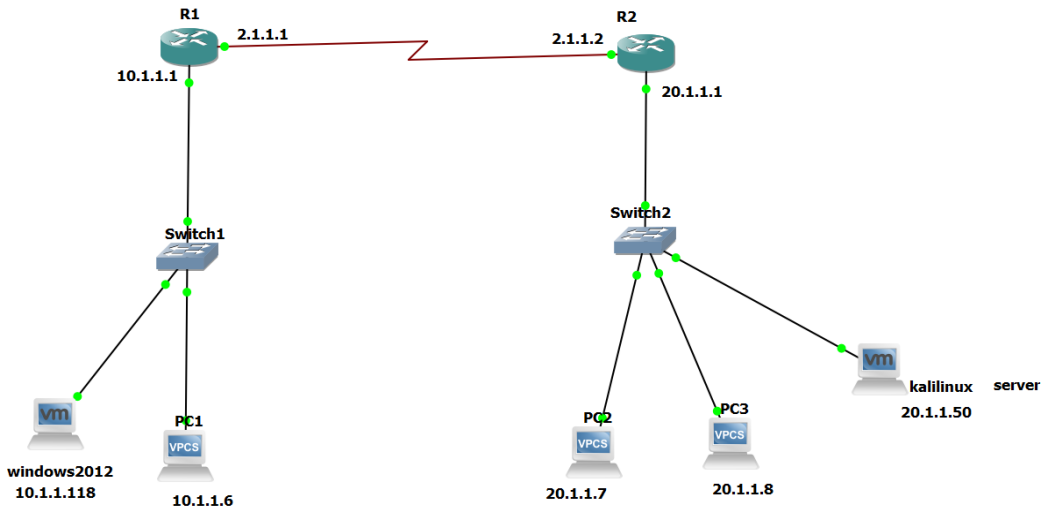

Figure 1. Model network configuration

The following procedure describes the communication from PC1 to PC2 in the WoL network in our simulation:

1. Switch1 holds the MAC address of the PC1 and Switch2 holds the MAC addresses of PC2 & PC3
2. When it pings 20.1.1.7(PC2) from PC1(10.1.1.6), the IP goes to the network gateway 10.1.1.1 which is the IP address of Router 1
3. Router 2 advertises its own network (20.1.1.2/24) and broadcasts it to other Routers
4. when Router 1 receives 20.1.1.0/24 network information, it checks for the shortest path and the advertising Routes it has.
5. Since Router 1 has the network path of the destination ones, Router 1 sends the network (20.1.1.0/24) to Router 2.
6. Router 2 receives the IP address of 20.1.1.7/24 from PC1 of Router 1 and sends it to the Switch 2 port of PC2.
7. Switch 2 receives IP address 20.1.1.7. Switch 2 holds the MAC address of PC2. Now the Switch 2 sends the received packet to the PC2 based on the MAC address.

A. Advantage of Using WoL

Any office files and equipment can be accessed remotely with the described WoL setup. This setup is more useful for network administrators or IT people who are working remotely, as it enables full access to a computer despite being remote. When it is combined with the correct set of remote tools, WoL technology can be used as a possible remote approximation of being in the office.

 ISBN: 978-1-68558-037-7

B. Disadvantage of Using WoL

There are some security concerns when utilizing this technology. First, most WoL compatible adapters do not distinguish between which PC is sending the magic bundle. This means that anyone on a network with a good and compatible IP address can possibly remotely access the computer. Thus, such a technology should be handled with additional network security provisions.

V. CONCLUSION AND FUTURE WORK

Although WoL is a generally mature technology, numerous associations and organizations do not execute it due to confinements. In this work, we implemented a simple operation management to perform important functions such as security patch delivery and framework maintenance by utilizing WoL. Given the developing nature of this technology, future research is needed to do more simulations to increase robustness because our work is still premature stage. We will also discuss with the IT department to apply our system to the live network.

ACKNOWLEDGMENT

Mr. C. R. Dendi assisted with simulations of operations.

REFERENCES

[1] M. Stefanovic, D. Przulj, M. Vukmanovic, and S. Ristic, “Mutual Impact of High Computer Network Utilization and Business Processes”, International Scientific Conference on Industrial Systems, 2007.

[2] Jithin, “What is SYN Flood attack and how to prevent it?”, https://www.interserver.net/tips/kb/syn-flood-attack-prevent/, 2016, [retrieved: March 2023].

[3] Sheetg09, Mestew, Aczechowski, Dougeby, “How to configure Wake on LAN in Configuration Manager”, https://learn.microsoft.com/en-us/mem/configmgr/core/clients/deploy/configure-wake-on-lan, 2022, [retrieved: March 2023].

[4] CISCO, “How to configure the router to minimize a Denial of Service (DOS) attack”, https://community.cisco.com/t5/security-documents/how-to-configure-the-router-to-minimize-a-denial-of-service-dos/ta-p/3117624, [retrieved: March 2023].

[5] GNS official website, “GNS-3 download” https://www.gns3.com, [retrieved: March 2023].

 ISBN: 978-1-68558-037-7