Journal of Computer Technology and Applied Mathematics
Vol. 1, No. 1, 2024

Practical Application of N2N Technology in Virtual LAN Management System

WU, Zhen [1*] SONG, Qingqing [2]

[1] Nanjing University of Aeronautics and Astronautics, China
[2] Belarusian State University, Belarus

**** WU, Zhen is the corresponding author, E-mail: 13wuzhen@sina.com***

Abstract: Due to the impact of the COVID-19 epidemic and related policies, remote collaboration technology that is not limited by geographical location has begun to be widely used. Among them, virtual LAN, as an important remote collaboration technology, has received widespread attention. This study is based on N2N peer-to-peer virtual private network technology, utilizing its advantages of high performance, high convenience, and direct traffic connection between nodes under specific conditions, and making it the core technology for constructing and accessing virtual local area networks. In this study, we introduced the application of N2N technology in virtual LAN management systems, and verified the feasibility of applying N2N technology to virtual LAN management systems through the design of the overall system architecture and various parts. Finally, we proposed a solution based on N2N technology that integrates LAN construction, network partitioning, and user management.

Keywords: N2N, virtual LAN, Management System, Remote Office, Multi-Region Collaboration, Network Software Facility Construction

DOI: https://doi.org/10.5281/zenodo.10938128

1 Introduction

The rapid spread of the COVID-19 epidemic worldwide has led governments to implement blockade and isolation measures to prevent the spread of the epidemic [1]. These measures have forced the suspension of commercial activities and the cessation of public transportation services. In addition, educational institutions have also stopped traditional offline teaching activities and turned to online teaching models to ensure the continuity of educational activities [2-3]. Therefore, remote collaboration technology that is not limited by geographical location has begun to receive widespread attention and application.

At the same time, China is actively promoting enterprise intelligence and Internet to build a unified national market and promote cross regional integration **[4]**. However, for most enterprises, investing a large amount of funds in network construction is a daunting task. It is difficult to implement dedicated lines built by operators for each office location, especially when it involves cross-border or cross sea situations, and the cost will be even more expensive. Therefore, how to achieve the sharing of enterprise resources and information has become an urgent problem to be solved.

This study integrates software technology, computer network technology, and database technology, with N2N technology as the core, and designs a solution that integrates LAN construction, network partitioning, and user management. We have designed and implemented both a user oriented client and an administrator oriented System Administrator Console and Organization Administrator Console to achieve efficient network management. For users, this system is easy to operate and does not require a significant investment of time and funds for training.

2 Current Solution

At present, Oray Company is the main supplier of virtual LAN networking solutions in China, with products including peanut shells, sunflowers, and dandelions. Oray provides software and hardware services for individuals and businesses, and can provide integrated software and hardware solutions for enterprise users. The Hamachi software developed by LogMeIn in 2004 is one of the earlier LAN networking software developed outside of China **[5]**. In recent years, ZeroTier has also become widely used **[6]**. The software was first released in 2014, providing free and paid services for individuals, as well as service licenses for commercial companies.

3 Main Technology

3.1 Virtual LAN Technology

VLAN, also known as Virtual Local Area Network, is a technical means that can divide a physical local area

network (LAN) into new broadcast domains according to specific conditions. The division of VLANs can be based on factors such as the interface of the switch, MAC address, IP network segment, etc. A notable feature of VLAN is that it can partition networks without being limited by the physical location of devices. If the devices belong to different VLANs, even if they are in the same physical network topology, they cannot communicate with each other. This feature can effectively manage resource access and prevent unauthorized operations. By dividing different VLANs, network isolation can be achieved, making networking more convenient. At the same time, a single fault will not affect other networks.

3.2 Access Control List (ACL) Technology

Access Control List (ACL) is a packet filtering based network security technology that processes, forwards, or discards access requests based on preset conditions. By implementing access control, network security can be effectively protected, preventing malicious visitors from easily accessing services, thereby improving the ability to prevent malicious destructive behavior.

