ALPS: A service model-based automatic network management system (experimental)

1. Background

1.1 Service Models in IETF

The purpose of network system configuration is to allow the deployment of services requested by customers across networks. Essentially, these services are built from a combination of network elements and protocol configuration. However, they are presented to service customers in a more abstract way.

To facilitate service automation control and configuration more automatic and much simpler, service models are proposed and specified in IETF to help customers express their service requirements as well as operators configure their networks per these requirements. Service Models are created to describe the characteristics of a service, as agreed upon with consumers of that service while Network Models describe the configuration, state data and operations of a network device as defined by the vendor of that device. The detailed explanation can be found in [1].

1.2 The Layer 3 VPN Service Model

The Layer 3 VPN service model is such a service model aimed to provide an abstracted view of a Layer 3 IP VPN service configuration components, which can be further broken down into specific Network Element data models to configure the involved network elements to perform the service.

As described in [I.D-ietf-l3sm-l3vpn-service-model], a typical usage is to use this model as an input for an orchestration layer who will be responsible to translate it to orchestrated configuration of network elements who will be part of the service. The network elements can be routers, but also servers (like AAA), and not limited to these examples. The configuration of network elements MAY be done by CLI, or by NetConf/RestConf coupled with specific configuration YANG data models (BGP, VRF, BFD ...) or any other way.

```
         L3VPN-SVC |
           MODEL   |
                   |
                +------------------+         +-----+
                |   Orchestration  | < --- > | OSS |
                +------------------+         +-----+
                   |            |
           +----------------+   |
           | Config manager |   |
           +----------------+   |
                   |            |
                   | Netconf/CLI ...
                   |            |
     +-------------------------------------------------+
                          Network

                        +++++++
                        + AAA +
                        +++++++

+++++++  Bearer ++++++++             ++++++++       +++++++
+ CEA + ------- + PE A +             + PE B + ----- + CEB +
+++++++  Cnct   ++++++++             ++++++++       +++++++

Site A                                       Site B
```

2. Experimental system: The ALPS

The ALPS system is a service model-based automatic network management system which implements the L3VPN Service Model defined in IETF L3SM Working Group to provide L3 VPN services for users. It can also be considered as a demonstration of L3SM work in IETF. More services models can be installed and implemented in this demo system to provide automatic service management for users.

The following depicts the architecture and components of the automatic management system, in which the main ALPS component acts as the Orchestrator and Config Manager described in [I.D-ietf-l3sm-l3vpn-service-model].

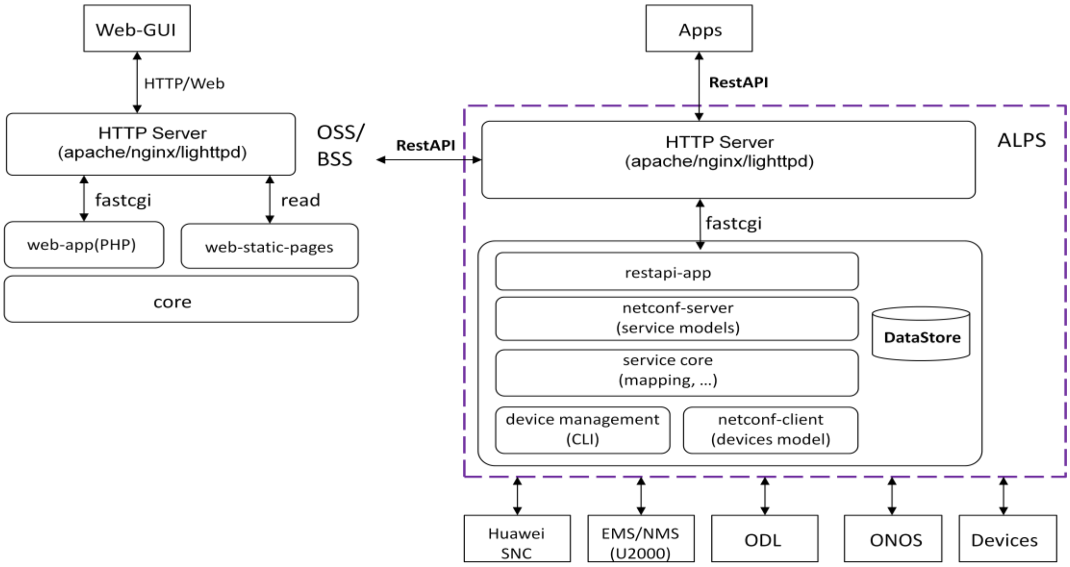


Figure 1 ALPS architecture and components

The ALPS system uses RESTCONF for applications to request services to networks. For Layer 3 VPN service users, the Layer 3 service model specified in IETF L3SM WG is used to request L3

VPN services over the network.

