The network test tools based on SDN

Song Yang (杨 松)[1,2*], Xiaoguang Zhang (张晓光)[1,2], Lixia Xi (席丽霞)[1,2], and DongHe Zhao (赵东鹤)[1,2]

[1]*State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[2]*Institute of Information Photonics and Optical Communication, Beijing University of Posts and Telecommunications, Beijing 100876, China*

**Corresponding author: y14681@sina.com*

Received October 1, 2013; accepted October 13, 2013; posted online February 28, 2014

Based on Software defined network (SDN), we brought up the NetWork Test Tools for communication networks. It is an innovative application of SDN, which can support the application traffic test.

OCIS codes: 060.4250060.4510.

doi: 10.3788/COL201412.S10602.

OpenFlow[1] is an open standard based on SDN that provides a set of standardized software interfaces to control packets routing and forwarding. It can achieve its realization by hardware. The essence of OpenFlow can be concluded as follows: 1) An Openflow switch separates the two functions (fast packet forwarding and high-level routing decisions) of a classical router or switch into OpenFlow Switch and OpenFlow controller; 2) Switch the "Optimization of one node" to the "Optimization of all"; 3) Concentrical management and standard interfaces make maintenance easier and the efficiency of synchronization higher. For now, OpenFlow already has many applications—for example, Packet and Circuit Network Convergence with OpenFlow[2].This paper is an enhancement of the application traffic test based on SDN, as we have made the test tools a NetWork, which is an innovation of SDN and OpenFlow. The improvement we made here is to connect large number of equipments and hand them over to one Controller, which forms our NetWork Test Tools, service users and equipments under tests can be easily accessed to. The main functions that NetWork Test Tools provide include the following: 1) Providing different networking environment according to test requirement; 2) WEB access for users to sign their tasks; 3) Controller asks the virtual machine to configurate resources according to demands and analysis into mini-tasks then boot ontest equipments; 4) Virtual machines report resource usage and test index to the controller, and the controller adjusts resources to achieve the highest efficiency with minimum resources; 5) Test dispatch and results report.

The NetWork test tool software platform (Fig. 1) includes the following: 1) Maintenance platform mainly provides routine monitoring of optical network physical parameters, online monitoring, failure awareness, network planning; 2) Protocol fuzzy test and telecommunication scenario performance test, we designed Network stream engine (NSE) tools module; 3) Environment (test bed) management platform; 4) Automation engine and hardware; 5) Extended development interface and third-parts integration engine.

The NetWork tools provide full-day automatic test service by providing automation interface. With test NetWork, service users only need to select the appropriate test protocol. The automation engine automatically extracts the task, requires environment, dispatches subtasks and accomplishes the corresponding tests and reports the results. Meanwhile, as test tools are added up to network under test, we can upgrade and monitor test tools in a centralized way, which leads to a higher efficiency of testing and maintenance. With syslog journal recording and TelNet management, we can easily debug when a problem occurs. The hardware is mainly based on servers or PCs (virtual machines). Each hardware with an OpenFlow control module and test engine runs under the controller's command (Fig. 2). For network test, the test bed management is very important. The test bed control module provides dynamic optical networks function. NetWork tools may run multiple test tasks at the same time, and each case with different scenario will be mapped to different devices in the bed. Since test beds consist of different communication equipments such as optical networks, switches and routers, if we organize test beds independently, the equipments resources will be tremendously wasted. The best way to solve this problem is to connect all the equipments to the switches (layer 1 or layer 2 switch) to form a big equipments-resource pool. On the stage of environment preparing, the equipments resources are dynamic networked and become non-interfering local network. It makes full use of equipments resources with reduced investment and high efficiency parallel execution of the cases.

The Tools provide the visual management of network system topology. Through dragging and automatic discovery, it can find all the nodes (Agent) in the NetWork quickly. Besides, the telemanagement function of appropriate agents can offer clients online monitoring of tested equipments and NetWork nodes, which is an excellent working experience for clients. The management software of the tools provide several functions for physical machine such as deployment, drag, zoom, search, filter, offline configuration and states' display. It can operate physical machine plug-in with start, stop, statistics gather, log viewer and graphic functions. With high-level automation control, it is very simple to do complex test with the NetWork tools. For complex