3.3 NAT Penetration Technology

Network Address Translation (NAT) is a temporary solution proposed to alleviate the shortage of IPv4 addresses. NAT implements the mapping of internal device IPs to external IPs, allowing multiple internal devices to share a common IP address, thereby providing network connection services for more devices with fewer IP addresses. However, NAT also has many problems, such as disrupting end-to-end communication. Due to the type limitations of NAT, externally initiated connections may not be able to reach internal devices properly. Unfortunately, due to cost and security considerations, most Internet Service Providers (ISPs) currently use NAT technology. In order to solve this problem, some technologies for network penetration have emerged, such as FRP reverse proxy. NAT is usually divided into several types, including full cone NAT, restricted NAT, port restricted NAT, and symmetric NAT **[7]**.

3.4 N2N Point-to-Point Virtual Private Network Technology

N2N is a layer two peer-to-peer virtual private network (VPN) technology that allows users to use protocols at the network level. N2N provides a method for users to establish their own VPN. It uses user-defined keys for encryption on nodes, rather than application layer encryption, which greatly improves the security and privacy of user data **[8]**. N2N has the ability to penetrate the network environment located after Network Address Translation (NAT). N2N has designed an architecture that includes EdgeNodes and SuperNodes. EdgeNodes can obtain their recorded edge node information through SuperNodes and select connection paths.

4 N2N Operation Methods and Instructions

This paper takes N2N technology as the core of the virtual LAN management system, so it is necessary to explore the common operating methods of N2N and understand its command functions. In this section, common operating methods and instructions for N2N will be introduced.

4.1 SuperNode startup parameters

SuperNode does not have a UI interface, so it needs to be configured with parameters during startup. The startup parameters and purpose of SuperNode are shown in Table 1. Multiple different parameters can be combined and used with each other.

Table 1 SuperNode startup parameters and purposes

Parameter format	Description
-p *port*	SuperNode listening port, default 7654
-F *federation name*	SuperNode Federation name, default to * Federation
-l *host:port*	In conjunction with - F, the known address and port of another SuperNode
-M	Turn off MAC and IP address spoofing protection for groups with non username and password authentication
-V *text*	Custom string (up to 19 bits), used to display in management output logs
-C *group name configuration file path*	This configuration file contains allowed group names
-A *IP segment*	Used for automatic IP allocation, format such as - a 192.168.0.0-192.168.255.0/24
-t *port*	Configure SuperNode management port
--management_password *pw*	Manage Passwords
-v	Output more logs

4.2 EdgeNode startup parameters

Like SuperNode, EdgeNode also does not have a UI interface, so parameters need to be added at startup to configure it. The starting parameters and purpose of EdgeNode are shown in Table 2. Multiple different parameters can be combined and used with each other.

Table 2 EdgeNode startup parameters and purposes

Parameter format	Description
-c *Group Name*	Used to distinguish different virtual LANs
-l *SuperNode IP: port*	N2N server (SuperNode Address)
-p *Local UDP port*	Bind the specified UDP port on the local machine to prevent UDP restrictions from affecting N2N networking in some environments
-D	Enable PMTU discovery. PMTU has found that it can reduce fragmentation, but improper support can cause connection pauses
-e *IP address*	As the preferred local IP address provided by the broadcast, it is useful if multicast peer detection is not available, and the "- e auto" parameter attempts to automatically detect the IP address
-S1	Do not use P2P connection, always use UDP mode to relay through supernode (not recommended)
-S2	Always use TCP mode to relay through supernode (Windows does not support this parameter)
-i *seconds*	Set NAT punching interval, default: 20
-L *TTL value*	When UDP NAT punching passes through the server (central node), register the TTL of the package (default is 0, indicating no setting)
-v	Output more detailed logs
-t *port*	Manage UDP ports (for running multiple edges simultaneously on the local machine)
-n *Routing table (format: Target IP segment: Gateway)*	Additional routing table that can be called multiple times (e.g. - n 192.168.2.0/24:192.168.6.5)
--no-port-forwarding	Turn off UPnP/PMP function

4.3 Data Interaction API

The data interaction API in N2N is used to obtain data from SuperNodes or EdgeNodes. The operation method is to send UDP messages to the management port of the SuperNode/EdgeNode in any way. The default management port for SuperNodes is 5645, and the default management port for EdgeNodes is 5644.

