Research Journal of Applied Sciences, Engineering and Technology 7(2): 221-226, 2014
DOI:10.19026/rjaset.7.244
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: March 11, 2013 Accepted: April 08, 2013 Published: January 10, 2014

Research Article

A Novel Solution based on NAT Traversal for High-speed Accessing the Campus Network from the Public Network

[1, 2]Meng Liu, [1]Bing Liu, [1]Jie Liu and [1]Meng Du
[1]School of Mechanical, Electrical and Information Engineering,
Shandong University, Weihai, Weihai 264209, China
[2]Computer Application Research Center, Harbin Institute of Technology
Shenzhen Graduate School, Shenzhen 518055, China

Abstract: Chinese universities use the multi-outgoing exports to solve the problem of the traffic of bandwidth to the Internet for the campus network, but the world wide web servers in the campus network might still be accessed very slowly by some users outside the campus network (from the public network). We discuss and analyze the reasons for slowly accessing to the campus network form the public networks and a novel solution for high-speed accessing to the campus network for the local client in public network is put forward. We first introduce an NAT (Network Address Translation) traversal approach based on reverse TCP (Transmission Control Protocol) connection, which has the advantage of not requiring any intermediary server. We test our NAT traversal approach in real network environment and the results show that it is effective. Meanwhile, we also test the network performance between the campus network and the local public network after the NAT Router between them has been traversed by our approach and the results show that the network performance by the second export accessing to the campus network is much better than by the campus network export.

Keywords: Campus network, multi-outgoing exports, NAT traversal, reverse connection

INTRODUCTION

In early times Chinese university campus network accessed the Internet through the CERNET (Chinese Education and Research Network). But with the users of the campus network are more and more, the network export bandwidth to the CERNET has not satisfied the corresponding actual requirements. Especially it is very slow to visit the public network such as ChinaNet, sometimes the access speed is too slow to be intolerable. So some universities upgrade their links to the Internet. They increase a new 155 M fiber link or upgrade the link to 1 G. And now the access bandwidth of CERNET backbone to the Internet cannot follow the development of the whole CERNET, the access speed to the public network would be still so slow. So some universities increase the second or the third access link offered by the local ISP (Internet Service Provider), such as China Telecom or China Unicom, to the Internet. For distributing users' accessing to the Internet, some universities all take the following policies:

- If one computer in the campus network would access the CERNET resources, the data will still go through the primary access export of the CERNET network because it is fast to access the resources in the education network via the access link to the CERNET.
- If it would access the resources in the public network (outside the CERNET), the data will go through the second new export to the local public network offered by the local ISP. So the access speed to the Internet is improved greatly.

There are three key technologies to carry out the above solution. They include Routing, NAT technology and Policy-Based Routing (PBR) technology (Zhuang, 2004):

- Routing can solve the problem that whether the data to go through the CERNET export or the second new export according to the destination IP address.
- NAT technology can finish Network Address Translation in the case of not changing the structure of the campus network and altering the client network configuration when one computer accessing the public network via the second new export.
- When accessing WWW (World Wide Web), FTP (File Transfer Protocol), E-MAIL services in the

Corresponding Author: Meng Liu, School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai, Weihai 264209, China

