Solution Brief

anuta networks

L3VPN Service Automation with Anuta ATOM

Highly Scalable Vendor Agnostic Service Orchestration

Key Capabilities

- Supports IETF YANG & OpenConfig Models
- Ensures Service Compliance
- Automated delivery of Model-driven Service UI
- Supports brownfield network discovery
- Supports complete lifecycle management of services
- Dry-run mode to validate command generation
- Vendor Agnostic
- Integration into Internal & External IPAM, VLAN, RD & RT Manager
- Workflow Integration for Pre & Post Validations
- Quickly scale up to 1M+ devices across 45+ vendors

It is a well-known fact that Service Providers & Enterprises take time to introduce new services to the market. The networks end up playing an antagonist in most cases, purely due to how they are managed. In this digital age, as the world is getting ready to embrace the high speeds of 5G, existing service provisioning processes do not scale or meet the agile market requirements. With the growing OTT competitors' who preach rapid service delivery and intolerance among customers on the lack of timely delivery of services, it is evident that network service fulfillment is the elephant in the room.

Multi-vendor networks, manual processes, varied configuration data sets, the introduction of new vendor platforms, siloed automation, integration hassles, and proprietary vendor solutions contribute to this ineffective and passive delivery of services.

Anuta ATOM is built ground up to support agile network service delivery. It introduces network service orchestration as a replacement for the existing methodologies of service provisioning. ATOM utilized YANG models as the underpinning to facilitate end-to-end complex service provisioning in heterogeneous networks. ATOM's service models go beyond the initial provisioning of services and manage the complete lifecycle to ensure full control. It goes a long way to accommodate the dynamic nature of today's businesses. The multi-vendor support of 150+ platforms across 45+ vendors enables Anuta ATOM to be the force that propels service delivery in organizations.

The service models in Anuta ATOM is built on the following principles to form the network abstraction layer:

1. Offers a model-driven view of services and their configurations
2. Offers a model-driven view of devices by supporting both Native YANG & OpenConfig
3. Maintains the device & service configured state to support CRUD operations
4. Built-in exception handling to address unexpected issues during service provisioning
5. Dry run mode enables complete visibility to network teams before command provisioning
6. Supports atomic transaction to ensure data consistency across the network
7. Supports integration into other ecosystem tools such as IPAM
8. Integrated to ATOM's workflow engine for Pre & Post Service validations

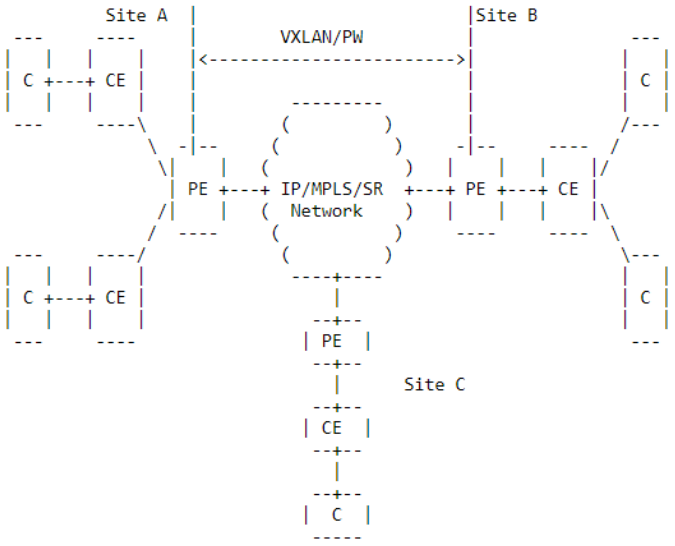
Anuta ATOM supports several out-of-box service models. This catalog includes a wide range of services for Service Providers, Branch, Campus, and Datacenter networks. Some of the IETF & custom service models delivering VPN services are discussed below.

anuta networks

IETF L3VPN Automation

Anuta ATOM offers out-of-box support for IETF L3VPN. ATOM's L3VPN model is based on draft-aguado-opsawg-l3sm-l3nm-01 that complements RFC 8299 YANG data model for a Layer 3 provider-provisioned VPN service. The model defines service configuration elements that can be used in communication protocols between customers and network operators.

The L3VPN service model is architected as a collection of sites that exchange traffic over a shared infrastructure. It aims at providing a common understanding of how the corresponding IP VPN service is to be deployed over the shared infrastructure.



ATOM's L3VPN Service model offers lifecycle management through an abstracted interface to request, configure, and manage L3VPN service components. The configuration of network elements may be done using the CLI or other southbound interfaces such as NETCONF in conjunction with ATOM's device models based on CLI, Native YANG, or OpenConfig.

ATOM L3VPN Service Model Design

The L3VPN service model is structured such that the Service Provider can list the multiple circuits that it serves for the same customer. The Customer Edge (CE) and Provider Edge (PE) devices are directly connected at Layer 3 via attachment circuits. ATOM's L3VPN service model provides an abstracted interface between customers and network operators to manage configuration of components of an L3VPN service. The YANG module is divided into two primary containers: *sites* & *vpn-services.*

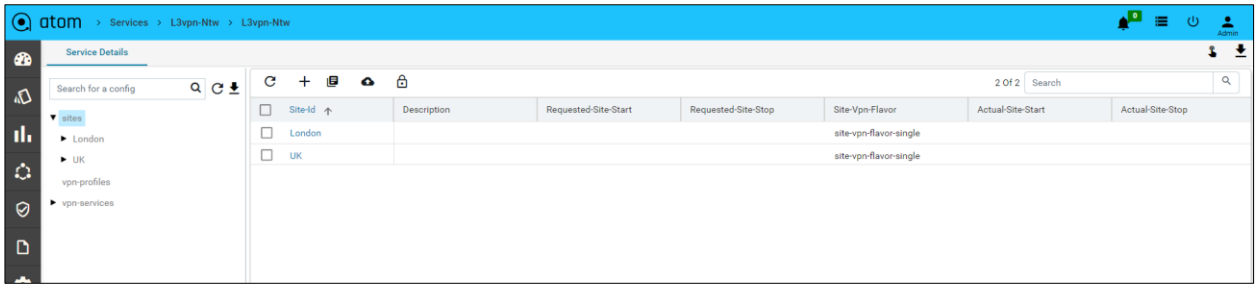
Sites

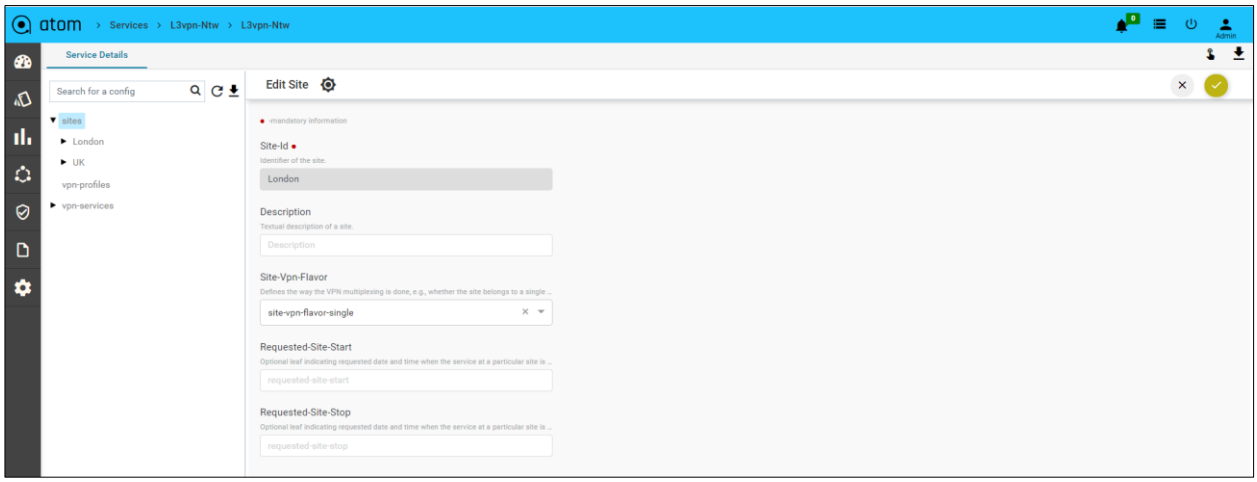
A site represents a connection of a customer office to one or more VPN services. The site container stores information regarding detailed implementation arrangements made with the customer. In ATOM, the following critical characteristics of a site are captured.