For UDP packets sent to the data exchange API of SuperNode or EdgeNode, there are two main types: r type and w type. The r type is a read method, which is used to obtain information; W represents the use of the write method when updating parameters.

There are two numerical fields in the UDP message at the same time. The first one is the message label, with a value range of 0-999. Its function is to distinguish requests from different sources. When the requester provides a label value during the request, any non error response message associated with this label value will contain this label value. The second one is the message flag, with a value range of 0-1. Its function is to describe any remaining optional subfields. 0 represents that there are no other subfields in the request message, and 1 represents that there is an additional field in the request message, including the authentication key.

The authentication key is one of the security measures of the data exchange API in N2N, which provides a simple string password for the client to verify whether the request is allowed to pass.

The content format of the request message contains multiple fields, each separated by a space. The first field is the message type, the second field is the option, and the third field is the additional parameter. The option field is a special set of subfields separated by colons, which includes three subfields: message label, message flag, and authentication key (optional). The request example is shown below.

The content of the request message with the authentication key:

r 666: 1: password communities

Request message content without authentication key:

r 888: 0 communities

For the additional parameter of the third field, different parameters have different functions, and the function description is shown in Table 3.

Table 3 Function Description of Additional Parameters in Data Interaction API

Additional Parameters	Function Description
edges	List all edges (client, edge nodes) connected under the current supernode
communities	List all communities (virtual groups) connected under the current supernode
reload_communities	Reload the community. list and user public key provided through the - c parameter
timestamps	List the timestamps related to supernodes (including starttime \ last_fwd \ last-reg_super)
packetstats	List traffic statistics data for supernodes (including forward \ broadcast \ reg_super \ errors)
verbose	Log level, default to 3

The data exchange API in N2N returns an UPD message in JSON format. Its content includes message header, message body, message tail, and error message. Each return message contains two fixed key values, namely _tag and _type. The value of _tag comes from the message label in the request, while _type is used to mark the content type of the packet. For example, the message header corresponds to a value of begin, the message body is row, the message tail is end, and the error message is marked as "error".

In practical applications, after sending a data exchange API request message, the start tag can be used as the entry point to obtain the main text, and then the end tag can be used to determine the end position of the main text. If an error is encountered, it enters the exception handling process.

5 Design of Virtual LAN Management System based on N2N

5.1 System Design Overall

In the virtual LAN management system, we divide it into five parts: the data control end responsible for data management and control, the System Administrator Console responsible for overall system operation control, the Organization Administrator Console responsible for managing access control within the organization, the SuperNode server responsible for virtual LAN broadcasting and packet relay, and the EdgeNode accessor responsible for virtual LAN access. The overall architecture is shown in Figure 1.

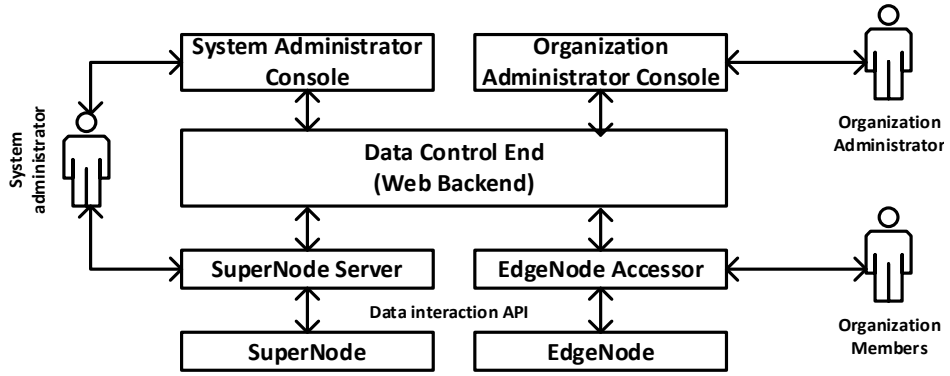

Figure 1 Schematic diagram of the overall system structure

The data control end shown in Figure 1 is the web backend. It is developed in Java language, with the SpringBoot framework as the core, adopting MVC mode, and using MySQL database as the data persistence layer. The specific internal structure is shown in Figure 2.