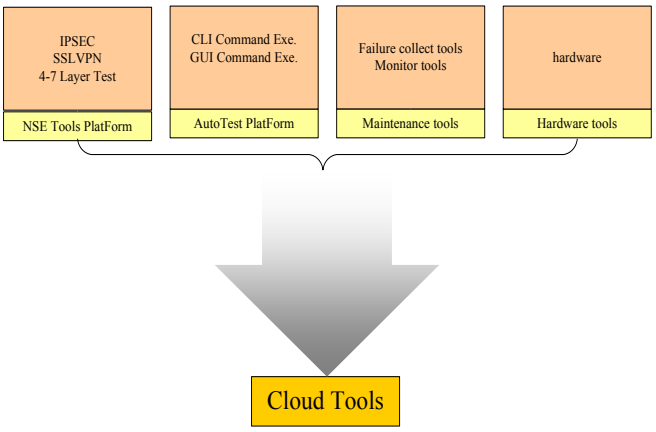

Fig. 1. Software platform of tools.

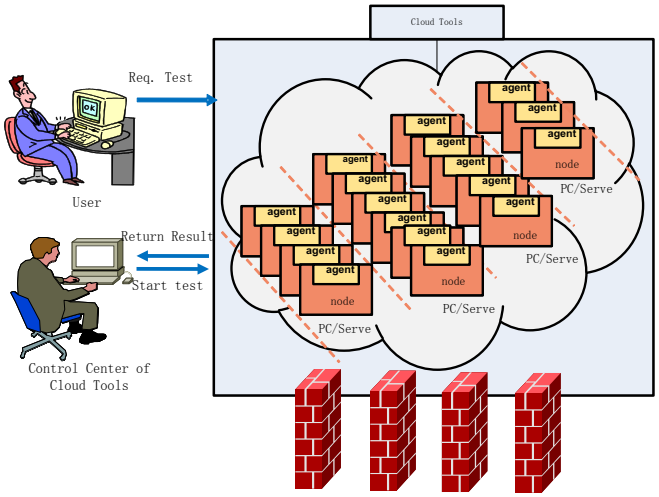

Fig. 2. Test topology of tools.

data traffic, different OpenFlow Agents need to be combined. For example, Tool IPSEC only provides IPSEC test function, and the data traffic only concludes HTTP, FTP, ICMP, UDP, TCP, testing range is confined. Through uncoupling, NSE can isolate application layer protocol from the functional module, which makes it easier to expand and form the function module block. By simply combining module blocks, complex data traffic can be clearly monitored. Here, we have two instances: 1) To config IPsec channel data traffic, the ability of monitoring complex data traffic can be achieved through checking corresponding protocol and traffic configuration; 2) To test the channel newly built http index, the only operation is to select protocols like IPSEC, L2TP and newly built http-index test packets.

Based on the mainly software parts Tools (Fig. 3), automatic engine and management platform, the Tools provide users' NetWork test services. Users log in Tools, sign in the test requests, then the Controller dynamically divides NetWork resources according to the ability of each NetWork node, which will boot on automation industry to sign off tasks. Once the tasks are accomplished, test results are fedback to users and occupied resources are released. For the data traffic monitoring of an equipment, only one NSE is needed to test Newly TCP connection and report back results. The hardware platform is designed in a card plug-in way, which can be used on a server or simply a PC's PCIE slot with all kinds of Interfaces (Fig. 4). If the test requires high speed or a complex network, multiple NSE nodes can be combined and making use of the stacking of high-performance server blades, since each blade can offer only 100–400 thousand newly linking ones. For example, if a network equipment requests 2.4–4.8 million new connection test, two 14-U server blades will be required.

Comment 1: ATCA Server, CPU:2.4GHz*8 cores, RAM:8G, Network interface: GE adapter with Intel chipset.

Comment 2: Professional hardware has GE and 10GE series. Data listed here are tested on 2*10GE card.

Description of testing function, VPN tunnel calltool is mainly used for VPN performance testing. By using VPN calltools, we can build a specific VPN application scenario quickly, such as plenty of users online, plenty of users offline, establishment of massive tunnel, load supporting of massive application data (HTTP, FTP, etc.) and so on. The entire tool supports distributed framework which means a control terminal supports multiple VPN Agents, up to 30.

VPN tunnelcall tool is composed of four parts: tool control, VPN Agent, VPN Server and Radius Server. A typical testnet working is shown in Fig. 5. Tool control mainly realizes the configuration and issue of the enduser parameters. VPN Agent mainly realizes the implementation of user configuration parameters. VPN Server mainly makes response to the application requests from the VPN Agent. Radius Server will be used only in some certain circumstances, such as IKEv2 + EAP test scenarios.

