



Cumulus Linux 2.5 ESR

User Guide

Table of Contents

Welcome to Cumulus Networks	5
Extended Support Release	6
Contents	7
Quick Start Guide	8
Contents	8
What's New in Cumulus Linux 2.5.11	8
Open Source Contributions	8
Prerequisites	9
Hardware Compatibility List	9
Installing Cumulus Linux	9
Upgrading Cumulus Linux	10
Configuring Cumulus Linux	10
Configuring 4x10G Port Configuration (Splitter Cables)	13
Testing Cable Connectivity	13
Configuring Switch Ports	14
Configuring a Loopback Interface	16
Installation, Upgrading and Package Management	18
Managing Cumulus Linux Disk Images	18
Adding and Updating Packages	50
Zero Touch Provisioning - ZTP	57
System Management	67
Setting Date and Time	67
Authentication, Authorization, and Accounting	70
Netfilter - ACLs	89
Configuring switchd	112
Power over Ethernet - PoE	116
Configuring a Global Proxy	119
Configuring and Managing Network Interfaces	121
Contents	121
Commands	121
Man Pages	122
Configuration Files	122
Basic Commands	122
Bringing All auto Interfaces Up or Down	123
ifupdown Behavior with Child Interfaces	123

ifupdown2 Interface Dependencies	125
Configuring IP Addresses	128
Specifying User Commands	130
Sourcing Interface File Snippets	130
Using Globs for Port Lists	131
Using Templates	131
Adding Descriptions to Interfaces	132
Caveats and Errata	133
Useful Links	133
Layer 1 and Switch Port Attributes	134
Buffer and Queue Management	143
Layer 1 and Layer 2 Features	150
Spanning Tree and Rapid Spanning Tree	150
Link Layer Discovery Protocol	165
Prescriptive Topology Manager - PTM	172
Bonding - Link Aggregation	184
Ethernet Bridging - VLANs	187
Multi-Chassis Link Aggregation - MLAG	217
LACP Bypass	234
Virtual Router Redundancy - VRR	240
Network Virtualization	245
IGMP and MLD Snooping	328
Layer 3 Features	335
Routing	335
Introduction to Routing Protocols	340
Network Topology	342
Quagga Overview	344
Configuring Quagga	346
Open Shortest Path First - OSPF - Protocol	358
Open Shortest Path First v3 - OSPFv3 - Protocol	369
Configuring Border Gateway Protocol - BGP	372
Bidirectional Forwarding Detection - BFD	394
Equal Cost Multipath Load Sharing - Hardware ECMP	399
Management VRF	408
Monitoring and Troubleshooting	414
Contents	414
Commands	414
Using the Serial Console	414
Diagnostics Using cl-support	416
Sending Log Files to a syslog Server	417
Next Steps	419
Single User Mode - Boot Recovery	419

Using netshow to Troubleshoot Your Network Configuration	425
Monitoring Interfaces and Transceivers Using ethtool	431
Resource Diagnostics Using cl-resource-query	436
Monitoring System Hardware	437
Monitoring System Statistics and Network Traffic with sFlow	443
Monitoring Virtual Device Counters	445
Understanding and Decoding the cl-support Output File	449
Managing Application Daemons	467
Troubleshooting Network Interfaces	470
Network Troubleshooting	475
SNMP Monitoring	487
Network Solutions	509
Data Center Host to ToR Architecture	509
Index	527

Welcome to Cumulus Networks

We are transforming networking with Cumulus Linux, the industry's first, full-featured Linux operating system for networking hardware. Cumulus Linux is a complete network operating system, based on [Debian wheezy](#). Unlike traditional embedded platforms, Cumulus Linux provides a complete environment pre-installed with scripting languages, server utilities, and monitoring tools. Management tasks are accomplished via SSH using standard Linux commands or over a serial console connection.



This documentation is current as of November 28, 2016 for version 2.5.11. Please visit the [Cumulus Networks Web site](#) for the most up to date documentation.

Read the [release notes](#) for new features and known issues in this release.

Extended Support Release

This version of Cumulus Linux is an Extended Support Release (ESR). Cumulus Linux 2.5 ESR started with Cumulus Linux 2.5.6 and all future releases in the 2.5 product family will all be ESR releases. To learn about ESR, please read [this article](#).

Cumulus Linux Version	Release Notes
2.5.11	Release notes
2.5.10	Release notes
2.5.9	Release notes
2.5.8	Release notes
2.5.7	Release notes
2.5.6	Release notes

Contents

- Quick Start Guide (see page 8)
- Installation, Upgrading and Package Management (see page 18)
- System Management (see page 67)
- Configuring and Managing Network Interfaces (see page 121)
- Layer 2 Features (see page 150)
- Layer 3 Features (see page 335)
- Monitoring and Troubleshooting (see page 414)

Quick Start Guide

This chapter helps you get up and running with Cumulus Linux quickly and easily.

Contents

(Click to expand)

- [Contents \(see page 8\)](#)
- [What's New in Cumulus Linux 2.5.11 \(see page 8\)](#)
- [Open Source Contributions \(see page 8\)](#)
- [Prerequisites \(see page 9\)](#)
- [Hardware Compatibility List \(see page 9\)](#)
- [Installing Cumulus Linux \(see page 9\)](#)
- [Upgrading Cumulus Linux \(see page 10\)](#)
- [Configuring Cumulus Linux \(see page 10\)
 - \[Login Credentials \\(see page 11\\)\]\(#\)
 - \[Serial Console Management \\(see page 11\\)\]\(#\)
 - \[Wired Ethernet Management \\(see page 11\\)\]\(#\)
 - \[Configuring the Hostname and Time Zone \\(see page 11\\)\]\(#\)
 - \[Installing the License \\(see page 12\\)\]\(#\)](#)
- [Configuring 4x10G Port Configuration \(Splitter Cables\) \(see page 13\)](#)
- [Testing Cable Connectivity \(see page 13\)](#)
- [Configuring Switch Ports \(see page 14\)
 - \[Layer 2 Port Configuration \\(see page 14\\)\]\(#\)
 - \[Layer 3 Port Configuration \\(see page 15\\)\]\(#\)](#)
- [Configuring a Loopback Interface \(see page 16\)](#)

What's New in Cumulus Linux 2.5.11

Cumulus Linux 2.5.11 is part of Cumulus Linux 2.5 ESR and as such, contains bug fixes only. The [release notes](#) contain information about the release as well as the fixed and known issues.

Open Source Contributions

Cumulus Networks has forked various software projects, like CFEngine, Netdev and some Puppet Labs packages in order to implement various Cumulus Linux features. The forked code resides in the Cumulus Networks [GitHub repository](#).

Cumulus Networks developed and released as open source some new applications as well.

The list of open source projects is on the [open source software](#) page.

Prerequisites

Prior intermediate Linux knowledge is assumed for this guide. You should be familiar with basic text editing, Unix file permissions, and process monitoring. A variety of text editors are pre-installed, including `vi` and `nano`.

You must have access to a Linux or UNIX shell. If you are running Windows, you should use a Linux environment like [Cygwin](#) as your command line tool for interacting with Cumulus Linux.



- If you're a networking engineer but are unfamiliar with Linux concepts, use [this reference guide](#) to see examples of the Cumulus Linux CLI and configuration options, and their equivalent Cisco Nexus 3000 NX-OS commands and settings for comparison. You can also [watch a series of short videos](#) introducing you to Linux in general and some Cumulus Linux-specific concepts in particular.

Hardware Compatibility List

You can find the most up to date hardware compatibility list (HCL) [here](#). Use the HCL to confirm that your switch model is supported by Cumulus Networks. The HCL is updated regularly, listing products by port configuration, manufacturer, and SKU part number.

Installing Cumulus Linux

This quick start guide walks you through the steps necessary for getting Cumulus Linux up and running on your switch, which includes:

1. Powering on the switch and entering ONIE, the Open Network Install Environment.
2. Installing Cumulus Linux on the switch via ONIE.
3. Booting into Cumulus Linux and installing the license.
4. Rebooting the switch to activate the switch ports.
5. Configuring switch ports and a loopback interface.

To install Cumulus Linux, you use [ONIE](#) (Open Network Install Environment), an extension to the traditional U-Boot software that allows for automatic discovery of a network installer image. This facilitates the ecosystem model of procuring switches, with a user's own choice of operating system loaded, such as Cumulus Linux.



- If Cumulus Linux is already installed on your switch, and you need to upgrade the software only, you can skip to [Upgrading Cumulus Linux \(see page 10\)](#) below.

The easiest way to install Cumulus Linux with ONIE is via local HTTP discovery:

1. If your host (like a laptop or server) is IPv6-enabled, make sure it is running a Web server.
If the host is IPv4-enabled, make sure it is running DHCP as well as a Web server.

2. [Download](#) the Cumulus Linux installation file to the root directory of the Web server. Rename this file `onie-installer`.
3. Connect your host via Ethernet cable to the management Ethernet port of the switch.
4. Power on the switch. The switch downloads the ONIE image installer and boots it. You can watch the progress of the install in your terminal. After the installation finishes, the Cumulus Linux login prompt appears in the terminal window.



These steps describe a flexible unattended installation method. You should not need a console cable. A fresh install via ONIE using a local Web server should generally complete in less than 10 minutes.

You have more options for installing Cumulus Linux with ONIE. Read [Installing a New Cumulus Linux Image](#) (see page 27) to install Cumulus Linux using ONIE in the following ways:

- DHCP/Web server with and without DHCP options
- Web server without DHCP
- FTP or TFTP without a Web server
- Local file
- USB

ONIE supports many other discovery mechanisms using USB (copy the installer to the root of the drive), DHCPv6 and DHCPv4, and image copy methods including HTTP, FTP, and TFTP. For more information on these discovery methods, refer to the [ONIE documentation](#).

After installing Cumulus Linux, you are ready to:

- Log in to Cumulus Linux on the switch.
- Install the Cumulus Linux license.
- Configure Cumulus Linux. This quick start guide provides instructions on configuring switch ports and a loopback interface.

Upgrading Cumulus Linux

If you already have Cumulus Linux installed on your switch and are upgrading to a maintenance release (X.Y.Z, like 2.5.1) from an earlier release in the same major and minor release family **only** (like 2.2.1 to 2.2.2, or 2.5.0 to 2.5.1), you can use various methods, including `apt-get`, to upgrade to the new version instead. See [Upgrading Cumulus Linux](#) (see page 19) for details.

Configuring Cumulus Linux

When bringing up Cumulus Linux for the first time, the management port makes a DHCPv4 request. To determine the IP address of the switch, you can cross reference the MAC address of the switch with your DHCP server. The MAC address should be located on the side of the switch or on the box in which the unit was shipped.

Login Credentials

The default installation includes one system account, *root*, with full system privileges, and one user account, *cumulus*, with *sudo* privileges. The *root* account password is set to null by default (which prohibits login), while the *cumulus* account is configured with this default password:

```
CumulusLinux!
```

In this quick start guide, you will use the *cumulus* account to configure Cumulus Linux.



For best security, you should change the default password (using the `passwd` command) before you configure Cumulus Linux on the switch.

All accounts except *root* are permitted remote SSH login; *sudo* may be used to grant a non-root account root-level access. Commands which change the system configuration require this elevated level of access.

For more information about *sudo*, read [Using sudo to Delegate Privileges \(see page 72\)](#).

Serial Console Management

Users are encouraged to perform management and configuration over the network, either in band or out of band. Use of the serial console is fully supported; however, many customers prefer the convenience of network-based management.

Typically, switches will ship from the manufacturer with a mating DB9 serial cable. Switches with ONIE are always set to a 115200 baud rate.

Wired Ethernet Management

Switches supported in Cumulus Linux always contain at least one dedicated Ethernet management port, which is named *eth0*. This interface is geared specifically for out-of-band management use. The management interface uses DHCPv4 for addressing by default. You can set a static IP address in the `/etc/network/interfaces` file:

```
auto eth0
iface eth0
    address 192.0.2.42/24
    gateway 192.0.2.1
```

Configuring the Hostname and Time Zone

To change the hostname, modify the `/etc/hostname` and `/etc/hosts` files with the desired hostname and reboot the switch. First, edit `/etc/hostname`:

```
cumulus@switch:~$ sudo vi /etc/hostname
```

Then replace the 127.0.1.1 IP address in `/etc/hosts` with the new hostname:

```
cumulus@switch:~$ sudo vi /etc/hosts
```

Reboot the switch:

```
cumulus@switch:~$ sudo reboot
```

To update the time zone, update the `/etc/timezone` file with the [correct timezone](#), run `dpkg-reconfigure --frontend noninteractive tzdata`, then reboot the switch:

```
cumulus@switch:~$ sudo vi /etc/timezone
cumulus@switch:~$ sudo dpkg-reconfigure --frontend noninteractive tzdata
cumulus@switch:~$ sudo reboot
```



It is possible to change the hostname without a reboot via a script available on [Cumulus Networks GitHub site](#).

Installing the License

Cumulus Linux is licensed on a per-instance basis. Each network system is fully operational, enabling any capability to be utilized on the switch with the exception of forwarding on switch panel ports. Only eth0 and console ports are activated on an unlicensed instance of Cumulus Linux. Enabling front panel ports requires a license.

You should have received a license key from Cumulus Networks or an authorized reseller. Here is a sample license key:

```
user@company.com|thequickbrownfoxjumpsoverthelazydog312
```

There are three ways to install the license onto the switch:

- Copy it from a local server. Create a text file with the license and copy it to a server accessible from the switch. On the switch, use the following command to transfer the file directly on the switch, then install the license file:

```
cumulus@switch:~$ scp user@my_server:/home/user/my_license_file.txt .
cumulus@switch:~$ sudo cl-license -i my_license_file.txt
```

- Copy the file to an HTTP server (not HTTPS), then reference the URL when you run `cl-license`:

```
cumulus@switch:~$ sudo cl-license -i <URL>
```

- Copy and paste the license key into the `cl-license` command:

```
cumulus@switch:~$ sudo cl-license -i  
<paste license key>  
^d
```

Once the license is installed successfully, reboot the system:

```
cumulus@switch:~$ sudo reboot
```

After the switch reboots, all front panel ports will be active. The front panel ports are identified as switch ports, and show up as `swp1`, `swp2`, and so forth.

Configuring 4x10G Port Configuration (Splitter Cables)

If you are using 4x10G DAC or AOC cables, edit the `/etc/cumulus/ports.conf` to enable support for these cables then [restart the `switchd` service \(see page 115\)](#) using the `sudo service switchd restart` command. For more details, see [Layer 1 and Switch Port Attributes \(see page 134\)](#).

Testing Cable Connectivity

By default, all data plane ports (every Ethernet port except the management interface, `eth0`) are disabled.

To test cable connectivity, administratively enable a port using `ip link set <interface> up`:

```
cumulus@switch:~$ sudo ip link set swp1 up
```

Run the following bash script, as root, to administratively enable all physical ports:

```
cumulus@switch:~$ sudo su -  
cumulus@switch:~$ for i in /sys/class/net/*; do iface=`basename $i`; if [[  
$iface == swp* ]]; then ip link set $iface up; fi done
```

To view link status, use `ip link show`. The following examples show the output of a port in "admin down", "down" and "up" mode, respectively:

```
# Administratively Down
swp1: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN mode
DEFAULt qlen 1000

# Administratively Up but Layer 2 protocol is Down
swp1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state
DOWN mode DEFAULt qlen 500

# Administratively Up, Layer 2 protocol is Up
swp1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
mode DEFAULt qlen 500
```

Configuring Switch Ports

Layer 2 Port Configuration

Cumulus Linux does not put all ports into a bridge by default. To configure a front panel port or create a bridge, edit the `/etc/network/interfaces` file. After saving the file, to activate the change, use the `ifup` command.

Examples

In the following configuration example, the front panel port `swp1` is placed into a bridge called `br0`:

```
auto br0
iface br0
    bridge-ports swp1
    bridge-stp on
```

To put a range of ports into a bridge, use the `glob` keyword. For example, add `swp1` through `swp10`, `swp12`, and `swp14` through `swp20` to `br0`:

```
auto br0
iface br0
    bridge-ports glob swp1-10 swp12 glob swp14-20
    bridge-stp on
```

To activate or apply the configuration to the kernel:

```
# First, check for typos:  
cumulus@switch:~$ sudo ifquery -a  
  
# Then activate the change if no errors are found:  
cumulus@switch:~$ sudo ifup -a
```

To view the changes in the kernel, use the `brctl` command:

```
cumulus@switch:~$ brctl show  
bridge name      bridge id          STP enabled    interfaces  
br0              8000.089e01cedcc2    yes           swp1
```



A script is available to generate a configuration that [places all physical ports in a single bridge](#).

Layer 3 Port Configuration

To configure a front panel port or bridge interface as a Layer 3 port, edit the `/etc/network/interfaces` file.

In the following configuration example, the front panel port `swp1` is configured a Layer 3 access port:

```
auto swp1  
iface swp1  
    address 10.1.1.1/30
```

To add an IP address to a bridge interface, include the address under the `iface` configuration in `/etc/network/interfaces`:

```
auto br0  
iface br0  
    address 10.2.2.1/24  
    bridge-ports glob swp1-10 swp12 glob swp14-20  
    bridge-stp on
```

To activate or apply the configuration to the kernel:

```
# First check for typos:  
cumulus@switch:~$ sudo ifquery -a
```

```
# Then activate the change if no errors are found:  
cumulus@switch:~$ sudo ifup -a
```

To view the changes in the kernel use the `ip addr show` command:

```
br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP  
link/ether 00:02:00:00:00:28 brd ff:ff:ff:ff:ff:ff  
inet 10.2.2.1/24 scope global br0  
  
swp1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP  
link/ether 44:38:39:00:6e:fe brd ff:ff:ff:ff:ff:ff  
inet 10.1.1.1/30 scope global swp1
```

Configuring a Loopback Interface

Cumulus Linux has a loopback preconfigured in `/etc/network/interfaces`. When the switch boots up, it has a loopback interface, called `lo`, which is up and assigned an IP address of 127.0.0.1.

To see the status of the loopback interface (`lo`), use the `ip addr show lo` command:

```
cumulus@switch:~$ ip addr show lo  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        inet6 ::1/128 scope host  
            valid_lft forever preferred_lft forever
```

Note that the loopback is up and is assigned an IP address of 127.0.0.1.

To add an IP address to a loopback interface, add it directly under the `iface lo inet loopback` definition in `/etc/network/interfaces`:

```
auto lo  
iface lo inet loopback  
    address 10.1.1.1
```



If an IP address is configured without a mask, as shown above, the IP address becomes a /32. So, in the above case, 10.1.1.1 is actually 10.1.1.1/32.

Multiple loopback addresses can be configured by adding additional address lines:

```
auto lo
iface lo inet loopback
    address 10.1.1.1
    address 172.16.2.1/24
```

Installation, Upgrading and Package Management

A Cumulus Linux switch can have up to two images of the operating system installed. This section discusses installing new and updating existing Cumulus Linux disk images, and configuring those images with additional applications (via packages) if desired.

Zero touch provisioning is a way to quickly deploy and configure new switches in a large-scale environment.

Managing Cumulus Linux Disk Images

The Cumulus Linux operating system resides on a switch as a *disk image*. Switches running Cumulus Linux can be configured with 2 separate disk images. This section discusses how to manage them including installation and upgrading.

Contents

(Click to expand)

- [Contents \(see page 18\)](#)
- [Commands \(see page 18\)](#)
- [Installing a New Cumulus Linux Image \(see page 18\)](#)
- [Upgrading Cumulus Linux \(see page 19\)](#)
- [Understanding Image Slots \(see page 19\)
 - \[PowerPC vs x86 vs ARM Switches \\(see page 20\\)\]\(#\)
 - \[PowerPC Image Slots \\(see page 20\\)\]\(#\)
 - \[x86 and ARM Image Slots \\(see page 21\\)\]\(#\)](#)
- [Reverting an Image to its Original Configuration \(PowerPC Only\) \(see page 24\)](#)
- [Reprovisioning the System \(Restart Installer\) \(see page 24\)](#)
- [Uninstalling All Images and Removing the Configuration \(see page 25\)](#)
- [Booting into Rescue Mode \(see page 25\)](#)
- [Inspecting Image File Contents \(see page 26\)](#)
- [Useful Links \(see page 27\)](#)

Commands

- [apt-get](#)
- [cl-img-install](#)
- [cl-img-select](#)
- [cl-img-clear-overlay](#)
- [cl-img-pkg](#)

Installing a New Cumulus Linux Image

For details, read the chapter, [Installing a New Cumulus Linux Image \(see page 27\)](#).

Upgrading Cumulus Linux

There are two ways you can upgrade Cumulus Linux:

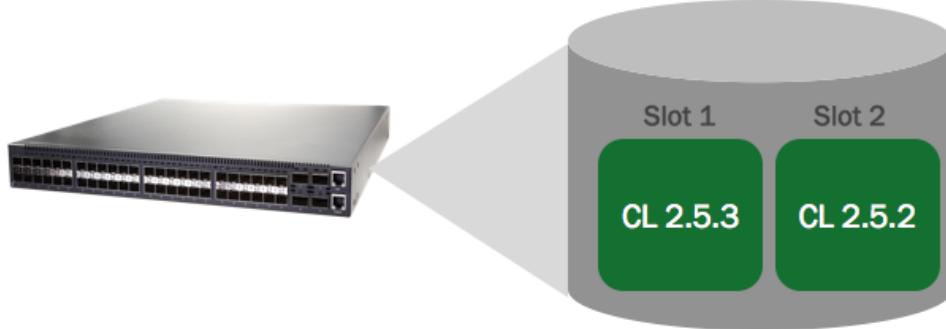
- Perform a binary (full image) install of the new version, running `cl-img-install` on the switch
- Upgrade only the changed packages, using `apt-get update` and `apt-get dist-upgrade`

The entire upgrade process is described in [Upgrading Cumulus Linux \(see page 37\)](#).

Understanding Image Slots

Cumulus Linux uses the concept of *image slots* to manage two separate Cumulus Linux images. The important terminology for the slots is as follows:

- **Active image slot:** The currently running image slot.
- **Primary image slot:** The image slot that is selected for the next boot. Often this is the same as the active image slot.
- **Alternate image slot:** The inactive image slot, **not** selected for the next boot.



To identify which slot is active, which slot is the primary, and which slot is alternate use the `cl-img-select` command:

```
cumulus@switch$ sudo cl-img-select
active => slot 1 (primary): 2.5.3-c4e83ad-201506011818-build
           slot 2 (alt     ): 2.5.2-727a0c6-201504132125-build
```

Slot 1 is the active slot, as indicated by the **active**. When the switch is rebooted, it will boot into slot 1, as indicated by **primary**. The **alternate** slot won't be booted into unless the user selects it.



`cl-img-select` displays the version of the software that was *initially* installed on the switch; if you've upgraded your switch, `cl-img-select` won't display the most current version of Cumulus Linux installed. The above switch had Cumulus Linux 2.5.3 installed initially in slot 1, and Cumulus Linux 2.5.2 initially installed in slot 2.

To see the current version of Cumulus Linux running on the switch, use `cat /etc/lsb-release`.

PowerPC vs x86 vs ARM Switches

The characteristics of the image slots vary, based on whether your switch is on a PowerPC, ARM or x86 platform. You can easily determine which platform the switch is on by using the `uname -m` command.

For example, on a PowerPC platform, `uname -m` outputs `ppc`:

```
cumulus@PPCswitch$ uname -m
ppc
```

While on an x86 platform, `uname -m` outputs `x86_64`:

```
cumulus@x86switch$ uname -m
x86_64
```

While on an ARM platform, `uname -m` outputs `armv7l`:

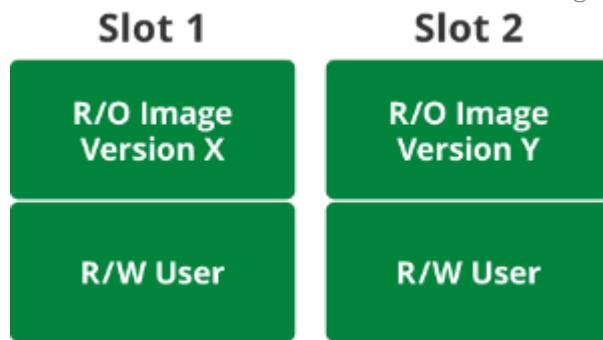
```
cumulus@ARMswitch$ uname -m
armv7l
```

You can also visit the HCL ([hardware compatibility list](#)) to look at your hardware to determine the processor type.

PowerPC Image Slots

Read more about PowerPC image slots

On the PowerPC platform, each image slot consists of a read-only Cumulus Linux base image overlaid with a read-write user area, as shown in the following diagram:



Files you edit and create reside in the read-write user overlay. This also includes any additional software you install on top of Cumulus Linux. After an install, the user overlay is empty.

PowerPC Image Slot Overlay Detailed Information

The root directory of an image slot on a PowerPC system is created using an `overlayfs` file system. The lower part of the overlay is a *read-only* `squashfs` file system containing the base Cumulus Linux image. The upper part of the overlay is a *read-write* directory containing all the user modifications.

The following table describes the mount points and directories used to create the overlay for image slots 1 and 2.

Slot Number	R/O squashfs device	R/O mount point	R/W block device	R/W directory
1	/dev/sysroot1	/mnt/root-ro	/dev/overlay_rw	/mnt/root-rw/config1
2	/dev/sysroot2	/mnt/root-ro	/dev/overlay_rw	/mnt/root-rw/config2



A single read-write partition provides separate read-write directories for the upper part of the overlay. The lower part of the overlay is a **partition**, while the upper part is a **directory**.

The following table describes all the interesting mount points.

Mount Point	File System	Purpose
/mnt/root-ro	squashfs	Contains the read-only base Cumulus Linux image.
/mnt/root-rw	ext2	Contains the read-write user directories for the overlay.
/	overlays	The union of /mnt/root-ro and /mnt/root-rw/config1 (or config2).
/mnt/persist	ext2	Contains the persistent user configuration applied to each image slot.
/mnt/initramfs	tmpfs	Contains the <code>initramfs</code> used at boot. Needed during shutdown.

x86 and ARM Image Slots

Read more about x86 image slots

Unlike PowerPC-based switches, there is no overlay for an x86-based or ARM-based switch; instead each slot is a logical volume in the physical partition, which you can manage with [LVM](#).

When you install Cumulus Linux on an x86 or ARM switch, the following entities are created on the disk:

- A disk partition using an ext4 file system that contains three logical volumes: two logical volumes named `sysroot1` and `sysroot2`, and the `/mnt/persist` logical volume. The logical volumes represent the Cumulus Linux image slots, so `sysroot1` is slot 1 and `sysroot2` is slot 2. `/mnt/persist` is where you store your [persistent configuration](#) (see page).
- A boot partition, shared by the logical volumes. Each volume mounts this partition as `/boot`.

Managing Slot Sizes

As space in a slot is used, you may need to increase the size of the root filesystem by increasing the size of the corresponding logical volume. This section shows you how to check current utilization and expand the filesystem as needed.

1. Check utilization on the root filesystem with the `df` command. In the following example, filesystem utilization is 16%:

```
cumulus@switch$ df -h /
Filesystem           Size  Used Avail Use% Mounted on
/dev/disk/by-uuid/64650289-cebf-4849-91ae-a34693fce2f1  4.0G
579M   3.2G  16%  /

```

2. To increase available space in the root filesystem, first use the `vgs` command to check the available space in the volume group. In this example, there is 6.34 Gigabytes of free space available in the volume group CUMULUS:

```
cumulus@switch$ sudo vgs
VG      #PV #LV #SN Attr   VSize   VFree
CUMULUS  1    3    0 wz--n- 14.36g 6.34g
```

3. Once you confirm the available space, determine the number of the currently active slot using `cl-img-select`.

```
cumulus@switch$ sudo cl-img-select | grep active
active => slot 1 (primary): 2.5.0-199c587-201501081931-build
```

`cl-img-select` indicates slot number 1 is active.

4. Resize the slot with the `lvresize` command. The following example increases slot size by 20 percent of total available space. Replace the "#" character in the example with the active slot number from the last step.

```
cumulus@switch$ sudo lvresize -l +20%FREE CUMULUS/SYSROOT#
Extending logical volume SYSROOT# to 5.27 GiB
Logical volume SYSROOT# successfully resized
```



The use of + is very important with the `lvresize` command. Issuing `lvresize` without the + results in the logical volume size being set directly to the specified size, rather than extended.

- Once the slot has been extended, use the `resize2fs` command to expand the filesystem to fit the new space in the slot. Again, replace the "#" character in the example with the active slot number.

```
cumulus@switch$ sudo resize2fs /dev/CUMULUS/SYSROOT#
resize2fs 1.42.5 (29-Jul-2012)
Filesystem at /dev/CUMULUS/SYSROOT# is mounted on /; on-line
resizing required
old_desc_blocks = 1, new_desc_blocks = 1
Performing an on-line resize of /dev/CUMULUS/SYSROOT# to 1381376
(4k) blocks.
The filesystem on /dev/CUMULUS/SYSROOT# is now 1381376 blocks long.
```

Accessing the Alternate Image Slot on x86 and ARM Platforms

It may be useful to access the content of the alternate slot to retrieve the configuration or logs.



`cl-img-install` fails while the alternate slot is mounted. It is important to unmount the alternate slot as shown in step 4 below when done.

- Determine which slot is the alternate with `cl-img-select`:

```
cumulus@switch$ sudo cl-img-select
active => slot 1 (primary): 2.5.3-c4e83ad-201506011818-build
slot 2 (alt      ): 2.5.2-727a0c6-201504132125-build
```

This output indicates slot 2 is the alternate slot.

- Create a mount point for the alternate slot:

```
cumulus@switch$ sudo mkdir /mnt/alt
```

- Mount the alternate slot to the mount point:

```
cumulus@switch$ sudo mount /dev/mapper/CUMULUS-SYSROOT# /mnt/alt
```

Where # is the number of the alternate slot.

The alternate slot is now accessible under `/mnt/alt`.

- Unmount the mount point `/mnt/alt` when done.

```
cumulus@switch$ cd /
```

```
cumulus@switch$ sudo umount /mnt/alt/
```

Reverting an Image to its Original Configuration (PowerPC Only)

On PowerPC-based systems, you may want to clear out the read-write user overlay area. Perhaps something was misconfigured, or was deleted by mistake, or some unneeded software was installed.

You can purge the read-write overlay using the `cl-img-clear-overlay` command, passing the slot number as an argument. For example, to purge the read-write overlay for image slot 2, run:

```
cumulus@switch:~$ sudo cl-img-clear-overlay 2
Success: Overlay configuration 2 will be re-initialized during the next
reboot.
```

 You must reboot the switch to complete the purge.

Reprovisioning the System (Restart Installer)

You can reprovision the system, wiping out the contents of both image slots and `/mnt/persist`.

To initiate the provisioning and installation process, use `cl-img-select -i`:

```
cumulus@switch:~$ sudo cl-img-select -i
WARNING:
WARNING: Operating System install requested.
WARNING: This will wipe out all system data.
WARNING:
Are you sure (y/N)? y
Enabling install at next reboot...done.
Reboot required to take effect.
```

 A reboot is required for the reinstall to begin.

 If you change your mind, you can cancel a pending reinstall operation by using `cl-img-select -c`:

```
cumulus@switch:~$ sudo cl-img-select -c
Cancelling pending install at next reboot...done.
```

Uninstalling All Images and Removing the Configuration

To remove all installed images and configurations, returning the switch to its factory defaults, use `cl-img-select -k`:

```
cumulus@switch:~$ sudo cl-img-select -k
WARNING:
WARNING: Operating System uninstall requested.
WARNING: This will wipe out all system data.
WARNING:
Are you sure (y/N)? y
Enabling uninstall at next reboot...done.
Reboot required to take effect.
```



A reboot is required for the uninstall to begin.



If you change your mind you can cancel a pending uninstall operation by using `cl-img-select -c`:

```
cumulus@switch:~$ sudo cl-img-select -c
Cancelling pending uninstall at next reboot...done.
```

Booting into Rescue Mode

If your system becomes broken in some way, you may be able to correct things by booting into ONIE rescue mode. In rescue mode, the file systems are unmounted and you can use various Cumulus Linux utilities to try and fix the problem.

To reboot the system into the ONIE rescue mode, use `cl-img-select -r`:

```
cumulus@switch:~$ sudo cl-img-select -r
WARNING:
WARNING: Rescue boot requested.
WARNING:
Are you sure (y/N)? y
Enabling rescue at next reboot...done.
Reboot required to take effect.
```



 A reboot is required to boot into rescue mode.

-  If you change your mind you can cancel a pending rescue boot operation by using `cl-img-select -c`:

```
cumulus@switch:~$ sudo cl-img-select -c
Cancelling pending rescue at next reboot...done.
```

Inspecting Image File Contents

From a running system you can display the contents of a Cumulus Linux image file using `cl-img-pkg -d`:

```
cumulus@switch:~$ sudo cl-img-pkg -d /var/lib/cumulus/installer/onie-
installer
Verifying image checksum ... OK.
Preparing image archive ... OK.
Control File Contents
=====
Description: Cumulus Linux
OS-Release: 2.1.0-0556262-201406101128-NB
Architecture: amd64
Date: Tue, 10 Jun 2014 11:44:28 -0700
Installer-Version: 1.2
Platforms: im_n29xx_t40n mlx_sx1400_i73612 dell_s6000_s1220
Homepage: http://www.cumulusnetworks.com/

Data Archive Contents
=====
  128 2014-06-10 18:44:26 file.list
    44 2014-06-10 18:44:27 file.list.sha1
104276331 2014-06-10 18:44:27 sysroot-internal.tar.gz
    44 2014-06-10 18:44:27 sysroot-internal.tar.gz.sha1
  5391348 2014-06-10 18:44:26 vmlinuz-initrd.tar.xz
    44 2014-06-10 18:44:27 vmlinuz-initrd.tar.xz.sha1
cumulus@switch:~$
```

You can also extract the image files to the current directory with the `-e` option:

```
cumulus@switch:~$ sudo cl-img-pkg -e /var/lib/cumulus/installer/onie-
installer
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

```

file.list
file.list.sha1
sysroot-internal.tar.gz
sysroot-internal.tar.gz.sha1
vmlinuz-initrd.tar.xz
vmlinuz-initrd.tar.xz.sha1
Success: Image files extracted OK.
cumulus@switch:~$ sudo ls -l
total 107120
-rw-r--r-- 1 1063 3000      128 Jun 10 18:44 file.list
-rw-r--r-- 1 1063 3000      44 Jun 10 18:44 file.list.sha1
-rw-r--r-- 1 1063 3000 104276331 Jun 10 18:44 sysroot-internal.tar.gz
-rw-r--r-- 1 1063 3000      44 Jun 10 18:44 sysroot-internal.tar.gz.
sha1
-rw-r--r-- 1 1063 3000 5391348 Jun 10 18:44 vmlinuz-initrd.tar.xz
-rw-r--r-- 1 1063 3000      44 Jun 10 18:44 vmlinuz-initrd.tar.xz.
sha1

```

Useful Links

- Open Network Install Environment (ONIE) Home Page

Installing a New Cumulus Linux Image

Before you install Cumulus Linux, the switch can be in two different states:

- The switch has no image on it (so the switch is only running [ONIE](#)) or you desire or require a clean installation. In this case, you can install Cumulus Linux in one of the following ways, using:
 - DHCP/a Web server with DHCP options (see page 28)
 - DHCP/a Web server without DHCP options (see page 29)
 - A Web server with no DHCP (see page 29)
 - FTP or TFTP without a Web server (see page 30)
 - Local file installation (see page 30)
 - USB (see page 30)
- The switch already has Cumulus Linux installed on it, so you only need to [upgrade it](#) (see page 37)



[ONIE](#) is an open source project, equivalent to PXE on servers, that enables the installation of network operating systems (NOS) on bare metal switches.

Understanding these Examples

- This sections in this chapter are ordered from the most repeatable to the least repeatable methods. For instance, DHCP can scale to hundreds of switch installs with zero manual input, compared to something like USB installs. Installing via USB is fine for a single switch here and there but is not scalable.
- You can name your Cumulus Linux installer binary using any of the [ONIE naming schemes](#) mentioned here.

- In the examples below, [PLATFORM] can be any supported Cumulus Linux platform, such as `x86_64`, `arm`, or `powerpc`.

Contents

Click to expand...

- Understanding these Examples (see page 27)
- Contents (see page 28)
- Installing via a DHCP/Web Server Method with DHCP Options (see page 28)
- Installing via a DHCP/Web Server Method without DHCP Options (see page 29)
- Installing via a Web Server with no DHCP (see page 29)
- Installing via FTP or TFTP without a Web Server (see page 30)
- Installing via a Local File (see page 30)
- Installing via USB (see page 30)
 - Preparing for USB Installation (see page 31)
 - Instructions for x86 Platforms (see page 32)
 - Instructions for PowerPC and ARM Platforms (see page 35)
- Installing a New Image when Cumulus Linux Is already Installed (see page 37)

Installing via a DHCP/Web Server Method with DHCP Options

Installing Cumulus Linux in this manner is as simple as setting up a DHCP/Web server on your laptop and connecting the `eth0` management port of the switch to your laptop.

Once you connect the cable, the installation proceeds as follows:

1. The bare metal switch boots up and asks for an address (DHCP request).
2. The DHCP server acknowledges and responds with DHCP option 114 and the location of the installation image.
3. ONIE downloads the Cumulus Linux binary, installs and reboots.
4. Success! You are now running Cumulus Linux.



The most common method is for you to send DHCP option 114 with the entire URL to the Web server (this could be the same system). However, there are many other ways to use DHCP even if you don't have full control over DHCP. See the ONIE user guide for help.

Here's an example DHCP configuration with an ISC DHCP server:

```

subnet 172.0.24.0 netmask 255.255.255.0 {
    range 172.0.24.20 172.0.24.200;
    option www-server = "http://172.0.24.14/onie-installer-[PLATFORM]" ;
}

```

Here's an example DHCP configuration with [dnsmasq](#) (static address assignment):

```

dhcp-host=sw4,192.168.100.14,6c:64:1a:00:03:ba,set:sw4
dhcp-option>tag:sw4,114,"http://roz.rtplab.test/onie-installer-[PLATFORM]"

```

Don't have a Web server? There is a [free Apache example](#) you can utilize.

Installing via a DHCP/Web Server Method without DHCP Options

If you have a laptop on same network and the switch can pull DHCP from the corporate network, but you cannot modify DHCP options (maybe it's controlled by another team), do the following:

1. Place the Cumulus Linux binary in a directory on the Web server.
2. Run the `onie-nos-install` command manually, since DHCP options can't be modified:

```

ONIE:/ #onie-nos-install http://10.0.1.251/path/to/cumulus-install-
[PLATFORM].bin

```

Installing via a Web Server with no DHCP

Use the following method if your laptop is on the same network as the switch `eth0` interface but no DHCP server is available.

One thing to note is ONIE is in [discovery mode](#), so if you are setting a static IPv4 address for the `eth0` management port, you need to disable discovery mode or else ONIE may get confused.

1. To disable discovery mode, run:

```

onie# onie-discovery-stop

```

or, on older ONIE versions if that command isn't supported:

```

onie# /etc/init.d/discover.sh stop

```

2. Assign a static address to `eth0` via ONIE (using `ip addr add`):

```
ONIE:/ #ip addr add 10.0.1.252/24 dev eth0
```

3. Place the Cumulus Linux installer image in a directory on your Web server.
4. Run the `onie-nos-install` command manually since there are no DHCP options:

```
ONIE:/ #onie-nos-install http://10.0.1.251/path/to/cumulus-install-[PLATFORM].bin
```

Installing via FTP or TFTP without a Web Server

1. Set up DHCP or static addressing for eth0, as in the examples above.
2. If you are utilizing static addressing, disable ONIE discovery mode.
3. Place the Cumulus Linux installer image into a TFTP or FTP directory.
4. If you are not utilizing DHCP options, run one of the following commands (`tftp` for TFTP or `ftp` for FTP):

```
ONIE# onie-nos-install ftp://local-ftp-server/cumulus-install-[PLATFORM].bin
```

```
ONIE# onie-nos-install tftp://local-tftp-server/cumulus-install-[PLATFORM].bin
```

Installing via a Local File

1. Set up DHCP or static addressing for eth0, as in the examples above.
2. If you are utilizing static addressing, disable ONIE discovery mode.
3. Use `scp` to copy the Cumulus Linux binary to the switch.
Note: Windows users can use [WinScp](#).
4. Run the following command:

```
ONIE# onie-nos-install /path/to/local/file/cumulus-install-[PLATFORM].bin
```

Installing via USB

Following the steps below produces a clean installation of Cumulus Linux. This wipes out all pre-existing configuration files that may be present on the switch. Instructions are offered for x86, ARM and PowerPC platforms, and also cover the installation of a license after the software installation.



Make sure to [back up \(see page 37\)](#) any important configuration files that you may need to restore the configuration of your switch after the installation finishes.

Preparing for USB Installation

1. Download the appropriate Cumulus Linux image for your x86, ARM or PowerPC platform from the [Cumulus Networks Downloads](#) page.
2. Prepare your flash drive by formatting in one of the supported formats: FAT32, vFAT or EXT2.

Optional: Preparing a USB Drive inside Cumulus Linux



It is possible that you could severely damage your system with the following utilities, so please use caution when performing the actions below!

- a. Insert your flash drive into the USB port on the switch running Cumulus Linux and log in to the switch.
- b. Determine and note at which device your flash drive can be found by using output from `cat /proc/partitions` and `sudo fdisk -l [device]`. For example, `sudo fdisk -l /dev/sdb`.



These instructions assume your USB drive is the `/dev/sdb` device, which is typical if the USB stick was inserted after the machine was already booted. However, if the USB stick was plugged in during the boot process, it is possible the device could be `/dev/sda`. Make sure to modify the commands below to use the proper device for your USB drive!

- c. Create a new partition table on the device:

```
sudo parted /dev/sdb mklabel msdos
```



The `parted` utility should already be installed. However, if it is not, install it with:
`sudo apt-get install parted`

- d. Create a new partition on the device:

```
sudo parted /dev/sdb -a optimal mkpart primary 0% 100%
```

- e. Format the partition to your filesystem of choice using ONE of the examples below:

```
sudo mkfs.ext2 /dev/sdb1  
sudo mkfs.msdos -F 32 /dev/sdb1
```

```
sudo mkfs.vfat /dev/sdb1
```

⚠ To use `mkfs.msdos` or `mkfs.vfat`, you need to install the `dosfstools` package from the [Debian software repositories](#) (step 3 here shows you how to add repositories from Debian), as they are not included by default.

- f. To continue installing Cumulus Linux, mount the USB drive in order to move files to it.

```
sudo mkdir /mnt/usb  
sudo mount /dev/sdb1 /mnt/usb
```

3. Copy the image and license files over to the flash drive and rename the image file to:

- `onie-installer-x86_64`, if installing on an x86 platform
- `onie-installer-powerpc`, if installing on a PowerPC platform
- `onie-installer-arm`, if installing on an ARM platform

⚠ You can also use any of the [ONIE naming schemes mentioned here](#).

❗ When using a Mac or Windows computer to rename the installation file the file extension may still be present. Make sure to remove the file extension otherwise ONIE will not be able to detect the file!

4. Insert the USB stick into the switch, then continue with the appropriate instructions below for your x86, ARM or PowerPC platform.

Instructions for x86 Platforms

Click to expand x86 instructions...

1. Prepare the switch for installation:

- If the switch is offline, connect to the console and power on the switch.
- If the switch is already online in Cumulus Linux, connect to the console and reboot the switch into the ONIE environment with the `sudo cl-img-select -i` command, followed by `sudo reboot`. Then skip to step 4 below.
- If the switch is already online in ONIE, use the `reboot` command.

⚠ SSH sessions to the switch get dropped after this step. To complete the remaining instructions, connect to the console of the switch. Cumulus Linux switches display their boot process to the console, so you need to monitor the console specifically to complete the next step.

- Monitor the console and select the ONIE option from the first GRUB screen shown below.

```
GNU GRUB version 1.99-27+deb7u2

+-----+
| Cumulus Linux 2.5.3a-3b46bef-201509041633-build - slot 1
| Cumulus Linux 2.5.3a-3b46bef-201509041633-build - slot 1 (recovery mode)
| Cumulus Linux 2.5.3a-3b46bef-201509041633-build - slot 2
| Cumulus Linux 2.5.3a-3b46bef-201509041633-build - slot 2 (recovery mode)
| ONIE
+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line.
```

- Cumulus Linux on x86 uses GRUB chainloading to present a second GRUB menu specific to the ONIE partition. No action is necessary in this menu to select the default option *ONIE: Install OS*.

```
GNU GRUB version 2.02~beta2+e4a1fe391

+-----+
| *ONIE: Install OS
| ONIE: Rescue
| ONIE: Uninstall OS
| ONIE: Update ONIE
| ONIE: Embed ONIE
+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line.
```

- At this point, the USB drive should be automatically recognized and mounted. The image file should be located and automatic installation of Cumulus Linux should begin. Here is some sample output:

```
ONIE: OS Install Mode ...
Version : quanta_common_rangeley-2014.05.05-6919d98-201410171013
Build Date: 2014-10-17T10:13+0800
Info: Mounting kernel filesystems... done.
Info: Mounting LABEL=ONIE-BOOT on /mnt/onie-boot ...
initializing eth0...
scsi 6:0:0:0: Direct-Access SanDisk Cruzer Facet 1.26 PQ: 0
ANSI: 6
```

```

sd 6:0:0:0: [sdb] 31266816 512-byte logical blocks: (16.0 GB/14.9
GiB)
sd 6:0:0:0: [sdb] Write Protect is off
sd 6:0:0:0: [sdb] Write cache: disabled, read cache: enabled,
doesn't support DPO or FUA
sd 6:0:0:0: [sdb] Attached SCSI disk
<...snip...
ONIE: Executing installer: file://dev/sdb1/onie-installer-x86_64
Verifying image checksum ... OK.
Preparing image archive ... OK.
Dumping image info...
Control File Contents
=====
Description: Cumulus Linux
OS-Release: 2.5.3a-3b46bef-201509041633-build
Architecture: amd64
Date: Fri, 04 Sep 2015 17:10:30 -0700
Installer-Version: 1.2
Platforms: accton_as5712_54x accton_as6712_32x
mlx_sx1400_i73612 dell_s6000_s1220 dell_s4000_c2338
dell_s3000_c2338 cel_redstone_xp cel_smallstone_xp cel_pebble
quanta_panther quanta_ly8_rangeley quanta_ly6_rangeley
quanta_ly9_rangeley
Homepage: http://www.cumulusnetworks.com/

```

5. After installation completes, the switch automatically reboots into the newly installed instance of Cumulus Linux.
6. Determine and note at which device your flash drive can be found by using output from `cat /proc/partitions` and `sudo fdisk -l [device]`. For example, `sudo fdisk -l /dev/sdb`.



These instructions assume your USB drive is the `/dev/sdb` device, which is typical if the USB stick was inserted after the machine was already booted. However, if the USB stick was plugged in during the boot process, it is possible the device could be `/dev/sda`. Make sure to modify the commands below to use the proper device for your USB drive!

7. Create a mount point to mount the USB drive to:

```
sudo mkdir /mnt/mountpoint
```

8. Mount the USB drive to the newly created mount point:

```
sudo mount /dev/sdb1 /mnt/mountpoint
```

9. Install your license file with the `cl-license` command:

```
sudo cl-license -i /mnt/mountpoint/license.txt
```

10. Check that your license is installed with the `cl-license` command.
11. Reboot the switch to utilize the new license.

```
sudo reboot
```

Instructions for PowerPC and ARM Platforms

Click to expand PowerPC instructions...

1. Prepare the switch for installation:

- If the switch is offline, connect to the console and power on the switch.
- If the switch is already online in Cumulus Linux, connect to the console and reboot the switch into the ONIE environment with the `sudo cl-img-select -i` command, followed by `sudo reboot`. Then skip to step 4.
- If the switch is already online in ONIE, use the `reboot` command.



SSH sessions to the switch get dropped after this step. To complete the remaining instructions, connect to the console of the switch. Cumulus Linux switches display their boot process to the console, so you need to monitor the console specifically to complete the next step.

2. Interrupt the normal boot process before the countdown (shown below) completes. Press any key to stop the autobooting.

```
U-Boot 2013.01-00016-gddbf4a9-dirty (Feb 14 2014 - 16:30:46)
Accton: 1.4.0.5
CPU0: P2020, Version: 2.1, (0x80e20021)
Core: E500, Version: 5.1, (0x80211051)
Clock Configuration:
  CPU0:1200 MHz, CPU1:1200 MHz,
  CCB:600 MHz,
  DDR:400 MHz (800 MT/s data rate) (Asynchronous), LBC:37.500 MHz
  L1: D-cache 32 kB enabled
    I-cache 32 kB enabled
<...snip...
USB: USB2513 hub OK
Hit any key to stop autoboot: 0
```

3. A command prompt appears, so you can run commands. Execute the following command:

```
run onie_bootcmd
```

- At this point the USB drive should be automatically recognized and mounted. The image file should be located and automatic installation of Cumulus Linux should begin. Here is some sample output:

```

Loading Open Network Install Environment ...
Platform: powerpc-as6701_32x-r0
Version : 1.6.1.3
WARNING: adjusting available memory to 30000000
## Booting kernel from Legacy Image at ec040000 ...
  Image Name: as6701_32x.1.6.1.3
  Image Type: PowerPC Linux Multi-File Image (gzip compressed)
  Data Size: 4456555 Bytes = 4.3 MiB
  Load Address: 00000000
  Entry Point: 00000000
  Contents:
    Image 0: 3738543 Bytes = 3.6 MiB
    Image 1: 706440 Bytes = 689.9 KiB
    Image 2: 11555 Bytes = 11.3 KiB
  Verifying Checksum ... OK
## Loading init Ramdisk from multi component Legacy Image at
ec040000 ...
## Flattened Device Tree from multi component Image at EC040000
  Booting using the fdt at 0xec47d388
  Uncompressing Multi-File Image ... OK
  Loading Ramdisk to 2ff53000, end 2fffff788 ... OK
  Loading Device Tree to 03ffa000, end 03ffd22 ... OK
<....snip...
ONIE: Starting ONIE Service Discovery
ONIE: Executing installer: file://dev/sdb1/onie-installer-powerpc
Verifying image checksum ... OK.
Preparing image archive ... OK.
Dumping image info...
Control File Contents
=====
Description: Cumulus Linux
OS-Release: 2.5.3a-3b46bef-201509041633-build
Architecture: powerpc
Date: Fri, 04 Sep 2015 17:08:35 -0700
Installer-Version: 1.2
Platforms: accton_as4600_54t, accton_as6701_32x, accton_5652,
accton_as5610_52x, dni_6448, dni_7448, dni_c7448n, cel_kennisis,
cel_redstone, cel_smallstone, cumulus_p2020, quanta_lb9,
quanta_ly2, quanta_ly2r, quanta_ly6_p2020
Homepage: http://www.cumulusnetworks.com/

```

- After installation completes, the switch automatically reboots into the newly installed instance of Cumulus Linux.
- Determine and note at which device your flash drive can be found by using output from `cat /proc/partitions` and `sudo fdisk -l [device]`. For example, `sudo fdisk -l /dev/sdb`.



These instructions assume your USB drive is the `/dev/sdb` device, which is typical if the USB stick was inserted after the machine was already booted. However, if the USB stick was plugged in during the boot process, it is possible the device could be `/dev/sda`. Make sure to modify the commands below to use the proper device for your USB drive!

7. Create a mount point to mount the USB drive to:

```
sudo mkdir /mnt/mountpoint
```

8. Mount the USB drive to the newly created mount point:

```
sudo mount /dev/sdb1 /mnt/mountpoint
```

9. Install your license file with the `cl-license` command:

```
sudo cl-license -i /mnt/mountpoint/license.txt
```

10. Check that your license is installed with the `cl-license` command.

11. Reboot the switch to utilize the new license.

```
sudo reboot
```

Installing a New Image when Cumulus Linux Is already Installed

Follow these upgrade steps for both major and minor releases, where:

- A major release upgrade is 2.X.X to 3.X.X (e.g. 1.5.1 to 2.5.0)
- A minor release upgrade is X.2.X to X.3.X (e.g. 2.2.0 to 2.5.5)

For more information, see [Upgrading Cumulus Linux \(see page 45\)](#).

Upgrading Cumulus Linux

Cumulus Networks software melds the Linux host world with the networking devices world. Each world comes with its own paradigm on how to upgrade software. Before we discuss the various ways to upgrade Cumulus Linux switches, let's review the general considerations and strategies used to upgrade network devices and Linux hosts.

Contents

Click to expand...

- [Contents \(see page 37\)](#)
- [Upgrades: Comparing the Network Device Worldview vs. the Linux Host Worldview \(see page 38\)](#)
 - [Manual vs. Automated Configuration \(see page 38\)](#)

- Locations of Configuration Data vs. Executables (see page 38)
- Pre-deployment Testing of Production Environments (see page 39)
- Upgrade Procedure (see page 39)
- Rollback Procedure (see page 39)
- Third Party Packages (see page 40)
- Upgrading Cumulus Linux Devices: Strategies and Processes (see page 40)
 - Automated Configuration Is Preferred over Manual Configuration (see page 40)
 - Out-of-Band Management Is Worth the Investment (see page 40)
 - Pre-Deployment Testing of New Releases Is Advised and Enabled (see page 41)
 - Understanding the Locations of Configuration Data for Management, Migration, and Backup (see page 41)
 - Upgrading Switches in an MLAG Pair (see page 44)
- Upgrading Cumulus Linux: Choosing between a Binary Install vs. Package Upgrade (see page 45)
 - Upgrading via Binary Install (cl-img-install) (see page 45)
 - Upgrading Using Package Installs (apt-get update && apt-get dist-upgrade) (see page 47)
- Using Automation Tools to Back Up Configurations (see page 49)
- Rolling Back a Cumulus Linux Installation (see page 50)
 - Rolling Back after Using Binary Install (see page 50)
 - Rolling Back after Using Package Install (see page 50)
- Third Party Package Considerations (see page 50)
- Caveats while Upgrading Cumulus Linux 2.5.x (see page 50)

Upgrades: Comparing the Network Device Worldview vs. the Linux Host Worldview

Manual vs. Automated Configuration

Historically, *network devices* were configured in place, and most network devices required customized configurations, which led predominantly to configuring the hardware manually. A lack of standardization between vendors, device types, and device roles hampered the development of APIs and automation tools. However, in the case of very large data centers, configurations became uniform and repeatable, and therefore scriptable. Some larger enterprises had to develop their own custom scripts to roll out data center network configurations. Virtually no industry-standard provisioning tools existed.

In contrast to data center network devices, *Linux hosts* in the data center number in the thousands and tend to have similar configurations. This increased scale led Linux sysadmins long ago to move to common tools to automate installation and configuration, since manually installing and configuring hosts did not work at the scale of a data center. Nearly all tasks are done via commonly available provisioning and orchestration tools.

Locations of Configuration Data vs. Executables

Network devices generally separate configuration data from the executable code. On bootup, the executable code looks into a different file system and retrieves the configuration file or files, parses the text and uses that data to configure the software options for each software subsystem. The model is very centralized,

with the executables generally being packaged together, and the configuration data following a set of rules that can be read by a centralized parser. Each vendor controls the configuration format for the entire box, since each vendor generally supports only their own software. This made sense since the platform was designed as an application-specific appliance.

Since a *Linux host* is a general purpose platform, with applications running on top of it, the locations of the files are much more distributed. Applications install and read their configuration data from text files usually stored in the /etc directory tree. Executables are generally stored in one of several *bin* directories, but the bin and etc directories are often on the same physical device. Since each *module* (application or executable) was often developed by a different organization and shared with the world, each module was responsible for its own configuration data format. Most applications are community supported, and while there are some generally accepted guiding principles on how their configuration data is formatted, no central authority exists to control or ensure compliance.

Pre-deployment Testing of Production Environments

Historically, the cost of *network device* testing has been hampered by the cost of a single device. Setting up an appropriately sized lab topology can be very expensive. As a result, it is difficult to do comprehensive topology-based testing of a release before deploying it. Thus, many network admins cannot or will not do comprehensive system testing of a new release before deploying it.

Alternatively, the cost of a *Linux host* is cheap (or nearly free when using virtualization), so rigorous testing of a release before deploying it is not encumbered by budgeting concerns. Most sysadmins extensively test new releases in the complete application environment.

Upgrade Procedure

Both network admins and sysadmins generally plan upgrades only to gain new functionality or to get bug fixes when the workarounds become too onerous. The goal is to reduce the number of upgrades as much as possible.

The *network device* upgrade paradigm is to leave the configuration data in place, and *replace the executable files* either all at once from a single binary image or in large chunks (subsystems). A full release upgrade comes with risk due to unexpected behavior changes in subsystems where the admin did not anticipate or need changes.

The *Linux host* upgrade paradigm is to independently *upgrade a small list of packages* while leaving most of the OS untouched. Changing a small list of packages reduces the risk of unintended consequences. Usually upgrades are a "forward only" paradigm, where the sysadmins generally plan to move to the latest code within the same major release when needed. Every few years, when a new kernel train is released, a major upgrade is planned. A major upgrade involves wiping and replacing the entire OS and migrating configuration data.

Rollback Procedure

Even the most well planned and tested upgrades can result in unforeseen problems, and sometimes the best solution to new problems is to roll back to the previous state.

Since *network devices* clearly separate data and executables, generally the process is to *overwrite the new release executable* with the previously running executable. If the configuration was changed by the newer release, then you either have to manually back out or repair the changes, or restore from an already backed up configuration.

The *Linux host* scenario can be more complicated. There are three main approaches:

- Back out individual packages: If the problematic package is identified, the sysadmin can downgrade the affected package directly. In rare cases the configuration files may have to be restored from backup, or edited to back out any changes that were automatically made by the upgrade package.

- Flatten and rebuild: If the OS becomes unusable, you can use orchestration tools to reinstall the previous OS release from scratch and then automatically rebuild the configuration.
- Backup and restore: Another common strategy is to restore to a previous state via a backup captured before the upgrade.

Third Party Packages

Third party packages are rare in the *network device* world. Because the network OS is usually proprietary, third party packages are usually packaged by the network device vendor and upgrades of those packages is handled by the network device upgrade system.

Third party packages in *Linux host* world often use the same package system as the distribution into which it is to be installed (for example, Debian uses `apt-get`). Or the package may be compiled and installed by the sysadmin. Configuration and executable files generally follow the same filesystem hierarchy standards as other applications.

Upgrading Cumulus Linux Devices: Strategies and Processes

Because Cumulus Linux is both Linux *and* a network device, it has characteristics of both paradigms. The following describes the Cumulus Linux paradigm with respect to upgrade planning and execution.

Automated Configuration Is Preferred over Manual Configuration

Because Cumulus Linux is Linux, Cumulus Networks recommends that even with small networks or test labs, network admins should make the jump to deploy, provision, configure, and upgrade switches using automation from the very beginning. The small up front investment of time spent learning an orchestration tool, even to provision a small number of Cumulus Linux devices, will pay back dividends for a long time. The biggest gain is realized during the upgrade process, where the network admin can quickly upgrade dozens of devices in a repeatable manner.

Switches, like servers, should be treated like *cattle, not pets*.

Out-of-Band Management Is Worth the Investment

Because network devices are reachable via the IP addresses on the front panel ports, many network admins of small-to-medium sized networks use *in-band* networks to manage their switches. In this design, management traffic like SSH, SNMP, and console server connections use the same networks that regular network traffic traverses — there is no separation between the *management plane* and the *data plane*. Larger data centers create a separate *out-of-band* network with a completely separate subnet and reachability path to attach to the management ports — that is accessible via `eth0` and the serial console.

This is a situation where smaller companies should learn from the big companies. A separate management network isn't free, but it is relatively cheap. With an inexpensive **Cumulus RMP** management switch, an inexpensive console server, and a separate cable path, up to 48 devices can be completely controlled via the out-of-band network in the case of a network emergency.

There are many scenarios where in-band networking can fail and leave the network admin waiting for someone to drive to the data center or remote site to connect directly to the console of a misconfigured or failing device. The cost of one outage would usually more than pay for the investment in a separate network. For even more security, attach remote-controllable power distribution units (PDUs) in each rack to the management network, so you can have complete control to remote power cycle every device in that rack.

Pre-Deployment Testing of New Releases Is Advised and Enabled

White box switches and virtualization (Cumulus VX) brings the cost of networking devices down, so network admins' testing of their own procedures, configurations, applications, and network topology in an appropriately-sized lab topology becomes extremely affordable.

Understanding the Locations of Configuration Data for Management, Migration, and Backup

As with other Linux distributions, the `/etc` directory is the primary location for all configuration data in Cumulus Linux. You can use the [Config File Migration script](#) to identify, archive and migrate configuration files that have changed since the image was installed.

The table below lists the most likely and recommended files to back up and migrate to a new release, but any file that has been changed would need to be examined:

Network Configuration Files

File Name and Location	Explanation	Cumulus Linux Documentation	Debian Documentation
<code>/etc/network/</code>	Network configuration files, most notably <code>/etc/network/interfaces</code> and <code>/etc/network/interfaces.d/</code>	Configuring and Managing Network Interfaces (see page 121)	wiki.debian.org/NetworkConfiguration
<code>/etc/resolv.conf</code>	DNS resolution	Not unique to Cumulus Linux: wiki.debian.org/NetworkConfiguration#The_resolv.conf_configuration_file	www.debian.org/doc/manuals/debian-reference/ch05.en.html
<code>/etc/quagga/</code>	Routing application (responsible for BGP and OSPF)	Quagga Overview (see page 344)	packages.debian.org/wheezy/quagga
<code>/etc/hostname</code>	Configuration file for the hostname of the switch	Quick Start Guide#ConfiguringtheHostnameandTimeZone (see page 11)	wiki.debian.org/HowTo/ChangeHostname
	Breakout cable configuration file	Layer 1 and Switch Port Attributes#ConfiguringBreakoutPorts (see page 139)	N/A; please read the guide on breakout cables

File Name and Location	Explanation	Cumulus Linux Documentation	Debian Documentation
/etc/cumulus/ports.conf			
/etc/cumulus/switchd.conf	Switchd configuration	Configuring switchd (see page 112)	N/A; please read the guide on switchd configuration

Additional Commonly Used Files

File Name and Location	Explanation	Cumulus Linux Documentation	Debian Documentation
/etc/motd	Message of the day	Not unique to Cumulus Linux	wiki.debian.org/motd#Wheezy
/etc/passwd	User account information	Not unique to Cumulus Linux	www.debian.org/doc/manuals/debian-reference/ch04.en.html
/etc/shadow	Secure user account information	Not unique to Cumulus Linux	www.debian.org/doc/manuals/debian-reference/ch04.en.html
/etc/group	Defines user groups on the switch	Not unique to Cumulus Linux	www.debian.org/doc/manuals/debian-reference/ch04.en.html
/etc/lldpd.conf	Link Layer Discover Protocol (LLDP) daemon configuration	Link Layer Discovery Protocol (see page 165)	packages.debian.org/wheezy/llpd
/etc/lldpd.d/	Configuration directory for llpd	Link Layer Discovery Protocol (see page 165)	packages.debian.org/wheezy/llpd
/etc/nsswitch.conf	Name Service Switch (NSS) configuration file	LDAP Authentication and Authorization (see page 79)	wiki.debian.org/LDAP/NSS
/etc/ssh/	SSH configuration files		wiki.debian.org/SSH

File Name and Location	Explanation	Cumulus Linux Documentation	Debian Documentation
		SSH for Remote Access (see page 70)	
/etc/ldap/ldap.conf	Lightweight Directory Access Protocol configuration file	LDAP Authentication and Authorization (see page 79)	www.debian.org/doc/manuals/debian-reference/ch04.en.html

- If you are using the root user account, consider including `/root/`.
- If you have custom user accounts, consider including `/home/<username>/`.

Files That Should Never Be Migrated Between Versions or Boxes

File Name and Location	Explanation
/etc/adjtime	System clock adjustment data. NTP manages this automatically. It is incorrect when the switch hardware is replaced. Do not copy.
/etc/bcm.d/	Per-platform hardware configuration directory, created on first boot. Do not copy.
/etc/blkid.tab	Partition table. It should not be modified manually. Do not copy.
/etc/blkid.tab.old	A previous partition table; it should not be modified manually. Do not copy.
/etc/cumulus/init	Platform hardware-specific files. Do not copy.
/etc/default/clagd	Created and managed by <code>ifupdown2</code> . Do not copy.
/etc/default/grub	Grub <code>init</code> table; it should not be modified manually.
/etc/default/hwclock	Platform hardware-specific file. Created during first boot. Do not copy.
/etc/init	Platform initialization files. Do not copy.
/etc/init.d/	Platform initialization files. Do not copy.
/etc/fstab	Static info on filesystem. Do not copy.

File Name and Location	Explanation
/etc/image-release	System version data. Do not copy.
/etc/os-release	System version data. Do not copy.
/etc/lsb-release	System version data. Do not copy.
/etc/lvm/archive	Filesystem files. Do not copy.
/etc/lvm/backup	Filesystem files. Do not copy.
/etc/modules	Created during first boot. Do not copy.
/etc/modules-load.d/	Created during first boot. Do not copy.
/etc/sensors.d	Platform-specific sensor data. Created during first boot. Do not copy.
/root/.ansible	Ansible tmp files. Do not copy.
/home/cumulus/.ansible	Ansible tmp files. Do not copy.

Upgrading Switches in an MLAG Pair

If you have a pair of Cumulus Linux switches as part of an **MLAG** (multi-chassis link aggregation) pair (see [page 217](#)), you should only upgrade each switch when it is in the *secondary role*. The upgrade path is as follows:

1. Upgrade Cumulus Linux on the switch already in the secondary role. This is the switch with the higher `cldagd-priority` value.
2. Set the switch in the secondary role into the primary role by setting its `cldagd-priority` to a value lower than the `cldagd-priority` setting on the switch in the primary role.

```
cumulus@switch:~$ sudo clagctl priority VALUE
```

3. Upgrade the switch that just took on the secondary role.
4. Put that switch into the primary role again, if you so choose.

```
cumulus@switch:~$ sudo clagctl priority VALUE
```

For more information about setting the priority, see [Understanding Switch Roles \(see page 220\)](#).

Upgrading Cumulus Linux: Choosing between a Binary Install vs. Package Upgrade

Network admins have two ways to upgrade Cumulus Linux:

- Performing a binary (full image) install of the new version, running `cl-img-install` on the switch
- Upgrading only the changed packages, using `apt-get update` and `apt-get dist-upgrade`

There are advantages and disadvantages to using these methods, which are outlined below.

Upgrading via Binary Install (`cl-img-install`)

Pros:

- Image is installed to the [alternate disk image slot \(see page 19\)](#) while the switch remains operational.
- The only downtime is the reboot/init process.
- You choose the exact version that you want to upgrade to.
- Rolling back to the previous version and config is easy and quick; it requires only running `cl-img-select -s` and reboot.
- This is the only method for upgrading to a new major (X.0) or minor version (X.Y). For example, when you are upgrading from 2.5.5 to 3.0 or from 2.2.2 to 2.5.5.

Cons:

- Configuration data must be moved to the new OS via some mechanism before the new OS is booted, or soon afterwards via out-of-band management.
- Moving the configuration file can go wrong in various ways:
 - Identifying all the locations of config data is not always an easy task.
 - Config file changes in the new version may cause merge conflicts that go undetected.

To upgrade the switch by running a binary install:

1. Back up the configurations off the switch using the [Config File Migration script](#) with the `--backup` option and then copy the archive off the switch.
Optional: Use the Ansible playbook included with the [Config File Migration script](#) to automate the backup of all your Cumulus Linux 2.5 switches. See the section below on [Using Automation Tools to Backup Configurations \(see page 49\)](#) for more details.
2. Install the binary image to the [alternate slot \(see page 19\)](#) and select it as the new primary slot.

```
cumulus@switch$ sudo cl-img-install -s <image_url>
```



If you don't use the `-s` flag here, you will have to run `cl-img-select -s` after the installation to manually select the alternate slot.

Click to expand full output

```
cumulus@switch$ sudo cl-img-install -s CumulusLinux-2.5.3a-amd64.bin
Defaulting to image slot 2 for install.
Dumping image info from CumulusLinux-2.5.3a-amd64.bin ...
Verifying image checksum ... OK.
Preparing image archive ... OK.
Control File Contents
=====
Description: Cumulus Linux
OS-Release: 2.5.3a-3b46bef-201509041633-build
Architecture: amd64
Date: Fri, 04 Sep 2015 17:10:30 -0700
Installer-Version: 1.2
Platforms: accton_as5712_54x accton_as6712_32x mlx_sx1400_i73612
dell_s6000_s1220 dell_s4000_c2338 dell_s3000_c2338
cel_redstone_xp cel_smallstone_xp cel_pebble quanta_panther
quanta_ly8_rangeley quanta_ly6_rangeley quanta_ly9_rangeley
Homepage: http://www.cumulusnetworks.com/
Data Archive Contents
=====
-rw-r--r-- build/Development      131 2015-09-05 00:10:29 file.
list
-rw-r--r-- build/Development      44 2015-09-05 00:10:29 file.
list.sha1
-rw-r--r-- build/Development 140238619 2015-09-05 00:10:29
sysroot-release.tar.gz
-rw-r--r-- build/Development      44 2015-09-05 00:10:30
sysroot-release.tar.gz.sha1
-rw-r--r-- build/Development 8094220 2015-09-05 00:10:29
vmlinuz-initrd.tar.xz
-rw-r--r-- build/Development      44 2015-09-05 00:10:30
vmlinuz-initrd.tar.xz.sha1
Current image slot setup:
active => slot 1 (primary): 2.5.3-c4e83ad-201506011818-build
slot 2 (alt    ): 2.5.2-727a0c6-201504132125-build
About to update image slot 2 using:
/home/cumulus/CumulusLinux-2.5.3a-amd64.bin
Are you sure (y/N)? y
Verifying image checksum ... OK.
Preparing image archive ... OK.
Validating sha1 for vmlinuz-initrd.tar.xz... done.
Validating sha1 for sysroot-release.tar.gz... done.
Installing OS-Release 2.5.3a-3b46bef-201509041633-build into
image slot 2 ...
Info: Copying sysroot into slot 2
Creating logical volume SYSROOT2 on volume group CUMULUS... done.
Verifying sysroot copy... OK.
Copying kernel into CLBOOT partition... done.
Verifying kernel copy... OK.
```

```
Generating grub.cfg ...
Found Cumulus Linux image: /boot/cl-vmlinuz-3.2.65-1+deb7u2+c12.5
+5-slot-1
Found Cumulus Linux image: /boot/cl-vmlinuz-3.2.65-1+deb7u2+c12.5
+5-slot-2
done
Success: /home/cumulus/CumulusLinux-2.5.3a-amd64.bin loaded into
image slot 2.
```

3. **Optional:** Migrate the configuration files to the alternate slot using the [Config File Migration script](#) with the `--sync` option.
4. Reboot the switch.

```
cumulus@switch$ sudo reboot
```

5. Restore the configuration files to the new version — ideally via automation — if the files were not migrated in step 3. To manually restore an archive created by the [Config File Migration script](#):

```
# On the switch, copy the config file archive back from the
server:
cumulus@switch$ scp user@my_external_server:PATH/SWITCHNAME-
config-archive-DATE_TIME.tar.gz .

# Untar the archive to the root of the box
cumulus@switch$ sudo tar -C / -xvf SWITCHNAME-config-archive-
DATE_TIME.tar.gz
```

6. Verify correct operation with the old configurations on the new version.
7. Reinstall third party apps and associated configurations.

Upgrading Using Package Installs (`apt-get update && apt-get dist-upgrade`)

Pros:

- Configuration data stays in place while the binaries are upgraded.
- Third-party apps stay in place.

Cons:

- This method works only if you are upgrading to a later maintenance release (X.Y.Z, like 2.5.5) from an earlier release in the same major and minor release family **only** (like 2.5.0 to 2.5.4, or 2.5.2 to 2.5.5).
- Rollback is quite difficult and tedious.
- You can't choose the exact release version that you want to run.
- When you upgrade, you upgrade all packages to the latest available version.

- The upgrade process takes a while to complete, and various switch functions are intermittently available during the upgrade.
- Some upgrade operations will terminate SSH sessions on the in-band (front panel) ports, leaving the user unable to monitor the upgrade process. As a workaround, use the [dtach tool](#).
- Just like the binary install method, you still must reboot after the upgrade, lengthening the downtime.



Before you upgrade a PowerPC switch, run `df -m` and make sure the overlay filesystem `/mnt/root-rw` has at least 200MB of free disk space. See [this release note](#) for more details.

To upgrade the switch by updating the packages:

1. Back up the configurations off the switch.
2. Fetch the latest update meta-data from the repository.

```
cumulus@switch$ sudo apt-get update
```

3. Upgrade all the packages to the latest distribution.

```
cumulus@switch$ sudo apt-get dist-upgrade
```

4. Reboot the switch.

```
cumulus@switch$ sudo reboot
```

5. Verify correct operation with the old configurations on new version.



While this method doesn't overwrite the [target image slot \(see page 19\)](#), the disk image does occupy a lot of disk space used by both Cumulus Linux image slots.



After you successfully upgrade Cumulus Linux, you may notice some results that you may or may not have expected:

- `apt-get dist-upgrade` always updates the operating system to the most current version, so if you are currently running Cumulus Linux 2.5.2 and run `apt-get dist-upgrade` on that switch, the packages will get upgraded to the latest version.

- When you run `cl-img-select`, the output still shows the version of Cumulus Linux from the last binary install. So if you installed Cumulus Linux 2.5.3 as a full image install and then upgraded to 2.5.8 using `apt-get dist-upgrade`, the output from `cl-img-select` still shows version 2.5.3. To see the current version of Cumulus Linux running on the switch, use `cat /etc/lsb-release`.

Why you should use `apt-get dist-upgrade` instead of `apt-get upgrade` (Click here to expand...)



Cumulus Networks recommends you upgrade Cumulus Linux using `apt-get dist-upgrade` instead of `apt-get upgrade`.

This ensures all the packages in the distribution get updated to the current version. `apt-get upgrade` **may** work correctly if no packages are held back by `apt`. A package can be held back if one or more of its dependencies has changed, or it can occur for other reasons. For example, if you see this message when running `apt-get upgrade`:

```
"The following packages have been kept back:  
linux-image-powerpc"
```

It means `apt-get upgrade` did not install the kernel package. However, `apt-get dist-upgrade` would have picked it up. Most applications in Cumulus Linux rely on the correct kernel version. If an application doesn't get the kernel version it expects, it may result in a non-functional system.

You can manually install a held back package by running `apt-get install` on it:

```
apt-get install linux-image-powerpc
```

If you must use `apt-get upgrade`, run it twice. For the second time, include the `-s` or `--dry-run` option to verify that all packages were picked up when you upgraded. Otherwise, you must manually install any held back packages to complete the upgrade.

```
apt-get upgrade --dry-run
```

Using Automation Tools to Back Up Configurations

Adopting the use of automation tools like Ansible, Chef or Puppet for configuration management greatly increases the speed and accuracy of the next major upgrade; they also enable the quick swap of failed switch hardware. Included with the [Config Migration Script](#) is an Ansible playbook that can be used to create a backup archive of all deployed Cumulus Linux 2.5.z switch configuration files and to retrieve them to a central server. This is a quick start on the road to setting up automated configuration and control for your deployment. For more details on integrating automation into your Cumulus Linux deployment, see the [Automation Solutions section on cumulusnetworks.com](#).

Rolling Back a Cumulus Linux Installation

Rolling Back after Using Binary Install

1. Select the alternate slot as the new primary slot. (The primary slot will be booted at the next reboot)

```
cumulus@switch$ sudo cl-img-select -s
```

2. Reboot the switch.

```
cumulus@switch$ sudo reboot
```

Rolling Back after Using Package Install

Rolling back to an earlier release after upgrading the packages on the switch follows the same procedure as described for the Linux host OS rollback above. There are three main strategies, and all require detailed planning and execution:

- Back out individual packages: If the problematic package is identified, the network admin can downgrade the affected package directly. In rare cases the configuration files may have to be restored from backup, or edited to back out any changes that were automatically made by the upgrade package.
- Flatten and rebuild: If the OS becomes unusable, you can use orchestration tools to reinstall the previous OS release from scratch and then automatically rebuild the configuration.
- Backup and restore: Another common strategy is to restore to a previous state via a backup captured before the upgrade.

Which method you employ is specific to your deployment strategy, so providing detailed steps for each scenario is outside the scope of this document.

Third Party Package Considerations

Note that if you install any third party apps on a Cumulus Linux switch, any configuration data will likely be installed into the /etc directory, but it is not guaranteed. It is the responsibility of the network admin to understand the behavior and config file information of any third party packages installed on a Cumulus Linux switch.

After you upgrade the OS in the alternate image slot, you will need to reinstall any third party packages or any Cumulus Linux add-on packages, such as `cl-mgmtvrf`, or `vxsnd` and `vxrd`.

Caveats while Upgrading Cumulus Linux 2.5.x

- **RN-287:** Copying the `/etc/passwd` file to the other slot when one version is earlier than Cumulus Linux 2.5.3 and the other version is later than Cumulus Linux 2.5.3 causes issues with LLDP not starting and Quagga logs not being created.

Adding and Updating Packages

You use the Advanced Packaging Tool (APT) to manage additional applications (in the form of packages) and to install the latest updates.

Contents

(Click to expand)

- [Contents \(see page 51\)](#)
- [Commands \(see page 51\)](#)
- [Updating the Package Cache \(see page 51\)](#)
- [Listing Available Packages \(see page 52\)](#)
- [Adding a Package \(see page 53\)](#)
- [Listing Installed Packages \(see page 54\)](#)
- [Upgrading to Newer Versions of Installed Packages \(see page 55\)
 - \[Upgrading a Single Package \\(see page 55\\)\]\(#\)
 - \[Upgrading All Packages \\(see page 55\\)\]\(#\)](#)
- [Adding Packages from Another Repository \(see page 55\)](#)
- [Configuration Files \(see page 57\)](#)
- [Useful Links \(see page 57\)](#)

Commands

- `apt-get`
- `apt-cache`
- `dpkg`

Updating the Package Cache

To work properly, APT relies on a local cache of the available packages. You must populate the cache initially, and then periodically update it with `apt-get update`:

```
cumulus@switch:~$ sudo apt-get update
Get:1 http://repo.cumulusnetworks.com CumulusLinux-2.5 Release.gpg [490 B]
Get:2 http://repo.cumulusnetworks.com CumulusLinux-2.5 Release [16.2 kB]
Get:3 http://repo.cumulusnetworks.com CumulusLinux-2.5/main powerpc
    Packages [181 kB]
Get:4 http://repo.cumulusnetworks.com CumulusLinux-2.5/addons powerpc
    Packages [75.1 kB]
Get:5 http://repo.cumulusnetworks.com CumulusLinux-2.5/updates powerpc
    Packages [112 kB]
Get:6 http://repo.cumulusnetworks.com CumulusLinux-2.5/security-updates
    powerpc Packages [28.5 kB]
```

```
Ign http://repo.cumulusnetworks.com CumulusLinux-2.5/addons Translation-en
Ign http://repo.cumulusnetworks.com CumulusLinux-2.5/main Translation-en
Ign http://repo.cumulusnetworks.com CumulusLinux-2.5/security-updates
Translation-en
Ign http://repo.cumulusnetworks.com CumulusLinux-2.5/updates Translation-en
Fetched 413 kB in 3s (117 kB/s)
Reading package lists... Done
```

Listing Available Packages

Once the cache is populated, use `apt-cache` to search the cache to find the packages you are interested in or to get information about an available package. Here are examples of the `search` and `show` sub-commands:

```
cumulus@switch:~$ apt-cache search tcp
netbase - Basic TCP/IP networking system
quagga-doc - documentation files for quagga
libwrap0-dev - Wietse Venema's TCP wrappers library, development files
libwrap0 - Wietse Venema's TCP wrappers library
librexp0 - Reliable Event Logging Protocol (RELP) library
socat - multipurpose relay for bidirectional data transfer
openssh-client - secure shell (SSH) client, for secure access to remote
machines
libpq5 - PostgreSQL C client library
rsyslog - reliable system and kernel logging daemon
tcpdump - command-line network traffic analyzer
openssh-server - secure shell (SSH) server, for secure access from remote
machines
librexp-dev - Reliable Event Logging Protocol (RELP) library - development
files
fakeroott - tool for simulating superuser privileges
quagga - BGP/OSPF/RIP routing daemon
monit - utility for monitoring and managing daemons or similar programs
python-dpkt - Python packet creation / parsing module
iperf - Internet Protocol bandwidth measuring tool
nmap - The Network Mapper
tcpstat - network interface statistics reporting tool
tcpreplay - Tool to replay saved tcpdump files at arbitrary speeds
nuttcp - network performance measurement tool
collectd-core - statistics collection and monitoring daemon (core system)
tcpextract - extracts files from network traffic based on file signatures
nagios-plugins-basic - Plugins for nagios compatible monitoring systems
tcptrace - Tool for analyzing tcpdump output
jdoo - utility for monitoring and managing daemons or similar programs
hping3 - Active Network Smashing Tool
```

```

cumulus@switch:~$ apt-cache show tcpreplay
Package: tcpreplay
Priority: optional
Section: net
Installed-Size: 984
Maintainer: Noël Köthe <noel@debian.org>
Architecture: powerpc
Version: 3.4.3-2+wheezy1
Depends: libc6 (>= 2.7), libpcap0.8 (>= 0.9.8)
Filename: pool/CumulusLinux-2.5/addons/tcpreplay_3.4.3-2+wheezy1_powerpc.deb
Size: 435904
MD5sum: cf20bec7282ef77a091e79372a29fe1e
SHA1: 8ee1b9b02dacd0c48a474844f4466eb54c7e1568
SHA256: 03dc29057cb608d2ddf08207aedf18d47988ed6c23db0af69d30746768a639ae
SHA512:
a411b08e7a7bea62331c527d152533afca735b795f2118507260a5a0c3b6143500df9f6723cf
f736a1de0969a63e7a7ad0ce8a181ea7dfb36e2330a95d046fb1
Description: Tool to replay saved tcpdump files at arbitrary speeds
Tcpreplay is aimed at testing the performance of a NIDS by
replaying real background network traffic in which to hide
attacks. Tcpreplay allows you to control the speed at which the
traffic is replayed, and can replay arbitrary tcpdump traces. Unlike
programmatically-generated artificial traffic which doesn't
exercise the application/protocol inspection that a NIDS performs,
and doesn't reproduce the real-world anomalies that appear on
production networks (asymmetric routes, traffic bursts/lulls,
fragmentation, retransmissions, etc.), tcpreplay allows for exact
replication of real traffic seen on real networks.
Homepage: http://tcpreplay.synfin.net/
cumulus@switch:~$
```



The search commands look for the search terms not only in the package name but in other parts of the package information. Consequently, it will match on more packages than you would expect.

Adding a Package

In order to add a new package, first ensure the package is not already installed in the system:

```
cumulus@switch:~$ dpkg -l | grep {name of package}
```

If the package is installed already, ensure it's the version you need. If it's an older version, then update the package from the Cumulus Linux repository:

```
cumulus@switch:~$ sudo apt-get update
```

If the package is not already on the system, add it by running `apt-get install`. This retrieves the package from the Cumulus Linux repository and installs it on your system together with any other packages that this package might depend on.

For example, the following adds the package `tcpreplay` to the system:

```
cumulus@switch:~$ sudo apt-get install tcpreplay
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
tcpreplay
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 436 kB of archives.
After this operation, 1008 kB of additional disk space will be used.
Get:1 https://repo.cumulusnetworks.com/ CumulusLinux-1.5/main tcpreplay
powerpc 3.4.3-2+wheezy1 [436 kB]
Fetched 436 kB in 0s (1501 kB/s)
Selecting previously unselected package tcpreplay.
(Reading database ... 15930 files and directories currently installed.)
Unpacking tcpreplay (from .../tcpreplay_3.4.3-2+wheezy1_powerpc.deb) ...
Processing triggers for man-db ...
Setting up tcpreplay (3.4.3-2+wheezy1) ...
cumulus@switch:~$
```

Listing Installed Packages

The APT cache contains information about all the packages available on the repository. To see which packages are actually installed on your system, use `dpkg`. The following example lists all the packages on the system that have "tcp" in their package names:

```
cumulus@switch:~$ dpkg -l \*tcp\*
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/half-conf/Half-inst/trig-aWait/Trig-
pend
|| Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name          Version       Architecture Description
=====
```

```
=====
ii  tcpd          7.6.q-24      powerpc      Wietse Venema's TCP wrapper
utili
ii  tcpdump       4.3.0-1      powerpc      command-line network traffic
anal
ii  tcpreplay     3.4.3-2+whee powerpc      Tool to replay saved tcpdump
file
cumulus@switch:~$
```

Upgrading to Newer Versions of Installed Packages

Upgrading a Single Package

A single package can be upgraded by simply installing that package again with `apt-get install`. You should perform an update first so that the APT cache is populated with the latest information about the packages.

To see if a package needs to be upgraded, use `apt-cache show <pkgname>` to show the latest version number of the package. Use `dpkg -l <pkgname>` to show the version number of the installed package.



Upgrading a single package in the Cumulus Linux distribution is not advised unless directed by Cumulus Networks Support.

Upgrading All Packages

You can update all packages on the system by running `apt-get update`, then `apt-get dist-upgrade`. This upgrades all installed versions with their latest versions but will not install any new packages.

Adding Packages from Another Repository

As shipped, Cumulus Linux searches the Cumulus Linux repository for available packages. You can add additional repositories to search by adding them to the list of sources that `apt-get` consults. See `man sources.list` for more information.



For several packages, Cumulus Networks has added features or made bug fixes and these packages must not be replaced with versions from other repositories. Cumulus Linux has been configured to ensure that the packages from the Cumulus Linux repository are always preferred over packages from other repositories.

If you want to install packages that are not in the Cumulus Linux repository, the procedure is the same as above with one additional step.



Packages not part of the Cumulus Linux Repository have generally not been tested, and may not be supported by Cumulus Linux support.

Installing packages outside of the Cumulus Linux repository requires the use of `apt-get`, but, depending on the package, `easy-install` and other commands can also be used.

To install a new package, please complete the following steps:

1. First, ensure package is not already installed in the system. Use the `dpkg` command:

```
cumulus@switch:~$ dpkg -l | grep {name of package}
```

2. If the package is installed already, ensure it's the version you need. If it's an older version, then update the package from the Cumulus Linux repository:

```
cumulus@switch:~$ sudo apt-get update
cumulus@switch:~$ sudo apt-get install {name of package}
```

3. If the package is not on the system, then most likely the package source location is also **not** in the `/etc/apt/sources.list` file. If the source for the new package is **not** in `sources.list`, please edit and add the appropriate source to the file. For example, add the following if you wanted a package from the Debian repository that is **not** in the Cumulus Linux repository:

```
deb http://http.us.debian.org/debian wheezy main
deb http://security.debian.org/ wheezy/updates main
```

Otherwise, the repository may be listed in `/etc/apt/sources.list` but is commented out, as can be the case with the testing repository:

```
#deb http://repo.cumulusnetworks.com CumulusLinux-VERSION testing
```

To uncomment the repository, remove the `#` at the start of the line, then save the file:

```
deb http://repo.cumulusnetworks.com CumulusLinux-VERSION testing
```

4. Run `apt-get update` then install the package:

```
cumulus@switch:~$ sudo apt-get update
cumulus@switch:~$ sudo apt-get install {name of package}
```

Configuration Files

- /etc/apt/apt.conf
- /etc/apt/preferences
- /etc/apt/sources.list

Useful Links

- Debian GNU/Linux FAQ, Ch 8 Package management tools
- man pages for apt-get, dpkg, sources.list, apt_preferences

Zero Touch Provisioning - ZTP

Zero touch provisioning (ZTP) allows devices to be quickly deployed in large-scale environments. Data center engineers only need to rack and stack the switch, connect it to the management network, then install Cumulus Linux via ONIE; the initial configuration gets invoked via ZTP. Alternatively, you can insert a USB stick with the configuration so the provisioning process can start automatically.

The provisioning framework allows for a one-time, user-provided script to be executed. This script can be used to add the switch to a configuration management (CM) platform such as [puppet](#), [Chef](#), [CFEngine](#), or even a custom, home-grown tool.

In addition, you can use the `autoprovision` command in Cumulus Linux to manually invoke your provisioning script.

ZTP in Cumulus Linux can occur automatically in one of two ways:

- Via DHCP
- Using a USB drive inserted into the switch (ZTP-USB)

The two methods for using ZTP are discussed below in greater detail.



The standard Cumulus Linux license requires you to page through the license file before accepting the terms, which can hinder an unattended installation like zero touch provisioning. To request a license without the EULA, email licensing@cumulusnetworks.com.

Contents

(Click to expand)

- [Contents \(see page 57\)](#)
- [Commands \(see page 58\)](#)
- [Zero Touch Provisioning over DHCP \(see page 58\)
 - \[Triggering ZTP over DHCP \\(see page 58\\)\]\(#\)
 - \[Configuring The DHCP Server \\(see page 58\\)\]\(#\)
 - \[Detailed Look at HTTP Headers \\(see page 59\\)\]\(#\)
 - \[Testing and Debugging ZTP Scripts for DHCP \\(see page 59\\)\]\(#\)](#)

- Zero Touch Provisioning Using USB (ZTP-USB) (see page 60)
 - Testing and Debugging ZTP-USB Scripts (see page 61)
- Writing ZTP Scripts (see page 62)
 - Example ZTP Scripts (see page 63)
- Manually Using the autoprovion Command (see page 65)
- Notes (see page 66)
- Configuration Files (see page 66)

Commands

- autoprovision

Zero Touch Provisioning over DHCP

For ZTP using DHCP, provisioning initially takes place over the management network and is initiated via a DHCP hook. A DHCP option is used to specify a configuration script. This script is then requested from the Web server and executed locally on the switch.

The zero touch provisioning process over DHCP follows these steps:

1. The first time you boot Cumulus Linux, eth0 is configured for DHCP and makes a DHCP request.
2. The DHCP server offers a lease to the switch.
3. If option 239 is present in the response, the zero touch provisioning process itself will start.
4. The zero touch provisioning process requests the contents of the script from the URL, sending additional [HTTP headers \(see page 59\)](#) containing details about the switch.
5. The script's contents are parsed to ensure it contains the `CUMULUS-AUTOPROVISIONING` flag ([see example scripts \(see page 66\)](#)).
6. The `autoprovion` command checks its [configuration file \(see page 66\)](#) to see if autoprovioning has already occurred and completed.
7. If `autoprovion` determines that provisioning is necessary, then the script executes locally on the switch with root privileges.
8. The return code of the script gets examined. If it is 0, then the provisioning state is marked as complete in the autoprovioning configuration file.

Triggering ZTP over DHCP

If provisioning has not already occurred, it is possible to trigger the zero touch provisioning process over DHCP when eth0 is set to use DHCP and one of the following events occur:

- Booting the switch
- Plugging a cable into or unplugging it from the eth0 port
- Disconnecting then reconnecting the switch's power cord

Configuring The DHCP Server

During the DHCP process over eth0, Cumulus Linux will request DHCP option 239. This option is used to specify the custom provisioning script.

For example, the `/etc/dhcp/dhcpd.conf` file for an ISC DHCP server would look like:

```
option cumulus-provision-url code 239 = text;

subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.100 192.168.0.200;
    option cumulus-provision-url "http://192.168.0.2/demo.sh";
}
```

Additionally, the hostname of the switch can be specified via the `host-name` option:

```
subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.100 192.168.0.200;
    option cumulus-provision-url "http://192.168.0.2/demo.sh";
    host dcl-tor-sw1 { hardware ethernet 44:38:39:00:1a:6b; fixed-
address 192.168.0.101; option host-name "dcl-tor-sw1"; }
```

Detailed Look at HTTP Headers

The following HTTP headers are sent in the request to the webserver to retrieve the provisioning script:

Header	Value	Example
User-Agent		CumulusLinux-
AutoProvision/0.4		
CUMULUS-ARCH	CPU architecture	powerpc
CUMULUS-BUILD		1.5.1-5c6829a-2013
09251712-final		
CUMULUS-LICENSE-INSTALLED	Either 0 or 1	1
CUMULUS-MANUFACTURER		dni
CUMULUS-PRODUCTNAME		et-7448bf
CUMULUS-SERIAL		XYZ123004
CUMULUS-VERSION		1.5.1
CUMULUS-PROV-COUNT		0
CUMULUS-PROV-MAX		32

Testing and Debugging ZTP Scripts for DHCP

One can manually run a provisioning session at any time using `--force (-f)` option with the `autoprovision` command as shown below:

```
cumulus@switch:~$ sudo /usr/lib/cumulus/autoprovision --force --url
http://192.168.1.1/demo.sh
```

Zero Touch Provisioning Using USB (ZTP-USB)



This feature has been tested only with "thumb" drives, not an actual external large USB hard drive.

Cumulus Linux supports the use of a FAT32, FAT16, or VFAT-formatted USB drive as an installation source for ZTP scripts. A daemon called `ztp-usb` runs by default in Cumulus Linux (you can disable it by specifying `START=no` in `/etc/default/ztp-usb`). You can plug in a USB stick at any time — when you power up a switch or even when the switch has been running for some time. This is useful for performing a full installation of the operating system for cases like fresh installs or disaster recovery.

At minimum, the script should:

- Install the Cumulus Linux operating system and license.
- Copy over a basic configuration to the switch.
- Restart the switch or the relevant server to get `switchd` up and running with that configuration.

Follow these steps to perform zero touch provisioning using USB:

1. Copy the Cumulus Linux license and installation image to the USB stick.
2. When Cumulus Linux boots, the `ztp-usb` daemon starts.
3. Each new device detected by the kernel is mounted to `/mnt/usb`.
4. The daemon searches the root filesystem of the newly mounted device for filenames matching an [ONIE-style waterfall](#) (see the patterns and examples below), looking for the most specific name first, and ending at the most generic.
5. The script's contents are parsed to ensure it contains the `CUMULUS-AUTOPROVISIONING` flag (see [example scripts \(see page 66\)](#)).
6. The `autoprovision` command checks its [configuration file \(see page 66\)](#) to see if autoprovisioning has already occurred and completed.
7. If `autoprovision` determines that provisioning is necessary, then the script executes locally on the switch with root privileges.
8. After it completes one pass through all the devices, the `ztp-usb` daemon exits.

The filenames searched are as follows:

- `'cumulus-ztp-' + architecture + '-' + vendor + '_' + model + '-r' + revision`
- `'cumulus-ztp-' + architecture + '-' + vendor + '_' + model`
- `'cumulus-ztp-' + vendor + '_' + model`
- `'cumulus-ztp-' + architecture`
- `'cumulus-ztp'`

For example:

```
/mnt/usb/cumulus-ztp-powerpc-cel_smallstone-rUNKNOWN  
/mnt/usb/cumulus-ztp-powerpc-cel_smallstone
```

```
/mnt/usb/cumulus-ztp-cel_smallstone
/mnt/usb/cumulus-ztp-powerpc
/mnt/usb/cumulus-ztp
```

Testing and Debugging ZTP-USB Scripts

It is possible to test the scripts you've written for ztp-usb using the techniques described below. Once a script has been placed on a USB drive and is ready for testing follow the procedure below:

1. Disable the ztp-usb daemon.

```
cumulus@switch:~$ sudo service ztp-usb stop
cumulus@switch:~$ sudo service ztp-usb status
[FAIL] ztp-usb is not running ... failed!
```

2. Insert the USB stick into the switch.
3. Move the autoprovision configuration file to a safe location.

```
cumulus@switch:~$ sudo mv /var/lib/cumulus/autoprovision.conf
/var/lib/cumulus/autoprovision.conf.original
```

By moving the configuration file to a new location, the autoprovision framework has no record of previous provisioning successes or failures, which means any new attempt to autoprovision succeeds.

4. Use debugging mode to run the ztp-usb script.

```
cumulus@wan1$ sudo /usr/lib/cumulus/ztp-usb -d
ztp-usb: 2015-09-18 14:39:49,280 Initial hash value
731845549779ee9c37bd630c7d24cc1d
ztp-usb: 2015-09-18 14:39:49,280 Parsing partitions
ztp-usb: 2015-09-18 14:39:49,518 /dev/sda: unsupported partition
type =
ztp-usb: 2015-09-18 14:39:49,519 INFO: Trying to mount: "/dev
/sda1" of type: "vfat"
ztp-usb: 2015-09-18 14:39:49,519 Creating /mnt/usb mount
directory
ztp-usb: 2015-09-18 14:39:49,640 Waterfall search for /mnt/usb
/cumulus-ztp-unknown-accton_as5712_54x-rUNKNOWN
ztp-usb: 2015-09-18 14:39:49,640 Waterfall search for /mnt/usb
/cumulus-ztp-unknown-accton_as5712_54x
ztp-usb: 2015-09-18 14:39:49,640 Waterfall search for /mnt/usb
/cumulus-ztp-unknown-accton
ztp-usb: 2015-09-18 14:39:49,640 Waterfall search for /mnt/usb
/cumulus-ztp-unknown
```

```

ztp-usb: 2015-09-18 14:39:49,640 Waterfall search for /mnt/usb
/cumulus-ztp
ztp-usb: 2015-09-18 14:39:49,641 Found matching name, passing
/mnt/usb/cumulus-ztp to autoprovision wrapper
ztp-usb: 2015-09-18 14:39:49,641 Found /mnt/usb/cumulus-ztp
script, passing to autoprovision
ztp-usb: 2015-09-18 14:39:51,370 Script returned exit code 0
ztp-usb: 2015-09-18 14:39:51,370 Unmounting drive and removing
mountpoint.
ztp-usb: 2015-09-18 14:39:51,396 /dev/sdb: unsupported partition
type =
ztp-usb: 2015-09-18 14:39:51,396 /dev/sdb1: unsupported
partition type =
ztp-usb: 2015-09-18 14:39:51,396 /dev/sdb2: unsupported
partition type = ext4
ztp-usb: 2015-09-18 14:39:51,396 /dev/sdb3: unsupported
partition type = ext4
ztp-usb: 2015-09-18 14:39:51,396 /dev/sdb4: unsupported
partition type = LVM2_member
ztp-usb: 2015-09-18 14:39:51,396 /dev/CUMULUS-PERSIST:
unsupported partition type = RM=0
ztp-usb: 2015-09-18 14:39:51,396 /dev/CUMULUS-SYSROOT1:
unsupported partition type = RM=0
ztp-usb: 2015-09-18 14:39:51,397 /dev/CUMULUS-SYSROOT2:
unsupported partition type = RM=0
ztp-usb: 2015-09-18 14:39:51,397 Current hash value
731845549779ee9c37bd630c7d24cc1d
ztp-usb: 2015-09-18 14:40:21,427 Current hash value
731845549779ee9c37bd630c7d24cc1d
  
```

Writing ZTP Scripts



Remember to include the following line in any of the supported scripts which are expected to be run via the autoprovisioning framework.