1. *Site-Id*: This field provides a unique identification of the site in the overall network infrastructure.
    1. *Site-VPN-Flavor*: Defines the way that the VPN multiplexing is done, e.g., whether the site belongs to a single VPN site or a multi-VPN site. The following options are supported.
        i. *Site-Vpn-Flavor*
        ii. *Site-Vpn-Flavor-Multi*
        iii. *Site-Vpn-Flavor-Single*
        iv. *Site-Vpn-Flavor-sub*
        v. *Site-Vpn-Flavor-Nni*

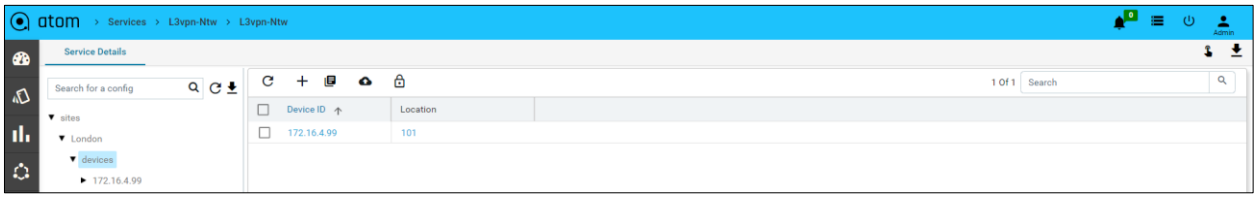
        By default, the site belongs to a single VPN.
    2. *Management*: The following options are supported
        i. *Management*
        ii. *Provider-Managed*
        iii. *Co-Managed*
        iv. *Customer-Managed*

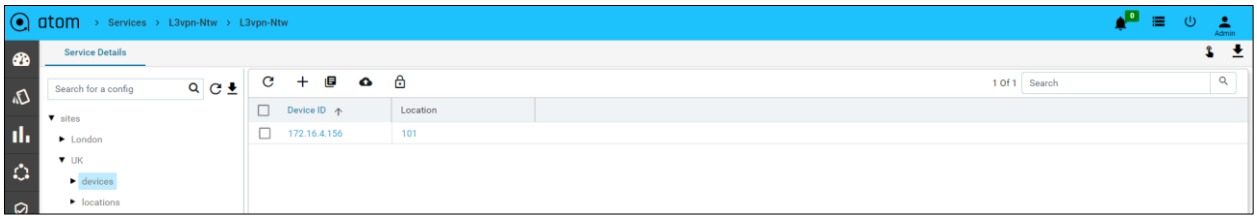
In the example illustrated in this brief, there are two sites, London, and UK.





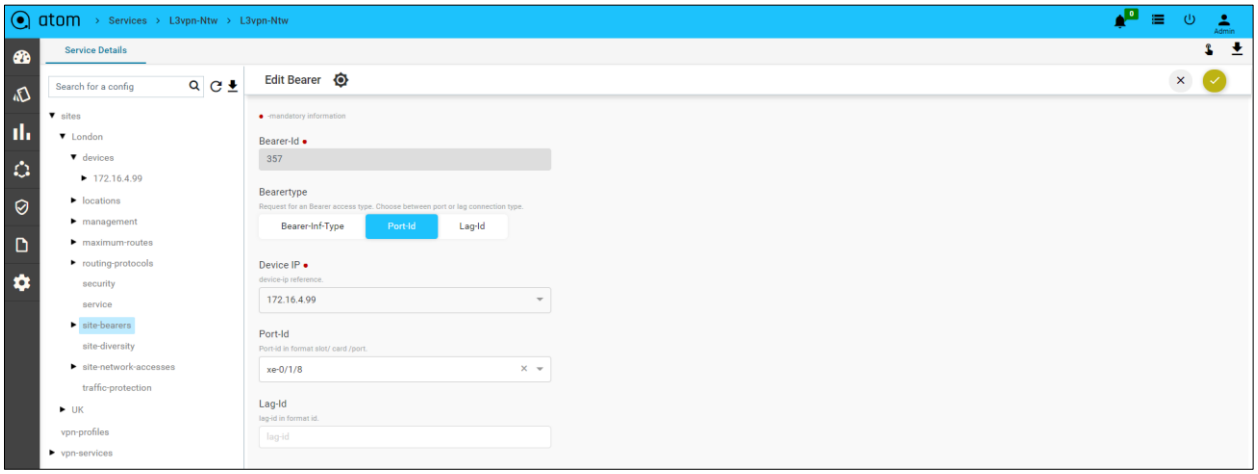
2. *Devices*: It denotes the Provider Edge (PE) devices to connect the Customer Edge (CE) devices. One or more PE devices can be created as part of the devices list. In the example, London hosts PE device 172.16.4.99, while UK hosts PE device 172.16.4.156



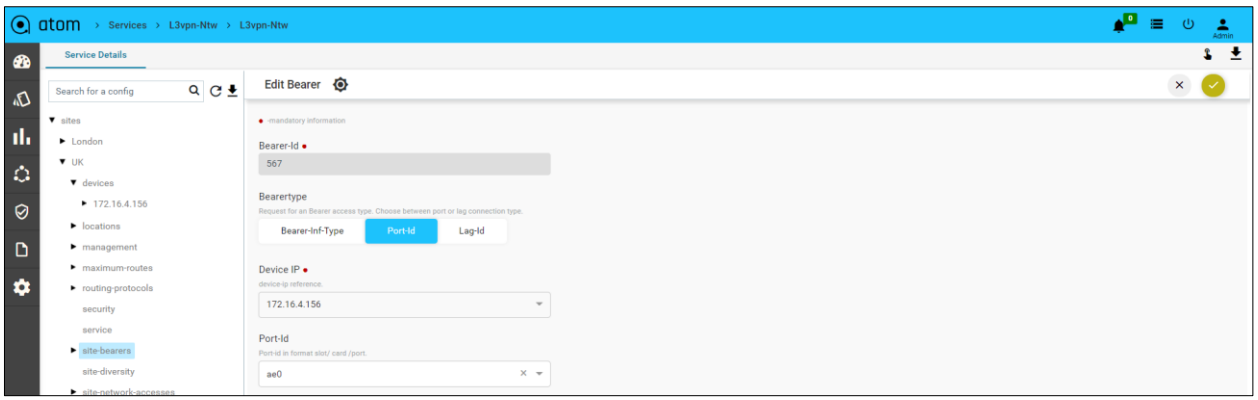


Creating a site in ATOM L3VPN service acts as a resource model that does not generate any commands. The site holds the device details involved in the L3VPN service.

3. *Site-bearers*: Once the sites are created listing the devices involved, the physical port connected to the CE device is defined. In the example below, the device 172.16.4.99 under London uses port xe-0/1/8



