Quick Intro to Cisco SD-WAN Configuration Templates

Introduction

There is a point in time when many route-switch Cisco engineers face SD-WAN. After living the CLI lifestyle for so many years, a centralized, GUI-based approach brings a different way of deploying configurations to routers.

The purpose of this paper is to give you a quick understanding of SD-WAN Templates as implemented by Cisco.

Are you ready?

Let's dive right in.

Background

Traditionally, if you have worked with Cisco routers and switches, route-switch Cisco engineers know that the device configuration is conducted via Command Line Interface, or CLI. This configuration is done on a device-basis. Network Engineers have found ways to "templatize" all configurations to maintain configuration consistency throughout the network.

But what happens when configuration is done independently on every device?

Problem Statement

With the growth of the network (more and more devices) and implementation assignments to different engineers, configuration consistency is lost many times. You might find different configuration parameters

ABOUT THE AUTHOR

Alirio (Rio) Zavarce possesses over 24 years of technical network consulting experience in LAN, WAN, datacenter, and security technologies. His broad range of experience in architecting and implementing advanced technology solutions includes working with clients across multiple verticals including manufacturing, financial services, real estate, higher education, and healthcare. Rio holds numerous industry certifications including Cisco Certified Internetwork Expert (CCIE) Routing and Switching.

What are some of the configuration entries that commonly differ from device to device?

- NTP server
- Disabled/enabled unnecessary services such as telnet, IP redirects, IP unreachables, etc.
- Control plane policing
- Interface descriptions
- Shutdown/enabled interfaces
- QoS
- Etc.

Likewise, it is common to find different IoS versions

But how can we standardize all configurations effectively and easily?