Upon receiving the service model, the orchestrator (that is ALPS component) then *maps* the L3SM model into models used to operate the network. The mapping is taking the description of the service and using the data to work out what to ask the network to do.
In the ALPS, the mapped results can be device models which can be deployed onto specific network nodes by using NETCONF. Alternatively, it can also be configuration data which can be configured on corresponding network nodes by CLI. For configuration by CLI, we use OVS and openflow to deploy the mapped confutation data derived from the L3 service model onto the network nodeds. The configured network nodes can be network devices, as well as network controllers (such as ODL Controller and ONOS Controller).

3. Simulation Examples

3.1 Network Topology

The following is the network topology for the simulation. Originally, the hosts are connected to the adjacent CEs (Customer Edge routers) but cannot exchange data among them since no configuration on network nodes, i.e. CEs and PEs (Provider Edge Router) in this case, yet.

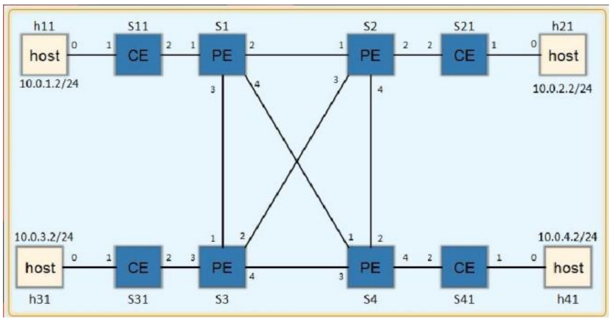
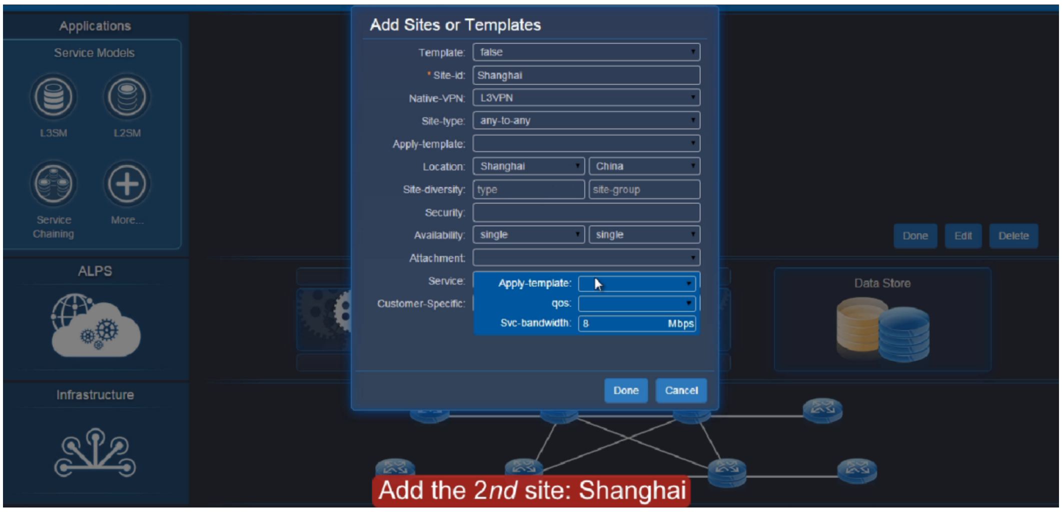


Figure 2 simulated network topology

3.2 L3 VPN service configuration in ALPS system

We use Layer 3 IP VPN service model developed in IETF as an example in the demo. With the Web GUI, we could add new sites into the network and configure requested L3VPN services between these sites. A snapshot of the configuration GUI is shown as below.



Add Sites or Templates

Template: false
* Site-id: Shanghai
Native-VPN: L3VPN
Site-type: any-to-any
Apply-template:
Location: Shanghai China
Site-diversity: type site-group
Security:
Availability: single single
Attachment:
Service: Apply-template:
Customer-Specific: qos:
Svc-bandwidth: 8 Mbps

Done Cancel

Add the 2*nd* site: Shanghai

Figure 3 Configuration GUI

For the demonstration, we add three sites (Nanjing, Shanghai and Shenzhen) into the network and configure the L3 VPNs among them to provide data exchange VPN service. The result is shown as in figure 5.