Device 172.16.4.156 under UK uses port ae0

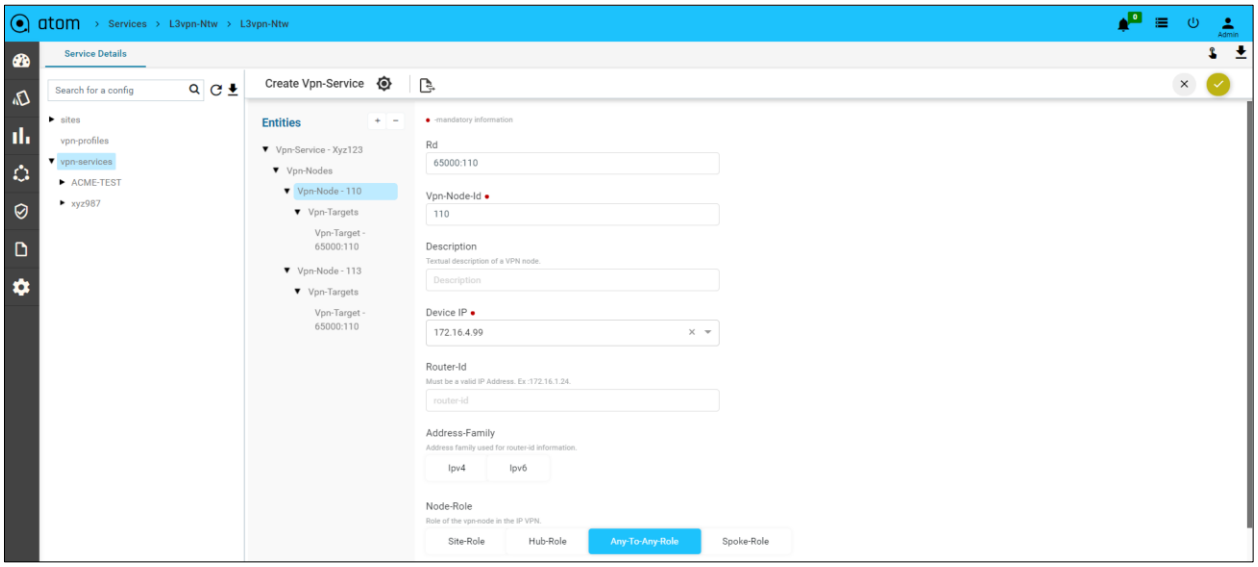


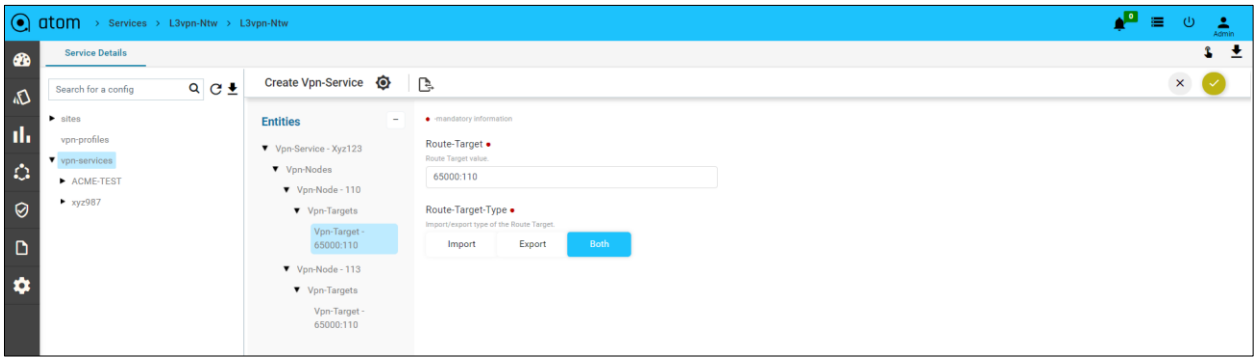
VPN Service

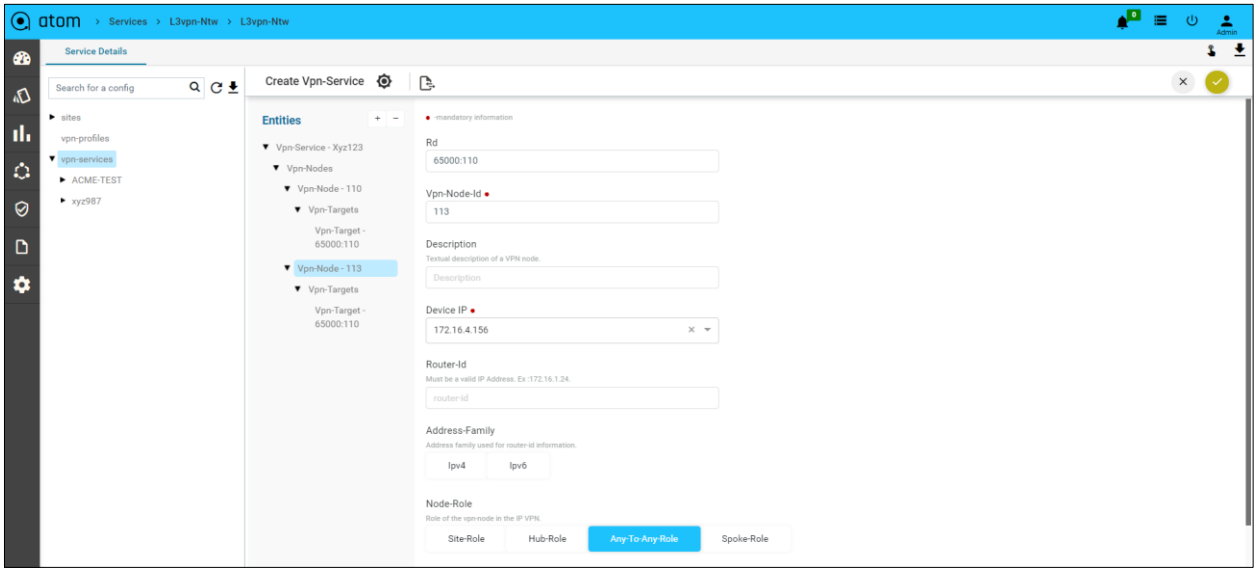
ATOM's L3VPN service model has been customized to ensure a smooth provisioning experience. The *vpn-service* list includes *vpn-nodes* list where route distinguisher (RD) and route targets (RT) for each PE device can be defined.

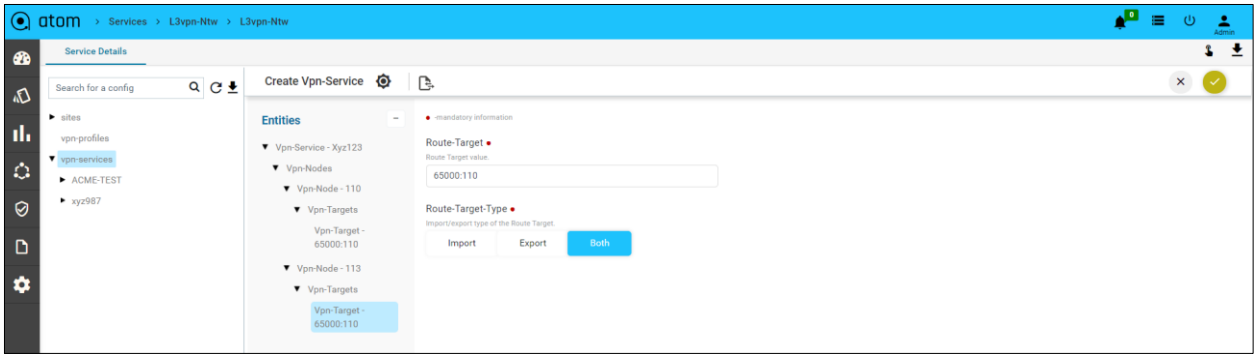
The *vpn-node* captures *rd* values to distinguish routes from each VRF and support type-0, type-1, and type-2 formats. The *vpn-targets* capture the rt values in type-0, type-1, and type-2 forms and supports options of import, export, and both to facilitate route sharing among VRFs. The vpn-node also captures the *Node-Role,* which can be one of *Site-Role*, *Hub-Role*, *Any-to-Any-Role* & *Spoke-Role.* In the example illustrated, since the service topology is chosen as *Any-to-Any*, the Node-Role will be *Any-to-Any-Role*.

Continuing the L3VPN service "xyz123" creation, VPN-Node 110 captures the RD and RT values for the device 172.16.4.99, while VPN-Node 113 captures the RD and RT values for the device 172.16.4.156