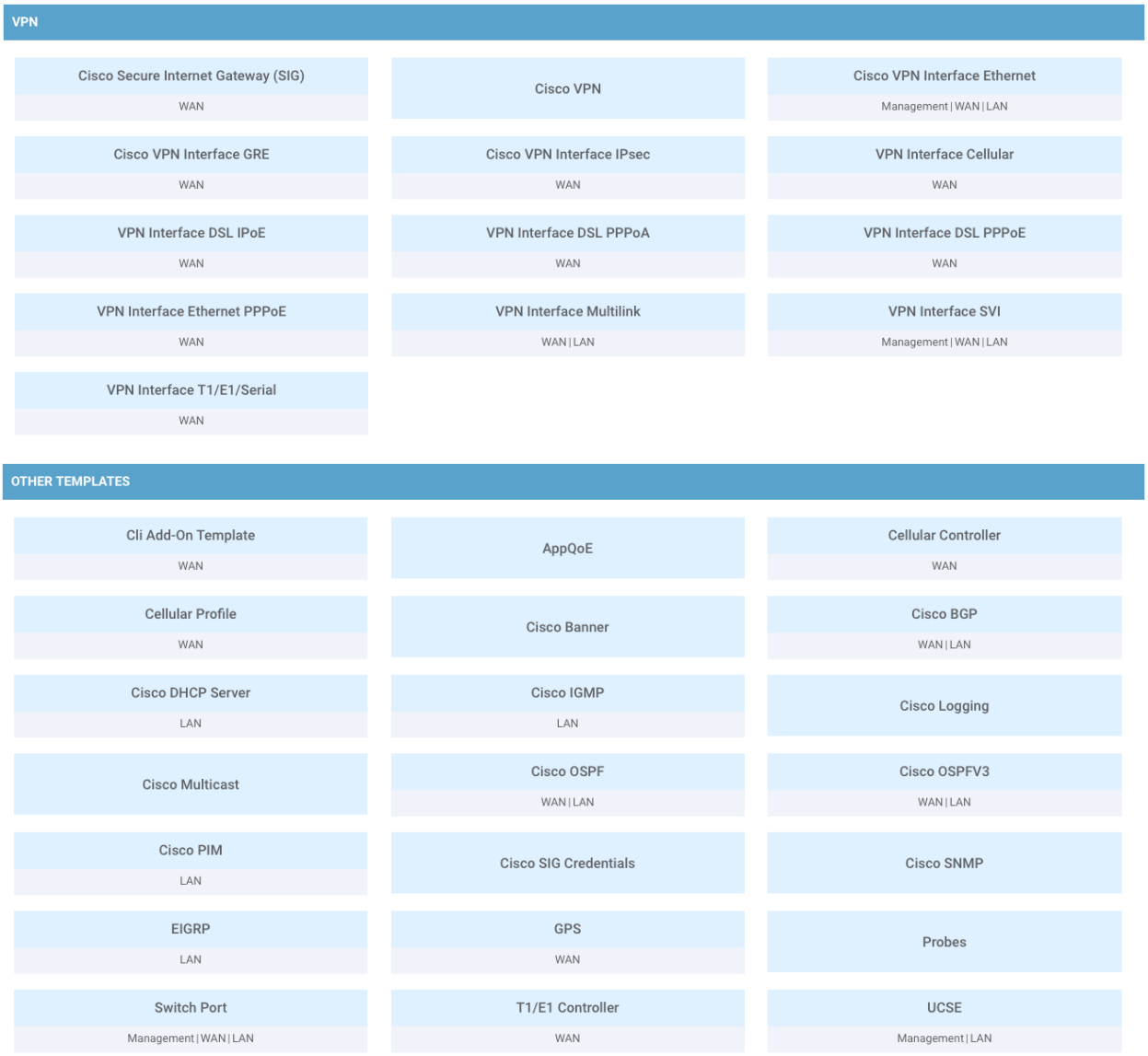
Solution

The Cisco SD-WAN solution relies on a management server called the vManage. On the vManage server, network administrators have access to configuration Templates. These templates are categorized per device type into:

- Feature Templates
- Device templates

Feature Templates allow you to specifically define configuration parameters per feature. For instance, there is a Feature Template for EIGRP, OSPF, interfaces, VPNs, banner, AAA settings, NTP, OMP, etc.

For an ISR 4431, these are the available Feature Templates on vManage version 20.3.2.1.



Each template has default, but customizable, parameters.

Device Templates are a collection of Feature Templates. A Device Template can include VPN templates for VPN 0 (transport VPN where tunnels originate), VPN 1-511 (service VPN where users come through), VPN 512 (management VPN), templates for interfaces that belong to each of those VPNs, an NTP template, an EIGRP template, an OMP template, a AAA template, etc.

Network devices can then be assigned to Device Templates. Once this assignment is done, the vManage will deploy those Device Templates to the network devices attached to each Device Template.

For instance, let's say you have two sites: Orlando and San Diego. A template structure could look this way:

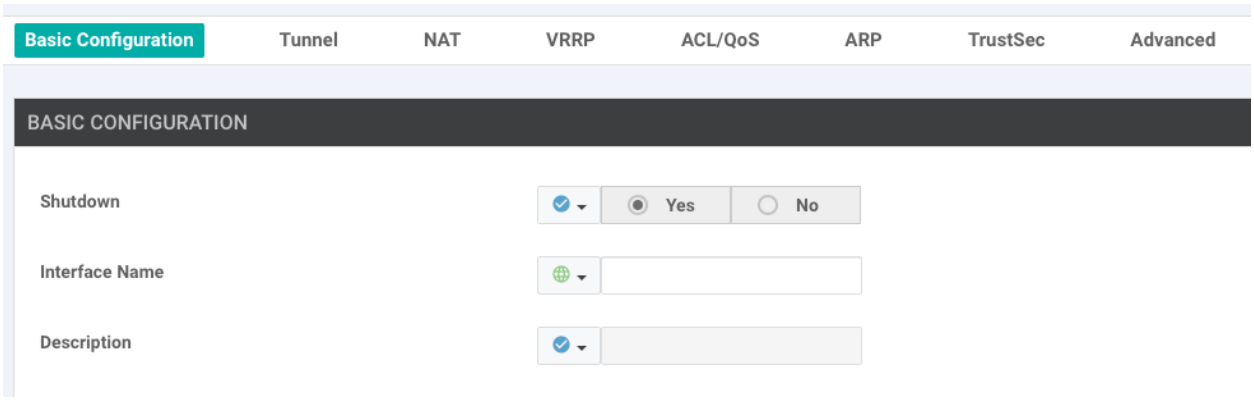
- Device Template called FL-Orlando-R01 for the router in Orlando
    - Includes the following Feature Templates

        - **Cisco AAA**
        - **Cisco NTP**
        - **Cisco VPN** for VPN 0 (Internet/MPLS transport VPN)
            - **Cisco VPN Interface Ethernet** for interfaces within VPN 0
        - **Cisco VPN** for VPN 10 (user VPN)
            - **Cisco VPN Interface Ethernet** for interfaces within VPN 10
        - **Cisco VPN** for VPN 512 (management VPN)
            - **Cisco VPN Interface Ethernet** for the interface within VPN 512
        - **EIGRP**
        - **Cisco Logging**
- Device Template called CA-SanDiego-R01 for the router in San Diego
    - Includes the following Feature Templates
        - **Cisco AAA**
        - **Cisco NTP**
        - **Cisco VPN** for VPN 0 (Internet/MPLS transport VPN)
            - **Cisco VPN Interface Ethernet** for interfaces within VPN 0
        - **Cisco VPN** for VPN 10 (user VPN)
            - **Cisco VPN Interface Ethernet** for interfaces within VPN 10
        - **Cisco VPN** for VPN 512 (management VPN)
            - **Cisco VPN Interface Ethernet** for the interface within VPN 512
        - **EIGRP**
        - **Cisco Logging**