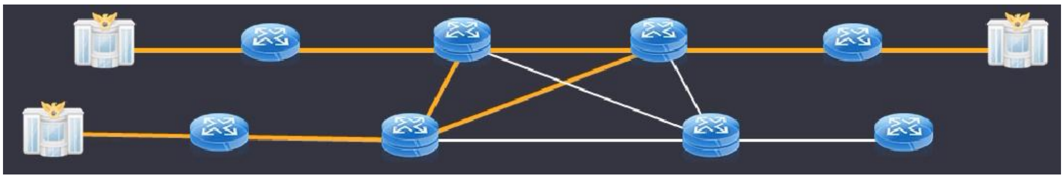
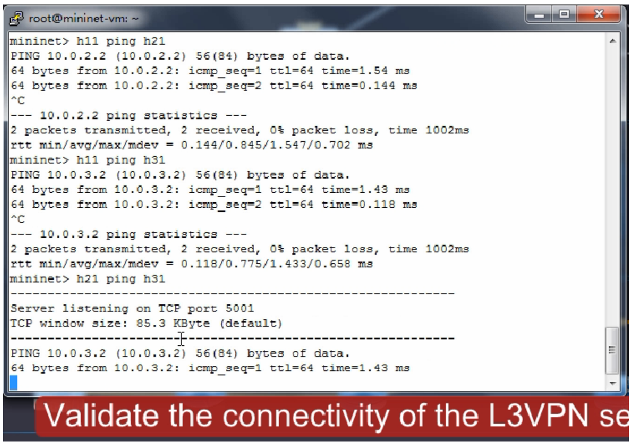


Figure 4 configured L3VPN example

3.3 L3VPN Connection validation

The validation of the configuration is shown as below.



```
mininet> h11 ping h21
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_seq=1 ttl=64 time=1.54 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=64 time=0.144 ms
^C
--- 10.0.2.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.144/0.845/1.547/0.702 ms
mininet> h11 ping h31
PING 10.0.3.2 (10.0.3.2) 56(84) bytes of data.
64 bytes from 10.0.3.2: icmp_seq=1 ttl=64 time=1.43 ms
64 bytes from 10.0.3.2: icmp_seq=2 ttl=64 time=0.118 ms
^C
--- 10.0.3.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.118/0.775/1.433/0.658 ms
mininet> h21 ping h31
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
PING 10.0.3.2 (10.0.3.2) 56(84) bytes of data.
64 bytes from 10.0.3.2: icmp_seq=1 ttl=64 time=1.43 ms
```

Validate the connectivity of the L3VPN se

Figure 5 connection validation of L3VPNs among sites

The results show that VPNs between sites work well.

3.4 L3VPN performance management

Furthermore, with the configured L3VPNs, the system can also modify the bandwidth of the VPN provided by sites, for example change bandwidth of Nanjing Site from 8M to 4M. The monitored traffic flow of the site shows the change of the bandwidth management immediately in figure 6.

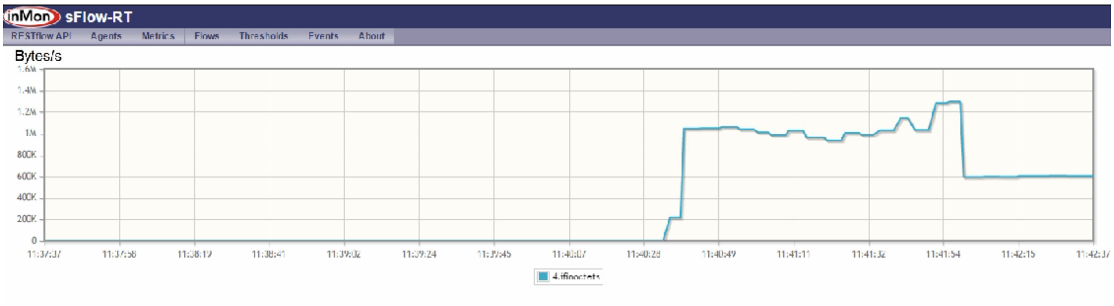


Figure 6 monitored traffic flow on Nanjing Site

Reference

[1] Bogdanovic, D., Claise, B., Moberg, C., “YANG model classification”, draft-bogdanovic-netmod-yang-model-classification-03 (work in progress), June 3, 2015.