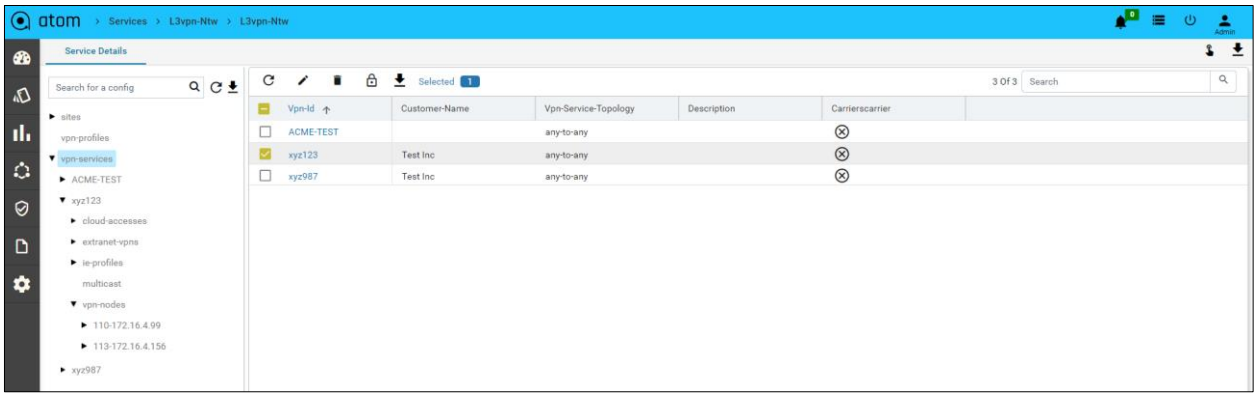




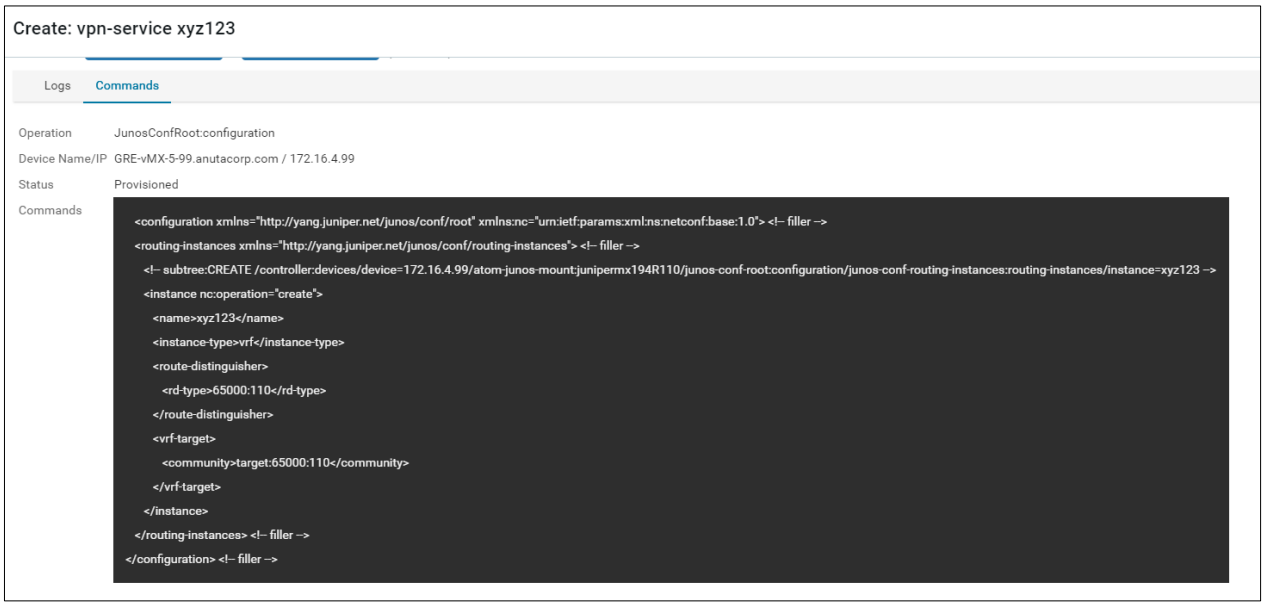


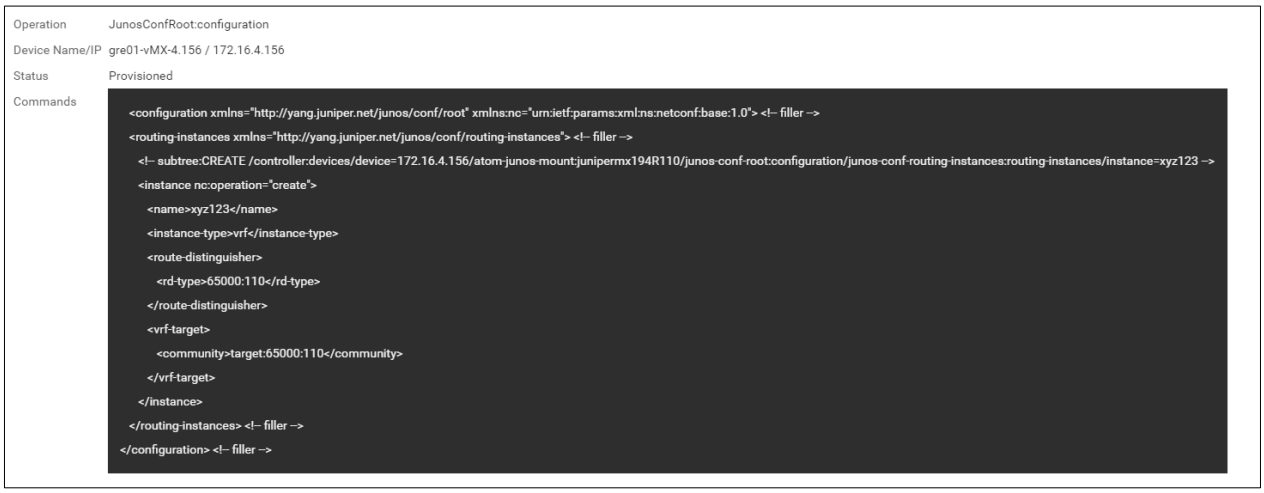


ATOM offers a one-click creation of services. The *vpn-services* list*,* when applied, ATOM generates the corresponding commands for the devices involved in the service. The device could be one or a combination of legacy CLI based devices, Native YANG, or OpenConfig based to complete an end-to-end service provisioning. In the example below, Juniper MX devices supporting Native YANG are provisioned with VPWS flavor for illustration purposes.



The below snapshot shows the NETCONF payload generated and provisioned on both 172.16.4.99 & 172.16.4.156.



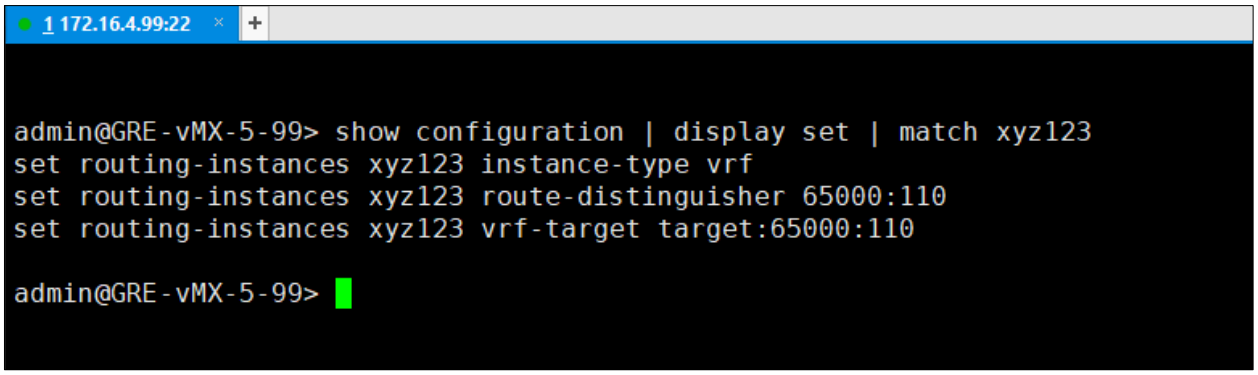


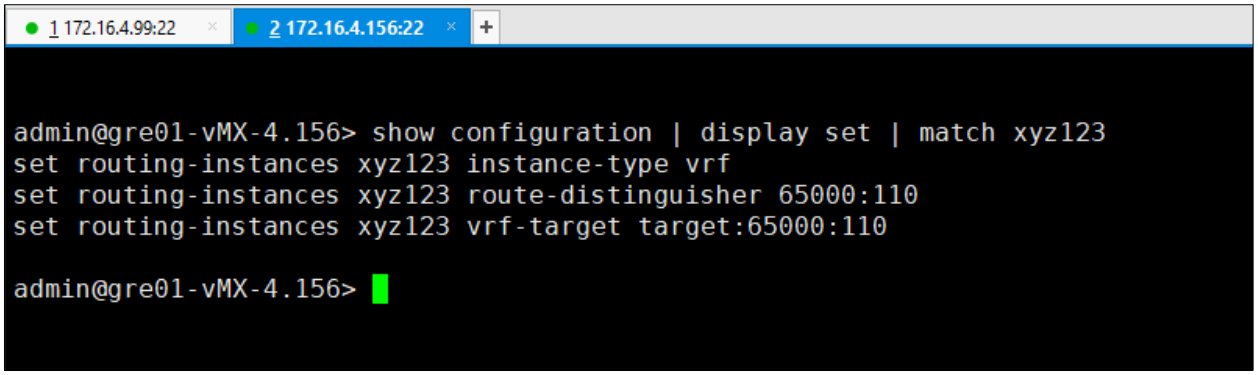
The below screenshot shows the service details on ATOM side.

Vpn-Service

```
<vpn-services xmlns="urn:ietf:params:xml:ns:yang:ietf_l3vpn_ntw">
   <vpn-service>
      <cloud-accesses/>
      <extranet-vpns/>
      <ie-profiles/>
      <vpn-nodes>
         <vpn-node>
            <vpn-targets>
               <vpn-target>
                  <route-target>65000:110</route-target>
                  <route-target-type>both</route-target-type>
               </vpn-target>
            </vpn-targets>
            <rd>65000:110</rd>
            <vpn-node-id>110</vpn-node-id>
            <device-ip>172.16.4.99</device-ip>
            <node-role>any-to-any-role</node-role>
         </vpn-node>
         <vpn-node>
            <vpn-targets>
               <vpn-target>
                  <route-target>65000:110</route-target>
                  <route-target-type>both</route-target-type>
               </vpn-target>
            </vpn-targets>
            <rd>65000:110</rd>
            <vpn-node-id>113</vpn-node-id>
            <device-ip>172.16.4.156</device-ip>
            <node-role>any-to-any-role</node-role>
         </vpn-node>
      </vpn-nodes>
      <carrierscarrier>false</carrierscarrier>
      <customer-name>Test Inc</customer-name>
      <vpn-id>xyz123</vpn-id>
      <vpn-service-topology>any-to-any</vpn-service-topology>
   </vpn-service>
</vpn-services>
```

The below screenshot shows the commands provisioned on both the Juniper MX devices.

