TELKOMNIKA, Vol. 11, No. 9, September 2013, pp. 5011~5017
ISSN: 2302-4046

Research on Remote Network Bidirectional Detect and Control Model

Hongyao Ju*[1,a], Xin Wang[2,b], Fei Luo[3,c]
[1]Zhejiang Textile & Fashion College, Ningbo 315211, P.R.China
[2]Department of Information Engineering in Zhejiang Textile & Fashion College, Ningbo 315211, P.R.China
[3]Sichuan Anmeng Information Safety Ltd , Ningbo Branch Company, Ningbo 315000, P.R.China
*Corresponding author, e-mail: juhongyao@163.com[a], wangxin_02@sohu.com[b], luofei@anmeng.com.cn[c]

Abstract

Remote network bidirectional detect and control technologies are the key factors to solve local network allopatry expansibility and management. With studying gateway integration technology, bidirectional VPN technology, identity authentication technology and dynamic host management technology can be integrated into gateway. Thus, bidirectional connect and control among allopatry local networks based on Internet can be solved. Whole area expansibility of local network is realized. With experiment, the model is proved to finish remote bidirectional interconnection of local network automatically and to obtain allopatry local users authority. The equipment detecting and controlling in remote local networks are realized.

Keywords*: remote network, bidirectional detect and control, VPN technology, identity authentication, dynamic host*

1. Introduction

With the development of network technology, more and more people pay attention to communication and control technology research based on network, especially in the high speed rail transit and aerospace area. To realize ultra long distance expansibility of local network coverage area has more important significance to solve working condition detect, parameter adjustment and control of locomotive, spacecraft and so on devices which are in the local network [1-3]. Therefore, how to find a kind of feasible technology to solve local network to realize ultra long distance expansibility, to realize bidirectional remote data acquisition and to control remote device is the problem to be solved. With studying bidirectional interconnection and integration technology of local network, in the paper, a kind of remote network bidirectional detect and control model is given [4-6]. How to realize the model is solved at the aspect of technology. The model solves remote data detect and equipment control problems during the period of the railway locomotive and aircraft maintenance. Thus, railway locomotive and aircraft can be maintained anywhere.

2. Remote Network Bidirectional Detect and Control Model

The model includes three parts, which are internet, regional network A and regional network B [7-8]. Where internet based on tunnel technology realizes secure connection channel between local network A and local network B which are in different regional to process same or different application software about detecting and controlling. The regional networks can be connected to Internet with integration gateway [9]. The integration gateway including three parts which are identity authentication unit, VPN route unit and dynamic host management unit is connection device between local network and Internet. Remote network bidirectional detect and control model structure is as following Figure 1.