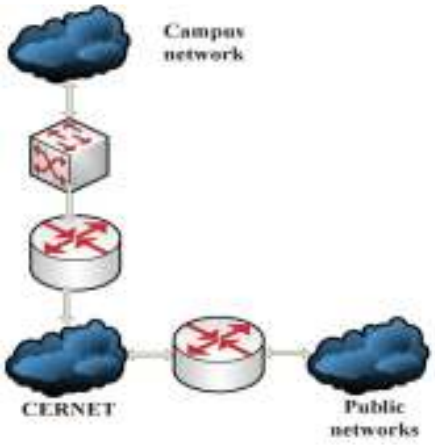

Fig. 1: Traditional single export campus network

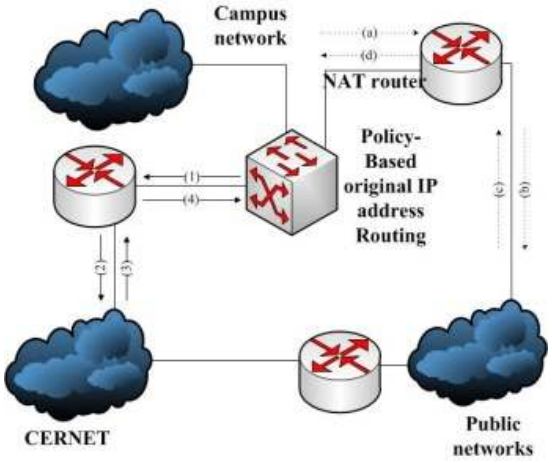

Fig. 2: A dual-export campus network

campus network from the outside networks by one computer in the CERNET or the public network, the data should go through the CERNET access port and Policy-Based Routing technology can guarantee that the campus network services can be normally accessed.

Problem description: The traditional single export campus network is shown in Fig. 1. All networks outside one campus network including the CERNET and the public network can be accessed via the single export to the CERNET. A classical dual-export campus network is shown in Fig. 2. These computers without policy-based routing in the campus network can access to the CERNET along the path of $(1)\rightarrow(2)\rightarrow(3)\rightarrow(4)$ and can access to the Internet outside the CERNET along the path of $(a)\rightarrow(b)\rightarrow(c)\rightarrow(d)$. So the access speed to the Internet is improved greatly.

In order to continue to provide the network services, such as WWW services, E-mail services, FTP services and so on for the campus network, some IP addresses inside the campus network must be set the

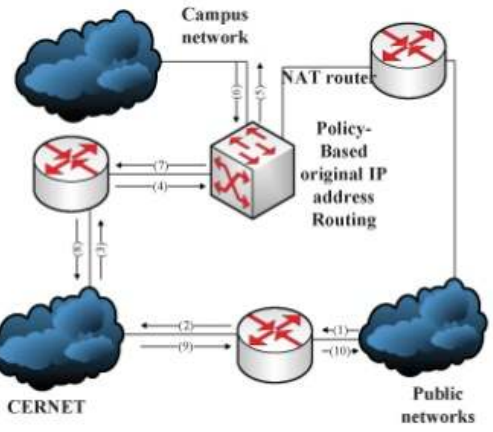

Fig. 3: A path to the campus network when access to a server with the PBR

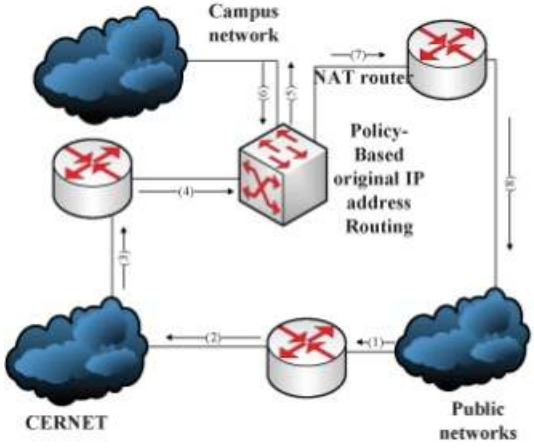

Fig. 4: A path to the campus network when access to a server without the PBR

Policy-Based original IP address Routing. Otherwise, the servers cannot be accessed outside the CERNET. According to Fig. 3, the computers outside the CERNET can access to the campus network along the path of $(1)\rightarrow(2)\rightarrow(3)\rightarrow(4)\rightarrow(5)\rightarrow(6)\rightarrow(7)\rightarrow(8)\rightarrow(9)\rightarrow(10)$. And the computers inside the CERNET can access to the campus network along the path of $(3)\rightarrow(4)\rightarrow(5)\rightarrow(6)\rightarrow(7)\rightarrow(8)$. When one computer would access to the CERNET and the public network, it is the same as the traditional single export campus network in Fig. 1.

According to Fig. 4, if IP addresses inside the campus network is not set the Policy-Based original IP address Routing, the connection response (8) will be dropped by the computer accessing the server because the original IP address and the port can be modified by the NAT Router in the second export of the campus network.