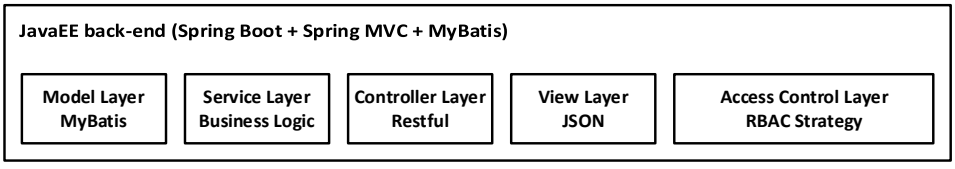

Figure 2 Schematic diagram of back-end structure

The System Administrator Console and Organization Administrator Console are web frontends developed in HTML + CSS + JavaScript language using Vue.Js framework is the core, adopting the MVVM pattern, using Element UI as the style framework, and D2Admin as the routing and interaction control framework. The specific internal structure is shown in Figure 3.

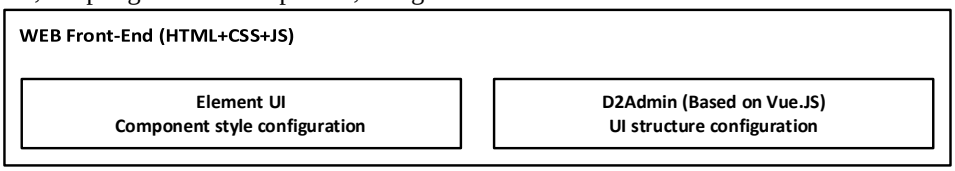

Figure 3 Schematic diagram of WEB front-end structure

The SuperNode server and edgeNode accessor are Windows application. It is developed using EPL5.8 and adopts the C/S client and server mode, using the N2N scheme as the core for virtual LAN control and access. The specific internal structure is shown in Figure 4.

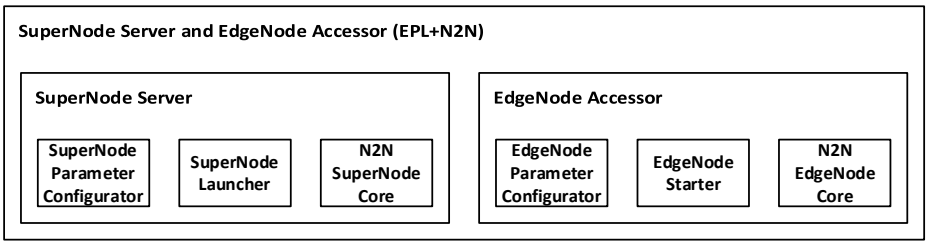

Figure 4 Application side structure diagram

The web front-end is developed based on the MVVM (Model-View-Viewmodel) model, which is an evolution of the MVC model. The ViewModel layer of the MVVM model replaces the Controller layer of the MVC model. The MVVM model used in the system described in this paper is shown in Figure 5, which also shows the interaction between the front-end and back-end of the webpage.

