Ansible Network Modules

Welcome to [*Chapter 8*](https://subscription.packtpub.com/book/cloud-and-networking/9781835088913/8); this chapter will look at an often-overlooked use case for Ansible and delve into Ansible’s expansive community of networking modules.

In this chapter, instead of a deep dive into every collection—which could be an entire book—we’ll provide an overview, highlighting these modules’ capabilities and flexibilities.

The chapter covers the following topic:

* Manufacturer and device support

Manufacturer and device support

So far, we have been looking at modules that interact with servers. In our case, they have mostly been running locally. In the upcoming chapters, we will be communicating more with remotely cloud-hosted servers. But, before interacting with remote servers, we should cover the core network modules.

These modules have all been designed to interact with and manage the configuration of various network devices, from your traditional top-of-rack switches and fully virtualized network infrastructure to firewalls and load balancers. Ansible supports many devices, from open source virtual appliances to hardware solutions, some of which could have a starting price of over USD 500,000, depending on your configuration.

So, what do all these collections and modules have in common?

Well, they all interact with what are traditionally complex to configure devices, which, in most deployments and environments, are both the core and critical elements; after all, everything connected to them needs some level of network connectivity.

These modules give you a standard interface, i.e., Ansible, for many of these devices and remove the need for engineers to access these devices directly. They can, instead, run Ansible playbooks, which run roles created by experienced network engineers to configure them in a controlled and consistent way by just changing a few variables.

The only downside of using Ansible to manage this critical core infrastructure is that the host running Ansible requires a line of sight to the management interface or API running on the devices, which may sometimes raise some security concerns. Hence, Ansible’s instructions on how to manage your network devices need some serious thought.

The collections

The following list of collections is in the order of the namespaces and then the collection name; this is listed at the end of each item as **[namespace.collection-name]**.

Apstra Extensible Operating System (EOS) [arista.eos]

There are over 30 modules that allow you to manage your devices running EOS. These modules let you operate **access control lists** (**ACLs**) interfaces, configure **border gateway protocol** (**BGP**) settings, run arbitrary commands on devices, manage hostname, interface configurations, logging, and more. A module also allows you to gather facts from each device.

Additionally, there are plugins for command line and HTTP API interactions.

Check Point [check\_point.mgmt]

The Ansible collection for Check Point Management comprises many modules; at the time of writing, there are over 250 modules.

Each manages different aspects of your Check Point device, such as access layers, rules, administrators, or network feeds on your Check Point firewall using the Web Services API. They provide functionalities ranging from fetching facts and adding or managing objects to workflow features such as approving and publishing sessions on your Check Point firewall.

Cisco

Given the number of Cisco device types and classes, there are several collections in the Cisco namespace.

Cisco Application Centric Infrastructure (ACI) [cisco.aci]

The 150+ ACI modules are used to manage all aspects of Cisco’s ACI, which is to be expected of Cisco’s next-generation API-driven networking stack.

There are modules for managing various aspects of the Cisco ACI, such as AAAA records (these are address records that store IPv6 addresses), roles, users, certificates, Access SPAN configurations, **bridge domains** (**BDs**) and subnets, BGP route reflectors, and many more. There are modules for managing Cloud Application Profiles and Cloud AWS Provider configurations.

Cisco Adaptive Security Appliance (ASA) [cisco.asa]

With the five ASA modules, you can manage access lists, run commands, and manage the configuration of physical and virtual Cisco ASA-powered devices.

Cisco DNA Center (DNAC) [cisco.dnac]

The Ansible collection for the Cisco DNAC comprises nearly 400 modules to manage different aspects of your Cisco DNAC deployment. The modules cover a range of functionalities, from fetching the configuration details of access points, managing application policies, assigning devices to sites, importing authentication certificates, and running compliance checks to managing configuration templates.

Cisco IOS and IOS XR [cisco.ios and cisco.iosxr]

These two collections contain modules that allow you to manage your Cisco IOS and IOS XR-powered devices. You can gather facts on your devices and configure users, interfaces, logging, banners, and more with them.

Identity Services Engine (ISE) [cisco.ise]

This collection manages your ISE; it comprises a variety of modules for managing settings and configurations, such as handling ACI bindings and settings, managing Active Directory settings, handling allowed protocols, administering ANC endpoints and policies, managing backup configurations and schedules, handling certificates, and more.