Now, we introduce a new question. For the servers with policy-based routing, it is an important issue that the solution of multi-outgoing exports mentioned above

only increase the speed of the campus users accessing to the external network, but still cannot solve the slow speed of the external public network accessing to the campus network according to Fig. 3. Furthermore, the computers outside the CERNET cannot directly access to the computer without the PBR in the campus network according to the previous discussion in Fig. 4. Based on the above issues, a better target is given as follows: The computers without policy-based routing in the campus network can also provide services to the users outside the CERNET, i.e., the inbound and outbound packet are through the second export while the users outside the CERNET accessing to the campus network. According to our understanding of NAT and knowing how it works, we can get a simple solution to achieve the goal. The NAT router in the second export can be configure NAT port mapping or directly IP address mapping to the IP address of the computer accessed in the campus network and then the users in the public network can access the computer in the campus network with the IP global external address of the NAT router. But we must request the Campus network administrator to do it. In this study, we introduce a solution to achieve the same goal but without NAT mapping. According to the characteristics of the multi-outgoing-export campus network, we use reverse TCP connection to solve the problem of NAT traversal, then the users outside the CERNET, particularly those users who use their local ISP accessing to the campus network, can directly access to the campus network based on Virtual Private Network technology (VPN) and can also get a high-speed access.

NAT traversal of the campus network: Before one user in the public network can access to the computers without the PBR in the campus network, NAT traversal of the NAT Router box in the second export of the campus network had to be finished. The computers without the PBR in the campus network are surely behind NAT in the second export, NAT type is likely to be one of Full Cone NAT, Restricted Cone NAT, Port Restricted Cone NAT, Symmetric NAT (Egevang and Francis, 1994; Tsirtsis and Srisuresh, 2000; Rosenberg *et al*., 2003). The local client in the public network can also be behind NAT box, but we only considered those local clients that have their own global IP address in this study.

The traditional NAT traversal using reverse TCP connection needs an intermediary server in the Internet which must has an own global IP addresses. It can be accessed by both of the two ends of the NAT traversal to determine their NAT type and NAT TCP Characteristics based on some mature technology, e.g., STUNT (Simple Traversal of UDP Through NATs and TCP too) (Guha *et al*., 2004; Guha and Francis, 2005; Guha, 2004; Jennings, 2007). The STUNT server can also be used to complete TCP NAT traversal. It can help both of the computers get IP and port information

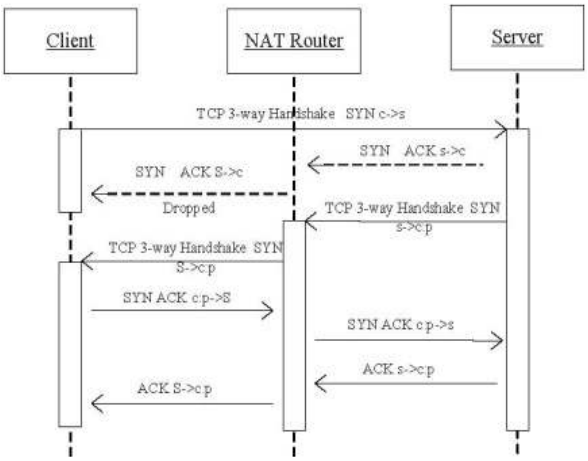

Fig. 5: TCP NAT-traversal approach

and transmit the needed information each other. According to the characteristics of the multi-outgoing-export campus network, we propose a better solution of NAT traversal using reverse TCP connection not requiring any STUNT server. The computer accessed in the campus network will act as an intermediary server by itself. The client computer in the public networks, as an initiator, takes the initiative to access to the server in the campus network. We assume that the global IP address of the computer server accessed in the campus network is s, the client IP address is c, the global external IP address of the NAT router in the campus network is S. The Port p is bound to the IP c of the client computer. We use UML sequence diagram to describe the solution of NAT traversal.

The TCP NAT traversal is illustrated in Fig. 5. Firstly, the client sends out an initial connection request to s, the global IP of the server. Then the connection request will arrive at the server along the path $(1)\rightarrow(2)\rightarrow(3)\rightarrow(4)\rightarrow(5)$ in Fig. 4, then the connection response will be transmitted along $(6)\rightarrow(7)\rightarrow(8)$ and the response packet will be dropped by the client because of the source IP and port of the response packet with SYN (Synchronize) and ACK (Acknowledge) flag is modified by the campus NAT Router box, i.e., the TCP 3-way shake of the connection will be unsuccessful. But the connection request is very important to our TCP NAT-traversal approach and the server can get the IP address information of the client according to the packet with SYN flag of the connection request. Secondly, the server can send out a new connection request to c. the IP address of the client. The connection will be successful and the reverse TCP NAT traversal will be also completed. Then the server and the client can communicate each other with the successful connection.