Received February 17, 2013; Revised May 31, 2013; Accepted June 14, 2013

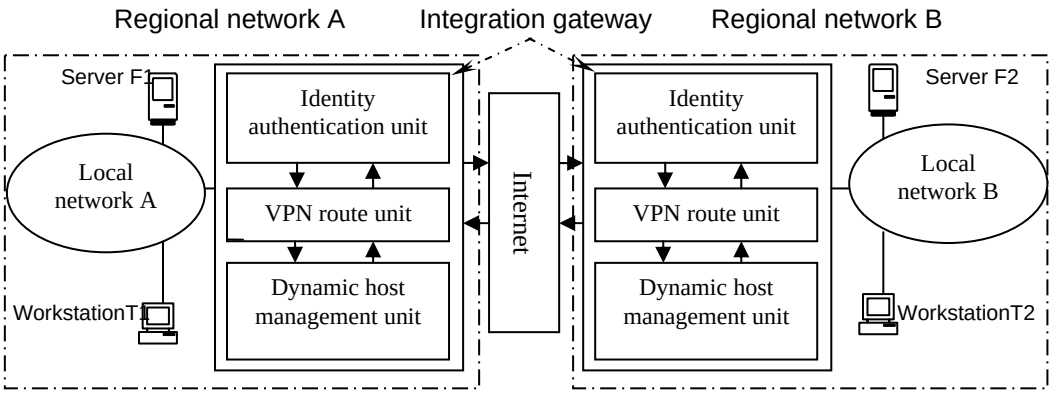

Figure 1. Remote Network Bidirectional Detect and Control Model

3. Remote Network Bidirectional Detect and Control Mechanism

3.1 Identity Authentication Unit

Identity authentication service is based on identity authentication unit [10-12]. The identity authentication is to take local authentication strategy. After integration gateway receives connection request which is sent by internet, firstly, user name and password are refined and local user information database is selected. If user identity of connection request is detected to be correct, the connection request is accepted and the resource right is authorized to the connection user. Authorities including IP address which is rent by user, dial-up network rights and control rights are realized. Otherwise, the authorities are refused. Identity authentication mechanism model is as following Figure 2:

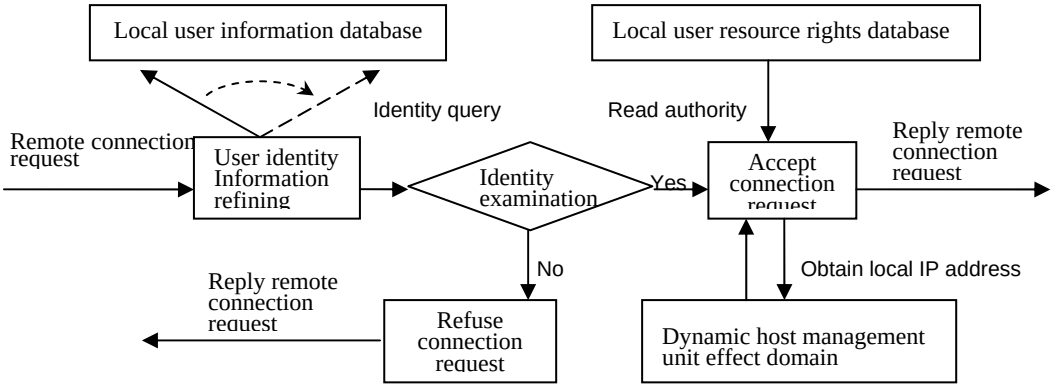

Figure 2. Identity Authentication Mechanism Model

3.2 VPN Route Unit

VPN route unit is to take tunnel technology to connect allopatry local network based on internet [13-15]. To take tunnel technology among the allopatry local networks is to realize bidirectional automatic dial-up connection. The working mode is as following Figure 3:

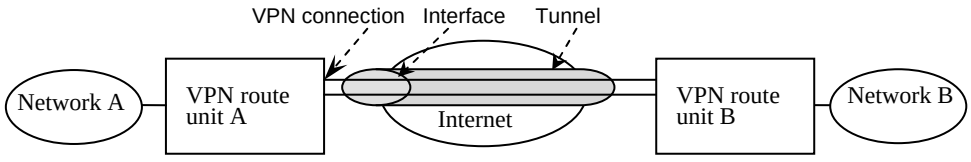

Figure 3. Two Special Network VPN Connection Model

VPN route unit is to take local user account information to realize dialing-in, identity authentication evidence and to take remote user account information to realize dialing-out evidence. Therefore, in each response VPN route unit, calling party identity authentication evidence is included. The consistency of identity authentication evidence is realized with consistency between response VPN route unit interface name and calling party user account name. That means when VPN route unit connection interface is created, at the same time, the user account with interface same name in local network is created. The account is remote VPN route unit to start connection request dialing-out evidence, and is local VPN route unit dialing-in identity authentication evidence. The user account includes starting and receiving dialing-up connection authentication. Route from local network to remote network is configured in each VPN route unit. Dialing-out evidence and dialing-in evidence of VPN route unit are stored in the local user information database and bound with user resource rights. VPN route unit connection process is as following Figure 4.