```
# CUMULUS-AUTOPROVISIONING
```

This line is required somewhere in the script file in order for execution to occur.

The script must contain the `CUMULUS-AUTOPROVISIONING` flag. This can be in a comment or remark and does not need to be echoed or written to `stdout`.

The script can be written in any language currently supported by Cumulus Linux, such as:

- Perl
- Python
- Ruby

- Shell

The script must return an exit code of 0 upon success, as this triggers the autoprovisioning process to be marked as complete in the autoprovisioning configuration file.

Example ZTP Scripts

The following script install Cumulus Linux and its license from USB and applies a configuration:

```
#!/bin/bash
function error() {
    echo -e "\e[0;33mERROR: The Zero Touch Provisioning script failed
while running the command $BASH_COMMAND at line $BASH_lineno.\e[0m" >&
2
    exit 1
}

# Log all output from this script
exec >/var/log/autoprovision 2>&1

trap error ERR

#Add Debian Repositories
echo "deb http://http.us.debian.org/debian wheezy main" >> /etc/apt
/sources.list
echo "deb http://security.debian.org/ wheezy/updates main" >> /etc/apt
/sources.list

#Update Package Cache
apt-get update -y

#Install netshow diagnostics commands
apt-get install -y netshow htop nmap

#Load interface config from usb
cp /mnt/usb/interfaces /etc/network/interfaces

#Load port config from usb
#  (if breakout cables are used for certain interfaces)
cp /mnt/usb/ports.conf /etc/cumulus/ports.conf

#Install a License from usb and restart switchd
cl-license -i /mnt/usb/license.txt && service switchd restart

#Reload interfaces to apply loaded config
ifreload -a

#Output state of interfaces
netshow interface

# CUMULUS-AUTOPROVISIONING
```

```
exit 0
```

Here is a simple script to install puppet:

```
#!/bin/bash
function error() {
    echo -e "\e[0;33mERROR: The Zero Touch Provisioning script failed
while running the command $BASH_COMMAND at line $BASH_LINENO.\e[0m" >&
2
    exit 1
}
trap error ERR
apt-get update -y
apt-get upgrade -y
apt-get install puppet -y
sed -i /etc/default/puppet -e 's/START=no/START=yes/'
sed -i /etc/puppet/puppet.conf -e 's/\\[main\\]\\/[main\\]
\npluginsync=true'
service puppet restart
# CUMULUS-AUTOPROVISIONING
exit 0
```

This script illustrates how to specify an internal APT mirror and puppet master:

```
#!/bin/bash
function error() {
    echo -e "\e[0;33mERROR: The Zero Touch Provisioning script failed
while running the command $BASH_COMMAND at line $BASH_LINENO.\e[0m" >&
2
    exit 1
}
trap error ERR
sed -i /etc/apt/sources.list -e 's/repo.cumulusnetworks.com/labrepo.
mycompany.com/'
apt-get update -y
apt-get upgrade -y
apt-get install puppet -y
sed -i /etc/default/puppet -e 's/START=no/START=yes/'
sed -i /etc/puppet/puppet.conf -e 's/\\[main\\]\\/[main\\]
\npluginsync=true'
sed -i /etc/puppet/puppet.conf -e 's/\\[main\\]\\/[main\\]
\nserver=labpuppet.mycompany.com/'
service puppet restart
# CUMULUS-AUTOPROVISIONING
exit 0
```

Now puppet can take over management of the switch, configuration authentication, changing the default root password, and setting up interfaces and routing protocols.

Several ZTP example scripts are available in the [Cumulus GitHub repository](#).

Manually Using the autoprovioning Command



Be sure to specify the full path to the `autoprovioning` command.

All forms of ZTP use the `autoprovioning` command on the backend to execute a provided provisioning script, whether that script is sourced from a URL over the network or locally via a file from a USB drive. One of the benefits of using the `autoprovioning` command — instead of simply scheduling a cronjob to run your script — is that `autoprovioning` tracks whether or not a script has already been executed (and when) in its configuration file `/var/lib/cumulus/autoprovioning.conf`, ensuring that a switch that has already been provisioned is not accidentally provisioned again at a later date.

Users with root privileges can interact with the `autoprovioning` command directly using the examples below.

To enable zero touch provisioning, use the `-e` option:

```
cumulus@switch:~$ sudo /usr/lib/cumulus/autoprovioning -e
```

To run the provisioning script against a script hosted on a Web server, use the `-u` option and include the URL to the script:

```
cumulus@switch:~$ sudo /usr/lib/cumulus/autoprovioning -u http://192.168.0.1/ztp.sh
```

To run the provisioning script against a script hosted on the local filesystem, use the `--file` or `-i` option and include the file location of the script:

```
cumulus@switch:~$ sudo /usr/lib/cumulus/autoprovioning --file /mnt/usb/cumulus-ztp.sh
```

To disable zero touch provisioning, use the `-x` option:

```
cumulus@switch:~$ sudo /usr/lib/cumulus/autoprovioning -x
```

To enable startup discovery mode, without relying on DHCP when you boot the switch, use the `-s` option:

```
cumulus@switch:~$ sudo /usr/lib/cumulus/autoprovioning -s
```

To force provisioning to occur and ignore the status listed in the configuration file use the `-f` option:

```
cumulus@switch:~$ sudo /usr/lib/cumulus/autoprovision -f --file /mnt  
/usb/cumulus-ztp.sh
```

Notes

- During the development of a provisioning script, the switch may need to be reset.
- You can use the Cumulus Linux `cl-img-clear-overlay` command to revert the image to its original configuration.
- You can use the Cumulus Linux `cl-img-select -i` command to cause the switch to reprovision itself and install a network operating system again using ONIE.

Configuration Files

- `/var/lib/cumulus/autoprovision.conf`: Stores configuration options and details for the autoprovisioning framework
- `/etc/default/ztp-usb`: Stores the enable/disable flag for the `ztp-usb` service

System Management

Setting Date and Time

Setting the time zone, date and time requires root privileges; use `sudo`.

Contents

(Click to expand)

- [Contents \(see page 67\)](#)
- [Commands \(see page 67\)](#)
- [Setting the Time Zone \(see page 67\)](#)
- [Setting the Date and Time \(see page 68\)](#)
- [Setting Time Using NTP \(see page 69\)](#)
- [Specifying the NTP Source Interface \(see page 70\)](#)
- [Configuration Files \(see page 70\)](#)
- [Useful Links \(see page 70\)](#)

Commands

- `date`
- `dpkg-reconfigure tzdata`
- `hwclock`
- `ntpd` (daemon)
- `ntpq`

Setting the Time Zone

To see the current time zone, list the contents of `/etc/timezone`:

```
cumulus@switch:~$ cat /etc/timezone
US/Eastern
```

To set the time zone, run `dpkg-reconfigure tzdata` as root:

```
cumulus@switch:~$ sudo dpkg-reconfigure tzdata
```

Then navigate the menus to enable the time zone you want. The following example selects the US/Pacific time zone:

```
cumulus@switch:~$ sudo dpkg-reconfigure tzdata

Configuring tzdata
-----
Please select the geographic area in which you live. Subsequent
configuration
questions will narrow this down by presenting a list of cities, representing
the time zones in which they are located.

 1. Africa      4. Australia   7. Atlantic   10. Pacific   13. Etc
 2. America     5. Arctic       8. Europe     11. SystemV
 3. Antarctica  6. Asia        9. Indian     12. US

Geographic area: 12

Please select the city or region corresponding to your time zone.

 1. Alaska      4. Central     7. Indiana-Starke 10. Pacific
 2. Aleutian    5. Eastern     8. Michigan      11. Pacific-New
 3. Arizona     6. Hawaii      9. Mountain     12. Samoa

Time zone: 10

Current default time zone: 'US/Pacific'
Local time is now:      Mon Jun 17 09:27:45 PDT 2013.
Universal Time is now:  Mon Jun 17 16:27:45 UTC 2013.
```

For more info see the Debian [System Administrator's Manual – Time](#).

Setting the Date and Time

The switch contains a battery backed hardware clock that maintains the time while the switch is powered off and in between reboots. When the switch is running, the Cumulus Linux operating system maintains its own software clock.

During boot up, the time from the hardware clock is copied into the operating system's software clock. The software clock is then used for all timekeeping responsibilities. During system shutdown the software clock is copied back to the battery backed hardware clock.

You can set the date and time on the software clock using the `date` command. First, determine your current time zone:

```
cumulus@switch$ date +%Z
```



If you need to reconfigure the current time zone, refer to the instructions above.

Then, to set the system clock according to the time zone configured:

```
cumulus@switch$ sudo date -s "Tue Jan 12 00:37:13 2016"
```

See `man date(1)` for if you need more information.

You can write the current value of the system (software) clock to the hardware clock using the `hwclock` command:

```
cumulus@switch$ sudo hwclock -w
```

See `man hwclock(8)` if you need more information.

You can find a good overview of the software and hardware clocks in the Debian [System Administrator's Manual – Time](#), specifically the section [Setting and showing hardware clock](#).

Setting Time Using NTP

The `ntpd` daemon running on the switch implements the NTP protocol. It synchronizes the system time with time servers listed in `/etc/ntp.conf`. It is started at boot by default. See `man ntpd(8)` for `ntpd` details.

By default, `/etc/ntp.conf` contains some default time servers. Edit `/etc/ntp.conf` to add or update time server information. See `man ntp.conf(5)` for details on configuring `ntpd` using `ntp.conf`.

To set the initial date and time via NTP before starting the `ntpd` daemon, use `ntpd -q` (This is same as `ntpdate`, which is to be retired and not available).



`ntpd -q` can hang if the time servers are not reachable.

To verify that `ntpd` is running on the system:

```
cumulus@switch:~$ ps -ef | grep ntp
ntp      4074      1  0 Jun20 ?          00:00:33 /usr/sbin/ntpd -p /var/run
/ntpd.pid -g -u 101:102
```

To check the NTP peer status:

```
cumulus@switch:~$ ntpq -p      remote                  refid      st t when poll
reach    delay   offset   jitter
=====
==                                          
*level1f.cs.unc. .PPS.           1 u   225 1024  377    92.505   -1.296
```

```
1.139
+ip.tcp.lv      193.11.166.8      2 u    29 1024 377 192.701      2.424
1.227
-host-86.3.217.2 131.107.13.100  2 u 1024 1024 367 240.622      11.250
7.785
+li290-38.member 128.138.141.172  2 u  553 1024 377  38.944     -0.810
1.139
```

Specifying the NTP Source Interface

You can change the source interface that NTP uses if you want to use something other than the default of eth0. Edit `ntp.conf` and edit the entry under the **# Specify interfaces** comment:

```
# Specify interfaces
interface listen bridge10
```

Configuration Files

- /etc/default/ntp — `ntpd init.d` configuration variables
- /etc/ntp.conf — default NTP configuration file
- /etc/init.d/ntp — `ntpd init` script

Useful Links

- Debian System Administrator's Manual – Time
- <http://www.ntp.org>
- http://en.wikipedia.org/wiki/Network_Time_Protocol
- <http://wiki.debian.org/NTP>

Authentication, Authorization, and Accounting

- SSH for Remote Access (see page 70)
- User Accounts (see page 72)
- Using sudo to Delegate Privileges (see page 72)
- PAM and NSS (see page 79)

SSH for Remote Access

You use **SSH** to securely access a Cumulus Linux switch remotely.

Contents

(Click to expand)

- [Contents \(see page 70\)](#)
- [Access Using Passkey \(Basic Setup\) \(see page 71\)](#)
 - Completely Passwordless System (see page 72)
- [Useful Links \(see page 72\)](#)

Access Using Passkey (Basic Setup)

Cumulus Linux uses the openSSH package to provide SSH functionality. The standard mechanisms of generating passwordless access just applies. The example below has the cumulus user on a machine called management-station connecting to a switch called *cumulus-switch1*.

First, on management-station, generate the SSH keys:

```
cumulus@management-station:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/cumulus/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/cumulus/.ssh/id_rsa.
Your public key has been saved in /home/cumulus/.ssh/id_rsa.pub.
The key fingerprint is:
8c:47:6e:00:fb:13:b5:07:b4:1e:9d:f4:49:0a:77:a9 cumulus@management-
station
The key's randomart image is:
+--[ RSA 2048 ]----+
|   . = o o. |
|   o . O *.. |
|   . o = =.o |
|   . O oE |
|   + S |
|   + |
|   |
|   |
|   |
+-----+
```

Next, append the public key in `~/.ssh/id_rsa.pub` into `~/.ssh/authorized_keys` in the target user's home directory:

```
cumulus@management-station:~$ scp .ssh/id_rsa.pub cumulus@cumulus-switch1:.
ssh/authorized_keys
Enter passphrase for key '/home/cumulus/.ssh/id_rsa':
id_rsa.pub
```



Remember, you cannot use the root account to SSH to a switch in Cumulus Linux unless you [set a password \(see page 72\)](#) for the account.

Completely Passwordless System

When generating the passphrase and its associated keys, as in the first step above, do not enter a passphrase. Follow all the other instructions.

Useful Links

- <http://www.debian-administration.org/articles/152>

User Accounts

By default, Cumulus Linux has two user accounts: *cumulus* and *root*.

The *cumulus* account:

- Default password is *CumulusLinux!*
- Is a user account in the *sudo* group with sudo privileges
- User can log in to the system via all the usual channels like console and [SSH \(see page 70\)](#)

The *root* account:

- Default password is disabled by default
- Has the standard Linux root user access to everything on the switch
- Disabled password prohibits login to the switch by SSH, telnet, FTP, and so forth

For best security, you should change the default password (using the `passwd` command) before you configure Cumulus Linux on the switch.

You can enable a valid password for the root account using the `sudo passwd root` command and can install an SSH key for the root account if needed. Enabling a password for the root account allows the root user to log in directly to the switch. The Cumulus Linux default root account behavior is consistent with Debian.

You can add more user accounts as needed. Like the *cumulus* account, these accounts must use `sudo` to [execute privileged commands \(see page 72\)](#), so be sure to include them in the *sudo* group.

To access the switch without any password requires booting into a single shell/user mode. [Here are the instructions \(see page 419\)](#) on how to do this using PowerPC and x86 switches.

Using `sudo` to Delegate Privileges

By default, Cumulus Linux has two user accounts: *root* and *cumulus*. The *cumulus* account is a normal user and is in the group *sudo*.

You can add more user accounts as needed. Like the *cumulus* account, these accounts must use `sudo` to execute privileged commands.

Contents

(Click to expand)

- [Contents \(see page 72\)](#)
- [Commands \(see page 73\)](#)
- [Using sudo \(see page 73\)](#)
- [sudoers Examples \(see page 74\)](#)
- [Configuration Files \(see page 79\)](#)
- [Useful Links \(see page 79\)](#)

Commands

- `sudo`
- `visudo`

Using sudo

`sudo` allows you to execute a command as superuser or another user as specified by the security policy. See `man sudo(8)` for details.

The default security policy is `sudoers`, which is configured using `/etc/sudoers`. Use `/etc/sudoers.d/` to add to the default `sudoers` policy. See `man sudoers(5)` for details.



Use `visudo` only to edit the `sudoers` file; do not use another editor like `vi` or `emacs`. See `man visudo(8)` for details.

Errors in the `sudoers` file can result in losing the ability to elevate privileges to root. You can fix this issue only by power cycling the switch and booting into single user mode. Before modifying `sudoers`, enable the root user by setting a password for the root user.

By default, users in the `sudo` group can use `sudo` to execute privileged commands. To add users to the `sudo` group, use the `useradd(8)` or `usermod(8)` command. To see which users belong to the `sudo` group, see `/etc/group` (`man group(5)`).

Any command can be run as `sudo`, including `su`. A password is required.

The example below shows how to use `sudo` as a non-privileged user `cumulus` to bring up an interface:

```
cumulus@switch:~$ ip link show dev swp1
3: swp1: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master br0 state
DOWN mode DEFAULT qlen 500
link/ether 44:38:39:00:27:9f brd ff:ff:ff:ff:ff:ff

cumulus@switch:~$ ip link set dev swp1 up
RTNETLINK answers: Operation not permitted

cumulus@switch:~$ sudo ip link set dev swp1 up
Password:

cumulus@switch:~$ ip link show dev swp1
```

```
3: swp1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master
br0 state UP mode DEFAULT qlen 500
link/ether 44:38:39:00:27:9f brd ff:ff:ff:ff:ff:ff
```

sudoers Examples

The following examples show how you grant as few privileges as necessary to a user or group of users to allow them to perform the required task. For each example, the system group *noc* is used; groups are prefixed with an %.

When executed by an unprivileged user, the example commands below must be prefixed with `sudo`.

Category	Privilege	Example Command	sudoers Entry
Monitoring	Switch port info	<code>ethtool -m swp1</code>	<code>%noc ALL=(ALL) NOPASSWD: /sbin/ethtool</code>
Monitoring	System diagnostics	<code>cl-support</code>	<code>%noc ALL=(ALL) NOPASSWD:/usr/cumulus/bin/cl-support</code>
Monitoring	Routing diagnostics	<code>cl-resource-query</code>	<code>%noc ALL=(ALL) NOPASSWD:/usr/cumulus/bin/cl-resource-query</code>
Image management	Install images	<code>cl-img-install http://lab/install.bin</code>	<code>%noc ALL=(ALL) NOPASSWD:/usr/cumulus/bin/cl-img-install</code>
Image management	Swapping slots	<code>cl-img-select 1</code>	<code>%noc ALL=(ALL) NOPASSWD:/usr/cumulus/bin/cl-img-select</code>

Category	Privilege	Example Command	sudoers Entry
Image management	Clearing an overlay	<code>cl-img-clear-overlay 1</code>	<code>%noc ALL=(ALL) NOPASSWD:/usr/cumulus/bin/cl-img-clear-overlay</code>
Package management	Any apt-get command	<code>apt-get update</code> or <code>apt-get install</code>	<code>%noc ALL=(ALL) NOPASSWD:/usr/bin/apt-get</code>
Package management	Just apt-get update	<code>apt-get update</code>	<code>%noc ALL=(ALL) NOPASSWD:/usr/bin/apt-get update</code>
Package management	Install packages	<code>apt-get install mtr-tiny</code>	<code>%noc ALL=(ALL) NOPASSWD:/usr/bin/apt-get install *</code>
Package management	Upgrading	<code>apt-get upgrade</code>	<code>%noc ALL=(ALL) NOPASSWD:/usr/bin/apt-get upgrade</code>
Netfilter	Install ACL policies	<code>cl-acltool -i</code>	<code>%noc ALL=(ALL) NOPASSWD:/usr/cumulus/bin/cl-acltool</code>
Netfilter	List iptables rules	<code>iptables -L</code>	<code>%noc ALL=(ALL) NOPASSWD:/sbin/iptables</code>

Category	Privilege	Example Command	sudoers Entry
L1 + 2 features	Any LLDP command	lldpcli show neighbors / configure	%noc ALL=(ALL) NOPASSWD:/usr/sbin/lldpcli
L1 + 2 features	Just show neighbors	lldpcli show neighbors	%noc ALL=(ALL) NOPASSWD:/usr/sbin/lldpcli show neighbours*
Interfaces	Modify any interface	ip link set dev swp1 {up down}	%noc ALL=(ALL) NOPASSWD:/sbin/ip link set *
Interfaces	Up any interface	ifup swp1	%noc ALL=(ALL) NOPASSWD:/sbin/ifup
Interfaces	Down any interface	ifdown swp1	%noc ALL=(ALL) NOPASSWD:/sbin/ifdown
Interfaces	Up/down only swp2	ifup swp2 / ifdown swp2	%noc ALL=(ALL) NOPASSWD:/sbin/ifup swp2,/sbin/ifdown swp2
Interfaces	Any IP address chg		

Category	Privilege	Example Command	sudoers Entry
		<pre>ip addr {add del} 192.0.2.1/30 dev swp1</pre>	<pre>%noc ALL=(ALL) NOPASSWD: /sbin/ip addr *</pre>
Interfaces	Only set IP address	<pre>ip addr add 192.0.2.1/30 dev swp1</pre>	<pre>%noc ALL=(ALL) NOPASSWD: /sbin/ip addr add *</pre>
Ethernet bridging	Any bridge command	<pre>brctl addbr br0 / brctl delif br0 swp1</pre>	<pre>%noc ALL=(ALL) NOPASSWD: /sbin/brctl</pre>
Ethernet bridging	Add bridges and ints	<pre>brctl addbr br0 / brctl addif br0 swp1</pre>	<pre>%noc ALL=(ALL) NOPASSWD: /sbin/brctl addbr *,/sbin /brctl addif *</pre>
Spanning tree	Set STP properties	<pre>mstptctl setmaxage br2 20</pre>	<pre>%noc ALL=(ALL) NOPASSWD: /sbin/mstptctl</pre>
Troubleshooting	Restart switchd	<pre>service switchd restart</pre>	<pre>%noc ALL=(ALL) NOPASSWD:/usr /sbin/service switchd *</pre>

Category	Privilege	Example Command	sudoers Entry
Troubleshooting	Restart any service	<pre>service switchd cron</pre>	<pre>%noc ALL=(ALL) NOPASSWD:/usr /sbin/service</pre>
Troubleshooting	Packet capture	<pre>tcpdump</pre>	<pre>%noc ALL=(ALL) NOPASSWD:/usr /sbin/tcpdump</pre>
L3	Add static routes	<pre>ip route add 10.2.0.0/16 via 10.0.0.1</pre>	<pre>%noc ALL=(ALL) NOPASSWD:/bin /ip route add *</pre>
L3	Delete static routes	<pre>ip route del 10.2.0.0/16 via 10.0.0.1</pre>	<pre>%noc ALL=(ALL) NOPASSWD:/bin /ip route del *</pre>
L3	Any static route chg	<pre>ip route *</pre>	<pre>%noc ALL=(ALL) NOPASSWD:/bin /ip route *</pre>
L3	Any iproute command	<pre>ip *</pre>	<pre>%noc ALL=(ALL) NOPASSWD:/bin /ip</pre>
L3	Non-modal OSPF		<pre>%noc ALL=(ALL) NOPASSWD:/usr /bin/cl-ospf</pre>

Category	Privilege	Example Command	sudoers Entry
		<pre>cl-ospf area 0.0.0.1 range 10.0.0.0/24</pre>	

Configuration Files

- /etc/sudoers - default security policy
- /etc/sudoers.d/ - default security policy

Useful Links

- sudo
- Adding Yourself to sudoers

LDAP Authentication and Authorization

Cumulus Linux uses Pluggable Authentication Modules (PAM) and Name Service Switch (NSS) for user authentication.

NSS specifies the order of information sources used to resolve names for each service. Using this with authentication and authorization, it provides the order and location used for user lookup and group mapping on the system. PAM handles the interaction between the user and the system, providing login handling, session setup, authentication of users and authorization of a user actions.

NSS enables PAM to use LDAP for providing user authentication, group mapping and information for other services on the system.

Contents

(Click to expand)

- Contents (see page 79)
- Configuring LDAP Authentication (see page 80)
- Installing libnss-ldapd (see page 80)
- Configuring nslcd.conf (see page 81)
 - Connection (see page 81)
 - Search Function (see page 82)
 - Search Filters (see page 82)
 - Attribute Mapping (see page 82)
 - Example Configuration (see page 83)
- Troubleshooting (see page 83)

- Using nslcd Debug Mode (see page 83)
- Common Problems (see page 84)
- Configuring LDAP Authorization (see page 86)
- Active Directory Configuration (see page 86)
- LDAP Verification Tools (see page 86)
 - Identifying a User with the id Command (see page 86)
 - Using getent (see page 87)
 - Using LDAP search (see page 87)
 - LDAP Browsers (see page 88)
- References (see page 89)

Configuring LDAP Authentication

There are 3 common ways of configuring LDAP authentication on Linux:

- libnss-ldap
- libnss-ldapd
- libnss-sss

This chapter covers using `libnss-ldapd` only. From internal testing, this library worked best with Cumulus Linux and was the easiest to configure, automate and troubleshoot.

Installing libnss-ldapd



The `libnss-ldapd` and `ldap-utils` packages are not available in the Cumulus Networks repository. You must install them from the Debian repository. You need to configure the switch to reference the Debian repository. To do so, edit the `/etc/apt/sources.list` file and adding the following line:

```
deb http://ftp.us.debian.org/debian/ wheezy main
```

If *nested group support* is required, `libnss-ldapd` must be version 0.9 or higher. For Cumulus Linux 2.x, you should add the `wheezy-backports` repo instead of the `wheezy` repo:

```
deb http://ftp.us.debian.org/debian/ wheezy-backports main
```

Then run `apt-get update` to sync with the Debian repo.

Once you reference the Debian repository, install `libnss-ldapd`, `libpam-ldapd` and `ldap-utils`. Run:

```
cumulus@switch:~$ sudo apt-get install libnss-ldapd libpam-ldapd ldap-utils
```

This brings up an interactive prompt asking questions about the LDAP URI, search base distinguished name (DN) and services that should have LDAP lookups enabled. This creates a very basic LDAP configuration, using anonymous bind, and initiating the search for a user under the base DN specified.



Alternatively, these parameters can be pre-seeded using the `debconf-utils`. To use this method, run `apt-get install debconf-utils` and create the pre-seeded parameters using `debconf-set-selections` with the appropriate answers. Run `debconf-show <pkg>` to check the settings. Here is an [example of how to preseed answers to the installer questions using `debconf-set-selections`](#).

Once the install is complete, the *name service LDAP caching daemon* (`nslcd`) will be running. This is the service that handles all of the LDAP protocol interactions, and caches the information returned from the LDAP server. In `/etc/nsswitch.conf`, `ldap` has been appended and is the secondary information source for `passwd`, `group` and `shadow`. The local files (`/etc/passwd`, `/etc/groups` and `/etc/shadow`) are used first, as specified by the `compat` source.

```
passwd: compat ldap
group: compat ldap
shadow: compat ldap
```



You are strongly advised to keep `compat` as the first source in NSS for `passwd`, `group` and `shadow`. This prevents you from getting locked out of the system.

Configuring `nslcd.conf`

You need to update the main configuration file (`/etc/nslcd.conf`) after installation to accommodate the expected LDAP server settings. The [nslcd.conf man page](#) details all the available configuration options. Some of the more important options are related to security and how the queries are handled.

Connection

The LDAP client starts a session by connecting to the LDAP server, by default, on TCP and UDP port 389, or on port 636 for LDAPS. Depending on the configuration, this connection may be unauthenticated (anonymous bind); otherwise, the client must provide a bind user and password. The variables used to define the connection to the LDAP server are the URI and bind credentials.

The URI is mandatory, and specifies the LDAP server location using the FQDN or IP address. It also designates whether to use `ldap://` for clear text transport, or `ldaps://` for SSL/TLS encrypted transport. Optionally, an alternate port may also be specified in the URL. Typically, in production environments, it is best to utilize the LDAPS protocol. Otherwise all communications are clear text and not secure.

After the connection to the server is complete, the BIND operation authenticates the session. The BIND credentials are optional, and if not specified, an anonymous bind is assumed. This is typically not allowed in most production environments. Configure authenticated (Simple) BIND by specifying the user (`binddn`) and

password (*bindpw*) in the configuration. Another option is to use SASL (Simple Authentication and Security Layer) BIND, which provides authentication services using other mechanisms, like Kerberos. Contact your LDAP server administrator for this information since it depends on the configuration of the LDAP server and what credentials are created for the client device.

```
# The location at which the LDAP server(s) should be reachable.  
uri ldaps://ldap.example.com  
# The DN to bind with for normal lookups.  
binddn cn=CLswitch,ou=infra,dc=example,dc=com  
bindpw CuMuLuS
```

Search Function

When an LDAP client requests information about a resource, it must connect and bind to the server. Then it performs one or more resource queries depending on what it is looking up. All search queries sent to the LDAP server are created using the configured search *base*, *filter*, and the desired entry (*uid=myuser*) being searched for. If the LDAP directory is large, this search may take a significant amount of time. It is a good idea to define a more specific search base for the common *maps* (*passwd* and *group*).

```
# The search base that will be used for all queries.  
base dc=example,dc=com  
# Mapped search bases to speed up common queries.  
base passwd ou=people,dc=example,dc=com  
base group ou=groups,dc=example,dc=com
```

Search Filters

It is also common to use search filters to specify criteria used when searching for objects within the directory. This is used to limit the search scope when authenticating users. The default filters applied are:

```
filter passwd (objectClass=posixAccount)  
filter group (objectClass=posixGroup)
```

Attribute Mapping

The *map* configuration allows for overriding the attributes pushed from LDAP. To override an attribute for a given *map**, specify the attribute name and the new value. One example of how this is useful is ensuring the shell is *bash* and the home directory is */home/cumulus*:

```
map    passwd homeDirectory "/home/cumulus"  
map    passwd shell "/bin/bash"
```



*In LDAP, the **map** refers to one of the supported maps specified in the manpage for `nslcd.conf` (such as `passwd` or `group`).

Example Configuration

Here is an [example configuration](#) using Cumulus Linux.

Troubleshooting

Using `nslcd` Debug Mode

When setting up LDAP authentication for the first time, Cumulus Networks recommends you turn off this service using `service nslcd stop` and run it in debug mode. Debug mode works whether you are using LDAP over SSL (port 636) or an unencrypted LDAP connection (port 389).

```
cumulus@switch:~$ sudo service nslcd stop
cumulus@switch:~$ sudo nslcd -d
```

Once you enable debug mode, run the following command to test LDAP queries:

```
cumulus@switch:~$ sudo getent myuser
```

If LDAP is configured correctly, the following messages appear after you run the `getent` command:

```
nslcd: DEBUG: accept() failed (ignored): Resource temporarily unavailable
nslcd: [8e1f29] DEBUG: connection from pid=11766 uid=0 gid=0
nslcd: [8e1f29] <passwd(all)> DEBUG: myldap_search(base="dc=example,
dc=com", filter="(objectClass=posixAccount)")
nslcd: [8e1f29] <passwd(all)> DEBUG: ldap_result(): uid=myuser,ou=people,
dc=example,dc=com
nslcd: [8e1f29] <passwd(all)> DEBUG: ldap_result(): ... 152 more results
nslcd: [8e1f29] <passwd(all)> DEBUG: ldap_result(): end of results (162
total)
```

In the output above, `<passwd(all)>` indicates that the entire directory structure was queried.

A specific user can be queried using the command:

```
cumulus@switch:~$ sudo getent passwd myuser
```

You can replace *myuser* with any username on the switch. The following debug output indicates that user *myuser* exists:

```
nslcd: DEBUG: add_uri(ldap://10.50.21.101)
nslcd: version 0.8.10 starting
nslcd: DEBUG: unlink() of /var/run/nslcd/socket failed (ignored): No such
file or directory
nslcd: DEBUG: setgroups(0,NULL) done
nslcd: DEBUG: setgid(110) done
nslcd: DEBUG: setuid(107) done
nslcd: accepting connections
nslcd: DEBUG: accept() failed (ignored): Resource temporarily unavailable
nslcd: [8b4567] DEBUG: connection from pid=11369 uid=0 gid=0
nslcd: [8b4567] <passwd="myuser"> DEBUG: myldap_search(base="
dc=cumulusnetworks,dc=com", filter="(objectClass=posixAccount"
(uid=myuser))")
nslcd: [8b4567] <passwd="myuser"> DEBUG: ldap_initialize
(ldap://<ip_address>)
nslcd: [8b4567] <passwd="myuser"> DEBUG: ldap_set_rebind_proc()
nslcd: [8b4567] <passwd="myuser"> DEBUG: ldap_set_option
(LDAP_OPT_PROTOCOL_VERSION, 3)
nslcd: [8b4567] <passwd="myuser"> DEBUG: ldap_set_option(LDAP_OPT_DEREF, 0)
nslcd: [8b4567] <passwd="myuser"> DEBUG: ldap_set_option(LDAP_OPT_TIMELIMIT,
0)
nslcd: [8b4567] <passwd="myuser"> DEBUG: ldap_set_option(LDAP_OPT_TIMEOUT, 0)
nslcd: [8b4567] <passwd="myuser"> DEBUG: ldap_set_option
(LDAP_OPT_NETWORK_TIMEOUT, 0)
nslcd: [8b4567] <passwd="myuser"> DEBUG: ldap_set_option(LDAP_OPT_REFERRALS,
LDAP_OPT_ON)
nslcd: [8b4567] <passwd="myuser"> DEBUG: ldap_set_option(LDAP_OPT_RESTART,
LDAP_OPT_ON)
nslcd: [8b4567] <passwd="myuser"> DEBUG: ldap_simple_bind_s(NULL,NULL)
(uri="ldap://<ip_address>")
nslcd: [8b4567] <passwd="myuser"> DEBUG: ldap_result(): end of results (0
total)
```

Notice how the <passwd="myuser"> shows that the specific *myuser* user was queried.

Common Problems

SSL/TLS

- The FQDN of the LDAP server URI does not match the FQDN in the CA-signed server certificate exactly.

- `nslcd` cannot read the SSL certificate, and will report a "Permission denied" error in the debug during server connection negotiation. Check the permission on each directory in the path of the root SSL certificate. Ensure that it is readable by the `nslcd` user.

NSCD

- If the `nsqd cache` daemon is also enabled and you make some changes to the user from LDAP, you may want to clear the cache using the commands:

```
nsqd --invalidate = passwd
nsqd --invalidate = group
```

- The `nsqd` package works with `nslcd` to cache name entries returned from the LDAP server. This may cause authentication failures. To work around these issues:

1. Disable `nsqd` by running:

```
cumulus@switch:~$ sudo nsqd -K
```

2. Restart the `nslcd` service:

```
cumulus@switch:~$ sudo service nslcd restart
```

3. Try the authentication again.

LDAP

- The search filter returns wrong results. Check for typos in the search filter. Use `ldapsearch` to test your filter.
- Optionally, configure the basic LDAP connection and search parameters in `/etc/ldap/ldap.conf`

```
# ldapsearch -D 'cn=CLadmin' -w 'CuMuLuS' "(&
(ObjectClass=inetOrgUser)(uid=myuser))"
```

- When a local username also exists in the LDAP database, the order of the information sources in `/etc/nsswitch` can be updated to query LDAP before the local user database. This is generally not recommended. For example, the configuration below ensures that LDAP is queried before the local database.

```
# /etc/nsswitch.conf
passwd:      ldap  compat
```

Configuring LDAP Authorization

Linux uses the `sudo` command to allow non-administrator users — like the default *cumulus* user account — to perform privileged operations. To control the users authorized to use sudo, the `/etc/sudoers` file and files located in the `/etc/sudoers.d/` directory have a series of rules defined. Typically, the rules are based on groups, but can also be defined for specific users. Therefore, sudo rules can be added using the group names from LDAP. For example, if a group of users were associated with the group *netadmin*, a rule can be added to give those users sudo privileges. Refer to the sudoers manual (`man sudoers`) for a complete usage description. Here's an illustration of this in `/etc/sudoers`:

```
# The basic structure of a user specification is "who where = (as_whom)
# what".
%sudo ALL=(ALL:ALL) ALL
%netadmin ALL=(ALL:ALL) ALL
```

Active Directory Configuration

Active Directory (AD) is a fully featured LDAP-based NIS server created by Microsoft. It offers unique features that classic OpenLDAP servers lack. Therefore, it can be more complicated to configure on the client and each version of AD is a little different in how it works with Linux-based LDAP clients. Some more advanced configuration examples, from testing LDAP clients on Cumulus Linux with Active Directory (AD/LDAP), are available in our [knowledge base](#).

LDAP Verification Tools

Typically, password and group information is retrieved from LDAP and cached by the LDAP client daemon. To test the LDAP interaction, these command line tools can be used to trigger an LDAP query from the device. This helps to create the best filters and verify the information sent back from the LDAP server.

Identifying a User with the id Command

The `id` command performs a username lookup by following the lookup information sources in NSS for the `passwd` service. This simply returns the user ID, group ID and the group list retrieved from the information source. In the following example, the user *cumulus* is locally defined in `/etc/passwd`, and *myuser* is on LDAP. The NSS configuration has the `passwd` map configured with the sources `compat ldap`:

```
cumulus@switch:~$ id cumulus
uid=1000(cumulus) gid=1000(cumulus) groups=1000(cumulus),4(adm),27(sudo)
cumulus@switch:~$ id myuser
```

```
uid=1230(myuser) gid=3000(Development) groups=3000(Development),500
(Employees),27(sudo)
```

Using getent

The `getent` command retrieves all records found via NSS for a given map. It can also get a specific entry under that map. Tests can be done with the `passwd`, `group`, `shadow` or any other map configured in `/etc/nsswitch.conf`. The output from this command is formatted according to the map requested. Thus, for the `passwd` service, the structure of the output is the same as the entries in `/etc/passwd`. The same can be said for the `group` map will output the same as `/etc/group`. In this example, looking up a specific user in the `passwd` map, the user `cumulus` is locally defined in `/etc/passwd`, and `myuser` is only in LDAP.

```
cumulus@switch:~$ getent passwd cumulus
cumulus:x:1000:1000::/home/cumulus:/bin/bash
cumulus@switch:~$ getent passwd myuser
myuser:x:1230:3000:My Test User:/home/myuser:/bin/bash
```

In the next example, looking up a specific group in the `group` service, the group `cumulus` is locally defined in `/etc/groups`, and `netadmin` is on LDAP.

```
cumulus@switch:~$ getent group cumulus
cumulus:x:1000:
cumulus@switch:~$ getent group netadmin
netadmin:*:502:matthew,mark,luke,john
```

Running the command `getent passwd` or `getent group` without a specific request, returns **all** local and LDAP entries for the `passwd` and `group` maps, respectively.

Using LDAP search

The `ldapsearch` command performs LDAP operations directly on the LDAP server. This does not interact with NSS. This command helps display what the LDAP daemon process is receiving back from the server. The command has many options. The simplest uses anonymous bind to the host and specifies the search DN and what attribute to lookup.

```
cumulus@switch:~$ ldapsearch -H ldap://ldap.example.com -b dc=example,
dc=com -x uid=myuser
```

[Click here to expand output of command](#)

```
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope subtree
# filter: uid=myuser
# requesting: ALL
#
# myuser, people, example.com
dn: uid=myuser,ou=people,dc=example,dc=com
cn: My User
displayName: My User
gecos: myuser
gidNumber: 3000
givenName: My
homeDirectory: /home/myuser
initials: MU
loginShell: /bin/bash
mail: myuser@example.com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
shadowExpire: -1
shadowFlag: 0
shadowMax: 999999
shadowMin: 8
shadowWarning: 7
sn: User
uid: myuser
uidNumber: 1234

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

LDAP Browsers

There are some GUI LDAP clients that help to work with LDAP servers. These are free tools to help graphically show the structure of the LDAP database.

- Apache Directory Studio
- LDAPManager

References

- <https://wiki.debian.org/LDAP/PAM>
- <https://raw.githubusercontent.com/arthurdejong/nss-pam-ldapd/master/nsLCD.conf>
- <http://backports.debian.org/Instructions/>

Netfilter - ACLs

Netfilter is the packet filtering framework in Cumulus Linux as well as most other Linux distributions. `iptables`, `ip6tables` and `ebtables` are userspace tools in Linux to administer filtering rules for IPv4 packets, IPv6 packets and Ethernet frames (layer 2 using MAC addresses) respectively. `cl-acltool` is the userspace tool to administer filtering rules on Cumulus Linux, and is the only tool for configuring ACLs in Cumulus Linux.

`cl-acltool` operates on a series of configuration files, and uses `iptables`, `ip6tables` and `ebtables` to install rules into the kernel. In addition to programming rules in the kernel, `cl-acltool` programs rules in hardware for interfaces involving switch port interfaces, which `iptables`, `ip6tables` and `ebtables` cannot do on their own.

Contents

(Click to expand)

- Contents (see page 89)
- Commands (see page 90)
- Files (see page 90)
- Understanding Traffic Rules In Cumulus Linux (see page 90)
 - Understanding Chains (see page 90)
 - Understanding Tables (see page 91)
 - Understanding Rules (see page 93)
 - How Rules Are Parsed and Applied (see page 94)
 - Rule Placement in Memory (see page 95)
 - Enabling Nonatomic Updates (see page 95)
 - Using `iptables`/`ip6tables`/`ebtables` Directly (see page 96)
- Installing and Managing ACL Rules with `cl-acltool` (see page 97)
 - Installing Packet Filtering (ACL) Rules (see page 98)
 - Specifying which Policy Files to Install (see page 100)
 - Hardware Limitations on Number of Rules (see page 100)
- Supported Rule Types (see page 102)
 - `iptables`/`ip6tables` Rule Support (see page 102)
 - `ebtables` Rule Support (see page 103)

- Other Unsupported Rules (see page 104)
- Common Examples (see page 104)
 - Policing Control Plane and Data Plane Traffic (see page 104)
 - Setting DSCP on Transit Traffic (see page 105)
 - Verifying DSCP Values on Transit Traffic (see page 106)
 - Checking the Packet and Byte Counters for ACL Rules (see page 106)
 - Filtering Specific TCP Flags (see page 108)
- Example Scenario (see page 109)
 - Switch 1 Configuration (see page 109)
 - Switch 2 Configuration (see page 110)
 - Egress Rule (see page 111)
 - Ingress Rule (see page 111)
 - Input Rule (see page 111)
 - Output Rule (see page 111)
 - Combined Rules (see page 111)
 - Layer 2-only Rules/ebtables (see page 112)
 - Useful Links (see page 112)
- Caveats and Errata (see page 112)

Commands

- cl-acltool
- ebtables
- iptables
- ip6tables

Files

- /etc/cumulus/acl/policy.conf
- /etc/cumulus/acl/policy.d/

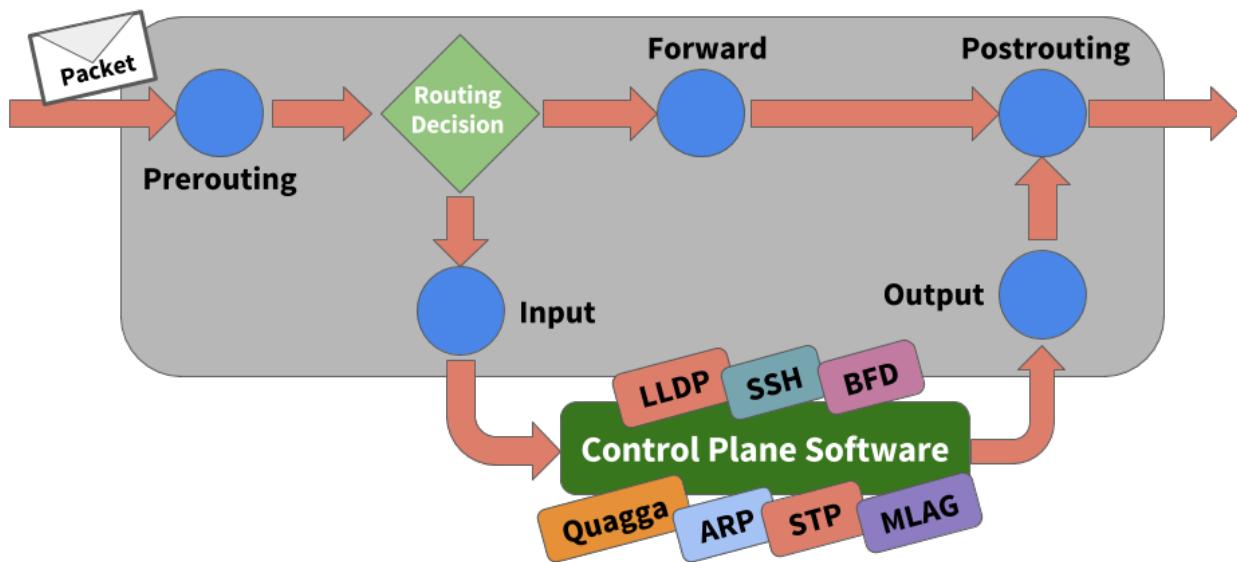
Understanding Traffic Rules In Cumulus Linux

Understanding Chains

Netfilter describes the mechanism for which packets are classified and controlled in the Linux kernel. Cumulus Linux uses the Netfilter framework to control the flow of traffic to, from and across the switch. Netfilter does not require a separate software daemon to run because it is part of the Linux kernel itself. Netfilter asserts policies at layers 2, 3 and 4 of the [OSI model](#) by inspecting packet and frame headers based on a list of rules. Rules are defined using syntax provided by the `iptables`, `ip6tables` and `ebtables` userspace applications.

The rules created by these programs inspect or operate on packets at several points in the life of the packet through the system. These five points are known as *chains* and are shown here:

Traffic Inspection Points (aka Chains)



The chains and their uses are:

- **PREROUTING:** Touches packets before they are routed
- **INPUT:** Touches packets once they are determined to be destined for the local system but before they are received by the control plane software
- **FORWARD:** Touches transit traffic as it moves through the box
- **OUTPUT:** Touches packets that are sourced by the control plane software before they are put on the wire
- **POSTROUTING:** Touches packets immediately before they are put on the wire but after the routing decision has been made

Understanding Tables

When building rules to affect the flow of traffic, the individual chains can be accessed by *tables*. Linux provides three tables by default:

- **Filter:** Classifies traffic or filters traffic
- **NAT:** Applies Network Address Translation rules

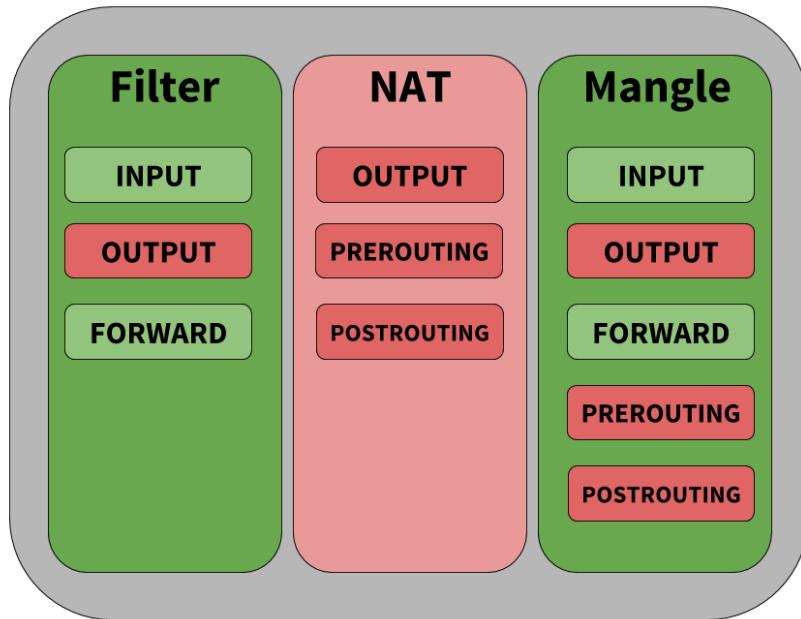


Cumulus Linux does not support NAT.

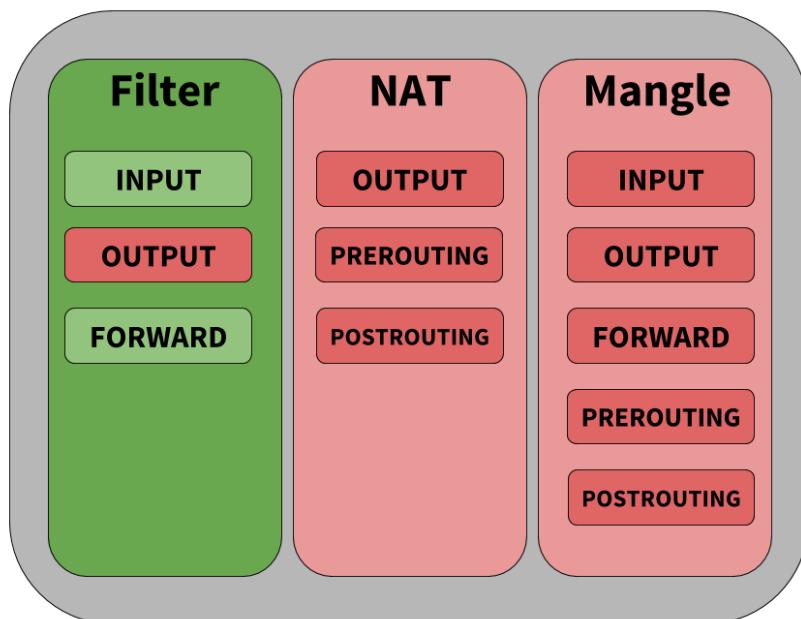
- **Mangle:** Alters packets as they move through the switch

Each table has a set of default chains that can be used to modify or inspect packets at different points of the path through the switch. Chains contain the individual rules to influence traffic. Each table and the default chains they support are shown below. Tables and chains in green are supported by Cumulus Linux, those in red are not supported (that is, they are not hardware accelerated) at this time.

IPtables/IP6tables Table Support



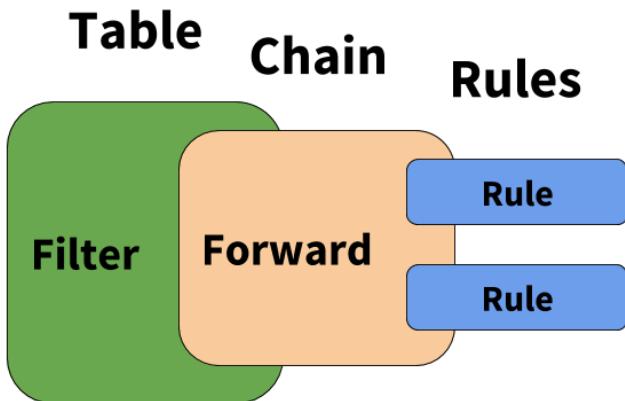
EBtables Table Support





Understanding Rules

Rules are the items that actually classify traffic to be acted upon. Rules are applied to chains, which are attached to tables, similar to the graphic below.



Rules have several different components; the examples below highlight those different components.

(Sets SSH as high priority traffic)

-t mangle	-A FORWARD	-p tcp --dport 22	-j	DSCP --set-dscp 46
-----------	------------	-------------------	----	--------------------

Table	Chain	Matches	Jump	Targets
-------	-------	---------	------	---------

	-A INPUT	-i swp1 -p tcp --dport bgp	-j	POLICE --set-mode pkt
				--set-rate 2000 --set-burst 2000 --set-class 7

(Police and Prioritize BGP Traffic)

- **Table:** The first argument is the *table*. Notice the second example does not specify a table, that is because the filter table is implied if a table is not specified.
- **Chain:** The second argument is the *chain*. Each table supports several different chains. See Understanding Tables above.

- **Matches:** The third argument(s) are called the *matches*. You can specify multiple matches in a single rule. However, the more matches you use in a rule, the more memory that rule consumes.
- **Jump:** The *jump* specifies the target of the rule; that is, what action to take if the packet matches the rule. If this option is omitted in a rule, then matching the rule will have no effect on the packet's fate, but the counters on the rule will be incremented.
- **Target(s):** The *target* can be a user-defined chain (other than the one this rule is in), one of the special built-in targets that decides the fate of the packet immediately (like `DROP`), or an extended target. See the [Supported Rule Types and Common Usages](#) (see page 102) section below for examples of different targets.

How Rules Are Parsed and Applied

All the rules from each chain are read from `iptables`, `ip6tables` and `ebtables` and entered in order into either the filter table or the mangle table. The rules are read from the kernel in the following order:

- IPv6 (`ip6tables`)
- IPv4 (`iptables`)
- `ebtables`

When rules are combined and put into one table, the order determines the relative priority of the rules; `iptables` and `ip6tables` have the highest precedence and `ebtables` has the lowest.

The Linux packet forwarding construct is an overlay for how the silicon underneath processes packets; to that end, here are some things to be aware of:

- The order of operations for how rules are processed is not perfectly maintained when you compare how `iptables` and the switch silicon process packets. The switch silicon reorders rules when `switchd` writes to the ASIC, whereas traditional `iptables` executes the list of rules in order.
- When processing traffic, rules affecting the FORWARD chain that specify an ingress interface are performed prior to rules that match on an egress interface. As a workaround, rules that only affect the egress interface can have an ingress interface wildcard (currently, only `swp+` and `bond+` are supported as wildcard names; see below) that matches any interface applied so that you can maintain order of operations with other input interface rules. Take the following rules, for example:

```
-A FORWARD -i $PORTA -j ACCEPT
-A FORWARD -o $PORTA -j ACCEPT    <-- This rule is performed LAST
                                   (because of egress interface matching)
-A FORWARD -i $PORTB -j DROP
```

If you modify the rules like this, they are performed in order:

```
-A FORWARD -i $PORTA -j ACCEPT
-A FORWARD -i swp+ -o $PORTA -j ACCEPT    <-- These rules are
                                             performed in order (because of wildcard match on ingress interface)
-A FORWARD -i $PORTB -j DROP
```

- When using rules that do a mangle and a filter lookup for a packet, Cumulus Linux does them in parallel and combines the action.

- If a switch port is assigned to a bond, any egress rules must be assigned to the bond.
- When using the OUTPUT chain, rules must be assigned to the source. For example, if a rule is assigned to the switch port in the direction of traffic but the source is a bridge (VLAN), the traffic won't be affected by the rule and must be applied to the bridge.
- If all transit traffic needs to have a rule applied, use the FORWARD chain, not the OUTPUT chain.
- `ebtables` rules are put into either the IPv4 or IPv6 memory space depending on whether the rule utilizes IPv4 or IPv6 to make a decision. Layer 2-only rules, which match the MAC address, are put into the IPv4 memory space.

Rule Placement in Memory

INPUT and ingress (FORWARD -i) rules occupy the same memory space. A rule counts as ingress if the -i option is set. If both input and output options (-i and -o) are set, the rule is considered as ingress and occupies that memory space. For example:

```
-A FORWARD -i swp1 -o swp2 -s 10.0.14.2 -d 10.0.15.8 -p tcp -j ACCEPT
```



If you set an output flag with the INPUT chain you will get an error. For example, running `cl-acltool -i` on the following rule:

```
-A FORWARD,INPUT -i swp1 -o swp2 -s 10.0.14.2 -d 10.0.15.8 -p tcp -j  
ACCEPT
```

generates the following error:

```
error: line 2 : output interface specified with INPUT chain error  
processing rule '-A FORWARD,INPUT -i swp1 -o swp2 -s 10.0.14.2 -d  
10.0.15.8 -p tcp -j ACCEPT'
```

However, simply removing the -o option and interface would make it a valid rule.

Enabling Nonatomic Updates

You can enable nonatomic updates for `switchd`, which offer better scaling because all hardware resources are used to actively impact traffic. With atomic updates, half of the hardware resources are on standby and do not actively impact traffic.

To always start `switchd` with nonatomic updates:

1. Edit `/etc/cumulus/switchd.conf`.
2. Add the following line to the file:

```
acl.non_atomic_update_mode = TRUE
```

3. Restart `switchd` (see page 115):

```
cumulus@switch:~$ sudo systemctl restart switchd
```



During nonatomic updates, traffic is stopped first, and enabled after the new configuration is written into the hardware completely.

Using `iptables/ip6tables/ebtables` Directly

Using `iptables/ip6tables/ebtables` directly is not recommended because any rules installed in these cases only are applied to the Linux kernel and are not hardware accelerated via synchronization to the switch silicon. Also running `cl-acltool -i` (the installation command) resets all rules and deletes anything that is not stored in `/etc/cumulus/acl/policy.conf`.

For example, performing:

```
cumulus@switch:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

Appears to work, and the rule appears when you run `cl-acltool -L`:

```
cumulus@switch:~$ sudo cl-acltool -L ip
-----
Listing rules of type iptables:
-----
TABLE filter :
Chain INPUT (policy ACCEPT 72 packets, 5236 bytes)
pkts bytes target prot opt in out source destination
0 0 DROP icmp -- any any anywhere anywhere icmp echo-request
```

However, the rule is not synced to hardware when applied in this fashion and running `cl-acltool -i` or `reboot` removes the rule without replacing it. To ensure all rules that can be in hardware are hardware accelerated, place them in `/etc/cumulus/acl/policy.conf` and install them by running `cl-acltool -i`.

Installing and Managing ACL Rules with `cl-acltool`

You manage Cumulus Linux ACLs with `cl-acltool`. Rules are first written to the `iptables` chains, as described above, and then synced to hardware via `switchd`.

To examine the current state of chains and list all installed rules, run:

```
cumulus@switch:~$ sudo cl-acltool -L all
-----
Listing rules of type iptables:
-----
TABLE filter :
Chain INPUT (policy ACCEPT 90 packets, 14456 bytes)
pkts bytes target prot opt in out source destination
0 0 DROP all -- swp+ any 240.0.0.0/5 anywhere
0 0 DROP all -- swp+ any loopback/8 anywhere
0 0 DROP all -- swp+ any base-address.mcast.net/8 anywhere
0 0 DROP all -- swp+ any 255.255.255.255 anywhere ...
```

To list installed rules using native `iptables`, `ip6tables` and `ebtables`, run these commands:

```
cumulus@switch:~$ sudo iptables -L
cumulus@switch:~$ sudo ip6tables -L
cumulus@switch:~$ sudo ebtables -L
```

To flush all installed rules, run:

```
cumulus@switch:~$ sudo cl-acltool -F all
```

To flush only the IPv4 `iptables` rules, run:

```
cumulus@switch:~$ sudo cl-acltool -F ip
```

If the install fails, ACL rules in the kernel and hardware are rolled back to the previous state. Errors from programming rules in the kernel or ASIC are reported appropriately.

Installing Packet Filtering (ACL) Rules

`cl-acltool` takes access control list (ACL) rules input in files. Each ACL policy file contains `iptables`, `ip6tables` and `ebtables` categories under the tags `[iptables]`, `[ip6tables]` and `[ebtables]` respectively.

Each rule in an ACL policy must be assigned to one of the rule categories above.

See `man cl-acltool(5)` for ACL rule details. For `iptables` rule syntax, see `man iptables(8)`. For `ip6tables` rule syntax, see `man ip6tables(8)`. For `ebtables` rule syntax, see `man ebttables(8)`.

See `man cl-acltool(5)` and `man cl-acltool(8)` for further details on using `cl-acltool`; however, some examples are listed here, and more are listed [later in this chapter \(see page\)](#).



By default:

- ACL policy files are located in `/etc/cumulus/acl/policy.d/`.
- All `*.rules` files in this directory are included in `/etc/cumulus/acl/policy.conf`.
- All files included in this `policy.conf` file are installed when the switch boots up.
- The `policy.conf` file expects rules files to have a `.rules` suffix as part of the file name.

Here is an example ACL policy file:

```
[iptables]
-A INPUT --in-interface swp1 -p tcp --dport 80 -j ACCEPT
-A FORWARD --in-interface swp1 -p tcp --dport 80 -j ACCEPT

[ip6tables]
-A INPUT --in-interface swp1 -p tcp --dport 80 -j ACCEPT
-A FORWARD --in-interface swp1 -p tcp --dport 80 -j ACCEPT

[ebtables]
-A INPUT -p IPv4 -j ACCEPT
-A FORWARD -p IPv4 -j ACCEPT
```

You can use wildcards or variables to specify chain and interface lists to ease administration of rules.



Interface Wildcards – Currently only `swp+` and `bond+` are supported as wildcard names. There may be kernel restrictions in supporting more complex wildcards like `swp1+` etc.

```
INGRESS = swp+
INPUT_PORT_CHAIN = INPUT,FORWARD
```

```
[iptables]
-A $INPUT_PORT_CHAIN --in-interface $INGRESS -p tcp --dport 80 -j ACCEPT

[ip6tables]
-A $INPUT_PORT_CHAIN --in-interface $INGRESS -p tcp --dport 80 -j ACCEPT

[ebtables]
-A INPUT -p IPv4 -j ACCEPT
```

ACL rules for the system can be written into multiple files under the default `/etc/cumulus/acl/policy.d/` directory. The ordering of rules during installation follows the sort order of the files based on their file names.

Use multiple files to stack rules. The example below shows two rules files separating rules for management and datapath traffic:

```
cumulus@switch:~$ ls /etc/cumulus/acl/policy.d/ 00sample_mgmt.rules
01sample_datapath.rules
cumulus@switch:~$ cat /etc/cumulus/acl/policy.d/00sample_mgmt.rules

INGRESS_INTF = swp+
INGRESS_CHAIN = INPUT

[iptables]
# protect the switch management
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -s 10.0.14.2 -d 10.0.15.8 -p
tcp -j ACCEPT
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -s 10.0.11.2 -d 10.0.12.8 -p
tcp -j ACCEPT
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -d 10.0.16.8 -p udp -j DROP

cumulus@switch:~$ cat /etc/cumulus/acl/policy.d/01sample_datapath.rules
INGRESS_INTF = swp+
INGRESS_CHAIN = INPUT, FORWARD

[iptables]
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -s 192.0.2.5 -p icmp -j
ACCEPT
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -s 192.0.2.6 -d 192.0.2.4 -j
DROP
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -s 192.0.2.2 -d 192.0.2.8 -j
DROP
```

Install all ACL policies under a directory:

```
cumulus@switch:~$ sudo cl-acltool -i -P ./rules
Reading files under rules
Reading rule file ./rules/01_http_rules.txt ...
Processing rules in file ./rules/01_http_rules.txt ...
Installing acl policy ...
Done.
```

Install all rules and policies included in /etc/cumulus/acl/policy.conf:

```
cumulus@switch:~$ sudo cl-acltool -i
```

Specifying which Policy Files to Install

By default, any .rules file you configure in /etc/cumulus/acl/policy.d/ get installed by Cumulus Linux. To add other policy files to an ACL, you need to include them in /etc/cumulus/acl/policy.conf . For example, in order for Cumulus Linux to install a rule in a policy file called 01_new.rules , you would add `include /etc/cumulus/acl/policy.d/01_new.rules` to policy.conf , as in this example:

```
cumulus@switch:~$ sudo vi /etc/cumulus/acl/policy.conf

#
# This file is a master file for acl policy file inclusion
#
# Note: This is not a file where you list acl rules.
#
# This file can contain:
# - include lines with acl policy files
#   example:
#     include <filepath>
#
# see manpage cl-acltool(5) and cl-acltool(8) for how to write policy files
#

include /etc/cumulus/acl/policy.d/*.rules
include /etc/cumulus/acl/policy.d/01_new.rules
```

Hardware Limitations on Number of Rules

The maximum number of rules that can be handled in hardware is a function of the platform type (Apollo2, Firebolt2, Triumph, Trident, Trident+ or Trident II) and a mix of IPv4 and/or IPv6. See the [HCL](#) to determine which platform type applies to a particular switch.

Apollo2 and Triumph2 Limits

Direction	Atomic Mode IPv4 Rules	Atomic Mode IPv6 Rules	Nonatomic Mode IPv4 Rules	Nonatomic Mode IPv6 Rules
Ingress	2048	1024	4096	2048
Egress	512	256	1024	512

Firebolt2 Limits

Direction	Atomic Mode IPv4 Rules	Atomic Mode IPv6 Rules	Nonatomic Mode IPv4 Rules	Nonatomic Mode IPv6 Rules
Ingress	1024	512	2048	1024
Egress	512	256	512	256

Trident/Trident+ Limits

Direction	Atomic Mode IPv4 Rules	Atomic Mode IPv6 Rules	Nonatomic Mode IPv4 Rules	Nonatomic Mode IPv6 Rules
Ingress	384	384	1024	1024
Egress	512	256	1024	512

Trident II Limits

Direction	Atomic Mode IPv4 Rules	Atomic Mode IPv6 Rules	Nonatomic Mode IPv4 Rules	Nonatomic Mode IPv6 Rules
Ingress	1024	1024	2048	2048
Egress	512	256	1024	512

If the maximum number of rules for a particular table is exceeded, `cl-acltool -i` generates the following error:

```
error: hw sync failed (sync_acl hardware installation failed) Rolling back
.. failed.
```

Supported Rule Types

The `iptables`/`ip6tables`/`ebtables` construct tries to layer the Linux implementation on top of the underlying hardware but they are not always directly compatible. Here are the supported rules for chains in `iptables`, `ip6tables` and `ebtables`.



To learn more about any of the options shown in the tables below, run `iptables -h [name of option]`. The same help syntax works for options for `ip6tables` and `ebtables`.

[Click here to see Example of Help Syntax for an Ebttables target](#)

```
root@leaf1# ebtables -h tricolorpolice
<...snip...
tricolorpolice option:
  --set-color-mode STRING setting the mode in blind or aware
  --set-cir INT setting committed information rate in kbits per
second
  --set-cbs INT setting committed burst size in kbyte
  --set-pir INT setting peak information rate in kbits per
second
  --set-ebs INT setting excess burst size in kbyte
  --set-conform-action-dscp INT setting dscp value if the
action is accept for conforming packets
  --set-exceed-action-dscp INT setting dscp value if the action
is accept for exceeding packets
  --set-violate-action STRING setting the action (accept/drop) f
or violating packets
  --set-violate-action-dscp INT setting dscp value if the
action is accept for violating packets
Supported chains for the filter table:
INPUT FORWARD OUTPUT
```

`iptables`/`ip6tables` Rule Support

Rule Element	Supported	Unsupported
Matches	<ul style="list-style-type: none"> Src/Dst, IP protocol In/out interface IPv4: icmp, ttl, IPv6: icmp6, frag, hl, IP common: tcp (with flags (see page 108)), udp, multiport, TOS, DSCP, addrtype 	<ul style="list-style-type: none"> Rules with input/output Ethernet interfaces are ignored Inverse matches
	<ul style="list-style-type: none"> ACCEPT, DROP 	

Rule Element	Supported	Unsupported
Standard Targets		<ul style="list-style-type: none"> • RETURN, QUEUE, STOP, Fall Thru, Jump
Extended Targets	<ul style="list-style-type: none"> • LOG (IPv4/IPv6); UID is not supported for LOG • TCP SEQ, TCP options or IP options • ULOG • SETQOS • DSCP <p><i>Unique to Cumulus Linux:</i></p> <ul style="list-style-type: none"> • SPAN • ERSPAN (IPv4/IPv6) • POLICE • TRICOLORPOLICE • SETCLASS 	

ebtables Rule Support

Rule Element	Supported	Unsupported
Matches	<ul style="list-style-type: none"> • ether type • input interface/wildcard • output interface/wildcard • src/dst MAC • IP: src, dest, tos, proto, sport, dport • IPv6: tclass, icmp6: type, icmp6: code range, src /dst addr, sport, dport 	<ul style="list-style-type: none"> • Inverse matches • Proto length • VLAN
Standard Targets	<ul style="list-style-type: none"> • ACCEPT, DROP 	<ul style="list-style-type: none"> • Return, Continue, Jump, Fall Thru
Extended Targets	<ul style="list-style-type: none"> • Ulog • log <p><i>Unique to Cumulus Linux:</i></p> <ul style="list-style-type: none"> • span • erspan • police 	

Rule Element	Supported	Unsupported
	<ul style="list-style-type: none"> • tricolorpolice • setclass 	

Other Unsupported Rules

- Rules that have no matches and accept all packets in a chain are currently ignored. This probably has side effects in the sense that the rules below them do get hit, when normally they wouldn't.
- Chain default rules (which are ACCEPT) are also ignored.
- Rules that match on eth* interfaces are assumed to be Linux management interfaces and are ignored.

Common Examples

Policing Control Plane and Data Plane Traffic

You can configure quality of service for traffic on both the control plane and the data plane. By using QoS policers, you can rate limit traffic so incoming packets get dropped if they exceed specified thresholds.



Counters on POLICE ACL rules in `iptables` do not currently show the packets that are dropped due to those rules.

Use the POLICE target with `iptables`. POLICE takes these arguments:

- `--set-class value`: Sets the system internal class of service queue configuration to *value*.
- `--set-rate value`: Specifies the maximum rate in kilobytes (KB) or packets.
- `--set-burst value`: Specifies the number of packets or kilobytes (KB) allowed to arrive sequentially.
- `--set-mode string`: Sets the mode in KB (kilobytes) or pkt (packets) for rate and burst size.

For example, to rate limit the incoming traffic on swp1 to 400 packets/second with a burst of 100 packets /second and set the class of the queue for the policed traffic as 0, set this rule in your appropriate `.rules` file:

```
-A INPUT --in-interface swp1 -j POLICE --set-mode pkt --set-rate 400 --set-burst 100 --set-class 0
```

Here is another example of control plane ACL rules to lock down the switch. You specify them in `/etc/cumulus/acl/policy.d/00control_plane.rules`:

```
INGRESS_INTF = swp+
INGRESS_CHAIN = INPUT
```

```

INNFWD_CHAIN = INPUT, FORWARD
MARTIAN_SOURCES_4 = "240.0.0.0/5,127.0.0.0/8,224.0.0.0/8,255.255.255.255
/32"
MARTIAN_SOURCES_6 = "ff00::/8, ::/128, ::ffff:0.0.0.0/96, ::1/128"

# Custom Policy Section
SSH_SOURCES_4 = "192.168.0.0/24"
NTP_SERVERS_4 = "192.168.0.1/32,192.168.0.4/32"
DNS_SERVERS_4 = "192.168.0.1/32,192.168.0.4/32"
SNMP_SERVERS_4 = "192.168.0.1/32"

[iptables]
-A $INNFWD_CHAIN --in-interface $INGRESS_INTF -s $MARTIAN_SOURCES_4 -j DROP
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p ospf -j POLICE --set-mode
pkt --set-rate 2000 --set-burst 2000 --set-class 7
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p tcp --dport bgp -j POLICE
--set-mode pkt --set-rate 2000 --set-burst 2000 --set-class 7
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p tcp --sport bgp -j POLICE
--set-mode pkt --set-rate 2000 --set-burst 2000 --set-class 7
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p icmp -j POLICE --set-mode
pkt --set-rate 100 --set-burst 40 --set-class 2
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p udp --dport bootps:bootpc
-j POLICE --set-mode pkt --set-rate 100 --set-burst 100 --set-class 2
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p tcp --dport bootps:bootpc
-j POLICE --set-mode pkt --set-rate 100 --set-burst 100 --set-class 2
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p igmp -j POLICE --set-mode
pkt --set-rate 300 --set-burst 100 --set-class 6

# Custom policy
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p tcp --dport 22 -s
$SSH_SOURCES_4 -j ACCEPT
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p udp --sport 123 -s
$NTP_SERVERS_4 -j ACCEPT
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p udp --sport 53 -s
$DNS_SERVERS_4 -j ACCEPT
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p udp --dport 161 -s
$SNMP_SERVERS_4 -j ACCEPT

# Allow UDP traceroute when we are the current TTL expired hop
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p udp --dport 1024:65535 -m
ttl --ttl-eq 1 -j ACCEPT
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -j DROP

```

Setting DSCP on Transit Traffic

The examples here use the *mangle* table to modify the packet as it transits the switch. DSCP is expressed in **decimal notation** in the examples below.

```
[iptables]

#Set SSH as high priority traffic.
-t mangle -A FORWARD -p tcp --dport 22 -j DSCP --set-dscp 46

#Set everything coming in SWP1 as AF13
-t mangle -A FORWARD --in-interface swp1 -j DSCP --set-dscp 14

#Set Packets destined for 10.0.100.27 as best effort
-t mangle -A FORWARD -d 10.0.100.27/32 -j DSCP --set-dscp 0

#Example using a range of ports for TCP traffic
-t mangle -A FORWARD -p tcp -s 10.0.0.17/32 --sport 10000:20000 -d 10.0.100.27/32 --dport 10000:20000 -j DSCP --set-dscp 34
```

Verifying DSCP Values on Transit Traffic

The examples here use the DSCP match criteria in combination with other IP, TCP and interface matches to identify traffic and count the number of packets.

```
[iptables]

#Match and count the packets that match SSH traffic with DSCP EF
-A FORWARD -p tcp --dport 22 -m dscp --dscp 46 -j ACCEPT

#Match and count the packets coming in SWP1 as AF13
-A FORWARD --in-interface swp1 -m dscp --dscp 14 -j ACCEPT
#Match and count the packets with a destination 10.0.0.17 marked best
#effort
-A FORWARD -d 10.0.100.27/32 -m dscp --dscp 0 -j ACCEPT

#Match and count the packets in a port range with DSCP AF41
-A FORWARD -p tcp -s 10.0.0.17/32 --sport 10000:20000 -d 10.0.100.27/32 --dport 10000:20000 -m dscp --dscp 34 -j ACCEPT
```

Checking the Packet and Byte Counters for ACL Rules

To verify the counters, using the above example rules, first send test traffic matching the patterns through the network. The following example generates traffic with **mz**, which can be installed on host servers or even on Cumulus Linux switches. Once traffic is sent to validate the counters, they are matched on switch1 use **cl-acltool**.

```
# Send 100 TCP packets on Host1 with a DSCP value of EF with a
destination of Host2 TCP port 22:

cumulus@host1$ mz eth1 -A 10.0.0.17 -B 10.0.100.27 -c 100 -v -t tcp "d
p=22,dscp=46"
    IP: ver=4, len=40, tos=184, id=0, frag=0, ttl=255, proto=6, sum=0,
    SA=10.0.0.17, DA=10.0.100.27,
        payload=[see next layer]
    TCP: sp=0, dp=22, S=42, A=42, flags=0, win=10000, len=20, sum=0,
        payload=

# Verify the 100 packets are matched on switch1
cumulus@switch1$ sudo cl-acltool -L ip
-----
Listing rules of type iptables:
-----
TABLE filter :
Chain INPUT (policy ACCEPT 9314 packets, 753K bytes)
  pkts bytes target      prot opt in     out      source
destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target      prot opt in     out      source
destination
    100   6400 ACCEPT      tcp   --  any     any     anywhere
anywhere          tcp dpt:ssh DSCP match 0x2e
      0     0 ACCEPT      all   --  swp1   any     anywhere
anywhere          DSCP match 0x0e
      0     0 ACCEPT      all   --  any     any     10.0.0.17
anywhere          DSCP match 0x00
      0     0 ACCEPT      tcp   --  any     any     10.0.0.17
.0.100.27          tcp spts:webmin:20000 dpts:webmin:2002      10
```

```
# Send 100 packets with a small payload on Host1 with a DSCP value of
AF13 with a destination of Host2:

cumulus@host1$ mz eth1 -A 10.0.0.17 -B 10.0.100.27 -c 100 -v -t ip
    IP: ver=4, len=20, tos=0, id=0, frag=0, ttl=255, proto=0, sum=0, SA=
10.0.0.17, DA=10.0.100.27,
        payload=

# Verify the 100 packets are matched on switch1
cumulus@switch1$ sudo cl-acltool -L ip
-----
Listing rules of type iptables:
-----
TABLE filter :
Chain INPUT (policy ACCEPT 9314 packets, 753K bytes)
  pkts bytes target      prot opt in     out      source
destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
```

pkts	bytes	target	prot	opt	in	out	source
destination							
100	6400	ACCEPT	tcp	--	any	any	anywhere
anywhere				dpt:ssh	DSCP	match	0x2e
100	7000	ACCEPT	all	--	swp3	any	anywhere
anywhere				DSCP	match	0x0e	
100	6400	ACCEPT	all	--	any	any	10.0.0.17
anywhere				DSCP	match	0x00	
0	0	ACCEPT	tcp	--	any	any	10.0.0.17
.0.100.27				spts:webmin:20000	dpts:webmin:2002		10

```
# Send 100 packets on Host1 with a destination of Host2:
```

```
cumulus@host1$ mz eth1 -A 10.0.0.17 -B 10.0.100.27 -c 100 -v -t ip
  IP: ver=4, len=20, tos=56, id=0, frag=0, ttl=255, proto=0, sum=0,
  SA=10.0.0.17, DA=10.0.100.27,
    payload=
```

```
# Verify the 100 packets are matched on switch1
cumulus@switch1$ sudo cl-acltool -L ip
```

```
-----
Listing rules of type iptables:
-----
```

```
TABLE filter :
```

Chain INPUT (policy ACCEPT 9314 packets, 753K bytes)							
pkts	bytes	target	prot	opt	in	out	source
destination							
100	6400	ACCEPT	tcp	--	any	any	anywhere
anywhere				dpt:ssh	DSCP	match	0x2e
100	7000	ACCEPT	all	--	swp3	any	anywhere
anywhere				DSCP	match	0x0e	
0	0	ACCEPT	all	--	any	any	10.0.0.17
anywhere				DSCP	match	0x00	
0	0	ACCEPT	tcp	--	any	any	10.0.0.17
.0.100.27				spts:webmin:20000	dpts:webmin:2002		10

Filtering Specific TCP Flags

The example solution below creates rules on the INPUT and FORWARD chains to drop ingress IPv4 and IPv6 TCP packets when the SYN bit is set and the RST, ACK and FIN bits are reset. The default for the INPUT and FORWARD chains allows all other packets. The ACL is applied to ports swp20 and swp21. After configuring this ACL, new TCP sessions that originate from ingress ports swp20 and swp21 will not be allowed. TCP sessions that originate from any other port are allowed.

```
INGRESS_INTF = swp20,swp21
```

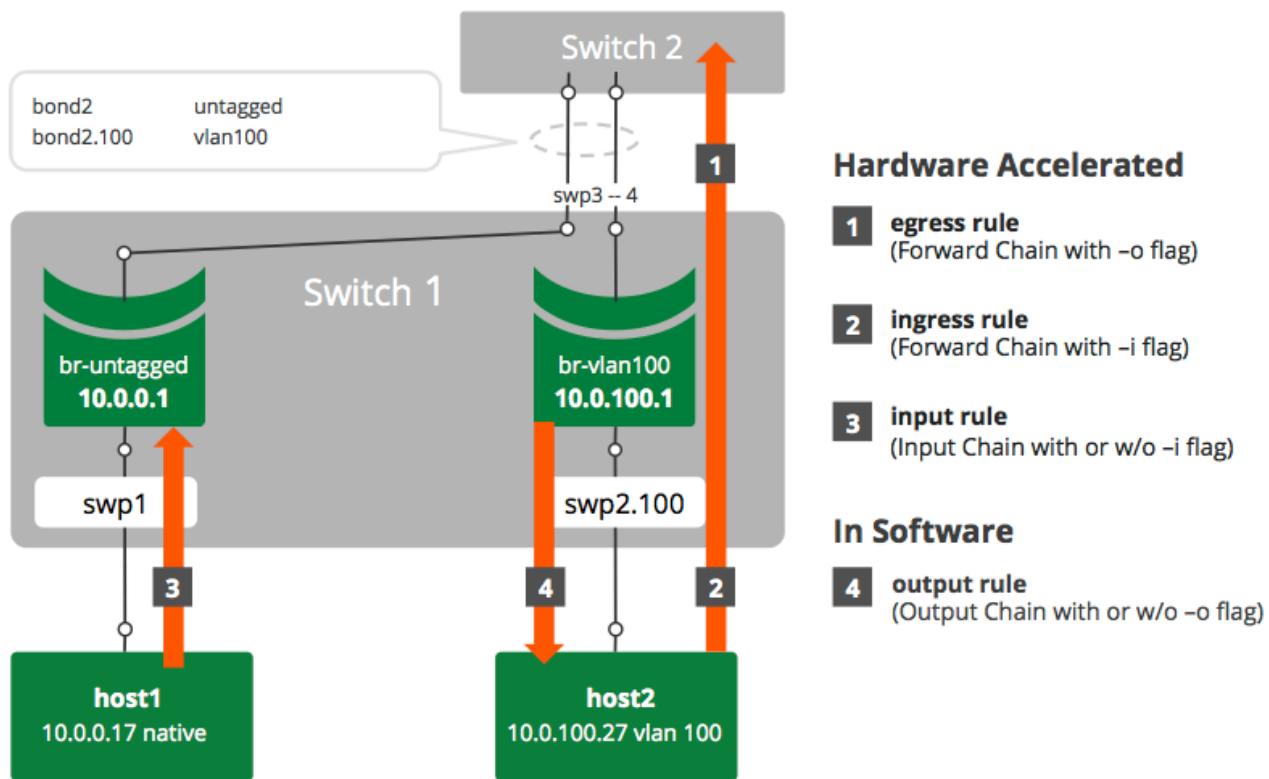
```
[iptables]
-A INPUT, FORWARD --in-interface $INGRESS_INTF -p tcp --syn -j DROP
[ip6tables]
-A INPUT, FORWARD --in-interface $INGRESS_INTF -p tcp --syn -j DROP
```

The `--syn` flag in the above rule matches packets with the SYN bit set and the ACK, RST and FIN bits are cleared. It is equivalent to using `-tcp-flags SYN,RST,ACK,FIN SYN`. For example, the above rule could be re-written as:

```
-A INPUT, FORWARD --in-interface $INGRESS_INTF -p tcp --tcp-flags SYN,
RST,ACK,FIN SYN -j DROP
```

Example Scenario

The following example scenario demonstrates where several different rules are applied to show what is possible.



Following are the configurations for the two switches used in these examples. The configuration for each switch appears in `/etc/network/interfaces` on that switch.

Switch 1 Configuration

```
auto swp1
```

```
iface swp1

auto swp2
iface swp2

auto swp3
iface swp3

auto swp4
iface swp4

auto bond2
iface bond2
    bond-slaves swp3 swp4

auto br-untagged
iface br-untagged
    address 10.0.0.1/24
    bridge_ports swp1 bond2
    bridge_stp on

auto br-tag100
iface br-tag100
    address 10.0.100.1/24
    bridge_ports swp2.100 bond2.100
    bridge_stp on
```

Switch 2 Configuration

```
auto swp3
iface swp3

auto swp4
iface swp4

auto br-untagged
iface br-untagged
    address 10.0.0.2/24
    bridge_ports bond2
    bridge_stp on

auto br-tag100
iface br-tag100
    address 10.0.100.2/24
    bridge_ports bond2.100
    bridge_stp on

auto bond2
iface bond2
```

```
bond-slaves swp3 swp4
```

Egress Rule

The following rule blocks any TCP with destination port 200 traffic going from host1 or host2 through the switch (corresponding to rule 1 in the diagram above).

```
[iptables] -A FORWARD -o bond2 -p tcp --dport 200 -j DROP
```

Ingress Rule

The following rule blocks any UDP traffic with source port 200 going from host1 through the switch (corresponding to rule 2 in the diagram above).

```
[iptables] -A FORWARD -i swp2 -p udp --sport 200 -j DROP
```

Input Rule

The following rule blocks any UDP traffic with source port 200 and destination port 50 going from host1 to the switch (corresponding to rule 3 in the diagram above).

```
[iptables] -A INPUT -i swp1 -p udp --sport 200 --dport 50 -j DROP
```

Output Rule

The following rule blocks any TCP traffic with source port 123 and destination port 123 going from Switch 1 to host2 (corresponding to rule 4 in the diagram above).

```
[iptables] -A OUTPUT -o br-tag100 -p tcp --sport 123 --dport 123 -j DROP
```

Combined Rules

The following rule blocks any TCP traffic with source port 123 and destination port 123 going from any switch port egress or generated from Switch 1 to host1 or host2 (corresponding to rules 1 and 4 in the diagram above).

```
[iptables] -A OUTPUT, FORWARD -o swp+ -p tcp --sport 123 --dport 123 -j DROP
```

This also becomes 2 ACLs, and is effectively the same as:

```
[iptables]
-A FORWARD -o swp+ -p tcp --sport 123 --dport 123 -j DROP
-A OUTPUT -o swp+ -p tcp --sport 123 --dport 123 -j DROP
```

Layer 2-only Rules/ebtables

The following rule blocks any traffic with source MAC address 00:00:00:00:00:12 and destination MAC address 08:9e:01:ce:e2:04 going from any switch port egress/ingress.

```
[ebtables] -A FORWARD -s 00:00:00:00:00:12 -d 08:9e:01:ce:e2:04 -j
DROP
```

Useful Links

- www.netfilter.org
- Netfilter.org packet filtering how-to

Caveats and Errata

- As mentioned in the [Supported Rules](#) section (see page 102) above, not all `iptables`, `ip6tables` or `ebtables` rules are supported. Reference that section for specific rule support.
- Logged packets cannot be forwarded. The hardware cannot both forward a packet and send the packet to the control plane (or kernel) for logging. To emphasize this, a log action must also have a drop action.
- Bridge traffic that matches LOG ACTION rules are not logged in syslog, as the kernel and hardware identify packets using different information.

Configuring switchd

`switchd` is the daemon at the heart of Cumulus Linux. It communicates between the switch and Cumulus Linux, and all the applications running on Cumulus Linux.

The `switchd` configuration is stored in `/etc/cumulus/switchd.conf`.



Versions of Cumulus Linux prior to 2.1 stored the `switchd` configuration at `/etc/default/switchd`.

Contents

(Click to expand)

- [Contents \(see page 112\)](#)
- [The switchd File System \(see page 113\)](#)

- Configuring switchd Parameters (see page 114)
- Restarting switchd (see page 115)
- Commands (see page 115)
- Configuration Files (see page 116)

The switchd File System

switchd also exports a file system, mounted on /cumulus/switchd, that presents all the switchd configuration options as a series of files arranged in a tree structure. You can see the contents by parsing the switchd tree; run `tree /cumulus/switchd`. The output below is for a switch with one switch port configured:

```
cumulus@cumulus:~# sudo tree /cumulus/switchd/
/cumulus/switchd/
|-- config
|   |-- acl
|   |   |-- non_atomic_update_mode
|   |   `-- optimize_hw
|   |-- arp
|   |   '-- next_hops
|   |-- buf_util
|   |   |-- measure_interval
|   |   '-- poll_interval
|   |-- coalesce
|   |   |-- reducer
|   |   '-- timeout
|   |-- disable_internal_restart
|   |-- ignore_non_swps
|   |-- interface
|   |   |-- swp1
|   |   |   '-- storm_control
|   |   |       |-- broadcast
|   |   |       |-- multicast
|   |   |       '-- unknown_unicast
|   |-- logging
|   |-- route
|   |   |-- host_max_percent
|   |   |-- max_routes
|   |   '-- table
`-- stats
    '-- poll_interval
|-- ctrl
|   |-- acl
|   '-- hal
```

```
|   |   `-- resync
|   |-- logger
|   |-- netlink
|   |   `-- resync
|   |-- resync
`-- sample
    `-- ulog_channel
`-- run
    `-- route_info
        |-- ecmp_nh
        |   |-- count
        |   |-- max
        |   `-- max_per_route
        |-- host
        |   |-- count
        |   |-- count_v4
        |   |-- count_v6
        |   `-- max
        |-- mac
        |   |-- count
        |   `-- max
    `-- route
        |-- count_0
        |-- count_1
        |-- count_total
        |-- count_v4
        |-- count_v6
        |-- mask_limit
        |-- max_0
        |-- max_1
        `-- max_total
`-- version
```

Configuring switchd Parameters

You can use `cl-cfg` to configure many `switchd` parameters at runtime (like ACLs, interfaces, and route table utilization), which minimizes disruption to your running switch. However, some options are read only and cannot be configured at runtime.

For example, to see data related to routes, run:

```
cumulus@cumulus:~$ sudo cl-cfg -a switchd | grep route
route.table = 254
```

```
route.max_routes = 32768  
route.host_max_percent = 50  
cumulus@cumulus:~$
```

To modify the configuration, run `cl-cfg -w`. For example, to set the buffer utilization measurement interval to 1 minute, run:

```
cumulus@cumulus:~$ sudo cl-cfg -w switchd buf_util.measure_interval=1
```

To verify that the value changed, use `grep`:

```
cumulus@cumulus:~# cl-cfg -a switchd | grep buf  
buf_util.poll_interval = 0  
buf_util.measure_interval = 1
```



You can get some of this information by running `cl-resource-query`; though you cannot update the `switchd` configuration with it.

Restarting `switchd`

Whenever you modify any `switchd` hardware configuration file (typically changing any `*.conf` file that requires making a change to the switching hardware, like `/etc/cumulus/datapath/traffic.conf`), you must restart `switchd` for the change to take effect:

```
cumulus@switch:~$ sudo service switchd restart
```



You do not have to restart the `switchd` service when you update a network interface configuration (that is, edit `/etc/network/interfaces`).



Restarting `switchd` causes all network ports to reset in addition to resetting the switch hardware configuration.

Commands

- `cl-cfg`

Configuration Files

- /etc/cumulus/switchd.conf

Power over Ethernet - PoE

Cumulus Linux supports Power over Ethernet (PoE), so certain Cumulus Linux switches can supply power from Ethernet switch ports to enabled devices over the Ethernet cables that connect them.

The [currently supported platforms](#) include:

- Accton AS4610-54P, a newly supported switch with an ARM processor



PoE+ and uPoE are not supported at this time.

How It Works

When a powered device is connected to the switch via an Ethernet cable:

- If the available power is greater than the power required by the connected device, power is supplied to the switch port, and the device powers on
- If available power is less than the power required by the connected device and the switch port's priority is less than the port priority set on all powered ports, power is **not** supplied to the port
- If available power is less than the power required by the connected device and the switch port's priority is greater than the priority of a currently powered port, power is removed from lower priority port(s) and power is supplied to the port
- If the total consumed power exceeds the configured power limit of the power source, low priority ports are turned off. In the case of a tie, the port with the lower port number gets priority

For the Accton AS4610-54P switch, power is available as follows:

PSU 1	PSU 2	PoE Power Budget
920W	x	750W
x	920W	750W
920W	920W	1650W

The AS4610-54P has an LED on the front panel to indicate PoE status:

- Green: The `poed` daemon is running and no errors are detected
- Yellow: One or more errors are detected or the `poed` daemon is not running

About Link State and PoE State

Link state and PoE state are completely independent of each other. When a link is brought down on particular port using `ip link <port> down`, power on that port is not turned off.

LLDP with POE Attributes not Supported

Cumulus Linux does not support LLDP auto discovery and negotiation of PoE attributes via LLDP between the powered device and the switch.

Configuring PoE

You use the `poectl` command utility to configure PoE on a [switch that supports](#) the feature. You can:

- Enable or disable PoE for a given switch port
- Set a switch port's PoE priority to one of three values: *low*, *high* or *critical*

By default, PoE is enabled on all Ethernet/1G switch ports, and these ports are set with a low priority. Switch ports can have low, high or critical priority.

To change the priority for one or more switch ports, run `poectl -p swp# [low|high|critical]`. For example:

```
cumulus@switch:~$ sudo poectl -p swp1-swp5,swp7 high
```

To disable PoE for one or more ports, run `poectl -d [port_numbers]`:

```
cumulus@switch:~$ sudo poectl -d swp1-swp5,swp7
```

To display PoE information for a set of switch ports, run `poectl -i [port_numbers]`:

Port	Status	Priority	PD type	PD class	Voltage	Current
Power						
swp1	searching	low	none	none	0.00 V	0 mA
swp2	searching	low	none	none	0.00 V	0 mA
swp3	searching	low	none	none	0.00 V	0 mA
swp4	disabled	low	none	none	0.00 V	0 mA
swp5	delivering power	low	802.3af	1	53.94 V	39 mA
swp7	searching	high	none	none	0.00 V	0 mA

Or to see all the PoE information for a switch, run `poectl -s`:

```
cumulus@switch:~$ poectl -s
System power:
  Total:      730.0 W
  Used:       11.0 W
  Available:  719.0 W
Connected ports:
  swp11, swp24, swp27, swp48
```

The set commands (priority, enable, disable) either succeed silently or display an error message if the command fails.

poectl Arguments

The `poectl` command takes the following arguments:

Argument	Description
<code>-h, --help</code>	Show this help message and exit
<code>-i, --port-info PORT_LIST</code>	Returns detailed information for the specified ports. For example: <code>-i swp1-swp5,swp10</code>
<code>-p, --priority PORT_LIST PRIORITY</code>	Sets priority for the specified ports: low, high, critical.
<code>-d, --disable-ports PORT_LIST</code>	Disables PoE operation on the specified ports.
<code>-e, --enable-ports PORT_LIST</code>	Enables PoE operation on the specified ports.
<code>-s, --system</code>	Returns PoE status for the entire switch.
<code>-r, --reset PORT_LIST</code>	Performs a hardware reset on the specified ports. Use this if one or more ports are stuck in an error state. This does not reset any configuration settings for the specified ports.
<code>-v, --version</code>	Displays version information.
<code>--save</code>	Saves the current configuration. The saved configuration is automatically loaded on system boot.

Argument	Description
--load	Loads and applies the saved configuration.

Logging poed Events

The poed service logs the following events to syslog:

- When a switch provides power to a powered device
- When a device that was receiving power is removed
- When the power available to the switch changes
- Errors

Man Pages

man poectl

Configuring a Global Proxy

Global HTTP and HTTPS proxies are configured in the `/etc/profile.d/` directory of Cumulus Linux.

1. In a terminal, create a new file in the `/etc/profile.d/` directory. In the code example below, the file is called `proxy`, and is created using the text editor `vi`.

```
cumulus@switch:~$ sudo vi /etc/profile.d/proxy
```

2. Add a line to the file to configure either an HTTP or an HTTPS proxy, and save the file:

- HTTP proxy:

```
http_proxy=http://myproxy.domain.com:8080
export http_proxy
```

- HTTPS proxy:

```
https_proxy=https://myproxy.domain.com:8080
export https_proxy
```

3. Run the `source` command, to execute the file in the current environment:

```
cumulus@switch:~$ source /etc/profile.d/proxy
```

The proxy is now configured. The echo command can be used to confirm a proxy is set up correctly:

- HTTP proxy:

```
cumulus@switch:~$ echo $http_proxy  
http://myproxy.domain.com:8080
```

- HTTPS proxy:

```
cumulus@switch:~$ echo $https_proxy  
https://myproxy.domain.com:8080
```

Configuring and Managing Network Interfaces

`ifupdown` is the network interface manager for Cumulus Linux. Cumulus Linux 2.1 and later uses an updated version of this tool, `ifupdown2`.

For more information on network interfaces, see [Layer 1 and Switch Port Attributes \(see page 134\)](#).



By default, `ifupdown` is quiet; use the verbose option `-v` when you want to know what is going on when bringing an interface down or up.

Contents

(Click to expand)

- [Contents \(see page 121\)](#)
- [Commands \(see page 121\)](#)
- [Man Pages \(see page 122\)](#)
- [Configuration Files \(see page 122\)](#)
- [Basic Commands \(see page 122\)](#)
- [Bringing All auto Interfaces Up or Down \(see page 123\)](#)
- [ifupdown Behavior with Child Interfaces \(see page 123\)](#)
- [ifupdown2 Interface Dependencies \(see page 125\)
 - \[ifup Handling of Upper \\(Parent\\) Interfaces \\(see page 127\\)\]\(#\)](#)
- [Configuring IP Addresses \(see page 128\)
 - \[Purging Existing IP Addresses on an Interface \\(see page 130\\)\]\(#\)](#)
- [Specifying User Commands \(see page 130\)](#)
- [Sourcing Interface File Snippets \(see page 130\)](#)
- [Using Globs for Port Lists \(see page 131\)](#)
- [Using Templates \(see page 131\)](#)
- [Adding Descriptions to Interfaces \(see page 132\)](#)
- [Caveats and Errata \(see page 133\)](#)
- [Useful Links \(see page 133\)](#)

Commands

- [ifdown](#)
- [ifquery](#)

- ifreload
- ifup
- mako-render

Man Pages

The following man pages have been updated for `ifupdown2`:

- man ifdown(8)
- man ifquery(8)
- man ifreload
- man ifup(8)
- man ifupdown-addons-interfaces(5)
- man interfaces(5)

Configuration Files

- /etc/network/interfaces

Basic Commands

To bring up an interface or apply changes to an existing interface, run:

```
cumulus@switch:~$ sudo ifup <ifname>
```

To bring down a single interface, run:

```
cumulus@switch:~$ sudo ifdown <ifname>
```

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

To administratively bring an interface up or down, run:

```
cumulus@switch:~$ sudo ip link set dev swp1 {up|down}
```

If you specified *manual* as the address family, you must bring up that interface manually using `ifconfig`. For example, if you configured a bridge like this:

```
auto bridge01
iface bridge01 inet manual
```

You can only bring it up by running `ifconfig bridge01 up`.



`ifdown` always deletes logical interfaces after bringing them down. Use the `--admin-state` option if you only want to administratively bring the interface up or down.

To see the link and administrative state, use the `ip link show` command:

```
cumulus@switch:~$ ip link show dev swp13: swp1: <BROADCAST,MULTICAST,
UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT qlen 500
link/ether 44:38:39:00:03:c1 brd ff:ff:ff:ff:ff:ff
```

In this example, `swp1` is administratively UP and the physical link is UP (`LOWER_UP` flag). More information on interface administrative state and physical state can be found in [this knowledge base article](#).

Bringing All auto Interfaces Up or Down

You can easily bring up or down all interfaces marked `auto` in `/etc/network/interfaces`. Use the `-a` option. For further details, see individual man pages for `ifup(8)`, `ifdown(8)`, `ifreload(8)`.

To administratively bring up all interfaces marked `auto`, run:

```
cumulus@switch:~$ sudo ifup -a
```

To administratively bring down all interfaces marked `auto`, run:

```
cumulus@switch:~$ sudo ifdown -a
```

To reload all network interfaces marked `auto`, use the `ifreload` command, which is equivalent to running `ifdown` then `ifup`, the one difference being that `ifreload` skips any configurations that didn't change):

```
cumulus@switch:~$ sudo ifreload -a
```

ifupdown Behavior with Child Interfaces

By default, ifupdown recognizes and uses any interface present on the system — whether a VLAN, bond or physical interface — that is listed as a dependent of an interface. You are not required to list them in the `interfaces` file unless they need a specific configuration, for MTU, link speed, and so forth (see page 134). And if you need to delete a child interface, you should delete all references to that interface from the `interfaces` file.

For this example, `swp1` and `swp2` below do not need an entry in the `interfaces` file. The following stanzas defined in `/etc/network/interfaces` provide the exact same configuration:

With Child Interfaces Defined	Without Child Interfaces Defined
<pre>auto swp1 iface swp1 auto swp2 iface swp2 auto bridge iface bridge bridge-vlan-aware yes bridge-ports swp1 swp2 bridge-vids 1-100 bridge-pvid 1 bridge-stp on</pre>	<pre>auto bridge iface bridge bridge-vlan-aware yes bridge-ports swp1 swp2 bridge-vids 1-100 bridge-pvid 1 bridge-stp on</pre>

Bridge in Traditional Mode - Example

For this example, `swp1.100` and `swp2.100` below do not need an entry in the `interfaces` file. The following stanzas defined in `/etc/network/interfaces` provide the exact same configuration:

With Child Interfaces Defined	Without Child Interfaces Defined
<pre>auto swp1.100 iface swp1.100 auto swp2.100 iface swp2.100 auto br-100 iface br-100 address 10.0.12.2/2 /24 address 2001:dad: beef::3/64 bridge-ports swp1.100 swp2.100 bridge-stp on</pre>	<pre>auto br-100 iface br-100 address 10.0.12.2/2 4 address 2001:dad: beef::3/64 bridge-ports swp1.1 00 swp2.100 bridge-stp on</pre>

For more information on the bridge in traditional mode vs the bridge in VLAN-aware mode, please read [this knowledge base article](#).

ifupdown2 Interface Dependencies

`ifupdown2` understands interface dependency relationships. When `ifup` and `ifdown` are run with all interfaces, they always run with all interfaces in dependency order. When run with the interface list on the command line, the default behavior is to not run with dependents. But if there are any built-in dependents, they will be brought up or down.

To run with dependents when you specify the interface list, use the `--with-dependents` option. `--with-dependents` walks through all dependents in the dependency tree rooted at the interface you specify. Consider the following example configuration:

```
auto bond1
iface bond1
    address 100.0.0.2/16
    bond-slaves swp29 swp30

auto bond2
iface bond2
    address 100.0.0.5/16
    bond-slaves swp31 swp32

auto br2001
iface br2001
    address 12.0.1.3/24
    bridge-ports bond1.2001 bond2.2001
    bridge-stp on
```

Using `ifup --with-dependents br2001` brings up all dependents of `br2001`: `bond1.2001`, `bond2.2001`, `bond1`, `bond2`, `bond1.2001`, `bond2.2001`, `swp29`, `swp30`, `swp31`, `swp32`.

```
cumulus@switch:~$ sudo ifup --with-dependents br2001
```

Similarly, specifying `ifdown --with-dependents br2001` brings down all dependents of `br2001`: `bond1.2001`, `bond2.2001`, `bond1`, `bond2`, `bond1.2001`, `bond2.2001`, `swp29`, `swp30`, `swp31`, `swp32`.