EXPERIMENTS AND RESULT ANALYSIS

We test the TCP performance for some fact cases using Iperf on Windows XP. There are two cases in our

Table 1: Route path with policy-based routing during a busy period

Tracing route to www.whinfo.net.cn [61.156.23.16] over a maximum of 30 hops:				
1	<1 ms	<1 ms	<1 ms	219.231.160.126
2	1 ms	1 ms	1 ms	202.194.40.133
3	10 ms	10 ms	10 ms	202.194.99.229
4	9 ms	9 ms	9 ms	202.112.53.21
5	9 ms	9 ms	9 ms	202.112.61.25
6	15 ms	15 ms	15 ms	202.112.36.137
7	15 ms	15 ms	15 ms	202.112.62.50
8	126 ms	125 ms	126 ms	219.158.34.201
9	126 ms	121 ms	122 ms	219.158.11.101
10	97 ms	98 ms	98 ms	219.158.96.30
11	89 ms	117 ms	240 ms	60.217.40.126
12	239 ms	254 ms	262 ms	60.215.131.214
13	225 ms	222 ms	220 ms	221.2.132.138
14	249 ms	253 ms	250 ms	61.156.24.116
15	244 ms	236 ms	235 ms	61.156.23.16

Table 2: Route path with policy-based routing during a quiet period

Tracing route to www.whinfo.net.cn [61.156.23.16] over a maximum of 30 hops:				
1	<1 ms	<1 ms	<1 ms	219.231.160.126
2	1 ms	1 ms	2 ms	202.194.40.133
3	10 ms	10 ms	10 ms	202.194.99.217
4	9 ms	10 ms	9 ms	202.112.53.21
5	9 ms	9 ms	9 ms	202.112.61.25
6	16 ms	17 ms	16 ms	202.127.216.5
7	15 ms	15 ms	15 ms	202.112.62.50
8	45 ms	46 ms	47 ms	219.158.34.197
9	50 ms	50 ms	52 ms	219.158.11.113
10	73 ms	75 ms	73 ms	219.158.10.114
11	70 ms	70 ms	71 ms	60.215.136.50
12	60 ms	65 ms	63 ms	60.215.131.214
13	65 ms	64 ms	53 ms	221.2.132.138
14	51 ms	51 ms	53 ms	61.156.24.116
15	66 ms	67 ms	69 ms	61.156.23.16

experiments and each of them is done during different period.

Case (1): One computer runs in the local ISP network and one computer with policy-based routing runs in the campus network.

The computer in the campus network has been set with policy-based routing. So the route path is along (1) $\rightarrow$ (2) $\rightarrow$ (3) $\rightarrow$ (4) $\rightarrow$ (5) $\rightarrow$ (6) $\rightarrow$ (7) $\rightarrow$ (8) $\rightarrow$ (9) $\rightarrow$ (10) in Fig. 3. And in this case we test during two periods. The first test is done during a quiet period on the network before 7:00 a.m. and the second test is done during a busy period on the network between 2:00 and 5:00 p.m.

Case (2): One computer runs in the local ISP network and one computer without policy-based routing runs in the campus network.

So the route path is along (a) $\rightarrow$ (b) $\rightarrow$ (c) $\rightarrow$ (d) in Fig. 2. The same two tests are done during a quiet and busy periods.

Firstly, we run Tracert on the computer with policy-based routing in the campus network to get the route path to one server in the local ISP network for the first case during a quiet period and a busy period. The results are shown in Table 1 and 2.