Cisco Meraki [cisco.meraki]

Here, we have just short of 500 modules that manage the different elements of your Meraki deployment, such as administered identities, device details, camera settings, cellular gateway configurations, and sensor relationships. Each module is designed to fetch information or modify settings, which helps you manage your Cisco Meraki devices by using automation.

Cisco Network Services Orchestrator (NSO) [cisco.nso]

A handful of modules allow you to interact with your Cisco NSO-managed devices. You can execute NSO actions, query data from your installation, and verify your configuration alongside service synchronization and configuration.

Cisco Network Operating System Software (NX-OS) [cisco.nxos]

As you can imagine, there are a lot of modules for managing devices running Cisco NXOS; there are over 80 that cover a range of functions such as managing AAA server configurations, ACLs, BGP configurations, executing arbitrary commands, managing interfaces, and handling various other configurations and settings on Cisco NX-OS devices.

Cisco Unified Computing System (UCS) [cisco.ucs]

While not strictly a networking device, the modules to manage Cisco’s unified computing, storage, and network system include one that allows you to manage DNS servers, IP address pools, LAN connectivity policies, MAC address pools, QoS settings, VLANs, and vNICs. The rest of the modules allow you to programmatically manage computing and storage across your blades and chassis.

F5 BIG-IP Imperative [F5Networks.F5\_Modules]

There are 160 modules, all prefixed with BIG-IP, that allow you to manage all aspects of your F5 BIG-IP Application Delivery Controller.

Fortinet

There are just two collections in the Fortinet namespace, but, as you can see from the number of modules in each, they are very feature-rich.

Fortinet FortiManager [fortinet.fortimanager]

There are over 1,100 modules (yes, you read that correctly), including configuring antivirus profiles and options, managing AP local configuration profiles and command lists, configuring custom application signatures and firewall application groups, managing internet service applications, and more.

Fortinet FortiOS v6 (fortinet.fortios)

While this has fewer modules than the FortiManager collection, there are still over 650 modules for configuring antivirus settings, application control lists, authentication schemes, and certificate settings.

Free Range Routing (FRR) [Frr.Frr]

There are just two modules here: one that allows you to configure BGP, and the other lets you gather facts about devices running FRR.

Juniper Networks Junos [junipernetworks.junos]

A total of 40 modules enable you to interact with Juniper devices running Junos from within your playbooks. These range from the standard command, configuration, and fact-gathering modules to those that allow you to install packages and copy files to your devices.

Open vSwitch [Openvswitch.Openvswitch]

The four modules in the namespace allow you to manage bonds, bridges, ports, and databases on your OVS virtual switches.

VyOS [vyos.vyos]

The VyOS collection includes modules for managing various configurations and resources on VyOS devices. Some of these modules include managing multiline banners, configuring BGP global and address family settings, running commands, managing firewall settings, interface configurations, logging, NTP, OSPF, SNMP, static routes, system commands, user management, and VLAN configurations, among others.

The Community Network Collection [Community.Network]

This collection is a catch-all for all other network modules without dedicated namespace or development teams; the module prefix is now in the square brackets.

A10 Networks [a10]

The A10 modules support A10 Networks AX, SoftAX, Thunder, and vThunder devices. These are all application delivery platforms that provide load balancing.

Cisco AireOS [aireos]

The two AireOS modules allow you to interact with the Cisco Wireless LAN Controllers running AireOS. One of the modules will enable you to run commands directly on the devices, and the other is for managing the configuration.

APCON [apcon]

A single module that allows you to run commands on your APCON device.

Aruba Mobility Controller [aruba]

There are just two Aruba modules. These allow you to manage the configuration and execute commands on the Aruba Mobility Controllers from Hewlett Packard.

Avi Networks [avi]

There are a total of 65 Avi modules that allow you to interact with all aspects of the Avi application services platform, including the load-balancing and **web application firewall** (**WAF**) features.

Big Cloud Fabric and Big Switch Network [bcf + bigmon]

There are three Big Switch Network modules. **Big Cloud Fabric** (**BCF**) allows you to create and delete BCF switches. The other two modules enable you to create **Big Monitoring Fabric** (**Big Mon**) service chains and policies.

Huawei Cloud Engine [ce]

Over 75 Cloud Engine modules allow you to manage all aspects of these robust switches from Huawei, including BGP, access control lists, MTU, static routes, VXLANs, and SNMP configuration.

Lenovo CNOS [cnos]

There are nearly 30 modules that allow you to manage devices running the CNOS operating system from Lenovo; they enable you to configure everything from BGP and port aggregation to VLAG, VLANs, and factory reset devices, should you need to.