```
cumulus@switch:~$ sudo ifdown --with-dependents br2001
```



As mentioned earlier, `ifdown2` always deletes logical interfaces after bringing them down. Use the `--admin-state` option if you only want to administratively bring the interface up or down. In terms of the above example, `ifdown br2001` deletes `br2001`.

To guide you through which interfaces will be brought down and up, use the `--print-dependency` option to get the list of dependents.

Use `ifquery --print-dependency=list -a` to get the dependency list of all interfaces:

```
cumulus@switch:~$ sudo ifquery --print-dependency=list -a
lo : None
eth0 : None
bond0 : ['swp25', 'swp26']
bond1 : ['swp29', 'swp30']
bond2 : ['swp31', 'swp32']
br0 : ['bond1', 'bond2']
bond1.2000 : ['bond1']
bond2.2000 : ['bond2']
br2000 : ['bond1.2000', 'bond2.2000']
bond1.2001 : ['bond1']
bond2.2001 : ['bond2']
br2001 : ['bond1.2001', 'bond2.2001']
swp40 : None
swp25 : None
swp26 : None
swp29 : None
swp30 : None
swp31 : None
swp32 : None
```

To print the dependency list of a single interface, use:

```
cumulus@switch:~$ sudo ifquery --print-dependency=list br2001
br2001 : ['bond1.2001', 'bond2.2001']
bond1.2001 : ['bond1']
bond2.2001 : ['bond2']
bond1 : ['swp29', 'swp30']
bond2 : ['swp31', 'swp32']
swp29 : None
swp30 : None
swp31 : None
swp32 : None
```

To print the dependency information of an interface in dot format:

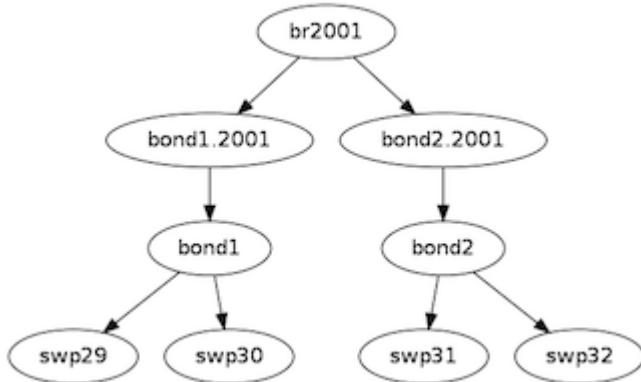
```
cumulus@switch:~$ sudo ifquery --print-dependency=dot br2001
/* Generated by GvGen v.0.9 (http://software.inl.fr/trac/wiki/GvGen)
*/
digraph G {
    compound=true;
    node1 [label="br2001"];
    node2 [label="bond1.2001"];
```

```

node3 [label="bond2.2001"];
node4 [label="bond1"];
node5 [label="bond2"];
node6 [label="swp29"];
node7 [label="swp30"];
node8 [label="swp31"];
node9 [label="swp32"];
node1->node2;
node1->node3;
node2->node4;
node3->node5;
node4->node6;
node4->node7;
node5->node8;
node5->node9;
}

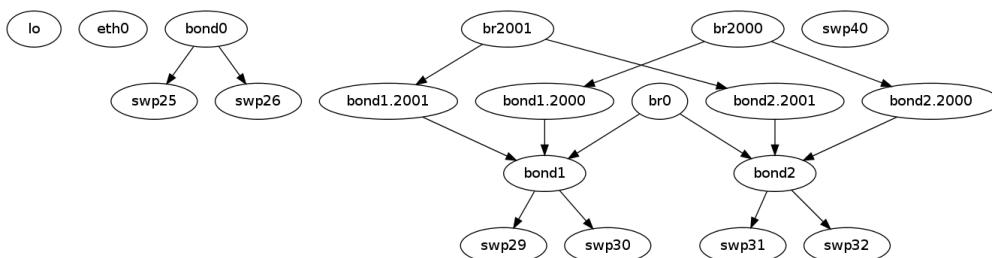
```

You can use dot to render the graph on an external system where dot is installed.



To print the dependency information of the entire `interfaces` file:

```
cumulus@switch:~$ sudo ifquery --print-dependency=dot -a >interfaces_all.dot
```



ifup Handling of Upper (Parent) Interfaces

When you run `ifup` on a logical interface (like a bridge, bond or VLAN interface), if the `ifup` resulted in the creation of the logical interface, by default it implicitly tries to execute on the interface's upper (or parent) interfaces as well. This helps in most cases, especially when a bond is brought down and up, as in the example below. This section describes the behavior of bringing up the upper interfaces.

Consider this example configuration:

```
auto br100
iface br100
    bridge-ports bond1.100 bond2.100

auto bond1
iface bond1
    bond-slaves swp1 swp2
```

If you run `ifdown bond1`, `ifdown` deletes bond1 and the VLAN interface on bond1 (bond1.100); it also removes bond1 from the bridge br100. Next, when you run `ifup bond1`, it creates bond1 and the VLAN interface on bond1 (bond1.100); it also executes `ifup br100` to add the bond VLAN interface (bond1.100) to the bridge br100.

As you can see above, implicitly bringing up the upper interface helps, but there can be cases where an upper interface (like br100) is not in the right state, which can result in warnings. The warnings are mostly harmless.

If you want to disable these warnings, you can disable the implicit upper interface handling by setting `skip_upperinterfaces=1` in `/etc/network/ifupdown2/ifupdown2.conf`.

With `skip_upperinterfaces=1`, you will have to explicitly execute `ifup` on the upper interfaces. In this case, you will have to run `ifup br100` after an `ifup bond1` to add bond1 back to bridge br100.



Although specifying a subinterface like `swp1.100` and then running `ifup swp1.100` will also result in the automatic creation of the `swp1` interface in the kernel, Cumulus Networks recommends you specify the parent interface `swp1` as well. A parent interface is one where any physical layer configuration can reside, such as `link-speed 1000` or `link-duplex full`.

It's important to note that if you only create `swp1.100` and not `swp1`, then you cannot run `ifup swp1` since you did not specify it.

Configuring IP Addresses

In `/etc/network/interfaces`, list all IP addresses as shown below under the `iface` section (see `man interfaces` for more information):

```
auto swp1
iface swp1
    address 12.0.0.1/30
    address 12.0.0.2/30
```

The address method and address family are not mandatory. They default to `inet/inet6` and `static`, but `inet/inet6` **must** be specified if you need to specify `dhcp` or `loopback`:

```
auto lo
```

```
iface lo inet loopback
```

You can specify both IPv4 and IPv6 addresses in the same `iface` stanza:

```
auto swp1
iface swp1
    address 192.0.2.1/30
    address 192.0.2.2/30
    address 2001:DB8::1/126
```

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

To make non-persistent changes to interfaces at runtime, use `ip addr add`:

```
cumulus@switch:~$ sudo ip addr add 192.0.2.1/30 dev swp1
cumulus@switch:~$ sudo ip addr add 2001:DB8::1/126 dev swp1
```

To remove an addresses from an interface, use `ip addr del`:

```
cumulus@switch:~$ sudo ip addr del 192.0.2.1/30 dev swp1
cumulus@switch:~$ sudo ip addr del 2001:DB8::1/126 dev swp1
```

See `man ip` for more details on the options available to manage and query interfaces.

To show the assigned address on an interface, use `ip addr show`:

```
cumulus@switch:~$ ip addr show dev swp1
3: swp1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 500
    link/ether 44:38:39:00:03:c1 brd ff:ff:ff:ff:ff:ff
    inet 192.0.2.1/30 scope global swp1
        inet 192.0.2.2/30 scope global swp1
        inet6 2001:DB8::1/126 scope global tentative
            valid_lft forever preferred_lft forever
```

Purging Existing IP Addresses on an Interface

By default, `ifupdown2` purges existing IP addresses on an interface. If you have other processes that manage IP addresses for an interface, you can disable this feature including the `address-purge` setting in the interface's configuration. For example, add the following to the interface configuration in `/etc/network/interfaces`:

```
auto swp1
iface swp1
    address-purge no
```



Purging existing addresses on interfaces with multiple `iface` stanzas is not supported. Doing so can result in the configuration of multiple addresses for an interface after you change an interface address and reload the configuration with `ifreload -a`. If this happens, you must shut down and restart the interface with `ifup` and `ifdown`, or manually delete superfluous addresses with `ip address delete specify.ip.address.here/mask dev DEVICE`. See also the [Caveats and Errata \(see page 133\)](#) section below for some cautions about using multiple `iface` stanzas for the same interface.

Specifying User Commands

You can specify additional user commands in the `interfaces` file. As shown in the example below, the interface stanzas in `/etc/network/interfaces` can have a command that runs at pre-up, up, post-up, pre-down, down, and post-down:

```
auto swp1
iface swp1
    address 12.0.0.1/30
    up /sbin/foo bar
```

Any valid command can be hooked in the sequencing of bringing an interface up or down, although commands should be limited in scope to network-related commands associated with the particular interface.

For example, it wouldn't make sense to install some Debian package on `ifup` of `swp1`, even though that is technically possible. See `man interfaces` for more details.

Sourcing Interface File Snippets

Sourcing interface files helps organize and manage the `interfaces(5)` file. For example:

```
cumulus@switch:~$ cat /etc/network/interfaces
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

source /etc/network/interfaces.d/bond0
```

The contents of the sourced file used above are:

```
cumulus@switch:~$ cat /etc/network/interfaces.d/bond0
auto bond0
iface bond0
    address 14.0.0.9/30
    address 2001:ded:beef:2::1/64
    bond-slaves swp25 swp26
```

Using Globs for Port Lists

Some modules support globs to define port lists (that is, a range of ports). You can use the `glob` keyword to specify bridge ports and bond slaves:

```
auto br0
iface br0
    bridge-ports glob swp1-6.100

auto br1
iface br1
    bridge-ports glob swp7-9.100  swp11.100 glob swp15-18.100
```

Using Templates

`ifupdown2` supports Mako-style templates. The Mako template engine is run over the `interfaces` file before parsing.

Use the template to declare cookie-cutter bridges in the `interfaces` file:

```
%for v in [11,12]:
auto vlan${v}
iface vlan${v}
    address 10.20.${v}.3/24
```

```
bridge-ports glob swp19-20.${v}
bridge-stp on
%endfor
```

And use it to declare addresses in the `interfaces` file:

```
%for i in [1,12]:
auto swp${i}
iface swp${i}
    address 10.20.${i}.3/24
```



Regarding Mako syntax, use square brackets ([1,12]) to specify a list of individual numbers (in this case, 1 and 12). Use `range(1,12)` to specify a range of interfaces.



You can test your template and confirm it evaluates correctly by running `mako-render /etc/network/interfaces`.



For more examples of configuring Mako templates, read this [knowledge base article](#).

Adding Descriptions to Interfaces

You can add descriptions to the interfaces configured in `/etc/network/interfaces` by using the `alias` keyword. For example:

```
auto swp1
iface swp1
    alias swp1 hypervisor_port_1
```

You can query interface descriptions by running `ip link show`. The alias appears on the `alias` line:

```
cumulus@switch$ ip link show swp1
3: swp1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast
state DOWN mode DEFAULT qlen 500
    link/ether aa:aa:aa:aa:aa:bc brd ff:ff:ff:ff:ff:ff
    alias hypervisor_port_1
```

Interface descriptions also appear in the SNMP OID (see page 441) IF-MIB::ifAlias.



Aliases are limited to 256 characters.

Caveats and Errata

While `ifupdown2` supports the inclusion of multiple `iface` stanzas for the same interface, Cumulus Networks recommends you use a single `iface` stanza for each interface, if possible.

There are cases where you must specify more than one `iface` stanza for the same interface. For example, the configuration for a single interface can come from many places, like a template or a sourced file.

If you do specify multiple `iface` stanzas for the same interface, make sure the stanzas do not specify the same interface attributes. Otherwise, unexpected behavior can result.

For example, `swp1` is configured in two places:

```
cumulus@switch:~$ cat /etc/network/interfaces  
  
source /etc/interfaces.d/speed_settings  
  
auto swp1  
iface swp1  
    address 10.0.14.2/24
```

As well as `/etc/interfaces.d/speed_settings`

```
cumulus@switch:~$ cat /etc/interfaces.d/speed_settings  
  
auto swp1  
iface swp1  
    link-speed 1000  
    link-duplex full
```

`ifupdown2` correctly parses a configuration like this because the same attributes are not specified in multiple `iface` stanzas.

And, as stated in the note above, you cannot purge existing addresses on interfaces with multiple `iface` stanzas.

Useful Links

- <http://wiki.debian.org/NetworkConfiguration>
- <http://www.linuxfoundation.org/collaborate/workgroups/networking/bonding>
- <http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge>

- <http://www.linuxfoundation.org/collaborate/workgroups/networking/vlan>

Layer 1 and Switch Port Attributes

This chapter discusses the various network interfaces on a switch running Cumulus Linux.

Contents

(Click to expand)

- Contents (see page 134)
- Commands (see page 134)
- Man Pages (see page 134)
- Configuration Files (see page 135)
- Interface Types (see page 135)
- Settings (see page 135)
 - Port Speed and Duplexing (see page 135)
 - Auto-negotiation (see page 137)
 - MTU (see page 137)
- Configuring Breakout Ports (see page 139)
 - Breaking out a 40G port into 4x10G Ports (see page 139)
 - Combining Four 10G Ports into One 40G Port (see page 140)
- Logical Switch Port Limitations (see page 141)
- Verification and Troubleshooting Commands (see page 142)
 - Statistics (see page 142)
 - Querying SFP Port Information (see page 143)
- Useful Links (see page 143)

Commands

- ethtool
- ip

Man Pages

- man ethtool
- man interfaces
- man ip
- man ip addr
- man ip link

Configuration Files

- /etc/network/interfaces

Interface Types

Cumulus Linux exposes network interfaces for several types of physical and logical devices:

- lo, network loopback device
- ethN, switch management port(s), for out of band management only
- swpN, switch front panel ports
- (optional) brN, bridges (IEEE 802.1Q VLANs)
- (optional) bondN, bonds (IEEE 802.3ad link aggregation trunks, or port channels)

Settings

You can set the MTU, speed, duplex and auto-negotiation settings under a physical or logical interface stanza:

```
auto swp1
iface swp1
    address 10.1.1.1/24
    mtu 9000
    link-speed 10000
    link-duplex full
    link-autoneg off
```

To load the updated configuration, run the `ifreload -a` command:

```
cumulus@switch:~$ sudo ifreload -a
```

Port Speed and Duplexing

Cumulus Linux supports both half- and **full-duplex** configurations. Supported port speeds include 1G, 10G and 40G. Set the speeds in terms of Mbps, where the setting for 1G is 1000, 10G is 10000 and 40G is 40000.

You can create a persistent configuration for port speeds in `/etc/network/interfaces`. Add the appropriate lines for each switch port stanza. For example:

```
auto swp1
iface swp1
    address 10.1.1.1/24
    link-speed 10000
    link-duplex full
```



If you specify the port speed in `/etc/network/interfaces`, you must also specify the duplex mode setting along with it; otherwise, `ethtool` defaults to half duplex.

You can also configure these settings at run time, using `ethtool`.

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

You can use `ethtool` to configure duplexing and the speed for your switch ports. You must specify both port speed and duplexing in the `ethtool` command; auto-negotiation is optional. The following examples use `swp1`.

- To set the port speed to 1G, run:

```
ethtool -s swp1 speed 1000 duplex full
```

- To set the port speed to 10G, run:

```
ethtool -s swp1 speed 10000 duplex full
```

- To enable duplexing, run:

```
ethtool -s swp1 speed 10000 duplex full|half
```

Port Speed Limitations

Ports can be configured to one speed less than their maximum speed.

Switch port Type	Lowest Configurable Speed
1G	100 Mb
10G	1 Gigabit (1000 Mb)
40G	10G*

*Requires the port to be converted into a breakout port.

Auto-negotiation

You can enable or disable **auto-negotiation** (that is, set it *on* or *off*) on a switch port.



Cumulus Linux does not support auto-negotiation for 10G or 40G interfaces.

```
auto swp1
iface swp1
    link-autoneg off
```

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

You can use `ethtool` to configure auto-negotiation for your switch ports. The following example use `swp1`:

- To enable or disable auto-negotiation, run:

```
ethtool -s swp1 speed 10000 duplex full autoneg on|off
```

MTU

Interface MTU applies to the management port, front panel port, bridge, VLAN subinterfaces and bonds.

```
auto swp1
iface swp1
    mtu 9000
```

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

To set `swp1` to Jumbo Frame MTU=9000, use `ip link set`:

```
cumulus@switch:~$ sudo ip link set dev swp1 mtu 9000
```

```
cumulus@switch:~$ ip link show dev swp1
3: swp1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9000 qdisc pfifo_fast
    state UP mode DEFAULT qlen 500
        link/ether 44:38:39:00:03:c1 brd ff:ff:ff:ff:ff:ff
```



You must take care to ensure there are no MTU mismatches in the conversation path. MTU mismatches will result in dropped or truncated packets, degrading or blocking network performance.

When you are configuring MTU for a bridge, don't set MTU on the bridge itself; set it on the individual members of the bridge. The MTU setting is the lowest MTU setting of any interface that is a member of that bridge (that is, every interface specified in `bridge-ports` in the bridge configuration in the `interfaces` file), even if another bridge member has a higher MTU value. Consider this bridge configuration:

```
auto br0
iface br0
    bridge-ports bond1 bond2 bond3 bond4 peer5
    bridge-vlan-aware yes
    bridge-vids 100-110
    bridge-stp on
```

In order for br0 to have an MTU of 9000, set the MTU for each of the member interfaces (bond1 to bond 4, and peer5), to 9000 at minimum.

```
auto peer5
iface peer5
    bond-slaves swp3 swp4
    mtu 9000
```

When configuring MTU for a bond, configure the MTU value directly under the bond interface; the configured value is inherited by member links.

To show MTU, use `ip link show`:

```
cumulus@switch:~$ ip link show dev swp1
3: swp1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    state UP mode DEFAULT qlen 500
        link/ether 44:38:39:00:03:c1 brd ff:ff:ff:ff:ff:ff
```

Configuring MTU for a VXLAN Virtual Network Interface

If you are working with [VXLANS](#), the MTU for a virtual network interface (VNI) must be 50 bytes smaller than the MTU of the physical interfaces on the switch, as those 50 bytes are required for various headers and other data. You should also consider setting the MTU much higher than the default 1500.

Two common MTUs for physical interfaces are 9216 and 9000 bytes. The corresponding MTUs for the VNIs would be 9166 and 8950.

Configuring Breakout Ports

Cumulus Linux has the ability to:

- Break out 40G switch ports into four separate 10G ports for use with a breakout cable.
- Combine (also called *aggregating* or *ganging*) four 10G switch ports into one 40G port for use with a breakout cable ([not to be confused with a bond](#) (see page 184)).

A typical DAC (directly-attached copper) 40G 1xQSFP to 4xSFP+ looks like this:



You configure breakout ports with the `/etc/cumulus/ports.conf` file. After you modify the configuration, restart `switchd` to push the new configuration (run `sudo service switchd restart`; this interrupts network services (see page 115)).

Breaking out a 40G port into 4x10G Ports



`/etc/cumulus/ports.conf` varies across different hardware platforms. Check the current list of supported platforms on [the hardware compatibility list](#).

A snippet from the `/etc/cumulus/ports.conf` looks like this:

```
# QSFP+ ports
```

```
#  
# <port label 49-52> = [4x10G|40G]  
49=40G  
50=40G  
51=40G  
52=40G
```

To change a 40G port to 4x10G ports, edit the `/etc/cumulus/ports.conf` file with a text editor (nano, vi, zile). Change `40G` to `4x10G`.

In the following example, switch port 49 is changed to a breakout port:

```
# QSFP+ ports  
#  
# <port label 49-52> = [4x10G|40G]  
49=4x10G  
50=40G  
51=40G  
52=40G
```

To load the change restart `switchd`:

```
cumulus@switch:~$ sudo service switchd restart
```

Many services depend on `switchd`. It is highly recommended to restart Cumulus Linux if possible in this situation.

Combining Four 10G Ports into One 40G Port

To gang (aggregate) four 10G ports into one 40G port for use with a breakout cable, you must edit `/etc/cumulus/ports.conf`.



`/etc/cumulus/ports.conf` varies across different hardware platforms. Check the current list of supported platforms on the [hardware compatibility list](#).

A snippet from the `/etc/cumulus/ports.conf` looks like this:

```
# SFP+ ports#  
# <port label 1-48> = [10G|40G/4]  
1=10G  
2=10G  
3=10G  
4=10G  
5=10G
```

To change four 10G ports into one 40G port, edit the `/etc/cumulus/ports.conf` file with a text editor (nano, vi, zile). Change `10G` to `40G/4` for every port being ganged.

In the following example, switch ports `swp1-4` are changed to a ganged port:

```
# SFP+ ports#
# <port label 1-48> = [10G|40G/4]
1=40G/4
2=40G/4
3=40G/4
4=40G/4
5=10G
```

To load the change, restart `switchd`.

```
cumulus@switch:~$ sudo service switchd restart
```

Many services depend on `switchd`. It is highly recommended to restart Cumulus Linux if possible in this situation.



- You must gang four 10G ports in sequential order. For example, you cannot gang `swp1`, `swp10`, `swp20` and `swp40` together.
- The ports must be in increments of four, with the starting port being `swp1` (or `swp5`, `swp9`, or so forth); so you cannot gang `swp2`, `swp3`, `swp4` and `swp5` together.

Logical Switch Port Limitations

40G switches with Trident II chipsets (check the *40G Portfolio* section of the [HCL](#)) can support a certain number of logical ports, depending upon the manufacturer.

Before you configure any logical/unganged ports on a switch, check the limitations listed in `/etc/cumulus/ports.conf`; this file is specific to each manufacturer.

For example, the Dell S6000 `ports.conf` file indicates the logical port limitation like this:

```
# ports.conf --
#
# This file controls port aggregation and subdivision.  For example,
QSFP+
# ports are typically configurable as either one 40G interface or four
# 10G/1000/100 interfaces.  This file sets the number of interfaces
per port
# while /etc/network/interfaces and ethtool configure the link speed f
or each
# interface.
#
# You must restart switchd for changes to take effect.
```

```

#
# The DELL S6000 has:
#   32 QSFP ports numbered 1-32
#   These ports are configurable as 40G, split into 4x10G ports or
#   disabled.
#
#   The X pipeline covers QSFP ports 1 through 16 and the Y pipeline
#   covers QSFP ports 17 through 32.
#
#   The Trident2 chip can only handle 52 logical ports per pipeline.
#
#   This means 13 is the maximum number of 40G ports you can ungang
#   per pipeline, with the remaining three 40G ports set to
#   "disabled". The 13 40G ports become 52 unganged 10G ports, which
#   totals 52 logical ports for that pipeline.
#

```

The means the maximum number of ports for this Dell S6000 is 104.

Verification and Troubleshooting Commands

Statistics

High-level interface statistics are available with the `ip -s link` command:

```

cumulus@switch:~$ ip -s link show dev swp1
3: swp1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP mode DEFAULT qlen 500
    link/ether 44:38:39:00:03:c1 brd ff:ff:ff:ff:ff:ff
    RX: bytes    packets    errors    dropped overrun mcast
      21780        242        0        0        0       242
    TX: bytes    packets    errors    dropped carrier collsns
      1145554     11325        0        0        0         0

```

Low-level interface statistics are available with `ethtool`:

```

cumulus@switch:~$ sudo ethtool -S swp1
NIC statistics:
    HwIfInOctets: 21870
    HwIfInUcastPkts: 0
    HwIfInBcastPkts: 0
    HwIfInMcastPkts: 243
    HwIfOutOctets: 1148217
    HwIfOutUcastPkts: 0
    HwIfOutMcastPkts: 11353
    HwIfOutBcastPkts: 0
    HwIfInDiscards: 0
    HwIfInL3Drops: 0

```

```

HwIfInBufferDrops: 0
HwIfInAclDrops: 0
HwIfInBlackholeDrops: 0
HwIfInDot3LengthErrors: 0
HwIfInErrors: 0
SoftInErrors: 0
SoftInDrops: 0
SoftInFrameErrors: 0
HwIfOutDiscards: 0
HwIfOutErrors: 0
HwIfOutQDrops: 0
HwIfOutNonQDrops: 0
SoftOutErrors: 0
SoftOutDrops: 0
SoftOutTxFifoFull: 0
HwIfOutQLen: 0

```

Querying SFP Port Information

You can verify SFP settings using `ethtool -m`. The following example shows the output for 1G and 10G modules:

```

cumulus@switch:~# sudo ethtool -m | egrep '(swp|RXPower :|TXPower :|EthernetComplianceCode)'

swp1: SFP detected
    EthernetComplianceCodes : 1000BASE-LX
    RXPower : -10.4479dBm
    TXPower : 18.0409dBm
swp3: SFP detected
    10GEthernetComplianceCode : 10G Base-LR
    RXPower : -3.2532dBm
    TXPower : -2.0817dBm

```

Useful Links

- <http://wiki.debian.org/NetworkConfiguration>
- <http://www.linuxfoundation.org/collaborate/workgroups/networking/vlan>
- <http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge>
- <http://www.linuxfoundation.org/collaborate/workgroups/networking/bonding>

Buffer and Queue Management

Hardware datapath configuration manages packet buffering, queueing, and scheduling in hardware. There are two configuration input files:

- `/etc/cumulus/datapath/traffic.conf`, which describes priority groups and assigns the scheduling algorithm and weights
- `/etc/bcm.d/datapath.conf`, which assigns buffer space and egress queues



Versions of these files prior to Cumulus Linux 2.1 are incompatible with Cumulus Linux 2.1 and later; using older files will cause `switchd` to fail to start and return an error that it cannot find the `/var/lib/cumulus/rc.datapath` file.

Each packet is assigned to an ASIC Class of Service (CoS) value based on the packet's priority value stored in the 802.1p (Class of Service) or DSCP (Differentiated Services Code Point) header field. The packet is assigned to a priority group based on the CoS value.

Priority groups include:

- *Control*: Highest priority traffic
- *Service*: Second-highest priority traffic
- *Lossless*: Traffic protected by priority flow control
- *Bulk*: All remaining traffic

A lossless traffic group is protected from packet drops by configuring the datapath to use priority pause. A lossless priority group requires a port group configuration, which specifies the ports configured for priority flow control and the additional buffer space assigned to each port for packets in the lossless priority group.

The scheduler is configured to use a hybrid scheduling algorithm. It applies strict priority to control traffic queues and a weighted round robin selection from the remaining queues. Unicast packets and multicast packets with the same priority value are assigned to separate queues, which are assigned equal scheduling weights.

Datapath configuration takes effect when you initialize `switchd`. Changes to the `traffic.conf` file require you to [restart `switchd` \(see page 115\)](#).

Contents

(Click to expand)

- [Contents \(see page 144\)](#)
- [Commands \(see page 144\)](#)
- [Configuration Files \(see page 145\)](#)
- [Configuring Traffic Marking through ACL Rules \(see page 147\)](#)
- [Configuring Link Pause \(see page 148\)](#)
- [Useful Links \(see page 149\)](#)
- [Caveats and Errata \(see page 149\)](#)

Commands

If you modify the configuration in the `/etc/cumulus/datapath/traffic.conf` file, you must [restart `switchd` \(see page 115\)](#) for the changes to take effect:

```
cumulus@switch:~$ sudo service switchd restart
```

Configuration Files

The following configuration applies to 10G and 40G switches only ([any switch](#) on the Trident, Trident+, or Trident II platform).

- `/etc/cumulus/datapath/traffic.conf`: The datapath configuration file.

Sample traffic.conf file (Click to expand)

```
cumulus@switch:~$ cat /etc/cumulus/datapath/traffic.conf
#
# /etc/cumulus/datapath/traffic.conf
#
# packet header field used to determine the packet priority
level
# fields include {802.1p,
dscp}
traffic.packet_priority_source = 802.
1p
# remark packet priority
value
# fields include {802.1p,
none}
traffic.remark_packet_priority = none
# packet priority values assigned to each internal cos
value
# internal cos values {cos_0..
cos_7}
# (internal cos 3 has been reserved for CPU-generated
traffic)
# 802.1p values = {0..7}, dscp values = {0..63}
traffic.cos_0.packet_priorities = [0]
traffic.cos_1.packet_priorities = [1]
traffic.cos_2.packet_priorities = [2]
traffic.cos_3.packet_priorities = []
traffic.cos_4.packet_priorities = [3,4]
traffic.cos_5.packet_priorities = [5]
traffic.cos_6.packet_priorities = [6]
traffic.cos_7.packet_priorities = [7]
# priority groups
traffic.priority_group_list = [control, service, bulk]
# internal cos values assigned to each priority group
# each cos value should be assigned exactly once
# internal cos values {0..7}
priority_group.control.cos_list = [7]
priority_group.service.cos_list = [2]
priority_group.bulk.cos_list = [0,1,3,4,5,6]
# to configure a lossless priority group:
# -- uncomment the cos list config and and assign cos value(s)
```

```
# -- uncomment port_group_0 configurations and set the lossless flag,
buffer si
ze,
ports
# -- (currently only one traffic group is allowed, with port range 'al
lports')
# priority_group.lossless.cos_list = []
# lossless port group
# -- lossless flag
arranging in: tiled
arranging in: tiled
# -- buffer size in bytes for each port
# -- port group
# priority_group.lossless.lossless_flag = true
# priority_group.lossless.port_group_0.port_buffer_bytes = 4096
# priority_group.lossless.port_group_0.port_range = allports
# to configure pause on a group of ports:
# uncomment the link pause port group list
# add or replace a port group name to the list
# populate the port set, e.g.
#     swp1-swp4,swp8,swp50s0-swp50s3
# enable pause frame transmit and/or pause frame receive
# link pause
# link_pause.port_group_list = [port_group_0]
# link_pause.port_group_0.port_set = swp1-swp4,swp6
# link_pause.port_group_0.rx_enable = true
# link_pause.port_group_0.tx_enable = true
# scheduling algorithm: algorithm values = {dwrr}
scheduling.algorithm = dwrr
# traffic group scheduling weight
# weight values = {0..127}
# '0' indicates strict priority
priority_group.control.weight = 0
priority_group.service.weight = 32
priority_group.bulk.weight = 16
priority_group.lossless.weight = 16
# To turn on/off Denial of service (DOS) prevention checks
dos_enable = false
# To enable cut-through forwarding
cut_through_enable = true
# Enable resilient hashing
#resilient_hash_enable = FALSE
# Resilient hashing flowset entries per ECMP group
# Valid values - 64, 128, 256, 512, 1024
#resilient_hash_entries_ecmp = 128
# Enable symmetric hashing
#symmetric_hash_enable = TRUE
# Set sflow/sample ingress cpu packet rate and burst in packets/sec
# Values: {0..16384}
#sflow.rate = 16384
#sflow.burst = 16384
#Specify the maximum number of paths per route entry.
```

```
# Maximum paths supported is 200.
# Default value 0 takes the number of physical ports as the max path
size.
#ecmp_max_paths = 0
```

Configuring Traffic Marking through ACL Rules

You can mark traffic for egress packets through `iptables` or `ip6tables` rule classifications. To enable these rules, you do one of the following:

- Mark DSCP values in egress packets.
- Mark 802.1p CoS values in egress packets.

To enable traffic marking, use `cl-acltool`. Add the `-p` option to specify the location of the policy file. By default, if you don't include the `-p` option, `cl-acltool` looks for the policy file in `/etc/cumulus/acl/policy.d/`.

The `iptables`-`ip6tables`-based marking is supported via the following action extension:

```
-j SETQOS --set-dscp 10 --set-cos 5
```

You can specify one of the following targets for `SETQOS`:

Option	Description
<code>-set-cos INT</code>	Sets the datapath resource/queuing class value. Values are defined in IEEE_P802.1p .
<code>-set-dscp value</code>	Sets the DSCP field in packet header to a value, which can be either a decimal or hex value.
<code>-set-dscp-class class</code>	Sets the DSCP field in the packet header to the value represented by the DiffServ class value. This class can be EF, BE or any of the CSxx or AFxx classes.



You can specify either `--set-dscp` or `--set-dscp-class`, but not both.

Here are two example rules:

```
[iptables]
-t mangle -A FORWARD --in-interface swp+ -p tcp --dport bgp -j SETQOS --set-
dscp 10 --set-cos 5

[ip6tables]
-t mangle -A FORWARD --in-interface swp+ -j SETQOS --set-dscp 10
```

You can put the rule in either the *mangle* table or the default *filter* table; the mangle table and filter table are put into separate TCAM slices in the hardware.

To put the rule in the mangle table, include `-t mangle`; to put the rule in the filter table, omit `-t mangle`.

Configuring Link Pause

The PAUSE frame is a flow control mechanism that halts the transmission of the transmitter for a specified period of time. A server or other network node within the data center may be receiving traffic faster than it can handle it, thus the PAUSE frame. In Cumulus Linux, individual ports can be configured to execute link pause by:

- Transmitting pause frames when its ingress buffers become congested (TX pause enable) and/or
- Responding to received pause frames (RX pause enable).

Just like configuring buffer and queue management link pause is configured by editing `/etc/cumulus/datapath/traffic.conf`.

Here is an example configuration which turns of both types of link pause for `swp2` and `swp3`:

```
# to configure pause on a group of ports:  
# uncomment the link pause port group list  
# add or replace a port group name to the list  
# populate the port set, e.g.  
# swp1-swp4,swp8,swp50s0-swp50s3  
# enable pause frame transmit and/or pause frame receive  
# link pause  
link_pause.port_group_list = [port_group_0]  
link_pause.port_group_0.port_set = swp2-swp3  
link_pause.port_group_0.rx_enable = true  
link_pause.port_group_0.tx_enable = true
```

A *port group* refers to one or more sequences of contiguous ports. Multiple port groups can be defined by:

- Adding a comma-separated list of port group names to the `port_group_list`.
- Adding the `port_set`, `rx_enable`, and `tx_enable` configuration lines for each port group.

You can specify the set of ports in a port group in comma-separated sequences of contiguous ports; you can see which ports are contiguous in `/var/lib/cumulus/porttab`. The syntax supports:

- A single port (`swp1s0` or `swp5`)
- A sequence of regular `swp` ports (`swp2-swp5`)
- A sequence within a breakout `swp` port (`swp6s0-swp6s3`)
- A sequence of regular and breakout ports, provided they are all in a contiguous range. For example:

```
...  
swp2  
swp3  
swp4
```

```
swp5  
swp6s0  
swp6s1  
swp6s2  
swp6s3  
swp7  
...
```

Restart `switchd` (see page 115) to allow link pause configuration changes to take effect:

```
cumulus@switch:~$ sudo service switchd restart
```

Useful Links

- [iptables-extensions man page](#)

Caveats and Errata

- You can configure Quality of Service (QoS) for 10G and 40G switches only; that is, any switch on the Trident, Trident+, or Trident II platform.

Layer 1 and Layer 2 Features

Spanning Tree and Rapid Spanning Tree

Spanning tree protocol (STP) is always recommended in layer 2 topologies, as it prevents bridge loops and broadcast radiation on a bridged network.

`mstpd` is a daemon that implements IEEE802.1D 2004 and IEEE802.1Q 2011. Currently, STP is disabled by default on the bridge in Cumulus Linux.

To enable STP, configure `brctl stp <bridge> on`.



The STP modes Cumulus Linux supports vary depending upon which [bridge driver mode](#) (see page 187) is in use. For a bridge configured in *traditional* mode, STP, RSTP, PVST and PVRST are supported; with the default set to PVRST. [VLAN-aware](#) (see page 208) bridges only operate in RSTP mode.

If a bridge running RSTP (802.1w) receives a common STP (802.1D) BPDU, it will automatically fall back to 802.1D operation.

You can configure `mstpd` to be in common STP mode only, by setting `setforcevers` to *STP*.

Contents

(Click to expand)

- [Contents \(see page 150\)](#)
- [Commands \(see page 150\)](#)
- [PVST/PVRST \(see page 151\)](#)
- [Creating a Bridge and Configuring STP \(see page 151\)](#)
- [Configuring Spanning Tree Parameters \(see page 153\)](#)
 - [Understanding the Spanning Tree Parameters \(see page 153\)](#)
- [Bridge Assurance \(see page 161\)](#)
- [BPDU Guard \(see page 162\)](#)
 - [Configuring BPDU Guard \(see page 162\)](#)
 - [Recovering a Port Disabled by BPDU Guard \(see page 163\)](#)
- [BPDU Filter \(see page 164\)](#)
- [Configuration Files \(see page 165\)](#)
- [Man Pages \(see page 165\)](#)
- [Useful Links \(see page 165\)](#)
- [Caveats and Errata \(see page 165\)](#)

Commands

- `brctl`

- `mstptcl`

`mstptcl` is a utility to configure STP. `mstp` is started by default on bootup. `mstp` logs and errors are located in `/var/log/syslog`.

PVST/PVRST

Per VLAN Spanning Tree (PVST) creates a spanning tree instance for a bridge. Rapid PVST (PVRST) supports RSTP enhancements for each spanning tree instance. You must create a bridge corresponding to the untagged native/access VLAN, and all the physical switch ports must be part of the same VLAN. When connected to a switch that has a native VLAN configuration, the native VLAN **must** be configured to be VLAN 1 only.

Cumulus Linux supports the RSTP/PVRST/PVST modes of STP natively when the bridge is configured in **traditional mode** (see page 187).

Creating a Bridge and Configuring STP

To create a bridge, configure the bridge stanza under `/etc/network/interfaces`. More information on configuring [bridges can be found here](#). (see page 187) To enable STP on the bridge, include the keyword `bridge-stp on`.

```
auto br2
iface br2
    bridge-ports swp1.101 swp4.101 swp5.101
    bridge-stp on
```

To enable the bridge, run `ifreload -a`:

```
cumulus@switch:~$ sudo ifreload -a
```

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

You use `brctl` to create the bridge, add bridge ports in the bridge and configure STP on the bridge. `mstptcl` is used only when an admin needs to change the default configuration parameters for STP:

```
cumulus@switch:~$ sudo brctl addbr br2
cumulus@switch:~$ sudo brctl addif br2 swp1.101 swp4.101 swp5.101
cumulus@switch:~$ sudo brctl stp br2 on
cumulus@switch:~$ sudo ifconfig br2 up
```

To get the bridge state, use:

```
cumulus@switch:~$ sudo brctl show
bridge name      bridge id          STP enabled    interfaces
br2              8000.001401010100  yes           swp1.101
                                         swp4.101
                                         swp5.101
```

To get the mstpd bridge state, use:

```
cumulus@switch:~$ sudo mstpcctl showbridge br2
br2 CIST info
enabled        yes
bridge id      F.000.00:14:01:01:01:00
designated root F.000.00:14:01:01:01:00
regional root  F.000.00:14:01:01:01:00
root port      none
path cost      0          internal path cost  0
max age        20         bridge max age     20
forward delay  15         bridge forward delay 15
tx hold count 6          max hops            20
hello time    2          ageing time       200
force protocol version   rstp
time since topology change 90843s
topology change count    4
topology change          no
topology change port     swp4.101
last topology change port swp5.101
```

To get the mstpd bridge port state, use:

```
cumulus@switch:~$ sudo mstpcctl showport br2
E swp1.101 8.001 forw F.000.00:14:01:01:01:00 F.000.00:14:01:01:01:00
8.001 Desg
      swp4.101 8.002 forw F.000.00:14:01:01:01:00 F.000.00:14:01:01:01:00
8.002 Desg
      E swp5.101 8.003 forw F.000.00:14:01:01:01:00 F.000.00:14:01:01:01:00
8.003 Desg

cumulus@switch:~$ sudo mstpcctl showportdetail br2 swp1.101
br2:swp1.101 CIST info
  enabled        yes          role          Designated
  port id       8.001        state         forwarding
  external port cost 2000    admin external cost 0
```

internal port cost	2000	admin internal cost	0
designated root	F.000.00:14:01:01:01:00	dsgn external cost	0
dsgn regional root	F.000.00:14:01:01:01:00	dsgn internal cost	0
designated bridge	F.000.00:14:01:01:01:00	designated port	8.001
admin edge port	no	auto edge port	yes
oper edge port	yes	topology change ack	no
point-to-point	yes	admin point-to-point	auto
restricted role	no	restricted TCN	no
port hello time	2	disputed	no
bpdu guard port	no	bpdu guard error	no
network port	no	BA inconsistent	no
Num TX BPDU	45772	Num TX TCN	4
Num RX BPDU	0	Num RX TCN	0
Num Transition FWD	2	Num Transition BLK	2

Configuring Spanning Tree Parameters

The persistent configuration for a bridge is set in `/etc/network/interfaces`. The configuration below shows every possible option configured. There is no requirement to configure any of these options:

```
auto br2
iface br2 inet static
    bridge-ports swp1 swp2 swp3 swp4
    bridge-stp on
    mstptctl-maxage 20
    mstptctl-ageing 300
    mstptctl-fdelay 15
    mstptctl-maxhops 20
    mstptctl-txholdcount 6
    mstptctl-forcevers rstp
    mstptctl-treepriority 32768
    mstptctl-treeportpriority swp3=128
    mstptctl-hello 2
    mstptctl-portpathcost swp1=0 swp2=0
    mstptctl-portadminedge swp1=no swp2=no
    mstptctl-portautoedge swp1=yes swp2=yes
    mstptctl-portp2p swp1=no swp2=no
    mstptctl-portrestrole swp1=no swp2=no
    mstptctl-portresttcn swp1=no swp2=no
    mstptctl-portnetwork swp1=no
    mstptctl-bpduguard swp1=no swp2=no
    mstptctl-portbpdufilter swp4=yes
```

Understanding the Spanning Tree Parameters

The spanning tree parameters are defined in the IEEE [802.1D](#), [802.1Q](#) specifications and in the table below.

While configuring spanning tree in a persistent configuration, as described above, is the preferred method, you can also use `mstptcl` to configure spanning tree protocol parameters at runtime.



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

The `mstp` daemon is an open source project that some network engineers may be unfamiliar with. For example, many incumbent vendors use the keyword `portfast` to describe a port that is automatically set to forwarding when the port is brought up. The `mstpd` equivalent is `mstptcl-portadminedge`. For more comparison [please read this knowledge base article](#).

Examples are included below:

Parameter	Description
maxage	<p>Sets the bridge's <i>maximum age</i> to <max_age> seconds. The default is 20. The maximum age must meet the condition $2 * (\text{Bridge Forward Delay} - 1 \text{ second}) \geq \text{Bridge Max Age}$.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre>mstptcl-maxage 24</pre> <p>To set this parameter at runtime, use:</p> <pre>mstptcl setmaxage <bridge> <max_age></pre> <pre>cumulus@switch:~\$ sudo mstptcl setmaxage br2 24</pre>
ageing	<p>Sets the Ethernet (MAC) address <i>ageing time</i> in <time> seconds for the bridge when the running version is STP, but not RSTP/MSTP. The default is 300.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre>mstptcl-ageing 240</pre> <p>To set this parameter at runtime, use:</p> <pre>mstptcl setageing <bridge> <time></pre> <pre>cumulus@switch:~\$ sudo mstptcl setageing br2 240</pre>

Parameter	Description
fdelay	<p>Sets the bridge's <i>bridge forward delay</i> to <time> seconds. The default is 15.</p> <p>The bridge forward delay must meet the condition $2 * (\text{Bridge Forward Delay} - 1 \text{ second}) \geq \text{Bridge Max Age}$.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre data-bbox="453 530 763 566">mstpctl -fdelay 15</pre> <p>To set this parameter at runtime, use:</p> <pre data-bbox="453 720 992 756">mstpctl setfdelay <bridge> <time></pre> <pre data-bbox="453 861 1286 897">cumulus@switch:~\$ sudo mstpctl setfdelay br2 15</pre>
maxhops	<p>Sets the bridge's <i>maximum hops</i> to <max_hops>. The default is 20.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre data-bbox="453 1127 780 1163">mstpctl -maxhops 24</pre> <p>To set this parameter at runtime, use:</p> <pre data-bbox="453 1317 1073 1353">mstpctl setmaxhops <bridge> <max_hops></pre> <pre data-bbox="453 1459 1310 1495">cumulus@switch:~\$ sudo mstpctl setmaxhops br2 24</pre>
txholdcount	<p>Sets the bridge's <i>bridge transmit hold count</i> to <tx_hold_count>. The default is 6.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre data-bbox="453 1719 829 1755">mstpctl -txholdcount 6</pre> <p>To set this parameter at runtime, use:</p> <pre data-bbox="421 1854 1188 1890">mstpctl settxholdcount <bridge> <tx_hold_count></pre>

Parameter	Description
	<pre>cumulus@switch:~\$ sudo mstpcctl settxholdcount br2 5</pre>
forcevers	<p>Sets the bridge's <i>force STP</i> version to either RSTP/STP. MSTP is not supported currently. The default is <i>RSTP</i>.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre>mstpctl-forcevers rstp</pre> <p>To set this parameter at runtime, use:</p> <pre>mstpctl setforcevers <bridge> {mstp rstp stp}</pre> <pre>cumulus@switch:~\$ sudo mstpctl setforcevers br2 rstp</pre>
treeprion	<p>Sets the bridge's <i>tree priority</i> to <priority> for an MSTI instance. The priority value is a number between 0 and 65535 and must be a multiple of 4096. The bridge with the lowest priority is elected the <i>root bridge</i>. The default is 32768.</p> <div style="border: 2px solid red; padding: 5px; margin-top: 10px;"> ! For <code>msti</code>, only 0 is supported currently. </div>
	<p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre>mstpctl-treeprion 8192</pre> <p>To set this parameter at runtime, use:</p> <pre>mstpctl settreeprion <bridge> <mstid> <priority></pre> <pre>cumulus@switch:~\$ sudo mstpctl settreeprion br2 0 8192</pre>
treportprion	<p>Sets the <i>priority</i> of port <port> to <priority> for the MSTI instance. The priority value is a number between 0 and 240 and must be a multiple of 16. The default is 128.</p>

Parameter	Description
	<p>For <code>msti</code>, only 0 is supported currently.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre data-bbox="453 481 1024 513"><code>mstpctl-treeportpri swp4.101 64</code></pre> <p>To set this parameter at runtime, use:</p> <pre data-bbox="453 661 1392 692"><code>mstpctl settreeportpri <bridge> <port> <mstid> <priority></code></pre> <pre data-bbox="453 808 1346 872"><code>cumulus@switch:~\$ sudo mstpctl settreeportpri br2 swp4.101 0 64</code></pre>
hello	<p>Sets the bridge's <i>bridge hello time</i> to <code><time></code> seconds. The default is 2.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre data-bbox="453 1115 747 1146"><code>mstpctl-hello 20</code></pre> <p>To set this parameter at runtime, use:</p> <pre data-bbox="453 1294 975 1326"><code>mstpctl sethello <bridge> <time></code></pre> <pre data-bbox="453 1442 1269 1474"><code>cumulus@switch:~\$ sudo mstpctl sethello br2 20</code></pre>
portpathcost	<p>Sets the <i>port cost</i> of the port <code><port></code> in bridge <code><bridge></code> to <code><cost></code>. The default is 0. <code>mstp</code> supports only long mode; that is, 32 bits for the path cost.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre data-bbox="453 1759 1024 1790"><code>mstpctl-portpathcost swp1.101=10</code></pre> <p>To set this parameter at runtime, use:</p>

Parameter	Description
	<pre>mstpctl setportpathcost <bridge> <port> <cost></pre> <pre>cumulus@switch:~\$ sudo mstpctl setportpathcost br2 swp1.101 10</pre>
portadminedge	<p>Enables/disables the <i>initial edge state</i> of the port <port> in bridge <bridge>. The default is <i>no</i>.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre>mstpctl -portadminedge swp1.101=yes</pre> <p>To set this parameter at runtime, use:</p> <pre>mstpctl setportadminedge <bridge> <port> {yes no}</pre> <pre>cumulus@switch:~\$ sudo mstpctl setportadminedge br2 swp1.101 yes</pre>
portautoedge	<p>Enables/disables the <i>auto transition</i> to/from the edge state of the port <port> in bridge <bridge>. The default is <i>yes</i>.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre>mstpctl -portautoedge swp1.101=no</pre> <p>To set this parameter at runtime, use:</p> <pre>mstpctl setportautoedge <bridge> <port> {yes no}</pre> <pre>cumulus@switch:~\$ sudo mstpctl setportautoedge br2 swp1.101 no</pre>
portp2p	

Parameter	Description
	<p>Enables/disables the <i>point-to-point detection mode</i> of the port <port> in bridge <bridge>. The default is <i>auto</i>.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre data-bbox="453 487 943 519">mstpctl -portp2p swp1.101=no</pre> <p>To set this parameter at runtime, use:</p> <pre data-bbox="453 671 1230 703">mstpctl setportp2p <bridge> <port> {yes no auto}</pre> <pre data-bbox="453 819 1410 872">cumulus@switch:~\$ sudo mstpctl setportp2p br2 swp1.101 no</pre>
portrestrrole	<p>Enables/disables the ability of the port <port> in bridge <bridge> to take the <i>root role</i>. The default is <i>no</i>.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre data-bbox="453 1157 1046 1189">mstpctl -portrestrrole swp1.101=no</pre> <p>To set this parameter at runtime, use:</p> <pre data-bbox="453 1341 1246 1370">mstpctl setportrestrrole <bridge> <port> {yes no}</pre> <pre data-bbox="453 1486 1361 1550">cumulus@switch:~\$ sudo mstpctl setportrestrrole br2 swp1.101 yes</pre>
portrestrtcn	<p>Enables/disables the ability of the port <port> in bridge <bridge> to propagate <i>received topology change notifications</i>. The default is <i>no</i>.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre data-bbox="453 1818 1046 1850">mstpctl -portrestrtcn swp1.101=yes</pre> <p>To set this parameter at runtime, use:</p>

Parameter	Description
	<pre>mstpctl setportrestrtcn <bridge> <port> {yes no}</pre> <pre>cumulus@switch:~\$ sudo mstpctl setportrestrtcn br2 swp1.101 yes</pre>
portnetwork	<p>Enables/disables the <i>bridge assurance capability</i> for a network port <code><port></code> in bridge <code><bridge></code>. The default is <i>no</i>.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre>mstpctl -portnetwork swp4.101=yes</pre> <p>To set this parameter at runtime, use:</p> <pre>mstpctl setportnetwork <bridge> <port> {yes no}</pre> <pre>cumulus@switch:~\$ sudo mstpctl setportnetwork br2 swp4. 101 yes</pre>
bpduguard	<p>Enables/disables the <i>BPDU guard configuration</i> of the port <code><port></code> in bridge <code><bridge></code>. The default is <i>no</i>.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre>mstpctl -bpduguard swp1=no</pre> <p>To set this parameter at runtime, use:</p> <pre>mstpctl setbpduguard <bridge> <port> {yes no}</pre> <pre>cumulus@switch:~\$ sudo mstpctl setbpduguard br2 swp1. 101 yes</pre>
portbpdufilter	

Parameter	Description
	<p>Enables/disables the <i>BPDU filter</i> functionality for a port <port> in bridge <bridge>. The default is <i>no</i>.</p> <p>To set this parameter persistently, configure it under the bridge stanza:</p> <pre>mstpctl -portbpdufilter swp4.101=yes</pre> <p>To set this parameter at runtime, use:</p> <pre>mstpctl setportbpdufilter <bridge> <port> {yes no}</pre> <pre>cumulus@switch:~\$ sudo mstpctl setportbpdufilter br2 swp4.101 yes</pre>

Bridge Assurance

On a point-to-point link where RSTP is running, if you want to detect unidirectional links and put the port in a discarding state (in error), you can enable bridge assurance on the port by enabling a port type network. The port would be in a bridge assurance inconsistent state until a BPDU is received from the peer. You need to configure the port type network on both the ends of the link in order for bridge assurance to operate properly.

The default setting for bridge assurance is off. This means that there is no difference between disabling bridge assurance on an interface and not configuring bridge assurance on an interface.

To enable bridge assurance on an interface, edit `/etc/network/interfaces` and add a line similar to the example below to the bridge configuration:

```
mstpctl -portnetwork swp1=no
```

You can monitor logs for bridge assurance messages by doing the following:

```
cumulus@switch:~$ sudo grep -in assurance /var/log/syslog | grep mstp
1365:Jun 25 18:03:17 mstpd: br1007:swp1.1007 Bridge assurance
inconsistent
```

To load the new configuration from `/etc/network/interfaces`, run `ifreload -a`:

```
cumulus@switch:~$ sudo ifreload -a
```

Runtime Configuration (Advanced)

- ❗ A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

To enable bridge assurance at runtime, run `mstpctl`:

```
cumulus@switch:~$ sudo mstpctl setportnetwork br1007 swp1.1007 yes
cumulus@switch:~$ sudo mstpctl showportdetail br1007 swp1.1007 | grep
network
    network port          yes           BA inconsistent      yes
```

BPDU Guard

To protect the spanning tree topology from unauthorized switches affecting the forwarding path, you can configure *BPDU guard* (Bridge Protocol Data Unit). One very common example is when someone hooks up a new switch to an access port off of a leaf switch. If this new switch is configured with a low priority, it could become the new root switch and affect the forwarding path for the entire Layer 2 topology.

Configuring BPDU Guard

You configure BPDU guard under the bridge stanza in `/etc/network/interfaces`:

```
auto br2
iface br2 inet static
    bridge-ports swp1 swp2 swp3 swp4 swp5 swp6
    bridge-stp on
    mstpctl-bpduguard swp1=yes swp2=yes swp3=yes swp4=yes
```

To load the new configuration, run `ifreload -a`:

```
cumulus@switch:~$ sudo ifreload -a
```

Non-Persistent Configuration

You can also configure BPDU guard on an individual port using a runtime configuration.

Runtime Configuration (Advanced)

- ❗ A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

```
cumulus@switch:~$ sudo mstpcctl setbpduguard br2 swp1 yes
cumulus@switch:~$ sudo mstpcctl setbpduguard br2 swp2 yes
cumulus@switch:~$ sudo mstpcctl setbpduguard br2 swp3 yes
cumulus@switch:~$ sudo mstpcctl setbpduguard br2 swp4 yes
```

Recovering a Port Disabled by BPDU Guard

If a BPDU is received on the port, STP will bring down the port and log an error in `/var/log/syslog`. The following is a sample error:

```
mstpd: error, MSTP_IN_rx_bpdu: bridge:bond0 Recvd BPDU on BPDU Guard
Port - Port Down
```

To determine whether BPDU guard is configured, or if a BPDU has been received, run `mstpcctl showportdetail <bridge name>`:

```
cumulus@switch:~$ sudo mstpcctl showportdetail br2 swp1 | grep guard
bpdu guard port      yes
bpdu guard error      yes
```

The only way to recover a port that has been placed in the disabled state is to manually un-shut or bring up the port with `sudo ifup [port]`, as shown in the example below:



Bringing up the disabled port does not fix the problem if the configuration on the connected end-station has not been rectified.

```
cumulus@leaf2$ mstpcctl showportdetail bridge bond0
bridge:bond0 CIST info
  enabled          no
  role
Disabled
  port id        8.001
  state
discarding
  external port cost 305
  internal port cost 305
  designated root   8.000.6C:64:1A:00:4F:9C dsgn external cost 0
  dsgn regional root 8.000.6C:64:1A:00:4F:9C dsgn internal cost 0
  designated bridge 8.000.6C:64:1A:00:4F:9C designated port 8.00
1
  admin edge port    no
  oper edge port     no
  point-to-point     yes
  restricted role    no
  port hello time    10
  bpdu guard port     yes
  network port       no
  Num TX BPDU        3
  auto edge port      yes
  topology change ack no
  admin point-to-point auto
  restricted TCN      no
  disputed
  bpdu guard error    yes
  BA inconsistent     no
  Num TX TCN          2
```

```

Num RX BPDU      488
Num Transition FWD 1
bpdufilter port   no
clag ISL          no
clag role         unknown
0:0:0:0
      clag remote portID F.FFF
0:0:0:0

Num RX TCN        2
Num Transition BLK 2
clag ISL Oper UP  no
clag dual conn mac 0:0:
clag system mac   0:0:

cumulus@leaf2$ sudo ifup bond0

cumulus@leaf2$ mstpcctl showportdetail bridge bond0
bridge:bond0 CIST info
  enabled           yes
  port id          8.001
  role              Root
  state
forwarding
  external port cost 305
  internal port cost 305
  designated root    8.000.6C:64:1A:00:4F:9C
  dsgn external cost 0
  dsgn regional root 8.000.6C:64:1A:00:4F:9C
  dsgn internal cost 0
  designated bridge  8.000.6C:64:1A:00:4F:9C
  designated port    8.00
1
  admin edge port   no
  oper edge port   no
  point-to-point    yes
  restricted role   no
  port hello time   2
  bpdu guard port   no
  network port      no
  Num TX BPDU       3
  Num RX BPDU       43
  Num Transition FWD 1
  bpdufilter port   no
  clag ISL          no
  clag role         unknown
0:0:0:0
      clag remote portID F.FFF
0:0:0:0

  auto edge port     yes
  topology change ack no
  admin point-to-point auto
  restricted TCN     no
  disputed            no
  bpdu guard error   no
  BA inconsistent     no
  Num TX TCN         2
  Num RX TCN         1
  Num Transition BLK 0
  clag ISL Oper UP   no
  clag dual conn mac 0:0:
  clag system mac   0:0:

```

BPDU Filter

You can enable `bpdufilter` on a switch port, which filters BPDUs in both directions. This effectively disables STP on the port.

To enable it, add the following to `/etc/network/interfaces` under the `bridge port iface` section example:

```
auto br100
```

```
iface br100
    bridge-ports swp1.100 swp2.100
    mstpcctl-portbpdufilter swp1=yes swp2=yes
```

To load the new configuration from /etc/network/interfaces, run ifreload -a:

```
cumulus@switch:~$ sudo ifreload -a
```

For more information, see `man(5) ifupdown-addons-interfaces`.

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

To enable BPDU filter at runtime, run `mstpcctl`:

```
cumulus@switch:~$ sudo mstpcctl setportbpdufilter br100 swp1.100=yes swp2.
100=yes
```

Configuration Files

- /etc/network/interfaces

Man Pages

- `brctl(8)`
- `bridge-utils-interfaces(5)`
- `ifupdown-addons-interfaces(5)`
- `mstpcctl(8)`
- `mstpcctl-utils-interfaces(5)`

Useful Links

The source code for `mstpd/mstpcctl` was written by [Vitalii Demianets](#) and is hosted at the sourceforge URL below.

- <https://sourceforge.net/projects/mstpd/>
- http://en.wikipedia.org/wiki/Spanning_Tree_Protocol

Caveats and Errata

- MSTP is not supported currently. However, interoperability with MSTP networks can be accomplished using PVRSTP or PVSTP.

Link Layer Discovery Protocol

The `lldpd` daemon implements the IEEE802.1AB (Link Layer Discovery Protocol, or LLDP) standard. LLDP allows you to know which ports are neighbors of a given port. By default, `lldpd` runs as a daemon and is started at system boot. `lldpd` command line arguments are placed in `/etc/default/lldpd`. `lldpd` configuration options are placed in `/etc/lldpd.conf` or under `/etc/lldpd.d/`.

For more details on the command line arguments and config options, please see `man lldpd(8)`.

`lldpd` supports CDP (Cisco Discovery Protocol, v1 and v2). `lldpd` logs by default into `/var/log/daemon.log` with an `lldpd` prefix.

`lldpcli` is the CLI tool to query the `lldpd` daemon for neighbors, statistics and other running configuration information. See `man lldpcli(8)` for details.

Contents

(Click to expand)

- [Contents \(see page 166\)](#)
- [Commands \(see page 166\)](#)
- [Man Pages \(see page 166\)](#)
- [Configuring LLDP \(see page 166\)](#)
- [Example lldpcli Commands \(see page 167\)](#)
- [Enabling the SNMP Subagent in LLDP \(see page 171\)](#)
- [Configuration Files \(see page 171\)](#)
- [Useful Links \(see page 171\)](#)
- [Caveats and Errata \(see page 171\)](#)

Commands

- `lldpd` (daemon)
- `lldpcli` (interactive CLI)

Man Pages

- `man lldpd`
- `man lldpcli`

Configuring LLDP

You configure `lldpd` settings in `/etc/lldpd.conf` or `/etc/lldpd.d/`.

Here is an example persistent configuration:

```
cumulus@switch:~$ sudo cat /etc/lldpd.conf
configure lldp tx-interval 40
configure lldp tx-hold 3
configure system interface pattern-blacklist "eth0"
```

lldpd logs to `/var/log/daemon.log` with the `lldpd` prefix:

```
cumulus@switch:~$ sudo tail -f /var/log/daemon.log | grep lldp
Aug  7 17:26:17 switch lldpd[1712]: unable to get system name
Aug  7 17:26:17 switch lldpd[1712]: unable to get system name
Aug  7 17:26:17 switch lldpccli[1711]: lldpd should resume operations
Aug  7 17:26:32 switch lldpd[1805]: NET-SNMP version 5.4.3 AgentX subagent
connected
```

Example lldpcli Commands

To see all neighbors on all ports/interfaces:

```
cumulus@switch:~$ sudo lldpcli show neighbors
-----
LLDP neighbors:
-----
Interface: eth0, via: CDPv1, RID: 72, Time: 0 day, 00:33:40
Chassis:
    ChassisID: local test-server-1
    SysName: test-server-1
    SysDescr: Linux running on
    Linux 3.2.2+ #1 SMP Mon Jun 10 16:21:22 PDT 2013 ppc
    MgmtIP: 192.0.2.72
    Capability: Router, on
Port:
    PortID: ifname eth1
-----
Interface: swp1, via: CDPv1, RID: 87, Time: 0 day, 00:36:27
nChassis:
    ChassisID: local T1
    SysName: T1
    SysDescr: Linux running on
Cumulus Linux
    MgmtIP: 192.0.2.15
```

```
Capability: Router, on
Port:
  PortID:      iface swp1
  PortDescr:   swp1
-----
... and more (output truncated to fit this doc)
```

To see neighbors on specific ports:

```
cumulus@switch:~$ sudo lldpcli show neighbors ports swp1,swp2
-----
Interface:    swp1, via: CDPv1, RID: 87, Time: 0 day, 00:36:27
Chassis:
  ChassisID:   local T1
  SysName:     T1
  SysDescr:    Linux running on
Cumulus Linux
  MgmtIP:      192.0.2.15
  Capability:  Router, on
Port:
  PortID:      iface swp1
  PortDescr:   swp1
-----
Interface:    swp2, via: CDPv1, RID: 123, Time: 0 day, 00:36:27
Chassis:
  ChassisID:   local T2
  SysName:     T2
  SysDescr:    Linux running on
Cumulus Linux
  MgmtIP:      192.0.2.15
  Capability:  Router, on
Port:
  PortID:      iface swp1
  PortDescr:   swp1
```

To see lldpd statistics for all ports:

```
cumulus@switch:~$ sudo lldpcli show statistics
-----
LLDP statistics:
-----
Interface:    eth0
```

```
Transmitted: 9423
Received: 17634
Discarded: 0
Unrecognized: 0
Ageout: 10
Inserted: 20
Deleted: 10
```

```
Interface: swp1
Transmitted: 9423
Received: 6264
Discarded: 0
Unrecognized: 0
Ageout: 0
Inserted: 2
Deleted: 0
```

```
Interface: swp2
Transmitted: 9423
Received: 6264
Discarded: 0
Unrecognized: 0
Ageout: 0
Inserted: 2
Deleted: 0
```

```
Interface: swp3
Transmitted: 9423
Received: 6265
Discarded: 0
Unrecognized: 0
Ageout: 0
Inserted: 2
Deleted: 0
```

```
... and more (output truncated to fit this document)
```

To see lldpd statistics summary for all ports:

```
cumulus@switch:~$ sudo lldpcli show statistics summary
-----
LLDP Global statistics:
-----
```

Summary of stats:

```
Transmitted: 648186
Received: 437557
Discarded: 0
Unrecognized: 0
Ageout: 10
Inserted: 38
Deleted: 10
```

To see the lldpd running configuration:

```
cumulus@switch:~$ sudo lldpcli show running-configuration
-----
Global configuration:
-----
Configuration:
  Transmit delay: 1
  Transmit hold: 4
  Receive mode: no
  Pattern for management addresses: (none)
  Interface pattern: (none)
  Interface pattern for chassis ID: (none)
  Override description with: (none)
  Override platform with: (none)
  Advertise version: yes
  Disable LLDP-MED inventory: yes
  LLDP-MED fast start mechanism: yes
  LLDP-MED fast start interval: 1
-----
```

Runtime Configuration (Advanced)



A runtime configuration does not persist when you reboot the switch — all changes are lost.

To configure active interfaces:

```
lldpcli configure system interface pattern "swp*"
```

To configure inactive interfaces:

```
lldpcli configure system interface pattern-blacklist "eth0"
```



The active interface list always overrides the inactive interface list.

To reset any interface list to none:

```
lldpcli configure system interface pattern-blacklist ""
```

Enabling the SNMP Subagent in LLDP

LLDP does not enable the SNMP subagent by default. You need to edit /etc/default/lldpd and enable the -x option.

```
cumulus@switch:~$ sudo nano /etc/default/lldpd
# Uncomment to start SNMP subagent and enable CD
P, SONMP and EDP protocol
#DAEMON_OPTS="-x -c -s -e"

# Enable CDP by default
DAEMON_OPTS="-c"
DAEMON_OPTS="-x"
```

Configuration Files

- /etc/lldpd.conf
- /etc/lldpd.d
- /etc/default/lldpd

Useful Links

- <http://vincentbernat.github.io/lldpd/>
- http://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

Caveats and Errata

- Annex E (and hence Annex D) of IEEE802.1AB (lldp) is not supported.

Prescriptive Topology Manager - PTM

In data center topologies, right cabling is a time-consuming endeavor and is error prone. Prescriptive Topology Manager (PTM) is a dynamic cabling verification tool to help detect and eliminate such errors. It takes a graphviz-DOT specified network cabling plan (something many operators already generate), stored in a `topology.dot` file, and couples it with runtime information derived from LLDP to verify that the cabling matches the specification. The check is performed on every link transition on each node in the network.

You can customize the `topology.dot` file to control `ptmd` at both the global/network level and the node/port level.

PTM runs as a daemon, named `ptmd`.

For more information, see `man ptmd(8)`.

Contents

(Click to expand)

- [Contents \(see page 172\)](#)
- [Supported Features \(see page 172\)](#)
- [Configuring PTM \(see page 173\)](#)
- [Basic Topology Example \(see page 173\)](#)
- [Advanced PTM Configuration \(see page 174\)
 - \[Scripts \\(see page 174\\)\]\(#\)
 - \[Configuration Parameters \\(see page 175\\)
 - \\[Host-only Parameters \\\(see page 175\\\)\\]\\(#\\)
 - \\[Global Parameters \\\(see page 175\\\)\\]\\(#\\)
 - \\[Per-port Parameters \\\(see page 176\\\)\\]\\(#\\)
 - \\[Templates \\\(see page 176\\\)\\]\\(#\\)
 - \\[Supported BFD and LLDP Parameters \\\(see page 177\\\)\\]\\(#\\)\]\(#\)
 - \[Bidirectional Forwarding Detection \\(BFD\\) \\(see page 178\\)
 - \\[Configuring BFD \\\(see page 178\\\)\\]\\(#\\)
 - \\[Echo Function \\\(see page 178\\\)\\]\\(#\\)\]\(#\)](#)
- [Enabling Quagga to Check Link State \(see page 180\)](#)
- [Using ptmd Service Commands \(see page 180\)](#)
- [Using ptmctl Commands \(see page 181\)
 - \[ptmctl Examples \\(see page 181\\)\]\(#\)
 - \[ptmctl Error Outputs \\(see page 183\\)\]\(#\)](#)
- [Configuration Files \(see page 184\)](#)
- [Useful Links \(see page 184\)](#)
- [Caveats and Errata \(see page 184\)](#)

Supported Features

- Topology verification using LLDP. `ptmd` creates a client connection to the LLDP daemon, `lldpd`, and retrieves the neighbor relationship between the nodes/ports in the network and compares them against the prescribed topology specified in the `topology.dot` file.
- Only physical interfaces, like `swp1` or `eth0`, are currently supported. Cumulus Linux does not support specifying virtual interfaces like bonds or subinterfaces like `eth0.200` in the topology file.
- Forwarding path failure detection using **Bidirectional Forwarding Detection** (BFD); however, demand mode is not supported. For more information on how BFD operates in Cumulus Linux, [see below](#) ([see page 178](#)) and see `man ptmd(8)`.
- Integration with Quagga (PTM to Quagga notification).
- Client management: `ptmd` creates an abstract named socket `/var/run/ptmd.socket` on startup. Other applications can connect to this socket to receive notifications and send commands.
- Event notifications: see Scripts below.
- User configuration via a `topology.dot` file; [see below](#) ([see page 173](#)).

Configuring PTM

`ptmd` verifies the physical network topology against a DOT-specified network graph file, `/etc/ptm.d/topology.dot`.



This file must be present or else `ptmd` will not start. You can specify an alternate file using the `-c` option.

PTM supports [undirected graphs](#).

At startup, `ptmd` connects to `lldpd`, the LLDP daemon, over a Unix socket and retrieves the neighbor name and port information. It then compares the retrieved port information with the configuration information that it read from the topology file. If there is a match, then it is a PASS, else it is a FAIL.



PTM performs its LLDP neighbor check using the PortID ifname TLV information. Previously, it used the PortID port description TLV information.

Basic Topology Example

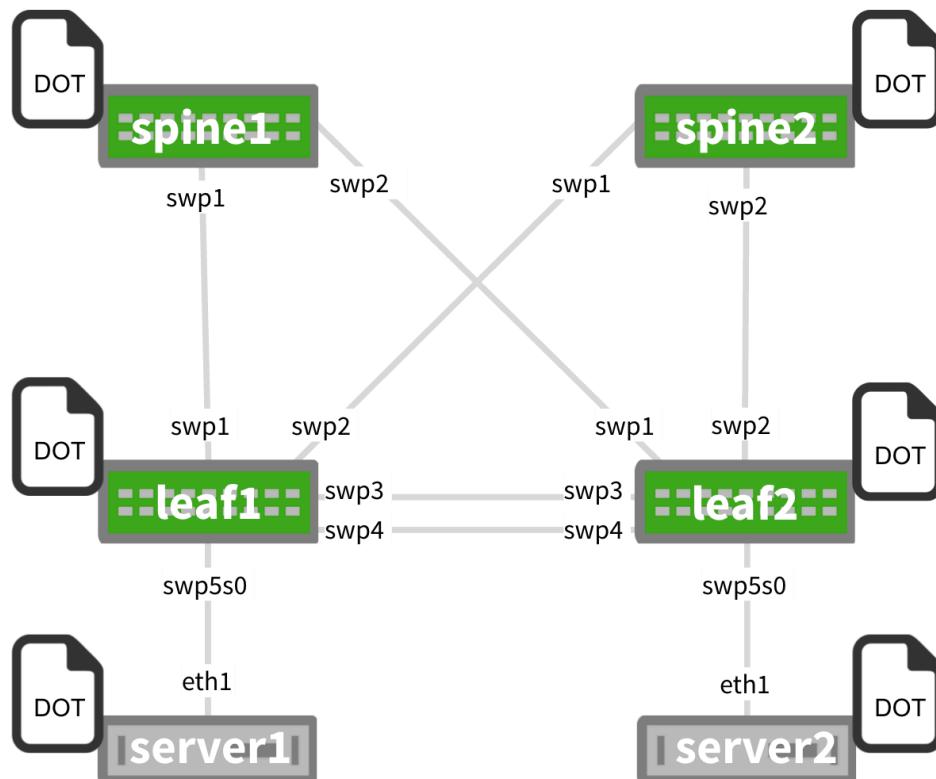
This is a basic example DOT file and its corresponding topology diagram. You should use the same `topology.dot` file on all switches, and don't split the file per device; this allows for easy automation by pushing/pulling the same exact file on each device!

```
graph G {
    "spine1":"swp1" -- "leaf1":"swp1";
    "spine1":"swp2" -- "leaf2":"swp1";
    "spine2":"swp1" -- "leaf1":"swp2";
    "spine2":"swp2" -- "leaf2":"swp2";
```

```

"leaf1": "swp3" -- "leaf2": "swp3";
"leaf1": "swp4" -- "leaf2": "swp4";
"leaf1": "swp5s0" -- "server1": "eth1";
"leaf2": "swp5s0" -- "server2": "eth1";
}

```



Advanced PTM Configuration

PTM allows for more advanced configuration of the topology file using parameters you specify in the topology file.

Scripts

`ptmd` executes scripts at `/etc/ptm.d/if-topo-pass` and `/etc/ptm.d/if-topo-fail` for each interface that goes through a change, running `if-topo-pass` when an LLDP or BFD check passes and running `if-topo-fails` when the check fails. The scripts receive an argument string that is the result of the `ptmctl` command, described in the [ptm commands section below](#) (see page 180).

You should modify these default scripts as needed.

Configuration Parameters

You can configure `ptmd` parameters in the topology file. The parameters are classified as host-only, global, per-port/node and templates.

Host-only Parameters

Host-only parameters apply to the entire host on which PTM is running. You can include the `hostnametype` host-only parameter, which specifies whether PTM should use only the host name (`hostname`) or the fully-qualified domain name (`fqdn`) while looking for the `self-node` in the graph file. For example, in the graph file below, PTM will ignore the FQDN and only look for `switch04`, since that is the host name of the switch it's running on:

- ✔ It's a good idea to always wrap the hostname in double quotes, like "`www.example.com`". Otherwise, `ptmd` can fail if you specify a fully-qualified domain name as the hostname and do not wrap it in double quotes.
Further, to avoid errors when starting the `ptmd` process, make sure that `/etc/hosts` and `/etc/hostname` both reflect the hostname you are using in the `topology.dot` file.

```
graph G {
    hostnametype="hostname"
    BFD="upMinTx=150,requiredMinRx=250"
    "cumulus": "swp44" -- "switch04.cumulusnetworks.com": "swp20"
    "cumulus": "swp46" -- "switch04.cumulusnetworks.com": "swp22"
}
```

However, in this next example, PTM will compare using the FQDN and look for `switch05.cumulusnetworks.com`, which is the FQDN of the switch it's running on:

```
graph G {
    hostnametype="fqdn"
    "cumulus": "swp44" -- "switch05.cumulusnetworks.com": "swp20"
    "cumulus": "swp46" -- "switch05.cumulusnetworks.com": "swp22"
}
```

Global Parameters

Global parameters apply to every port listed in the topology file. There are two global parameters: LLDP and BFD. LLDP is enabled by default; if no keyword is present, default values are used for all ports. However, BFD is disabled if no keyword is present, unless there is a per-port override configured. For example:

```
graph G {
    LLDP= ""
    BFD="upMinTx=150,requiredMinRx=250,afi=both"
    "cumulus": "swp44" -- "qct-ly2-04": "swp20"
    "cumulus": "swp46" -- "qct-ly2-04": "swp22"
}
```

Per-port Parameters

Per-port parameters provide finer-grained control at the port level. These parameters override any global or compiled defaults. For example:

```
graph G {
    LLDP= ""
    BFD="upMinTx=300,requiredMinRx=100"
    "cumulus": "swp44" -- "qct-ly2-04": "swp20" [BFD="upMinTx=150,
requiredMinRx=250,afi=both"]
    "cumulus": "swp46" -- "qct-ly2-04": "swp22"
}
```

Templates

Templates provide flexibility in choosing different parameter combinations and applying them to a given port. A template instructs `ptmd` to reference a named parameter string instead of a default one. There are two parameter strings `ptmd` supports:

- `bfdtmp1`, which specifies a custom parameter tuple for BFD.
- `lldptmp1`, which specifies a custom parameter tuple for LLDP.

For example:

```
graph G {
    LLDP= ""
    BFD="upMinTx=300,requiredMinRx=100"
    BFD1="upMinTx=200,requiredMinRx=200"
    BFD2="upMinTx=100,requiredMinRx=300"
    LLDP1="match_type=ifname"
    LLDP2="match_type=portdescr"
    "cumulus": "swp44" -- "qct-ly2-04": "swp20" [BFD="bfdtmp1=BFD1",
LLDP="lldptmp1=LLDP1"]
    "cumulus": "swp46" -- "qct-ly2-04": "swp22" [BFD="bfdtmp1=BFD2",
LLDP="lldptmp1=LLDP2"]
    "cumulus": "swp46" -- "qct-ly2-04": "swp22"
}
```

In this template, LLDP1 and LLDP2 are templates for LLDP parameters while BFD1 and BFD2 are templates for BFD parameters.

Supported BFD and LLDP Parameters

ptmd supports the following BFD parameters:

- `upMinTx`: the minimum transmit interval, which defaults to `300ms`, specified in milliseconds.
- `requiredMinRx`: the minimum interval between received BFD packets, which defaults to `300ms`, specified in milliseconds.
- `detectMult`: the detect multiplier, which defaults to `3`, and can be any non-zero value.
- `afi`: the address family to be supported for the edge. The address family must be one of the following:
 - `v4`: BFD sessions will be built for only IPv4 connected peer. This is the default value.
 - `v6`: BFD sessions will be built for only IPv6 connected peer.
 - `both`: BFD sessions will be built for both IPv4 and IPv6 connected peers.

The following is an example of a topology with BFD applied at the port level:

```
graph G {
    "cumulus-1": "swp44" -- "cumulus-2": "swp20" [BFD="upMinTx=300,
requiredMinRx=100,afi=v6"]
    "cumulus-1": "swp46" -- "cumulus-2": "swp22" [BFD="detectMult=4"]
}
```

ptmd supports the following LLDP parameters:

- `match_type`, which defaults to the interface name (`ifname`), but can accept a port description (`portdescr`) instead if you want `lldpd` to compare the topology against the port description instead of the interface name. You can set this parameter globally or at the per-port level.
- `match_hostname`, which defaults to the host name (`hostname`), but enables PTM to match the topology using the fully-qualified domain name (`fqdn`) supplied by LLDP.

The following is an example of a topology with LLDP applied at the port level:

```
graph G {
    "cumulus-1": "swp44" -- "cumulus-2": "swp20" [LLDP=
match_hostname=fqdn"]
    "cumulus-1": "swp46" -- "cumulus-2": "swp22" [LLDP=
match_type=portdescr"]
}
```



When you specify `match_hostname=fqdn`, `ptmd` will match the entire FQDN, like `cumulus-2.domain.com` in the example below. If you do not specify anything for `match_hostname`, `ptmd` will match based on hostname only, like `cumulus-3` below, and ignore the rest of the URL:

```
graph G {
    "cumulus-1": "swp44" -- "cumulus-2.domain.com": "swp20"
    [LLDP="match_hostname=fqdn"]
    "cumulus-1": "swp46" -- "cumulus-3": "swp22" [LLDP=
    match_type=portdescr]
}
```

Bidirectional Forwarding Detection (BFD)

BFD provides low overhead and rapid detection of failures in the paths between two network devices. It provides a unified mechanism for link detection over all media and protocol layers. Use BFD to detect failures for IPv4 and IPv6 single or multihop paths between any two network devices, including unidirectional path failure detection. For more information, see the [BFD chapter \(see page 394\)](#).



BFD requires an IP address for any interface on which it is configured. The neighbor IP address for a single hop BFD session must be in the ARP table before BFD can start sending control packets.



You cannot specify BFD multihop sessions in the `topology.dot` file since you cannot specify the source and destination IP address pairs in that file. Use [Quagga \(see page 346\)](#) to configure multihop sessions.

Configuring BFD

You configure BFD one of two ways: by specifying the configuration in the `topology.dot` file, or using [Quagga \(see page 346\)](#). However, the topology file has some limitations:

- The `topology.dot` file supports creating BFD IPv4 and IPv6 single hop sessions only; you cannot specify IPv4 or IPv6 multihop sessions in the topology file.
- The topology file supports BFD sessions for only link-local IPv6 peers; BFD sessions for global IPv6 peers discovered on the link will not be created.

Echo Function

Cumulus Linux supports the *echo function* for IPv4 single hops only, and with the a synchronous operating mode only (Cumulus Linux does not support demand mode).

You use the echo function primarily to test the forwarding path on a remote system. To enable the echo function, set `echoSupport` to 1 in the topology file.

Once the echo packets are looped by the remote system, the BFD control packets can be sent at a much lower rate. You configure this lower rate by setting the `slowMinTx` parameter in the topology file to a non-zero value of milliseconds.

You can use more aggressive detection times for echo packets since the round-trip time is reduced because they are accessing the forwarding path. You configure the detection interval by setting the `echoMinRx` parameter in the topology file to a non-zero value of milliseconds; the minimum setting is 50 milliseconds. Once configured, BFD control packets are sent out at this required minimum echo Rx interval. This indicates to the peer that the local system can loop back the echo packets. Echo packets are transmitted if the peer supports receiving echo packets.

About the Echo Packet

BFD echo packets are encapsulated into UDP packets over destination and source UDP port number 3785. The BFD echo packet format is vendor-specific and has not been defined in the RFC. BFD echo packets that originate from Cumulus Linux are 8 bytes long and have the following format:

0	1	2	3
Version	Length	Reserved	
My Discriminator			

Where:

- **Version** is the version of the BFD echo packet.
- **Length** is the length of the BFD echo packet.
- **My Discriminator** is a non-zero value that uniquely identifies a BFD session on the transmitting side. When the originating node receives the packet after being looped back by the receiving system, this value uniquely identifies the BFD session.

Transmitting and Receiving Echo Packets

BFD echo packets are transmitted for a BFD session only when the peer has advertised a non-zero value for the required minimum echo Rx interval (the `echoMinRx` setting) in the BFD control packet when the BFD session starts. The transmit rate of the echo packets is based on the peer advertised echo receive value in the control packet.

BFD echo packets are looped back to the originating node for a BFD session only if locally the `echoMinRx` and `echoSupport` are configured to a non-zero values.

Using Echo Function Parameters

You configure the echo function by setting the following parameters in the topology file at the global, template and port level:

- **echoSupport:** Enables and disables echo mode. Set to 1 to enable the echo function. It defaults to 0 (disable).
- **echoMinRx:** The minimum interval between echo packets the local system is capable of receiving. This is advertised in the BFD control packet. When the echo function is enabled, it defaults to 50. If you disable the echo function, this parameter is automatically set to 0, which indicates the port or the node cannot process or receive echo packets.

- **slowMinTx:** The minimum interval between transmitting BFD control packets when the echo packets are being exchanged.

Enabling Quagga to Check Link State

The Quagga routing suite enables additional checks to ensure that routing adjacencies are formed only on links that have connectivity conformant to the specification, as determined by `ptmd`.



You only need to do this to check link state; you don't need to enable PTM to determine BFD status.

To enable the check:

```
quagga# conf t
quagga(config)# ptm-enable
quagga(config)#+
```

To disable the checks:

```
quagga# conf t
quagga(config)# no ptm-enable
quagga(config)#+
```

When the `ptm-enable` flag is configured by the user, the `zebra` daemon connects to `ptmd` over a Unix socket. Any time there is a change of status for an interface, `ptmd` sends notifications to `zebra`. Zebra maintains a `ptm-status` flag per interface and evaluates routing adjacency based on this flag. To check the per-interface `ptm-status`:

```
quagga# show interface swp1
Interface swp1 is up, line protocol is up
  PTM status: pass
  Description: T1
  index 3 metric 1 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 44:38:39:00:27:1d
  inet 192.0.2.1/31 broadcast 255.255.255.255
  inet6 2001:DB8::271d/64
quagga#
```

Using ptmd Service Commands

PTM sends client notifications in CSV format.

cumulus@switch:~\$ sudo service ptmd start|restart|force-reload: Starts or restarts the ptmd service. The topology.dot file must be present in order for the service to start.

cumulus@switch:~\$ sudo service ptmd reconfig: Instructs ptmd to read the topology.dot file again without restarting, applying the new configuration to the running state.

cumulus@switch:~\$ sudo service ptmd stop: Stops the ptmd service.

cumulus@switch:~\$ sudo service ptmd status: Retrieves the current running state of ptmd.

Using ptmctl Commands

ptmctl is a client of ptmd; it retrieves the daemon's operational state. It connects to ptmd over a Unix socket and listens for notifications. ptmctl parses the CSV notifications sent by ptmd.

See `man ptmctl` for more information.

ptmctl Examples

For basic output, use `ptmctl` without any options:

```
cumulus@switch:~$ sudo ptmctl

-----
port  cbl      BFD      BFD
      status   status   peer
                           local   type
-----
swp1  pass     pass    11.0.0.2
      N/A      N/A
      N/A      N/A
      N/A      N/A
      N/A      N/A
```

For more detailed output, use the `-d` option:

```
cumulus@switch:~$ sudo ptmctl -d

-----
port  cbl      exp      act      sysname  portID  portDescr  match  last
BFD   BFD      BFD      BFD      det_mult tx_timeout rx_timeout
echo_tx_timeout echo_rx_timeout max_hop_cnt
      status  nbr      nbr
      Type   state   peer  DownDiag
```

```
-----
-----
swp45 pass    h1:swp1 h1:swp1  h1          swp1      swp1      IfName 5m: 5s  N
/A     N/A     N/A     N/A          N/A       N/A       N
/A           N/A          N/A
swp46 fail    h2:swp1 h2:swp1  h2          swp1      swp1      IfName 5m: 5s  N
/A     N/A     N/A     N/A          N/A       N/A       N
/A           N/A          N/A
```

To return information on active BFD sessions `ptmd` is tracking, use the `-b` option:

```
cumulus@switch:~$ sudo ptmctl -b

-----
port  peer          state  local          type      diag
-----

swp1  11.0.0.2    Up     N/A          singlehop  N/A
N/A   12.12.12.1  Up     12.12.12.4  multihop   N/A
```

To return LLDP information, use the `-l` option. It returns only the active neighbors currently being tracked by `ptmd`.

```
cumulus@switch:~$ sudo ptmctl -l

-----
port  sysname  portID  port      match  last
                  descr   on      upd
-----

swp45 h1        swp1    swp1    IfName 5m:59s
swp46 h2        swp1    swp1    IfName 5m:59s
```

To return detailed information on active BFD sessions `ptmd` is tracking, use the `-b` and `-d` options (results are for an IPv6-connected peer):

```
cumulus@switch:~$ sudo ptmctl -b -d

-----
-----
-----
port  peer          state  local  type      diag  det  tx_timeout
-----
```

```

rx_timeout echo      echo      max      rx_ctrl tx_ctrl rx_echo
tx_echo

mult          tx_timeout rx_timeout
hop_cnt

-----
-----
-----

swp1 fe80::202:ff:fe00:1 Up      N/A     singlehop N/A   3    300
900      0           0          N/A     187172  185986 0
0

swp1 3101:abc:bcad::2 Up      N/A     singlehop N/A   3    300
900      0           0          N/A     501     533    0
0

```

ptmctl Error Outputs

If there are errors in the topology file or there isn't a session, PTM will return appropriate outputs. Typical error strings are:

```

Topology file error [/etc/ptm.d/topology.dot] [cannot find node cumulus] -
please check /var/log/ptmd.log for more info

Topology file error [/etc/ptm.d/topology.dot] [cannot open file (errno 2)] -
please check /var/log/ptmd.log for more info

No Hostname/MgmtIP found [Check LLDPD daemon status] -
please check /var/log/ptmd.log for more info

No BFD sessions . Check connections

No LLDP ports detected. Check connections

Unsupported command

```

For example:

```

cumulus@switch:~$ sudo ptmctl
-----
cmd      error

```

```
-----  
get-status Topology file error [/etc/ptm.d/topology.dot] [cannot open file  
(errno 2)] - please check /var/log/ptmd.log for more info
```



If you encounter errors with the `topology.dot` file, you can use `dot` (included in the Graphviz package) to validate the syntax of the topology file.

By simply opening the topology file with Graphviz, you can ensure that it is readable and that the file format is correct.

If you edit `topology.dot` file from a Windows system, be sure to double check the file formatting; there may be extra characters that keep the graph from working correctly.

Configuration Files

- `/etc/ptm.d/topology.dot`
- `/etc/ptm.d/if-topo-pass`
- `/etc/ptm.d/if-topo-fail`

Useful Links

- Bidirectional Forwarding Detection (BFD)
- Graphviz
- LLDP on Wikipedia
- PTMd GitHub repo

Caveats and Errata

- Prior to version 2.1, Cumulus Linux stored the `ptmd` configuration files in `/etc/cumulus/ptm.d`. When you upgrade to version 2.1 or later, all the existing `ptmd` files are copied from their original location to `/etc/ptm.d` with a `dpkg-old` extension, except for `topology.dot`, which gets copied to `/etc/ptm.d`. If you customized the `if-topo-pass` and `if-topo-fail` scripts, they are also copied to `dpgk-old`, and you must modify them so they can parse the CSV output correctly. Sample `if-topo-pass` and `if-topo-fail` scripts are available in `/etc/ptm.d`. A sample `topology.dot` file is available in `/usr/share/doc/ptmd/examples`.

Bonding - Link Aggregation

Linux bonding provides a method for aggregating multiple network interfaces (the slaves) into a single logical bonded interface (the bond). Cumulus Linux bonding supports the IEEE 802.3ad link aggregation mode. Link aggregation allows one or more links to be aggregated together to form a *link aggregation group* (LAG), such that a media access control (MAC) client can treat the link aggregation group as if it were a single link. The benefits of link aggregation are:

- Linear scaling of bandwidth as links are added to LAG

- Load balancing
- Failover protection

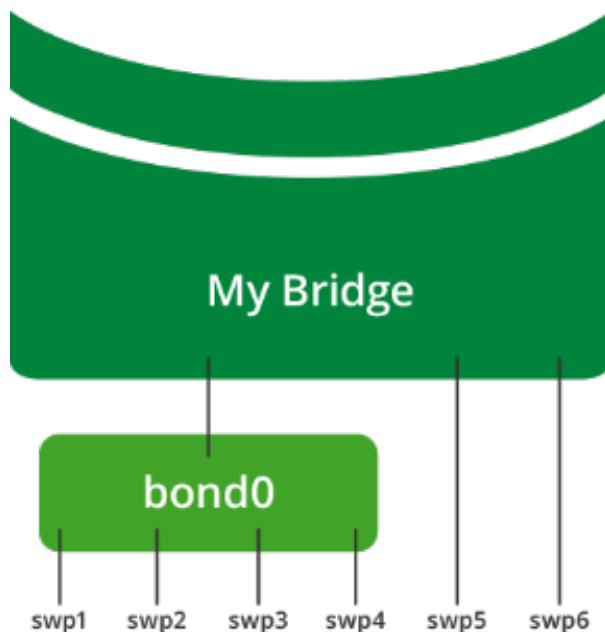
Cumulus Linux LAG control protocol is LACP version 1.

Contents

(Click to expand)

- [Contents \(see page 185\)](#)
- [Example: Bonding 4 Slaves \(see page 185\)](#)
- [Hash Distribution \(see page 187\)](#)
- [Configuration Files \(see page 187\)](#)
- [Useful Links \(see page 187\)](#)
- [Caveats and Errata \(see page 187\)](#)

Example: Bonding 4 Slaves



In this example, front panel port interfaces swp1-swp4 are slaves in bond0 (swp5 and swp6 are not part of bond0).

The name of the bond is arbitrary as long as it follows Linux interface naming guidelines, and is unique within the switch. The only bonding mode supported in Cumulus Linux is 802.3ad. There are several 802.3 ad settings that can be applied to each bond.

All of the following settings except for `bond-slaves` are set to the recommended defaults and should only be added to a configuration in `/etc/network/interfaces` if you plan to use a different setting.

- `bond-slaves`: The list of slaves in bond.
- `bond-mode`: Is set to `802.3ad` by default and **must not** be changed.
- `bond-miimon`: How often the link state of each slave is inspected for link failures. It `100`, the recommended value.

- **bond-use-carrier**: How to determine link state. It defaults to 1.
- **bond-xmit-hash-policy**: Hash method used to select the slave for a given packet; it defaults to **layer3+4** and **must not** be changed.
- **bond-lacp-rate**: Rate to ask link partner to transmit LACP control packets. It defaults to 1.
- **bond-min-links**: Specifies the minimum number of links that must be active before asserting carrier on the bond. It defaults to 1, but a value greater than 1 is useful if higher level services need to ensure a minimum of aggregate bandwidth before putting the bond in service.

See Useful Links below for more details on settings.

To configure the bond, edit `/etc/network/interfaces` and add a stanza for bond0:

```
auto bond0
iface bond0
  address 10.0.0.1/30
  bond-slaves swp1 swp2 swp3 swp4
```

However, if you are intending that the bond become part of a bridge, you don't need to specify an IP address. The configuration would look like this:

```
auto bond0
iface bond0
  bond-slaves glob swp1-4
```

See `man interfaces` for more information on `/etc/network/interfaces`.

Here the link state sampling rate is 1/10 sec, and the LACP transmit rate is set to high. `bond-min-links` is set to 1 to indicate the bond must have at least one active member for bond to assert carrier. If the number of active members drops below the `bond-min-links` setting, the bond will appear to upper-level protocols as *link-down*. When the number of active links returns to greater than or equal to `bond-min-links`, the bond will become *link-up*.

When networking is started on switch, bond0 is created as MASTER and interfaces swp1-swp4 come up in SLAVE mode, as seen in the `ip link show` command:

```
3: swp1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
  master bond0 state UP mode DEFAULT qlen 500
    link/ether 44:38:39:00:03:c1 brd ff:ff:ff:ff:ff:ff
4: swp2: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
  master bond0 state UP mode DEFAULT qlen 500
    link/ether 44:38:39:00:03:c1 brd ff:ff:ff:ff:ff:ff
5: swp3: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
  master bond0 state UP mode DEFAULT qlen 500
    link/ether 44:38:39:00:03:c1 brd ff:ff:ff:ff:ff:ff
6: swp4: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
```

```
master bond0 state UP mode DEFAULT qlen 500
    link/ether 44:38:39:00:03:c1 brd ff:ff:ff:ff:ff:ff
```

And

```
55: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP mode DEFAULT
    link/ether 44:38:39:00:03:c1 brd ff:ff:ff:ff:ff:ff
```



All slave interfaces within a bond will have the same MAC address as the bond. Typically, the first slave added to the bond donates its MAC address for the bond. The other slaves' MAC addresses are set to the bond MAC address. The bond MAC address is used as source MAC address for all traffic leaving the bond, and provides a single destination MAC address to address traffic to the bond.

Hash Distribution

Egress traffic through a bond is distributed to a slave based on a packet hash calculation. This distribution provides load balancing over the slaves. The hash calculation uses packet header data to pick which slave to transmit the packet. For IP traffic, IP header source and destination fields are used in the calculation. For IP + TCP/UDP traffic, source and destination ports are included in the hash calculation. Traffic for a given conversation flow will always hash to the same slave. Many flows will be distributed over all the slaves to load balance the total traffic. In a failover event, the hash calculation is adjusted to steer traffic over available slaves.

Configuration Files

- /etc/network/interfaces

Useful Links

- <http://www.linuxfoundation.org/collaborate/workgroups/networking/bonding>
- 802.3ad (Accessible writeup)
- Link aggregation from Wikipedia

Caveats and Errata

- An interface cannot belong to multiple bonds.
- Slave ports within a bond should all be set to the same speed/duplex, and should match the link partner's slave ports.
- A bond cannot enslave VLAN subinterfaces. A bond can have subinterfaces, but not the other way around.

Ethernet Bridging - VLANs

Ethernet bridges provide a means for hosts to communicate at layer 2. Bridge members can be individual physical interfaces, bonds or logical interfaces that traverse an 802.1Q VLAN trunk. Cumulus Linux does not put all ports into a bridge by default.

Cumulus Linux 2.5.0 introduced a new method for configuring bridges that are [VLAN-aware \(see page 208\)](#). The bridge driver in Cumulus Linux 2.5.x is capable of VLAN filtering, which allows for configurations that are similar to incumbent network devices. While Cumulus Linux supports Ethernet bridges in traditional mode Cumulus Networks recommends using [VLAN-aware](#) mode unless you are using VXLANS in your network.

For a comparison of traditional and VLAN-aware modes, read [this knowledge base article](#).



You can configure both VLAN-aware and traditional mode bridges on the same network in Cumulus Linux; however you should not have more than one VLAN-aware bridge on a given switch. If you are implementing [VXLANS \(see page 322\)](#), you **must** use traditional bridge mode.

Contents

(Click to expand)

- [Contents \(see page 188\)](#)
- [Configuration Files \(see page 188\)](#)
- [Commands \(see page 189\)](#)
- [Creating a Bridge between Physical Interfaces \(see page 189\)](#)
 - [Creating the Bridge and Adding Interfaces \(see page 189\)](#)
 - [Showing and Verifying the Bridge Configuration \(see page 191\)](#)
- [Examining MAC Addresses \(see page 191\)](#)
- [Multiple Bridges \(see page 192\)](#)
- [Configuring an SVI \(Switch VLAN Interface\) \(see page 195\)](#)
 - [Showing and Verifying the Bridge Configuration \(see page 196\)](#)
- [Using Trunks in Traditional Bridging Mode \(see page 197\)](#)
 - [Trunk Example \(see page 198\)](#)
 - [Showing and Verifying the Trunk \(see page 199\)](#)
 - [Additional Examples \(see page 199\)](#)
- [Configuration Files \(see page 199\)](#)
- [Useful Links \(see page 200\)](#)
- [Caveats and Errata \(see page 200\)](#)

Configuration Files

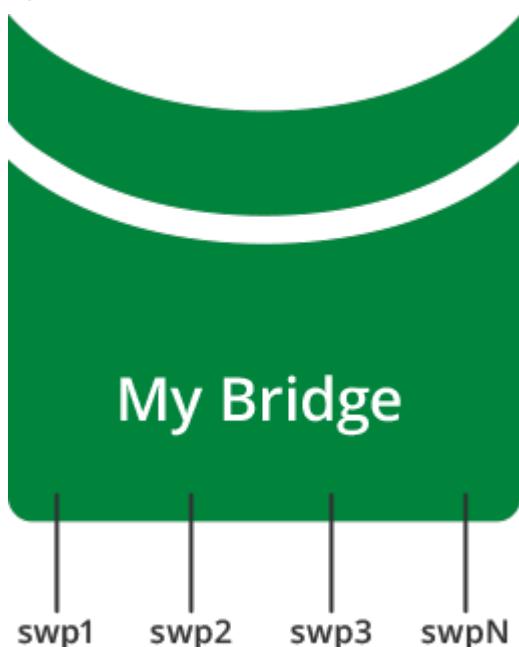
- [/etc/network/interfaces](#)

Commands

- brctl
- bridge
- ip addr
- ip link

Creating a Bridge between Physical Interfaces

The basic use of bridging is to connect all of the physical and logical interfaces in the system into a single layer 2 domain.



Creating the Bridge and Adding Interfaces

You statically manage bridge configurations in `/etc/network/interfaces`. The following configuration snippet details an example bridge used throughout this chapter, explicitly enabling [spanning tree \(see page 150\)](#) and setting the bridge MAC address ageing timer. First, create a bridge with a descriptive name of 15 characters or fewer. Then add the logical interfaces (`bond0`) and physical interfaces (`swp5`, `swp6`) to assign to that bridge.

```
auto my_bridge
iface my_bridge
    bridge-ports bond0 swp5 swp6
    bridge-ageing 150
    bridge-stp on
```

Keyword	Explanation
bridge-ports	List of logical and physical ports belonging to the logical bridge.
bridge-ageing	Maximum amount of time before a MAC addresses learned on the bridge expires from the bridge MAC cache. The default value is 300 seconds.
bridge-stp	Enables spanning tree protocol on this bridge. The default spanning tree mode is Per VLAN Rapid Spanning Tree Protocol (PVRST). For more information on spanning-tree configurations see the configuration section: Spanning Tree and Rapid Spanning Tree (see page 150) .

To bring up the bridge `my_bridge`, use the `ifreload` command:

```
cumulus@switch:~$ sudo ifreload -a
```

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

To create the bridge and interfaces on the bridge, run:

```
cumulus@switch:~$ sudo brctl addbr my_bridge

cumulus@switch:~$ sudo brctl addif my_bridge bond0 swp5 swp6

cumulus@switch:~$ sudo brctl show
bridge name          bridge id      STP enabled     interfaces
my_bridge            8000.44383900129b  yes           bond0
                                         swp5
                                         swp6
```

```
cumulus@switch:~$ sudo ip link set up dev my_bridge
```

```
cumulus@switch:~$ sudo ip link set up dev bond0
```

```
cumulus@switch:~$ sudo for I in {5..6}; do ip link set up dev swp$I; done
```

Showing and Verifying the Bridge Configuration

```
cumulus@switch:~$ ip link show my_bridge
56: my_bridge: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP mode DEFAULT
    link/ether 44:38:39:00:12:9b brd ff:ff:ff:ff:ff:ff
```



Do not try to bridge the management port, eth0, with any switch ports (like swp0, swp1, and so forth). For example, if you created a bridge with eth0 and swp1, it will **not** work.

Using netshow to Display Bridge Information

`netshow` is a Cumulus Linux tool for retrieving information about your network configuration.

```
cumulus@switch$ netshow interface bridge
      Name      Speed      Mtu      Mode      Summary
      --  -----  -----  -----  -----
UP   my_bridge  N/A      1500  Bridge/L2  Untagged: bond0, swp5-6
                                         Root Port: bond0
                                         VlanID: Untagged
```

Bridge Interface MAC Address and MTU

A bridge is a logical interface with a MAC address and an [MTU \(see page 137\)](#) (maximum transmission unit). The bridge MTU is the minimum MTU among all its members. The bridge's MAC address is inherited from the first interface that is added to the bridge as a member. The bridge MAC address remains unchanged until the member interface is removed from the bridge, at which point the bridge will inherit from the next member interface, if any. The bridge can also be assigned an IP address, as discussed later in this section.

Examining MAC Addresses

A bridge forwards frames by looking up the destination MAC address. A bridge learns the source MAC address of a frame when the frame enters the bridge on an interface. After the MAC address is learned, the bridge maintains an age for the MAC entry in the bridge table. The age is refreshed when a frame is seen again with the same source MAC address. When a MAC is not seen for greater than the MAC ageing time, the MAC address is deleted from the bridge table.

The following shows the MAC address table of the example bridge. Notice that the `is_local?` column indicates if the MAC address is the interface's own MAC address (`is_local` is *yes*), or if it is learned on the interface from a packet's source MAC (where `is_local` is *no*):

```
cumulus@switch:~$ sudo brctl showmacs my_bridge
port name mac addr      is local? ageing timer
swp4      06:90:70:22:a6:2e    no        19.47
swp1      12:12:36:43:6f:9d    no        40.50
bond0     2a:95:22:94:d1:f0    no        1.98
swp1      44:38:39:00:12:9b    yes       0.00
swp2      44:38:39:00:12:9c    yes       0.00
swp3      44:38:39:00:12:9d    yes       0.00
swp4      44:38:39:00:12:9e    yes       0.00
bond0     44:38:39:00:12:9f    yes       0.00
swp2      90:e2:ba:2c:b1:94    no        12.84
swp2      a2:84:fe:fc:bf:cd    no        9.43
```

You can use the `bridge fdb` command to display the MAC address table as well:

```
cumulus@switch:~$ bridge fdb show
44:38:39:00:12:9c dev swp2 VLAN 0 master bridge-A permanent
44:38:39:00:12:9b dev swp1 VLAN 0 master bridge-A permanent
44:38:39:00:12:9e dev swp4 VLAN 0 master bridge-B permanent
44:38:39:00:12:9d dev swp3 VLAN 0 master bridge-B permanent
```

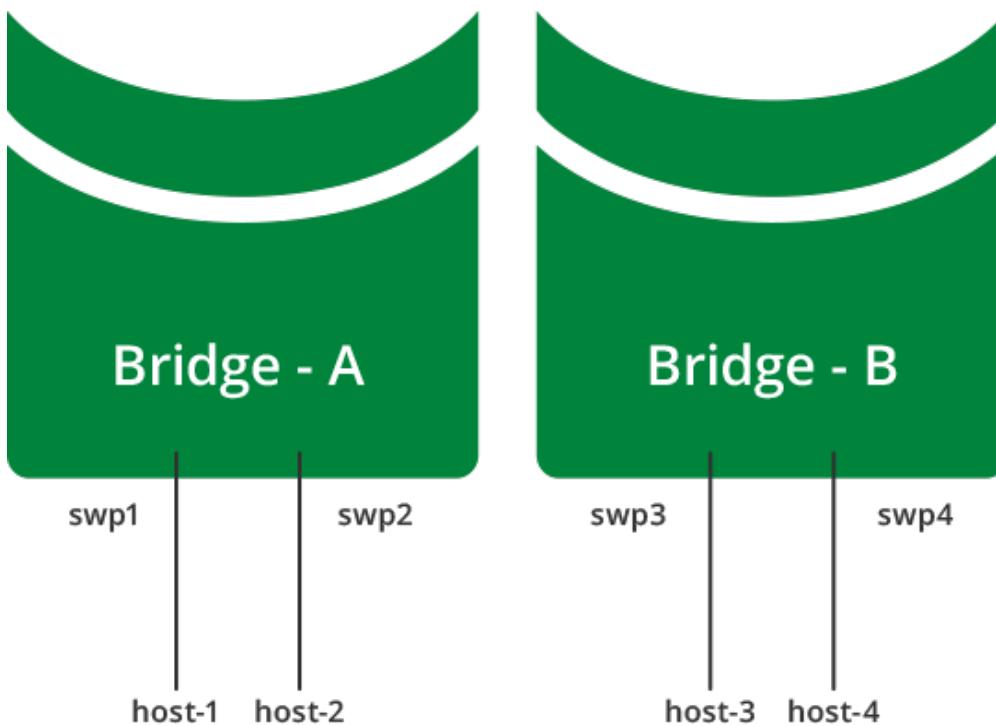


You can clear a MAC address from the table using the `bridge fdb` command:

```
cumulus@switch:~$ sudo bridge fdb del 44:38:39:00:12:9c dev swp2
```

Multiple Bridges

Sometimes it is useful to logically divide a switch into multiple layer 2 domains, so that hosts in one domain can communicate with other hosts in the same domain but not in other domains. You can achieve this by configuring multiple bridges and putting different sets of interfaces in the different bridges. In the following example, host-1 and host-2 are connected to the same bridge (bridge-A), while host-3 and host-4 are connected to another bridge (bridge-B). host-1 and host-2 can communicate with each other, so can host-3 and host-4, but host-1 and host-2 cannot communicate with host-3 and host-4.



To configure multiple bridges, edit `/etc/network/interfaces`:

```

auto bridge-A
iface bridge-A
    bridge-ports swp1 swp2
    bridge-stp on

auto bridge-B
iface bridge-B
    bridge-ports swp3 swp4
    bridge-stp on

```

To bring up the bridges bridge-A and bridge-B, use the `ifreload` command:

```
cumulus@switch:~$ sudo ifreload -a
```

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

```

cumulus@switch:~$ sudo brctl addbr bridge-A

cumulus@switch:~$ sudo brctl addif bridge-A swp1 swp2

cumulus@switch:~$ sudo brctl addbr bridge-B

cumulus@switch:~$ sudo brctl addif bridge-B swp3 swp4

cumulus@switch:~$ sudo for I in {1..4}; do ip link set up dev swp$I; done

cumulus@switch:~$ sudo ip link set up dev bridge-A

cumulus@switch:~$ sudo ip link set up dev bridge-B

cumulus@switch:~$ sudo brctl show
bridge name      bridge id          STP enabled    interfaces
bridge-A        8000.44383900129b    yes           swp1
                                         swp2
bridge-B        8000.44383900129d    yes           swp3
                                         swp4

cumulus@switch:~$ ip link show bridge-A
97: bridge-A: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP mode DEFAULT
    link/ether 70:72:cf:9d:4e:35 brd ff:ff:ff:ff:ff:ff
cumulus@switch:~$ ip link show bridge-B
98: bridge-B: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP mode DEFAULT
    link/ether 70:72:cf:9d:4e:37 brd ff:ff:ff:ff:ff:ff

```

Using netshow to Display the Bridges

netshow is a Cumulus Linux tool for retrieving information about your network configuration.