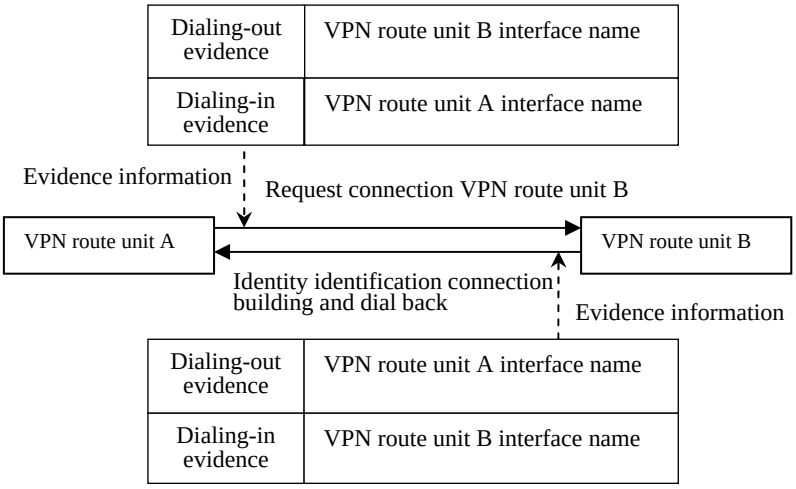

Figure 4. VPN Unit Connection Building Process

3.3. Dynamic Host Management Unit

Dynamic host management unit is to realize remote connection user to distribute local TCP/IP working parameters, which include IP address, subnet mask, default gateway and preferred DNS server address. With taking valid domain, the unit can manage TCP/IP parameters. After remote connection request is authenticated, valid domain begins to query parameter database immediately and chooses spare IP address. The IP address and other parameters can be sent to request connection user and user receives the group of parameters. If request connection user accepted the group of parameters successfully, renting confirmation message is sent to valid domain. To propose request connection user IP address is marked in valid domain. The IP address can not be used to rent other user until the user doesn't stop to rent the IP address. If user renting IP address failed, valid domain can not mark the IP address. The IP address can be used to other users. Dynamic renting process of TCP/IP parameters is as following Figure 5.

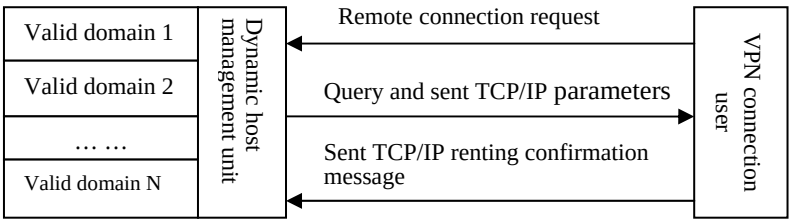

Figure 5. TCP/IP Parameters Dynamic Renting Process

4. Testing

4.1. Testing Way

During the period of test, we construct two local network which can set one intergate gateway. Two intergate gateways are connected with Internet. The device being tested is connected to local network. Work parameters of equipment in one local network are set with other local network. We control to operate these parameters to test the model effectiveness.

4.2 Main Testing Equipments and Configue Parameters

Testing surroundings is constructed of regional network A and regional network B based on internet connection [16-19]. In each regional network, there is one integration gateway, one server F and one workstation T. The two regional network are connected into internet with themselves integration gateway. Integration gateway is based on double network cards server. The operation system is Windows server 2008. The server function includes DHCP server and DNS server. The IP address which is bound in the outside network card of integration gateway A is 172.18.14.42, the IP address which is bound in the inner network card is 192.168.1.6, DHCP valid domain IP address range in local network A is 192.168.1.10—192.168.1.20, subnet mask is 255.255.255.0, gateway is 192.168.1.6, DNS address is 192.168.1.6. The IP address which is bound in the outside network card of integration gateway B is 172.18.12.42, the IP address which is bound in the inner network card is 192.168.2.6, DHCP valid domain IP address range in local network B is 192.168.2.10—192.168.2.20, subnet mask is 255.255.255.0, gateway is 192.168.2.6, DNS address is 192.168.2.6. Each operation system in two regional network servers F is Windows server 2008. Operation system in the workstation T1 is Windows vista. IP address of server F1 operation system in local network A is 192.168.1.100. IP address in workstation T1 is 192.168.1.50. IP address of server F2 operation system in regional network B is 192.168.2.100. IP address in workstation T2 is 192.168.2.50.