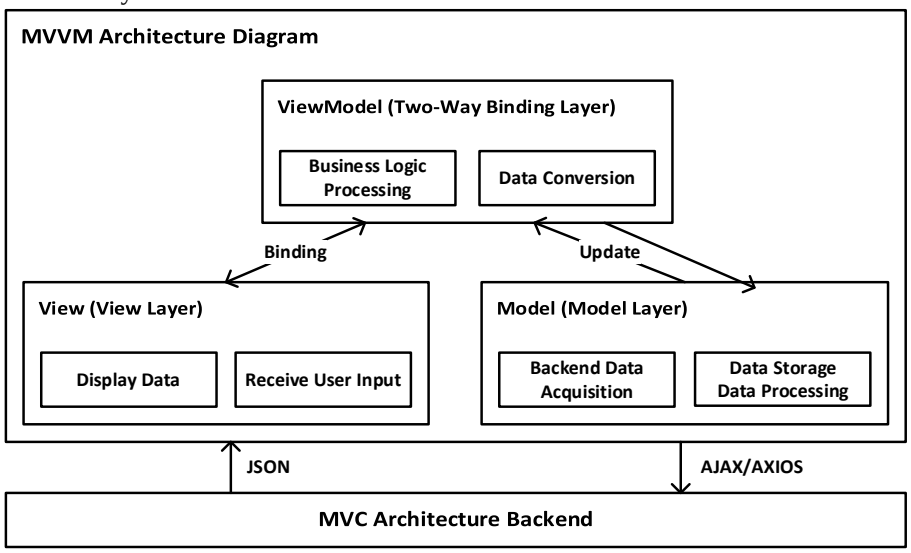

Figure 5 Schematic diagram of MVVM architecture hierarchy

5.2 Entity Relationship Design

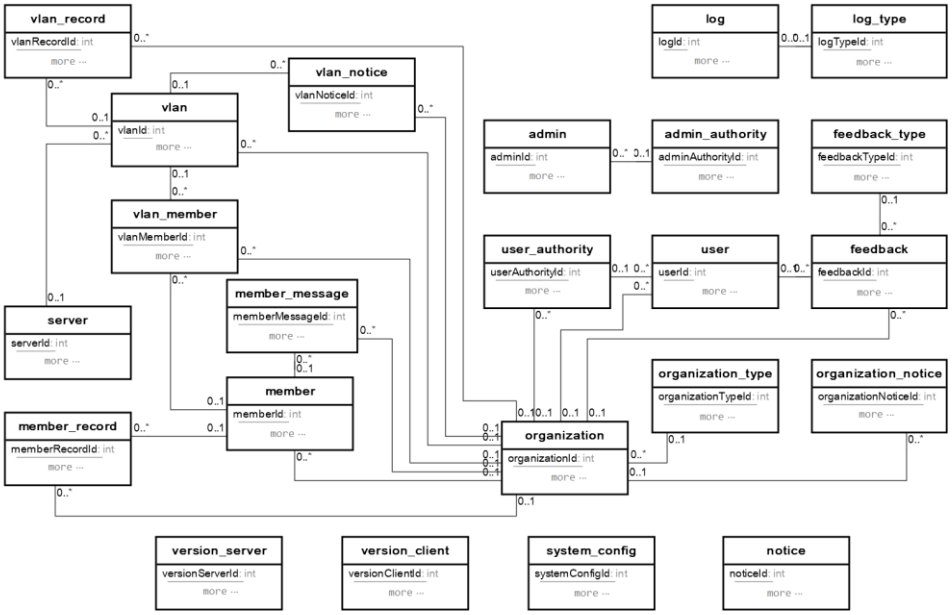

Figure 6 Schematic diagram of system entity relationship design

In Figure 6, we can see that the Organization organization is the core entity, and the vast majority of entities have one-to-one or one to many connections with it.

At the same time, through the entity connection diagram, we can also know that there is a set of many to many entity connections in the system, which are the connections between ***vlan*** and ***member***. A member can belong to multiple vlans, and there can also be multiple members in a vlan. Therefore, it is necessary to add a vlan_member data table as a multi to many association table between vlans and members.

6 Discuss

N2N peer-to-peer virtual private network technology has many advantages, such as high performance, convenience, and direct traffic between nodes without the need for SuperNode forwarding under NAT conditions. However, it is worth noting that the working principle of N2N relies on SuperNode for node registration and information acquisition. If the SuperNode fails or is attacked, it may affect the stability of the entire N2N network. At the same time, N2N requires running client software EdgeNode on all terminals. This may cause inconvenience to some users, especially those who are not familiar with how to install and configure client software.

Although we have improved the user's convenience to some extent through the SuperNode server and EdgeNode accessor, SuperNode is still the most vulnerable part of the entire system. Therefore, an efficient and stable virtual local area network construction and management scheme remains a worthwhile issue for future exploration.

7 Conclusion

This paper introduces the practical application of N2N peer-to-peer virtual private network technology in virtual local area network management systems. Through this study, we have confirmed that the application of N2N peer-to-peer virtual private network technology in virtual local area network management systems is feasible, and it has the advantages of high performance and high convenience.