```

cumulus@switch$ netshow interface bridge
      Name      Speed      Mtu      Mode      Summary
      --  -----  -----  -----  -----
UP   bridge-A    N/A      1500  Bridge/L2  Untagged: swp1-2
                                         Root Port: swp2
                                         VlanID: Untagged
UP   bridge-B    N/A      1500  Bridge/L2  Untagged: swp3-4
                                         Root Port: swp3
                                         VlanID: Untagged

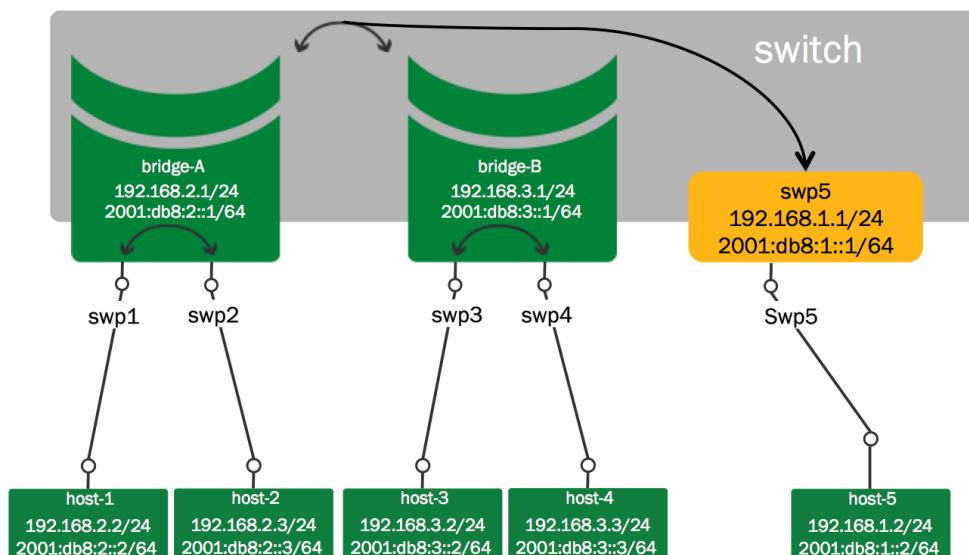
```

Configuring an SVI (Switch VLAN Interface)

A bridge creates a layer 2 forwarding domain for hosts to communicate. A bridge can be assigned an IP address — typically of the same subnet as the hosts that are members of the bridge — and participate in routing topologies. This enables hosts within a bridge to communicate with other hosts outside the bridge through layer 3 routing.



When an interface is added to a bridge, it ceases to function as a router interface, and the IP address on the interface, if any, becomes unreachable.



The configuration for the two bridges example looks like the following:

```

auto swp5
iface swp5
    address 192.168.1.1/24
    address 2001:DB8:1::1/64
auto bridge-A
iface bridge-A
    address 192.168.2.1/24
    address 2001:DB8:2::1/64
    bridge-ports swp1 swp2
    bridge-stp on
auto bridge-B
iface bridge-B
    address 192.168.3.1/24
    address 2001:DB8:3::1/64
    bridge-ports swp3 swp4
    bridge-stp on

```

To bring up swp5 and bridges bridge-A and bridge-B, use the `ifreload` command:

```
cumulus@switch:~$ sudo ifreload -a
```

Showing and Verifying the Bridge Configuration

```
cumulus@switch$ ip addr show bridge-A
106: bridge-A: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP
link/ether 70:72:cf:9d:4e:35 brd ff:ff:ff:ff:ff:ff
inet 192.168.2.1/24 scope global bridge-A
inet6 2001:db8:2::1/64 scope global
valid_lft forever preferred_lft forever
inet6 fe80::7272:cfffe:9d:4e35/64 scope link
valid_lft forever preferred_lft forever
```

```
cumulus@switch$ ip addr show bridge-B
107: bridge-B: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP
link/ether 70:72:cf:9d:4e:37 brd ff:ff:ff:ff:ff:ff
inet 192.168.3.1/24 scope global bridge-B
inet6 2001:db8:3::1/64 scope global
valid_lft forever preferred_lft forever
inet6 fe80::7272:cfffe:9d:4e37/64 scope link
valid_lft forever preferred_lft forever
```

To see all the routes on the switch use the `ip route show` command:

```
cumulus@switch$ ip route show
192.168.1.0/24 dev swp5 proto kernel scope link src 192.168.1.2 dead
192.168.2.0/24 dev bridge-A proto kernel scope link src 192.168.2.1
192.168.3.0/24 dev bridge-B proto kernel scope link src 192.168.3.1
```

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

To add an IP address to a bridge:

```
cumulus@switch:~$ sudo ip addr add 192.0.2.101/24 dev bridge-A
```

```
cumulus@switch:~$ sudo ip addr add 192.0.2.102/24 dev bridge-B
```

Using netshow to Display the SVI

`netshow` is a Cumulus Linux tool for retrieving information about your network configuration.

```
cumulus@switch$ netshow interface bridge
      Name      Speed      Mtu      Mode      Summary
--  -----  -----  -----  -----
----- 
UP  bridge-A  N/A      1500    Bridge/L3  IP: 192.168.2.1/24, 2001:db8:2::1
/64
                                         Untagged: swp1-2
                                         Root Port: swp2
                                         VlanID: Untagged
UP  bridge-B  N/A      1500    Bridge/L3  IP: 192.168.3.1/24, 2001:db8:3::1
/64
                                         Untagged: swp3-4
                                         Root Port: swp3
                                         VlanID: Untagged
```

Using Trunks in Traditional Bridging Mode

The [IEEE standard](#) for trunking is 802.1Q. The 802.1Q specification adds a 4 byte header within the Ethernet frame that identifies the VLAN of which the frame is a member.

802.1Q also identifies an *untagged* frame as belonging to the *native VLAN* (most network devices default their native VLAN to 1). The concept of native, non-native, tagged or untagged has generated confusion due to mixed terminology and vendor-specific implementations. Some clarification is in order:

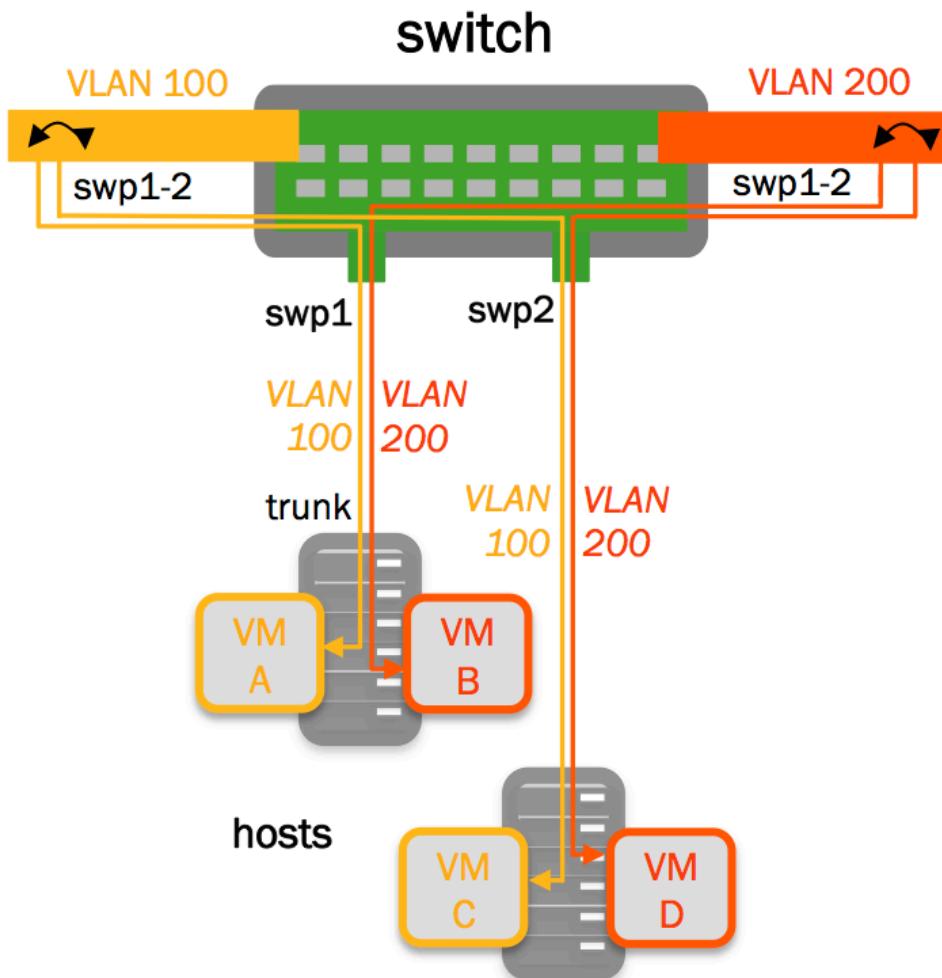
- A *trunk port* is a switch port configured to send and receive 802.1Q tagged frames.
- A switch sending an untagged (bare Ethernet) frame on a trunk port is sending from the native VLAN defined on the trunk port.
- A switch sending a tagged frame on a trunk port is sending to the VLAN identified by the 802.1Q tag.
- A switch receiving an untagged (bare Ethernet) frame on a trunk port places that frame in the native VLAN defined on the trunk port.
- A switch receiving a tagged frame on a trunk port places that frame in the VLAN identified by the 802.1Q tag.

A bridge in traditional mode has no concept of trunks, just tagged or untagged frames. With a trunk of 200 VLANs, there would need to be 199 bridges, each containing a tagged physical interface, and one bridge containing the native untagged VLAN. See the examples below for more information.



The interaction of tagged and un-tagged frames on the same trunk often leads to undesired and unexpected behavior. A switch that uses VLAN 1 for the native VLAN may send frames to a switch that uses VLAN 2 for the native VLAN, thus merging those two VLANs and their spanning tree state.

Trunk Example



Configure the following in `/etc/network/interfaces`:

```
auto br-VLAN100
iface br-VLAN100
    bridge-ports swp1.100 swp2.100
    bridge-stp on
auto br-VLAN200
iface br-VLAN200
    bridge-ports swp1.200 swp2.200
    bridge-stp on
```

To bring up br-VLAN100 and br-VLAN200, use the `ifreload` command:

```
cumulus@switch:~$ sudo ifreload -a
```

Showing and Verifying the Trunk

```
cumulus@switch:~$ brctl show
bridge name bridge id          STP enabled interfaces
br-VLAN100  8000.7072cf9d4e35  yes      swp1.100
                                         swp2.100
br-VLAN200  8000.7072cf9d4e35  yes      swp1.200
                                         swp2.200
```

Using `netshow` to Display the Trunk

`netshow` is a Cumulus Linux tool for retrieving information about your network configuration.

```
cumulus@switch$ netshow interface bridge
      Name      Speed      Mtu      Mode      Summary
      --  -----  -----  -----  -----
UP   br-VLAN100    N/A      1500  Bridge/L2  Tagged: swp1-2
                                         STP: rootSwitch(32768)
                                         VlanID: 100
UP   br-VLAN200    N/A      1500  Bridge/L2  Tagged: swp1-2
                                         STP: rootSwitch(32768)
                                         VlanID: 200
```

Additional Examples

You can find additional examples of VLAN tagging in this chapter (see page 200).

Configuration Files

- `/etc/network/interfaces`
- `/etc/network/interfaces.d/`
- `/etc/network/if-down.d/`
- `/etc/network/if-post-down.d/`
- `/etc/network/if-pre-up.d/`
- `/etc/network/if-up.d/`

Useful Links

- www.linuxfoundation.org/collaborate/workgroups/networking/bridge
- www.linuxfoundation.org/collaborate/workgroups/networking/vlan
- www.linuxjournal.com/article/8172

Caveats and Errata

- The same bridge cannot contain multiple subinterfaces of the **same** port as members. Attempting to apply such a configuration will result in an error.
- In environments where both VLAN-aware and traditional bridges are in use, where a traditional bridge has a subinterface of a bond that is present as a normal interface in a VLAN-aware bridge, when the traditional bridge's bond subinterface is brought down, it flaps the bridge.

VLAN Tagging

This article shows two examples of VLAN tagging (see page), one basic and one more advanced. They both demonstrate the streamlined interface configuration from `ifupdown2`. For more information, see Configuring and Managing Network Interfaces (see page 121).

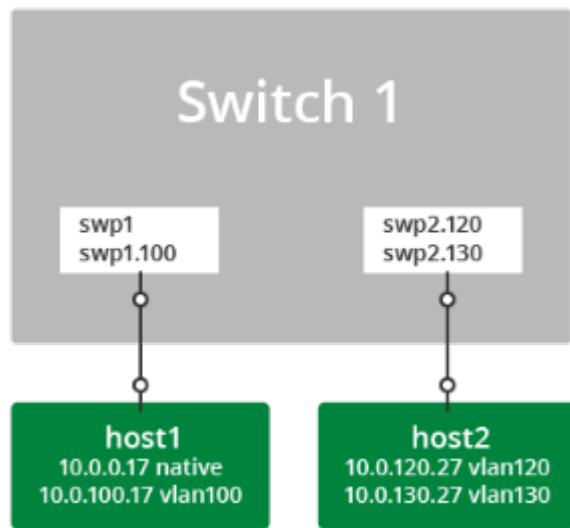
Contents

(Click to expand)

- Contents (see page 200)
- VLAN Tagging, a Basic Example (see page 200)
 - Persistent Configuration (see page 201)
- VLAN Tagging, an Advanced Example (see page 201)
 - Persistent Configuration (see page 202)
 - VLAN Translation (see page 207)

VLAN Tagging, a Basic Example

A simple configuration demonstrating VLAN tagging involves two hosts connected to a switch.



- *host1* connects to *swp1* with both untagged frames and with 802.1Q frames tagged for *vlan100*.
- *host2* connects to *swp2* with 802.1Q frames tagged for *vlan120* and *vlan130*.

Persistent Configuration

To configure the above example persistently, configure `/etc/network/interfaces` like this:

```

# Config for host1

auto swp1
iface swp1

auto swp1.100
iface swp1.100

# Config for host2
# swp2 must exist to create the .1Q subinterfaces, but it is not assigned
# an address

auto swp2
iface swp2

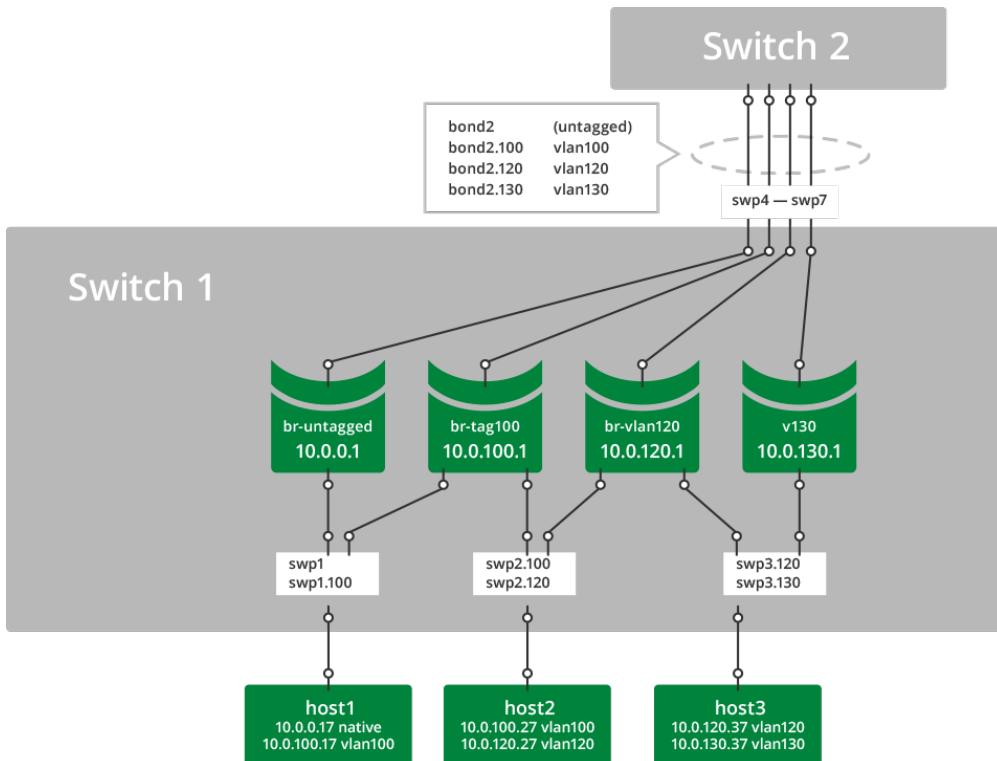
auto swp2.120
iface swp2.120

auto swp2.130
iface swp2.130

```

VLAN Tagging, an Advanced Example

This example of VLAN tagging is more complex, involving three hosts and two switches, with a number of bridges and a bond connecting them all.



- *host1* connects to bridge *br-untagged* with bare Ethernet frames and to bridge *br-tag100* with 802.1q frames tagged for *vlan100*.
- *host2* connects to bridge *br-tag100* with 802.1q frames tagged for *vlan100* and to bridge *br-vlan120* with 802.1q frames tagged for *vlan120*.
- *host3* connects to bridge *br-vlan120* with 802.1q frames tagged for *vlan120* and to bridge *v130* with 802.1q frames tagged for *vlan130*.
- *bond2* carries tagged and untagged frames in this example.

Although not explicitly designated, the bridge member ports function as 802.1Q access ports and *trunk ports*. In the example above, comparing Cumulus Linux with a traditional Cisco device:

- *swp1* is equivalent to a trunk port with untagged and *vlan100*.
- *swp2* is equivalent to a trunk port with *vlan100* and *vlan120*.
- *swp3* is equivalent to a trunk port with *vlan120* and *vlan130*.
- *bond2* is equivalent to an EtherChannel in trunk mode with untagged, *vlan100*, *vlan120*, and *vlan130*.
- Bridges *br-untagged*, *br-tag100*, *br-vlan120*, and *v130* are equivalent to SVIs (switched virtual interfaces).

Persistent Configuration

From /etc/network/interfaces :

```
# Config for host1 -----
```

```

-----  

# swp1 does not need an iface section unless it has a specific setting,  

# it will be picked up as a dependent of swp1.100.  

# And swp1 must exist in the system to create the .1q subinterfaces..  

# but it is not applied to any bridge..or assigned an address.  

auto swp1.100  

iface swp1.100  

# Config for host2  

# swp2 does not need an iface section unless it has a specific setting,  

# it will be picked up as a dependent of swp2.100 and swp2.120.  

# And swp2 must exist in the system to create the .1q subinterfaces..  

# but it is not applied to any bridge..or assigned an address.  

auto swp2.100  

iface swp2.100  

auto swp2.120  

iface swp2.120  

# Config for host3  

# swp3 does not need an iface section unless it has a specific setting,  

# it will be picked up as a dependent of swp3.120 and swp3.130.  

# And swp3 must exist in the system to create the .1q subinterfaces..  

# but it is not applied to any bridge..or assigned an address.  

auto swp3.120  

iface swp3.120  

auto swp3.130  

iface swp3.130  

# Configure the bond -----  

-----  

auto bond2  

iface bond2  

bond-slaves glob swp4-7  

# configure the bridges -----  

-----  

auto br-untagged

```

```
iface br-untagged
    address 10.0.0.1/24
    bridge-ports swp1 bond2
    bridge-stp on

auto br-tag100
iface br-tag100
    address 10.0.100.1/24
    bridge-ports swp1.100 swp2.100 bond2.100
    bridge-stp on

auto br-vlan120
iface br-vlan120
    address 10.0.120.1/24
    bridge-ports swp2.120 swp3.120 bond2.120
    bridge-stp on

auto v130
iface v130
    address 10.0.130.1/24
    bridge-ports swp2.130 swp3.130 bond2.130
    bridge-stp on
```

```
# -----
```

To verify:

```
cumulus@switch:~$ sudo mstptctl showbridge br-tag100
br-tag100 CIST info
  enabled      yes
  bridge id    8.000.44:38:39:00:32:8B
  designated root 8.000.44:38:39:00:32:8B
  regional root 8.000.44:38:39:00:32:8B
  root port     none
  path cost     0          internal path cost  0
  max age       20         bridge max age     20
  forward delay 15         bridge forward delay 15
  tx hold count 6          max hops           20
  hello time    2          ageing time        300
  force protocol version   rstp
  time since topology change 333040s
  topology change count    1
  topology change          no
```

```

topology change port      swp2.100
last topology change port None

cumulus@switch:~$ sudo mstpcctl showportdetail br-tag100 | grep -B 2 state
br-tag100:bond2.100 CIST info
    enabled          yes           role          Designated
    port id         8.003        state          forwarding
--
br-tag100:swp1.100 CIST info
    enabled          yes           role          Designated
    port id         8.001        state          forwarding
--
br-tag100:swp2.100 CIST info
    enabled          yes           role          Designated
    port id         8.002        state          forwarding

cumulus@switch:~$ cat /proc/net/vlan/config
VLAN Dev name      | VLAN ID
Name-Type: VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
bond2.100          | 100  | bond2
bond2.120          | 120  | bond2
bond2.130          | 130  | bond2
swp1.100          | 100  | swp1
swp2.100          | 100  | swp2
swp2.120          | 120  | swp2
swp3.120          | 120  | swp3
swp3.130          | 130  | swp3

cumulus@switch:~$ cat /proc/net/bonding/bond2
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: IEEE 802.3ad Dynamic link aggregation
Transmit Hash Policy: layer3+4 (1)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

802.3ad info
LACP rate: fast
Min links: 0
Aggregator selection policy (ad_select): stable
Active Aggregator Info:
    Aggregator ID: 3

```

```
Number of ports: 4
Actor Key: 33
Partner Key: 33
Partner Mac Address: 44:38:39:00:32:cf

Slave Interface: swp4
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 44:38:39:00:32:8e
Aggregator ID: 3
Slave queue ID: 0

Slave Interface: swp5
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 44:38:39:00:32:8f
Aggregator ID: 3
Slave queue ID: 0

Slave Interface: swp6
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 44:38:39:00:32:90
Aggregator ID: 3
Slave queue ID: 0

Slave Interface: swp7
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 44:38:39:00:32:91
Aggregator ID: 3
Slave queue ID: 0
```



A single bridge cannot contain multiple subinterfaces of the **same** port as members. Attempting to apply such a configuration will result in an error:

```
cumulus@switch:~$ sudo brctl addbr another_bridge
cumulus@switch:~$ sudo brctl addif another_bridge swp9 swp9.100
bridge cannot contain multiple subinterfaces of the same port: swp9,
swp9.100
```

VLAN Translation

By default, Cumulus Linux does not allow VLAN subinterfaces associated with different VLAN IDs to be part of the same bridge. Base interfaces are not explicitly associated with any VLAN IDs and are exempt from this restriction:

```
cumulus@switch:~$ sudo brctl addbr br_mix

cumulus@switch:~$ sudo ip link add link swp10 name swp10.100 type vlan id
100
cumulus@switch:~$ sudo ip link add link swp11 name swp11.200 type vlan id
200

cumulus@switch:~$ sudo brctl addif br_mix swp10.100 swp11.200
can't add swp11.200 to bridge br_mix: Invalid argument
```

In some cases, it may be useful to relax this restriction. For example, two servers may be connected to the switch using VLAN trunks, but the VLAN numbering provisioned on the two servers are not consistent. You can choose to just bridge two VLAN subinterfaces of different VLAN IDs from the servers. You do this by enabling the `sysctl net.bridge.bridge-allow-multiple-vlans`. Packets entering a bridge from a member VLAN subinterface will egress another member VLAN subinterface with the VLAN ID translated.



A bridge in [VLAN-aware mode \(see page 208\)](#) cannot have VLAN translation enabled for it; only bridges configured in traditional mode can utilize VLAN translation.

The following example enables the VLAN translation `sysctl`:

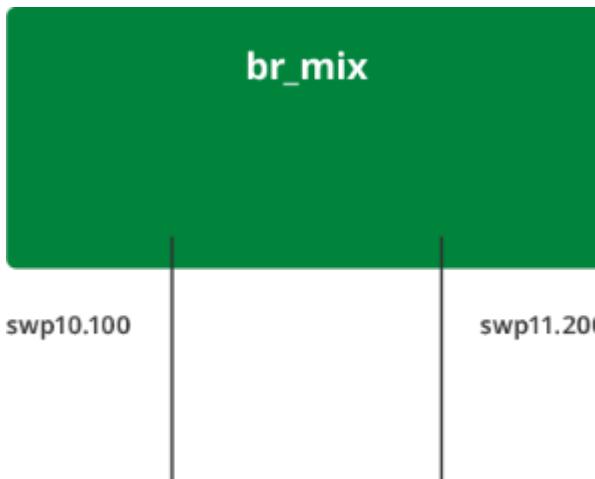
```
cumulus@switch:~$ echo net.bridge.bridge-allow-multiple-vlans = 1 | sudo
tee /etc/sysctl.d/multiple_vlans.conf
net.bridge.bridge-allow-multiple-vlans = 1
cumulus@switch:~$ sudo sysctl -p /etc/sysctl.d/multiple_vlans.conf
net.bridge.bridge-allow-multiple-vlans = 1
```

If the `sysctl` is enabled and you want to disable it, run the above example, setting the `sysctl net.bridge.bridge-allow-multiple-vlans` to 0.

Once the `sysctl` is enabled, ports with different VLAN IDs can be added to the same bridge. In the following example, packets entering the bridge `br_mix` from `swp10.100` will be bridged to `swp11.200` with the VLAN ID translated from 100 to 200:

```
cumulus@switch:~$ sudo brctl addif br_mix swp10.100 swp11.200

cumulus@switch:~$ sudo brctl show br_mix
bridge name      bridge id          STP enabled     interfaces
br_mix           8000.4438390032bd    yes            swp10.100
                                         swp11.200
```



VLAN-aware Bridge Mode for Large-scale Layer 2 Environments

Cumulus Linux bridge driver supports two configuration modes, one that is VLAN-aware, and one that follows a more traditional Linux bridge model.

For traditional Linux bridges, the kernel supports VLANs in the form of VLAN subinterfaces. Enabling bridging on multiple VLANs means configuring a bridge for each VLAN and, for each member port on a bridge, creating one or more VLAN subinterfaces out of that port. This mode poses scalability challenges in terms of configuration size as well as boot time and run time state management, when the number of ports times the number of VLANs becomes large.

The VLAN-aware mode in Cumulus Linux implements a configuration model for large-scale L2 environments, with **one single instance** of Spanning Tree (see page 150). Each physical bridge member port is configured with the list of allowed VLANs as well as its port VLAN ID (either PVID or native VLAN — see below). MAC address learning, filtering and forwarding are *VLAN-aware*. This significantly reduces the configuration size, and eliminates the large overhead of managing the port/VLAN instances as subinterfaces, replacing them with lightweight VLAN bitmaps and state updates.



You can configure both VLAN-aware and traditional mode bridges on the same network in Cumulus Linux; however you should not have more than one VLAN-aware bridge on a given switch. If you are implementing **VXLANs** (see page 322), you **must** use non-aware bridges.

Contents

(Click to expand)

- [Contents \(see page 209\)](#)
- [Defining VLAN-aware Bridge Attributes \(see page 209\)](#)
- [Basic Trunking \(see page 209\)](#)
- [VLAN Filtering/VLAN Pruning \(see page 210\)](#)
- [Untagged/Access Ports \(see page 211\)](#)
 - [Dropping Untagged Frames \(see page 211\)](#)
- [VLAN Layer 3 Addressing/Switch Virtual Interfaces and other VLAN Attributes \(see page 212\)](#)
- [Using the glob Keyword to Configure Multiple Ports in a Range \(see page 213\)](#)
- [Example Configuration with Access Ports and Pruned VLANs \(see page 214\)](#)
- [Example Configuration with Bonds \(see page 214\)](#)
- [Converting a Traditional Bridge to VLAN-aware or Vice Versa \(see page 216\)](#)
- [Caveats and Errata \(see page 216\)](#)

Defining VLAN-aware Bridge Attributes

To configure a VLAN-aware bridge, include the `bridge-vlan-aware` attribute, setting it to `yes`. Name the bridge `bridge` to help ensure it is the only VLAN-aware bridge on the switch. The following attributes are useful for configuring VLAN-aware bridges:

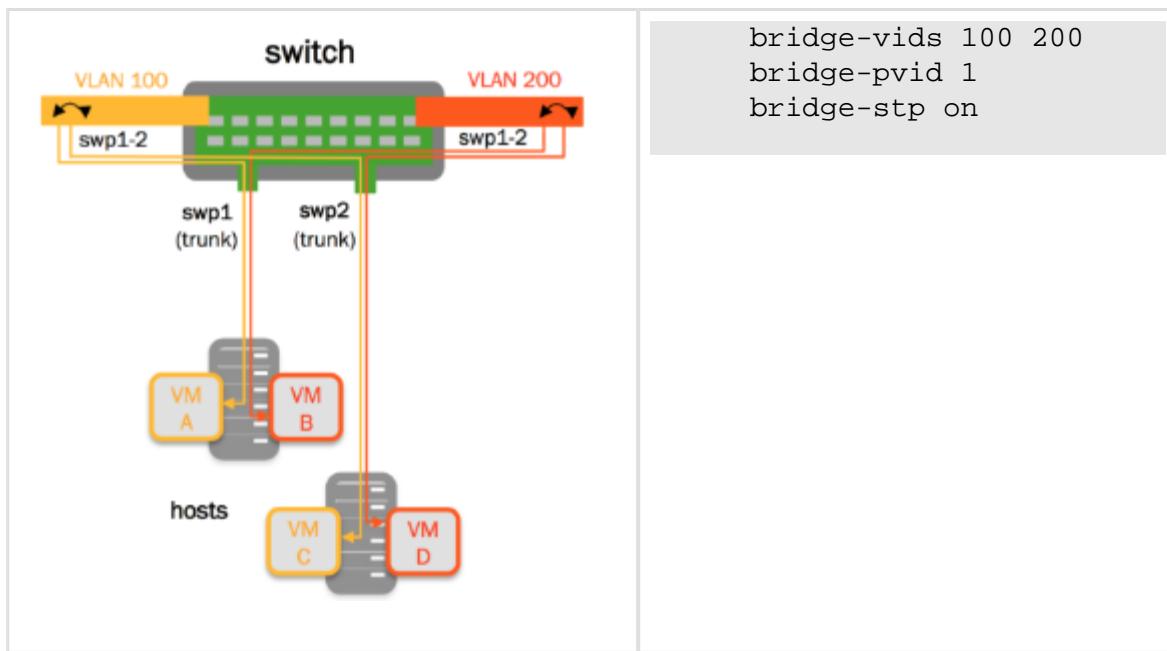
- `bridge-vlan-aware`: Set to `yes` to indicate that the bridge is in VLAN-aware mode.
- `bridge-pvid`: A PVID is the bridge's *Primary VLAN Identifier*. The PVID defaults to 1; specifying the PVID identifies that VLAN as the native VLAN.
- `bridge-vids`: A VID is the *VLAN Identifier*, which declares the VLANs associated with this bridge.
- `bridge-access`: Declares the physical switch port as an *access port*. Access ports ignore all tagged packets; put all untagged packets into the `bridge-pvid`.
- `bridge-allow-untagged`: When set to `no`, it drops any untagged frames for a given switch port.

For a definitive list of bridge attributes, run `ifquery --syntax-help` and look for the entries under **bridge**, **bridgevlan** and **mstpclt**.

Basic Trunking

A basic configuration for a VLAN-aware bridge configured for STP that contains two switch ports looks like this:

```
auto bridge
iface bridge
    bridge-vlan-aware yes
    bridge-ports swp1
    swp2
```



The above configuration actually includes 3 VLANs: the tagged VLANs 100 and 200 and the untagged (native) VLAN of 1.



The `bridge-pvid 1` is implied by default. You do not have to specify `bridge-pvid`. And while it does not hurt the configuration, it helps other users for readability.

The following configurations are identical to each other and the configuration above:

```
auto bridge
iface bridge
    bridge-vlan-
    aware yes
    bridge-ports
    swp1 swp2
    bridge-vids
    1 100 200
    bridge-stp on
```

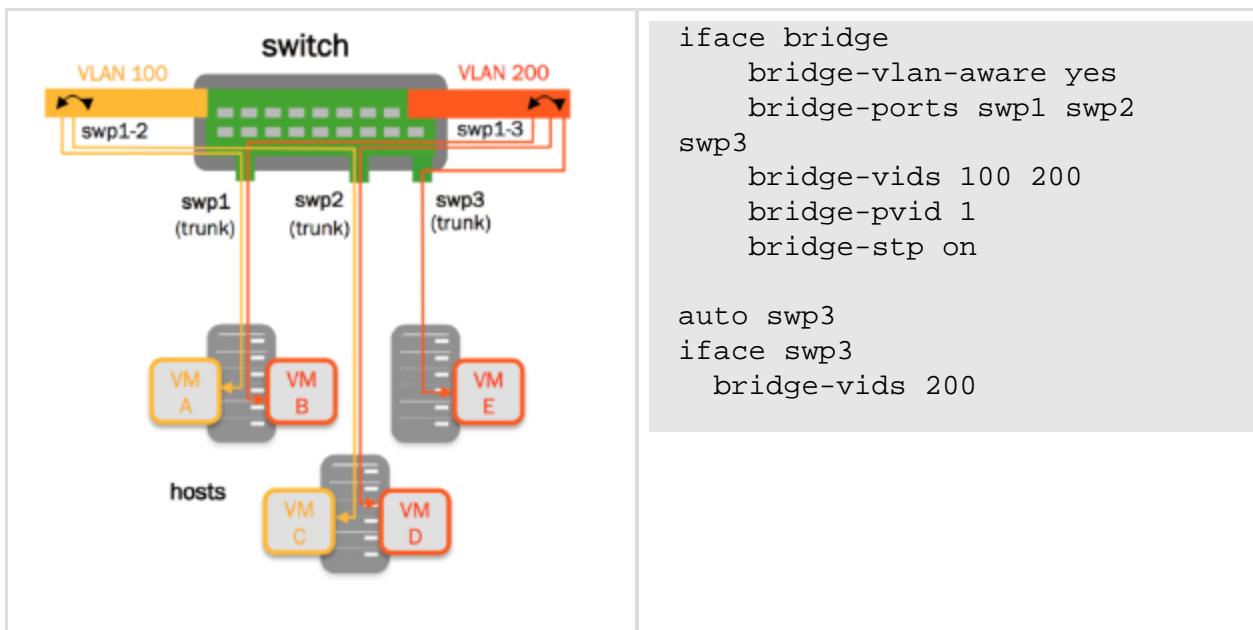
```
auto bridge
iface bridge
    bridge-vlan-
    aware yes
    bridge-ports
    swp1 swp2
    bridge-vids
    1 100 200
    bridge-pvid 1
    bridge-stp on
```

```
auto bridge
iface bridge
    bridge-vlan-
    aware yes
    bridge-ports
    swp1 swp2
    bridge-vids
    100 200
    bridge-stp on
```

VLAN Filtering/VLAN Pruning

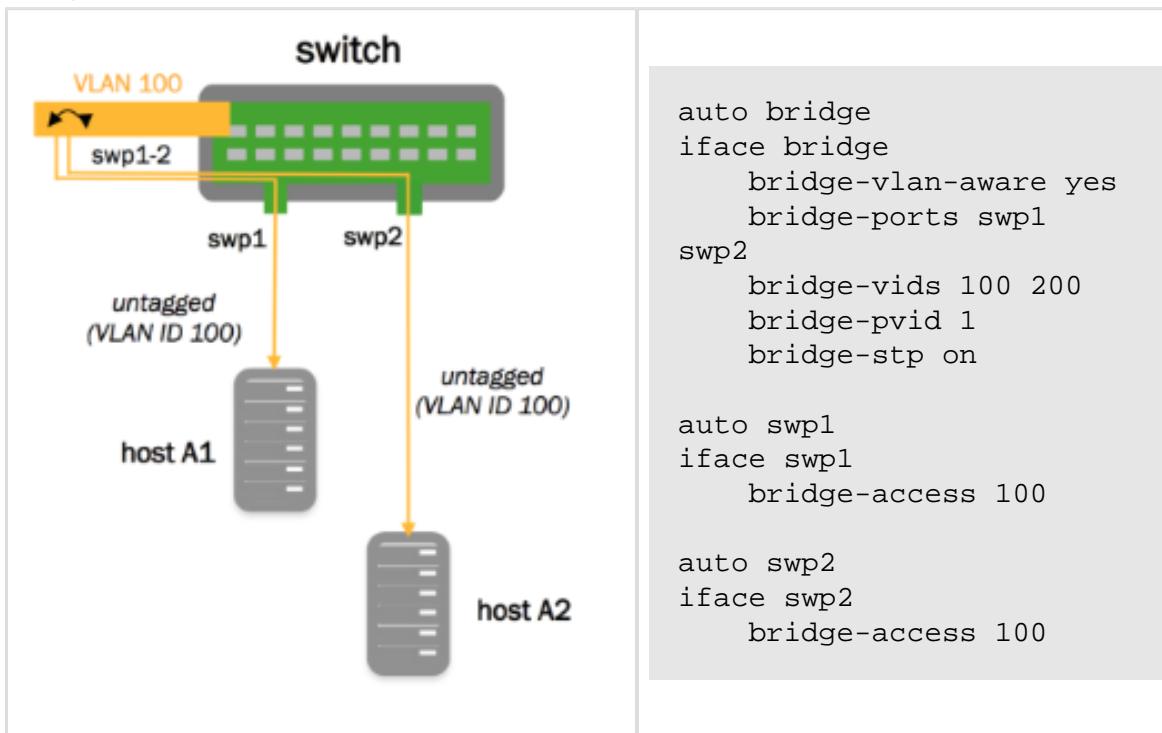
By default, the bridge port inherits the bridge VIDs. A port's configuration can override the bridge VIDs. Do this by specifying port-specific VIDs using the `bridge-vids` attribute.

```
auto bridge
```



Untagged/Access Ports

As described above, access ports ignore all tagged packets. In the configuration below, swp1 and swp2 are configured as access ports. All untagged traffic goes to the specified VLAN, which is VLAN 100 in the example below.



Dropping Untagged Frames

With VLAN-aware bridge mode, it's possible to configure a switch port so it drops any untagged frames. To do this, add `bridge-allow-untagged no` under the switch port stanza in `/etc/network/interfaces`. This leaves the bridge port without a PVID and drops untagged packets.

Consider the following example bridge:

```
auto bridge
iface bridge
    bridge-vlan-aware yes
    bridge-ports swp1 swp9
    bridge-vids 2-100
    bridge-pvid 101
    bridge-stp on
```

Here is the VLAN membership for that configuration:

```
cumulus@switch$ bridge vlan show
portvlan ids
swp1 101 PVID Egress Untagged
2-100

swp9 101 PVID Egress Untagged
2-100

bridge 101
```

To configure swp9 to drop untagged frames, add `bridge-allow-untagged no`:

```
auto swp9
iface swp9
    bridge-allow-untagged no
```

When you check VLAN membership for that port, it shows that there is **no** untagged VLAN.

```
cumulus@switch$ bridge vlan show
portvlan ids
swp1 101 PVID Egress Untagged
2-100

swp9 2-100

bridge 101
```

VLAN Layer 3 Addressing/Switch Virtual Interfaces and other VLAN Attributes

When configuring the VLAN attributes for the bridge, put the attributes in a separate stanza for each VLAN interface: <bridge>.<vlanid>. If you are configuring the SVI for the native VLAN, you must declare the native VLAN in its own stanza and specify its IP address. Specifying the IP address in the bridge stanza itself returns an error.

```

auto bridge.100
iface bridge.100
    address 192.168.10.1/24
    address 2001:db8::1/32
    hwaddress 44:38:39:ff:00:00

# 12 attributes
auto bridge.100
vlan bridge.100
    bridge-igmp-querier-src 172.16.101.1

```



The `vlan` object type in the l2 attributes section above is used to specify layer 2 VLAN attributes only. Currently, the only supported layer 2 VLAN attribute is `bridge-igmp-querier-src`.

However, if your switch is configured for multicast routing, then you do not need to specify `bridge-igmp-querier-src`, as there is no need for a static IGMP querier configuration on the switch. Otherwise, the static IGMP querier configuration helps to probe the hosts to refresh their IGMP reports.

You can specify a range of VLANs as well. For example:

```

auto bridge.[1-2000]
vlan bridge.[1-2000]
    ATTRIBUTE VALUE

```

Using the `glob` Keyword to Configure Multiple Ports in a Range

The `glob` keyword referenced in the `bridge-ports` attribute indicates that swp1 through swp52 are part of the bridge, which is a short cut that saves you from enumerating each port individually:

```

auto bridge
iface bridge
    bridge-vlan-aware yes
    bridge-ports glob swp1-52
    bridge-stp on
    bridge-vids 310 700 707 712 850 910

```

Example Configuration with Access Ports and Pruned VLANs

The following example contains an access port and a switch port that is *pruned*; that is, it only sends and receives traffic tagged to and from a specific set of VLANs declared by the `bridge-vids` attribute. It also contains other switch ports that send and receive traffic from all the defined VLANs.

```
# ports swp3-swp48 are trunk ports which inherit vlans from the
'bridge'
# ie vlans 310,700,707,712,850,910
#
auto bridge
iface bridge
    bridge-vlan-aware yes
    bridge-ports glob swp1-52
    bridge-stp on
    bridge-vids 310 700 707 712 850 910

auto swp1
iface swp1
    mstpctl-portadminedge yes
    mstpctl-bpduguard yes
    bridge-access 310

# The following is a trunk port that is "pruned".
# native vlan is 1, but only .1q tags of 707, 712, 850 are
# sent and received
#
auto swp2
iface swp2
    mstpctl-portadminedge yes
    mstpctl-bpduguard yes
    bridge-vids 707 712 850

# The following port is the trunk uplink and inherits all vlans
# from 'bridge'; bridge assurance is enabled using 'portnetwork'
attribute
auto swp49
iface swp49
    mstpctl-portpathcost 10
    mstpctl-portnetwork yes

# The following port is the trunk uplink and inherits all vlans
# from 'bridge'; bridge assurance is enabled using 'portnetwork'
attribute
auto swp50
iface swp50
    mstpctl-portpathcost 0
    mstpctl-portnetwork yes
```

Example Configuration with Bonds

This configuration demonstrates a VLAN-aware bridge with a large set of bonds. The bond configurations are generated from a [Mako](#) template.

```

#
# vlan-aware bridge with bonds example
#
# uplink1, peerlink and downlink are bond interfaces.
# 'bridge' is a vlan aware bridge with ports uplink1, peerlink
# and downlink (swp2-20).
#
# native vlan is by default 1
#
# 'bridge-vids' attribute is used to declare vlans.
# 'bridge-pvid' attribute is used to specify native vlans if other
than 1
# 'bridge-access' attribute is used to declare access port
#
auto lo
iface lo

auto eth0
iface eth0 inet dhcp

# bond interface
auto uplink1
iface uplink1
    bond-slaves swp32
    bridge-vids 2000-2079

# bond interface
auto peerlink
iface peerlink
    bond-slaves swp30 swp31
    bridge-vids 2000-2079 4094

# bond interface
auto downlink
iface downlink
    bond-slaves swp1
    bridge-vids 2000-2079

#
# Declare vlans for all swp ports
# swp2-20 get vlans from 2004 to 2022.
# The below uses mako templates to generate iface sections
# with vlans for swp ports
#
%for port, vlanid in zip(range(2, 20), range(2004, 2022)) :
    auto swp${port}

```

```

iface swp${port}
  bridge-vids ${vlanid}

%endfor

# svi vlan 4094
auto bridge.4094
iface bridge.4094
  address 11.100.1.252/24

# 12 attributes for vlan 4094
auto bridge.4094
vlan bridge.4094
  bridge-igmp-querier-src 172.16.101.1

#
# vlan-aware bridge
#
auto bridge
iface bridge
  bridge-vlan-aware yes
  bridge-ports uplink1 peerlink downlink glob swp2-20
  bridge-stp on

# svi peerlink vlan
auto peerlink.4094
iface peerlink.4094
  address 192.168.10.1/30
  broadcast 192.168.10.3

```

Converting a Traditional Bridge to VLAN-aware or Vice Versa

You cannot automatically convert a traditional bridge to/from a VLAN-aware bridge simply by changing the configuration in the /etc/network/interfaces file. If you need to change the mode for a bridge, do the following:

1. Delete the traditional mode bridge from the configuration and bring down all its member switch port interfaces.
2. Create a new VLAN-aware bridge, as described above.
3. Bring up the bridge.

These steps assume you are converting a traditional mode bridge to a VLAN-aware one. To do the opposite, delete the VLAN-aware bridge in step 1, and create a new traditional mode bridge in step 2.

Caveats and Errata

- **STP:** Because [Spanning Tree and Rapid Spanning Tree \(see page 150\)](#) (STP) are enabled on a per-bridge basis, VLAN-aware mode essentially supports a single instance of STP across all VLANs. A common practice when using a single STP instance for all VLANs is to define all every VLAN on each switch in the spanning tree instance. `mstpd` continues to be the user space protocol daemon, and Cumulus Linux supports RSTP.

- **IGMP snooping:** IGMP snooping and group membership are supported on a per-VLAN basis, though the IGMP snooping configuration (including enable/disable, mrouter port and so forth) are defined on a per-bridge port basis.
- **VXLANS:** Use the traditional configuration mode for [VXLAN configuration \(see page 322\)](#).
- **Reserved VLAN range:** For hardware data plane internal operations, the switching silicon requires VLANs for every physical port, Linux bridge, and layer 3 subinterface. Cumulus Linux reserves a range of 700 VLANs by default; this range is 3300-3999. In case any of your user-defined VLANs conflict with the default reserved range, you can modify the range, as long as the new range is a contiguous set of VLANs with IDs anywhere between 2 and 4094, and the minimum size of the range is 300 VLANs:

1. Edit `/etc/cumulus/switchd.conf`, uncomment `resv_vlan_range` and specify the new range.
2. Restart `switchd` ([see page 115](#)) (`sudo service switchd restart`) for the new range to take effect.



While restarting `switchd`, all running ports will flap and forwarding will be interrupted ([see page 115](#)).

- **VLAN translation:** A bridge in VLAN-aware mode cannot have VLAN translation enabled for it; only bridges configured in [traditional mode \(see page 187\)](#) can utilize VLAN translation.

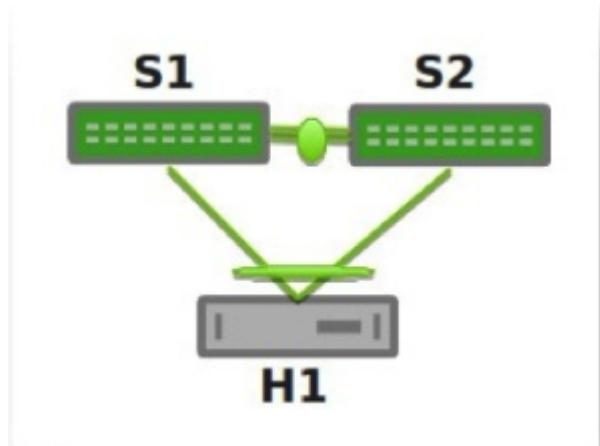
Multi-Chassis Link Aggregation - MLAG

Host HA is a set of L2 and L3 features supporting high availability for hosts, including multi-Chassis Link Aggregation (MLAG) for L2 and [redistribute neighbor](#) (an experimental L3 feature).

Multi-Chassis Link Aggregation, or MLAG, enables a server or switch with a two-port bond (such as a link aggregation group/LAG, EtherChannel, port group, or trunk) to connect those ports to different switches and operate as if they are connected to a single, logical switch. This provides greater redundancy and greater system throughput.

Dual-connected devices can create LACP bonds that contain links to each physical switch. Thus, active-active links from the dual-connected devices are supported even though they are connected to two different physical switches.

A basic setup looks like this:



The two switches, S1 and S2, known as *peer switches*, cooperate so that they appear as a single device to host H1's bond. H1 distributes traffic between the two links to S1 and S2 in any manner that you configure on the host. Similarly, traffic inbound to H1 can traverse S1 or S2 and arrive at H1.

Contents

(Click to expand)

- Contents (see page 218)
- MLAG Requirements (see page 218)
- LACP and Dual-Connectedness (see page 220)
- Understanding Switch Roles (see page 220)
- Configuring MLAG (see page 221)
 - Reserved MAC Address Range (see page 221)
 - Configuring the Host or Switch (see page 221)
 - Configuring the Interfaces (see page 222)
 - Example MLAG Configuration (see page 223)
 - Configuring MLAG with a Traditional Mode Bridge (see page 226)
 - Using the clagd Command Line Interface (see page 227)
- Peer Link Interfaces and the protodown State (see page 227)
 - Specifying a Backup Link (see page 228)
- Monitoring Dual-Connected Peers (see page 229)
- Configuring Layer 3 Routed Uplinks (see page 230)
- IGMP Snooping with MLAG (see page 230)
- Monitoring the Status of the clagd Service (see page 231)
- MLAG Best Practices (see page 232)
 - Understanding MTU in an MLAG Configuration (see page 232)
- STP Interoperability with MLAG (see page 233)
 - Debugging STP with MLAG (see page 233)
 - Best Practices for STP with MLAG (see page 233)
- Troubleshooting MLAG (see page 234)
 - Understanding STP and LACP Behavior when MLAG Fails (see page 234)
- Caveats and Errata (see page 234)
- Configuration Files (see page 234)

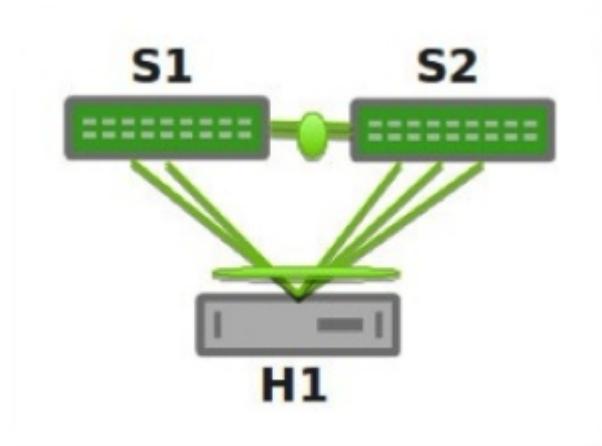
MLAG Requirements

MLAG has these requirements:

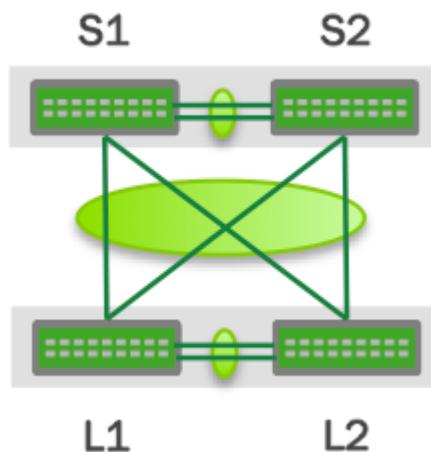
- There must be a direct connection between the two peer switches implementing MLAG (S1 and S2). This is typically a bond for increased reliability and bandwidth.
- There must be only two peer switches in one MLAG configuration, but you can have multiple configurations in a network for *switch-to-switch MLAG* (see below).

- The peer switches implementing MLAG must be running Cumulus Linux version 2.5 or later.
- You must specify a unique `c1ag-id` for every dual-connected bond on each peer switch; the value must be between 1 and 65535 and must be the same on both peer switches in order for the bond to be considered *dual-connected*.
- The dual-connected devices (hosts or switches) must use LACP (IEEE 802.3ad/802.1ax) to form the bond. The peer switches must also use LACP.

More elaborate configurations are also possible. The number of links between the host and the switches can be greater than two, and does not have to be symmetrical:



Additionally, since S1 and S2 appear as a single switch to other bonding devices, pairs of MLAG switches can also be connected to each other in a switch-to-switch MLAG setup:

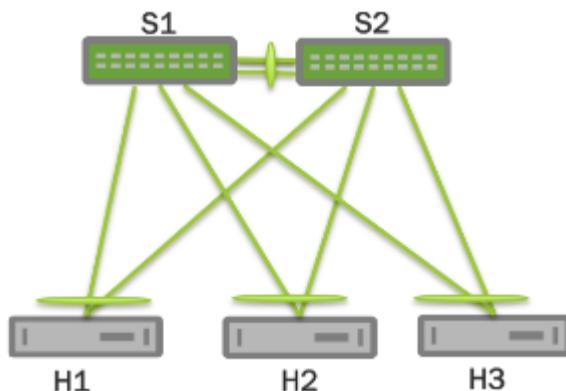


In this case, L1 and L2 are also MLAG peer switches, and thus present a two-port bond from a single logical system to S1 and S2. S1 and S2 do the same as far as L1 and L2 are concerned. For a switch-to-switch MLAG configuration, each switch pair must have a unique system MAC address. In the above example, switches L1 and L2 each have the same system MAC address configured. Switch pair S1 and S2 each have the same system MAC address configured; however, it is a different system MAC address than the one used by the switch pair L1 and L2.

LACP and Dual-Connectedness

In order for MLAG to operate correctly, the peer switches must know which links are *dual-connected*, or are connected to the same host or switch. To do this, specify a `c1ag-id` for every dual-connected bond on each peer switch; the `c1ag-id` must be the same for the corresponding bonds on both peer switches. [Link Aggregation Control Protocol \(LACP\)](#), the IEEE standard protocol for managing bonds, is used for verifying dual-connectedness. LACP runs on the dual-connected device and on each of the peer switches. On the dual-connected device, the only configuration requirement is to create a bond that will be managed by LACP.

On each of the peer switches the links connected to the dual-connected host or switch must be placed in the bond. This is true even if the links are a single port on each peer switch, where each port is placed into a bond, as shown below:



All of the dual-connected bonds on the peer switches have their system ID set to the MLAG system ID. Therefore, from the point of view of the hosts, each of the links in its bond is connected to the same system, and so the host will use both links.

Each peer switch periodically makes a list of the LACP partner MAC addresses of all of their bonds and sends that list to its peer (using the `c1agd` service; see below). The LACP partner MAC address is the MAC address of the system at the other end of a bond, which in the figure above would be hosts H1, H2 and H3. When a switch receives this list from its peer, it compares the list to the LACP partner MAC addresses on its switch. If any matches are found and the `c1ag-id` for those bonds match, then that bond is a dual-connected bond. You can also find the LACP partner MAC address in the `/sys/class/net/<bondname>/bonding/ad_partner_mac sysfs` file for each bond.

Understanding Switch Roles

Each MLAG-enabled switch in the pair has a role. When the peering relationship is established between the two switches, one switch will be in *primary* role, and the other one will be in *secondary* role. When an MLAG-enabled switch is in the secondary role, it does not send STP BPDUs on dual-connected links; it only sends BPDUs on single-connected links. The switch in the primary role sends STP BPDUs on all single- and dual-connected links.

Send BPDUs	Primary	Secondary
Single-connected links	Yes	Yes
Dual-connected links	Yes	No

By default, the role is determined by comparing the MAC addresses of the two sides of the peering link; the switch with the lower MAC address assumes the primary role. You can override this by setting the priority configuration, either by specifying the `c1agd-priority` option in `/etc/network/interfaces`, or by using `c1agctl`. The switch with the lower priority value is given the primary role; the default value is 32768, and the range is 0 to 65535. Read the `c1agd(8)` and `c1agctl(8)` man pages for more information.

When the `c1agd` service is exited during switch reboot or the service is stopped in the primary switch, the peer switch that is in the secondary role will become primary. If the primary switch goes down without stopping the `c1agd` service for any reason or the peer link goes down, the secondary switch will **not** change its role. In case the peer switch is determined to be not alive, the switch in the secondary role will roll back the LACP system ID to be the bond interface MAC address instead of the `c1agd-sys-mac` and the switch in primary role uses the `c1agd-sys-mac` as the LACP system ID on the bonds.

Configuring MLAG

Configuring MLAG involves:

- On the dual-connected devices, create a bond that uses LACP.
- On each peer switch, configure the interfaces, including bonds, VLANs, bridges and peer links.



MLAG synchronizes the dynamic state between the two peer switches, but it does not synchronize the switch configurations. After modifying the configuration of one peer switch, you must make the same changes to the configuration on the other peer switch. This applies to all configuration changes, including:

- Port configuration: For example, VLAN membership, [MTU \(see page 232\)](#), and bonding parameters.
- Bridge configuration: For example, spanning tree parameters or bridge properties.
- Static address entries: For example, static FDB entries and static IGMP entries.
- QoS configuration: For example, ACL entries.

You can verify the configuration of VLAN membership using the `c1agctl -v verifyvlans` command.

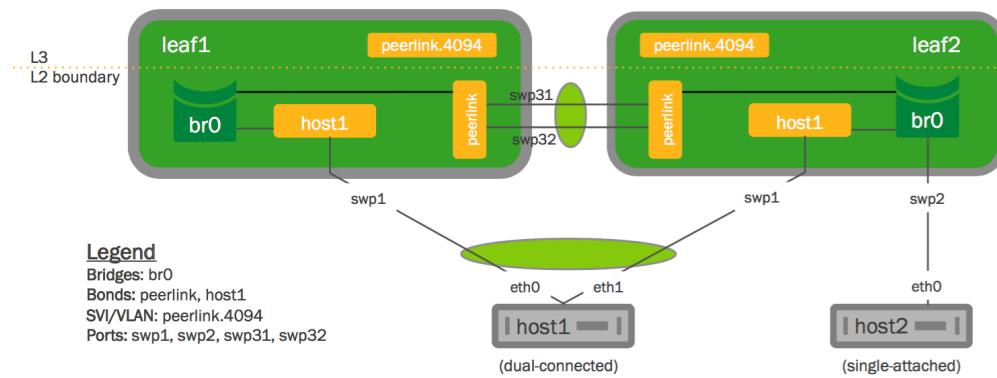
Reserved MAC Address Range

In order to prevent MAC address conflicts with other interfaces in the same bridged network, Cumulus Networks has [reserved a range of MAC addresses](#) specifically to use with MLAG. This range of MAC addresses is 44:38:39:ff:00:00 to 44:38:39:ff:ff:ff.

Cumulus Networks recommends you use this range of MAC addresses when configuring MLAG.

Configuring the Host or Switch

On your dual-connected device, create a bond that uses LACP. The method you use varies with the type of device you are configuring. The following image is a basic MLAG configuration, showing all the essential elements; a more detailed two-leaf/two-spine configuration is [below \(see page \)](#).



Configuring the Interfaces

Every interface that connects to the MLAG pair from a dual-connected device should be placed into a [bond](#) ([see page 184](#)), even if the bond contains only a single link on a single physical switch (since the MLAG pair contains two or more links). Layer 2 data travels over this bond. In the examples throughout this chapter, *peerlink* is the name of the bond.

Single-attached hosts, also known as *orphan ports*, can be just a member of the bridge.

Additionally, the fast mode of LACP should be configured on the bond to allow more timely updates of the LACP state. These bonds will then be placed in a bridge, which will include the peer link between the switches.

In order to enable communication between the `clagd` services on the peer switches, you should choose an unused VLAN (also known as a *switched virtual interface* or *SVI* here) and assign an unrouteable link-local address to give the peer switches layer 3 connectivity between each other. To ensure that the VLAN is completely independent of the bridge and spanning tree forwarding decisions, configure the VLAN as a VLAN subinterface on the peer link bond rather than the VLAN-aware bridge. Cumulus Networks recommends you use 4094 for the peer link VLAN (*peerlink.4094* below) if possible. In addition, to avoid issues with STP, make sure you include untagged traffic on the peer link.

You can also specify a backup interface, which is any layer 3 backup interface for your peer links in the event that the peer link goes down. [See below \(see page 228\)](#) for more information about the backup link.

For example, if *peerlink* is the inter-chassis bond, and VLAN 4094 is the peer link VLAN, configure *peerlink.4094* using:

```
auto peerlink.4094
iface peerlink.4094
  address 169.254.1.1/30
  clagd-enable yes
  clagd-peer-ip 169.254.1.2
  clagd-backup-ip 10.0.1.50
  clagd-sys-mac 44:38:39:FF:40:94
```

Then run `ifup` on the *peerlink* VLAN interface. In this example, the command would be `sudo ifup peerlink.4094`.

There is no need to add VLAN 4094 to the bridge VLAN list, as it is unnecessary there.



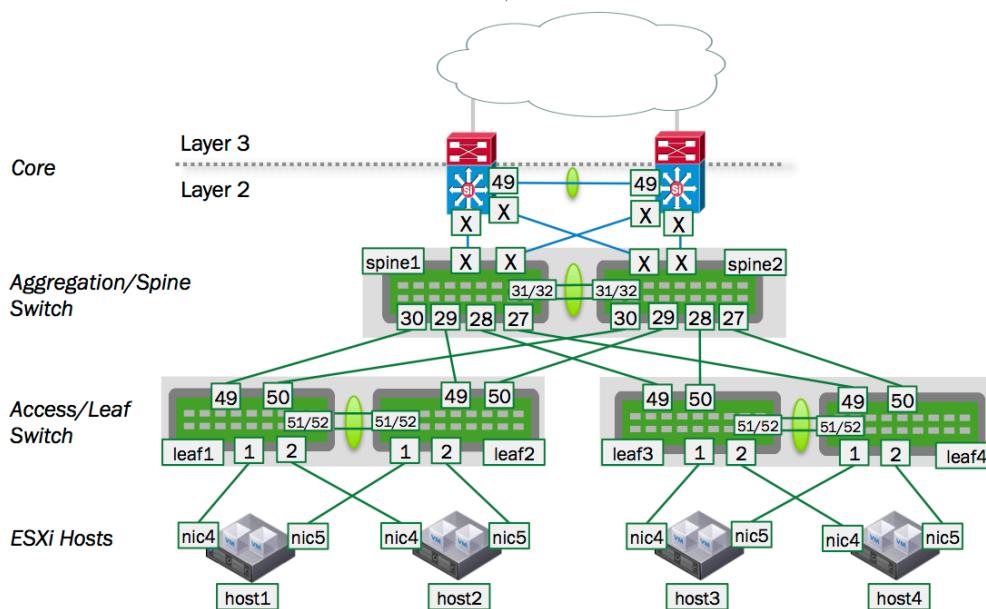
Keep in mind that when you change the MLAG configuration in the `interfaces` file, the changes take effect when you bring the peerlink interface up with `ifup`. Do **not** use `service clagd restart` to apply the new configuration.



Do not use 169.254.0.1 as the MLAG peerlink IP address, as Cumulus Linux uses this address exclusively for BGP unnumbered (see page 377) interfaces.

Example MLAG Configuration

An example configuration is included below. It configures two bonds for MLAG, each with a single port, a peer link that is a bond with two member ports, and three VLANs on each port. You store the configuration in `/etc/network/interfaces` on each peer switch.



Configuring these interfaces uses syntax from `ifupdown2` and the [VLAN-aware bridge driver mode](#) (see page 208). The bridges use these Cumulus Linux-specific keywords:

- `bridge-vids`, which defines the allowed list of tagged 802.1q VLAN IDs for all bridge member interfaces. You can specify non-contiguous ranges with a space-separated list, like `bridge-vids 100-200 300 400-500`.
- `bridge-pvid`, which defines the untagged VLAN ID for each port. This is commonly referred to as the *native VLAN*.

The bridge configurations below indicate that each bond carries tagged frames on VLANs 1000 to 3000 but untagged frames on VLAN 1. Also, take note on how you configure the VLAN subinterface used for `clagd` communication (`peerlink.4094` in the sample configuration below).



At minimum, this VLAN subinterface should not be in your Layer 2 domain, and you should give it a very high VLAN ID (up to 4094). Read more about the [range of VLAN IDs you can use](#) (see page 377).

The configuration for the spines should look like the following (note that the `clag-id` and `clagd-sys-mac` must be the same for the corresponding bonds on spine1 and spine2):

spine1

```

# The loopback network
interface auto lo
iface lo
inet loopback

# The primary network
interface
auto eth0
iface eth0
  address 10.0.0.1
  netmask 255.255.255.0

auto peerlink
iface peerlink
  bond-slaves swp31 swp32

auto peerlink.4094
iface peerlink.4094
  address 169.254.255.1
  netmask 255.255.255.0
  clagd-priority 4096
  clagd-peer-ip 169.254.255.2
  clagd-backup-ip 10.0.0.2
  clagd-sys-mac 44:38:39:ff:00:01

# ToR pair #1
auto downlink1
iface downlink1
  bond-slaves swp29 swp30
  clag-id 1

# ToR pair #2
auto downlink2
iface downlink2
  bond-slaves swp27 swp28
  clag-id 2

auto br
iface br
  bridge-vlan-aware yes
  bridge-ports uplinkA
  peerlink downlink1 downlink2
  bridge-stp on

```

spine2

```

# The loopback network
interface auto lo
iface lo
inet loopback

# The primary network
interface
auto eth0
iface eth0
  address 10.0.0.2
  netmask 255.255.255.0

auto peerlink
iface peerlink
  bond-slaves swp31 swp32

auto peerlink.4094
iface peerlink.4094
  address 169.254.255.2
  netmask 255.255.255.0
  clagd-priority 8192
  clagd-peer-ip 169.254.255.1
  clagd-backup-ip 10.0.0.1
  clagd-sys-mac 44:38:39:ff:00:01

# ToR pair #1
auto downlink1
iface downlink1
  bond-slaves swp29 swp30
  clag-id 1

# ToR pair #2
auto downlink2
iface downlink2
  bond-slaves swp27 swp28
  clag-id 2

auto br
iface br
  bridge-vlan-aware yes
  bridge-ports uplinkA
  peerlink downlink1 downlink2
  bridge-stp on

```

```
bridge-vids 1000-2999
bridge-pvid 1
bridge-mcsnoop 1
```

```
bridge-vids 1000-2999
bridge-pvid 1
bridge-mcsnoop 1
```

Here is an example configuration file for the switches leaf1 and leaf2. Note that the `clag-id` and `clagd-sys-mac` must be the same for the corresponding bonds on leaf1 and leaf2:

leaf1

```
# The loopback network
interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0
    address 10.0.0.3
    netmask 255.255.255.0

auto spine1-2
iface spine1-2
    bond-slaves swp49 swp50
    clag-id 1

auto peerlink
iface peerlink
    bond-slaves swp51 swp52

auto peerlink.4094
iface peerlink.4094
    address 169.254.255.3
    netmask 255.255.255.0
    clagd-priority 4096
    clagd-peer-ip 169.254.255.4
    clagd-backup-ip 10.0.0.4
    clagd-sys-mac 44:38:39:ff:01:02

auto host1
iface host1
    bond-slaves swp1
    clag-id 2
    mstptctl-portadmindedge yes
    mstptctl-bpduguard yes

auto host2
```

leaf2

```
# The loopback network
interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0
    address 10.0.0.4
    netmask 255.255.255.0

auto spine1-2
iface spine1-2
    bond-slaves swp49 swp50
    clag-id 1

auto peerlink
iface peerlink
    bond-slaves swp51 swp52

auto peerlink.4094
iface peerlink.4094
    address 169.254.255.4
    netmask 255.255.255.0
    clagd-priority 8192
    clagd-peer-ip 169.254.255.3
    clagd-backup-ip 10.0.0.3
    clagd-sys-mac 44:38:39:ff:01:02

auto host1
iface host1
    bond-slaves swp1
    clag-id 2
    mstptctl-portadmindedge yes
    mstptctl-bpduguard yes

auto host2
```

```

iface host2
    bond-slaves swp2
    clag-id 3
    mstptctl-portadminedge yes
    mstptctl-bpduguard yes

auto br0
iface br0
    bridge-vlan-aware yes
    bridge-ports spinel-2
peerlink host1 host2
    bridge-stp on
    bridge-vids 1000-2999
    bridge-pvid 1

```

```

iface host2
    bond-slaves swp2
    clag-id 3
    mstptctl-portadminedge yes
    mstptctl-bpduguard yes

auto br0
iface br0
    bridge-vlan-aware yes
    bridge-ports spinel-2
peerlink host1 host2
    bridge-stp on
    bridge-vids 1000-2999
    bridge-pvid 1

```

The configuration is almost identical, except for the IP addresses used for managing the `clagd` service.



In the configurations above, the `clagd-peer-ip` and `clagd-sys-mac` parameters are mandatory, while the rest are optional. When mandatory `clagd` commands are present under a peer link subinterface, by default `clagd-enable` is treated as `yes`; to disable `clagd` on the subinterface, set `clagd-enable` to `no`. Use `clagd-priority` to set the role of the MLAG peer switch to primary or secondary. Each peer switch in an MLAG pair must have the same `clagd-sys-mac` setting. Each `clagd-sys-mac` setting should be unique to each MLAG pair in the network. For more details refer to `man clagd`.

Configuring MLAG with a Traditional Mode Bridge

It's possible to configure MLAG with a bridge in [traditional mode](#) (see page 187) instead of [VLAN-aware mode](#) (see page 208). In order to do so, the peer link and all dual-connected links must be configured as [untagged/native](#) (see page 197) ports on a bridge (note the absence of any VLANs in the `bridge-ports` line and the lack of the `bridge-vlan-aware` parameter below):

```

auto br
iface br
    bridge-ports peerlink spinel-2 host1 host2

```

Because you can have multiple bridges in traditional mode, you can create more than one bridge on the switch, in case you need to use tagged VLANs, as the following example shows:

```

#native vlan (default vlan1)
auto bridge
iface bridge
    bridge-ports peerlink host1 host2 host3

```

```
bridge-stp on

# also can configure additional tagged bridges
auto bridge1000
iface bridge1000
    bridge-ports peerlink.1000 host1.1000 host2.1000 host3.1000
    bridge-stp on
```



For a deeper comparison of traditional versus VLAN-aware bridge modes, read this [knowledge base article](#).

Using the clagd Command Line Interface

A command line utility called `clagctl` is available for interacting with a running `clagd` service to get status or alter operational behavior. For detailed explanation of the utility, please refer to the `clagctl(8)` man page. The following is a sample output of the MLAG operational status displayed by the utility:

```
cumulus@switch$ clagctl
The peer is alive
    Our Priority, ID, and Role: 8192 00:e0:ec:26:50:89 primary
    Peer Priority, ID, and Role: 8192 00:e0:ec:27:49:f6 secondary
        Peer Interface and IP: peerlink.4094 169.254.255.2
        System MAC: 44:38:39:ff:00:01

        Dual Attached Ports
Our Interface      Peer Interface      CLAG Id
-----            -----
downlink1         downlink1          1
downlink2         downlink2          2
```

Peer Link Interfaces and the protodown State

In addition to the standard UP and DOWN administrative states, an interface that is a member of an MLAG bond can also be in a `protodown` state. When MLAG detects a problem that could result in connectivity issues such as traffic black-holing or a network meltdown if the link carrier was left in an UP state, it can put that interface into `protodown` state. Such connectivity issues include:

- When the peer link goes down but the peer switch is up (that is, the backup link is active).
- When the bond is configured with an MLAG ID, but the `clagd` service is not running (whether it was deliberately stopped or simply died).
- When an MLAG-enabled node is booted or rebooted, the MLAG bonds are placed in a `protodown` state until the node establishes a connection to its peer switch, or five minutes have elapsed.

When an interface goes into a `protodown` state, it results in a local OPER DOWN (carrier down) on the interface. As of Cumulus Linux 2.5.5, the `protodown` state can be manipulated with the `ip link set` command. Given its use in preventing network meltdowns, manually manipulating `protodown` is not recommended outside the scope of interaction with the Cumulus Networks support team.

The following `ip link show` command output shows an interface in `protodown` state. Notice that the link carrier is down (NO-CARRIER):

```
cumulus@switch:~$ ip link show swp1
3: swp1: <NO-CARRIER,BROADCAST,MULTICAST,SLAVE,UP> mtu 1500 qdisc pfifo_fast
    master host-bond1 state DOWN mode DEFAULT qlen 500 protodown on
      link/ether 44:38:39:00:69:84 brd ff:ff:ff:ff:ff:ff
```

Specifying a Backup Link

You can specify a backup link for your peer links in the event that the peer link goes down. When this happens, the `clagd` service uses the backup link to check the health of the peer switch. To configure this, edit `/etc/network/interfaces` and add `clagd-backup-ip <ADDRESS>` to the peer link configuration. Here's an example:

```
auto peerlink.4094
iface peerlink.4094
  address 169.254.255.1
  netmask 255.255.255.0
  clagd-enable yes
  clagd-priority 8192
  clagd-peer-ip 169.254.255.2
  clagd-backup-ip 10.0.1.50
  clagd-sys-mac 44:38:39:ff:00:01
  clagd-args --priority 1000
```



The backup IP address must be different than the peer link IP address (`clagd-peer-ip` above). It must be reachable by a route that doesn't use the peer link and it must be in the same network namespace as the peer link IP address.

Cumulus Networks recommends you use the switch's management IP address for this purpose.

You can also specify the backup UDP port. The port defaults to 5342, but you can configure it as an argument in `clagd-args` using `--backupPort <PORT>`.

```
auto peerlink.4094
iface peerlink.4094
  address 169.254.255.1
```

```
netmask 255.255.255.0
clagd-enable yes
clagd-priority 8192
clagd-peer-ip 169.254.255.2
clagd-backup-ip 10.0.1.50
clagd-sys-mac 44:38:39:ff:00:01
clagd-args --backupPort 5400
```

You can see the backup IP address if you run `clagctl`:

```
cumulus@switch$ clagctl
The peer is alive
    Our Priority, ID, and Role: 8192 00:e0:ec:26:50:89 primary
    Peer Priority, ID, and Role: 8192 00:e0:ec:27:49:f6 secondary
        Peer Interface and IP: peerlink.4094 169.254.255.2
            Backup IP: 10.0.1.50
            System MAC: 44:38:39:ff:00:01

        Dual Attached Ports
Our Interface      Peer Interface      CLAG Id
-----            -----
        downlink1      downlink1          1
        downlink2      downlink2          2
```

Monitoring Dual-Connected Peers

Upon receipt of a valid message from its peer, the switch knows that `clagd` is alive and executing on that peer. This causes `clagd` to change the system ID of each bond that was assigned a `clag-id` from the default value (the MAC address of the bond) to the system ID assigned to both peer switches. This makes the hosts connected to each switch act as if they are connected to the same system so that they will use all ports within their bond. Additionally, `clagd` determines which bonds are dual-connected and modifies the forwarding and learning behavior to accommodate these dual-connected bonds.

If the peer does not receive any messages for three update intervals, then that peer switch is assumed to no longer be acting as an MLAG peer. In this case, the switch reverts all configuration changes so that it operates as a standard non-MLAG switch. This includes removing all statically assigned MAC addresses, clearing the egress forwarding mask, and allowing addresses to move from any port to the peer port. Once a message is again received from the peer, MLAG operation starts again as described earlier. You can configure a custom timeout setting by adding `--peerTimeout <VALUE>` to `clagd-args` in `/etc/network/interfaces`.

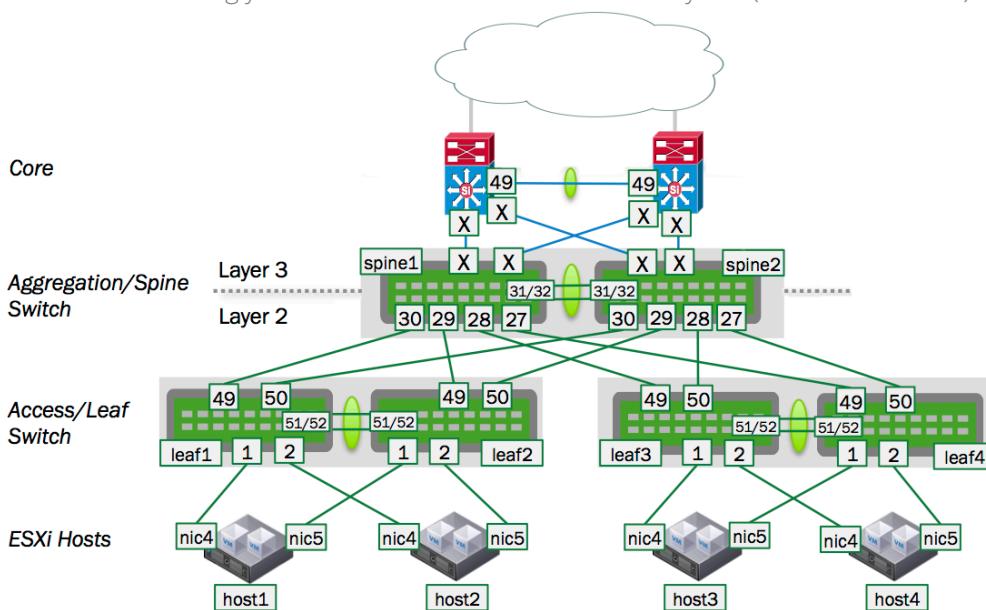
Once bonds are identified as dual-connected, `clagd` sends more information to the peer switch for those bonds. The MAC addresses (and VLANs) that have been dynamically learned on those ports are sent along with the LACP partner MAC address for each bond. When a switch receives MAC address information from its peer, it adds MAC address entries on the corresponding ports. As the switch learns and ages out MAC

addresses, it informs the peer switch of these changes to its MAC address table so that the peer can keep its table synchronized. Periodically, at 45% of the bridge ageing time, a switch will send its entire MAC address table to the peer, so that peer switch can verify that its MAC address table is properly synchronized.

The switch sends an update frequency value in the messages to its peer, which tells `c1agd` how often the peer will send these messages. You can configure a different frequency by adding `--lacpPoll <SECONDS>` to `c1agd-args` in `/etc/network/interfaces`.

Configuring Layer 3 Routed Uplinks

In this scenario, the spine switches connect at layer 3, as shown in the image below. Alternatively, the spine switches can be singly connected to each core switch at layer 3 (not shown below).



In this design, the spine switches route traffic between the server hosts in the layer 2 domains and the core. The servers (host1 - host4) each have a layer 2 connection up to the spine layer where the default gateway for the host subnets resides. However, since the spine switches act as gateway devices communicate at layer 3, you need to configure a protocol such as [VRR \(see page 240\)](#) (Virtual Router Redundancy) between the spine switch pair to support active/active forwarding.

Then, to connect the spine switches to the core switches, you need to determine whether the routing is static or dynamic. If it's dynamic, you must choose which protocol — [OSPF \(see page 358\)](#) or [BGP \(see page 372\)](#) — to use. When enabling a routing protocol in an MLAG environment it is also necessary to manage the uplinks, because by default MLAG is not aware of layer 3 uplink interfaces. In the event of a peerlink failure MLAG does not remove static routes or bring down a BGP or OSPF adjacency unless a separate link state daemon such as `ifplugged` is used.

IGMP Snooping with MLAG

IGMP snooping processes IGMP reports received on a bridge port in a bridge to identify hosts that are configured to receive multicast traffic destined to that group. An IGMP query message received on a port is used to identify the port that is connected to a router and configured to receive multicast traffic.

IGMP snooping is enabled by default on the bridge. IGMP snooping multicast database entries and router port entries are synced to the peer MLAG switch. If there is no multicast router in the VLAN, the IGMP querier can be configured on the switch to generate IGMP query messages by adding a configuration like the following to `/etc/network/interfaces`:

```
auto br.100
vlan br.100
    #igmp snooping is enabled by default, but is shown here for completeness
    bridge-mcsnoop 1
    # If you need to specify the querier IP address
    bridge-igmp-querier-source 123.1.1.1
```

To display multicast group and router port information, use the `bridge -d mdb show` command:

```
cumulus@switch:~# sudo bridge -d mdb show
dev br port bond0 vlan 100 grp 234.1.1.1 temp
router ports on br: bond0
```

Runtime Configuration (Advanced)

```
cumulus@switch:~# sudo brctl setmcqv4src br 100 123.1.1.1
cumulus@switch:~# sudo brctl setmcquerier br 1
cumulus@switch:~# sudo brctl showmcqv4src br

vlan          querier address
100           123.1.1.1
```

Monitoring the Status of the clagd Service

Due to the critical nature of the `clagd` service, an external process, called `jdo0`, continuously monitors the status of `clagd`. If the `clagd` service dies or becomes unresponsive for any reason, the `jdo0` process will get `clagd` up and running again. This monitoring is automatically configured and enabled as long as `clagd` is enabled (that is, `clagd-peer-ip` and `clagd-sys-mac` are configured in `/etc/network/interfaces`) and `clagd` been started. When `clagd` is explicitly stopped, for example with the `service clagd stop` command, monitoring of `clagd` is also stopped.

The `jdo0` process checks two things to make sure the `clagd` service is operating properly:

- The result of the `service clagd status` command. If the command returns that `clagd` is running, or that `clagd` is not configured to run, then `jdo0` does nothing. If `service clagd status` returns that `clagd` is *not* running but was configured to run, `jdo0` will start the `clagd` service. This check is performed every 30 seconds. Due to the way the `jdo0` process implements this check, it may start the `clagd` process twice. This is harmless, since `clagd` checks to make sure another instance is not already running when it begins executing. This is indicated with a message in the `clagd` log file, `/var/log/clagd.log`.
- The modification time of the `/var/run/clagd.alive` file. As `clagd` runs, it periodically updates the modification time of the `/var/run/clagd.alive` file (by default, every 4 seconds). If `jdo0` notices that this file's modification time has not been updated within the last 4 minutes, it will

assume `clagd` is alive, but hung, and will restart `clagd`. If `clagd` is not enabled to run, this check still occurs and `jdoe` will start `clagd`. But since `clagd` is not configured to run, nothing will happen except that a message is written to the `jdoe` log file that it tried to start `clagd`.

You can check the status of `clagd` monitoring by using the `jdoe summary` command:

```
cumulus@switch:~$ sudo jdoe summary
The jdoe daemon 5.4 uptime: 15m
...
Program 'clagd'           Status ok
File 'clagd.alive'        Waiting
...
...
```

MLAG Best Practices

For MLAG to function properly, the dual-connected hosts' interfaces should be configured identically on the pair of peering switches. See the note above in the [Configuring MLAG \(see page 221\)](#) section.

Understanding MTU in an MLAG Configuration

Note that the [MTU \(see page 137\)](#) in MLAG traffic is determined by the bridge MTU. Bridge MTU is determined by the lowest MTU setting of an interface that is a member of the bridge. If an MTU other than the default of 1500 bytes is desired, you must configure the MTU on each physical interface and bond interface that are members of the MLAG bridges in the entire bridged domain.

For example, if an MTU of 9216 is desired through the MLAG domain in the example shown above:

On the leaf switches, [configure mtu 9216 \(see page 137\)](#) for each of following interfaces, since they are members of bridge `br0`: spine1-2, peerlink, host1, host2.

```
auto br0
iface br0
  bridge-vlan-aware yes
  bridge-ports spine1-2 peerlink host1 host2    <- List of bridge member
  interfaces
  ...
...
```

Likewise, to ensure the MTU 9216 path is respected through the spine switches above, also change the MTU setting for bridge `br` by configuring `mtu 9216` for each of the following members of bridge `br` on spine1 and spine2: uplinkA, peerlink, downlink1, downlink2.

```
auto br
iface br
  bridge-vlan-aware yes
  bridge-ports uplinkA peerlink downlink1 downlink2
  ...
...
```

STP Interoperability with MLAG

Cumulus Networks recommends that you always enable STP in your layer 2 network.

Further, with MLAG, Cumulus Networks recommends you enable BPDU guard on the host-facing bond interfaces. (For more information about BPDU guard, see [BPDU Guard and Bridge Assurance \(see page 162\)](#).)

Debugging STP with MLAG

/var/log/daemon.log has mstpd logs.

Run mstpctl debuglevel 3 to see MLAG-related logs in /var/log/daemon.log:

```
cumulus@switch:~$ sudo mstpctl showportdetail br peer-bond
br:peer-bond CIST info
  enabled          yes           role      Designated
  port id         8.008        state      forwarding
  .....
  bpdufilter port no
  clag ISL        yes          clag ISL Oper UP   yes
  clag role       primary      clag dual conn mac 0:0:0:0:0:0:
  0
  clag remote portID F.FFFF    clag system mac 44:38:39:
ff:0:1
cumulus@switch:~$

cumulus@switch:~$ sudo mstpctl showportdetail br downlink-1
br:downlink-1 CIST info
  enabled          yes           role      Designated
  port id         8.006        state      forwarding
  .....
  bpdufilter port no
  clag ISL        no           clag ISL Oper UP   no
  clag role       primary      clag dual conn mac 0:0:0:3:
  11:1
  clag remote portID F.FFFF    clag system mac 44:38:39:
ff:0:1
cumulus@switch:~$
```

Best Practices for STP with MLAG

- The STP global configuration must be the same on both the switches.
- The STP configuration for dual-connected ports should be the same on both peer switches.

- Use `mstptcl` commands for all spanning tree configurations, including bridge priority, path cost and so forth. Do not use `brctl` commands for spanning tree, except for `brctl stp on/off`, as changes are not reflected to `mstpd` and can create conflicts.

Troubleshooting MLAG

By default, when `clagd` is running, it logs its status to the `/var/log/clagd.log` file and syslog. Example log file output is below:

```
Jan 14 23:45:10 switch clagd[3704]: Beginning execution of clagd version
1.0.0
Jan 14 23:45:10 switch clagd[3704]: Invoked with: /usr/sbin/clagd --daemon
169.254.2.2 peer-bond.4000 44:38:39:ff:00:01 --priority 8192
Jan 14 23:45:11 switch clagd[3995]: Role is now secondary
Jan 14 23:45:31 switch clagd[3995]: Role is now primary
Jan 14 23:45:32 switch clagd[3995]: The peer switch is active.
Jan 14 23:45:35 switch clagd[3995]: downlink-1 is now dual connected.
```

Understanding STP and LACP Behavior when MLAG Fails

For an in-depth look at how LACP and STP react during a number of failure scenarios, read this [knowledge base article](#).

Caveats and Errata

If both the backup and peer connectivity are lost within a 30-second window, the switch in the secondary role misinterprets the event sequence, believing the peer switch is down, so it takes over as the primary.

Configuration Files

- `/etc/network/interfaces`

LACP Bypass

On Cumulus Linux, *LACP Bypass* is a feature that allows a [bond](#) (see page 184) configured in 802.3ad mode to become active and forward traffic even when there is no LACP partner. A typical use case for this feature is to enable a host, without the capability to run LACP, to PXE boot while connected to a switch on a bond configured in 802.3ad mode. Once the pre-boot process finishes and the host is capable of running LACP, the normal 802.3ad link aggregation operation takes over.

Contents

(Click to expand)

- [Contents \(see page 234\)](#)
- [Understanding LACP Bypass Modes \(see page 235\)](#)
 - [LACP Bypass Timeout \(see page 235\)](#)

- LACP Bypass and MLAG Deployments (see page 235)
- Configuring LACP Bypass (see page 236)
- Configuration Examples (see page 236)
 - Default Configuration with Priority Mode and Optional Timeout Period (see page 236)
 - All-active Mode Configuration with Multiple Simultaneous Active Interfaces (see page 237)

Understanding LACP Bypass Modes

When a bond has multiple slave interfaces, you can control which of them should go into LACP bypass using one of two modes:

- *Priority mode*: This is the default mode. On a switch, if a bond has multiple slave interfaces, you can configure a bypass priority value (default is 0) for each interface in the bond; the one with higher numerical priority value wins. A string comparison of the interface names serves as a tiebreaker in case the priority values are equal; the string with the lower ASCII values wins. Note that the priority value is significant within a switch; there is no coordination between two switches in an [MLAG \(see page 217\)](#) peering relationship.
- *All-active mode*: In this mode, each bond slave interface operates as an active link while the bond is in bypass mode. This mode is useful during PXE boot of a server with multiple NICs, when the user cannot determine beforehand which port needs to be active. By default, all-active mode is disabled.



All-active mode is not supported on bonds that are not specified as bridge ports on the switch.



STP does not run on the individual bond slave interfaces, when the LACP bond is in all-active mode. Therefore, only use all-active mode on host-facing LACP bonds. Cumulus Networks highly recommends you configure [STP BPDU guard](#) along with all-active mode.

LACP Bypass Timeout

As a safeguard, you can configure a timeout period to limit the duration in which bypass is enabled. The timeout period works with both modes. The valid range of timeout period is 0 to 900 seconds; the default is 0 seconds, which indicates no timeout. If no LACP partner is detected before the timeout period expires, the bond becomes inactive and stops forwarding traffic. The timer is restarted when any slave interfaces are enabled; which can be achieved by setting the interface down and then up. At any point in time, receiving LACP PDU on any slave interface aborts the bypass, and normal LACP protocol negotiation takes over. Enabling or disabling bypass during LACP exchange does not affect link aggregation.

LACP Bypass and MLAG Deployments

In an [MLAG deployment \(see page 217\)](#) where bond slaves of a host are connected to two switches and the bond is in **priority mode**, the bypass priority is determined using the MLAG switch role. The bond on the switch with the primary role has a **higher** bypass priority than the bond on the switch with the secondary role. When multiple slave interfaces of a bond are connected to each switch, the slave with the highest priority on the primary MLAG switch will be the active interface. All other slaves on the same device will not be active during bypass mode.

When a dual-connected (MLAG) bond is in ***all-active mode***, all the slaves of bond are active on both the primary and secondary MLAG nodes.

Configuring LACP Bypass

You configure LACP bypass in the `/etc/network/interfaces` file.

To enable LACP bypass on the host-facing bond, under the bond interface stanza, set `bond-lacp-bypass-allow` to 1. Then optionally configure one of the following:

- To configure **priority mode**, which is the *default* mode, set `bond-lacp-bypass-priority` to a value, with the priority values for each slave interface. The default priority value is 0.
- To configure **all-active mode** for multiple active interfaces, set `bond-lacp-bypass-all-active` to 1. This enables all interfaces to pass traffic (become active) until the server can form an LACP bond.

(Optional): To configure a timeout period for either mode, set `bond-lacp-bypass-period` to a valid value (0-900); however, it is recommended to not configure this, and use the default value of 0.

Configuration Examples

Default Configuration with Priority Mode and Optional Timeout Period

The following configuration shows LACP bypass enabled in the default priority mode, with a timeout period set. Here there are two slave interfaces, and `swp2` will be preferred as the active bypass interface:

```
auto bond0
iface bond0
    bond-lacp-bypass-allow 1
    bond-slaves swp4 swp5
    bond-lacp-bypass-period 300
    bond-lacp-bypass-priority swp4=2 swp5=1
```

The following command shows that `swp4` bypass timeout has expired and the bond is operationally down:

```
cumulus@switch$ ip link show bond0
7: bond0: <NO-CARRIER,BROADCAST,MULTICAST,MASTER,UP> mtu 1500 qdisc noqueue
state DOWN mode DEFAULT
    link/ether 00:02:00:00:00:02 brd ff:ff:ff:ff:ff:ff
cumulus@switch$ cat /proc/net/bonding/bond0
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)
Bonding Mode: IEEE 802.3ad Dynamic link aggregation
Transmit Hash Policy: layer2 (0)
MII Status: up
MII Polling Interval (ms): 0
Up Delay (ms): 0
```

```

Down Delay (ms): 0
802.3ad info
LACP rate: fast
Min links: 1
Aggregator selection policy (ad_select): stable
System Identification: 65535 00:02:00:00:00:02
Active Aggregator Info:
    Aggregator ID: 1
    Number of ports: 1
    Actor Key: 33
    Partner Key: 1
    Partner Mac Address: 00:00:00:00:00:00
Fall back Info:
    Allowed: 1
    Timeout: 300
Slave Interface: swp4
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:02:00:00:00:02
Aggregator ID: 1
LACP bypass priority: 2
LACP bypass: expired
Slave queue ID: 0
Slave Interface: swp5
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:02:00:00:00:01
Aggregator ID: 2
Bypass priority: 1
Slave queue ID: 0

```

All-active Mode Configuration with Multiple Simultaneous Active Interfaces

The following configuration shows LACP bypass enabled for multiple active interfaces (all-active mode) with a bridge in VLAN-aware mode (see page 208):

```

auto bond1
iface bond1 inet static
    bond-slaves swp3 swp4
    bond-lacp-bypass-allow 1

```

```
bond-lacp-bypass-all-active 1

auto br0
iface br0 inet static
    bridge-vlan-aware yes
    bridge-ports bond1 bond2 bond3 bond4 peer5
    bridge-stp on
    bridge-vids 100-105
    mstpctl-bpduguard bond1=yes

cumulus@switch:~$ ip link show bond1
58: bond1: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue
master br0 state UP mode DORMANT
    link/ether 44:38:39:00:38:44 brd ff:ff:ff:ff:ff:ff
cumulus@switch:~$ ip link show swp3
5: swp3: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
master bond1 state UP mode DEFAULT qlen 500
    link/ether 44:38:39:00:38:44 brd ff:ff:ff:ff:ff:ff
cumulus@switch:~$ ip link show swp4
6: swp4: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
master bond1 state UP mode DEFAULT qlen 500
    link/ether 44:38:39:00:38:44 brd ff:ff:ff:ff:ff:ff

cumulus@switch:~$ cat /proc/net/bonding/bond1
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: IEEE 802.3ad Dynamic link aggregation
Transmit Hash Policy: layer3+4 (1)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

802.3ad info
LACP rate: fast
Min links: 1
Aggregator selection policy (ad_select): stable
System Identification: 65535 00:00:00:aa:bb:01
Active Aggregator Info:
    Aggregator ID: 1
    Number of ports: 1
    Actor Key: 33
    Partner Key: 33
```

```

Partner Mac Address: 00:02:00:00:00:05

LACP Bypass Info:
    Allowed: 1
    Timeout: 0
    All-active: 1

Slave Interface: swp3
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 1
Permanent HW addr: 44:38:39:00:38:44
Aggregator ID: 1
LACP bypass priority: 0
LACP bypass: on
Slave queue ID: 0

Slave Interface: swp4
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 1
Permanent HW addr: 44:38:39:00:38:45
Aggregator ID: 2
LACP bypass priority: 0
LACP bypass: on
Slave queue ID: 0

```

The following configuration shows LACP bypass enabled for multiple active interfaces (all-active mode) with a bridge in [traditional bridge mode](#) (see page 187):

```

auto bond1
iface bond1 inet static
    bond-slaves swp3 swp4
    bond-lacp-bypass-allow 1
    bond-lacp-bypass-all-active 1

auto br0
iface br0 inet static
    bridge-ports bond1 bond2 bond3 bond4 peer5
    bridge-stp on
    mstpcctl-bpduguard bond1=yes

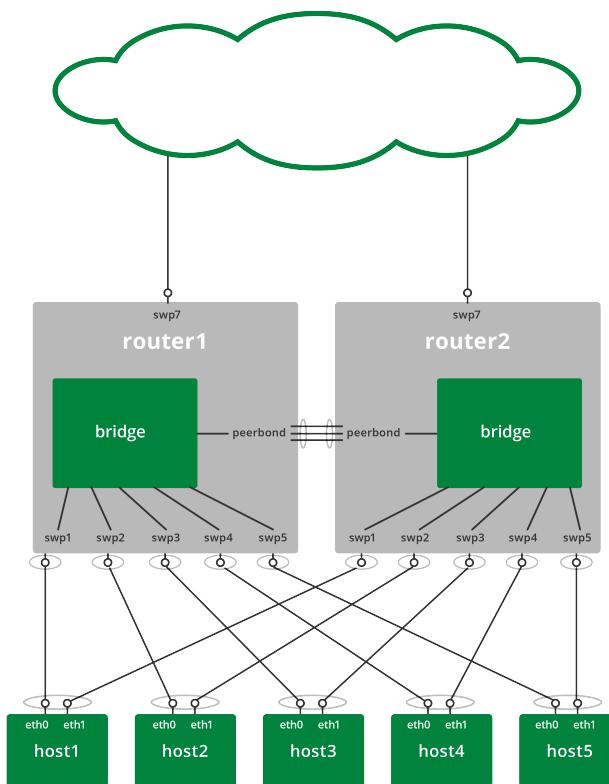
```

Virtual Router Redundancy - VRR

VRR provides virtualized router redundancy in network configurations, which enables the hosts to communicate with any redundant router without:

- Needing to be reconfigured
- Having to run dynamic router protocols
- Having to run router redundancy protocols

A basic VRR-enabled network configuration is shown below. The network consists of several hosts, two routers running Cumulus Linux and configured with [MLAG \(see page 217\)](#), and the rest of the network:



An actual implementation will have many more server hosts and network connections than are shown here. But this basic configuration provides a complete description of the important aspects of the VRR setup.

Contents

(Click to expand)

- Contents (see page 240)
- Configuring the Network (see page 241)
 - Reserved MAC Address Range (see page 242)
 - Configuring the Hosts (see page 242)

- Configuring the Routers (see page 242)
- Other Network Connections (see page 243)
- Handling ARP Requests (see page 243)
- Monitoring Peer Links and Uplinks (see page 243)
- Using ifplugd (see page 243)
- Notes (see page 245)

Configuring the Network

Configuring this network is fairly straightforward. First create the bridge subinterface, then create the secondary address for the virtual router. Configure each router with a bridge; edit each router's `/etc/network/interfaces` file and add a configuration similar to the following:

```
auto bridge.500
iface bridge.500
    address 192.168.0.252/24
    address-virtual 00:00:5e:00:01:01 192.168.0.254/24 2001:aa::1/48
```



Notice the simpler configuration of the bridge with `ifupdown2`. For more information, see [Configuring and Managing Network Interfaces \(see page 121\)](#).

You should always use `ifupdown2` to configure VRR, because it ensures correct ordering when bringing up the virtual and physical interfaces and it works best with [VLAN-aware bridges \(see page 208\)](#).

If you are using the `traditional mode` bridge driver, the configuration would look like this:

```
auto bridge500
iface bridge500
    address 192.168.0.252/24
    address-virtual 00:00:5e:00:01:01 192.168.0.254/24 2001:aa::1/48
    bridge-ports bond1.500 bond2.500 bond3.500
```

The IP address assigned to the bridge is the unique address for the bridge. The parameters of this configuration are:

- `bridge.500`: 500 represents a VLAN subinterface of the bridge, sometimes called a switched virtual interface, or SVI.
- `192.168.0.252/24`: The unique IP address assigned to this bridge. It is unique because, unlike the 192.168.0.254 address, it is assigned only to this bridge, not the bridge on the other router.
- `00:00:5e:00:01:01`: The MAC address of the virtual router. This must be the same on all virtual routers. Cumulus Linux has a reserved range for VRR MAC addresses. See below for details.

- *192.168.0.254/24, 2001:aa::1/48*: The IPv4 and IPv6 addresses of the virtual router, including the routing prefixes. These addresses must be the same on all the virtual routers and must match the default gateway address configured on the servers as well as the size of the subnet.
- `address-virtual1`: This keyword enables and configures VRR.

The above bridge configuration enables VRR by creating a *MAC VLAN interface* on the SVI. This MAC VLAN interface is:

- Named *bridge-500-v0*, which is the name of the SVI with dots changed to dashes and *-v0* appended to the end.
- Assigned a MAC address of *00:00:5e:00:01:01*.
- Assigned an IPv4 address of *192.168.0.254* and an IPv6 address of *2001:aa::1/48*.

Reserved MAC Address Range

In order to prevent MAC address conflicts with other interfaces in the same bridged network, Cumulus Networks has **reserved a range of MAC addresses** specifically to use with VRR. This range of MAC addresses is *00:00:5E:00:01:00* to *00:00:5E:00:01:ff*.

You may notice that this is the same range reserved for VRRP, since VRR serves a similar function. Cumulus Networks recommends you use this range of MAC addresses when configuring VRR.

Configuring the Hosts

Each host should have two network interfaces. The routers configure the interfaces as bonds running LACP; the hosts should also configure its two interfaces using teaming, port aggregation, port group, or EtherChannel running LACP. Configure the hosts, either statically or via DHCP, with a gateway address that is the IP address of the virtual router; this default gateway address never changes.

Configure the links between the hosts and the routers in *active-active* mode for First Hop Redundancy Protocol.



If you are configuring VRR without **MLAG** (see page 217), use *active-standby* mode instead. For example, configure the bond like this:

```
auto bond0
iface bond0
    bond-mode active-backup
```

The configuration may vary, depending upon the host OS.

Configuring the Routers

The routers implement the layer 2 network interconnecting the hosts, as well as the redundant routers. If you are using **MLAG** (see page 217), configure each router with a bridge interface, named *bridge* in our example, with these different types of interfaces:

- One bond interface to each host (swp1-swp5 in the image above).

- One or more interfaces to each peer router (peerbond in the image above). Multiple inter-peer links are typically bonded interfaces in order to accommodate higher bandwidth between the routers and to offer link redundancy.



If you are not using MLAG, then the bridge should have one switch port interface to each host instead of a bond.

Other Network Connections

Other interfaces on the router can connect to other subnets and are accessed through layer 3 forwarding (swp7 in the image above).

Handling ARP Requests

The entire purpose of this configuration is to have all the redundant routers respond to ARP requests from hosts for the virtual router IP address (192.168.0.254 in the example above) with the virtual router MAC address (00:00:5e:00:01:01 in the example above). All of the routers should respond in an identical manner, but if one router fails, the other redundant routers will continue to respond in an identical manner, leaving the hosts with the impression that nothing has changed.

Since the bridges in each of the redundant routers are connected, they will each receive and reply to ARP requests for the virtual router IP address. Each ARP request made by a host will receive multiple replies (typically two). But these replies will be identical and so the host that receives these replies will not get confused over which response is "correct" and will either ignore replies after the first, or accept them and overwrite the previous reply with identical information.

Monitoring Peer Links and Uplinks

When an uplink on a switch in active-active mode goes down, the peer link may get congested. When this occurs, you should monitor the uplink and shut down all host-facing ports using `ifplugd` (or another script).

When the peer link goes down in a MLAG environment, one of the switches becomes secondary and all host-facing dual-connected bonds go down. The host side bond sees two different system MAC addresses, so the link to primary is active on host. If any traffic from outside this environment goes to the secondary MLAG switch, traffic will be black-holed. To avoid this, shut down all the uplinks when the peer link goes down using `ifplugd`.

Using `ifplugd`

`ifplugd` is a link state monitoring daemon that can execute user-specified scripts on link transitions (not admin-triggered transitions, but transitions when a cable is plugged in or removed).

Run the following commands to install the `ifplugd` service:

```
cumulus@switch:$ sudo apt-get update  
cumulus@switch:$ sudo apt-get install ifplugd
```

Next, configure `ifplugd`. The example below indicates that when the peerbond goes down in a MLAG environment, `ifplugd` brings down all the uplinks. Run the following `ifplugd` script on both the primary and secondary MLAG (see page 217) switches.

To configure `ifplugd`, modify `/etc/default/ifplugd` and add the appropriate peerbond interface name. `/etc/default/ifplugd` will look like this:

```
INTERFACES="peerbond"
HOTPLUG_INTERFACES=""
ARGS="-q -f -u0 -d1 -w -I"
SUSPEND_ACTION="stop"
```

Next, modify the `/etc/ifplugd/action.d/ifupdown` script.