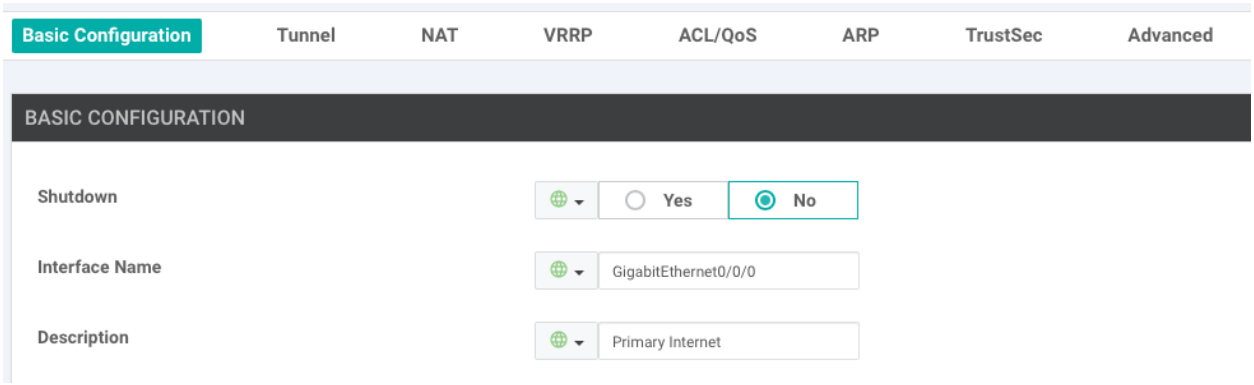
With each Feature Template, there are fields that can be left empty, or as variable; for when the template is applied to the router, the administrator can enter the value of the field, according to the device being configured.

Let me give you an example. The Cisco NTP template, configured with static NTP servers, can assign the same NTP servers to both routers. But the Cisco VPN Interface Ethernet template can have the IP address field, for the interface in question, designated as a variable so when the template is applied to the router, the admin can type in the corresponding IP address and mask prior to downloading the template to the router. In this way, you can configure one Feature Template with variables (empty fields) that will be customized according to the target device.

Let me illustrate this example. See this section of the Cisco VPN Interface Ethernet feature template. These are the default values.

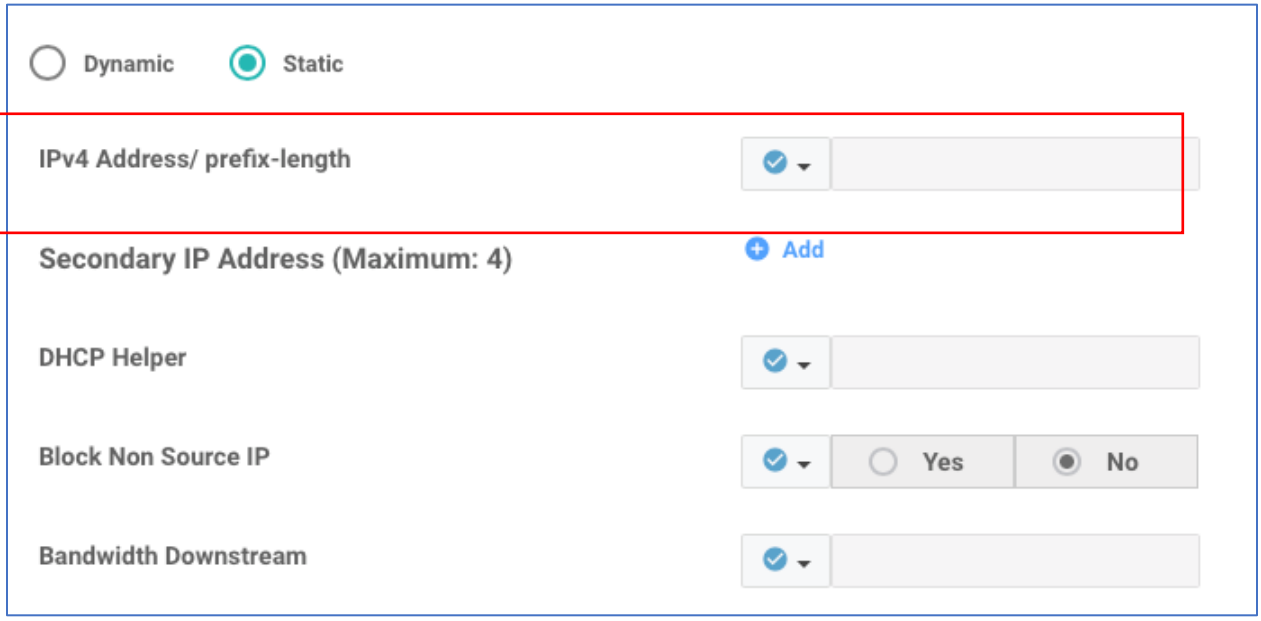


These are customized values that will be applied to both routers:

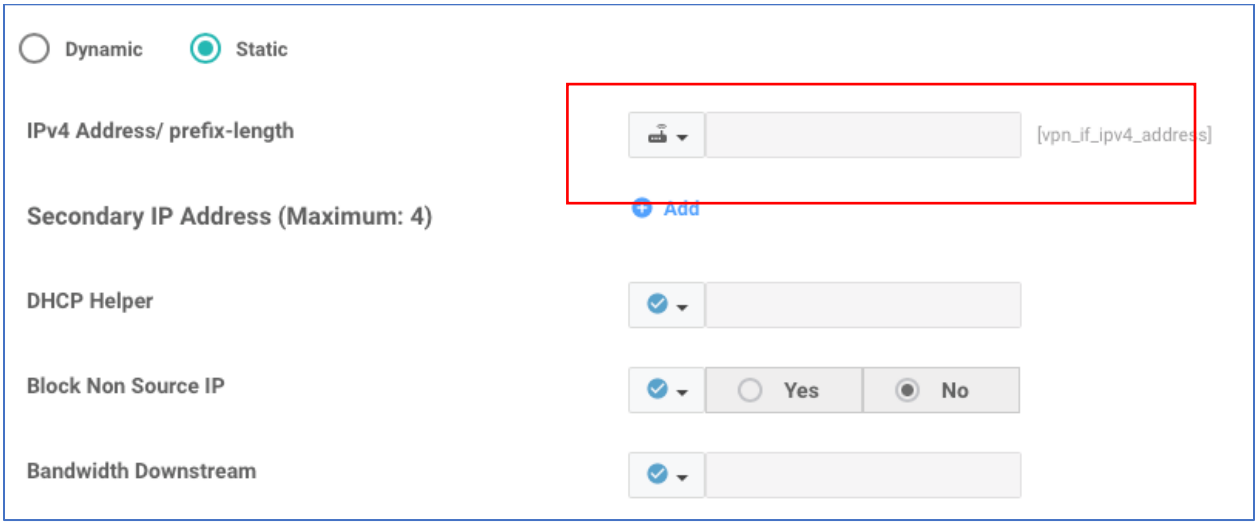


This means that both routers will have their Gi0/0/0 interface switched from shutdown to enabled and with a description of Primary Internet.

Now, the IP address for that interface will be different on both routers. If you scroll down to the IP settings section, you will see the following default values:



You can change the **IPv4 Address/prefix-length** field to device-specific so the value on this field must be entered by the administrator prior to deploying the template to the router.



Alternatively, you can also create a Cisco VPN Interface Ethernet feature template for the router in Orlando and another one for the router in San Diego. Each feature template would include the corresponding IP address of the device.

If for any reason your remote router loses connectivity to the vManage server after a configuration template was applied, the router will revert to the last working configuration to regain connectivity to the vManage server.

Notice that each field on the Feature Template can bet set to:

- **Default** – the template uses the default values already loaded on the template
- **Global** – all routers that receive the template will have this value set
- **Specific** – this field is left blank to be filled out by the administrator when deploying the Feature Template via a a Device Template from the vManage

Lastly, I would like to mention that when you configure a router with a Device Template, you are disabling local CLI configuration, which would work to your advantage as a security measure. In other words, the only way to add new configuration and changes will be via templates from the vManage controller.

Conclusion

Configuration templates are ideal to homogenize the configuration settings across all the routers within your SD-WAN infrastructure and to avoid misconfigurations. As a reminder, you will need to create a logical naming convention for both Device and Feature Templates so you can easily locate them in case of a large network with numerous templates.

About Aspire Technology Partners

Aspire is a professional technology services firm specializing in the delivery of digital infrastructure solutions and managed services designed specifically to achieve our clients' business goals. We believe technology sits at the heart of every enterprise strategy. Our team takes time to understand your business initiatives and align technology solutions to drive the organization forward. Aspire's outcome-driven approach accelerates your journey by combining secure digital infrastructure, world-class design and implementation expertise, and managed services – all centered around transforming today's multi-cloud architectures into enablers of business value. Headquartered in Eatontown, New Jersey, Aspire is focused on serving the tri-state and mid-Atlantic regions with local operations in Mount Laurel, NJ; Albany and White Plains, NY. For more information, visit www.aspiretransforms.com.