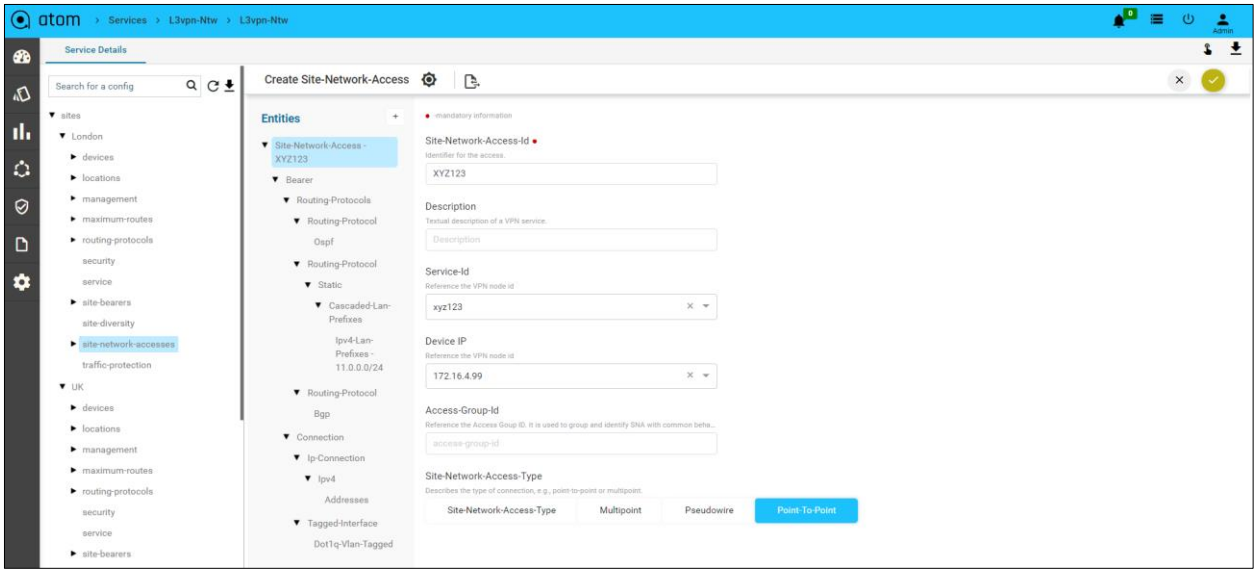


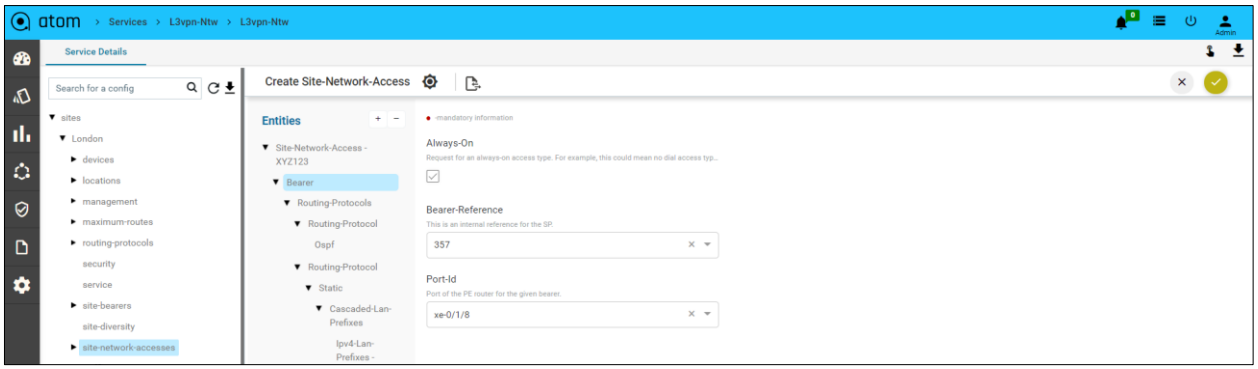


Site Network Access

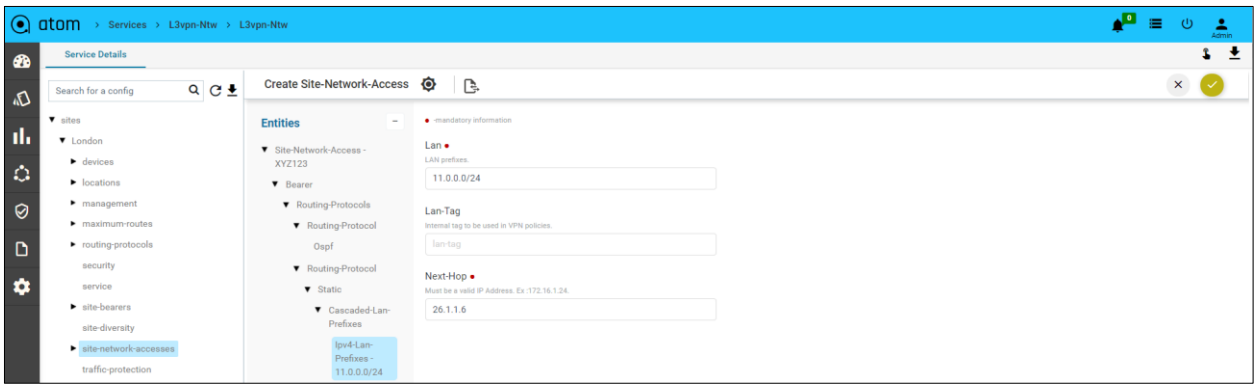
The *site-network-accesses* is a characteristic under the *site.* It defines the list of ports to the site and its properties. It is also the sub-container where the physical port or bearer is bound to the *vpn-service*. The site-network-access represents a logical ethernet connection to a site with multiple site-network-accesses, like in multi-homing. It also captures the routing information for PE-CE connection. The following essential characteristics are grouped under site-network-access.

1. *Bearer*: Gives a reference back into the site-bearer created above and the PE device port.