```
#!/bin/sh
set -e
case "$2" in
up)
    clagrole=$(clagctl | grep "Our Priority" | awk '{print $8}')
    if [ "$clagrole" = "secondary" ]
    then
        #List all the interfaces below to bring up when clag
        peerbond comes up.
        for interface in swp1 bond1 bond3 bond4
        do
            echo "bringing up : $interface"
            ip link set $interface up
        done
    fi
;;
down)
    clagrole=$(clagctl | grep "Our Priority" | awk '{print $8}')
    if [ "$clagrole" = "secondary" ]
    then
        #List all the interfaces below to bring down when clag
        peerbond goes down.
        for interface in swp1 bond1 bond3 bond4
        do
            echo "bringing down : $interface"
            ip link set $interface down
        done
    fi
;;
```

```
    fi  
    ;;  
esac
```

Finally, restart `ifplugd` for your changes to take effect:

```
cumulus@switch:~$ sudo service ifplugd restart
```

Notes

- The default shell is `/bin/sh`, which is `dash` and not `bash`. This makes for faster execution of the script since `dash` is small and quick, but consequently less featureful than `bash`. For example, it doesn't handle multiple uplinks.

Network Virtualization

Cumulus Linux supports these forms of [network virtualization](#):

VXLAN (Virtual Extensible LAN), is a standard overlay protocol that abstracts logical virtual networks from the physical network underneath. You can deploy simple and scalable layer 3 Clos architectures while extending layer 2 segments over that layer 3 network.

VXLAN uses a VLAN-like encapsulation technique to encapsulate MAC-based layer 2 Ethernet frames within layer 3 UDP packets. Each virtual network is a VXLAN logical L2 segment. VXLAN scales to 16 million segments – a 24-bit VXLAN network identifier (VNI ID) in the VXLAN header – for multi-tenancy.

Hosts on a given virtual network are joined together through an overlay protocol that initiates and terminates tunnels at the edge of the multi-tenant network, typically the hypervisor vSwitch or top of rack. These edge points are the VXLAN tunnel end points (VTEP).

Cumulus Linux can initiate and terminate VTEPs in hardware and supports wire-rate VXLAN with Trident II platforms. VXLAN provides an efficient hashing scheme across IP fabric during the encapsulation process; the source UDP port is unique, with the hash based on L2-L4 information from the original frame. The UDP destination port is the standard port 4789.

Cumulus Linux includes the native Linux VXLAN kernel support and integrates with controller-based overlay solutions like VMware NSX and Midokura MidoNet.

VXLAN is supported only on switches in the [Cumulus Linux HCL](#) using Trident II chipsets.



VXLAN encapsulation over layer 3 subinterfaces is not supported. Therefore, VXLAN uplinks should be only configured as layer 3 interfaces without any subinterfaces.

Furthermore the VXLAN tunnel endpoints cannot share a common subnet; there must be at least one layer 3 hop between the VXLAN source and destination.

Commands

- `brctl`
- `bridge fdb`

- ip link
- ovs-pki
- ovsdb-client
- vtep-ctl

Caveats/Errata

Cut-through Mode

Cut-through mode is disabled in Cumulus Linux by default. With cut-through mode enabled and link pause is asserted, Cumulus Linux generates a TOVR and TUFL ERROR; certain error counters increment on a given physical port.

```
cumulus@switch:~$ sudo ethtool -S swp49 | grep Error
HwIfInDot3LengthErrors: 0
HwIfInErrors: 0
HwIfInDot3FrameErrors: 0
SoftInErrors: 0
SoftInFrameErrors: 0
HwIfOutErrors: 35495749
SoftOutErrors: 0

cumulus@switch:~$ sudo ethtool -S swp50 | grep Error
HwIfInDot3LengthErrors: 3038098
HwIfInErrors: 297595762
HwIfInDot3FrameErrors: 293710518
```

To work around this issue, disable link pause or disable cut-through in /etc/cumulus/datapath/traffic.conf.

To disable link pause, comment out the link_pause* section in /etc/cumulus/datapath/traffic.conf:

```
cumulus@switch:~$ sudo nano /etc/cumulus/datapath/traffic.conf
#link_pause.port_group_list = [port_group_0]
#link_pause.port_group_0.port_set = swp45-swp54
#link_pause.port_group_0.rx_enable = true
#link_pause.port_group_0.tx_enable = true
```

To enable store and forward switching, set cut_through_enable to false in /etc/cumulus/datapath/traffic.conf:

```
cumulus@switch:~$ sudo nano /etc/cumulus/datapath/traffic.conf
cut_through_enable = false
```

MTU Size for Virtual Network Interfaces

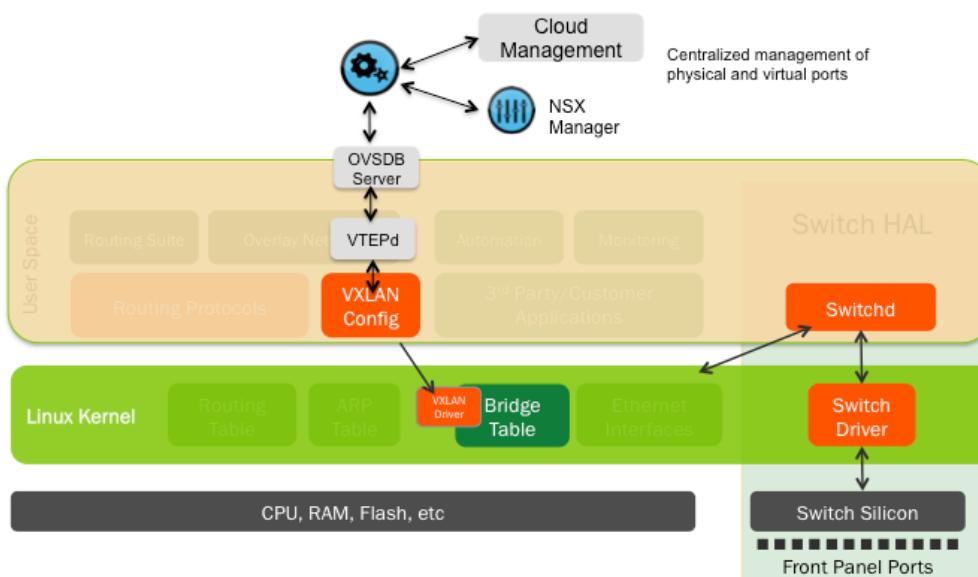
The maximum transmission unit (MTU) size for a virtual network interface should be 50 bytes smaller than the MTU for the physical interfaces on the switch. For more information, read [Layer 1 and Switch Port Attributes](#) (see page 139).

Useful Links

- VXLAN IETF draft
- ovsdb-server

Integrating with VMware NSX

Switches running Cumulus Linux can integrate with VMware NSX to act as VTEP gateways. The VMware NSX controller provides consistent provisioning across virtual and physical server infrastructures.



Contents

(Click to expand)

- [Contents \(see page 247\)](#)
- [Getting Started \(see page 248\)](#)
 - [Caveats and Errata \(see page 248\)](#)
- [Bootstrapping the NSX Integration \(see page 248\)](#)
 - [Enabling the openvswitch-vtep Package \(see page 248\)](#)
 - [Using the Bootstrapping Script \(see page 249\)](#)
 - [Manually Bootstrapping the NSX Integration \(see page 250\)](#)
 - [Generating the Credentials Certificate \(see page 250\)](#)
 - [Configuring the Switch as a VTEP Gateway \(see page 252\)](#)
- [Configuring the Transport Layer \(see page 255\)](#)

- Configuring the Logical Layer (see page 256)
 - Defining Logical Switches (see page 256)
 - Defining Logical Switch Ports (see page 258)
- Verifying the VXLAN Configuration (see page 260)
- Persistent VXLAN Configuration in NSX (see page 261)
- Troubleshooting VXLANs in NSX (see page 261)

Getting Started

Before you integrate VXLANs with NSX, make sure you have the following components:

- A switch (L2 gateway) with a Trident II chipset running Cumulus Linux 2.0 or later;
- OVSDB server (ovsdb-server), included in Cumulus Linux 2.0 and later
- VTEPd (ovs-vtep), included in Cumulus Linux 2.0 and later

Integrating a VXLAN with NSX involves:

- Bootstrapping the NSX Integration
- Configuring the Transport Layer
- Configuring the Logical Layer
- Verifying the VXLAN Configuration

Once you finish the integration, you can make the configuration persistent across upgrades (see [Persistent VXLAN Configuration in NSX](#) (see page 261) below).

Caveats and Errata

- As mentioned in [Network Virtualization](#) (see page 245), the switches with the source and destination VTEPs cannot reside on the same subnet; there must be at least one layer 3 hop between the VXLAN source and destination.
- There is no support for VXLAN routing in the Trident II chip; use a loopback interface or external router.
- Do not use 0 or 16777215 as the VNI ID, as they are reserved values under Cumulus Linux.
- For more information about NSX, see the VMware NSX User Guide, version 4.0.0 or later.

Bootstrapping the NSX Integration

Before you start configuring the gateway service and logical switches and ports that comprise the VXLAN, you need to complete some steps to bootstrap the process. You need to do the bootstrapping just once, before you begin the integration.

Enabling the `openvswitch-vtep` Package

Before you start bootstrapping the integration, you need to enable the `openvswitch-vtep` package, as it is disabled by default in Cumulus Linux.

1. In `/etc/default/openvswitch-vtep`, change the `START` option from `no` to `yes`:

```
cumulus@switch$ cat /etc/default/openvswitch-vtep
# This is a POSIX shell fragment          -*- sh -*-

# Start openvswitch at boot ? yes/no
START=yes

# FORCE_COREFILES: If 'yes' then core files will be enabled.
# FORCE_COREFILES=yes

# BRCOMPAT: If 'yes' and the openvswitch-brcompat package is
installed, then
# Linux bridge compatibility will be enabled.
# BRCOMPAT=no
```

2. Start the daemon:

```
cumulus@switch$ sudo service openvswitch-vtep start
```

Make sure to include this file in your persistent configuration (see [Persistent VXLAN Configuration in NSX \(see page 261\)](#) below) so it's available after you upgrade Cumulus Linux.

Using the Bootstrapping Script

A script is available so you can do the bootstrapping automatically. For information, read `man vtep-bootstrap`. The output of the script is displayed here:

```
cumulus@vtep7: ~
cumulus@vtep7$ sudo vtep-bootstrap --credentials-path /var/lib/openvswitch vtep7 192.168.100.17 172.1
6.20.157 192.168.100.157
Executed:
  create certificate on a switch, to be used for authentication with controller
  () .
Executed:
  sign certificate
  (vtep7-req.pem      Fri Jan 17 18:04:33 UTC 2014
   fingerprint 6f443eb8445317b545d8564c2ae9638ea0a9184a).
Executed:
  define physical switch
  () .
Executed:
  define NSX controller IP address in OVSDB
  () .
Executed:
  define local tunnel IP address on the switch
  () .
Executed:
  define management IP address on the switch
  () .
Executed:
  restart a service
  (Killing ovs-vtepd (4973).
Killing ovsdb-server (4969).
Starting ovsdb-server.
Starting ovs-vtepd.).
cumulus@vtep7$ 
cumulus@vtep7$ 
cumulus@vtep7$ ps xa | grep ovsdb-server
 5184 pts/0    S<     0:00 ovsdb-server: monitoring pid 5185 (healthy)

 5185 ?      S<     0:00 ovsdb-server /var/lib/openvswitch/conf.db -vANY:CONSOLE:EMER -vANY:SYSLOG:
ERR -vANY:FILE:INFO --remote=unix:/var/run/openvswitch/db.sock --remote=db:Global,managers --remote=
ptcp:6633: --private-key=/var/lib/openvswitch/vtep7-privkey.pem --certificate=/var/lib/openvswitch/vt
ep7-cert.pem --bootstrap-ca-cert=/var/lib/openvswitch/controller.ca.cert --no-chdir --log-file=/var/lo
g/openvswitch/ovsdb-server.log --pidfile=/var/run/openvswitch/ovsdb-server.pid --detach --monitor
 5436 pts/0    S+    0:00 grep ovsdb-server
cumulus@vtep7$
```

In the above example, the following information was passed to the `vtep-bootstrap` script:

- `--credentials-path /var/lib/openvswitch`: Is the path to where the certificate and key pairs for authenticating with the NSX controller are stored.
- `vtep7`: is the ID for the VTEP.
- `192.168.100.17`: is the IP address of the NSX controller.
- `172.16.20.157`: is the datapath IP address of the VTEP.
- `192.168.100.157`: is the IP address of the management interface on the switch.

These IP addresses will be used throughout the rest of the examples below.

Manually Bootstrapping the NSX Integration

If you don't use the script, then you must:

- Initialize the OVS database instance
- Generate a certificate and key pair for authentication by NSX
- Configure a switch as a VTEP gateway

These steps are described next.

Generating the Credentials Certificate

First, in Cumulus Linux, you must generate a certificate that the NSX controller uses for authentication.

1. In a terminal session connected to the switch, run the following commands:

```
cumulus@switch:~$ sudo ovs-pki init
Creating controllerca...
Creating switchca...
cumulus@switch:~$ sudo ovs-pki req+sign cumulus

cumulus-req.pem Wed Oct 23 05:32:49 UTC 2013
    fingerprint b587c9fe36f09fb371750ab50c430485d33a174a
cumulus@switch:~$
cumulus@switch:~$ ls -l
total 12
-rw-r--r-- 1 root root 4028 Oct 23 05:32 cumulus-cert.pem
-rw------- 1 root root 1679 Oct 23 05:32 cumulus-privkey.pem
-rw-r--r-- 1 root root 3585 Oct 23 05:32 cumulus-req.pem
```

2. In `/usr/share/openvswitch/scripts/ovs-ctl-vtep`, make sure the lines containing **private-key**, **certificate** and **bootstrap-ca-cert** point to the correct files; **bootstrap-ca-cert** is obtained dynamically the first time the switch talks to the controller:

```
# Start ovsdb-server.
set ovsdb-server "$DB_FILE"
set "$@" -vANY:CONSOLE:EMER -vANY:SYSLOG:ERR -vANY:FILE:INFO
set "$@" --remote=punix:"$DB_SOCK"
set "$@" --remote=db:Global,managers
set "$@" --remote=ptcp:$LOCALIP
set "$@" --private-key=/root/cumulus-privkey.pem
set "$@" --certificate=/root/cumulus-cert.pem
set "$@" --bootstrap-ca-cert=/root/controller.cacert
```

If files have been moved or regenerated, restart the OVSDB server and `vtep`:

```
cumulus@switch:~$ sudo service openvswitch-vtep restart
```

3. Define the NSX controller cluster IP address in OVSDB. This causes the OVSDB server to start contacting the NSX controller:

```
cumulus@switch:~$ sudo vtep-ctl set-manager ssl:192.168.100.17:6632
```

4. Define the local IP address on the VTEP for VXLAN tunnel termination. First, find the physical switch name as recorded in OVSDB:

```
cumulus@switch:~$ sudo vtep-ctl list-ps  
vtep7
```

Then set the tunnel source IP address of the VTEP. This is the datapath address of the VTEP, which is typically an address on a loopback interface on the switch that is reachable from the underlying L3 network:

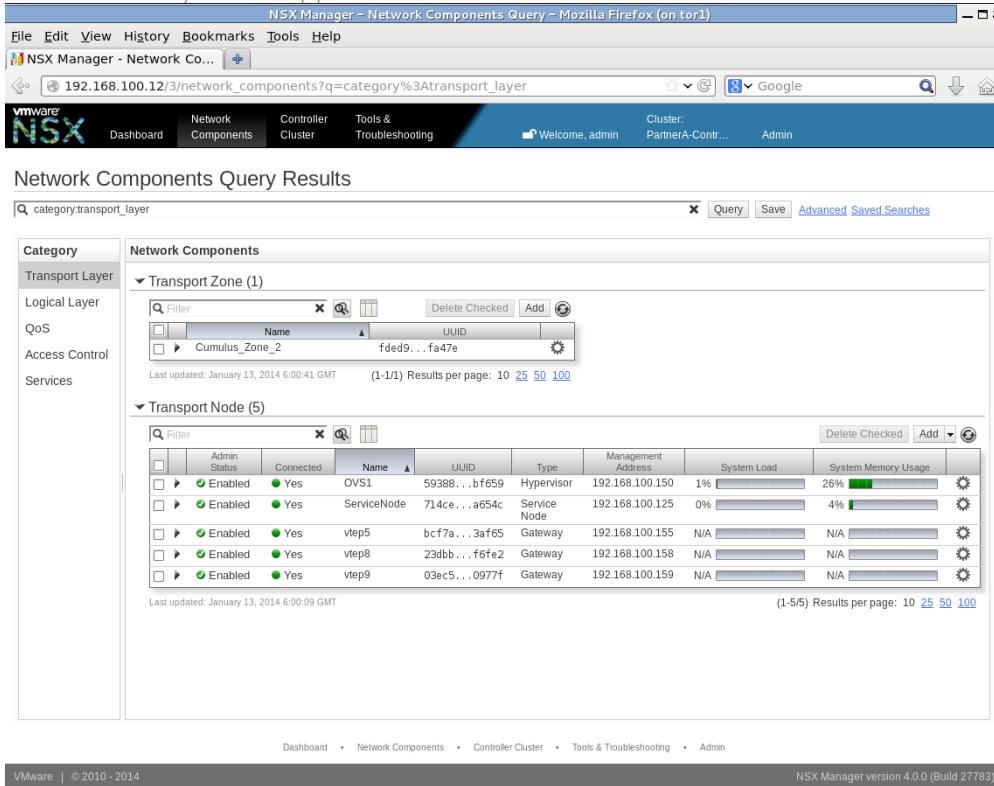
```
cumulus@switch:~$ sudo vtep-ctl set Physical_Switch vtep7  
tunnel_ip=172.16.20.157
```

Once you finish generating the certificate, keep the terminal session active, as you need to paste the certificate into NSX Manager when you configure the VTEP gateway.

Configuring the Switch as a VTEP Gateway

After you create a certificate, connect to NSX Manager in a browser to configure a Cumulus Linux switch as a VTEP gateway. In this example, the IP address of the NSX manager is 192.168.100.12.

- In NSX Manager, add a new gateway. Click the **Network Components** tab, then the **Transport Layer** category. Under **Transport Node**, click **Add**, then select **Manually Enter All Fields**. The Create Gateway wizard appears.



The screenshot shows the NSX Manager interface for Network Components. The left sidebar has categories: Transport Layer (selected), Logical Layer, QoS, Access Control Services. The main area has two tables:

- Transport Zone (1)**: Shows one entry: Cumulus_Zone_2 (UUID: fded9...fa47e).
- Transport Node (5)**: Shows five entries:

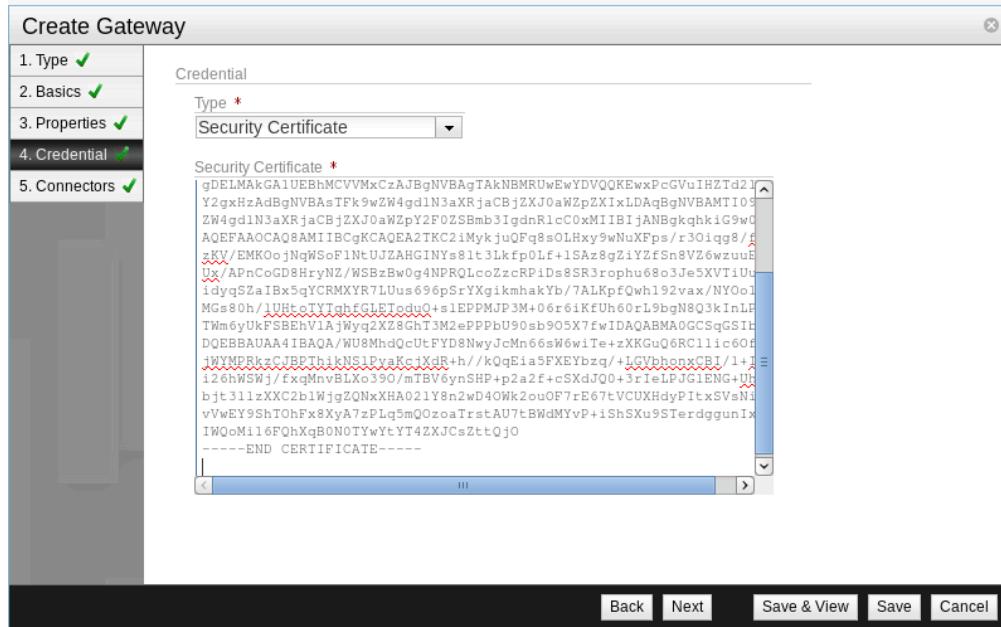
Name	UUID	Type	Management Address	System Load	System Memory Usage
OVS1	59388...bf659	Hypervisor	192.168.100.150	1%	26%
ServiceNode	714ce...a654c	Service Node	192.168.100.125	0%	4%
vtep5	bcf7a...3af65	Gateway	192.168.100.155	N/A	N/A
vtep8	23dbb...f6fe2	Gateway	192.168.100.158	N/A	N/A
vtep9	03ec5...0977f	Gateway	192.168.100.159	N/A	N/A

At the bottom, it says "Last updated: January 13, 2014 6:00:41 GMT" and "(1-1/1) Results per page: 10 25 50 100".

- In the Create Gateway dialog, select **Gateway** for the **Transport Node Type**, then click **Next**.
- In the **Display Name** field, give the gateway a name, then click **Next**.
- Enable the VTEP service. Select the **VTEP Enabled** checkbox, then click **Next**.
- From the terminal session connected to the switch where you generated the certificate, copy the certificate and paste it into the **Security Certificate** text field. Copy only the bottom portion, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines. For example, copy all the highlighted text in the terminal:

```
ubuntu@tor1: ~
87:3f:ea:76:6b:67:fe:71:25:dd:25:0d:3e:de:b2:1e:2c:f2;
46:94:43:46:94:49:43:6e:3b:77:96:5c:d7:75:c2:db:9b:95:68;
e0:65:03:71:5c:70:34:d1:56:3c:9f:6c:30:e0:e5:a4:da:8b;
8e:17:ba:c4:eb:bb:55:09:45:77:23:08:b7:14:95:b0:08;
ba:bd:5c:04:63:d4:a1:4c:e8:45:c7:c5:f2:03:bc:cf:2e:ae;
66:40:ece:68:3a:ec:b4:05:3b:b4:15:9d:31:8b:cf:fa:24;
a1:49:7:b:bd:49:37:ab:76:08:ze:9c:8c:44:21:b4:28:32:2d;
7a:15:08:57:8:1d:0d:dd:36:30:62:d6:13:e1:95:c9:0:a:c6;
6d:b5:0:ce
-----BEGIN CERTIFICATE-----
MIIddzCA18CAQyD0YKoZIwvNAQEEB0IwgYEcxZzAJBgNVBAYTAlVTM0swQYD
VQ0IEwJDT0TEVMBMGqAUECHmHNT3B1b1B2U3dpC0N0REwIwYDVOQLEwhzd21OY2hj
YTE7MDkG41UEAxRyT1ZTHNsaaKRjaGWhENBLEN1cnRpZmJyYKR1ICgMBeZI
YgJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJyJy
gjDELMAkGg1UEBhMCVWmxCzA3BgNBgTAkNBRUuIwUDVQ0KEuwpvWIH2d21O
Y2gXzkdBgNVBAsTFk9wZl4gd1N3aKRjaCBjZXJ0aWZpZXIxLDAaBgNVBAMTI09w
Zl4g9IN3aKRjaCjRjZkI0alZgYFZ0Smb31ghnRlc0xM1BIjANBgkhkiG9w0B
AQEFRA0C003AM1IBCgKCADeR2TKC21mkJu0Fq8s0Lhx9wNxFps/r301qb8/F
zKV/EMK0ojNqISoF1ntUJ2AGINt's81t3LkfpolF+1Sa2g2iY2F9n8VZbwzuE8
Ux/APhCoDBHrhyNZ/WSBzhu9NPRLQcoZzcP1D85R3rroph68o3je5XViUUZ
idy9Za1B1SqYCRMXYR7LUus656gSrYgiknhakYb/7ALKpFQwh192vax/NY0o1i
MgS80h/1UHc0TYTqhfGLEtodu+1ePPMPJ3h+06:61KFU60rL9b6N8Q3InLPN
Tlw6yUkFSBEhvTYIwq2XZ8GhT3M2epPPBu90sb905X7fuIIAQABM40GCSqGSIB3
D0EBB4l9a941B9Q0/WJ8hhd0UFYD8WwJcMn6Ss6wiTe+zXGw0GRCllic6Ofq
jiYMPRkzJBThkNS1PyakcJxdR+h/+kQqE1a5FXEYbzq/+LGvbihnxCBI/1+IG
126HMSMjfxqlhnlBLXo390/nTBW6ySHP+2a2f+cSxdJ00+3r1eLPJG1ENG+UhD
bjt31zXC2b1ljqZDNxXHA021YBn2u040Wk2ou07rE677tCUKhdPtxSVsNi6
vvEY95hTOFx8KyA7zL5mQD0zoaTrsAU7tBlhdMyvP+iShSxu9STerdggunIxE
IMQoh116FQhXgBONOTyWYtYT4ZJCScZttQj0
-----END CERTIFICATE-----
root@vtep1:~#
```

And paste it into NSX Manager:



Then click **Next**.

6. In the Connectors dialog, click **Add Connector** to add a transport connector. This defines the tunnel endpoint that terminates the VXLAN tunnel and connects NSX to the physical gateway. You must choose a tunnel **Transport Type** of **VXLAN**. Choose an existing transport zone for the connector, or click **Create** to create a new transport zone.
7. Define the connector's IP address (that is, the underlay IP address on the switch for tunnel termination).
8. Click **OK** to save the connector, then click **Save** to save the gateway.

Once communication is established between the switch and the controller, a `controller.cacert` file will be downloaded onto the switch.

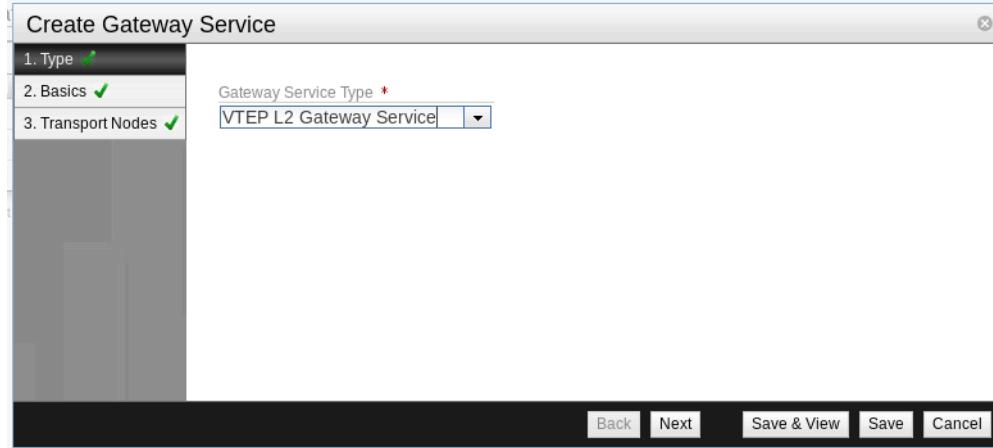
Verify the controller and switch handshake is successful. In a terminal connected to the switch, run this command:

```
cumulus@switch:~$ sudo ovsdb-client dump -f list | grep -A 7 "Manager"
Manager table
_uuid : 505f32af-9acb-4182-a315-022e405aa479
inactivity_probe : 30000
is_connected : true
max_backoff : []
other_config : {}
status : {sec_since_connect="18223", sec_since_disconnect="18225", state=ACTIVE}
target : "ssl:192.168.100.17:6632"
```

Configuring the Transport Layer

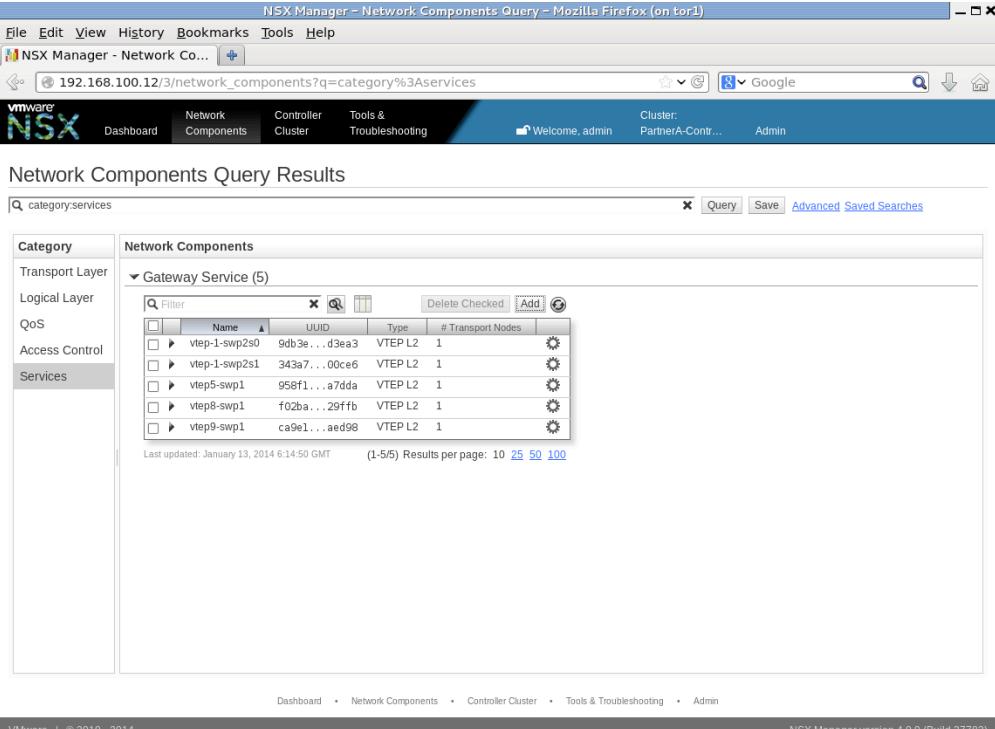
After you finish bootstrapping the NSX integration, you need to configure the transport layer. For each host-facing switch port that is to be associated with a VXLAN instance, define a **Gateway Service** for the port.

1. In NSX Manager, add a new gateway service. Click the **Network Components** tab, then the **Services** category. Under **Gateway Service**, click **Add**. The Create Gateway Service wizard appears.
2. In the Create Gateway Service dialog, select *VTEP L2 Gateway Service* as the **Gateway Service Type**.



3. Give the service a **Display Name** to represent the VTEP in NSX.
4. Click **Add Gateway** to associate the service with the gateway you created earlier.
5. In the **Transport Node** field, choose the name of the gateway you created earlier.
6. In the **Port ID** field, choose the physical port on the gateway (for example, swp10) that will connect to a logical L2 segment and carry data traffic.
7. Click **OK** to save this gateway in the service, then click **Save** to save the gateway service.

The gateway service shows up as type *VTEP L2* in NSX.



The screenshot shows the NSX Manager interface for querying network components. The left sidebar has a 'Category' dropdown set to 'Services'. Under 'Logical Layer', 'Gateway Service' is selected, showing 5 results:

Name	UUID	Type	# Transport Nodes
vtep-1-swp2s0	9db3e...d3ea3	VTEP L2	1
vtep-1-swp2s1	343a7...00ce6	VTEP L2	1
vtep5-swp1	958f1...a7dda	VTEP L2	1
vtep8-swp1	f02ba...29ffb	VTEP L2	1
vtep9-swp1	c9e01...aed98	VTEP L2	1

Last updated: January 13, 2014 6:14:50 GMT (1-5/5) Results per page: 10 25 50 100

At the bottom, it says 'NSX Manager version 4.0.0 (Build 27783)'.

Next, you will configure the logical layer on NSX.

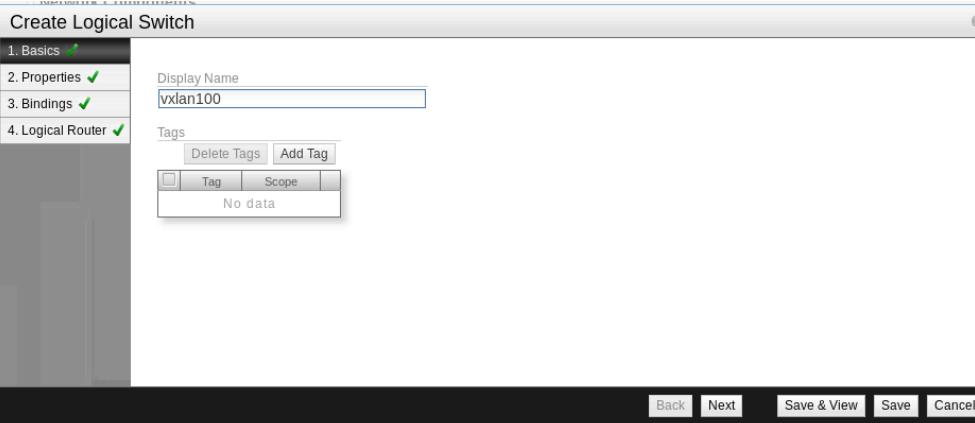
Configuring the Logical Layer

To complete the integration with NSX, you need to configure the logical layer, which requires defining a logical switch (the VXLAN instance) and all the logical ports needed.

Defining Logical Switches

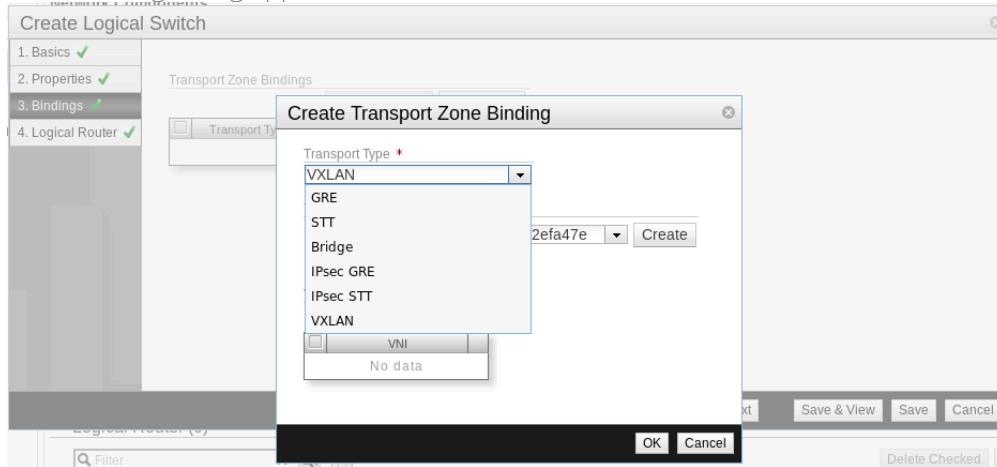
To define the logical switch, do the following:

1. In NSX Manager, add a new logical switch. Click the **Network Components** tab, then the **Logical Layer** category. Under **Logical Switch**, click **Add**. The Create Logical Switch wizard appears.
2. In the **Display Name** field, enter a name for the logical switch, then click **Next**.

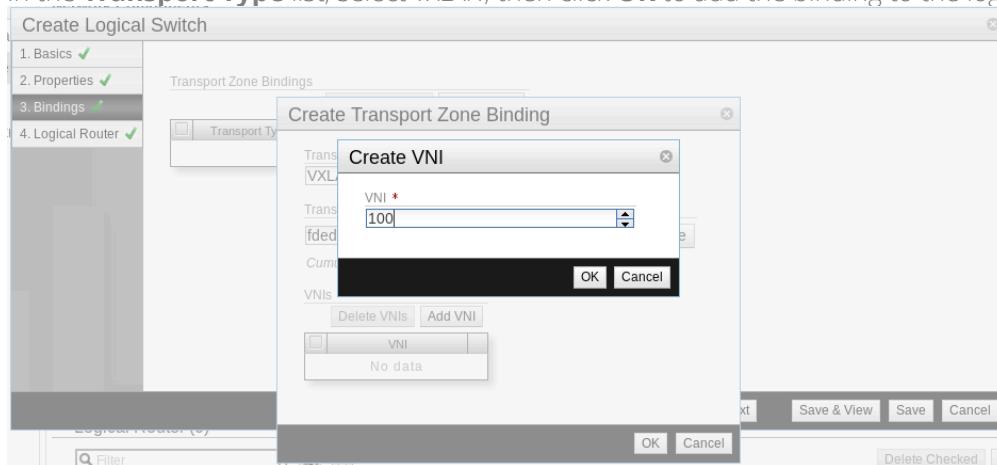


3. Under **Replication Mode**, select **Service Nodes**, then click **Next**.

- Specify the transport zone bindings for the logical switch. Click **Add Binding**. The Create Transport Zone Binding dialog appears.



- In the **Transport Type** list, select **VXLAN**, then click **OK** to add the binding to the logical switch.



- In the **VNI** field, assign the switch a VNI ID, then click **OK**.



Do not use 0 or 16777215 as the VNI ID, as they are reserved values under Cumulus Linux.

- Click **Save** to save the logical switch configuration.

NSX Manager - Network Components Query - Mozilla Firefox (on tor1)

File Edit View History Bookmarks Tools Help

NSX Manager - Network Co... [+]

192.168.100.12/3/network_components?q=category%3Alogical_layer

Google

VMware NSX Dashboard Network Components Controller Cluster Tools & Troubleshooting Welcome, admin Cluster: PartnerA-Contr... Admin

Network Components Query Results

category:logical_layer Query Save [Advanced Saved Searches](#)

Category	Network Components																																									
Transport Layer																																										
Logical Layer	Logical Switch (3) <table border="1"> <thead> <tr> <th>Fabric</th> <th>Name</th> <th>UUID</th> <th>Logical Switch Ports</th> <th>Logical Router</th> <th>Transport Zone Bindings</th> <th>Replication Mode</th> <th>Port Isolation</th> </tr> </thead> <tbody> <tr> <td>vxlan100</td> <td>47a37...b1790</td> <td></td> <td>0</td> <td>-</td> <td>1</td> <td>Service Node</td> <td>Disabled</td> </tr> <tr> <td>LS-B</td> <td>80b3e...36454</td> <td></td> <td>1</td> <td>-</td> <td>1</td> <td>Service Node</td> <td>Disabled</td> </tr> <tr> <td>LS-A</td> <td>c1be3...fb689</td> <td></td> <td>1</td> <td>-</td> <td>1</td> <td>Service Node</td> <td>Disabled</td> </tr> </tbody> </table> <p>Last updated: January 13, 2014 15:12:16 GMT (1-3/3) Results per page: 10 25 50 100</p>										Fabric	Name	UUID	Logical Switch Ports	Logical Router	Transport Zone Bindings	Replication Mode	Port Isolation	vxlan100	47a37...b1790		0	-	1	Service Node	Disabled	LS-B	80b3e...36454		1	-	1	Service Node	Disabled	LS-A	c1be3...fb689		1	-	1	Service Node	Disabled
Fabric	Name	UUID	Logical Switch Ports	Logical Router	Transport Zone Bindings	Replication Mode	Port Isolation																																			
vxlan100	47a37...b1790		0	-	1	Service Node	Disabled																																			
LS-B	80b3e...36454		1	-	1	Service Node	Disabled																																			
LS-A	c1be3...fb689		1	-	1	Service Node	Disabled																																			
QoS																																										
Access Control																																										
Services																																										
	Logical Switch Port (2) <table border="1"> <thead> <tr> <th>Admin</th> <th>Link</th> <th>Fabric</th> <th>Message</th> <th>Name</th> <th>Port</th> <th>Switch Name</th> <th>UUID</th> <th>Attachment</th> <th>Attached MAC</th> </tr> </thead> <tbody> <tr> <td>Up</td> <td>Up</td> <td>Up</td> <td>-</td> <td>v1</td> <td>1</td> <td>LS-A</td> <td>3db81...e2af</td> <td>VIF:5e690...42df</td> <td>52:54:00:15:44:34</td> </tr> <tr> <td>Up</td> <td>Up</td> <td>Up</td> <td>-</td> <td>v2</td> <td>3</td> <td>LS-B</td> <td>a080d...b5588</td> <td>VIF:0afff...a8571</td> <td>52:54:00:92:25:bd</td> </tr> </tbody> </table> <p>Last updated: January 13, 2014 9:03:07 GMT (1-2/2) Results per page: 10 25 50 100</p>										Admin	Link	Fabric	Message	Name	Port	Switch Name	UUID	Attachment	Attached MAC	Up	Up	Up	-	v1	1	LS-A	3db81...e2af	VIF:5e690...42df	52:54:00:15:44:34	Up	Up	Up	-	v2	3	LS-B	a080d...b5588	VIF:0afff...a8571	52:54:00:92:25:bd		
Admin	Link	Fabric	Message	Name	Port	Switch Name	UUID	Attachment	Attached MAC																																	
Up	Up	Up	-	v1	1	LS-A	3db81...e2af	VIF:5e690...42df	52:54:00:15:44:34																																	
Up	Up	Up	-	v2	3	LS-B	a080d...b5588	VIF:0afff...a8571	52:54:00:92:25:bd																																	
	Logical Router (0) <table border="1"> <thead> <tr> <th>Fabric</th> <th>Name</th> <th>UUID</th> <th>Distributed</th> <th>NAT Synchronization</th> <th>Replication Mode</th> <th>Logical Router Ports</th> <th>Routing Type</th> <th>L3 Gateway Service</th> </tr> </thead> <tbody> <tr> <td colspan="9">No Logical Routers</td> </tr> </tbody> </table>										Fabric	Name	UUID	Distributed	NAT Synchronization	Replication Mode	Logical Router Ports	Routing Type	L3 Gateway Service	No Logical Routers																						
Fabric	Name	UUID	Distributed	NAT Synchronization	Replication Mode	Logical Router Ports	Routing Type	L3 Gateway Service																																		
No Logical Routers																																										

Dashboard • Network Components • Controller Cluster • Tools & Troubleshooting • Admin

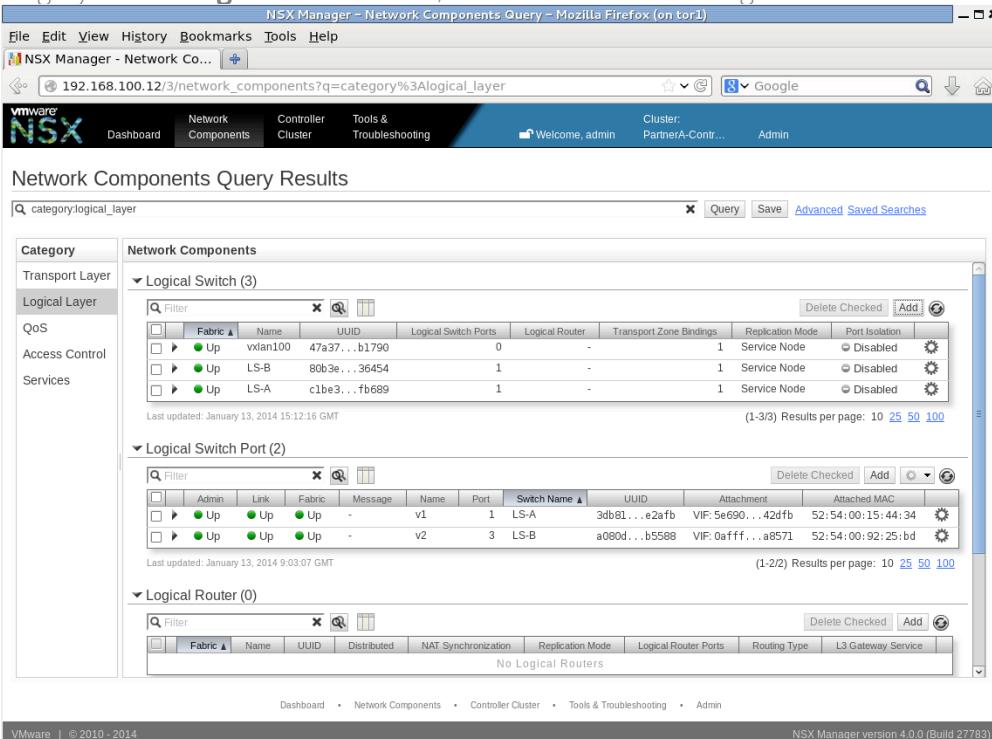
VMware | © 2010 - 2014 NSX Manager version 4.0.0 (Build 27783)

Defining Logical Switch Ports

As the final step, define the logical switch ports. They can be virtual machine VIF interfaces from a registered OVS, or a VTEP gateway service instance on this switch, as defined above in the Configuring the Transport Layer. A VLAN binding can be defined for each VTEP gateway service associated with the particular logical switch.

To define the logical switch ports, do the following:

- In NSX Manager, add a new logical switch port. Click the **Network Components** tab, then the **Logical Layer** category. Under **Logical Switch Port**, click **Add**. The Create Logical Switch Port



The screenshot shows the NSX Manager interface with the following details:

- Network Components Query Results**
- Category** sidebar: Transport Layer, Logical Layer, QoS, Access Control, Services.
- Logical Switch (3)** table:

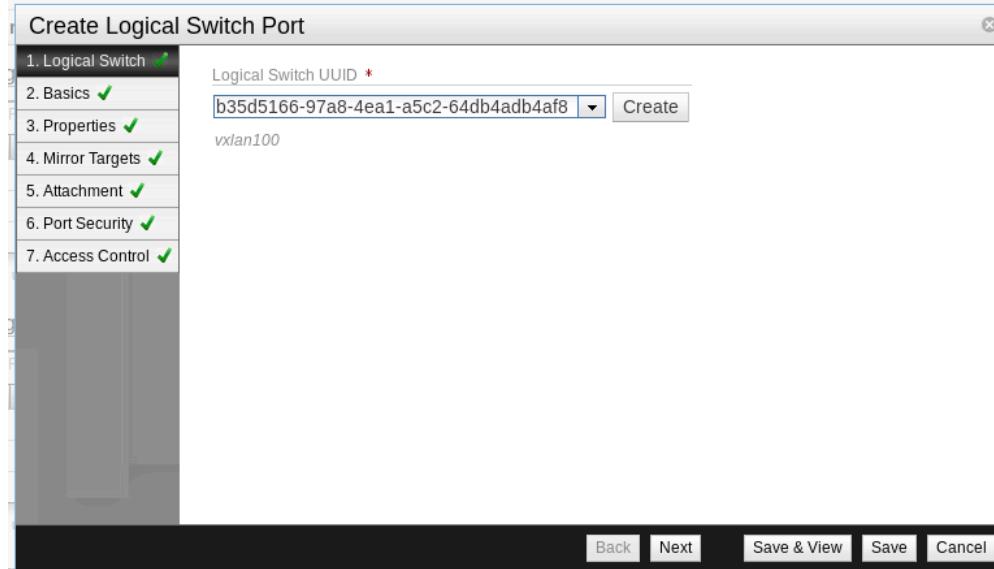
Fabric	Name	UUID	Logical Switch Ports	Logical Router	Transport Zone Bindings	Replication Mode	Port Isolation
Up	vxlan100	47a37...b1790	0	-	1	Service Node	Disabled
Up	LS-B	80b3e...36454	1	-	1	Service Node	Disabled
Up	LS-A	c1be3...fb689	1	-	1	Service Node	Disabled
- Logical Switch Port (2)** table:

Admin	Link	Fabric	Message	Name	Port	Switch Name	UUID	Attachment	Attached MAC
Up	Up	Up	-	v1	1	LS-A	3db81...e2af	VIF: 5e690...42df	52:54:00:15:44:34
Up	Up	Up	-	v2	3	LS-B	a080d...b5588	VIF: 0affff...a8571	52:54:00:92:25:bd
- Logical Router (0)** table:

Fabric	Name	UUID	Distributed	NAT Synchronization	Replication Mode	Logical Router Ports	Routing Type	L3 Gateway Service
No Logical Routers								

wizard appears.

- In the **Logical Switch UUID** list, select the logical switch you created above, then click **Create**.

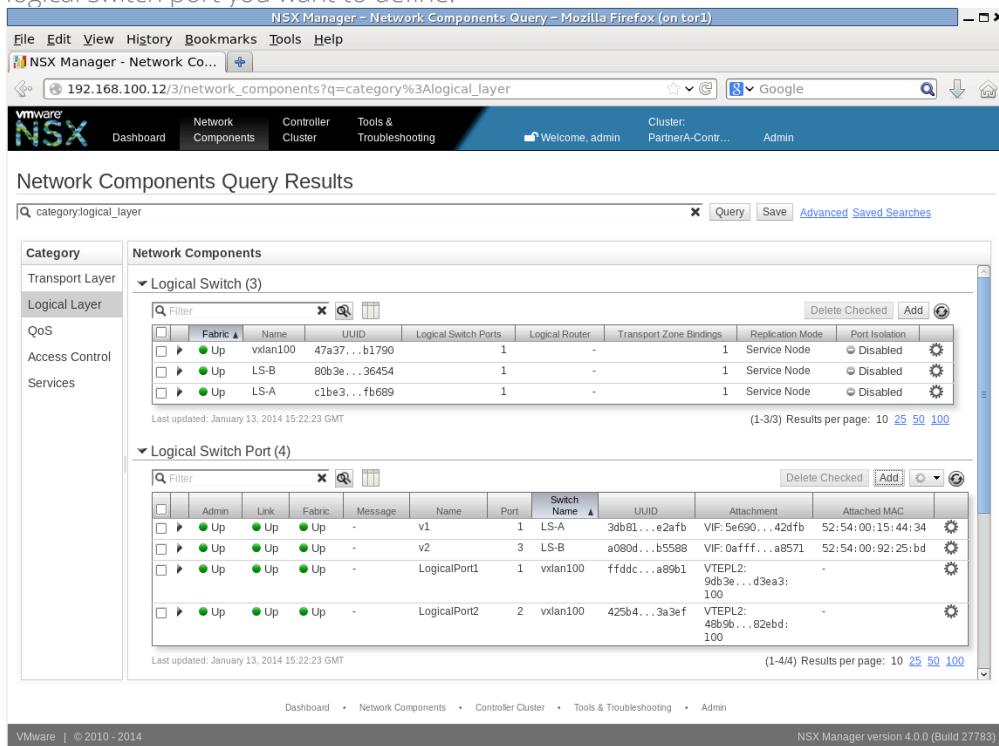


The screenshot shows the 'Create Logical Switch Port' wizard step 2: Basics. The left sidebar shows steps 1 through 7, all completed with green checkmarks. The main area has the following fields:

- Logical Switch UUID ***: A dropdown menu showing 'b35d5166-97a8-4ea1-a5c2-64db4adb4af8'.
- Create** button: A grey button with white text.

- In the **Display Name** field, give the port a name that indicates it is the port that connects the gateway, then click **Next**.
- In the **Attachment Type** list, select **VTEP L2 Gateway**.
- In the **VTEP L2 Gateway Service UUID** list, choose the name of the gateway service you created earlier.
- In the **VLAN** list, you can optionally choose a VLAN if you wish to connect only traffic on a specific VLAN of the physical network. Leave it blank to handle all traffic.

7. Click **Save** to save the logical switch port. Connectivity is established. Repeat this procedure for each logical switch port you want to define.



The screenshot shows the NSX Manager interface for Network Components Query. The left sidebar has categories: Transport Layer, Logical Layer (selected), QoS, Access Control, and Services. The main area displays two tables:

- Logical Switch (3)**: Shows three entries:

Fabric	Name	UUID	Logical Switch Ports	Logical Router	Transport Zone Bindings	Replication Mode	Port Isolation
Up	vxlan100	47a37...b1790	1	-	1 Service Node	Disabled	
Up	LS-B	80b3e...36454	1	-	1 Service Node	Disabled	
Up	LS-A	c1be3...fb689	1	-	1 Service Node	Disabled	

 Last updated: January 13, 2014 15:22:23 GMT
- Logical Switch Port (4)**: Shows four entries:

Admin	Link	Fabric	Message	Name	Port	Switch Name	UUID	Attachment	Attached MAC
Up	Up	Up	-	v1	1	LS-A	3db81...e2afb	VIF: 5e690...42dfb	52:54:00:15:44:34
Up	Up	Up	-	v2	3	LS-B	a080d...b5588	VIF: 0afff...a8571	52:54:00:92:25:bd
Up	Up	Up	-	LogicalPort1	1	vxlan100	ffddc...a89b1	VTEPL2: 9db3e...d3ea3: 100	
Up	Up	Up	-	LogicalPort2	2	vxlan100	425b4...3a3ef	VTEPL2: 489b...82ebd: 100	

 Last updated: January 13, 2014 15:22:23 GMT

Verifying the VXLAN Configuration

Once configured, you can verify the VXLAN configuration using these Cumulus Linux commands in a terminal connected to the switch:

```
cumulus@switch1:~$ sudo ip -d link show vxln100
71: vxln100: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
  master br-vxln100 state UNKNOWN mode DEFAULT
    link/ether d2:ca:78:bb:7c:9b brd ff:ff:ff:ff:ff:ff
    vxlan id 100 local 172.16.20.157 port 32768 61000 nolearning ageing 300
      svcnode 172.16.21.125
```

or

```
cumulus@switch1:~$ sudo bridge fdb show
52:54:00:ae:2a:e0 dev vxln100 dst 172.16.21.150 self permanent
d2:ca:78:bb:7c:9b dev vxln100 permanent
90:e2:ba:3f:ce:34 dev swp2s1.100
90:e2:ba:3f:ce:35 dev swp2s0.100
44:38:39:00:48:0e dev swp2s1.100 permanent
44:38:39:00:48:0d dev swp2s0.100 permanent
```

Persistent VXLAN Configuration in NSX

If you want your VXLAN configuration to persist across upgrades of Cumulus Linux (see [Making Configurations Persist across Upgrades \(see page\)](#)), you need to include the following items in the persistent configuration. Use `scp` to copy the files to `/mnt/persist`:

- `/usr/share/openvswitch/ovs-ctl-vtep`
- Certificates and key pairs, as above
- `/etc/default/openvswitch-vtep`
- The `ovsdb` database file; the default is `/var/lib/openvswitch/conf.db`



Copying the `ovsdb` database file is optional; the persistent database file helps to speed up convergence on a system upgrade. NSX Manager pushes any configuration created or changed in NSX Manager when the connection with the VTEP is reestablished, which overwrites the database file.

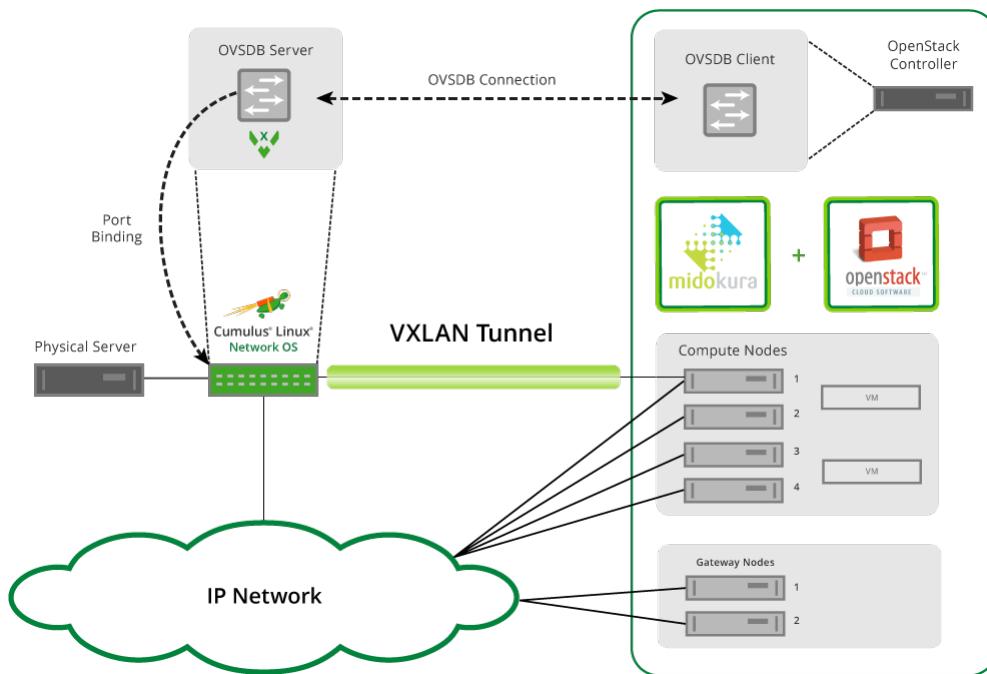
Troubleshooting VXLANs in NSX

Use `ovsdb-client dump` to troubleshoot issues on the switch. It verifies that the controller and switch handshake is successful. This command works only for VXLANs integrated with NSX:

```
cumulus@switch:~$ sudo ovsdb-client dump -f list | grep -A 7 "Manager"
Manager table
_uuid              : 505f32af-9acb-4182-a315-022e405aa479
inactivity_probe   : 30000
is_connected       : true
max_backoff        : []
other_config       : {}
status             : {sec_since_connect="18223", sec_since_disconnect="
18225", state=ACTIVE}
target             : "ssl:192.168.100.17:6632"
```

Integrating Hardware VTEPs with Midokura MidoNet and OpenStack

Cumulus Linux seamlessly integrates with the MidoNet OpenStack infrastructure, where the switches provide the VTEP gateway for terminating VXLAN tunnels from within MidoNet. MidoNet connects to the OVSDB server running on the Cumulus Linux switch, and exchanges information about the VTEPs and MAC addresses associated with the OpenStack Neutron networks. This provides seamless Ethernet connectivity between virtual and physical server infrastructures.



Contents

- Contents (see page 262)
- Getting Started (see page 263)
 - Caveats and Errata (see page 263)
 - Preparing for the MidoNet Integration (see page 263)
 - Enabling the openvswitch-vtep Package (see page 263)
 - Bootstrapping the OVSDB Server and VTEP (see page 264)
 - Automating with the Bootstrap Script (see page 264)
 - Manually Bootstrapping (see page 265)
 - Configuring MidoNet VTEP and Port Bindings (see page 266)
 - Using the MidoNet Manager GUI (see page 266)
 - Creating a Tunnel Zone (see page 266)
 - Adding Hosts to a Tunnel Zone (see page 266)
 - Creating the VTEP (see page 267)
 - Binding Ports to the VTEP (see page 268)
 - Using the MidoNet CLI (see page 269)
- Troubleshooting MidoNet and Cumulus VTEPs (see page 271)
 - Troubleshooting the Control Plane (see page 272)
 - Verifying VTEP and OVSDB Services (see page 272)
 - Verifying OVSDB-server Connections (see page 272)
 - Verifying the VXLAN Bridge and VTEP Interfaces (see page 272)
 - Datapath Troubleshooting (see page 273)

- Verifying IP Reachability (see page 274)
- MidoNet VXLAN Encapsulation (see page 274)
- Inspecting the OVSDB (see page 275)
 - Using VTEP-CTL (see page 275)
 - Listing the Physical Switch (see page 275)
 - Listing the Logical Switch (see page 275)
 - Listing Local or Remote MAC Addresses (see page 275)
 - Getting Open Vswitch Database (OVSDB) Data (see page 276)

Getting Started

Before you create VXLANs with MidoNet, make sure you have the following components:

- A switch (L2 gateway) with a Trident 2 chipset running Cumulus Linux 2.0 and later
- OVSDB server (`ovsdb-server`), included in Cumulus Linux 2.0 and later
- VTEPd (`ovs-vtep`), included in Cumulus Linux 2.0 and later

Integrating a VXLAN with MidoNet involves:

- Preparing for the MidoNet integration
- Bootstrapping the OVS and VTEP
- Configuring the MidoNet VTEP binding
- Verifying the VXLAN configuration

Caveats and Errata

- There is no support for VXLAN routing in the Trident 2 chipset; use a loopback interface or external router.
- For more information about MidoNet, see the MidoNet Operations Guide, version 1.8 or later.

Preparing for the MidoNet Integration

Before you start configuring the MidoNet tunnel zones, VTEP binding and connecting virtual ports to the VXLAN, you need to complete the bootstrap process on each switch to which you plan to build VXLAN tunnels. This creates the VTEP gateway and initializes the OVS database server. You only need to do the bootstrapping once, before you begin the MidoNet integration.

Enabling the `openvswitch-vtep` Package

Before you start bootstrapping the integration, you need to enable the `openvswitch-vtep` package, since it is disabled by default in Cumulus Linux.

1. Edit the `/etc/default/openvswitch-vtep` file, changing the `START` option from `no` to `yes`. This simple `sed` command does this, and creates a backup as well:

```
sudo sed -i.bak s/START=no/START=yes/g /etc/default/openvswitch-vtep
```



Make sure to include this file in persistent storage prior to Cumulus Linux upgrades.

2. Start the daemon:

```
cumulus@switch$ sudo service openvswitch-vtep start
```



Prior to Cumulus Linux 2.5.1, you must edit the control file `/usr/share/openvswitch/scripts/ovs-ctl-vtep`, by adding a parameter for the remote OVS connection. The OVS server connection is not encrypted, so it is necessary to change the PTCP port in this file. The following `sed` command makes the proper change:

```
sed -i.bak "/remote=db/a \\\tset \"\$@\\" --remote-ptcp:6632"
/usr/share/openvswitch/scripts/ovs-ctl-vtep
```

Bootstrapping the OVSDB Server and VTEP

Automating with the Bootstrap Script

The `vtep-bootstrap` script is available so you can do the bootstrapping automatically. For information, read `man vtep-bootstrap`. This script requires three parameters, in this order:

- Switch name: The name of the switch that is the VTEP gateway.
- Tunnel IP address: The datapath IP address of the VTEP.
- Management IP address: The IP address of the switch's management interface.

For example, click [here](#) ...

```
root@sw11:~# vtep-bootstrap sw11 10.111.1.1 10.50.20.21 --no_encryption
```

```
Executed:
define physical switch
().
Executed:
define local tunnel IP address on the switch
().
Executed:
define management IP address on the switch
().
Executed:
restart a service
```

```
(Killing ovs-vtep (28170).  
Killing ovsdb-server (28146).  
Starting ovsdb-server.  
Starting ovs-vtep (28170).)
```



Prior to Cumulus Linux 2.5.1, the `vtep-bootstrap` command required 4 parameters: `<switch_name> <controller_ip> <tunnel_ip> <management_ip>`. Since MidoNet does not have a controller, you need to use a dummy IP address (for example, 1.1.1.1) for the controller parameter in the bootstrap script. After the script completes, delete the VTEP manager, since it is not needed and will otherwise fill the logs with inconsequential error messages:

```
vtep-ctl del-manager
```

Manually Bootstrapping

If you don't use the bootstrap script, then you must initialize the OVS database instance manually, and create the VTEP.

Perform the following commands in order (see the automated bootstrapping example above for values):

1. Define the switch in OVSDB:

```
sudo vtep-ctl add-ps <switch_name>
```

2. Define the VTEP tunnel IP address:

```
sudo vtep-ctl set Physical_switch <switch_name> tunnel_ips=<tunnel_ip>
```

3. Define the management interface IP address:

```
sudo vtep-ctl set Physical_switch <switch_name>  
management_ips=<management_ip>
```

4. Restart the OVSDB server and vtep:

```
sudo service openvswitch-vtep restart
```

At this point, the switch is ready to connect to MidoNet. The rest of the configuration is performed in the MidoNet Manager GUI, or using the MidoNet API.

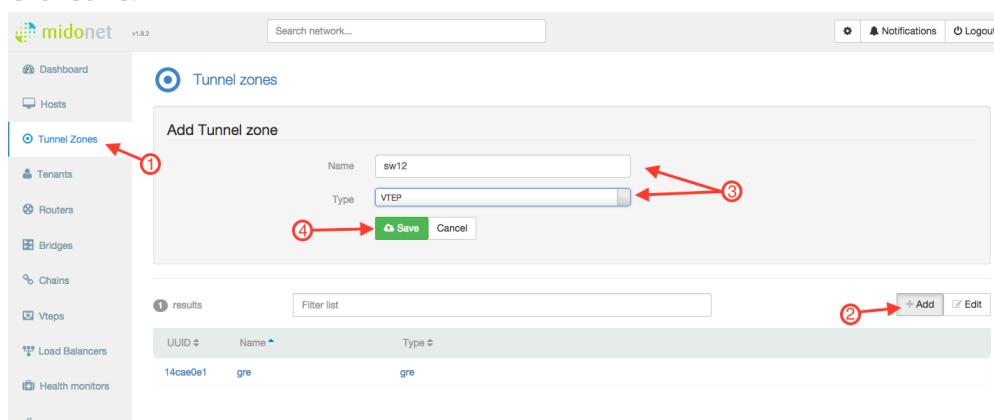
Configuring MidoNet VTEP and Port Bindings

This part of the configuration sets up MidoNet and OpenStack to connect the virtualization environment to the Cumulus Linux switch. The `midonet-agent` is the networking component that manages the VXLAN, while the Open Virtual Switch (OVS) client on the OpenStack controller node communicates MAC address information between the `midonet-agent` and the Cumulus Linux OVS database (OVSDB) server.

Using the MidoNet Manager GUI

Creating a Tunnel Zone

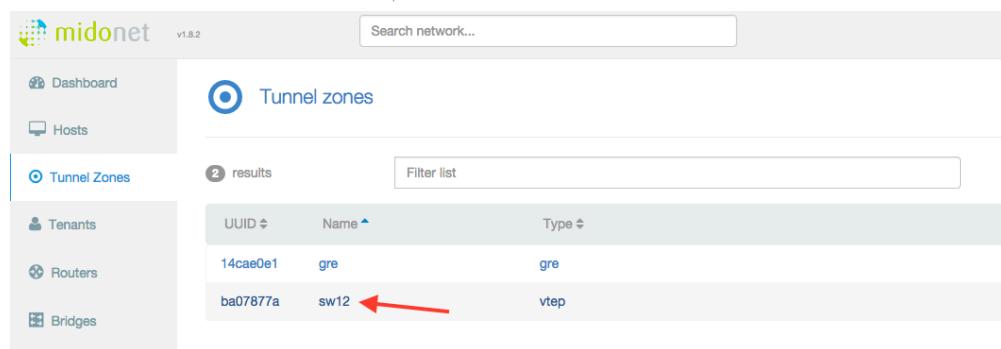
1. Click **Tunnel Zones** in the menu on the left side.
2. Click **Add**.
3. Give the tunnel zone a **Name** and select "**VTEP**" for the **Type**.
4. Click **Save**.



UUID	Name	Type
14cae0e1	gre	gre

Adding Hosts to a Tunnel Zone

Once the tunnel zone is created, click the name of the tunnel zone to view the hosts table.

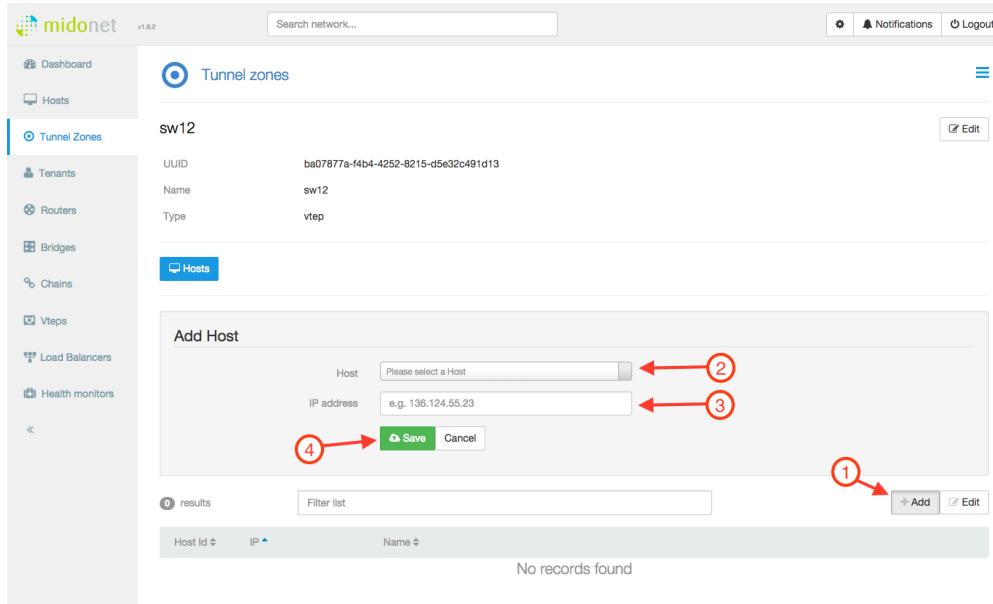


UUID	Name	Type
14cae0e1	gre	gre
ba07877a	sw12	vtep

The tunnel zone is a construct used to define the VXLAN source address used for the tunnel. This host's address is used for the source of the VXLAN encapsulation, and traffic will transit into the routing domain from this point. Thus, the host must have layer 3 reachability to the Cumulus Linux switch tunnel IP.

Next, add a host entry to the tunnel zone:

1. Click **Add**.
2. Select a host from the **Host** list.
3. Provide the tunnel source **IP Address** to use on the selected host.
4. Click **Save**.



The screenshot shows the midonet web interface. On the left, a sidebar menu includes options like Dashboard, Hosts, Tunnel Zones, Tenants, Routers, Bridges, Chains, Vteps, Load Balancers, and Health monitors. The 'Tunnel Zones' option is selected. In the main area, a 'Tunnel zones' table is shown with one entry: 'sw12' (UUID: ba07877a-f4b4-4252-8215-d5e32c491d13, Name: sw12, Type: vtep). Below this is a 'Hosts' table with one entry: '4d03509b' (Host Id), '10.50.21.182' (IP), and 'os-compute1' (Name). A modal dialog titled 'Add Host' is open, containing fields for 'Host' (dropdown) and 'IP address' (input field with placeholder 'e.g. 136.124.55.23'). At the bottom of the dialog are 'Save' and 'Cancel' buttons. Red numbered arrows indicate the steps: 1 points to the 'Host' dropdown, 2 points to the 'IP address' input, 3 points to the 'Save' button, and 4 points to the 'Cancel' button. A red circle also highlights the 'Add' button in the 'Hosts' table header.

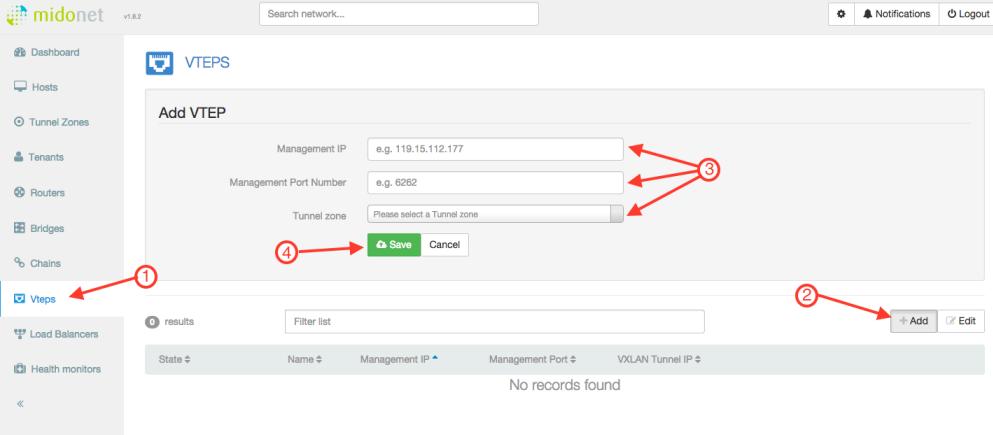
The host list now displays the new entry:



Host Id	IP	Name
4d03509b	10.50.21.182	os-compute1

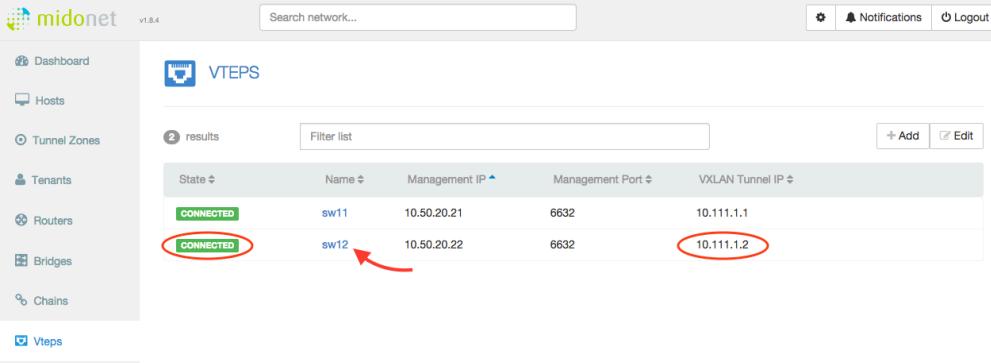
Creating the VTEP

1. Click the **Vteps** menu on the left side.
2. Click **Add**.
3. Fill out the fields using the same information you used earlier on the switch for the bootstrap procedure:
 - **Management IP** is typically the eth0 address of the switch. This tells the OVS-client to connect to the OVSDB-server on the Cumulus Linux switch.
 - **Management Port Number** is the PTCP port you configured in the `ovs-ctl-vtep` script earlier (the example uses 6632).
 - **Tunnel Zone** is the name of the zone you created in the previous procedure.
4. Click **Save**.



The screenshot shows the MidoNet web interface with the 'VTEPS' tab selected. On the left, a sidebar has a checked checkbox next to 'Vteps'. In the main area, there's a 'Add VTEP' form with fields for 'Management IP' (e.g., 119.15.112.177), 'Management Port Number' (e.g., 6262), and 'Tunnel zone' (a dropdown menu). Below the form are buttons for 'Save' and 'Cancel'. Red numbered arrows indicate: 1) the 'Vteps' link in the sidebar; 2) the '+ Add' button; 3) the 'Management IP' and 'Management Port Number' fields; and 4) the 'Save' button.

The new VTEP appears in the list below. MidoNet then initiates a connection between the OpenStack Controller and the Cumulus Linux switch. If the OVS client is successfully connected to the OVSDB server, the VTEP entry should display the switch name and VXLAN tunnel IP address, which you specified during the bootstrapping process.

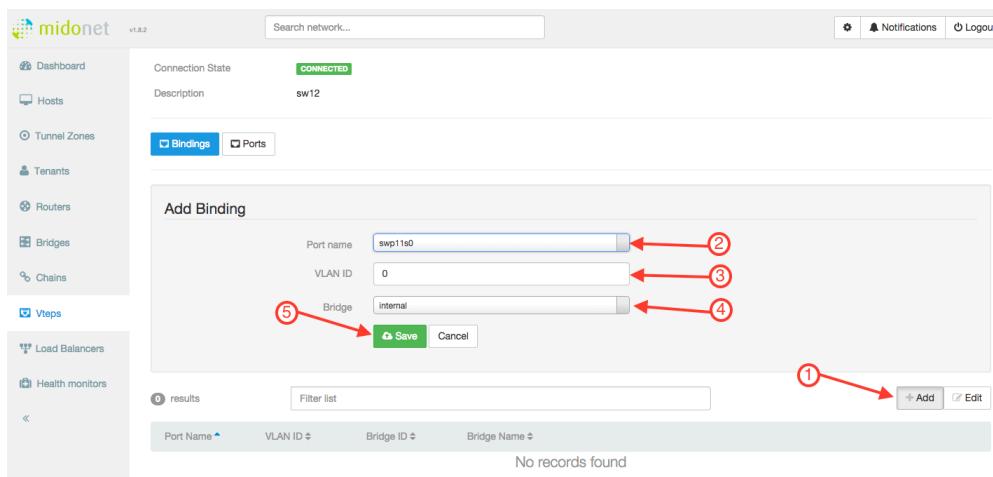


The screenshot shows the MidoNet web interface with the 'VTEPS' tab selected. The sidebar has a checked checkbox next to 'Vteps'. The main area displays a table of VTEPs with columns: State, Name, Management IP, Management Port, and VXLAN Tunnel IP. There are two entries: 'sw11' and 'sw12'. Both entries show 'CONNECTED' in the State column, '10.50.20.21' in the Management IP column, '6632' in the Management Port column, and '10.111.1.1' in the VXLAN Tunnel IP column for sw11. For sw12, the VXLAN Tunnel IP is '10.111.1.2'. Red circles highlight the 'CONNECTED' status for both entries and the VXLAN Tunnel IP for sw12.

Binding Ports to the VTEP

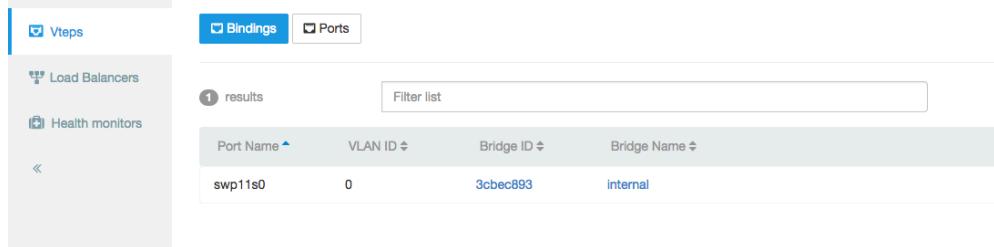
Now that connectivity is established to the switch, you need to add a physical port binding to the VTEP on the Cumulus Linux switch:

1. Click **Add**.
2. In the **Port Name** list, select the port on the Cumulus Linux switch that you are using to connect to the VXLAN segment.
3. Specify the **VLAN ID** (enter 0 for untagged).
4. In the **Bridge** list, select the MidoNet bridge that the instances (VMs) are using in OpenStack.
5. Click **Save**.



The screenshot shows the MidoNet Manager interface. On the left, there's a sidebar with various navigation options like Dashboard, Hosts, Tunnel Zones, Tenants, Routers, Bridges, Chains, Vtaps, Load Balancers, and Health monitors. The main area shows a 'Connected' status for a device named 'sw12'. Below that, there are tabs for 'Bindings' and 'Ports'. An 'Add Binding' dialog is open, prompting for a Port name (swp11s0), VLAN ID (0), and Bridge (internal). A red arrow labeled 1 points to the 'Save' button in the dialog. Red arrows labeled 2, 3, 4, and 5 point to the Port name, VLAN ID, Bridge, and Save buttons respectively. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

You should see the port binding displayed in the binding table under the VTEP.



The screenshot shows the 'Bindings' table under the Vtaps tab. It contains one row of data: Port Name: swp11s0, VLAN ID: 0, Bridge ID: 3bec893, and Bridge Name: internal. A red arrow labeled 1 points to the 'Add' button located at the top right of the table header.

Once the port is bound, this automatically configures a VXLAN bridge interface, and includes the VTEP interface and the port bound to the bridge. Now the OpenStack instances (VMs) should be able to ping the hosts connected to the bound port on the Cumulus switch. The Troubleshooting section below demonstrates the verification of the VXLAN data and control planes.

Using the MidoNet CLI

To get started with the MidoNet CLI, you can access the CLI prompt on the OpenStack Controller:

```
root@os-controller:~# midonet-cli
midonet>
```

Now from the MidoNet CLI, the commands explained in this section perform the same operations depicted in the previous section with the MidoNet Manager GUI.

1. Create a tunnel zone with a name and type vtep:

```
midonet> tunnel-zone create name sw12 type vtep
tzone1
```

2. The tunnel zone is a construct used to define the VXLAN source address used for the tunnel. This host's address is used for the source of the VXLAN encapsulation, and traffic will transit into the routing domain from this point. Thus, the host must have layer 3 reachability to the Cumulus Linux switch tunnel IP.

- First, get the list of available hosts connected to the Neutron network and the MidoNet bridge.
- Next, get a listing of all the interfaces.
- Finally, add a host entry to the tunnel zone ID returned in the previous step, and specify which interface address to use.

```
midonet> list host
host host0 name os-compute1 alive true
host host1 name os-network alive true
midonet> host host0 list interface
iface midonet host_id host0 status 0 addresses [] mac 02:4b:
38:92:dd:ce mtu 1500 type Virtual endpoint DATAPATH
iface lo host_id host0 status 3 addresses [u'127.0.0.1',
u'169.254.169.254', u'0:0:0:0:0:0:0:1'] mac 00:00:00:00:00:00:
00 mtu 65536 type Virtual endpoint LOCALHOST
iface virbr0 host_id host0 status 1 addresses
[u'192.168.122.1'] mac 22:6e:63:90:1f:69 mtu 1500 type
Virtual endpoint UNKNOWN
iface tap7cfccf84c-26 host_id host0 status 3 addresses
[u'fe80:0:0:0:e822:94ff:fee2:d41b'] mac ea:22:94:e2:d4:1b
mtu 65000 type Virtual endpoint DATAPATH
iface eth1 host_id host0 status 3 addresses
[u'10.111.0.182', u'fe80:0:0:0:5054:ff:fe85:acd6'] mac 52:
54:00:85:ac:d6 mtu 1500 type Physical endpoint PHYSICAL
iface tapfd4abcea-df host_id host0 status 3 addresses
[u'fe80:0:0:0:14b3:45ff:fe94:5b07'] mac 16:b3:45:94:5b:07
mtu 65000 type Virtual endpoint DATAPATH
iface eth0 host_id host0 status 3 addresses
[u'10.50.21.182', u'fe80:0:0:0:5054:ff:feef:c5dc'] mac 52:
54:00:ef:c5:dc mtu 1500 type Physical endpoint PHYSICAL
midonet> tunnel-zone tzone0 add member host host0 address
10.111.0.182
zone tzone0 host host0 address 10.111.0.182
```

Repeat this procedure for each OpenStack host connected to the Neutron network and the MidoNet bridge.

3. Create a VTEP and assign it to the tunnel zone ID returned in the previous step. The management IP address (the destination address for the VXLAN/remote VTEP) and the port must be the same ones you configured in the `vtep-bootstrap` script or the manual bootstrapping:

```
midonet> vtep add management-ip 10.50.20.22 management-port 6632
tunnel-zone tzone0
name sw12 description sw12 management-ip 10.50.20.22 management-port
6632 tunnel-zone tzone0 connection-state CONNECTED
```

In this step, MidoNet initiates a connection between the OpenStack Controller and the Cumulus Linux switch. If the OVS client is successfully connected to the OVSDB server, the returned values should show the name and description matching the `switch-name` parameter specified in the bootstrap process.



Verify the connection-state as CONNECTED, otherwise if ERROR is returned, you must debug. Typically this only fails if the `management-ip` and/or `management-port` settings are wrong.

4. The VTEP binding uses the information provided to MidoNet from the OVSDB server, providing a list of ports that the hardware VTEP can use for layer 2 attachment. This binding virtually connects the physical interface to the overlay switch, and joins it to the Neutron bridged network.

First, get the UUID of the Neutron network behind the MidoNet bridge:

```
midonet> list bridge
bridge bridge0 name internal state up
bridge bridge1 name internal2 state up
midonet> show bridge bridge1 id
6c9826da-6655-4fe3-a826-4dcba6477d2d
```

Next, create the VTEP binding, using the UUID and the switch port being bound to the VTEP on the remote end. If there is no VLAN ID, set `vlan` to 0:

```
midonet> vtep name sw12 binding add network-id 6c9826da-6655-4fe3-a826-
4dcba6477d2d physical-port swp11s0 vlan 0
management-ip 10.50.20.22 physical-port swp11s0 vlan 0 network-id
6c9826da-6655-4fe3-a826-4dcba6477d2d
```

At this point, the VTEP should be connected, and the layer 2 overlay should be operational. From the openstack instance (VM), you should be able to ping a physical server connected to the port bound to the hardware switch VTEP.

Troubleshooting MidoNet and Cumulus VTEPs

As with any complex system, there is a control plane and data plane.

Troubleshooting the Control Plane

In this solution, the control plane consists of the connection between the OpenStack Controller, and each Cumulus Linux switch running the `ovsdb-server` and `vtep` daemons.

Verifying VTEP and OVSDB Services

First, it is important that the OVSDB server and `ovs-vtep` daemon are running. Verify this is the case:

```
cumulus@switch12:~$ service openvswitch-vtep status
ovsdb-server is running with pid 17440
ovs-vtep is running with pid 17444
```

Verifying OVSDB-server Connections

From the OpenStack Controller host, verify that it can connect to the `ovsdb-server`. Telnet to the switch IP address on port 6632:

```
root@os-controller:~# telnet 10.50.20.22 6632
Trying 10.50.20.22...
Connected to 10.50.20.22.
Escape character is '^]'.
<Ctrl+c>
Connection closed by foreign host.
```

If the connection fails, verify IP reachability from the host to the switch. If that succeeds, it is likely the bootstrap process did not set up port 6632. Redo the bootstrapping procedures above.

```
root@os-controller:~# ping -c1 10.50.20.22
PING 10.50.20.22 (10.50.20.22) 56(84) bytes of data.
64 bytes from 10.50.20.22: icmp_seq=1 ttl=63 time=0.315 ms
--- 10.50.20.22 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.315/0.315/0.315/0.000 ms
```

Verifying the VXLAN Bridge and VTEP Interfaces

After creating the VTEP in MidoNet and adding an interface binding, you should see `br-vxln` and `vxln` interfaces on the switch. You can verify that the VXLAN bridge and VTEP interface are created and UP:

```
cumulus@switch12:~$ sudo brctl show
bridge name  bridge id          STP      enabled interfaces
br-vxln10006 8000.00e0ec2749a2    no       swp11s0
                                         vxln10006
cumulus@switch12:~$ sudo ip -d link show vxln10006
55: vxln10006: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
master br-vxln10006 state UNKNOWN mode DEFAULT
    link/ether 72:94:eb:b6:6c:c3 brd ff:ff:ff:ff:ff:ff
        vxlan id 10006 local 10.111.1.2 port 32768 61000 nolearning ageing 300
        svcnode 10.111.0.182
        bridge_slave
```

Next, look at the bridging table for the VTEP and the forwarding entries. The bound interface and the VTEP should be listed along with the MAC addresses of those interfaces. When the hosts attached to the bound port send data, those MACs are learned, and entered into the bridging table, as well as the OVSDB.

```
cumulus@switch12:~$ brctl showmacs br-vxln10006
port name      mac addr          vlan      is
local?        ageing timer
swp11s0        00:e0:ec:27:49:a2   0
yes           0.00
swp11s0        64:ae:0c:32:f1:41   0
no            0.01
vxln10006     72:94:eb:b6:6c:c3   0
yes           0.00

cumulus@switch12:~$ sudo bridge fdb show br-vxln10006
fa:16:3e:14:04:2e dev vxln10004 dst 10.111.0.182 vlan 65535 self permanent
00:e0:ec:27:49:a2 dev swp11s0  vlan 0 master br-vxln10004 permanent
b6:71:33:3b:a7:83 dev vxln10004  vlan 0 master br-vxln10004 permanent
64:ae:0c:32:f1:41 dev swp11s0  vlan 0 master br-vxln10004
```

Datapath Troubleshooting

If you have verified the control plane is correct, and you still cannot get data between the OpenStack instances and the physical nodes on the switch, there may be something wrong with the data plane. The data plane consists of the actual VXLAN encapsulated path, between one of the OpenStack nodes running the `midolman` service. This is typically the compute nodes, but can include the Midonet gateway nodes. If the OpenStack instances can ping the tenant router address but cannot ping the physical device connected to the switch (or vice versa), then something is wrong in the data plane.

Verifying IP Reachability

First, there must be IP reachability between the encapsulating node, and the address you bootstrapped as the tunnel IP on the switch. Verify the OpenStack host can ping the tunnel IP. If this doesn't work, check the routing design, and fix the layer 3 problem first.

```
root@os-compute1:~# ping -c1 10.111.1.2
PING 10.111.1.2 (10.111.1.2) 56(84) bytes of data.
64 bytes from 10.111.1.2: icmp_seq=1 ttl=62 time=0.649 ms
--- 10.111.1.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.649/0.649/0.649/0.000 ms
```

MidoNet VXLAN Encapsulation

If the instance (VM) cannot ping the physical server, or the reply is not returning, look at the packets on the OpenStack node. Initiate a ping from the OpenStack instance, then using `tcpdump`, hopefully you can see the VXLAN data. This example displays what it looks like when it is working.

```
root@os-compute1:~# tcpdump -i eth1 -l -nnn -vvv -X -e port 4789
52:54:00:85:ac:d6 > 00:e0:ec:26:50:36, ethertype IPv4 (0x0800), length 148:
(tos 0x0, ttl 255, id 7583, offset 0, flags [none], proto UDP (17), length
134)
  10.111.0.182.41568 > 10.111.1.2.4789: [no cksum] VXLAN, flags [I] (0x08),
vni 10008
fa:16:3e:14:04:2e > 64:ae:0c:32:f1:41, ethertype IPv4 (0x0800), length 98:
(tos 0x0, ttl 64, id 64058, offset 0, flags [DF], proto ICMP (1), length 84)
  10.111.102.104 > 10.111.102.2: ICMP echo request, id 15873, seq 0, length
64
  0x0000: 4500 0086 1d9f 0000 ff11 8732 0a6f 00b6 E.....2.o...
  0x0010: 0a6f 0102 a260 12b5 0072 0000 0800 0000 .o...`....r.....
  0x0020: 0027 1800 64ae 0c32 f141 fa16 3e14 042e .'..d..2.A..>...
  0x0030: 0800 4500 0054 fa3a 4000 4001 5f26 0a6f ..E..T.:@._&.o
  0x0040: 6668 0a6f 6602 0800 f9de 3e01 0000 4233 fh.of.....>..B3
  0x0050: 7dec 0000 0000 0000 0000 0000 0000 0000 }.....
  0x0060: 0000 0000 0000 0000 0000 0000 0000 0000 .....
  0x0070: 0000 0000 0000 0000 0000 0000 0000 0000 .....
  0x0080: 0000 0000 0000 .....
00:e0:ec:26:50:36 > 52:54:00:85:ac:d6, ethertype IPv4 (0x0800), length 148:
(tos 0x0, ttl 62, id 2689, offset 0, flags [none], proto UDP (17), length
134)
  10.111.1.2.63385 > 10.111.0.182.4789: [no cksum] VXLAN, flags [I] (0x08),
```

```
vni 10008
64:ae:0c:32:f1:41 > fa:16:3e:14:04:2e, ethertype IPv4 (0x0800), length 98:
(tos 0x0, ttl 255, id 64058, offset 0, flags [DF], proto ICMP (1), length
84)
10.111.102.2 > 10.111.102.104: ICMP echo reply, id 15873, seq 0, length 64
0x0000: 4500 0086 0a81 0000 3e11 5b51 0a6f 0102 E.....>.[Q.o..
0x0010: 0a6f 00b6 f799 12b5 0072 0000 0800 0000 .o.....r.....
0x0020: 0027 1800 fa16 3e14 042e 64ae 0c32 f141 .'....>...d..2.A
0x0030: 0800 4500 0054 fa3a 4000 ff01 a025 0a6f ..E..T.:@....%o
0x0040: 6602 0a6f 6668 0000 01df 3e01 0000 4233 f..ofh....>...B3
0x0050: 7dec 0000 0000 0000 0000 0000 0000 0000 }.....
0x0060: 0000 0000 0000 0000 0000 0000 0000 0000 ..... .
0x0070: 0000 0000 0000 0000 0000 0000 0000 0000 ..... .
0x0080: 0000 0000 0000 ..... .
```

Inspecting the OVSDB

Using VTEP-CTL

These commands show you the information installed in the OVSDB. This database is structured using the *physical switch* ID, with one or more *logical switch* IDs associated with it. The bootstrap process creates the physical switch, and Midonet creates the logical switch after the control session is established.

Listing the Physical Switch

```
cumulus@switch12:~$ vtep-ctl list-ps
sw12
```

Listing the Logical Switch

```
cumulus@switch12:~$ vtep-ctl list-ls
mn-6c9826da-6655-4fe3-a826-4dcba6477d2d
```

Listing Local or Remote MAC Addresses

These commands show the MAC addresses learned from the connected port bound to the logical switch, or the MAC addresses advertised from Midonet. The *unknown-dst* entries are installed to satisfy the ethernet flooding of unknown unicast, and important for learning.

```
cumulus@switch12:~$ vtep-ctl list-local-macs mn-6c9826da-6655-4fe3-a826-
4dcba6477d2d
ucast-mac-local
64:ae:0c:32:f1:41 -> vxlan_over_ipv4/10.111.1.2
```

```
mcast-mac-local
unknown-dst -> vxlan_over_ipv4/10.111.1.2

cumulus@switch12:~$ vtep-ctl list-remote-macs mn-6c9826da-6655-4fe3-a826-
4dcba6477d2d
ucast-mac-remote
fa:16:3e:14:04:2e -> vxlan_over_ipv4/10.111.0.182
mcast-mac-remote
unknown-dst -> vxlan_over_ipv4/10.111.0.182oh
```

Getting Open Vswitch Database (OVSDB) Data

The `ovsdb-client dump` command is large, but shows all of the information and tables that are used in communication between the OVS client and server.