In this paper, in addition to setting up Data Control End, System Administrator Console, and Organization Administrator Console, we also independently set up SuperNode Server and EdgeNode Access to configure startup parameters and communicate with data exchange APIs for SuperNode and EdgeNode, in order to facilitate better collaboration between the virtual LAN management system and the N2N core.

Further research in the future will focus on how to make the server where SuperNode is located no longer the most vulnerable part of the system. Therefore, we need to delve deeper into the optimization strategies of SuperNodes, including but not limited to optimizing SuperNodes, adding redundant SuperNodes, and introducing load balancing strategies **[9]**. Meanwhile, future research objectives also include exploring or developing a new type of virtual private network technology, such as VXLAN **[10]**, NVGRE **[11]**, STT **[12]**, SPBM **[13]**, and other technologies.

Acknowledgments

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

Funding

Not applicable.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Conflict of Interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Author Contributions

Not applicable.

About the Authors

WU, Zhen

Nanjing University of Aeronautics and Astronautics; No. 29, Yudao Street, Qinhuai District, Nanjing City, Jiangsu Province 210016, China; e-mails: 13wuzhen@sina.com

SONG, Qingqing

Faculty of Applied Mathematics and Computer Science; Belarusian State University; 4 Nezavisimosti Avenue, Minsk 220030, Belarus; e-mails: fpm.sunC@bsu.by

References

[1] Koh D. COVID-19 lockdowns throughout the world[J]. Occupational Medicine, 2020, 70(5): 322-322.

[2] Aperribai L, Cortabarria L, Aguirre T, et al. Teacher's physical activity and mental health during lockdown due to the COVID-2019 pandemic[J]. Frontiers in psychology, 2020, 11: 577886.

[3] Wang C, Zhao H. The impact of COVID-19 on anxiety in Chinese university students[J]. Frontiers in psychology, 2020, 11: 1168.

[4] State News Network. The State Council Information Office held a regular briefing on the State Council's policies on the progress of accelerating the construction of a unified national market. [EB/OL].(2023-12-26). https://www.samr.gov.cn/xw/xwfbt/art/2023/art_7acc226e01344ffeb94261f059ca1cc1.html

[5] Bilinovac, D., & Rezic, S. (2010). Free solutions for VPN and computer remote control. na.

[6] Prasetyo, S. E., Hadinata, F., & Haeruddin, H. (2022, April). ANALYSIS OF ZEROTIER'S USAGE DURING THE COVID-19 PANDEMIC. In CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences (Vol. 2, No. 1, pp. 235-235).

[7] A NAT Traversal Mechanism for Peer-To-Peer Networks[C]//2009 International Symposium on Intelligent Ubiquitous Computing and Education. Chengdu, China: IEEE, 2009.

[8] Deri L, Andrews R. N2n: A layer two peer-to-peer vpn[C]//Resilient Networks and Services: Second International Conference on Autonomous Infrastructure, Management and Security, AIMS 2008 Bremen, Germany, July 1-3, 2008 Proceedings 2. Springer Berlin Heidelberg, 2008: 53-64.

[9] Song, Q., Wu, Z., & Xia, S. (2024). Design of Disaster Recovery and Load Balancing Strategies in Traditional Centralized Distributed Web Systems. Journal of Industrial Engineering and Applied Science, 2(2), 34–38.

[10] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., ... & Wright, C. (2014). Virtual extensible local area network (vxlan): A framework for overlaying virtualized layer 2 networks over layer 3 networks (No. rfc7348).

[11] Garg, P., & Wang, Y. (2015). NVGRE: Network virtualization using generic routing encapsulation (No. rfc7637).

[12] Davie, B., & Gross, J. (2012). A stateless transport tunneling protocol for network virtualization (STT). Mar, 5, 1-19.

[13] Transier, M., Füßler, H., Widmer, J., Mauve, M., & Effelsberg, W. (2004). Scalable position-based multicast for mobile ad-hoc networks. BroadWim.