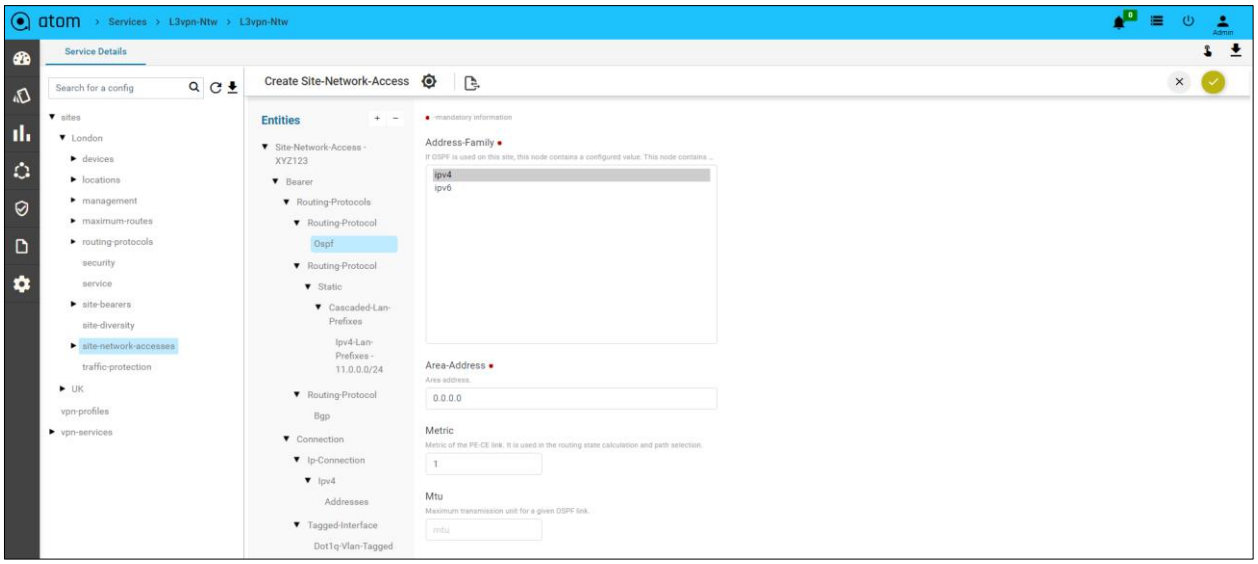


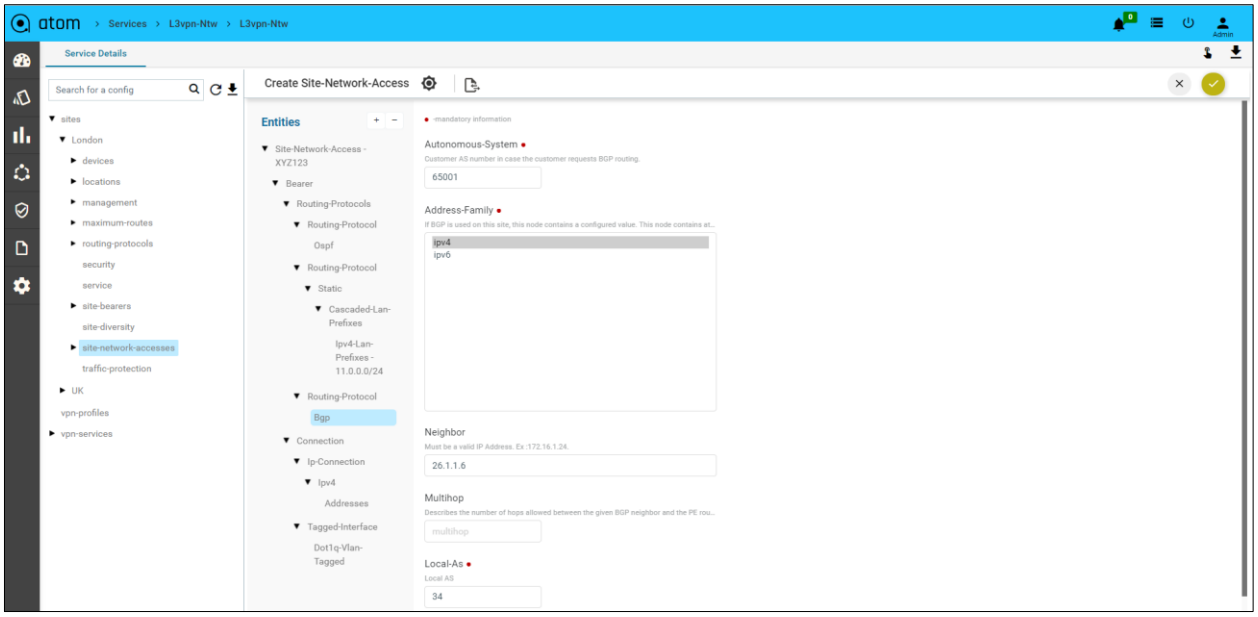


i. *Routing Protocols*: The routing protocol section of the model defines the routing between the PE and the CE routers. ATOM's L3VPN model supports BGP, OSPF, Static, Direct, RIP, and VRRP. In the example below, for site London, the PE-CE connection has been configured with BGP, static, and OSPF.



anuta networks





ii. *Connection: Offers the choice of encapsulation type & ethernet interface type. Options* under each category are listed below.

i. *Encapsulation-Type*

a. *Untagged-Int*

b. *Tagged-Int*

ii. *Tagged-Interface*

a. *qinq*

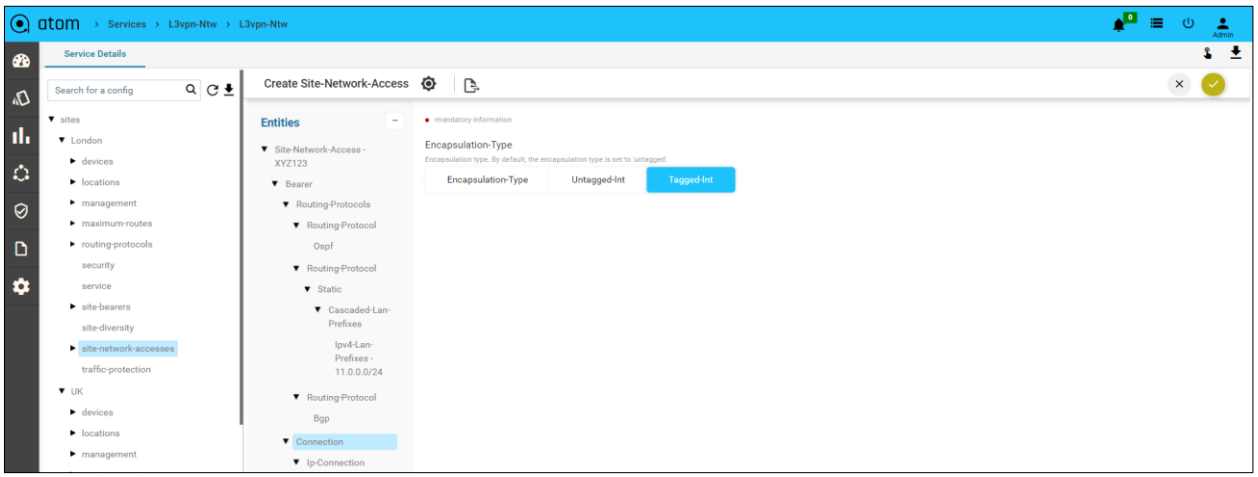
b. *vxlan*

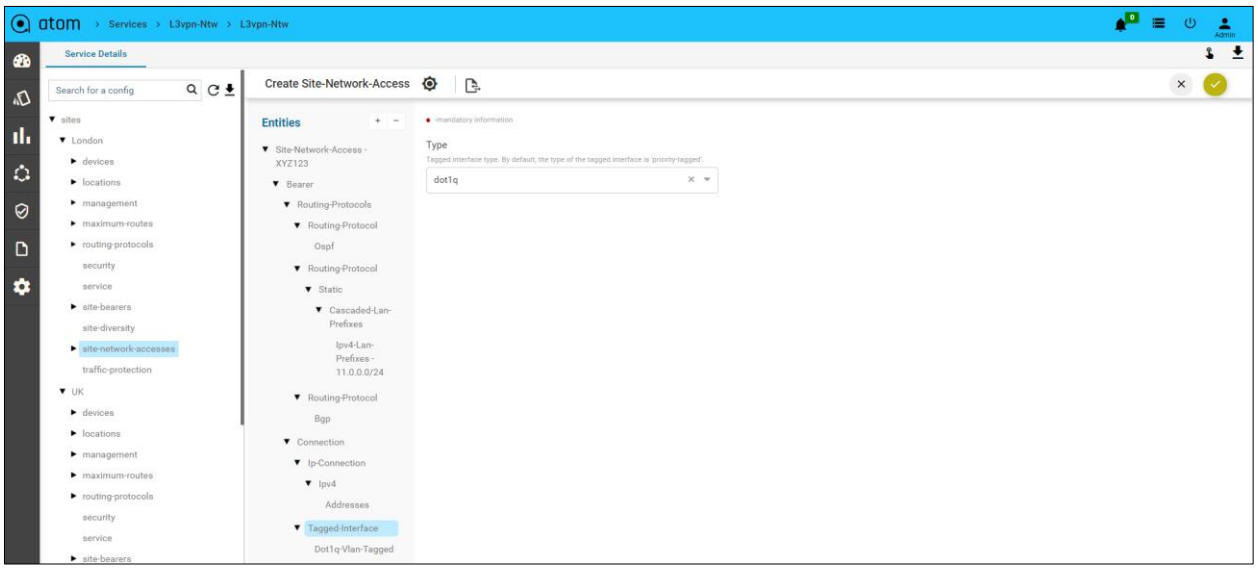
c. *dot1q*

d. *qinany*

e. *Priority-tagged*

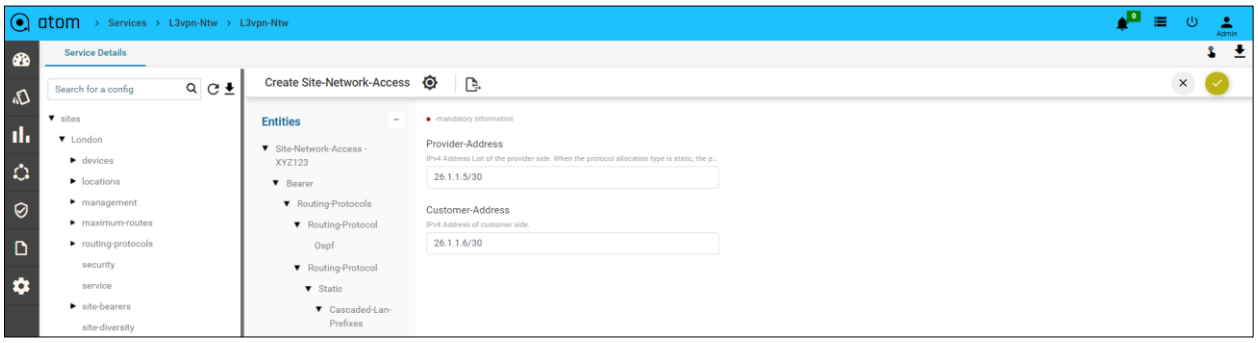
A tagged interface with Dot1q with tag type as C-Vlan is chosen for Site London, Device-172.16.4.99, for illustration in the example below.