```
cumulus@switch12:~$ ovsdb-client dump
Arp_Sources_Local table
_uuid locator src_mac
-----
Arp_Sources_Remote table
_uuid locator src_mac
-----
Global table
_uuid managers switches
-----
-----
76672d6a-2740-4c8d-9618-9e8dfb4b0bd7 [] [6d459554-0c75-4170-bb3d-
117eb4ce1f4d]
Logical_Binding_Stats table
_uuid bytes_from_local bytes_to_local packets_from_local packets_to_local
-----
-----
d2e378b4-61c1-4daf-9aec-a7fd352d3193 5782569 1658250 21687 14589
Logical_Router table
_uuid description name static_routes switch_binding
-----
-----
Logical_Switch table
_uuid description name tunnel_key
-----
-----
44d162dc-0372-4749-a802-5b153c7120ec "" "mn-6c9826da-6655-4fe3-a826-
4dcba6477d2d" 10006
Manager table
_uuid inactivity_probe is_connected max_backoff other_config status target
```

```
-----
Mcast_Macs_Local table
MAC _uuid ipaddr locator_set logical_switch
-----

unknown-dst 25eaf29a-c540-46e3-8806-3892070a2de5 "" 7a4c000a-244e-4b37-8f25-
fd816c1a80dc 44d162dc-0372-4749-a802-5b153c7120ec
Mcast_Macs_Remote table
MAC _uuid ipaddr locator_set logical_switch
-----

unknown-dst b122b897-5746-449e-83ba-fa571a64b374 "" 6c04d477-18d0-41df-8d52-
dc7b17845ebe 44d162dc-0372-4749-a802-5b153c7120ec
Physical_Locator table
_uuid dst_ip encapsulation_type
-----

2fcf8b7e-e084-4bcb-b668-755ae7ac0bfb "10.111.0.182" "vxlan_over_ipv4"
3f78dbb0-9695-42ef-a31f-aaaf525147f1 "10.111.1.2" "vxlan_over_ipv4"
Physical_Locator_Set table
_uuid locators
-----

6c04d477-18d0-41df-8d52-dc7b17845ebe [2fcf8b7e-e084-4bcb-b668-755ae7ac0bfb]
7a4c000a-244e-4b37-8f25-fd816c1a80dc [3f78dbb0-9695-42ef-a31f-aaaf525147f1]
Physical_Port table
_uuid description name port_fault_status vlan_bindings vlan_stats
-----

bf69fcbb-36b3-4dbc-a90d-fc7412e57076 "swp1" "swp1" [] {} {}
bf38137d-3a14-454e-8df0-9c56e4b4e640 "swp10" "swp10" [] {} {}
69585fff-4360-4177-901d-8360ade5391b "swp11s0" "swp11s0" [] {0=44d162dc-
0372-4749-a802-5b153c7120ec} {0=d2e378b4-61c1-4daf-9aec-a7fd352d3193}
2a2d04fa-7190-41fe-8cee-318fcbafb2ea "swp11s1" "swp11s1" [] {} {}
684f99d5-426c-45c8-b964-211489f45599 "swp11s2" "swp11s2" [] {} {}
47cc66fb-ef8a-4a9b-a497-1844b89f7d32 "swp11s3" "swp11s3" [] {} {}
5be3a052-be0f-4258-94cb-5e8be9afb896 "swp12" "swp12" [] {} {}
631b19bd-3022-4353-bb2d-f498b0c1cb17 "swp13" "swp13" [] {} {}
3001c904-b152-4dc4-9d8e-718f24ffa439 "swp14" "swp14" [] {} {}
a6f8a88a-3877-4f81-b9b4-d75394a09d2c "swp15" "swp15" [] {} {}
7cb681f4-2206-4c70-85b7-23b60963cd21 "swp16" "swp16" [] {} {}
3943fb6a-0b49-4806-a014-2bcd4d469537 "swp17" "swp17" [] {} {}
109a9911-d6c7-4142-b6c9-7c985506abb4 "swp18" "swp18" [] {} {}
93b85c31-be38-4384-8b7a-9696764f9ba9 "swp19" "swp19" [] {} {}
bcfb2920-6676-494c-9dc8-b474123b7e59 "swp2" "swp2" [] {} {}
4223559a-dal1c-4c34-b8bf-bff7ced376ad "swp20" "swp20" [] {} {}
```

```
6bbccda8-d7e5-4b19-b978-4ec7f5b868e0 "swp21" "swp21" [] {} {}
c6876886-8386-4e34-a307-931909fca58f "swp22" "swp22" [] {} {}
c5a88dd6-d931-4b2c-9baa-a0abfb9d41f5 "swp23" "swp23" [] {} {}
124d1e01-a187-4427-819f-21de66e76f13 "swp24" "swp24" [] {} {}
55b49814-b5c5-405e-8e9f-898f3df4f872 "swp25" "swp25" [] {} {}
b2b2cd14-662d-45a5-87c1-277acbccdf7d "swp26" "swp26" [] {} {}
c35f55f5-8ec6-4fed-bef4-49801cd0934c "swp27" "swp27" [] {} {}
a44c5402-6218-4f09-bf1e-518f41a5546e "swp28" "swp28" [] {} {}
a9294152-2b32-4058-8796-23520ff7379 "swp29" "swp29" [] {} {}
e0ee993a-8383-4701-a766-d425654dbb7f "swp3" "swp3" [] {} {}
d9db91a6-1c10-4154-9269-84877faa79b4 "swp30" "swp30" [] {} {}
b26ce4dd-b771-4d7b-8647-41fa97aa40e3 "swp31" "swp31" [] {} {}
652c6cd1-0823-4585-bb78-658e6ca2abfc "swp32" "swp32" [] {} {}
5b15372b-89f0-4e14-a50b-b6c6f937d33d "swp4" "swp4" [] {} {}
e00741f1-ba34-47c5-ae23-9269c5d1a871 "swp5" "swp5" [] {} {}
7096abaf-eebf-4ee3-b0cc-276224bc3e71 "swp6" "swp6" [] {} {}
439afb62-067e-4bbe-a0d9-ee33a23d2a9c "swp7" "swp7" [] {} {}
54f6c9df-01a1-4d96-9dcf-3035a33ffb3e "swp8" "swp8" [] {} {}
c85ed6cd-a7d4-4016-b3e9-34df592072eb "swp9s0" "swp9s0" [] {} {}
cf382ed6-60d3-43f5-8586-81f4f0f2fb28 "swp9s1" "swp9s1" [] {} {}
c32a9ff9-fd11-4399-815f-806322f26ff5 "swp9s2" "swp9s2" [] {} {}
9a7e42c4-228f-4b55-b972-7c3b8352c27d "swp9s3" "swp9s3" [] {} {}

Physical_Switch table
_uuid description management_ips name ports switch_fault_status tunnel_ips
tunnels
-----
```

6d459554-0c75-4170-bb3d-117eb4cef1f4d "sw12" ["10.50.20.22"] "sw12"
[109a9911-d6c7-4142-b6c9-7c985506abb4, 124d1e01-a187-4427-819f-
21de66e76f13, 2a2d04fa-7190-41fe-8cee-318fcbafb2ea, 3001c904-b152-4dc4-9d8e-
718f24ffa439, 3943fb6a-0b49-4806-a014-2bcd4d469537, 4223559a-dalc-4c34-b8bf-
bff7ced376ad, 439afb62-067e-4bbe-a0d9-ee33a23d2a9c, 47cc66fb-ef8a-4a9b-a497-
1844b89f7d32, 54f6c9df-01a1-4d96-9dcf-3035a33fffb3e, 55b49814-b5c5-405e-8e9f-
898f3df4f872, 5b15372b-89f0-4e14-a50b-b6c6f937d33d, 5be3a052-be0f-4258-94cb-
5e8be9afb896, 631b19bd-3022-4353-bb2d-f498b0c1cb17, 652c6cd1-0823-4585-bb78-
658e6ca2abfc, 684f99d5-426c-45c8-b964-211489f45599, 69585fff-4360-4177-901d-
8360ade5391b, 6bbccda8-d7e5-4b19-b978-4ec7f5b868e0, 7096abaf-eefbf-4ee3-b0cc-
276224bc3e71, 7cb681f4-2206-4c70-85b7-23b60963cd21, 93b85c31-be38-4384-8b7a-
9696764f9ba9, 9a7e42c4-228f-4b55-b972-7c3b8352c27d, a44c5402-6218-4f09-bf1e-
518f41a5546e, a6f8a88a-3877-4f81-b9b4-d75394a09d2c, a9294152-2b32-4058-8796-
23520ffb7379, b26ce4dd-b771-4d7b-8647-41fa97aa40e3, b2b2cd14-662d-45a5-87c1-
277acbccdff, bcfb2920-6676-494c-9dcb-b474123b7e59, bf38137d-3a14-454e-8df0-
9c56e4b4e640, bf69fcbb-36b3-4dbc-a90d-fc7412e57076, c32a9ff9-fd11-4399-815f-
806322f26ff5, c35f55f5-8ec6-4fed-bef4-49801cd0934c, c5a88dd6-d931-4b2c-9baa-
a0abfb9d41f5, c6876886-8386-4e34-a307-931909fca58f, c85ed6cd-a7d4-4016-b3e9-
34df592072eb, cf382ed6-60d3-43f5-8586-81f4f0f2fb28, d9db91a6-1c10-4154-9269-
84877faa79b4, e00741f1-ba34-47c5-ae23-9269c5d1a871, e0ee993a-8383-4701-a766-
d425654dbb7f] [] ["10.111.1.2"] [062eaf89-9bd5-4132-8b6b-09db254325af]
Tunnel table

```
Tunnel table  
_uuid bfd_config_local bfd_config_remote bfd_params bfd_status local remote
```

062eaf89-9bd5-4132-8b6b-09db254325af {bfd_dst_ip="169.254.1.0",
bfd_dst_mac="00:23:20:00:00:01"} {} {} {} 3f78dbb0-9695-42ef-a31f-
aaaf525147f1 2fcf8b7e-e084-4bcb-b668-755ae7ac0fbfb

Ucast Macs Local table

```
MAC _uuid ipaddr locator logical_switch
```

"64:ae:0c:32:f1:41" 47a83a7c-bd2d-4c02-9814-8222229c592f "" 3f78dbb0-9695-42ef-a31f-aaaf525147f1 44d162dc-0372-4749-a802-5b153c7120ec

Ucast_Macs_Remote table

MAC _uuid ipaddr locator logical_switch

"fa:16:3e:14:04:2e" 65605488-9ee5-4c8e-93e5-7b1cc15cfcc7 "" 2fcf8b7e-e084-4bcb-b668-755ae7ac0bfb 44d162dc-0372-4749-a802-5b153c7120ec

Lightweight Network Virtualization - LNV

Lightweight Network Virtualization (LNV) is a technique for deploying [VXLANS](#) (see page 245) without a central controller on bare metal switches. This solution requires no external controller or software suite; it runs the VXLAN service and registration daemons on Cumulus Linux itself. The data path between bridge entities is established on top of a layer 3 fabric by means of a simple service node coupled with traditional MAC address learning.

To see an example of a full solution before reading the following background information, [please read this chapter](#) (see page 315).



LNV is a lightweight controller option. Please [contact Cumulus Networks](#) with your scale requirements so we can make sure this is the right fit for you. There are also other controller options that can work on Cumulus Linux.

Contents

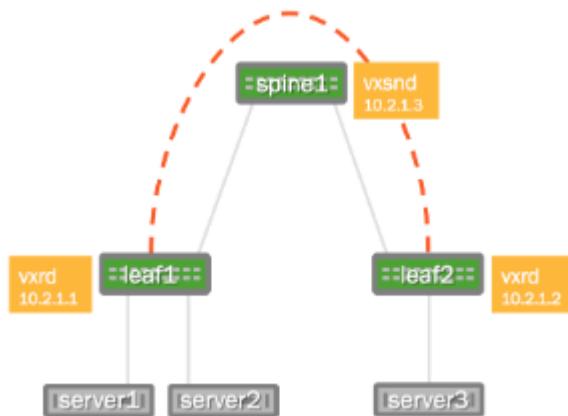
(Click to expand)

- [Contents](#) (see page 280)
- [Understanding LNV Concepts](#) (see page 281)
 - [Acquiring the Forwarding Database at the Service Node](#) (see page 281)
 - [MAC Learning and Flooding](#) (see page 281)
 - [Handling BUM Traffic](#) (see page 282)
- [Requirements](#) (see page 283)
 - [Hardware Requirements](#) (see page 283)
 - [Configuration Requirements](#) (see page 283)
 - [Installing the LNV Packages](#) (see page 283)
- [Sample LNV Configuration](#) (see page 283)
 - [Network Connectivity](#) (see page 284)
 - [Layer 3 IP Addressing](#) (see page 284)
 - [Layer 3 Fabric](#) (see page 285)
 - [Host Configuration](#) (see page 287)
- [Configuring the VLAN to VXLAN Mapping](#) (see page 288)
- [Verifying the VLAN to VXLAN Mapping](#) (see page 289)
- [Enabling and Managing Service Node and Registration Daemons](#) (see page 290)
 - [Enabling the Service Node Daemon](#) (see page 290)
 - [Enabling the Registration Daemon](#) (see page 290)
 - [Checking the Daemon Status](#) (see page 291)
- [Configuring the Registration Node](#) (see page 292)
- [Configuring the Service Node](#) (see page 294)
- [Verification and Troubleshooting](#) (see page 295)
 - [Verifying the Registration Node Daemon](#) (see page 295)

- Verifying the Service Node Daemon (see page 296)
- Verifying Traffic Flow and Checking Counters (see page 297)
- Pinging to Test Connectivity (see page 297)
- Troubleshooting with MAC Addresses (see page 299)
- Checking the Service Node Configuration (see page 299)
- Creating a Layer 3 Gateway (see page 300)
- Advanced LNV Usage (see page 300)
 - Scaling LNV by Load Balancing with Anycast (see page 300)
- Additional Resources (see page 306)
- See Also (see page 307)

Understanding LNV Concepts

To best describe this feature, consider the following example deployment:



The two switches running Cumulus Linux, called leaf1 and leaf2, each have a bridge configured. These two bridges contain the physical switch port interfaces connecting to the servers as well as the logical VXLAN interface associated with the bridge. By creating a logical VXLAN interface on both leaf switches, the switches become *VTEPs* (virtual tunnel end points). The IP address associated with this VTEP is most commonly configured as its loopback address — in the image above, the loopback address is 10.2.1.1 for leaf1 and 10.2.1.2 for leaf2.

Acquiring the Forwarding Database at the Service Node

In order to connect these two VXLANs together and forward BUM (Broadcast, Unknown-unicast, Multicast) packets to members of a VXLAN, the service node needs to acquire the addresses of all the VTEPs for every VXLAN it serves. The service node daemon does this through a registration daemon running on each leaf switch that contains a VTEP participating in LNV. The registration process informs the service node of all the VXLANs to which the switch belongs.

MAC Learning and Flooding

With LNV, as with traditional bridging of physical LANs or VLANs, a bridge automatically learns the location of hosts as a side effect of receiving packets on a port.

For example, when server1 sends an L2 packet to server3, leaf2 learns that server1's MAC address is located on that particular VXLAN, and the VXLAN interface learns that the IP address of the VTEP for server1 is 10.2.1.1. So when server3 sends a packet to server1, the bridge on leaf2 forwards the packet out of the port to the VXLAN interface and the VXLAN interface sends it, encapsulated in a UDP packet, to the address 10.2.1.1.

But what if server3 sends a packet to some address that has yet to send it a packet (server2, for example)? In this case, the VXLAN interface sends the packet to the service node, which sends a copy to every other VTEP that belongs to the same VXLAN.

Handling BUM Traffic

Cumulus Linux has two ways of handling BUM (Broadcast Unknown-Unicast and Multicast) traffic:

- Head end replication
- Service node replication

Head end replication is enabled by default in Cumulus Linux.



You cannot have both service node and head end replication configured simultaneously, as this causes the BUM traffic to be duplicated — both the source VTEP and the service node sending their own copy of each packet to every remote VTEP.

Head End Replication

The Trident II chipset is capable of head end replication — the ability to generate all the BUM (Broadcast Unknown-Unicast and Multicast) traffic in hardware. The most scalable solution available with LNV is to have each VTEP (top of rack switch) generate all of its own BUM traffic rather than relying on an external service node.

Cumulus Linux supports up to 64 VTEPs with head end replication.

To disable head end replication, edit `/etc/vxrd.conf` and set `head_rep` to `False`.

Service Node Replication

Cumulus Linux also supports service node replication for VXLAN BUM packets. This is useful with LNV if you have more than 64 VTEPs. However, it is not recommended because it forces the spine switches running the `vxsnd` (service node daemon) to replicate the packets in software instead of in hardware, unlike head end replication. If you're not using a controller but have more than 64 VTEPs, contact a [Cumulus Networks consultant](#).

To enable service node replication:

1. Disable head end replication; set `head_rep` to `False` in `/etc/vxrd.conf`.
2. Edit `/etc/network/interfaces` and configure a service node IP address for VXLAN interfaces using `vxrd-svcnode-ip <>`.
3. Edit `/etc/vxsnd.conf`, and configure the following:
 - Set the same service node IP address that you did in the previous step:
`svcnode_ip = <>`

- To forward VXLAN data traffic, set the following variable to *True*:
`enable_vxlan_listen = true`

Requirements

Hardware Requirements

- Switches with a Trident II chipset running Cumulus Linux 2.5.4 or later. Please refer to the Cumulus Networks [hardware compatibility list](#) for a list of supported switch models.

Configuration Requirements

- The VXLAN has an associated **VXLAN Network Identifier** (VNI), also interchangeably called a VXLAN ID.
- The VNI should not be 0 or 16777215, as these two numbers are reserved values under Cumulus Linux.
- The VXLAN link and physical interfaces are added to the bridge to create the association between the port, VLAN and VXLAN instance.
- Each bridge on the switch has only one VXLAN interface. Cumulus Linux does not support more than one VXLAN link in a bridge; however, a switch can have multiple bridges.
- Only use bridges in [traditional mode \(see page 187\)](#); [VLAN-aware bridges \(see page 208\)](#) are not supported with VXLAN at this time.
- An SVI (Switch VLAN Interface) or L3 address on the bridge is not supported. For example, you can't ping from the leaf1 SVI to the leaf2 SVI via the VXLAN tunnel; you would need to use server1 and server2 to verify. See [Creating a Layer 3 Gateway \(see page 299\)](#) below for more information.

Installing the LNV Packages

The LNV packages are not installed automatically if you upgrade Cumulus Linux. You can install LNV in one of two ways:

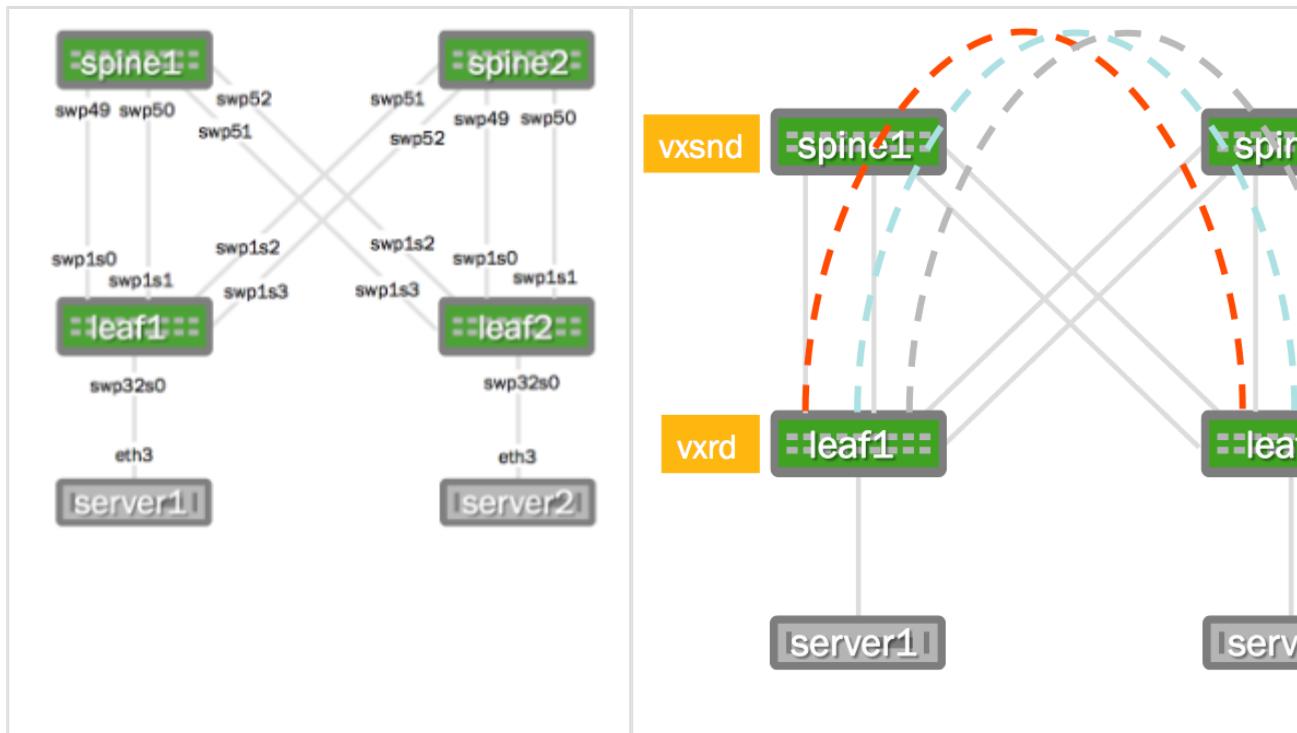
- Do a [binary image install \(see page 18\)](#) of Cumulus Linux, using `c1-img-install`
- Install the LNV packages for the registration and service node daemons using `apt-get install vxfld-vxrd` and/or `apt-get install vxfld-vxsnd`, depending upon how you intend to use LNV

Sample LNV Configuration

The following images illustrate the configuration that is referenced throughout this chapter.

Physical Cabling Diagram

Network Virtualization Diagram



Want to try out configuring LNV and don't have a Cumulus Linux switch? Check out [Cumulus VX](#).

Network Connectivity

There must be full network connectivity before you can configure LNV. The layer 3 IP addressing information as well as the OSPF configuration (`/etc/quagga/Quagga.conf`) below is provided to make the LNV example easier to understand.



OSPF is not a requirement for LNV, LNV just requires L3 connectivity. With Cumulus Linux this can be achieved with static routes, OSPF or BGP.

Layer 3 IP Addressing

Here is the configuration for the IP addressing information used in this example.

spine1: `/etc/network/interfaces`

```
auto lo
iface lo inet loopback
    address 10.2.1.3/32

auto eth0
iface eth0 inet dhcp
```

spine2: `/etc/network/interfaces`

```
auto lo
iface lo inet loopback
    address 10.2.1.4/32

auto eth0
iface eth0 inet dhcp
```

```

auto swp49
iface swp49
    address 10.1.1.2/30

auto swp50
iface swp50
    address 10.1.1.6/30

auto swp51
iface swp51
    address 10.1.1.50/30

auto swp52
iface swp52
    address 10.1.1.54/30

```

```

auto swp49
iface swp49
    address 10.1.1.18/30

auto swp50
iface swp50
    address 10.1.1.22/30

auto swp51
iface swp51
    address 10.1.1.34/30

auto swp52
iface swp52
    address 10.1.1.38/30

```

leaf1: /etc/network/interfaces

```

auto lo
iface lo inet loopback
    address 10.2.1.1/32

auto eth0
iface eth0 inet dhcp

auto swp1s0
iface swp1s0
    address 10.1.1.1/30

auto swp1s1
iface swp1s1
    address 10.1.1.5/30

auto swp1s2
iface swp1s2
    address 10.1.1.33/30

auto swp1s3
iface swp1s3
    address 10.1.1.37/30

```

leaf2: /etc/network/interfaces

```

auto lo
iface lo inet loopback
    address 10.2.1.2/32

auto eth0
iface eth0 inet dhcp

auto swp1s0
iface swp1s0
    address 10.1.1.17/30

auto swp1s1
iface swp1s1
    address 10.1.1.21/30

auto swp1s2
iface swp1s2
    address 10.1.1.49/30

auto swp1s3
iface swp1s3
    address 10.1.1.53/30

```

Layer 3 Fabric

The service nodes and registration nodes must all be routable between each other. The L3 fabric on Cumulus Linux can either be [BGP](#) (see page 372) or [OSPF](#) (see page 358). In this example, OSPF is used to demonstrate full reachability. Expand the Quagga configurations below.

Quagga configuration using OSPF:

spine1

```
interface lo
 ip ospf area 0.0.0.0
interface swp49
 ip ospf network point-to-point
 ip ospf area 0.0.0.0
!
interface swp50
 ip ospf network point-to-point
 ip ospf area 0.0.0.0
!
interface swp51
 ip ospf network point-to-point
 ip ospf area 0.0.0.0
!
interface swp52
 ip ospf network point-to-point
 ip ospf area 0.0.0.0
!
!
!
!
!
!
router-id 10.2.1.3
router ospf
 ospf router-id 10.2.1.3
```

spine2

```
interface lo
 ip ospf area 0.0.0.0
interface swp49
 ip ospf network point-to-point
 ip ospf area 0.0.0.0
!
interface swp50
 ip ospf network point-to-point
 ip ospf area 0.0.0.0
!
interface swp51
 ip ospf network point-to-point
 ip ospf area 0.0.0.0
!
interface swp52
 ip ospf network point-to-point
 ip ospf area 0.0.0.0
!
!
!
!
!
!
router-id 10.2.1.4
router ospf
 ospf router-id 10.2.1.4
```

leaf1

```
interface lo
 ip ospf area 0.0.0.0
interface swp1s0
 ip ospf network point-to-
point
 ip ospf area 0.0.0.0
!
interface swp1s1
 ip ospf network point-to-
point
 ip ospf area 0.0.0.0
!
```

leaf2

```
interface lo
 ip ospf area 0.0.0.0
interface swp1s0
 ip ospf network point-to-
point
 ip ospf area 0.0.0.0
!
interface swp1s1
 ip ospf network point-to-
point
 ip ospf area 0.0.0.0
!
```

```

interface swp1s2
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
interface swp1s3
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
!
!
!
!
router-id 10.2.1.1
router ospf
  ospf router-id 10.2.1.1

```

```

interface swp1s2
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
interface swp1s3
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
!
!
!
!
router-id 10.2.1.2
router ospf
  ospf router-id 10.2.1.2

```

Host Configuration

In this example, the servers are running Ubuntu 14.04. There needs to be a trunk mapped from server1 and server2 to the respective switch. In Ubuntu this is done with subinterfaces. You can expand the configurations below.

server1

```

auto eth3.10
iface eth3.10 inet
static
  address 10.10.10.1/24

auto eth3.20
iface eth3.20 inet
static
  address 10.10.20.1/24

auto eth3.30
iface eth3.30 inet
static
  address 10.10.30.1/24

```

server2

```

auto eth3.10
iface eth3.10 inet
static
  address 10.10.10.2/24

auto eth3.20
iface eth3.20 inet
static
  address 10.10.20.2/24

auto eth3.30
iface eth3.30 inet
static
  address 10.10.30.2/24

```

On Ubuntu it is more reliable to use `ifup` and `if down` to bring the interfaces up and down individually, rather than restarting networking entirely (that is, there is no equivalent to `if reload` like there is in Cumulus Linux):

```
cumulus@server1:~$ sudo ifup eth3.10
Set name-type for VLAN subsystem. Should be visible in /proc/net/vlan
/config
Added VLAN with VID == 10 to IF -:eth3:-
cumulus@server1:~$ sudo ifup eth3.20
Set name-type for VLAN subsystem. Should be visible in /proc/net/vlan
/config
Added VLAN with VID == 20 to IF -:eth3:-
cumulus@server1:~$ sudo ifup eth3.30
Set name-type for VLAN subsystem. Should be visible in /proc/net/vlan
/config
Added VLAN with VID == 30 to IF -:eth3:-
```

Configuring the VLAN to VXLAN Mapping

Configure the VLANS and associated VXLANS. In this example, there are 3 VLANS and 3 VXLAN IDs (VNIs). VLANS 10, 20 and 30 are used and associated with VNIs 10, 2000 and 30 respectively. The loopback address, used as the `vxlan-local-tunnelip`, is the only difference between leaf1 and leaf2 for this demonstration.

For leaf1:

```
cumulus@leaf1$ sudo nano /etc
/network/interfaces
```

Add the following to the loopback stanza

```
auto lo
iface lo
    vxrd-src-ip 10.2.1.1
    vxrd-svcnode-ip 10.2.1.3
```

Now append the following for the VXLAN configuration itself:

```
leaf1: /etc/network/interfaces

auto vni-10
iface vni-10
    vxlan-id 10
    vxlan-local-tunnelip 10.2.1.1
    mstpcctl-bpduguard yes
    mstpcctl-portbpdufilter yes

auto vni-2000
iface vni-2000
    vxlan-id 2000
```

For leaf2:

```
cumulus@leaf2$ sudo nano /etc
/network/interfaces
```

Add the following to the loopback stanza

```
auto lo
iface lo
    vxrd-src-ip 10.2.1.2
    vxrd-svcnode-ip 10.2.1.3
```

Now append the following for the VXLAN configuration itself:

```
leaf2: /etc/network/interfaces

auto vni-10
iface vni-10
    vxlan-id 10
    vxlan-local-tunnelip 10.2.1.2
    mstpcctl-bpduguard yes
    mstpcctl-portbpdufilter yes

auto vni-2000
iface vni-2000
    vxlan-id 2000
```

```

vxlan-local-tunnelip 10.2.1.1
mstpctl-bpduguard yes
mstpctl-portbpdufilter yes

auto vni-30
iface vni-30
    vxlan-id 30
    vxlan-local-tunnelip 10.2.1.1
    mstpctl-bpduguard yes
    mstpctl-portbpdufilter yes

auto br-10
iface br-10
    bridge-ports swp32s0.10 vni-
10

auto br-20
iface br-20
    bridge-ports swp32s0.20 vni-
2000

auto br-30
iface br-30
    bridge-ports swp32s0.30 vni-
30

```

To bring up the bridges and VNIs, use the `ifreload` command:

```
cumulus@leaf1$ sudo ifreload -a
```

```

vxlan-local-tunnelip 10.2.1.2
mstpctl-bpduguard yes
mstpctl-portbpdufilter yes

auto vni-30
iface vni-30
    vxlan-id 30
    vxlan-local-tunnelip 10.2.1.2
    mstpctl-bpduguard yes
    mstpctl-portbpdufilter yes

auto br-10
iface br-10
    bridge-ports swp32s0.10 vni-
10

auto br-20
iface br-20
    bridge-ports swp32s0.20 vni-
2000

auto br-30
iface br-30
    bridge-ports swp32s0.30 vni-
30

```

To bring up the bridges and VNIs, use the `ifreload` command:

```
cumulus@leaf2$ sudo ifreload -a
```



Why is br-20 not vni-20? For example, why not tie VLAN 20 to VNI 20, or why was 2000 used? VLANs and VXLANs do not need to be the same number. This was done on purpose to highlight this fact. However if you are using fewer than 4096 VLANs, there is no reason not to make it easy and correlate VLANs to VXLANs. It is completely up to you.

Verifying the VLAN to VXLAN Mapping

Use the `brctl show` command to see the physical and logical interfaces associated with that bridge:

```

cumulus@leaf1:~$ brctl show
bridge name      bridge id      STP enabled      interfaces
br-10           8000.443839008404  no            swp32s0.10
                                         vni-10
br-20           8000.443839008404  no            swp32s0.20

```

<code>br-30</code>	<code>8000.443839008404</code>	<code>no</code>	<code>vni-2000</code> <code>swp32s0.30</code> <code>vni-30</code>
--------------------	--------------------------------	-----------------	---

As with any logical interfaces on Linux, the name does not matter (other than a 15-character limit). To verify the associated VNI for the logical name, use the `ip -d link show` command:

```
cumulus@leaf1$ ip -d link show vni-10
43: vni-10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
  master br-10 state UNKNOWN mode DEFAULT
    link/ether 02:ec:ec:bd:7f:c6 brd ff:ff:ff:ff:ff:ff
    vxlan id 10 srcport 32768 dstport 4789 ageing 300
      bridge_slave
```

The `vxlan id 10` indicates the VXLAN ID/VNI is indeed 10 as the logical name suggests.

Enabling and Managing Service Node and Registration Daemons

Every VTEP must run the registration daemon (`vxrd`). Typically, every leaf switch acts as a VTEP. A minimum of 1 switch (a switch not already acting as a VTEP) must run the service node daemon (`vxsnd`). The instructions for enabling these daemons follows.

Enabling the Service Node Daemon

The service node daemon (`vxsnd`) is included in the Cumulus Linux repository as `vxflid-vxsnd`. The service node daemon can run on any switch running Cumulus Linux as long as that switch is not also a VXLAN VTEP. In this example, enable the service node only on the spine1 switch.



Do not run `vxsnd` on a switch that is already acting as a VTEP.

Edit the `/etc/default/vxsnd` configuration file:

```
cumulus@spine1$ sudo nano /etc/default/vxsnd
```

Change the `vxsnd` file by changing `no` to `yes`:

```
START=yes
```

Save and quit the text editor and reboot the `vxsnd` daemon:

```
cumulus@spine1$ sudo service vxsnd restart
[ ok ] Starting /usr/bin/vxsnd ....
```

Enabling the Registration Daemon

The registration daemon (`vxrd`) is included in the Cumulus Linux package as `vxfld-vxrd`. The registration daemon must run on each VTEP participating in LNV, so you must enable it on every TOR (leaf) switch acting as a VTEP.

Edit the `/etc/default/vxrd` configuration file on leaf1:

```
cumulus@leaf1$ sudo nano /etc/default/vxrd
```

Change the `vxrd` file by changing `no` to `yes`:

```
START=yes
```

Save and quit the text editor and reboot the `vxrd` daemon:

```
cumulus@leaf1$ sudo service vxrd restart  
[ ok ] Starting /usr/bin/vxrd ....
```

Open the `vxrd` configuration file on leaf2 with the following commands:

```
cumulus@leaf2$ sudo nano /etc/default/vxrd
```

Change the `vxsnd` file by changing `no` to `yes`:

```
START=yes
```

Save and quit the text editor and reboot the `vxrd` daemon:

```
cumulus@leaf1$ sudo service vxrd restart  
[ ok ] Starting /usr/bin/vxrd ....
```

Checking the Daemon Status

To determine if the daemon is running, use the `service <daemon name> status` command.

For the service node daemon:

```
cumulus@spine1$ sudo service vxsnd status  
[ ok ] vxsnd is running.
```

For the registration daemon:

```
cumulus@leaf1$ sudo service vxrd status
[ ok ] vxrd is running.
```

Configuring the Registration Node

The registration node was configured earlier in `/etc/network/interfaces` in the [VXLAN mapping \(see page 288\)](#) section above; no additional configuration is typically needed. However, if you need to modify the registration node configuration, edit `/etc/vxrd.conf`.

Alternate location for configuration and additional knobs for the registration node are found in `/etc/vxrd.conf`

```
cumulus@leaf1$ sudo nano /etc/vxrd.conf
```

Then edit the `svcnod_ip` variable:

```
svcnod_ip = 10.2.1.3
```

Then perform the same on leaf2:

```
cumulus@leaf2$ sudo nano /etc/vxrd.conf
```

And again edit the `svcnod_ip` variable:

```
svcnod_ip = 10.2.1.3
```

Restart the registration node daemon for the change to take effect:

```
cumulus@leaf1$ sudo service vxrd restart
[ ok ] Starting /usr/bin/vxrd ....
```

Restart the daemon on leaf2:

```
cumulus@leaf2$ sudo service vxrd restart
[ ok ] Starting /usr/bin/vxrd ....
```

The complete list of options you can configure is listed below:

Name	Description	Default
loglevel	The log level, which can be DEBUG, INFO, WARNING, ERROR, CRITICAL.	INFO

Name	Description	Default
logdest	The destination for log messages. It can be a file name, <code>stdout</code> or <code>syslog</code> .	syslog
logfilesize	Log file size in bytes. Used when <code>logdest</code> is a file name.	512000
logbackupcount	Maximum number of log files stored on the disk. Used when <code>logdest</code> is a file name.	14
pidfile	The PIF file location for the <code>vxrd</code> daemon.	/var/run/vxrd.pid
udsfile	The file name for the Unix domain socket used for management.	/var/run/Vxrd.sock
vxld_port	The UDP port used for VXLAN control messages.	10001
svcnod_ip	The address to which registration daemons send control messages for registration and/or BUM packets for replication. This can also be configured under <code>/etc/network/interfaces</code> with the <code>vxrd-svcnode-ip</code> keyword.	
holdtime	Hold time (in seconds) for soft state, which is how long the service node waits before ageing out an IP address for a VNI. The <code>vxrd</code> includes this in the register messages it sends to a <code>vxsnd</code> .	90 seconds
src_ip	Local IP address to bind to for receiving control traffic from the service node daemon.	
refresh_rate	Number of times to refresh within the hold time. The higher this number, the more lost UDP refresh messages can be tolerated.	3 seconds
config_check_rate	The number of seconds to poll the system for current VXLAN membership.	5 seconds
head_rep	Enables self replication. Instead of using the service node to replicate BUM packets, it will be done in hardware on the VTEP switch.	true



Use `1`, `yes`, `true` or `on` for True for each relevant option. Use `0`, `no`, `false` or `off` for False.

Configuring the Service Node

To configure the service node daemon, edit the `/etc/vxsnd.conf` configuration file.



For the example configuration, default values are used, except for the `svcnod_ip` field.

```
cumulus@spine1$ sudo nano /etc/vxsnd.conf
```

The address field is set to the loopback address of the switch running the `vxsnd` dameon.

```
svcnod_ip = 10.2.1.3
```

Restart the service node daemon for the change to take effect:

```
cumulus@spine1$ sudo service vxsnd restart
[ ok ] Starting /usr/bin/vxsnd ....
```

The complete list of options you can configure is listed below:

Name	Description	Default
loglevel	The log level, which can be DEBUG, INFO, WARNING, ERROR, CRITICAL.	INFO
logdest	Destination for log messages. It can be a file name, <code>stdout</code> or <code>syslog</code> .	syslog
logfilesize	The log file size in bytes. Used when <code>logdest</code> is a file name.	512000
logbackupcount	Maximum number of log files stored on disk. Used when <code>logdest</code> is a file name.	14
pidfile	The PID file location for the <code>vxrd</code> daemon.	<code>/var/run/vxrd.pid</code>
udsfile	The file name for the Unix domain socket used for management.	<code>/var/run/vxrd.sock</code>
vxfld_port	The UDP port used for VXLAN control messages.	10001
svcnod_ip		0.0.0.0

Name	Description	Default
	This is the address to which registration daemons send control messages for registration and/or BUM packets for replication.	
holdtime	Holdtime (in seconds) for soft state. It is used when sending a register message to peers in response to learning a <vnid, addr> from a VXLAN data packet.	90
src_ip	Local IP address to bind to for receiving inter-vxsnd control traffic.	0.0.0.0
svcnodes_peers	Space-separated list of IP addresses with which the vxsnd shares its state.	
enable_vxlan_listen	When set to true, the service node listens for VXLAN data traffic.	true
install_svcnode_ip	When set to true, the <code>snd_peer_address</code> gets installed on the loopback interface. It gets withdrawn when the <code>vxsnd</code> is not in service. If set to true, you must define the <code>snd_peer_address</code> configuration variable.	false
age_check	Number of seconds to wait before checking the database to age out stale entries.	90 seconds



Use `1, yes, true` or `on` for True for each relevant option. Use `0, no, false` or `off` for False.

Verification and Troubleshooting

Verifying the Registration Node Daemon

Use the `vxrdctl vxlans` command to see the configured VNIs, the local address being used to source the VXLAN tunnel and the service node being used.

<pre>cumulus@leaf1\$ vxrdctl vxlans VNI Local Addr Svc Node === ===== 10 10.2.1.1 10.2.1.3 30 10.2.1.1 10.2.1.3 2000 10.2.1.1 10.2.1.3</pre>	<pre>cumulus@leaf2\$ vxrdctl vxlans VNI Local Addr Svc Node === ===== 10 10.2.1.2 10.2.1.3 30 10.2.1.2 10.2.1.3 2000 10.2.1.2 10.2.1.3</pre>
--	--

Use the `vxrdctl peers` command to see configured VNIs and all VTEPs (leaf switches) within the network that have them configured.

```
cumulus@leaf1$  
vxrdctl peers  
VNI          Peer Addrs  
===  
10           10.2.1.1,  
10.2.1.2  
30           10.2.1.1,  
10.2.1.2  
2000         10.2.1.1,  
10.2.1.2
```

```
cumulus@leaf2$  
vxrdctl peers  
VNI          Peer Addrs  
===  
10           10.2.1.1,  
10.2.1.2  
30           10.2.1.1,  
10.2.1.2  
2000         10.2.1.1,  
10.2.1.2
```



When head end replication mode is disabled, the command won't work.

Use the `vxrdctl peers` command to see the other VTEPs (leaf switches) and what VNIs are associated with them. This does not show anything unless you enabled head end replication mode by setting the `head_rep` option to *True*. Otherwise, replication is done by the service node.

```
cumulus@leaf2$ vxrdctl peers  
Head-end replication is turned off on this device.  
This command will not provide any output
```

Verifying the Service Node Daemon

Use the `vxsndctl fdb` command to verify which VNIs belong to which VTEP (leaf switches).

```
cumulus@spine1$ vxsndctl fdb  
VNI      Address      Ageout  
===  
10       10.2.1.1     82  
10       10.2.1.2     77  
30       10.2.1.1     82  
30       10.2.1.2     77  
2000     10.2.1.1     82  
2000     10.2.1.2     77
```

Verifying Traffic Flow and Checking Counters

VXLAN transit traffic information is stored in a flat file located at /cumulus/switchd/run/stats/vxlan/all.

```
cumulus@leaf1$ cat /cumulus/switchd/run/stats/vxlan/all
VNI : 10
Network In Octets : 1090
Network In Packets : 8
Network Out Octets : 1798
Network Out Packets : 13
Total In Octets : 2818
Total In Packets : 27
Total Out Octets : 3144
Total Out Packets : 39
VN Interface : vni: 10, swp32s0.10
Total In Octets : 1728
Total In Packets : 19
Total Out Octets : 552
Total Out Packets : 18
VNI : 30
Network In Octets : 828
Network In Packets : 6
Network Out Octets : 1224
Network Out Packets : 9
Total In Octets : 2374
Total In Packets : 23
Total Out Octets : 2300
Total Out Packets : 32
VN Interface : vni: 30, swp32s0.30
Total In Octets : 1546
Total In Packets : 17
Total Out Octets : 552
Total Out Packets : 17
VNI : 2000
Network In Octets : 676
Network In Packets : 5
Network Out Octets : 1072
Network Out Packets : 8
Total In Octets : 2030
Total In Packets : 20
Total Out Octets : 2042
Total Out Packets : 30
VN Interface : vni: 2000, swp32s0.20
Total In Octets : 1354
Total In Packets : 15
Total Out Octets : 446
```

Pinging to Test Connectivity

To test the connectivity across the VXLAN tunnel with an ICMP echo request (ping), make sure to ping from the server rather than the switch itself.



As mentioned above, SVIs (switch VLAN interfaces) are not supported when using VXLAN. That is, there cannot be an IP address on the bridge that also contains a VXLAN.

Following is the IP address information used in this example configuration.

VNI	server1	server2
10	10.10.10.1	10.10.10.2
2000	10.10.20.1	10.10.20.2
30	10.10.30.1	10.10.30.2

To test connectivity between VNI 10 connected servers by pinging from server1:

```
cumulus@server1:~$ ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=3.90 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.202 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=0.195 ms
^C
--- 10.10.10.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.195/1.432/3.900/1.745 ms
cumulus@server1:~$
```

The other VNIs were also tested and can be viewed in the expanded output below.

Test connectivity between VNI-2000 connected servers by pinging from server1:

```
cumulus@server1:~$ ping 10.10.20.2
PING 10.10.20.2 (10.10.20.2) 56(84) bytes of data.
64 bytes from 10.10.20.2: icmp_seq=1 ttl=64 time=1.81 ms
64 bytes from 10.10.20.2: icmp_seq=2 ttl=64 time=0.194 ms
64 bytes from 10.10.20.2: icmp_seq=3 ttl=64 time=0.206 ms
^C
--- 10.10.20.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.194/0.739/1.819/0.763 ms
```

Test connectivity between VNI-30 connected servers by pinging from server1:

```
cumulus@server1:~$ ping 10.10.30.2
PING 10.10.30.2 (10.10.30.2) 56(84) bytes of data.
64 bytes from 10.10.30.2: icmp_seq=1 ttl=64 time=1.85 ms
64 bytes from 10.10.30.2: icmp_seq=2 ttl=64 time=0.239 ms
64 bytes from 10.10.30.2: icmp_seq=3 ttl=64 time=0.185 ms
64 bytes from 10.10.30.2: icmp_seq=4 ttl=64 time=0.212 ms
^C
--- 10.10.30.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.185/0.622/1.853/0.711 ms
```

Troubleshooting with MAC Addresses

Since there is no SVI, there is no way to ping from the server to the directly attached leaf (top of rack) switch without cabling the switch to itself (see [Creating a Layer 3 Gateway \(see page 299\)](#) below). The easiest way to see if the server can reach the leaf switch is to check the MAC address table of the leaf switch.

First, get the MAC address of the server:

```
cumulus@server1:~$ ip addr show eth3.10 | grep ether
link/ether 90:e2:ba:55:f0:85 brd ff:ff:ff:ff:ff:ff
```

Next, check the MAC address table of the leaf switch:

```
cumulus@leaf1$ brctl showmacs br-10
port name mac addr      vlan   is local?    ageing timer
vni-10  46:c6:57:fc:1f:54  0     yes          0.00
swp32s0.10 90:e2:ba:55:f0:85  0     no           75.87
vni-10  90:e2:ba:7e:a9:c1  0     no           75.87
swp32s0.10 ec:f4:bb:fc:67:a1  0     yes          0.00
```

90:e2:ba:55:f0:85 appears in the MAC address table, which indicates that connectivity is occurring between leaf1 and server1.

Checking the Service Node Configuration

Use `ip -d link show` to verify the service node, VNI and administrative state of a particular logical VNI interface:

```
cumulus@leaf1$ ip -d link show vni-10
35: vni-10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
    master br-10 state UNKNOWN mode DEFAULT
        link/ether 46:c6:57:fc:1f:54 brd ff:ff:ff:ff:ff:ff
        vxlan id 10 remote 10.2.1.3 local 10.2.1.1 srcport 32768 dstport 61000
        dstport 4789 ageing 300 svcnode 10.2.1.3
        bridge_slave
```

Creating a Layer 3 Gateway

The Trident II ASIC has a limitation because of a restriction in the hardware, where an IP address cannot be configured on the same bridge of which a VXLAN is also a part. This limitation will not exist in future ASICs. For example, the Trident II+ has the RIOT (Routing In/Out of Tunnels) feature.

For the Trident II, this limitation means a physical cable must be attached from one port on leaf1 to another port on leaf1. One port is an L3 port while the other is a member of the bridge. For example, following the configuration above, in order for a layer 3 address to be used as the gateway for vni-10, you could configure the following on leaf1:

```
auto swp47
iface swp47
alias 12 port connected to swp48

auto swp48
iface swp48
alias gateway
address 10.10.10.3/24

auto vni-10
iface vni-10
vxlan-id 10
vxlan-local-tunnelip 10.2.1.1
mstpctl-bpduguard yes
mstpctl-portbpdufilter yes

auto br-10
iface br-10
bridge-ports swp47 swp32s0.10 vni-10
```

A loopback cable must be connected between swp47 and swp48 for this to work. This will be addressed in a future version of Cumulus Linux so a physical port does not need to be used for this purpose.

Advanced LNV Usage

Scaling LNV by Load Balancing with Anycast

The above configuration assumes a single service node. A single service node can quickly be overwhelmed by BUM traffic. To load balance BUM traffic across multiple service nodes, use [Anycast](#). Anycast enables BUM traffic to reach the topologically nearest service node rather than overwhelming a single service node.

Enabling the Service Node Daemon on Additional Spine Switches

In this example, spine1 already has the service node daemon enabled. Enable it on the spine2 switch with the following commands:

Edit the /etc/default/vxsnd configuration file:

```
cumulus@spine2$ sudo nano /etc/default/vxsnd
```

Change the vxsnd file by changing *no* to *yes*:

```
START=yes
```

Save and quit the text editor and reboot the vxsnd daemon:

```
cumulus@spine2$ sudo service vxsnd restart
[ ok ] Starting /usr/bin/vxsnd ....
```

Configuring the AnyCast Address on All Participating Service Nodes

spine1

Use a text editor to edit the network configuration:

```
cumulus@spine1$ sudo nano /etc/network/interfaces
```

Add the 10.10.10.10/32 address to the loopback address:

```
auto lo
iface lo inet loopback
  address 10.2.1.3/32
  address 10.10.10.10/32
```

Run ifreload -a:

```
cumulus@spine1$ sudo ifreload -a
```

Verify the IP address is configured:

```
cumulus@spine1$ ip addr show lo
1: lo: <LOOPBACK,UP,LOWER_UP>
mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host
          link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
            inet 10.2.1.3/32 scope global
              link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                inet 10.10.10.10/32 scope global
                  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                    inet6 ::1/128 scope host
                      valid_lft forever
                      preferred_lft forever
```

spine2

Use a text editor to edit the network configuration:

```
cumulus@spine2$ sudo nano /etc/network/interfaces
```

Add the 10.10.10.10/32 address to the loopback address:

```
auto lo
iface lo inet loopback
  address 10.2.1.4/32
  address 10.10.10.10/32
```

Run ifreload -a:

```
cumulus@spine2$ sudo ifreload -a
```

Verify the IP address is configured:

```
cumulus@spine2$ ip addr show lo
1: lo: <LOOPBACK,UP,LOWER_UP>
mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host
          link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
            inet 10.2.1.4/32 scope global
              link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                inet 10.10.10.10/32 scope global
                  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                    inet6 ::1/128 scope host
                      valid_lft forever
                      preferred_lft forever
```

Configuring the Service Node vxsnd.conf File

spine1

Use a text editor to edit the network configuration:

```
cumulus@spine1$ sudo nano /etc/vxsnd.conf
```

Change the following values:

```
svcnod_ip = 10.10.10.10
svcnod_peers = 10.2.1.4
src_ip = 10.2.1.3
```

i This sets the address on which the service node listens to VXLAN messages to the configured Anycast address and sets it to sync with spine2.

Restart the vxsnd daemon:

```
cumulus@spine1$ service vxsnd
restart
[ ok ] Starting /usr/bin/vxsnd
....
```

spine2

Use a text editor to edit the network configuration:

```
cumulus@spine2$ sudo nano /etc/vxsnd.conf
```

Change the following values:

```
svcnod_ip = 10.10.10.10
svcnod_peers = 10.2.1.3
src_ip = 10.2.1.4
```

i This sets the address on which the service node listens to VXLAN messages to the configured Anycast address and sets it to sync with spine1.

Restart the vxsnd daemon:

```
cumulus@spine1$ service vxsnd
restart
[ ok ] Starting /usr/bin/vxsnd
....
```

Reconfiguring the VTEPs (Leafs) to Use the Anycast Address

leaf1

Use a text editor to edit the network configuration:

```
cumulus@leaf1$ sudo nano /etc/network/interfaces
```

Change the vxrd-svcnode-ip field to the Anycast address:

```
auto lo
iface lo inet loopback
  address 10.2.1.1
  vxrd-svcnode-ip 10.10.10.10
```

Run ifreload -a:

```
cumulus@leaf1$ sudo ifreload -a
```

Verify the new service node is configured:

```
cumulus@leaf1$ ip -d link show vni-10
35: vni-10: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc noqueue master br-10 state UNKNOWN mode DEFAULT
      link/ether 46:c6:57:fc:1f:54 brd ff:ff:ff:ff:ff:ff
      vxlan id 10 remote 10.10.10.10 local 10.2.1.1 srcport 32768 dstport 4789 ageing 300 svcnode 10.10.10.10
          bridge_slave
```

```
cumulus@leaf1$ ip -d link show vni-2000
39: vni-2000: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc noqueue master br-20 state UNKNOWN mode DEFAULT
```

leaf2

Use a text editor to edit the network configuration:

```
cumulus@leaf2$ sudo nano /etc/network/interfaces
```

Change the vxrd-svcnode-ip field to the Anycast address:

```
auto lo
iface lo inet loopback
  address 10.2.1.2
  vxrd-svcnode-ip 10.10.10.10
```

Run ifreload -a:

```
cumulus@leaf2$ sudo ifreload -a
```

Verify the new service node is configured:

```
cumulus@leaf2$ ip -d link show vni-10
35: vni-10: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc noqueue master br-10 state UNKNOWN mode DEFAULT
      link/ether 4e:03:a7:47:a7:9d brd ff:ff:ff:ff:ff:ff
      vxlan id 10 remote 10.10.10.10 local 10.2.1.2 srcport 32768 dstport 4789 ageing 300 svcnode 10.10.10.10
          bridge_slave
```

```
cumulus@leaf2$ ip -d link show vni-2000
39: vni-2000: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc noqueue master br-20 state UNKNOWN mode DEFAULT
```

```

link/ether 4a:fd:88:c3:fa:
df brd ff:ff:ff:ff:ff:ff
    vxlan id 2000 remote
10.10.10.10 local 10.2.1.1
srcport 32768 61000 dstport
4789 ageing 300 svcnode
10.10.10.10
    bridge_slave

cumulus@leaf1$ ip -d link show
vni-30
37: vni-30: <BROADCAST,
MULTICAST,UP,LOWER_UP> mtu
1500 qdisc noqueue master br-
30 state UNKNOWN mode DEFAULT
    link/ether 3e:b3:dc:f3:bd:
2b brd ff:ff:ff:ff:ff:ff
    vxlan id 30 remote
10.10.10.10 local 10.2.1.1
srcport 32768 61000 dstport
4789 ageing 300 svcnode
10.10.10.10
    bridge_slave

```

 The svcnode 10.10.10.10 means the interface has the correct service node configured.

Use the `vxrdctl vxlans` command to check the service node:

```

cumulus@leaf1$ vxrdctl vxlans
VNI      Local Addr      Svc
Node
===
=====
10       10.2.1.1
10.2.1.3
30       10.2.1.1
10.2.1.3
2000     10.2.1.1
10.2.1.3

```

```

link/ether 72:3a:bd:06:00:
b7 brd ff:ff:ff:ff:ff:ff
    vxlan id 2000 remote
10.10.10.10 local 10.2.1.2
srcport 32768 61000 dstport
4789 ageing 300 svcnode
10.10.10.10
    bridge_slave

```

```

cumulus@leaf2$ ip -d link show
vni-30
37: vni-30: <BROADCAST,
MULTICAST,UP,LOWER_UP> mtu
1500 qdisc noqueue master br-
30 state UNKNOWN mode DEFAULT
    link/ether 22:65:3f:63:08:
bd brd ff:ff:ff:ff:ff:ff
    vxlan id 30 remote
10.10.10.10 local 10.2.1.2
srcport 32768 61000 dstport
4789 ageing 300 svcnode
10.10.10.10
    bridge_slave

```

 The svcnode 10.10.10.10 means the interface has the correct service node configured.

Use the `vxrdctl vxlans` command to check the service node:

```

cumulus@leaf2$ vxrdctl vxlans
VNI      Local Addr      Svc
Node
===
=====
10       10.2.1.2
10.2.1.3
30       10.2.1.2
10.2.1.3
2000     10.2.1.2
10.2.1.3

```

Testing Connectivity

Repeat the ping tests from the previous section. Here is the table again for reference:

VNI	server1	server2
10	10.10.10.1	10.10.10.2
2000	10.10.20.1	10.10.20.2
30	10.10.30.1	10.10.30.2

```
cumulus@server1:~$ ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=5.32 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.206 ms
^C
--- 10.10.10.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.206/2.767/5.329/2.562 ms

PING 10.10.20.2 (10.10.20.2) 56(84) bytes of data.
64 bytes from 10.10.20.2: icmp_seq=1 ttl=64 time=1.64 ms
64 bytes from 10.10.20.2: icmp_seq=2 ttl=64 time=0.187 ms
^C
--- 10.10.20.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.187/0.914/1.642/0.728 ms

cumulus@server1:~$ ping 10.10.30.2
PING 10.10.30.2 (10.10.30.2) 56(84) bytes of data.
64 bytes from 10.10.30.2: icmp_seq=1 ttl=64 time=1.63 ms
64 bytes from 10.10.30.2: icmp_seq=2 ttl=64 time=0.191 ms
^C
--- 10.10.30.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.191/0.913/1.635/0.722 ms
```

Additional Resources

Both vxsnd and vxrd have man pages in Cumulus Linux.

For vxsnd:

```
cumulus@spinel1$ man vxsnd
```

For vxrd:

```
cumulus@leaf1$ man vxrd
```

See Also

- <https://tools.ietf.org/html/rfc7348>
- <http://en.wikipedia.org/wiki/Anycast>

LNV VXLAN Active-Active Mode

VXLAN active-active mode allows a pair of MLAG (see page 217) switches to act as a single VTEP, providing active-active VXLAN termination for bare metal as well as virtualized workloads.

Contents

- Contents (see page 307)
- Requirements (see page 307)
- Anycast IP Addresses (see page 308)
- Checking VXLAN Interface Configuration Consistency (see page 308)
- Configuring VXLAN Active-Active Mode (see page 308)
 - Configuring the Anycast IP Address (see page 308)
 - Configuring MLAG (see page 309)
 - Configuration LNV (see page 309)
 - Configuring STP (see page 309)
- Example VXLAN Active-Active Configuration (see page 309)
 - leaf1 Configuration (see page 309)
 - leaf2 Configuration (see page 311)
 - Quagga Configuration (see page 312)
 - LNV Configuration (see page 313)
 - leaf1 Configuration (see page 313)
 - leaf2 Configuration (see page 314)
- VXLAN PROTO_DOWN State (see page 314)
- Caveats and Errata (see page 315)

Requirements

- Each MLAG switch should be provisioned with a virtual IP address in the form of an anycast IP address for VXLAN datapath termination.
- All MLAG requirements (see page 218) apply for VXLAN Active-Active mode.
- LNV (see page 279) is the only supported control plane option for VXLAN active-active mode in this release. LNV can be configured for either service node replication or head-end replication.

- If STP (see page 150) is enabled on the bridge that is connected to VXLAN, then BPDU filter and BPDU guard (see page 162) should be enabled in the VXLAN interface.

Anycast IP Addresses

The VXLAN termination address is an anycast IP address that you configure as a `c1agd` parameter (`c1agd-vxlan-anycast-ip`) under the loopback interface. `c1agd` dynamically adds and removes this address as the loopback interface address as follows:

- When the switches come up, `ifupdown2` places all VXLAN interfaces in a `PROTO_DOWN` state (see page 314).
- Upon MLAG peering and a successful VXLAN interface consistency check between the switches, `c1agd` adds the anycast address as the interface address to the loopback interface. It then changes the local IP address of the VXLAN interface from a unique non-virtual IP address to an anycast virtual IP address and puts the interface in an UP state.
- If after establishing MLAG peering, the peer link goes down, then the primary switch continues to keep all VXLAN interfaces up with the anycast IP address while the secondary switch brings down all VXLAN interfaces and places them in a `PROTO_DOWN` state. It also removes the anycast IP address from the loopback interface and changes the local IP address of the VXLAN interface to a unique non-virtual IP address.
- If after establishing MLAG peering, one of the switches goes down, then the other running switch continues to use the anycast IP address.
- If after establishing MLAG peering, `c1agd` is stopped, all VXLAN interfaces are put in a `PROTO_DOWN` state. The anycast IP address is removed from the loopback interface and the local IP addresses of the VXLAN interfaces are changed from the anycast IP address to unique non-virtual IP addresses.
- If MLAG peering could not be established between the switches, `c1agd` brings up all the VXLAN interfaces after the reload timer expires with unique non-virtual IP addresses. This allows the VXLAN interface to be up and running on both switches even though peering is not established.

Checking VXLAN Interface Configuration Consistency

The VXLAN active-active configuration for a given VNI has to be consistent between the MLAG switches for correct traffic behavior. `c1agd` ensures that the configuration consistency is met before bringing the VXLAN interfaces operationally up. The consistency checks include:

- The anycast virtual IP address for VXLAN termination must be the same on both switches
- A VXLAN interface with the same VNI must be configured and administratively up on both switches

Configuring VXLAN Active-Active Mode

Configuring the Anycast IP Address

With MLAG peering, both switches use an anycast IP address for VXLAN encapsulation and decapsulation. This allows remote VTEPs to learn the host MAC addresses attached to the MLAG switches against one logical VTEP even though the switches independently encapsulate and decapsulate layer 2 traffic originating from the host. You configure this anycast address under the loopback interface as shown below.

```
auto lo
iface lo
```

```
address 27.0.0.11/32
clagd-vxlan-anycast-ip 36.0.0.11
```



This is not a loopback interface address configuration. It's a `clagd` parameter configuration under the loopback interface. Only `clagd` can add or remove an anycast virtual IP address as an interface address to the loopback interface.

Configuring MLAG

Refer to the MLAG chapter (see page 221) for configuration information.

Configuration LNV

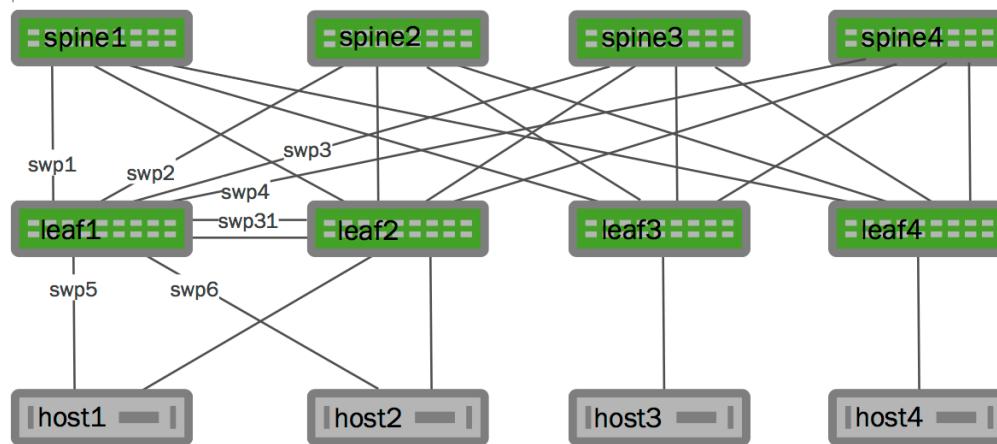
Refer to the LNV chapter (see page 279) for configuration information.

Configuring STP

You should enable **BPDU filter** and **BPDU guard** (see page 162) in the VXLAN interfaces if STP (see page 150) is enabled in the bridge that is connected to the VXLAN.

Example VXLAN Active-Active Configuration

The following example configures two bonds for MLAG, each with a single port, a peer link that is a bond with two member ports, and two traditional Linux bridges. It is a Clos network with spine nodes (spine1-4), 2 MLAG switches (leaf1, leaf2), 2 hosts connected to those switches and 2 standalone switches (leaf3 and leaf4) with hosts connected to them. The configuration is stored in `/etc/network/interfaces` on each peer switch.



Note the configuration of the local IP address in the VXLAN interfaces below. They are configured with individual IP addresses, which `clagd` changes to anycast upon MLAG peering.

leaf1 Configuration

leaf1 configuration; click here to expand...

```
auto eth0
    address 10.0.0.1
    netmask 255.255.255.0
auto lo
iface lo
    address 27.0.0.11/32
    clagd-vxlan-anycast-ip 36.0.0.11
auto swp1
iface swp1
    address 10.1.1.1/30
    mtu 9050
auto swp2
iface swp2
    address 10.1.1.5/30
    mtu 9050
auto swp3
iface swp3
    address 10.1.1.33/30
    mtu 9050
auto swp4
iface swp4
    address 10.1.1.37/30
    mtu 9050
auto peerlink
iface peerlink
    bond-slaves swp31 swp32
    mtu 9050
auto peerlink.4094
iface peerlink.4094
    address 27.0.0.11/32
    address 169.254.1.1/30
    mtu 9050
    clagd-priority 4096
    clagd-sys-mac 44:38:39:ff:ff:01
    clagd-peer-ip 169.254.0.2
    clagd-backup-ip 10.0.0.2
auto host1
iface host1
    bond-slaves swp5
    mtu 9050
    clag-id 1
auto host2
iface host2
    bond-slaves swp6
    mtu 9050
    clag-id 2
auto vxlan-1000
iface vxlan-1000
    vxlan-id 1000
    vxlan-local-tunnelip 27.0.0.11
    mtu 9000
```

```

auto vxlan-2000
iface vxlan-2000
    vxlan-id 2000
    vxlan-local-tunnelip 27.0.0.11
    mtu 9000
auto br1000
iface br1000
    bridge-ports host1 host2.1000 peerlink.1000 vxlan-1000
    bridge-stp on
    mstpcctl-portbpdufilter vxlan-1000=yes
    mstpcctl-bpduguard vxlan-1000=yes
    mstpcctl-portautoedge host1=yes host2.1000=yes peerlink.1000=yes
auto br2000
iface br2000
    bridge-ports host1.2000 host2 peerlink.2000 vxlan-2000
    bridge-stp on
    mstpcctl-portbpdufilter vxlan-2000=yes
    mstpcctl-bpduguard vxlan-2000=yes
    mstpcctl-portautoedge host1.2000=yes host2=yes peerlink.2000=yes

```

leaf2 Configuration

leaf2 configuration; click here to expand...

```

auto eth0
    address 10.0.0.2
    netmask 255.255.255.0
auto lo
iface lo
    address 27.0.0.12/32
    clagd-vxlan-anycast-ip 36.0.0.11
auto swp1
iface swp1
    address 10.1.1.17/30
    mtu 9050
auto swp2
iface swp2
    address 10.1.1.21/30
    mtu 9050
auto swp3
iface swp1
    address 10.1.1.49/30
    mtu 9050
auto swp4
iface swp2
    address 10.1.1.53/30
    mtu 9050
auto peerlink
iface peerlink
    bond-slaves swp31 swp32

```

```

    mtu 9050
auto peerlink.4094
iface peerlink.4094
    address 27.0.0.12/32
    address 169.254.0.2/30
    mtu 9050
    clagd-priority 4096
    clagd-sys-mac 44:38:39:ff:ff:01
    clagd-peer-ip 169.254.1.1
    clagd-backup-ip 10.0.0.1
auto host1
iface host1
    bond-slaves swp5
    mtu 9050
    clag-id 1
auto host2
iface host2
    bond-slaves swp6
    mtu 9050
    clag-id 2
auto vxlan-1000
iface vxlan-1000
    vxlan-id 1000
    vxlan-local-tunnelip 27.0.0.12
    mtu 9000
auto vxlan-2000
iface vxlan-2000
    vxlan-id 2000
    vxlan-local-tunnelip 27.0.0.12
    mtu 9000
auto br1000
iface br1000
    bridge-ports host1 host2.1000 peerlink.1000 vxlan-1000
    bridge-stp on
    mstpcctl-portbpdufilter vxlan-1000=yes
    mstpcctl-bpduguard vxlan-1000=yes
    mstpcctl-portautoedge host1=yes host2.1000=yes peerlink.1000=yes
auto br2000
iface br2000
    bridge-ports host1.2000 host2 peerlink.2000 vxlan-2000
    bridge-stp on
    mstpcctl-portbpdufilter vxlan-2000=yes
    mstpcctl-bpduguard vxlan-2000=yes
    mstpcctl-portautoedge host1.2000=yes host2=yes peerlink.2000=yes

```

Quagga Configuration

The layer 3 fabric can be configured using [BGP](#) (see page 372) or [OSPF](#) (see page 358). The following example uses OSPF; the configuration needed in the MLAG switches in the above specified topology is as follows:

leaf1: /etc/quagga/Quagga.conf

```

interface lo
  ip ospf area 0.0.0.0
interface swp1
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
interface swp2
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
interface swp3
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
interface swp4
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
!
!
!
!
!
router-id 10.2.1.1
router ospf
  ospf router-id 10.2.1.1

```

leaf2: /etc/quagga/Quagga.conf

```

interface lo
  ip ospf area 0.0.0.0
interface swp1
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
interface swp2
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
interface swp3
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
interface swp4
  ip ospf network point-to-
  point
  ip ospf area 0.0.0.0
!
!
!
!
!
router-id 10.2.1.2
router ospf
  ospf router-id 10.2.1.2

```

LNV Configuration

The following configuration variables should be set in leaf1 and leaf2 in `/etc/vxrd.conf`. This configuration assumes head-end replication is used to replicate BUM traffic. If service node based replication is used, then `svcnodes_ip` variable has to be set with service node address. Please refer to [Configuring the Registration Node \(see page 292\)](#) for setting that variable.

leaf1 Configuration

```
# Local IP address to bind to for receiving control traffic from the sdn
src_ip = 27.0.0.11
```

```
# Enable self replication
# Note: Use true, or on, for True and 0, no, false, or off,
# for False
head_rep = true
```

leaf2 Configuration

```
# Local IP address to bind to for receiving control traffic from the snd
src_ip = 27.0.0.12

# Enable self replication
# Note: Use true, or on, for True and 0, no, false, or off,
# for False
head_rep = true
```

VXLAN PROTO_DOWN State

Similar to a bond interface, if MLAG detects a problem that could result in connectivity issues such as traffic black-holing or a network meltdown if the link carrier was left in an UP state, it can put VXLAN interface into a [PROTO_DOWN state \(see page \)](#). Such connectivity issues include:

- When the peer link goes down but the peer switch is up (that is, the backup link is active).
- When an MLAG-enabled node is booted or rebooted, VXLAN interfaces are placed in a PROTO_DOWN state until the node establishes a connection to its peer switch, detects existence of corresponding VXLAN interfaces in the peer switch, or five minutes have elapsed.
- If the anycast address is not configured or if it is not the same in both MLAG switches, the VXLAN interfaces are placed into a PROTO_DOWN state.
- A configuration mismatch between the MLAG switches, such as the VXLAN interface is configured on just one of the switches or if the interface is shut down on one of the switches, then the VXLAN interface is placed into a PROTO_DOWN state on the secondary switch.

You can use the `clagctl` command to check if any VXLAN devices are in a PROTO_DOWN state. As shown below, VXLAN devices are kept in a PROTO_DOWN state due to the missing anycast configuration.

```
cumulus@switch$ clagctl
The peer is alive
  Our Priority, ID, and Role: 4096 c4:54:44:bd:01:71 primary
  Peer Priority, ID, and Role: 8192 00:02:00:00:00:36 secondary
    Peer Interface and IP: peerlink.4094 169.254.0.2
      Backup IP: 10.0.0.2 (active)
      System MAC: 44:38:39:ff:ff:01
```

CLAG Interfaces	Our Interface	Peer Interface	CLAG Id	Conflicts
Proto-Down Reason				

	host1	host2	1	-
	host1	host2	2	-
vxlan-1000	-	-	-	-
vxlan-single,no-anycast-ip				
vxlan-2000	-	-	-	-
vxlan-single,no-anycast-ip				

Caveats and Errata

- VLAN-aware bridge mode (see page 208) is not supported for VXLAN active-active mode in this release.
- The VLAN used for the peer link layer 3 subinterface should not be reused for any other interface in the system. It is recommended to use a high VLAN ID value. Read more about the [range of VLAN IDs you can use \(see page 217\)](#).
- Active-active mode works only with LNV in this release. Integration with controller-based VXLANs such as VMware NSX and Midokura MidoNet will be supported in the future.

LNV Full Example

Lightweight Network Virtualization (LNV) is a technique for deploying [VXLANs \(see page 245\)](#) without a central controller on bare metal switches. This a full example complete with diagram. Please reference the [Lightweight Network Virtualization chapter \(see page 279\)](#) for more detailed information. This full example uses the **recommended way** of deploying LNV, which is to use Anycast to load balance the service nodes.



LNV is a lightweight controller option. Please [contact Cumulus Networks](#) with your scale requirements and we can make sure this is the right fit for you. There are also other controller options that can work on Cumulus Linux.

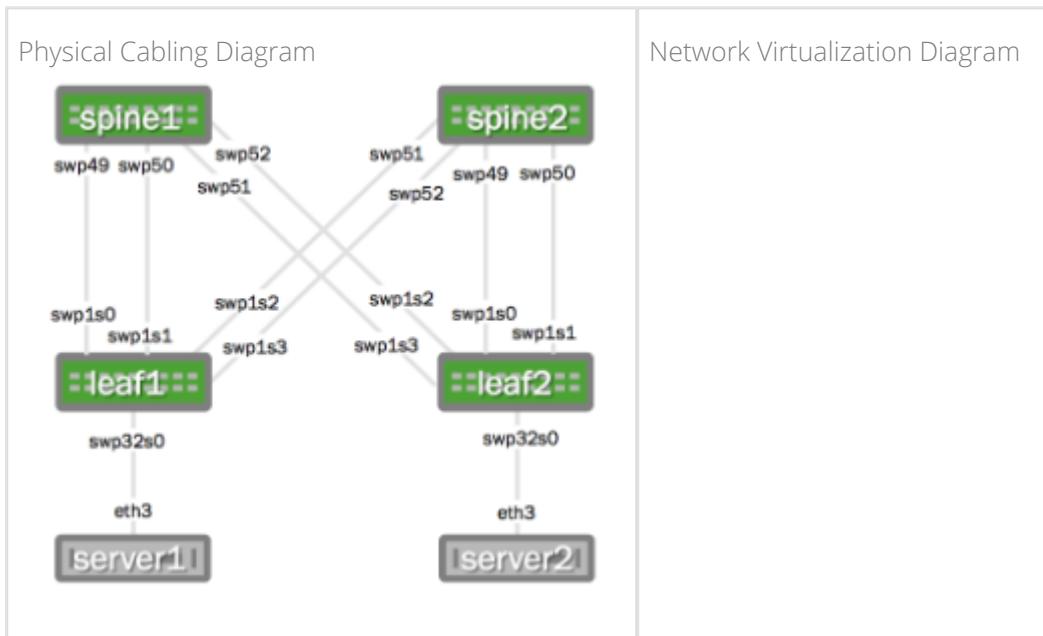
Contents

(Click to expand)

- [Contents \(see page 315\)](#)
- [Example LNV Configuration \(see page 315\)](#)
 - [Layer 3 IP Addressing \(see page 316\)](#)
 - [Quagga Configuration \(see page 318\)](#)
 - [Host Configuration \(see page 320\)](#)
 - [Service Node Configuration \(see page 321\)](#)
- [See Also \(see page 322\)](#)

Example LNV Configuration

The following images illustrate the configuration:



Want to try out configuring LNV and don't have a Cumulus Linux switch? Check out [Cumulus VX](#).



Feeling Overwhelmed? Come join a [Cumulus Boot Camp](#) and get instructor-led training!

Layer 3 IP Addressing

Here is the configuration for the IP addressing information used in this example:

spine1: /etc/network/interfaces

```
auto lo
iface lo inet loopback
    address 10.2.1.3/32
    address 10.10.10.10/32

auto eth0
iface eth0 inet dhcp

auto swp49
iface swp49
    address 10.1.1.2/30
```

spine2: /etc/network/interfaces

```
auto lo
iface lo inet loopback
    address 10.2.1.4/32
    address 10.10.10.10/32

auto eth0
iface eth0 inet dhcp

auto swp49
iface swp49
    address 10.1.1.18/30
```

```

auto swp50
iface swp50
    address 10.1.1.6/30

auto swp51
iface swp51
    address 10.1.1.50/30

auto swp52
iface swp52
    address 10.1.1.54/30

```

```

auto swp50
iface swp50
    address 10.1.1.22/30

auto swp51
iface swp51
    address 10.1.1.34/30

auto swp52
iface swp52
    address 10.1.1.38/30

```

leaf1: /etc/network/interfaces

```

auto lo
iface lo inet loopback
    address 10.2.1.1/32
    vxrd-src-ip 10.2.1.1
    vxrd-svcnode-ip 10.10.10.10

auto eth0
iface eth0 inet dhcp

auto swp1s0
iface swp1s0
    address 10.1.1.1/30

auto swp1s1
iface swp1s1
    address 10.1.1.5/30

auto swp1s2
iface swp1s2
    address 10.1.1.33/30

auto swp1s3
iface swp1s3
    address 10.1.1.37/30

auto vni-10
iface vni-10
    vxlan-id 10
    vxlan-local-tunnelip 10.2.1.1
    mstpctl-bpduguard yes
    mstpctl-portbpdufilter yes

auto vni-2000
iface vni-2000

```

leaf2: /etc/network/interfaces

```

auto lo
iface lo inet loopback
    address 10.2.1.2/32
    vxrd-src-ip 10.2.1.2
    vxrd-svcnode-ip 10.10.10.10

auto eth0
iface eth0 inet dhcp

auto swp1s0
iface swp1s0 inet static
    address 10.1.1.17/30

auto swp1s1
iface swp1s1 inet static
    address 10.1.1.21/30

auto swp1s2
iface swp1s2 inet static
    address 10.1.1.49/30

auto swp1s3
iface swp1s3 inet static
    address 10.1.1.53/30

auto vni-10
iface vni-10
    vxlan-id 10
    vxlan-local-tunnelip 10.2.1.2
    mstpctl-bpduguard yes
    mstpctl-portbpdufilter yes

auto vni-2000
iface vni-2000

```

```

vxlan-id 2000
vxlan-local-tunnelip 10.2.1.1
mstpcctl-bpduguard yes
mstpcctl-portbpdufilter yes

auto vni-30
iface vni-30
  vxlan-id 30
  vxlan-local-tunnelip 10.2.1.1
  mstpcctl-bpduguard yes
  mstpcctl-portbpdufilter yes

auto br-10
iface br-10
  bridge-ports swp32s0.10 vni-10

auto br-20
iface br-20
  bridge-ports swp32s0.20 vni-2000

auto br-30
iface br-30
  bridge-ports swp32s0.30 vni-30

```

```

vxlan-id 2000
vxlan-local-tunnelip 10.2.1.2
mstpcctl-bpduguard yes
mstpcctl-portbpdufilter yes

auto vni-30
iface vni-30
  vxlan-id 30
  vxlan-local-tunnelip 10.2.1.2
  mstpcctl-bpduguard yes
  mstpcctl-portbpdufilter yes

auto br-10
iface br-10
  bridge-ports swp32s0.10 vni-10

auto br-20
iface br-20
  bridge-ports swp32s0.20 vni-2000

auto br-30
iface br-30
  bridge-ports swp32s0.30 vni-30

```

Quagga Configuration

The service nodes and registration nodes must all be routable between each other. The L3 fabric on Cumulus Linux can either be [BGP](#) (see page 372) or [OSPF](#) (see page 358). In this example, OSPF is used to demonstrate full reachability.

Here is the Quagga configuration using OSPF:

spine1: /etc/quagga/Quagga.conf

```

interface lo
  ip ospf area 0.0.0.0
interface swp49
  ip ospf network point-to-point
  ip ospf area 0.0.0.0
!
interface swp50
  ip ospf network point-to-point
  ip ospf area 0.0.0.0
!
```

spine2: /etc/quagga/Quagga.conf

```

interface lo
  ip ospf area 0.0.0.0
interface swp49
  ip ospf network point-to-point
  ip ospf area 0.0.0.0
!
interface swp50
  ip ospf network point-to-point
  ip ospf area 0.0.0.0
!
```

```

interface swp51
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
interface swp52
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
!
!
!
!
router-id 10.2.1.3
router ospf
    ospf router-id 10.2.1.3

```

```

interface swp51
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
interface swp52
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
!
!
!
!
router-id 10.2.1.4
router ospf
    ospf router-id 10.2.1.4

```

leaf1: /etc/quagga/Quagga.conf

```

interface lo
    ip ospf area 0.0.0.0
interface swp1s0
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
interface swp1s1
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
interface swp1s2
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
interface swp1s3
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
!
!
!
!
router-id 10.2.1.1

```

leaf2: /etc/quagga/Quagga.conf

```

interface lo
    ip ospf area 0.0.0.0
interface swp1s0
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
interface swp1s1
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
interface swp1s2
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
interface swp1s3
    ip ospf network point-to-
    point
    ip ospf area 0.0.0.0
!
!
!
!
!
router-id 10.2.1.2

```

```
router ospf
  ospf router-id 10.2.1.1
```

```
router ospf
  ospf router-id 10.2.1.2
```

Host Configuration

In this example, the servers are running Ubuntu 14.04. A trunk must be mapped from server1 and server2 to the respective switch. In Ubuntu this is done with subinterfaces.

server1

```
auto eth3.10
iface eth3.10 inet
static
  address 10.10.10.1/24

auto eth3.20
iface eth3.20 inet
static
  address 10.10.20.1/24

auto eth3.30
iface eth3.30 inet
static
  address 10.10.30.1/24
```

server2

```
auto eth3.10
iface eth3.10 inet
static
  address 10.10.10.2/24

auto eth3.20
iface eth3.20 inet
static
  address 10.10.20.2/24

auto eth3.30
iface eth3.30 inet
static
  address 10.10.30.2/24
```

Service Node Configuration

spine1: /etc/vxsnd.conf

```
[common]
# Log level is one of DEBUG,
INFO, WARNING, ERROR, CRITICAL
#loglevel = INFO
# Destination for log
message. Can be a file name, '
stdout', or 'syslog'
#logdest = syslog
# log file size in bytes. Used
when logdest is a file
#logfilesize = 512000
# maximum number of log files
stored on disk. Used when
logdest is a file
#logbackupcount = 14
# The file to write the pid.
If using monit, this must
match the one
# in the vxsnd.rc
#pidfile = /var/run/vxsnd.pid
# The file name for the unix
domain socket used for mgmt.
#udsfile = /var/run/vxsnd.sock
# UDP port for vxfld control
messages
#vxfld_port = 10001
# This is the address to which
registration daemons send
control messages for
# registration and/or BUM
packets for replication
svcnode_ip = 10.10.10.10
# Holdtime (in seconds) for
soft state. It is used when
sending a
# register msg to peers in
response to learning a <vni,
addr> from a
# VXLAN data pkt
#holdtime = 90
# Local IP address to bind to f
or receiving inter-vxsnd
control traffic
src_ip = 10.2.1.3
```

spine2: /etc/vxsnd.conf

```
[common]
# Log level is one of DEBUG,
INFO, WARNING, ERROR, CRITICAL
#loglevel = INFO
# Destination for log
message. Can be a file name, '
stdout', or 'syslog'
#logdest = syslog
# log file size in bytes. Used
when logdest is a file
#logfilesize = 512000
# maximum number of log files
stored on disk. Used when
logdest is a file
#logbackupcount = 14
# The file to write the pid.
If using monit, this must
match the one
# in the vxsnd.rc
#pidfile = /var/run/vxsnd.pid
# The file name for the unix
domain socket used for mgmt.
#udsfile = /var/run/vxsnd.sock
# UDP port for vxfld control
messages
#vxfld_port = 10001
# This is the address to which
registration daemons send
control messages for
# registration and/or BUM
packets for replication
svcnode_ip = 10.10.10.10
# Holdtime (in seconds) for
soft state. It is used when
sending a
# register msg to peers in
response to learning a <vni,
addr> from a
# VXLAN data pkt
#holdtime = 90
# Local IP address to bind to f
or receiving inter-vxsnd
control traffic
src_ip = 10.2.1.4
```

```
[vxsnd]
# Space separated list of IP
addresses of vxsnd to share
state with
svcnode_peers = 10.2.1.4
# When set to true, the
service node will listen for
vxlan data traffic
# Note: Use 1, yes, true, or
on, for True and 0, no, false,
or off,
# for False
#enable_vxlan_listen = true
# When set to true, the
svcnode_ip will be installed
on the loopback
# interface, and it will be
withdrawn when the vxsnd is no
longer in
# service. If set to true,
the svcnode_ip configuration
# variable must be defined.
# Note: Use 1, yes, true, or
on, for True and 0, no, false,
or off,
# for False
#install_svcnode_ip = false
# Seconds to wait before
checking the database to age
out stale entries
#age_check = 90
```

```
[vxsnd]
# Space separated list of IP
addresses of vxsnd to share
state with
svcnode_peers = 10.2.1.3
# When set to true, the
service node will listen for
vxlan data traffic
# Note: Use 1, yes, true, or
on, for True and 0, no, false,
or off,
# for False
#enable_vxlan_listen = true
# When set to true, the
svcnode_ip will be installed
on the loopback
# interface, and it will be
withdrawn when the vxsnd is no
longer in
# service. If set to true,
the svcnode_ip configuration
# variable must be defined.
# Note: Use 1, yes, true, or
on, for True and 0, no, false,
or off,
# for False
#install_svcnode_ip = false
# Seconds to wait before
checking the database to age
out stale entries
#age_check = 90
```

See Also

- <https://tools.ietf.org/html/rfc7348>
- <http://en.wikipedia.org/wiki/Anycast>
- Detailed LNV Configuration Guide (see page 279)
- Cumulus Networks Training

Static MAC Bindings with VXLAN

Cumulus Linux includes native Linux VXLAN kernel support.

Contents

(Click to expand)

- [Contents \(see page 322\)](#)

- Requirements (see page 323)
- Example VXLAN Configuration (see page 323)
- Configuring the Static MAC Bindings VXLAN (see page 323)
- Troubleshooting VXLANs in Cumulus Linux (see page 327)

Requirements

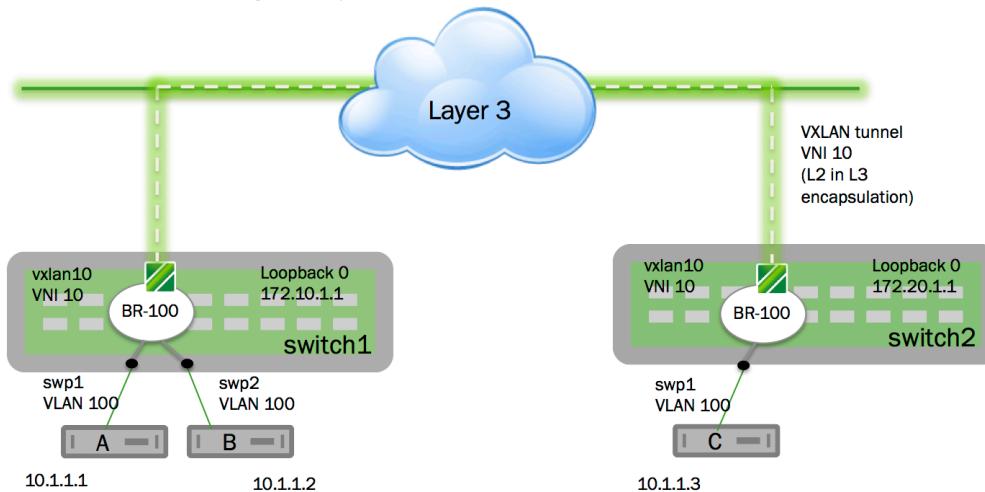
A VXLAN configuration requires a switch with a Trident II chipset running Cumulus Linux 2.0 or later.

For a basic VXLAN configuration, you should ensure that:

- The VXLAN has a network identifier (VNI); do not use 0 or 16777215 as the VNI ID, as they are reserved values under Cumulus Linux.
- The VXLAN link and local interfaces are added to bridge to create the association between port, VLAN and VXLAN instance.
- Each bridge on the switch has only one VXLAN interface. Cumulus Linux does not support more than one VXLAN link in a bridge; however a switch can have multiple bridges.

Example VXLAN Configuration

Consider the following example:



Preconfiguring remote MAC addresses does not scale. A better solution is to use the Cumulus Networks [Lightweight Network Virtualization](#) feature, or a controller-based option like [Midokura MidoNet](#) and [OpenStack](#) or [VMware NSX](#).

Configuring the Static MAC Bindings VXLAN

To configure the example illustrated above, edit `/etc/network/interfaces` with a text editor like vi, nano or zile.

Add the following configuration to the `/etc/network/interfaces` file on **switch1**:

```
auto vtep1000
```

```

iface vtep1000
  vxlan-id 1000
  vxlan-local-tunnelip 172.10.1.1

auto br-100
iface br-100
  bridge-ports swp1.100 swp2.100 vtep1000
  post-up bridge fdb add 0:00:10:00:00:0C dev vtep1000 dst 172.20.1.
1 vni 1000
  
```

Add the following configuration to the /etc/network/interfaces file on switch2:

```

auto vtep1000
iface vtep1000
  vxlan-id 1000
  vxlan-local-tunnelip 172.20.1.1

auto br-100
iface br-100
  bridge-ports swp1.100 swp2.100 vtep1000
  post-up bridge fdb add 00:00:10:00:00:0A dev vtep1000 dst 172.10.1
.1 vni 1000
  post-up bridge fdb add 00:00:10:00:00:0B dev vtep1000 dst 172.10.1
.1 vni 1000
  
```

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

In general, to configure a VXLAN in Cumulus Linux without a controller, run the following commands in a terminal connected to the switch:

1. Create a VXLAN link:

```

cumulus@switch1:~$ sudo ip link add <name> type vxlan id <vni> local
<ip addr> [group <mcast group address>] [no] nolearning [ttl] [tos]
[dev] [port MIN MAX] [ageing <value>] [svcnode addr]
  
```



If you are specifying ageing, you **must** specify the service node (svcnode).

2. Add a VXLAN link to a bridge:

```
cumulus@switch1:~$ sudo brctl addif br-vxlan <name>
```

3. Install a static MAC binding to a remote tunnel IP:

```
cumulus@switch1:~$ sudo bridge fdb add <mac addr> dev <device> dst <ip
addr> vni <vni> port <port> via <device>
```

4. Show VXLAN link and FDB:

```
cumulus@switch1:~$ sudo ip -d link show

cumulus@switch1:~$ sudo bridge fdb show
```

To create a runtime configuration that matches the image above, do the following:

1. Configure hosts A and B as part of the same tenant as C (VNI 10) on switch1. Hosts A and B are part of VLAN 100. To configure the VTEP interface with VNI 10, run the following commands in a terminal connected to switch1 running Cumulus Linux:

```
cumulus@switch1:~$ sudo ip link add link swp1 name swp1.100 type vlan
id 100
cumulus@switch1:~$ sudo ip link add link swp2 name swp2.100 type vlan
id 100
cumulus@switch1:~$ sudo ip link add vtep1000 type vxlan id 10 local
172.10.1.1 nolearning
cumulus@switch1:~$ sudo ip link set swp1 up
cumulus@switch1:~$ sudo ip link set swp2 up
cumulus@switch1:~$ sudo ip link set vtep1000 up
```

2. Configure VLAN 100 and VTEP 1000 to be part of the same bridge br-100 on switch1:

```
cumulus@switch1:~$ sudo brctl addbr br-100
cumulus@switch1:~$ sudo ip link set br-100 up
cumulus@switch1:~$ sudo brctl addif br-100 swp1.100 swp2.100
cumulus@switch1:~$ sudo brctl addif br-100 vtep1000
```

3. Install a static MAC binding to a remote tunnel IP, assuming the MAC address for host C is 00:00:10:00:00:0C:

```
cumulus@switch1:~$ sudo bridge fdb add 00:00:10:00:00:0C dev vtep1000  
dst 172.20.1.1
```

4. Configure host C as part of the same tenant as hosts A and B on switch2:

```
cumulus@switch2:~$ sudo ip link add link swp1 name swp1.100 type vlan  
id 100  
cumulus@switch2:~$ sudo ip link add name vtep1000 type vxlan id 10  
local 172.20.1.1 nolearning  
cumulus@switch2:~$ sudo ip link set swp1 up  
cumulus@switch2:~$ sudo ip link set vtep1000 up
```

5. Configure VLAN 100 and VTEP 1000 to be part of the same bridge br-100 on switch2:

```
cumulus@switch2:~$ sudo brctl addbr br-100  
cumulus@switch2:~$ sudo ip link set br-100 up  
cumulus@switch2:~$ sudo brctl addif br-100 swp1.100  
cumulus@switch2:~$ sudo brctl addif br-100 vtep1000
```

6. Install a static MAC binding to a remote tunnel IP on switch2, assuming the MAC address for host A is 00:00:10:00:00:0A and the MAC address for host B is 00:00:10:00:00:0B:

```
cumulus@switch2:~$ sudo bridge fdb add 00:00:10:00:00:0A dev vtep1000  
dst 172.10.1.1  
cumulus@switch2:~$ sudo bridge fdb add 00:00:10:00:00:0B dev vtep1000  
dst 172.10.1.1
```

7. Verify the configuration on switch1, then on switch2:

```
cumulus@switch1:~$ sudo ip -d link show  
cumulus@switch1:~$ sudo bridge fdb show  
  
cumulus@switch2:~$ sudo ip -d link show  
cumulus@switch2:~$ sudo bridge fdb show
```

8. Set the static arp for hosts B and C on host A:

```
root@hostA:~# sudo arp -s 10.1.1.3 00:00:10:00:00:0C
```

- Set the static arp for hosts A and C on host B:

```
root@hostB:~# sudo arp -s 10.1.1.3 00:00:10:00:00:0C
```

- Set the static arp for hosts A and B on host C:

```
root@hostC:~# arp -s 10.1.1.1 00:00:10:00:00:0A
root@hostC:~# arp -s 10.1.1.2 00:00:10:00:00:0B
```

Troubleshooting VXLANS in Cumulus Linux

Use the following commands to troubleshoot issues on the switch:

- `brctl show`: Verifies the VXLAN configuration in a bridge:

```
cumulus@switch:~$ sudo brctl show
bridge name      bridge id          STP enabled
interfaces
br-vxln100       8000.44383900480d    no
swp2s0.100
                           swp2s1.1
00
                           vxln100
```

- `bridge fdb show`: Displays the list of MAC addresses in an FDB:

```
cumulus@switch1:~$ sudo bridge fdb show
52:54:00:ae:2a:e0 dev vxln100 dst 172.16.21.150 self permanent
d2:ca:78:bb:7c:9b dev vxln100 permanent
90:e2:ba:3f:ce:34 dev swp2s1.100
90:e2:ba:3f:ce:35 dev swp2s0.100
44:38:39:00:48:0e dev swp2s1.100 permanent
44:38:39:00:48:0d dev swp2s0.100 permanent
```

- `ip -d link show`: Displays information about the VXLAN link:

```
cumulus@switch1:~$ sudo ip -d link show vxln100
71: vxln100: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
      master br-vxln100 state UNKNOWN mode DEFAULT
        link/ether d2:ca:78:bb:7c:9b brd ff:ff:ff:ff:ff:ff
        vxlan id 100 local 172.16.20.103 port 32768 61000 nolearning
        ageing 300 svcnode 172.16.21.125
```

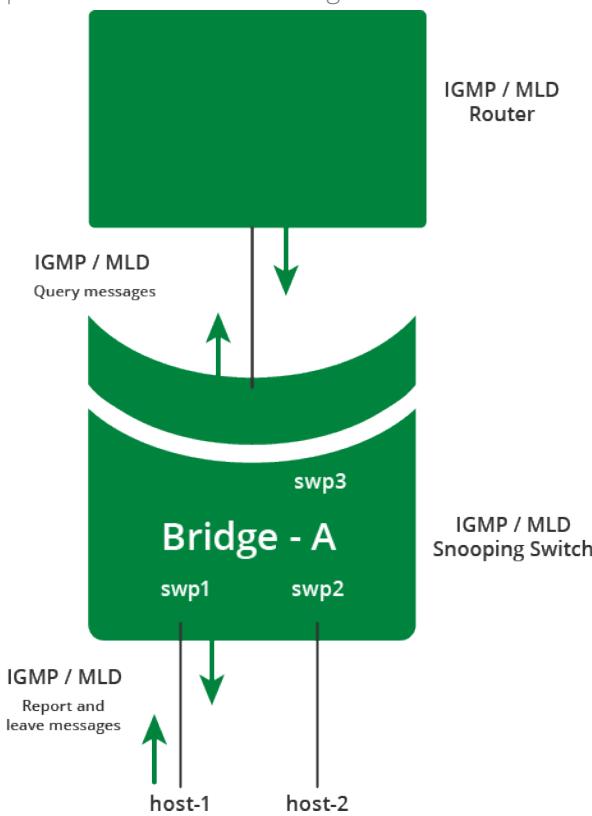
IGMP and MLD Snooping

IGMP (Internet Group Management Protocol) and MLD (Multicast Listener Discovery) snooping functionality is implemented in the bridge driver in the kernel. IGMP snooping processes IGMP v1/v2/v3 reports received on a bridge port in a bridge to identify the hosts which would like to receive multicast traffic destined to that group.

When an IGMPv2 leave message is received, a group specific query is sent to identify if there are any other hosts interested in that group, before the group is deleted.

An IGMP query message received on a port is used to identify the port that is connected to a router and is interested in receiving multicast traffic.

MLD snooping processes MLD v1/v2 reports, queries and v1 done messages for IPv6 groups. If IGMP or MLD snooping is disabled, multicast traffic will be flooded to all the bridge ports in the bridge. The multicast group IP address is mapped to a multicast MAC address and a forwarding entry is created with a list of ports interested in receiving multicast traffic destined to that group.



Contents

(Click to expand)

- [Contents \(see page 328\)](#)
- [Commands \(see page 329\)](#)
- [Creating a Bridge and Configuring IGMP/MLD Snooping \(see page 329\)](#)
- [Configuration Files \(see page 334\)](#)
- [Man Pages \(see page 334\)](#)
- [Useful Links \(see page 334\)](#)

Commands

- brctl
- bridge

Creating a Bridge and Configuring IGMP/MLD Snooping

You need to set a number of parameters for IGMP and MLD snooping, but the setting to enable it is `bridge-mcsnoop 1`. The following configuration in `/etc/network/interfaces` is for the example bridge above. For an explanation of the relevant parameters, see the `ifupdown-addons-interfaces` man page. In terms of IGMP/MLD snooping, make sure `bridge-mcsnoop` is true (it's enabled by default) and set the IP address for the querier in an SVI under the bridge.