Tunneling Protocol, the latest version of SEAK, which supports the VPN tunnel negotiation protocols includes: L2TP over IPSec, IPSec uses IKE v1 negotiation, L2TP protocol, IKE v2 + EAP, IKE V2. Load data, VPN tunnel-testing tools supports the following application-layer protocol packets: Tunnel-carrying UDP datagram; tunnel-carrying ICMP packets; tunnel-carrying HTTP packets; tunnel-carrying TCP packets; tunnel-carrying FTP data packets.

It is mainly used to test the maximum total number of tunnels that are supported by the device under test (DUT). In this test scenario, the tester does not

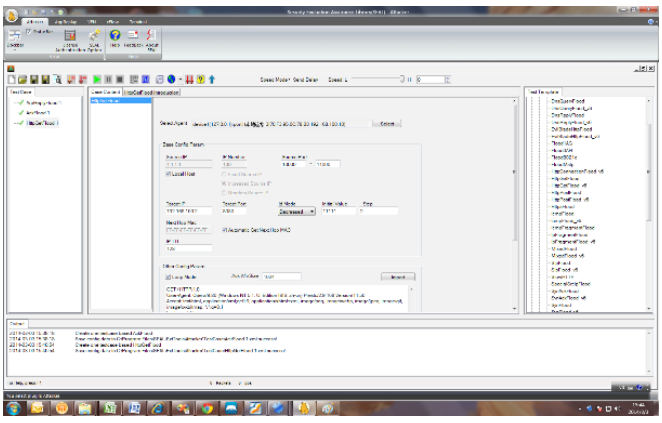

Fig. 3. Developed Tools NSE software.

Fig. 4. Developed Tools hardware.

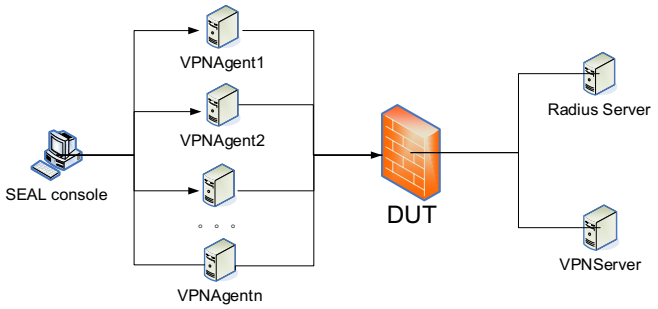

Fig. 5. Typical Network Testing.

care about the speed of the DUT renew, but focuses on whether its memory capacity can meet the test maximum number of tunnels' specifications or not. In the condition of maximum number of concurrent tunnels' working for the DUT, testers can improve the concurrent test capability of the tool by overlaying multiple VPN Agents. A typical tunnel concurrent test is shown in Fig. 6, where the testers carry out eight rounds of tests. The number of concurrent tunnels in the first round is 50, the second round is 100 and the eighth round is 5000, but only 4500 tunnels are successful. We can conclude that the character of concurrent tunnels cannot be more than 5000.

It is mainly used to test the number of newly built tunnel of the DUT. In this test scenario, the tester does not care about the concurrent performance of devices,

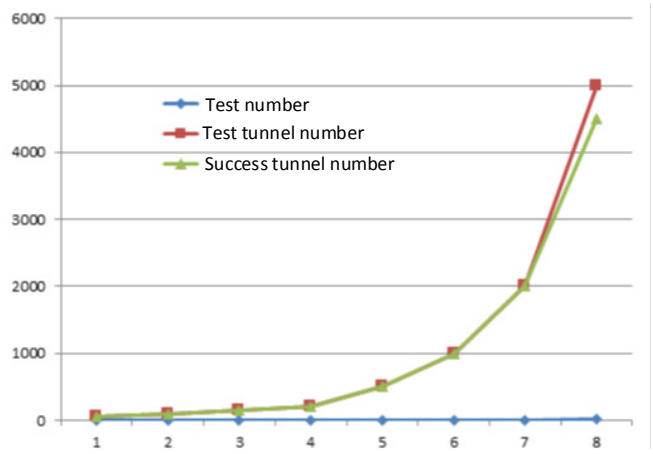

Fig. 6. Tunnel Concurrent Test.

but focuses on whether the CPU-processing ability can support the maximum performance of the new specifications or not. In the condition of new tunnel working for the DUT, testers can improve the new tunnel ability of the tool by overlaying multiple VPN Agents. Fig. 7 is a typical new test tunnel, the total number of concurrent tunnels is set to 4000, and testers carried out a total of eight tests. The new speed in the first round is 5, the second round is 10 and the eighth round is 300, but 4700 tunnels of them are successful. We can conclude that the character of new tunnels cannot be more than 300.