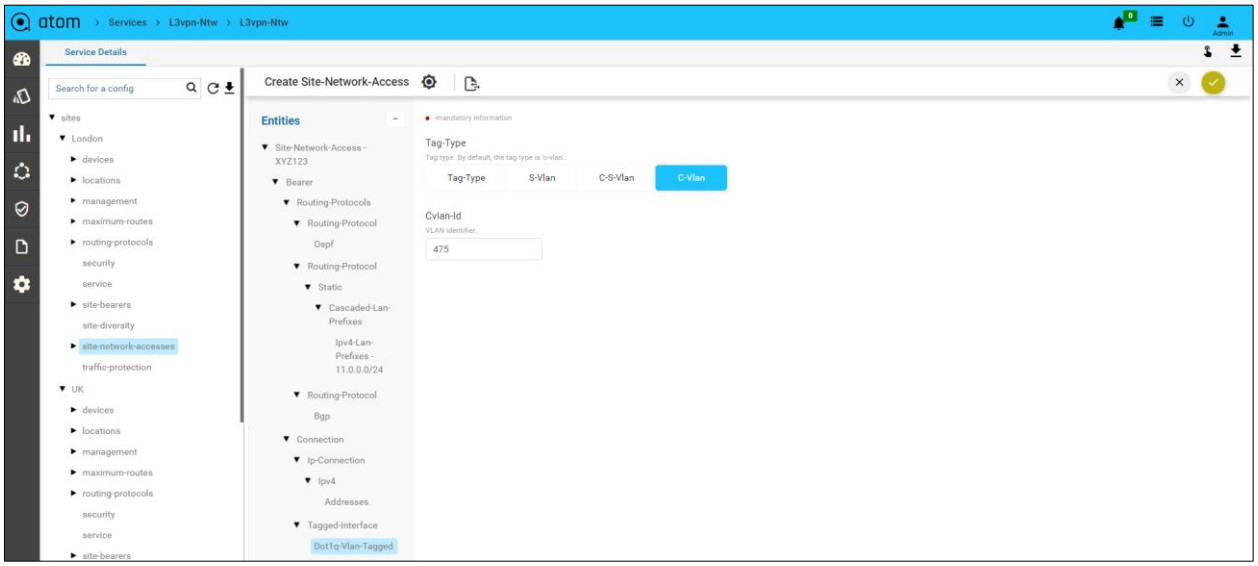




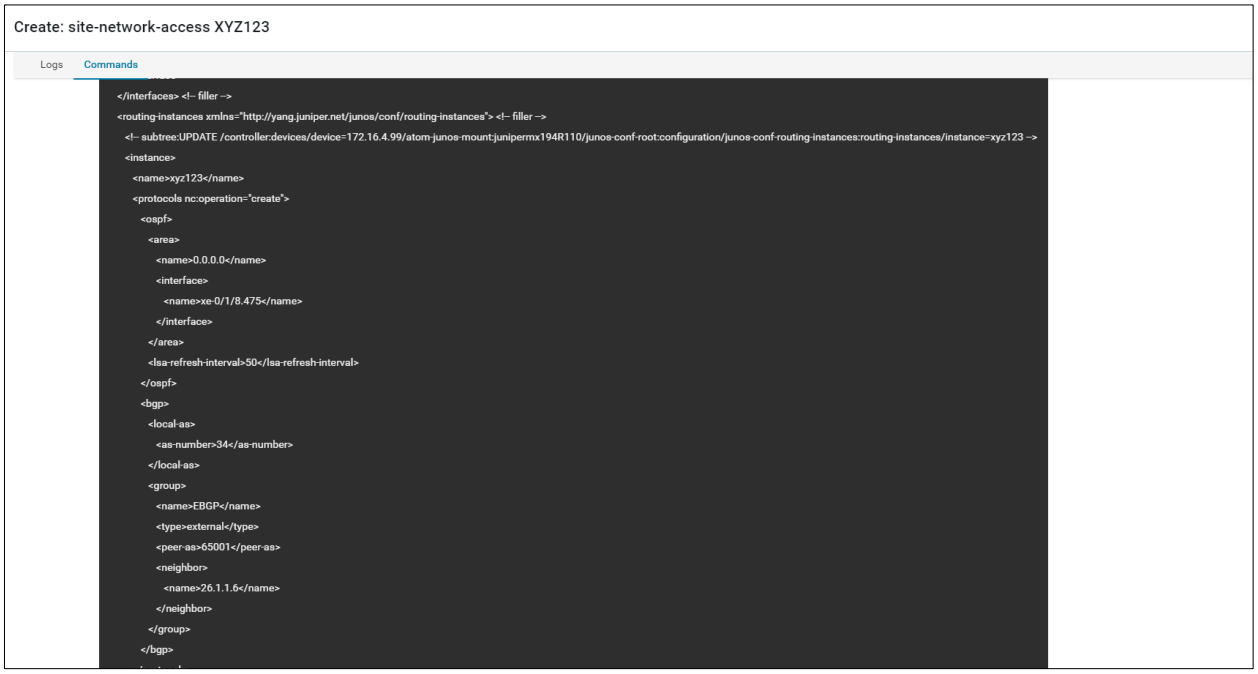
iii. *IP-Connection*: Customer & Provider addresses are captured in this leaf. The address allocation could be one of
   a. *static,*
   b. *provider-dhcp-relay*
   c. *provider-dhcp*
   d. *slaac*

In the site London, a static definition is done, as shown below. Both CE, PE IP connection details are captured.

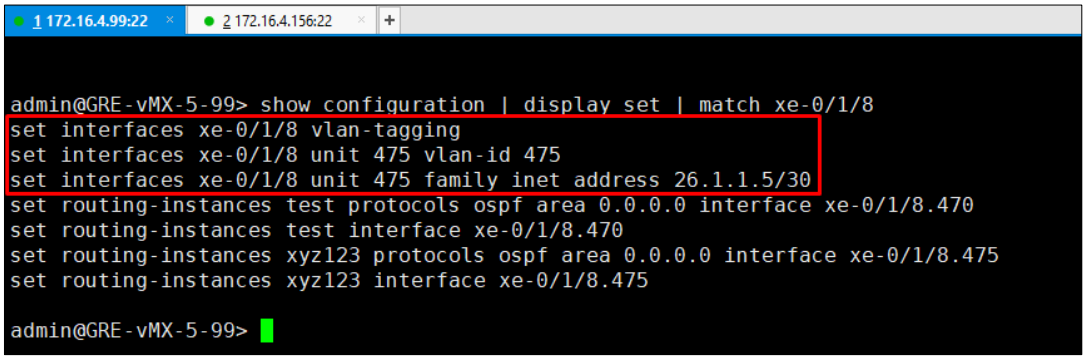


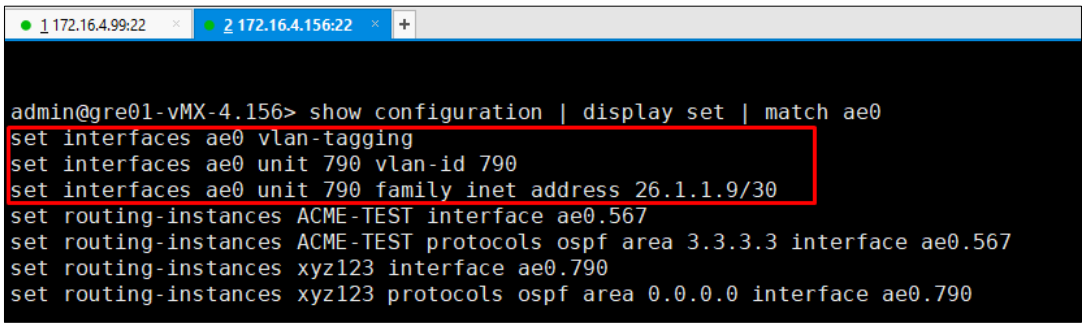


Similar configurations are performed for Site UK and its device 172.16.4.156. The below snapshot shows the NETCONF payload generated and provisioned on both 172.16.4.99 & 172.16.4.156.



The interface vlan tag, and IP addresses configured on the PE side is shown in the below screenshots.





The below screenshot shows the service details on ATOM side.

anuta networks

Site-Network-Access

```
<site-network-accesses xmlns="urn:ietf:params:xml:ns:yang:ietf_l3vpn_ntw">
   <site-network-access>
      <bearer>
         <always-on>true</always-on>
         <routing-protocols>
            <routing-protocol>
               <ospf>
                  <address-family>ipv4</address-family>
                  <area-address>0.0.0.0</area-address>
                  <metric>1</metric>
               </ospf>
               <type>ospf</type>
            </routing-protocol>
            <routing-protocol>
               <static>
                  <cascaded-lan-prefixes>
                     <ipv4-lan-prefixes>
                        <lan>11.0.0.0/24</lan>
                        <next-hop>26.1.1.6</next-hop>
                     </ipv4-lan-prefixes>
                  </cascaded-lan-prefixes>
               </static>
               <type>static</type>
            </routing-protocol>
            <routing-protocol>
               <bgp>
                  <autonomous-system>65001</autonomous-system>
                  <address-family>ipv4</address-family>
                  <neighbor>26.1.1.6</neighbor>
                  <Local-as>34</Local-as>
               </bgp>
               <type>bgp</type>
            </routing-protocol>
         </routing-protocols>
         <connection>
            <tagged-interface>
               <dot1q-vlan-tagged>
                  <tag-type>c-vlan</tag-type>
                  <cvlan-id>475</cvlan-id>
               </dot1q-vlan-tagged>
               <type>dot1q</type>
            </tagged-interface>
            <encapsulation-type>tagged-int</encapsulation-type>
```

```
            <ip-connection>
               <ipv4>
                  <addresses>
                     <provider-address>26.1.1.5/30</provider-address>
                     <customer-address>26.1.1.6/30</customer-address>
                  </addresses>
                  <address-allocation-type>static-address</address-allocation-type>
               </ipv4>
            </ip-connection>
         </connection>
         <bearer-reference>357</bearer-reference>
         <port-id>xe-0/1/8</port-id>
      </bearer>
      <device-ip>172.16.4.99</device-ip>
      <service-id>xyz123</service-id>
      <site-network-access-id>XYZ123</site-network-access-id>
      <site-network-access-type>point-to-point</site-network-access-type>
   </site-network-access>
</site-network-accesses>
```