```

auto br0
iface br0
    bridge-vlan-aware yes
    bridge-ports swp1 swp2 swp3
    bridge-vids 100 200
    bridge-pvid 1
    bridge-stp on
    bridge-mclmc 2
    bridge-mcrouter 1
    bridge-mcsnoop 1
    bridge-mcsqc 2
    bridge-mcqifaddr 0
    bridge-mcquerier 0
    bridge-hashel 4096
    bridge-hashmax 4096
    bridge-mclmi 1
    bridge-mcmi 260
    bridge-mcqpi 255
    bridge-mcqci 125
    bridge-mcqri 10
    bridge-mcsqi 31

# configure the source IP for the IGMP querier
auto bridge br0.100
iface br0.100
    bridge-mcsnoop 1
    bridge-igmp-querier-source 123.1.1.1

auto swp1
iface swp1
    bridge-vids 100

```

```
bridge-portmcrouter 1
bridge-portmcfl 0

auto swp2
iface swp2
    bridge-vids 200
    bridge-portmcrouter 1
    bridge-portmcfl 0

auto swp3
iface swp3
    bridge-access 100
```

Runtime Configuration (Advanced)



A runtime configuration is non-persistent, which means the configuration you create here does not persist after you reboot the switch.

To enable snooping at runtime, use the `brctl` command. Create a bridge and add bridge ports to the bridge. IGMP and MLD snooping are enabled by default on the bridge:

```
cumulus@switch:~$ sudo brctl addbr br0
cumulus@switch:~$ sudo brctl addif br0 swp1 swp2 swp3
cumulus@switch:~$ sudo ifconfig br0 up
```

To get the IGMP/MLD snooping bridge state, use:

```
cumulus@switch:~$ sudo brctl showstp br0
br0
bridge id          8000.7072cf8c272c
designated root    8000.7072cf8c272c
root port          0                  path cost      0
max age           20.00             bridge max age
20.00
hello time         2.00              bridge hello time
2.00
forward delay     15.00             bridge forward delay
15.00
ageing time       300.00            tcn timer
hello timer        0.00              gc timer
0.00
topology change timer 0.00
```

```

263.70
hash elasticity          4096           hash max           4096
mc last member count      2               mc init query count   2
mc router                  1               mc snooping          1
mc last member timer      1.00            mc membership timer
260.00
mc querier timer          255.00         mc query interval
125.00
mc response interval       10.00          mc init query interval
31.25
mc querier                 0               mc query ifaddr      0
flags

swp1 (1)
port id                   8001           state
forwarding
designated root            8000.7072cf8c272c path cost          2
designated bridge           8000.7072cf8c272c message age timer
0.00
designated port             8001           forward delay timer
0.00
designated cost              0              hold timer
0.00
mc router                   1               mc fast leave        0
flags

swp2 (2)
port id                   8002           state
forwarding
designated root            8000.7072cf8c272c path cost          2
designated bridge           8000.7072cf8c272c message age timer
0.00
designated port             8002           forward delay timer
0.00
designated cost              0              hold timer
0.00
mc router                   1               mc fast leave        0
flags

swp3 (3)
port id                   8003           state
forwarding
designated root            8000.7072cf8c272c path cost          2
designated bridge           8000.7072cf8c272c message age timer
0.00

```

designated port	8003	forward delay timer
8.98		
designated cost	0	hold timer
0.00		
mc router	1	mc fast leave
flags		0

To get the groups and bridge port state, use `bridge mdb show` command. To display router ports and group information use `bridge -d mdb show` command:

```
cumulus@switch:~$ sudo bridge -d mdb show
dev br0 port swp2 grp 234.10.10.10 temp
dev br0 port swp1 grp 238.39.20.86 permanent
dev br0 port swp1 grp 234.1.1.1 temp
dev br0 port swp2 grp ff1a::9 permanent
router ports on br0: swp3

cumulus@switch:~$ sudo bridge mdb show
dev br0 port swp2 grp 234.10.10.10 temp
dev br0 port swp1 grp 238.39.20.86 permanent
dev br0 port swp1 grp 234.1.1.1 temp
dev br0 port swp2 grp ff1a::9 permanent
```

To disable IGMP and MLD snooping, use:

```
cumulus@switch:~$ sudo brctl setmcsnoop br0 0
```

Configuring IGMP/MLD Snooping Parameters

For an explanation of these parameters, see the `brctl` and `ifupdown-addons-interfaces` man pages:

```
cumulus@switch:~$ sudo brctl setmclmc br0 2
cumulus@switch:~$ sudo brctl setmcrouter br0 1
cumulus@switch:~$ sudo brctl setmcsqc br0 2
cumulus@switch:~$ sudo brctl sethashel br0 4096
cumulus@switch:~$ sudo brctl sethashmax br0 4096
cumulus@switch:~$ sudo brctl setmclmi br0 1
cumulus@switch:~$ sudo brctl setmcmi br0 260
cumulus@switch:~$ sudo brctl setmcqpi br0 255
```

```
cumulus@switch:~$ sudo brctl setmcqi br0 125
cumulus@switch:~$ sudo brctl setmcqri br0 10
cumulus@switch:~$ sudo brctl setmsqi br0 31
```

Querier and Fast Leave Configuration

If there is no multicast router in the VLAN, the IGMP/MLD snooping querier can be configured to generate query messages.

To send queries with a non-zero IP address, configure an IP address on the bridge device, then set `setmcqifaddr` to 1:

```
cumulus@switch:~$ sudo brctl setmcquerier br0 1
cumulus@switch:~$ sudo brctl setmcqifaddr br0 1
```

If only one host is attached to each host port, fast leave can be configured on that port. When a leave message is received on that port, no query messages will be sent and the group will be deleted immediately:

```
cumulus@switch:~$ sudo brctl setportmcfl br0 swp1 1
```

Static Group and Router Port Configuration

To configure static permanent multicast group on a port, use:

```
cumulus@switch:~$ sudo bridge mdb add dev br0 port swp2 grp ff1a::9
permanent
cumulus@switch:~$ sudo bridge mdb add dev br0 port swp1 grp 238.39.20.86
permanent
```

A static temporary multicast group can also be configured on a port, which would be deleted after the membership timer expires, if no report is received on that port:

```
cumulus@switch:~$ sudo bridge mdb add dev br0 port swp1 grp 238.39.20.86
temp
```

To configure a static router port, use:

```
cumulus@switch:~$ sudo brctl setportmcrouter br0 swp3 2
```

Configuration Files

- /etc/network/interfaces

Man Pages

- brctl(8)
- bridge(8)
- ifupdown-addons-interfaces(5)

Useful Links

- <http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge#Snooping>
- <https://tools.ietf.org/html/rfc4541>
- http://en.wikipedia.org/wiki/IGMP_snooping
- <http://tools.ietf.org/rfc/rfc2236.txt>
- <http://tools.ietf.org/html/rfc3376>
- <http://tools.ietf.org/search/rfc2710>
- <http://tools.ietf.org/html/rfc3810>

Layer 3 Features

Routing

This chapter discusses routing on switches running Cumulus Linux.

Contents

(Click to expand)

- [Contents \(see page 335\)](#)
- [Commands \(see page 335\)](#)
- [Static Routing via ip route \(see page 335\)
 - \[Persistently Adding a Static Route \\(see page 337\\)\]\(#\)](#)
- [Static Routing via quagga \(see page 337\)
 - \[Persistent Configuration \\(see page 339\\)\]\(#\)](#)
- [Supported Route Table Entries \(see page 340\)](#)
- [Configuration Files \(see page 340\)](#)
- [Useful Links \(see page 340\)](#)
- [Caveats and Errata \(see page 340\)](#)

Commands

- [ip route](#)

Static Routing via ip route

The `ip route` command allows manipulating the kernel routing table directly from the Linux shell. See `man ip(8)` for details. `quagga` monitors the kernel routing table changes and updates its own routing table accordingly.

To display the routing table:

```
cumulus@switch:~$ ip route show
default via 10.0.1.2 dev eth0
10.0.1.0/24 dev eth0  proto kernel  scope link  src 10.0.1.52
192.0.2.0/24 dev swp1  proto kernel  scope link  src 192.0.2.12
192.0.2.10/24 via 192.0.2.1 dev swp1  proto zebra  metric 20
192.0.2.20/24  proto zebra  metric 20
    nexthop via 192.0.2.1  dev swp1 weight 1
    nexthop via 192.0.2.2  dev swp2 weight 1
192.0.2.30/24 via 192.0.2.1 dev swp1  proto zebra  metric 20
192.0.2.40/24 dev swp2  proto kernel  scope link  src 192.0.2.42
```

```
192.0.2.50/24 via 192.0.2.2 dev swp2 proto zebra metric 20
192.0.2.60/24 via 192.0.2.2 dev swp2 proto zebra metric 20
192.0.2.70/24 proto zebra metric 30
    nexthop via 192.0.2.1 dev swp1 weight 1
    nexthop via 192.0.2.2 dev swp2 weight 1
198.51.100.0/24 dev swp3 proto kernel scope link src 198.51.100.1
198.51.100.10/24 dev swp4 proto kernel scope link src 198.51.100.11
198.51.100.20/24 dev br0 proto kernel scope link src 198.51.100.21
```

To add a static route (does not persist across reboots):

```
cumulus@switch:~$ sudo ip route add 203.0.113.0/24 via 198.51.100.2
cumulus@switch:~$ ip route
default via 10.0.1.2 dev eth0
10.0.1.0/24 dev eth0 proto kernel scope link src 10.0.1.52
192.0.2.0/24 dev swp1 proto kernel scope link src 192.0.2.12
192.0.2.10/24 via 192.0.2.1 dev swp1 proto zebra metric 20
192.0.2.20/24 proto zebra metric 20
    nexthop via 192.0.2.1 dev swp1 weight 1
    nexthop via 192.0.2.2 dev swp2 weight 1
192.0.2.30/24 via 192.0.2.1 dev swp1 proto zebra metric 20
192.0.2.40/24 dev swp2 proto kernel scope link src 192.0.2.42
192.0.2.50/24 via 192.0.2.2 dev swp2 proto zebra metric 20
192.0.2.60/24 via 192.0.2.2 dev swp2 proto zebra metric 20
192.0.2.70/24 proto zebra metric 30
    nexthop via 192.0.2.1 dev swp1 weight 1
    nexthop via 192.0.2.2 dev swp2 weight 1
198.51.100.0/24 dev swp3 proto kernel scope link src 198.51.100.1
198.51.100.10/24 dev swp4 proto kernel scope link src 198.51.100.11
198.51.100.20/24 dev br0 proto kernel scope link src 198.51.100.21
203.0.113.0/24 via 198.51.100.2 dev swp3
```

To delete a static route (does not persist across reboots):

```
cumulus@switch:~$ sudo ip route del 203.0.113.0/24
cumulus@switch:~$ ip route
default via 10.0.1.2 dev eth0
10.0.1.0/24 dev eth0 proto kernel scope link src 10.0.1.52
192.0.2.0/24 dev swp1 proto kernel scope link src 192.0.2.12
192.0.2.10/24 via 192.0.2.1 dev swp1 proto zebra metric 20
192.0.2.20/24 proto zebra metric 20
    nexthop via 192.0.2.1 dev swp1 weight 1
```

```

nexthop via 192.0.2.2 dev swp2 weight 1
192.0.2.30/24 via 192.0.2.1 dev swp1 proto zebra metric 20
192.0.2.40/24 dev swp2 proto kernel scope link src 192.0.2.42
192.0.2.50/24 via 192.0.2.2 dev swp2 proto zebra metric 20
192.0.2.60/24 via 192.0.2.2 dev swp2 proto zebra metric 20
192.0.2.70/24 proto zebra metric 30
    nexthop via 192.0.2.1 dev swp1 weight 1
    nexthop via 192.0.2.2 dev swp2 weight 1
198.51.100.0/24 dev swp3 proto kernel scope link src 198.51.100.1
198.51.100.10/24 dev swp4 proto kernel scope link src 198.51.100.11
198.51.100.20/24 dev br0 proto kernel scope link src 198.51.100.21

```

Persistently Adding a Static Route

A static route can be persistently added by adding up ip route add .. into /etc/network/interfaces. For example:

```

cumulus@switch:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

auto swp3
iface swp3
    address 198.51.100.1/24
    up ip route add 203.0.113.0/24 via 198.51.100.2

```



Notice the simpler configuration of swp3 due to ifupdown2. For more information, see [Configuring Network Interfaces with ifupdown](#) (see page 121).

Static Routing via quagga

Static routes can also be managed via the quagga CLI. The routes are added to the quagga routing table, and then will be updated into the kernel routing table as well.

To add a static route (does not persist across reboot):

```
cumulus@switch:~$ sudo vtysh

Hello, this is Quagga (version 0.99.21).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

switch# conf t
switch(config)# ip route 203.0.113.0/24 198.51.100.2
switch(config)# end
switch# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 via 10.0.1.2, eth0
C>* 10.0.1.0/24 is directly connected, eth0
O   192.0.2.0/24 [110/10] is directly connected, swp1, 00:13:25
C>* 192.0.2.0/24 is directly connected, swp1
O>* 192.0.2.10/24 [110/20] via 192.0.2.1, swp1, 00:13:09
O>* 192.0.2.20/24 [110/20] via 192.0.2.1, swp1, 00:13:09
      *           via 192.0.2.41, swp2, 00:13:09
O>* 192.0.2.30/24 [110/20] via 192.0.2.1, swp1, 00:13:09
O   192.0.2.40/24 [110/10] is directly connected, swp2, 00:13:25
C>* 192.0.2.40/24 is directly connected, swp2
O>* 192.0.2.50/24 [110/20] via 192.0.2.41, swp2, 00:13:09
O>* 192.0.2.60/24 [110/20] via 192.0.2.41, swp2, 00:13:09
O>* 192.0.2.70/24 [110/30] via 192.0.2.1, swp1, 00:13:09
      *           via 192.0.2.41, swp2, 00:13:09
O   198.51.100.0/24 [110/10] is directly connected, swp3, 00:13:22
C>* 198.51.100.0/24 is directly connected, swp3
O   198.51.100.10/24 [110/10] is directly connected, swp4, 00:13:22
C>* 198.51.100.10/24 is directly connected, swp4
O   198.51.100.20/24 [110/10] is directly connected, br0, 00:13:22
C>* 198.51.100.20/24 is directly connected, br0
S>* 203.0.113.0/24 [1/0] via 198.51.100.2, swp3
C>* 127.0.0.0/8 is directly connected, lo
```

To delete a static route (does not persist across reboot):

```
cumulus@switch:~$ sudo vtysh

Hello, this is Quagga (version 0.99.21).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
```

```

switch# conf t
switch(config)# no ip route 203.0.113.0/24 198.51.100.2
switch(config)# end
switch# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 via 10.0.1.2, eth0
C>* 10.0.1.0/24 is directly connected, eth0
O   192.0.2.0/24 [110/10] is directly connected, swp1, 00:13:55
C>* 192.0.2.0/24 is directly connected, swp1
O>* 192.0.2.10/24 [110/20] via 11.0.0.1, swp1, 00:13:39
O>* 192.0.2.20/24 [110/20] via 11.0.0.1, swp1, 00:13:39
      *           via 11.0.4.1, swp2, 00:13:39
O>* 192.0.2.30/24 [110/20] via 11.0.0.1, swp1, 00:13:39
O   192.0.2.40/24 [110/10] is directly connected, swp2, 00:13:55
C>* 192.0.2.40/24 is directly connected, swp2
O>* 192.0.2.50/24 [110/20] via 11.0.4.1, swp2, 00:13:39
O>* 192.0.2.60/24 [110/20] via 11.0.4.1, swp2, 00:13:39
O>* 192.0.2.70/24 [110/30] via 11.0.0.1, swp1, 00:13:39
      *           via 11.0.4.1, swp2, 00:13:39
O   198.51.100.0/24 [110/10] is directly connected, swp3, 00:13:52
C>* 198.51.100.0/24 is directly connected, swp3
O   198.51.100.10/24 [110/10] is directly connected, swp4, 00:13:52
C>* 198.51.100.10/24 is directly connected, swp4
O   198.51.100.20/24 [110/10] is directly connected, br0, 00:13:52
C>* 198.51.100.20/24 is directly connected, br0
C>* 127.0.0.0/8 is directly connected, lo
switch#

```

Persistent Configuration

From the quagga CLI, the running configuration can be saved so it persists between reboots:

```

switch# write mem
Configuration saved to /etc/quagga/zebra.conf
switch# end

```

Supported Route Table Entries

Cumulus Linux supports different numbers of route entries, depending upon your switch platform (Trident, Trident+, or Trident II; see the [HCL](#)) and whether the routes are IPv4 or IPv6.

In addition, switches on the Trident II platform are configured to manage route table entries using Algorithm Longest Prefix Match (ALPM). In ALPM mode, the hardware can store significantly more route entries.

Following are the number of route supported on Trident II switches with ALPM:

- 32K IPv4 routes
- 16K IPv6 routes
- 32K total routes (both IPv4 and IPv6)

Following are the number of route supported on Trident and Trident+ switches:

- 16K IPv4 routes
- 8K IPv6 routes
- 16K total routes (both IPv4 and IPv6)

Configuration Files

- /etc/network/interfaces
- /etc/quagga/zebra.conf

Useful Links

- <http://linux-ip.net/html/tools-ip-route.html>
- <http://www.nongnu.org/quagga/docs/docs-info.html#Static-Route-Commands>

Caveats and Errata

- Static routes added via `quagga` can be deleted via Linux shell. This operation, while possible, should be avoided. Routes added by `quagga` should only be deleted by `quagga`, otherwise `quagga` might not be able to clean up all its internal state completely and incorrect routing can occur as a result.

Introduction to Routing Protocols

This chapter discusses the various routing protocols, and how to configure them.

Contents

(Click to expand)

- [Contents \(see page 340\)](#)
- [Defining Routing Protocols \(see page 341\)](#)
- [Configuring Routing Protocols \(see page 341\)](#)
- [Protocol Tuning \(see page 341\)](#)
- [Configuration Files \(see page 342\)](#)

Defining Routing Protocols

A *routing protocol* dynamically computes reachability between various end points. This enables communication to work around link and node failures, and additions and withdrawals of various addresses.

IP routing protocols are typically distributed; that is, an instance of the routing protocol runs on each of the routers in a network.



Cumulus Linux does **not** support running multiple instances of the same protocol on a router.

Distributed routing protocols compute reachability between end points by disseminating relevant information and running a routing algorithm on this information to determine the routes to each end station. To scale the amount of information that needs to be exchanged, routes are computed on address prefixes rather than on every end point address.

Configuring Routing Protocols

A routing protocol needs to know three pieces of information, at a minimum:

- Who am I (my identity)
- To whom to disseminate information
- What to disseminate

Most routing protocols use the concept of a router ID to identify a node. Different routing protocols answer the last two questions differently.

The way they answer these questions affects the network design and thereby configuration. For example, in a link-state protocol such as OSPF (see [Open Shortest Path First \(OSPF\) Protocol \(see page 358\)](#)) or IS-IS, complete local information (links and attached address prefixes) about a node is disseminated to every other node in the network. Since the state that a node has to keep grows rapidly in such a case, link-state protocols typically limit the number of nodes that communicate this way. They allow for bigger networks to be built by breaking up a network into a set of smaller subnetworks (which are called areas or levels), and by advertising summarized information about an area to other areas.

Besides the two critical pieces of information mentioned above, protocols have other parameters that can be configured. These are usually specific to each protocol.

Protocol Tuning

Most protocols provide certain tunable parameters that are specific to convergence during changes.

Wikipedia defines **convergence** as the “state of a set of routers that have the same topological information about the network in which they operate”. It is imperative that the routers in a network have the same topological state for the proper functioning of a network. Without this, traffic can be blackholed, and thus not reach its destination. It is normal for different routers to have differing topological states during changes, but this difference should vanish as the routers exchange information about the change and recompute the forwarding paths. Different protocols converge at different speeds in the presence of changes.

A key factor that governs how quickly a routing protocol converges is the time it takes to detect the change. For example, how quickly can a routing protocol be expected to act when there is a link failure. Routing protocols classify changes into two kinds: hard changes such as link failures, and soft changes such as a peer dying silently. They're classified differently because protocols provide different mechanisms for dealing with these failures.

It is important to configure the protocols to be notified immediately on link changes. This is also true when a node goes down, causing all of its links to go down.

Even if a link doesn't fail, a routing peer can crash. This causes that router to usually delete the routes it has computed or worse, it makes that router impervious to changes in the network, causing it to go out of sync with the other routers in the network because it no longer shares the same topological information as its peers.

The most common way to detect a protocol peer dying is to detect the absence of a heartbeat. All routing protocols send a heartbeat (or "hello") packet periodically. When a node does not see a consecutive set of these hello packets from a peer, it declares its peer dead and informs other routers in the network about this. The period of each heartbeat and the number of heartbeats that need to be missed before a peer is declared dead are two popular configurable parameters.

If you configure these timers very low, the network can quickly descend into instability under stressful conditions when a router is not able to keep sending the heartbeats quickly as it is busy computing routing state; or the traffic is so much that the hellos get lost. Alternately, configuring this timer to very high values also causes blackholing of communication because it takes much longer to detect peer failures. Usually, the default values initialized within each protocol are good enough for most networks. Cumulus Networks recommends you do not adjust these settings.

Configuration Files

- /etc/quagga/daemons

Network Topology

In computer networks, *topology* refers to the structure of interconnecting various nodes. Some commonly used topologies in networks are star, hub and spoke, leaf and spine, and broadcast.

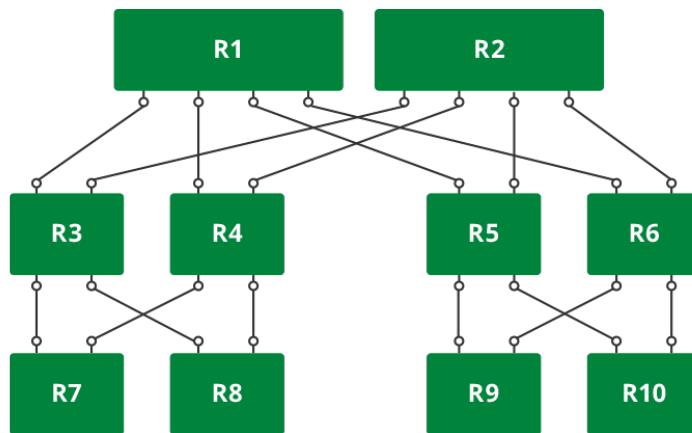
Contents

(Click to expand)

- [Contents \(see page 342\)](#)
- [Clos Topologies \(see page 342\)](#)
- [Over-Subscribed and Non-Blocking Configurations \(see page 343\)](#)
- [Containing the Failure Domain \(see page 343\)](#)
- [Load Balancing \(see page 344\)](#)

Clos Topologies

In the vast majority of modern data centers, [Clos or fat tree topology](#) is very popular. This topology is shown in the figure below. It is also commonly referred to as leaf-spine topology. We shall use this topology throughout the routing protocol guide.



This topology allows the building of networks of varying size using nodes of different port counts and/or by increasing the tiers. The picture above is a three-tiered Clos network. We number the tiers from the bottom to the top. Thus, in the picture, the lowermost layer is called tier 1 and the topmost tier is called tier 3.

The number of end stations (such as servers) that can be attached to such a network is determined by a very simple mathematical formula.

In a 2-tier network, if each node is made up of m ports, then the total number of end stations that can be connected is $m^2/2$. In more general terms, if tier-1 nodes are m -port nodes and tier-2 nodes are n -port nodes, then the total number of end stations that can be connected are $(m*n)/2$. In a three tier network, where tier-3 nodes are o -port nodes, the total number of end stations that can be connected are $(m*n*o)/2^{(\text{number of tiers}-1)}$.

Let's consider some practical examples. In many data centers, it is typical to connect 40 servers to a top-of-rack (ToR) switch. The ToRs are all connected via a set of spine switches. If a ToR switch has 64 ports, then after hooking up 40 ports to the servers, the remaining 24 ports can be hooked up to 24 spine switches of the same link speed or to a smaller number of higher link speed switches. For example, if the servers are all hooked up as 10GE links, then the ToRs can connect to the spine switches via 40G links. So, instead of connecting to 24 spine switches with 10G links, the ToRs can connect to 6 spine switches with each link being 40G. If the spine switches are also 64-port switches, then the total number of end stations that can be connected is 2560 ($40*64$) stations.

In a three tier network of 64-port switches, the total number of servers that can be connected are $(40*64*64)/2 = 81920$. As you can see, this kind of topology can serve quite a large network with three tiers.

Over-Subscribed and Non-Blocking Configurations

In the above example, the network is *over-subscribed*; that is, 400G of bandwidth from end stations (40 servers * 10GE links) is serviced by only 240G of inter-rack bandwidth. The over-subscription ratio is 0.6 ($240/400$).

This can lead to congestion in the network and hot spots. Instead, if network operators connected 32 servers per rack, then 32 ports are left to be connected to spine switches. Now, the network is said to be *rearrangably non-blocking*. Now any server in a rack can talk to any other server in any other rack without necessarily blocking traffic between other servers.

In such a network, the total number of servers that can be connected are $(64*64)/2 = 2048$. Similarly, a three-tier version of the same can serve up to $(64*64*64)/4 = 65536$ servers.

Containing the Failure Domain

Traditional data centers were built using just two spine switches. This means that if one of those switches fails, the network bandwidth is cut in half, thereby greatly increasing network congestion and adversely affecting many applications. To avoid this, vendors typically try and make the spine switches resilient to

failures by providing such features as dual control line cards and attempting to make the software highly available. However, as Douglas Adams famously noted, ">>>". In many cases, HA is among the top two or three causes of software failure (and thereby switch failure).

To support a fairly large network with just two spine switches also means that these switches have a large port count. This can make the switches quite expensive.

If the number of spine switches were to be merely doubled, the effect of a single switch failure is halved. With 8 spine switches, the effect of a single switch failure only causes a 12% reduction in available bandwidth.

So, in modern data centers, people build networks with anywhere from 4 to 32 spine switches.

Load Balancing

In a Clos network, traffic is load balanced across the multiple links using equal cost multi-pathing (ECMP).

Routing algorithms compute shortest paths between two end stations where shortest is typically the lowest path cost. Each link is assigned a metric or cost. By default, a link's cost is a function of the link speed. The higher the link speed, the lower its cost. A 10G link has a higher cost than a 40G or 100G link, but a lower cost than a 1G link. Thus, the link cost is a measure of its traffic carrying capacity.

In the modern data center, the links between tiers of the network are homogeneous; that is, they have the same characteristics (same speed and therefore link cost) as the other links. As a result, the first hop router can pick any of the spine switches to forward a packet to its destination (assuming that there is no link failure between the spine and the destination switch). Most routing protocols recognize that there are multiple equal-cost paths to a destination and enable any of them to be selected for a given traffic flow.

Quagga Overview

Cumulus Linux uses `quagga`, an open source routing software suite, to provide the routing protocols for dynamic routing. Cumulus Linux supports the latest Quagga version, 0.99.23.1. Quagga is a fork of the [GNU Zebra](#) project.

Quagga provides many routing protocols, of which Cumulus Linux supports the following:

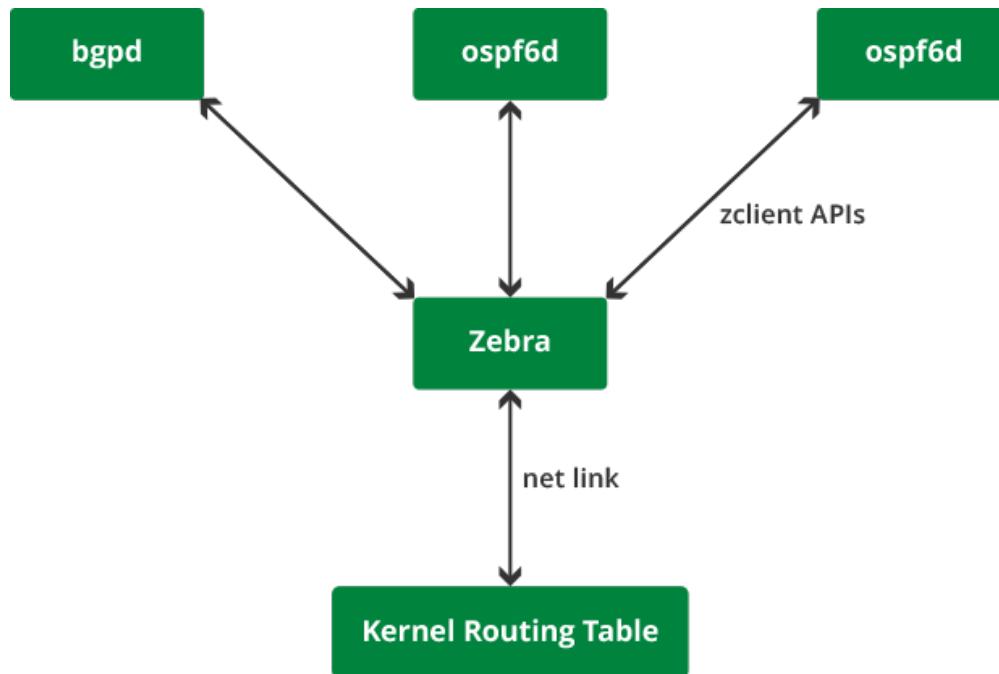
- Open Shortest Path First ([v2 \(see page 358\)](#) and [v3 \(see page 369\)](#))
- Border Gateway Protocol ([see page 372](#))

Contents

(Click to expand)

- [Contents \(see page 344\)](#)
- [Architecture \(see page 345\)](#)
- [Zebra \(see page 345\)](#)
- [Configuration Files \(see page 345\)](#)
- [Useful Links \(see page 346\)](#)

Architecture



As shown in the figure above, the Quagga routing suite consists of various protocol-specific daemons and a protocol-independent daemon called **zebra**. Each of the protocol-specific daemons are responsible for running the relevant protocol and building the routing table based on the information exchanged.

It is not uncommon to have more than one protocol daemon running at the same time. For example, at the edge of an enterprise, protocols internal to an enterprise (called IGP for Interior Gateway Protocol) such as [OSPF \(see page 358\)](#) or RIP run alongside the protocols that connect an enterprise to the rest of the world (called EGP or Exterior Gateway Protocol) such as [BGP \(see page 372\)](#).

zebra is the daemon that resolves the routes provided by multiple protocols (including static routes specified by the user) and programs these routes in the Linux kernel via **netlink** (in Linux). **zebra** does more than this, of course.

Zebra

The [quagga documentation](#) defines **zebra** as the IP routing manager for **quagga** that “provides kernel routing table updates, interface lookups, and redistribution of routes between different routing protocols.”

Configuration Files

- /etc/quagga/bgpd.conf
- /etc/quagga/daemons
- /etc/quagga/debian.conf
- /etc/quagga/ospf6d.conf
- /etc/quagga/ospfd.conf
- /etc/quagga/vtysh.conf
- /etc/quagga/zebra.conf

Useful Links

- <http://www.quagga.net/>
- <http://packages.debian.org/quagga>

Configuring Quagga

This section provides an overview of configuring quagga.

Before you run quagga, make sure all relevant daemons, such as zebra, are running. Make your changes in /etc/quagga/daemons then restart quagga with service quagga restart.

Contents

(Click to expand)

- Contents (see page 346)
- Configuration Files (see page 347)
 - Starting Quagga (see page 347)
 - Understanding Integrated Configurations (see page 347)
 - Restoring the Default Quagga Configuration (see page 349)
- Interface IP Addresses (see page 349)
- Using the vtysh Modal CLI (see page 349)
- Using the Cumulus Linux Non-Modal CLI (see page 354)
- Comparing vtysh and Cumulus Linux Commands (see page 354)
 - Displaying the Routing Table (see page 354)
 - Creating a New Neighbor (see page 355)
 - Redistributing Routing Information (see page 355)
 - Defining a Static Route (see page 355)
 - Configuring an IPv6 Interface (see page 355)
 - Enabling PTM (see page 356)
 - Configuring MTU in IPv6 Network Discovery (see page 356)
 - Logging OSPF Adjacency Changes (see page 356)
 - Setting OSPF Interface Priority (see page 357)
 - Configuring Timing for OSPF SPF Calculations (see page 357)
 - Configuring Hello Packet Intervals (see page 357)
 - Displaying OSPF Debugging Status (see page 358)
 - Displaying BGP Information (see page 358)
- Useful Links (see page 358)

Configuration Files

At startup, `quagga` reads a set of files to determine the startup configuration. The files and what they contain are specified below:

File	Description
Quagga.conf	The default, integrated, single configuration file for all <code>quagga</code> daemons.
daemons	Contains the list of <code>quagga</code> daemons that must be started.
zebra.conf	Configuration file for the <code>zebra</code> daemon.
ospfd.conf	Configuration file for the OSPFv2 daemon.
ospf6d.conf	Configuration file for the OSPFv3 daemon.
bgpd.conf	Configuration file for the BGP daemon.

Starting Quagga

Quagga does not start by default in Cumulus Linux 2.0 and later versions.

Before you start `quagga`, modify `/etc/quagga/daemons` to enable the corresponding daemons:

```
zebra=yes (* this one is mandatory to bring the others up)
bgpd=yes
ospfd=yes
ospf6d=yes
ripd=no
ripngd=no
isisd=no
babeld=no
```

Then, start `quagga`:

```
cumulus@switch1:~$ sudo service quagga start
```

Understanding Integrated Configurations

By default in Cumulus Linux, `quagga` saves the configuration of all daemons in a single integrated configuration file, `Quagga.conf`.

You can disable this mode by running:

```
quagga(config)# no service integrated-vtysh-config  
quagga(config)#
```

To enable the integrated configuration file mode again, run:

```
quagga(config)# service integrated-vtysh-config  
quagga(config)#
```

If you disable the integrated configuration mode, `quagga` saves each daemon-specific configuration file in a separate file. At a minimum for a daemon to start, that daemon must be specified in the `daemons` file and the daemon-specific configuration file must be present, even if that file is empty.

For example, to start `bgpd`, the `daemons` file needs to be formatted as follows, at minimum:

```
cumulus@switch:~$ sudo cat /etc/quagga/daemons  
zebra=yes  
bgpd=yes
```

The current configuration can be saved by running:

```
quagga# write mem  
Building Configuration...  
Integrated configuration saved to /etc/quagga/Quagga.conf  
[OK]
```



You can use `write file` instead of `write mem`.

When the integrated configuration mode disabled, the output looks like this:

```
quagga# write mem  
Building Configuration...  
Configuration saved to /etc/quagga/zebra.conf  
Configuration saved to /etc/quagga/bgpd.conf  
[OK]
```



The `daemons` file is not written using the `write mem` command.

Restoring the Default Quagga Configuration

If you need to restore the Quagga configuration to the default running configuration, you need to delete the Quagga.conf file and restart the quagga service.

1. Confirm service integrated-vtysh-config is enabled:

```
cumulus@switch$ sudo cl-rctl running-config |grep integrated  
service integrated-vtysh-config
```

2. Remove /etc/quagga/Quagga.conf:

```
cumulus@switch$ sudo rm /etc/quagga/Quagga.conf
```

3. Restart the quagga service:

```
cumulus@switch$ sudo service quagga restart
```



If for some reason service integrated-vtysh-config is not configured, then you should remove zebra.conf instead of Quagga.conf in step 2 above.

Interface IP Addresses

Quagga inherits the IP addresses for the network interfaces from the /etc/network/interfaces file. This is the recommended way to define the addresses. For more information, see [Configuring IP Addresses](#) (see page 123).

Using the vtysh Modal CLI

Quagga provides a CLI – vtysh – for configuring and displaying the state of the protocols. It is invoked by running:

```
cumulus@switch:~$ sudo vtysh  
  
Hello, this is Quagga (version 0.99.21).  
Copyright 1996-2005 Kunihiro Ishiguro, et al.  
  
quagga#
```

Launching `vtysh` brings you into `zebra` initially. From here, you can log into other protocol daemons, such as `bgpd`, `ospf` or `babeld`.

`vtysh` provides a Cisco-like modal CLI, and many of the commands are similar to Cisco IOS commands. By modal CLI, we mean that there are different modes to the CLI, and certain commands are only available within a specific mode. Configuration is available with the `configure terminal` command, which is invoked thus:

```
quagga# configure terminal  
quagga(config)#
```

The prompt displays the mode the CLI is in. For example, when the interface-specific commands are invoked, the prompt changes to:

```
quagga(config)# interface swp1  
quagga(config-if)#
```

When the routing protocol specific commands are invoked, the prompt changes to:

```
quagga(config)# router ospf  
quagga(config-router)#
```

At any level, "?" displays the list of available top-level commands at that level:

```
quagga(config-if)# ?  
babel      Babel interface commands  
bandwidth   Set bandwidth informational parameter  
description Interface specific description  
end        End current mode and change to enable mode  
exit        Exit current mode and down to previous mode  
ip          Interface Internet Protocol config commands  
ipv6       Interface IPv6 config commands  
isis        IS-IS commands  
link-detect Enable link detection on interface  
list        Print command list  
mpls-te    MPLS-TE specific commands  
multicast   Set multicast flag to interface  
no          Negate a command or set its defaults  
ospf        OSPF interface commands  
quit        Exit current mode and down to previous mode  
shutdown   Shutdown the selected interface
```

?-based completion is also available to see the parameters that a command takes:

```
quagga(config-if)# bandwidth ?
<1-10000000> Bandwidth in kilobits
quagga(config-if)# ip ?
address Set the IP address of an interface
irdp Alter ICMP Router discovery preference this interface
ospf OSPF interface commands
rip Routing Information Protocol
router IP router interface commands
```

Displaying state can be done at any level, including the top level. For example, to see the routing table as seen by zebra, you use:

```
quagga# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 via 192.168.0.2, eth0
C>* 192.0.2.11/24 is directly connected, swp1
C>* 192.0.2.12/24 is directly connected, swp2
B>* 203.0.113.30/24 [200/0] via 192.0.2.2, swp1, 10:43:05
B>* 203.0.113.31/24 [200/0] via 192.0.2.2, swp1, 10:43:05
B>* 203.0.113.32/24 [200/0] via 192.0.2.2, swp1, 10:43:05
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.0.0/24 is directly connected, eth0
```

To run the same command at a config level, you prepend do to it:

```
quagga(config-router)# do show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 via 192.168.0.2, eth0
C>* 192.0.2.11/24 is directly connected, swp1
C>* 192.0.2.12/24 is directly connected, swp2
B>* 203.0.113.30/24 [200/0] via 192.0.2.2, swp1, 10:43:05
B>* 203.0.113.31/24 [200/0] via 192.0.2.2, swp1, 10:43:05
```

```
B>* 203.0.113.32/24 [200/0] via 192.0.2.2, swp1, 10:43:05
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.0.0/24 is directly connected, eth0
```

Running single commands with `vtysh` is possible using the `-c` option of `vtysh`:

```
cumulus@switch:~$ sudo vtysh -c 'sh ip route'
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 via 192.168.0.2, eth0
C>* 192.0.2.11/24 is directly connected, swp1
C>* 192.0.2.12/24 is directly connected, swp2
B>* 203.0.113.30/24 [200/0] via 192.0.2.2, swp1, 11:05:10
B>* 203.0.113.31/24 [200/0] via 192.0.2.2, swp1, 11:05:10
B>* 203.0.113.32/24 [200/0] via 192.0.2.2, swp1, 11:05:10
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.0.0/24 is directly connected, eth0
```

Running a command multiple levels down is done thus:

```
cumulus@switch:~$ sudo vtysh -c 'configure terminal' -c 'router ospf' -c
'area 0.0.0.1 range 10.10.10.0/24'
```

Notice that the commands also take a partial command name (for example, `sh ip route` above) as long as the partial command name is not aliased:

```
cumulus@switch:~$ sudo vtysh -c 'sh ip r'
% Ambiguous command.
```

A command or feature can be disabled by prepending the command with `no`. For example:

```
quagga(config-router)# no area 0.0.0.1 range 10.10.10.0/24
```

The current state of the configuration can be viewed via:

```
quagga# show running-config
```

```
Building configuration...
```

```
Current configuration:
```

```
!
hostname quagga
log file /media/node/zebra.log
log file /media/node/bgpd.log
log timestamp precision 6
!
service integrated-vtysh-config
!
password xxxxxx
enable password xxxxxx
!
interface eth0
ipv6 nd suppress-ra
link-detect
!
interface lo
link-detect
!
interface swp1
ipv6 nd suppress-ra
link-detect
!
interface swp2
ipv6 nd suppress-ra
link-detect
!
router bgp 65000
bgp router-id 0.0.0.9
bgp log-neighbor-changes
bgp scan-time 20
network 29.0.1.0/24
timers bgp 30 90
neighbor tier-2 peer-group
neighbor 192.0.2.2 remote-as 65000
neighbor 192.0.2.2 ttl-security hops 1
neighbor 192.0.2.2 advertisement-interval 30
neighbor 192.0.2.2 timers 30 90
neighbor 192.0.2.2 timers connect 30
neighbor 192.0.2.2 next-hop-self
neighbor 192.0.2.12 remote-as 65000
neighbor 192.0.2.12 next-hop-self
neighbor 203.0.113.1 remote-as 65000
```

```
!
ip forwarding
ipv6 forwarding
!
line vty
exec-timeout 0 0
!
end
```

Using the Cumulus Linux Non-Modal CLI

The `vtysh` modal CLI can be difficult to work with and even more difficult to script. As an alternative to this, Cumulus Linux contains a non-modal version of these commands, structured similar to the Linux `ip` command. The available commands are:

Command	Description
<code>cl-bgp</code>	BGP (see page 372) commands. See <code>man cl-bgp</code> for details.
<code>cl-ospf</code>	OSPFv2 (see page 358) commands. For example: <code>cumulus@switch:~\$ sudo cl-ospf area 0.0.0.1 range 10.10.10.0/24</code>
<code>cl-ospf6</code>	OSPFv3 (see page 369) commands.
<code>cl-ra</code>	Route advertisement commands. See <code>man cl-ra</code> for details.
<code>cl-rctl</code>	Zebra and non-routing protocol-specific commands. See <code>man cl-rctl</code> for details.

Comparing `vtysh` and Cumulus Linux Commands

This section describes how you can use the various Cumulus Linux CLI commands to configure Quagga, without using `vtysh`.

Displaying the Routing Table

To display the routing table under Quagga, you would run:

```
quagga# show ip route
```

To display the routing table with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-rctl route
```

Creating a New Neighbor

To create a new neighbor under Quagga, you would run:

```
quagga(config)# router bgp 65002
quagga(config-router)# neighbor 14.0.0.22 remote-as 65007
```

To create a new neighbor with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-bgp as 65002 neighbor add 14.0.0.22 remote-as
65007
```

Redistributing Routing Information

To redistribute routing information from static route entries into RIP tables under Quagga, you would run:

```
quagga(config)# router bgp 65002
quagga(config-router)# redistribute static
```

To redistribute routing information from static route entries into RIP tables with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-bgp as 65002 redistribute add static
```

Defining a Static Route

To define a static route under Quagga, you would run:

```
quagga(config)# ip route 155.1.2.20/24 br2 45
```

To define a static route with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-rctl ip route add 175.0.0.0/28 interface br1
distance 25
```

Configuring an IPv6 Interface

To configure an IPv6 address under Quagga, you would run:

```
quagga(config)# int br3
quagga(config-if)# ipv6 address 3002:2123:1234:1abc::21/64
```

To configure an IPv6 address with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-rctl interface add swp3 ipv6 address 3002:2123:
abcd:2120::41/64
```

Enabling PTM

To enable topology checking (PTM) under Quagga, you would run:

```
quagga(config)# ptm-enable
```

To enable topology checking (PTM) with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-rctl ptm-enable set
```

Configuring MTU in IPv6 Network Discovery

To configure MTU (see page 137) in IPv6 network discovery for an interface under Quagga, you would run:

```
quagga(config)# int swp3
quagga(config-if)# ipv6 nd mtu 9000
```

To configure MTU in IPv6 network discovery for an interface with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-ra interface swp3 set mtu 9000
```

Logging OSPF Adjacency Changes

To log adjacency of OSPF changes under Quagga, you would run:

```
quagga(config)# router ospf
quagga(config-router)# router-id 2.0.0.21
quagga(config-router)# log-adjacency-changes
```

To log adjacency changes of OSPF with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-ospf log-adjacency-changes set  
cumulus@switch:~$ sudo cl-ospf router-id set 3.0.0.21
```

Setting OSPF Interface Priority

To set the OSPF interface priority under Quagga, you would run:

```
quagga(config)# int swp3  
quagga(config-if)# ip ospf priority 120
```

To set the OSPF interface priority with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-ospf interface set swp3 priority 120
```

Configuring Timing for OSPF SPF Calculations

To configure timing for OSPF SPF calculations under Quagga, you would run:

```
quagga(config)# router ospf6  
quagga(config-ospf6)# timer throttle spf 40 50 60
```

To configure timing for OSPF SPF calculations with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-ospf6 timer add throttle spf 40 50 60
```

Configuring Hello Packet Intervals

To configure the OSPF Hello packet interval in number of seconds for an interface under Quagga, you would run:

```
quagga(config)# int swp4  
quagga(config-if)# ipv6 ospf6 hello-interval 60
```

To configure the OSPF Hello packet interval in number of seconds for an interface with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-ospf6 interface set swp4 hello-interval 60
```

Displaying OSPF Debugging Status

To display OSPF debugging status under Quagga, you would run:

```
quagga# show debugging ospf
```

To display OSPF debugging status with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-ospf debug show
```

Displaying BGP Information

To display BGP information under Quagga, you would run:

```
quagga# show ip bgp summary
```

To display BGP information with the Cumulus Linux CLI, run:

```
cumulus@switch:~$ sudo cl-bgp summary
```

Useful Links

- <http://www.nongnu.org/quagga/docs/docs-info.html#BGP>
- <http://www.nongnu.org/quagga/docs/docs-info.html#IPv6-Support>
- <http://www.nongnu.org/quagga/docs/docs-info.html#Zebra>

Open Shortest Path First - OSPF - Protocol

OSPFv2 is a [link-state routing protocol](#) for IPv4. OSPF maintains the view of the network topology conceptually as a directed graph. Each router represents a vertex in the graph. Each link between neighboring routers represents a unidirectional edge. Each link has an associated weight (called cost) that is either automatically derived from its bandwidth or administratively assigned. Using the weighted topology graph, each router computes a shortest path tree (SPT) with itself as the root, and applies the results to build its forwarding table. The computation is generally referred to as *SPF computation* and the resultant tree as the *SPF tree*.

An LSA (*link-state advertisement*) is the fundamental quantum of information that OSPF routers exchange with each other. It seeds the graph building process on the node and triggers SPF computation. LSAs originated by a node are distributed to all the other nodes in the network through a mechanism called *flooding*. Flooding is done hop-by-hop. OSPF ensures reliability by using link state acknowledgement packets. The set of LSAs in a router's memory is termed *link-state database* (LSDB), a representation of the network graph. Thus, OSPF ensures a consistent view of LSDB on each node in the network in a distributed fashion (eventual consistency model); this is key to the protocol's correctness.

Contents

(Click to expand)

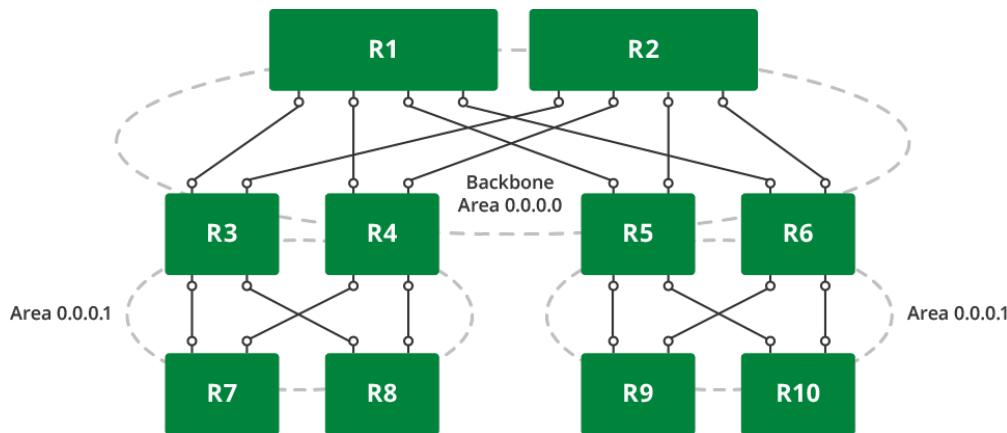
- [Contents \(see page 359\)](#)
- [Scalability and Areas \(see page 359\)](#)
- [Configuring OSPFv2 \(see page 360\)
 - Activating the OSPF and Zebra Daemons \(see page 360\)
 - Enabling OSPF \(see page 360\)
 - Defining \(Custom\) OSPF Parameters on the Interfaces \(see page 362\)](#)
- [Scaling Tip: Summarization \(see page 363\)](#)
- [Scaling Tip: Stub Areas \(see page 364\)](#)
- [Configuration Tip: Unnumbered Interfaces \(see page 365\)](#)
- [ECMP \(see page 366\)](#)
- [Topology Changes and OSPF Reconvergence \(see page 366\)
 - Example Configurations \(see page 366\)](#)
- [Debugging OSPF \(see page 367\)](#)
- [Configuration Files \(see page 368\)](#)
- [Supported RFCs \(see page 368\)](#)
- [Useful Links \(see page 369\)](#)

Scalability and Areas

An increase in the number of nodes affects OSPF scalability in the following ways:

- Memory footprint to hold the entire network topology,
- Flooding performance,
- SPF computation efficiency.

The OSPF protocol advocates hierarchy as a *divide and conquer* approach to achieve high scale. The topology may be divided into areas, resulting in a two-level hierarchy. Area 0 (or 0.0.0.0), called the backbone area, is the top level of the hierarchy. Packets traveling from one non-zero area to another must go via the backbone area. As an example, the leaf-spine topology we have been referring to in the routing section can be divided into areas as follows:



Here are some points to note about areas and OSPF behavior:

- Routers that have links to multiple areas are called *area border routers* (ABR). For example, routers R3, R4, R5, R6 are ABRs in the diagram. An ABR performs a set of specialized tasks, such as SPF computation per area and summarization of routes across areas.
- Most of the LSAs have an area-level flooding scope. These include router LSA, network LSA, and summary LSA.



In the diagram, we reused the same non-zero area address. This is fine since the area address is only a scoping parameter provided to all routers within that area. It has no meaning outside the area. Thus, in the cases where ABRs do not connect to multiple non-zero areas, the same area address can be used, thus reducing the operational headache of coming up with area addresses.

Configuring OSPFv2

Configuring OSPF involves the following tasks:

- Activating the OSPF daemon
- Enabling OSPF
- Defining (Custom) OSPF parameters on the interfaces

Activating the OSPF and Zebra Daemons

1. Activate the following daemons in `/etc/quagga/daemons`, by setting them to `yes`:

```
zebra=yes
ospfd=yes
```

2. Restart the `quagga` service to start the new daemons:

```
cumulus@switch:~$ sudo service quagga restart
```

Enabling OSPF

As we discussed in [Introduction to Routing Protocols](#) (see page 340), there are three steps to the configuration:

1. Identifying the router with the router ID.

2. With whom should the router communicate?
3. What information (most notably the prefix reachability) to advertise?

There are two ways to achieve (2) and (3) in the Quagga OSPF:

1. The `network` statement under `router ospf` does both. The statement is specified with an IP subnet prefix and an area address. All the interfaces on the router whose IP address matches the `network` subnet are put into the specified area. OSPF process starts bringing up peering adjacency on those interfaces. It also advertises the interface IP addresses formatted into LSAs (of various types) to the neighbors for proper reachability.

From the Cumulus Linux shell:

```
cumulus@switch:~$ sudo vtysh

Hello, this is Quagga (version 0.99.21).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

R3# configure terminal
R3(config)# router ospf
R3(config-router)# router-id 0.0.0.1
R3(config-router)# log-adjacency-changes detail
R3(config-router)# network 10.0.0.0/16 area 0.0.0.0
R3(config-router)# network 192.0.2.0/16 area 0.0.0.1
R3(config-router)#

```

Or through `cl-ospf`, from the Cumulus Linux shell:

```
cumulus@switch:~$ sudo cl-ospf router set id 0.0.0.1
cumulus@switch:~$ sudo cl-ospf router set log-adjacency-changes detail
cumulus@switch:~$ sudo cl-ospf router set network 10.0.0.0/16 area
0.0.0.0
cumulus@switch:~$ sudo cl-ospf router set network 192.0.2.0/16 area
0.0.0.1

```

The subnets in the `network` subnet can be as coarse as possible to cover the most number of interfaces on the router that should run OSPF.

There may be interfaces where it's undesirable to bring up OSPF adjacency. For example, in a data center topology, the host-facing interfaces need not run OSPF; however the corresponding IP addresses should still be advertised to neighbors. This can be achieved using the `passive-interface` construct.

From the vtysh/quagga CLI:

```
R3# configure terminal
R3(config)# router ospf
R3(config-router)# passive-interface swp10
R3(config-router)# passive-interface swp11
```

Or use the `passive-interface default` command to put all interfaces as passive and selectively remove certain interfaces to bring up protocol adjacency:

```
R3# configure terminal
R3(config)# router ospf
R3(config-router)# passive-interface default
R3(config-router)# no passive-interface swp1
```

2. Explicitly enable OSPF for each interface by configuring it under the interface configuration mode:

```
R3# configure terminal
R3(config)# interface swp1
R3(config-if)# ip ospf area 0.0.0.0
```

If OSPF adjacency bringup is not desired, you should configure the corresponding interfaces as passive as explained above.

This model of configuration is required for unnumbered interfaces as discussed later in this guide.

For achieving step (3) alone, the `quagga` configuration provides another method: *redistribution*. For example:

```
R3# configure terminal
R3(config)# router ospf
R3(config-router)# redistribute connected
```

Redistribution, however, unnecessarily loads the database with type-5 LSAs and should be limited to generating real external prefixes (for example, prefixes learned from BGP). In general, it is a good practice to generate local prefixes using `network` and/or `passive-interface` statements.

Defining (Custom) OSPF Parameters on the Interfaces

1. Network type, such as point-to-point, broadcast.
2. Timer tuning, like hello interval.
3. For unnumbered interfaces (see below), enable OSPF.

Using Quagga's vtysh:

```
R3(config)# interface swp1
R3(config-if)# ospf network point-to-point
R3(config-if)# ospf hello-interval 5
```

Or through cl-ospf, from the Cumulus Linux shell:

```
cumulus@switch:~$ sudo cl-ospf interface swp1 set network point-to-point
cumulus@switch:~$ sudo cl-ospf interface swp1 set hello-interval 5
```

The OSPF configuration is saved in `/etc/quagga/ospfd.conf`.

Scaling Tip: Summarization

By default, an ABR creates a summary (type-3) LSA for each route in an area and advertises it in adjacent areas. Prefix range configuration optimizes this behavior by creating and advertising one summary LSA for multiple routes.

To configure a range:

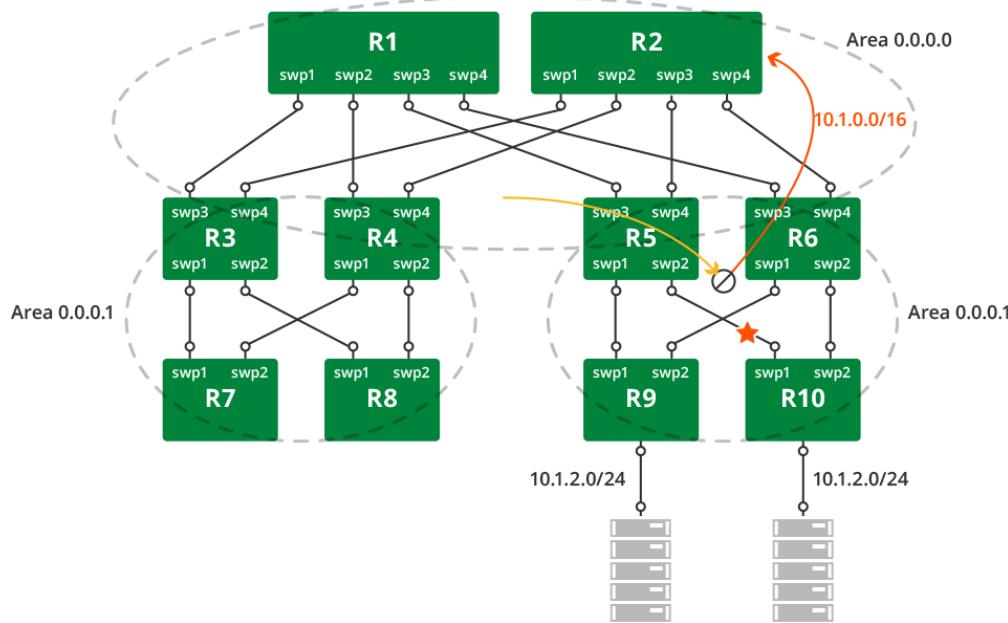
```
R3(config)# router ospf
R3(config-router)# area 0.0.0.1 range 30.0.0.0/8
```



Summarize in the direction to the backbone. The backbone receives summarized routes and injects them to other areas already summarized.



Summarization can cause non-optimal forwarding of packets during failures. Here is an example scenario:



As shown in the diagram, the ABRs in the right non-zero area summarize the host prefixes as 10.1.0.0/16. When the link between R5 and R10 fails, R5 will send a worse metric for the summary route (metric for the summary route is the maximum of the metrics of intra-area routes that are covered by the summary route. Upon failure of the R5-R10 link, the metric for 10.1.2.0/24 goes higher at R5 as the path is R5-R9-R6-R10). As a result, other backbone routers shift traffic destined to 10.1.0.0/16 towards R6. This breaks ECMP and is an under-utilization of network capacity for traffic destined to 10.1.1.0/24.

Scaling Tip: Stub Areas

Nodes in an area receive and store intra-area routing information and summarized information about other areas from the ABRs. In particular, a good summarization practice about inter-area routes through prefix range configuration helps scale the routers and keeps the network stable.

Then there are external routes. External routes are the routes redistributed into OSPF from another protocol. They have an AS-wide flooding scope. In many cases, external link states make up a large percentage of the LSDB.

Stub areas alleviate this scaling problem. A stub area is an area that does not receive external route advertisements.

To configure a stub area:

```
R3(config)# router ospf
R3(config-router)# area 0.0.0.1 stub
```

Stub areas still receive information about networks that belong to other areas of the same OSPF domain. Especially, if summarization is not configured (or is not comprehensive), the information can be overwhelming for the nodes. *Totally stubby areas* address this issue. Routers in totally stubby areas keep in their LSDB information about routing within their area, plus the default route.

To configure a totally stubby area:

```
R3(config)# router ospf
R3(config-router)# area 0.0.0.1 stub no-summary
```

Here is a brief tabular summary of the area type differences:

Type	Behavior
Normal non- zero area	LSA types 1, 2, 3, 4 area-scoped, type 5 externals, inter-area routes summarized
Stub area	LSA types 1, 2, 3, 4 area-scoped, No type 5 externals, inter-area routes summarized
Totally stubby area	LSA types 1, 2 area-scoped, default summary, No type 3, 4, 5 LSA types allowed

Configuration Tip: Unnumbered Interfaces

Unnumbered interfaces are interfaces without unique IP addresses. In OSPFv2, configuring unnumbered interfaces reduces the links between routers into pure topological elements, which dramatically simplifies network configuration and reconfiguration. In addition, the routing database contains only the real networks, so the memory footprint is reduced and SPF is faster.



Unnumbered is usable for point-to-point interfaces only.



If there is a `network <network number>/<mask> area <area ID>` command present in the Quagga configuration, the `ip ospf area <area ID>` command is rejected with the error "Please remove network command first." This prevents you from configuring other areas on some of the unnumbered interfaces. You can use either the `network area` command or the `ospf area` command in the configuration, but not both.



Unless the Ethernet media is intended to be used as a LAN with multiple connected routers, we recommend configuring the interface as point-to-point. It has the additional advantage of a simplified adjacency state machine; there is no need for DR/BDR election and *LSA reflection*. See [RFC5309](#) for a more detailed discussion.

To configure an unnumbered interface, take the IP address of another interface (called the *anchor*) and use that as the IP address of the unnumbered interface:

```
auto lo
iface lo inet loopback
    address 192.0.2.1/24
```

```

auto swp1
iface swp1
  address 192.0.2.1/24

auto swp2
iface swp2
  address 192.0.2.1/24
  
```

To enable OSPF on an unnumbered interface from within Quagga's vtysh:

```

R3(config)# interface swp1
R3(config-if)# ip ospf area 0.0.0.1
  
```

ECMP

During SPF computation for an area, if OSPF finds multiple paths with equal cost (metric), all those paths are used for forwarding. For example, in the reference topology diagram, R8 uses both R3 and R4 as next hops to reach a destination attached to R9.

Topology Changes and OSPF Reconvergence

Topology changes usually occur due to one of four events:

1. Maintenance of a router node
2. Maintenance of a link
3. Failure of a router node
4. Failure of a link

For the maintenance events, operators typically raise the OSPF administrative weight of the link(s) to ensure that all traffic is diverted from the link or the node (referred to as *costing out*). The speed of reconvergence does not matter. Indeed, changing the OSPF cost causes LSAs to be reissued, but the links remain in service during the SPF computation process of all routers in the network.

For the failure events, traffic may be lost during reconvergence; that is, until SPF on all nodes computes an alternative path around the failed link or node to each of the destinations. The reconvergence depends on layer 1 failure detection capabilities and at the worst case *DeadInterval* OSPF timer.

Example Configurations

Example configuration for event 1, using vtysh:

```

R3(config)# router ospf
R3(config-router)# max-metric router-lsa administrative
  
```

Or, with the non-modal shell command approach:

```
cumulus@switch:~$ sudo cl-ospf router set max-metric router-lsa
administrative
```

Example configuration for event 2, using vtysh:

```
R3(config)# interface swp1
R3(config-if)# ospf cost 65535
```

Or, with the non-modal shell command approach:

```
cumulus@switch:~$ sudo cl-ospf interface swp1 set cost 65535
```

Debugging OSPF

[OperState](#) lists all the commands to view the operational state of OSPF.

The three most important states while troubleshooting the protocol are:

1. Neighbors, with `show ip ospf neighbor`. This is the starting point to debug neighbor states (also see `tcpdump` below).
2. Database, with `show ip ospf database`. This is the starting point to verify that the LSDB is, in fact, synchronized across all routers in the network. For example, sweeping through the output of `show ip ospf database router` taken from all routers in an area will ensure if the topology graph building process is complete; that is, every node has seen all the other nodes in the area.
3. Routes, with `show ip ospf route`. This is the outcome of SPF computation that gets downloaded to the forwarding table, and is the starting point to debug, for example, why an OSPF route is not being forwarded correctly.



Compare the route output with kernel by using `show ip route | grep zebra` and with the hardware entries using `cl-route-check -V`.

Using `cl-ospf`:

```
cumulus@switch:~$ sudo cl-ospf neighbor show [all | detail]

cumulus@switch:~$ sudo cl-ospf database show [asbr-summary | network |
opaque-area |
opaque-link | summary | external |
nssa-external | opaque-as | router]
```

```
cumulus@switch:~$ sudo cl-ospf route show
```

Debugging-OSPF lists all of the OSPF debug options.

Using cl-ospf:

```
Usage: cl-ospf debug { COMMAND | help }

COMMANDS
  { set | clear } (all | event | ism | ism [OBJECT] | lsa | lsa
  [OBJECT] |
    nsm | nsm [OBJECT] | nssa | packet | packet [OBJECT] |
    zebra [OBJECT] | zebra all)
```

Using zebra under vtysh:

```
cumulus@switch:~$ sudo vtysh
R3# show [zebra]

IOBJECT := { events | status | timers }
OOBJECT := { interface | redistribute }
POBJECT := { all | dd | hello | ls-ack | ls-request | ls-update }
ZOBJECT := { all | events | kernel | packet | rib |
```

Using tcpdump to capture OSPF packets:

```
cumulus@switch:~$ sudo tcpdump -v -i swp1 ip proto ospf
```

Configuration Files

- /etc/quagga/daemons
- /etc/quagga/ospfd.conf

Supported RFCs

- RFC2328
- RFC3137
- RFC5309

Useful Links

- Bidirectional forwarding detection (see page 394) (BFD) and OSPF
- http://en.wikipedia.org/wiki/Open_Shortest_Path_First
- <http://www.nongnu.org/quagga/docs/docs-info.html#OSPFv2>
- Perlman, Radia (1999). Interconnections: Bridges, Routers, Switches, and Internetworking Protocols (2 ed.). Addison-Wesley.
- Moy, John T. OSPF: Anatomy of an Internet Routing Protocol. Addison-Wesley.

Open Shortest Path First v3 - OSPFv3 - Protocol

OSPFv3 is a revised version of OSPFv2 to support the IPv6 address family. Refer to [Open Shortest Path First \(OSPF\) Protocol \(see page 358\)](#) for a discussion on the basic concepts, which remain the same between the two versions.

OSPFv3 has changed the formatting in some of the packets and LSAs either as a necessity to support IPv6 or to improve the protocol behavior based on OSPFv2 experience. Most notably, v3 defines a new LSA, called intra-area prefix LSA to separate out the advertisement of stub networks attached to a router from the router LSA. It is a clear separation of node topology from prefix reachability and lends itself well to an optimized SPF computation.



IETF has defined extensions to OSPFv3 to support multiple address families (that is, both IPv6 and IPv4). Quagga (see page 344) does not support it yet.

Contents

(Click to expand)

- [Contents \(see page 369\)](#)
- [Configuring OSPFv3 \(see page 369\)](#)
- [Unnumbered Interfaces \(see page 371\)](#)
- [Debugging OSPF \(see page 371\)](#)
- [Configuration Files \(see page 371\)](#)
- [Supported RFCs \(see page 371\)](#)
- [Useful Links \(see page 371\)](#)

Configuring OSPFv3

Configuring OSPFv3 involves the following tasks:

1. Activating the OSPF6 and Zebra daemons:
 - a. Add the following to `/etc/quagga/daemons`:
`zebra=yes`
`ospf6d=yes`
 - b. Restart the `quagga` service to start the new daemons:

```
cumulus@switch:~$ sudo service quagga restart
```

2. Enabling OSPF6 and map interfaces to areas. From Quagga's vtysh shell:

```
cumulus@switch:~$ sudo vtysh

Hello, this is Quagga (version 0.99.21).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

R3# conf t
R3# configure terminal
R3(config)# router ospf6
R3(config-router)# router-id 0.0.1
R3(config-router)# log-adjacency-changes detail
R3(config-router)# interface swp1 area 0.0.0.0
R3(config-router)# interface swp2 area 0.0.0.1
R3(config-router)#

```

Or through cl-ospf6, from the Cumulus Linux shell:

```
cumulus@switch:~$ sudo cl-ospf6 router set id 0.0.0.1
cumulus@switch:~$ sudo cl-ospf6 router set log-adjacency-changes detail
cumulus@switch:~$ sudo cl-ospf6 interface swp1 set area 0.0.0.0
cumulus@switch:~$ sudo cl-ospf6 interface swp2 set area 0.0.0.1
```

3. Defining (custom) OSPF6 parameters on the interfaces:

- a. Network type (such as point-to-point, broadcast)
- b. Timer tuning (for example, hello interval)

Using Quagga's vtysh:

```
R3(config)# interface swp1
R3(config-if)# ipv6 ospf6 network point-to-point
R3(config-if)# ipv6 ospf6 hello-interval 5
```

Or through cl-ospf6, from the Cumulus Linux shell:

```
cumulus@switch:~$ sudo cl-ospf6 interface swp1 set network point-to-point
cumulus@switch:~$ sudo cl-ospf6 interface swp1 set hello-interval 5
```

The OSPFv3 configuration is saved in `/etc/quagga/ospf6d.conf`.

Unnumbered Interfaces

Unlike OSPFv2, OSPFv3 intrinsically supports unnumbered interfaces. Forwarding to the next hop router is done entirely using IPv6 link local addresses. Therefore, you are not required to configure any global IPv6 address to interfaces between routers.

Debugging OSPF

See [Debugging OSPF \(see page 367\)](#) for OSPFv2 for the troubleshooting discussion. The equivalent commands are:

```
cumulus@switch:~$ sudo vtysh
R3# show ipv6 ospf6 neighbor
R3# show ipv6 ospf6 database [detail | dump | internal |
                                as-external | group-membership |
                                inter-prefix | inter-router |
                                intra-prefix | link | network |
                                router | type-7 | * | adv-router |
                                linkstate-id | self-originated]
R3# show ip ospf route
```

Another helpful command is `show ipv6 ospf6 [area <id>] spf tree`. It dumps the node topology as computed by SPF to help visualize the network view.

Configuration Files

- `/etc/quagga/daemons`
- `/etc/quagga/ospf6d.conf`

Supported RFCs

- RFC5340
- RFC3137

Useful Links

- Bidirectional forwarding detection ([see page 394](#)) (BFD) and OSPF

- http://en.wikipedia.org/wiki/Open_Shortest_Path_First
- <http://www.nongnu.org/quagga/docs/docs-info.html#OSPFv3>

Configuring Border Gateway Protocol - BGP

BGP is the routing protocol that runs the Internet. It is an increasingly popular protocol for use in the data center as it lends itself well to the rich interconnections in a Clos topology. Specifically:

- It does not require routing state to be periodically refreshed unlike OSPF.
- It is less chatty than its link-state siblings. For example, a link or node transition can result in a bestpath change, causing BGP to send updates.
- It is multi-protocol and extensible.
- There are many robust vendor implementations.
- The protocol is very mature and comes with many years of operational experience.

This IETF draft provides further details of the use of BGP within the data center.

Contents

(Click to expand)

- Contents (see page 372)
- Commands (see page 373)
- Autonomous System Number (ASN) (see page 373)
- eBGP and iBGP (see page 374)
- Route Reflectors (see page 374)
- ECMP with BGP (see page 374)
 - Maximum Paths (see page 374)
 - Multipath Relax (see page 375)
- BGP for both IPv4 and IPv6 (see page 375)
- Configuring BGP (see page 375)
- Using BGP Unnumbered Interfaces (see page 377)
 - BGP and Extended Next-hop Encoding (see page 378)
 - Configuring BGP Unnumbered Interfaces (see page 378)
 - Managing Unnumbered Interfaces (see page 378)
 - How traceroute Interacts with BGP Unnumbered Interfaces (see page 380)
 - Advanced: Understanding How Next-hop Fields Are Set (see page 380)
 - Limitations (see page 382)
- Fast Convergence Design Considerations (see page 382)
 - Specifying the Interface Name in the neighbor Command (see page 382)
- Configuring BGP Peering Relationships across Switches (see page 383)
- Configuration Tips (see page 384)
 - Using peer-group to Simplify Configuration (see page 384)

- Preserving the AS_PATH Setting (see page 385)
- Utilizing Multiple Routing Tables and Forwarding (see page 385)
- Troubleshooting (see page 385)
 - Debugging Tip: Logging Neighbor State Changes (see page 388)
 - Troubleshooting Link-local Addresses (see page 388)
- Enabling Read-only Mode (see page 389)
- Applying a Route Map for Route Updates (see page 390)
- Protocol Tuning (see page 390)
 - Converging Quickly On Link Failures (see page 390)
 - Converging Quickly On Soft Failures (see page 391)
 - Reconnecting Quickly (see page 392)
 - Advertisement Interval (see page 392)
- Configuration Files (see page 393)
- Useful Links (see page 393)
- Caveats and Errata (see page 393)
 - ttl-security Issue (see page 393)

Commands

Cumulus Linux:

- bgp
- vtysh

Quagga:

- bgp
- neighbor
- router
- show

Autonomous System Number (ASN)

One of the key concepts in BGP is an *autonomous system number* or ASN. An *autonomous system* is defined as a set of routers under a common administration. Since BGP was originally designed to peer between independently managed enterprises and/or service providers, each such enterprise is treated as an autonomous system, responsible for a set of network addresses. Each such autonomous system is given a unique number called its ASN. ASNs are handed out by a central authority (ICANN). However, ASNs between 64512 and 65535 are reserved for private use. Using BGP within the data center relies on either using this number space or else using the single ASN you own.

The ASN is central to how BGP builds a forwarding topology. A BGP route advertisement carries with it not only the originator's ASN, but also the list of ASNs that this route advertisement has passed through. When forwarding a route advertisement, a BGP speaker adds itself to this list. This list of ASNs is called the *AS path*. BGP uses the AS path to detect and avoid loops.

ASNs were originally 16-bit numbers, but were later modified to be 32-bit. Quagga supports both 16-bit and 32-bit ASNs, but most implementations still run with 16-bit ASNs.

eBGP and iBGP

When BGP is used to peer between autonomous systems, the peering is referred to as *external BGP* or eBGP. When BGP is used within an autonomous system, the peering used is referred to as *internal BGP* or iBGP. eBGP peers have different ASNs while iBGP peers have the same ASN.

While the heart of the protocol is the same when used as eBGP or iBGP, there is a key difference in the protocol behavior between use as eBGP and iBGP: an iBGP node does not forward routing information learned from one iBGP peer to another iBGP peer. It expects the originating iBGP peer to send this information to all iBGP peers.

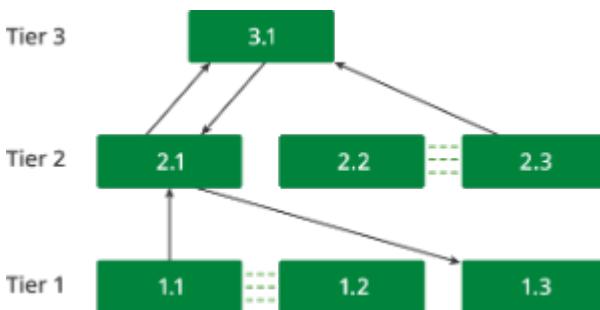
This implies that iBGP peers are all connected to each other. In a large network, this requirement can quickly become unscalable. The most popular method to avoid this problem is to introduce a *route reflector*.

Route Reflectors

Route reflectors are quite easy to understand in a Clos topology. In a two-tier Clos network, the leaf (or tier 1) switches are the only ones connected to end stations. Subsequently, this means that the spines themselves do not have any routes to announce. They're merely **reflecting** the routes announced by one leaf to the other leaves. Thus, the spine switches function as route reflectors while the leaf switches serve as route reflector clients.

In a three-tier network, the tier 2 nodes (or mid-tier spines) act as both route reflector servers and route reflector clients. They act as route reflectors because they announce the routes learned from the tier 1 nodes to other tier 1 nodes and to tier 3 nodes. They also act as route reflector clients to the tier 3 nodes, receiving routes learned from other tier 2 nodes. Tier 3 nodes act only as route reflectors.

In the following illustration, tier 2 node 2.1 is acting as a route reflector server, announcing the routes between tier 1 nodes 1.1 and 1.2 to tier 1 node 1.3. It is also a route reflector client, learning the routes between tier 2 nodes 2.2 and 2.3 from the tier 3 node, 3.1.



ECMP with BGP

If a BGP node hears a prefix **p** from multiple peers, it has all the information necessary to program the routing table to forward traffic for that prefix **p** through all of these peers. Thus, BGP supports equal-cost multipathing.

In order to perform ECMP in BGP, you may need to configure two parameters: *maximum paths* and, if you're using eBGP, *multipath relax*.

Maximum Paths

BGP does not install multiple routes by default. To do so, use the `maximum-paths` command. Or, if you're using iBGP, use the `maximum-paths ibgp` command as shown below.

```

leaf1# conf t
leaf1(config)# router bgp 65000
leaf1(config-router)# maximum-paths
  <1-255> Number of paths
    ibgp    iBGP-multipath
leaf1(config-router)# maximum-paths ibgp
  <1-255> Number of paths

```

Multipath Relax

If your data center uses eBGP, you need to configure an additional parameter for proper ECMP: the `bestpath as-path multipath-relax no-as-set` command. You configure it under the BGP routing process.

```

leaf1# conf t
leaf1(config)# router bgp 65000
leaf1(config-router)# bgp bestpath
as-path          compare-routerid med
leaf1(config-router)# bgp bestpath as-path
confed          ignore      multipath-relax
leaf1(config-router)# bgp bestpath as-path multipath-relax
<cr>
no-as-set  Do not generate an AS_SET
leaf1(config-router)# bgp bestpath as-path multipath-relax no-as-set

```

For more information on the `no-as-set` option, read [the AS_PATH section below \(see page 385\)](#).

BGP for both IPv4 and IPv6

Unlike OSPF, which has separate versions of the protocol to announce IPv4 and IPv6 routes, BGP is a multi-protocol routing engine, capable of announcing both IPv4 and IPv6 prefixes. It supports announcing IPv4 prefixes over an IPv4 session and IPv6 prefixes over an IPv6 session. It also supports announcing prefixes of both these address families over a single IPv4 session or over a single IPv6 session.

Configuring BGP

1. Activate the BGP and Zebra daemons:

- Add the following line to `/etc/quagga/daemons`:

```

zebra=yes
bgpd = yes

```

- Touch an empty `bgpd` configuration file:

```
cumulus@switch:~$ sudo touch /etc/quagga/bgpd.conf
```

A slightly more useful configuration file would contain the following lines:

```
hostname R7
password *****
enable password *****
log timestamp precision 6
log file /var/log/quagga/bgpd.log
!
line vty
  exec-timeout 0 0
!
```

The most important information here is the specification of the location of the log file, where the BGP process can log debugging and other useful information. A common convention is to store the log files under `/var/log/quagga`.

You must restart `quagga` when a new daemon is enabled:

```
cumulus@switch:~$ sudo service quagga restart
```

2. Identify the BGP node by assigning an ASN and `router-id`:

```
cumulus@switch:~$ sudo vtysh

Hello, this is Quagga (version 0.99.21).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

R7# configure terminal
R7(config)# router bgp 65000
R7(config-router)# bgp router-id 0.0.0.1
```

3. Specify to whom it must disseminate routing information:

```
R7(config-router)# neighbor 10.0.0.2 remote-as 65001
```

If it is an iBGP session, the `remote-as` is the same as the local AS:

```
R7(config-router)# neighbor 10.0.0.2 remote-as 65000
```

Specifying the peer's IP address allows BGP to set up a TCP socket with this peer, but it doesn't distribute any prefixes to it, unless it is explicitly told that it must via the `activate` command:

```
R7(config-router)# address-family ipv4 unicast
R7(config-router-af)# neighbor 10.0.0.2 activate
R7(config-router-af)# exit
R7(config-router)# address-family ipv6
R7(config-router-af)# neighbor 2002:0a00:0002::0a00:0002 activate
R7(config-router-af)# exit
```

As you can see, `activate` has to be specified for each address family that is being announced by the BGP session.

4. Specify some properties of the BGP session:

```
R7(config-router)# neighbor 10.0.0.2 next-hop-self
R7(config-router)# address-family ipv4 unicast
R7(config-router-af)# maximum-paths 64
```

For iBGP, the `maximum-paths` is selected by typing:

```
R7(config-router-af)# maximum-paths ibgp 64
```

If this is a route-reflector client, it can be specified as follows:

```
R3(config-router-af)# neighbor 10.0.0.1 route-reflector-client
```



It is node R3, the route reflector, on which the peer is specified as a client.

5. Specify what prefixes to originate:

```
R7(config-router)# address-family ipv4 unicast
R7(config-router-af)# network 192.0.2.0/24
R7(config-router-af)# network 203.0.113.1/24
```

Using BGP Unnumbered Interfaces

Unnumbered interfaces are interfaces without unique IP addresses. In BGP, you configure unnumbered interfaces using *extended next-hop encoding* (ENHE), which is defined by [RFC 5549](#). BGP unnumbered interfaces provide a means of advertising an IPv4 route with an IPv6 next-hop. Prior to RFC 5549, an IPv4 route could be advertised only with an IPv4 next-hop.

BGP unnumbered interfaces are particularly useful in deployments where IPv4 prefixes are advertised through BGP over a section without any IPv4 address configuration on links. As a result, the routing entries are also IPv4 for destination lookup and have IPv6 next-hops for forwarding purposes.

BGP and Extended Next-hop Encoding

Once enabled and active, BGP makes use of the available IPv6 next-hops for advertising any IPv4 prefixes. BGP learns the prefixes, calculates the routes and installs them in IPv4 AFI to IPv6 AFI format. However, ENHE in Cumulus Linux does not install routes into the kernel in IPv4 prefix to IPv6 next-hop format. For link-local peerings enabled by dynamically learning the other end's link-local address using IPv6 neighbor discovery router advertisements, an IPv6 next-hop is converted into an IPv4 link-local address and a static neighbor entry is installed for this IPv4 link-local address with the MAC address derived from the link-local address of the other end.



It is assumed that the IPv6 implementation on the peering device will use the MAC address as the interface ID when assigning the IPv6 link-local address, as suggested by RFC 4291.

Configuring BGP Unnumbered Interfaces

Configuring a BGP unnumbered interface requires enabling IPv6 neighbor discovery router advertisements. The `interval` you specify is measured in seconds, and defaults to 600 seconds. Extended next-hop encoding is sent only for the link-local address peerings:

```
interface swp1
  no ipv6 nd suppress-ra
  ipv6 nd ra-interval 5
!
router bgp 10
  neighbor swp1 interface
  neighbor swp1 remote-as 20
  neighbor swp1 capability extended-nexthop
!
```

Managing Unnumbered Interfaces

All the relevant BGP commands are now capable of showing IPv6 next-hops and/or the interface name for any IPv4 prefix:

```
# show ip bgp
BGP table version is 66, local router ID is 6.0.0.5
```

```

Status codes: s suppressed, d damped, h history, * valid, > best, =
multipath,
                i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop            Metric LocPrf Weight Path
*-> 6.0.0.5/32      0.0.0.0                  0        32768 ?
*= 6.0.0.6/32       swp2                   0  65534 64503 ?
*=                      swp6                   0  65002 64503 ?
*=                      swp5                   0  65001 64503 ?
*=                      swp1                   0  65534 64503 ?
*=                      swp4                   0  65534 64503 ?
*>                     swp3                   0  65534 64503 ?

# show ip bgp 6.0.0.14/32
BGP routing table entry for 6.0.0.14/32
Paths: (1 available, best #1, table Default-IP-Routing-Table)
      Advertised to non peer-group peers:
      swp1 swp2 swp3 swp4 swp5 swp6
      65534
      fe80::202:ff:fe00:3d from swp2 (6.0.0.14)
      (fe80::202:ff:fe00:3d) (used)
      Origin incomplete, metric 0, localpref 100, valid, external, best
      Last update: Tue May 12 17:18:41 2015

```

Quagga RIB commands are also modified:

```

# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel, T - Table,
       > - selected route, * - FIB route
K>* 0.0.0.0/0 via 192.168.0.2, eth0
C>* 6.0.0.5/32 is directly connected, lo
B>* 6.0.0.6/32 [20/0] via fe80::202:ff:fe00:45, swp3, 00:46:12
  *           via fe80::202:ff:fe00:35, swp1, 00:46:12
  *           via fe80::202:ff:fe00:3d, swp2, 00:46:12
  *           via fe80::202:ff:fe00:4d, swp4, 00:46:12
  *           via fe80::202:ff:fe00:55, swp5, 00:46:12
  *           via fe80::202:ff:fe00:5a, swp6, 00:46:12

```

The following commands show how the IPv4 link-local address 169.254.0.1 is used to install the route and static neighbor entry to facilitate proper forwarding without having to install an IPv4 prefix with IPv6 next-hop in the kernel:

```
# ip route show 6.0.0.6
6.0.0.6 proto zebra metric 20
  nexthop via 169.254.0.1 dev swp3 weight 1 onlink
  nexthop via 169.254.0.1 dev swp1 weight 1 onlink
  nexthop via 169.254.0.1 dev swp2 weight 1 onlink
  nexthop via 169.254.0.1 dev swp4 weight 1 onlink
  nexthop via 169.254.0.1 dev swp5 weight 1 onlink
  nexthop via 169.254.0.1 dev swp6 weight 1 onlink

# ip neigh
fe80::202:ff:fe00:35 dev swp1 lladdr 00:02:00:00:00:35 router REACHABLE
fe80::202:ff:fe00:5a dev swp6 lladdr 00:02:00:00:00:5a router REACHABLE
fe80::202:ff:fe00:3d dev swp2 lladdr 00:02:00:00:00:3d router REACHABLE
fe80::202:ff:fe00:55 dev swp5 lladdr 00:02:00:00:00:55 router REACHABLE
fe80::202:ff:fe00:45 dev swp3 lladdr 00:02:00:00:00:45 router REACHABLE
fe80::202:ff:fe00:4d dev swp4 lladdr 00:02:00:00:00:4d router REACHABLE
169.254.0.1 dev swp5 lladdr 00:02:00:00:00:55 PERMANENT
192.168.0.2 dev eth0 lladdr 52:55:c0:a8:00:02 REACHABLE
169.254.0.1 dev swp3 lladdr 00:02:00:00:00:45 PERMANENT
169.254.0.1 dev swp1 lladdr 00:02:00:00:00:35 PERMANENT
169.254.0.1 dev swp4 lladdr 00:02:00:00:00:4d PERMANENT
169.254.0.1 dev swp6 lladdr 00:02:00:00:00:5a PERMANENT
169.254.0.1 dev swp2 lladdr 00:02:00:00:00:3d PERMANENT
```

How traceroute Interacts with BGP Unnumbered Interfaces

Every router or end host must have an IPv4 address in order to complete a traceroute of IPv4 addresses. In this case, the IPv4 address used is that of the loopback device.

Even if ENHE is not used in the data center, link addresses are not typically advertised. This is because:

- Link addresses take up valuable FIB resources. In a large Clos environment, the number of such addresses can be quite large.
- Link addresses expose an additional attack vector for intruders to use to either break in or engage in DDOS attacks.

Therefore, assigning an IP address to the loopback device is essential.

Advanced: Understanding How Next-hop Fields Are Set

This section describes how the IPv6 next-hops are set in the MP_REACH_NLRI ([multiprotocol reachable NLRI](#)) initiated by the system, which applies whether IPv6 prefixes or IPv4 prefixes are exchanged with ENHE. There are two main aspects to determine — how many IPv6 next-hops are included in the MP_REACH_NLRI (since the RFC allows either one or two next-hops) and the values of the next-hop(s). This section also describes how a received MP_REACH_NLRI is handled as far as processing IPv6 next-hops.

- Whether peering to a global IPv6 address or link-local IPv6 address, the determination whether to send one or two next-hops is as follows:

1. If reflecting the route, two next-hops are sent only if the peer has `nexthop-local unchanged` configured and the attribute of the received route has an IPv6 link-local next-hop; otherwise, only one next-hop is sent.
 2. Otherwise (if it's not reflecting the route), two next-hops are sent if explicitly configured (`nexthop-local unchanged`) or the peer is directly connected (that is, either peering is on link-local address or the global IPv4 or IPv6 address is *directly connected*) and the route is either a local/self-originated route or the peer is an eBGP peer.
 3. In all other cases, only one next-hop gets sent, unless an outbound route map adds another next-hop.
- `route-map` can impose two next-hops in scenarios where Cumulus Linux would only send one next-hop — by specifying `set ipv6 nexthop link-local`.
 - For all routes to eBGP peers and self-originated routes to iBGP peers, the global next-hop (first value) is the peering address of the local system. If the peering is on the link-local address, this is the global IPv6 address on the peering interface, if present; otherwise, it is the link-local IPv6 address on the peering interface.
 - For other routes to iBGP peers (eBGP to iBGP or reflected), the global next-hop will be the global next-hop in the received attribute.



If this address were a link-local IPv6 address, it would get reset so that the link-local IPv6 address of the eBGP peer is not passed along to an iBGP peer, which most likely may be on a different link.

- `route-map` and/or the peer configuration can change the above behavior. For example, `route-map` can set the global IPv6 next-hop or the peer configuration can set it to `self` — which is relevant for *iBGP* peers. The route map or peer configuration can also set the next-hop to `unchanged`, which ensures the source IPv6 global next-hop is passed around — which is relevant for *eBGP* peers.
- Whenever two next-hops are being sent, the link-local next-hop (the second value of the two) is the link-local IPv6 address on the peering interface unless it is due to `nh-local-unchanged` or `route-map` has set the link-local next-hop.
- Network administrators cannot set **martian values** for IPv6 next-hops in `route-map`. Also, global and link-local next-hops are validated to ensure they match the respective address types.
- In a received update, a martian check is imposed for the IPv6 global next-hop. If the check fails, it gets treated as an implicit withdraw.
- If two next-hops are received in an update and the second next-hop is not a link-local address, it gets ignored and the update is treated as if only one next-hop was received.
- Whenever two next-hops are received in an update, the second next-hop is used to install the route into `zebra`. As per the previous point, it is already assured that this is a link-local IPv6 address. Currently, this is assumed to be reachable and is not registered with NHT.
- When `route-map` specifies the next-hop as `peer-address`, the global IPv6 next-hop as well as the link-local IPv6 next-hop (if it's being sent) is set to the *peering address*. If the peering is on a link-local address, the former could be the link-local address on the peering interface, unless there is a global IPv6 address present on this interface.

The above rules imply that there are scenarios where a generated update has two IPv6 next-hops, and both of them are the IPv6 link-local address of the peering interface on the local system. If you are peering with a switch or router that is not running Cumulus Linux and expects the first next-hop to be a global IPv6 address, a route map can be used on the sender to specify a global IPv6 address. This conforms with the recommendations in the Internet draft [draft-kato-bgp-ipv6-link-local-00.txt](#), "BGP4+ Peering Using IPv6 Link-local Address".

Limitations

- Interface-based peering with separate IPv4 and IPv6 sessions is not supported.
- ENHE is sent for IPv6 link-local peerings only.
- If a IPv4 /30 or /31 IP address is assigned to the interface IPv4 peering will be used over IPv6 link-local peering.

Fast Convergence Design Considerations

Without getting into the why (see the IETF draft cited in Useful Links below that talks about BGP use within the data center), we strongly recommend the following use of addresses in the design of a BGP-based data center network:

- Use of interface addresses: Set up BGP sessions only using interface-scoped addresses. This allows BGP to react quickly to link failures.
- Use of next-hop-self: Every BGP node says that it knows how to forward traffic to the prefixes it is announcing. This reduces the requirement to announce interface-specific addresses and thereby reduces the size of the forwarding table.

Specifying the Interface Name in the neighbor Command

When you are configuring BGP for the neighbors of a given interface, you can specify the interface name instead of its IP address. All the other `neighbor` command options remain the same.

This is equivalent to BGP peering to the link-local IPv6 address of the neighbor on the given interface. The link-local address is learned via IPv6 neighbor discovery router advertisements.

Consider the following example configuration:

```
router bgp 65000
  bgp router-id 0.0.0.1
  neighbor swp1 interface
  neighbor swp1 remote-as 65000
  neighbor swp1 next-hop-self
!
  address-family ipv6
  neighbor swp1 activate
  exit-address-family
```



Make sure that IPv6 neighbor discovery router advertisements are supported and not suppressed. In Quagga, you do this by checking the running configuration. Under the interface configuration, use `no ipv6 nd suppress-ra` to remove router suppression.

Cumulus Networks recommends you adjust the router advertisement's interval to a shorter value (`ipv6 nd ra-interval <interval>`) to address scenarios when nodes come up and miss router advertisement processing to relay the neighbor's link-local address to BGP. The `interval` is measured in seconds and defaults to 600 seconds.

Configuring BGP Peering Relationships across Switches

A BGP peering relationship is typically initiated with the `neighbor x.x.x.x remote-as <AS number>` command. In order to simplify configuration across multiple switches, you can specify the *internal* or *external* keyword to the configuration instead of the AS number.

Specifying *internal* signifies an iBGP peering; that is, the neighbor will only create or accept a connection with the specified neighbor if the remote peer AS number matches this BGP's AS number.

Specifying *external* signifies an eBGP peering; that is, the neighbor will only create a connection with the neighbor if the remote peer AS number does **not** match this BGP AS number.

You can make this distinction using the `neighbor` command or the `peer-group` command.

In general, use the following syntax with the `neighbor` command:

```
neighbor (ipv4 addr|ipv6 addr|WORD) remote-as (<1-
4294967295>|internal|external)
```

Some example configurations follow.

To connect to **the same AS** using the `neighbor` command, modify your configuration similar to the following:

```
router bgp 500
neighbor 192.168.1.2 remote-as internal
```

To connect to a **different AS** using the `neighbor` command, modify your configuration similar to the following:

```
router bgp 500
neighbor 192.168.1.2 remote-as external
```

To connect to **the same AS** using the `peer-group` command, modify your configuration similar to the following:

```
router bgp 500
neighbor swp1 interface
neighbor IBGP peer-group
neighbor IBGP remote-as internal
neighbor swp1 peer-group IBGP
neighbor 6.0.0.3 peer-group IBGP
neighbor 6.0.0.4 peer-group IBGP
```

To connect to a **different AS** using the `peer-group` command, modify your configuration similar to the following:

```
router bgp 500
neighbor swp2 interface
neighbor EBGP peer-group
neighbor EBGP remote-as external
neighbor 6.0.0.2 peer-group EBGP
neighbor swp2 peer-group EBGP
neighbor 6.0.0.4 peer-group EBGP
```

Configuration Tips

Using `peer-group` to Simplify Configuration

When there are many peers to connect to, the amount of redundant configuration becomes overwhelming. For example, repeating the `activate` and `next-hop-self` commands for even 60 neighbors makes for a very long configuration file. Using `peer-group` addresses this problem.

Instead of specifying properties of each individual peer, Quagga allows for defining one or more peer-groups and associating all the attributes common to that peer session to a peer-group.

After doing this, the only task is to associate an IP address with a peer-group. Here is an example of defining and using peer-groups:

```
R7(config-router)# neighbor tier-2 peer-group
R7(config-router)# neighbor tier-2 remote-as 65000
R7(config-router)# address-family ipv4 unicast
R7(config-router-af)# neighbor tier-2 activate
R7(config-router-af)# neighbor tier-2 next-hop-self
R7(config-router-af)# maximum-paths ibgp 64
R7(config-router-af)# exit
R7(config-router)# neighbor 10.0.0.2 peer-group tier-2
R7(config-router)# neighbor 192.0.2.2 peer-group tier-2
```

If you're using eBGP, besides specifying the neighbor's IP address, you also have to specify the neighbor's ASN, since it is different for each neighbor. In such a case, you wouldn't specify the `remote-as` for the peer-group.

Preserving the AS_PATH Setting

If you plan to use multipathing with the `multipath-relax` option, Quagga generates an AS_SET in place of the current AS_PATH for the bestpath. This helps to prevent loops but is unusual behavior. To preserve the AS_PATH setting, use the `no-as-set` option when configuring bestpath:

```
R7(config-router)# bgp bestpath as-path multipath-relax no-as-set
```

Utilizing Multiple Routing Tables and Forwarding

You can run multiple routing tables (one for in-band/data plane traffic and one for out-of-band/management plane traffic) on the same switch using [management VRF \(see page 408\)](#) (multiple routing tables and forwarding).

Troubleshooting

The most common starting point for troubleshooting BGP is to view the summary of neighbors connected to and some information about these connections. A sample output of this command is as follows:

```
R7# show ip bgp summary
BGP router identifier 0.0.0.9, local AS number 65000
RIB entries 7, using 672 bytes of memory
Peers 2, using 9120 bytes of memory

Neighbor          V     AS MsgRcvd MsgSent      TblVer  InQ OutQ Up/Down  State
/PfxRcd
10.0.0.2          4   65000      11       10          0     0     0 00:06:38      3
192.0.2.2          4   65000      11       10          0     0     0 00:06:38      3

Total number of neighbors 2
```

(Pop quiz: Are these iBGP or eBGP sessions? Hint: Look at the ASNs.)

It is also useful to view the routing table as defined by BGP:

```
R7# show ip bgp
BGP table version is 0, local router ID is 0.0.0.9
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
r RIB-failure, S Stale, R Removed
```

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 192.0.2.29/24	0.0.0.0	0		32768	i
*>i192.0.2.30/24	10.0.0.2	0	100	0	i
* i	192.0.2.2	0	100	0	i
*>i192.0.2.31/24	10.0.0.2	0	100	0	i
* i	192.0.2.2	0	100	0	i
*>i192.0.2.32/24	10.0.0.2	0	100	0	i
* i	192.0.2.2	0	100	0	i

Total number of prefixes 4

A more detailed breakdown of a specific neighbor can be obtained using `show ip bgp neighbor <neighbor ip address>`:

```
R7# show ip bgp neighbor 10.0.0.2
BGP neighbor is 10.0.0.2, remote AS 65000, local AS 65000, internal link
BGP version 4, remote router ID 0.0.0.5
BGP state = Established, up for 00:14:03
Last read 14:52:31, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
  4 Byte AS: advertised and received
  Route refresh: advertised and received(old & new)
  Address family IPv4 Unicast: advertised and received
Message statistics:
  Inq depth is 0
  Outq depth is 0
      Sent          Rcvd
Opens:           1            1
Notifications:   0            0
Updates:         1            3
Keepalives:     16           15
Route Refresh:  0            0
Capability:     0            0
Total:          18           19
Minimum time between advertisement runs is 5 seconds
```

For address family: IPv4 Unicast
 NEXT_HOP is always this router
 Community attribute sent to this neighbor(both)
 3 accepted prefixes

```

Connections established 1; dropped 0
Last reset never
Local host: 10.0.0.1, Local port: 35258
Foreign host: 10.0.0.2, Foreign port: 179
Nexthop: 10.0.0.1
Nexthop global: fe80::202:ff:fe00:19
Nexthop local: ::

BGP connection: non shared network
Read thread: on Write thread: off

```

To see the details of a specific route such as from whom it was received, to whom it was sent, and so forth, use the `show ip bgp <ip address/prefix>` command:

```

R7# show ip bgp 192.0.2.0
BGP routing table entry for 192.0.2.0/24
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Local
    10.0.0.2 (metric 1) from 10.0.0.2 (0.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Originator: 0.0.0.10, Cluster list: 0.0.0.5
      Last update: Mon Jul  8 10:12:17 2013
  Local
    192.0.2.2 (metric 1) from 192.0.2.2 (0.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal
      Originator: 0.0.0.10, Cluster list: 0.0.0.6
      Last update: Mon Jul  8 10:12:17 2013

```

This shows that the routing table prefix seen by BGP is 192.0.2.0/24, that this route was not advertised to any neighbor, and that it was heard by two neighbors, 10.0.0.2 and 192.0.2.2.

Here is another output of the same command, on a different node in the network:

```

cumulus@switch:~$ sudo vtysh -c 'sh ip bgp 192.0.2.0'
BGP routing table entry for 192.0.2.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
    10.0.0.1 192.0.2.21 192.0.2.22
  Local, (Received from a RR-client)
    203.0.113.1 (metric 1) from 203.0.113.1 (0.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Last update: Mon Jul  8 09:07:41 2013

```

Debugging Tip: Logging Neighbor State Changes

It is very useful to log the changes that a neighbor goes through to troubleshoot any issues associated with that neighbor. This is done using the `log-neighbor-changes` command:

```
R7(config-router)# bgp log-neighbor-changes
```

The output is sent to the specified log file, usually `/var/log/quagga/bgpd.log`, and looks like this:

```
2013/07/08 10:12:06.572827 BGP: %NOTIFICATION: sent to neighbor 10.0.0.2 6
/3 (Cease/Peer Unconfigured) 0 bytes
2013/07/08 10:12:06.572954 BGP: Notification sent to neighbor 10.0.0.2:
type 6/3
2013/07/08 10:12:16.682071 BGP: %ADJCHANGE: neighbor 192.0.2.2 Up
2013/07/08 10:12:16.682660 BGP: %ADJCHANGE: neighbor 10.0.0.2 Up
```

Troubleshooting Link-local Addresses

To verify that quagga learned the neighboring link-local IPv6 address via the IPv6 neighbor discovery router advertisements on a given interface, use the `show interface <if-name>` command. If `ipv6 nd suppress-ra` isn't enabled on both ends of the interface, then `Neighbor address(s)` should have the other end's link-local address. That is the address that BGP would use when BGP is enabled on that interface.

Use `vtysh` to run quagga, then verify the configuration:

```
cumulus@switch:~$ sudo vtysh

Hello, this is Quagga (version 0.99.21).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

R7# show interface swp1
Interface swp1 is up, line protocol is up
  PTM status: disabled
  Description: rut
  index 3 metric 1 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:02:00:00:00:09
  inet 11.0.0.1/24 broadcast 11.0.0.255
    inet6 fe80::202:ff:fe00:9/64
      ND advertised reachable time is 0 milliseconds
      ND advertised retransmit interval is 0 milliseconds
      ND router advertisements are sent every 600 seconds
```

```
ND router advertisements lifetime tracks ra-interval
ND router advertisement default router preference is medium
Hosts use stateless autoconfig for addresses.
Neighbor address(s):
inet6 fe80::4638:39ff:fe00:129b/128
```

Instead of the IPv6 address, the peering interface name is displayed in the `show ip bgp summary` command and wherever else applicable:

```
R7# show ip bgp summary
BGP router identifier 0.0.0.1, local AS number 65000
RIB entries 1, using 112 bytes of memory
Peers 1, using 8712 bytes of memory

Neighbor          V     AS MsgRcvd MsgSent      TblVer  InQ OutQ Up/Down  State
/PfxRcd
swp1            4  65000       161       170          0      0      0 00:02:28          0
```

Most of the show commands can take the interface name instead of the IP address, if that level of specificity is needed:

```
R7# show ip bgp neighbors
<cr>
A.B.C.D  Neighbor to display information about
WORD      Neighbor on bgp configured interface
X:X::X:X  Neighbor to display information about
R7# show ip bgp neighbors swp1
```

Enabling Read-only Mode

You can enable read-only mode for when the BGP process restarts or when the BGP process is cleared using `clear ip bgp *`. When enabled, read-only mode begins as soon as the first peer reaches its *established* state and a timer for `<max-delay>` seconds is started.

While in read-only mode, BGP doesn't run best-path or generate any updates to its peers. This mode continues until:

- All the configured peers, except the shutdown peers, have sent an explicit EOR (End-Of-RIB) or an implicit EOR. The first keep-alive after BGP has reached the established state is considered an implicit EOR. If the `<establish-wait>` option is specified, then BGP will wait for peers to reach the established state from the start of the `update-delay` until the `<establish-wait>` period is over; that is, the minimum set of established peers for which EOR is expected would be peers established during the `establish-wait` window, not necessarily all the configured neighbors.
- The `max-delay` period is over.

Upon reaching either of these two conditions, BGP resumes the decision process and generates updates to its peers.

To enable read-only mode:

```
cumulus@switch:$ sudo bgp update-delay <max-delay in seconds> [<establish-wait in seconds>]
```

The default <max-delay> is 0 — the feature is off by default.

Use output from `show ip bgp summary` for information about the state of the update delay.

This feature can be useful in reducing CPU/network usage as BGP restarts/clears. It's particularly useful in topologies where BGP learns a prefix from many peers. Intermediate best paths are possible for the same prefix as peers get established and start receiving updates at different times. This feature is also valuable if the network has a high number of such prefixes.

Applying a Route Map for Route Updates

You can apply a route map on route updates from BGP to Zebra. All the applicable match operations are allowed, such as match on prefix, next-hop, communities, and so forth. Set operations for this attach-point are limited to metric and next-hop only. Any operation of this feature does not affect BGPs internal RIB.

Both IPv4 and IPv6 address families are supported. Route maps work on multi-paths as well. However, the metric setting is based on the best path only.

To apply a route map for route updates:

```
cumulus@switch:$ sudo cl-bgp table-map <route-map-name>
```

Protocol Tuning

Converging Quickly On Link Failures

In the Clos topology, we recommend that you only use interface addresses to set up peering sessions. This means that when the link fails, the BGP session is torn down immediately, triggering route updates to propagate through the network quickly. This requires the following commands be enabled for all links: `link-detect` and `ttl-security hops <hops>`. `ttl-security hops` specifies how many hops away the neighbor is. For example, in a Clos topology, every peer is at most 1 hop away.



See Caveats and Errata below for information regarding `ttl-security hops`.

Here is an example:

```
cumulus@switch:~$ sudo vtysh  
  
Hello, this is Quagga (version 0.99.21).
```

Copyright 1996-2005 Kunihiro Ishiguro, et al.