Arista Cloud Vision [cv]

A single module lets you provision an Arista Cloud Vision server port using a configlet.

illumos [dladm + flowadm + ipadm]

illumos is a fork of the Open Solaris operating system. Its powerful networking features make it the perfect candidate for deploying as a self-built router or firewall. These modules allow you to manage the interfaces, NetFlow, and tunnels. Additionally, as illumos is a fork of Open Solaris, your playbook should work on Open Solaris-based operating systems.

Ubiquiti EdgeOS [edgeos + edgeswitch]

The modules for EdgeOS enable you to manage configurations, execute ad hoc commands, and collect facts on EdgeOS-running devices, such as the Ubiquiti Edge Router.

There are also a few modules for Edge Switches.

Lenovo Enterprise Networking Operating System [enos]

There are three modules for the Lenovo ENOS. Like other devices, these allow you to gather facts, execute commands, and manage the configuration.

Ericsson [eccli]

This single module allows you to run commands on devices running the Ericsson command-line interface.

ExtremeXOS [exos + nos + slxos]

These half-a dozen modules allow you to interact with the ExtremeXOS, Extreme Networks SLX-OS, and Extreme Networks NOS software on Extreme Networks switches.

Cisco Firepower Threat Defense [ftd]

A few modules allow you to configure and upload/download files to a Cisco Firepower Threat Defense device.

Itential Automation Platform [iap]

A few modules allow you to interact with workflows hosted on the Itential Automation Platform, as well as low-code automation and orchestration for hybrid cloud networks.

Ruckus ICX 7000 [icx]

These modules allow you to configure your Ruckus ICX 7000 series campus switches.

Ingate Session Border Controllers [ig]

While these are mainly used for **SIP**, or to give its full name, **session initiation protocol** services, there are a few modules to help configure the network elements.

NVIDIA Network Command Line Utility [nclu]

A single module that allows you to manage network interfaces using the NVIDIA Network Command Line Utility on compatible devices.

Nokia NetAct [netact]

A single module that allows you to upload and apply your Nokia NetAct-powered core and radio networks.

Citrix Netscaler [netscaler]

These modules are designed to manage and configure various aspects of Netscaler devices. They cover functionalities such as content switching, **Global Server Load-Balancing** (**GSLB**), load-balancing, issuing Nitro API requests, and saving configurations, as well as managing server configurations, services, service groups, and SSL certificate keys.

Nokia Nuage Networks Virtualized Services Platform (VSP) [nuage]

There is a single module that allows you to manage enterprises on your Nokia Nuage Networks VSP.

OpenSwitch [opx]

A single module that performs the specified action on the YANG object, utilizing the CPS API on the networking device operating OpenSwitch.

Ordnance Virtual Routers [ordnance]

There are two modules: one to manage configuration and the other to collect facts on Ordnance Virtual Routers.

Pluribus Networks Netvisor OS [pn]

These 40 modules allow you to manage your **Pluribus Networks** (**PN**) Netvisor OS-powered devices, from creating clusters and routers to running commands on your white-box switches.

Nokia Networks Service Router Operating System [sros]

There are three modules that let you run commands against, configure, and roll back changes to your Nokia Networks SROS devices.

Radware [vidrect]

A small number of modules that allow you to manage your Radware devices via a vDirect server.

Ansible Net Common [ansible.netcommon]

The final collection is a set of modules that could be considered tools to help support all the devices we have covered in this chapter. There are modules that can ping targets and run generic commands using custom prompts and answers.

Summary

I suspect most of you would not have heard of a lot of the devices we have listed in this chapter, and for the ones you have heard of—such as the Cisco ones—you will probably not have had direct access to them, leaving any configuration to your network administrators.

When we speak about triggering Ansible using CI/CD in [*Chapter 15*](https://subscription.packtpub.com/book/cloud-and-networking/9781835088913/15), *Using Ansible with GitHub Actions and Azure DevOps*, and [*Chapter 16*](https://subscription.packtpub.com/book/cloud-and-networking/9781835088913/16), *Introducing Ansible AWX and Red Hat Ansible Automation Platform*, we will learn about some deployment options that could help alleviate the concerns we mentioned at the start of the chapter, e.g., those about a host running your Ansible playbooks needing a line of sight of the potentially critical core infrastructure.

Before we get to those chapters, we will look at moving our workloads to the cloud, a journey that starts in the next chapter.