Table 3: Route path without policy-based routing during a busy period

Tracing route to www.whinfo.net.cn [61.156.23.16] over a maximum of 30 hops:				
1	<1 ms	<1 ms	<1 ms	219.231.160.254
2	<1 ms	<1 ms	<1 ms	10.0.0.2
3	<1 ms	<1 ms	<1 ms	221.2.163.225
4	1 ms	<1 ms	<1 ms	221.2.132.57
5	1 ms	1 ms	1 ms	221.2.132.138
6	<1 ms	<1 ms	<1 ms	61.156.24.116
7	1 ms	1 ms	<1 ms	61.156.23.16

In contrast, we also run Tracert on the computer without policy-based routing in the campus network to get the route path to one server in the local ISP network for the second case. The result is shown in Table 3.

Obviously, in the first case both of the route path are longer than the second case during a busy or quiet period. Likewise, the Round Trip Times (RTT) of Time Exceeded ICMP Message in the first case is much longer than in the second case. In the first case of the CERT export, the RTT is about 200 ms during a busy period and about 70 ms during a quiet period, but it is smaller than 1 ms in the second case of the second export (the local ISP export) during a busy period, so we can consider it is more smaller during a quiet period.

According to the following TCP throughput calculation formula:

$$Max\ TCP\ throughput = max\ TCP\ Window\ size / RTT,$$

Window systems have 64 KBytes of window size as default, so the max TCP throughput is about 2.5 Mbits/sec in the first case during a busy period and is about 7 Mbits/sec in the first case during a quiet period. Assume that RTT is 1 ms in the second case, the max TCP throughput could be about 512 Mbits/sec in theory.

We set the iperf's parameter, the length of buffer to write, to '8 K', '16 K', '32 K', '64 K', '128 K', '256 K', '512 K', '1 M', '2 M', '4 M' to test the TCP performance. And based on different parameter value, we test ten times for case (1) and case (2) during one quiet period and one busy period, respectively. We compute the average TCP performance for 10 times tests and the results are shown in Fig. 6. We can know that the test results are consistent with the calculated result according the TCP throughput calculation formula in the first case. Because the network Bandwidth of our selected computer in the local ISP network is 20 Mbits/sec, the test results of the second case are also reasonable when considering some other factors.

We notice several distinct conclusions:

- The TCP performance in case (1) during the quiet period is better than the busy period.
- The TCP performance in case (2) during the quiet period is almost as good as the busy period.