Tunnel abnormal is considered as the circumstances of tunnel negotiation or offline abnormality. The test is used to determine the exception handling capability and robustness of the DUT, mainly in the following cases: no down line, that is after the tunnel is on the line, it neither quits nor goes down. Go online and offline repeatedly, that is the tunnel is on the line, waiting for a specified time, and then goes off the line, and then again goes on the line, making a loop test. Real-time block on and off the line, that is a block of tunnels is on the line, waiting for a certain time, and then the block goes off the line, and then the block goes on line, making a loop test. Real-time on and off the line, that is each tunnel goes off the line immediately after it goes on the line, and then again on the line, making a loop test. In addition, in the different strategies of tunnel test, we can determine the packet loss and the working condition of the DUT via whether the tunnel configuration is normally removed in a current network environment. We can discover the

Table 1. Test Data in the Laboratory

Test Items	**ATCA Server(Comment 1)**	**Professional hardware(Comment 2)**
HTTP connections/second	100 thousand	400 thousand
HTTP concurrent connections	2 million	2 million
64 bytes UDP throughput	250 Mbps	10000 Mbps
IPSec negotiation(IKE v2)/second	65 connections/second	2000 connections/second
NetWork nodes managed	600 real nodes tested, 3000 simulated nodes tested	600 real nodes tested, 3000 simulated nodes tested

Table 2. Indicators of Ordinary PC Test Performance (100M network card)

Indicators of Ordinary PC test performance	**L2TP**	**L2TP OVER IPSEC**	**IKE V1**	**IKE V2**	**IKEV2 EAP**
Maximum concurrent connections	9000	7500	39000	60000	60000
Maximum connection rate (line/s)	50	30	50	50	50
Maximum UDP traffic (Mbps) Suggested tunnel number: 300	140	150	150	145	145
Maximum TCP traffic (Mbps) Suggested tunnel number: 300	135	130	130	130	130
Maximum HTTP traffic(Mbps) Suggested tunnel number: 300	135	130	130	130	130
Maximum FTP traffic(Mbps) Suggested tunnel number: 300	135	130	130	130	130

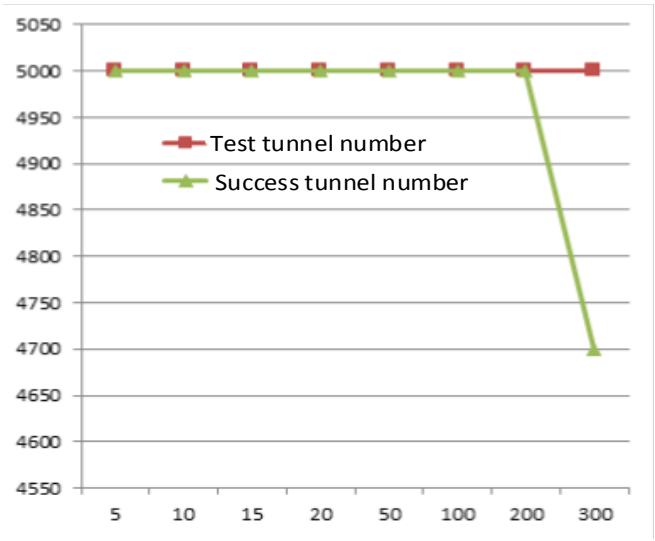

Fig. 7. Tunnel New Test.

underlying problems by applying this test, and thus we can improve the reliability and stability of the DUT.

The concept of SDN/OpenFlow is appropriate to the NetWork tools. Based on SDN/OpenFlow, we have developed the tools in telecommunication field. With this tool, we can do more research on efficient environment & task management (e.g., City network architecture simulates in seconds), high-speed OpenFlow hardware card, large scale of configuration extraction & combination (make the whole test investment lowest), dynamic test parameter adjustment (make the test efficiency highest), etc.

References

1. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, and J. Turner, J. ACM SIGCOMM Computer Communication Review, **38,** 69 (2008).
2. S. Das, G. Parulkar, N. McKeown, P. Singh, D. Getachew, and L. Ong, in *Optical Fiber Communication Conference*. OTuG1 (2010).