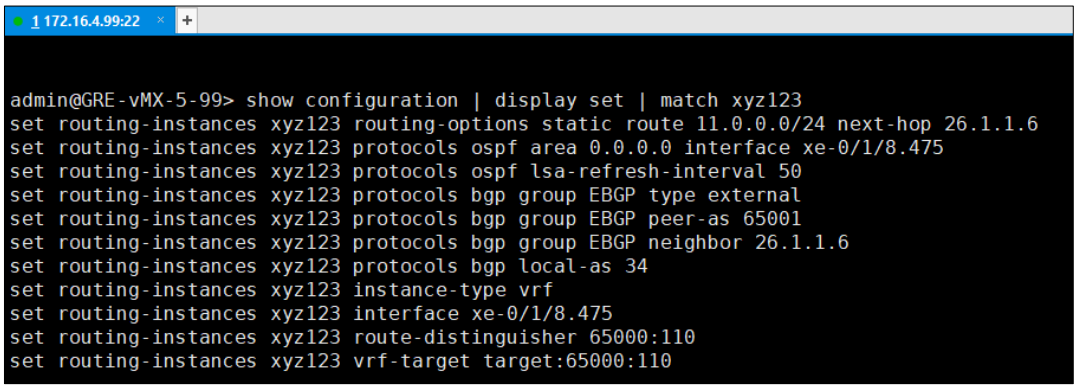
anuta networks

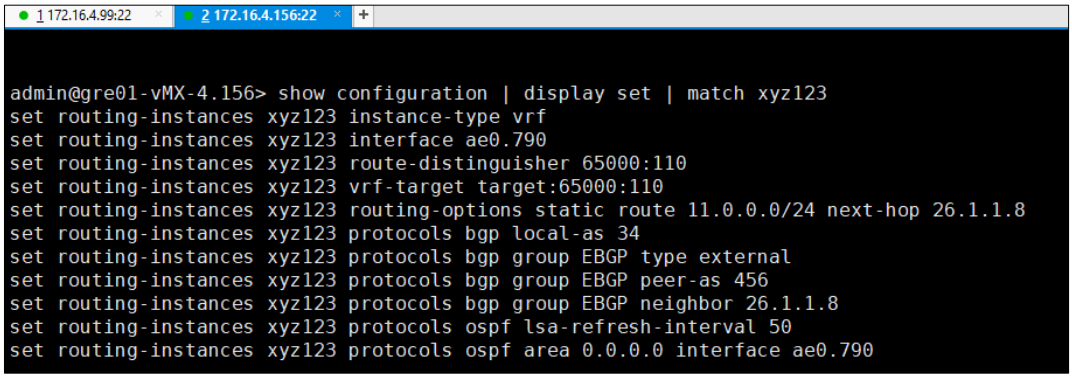
Site-Network-Access

```
<site-network-accesses xmlns="urn:ietf:params:xml:ns:yang:ietf_l3vpn_ntw">
   <site-network-access>
      <bearer>
         <always-on>true</always-on>
         <routing-protocols>
            <routing-protocol>
               <static>
                  <cascaded-lan-prefixes>
                     <ipv4-lan-prefixes>
                        <lan>11.0.0.0/24</lan>
                        <next-hop>26.1.1.8</next-hop>
                     </ipv4-lan-prefixes>
                  </cascaded-lan-prefixes>
               </static>
               <type>static</type>
            </routing-protocol>
            <routing-protocol>
               <ospf>
                  <address-family>ipv4</address-family>
                  <area-address>0.0.0.0</area-address>
                  <metric>1</metric>
               </ospf>
               <type>ospf</type>
            </routing-protocol>
            <routing-protocol>
               <bgp>
                  <autonomous-system>456</autonomous-system>
                  <address-family>ipv4</address-family>
                  <neighbor>26.1.1.8</neighbor>
                  <Local-as>34</Local-as>
               </bgp>
               <type>bgp</type>
            </routing-protocol>
         </routing-protocols>
         <connection>
            <tagged-interface>
               <dot1q-vlan-tagged>
                  <tag-type>c-vlan</tag-type>
                  <cvlan-id>790</cvlan-id>
               </dot1q-vlan-tagged>
               <type>dot1q</type>
            </tagged-interface>
            <encapsulation-type>tagged-int</encapsulation-type>
```

```
            <ip-connection>
               <ipv4>
                  <addresses>
                     <provider-address>26.1.1.9/30</provider-address>
                     <customer-address>26.1.1.8/30</customer-address>
                  </addresses>
                  <address-allocation-type>static-address</address-allocation-type>
               </ipv4>
            </ip-connection>
         </connection>
         <bearer-reference>567</bearer-reference>
         <port-id>ae0</port-id>
      </bearer>
      <device-ip>172.16.4.156</device-ip>
      <service-id>xyz123</service-id>
      <site-network-access-id>XYZ123_UK</site-network-access-id>
      <site-network-access-type>point-to-point</site-network-access-type>
   </site-network-access>
</site-network-accesses>
```

The below screenshot shows the commands provisioned on both the Juniper MX devices.



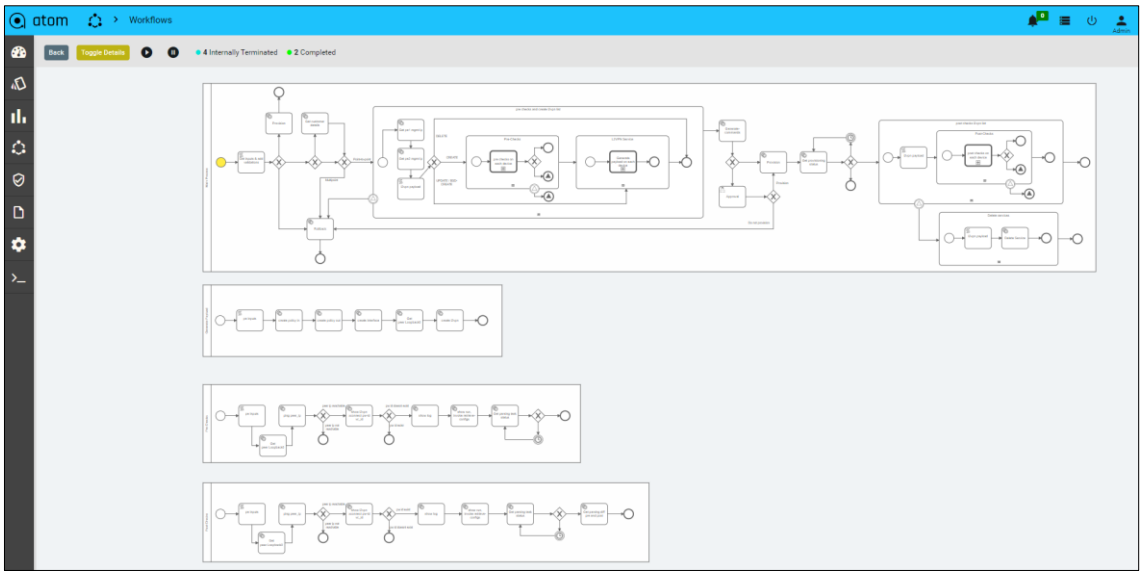


Service Compliance

Anuta ATOM's service modeling capabilities not only allows a smooth vendor agnostic provisioning, but also maintains the state and sanity of the services through its service compliance feature. The service compliance module detects the configuration drift to device configurations, performs service inventory to understand the nature of the changes and notifies upon deviation. ATOM also generates the difference in configuration along with the commands to be reconciled to ensure service compliance. The user is given the authority to overwrite the device or server (ATOM) service model configurations.

Workflow Integration

Every service provisioning is governed by a method-of-procedure in organizations. Integrating ATOM's service models into ATOM workflow engine, helps to execute a set of Pre-Checks, followed by the choice of services to be provisioned and Post-Checks to ensure a smooth and successful service provisioning. Below workflow executes an instance of VPN service with pre & post validations.



Additional Resources

Video-on-demand on ATOM L3VPN Service Automation

To learn how Anuta Network's ATOM Multi-Vendor Service Orchestration can accelerate your network automation journey, contact us at https://www.anutanetworks.com