4.3 Integration Gateway Configuration Step

(1) To start route and remote access, Firstly, choose dial-up connection remote network. Secondly, choose IP address automatic allocation.

(2) To create interface name in order to process request dial-up interface. Integration gateway A name is linenet2. Integration gateway B name is linenet1.

(3) To choose using VPN connection, VPN type is automatic choice.

(4) To input remote route IP address, here to input 172.168.12.42 in integration gateway A, and to input 172.168.14.42 in integration gateway B.

(5) Protocol and safety, to choose “route choosing IP data packet in the interface” and “to add a user account remote route to finish dialing-in ”.

(6) To configure remote network static routing, to input 192.168.2.0 in integration gateway A, to input 192.168.1.0 in integration gateway B, subnet mask is 255.255.255.0, jumping point numbers are 256.

(7) Inputting dialing-in evidence. To input “linenet2” in integration gateway A. To input “linenet1” in integration gateway B.

(8) Inputting dialing-out evidence. To input “linenet1” in integration gateway A. To input “linenet2” in integration gateway B.

(9) To add static routing. To add 192.168.2.0 in “linenet2” interface of integration gateway A. To add 192.168.1.0 in “linenet1” interface of integration gateway B. Subnet mask is 255.255.255.0. Jumping point numbers are 256.

(10) To create valid domain in integration gateway A and integration gateway B separately. the detail parameters are given in the testing surroundings.

5. Testing Contents and Results Analysis

Firstly, the testing instruction which is selected in server F2 of local network B is “systeminfo –s 192.168.1.6 –u administrator –p juhy123$%” to test gateway configuration information in local network A. Testing data is as follows Table 1.

The testing instruction which is selected in workstation T2 of local network B is “systeminfo –s 192.168.1.50 –u administrator –p juhy123$%” to test workstation T1 configuration information in local network A. Testing data is as follows Table 2.

Table 1. Configuration Testing Results in Integration Gateway of Server F2

Parameter name	Parameter information
System manufacturer	Hewlett-Packard
Processor	1 processor is installed [01]: x64 Family 6 Model 23 Stepping 10 GenuineIntel ~1603 MHZ
Total physical memory	4,094 MB
Available physical memory	3,422 MB
Netcard	2 NIC is installed [01]: Realtek PCIe GBE Family Controller IP address[01]: 172.18.14.42, [02]: fe80::ad12:a0e9:8f04:2e82 [02]: D-Link DFE-530TX PCI Fast Ethernet Adapter (rev.C) IP address[01]: 192.168.1.6, [02]: fe80::5d65:8a53:a54b:f20a

Table 2. Configuration Testing Results of Workstation T1

Parameter name	Parameter information
System manufacturer	Hewlett-Packard
Processor	1 processor is installed [01]: x64 Family 15 Model 4 Stepping 1 GenuineIntel ~2793 Mhz
Total physical memory	2,047 MB
Available physical memory	1,634 MB
Netcard	1 NIC is installed [01]: Realtek RTL8139/810x Family Fast Ethernet NIC IP address[01]: 192.168.1.50, [02]: fe80::f541:62fd:ab5c:fe61

With testing instruction in local network B and testing results in the Table 1 and Table 2, we can observe hardware type information in integration gateway of local network A, and obtain hardware working situation parameters. That means local network B can finish remote detecting function in local network A and can obtain suitable authorization in local network A.