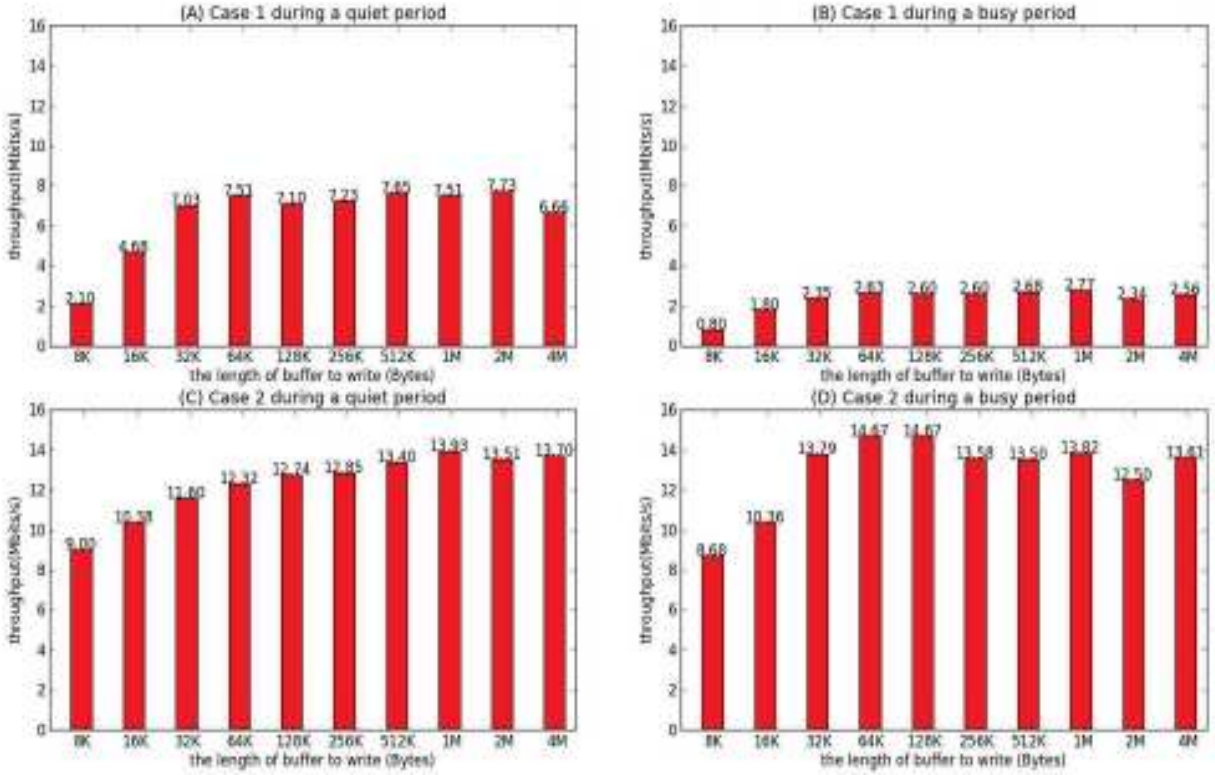

Fig. 6: Average TCP performance with different buffer size

- The TCP performance in case (2) during any period is much better than case (1) during the busy period.
- The TCP performance in case (2) during any period is better than case (1) during the quiet period.

So according to Table 1, 2 and Fig. 6, we can draw the conclusion that the network performance of accessing to the campus network by the second export was better than by the CERNET export. And the better TCP performance can be achieved while the length of buffer to write is about 256 KBytes.

CONCLUSION AND RECOMMENDATIONS

Though some universities in China use the multi-outgoing exports to solve the problem of the traffic of bandwidth to the Internet for the campus network, but the speed for accessing to one server in the campus network is still very slow for the client in the public network, especially during a busy period. This study has presented an approach to achieve NAT traversal of the second export NAT Router in the campus network not requiring any STUNT server by reverse TCP connection. After the second export NAT Router has been traversed, we tested the TCP performance between the campus network and the local public network by the second export. In contrast, we also tested the TCP performance by the CERNET export. The experiment results have shown that the network performance of accessing to the campus network by the second export was better than by the CERNET export. So our solution is effective. A future work is that how to implement easy communication between the client in the local public network and the server in the campus network. A workable solution is that TCP tunnel (Liu *et al*., 2012) based on our NAT traversal can be established between the campus network and the local public network via the second export and any application layer traffic based TCP or UDP can be allowed through the TCP tunnel.

REFERENCES

Egevang, K. and P. Francis, 1994. The ip Network Address Translator (NAT). Retrieved from: http://tools.ietf.org/html/rfc1631.

Guha, S., 2004. Stunt-simple traversal of udp through nats and tcp too. Work in progress, IETF Network Working Group, December 2004. Retrieved from: URL http://nutss.gforge.cis.cornell.edu/pub/draft-guha-STUNT-00.txt.

Guha, S. and P. Francis, 2005. Characterization and measurement of tcp traversal through nats and firewalls. Proceeding of the 5th ACM SIGCOMM Conference on Internet Measurement. USENIX Association, Berkeley, CA, USA, pp: 199-211.

Guha, S., Y. Takeda and P. Francis, 2004. NUTSS: A SIP-based approach to UDP and TCP network connectivity. Proceeding of the ACM SIGCOMM Workshop on Future Directions in Network Architecture, ACM Press, New York, USA, pp: 43-48.

Jennings, C., 2007. Internet draft: Nat classification test results draft-jennings-behave-test-results-04.

Liu, M., B. Liu, J. Liu and M. Du, 2012. A virtual private network solution for dual-export campus network. J. Inform. Comput. Sci., 9(16): 4953-4960.

Rosenberg, J., J. Weinberger, C. Huitema and R. Mahy, 2003. Stun-simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATS). Retrieved from: http://dl.acm.org/citation.cfm?id=RFC3489.

Tsirtsis, G. and P. Srisuresh, 2000. Network Address Translation-Protocol Translation (NAT-PT). Retrieved from: http://www.ietf.org/rfc/rfc2766.txt.

Zhuang, Y., 2004. Applying the policy based routing technology in multi-exports campus network. Comp. Syst. Appl., 13(6): 54-57.