Secondly, the testing instruction which is selected in server F1 of local network A is “driverquery –s 192.168.2.6 –u administrator –p juhy123$%” to test driver information of integration gateway F2 in local network B. Testing data is as follows in Table 3.

The instruction which is selected in workstation T1 of local network A is “driverquery –s 192.168.2.50 –u administrator –p juhy123$%” to test driver information of workstation T2 in local network B. Testing data is as follows in Table 4.

Table 3. System Driver Information Testing Results in Integration Gateway of server F1

Module name	Screen name	Driver program type	Link date
ac97intc	Intel(r) 82801 Audio D	Kernel Dr	2005/9/17 2:30:29
ACPI	Microsoft ACPI Driver	Kernel Dr	2008/1/19 13:32:48
adp94xx	adp94xx	Kernel Dr	2007/4/25 5:00:29
Adpahci	Adpahci	Kernel Dr	2007/5/2 1:29:26
adpu160m	adpu160m	Kernel Dr	2007/2/22 2:04:35

Table 4. System Driver Information Testing Results of Workstation T2

Module name	Screen name	Driver program type	Link date
1394ohci	1394 OHCI Compliant Ho	Kernel	2009/7/14 7:51:59
ACPI	Microsoft ACPI Driver	Kernel	2009/7/14 7:11:11
adp94xx	adp94xx	Kernel	2008/12/6 7:59:55
Adpahci	Adpahci	Kernel	2007/5/2 1:29:26
adpu320	adpu320	Kernel	2007/2/28 8:03:08

With testing instruction in local network A and testing results in the Table 3 and Table 4, we can observe driver type information in the integration gateway of local network B, and obtain hardware working situation parameters. That means we can finish remote detecting function from local network A to local network B and can obtain suitable user authorization in local network B.

Testing data which is produced by systeminfo instruction in local network A testing integration gateway and workstation T1 in local network B and by driverquery instruction in local network B tests integration gateway and workstation T2 in local network A is similar in the Table 1, Table 2, Table 3 and Table 4. To take ping instruction to test connection performance between F1 and F2, F1 and T2, T1 and F2, T1 and T2 can obtain wonderful response. Therefore, bidirectional detecting and control model can realize bidirectional detecting function.

Lastly, to take instruction "shutdown –s –m \\192.168.2.6" in server F1 of local network A tests system shutdown the integration gateway in local network B. The result is that there is "windows system will be shutdown during 1 minute" on the screen of integration gateway in local network B. After about 30 seconds, the integration gateway can be turned off successfully. With restarting integration gateway in local network A, to take instruction "shutdown –s –m \\192.168.1.6" in server F2 of local network B tests system shutdown the integration gateway in local network A, The result is that there is "windows system will be shutdown during 1 minute" on the screen of integration gateway in local network A. After about 30 seconds, the integration gateway can be turned off successfully. Testing results with Workstation T1 in local network A are same. Therefore, the bidirectional control function between local network A and local network B can be realized.

6. Conclusion

With studying bidirectional detect and control model and testing results analysis, we can draw following conclusion: (1) Bidirectional detect and control model among local networks is feasibility. The integration technology to be described in this paper can be realized successfully when we take the model based on Internet. The model can be applied to the field of large-scale industrial production to achieve unified management of the production branches in different regions. (2) Technologies to be adopted in this model are nature and the construction cost is low. Detect and control network to be build with this model can reduce construction funds significantly. (3) With comparing relevant papers, such as paper [5], [6] and [7], in the paper, by taking the patent technology which is owned by the author, the author solves the questions about interconnection, detect and control among each local network based on internet. Therefore, the technology is not only wonderful in the aspects of safety, practicability and generalization, but also important in the application research aspects of local network allopatry expansibility and remote detect and control. The model is used in railway locomotive and aircraft remote detecting and control areas especially.

Acknowledgements

This paper is supported by Natural Science Foundation of Zhejiang Province (Grant No.Y1101154) and Natural Science Foundation of Ningbo City (Grant No.2010A610128), China.

References

[1] Mao Pan, Jiangjun Jin, Jicheng Cheng. Theory and Application of City Information Process. Beijing: Electronics Industry Publications. 2006: 241-256.
[2] Tiezheng Huai. Outlet and Countermeasure in China - Information Technology. Beijing: Machinery Industry Publications. 2006: 228-233.
[3] Rui Wang, Weihua Gu, Yong Jiang. Enterprise Information Requirements and Evaluation. Shanghai: Shanghai Science and Technology Publications. 2010: 87-97.
[4] Faizal Hajamohideen, Dr.umamaheshwari. Analysis Of Hybrid Academic Network Protocols. *Journal of Theoretical and Applied Information Technology*. 2010; 17(2): 55-103.
[5] Gui Yu. LAN Interconnection Based on VPN Technology. *Sichuan University of Arts and Science Journal (Natural Science Edition).* 2007; 17(2) :50-52.

[6] Fan Wang. Discussion on LAN Interconnection with VPN Technology. *Silicon Valley.* 2010; (15): 12-22.
[7] Lang Wang. Parts of the Corporate Library Link Each Other By Using VPN Technology. *Modern Library and Information Technology.* 2004; (5): 35-37.
[8] Hongyao ju, Xin Wang. Research on the Model of Intelligence Redundancy Gateway System. *Applied Mechanics and Materials.* 2013; 241-244: 1688-1693.
[9] Hongyao Ju. Research on the Framework of High Performance the Internet of Things Based on Multilevel Disaster Recovery. *Advanced Materials Research.* 2012; 542-543: 462-468.
[10] Ligang Han, Lihui Han, Wenbin Li. Windows Server 2008 Network Infrastructure. Beijing: Tsinghua University Publications. 2010: 345-381.
[11] Hongyao Ju. *A kind of Network Connection System with Compound Gateway*. CN202111731U (Patent). 2012.
[12] Xiaohui Liu, Cheng Huang. Network Instruction Management. Chongqing: Computer Newspaper Electronic Audio-Video Publications. 2009: 102-104.
[13] Muchou Wang, Weifeng Pan, Rongye Wang, Zhuxin Hu. Complex Algorithm Network and its Toplogy Analysis: A Case Study. *Journal of Theoretical and Applied Information Technology*. 2012; 46(1): 108-113.
[14] Ms T Sheela, Dr J Raja. Studies On The Performance Improvement Of Window Adjustment Procedure In High Bandwidth Delay Product Network. *Journal of Theoretical and Applied Information Technology*. 2008; 14(10): 931-936.
[15] WF Pan, B Li, YT Ma, J Liu. Multi-Granularity Evolution Analysis of Software Using Complex Network Theory. *Journal of Systems Science and Complexity*. 2011; 24(6): 1068-1082.
[16] QF Kong, FM Zeng, JC Wu, JM Wu. Design and Realization of Experimental Autonomous Driving System Based on Neural Network Control. *Applied Mechanics and Materials*. 2012; 241-244: 1953-1958.
[17] Guoqing Tian, Zhiyi Wang, Zhiguang Shen. Application of Intranet to Monitoring and Control Solar Hot Water Units. *Energy Engineering*. 2007; (2): 34-37.
[18] Cao Pan, JianTao, Hongyuan Wang. The Research of the Intelligent Device Management and Diagnostic. *TELKOMNIKA Indonesian Journa of Electrical Engineering*. 2012; 10(8): 1999-2005.
[19] Lijing Zhang, Wei Xiong, Xuehui Xian. Research on Web-based Real-time Monitoring System on SVG and Comet. *TELKOMNIKA Indonesian Journa of Electrical Engineering*. 2012; 10(5): 1142-1146.