```
R7# configure terminal
R7(config)# interface swp1
R7(config-if)# link-detect
R7(config-if)# exit
R7(config)# router bgp 65000
R7(config-router)# neighbor 10.0.0.2 ttl-security hops 1
```

Converging Quickly On Soft Failures

It is possible that the link is up, but the neighboring BGP process is hung or has crashed. If a BGP process crashes, Quagga's `watchquagga` daemon, which monitors the various `quagga` daemons, will attempt to restart it. If the process is also hung, `watchquagga` will attempt to restart the process. BGP itself has a `keepalive` timer that is exchanged between neighbors. By default, this `keepalive` timer is set to 60 seconds. This time can be reduced to a lower number, but this has the disadvantage of increasing the CPU load, especially in the presence of a lot of neighbors. `keepalive-time` is the periodicity with which the `keepalive` message is sent. `hold-time` specifies how many `keepalive` messages can be lost before the connection is considered invalid. It is usually set to 3 times the `keepalive` time. Here is an example of reducing these timers:

```
R7(config-router)# neighbor 10.0.0.2 timers 30 90
```

We can make these the default for all BGP neighbors using a different command:

```
R7(config-router)# timers bgp 30 90
```

The following display snippet shows that the default values have been modified for this neighbor:

```
R7(config-router)# do show ip bgp neighbor 10.0.0.2
BGP neighbor is 10.0.0.2, remote AS 65000, local AS 65000, internal link
  BGP version 4, remote router ID 0.0.0.5
  BGP state = Established, up for 05:53:59
  Last read 14:53:25, hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 90, keepalive interval is 30 seconds
  ....
```



When you're in a configuration mode, such as when you're configuring BGP parameters, you can run any `show` command by adding `do` to the original command. For example, `do show ip bgp neighbor` was shown above. Under a non-configuration mode, you'd simply run:

```
show ip bgp neighbor 10.0.0.2
```

Reconnecting Quickly

A BGP process attempts to connect to a peer after a failure (or on startup) every `connect-time` seconds. By default, this is 120 seconds. To modify this value, use:

```
R7(config-router)# neighbor 10.0.0.2 timers connect 30
```

This command has to be specified per each neighbor, peer-group doesn't support this option in quagga.

Advertisement Interval

BGP by default chooses stability over fast convergence. This is very useful when routing for the Internet. For example, unlike link-state protocols, BGP typically waits for a duration of `advertisement-interval` seconds between sending consecutive updates to a neighbor. This ensures that an unstable neighbor flapping routes won't be propagated throughout the network. By default, this is set to 30 seconds for an eBGP session and 5 seconds for an iBGP session. For very fast convergence, set the timer to 0 seconds. You can modify this as follows:

```
R7(config-router)# neighbor 10.0.0.2 advertisement-interval 0
```

The following output shows the modified value:

```
R7(config-router)# do show ip bgp neighbor 10.0.0.2
BGP neighbor is 10.0.0.2, remote AS 65000, local AS 65000, internal link
  BGP version 4, remote router ID 0.0.0.5
  BGP state = Established, up for 06:01:49
  Last read 14:53:15, hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    Inq depth is 0
    Outq depth is 0
      Sent          Rcvd
    Opens:           1            1
    Notifications:  0            0
```

```

Updates:          1      3
Keepalives:       363    362
Route Refresh:    0      0
Capability:      0      0
Total:           365    366

Minimum time between advertisement runs is 0 seconds
....
```



This command is not supported with peer-groups.

See this [IETF draft](#) for more details on the use of this value.

Configuration Files

- /etc/quagga/daemons
- /etc/quagga/bgpd.conf

Useful Links

- Bidirectional forwarding detection (see page 394) (BFD) and BGP
- Wikipedia entry for BGP (includes list of useful RFCs)
- Quagga online documentation for BGP (may not be up to date)
- IETF draft discussing BGP use within data centers

Caveats and Errata

ttl-security Issue

Enabling `ttl-security` does not cause the hardware to be programmed with the relevant information. This means that frames will come up to the CPU and be dropped there. It is recommended that you use the `cl-acltool` command to explicitly add the relevant entry to hardware.

For example, you can configure a file, like `/etc/cumulus/acl/policy.d/01control_plane_bgp.rules`, with a rule like this for TTL:

```

INGRESS_INTF = swp1
INGRESS_CHAIN = INPUT, FORWARD

[iptables]
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p tcp --dport bgp -m
ttl --ttl 255 POLICE --set-mode pkt --set-rate 2000 --set-burst 1000
-A $INGRESS_CHAIN --in-interface $INGRESS_INTF -p tcp --dport bgp DROP
```



For more information about ACLs and `c1-acltool`, see [Netfilter \(ACLs\)](#) (see page 89).

Bidirectional Forwarding Detection - BFD

Bidirectional Forwarding Detection (BFD) provides low overhead and rapid detection of failures in the paths between two network devices. It provides a unified mechanism for link detection over all media and protocol layers. Use BFD to detect failures for IPv4 and IPv6 single or multihop paths between any two network devices, including unidirectional path failure detection.



Cumulus Linux does not support demand mode in BFD.

Using BFD Multihop Routed Paths

BFD multihop sessions are built over arbitrary paths between two systems, which results in some complexity that does not exist for single hop sessions. Here are some best practices for using multihop paths:

- **Spoofing:** To avoid spoofing with multihop paths, configure `max_hop_cnt` (maximum hop count) for each peer, which limits the number of hops for a BFD session. All BFD packets exceeding the max hop count will be dropped.
- **Demultiplexing:** Since multihop BFD sessions can take arbitrary paths, demultiplex the initial BFD packet based on the source/destination IP address pair. Use Quagga, which monitors connectivity to the peer, to determine the source/destination IP address pairs.

Multihop BFD sessions are supported for both IPv4 and IPv6 peers. See below for more details.

BFD Parameters

You can configure the following BFD parameters for both IPv4 and IPv6 sessions:

- The required minimum interval between the received BFD control packets.
- The minimum interval for transmitting BFD control packets.
- The detection time multiplier.

Configuring BFD

You configure BFD one of two ways: by specifying the configuration in the [PTM topology.dot file](#) (see page 172), or using [Quagga](#) (see page 344).

The [Quagga CLI](#) (see page) can track IPv4 and IPv6 peer connectivity — both single hop and multihop, and both link-local IPv6 peers and global IPv6 peers — using BFD sessions without needing the `topology.dot` file. Use Quagga to register multihop peers with PTM and BFD as well as for monitoring the connectivity to the remote BGP multihop peer. Quagga can dynamically register and unregister both IPv4 and IPv6 peers with BFD when the BFD-enabled peer connectivity is established or de-established, respectively. Also, you can configure BFD parameters for each BGP or OSPF peer using Quagga.



The BFD parameter configured in the topology file is given higher precedence over the client-configured BFD parameters for a BFD session that has been created by both topology file and client (Quagga).

BFD in BGP

For Quagga when using **BGP**, neighbors are registered and de-registered with PTM (see page 172) dynamically when you enable BFD in BGP:

```
quagga(config)# router bgp X
quagga(config-router)# neighbor <neighbor ip> bfd
```

You can configure BFD parameters for each BGP neighbor. For example:

BFD in BGP

```
quagga(config-router)# neighbor <neighbor ip> bfd
    <2-255> Detect Multiplier
    <cr>
quagga(config-router)# neighbor <neighbor ip> bfd 4
    <50-60000> Required min receive interval
quagga(config-router)# neighbor <neighbor ip> bfd 4 400
    <50-60000> Desired min transmit interval
quagga(config-router)# neighbor <neighbor ip> bfd 4 400 400
    <cr>
quagga(config-router)# neighbor <neighbor ip> bfd 4 400 400
```

To see neighbor information in BGP, including BFD status, run `show bgp neighbors <IP address>`.

Show BGP Neighbor

```
quagga# show bgp neighbors 12.12.12.1
BGP neighbor is 12.12.12.1, remote AS 65001, local AS 65000, external
link
Hostname: r1
    BGP version 4, remote router ID 0.0.0.1
    BGP state = Established, up for 00:01:39
    Last read 00:00:39, Last write 00:01:09
    Hold time is 180, keepalive interval is 60 seconds
    Neighbor capabilities:
        4 Byte AS: advertised and received
        AddPath:
            IPv4 Unicast: RX advertised and received
            Route refresh: advertised and received(old & new)
            Address family IPv4 Unicast: advertised and received
            Hostname Capability: advertised and received
```

```

Graceful Restart Capability: advertised and received
  Remote Restart timer is 120 seconds
  Address families by peer:
    none
Graceful restart informations:
  End-of-RIB send: IPv4 Unicast
  End-of-RIB received: IPv4 Unicast
Message statistics:
  Inq depth is 0
  Outq depth is 0
      Sent          Rcvd
  Opens:           1           1
  Notifications:  0           0
  Updates:        2           2
  Keepalives:     2           1
  Route Refresh:  0           0
  Capability:    0           0
  Total:          5           4
Minimum time between advertisement runs is 30 seconds
Update source is 12.12.12.7

For address family: IPv4 Unicast
  Update group 1, subgroup 1
  Packet Queue length 0
  NEXT_HOP is always this router
  Community attribute sent to this neighbor(both)
  1 accepted prefixes
  Connections established 1; dropped 0
  Last reset never
  External BGP neighbor may be up to 2 hops away.
  Local host: 12.12.12.7, Local port: 34274
  Foreign host: 12.12.12.1, Foreign port: 179
  Nexthop: 12.12.12.7
  Nexthop global: :::
  Nexthop local: :::
  BGP connection: non shared network
  Read thread: on  Write thread: off
  BFD: Type: multi hop
    Detect Mul: 3, Min Rx interval: 300, Min Tx interval: 300
    Status: Down, Last update: 0:00:00:13

```

BFD in OSPF

For Quagga using **OSPF**, neighbors are registered and de-registered dynamically with **PTM** (see page 172) when you enable or disable BFD in OSPF. A neighbor is registered with BFD when two-way adjacency is established and deregistered when adjacency goes down if the BFD is enabled on the interface. The BFD configuration is per interface and any IPv4 and IPv6 neighbors discovered on that interface inherit the configuration.

BFD in OSPF

```

quagga(config)# interface X
quagga(config-if)# ipv6 ospf6 bfd
    <2-255> Detect Multiplier
    <cr>
quagga(config-if)# ipv6 ospf6 bfd 5
    <50-60000> Required min receive interval
quagga(config-if)# ipv6 ospf6 bfd 5 500
    <50-60000> Desired min transmit interval
quagga(config-if)# ipv6 ospf6 bfd 5 500 500
    <cr>
quagga(config-if)# ipv6 ospf6 bfd 5 500 500

```

OSPF Show Commands

The BFD lines at the end of each code block shows the corresponding IPv6 or IPv4 OSPF interface or neighbor information.

Show IPv6 OSPF Interface

```

quagga# show ipv6 ospf6 interface swp2s0
swp2s0 is up, type BROADCAST
    Interface ID: 4
    Internet Address:
        inet : 11.0.0.21/30
        inet6: fe80::4638:39ff:fe00:6c8e/64
    Instance ID 0, Interface MTU 1500 (autodetect: 1500)
    MTU mismatch detection: enabled
    Area ID 0.0.0.0, Cost 10
    State PointToPoint, Transmit Delay 1 sec, Priority 1
    Timer intervals configured:
        Hello 10, Dead 40, Retransmit 5
    DR: 0.0.0.0 BDR: 0.0.0.0
    Number of I/F scoped LSAs is 2
        0 Pending LSAs for LSUpdate in Time 00:00:00 [thread off]
        0 Pending LSAs for LSAck in Time 00:00:00 [thread off]
    BFD: Detect Mul: 3, Min Rx interval: 300, Min Tx interval: 300

```

Show IPv6 OSPF Neighbor

```

quagga# show ipv6 ospf6 neighbor detail
Neighbor 0.0.0.4%swp2s0
    Area 0.0.0.0 via interface swp2s0 (ifindex 4)
    His IfIndex: 3 Link-local address: fe80::202:ff:fe00:a
    State Full for a duration of 02:32:33
    His choice of DR/BDR 0.0.0.0/0.0.0.0, Priority 1
    DbDesc status: Slave SeqNum: 0x76000000
    Summary-List: 0 LSAs

```

```

Request-List: 0 LSAs
Retrans-List: 0 LSAs
0 Pending LSAs for DbDesc in Time 00:00:00 [thread off]
0 Pending LSAs for LSReq in Time 00:00:00 [thread off]
0 Pending LSAs for LSUpdate in Time 00:00:00 [thread off]
0 Pending LSAs for LSAck in Time 00:00:00 [thread off]
BFD: Type: single hop
  Detect Mul: 3, Min Rx interval: 300, Min Tx interval: 300
  Status: Up, Last update: 0:00:00:20

```

Show IPv4 OSPF Interface

```

quagga# show ip ospf interface swp2s0
swp2s0 is up
  ifindex 4, MTU 1500 bytes, BW 0 Kbit <UP,BROADCAST,RUNNING,
MULTICAST>
    Internet Address 11.0.0.21/30, Area 0.0.0.0
    MTU mismatch detection:enabled
    Router ID 0.0.0.3, Network Type POINTOPOINT, Cost: 10
    Transmit Delay is 1 sec, State Point-To-Point, Priority 1
    No designated router on this network
    No backup designated router on this network
    Multicast group memberships: OSPFAllRouters
    Timer intervals configured, Hello 10s, Dead 40s, Wait 40s,
Retransmit 5
      Hello due in 7.056s
    Neighbor Count is 1, Adjacent neighbor count is 1
    BFD: Detect Mul: 5, Min Rx interval: 500, Min Tx interval: 500

```

Show IPv4 OSPF Neighbor

```

quagga# show ip ospf neighbor detail
Neighbor 0.0.0.4, interface address 11.0.0.22
  In the area 0.0.0.0 via interface swp2s0
  Neighbor priority is 1, State is Full, 5 state changes
  Most recent state change statistics:
    Progressive change 3h59m04s ago
  DR is 0.0.0.0, BDR is 0.0.0.0
  Options 2 *|-|-|---|E|*
  Dead timer due in 38.501s
  Database Summary List 0
  Link State Request List 0
  Link State Retransmission List 0
  Thread Inactivity Timer on
  Thread Database Description Retransmission off
  Thread Link State Request Retransmission on
  Thread Link State Update Retransmission on
  BFD: Type: single hop

```

```
Detect Mul: 5, Min Rx interval: 500, Min Tx interval: 500
Status: Down, Last update: 0:00:01:29
```

Troubleshooting BFD

To troubleshoot BFD, use `ptmctl -b`. For more information, see [Prescriptive Topology Manager - PTM](#) (see page 172).

Equal Cost Multipath Load Sharing - Hardware ECMP

Cumulus Linux supports hardware-based equal cost multipath (ECMP) load sharing. ECMP is enabled by default in Cumulus Linux. Load sharing occurs automatically for all routes with multiple next hops installed. ECMP load sharing supports both IPv4 and IPv6 routes.



ECMP is not supported in Cumulus RMP.

Contents

(Click to expand)

- Contents (see page 399)
- Understanding Equal Cost Routing (see page 399)
- Understanding ECMP Hashing (see page 400)
 - Using `cl-ecmpcalc` to Determine the Hash Result (see page 400)
 - `cl-ecmpcalc` Limitations (see page 401)
 - ECMP Hash Buckets (see page 401)
- Resilient Hashing (see page 403)
 - Resilient Hash Buckets (see page 404)
 - Removing Next Hops (see page 404)
 - Adding Next Hops (see page 406)
 - Configuring Resilient Hashing (see page 406)
- Caveats (see page 407)
- Useful Links (see page 407)

Understanding Equal Cost Routing

ECMP operates only on equal cost routes in the Linux routing table.

In this example, the 10.1.1.0/24 route has two possible next hops that have been installed in the routing table:

```
$ ip route show 10.1.1.0/24
10.1.1.0/24 proto zebra metric 20
```

```
nexthop via 192.168.1.1 dev swp1 weight 1 onlink
nexthop via 192.168.2.1 dev swp2 weight 1 onlink
```

For routes to be considered equal they must:

- Originate from the same routing protocol. Routes from different sources are not considered equal. For example, a static route and an OSPF route are not considered for ECMP load sharing.
- Have equal cost. If two routes from the same protocol are unequal, only the best route is installed in the routing table.



BGP does not install multiple routes by default. To do so, use the `maximum-paths` command. See the [ECMP section \(see page 372\)](#) of the BGP chapter for more information.

Understanding ECMP Hashing

Once multiple routes are installed in the routing table, a hash is used to determine which path a packet follows.

Cumulus Linux hashes on the following fields:

- IP protocol
- Ingress interface
- Source IPv4 or IPv6 address
- Destination IPv4 or IPv6 address

For TCP/UDP frames, Cumulus Linux also hashes on:

- Source port
- Destination port

ECMP Hash Fields

Source IP	Destination IP	Layer 4 Protocol	Source Port	Destination Port	Payload
-----------	----------------	------------------	-------------	------------------	---------

To prevent out of order packets, ECMP hashing is done on a per-flow basis meaning that all packets with the same source and destination IP addresses and the same source and destination ports always hash to the same next hop. ECMP hashing does not keep a record of flow states.

ECMP hashing does not keep a record of packets that have hashed to each next hop and does not guarantee that traffic sent to each next hop is equal.

Using `cl-ecmpcalc` to Determine the Hash Result

Since the hash is deterministic and always provides the same result for the same input, you can query the hardware and determine the hash result of a given input. This is useful when determining exactly which path a flow takes through a network.

On Cumulus Linux, use the `cl-ecmpcalc` command to determine a hardware hash result.

In order to use `cl-ecmpcalc`, all fields that are used in the hash must be provided. This includes ingress interface, layer 3 source IP, layer 3 destination IP, layer 4 source port and layer 4 destination port.

```
$ sudo cl-ecmpcalc -i swp1 -s 10.0.0.1 -d 10.0.0.1 -p tcp --sport 20000 --
dport 80
ecmpcalc: will query hardware
swp3
```

If any field is omitted, `cl-ecmpcalc` fails.

```
$ sudo cl-ecmpcalc -i swp1 -s 10.0.0.1 -d 10.0.0.1 -p tcp
ecmpcalc: will query hardware
usage: cl-ecmpcalc [-h] [-v] [-p PROTOCOL] [-s SRC] [--sport SPORT] [-d
DST]
                           [--dport DPORT] [--vid VID] [-i IN_INTERFACE]
                           [--sportid SPORTID] [--smodid SMODID] [-o OUT_INTERFACE]
                           [--dportid DPORTID] [--dmodid DMODID] [--hardware]
                           [--nohardware] [-hs HASHSEED]
                           [-hf HASHFIELDS [HASHFIELDS ...]]
                           [--hashfunction {crc16-ccitt,crc16-bisync}] [-e EGRESS]
                           [-c MCOUNT]
```

```
cl-ecmpcalc: error: --sport and --dport required for TCP and UDP frames
```

cl-ecmpcalc Limitations

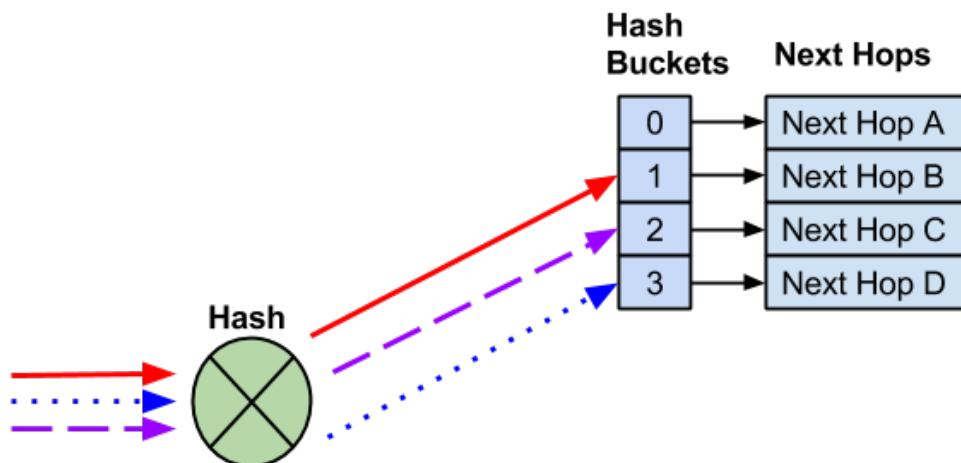
`cl-ecmpcalc` can only take input interfaces that can be converted to a single physical port in the port tab file, like the physical switch ports (swp). Virtual interfaces like bridges, bonds, and subinterfaces are not supported.

`cl-ecmpcalc` is supported only on switches with the [Trident](#), [Trident+](#), [Trident II](#) and [Trident II+](#) chipsets.

ECMP Hash Buckets

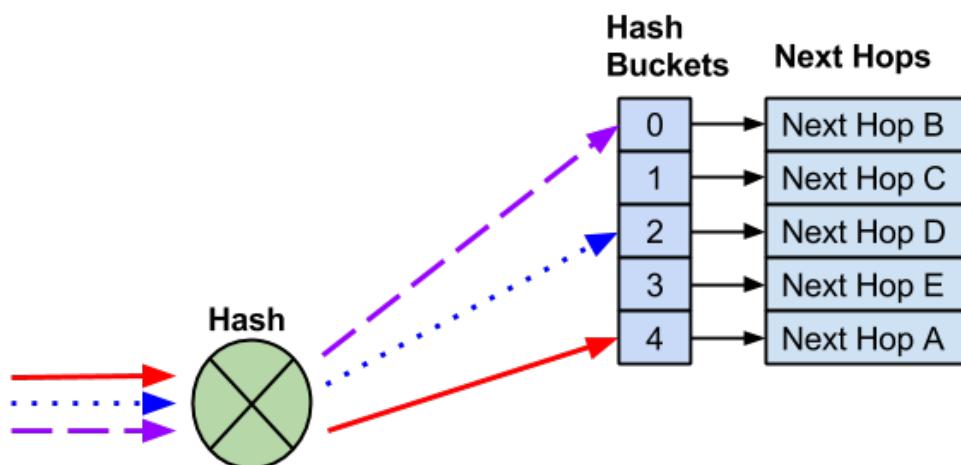
When multiple routes are installed in the routing table, each route is assigned to an ECMP *bucket*. When the ECMP hash is executed the result of the hash determines which bucket gets used.

In the following example, 4 next hops exist. Three different flows are hashed to different hash buckets. Each next hop is assigned to a unique hash bucket.



Adding a Next Hop

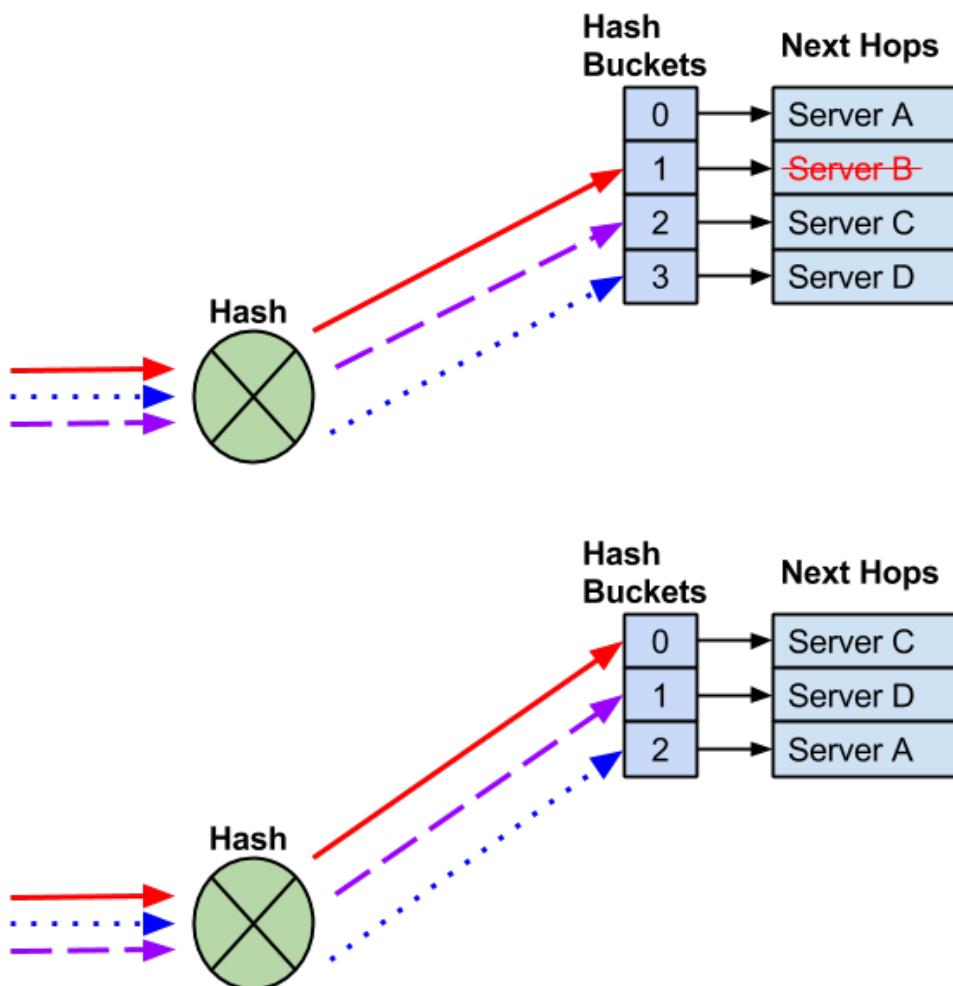
When a next hop is added, a new hash bucket is created. The assignment of next hops to hash buckets, as well as the hash result, may change when additional next hops are added.



A new next hop is added and a new hash bucket is created. As a result, the hash and hash bucket assignment changed, causing the existing flows to be sent to different next hops.

Removing a Next Hop

When a next hop is removed, the remaining hash bucket assignments may change, again, potentially changing the next hop selected for an existing flow.



A next hop fails and the next hop and hash bucket are removed. The remaining next hops may be reassigned.

In most cases, the modification of hash buckets has no impact on traffic flows as traffic is being forward to a single end host. In deployments where multiple end hosts are using the same IP address (anycast), *resilient hashing* must be used.

Resilient Hashing

In Cumulus Linux when a next hop fails or is removed from an ECMP pool, the hashing or hash bucket assignment can change. For deployments where there is a need for flows to always use the same next hop, like TCP anycast deployments, this can create session failures.

The ECMP hash performed with resilient hashing is exactly the same as the default hashing mode. Only the method in which next hops are assigned to hash buckets differs.

Resilient hashing supports both IPv4 and IPv6 routes.

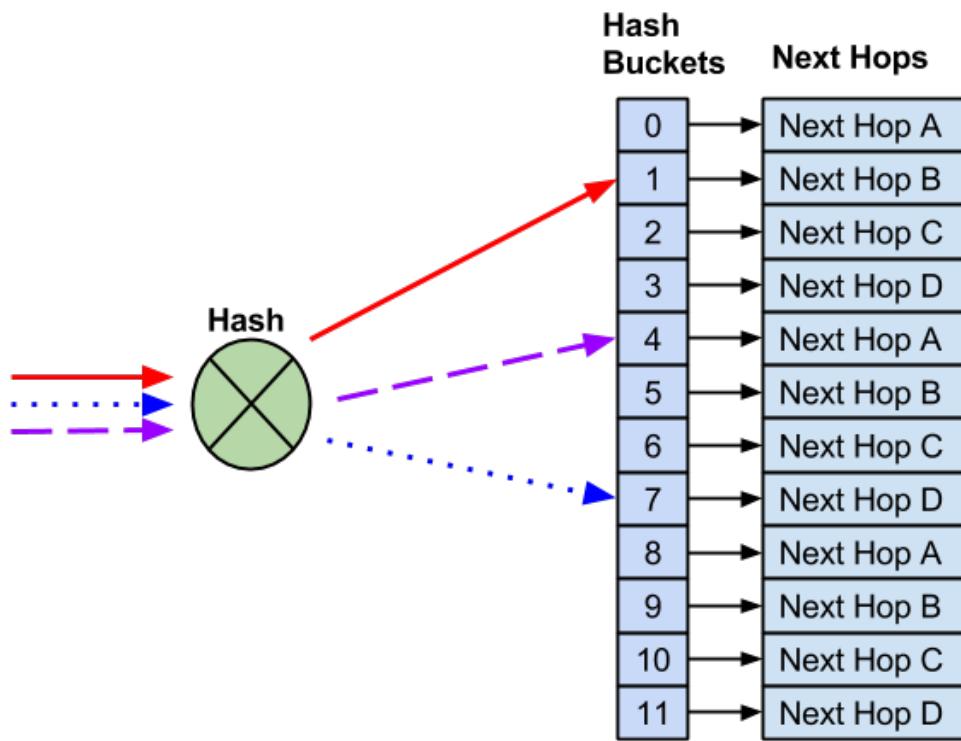
Resilient hashing is not enabled by default. See below for steps on configuring it.



Resilient hashing prevents disruptions when new next hops are removed. It does not prevent disruption when next hops are added.

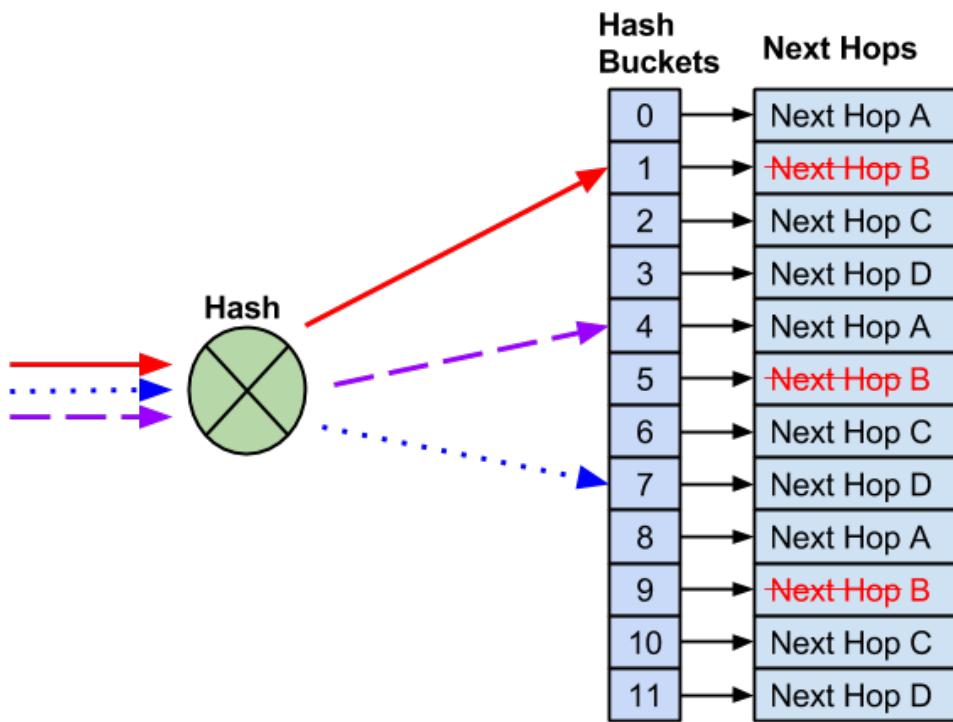
Resilient Hash Buckets

When resilient hashing is configured, a fixed number of buckets are defined. Next hops are then assigned in round robin fashion to each of those buckets. In this example, 12 buckets are created and four next hops are assigned.

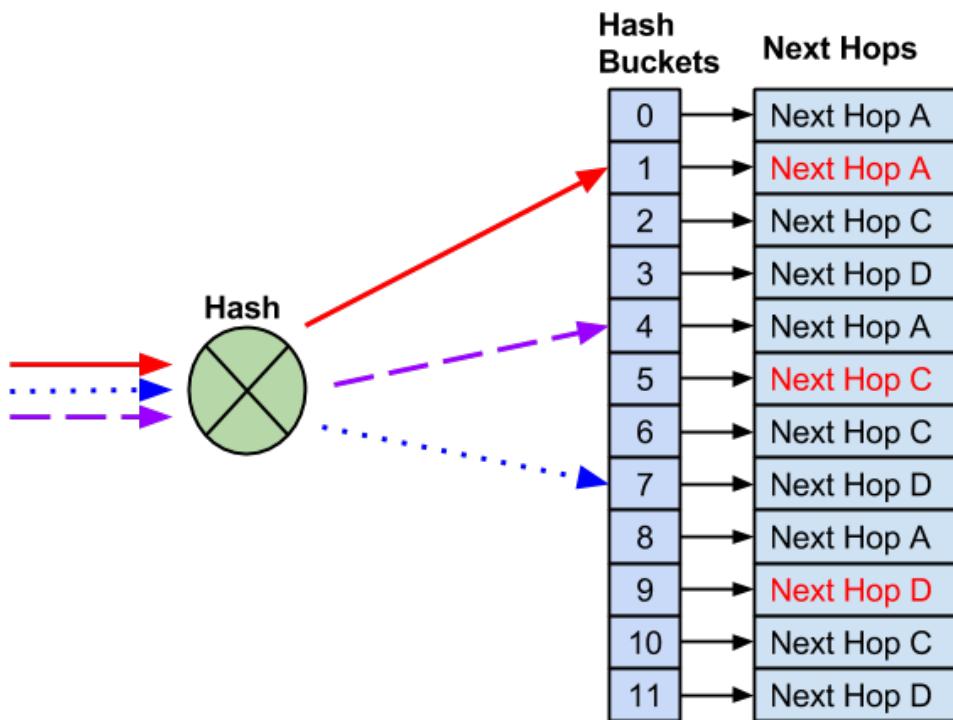


Removing Next Hops

Unlike default ECMP hashing, when a next hop needs to be removed, the number of hash buckets does not change.



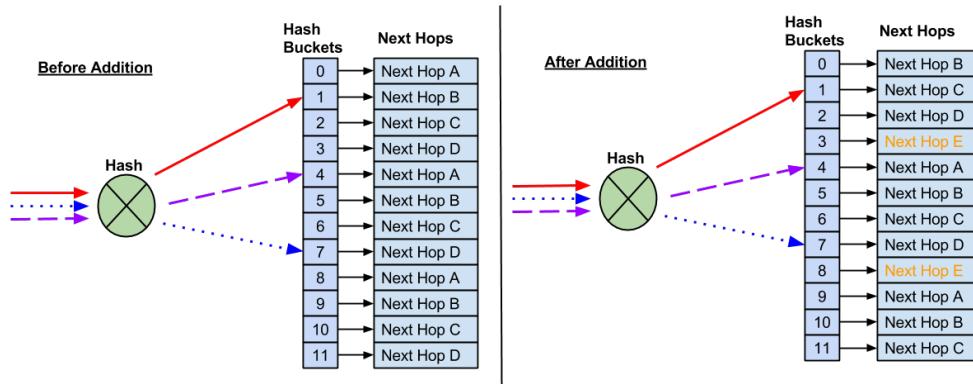
With 12 buckets assigned and four next hops, instead of reducing the number of buckets — which would impact flows to known good hosts — the remaining next hops replace the failed next hop.



After the failed next hop is removed, the remaining next hops are installed as replacements. This prevents impact to any flows that hash to working next hops.

Adding Next Hops

Resilient hashing does not prevent possible impact to existing flows when new next hops are added. Due to the fact there are a fixed number of buckets, a new next hop requires reassigning next hops to buckets.



As a result, some flows may hash to new next hops, which can impact anycast deployments.

Configuring Resilient Hashing

Resilient hashing is not enabled by default. When resilient hashing is enabled, 65,536 buckets are created to be shared among all ECMP routes.



An ECMP route counts as a single route with multiple next hops. The following example is considered to be a single ECMP route:

```
$ ip route show 10.1.1.0/24
10.1.1.0/24 proto zebra metric 20
  nexthop via 192.168.1.1 dev swp1 weight 1 onlink
  nexthop via 192.168.2.1 dev swp2 weight 1 onlink
```

All ECMP routes must use the same number of buckets (the number of buckets cannot be configured per ECMP route).

The number of buckets can be configured as 64, 128, 256, 512 or 1024; the default is 128:

Number of Hash Buckets	Number of Supported ECMP Routes
64	1024
128	512

Number of Hash Buckets	Number of Supported ECMP Routes
256	256
512	128
1024	64

A larger number of ECMP buckets reduces the impact on adding new next hops to an ECMP route. However, the system supports fewer ECMP routes. If the maximum number of ECMP routes have been installed, new ECMP routes log an error and are not installed.

To enable resilient hashing, edit `/etc/cumulus/datapath/traffic.conf`:

1. Enable resilient hashing:

```
# Enable resilient hashing
resilient_hash_enable = TRUE
```

2. **(Optional)** Edit the number of hash buckets:

```
# Resilient hashing flowset entries per ECMP group
# Valid values - 64, 128, 256, 512, 1024
resilient_hash_entries_ecmp = 256
```

3. Restart the `switchd` service:

```
cumulus@switch:~$ sudo service switchd restart
```

Caveats

Resilient hashing is supported only on switches with the [Trident II chipsets](#). You can run `netshow system` to determine the chipset.

Useful Links

- http://en.wikipedia.org/wiki/Equal-cost_multi-path_routing

Management VRF

Management VRF (multiple routing tables and forwarding) provides routing separation between the out-of-band management network and the in-band data plane network. When management VRF is enabled, applications running on control plane processor communicate out from the management network unless configured otherwise.

Management VRF creates two routing tables within the Linux kernel:

- *main*: This is the routing table for all the data plane switch ports.
- *mgmt*: This is the routing table for eth0.

Cumulus Linux only supports eth0 as the management interface. VLAN subinterfaces, bonds, bridges and the front panel switch ports are not supported as management interfaces.

Management VRF assumes all traffic *generated by the switch* (except via Quagga) will exit eth0 by default, so unless there is application-level intervention, any packet generated by an application on the switch will only reference the eth0 routing table (the *mgmt* table). Applications that need to communicate over the data plane network (the *main* table) **must** bind to the loopback IP address.

For example, if the switch is responding to an inbound SSH connection or inbound ping, management VRF does not force the traffic out through eth0. However, if you attempt to SSH from the switch outbound, then management VRF will force the traffic to exit eth0, unless you specify otherwise. For example, when initiating an SSH connection, you can use `-b <loopback IP address>` to SSH to a device via the data plane network.

Contents

- Enabling Management VRF (see page 408)
 - Verifying Management VRF (see page 409)
 - Disabling Management VRF (see page 409)
- Using ping or traceroute (see page 410)
- OSPF and BGP (see page 410)
 - Redistributing Routes in Management VRF (see page 410)
- SNMP Traps Use eth0 Only (see page 411)
- SSH (see page 411)
- Viewing the Routing Tables (see page 411)
 - Viewing a Single Route (see page 412)
- Using Static IP Addresses on eth0 (see page 412)
- Incompatibility with cl-ns-mgmt (see page 413)
- Log Files (see page 413)
- Caveats and Errata (see page 413)

Enabling Management VRF

To enable management VRF, complete the following steps:

1. Update the apt source list:

```
$ sudo apt-get update
```

2. Install the management VRF package:

```
sudo apt-get install cl-mgmtvrf
```

3. Run the management VRF script:

```
sudo cl-mgmtvrf --enable
```



Management VRF has hooks in the eth0 DHCP client to force the correct mgmt table routes when the DHCP address is obtained. If you use static IP address assignment on eth0, you have to manually configure the routes before you execute this step. See the 'Using Static IP Addresses on eth0' section below for more information.

4. Restart Quagga:

```
sudo service quagga restart
```



You can also bounce adjacency to the peer advertising the default route to get the default route from the data plane network into the main routing table.

Verifying Management VRF

To check the status of management VRF, run:

```
cl-mgmtvrf --status
```

This will display `cl-mgmtvrf` is NOT enabled or `cl-mgmtvrf` is enabled, depending upon whether management VRF is disabled or enabled.

Disabling Management VRF

To disable management VRF, run:

```
sudo cl-mgmtvrf --disable
```



If management VRF is disabled and the data plane adds a default route, the default route via the management interface will **not** be added to main routing table.

Using ping or traceroute

By default, issuing a `ping` or `traceroute` assumes the packet should be sent to the dataplane network (the main routing table). If you wish to use `ping` or `traceroute` on the control plane network, use the `-I` flag for `ping` and `-i` for `traceroute`.

```
ping -I eth0
```

or

```
sudo traceroute -i eth0
```



DNS does not work with `traceroute` or `ping` unless you explicitly add support for the DNS server in the *main* routing table.

OSPF and BGP

In general, no changes are required for either BGP or OSPF. Quagga was updated in Cumulus Linux 2.5.3 to be aware of the management VRF and automatically sends packets based on the switch port routing table. This includes BGP peering via loopback interfaces. BGP does routing lookups in the default table. However, one modification you may consider has to do with how your routes get redistributed.

Redistributing Routes in Management VRF

The control that management VRF has over the local routing table does not extend to how the routes are redistributed when using routing protocols such as OSPF and BGP.

To redistribute the routes in your network, use the `redistribute connected` command under BGP or OSPF. This enables the directly connected network out of eth0 to be advertised to its neighbor.



This also creates a route on the neighbor device to the management network through the data plane, which may not be desired.

Cumulus Networks recommends you always use route maps to control the advertised networks redistributed by the `redistribute connected` command. For example, you can specify a route map to redistribute routes in this way (for both BGP and OSPF):

```
<routing protocol>
redistribute connected route-map redistribute-connected

route-map redistribute-connected deny 100
  match interface eth0
!
route-map redistribute-connected permit 1000
```

SNMP Traps Use eth0 Only

SNMP cannot currently use a switch port to send data. For any SNMP traps, this traffic gets sent out to eth0. Cumulus Networks will support switch ports in the future.

This restriction only applies to traps; SNMP polling is not affected.

SSH

If you SSH to the switch through a switch port, it works as expected. If you need to SSH from the device out a switch port, use `ssh -b <ip_address_of_swp_port>`. For example:

```
cumulus@leaf1$ ip addr show swp17
19: swp17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
  state UP qlen 500
    link/ether ec:f4:bb:fc:19:23 brd ff:ff:ff:ff:ff:ff
      inet 10.23.23.2/24 scope global swp17
        inet6 fe80::eef4:bbff:fefc:1923/64 scope link
          valid_lft forever preferred_lft forever

cumulus@leaf1$ ssh -b 10.23.23.2 10.3.3.3
```

Viewing the Routing Tables

When you look at the routing table with `ip route show`, you are looking at the switch port (*main*) table. You can also see the dataplane routing table with `ip route show table main`.

To look at information about eth0 (the management routing table), use `ip route show table mgmt`.

```
cumulus@leaf1$ ip route show table mgmt
default via 192.168.0.1 dev eth0

cumulus@leaf1$ ip route show
default via 10.23.23.3 dev swp17 proto zebra metric 20
```

```
10.3.3.3 via 10.23.23.3 dev swp17
10.23.23.0/24 dev swp17  proto kernel  scope link  src 10.23.23.2
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.11
```

Viewing a Single Route

Note that if you use `ip route get` to return information about a single route, the command resolves over the `mgmt` table by default. To get information about the route in the switching silicon, use:

```
ip route get <addr> from <loopback IP>
```

Or:

```
sudo cl-ctl ip route show <addr>
```

Using Static IP Addresses on eth0

If you're using DHCP on your management network, the Management VRF feature has hooks in the `eth0` DHCP client to automatically add the correct default and interface routes into the `mgmt` table when the DHCP address is obtained.

If a static IP address is used in the `eth0` definition, you must manually control the connected and static routes attached to `eth0` *before running `cl-mgmtvrf --enable`*

To do this change the configuration in the `/etc/network/interfaces` as follows:

```
auto eth0
iface eth0 inet static
    address 192.1.1.254/24
    post-up ip route add 192.1.1.0/24 dev eth0 table mgmt
    post-up ip route add default via 192.1.1.1 dev eth0 table mgmt
    post-up ip route del 192.1.1.0/24 dev eth0 table main
    post-down ip route del 192.1.1.0/24 dev eth0 table mgmt
    post-down ip route del default via 192.1.1.1 dev eth0 table mgmt
```

Then bounce `eth0`:

```
sudo ifdown eth0; sudo ifup eth0
```

Enabling management VRF via `cl-mgmtvrf --enable` after this step should lead to the expected routing behavior.



The post-down commands are there to ensure that no routing race condition can occur on an interface experiencing route flapping. As a result, the following error messages during a link flap are harmless and can be ignored:

```
warning: eth0: post-down cmd 'ip route del 192.1.1.0/24 dev eth0
table mgmt' failed (RTNETLINK answers: No such process)
warning: eth0: post-down cmd 'ip route del default 192.1.1.1 via
eth0 table mgmt' failed (Error: either "to" is duplicate, or
"192.1.1.1" is a garbage.)
```

Incompatibility with `cl-ns-mgmt`



If you are using the Cumulus Linux [management namespace](#) feature (via the `cl-ns-mgmt` utility), you cannot enable management VRF, as the two features are incompatible. Management VRF does not run if Cumulus Linux detects that you have management namespaces enabled, and vice versa.

Log Files

- `/var/log/cl-mgmtvrf.log`

Caveats and Errata

- Unlike earlier versions of Cumulus Linux, with management VRF enabled, sFlow now sends and receives packets through switch ports as well as the management port, as long as `hsflowd` has a route available out of the main table. To enable this, contact the [Cumulus Networks support team](#).
- If you are using an [MLAG configuration \(see page 217\)](#) when the `eth0` management interface is enabled, you cannot specify a backup link (via `clagd-backup-ip`) over the switch ports.
- Duplicate IP addresses are not supported i.e. you cannot have the same IP address in both the management network and the data network.
- DHCP relay does not work with `cl-mgmtvrf` when the DHCP servers are on the management network. For more information, refer to the [knowledge base article](#).
- Cumulus Linux supports both DHCP and static DNS entries over management VRF through IP FIB rules. These rules are added to direct lookups to the DNS addresses out of the management VRF. However, nameservers configured through DHCP are automatically updated, while statically configured nameservers (configured in `/etc/resolv.conf`) only get updated when you run `ifreload -a`.

Because DNS lookups are forced out of the management interface using FIB rules, this could affect data plane ports if there are overlapping addresses.

Monitoring and Troubleshooting

This chapter introduces monitoring and troubleshooting Cumulus Linux.

Contents

(Click to expand)

- [Contents \(see page 414\)](#)
- [Commands \(see page 414\)](#)
- [Using the Serial Console \(see page 414\)
 - \[Configuring the Serial Console on PowerPC or ARM Switches \\(see page 414\\)\]\(#\)
 - \[Configuring the Serial Console on x86 Switches \\(see page 415\\)\]\(#\)](#)
- [Diagnostics Using cl-support \(see page 416\)](#)
- [Sending Log Files to a syslog Server \(see page 417\)](#)
- [Next Steps \(see page 419\)](#)

Commands

- [cl-support](#)
- [fw_setenv](#)

Using the Serial Console

The serial console can be a useful tool for debugging issues, especially when you find yourself rebooting the switch often or if you don't have a reliable network connection.

The default serial console baud rate is 115200, which is the baud rate ONIE uses.

Configuring the Serial Console on PowerPC or ARM Switches

On PowerPC switches, the U-Boot environment variable `baudrate` identifies the baud rate of the serial console. To change the `baudrate` variable, use the `fw_setenv` command:

```
cumulus@switch:~$ sudo fw_setenv baudrate 9600
Updating environment variable: `baudrate'
Proceed with update [N/y]? y
```

You must reboot the switch for the `baudrate` change to take effect.

The valid values for `baudrate` are:

- 300

- 600
- 1200
- 2400
- 4800
- 9600
- 19200
- 38400
- 115200

Configuring the Serial Console on x86 Switches

On x86 switches, you configure serial console baud rate by editing `grub`.



Incorrect configuration settings in `grub` can cause the switch to be inaccessible via the console. Grub changes should be carefully reviewed before implementation.

The valid values for the baud rate are:

- 300
- 600
- 1200
- 2400
- 4800
- 9600
- 19200
- 38400
- 115200

To change the serial console baud rate:

1. Edit `/etc/default/grub`. The two relevant lines in `/etc/default/grub` are as follows; replace the 115200 value with a valid value specified above in the `--speed` variable in the first line and in the `console` variable in the second line:

```
GRUB_SERIAL_COMMAND="serial --port=0x2f8 --speed=115200 --word=8 --
parity=no --stop=1"
GRUB_CMDLINE_LINUX="console=ttyS1,115200n8
cl_platform=accton_as5712_54x"
```

2. After you save your changes to the grub configuration, type the following at the command prompt:

```
cumulus@switch:~$ update-grub
```

3. If you plan on accessing your switch's BIOS over the serial console, you need to update the baud rate in the switch BIOS. For more information, see [this knowledge base article](#).
4. Reboot the switch.

Diagnostics Using cl-support

You can use `cl-support` to generate a single export file that contains various details and the configuration from a switch. This is useful for remote debugging and troubleshooting.

You should run `cl-support` before you submit a support request to Cumulus Networks as this file helps in the investigation of issues:

```
cumulus@switch:~$ sudo cl-support -h
Usage: cl-support [-h] [reason]...
Args:
[reason]: Optional reason to give for invoking cl-support.
          Saved into tarball's reason.txt file.
Options:
-h: Print this usage statement
```

Example output:

```
cumulus@switch:~$ ls /var/support
cl_support_20130806_032720.tar.xz
```

The directory structure is compressed using LZMA2 compression and can be extracted using the `unxz` command:

```
cumulus@switch:~$ cd /var/support
cumulus@switch:~$ sudo unxz cl_support_20130729_140040.tar.xz
cumulus@switch:~$ sudo tar xf cl_support_20130729_140040.tar
cumulus@switch:~$ ls -l cl_support_20130729_140040/
-rwxr-xr-x 1 root root 7724 Jul 29 14:00 cl-support
-rw-r--r-- 1 root root 52 Jul 29 14:00 cmdline.args
drwxr-xr-x 2 root root 4096 Jul 29 14:00 core
drwxr-xr-x 64 root root 4096 Jul 29 13:51 etc
drwxr-xr-x 4 root root 4096 Jul 29 14:00 proc
drwxr-xr-x 2 root root 4096 Jul 29 14:01 support
drwxr-xr-x 3 root root 4096 Jul 29 14:00 sys
drwxr-xr-x 3 root root 4096 Aug  8 15:22 var
```

The directory contains the following elements:

Directory	Description
core	Contains the core files generated from Cumulus Linux HAL process, <code>switchd</code> .
etc	Is a replica of the switch's <code>/etc</code> directory. <code>/etc</code> contains all the general Linux configuration files, as well as configurations for the system's network interfaces, <code>quagga</code> , <code>jdoe</code> , and other packages.
log	Is a replica of the switch's <code>/var/log</code> directory. Most Cumulus Linux log files are located in this directory. Notable log files include <code>switchd.log</code> , <code>daemon.log</code> , <code>quagga</code> log files, and <code>syslog</code> . For more information, read this knowledge base article .
proc	Is a replica of the switch's <code>/proc</code> directory. In Linux, <code>/proc</code> contains runtime system information (like system memory, devices mounted, and hardware configuration). These files are not actual files but the current state of the system.
support	Is a set of files containing further system information, which is obtained by <code>c1-support</code> running commands such as <code>ps -aux</code> , <code>netstat -i</code> , and so forth — even the routing tables.

`c1-support`, when untarred, contains a `reason.txt` file. This file indicates what reason triggered it. When contacting Cumulus Networks technical support, please attach the `c1-support` file if possible. For more information about `c1-support`, read [Understanding and Decoding the c1-support Output File](#) (see page 449).

Sending Log Files to a syslog Server

All logging on Cumulus Linux is done with `rsyslog`. `rsyslog` provides both local logging to the `syslog` file as well as the ability to export logs to an external `syslog` server. High precision timestamps are enabled for all `rsyslog` log files; here's an example:

```
2015-08-14T18:21:43.337804+00:00 cumulus switchd[3629]:  
switchd.c:1409 switchd version 1.0-c12.5+5
```

Local logging: Most logs within Cumulus Linux are sent to files in the `/var/log` directory. Most relevant information is placed within the `/var/log/syslog` file. For more information on specific log files, see [Troubleshooting Log Files](#) (see page 452).

Export logging: To send `syslog` files to an external `syslog` server, add a rule specifying to copy all messages (`*.*`) to the IP address and switch port of your `syslog` server in the `rsyslog` configuration files as described below.

In the following example, `192.168.1.2` is the remote `syslog` server and `514` is the port number. For UDP-based `syslog`, use a single `@` before the IP address: `@192.168.1.2:514`. For TCP-based `syslog`, use two `@@` before the IP address: `@@192.168.1.2:514`.

1. Create a file called something like `/etc/rsyslog.d/90-remotesyslog.conf`. Make sure it starts with a number lower than 99 so that it executes before `99-syslog.conf`. Add content like the following:

```
## Copy all messages to the remote syslog server at 192.168.1.2 port
514
*.*                                         @192.168.1.2:514
```

2. Restart `rsyslog`.

```
service rsyslog restart
```



Starting with Cumulus Linux 2.5.4, all Cumulus Linux rules have been moved from `/etc/rsyslog.conf` into separate files in `/etc/rsyslog.d/`, which are called at the end of the `GLOBAL DIRECTIVES` section of `/etc/rsyslog.conf`. As a result, the `RULES` section at the end of `rsyslog.conf` is ignored because the messages have to be processed by the rules in `/etc/rsyslog.d` and then dropped by the last line in `/etc/rsyslog.d/99-syslog.conf`.



In the case of the `switchd` rules file, the file must be numbered lower than 25. For example, `13-switchd-remote.conf`.

If you need to send other log files (e.g. `switchd` logs) to a `syslog` server, configure a new file in `/etc/rsyslog.d`, as described above, and add lines similar to the following lines:

```
## Logging switchd messages to remote syslog server
$ModLoad imfile
$InputFileName /var/log/switchd.log
$InputFileStateFile logfile-log
$InputFileTag switchd:
$InputFileSeverity info
$InputFileFacility local7
$InputFilePollInterval 5
$InputRunFileMonitor

if $programname == 'switchd' then @192.168.1.2:514
```

Then restart `syslog`:

```
service rsyslog restart
```

In the above configuration, each setting is defined as follows:

Setting	Description
\$ModLoad imfile	Enables the <code>rsyslog</code> module to watch file contents.
\$InputFileName	The file to be sent to the <code>syslog</code> server. In this example, you are going to send changes made to <code>/var/log/switchd.log</code> to the <code>syslog</code> server.
\$InputFileStateFile	This is used by <code>rsyslog</code> to track state of the file being monitored. This must be unique for each file being monitored.
\$InputFileTag	Defines the <code>syslog</code> tag that will precede the <code>syslog</code> messages. In this example, all logs are prefaced with <code>switchd</code> .
\$InputFileSeverity	Defines the logging severity level sent to the <code>syslog</code> server.
\$InputFileFacility	Defines the logging format. <code>local7</code> is common.
\$InputFilePollInterval	Defines how frequently in seconds <code>rsyslog</code> looks for new information in the file. Lower values provide faster updates but create slightly more load on the CPU.
\$InputRunFileMonitor	Enables the file monitor module with the configured settings.

In most cases, the settings to customize include:

Setting	Description
\$InputFileName	The file to stream to the <code>syslog</code> server.
\$InputFileStateFile	A unique name for each file being watched.
\$InputFileTag	A prefix to the log message on the server.

Finally, the `if $programname` line is what sends the log files to the `syslog` server. It follows the same syntax as the `/var/log/syslog` file, where @ indicates UDP, 192.168.1.2 is the IP address of the `syslog` server, and 514 is the UDP port. The value `switchd` must match the value in `$InputFileTag`.

Next Steps

The links below discuss more specific monitoring topics.

Single User Mode - Boot Recovery

Use single user mode to assist in troubleshooting system boot issues or for password recovery. Entering single user mode is [platform-specific](#), so follow the appropriate steps for your x86, ARM or PowerPC switch.

Contents

(Click to expand)

- Contents (see page 420)
 - Entering Single User Mode on an x86 Switch (see page 420)
 - Entering Single User Mode on a PowerPC Switch (see page 423)
 - Entering Single User Mode on an ARM Switch (see page 424)

Entering Single User Mode on an x86 Switch

1. Boot the switch, as soon as you see the GRUB menu, use the ^ and v arrow keys to select the boot entry you wish to modify, then press e to edit the entry. Be careful to select the correct image slot, so that the password change is applied correctly to the slot you desire. The active slot is the first selected image when the GRUB menu appears.

```
|  
|  
|  
|  
|  
|  
|  
+-----+  
-----+  
  
      Use the ^ and v keys to select which entry is highlighted.  
      Press enter to boot the selected OS, 'e' to edit the  
      commands  
      before booting or 'c' for a command-line.
```

2. After pressing *e*, a menu similar to the following should appear:

```
GNU GRUB  version 1.99-27+deb7u2  
  
+-----+  
-----+  
      | setparams 'Cumulus Linux 2.5.5-4cd66d9-201512071810-build - slot  
1'      |  
  
      |  
      |  
      | insmod  
gzio  
      | insmod  
part_gpt  
      | insmod  
ext2  
      | set root='(hd0,  
gpt4)'  
      | search --no-floppy --fs-uuid --set=root 23ea9c70-6d9f-414e-a26a-  
c501608\ |
```

```
|  
d3c3a  
|  
| echo 'Loading Linux  
...'  
| linux /cl-vmlinuz-3.2.68-6-slot-1 root=UUID=07197d9c-7dd7-407a-8cbc-  
4ff\ |  
| 1084b6337 console=ttyS1,115200n8 cl_platform=dell_s3000_c2338 quiet  
act\ |  
|  
ive=1  
|v  
  
-----  
----+  
  
Minimum Emacs-like screen editing is supported. TAB lists  
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for  
a command-line or ESC to discard edits and return to the GRUB  
menu.
```

3. Scroll down to the line that starts with "linux" and add *init=/bin/bash* to the end of the line. This allows the system to boot into single user mode.

```
GNU GRUB  version 1.99-27+deb7u2  
  
-----  
----+  
  
|  
|^  
| insmod  
gzio  
| insmod  
part_gpt  
| insmod  
ext2  
| set root='(hd0,  
gpt4)'  
| search --no-floppy --fs-uuid --set=root 23ea9c70-6d9f-414e-a26a-  
c501608\ |  
|  
d3c3a
```

```

| 
| echo 'Loading Linux
...
| linux /cl-vmlinuz-3.2.68-6-slot-1 root=UUID=07197d9c-7dd7-407a-8cbc-
4ff\ |
| 1084b6337 console=ttyS1,115200n8 cl_platform=dell_s3000_c2338 quiet
act\ |
| iive=1 init=/bin
/bash
| echo 'Loading initial ramdisk
...
| v

+-----+
-----+


Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
a command-line or ESC to discard edits and return to the GRUB
menu.

```

4. Press ctrl-x to reboot.
5. After the system reboots, re-mount the partition as read/write and set a new password.

```

# mount -o remount,rw /
# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully

```

6. Reboot the system:

```

# sync
# reboot -f
Restarting the system.

```

Entering Single User Mode on a PowerPC Switch

1. From the console, boot the switch, interrupting the U-Boot countdown to enter the U-Boot prompt. Enter the following:

```
=> setenv lbootargs init=/bin/bash  
=> boot
```

2. After the system boots, the shell command prompt appears. Set the root password:

```
# passwd  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully
```

3. Reboot the system.

```
cumulus@switch:~$ sudo sync  
cumulus@switch:~$ sudo reboot -f  
Restarting the system.
```

Entering Single User Mode on an ARM Switch

1. From the console, boot the switch, interrupting the U-Boot countdown to enter the U-Boot prompt. Enter the following:

```
=> setenv bootargs single  
=> boot
```

2. After the system boots, the shell command prompt appears. In this mode, you can change the root password or test a boot service that is hanging the boot process.

```
Welcome to rescu  
root@cumulus:~# passwd  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully
```

3. Reboot the system.

```
root@cumulus:~# sync  
root@cumulus:~# reboot -f  
Restarting the system.
```

Using netshow to Troubleshoot Your Network Configuration

`netshow` is a tool in Cumulus Linux that quickly returns a lot of information about your network configuration. It's a tool designed by network operators for network troubleshooters since existing command line tools have too many options. `netshow` addresses this by leveraging the network troubleshooting experience from a wide group of troubleshooters and boiling it down to just a few important options. `netshow` quickly aggregates basic network information on Linux devices with numerous interfaces. `netshow` intelligently informs the administrator what network type an interface belongs to, and shows the most relevant information to a network administrator.

`netshow` can be used on any distribution of Linux, not just Cumulus Linux.

Installing netshow

Starting with Cumulus Linux 2.5.5, `netshow` is included in the main repository for Cumulus Linux. However, it is not installed by default if you upgraded to this version using `apt-get dist-upgrade`. You install `netshow` in Cumulus Linux in one of two ways:

- By doing a [binary image install](#) (see page 18) of Cumulus Linux using `cl-img-install`
- Install the `netshow` package using `apt-get install netshow`

Installing netshow on a Linux Server or in OpenStack

To install `netshow` on a Linux server, run:

```
pip install netshow-linux-lib
```



Debian and Red Hat packages will be available in the near future.

Using netshow

Running `netshow` with no arguments displays all available command line arguments usable by `netshow`. (Running `netshow --help` gives you the same information.) The output looks like this:

```
cumulus@leaf1$ netshow
Usage:
  netshow system [--json | -j ]
  netshow counters [errors] [all] [--json | -j | -l | --legend ]
  netshow lldp [--json | -j | -l | --legend ]
  netshow interface [<iface>] [all] [--mac | -m ] [--oneline | -1 | --
json | -j | -l | --legend ]
  netshow access [all] [--mac | -m ] [--oneline | -1 | --json | -j | -l
```

```

| --legend ]
    netshow bridges [all] [--mac | -m ] [--oneline | -1 | --json | -j | -l
| --legend ]
    netshow bonds [all] [--mac | -m ] [--oneline | -1 | --json | -j | -l |
--legend ]
    netshow bondmems [all] [--mac | -m ] [--oneline | -1 | --json | -j | -l |
| --legend ]
    netshow mgmt [all] [--mac | -m ] [--oneline | -1 | --json | -j | -l |
--legend ]
    netshow 12 [all] [--mac | -m ] [--oneline | -1 | --json | -j | -l | --
legend ]
    netshow 13 [all] [--mac | -m ] [--oneline | -1 | --json | -j | -l | --
legend ]
    netshow trunks [all] [--mac | -m ] [--oneline | -1 | --json | -j | -l
| --legend ]
    netshow (--version | -V)

```

Help:

* default is to show interfaces only in the UP state.	
counters	summary of physical port counters.
interface	summary info of all interfaces
access	summary of physical ports with 12 or 13 config
bonds	summary of bonds
bondmems	summary of bond members
bridges	summary of ports with bridge members
mgmt	summary of mgmt ports
13	summary of ports with an IP.
12	summary of access, trunk and bridge interfaces
phy	summary of physical ports
trunks	summary of trunk interfaces
lldp	physical device neighbor information
interface <iface>	list summary of a single interface
system	system information

Options:

all	show all ports include those are down or admin down
--mac	show interface MAC in output
--version	netshow software version
--oneline	output each entry on one line
-1	alias for --oneline
--json	print output in json
-l	alias for --legend
--legend	print legend key explaining abbreviations

cumulus@leaf1\$

A Linux administrator can quickly see the few options available with the tool. One core tenet of `netshow` is for it to have a small number of command options. `netshow` is not designed to solve your network problem, but to help answer this simple question: "What is the basic network setup of my Linux device?" By helping to answer that question, a Linux administrator can spend more time troubleshooting the specific network problem instead of spending most of their time understanding the basic network state.

Originally developed for Cumulus Linux, `netshow` works on Debian-based servers and switches and Red Hat-based Linux systems.

`netshow` is designed by network operators, which has rarely occurred in the networking industry, where most command troubleshooting tools are designed by developers and are most useful in the network application development process.

Showing Interfaces

To show all available interfaces that are physically UP, run `netshow interface`:

```
cumulus@leaf1$ netshow interface
-----
To view the legend, rerun "netshow" cmd with the "--legend" option
-----
      Name      Speed       MTU     Mode      Summary
-----  -----
UP    eth0      1G        1500   Mgmt      IP: 192.168.0.12/24(DHCP)
UP    lo        N/A       16436   Mgmt      IP: 127.0.0.1/8, ::1/128
cumulus@leaf1$
```

Whereas `netshow interface all` displays every interface regardless of state:

```
cumulus@leaf1$ netshow interface all
      Name      Speed       Mtu     Mode      Summary
-----  -----
UP    lo        N/A       16436  Loopback  IP: 127.0.0.1/8, ::1/128
UP    eth0      1G        1500   Mgmt      IP: 192.168.0.11/24 (DHCP)
ADMDN swp1s0   10G(4x10)  1500   Unknwn
ADMDN swp1s1   10G(4x10)  1500   Unknwn
ADMDN swp1s2   10G(4x10)  1500   Unknwn
ADMDN swp1s3   10G(4x10)  1500   Unknwn
ADMDN swp2     40G(QSFP)  1500   Unknwn
ADMDN swp3     40G(QSFP)  1500   Unknwn
ADMDN swp4     40G(QSFP)  1500   Unknwn
ADMDN swp5     40G(QSFP)  1500   Unknwn
ADMDN swp6     40G(QSFP)  1500   Unknwn
ADMDN swp7     40G(QSFP)  1500   Unknwn
```

ADMDN	swp8	40G(QSFP)	1500	Unknwn
ADMDN	swp9	40G(QSFP)	1500	Unknwn
ADMDN	swp10	40G(QSFP)	1500	Unknwn
ADMDN	swp11	40G(QSFP)	1500	Unknwn
ADMDN	swp12	40G(QSFP)	1500	Unknwn
ADMDN	swp13	40G(QSFP)	1500	Unknwn
ADMDN	swp14	40G(QSFP)	1500	Unknwn
ADMDN	swp15	40G(QSFP)	1500	Unknwn
ADMDN	swp16	40G(QSFP)	1500	Unknwn
ADMDN	swp17	40G(QSFP)	1500	Unknwn
ADMDN	swp18	40G(QSFP)	1500	Unknwn
ADMDN	swp19	40G(QSFP)	1500	Unknwn
ADMDN	swp20	40G(QSFP)	1500	Unknwn
ADMDN	swp21	40G(QSFP)	1500	Unknwn
ADMDN	swp22	40G(QSFP)	1500	Unknwn
ADMDN	swp23	40G(QSFP)	1500	Unknwn
ADMDN	swp24	40G(QSFP)	1500	Unknwn
ADMDN	swp25	40G(QSFP)	1500	Unknwn
ADMDN	swp26	40G(QSFP)	1500	Unknwn
ADMDN	swp27	40G(QSFP)	1500	Unknwn
ADMDN	swp28	40G(QSFP)	1500	Unknwn
ADMDN	swp29	40G(QSFP)	1500	Unknwn
ADMDN	swp30	40G(QSFP)	1500	Unknwn
ADMDN	swp31	40G(QSFP)	1500	Unknwn
ADMDN	swp32s0	10G(4x10)	1500	Unknwn
ADMDN	swp32s1	10G(4x10)	1500	Unknwn
ADMDN	swp32s2	10G(4x10)	1500	Unknwn
ADMDN	swp32s3	10G(4x10)	1500	Unknwn

You can get information about the switch itself by running `netshow system`:

```
cumulus@leaf1$ netshow system

Quanta QuantaMesh BMS T1048-LB9
Cumulus Version 2.5.4
Build: 2.5.4-ecb2027-201510091646-build

Chipset: Broadcom Firebolt3 BCM56538

Port Config: 48x1G-T and 4x10G-SFP+

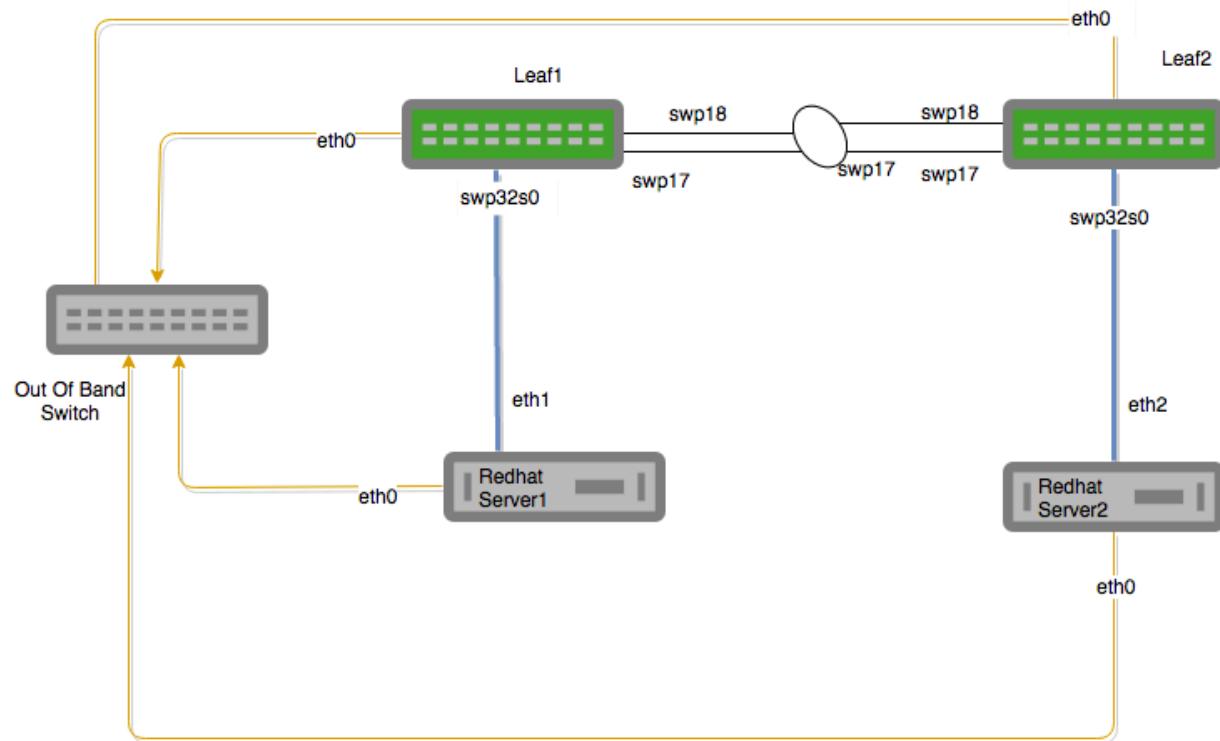
CPU: (ppc) Freescale MPC8541 e500 825MHz
```

UpTime: 20:01:17

cumulus@leaf1\$

Troubleshooting Example: OpenStack

Looking at an OpenStack Environment, here is the physical diagram:



For server2, netshow can help us see the OpenStack network configuration. The netshow output below shows an summary of a Kilo-based OpenStack server running 3 tenants.

```

[root@server2 ~]# netshow int
-----
To view the legend, rerun "netshow" cmd with the "--legend" option
-----
          Name      Speed     MTU     Mode      Summary
-----  -----
UP    brq0b6f10c7-42   N/A     1500  Bridge/L2  802.1q Tag: 141
                                         STP: Disabled
                                         Untagged Members:
                                         tap079cf993-c7
                                         Tagged Members: eth1.141

```

UP	brq8cdc0589-9b	N/A	1500	Bridge/L2	802.1q Tag: 155 STP: Disabled Untagged Members:
	tap5353b20a-68				Tagged Members: eth1.155
UP	brq8ff99102-29	N/A	1500	Bridge/L2	802.1q Tag: 168 STP: Disabled Untagged Members:
	tapfc2203e4-5b				Tagged Members: eth1.168
UP	eth0	N/A	1500	Interface/L3	IP: 192.168.0.105/24
UP	eth1	N/A	1500	IntTypeUnknown	
UP	eth1	N/A	1500	Trunk/L2	Bridge Membership: Tagged: brq0b6f10c7-42
	(141), brq8cdc0589-9b(155), brq8ff99102-29(168)				
UP	lo	N/A	65536	Loopback	IP: 127.0.0.1/8, ::1/128
UP	tap079cf993-c7	10M	1500	Access/L2	Untagged: brq0b6f10c7-42
UP	tap5353b20a-68	10M	1500	Access/L2	Untagged: brq8cdc0589-9b
UP	tapfc2203e4-5b	10M	1500	Access/L2	Untagged: brq8ff99102-29

OpenStack interface numbering is not the easiest read, but here `netshow` can quickly show you:

- A list of all the interfaces in admin UP state and carrier UP state
- 3 bridges
- That STP is disabled for all the bridges
- An uplink trunk interface with 3 VLANs configured on it
- Many tap interfaces, most likely the virtual machines

This output took about 5 seconds to get and another 1 minute to analyze. To get this same level of understanding using traditional tools such as:

- `ip link show`
- `brctl show`
- `ip addr show`

... could take about 10 minutes. This is a significant improvement in productivity!

`netshow` uses a plugin architecture and can be easily expanded. An OpenStack interface discovery module is currently in development. If `netshow` is run on a hypervisor with OpenStack Keystone login environment variables like `os_TENANT_NAME`, `netshow` should show the above output with a better interface discovery state, where `netshow` collects from OpenStack information from `libvirt`, `nova` and `neutron` to overlay the virtual machine and tenant subnet information over the interface kernel state information.

Interface discovery is one of the most powerful features of `netshow`. The ability to expand its interface discovery capabilities further simplifies understanding basic network troubleshooting, making the Linux administrator more productive and improving time to resolution while investigating network problems.

Other Useful netshow Features

netshow uses the `python network-docopt` package. This is inspired by `docopt` and provides the ability to specify partial commands, without tab completion and running the complete option. For example:

```
netshow int runs netshow interface  
netshow sys runs netshow system
```

netshow will eventually support interface name autocompletion. In the near future, if you run `netshow int tap123` and there is only one interface starting with `tap123`, netshow will autocomplete the command option with the full interface.

Contributions Welcome!

netshow is an open source project licensed under GPLv2. To contribute please contact Cumulus Networks through the [Cumulus Community Forum](#) or the [Netshow Linux Provider Github Repository Home](#). You can find developer documentation at [netshow.readthedocs.org](#). The documentation is still under development.

Monitoring Interfaces and Transceivers Using ethtool

The `ethtool` command enables you to query or control the network driver and hardware settings. It takes the device name (like `swp1`) as an argument. When the device name is the only argument to `ethtool`, it prints the current settings of the network device. See `man ethtool(8)` for details. Not all options are currently supported on switch port interfaces.

Contents

(Click to expand)

- Contents (see page 431)
- Commands (see page 431)
- Monitoring Interface Status Using ethtool (see page 431)
 - Viewing and Clearing Interface Counters (see page 433)
- Monitoring Switch Port SFP/QSFP Hardware Information Using ethtool (see page 433)

Commands

- cl-netstat
- ethtool

Monitoring Interface Status Using ethtool

To check the status of an interface using ethtool:

```
cumulus@switch:~$ ethtool swp1  
Settings for swp1:  
Supported ports: [ FIBRE ]
```

```
Supported link modes:  1000baseT/Full
                           10000baseT/Full
Supported pause frame use: No
Supports auto-negotiation: No
Advertised link modes:  1000baseT/Full
Advertised pause frame use: No
Advertised auto-negotiation: No
Speed: 10000Mb/s
Duplex: Full
Port: FIBRE
PHYAD: 0
Transceiver: external
Auto-negotiation: off
Current message level: 0x00000000 (0)

Link detected: yes
```

To query interface statistics:

```
cumulus@switch:~$ sudo ethtool -S swp1
NIC statistics:
    HwIfInOctets: 1435339
    HwIfInUcastPkts: 11795
    HwIfInBcastPkts: 3
    HwIfInMcastPkts: 4578
    HwIfOutOctets: 14866246
    HwIfOutUcastPkts: 11791
    HwIfOutMcastPkts: 136493
    HwIfOutBcastPkts: 0
    HwIfInDiscards: 0
    HwIfInL3Drops: 0
    HwIfInBufferDrops: 0
    HwIfInAclDrops: 28
    HwIfInDot3LengthErrors: 0
    HwIfInErrors: 0
    SoftInErrors: 0
    SoftInDrops: 0
    SoftInFrameErrors: 0
    HwIfOutDiscards: 0
    HwIfOutErrors: 0
    HwIfOutQDrops: 0
    HwIfOutNonQDrops: 0
    SoftOutErrors: 0
```

```
SoftOutDrops: 0
SoftOutTx_fifo_full: 0
HwIfOutQLen: 0
```

Viewing and Clearing Interface Counters

Interface counters contain information about an interface. You can view this information when you run `c1-netstat`, `ifconfig`, or `cat /proc/net/dev`. You can also use `c1-netstat` to save or clear this information:

```
cumulus@switch:~# sudo c1-netstat
Kernel Interface table
Iface      MTU Met          RX_OK RX_ERR RX_DRP RX_OVR          TX_OK TX_ERR
TX_DRP TX_OVR   Flg
-----
eth0      1500 0            611   0     0     0           487   0
0          0    BMRU
lo       16436 0            0     0     0     0           0     0
0          0    LRU
swp1      1500 0            0     0     0     0           0     0
0          0    BMU

cumulus@switch:~# sudo :~# c1-netstat -c
Cleared counters
```

Option	Description
-c	Copies and clears statistics. It does not clear counters in the kernel or hardware.
-d	Deletes saved statistics, either the <code>uid</code> or the specified tag.
-D	Deletes all saved statistics.
-l	Lists saved tags.
-r	Displays raw statistics (unmodified output of <code>c1-netstat</code>).
-t <tag name>	Saves statistics with <tag name>.
-v	Prints <code>c1-netstat</code> version and exits.

Monitoring Switch Port SFP/QSFP Hardware Information Using ethtool

To see hardware capabilities and measurement information on the SFP or QSFP module installed in a particular port, use the `ethtool -m` command. If the SFP/QSFP supports Digital Optical Monitoring (that is, the optical diagnostics support field in the output below is set to Yes), the optical power levels and thresholds are also printed below the standard hardware details.

In the sample output below, you can see that this module is a 1000BASE-SX short-range optical module, manufactured by JDSU, part number PLRXPL-VI-S24-22. The second half of the output displays the current readings of the Tx power levels (Laser output power) and Rx power (Receiver signal average optical power), temperature, voltage and alarm threshold settings.

```
cumulus@switch$ sudo ethtool -m swp3
      Identifier : 0x03 (SFP)
      Extended identifier : 0x04 (GBIC/SFP defined
by 2-wire interface ID)
      Connector : 0x07 (LC)
      Transceiver codes : 0x00 0x00 0x00 0x01
0x20 0x40 0x0c 0x05
      Transceiver type : Ethernet: 1000BASE-SX
      Transceiver type : FC: intermediate
      distance (I) :
      Transceiver type : FC: Shortwave laser w/o
OFC (SN)
      Transceiver type : FC: Multimode, 62.5um
(M6)
      Transceiver type : FC: Multimode, 50um (M5)
      Transceiver type : FC: 200 MBytes/sec
      Transceiver type : FC: 100 MBytes/sec
      Encoding : 0x01 (8B/10B)
      BR, Nominal : 2100MBd
      Rate identifier : 0x00 (unspecified)
      Length (SMF,km) : 0km
      Length (SMF) : 0m
      Length (50um) : 300m
      Length (62.5um) : 150m
      Length (Copper) : 0m
      Length (OM3) : 0m
      Laser wavelength : 850nm
      Vendor name : JDSU
      Vendor OUI : 00:01:9c
      Vendor PN : PLRXPL-VI-S24-22
      Vendor rev : 1
      Optical diagnostics support : Yes
      Laser bias current : 21.348 mA
      Laser output power : 0.3186 mW / -4.97 dBm
```

```

Receiver signal average optical power      : 0.3195 mW / -4.96 dBm
Module temperature                         : 41.70 degrees C /
107.05 degrees F
    Module voltage                          : 3.2947 V
    Alarm/warning flags implemented        : Yes
    Laser bias current high alarm         : Off
    Laser bias current low alarm          : Off
    Laser bias current high warning       : Off
    Laser bias current low warning        : Off
    Laser output power high alarm        : Off
    Laser output power low alarm         : Off
    Laser output power high warning       : Off
    Laser output power low warning        : Off
    Module temperature high alarm         : Off
    Module temperature low alarm          : Off
    Module temperature high warning       : Off
    Module temperature low warning        : Off
    Module voltage high alarm             : Off
    Module voltage low alarm              : Off
    Module voltage high warning           : Off
    Module voltage low warning            : Off
    Laser rx power high alarm            : Off
    Laser rx power low alarm             : Off
    Laser rx power high warning          : Off
    Laser rx power low warning           : Off
    Laser bias current high alarm threshold : 10.000 mA
    Laser bias current low alarm threshold : 1.000 mA
    Laser bias current high warning threshold : 9.000 mA
    Laser bias current low warning threshold : 2.000 mA
    Laser output power high alarm threshold : 0.8000 mW / -0.97 dBm
    Laser output power low alarm threshold : 0.1000 mW / -10.00 dBm
    Laser output power high warning threshold : 0.6000 mW / -2.22 dBm
    Laser output power low warning threshold : 0.2000 mW / -6.99 dBm
    Module temperature high alarm threshold : 90.00 degrees C /
194.00 degrees F
    Module temperature low alarm threshold : -40.00 degrees C /
-40.00 degrees F
    Module temperature high warning threshold : 85.00 degrees C /
185.00 degrees F
    Module temperature low warning threshold : -40.00 degrees C /
-40.00 degrees F
    Module voltage high alarm threshold   : 4.0000 V
    Module voltage low alarm threshold    : 0.0000 V
    Module voltage high warning threshold : 3.6450 V
    Module voltage low warning threshold : 2.9550 V

```

Laser rx power high alarm threshold	: 1.6000 mW / 2.04 dBm
Laser rx power low alarm threshold	: 0.0100 mW / -20.00 dBm
Laser rx power high warning threshold	: 1.0000 mW / 0.00 dBm
Laser rx power low warning threshold	: 0.0200 mW / -16.99 dBm

Resource Diagnostics Using cl-resource-query

You can use `cl-resource-query` to retrieve information about host entries, MAC entries, L2 and L3 routes, and ECMPs (equal-cost multi-path routes, see [Load Balancing \(see page 344\)](#)) that are in use. This is especially useful because Cumulus Linux syncs routes between the kernel and the switching silicon. If the required resource pools in hardware fill up, new kernel routes can cause existing routes to move from being fully allocated to being partially allocated.

In order to avoid this, routes in the hardware should be monitored and kept below the ASIC limits. For example, on systems with a Trident II chipset, the limits are as follows:

```
routes: 8092 <<< if all routes are IPv6, or 16384 if all routes are IPv4
long mask routes 2048 <<< these are routes with a mask longer than the
route mask limit
route mask limit 64
host_routes: 8192
ecmp_nhs: 16346
ecmp_nhs_per_route: 52
```

This translates to about 314 routes with ECMP next hops, if every route has the maximum ECMP NHs.

For systems with a Trident+ chipset, the limits are as follows:

```
routes: 16384 <<< if all routes are IPv4
long mask routes 256 <<< these are routes with a mask longer than the
route mask limit
route mask limit 64
host_routes: 8192
ecmp_nhs: 4044
ecmp_nhs_per_route: 52
```

This translates to about 77 routes with ECMP next hops, if every route has the maximum ECMP NHs.

You can monitor this in Cumulus Linux with the `cl-resource-query` command. Results vary between switches running on Trident+ and Trident II chipsets.

`cl-resource-query` results for a Trident II switch:

```
cumulus@switch:~$ sudo cl-resource-query
Host entries:           1,   0% of maximum value  8192 <<< this is
the default software-imposed limit, 50% of the hardware limit
IPv4 neighbors:          1           <<< these are counts of the number
of valid entries in the table
IPv6 neighbors:          0
IPv4 entries:            13,   0% of maximum value 32668
IPv6 entries:            18,   0% of maximum value 16384
IPv4 Routes:             13
IPv6 Routes:             18
Total Routes:            31,   0% of maximum value 32768
ECMP nexthops:           0,   0% of maximum value 16346
MAC entries:             12,   0% of maximum value 32768
```

cl-resource-query results for a Trident+ switch:

```
cumulus@switch:~$ sudo cl-resource-query
Host entries:           6,   0% of maximum value  4096 <<< same as
above
IPv4 neighbors:          6
IPv6 neighbors:          0
IPv4/IPv6 entries:       33,   0% of maximum value 16284
Long IPv6 entries:       0,   0% of maximum value    256
IPv4 Routes:              29
IPv6 Routes:              2
Total Routes:             31,   0% of maximum value 32768
ECMP nexthops:            0,   0% of maximum value  4041
MAC entries:              0,   0% of maximum value 131072
```

Monitoring System Hardware

You monitor system hardware in these ways, using:

- decode-syseeprom
- sensors
- smond
- Net-SNMP
- watchdog

Contents

(Click to expand)

- Contents (see page 438)
- Commands (see page 438)
- Monitoring Hardware Using decode-syseeprom (see page 438)
 - Command Options (see page 439)
 - Related Commands (see page 439)
- Monitoring Hardware Using sensors (see page 439)
 - Command Options (see page 440)
- Monitoring Switch Hardware Using SNMP (see page 441)
- Monitoring System Units Using smond (see page 441)
 - Command Options (see page 442)
- Keeping the Switch Alive Using the Hardware Watchdog (see page 442)
- Configuration Files (see page 442)
- Useful Links (see page 443)

Commands

- decode-syseeprom
- dmidecode
- lshw
- sensors
- smond

Monitoring Hardware Using decode-syseeprom

The decode-syseeprom command enables you to retrieve information about the switch's EEPROM. If the EEPROM is writable, you can set values on the EEPROM.

For example:

```
cumulus@switch:~$ decode-syseeprom
TlvInfo Header:
  Id String:      TlvInfo
  Version:        1
  Total Length:  114
  TLV Name          Code Len Value
  -----
Product Name        0x21    4  4804
Part Number        0x22   14  R0596-F0009-00
Device Version     0x26    1  2
```

Serial Number	0x23	19 D1012023918PE000012
Manufacture Date	0x25	19 10/09/2013 20:39:02
Base MAC Address	0x24	6 00:E0:EC:25:7B:D0
MAC Addresses	0x2A	2 53
Vendor Name	0x2D	17 Penguin Computing
Label Revision	0x27	4 4804
Manufacture Country	0x2C	2 CN
CRC-32	0xFE	4 0x96543BC5
(checksum valid)		

Command Options

Usage: /usr/cumulus/bin/decode-syseeprom [-a][-r][-s [args]][-t]

Option	Description
-h, -help	Displays the help message and exits.
-a	Prints the base MAC address for switch interfaces.
-r	Prints the number of MACs allocated for switch interfaces.
-s	Sets the EEPROM content if the EEPROM is writable. <code>args</code> can be supplied in command line in a comma separated list of the form ' <code><field>=<value></code> , ...'. '.', '=' and '!' are illegal characters in field names and values. Fields that are not specified will default to their current values. If <code>args</code> are supplied in the command line, they will be written without confirmation. If <code>args</code> is empty, the values will be prompted interactively.
-t TARGET	Selects the target EEPROM (<code>board</code> , <code>psu2</code> , <code>psu1</code>) for the read or write operation; default is <code>board</code> .
-e, -serial	Prints the device serial number.

Related Commands

You can also use the `dmidecode` command to retrieve hardware configuration information that's been populated in the BIOS.

You can use `apt-get` to install the `lshw` program on the switch, which also retrieves hardware configuration information.

Monitoring Hardware Using sensors

The `sensors` command provides a method for monitoring the health of your switch hardware, such as power, temperature and fan speeds. This command executes `lm-sensors`.

For example:

```
cumulus@switch:~$ sensors
tmp75-i2c-6-48
Adapter: i2c-1-mux (chan_id 0)
temp1:      +39.0 C  (high = +75.0 C, hyst = +25.0 C)

tmp75-i2c-6-49
Adapter: i2c-1-mux (chan_id 0)
temp1:      +35.5 C  (high = +75.0 C, hyst = +25.0 C)

ltc4215-i2c-7-40
Adapter: i2c-1-mux (chan_id 1)
in1:      +11.87 V
in2:      +11.98 V
power1:    12.98 W
curr1:    +1.09 A

max6651-i2c-8-48
Adapter: i2c-1-mux (chan_id 2)
fan1:      13320 RPM  (div = 1)
fan2:      13560 RPM
```



Output from the `sensors` command varies depending upon the switch hardware you use, as each platform ships with a different type and number of sensors.

Command Options

Usage: `sensors [OPTION]... [CHIP]...`

Option	Description
<code>-c, --config-file</code>	Specify a config file; use <code>-</code> after <code>-c</code> to read the config file from <code>stdin</code> ; by default, <code>sensors</code> references the configuration file in <code>/etc/sensors.d/</code> .
<code>-s, --set</code>	Executes set statements in the config file (root only); <code>sensors -s</code> is run once at boot time and applies all the settings to the boot drivers.
<code>-f, --fahrenheits</code>	Show temperatures in degrees Fahrenheit.
<code>-A, --no-adapter</code>	Do not show the adapter for each chip.

--bus-list	Generate bus statements for <code>sensors.conf</code> .
------------	---

If [CHIP] is not specified in the command, all chip info will be printed. Example chip names include:

- lm78-i2c-0-2d *-i2c-0-2d
- lm78-i2c-0-* *-i2c-0-*
- lm78-i2c-*-2d *-i2c-*-2d
- lm78-i2c-*-* *-i2c-*-*
- lm78-isa-0290 *-isa-0290
- lm78-isa-* *-isa-*
- lm78-*

Monitoring Switch Hardware Using SNMP

The Net-SNMP documentation has been moved to a new chapter, [available here](#).

Monitoring System Units Using smond

The `smond` daemon monitors system units like power supply and fan, updates their corresponding LEDs, and logs the change in the state. Changes in system unit state are detected via the `cp1d` registers. `smond` utilizes these registers to read all sources, which impacts the health of the system unit, determines the unit's health, and updates the system LEDs.

Use `smonctl` to display sensor information for the various system units:

```
cumulus@switch:~$ smonctl
Board : OK
Fan   : OK
PSU1  : OK
PSU2  : BAD
Temp1  (Networking ASIC Die Temp Sensor ) : OK
Temp10 (Right side of the board ) : OK
Temp2  (Near the CPU (Right) ) : OK
Temp3  (Top right corner ) : OK
Temp4  (Right side of Networking ASIC ) : OK
Temp5  (Middle of the board ) : OK
Temp6  (P2020 CPU die sensor ) : OK
Temp7  (Left side of the board ) : OK
Temp8  (Left side of the board ) : OK
Temp9  (Right side of the board ) : OK
```

Command Options

Usage: `smonctl [OPTION]... [CHIP]...`

Option	Description
<code>-s SENSOR, --sensor SENSOR</code>	Displays data for the specified sensor.
<code>-v, --verbose</code>	Displays detailed hardware sensors data.

For more information, read `man smond` and `man smonctl`.

Keeping the Switch Alive Using the Hardware Watchdog

Cumulus Linux includes a simplified version of the `wd_keepalive(8)` daemon from the standard Debian package `watchdog`. `wd_keepalive` writes to a file called `/dev/watchdog` periodically to keep the switch from resetting, at least once per minute. Each write delays the reboot time by another minute. After one minute of inactivity where `wd_keepalive` doesn't write to `/dev/watchdog`, the switch resets itself.

The watchdog is enabled by default on QuantaMesh BMS T1048-LB9 switches only; you must enable the watchdog on all other switch platforms. When enabled, it starts when you boot the switch, before `switchd` starts.

To enable the hardware watchdog, edit the `/etc/watchdog.d/<your_platform>` file and set `run_watchdog` to `1`:

```
run_watchdog=1
```

To disable the watchdog, edit the `/etc/watchdog.d/<your_platform>` file and set `run_watchdog` to `0`:

```
run_watchdog=0
```

Then stop the daemon:

```
cumulus@switch:~$ sudo service wd_keepalive stop
```

You can modify the settings for the watchdog — like the timeout setting and scheduler priority — in its configuration file, `/etc/watchdog.conf`.

Configuration Files

- `/etc/cumulus/switchd.conf`

- /etc/cumulus/sysledcontrol.conf
- /etc/sensors.d/<switch>.conf - sensor configuration file (do **not** edit it!)
- /etc/watchdog.conf

Useful Links

- <http://packages.debian.org/search?keywords=lshw>
- <http://lm-sensors.org>
- Net-SNMP tutorials

Monitoring System Statistics and Network Traffic with sFlow

sFlow is a monitoring protocol that samples network packets, application operations, and system counters. sFlow enables you to monitor your network traffic as well as your switch state and performance metrics. An outside server, known as an *sFlow collector*, is required to collect and analyze this data.

`hsflowd` is the daemon that samples and sends sFlow data to configured collectors. `hsflowd` is not included in the base Cumulus Linux installation. After installation, `hsflowd` will automatically start when the switch boots up.

Contents

(Click to expand)

- Contents (see page 443)
- Installing `hsflowd` (see page 443)
- Configuring sFlow (see page 443)
 - Configuring sFlow via DNS-SD (see page 444)
 - Manually Configuring `/etc/hsflowd.conf` (see page 444)
- Configuring sFlow Visualization Tools (see page 445)
- Configuration Files (see page 445)
- Useful Links (see page 445)

Installing `hsflowd`

To download and install the `hsflowd` package, use `apt-get`:

```
cumulus@switch:~$ sudo apt-get update
cumulus@switch:~$ sudo apt-get install -y hsflowd
```

Configuring sFlow

You can configure `hsflowd` to send to the designated collectors via two methods:

- DNS service discovery (DNS-SD)
- Manually configuring `/etc/hsflowd.conf`

Configuring sFlow via DNS-SD

With this method, you need to configure your DNS zone to advertise the collectors and polling information to all interested clients. Add the following content to the zone file on your DNS server:

```
_sflow._udp SRV 0 0 6343 collector1
_sflow._udp SRV 0 0 6344 collector2
_sflow._udp TXT (
  "txtvers=1"
  "sampling.1G=2048"
  "sampling.10G=4096"
  "sampling.40G=8192"
  "polling=20"
)
```

The above snippet instructs `hsflowd` to send sFlow data to collector1 on port 6343 and to collector2 on port 6344. `hsflowd` will poll counters every 20 seconds and sample 1 out of every 2048 packets.

After the initial configuration is ready, bring up the sFlow daemon by running:

```
cumulus@switch:~$ sudo service hsflowd start
```

No additional configuration is required in `/etc/hsflowd.conf`.

Manually Configuring /etc/hsflowd.conf

With this method you will set up the collectors and variables on each switch.

Edit `/etc/hsflowd.conf` and change `DNSSD = on` to `DNSSD = off`:

```
DNSSD = off
```

Then set up your collectors and sampling rates in `/etc/hsflowd.conf`:

```
# Manual Configuration (requires DNSSD=off above)
#####
#
# Typical configuration is to send every 30 seconds
polling = 20

sampling.1G=2048
sampling.10G=4096
```

```
sampling.40G=8192

collector {
    ip = 192.0.2.100
    udpport = 6343
}

collector {
    ip = 192.0.2.200
    udpport = 6344
}
```

This configuration polls the counters every 20 seconds, samples 1 of every 2048 packets and sends this information to a collector at 192.0.2.100 on port 6343 and to another collector at 192.0.2.200 on port 6344.



Some collectors require each source to transmit on a different port, others may listen on only one port. Please refer to the documentation for your collector for more information.

Configuring sFlow Visualization Tools

For information on configuring various sFlow visualization tools, read this [Help Center article](#).

Configuration Files

- /etc/hsflowd.conf

Useful Links

- [sFlow Collectors](#)
- [sFlow Wikipedia page](#)

Monitoring Virtual Device Counters

Cumulus Linux gathers statistics for VXLANS and VLANs using virtual device counters. These counters are supported on Trident II-based platforms only; see the [Cumulus Networks HCL](#) for a list of supported Trident II platforms.

You can retrieve the data from these counters using tools like `ip -s link show`, `ifconfig`, `/proc/net/dev`, or `netstat -i`.

Contents

(Click to expand)

- [Contents \(see page 445\)](#)

- Sample VXLAN Statistics (see page 446)
- Sample VLAN Statistics (see page 447)
 - For VLANs Using the non-VLAN-aware Bridge Driver (see page 447)
 - For VLANs Using the VLAN-aware Bridge Driver (see page 448)
- Configuring the Counters in switchd (see page 448)
 - Configuring the Poll Interval (see page 449)
 - Configuring Internal VLAN Statistics (see page 449)
 - Clearing Statistics (see page 449)
- Caveats and Errata (see page 449)

Sample VXLAN Statistics

VXLAN statistics are available as follows:

- Aggregate statistics are available per VNI; this includes access and network statistics.
- Network statistics are available for each VNI and displayed against the VXLAN device. This is independent of the VTEP used, so this is a summary of the VNI statistics across all tunnels.
- Access statistics are available per VLAN subinterface.

First, get interface information regarding the VXLAN bridge:

```
cumulus@switch:~$ brctl show br-vxln16757104
bridge name          bridge id      STP enabled    interfaces
-vxln16757104       8000.443839006988    no           swp2s0.6
                                         swp2s1.6
                                         swp2s2.6
                                         swp2s3.6
                                         vxln16757104
```

To get VNI statistics, run:

```
cumulus@switch:~$ ip -s link show br-vxln16757104
62: br-vxln16757104: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode DEFAULT
    link/ether 44:38:39:00:69:88 brd ff:ff:ff:ff:ff:ff
    RX: bytes   packets   errors   dropped overrun mcast
        10848      158       0        0        0        0
    TX: bytes   packets   errors   dropped carrier collsns
        27816      541       0        0        0        0
```

To get access statistics, run:

```
cumulus@switch:~$ ip -s link show swp2s0.6
63: swp2s0.6@swp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
    master br-vxln16757104 state UP mode DEFAULT
        link/ether 44:38:39:00:69:88 brd ff:ff:ff:ff:ff:ff
        RX: bytes   packets   errors   dropped overrun mcast
          2680       39        0        0        0        0
        TX: bytes   packets   errors   dropped carrier collsns
          7558      140        0        0        0        0
```

To get network statistics, run:

```
cumulus@switch:~$ ip -s link show vxln16757104
61: vxln16757104: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
    master br-vxln16757104 state UNKNOWN mode DEFAULT
        link/ether e2:37:47:db:f1:94 brd ff:ff:ff:ff:ff:ff
        RX: bytes   packets   errors   dropped overrun mcast
          0         0         0         0         0         0
        TX: bytes   packets   errors   dropped carrier collsns
          0         0         0         9         0         0
```

Sample VLAN Statistics

For VLANs Using the non-VLAN-aware Bridge Driver

In this case, each bridge is a single L2 broadcast domain and is associated with an internal VLAN. This internal VLAN's counters are displayed as bridge netdev stats.

```
cumulus@switch:~$ brctl show br0
bridge name     bridge id               STP enabled   interfaces
br0            8000.443839006989    yes           bond0.100
                                         swp2s2.100

cumulus@switch:~$ ip -s link show br0
42: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
mode DEFAULT
    link/ether 44:38:39:00:69:89 brd ff:ff:ff:ff:ff:ff
    RX: bytes   packets   errors   dropped overrun mcast
      23201498   227514     0        0        0        0
    TX: bytes   packets   errors   dropped carrier collsns
      18198262   178443     0        0        0        0
```

For VLANs Using the VLAN-aware Bridge Driver

For a bridge using the VLAN-aware driver (see page 208), the bridge is a just a container and each VLAN (VID /PVID) in the bridge is an independent L2 broadcast domain. As there is no netdev available to display these VLAN statistics, the `switchd` nodes are used instead:

```
cumulus@switch:~$ ifquery bridge
auto bridge
iface bridge inet static
  bridge-vlan-aware yes
  bridge-ports swp2s0 swp2s1
  bridge-stp on
  bridge-vids 2000-2002 4094
cumulus@switch:~$ ls /cumulus/switchd/run/stats/vlan/
2 2000 2001 2002 all
cumulus@switch:~$ cat /cumulus/switchd/run/stats/vlan/2000/aggregate
Vlan id : 2000
L3 Routed In Octets : -
L3 Routed In Packets : -
L3 Routed Out Octets : -
L3 Routed Out Packets : -
Total In Octets : 375
Total In Packets : 3
Total Out Octets : 387
Total Out Packets : 3
```

Configuring the Counters in switchd

These counters are enabled by default. To configure them, use `cl-cfg` and configure them as you would any other `switchd` parameter (see page 112). The `switchd` parameters are as follows:

- `stats.vlan.aggregate`, which controls the statistics available for each VLAN. Its value defaults to *BRIEF*.
- `stats.vxlan.aggregate`, which controls the statistics available for each VNI (access and network). Its value defaults to *DETAIL*.
- `stats.vxlan.member`, which controls the statistics available for each local/access port in a VXLAN bridge. Its value defaults to *BRIEF*.

The values for each parameter can be one of the following:

- NONE: This disables the counter.
- BRIEF: This provides tx/rx packet/byte counters for the associated parameter.
- DETAIL: This provides additional feature-specific counters. In the case of `stats.vxlan.aggregate`, DETAIL provides access vs. network statistics. For the other types, DETAIL has the same effect as BRIEF.



If you change one of these settings on the fly, the new configuration applies only to those VNIs or VLANs set up after the configuration changed; previously allocated counters remain as is.

Configuring the Poll Interval

The virtual device counters are polled periodically. This can be CPU intensive, so the interval is configurable in `switchd`, with a default of 2 seconds.

```
# Virtual devices hw-stat poll interval (in seconds)
#stats.vdev_hw_poll_interval = 2
```

Configuring Internal VLAN Statistics

For debugging purposes, you may need to access packet statistics associated with internal VLAN IDs. These statistics are hidden by default, but can be configured in `switchd`:

```
#stats.vlan.show_internal_vlans = FALSE
```

Clearing Statistics

Since `ethtool` is not supported for virtual devices, you cannot clear the statistics cache maintained by the kernel. You can clear the hardware statistics via `switchd`:

```
cumulus@switch:~$ sudo echo 1 > /cumulus/switchd/clear/stats/vlan
cumulus@switch:~$ sudo echo 1 > /cumulus/switchd/clear/stats/vxlan
cumulus@switch:~$
```

Caveats and Errata

- Currently the CPU port is internally added as a member of all VLANs. Because of this, packets sent to the CPU are counted against the corresponding VLAN's tx packets/bytes. There is no workaround.
- When checking the virtual counters for the bridge, the TX count is the number of packets destined to the CPU before any hardware policers take effect. For example, if 500 broadcast packets are sent into the bridge, the CPU is also sent 500 packets. These 500 packets are policed by the default ACLs in Cumulus Linux, so the CPU might receive fewer than the 500 packets if the incoming packet rate is too high. The TX counter for the bridge should be equal to $500 * (\text{number of ports in the bridge} - \text{incoming port} + \text{CPU port})$ or just $500 * \text{number of ports in the bridge}$.
- You cannot use `ethtool -S` for virtual devices. This is because the counters available via `netdev` are sufficient to display the vlan/vxlan counters currently supported in the hardware (only rx/tx packets/bytes are supported currently).

Understanding and Decoding the cl-support Output File

The cl-support command generates a tar archive of useful information for troubleshooting that can be auto-generated or manually created. To manually create it, run the cl-support command. The cl-support file is automatically generated when:

- There is a core file dump of any application (not specific to Cumulus Linux, but something all Linux distributions support)
- Memory usage surpasses 90% of the total system memory (memory usage > 90% for 1 cycle)
- The loadavg over 15 minutes has on average greater than 2 (loadavg (15min) > 2)

All of these conditions are triggered by jdoo, located at /etc/jdoo/jdoorc.

The Cumulus Networks support team may request you submit the output from cl-support to help with the investigation of issues you might experience with Cumulus Linux.

```
cumulus@switch:~$ sudo cl-support -h
Usage: cl-support [-h] [reason]...
Args:
[reason]: Optional reason to give for invoking cl-support.
          Saved into tarball's reason.txt file.
Options:
-h: Print this usage statement
```

Example output:

```
cumulus@switch:~$ ls /var/support
cl_support_switch_20141204_203833
```

(Click to expand)

- The cl-support command generates a tar archive of useful information for troubleshooting that can be auto-generated or manually created. To manually create it, run the cl-support command. The cl-support file is automatically generated when: (see page 450)
- Understanding the File Naming Scheme (see page 450)
- Decoding the Output (see page 451)

Understanding the File Naming Scheme

The cl-support command generates a file under /var/support with the following naming scheme. The following example describes the file called cl_support_switch_20141204_203833.tar.xz.

cl_support	switch	20141204	203833
------------	--------	----------	--------

This is always prepended to the <code>tar.gz</code> output.	This is the hostname of the switch where <code>cl-support</code> was executed.	The date in year, month, day; so 20141204 is December, 4th, 2014.	The time in hours, minutes, seconds; so 203833 is 20, 38, 33 (20:38:33) or the equivalent to 8:38:33 PM.
---	--	---	--

Decoding the Output

Decoding a `cl_support` file is a simple process performed using the `tar` command. The following example illustrates extracting the `cl_support` file:

```
tar -xf cl_support__switch_20141204_203834.tar.xz
```

The `-xf` options are defined here:

Option	Description
<code>-x</code>	Extracts to disk from the archive.
<code>-f</code>	Reads the archive from the specified file.

```
cumulus@switch:~$ ls -l cl_support__switch_20141204_203834/
-rwxr-xr-x 1 root root 7724 Jul 29 14:00 cl-support
-rw-r--r-- 1 root root 52 Jul 29 14:00 cmdline.args
drwxr-xr-x 2 root root 4096 Jul 29 14:00 core
drwxr-xr-x 64 root root 4096 Jul 29 13:51 etc
drwxr-xr-x 4 root root 4096 Jul 29 14:00 proc
drwxr-xr-x 2 root root 4096 Jul 29 14:01 support
drwxr-xr-x 3 root root 4096 Jul 29 14:00 sys
drwxr-xr-x 3 root root 4096 Aug  8 15:22 var
```

The `cl_support` file, when untarred, contains a `reason.txt` file. This file indicates what reason triggered the event. When contacting Cumulus Networks technical support, please attach the `cl-support` file if possible.

The directory contains the following elements:

Directory	Description
<code>cl-support</code>	This is a copy of the <code>cl-support</code> script that generated the <code>cl_support</code> file. It is copied so Cumulus Networks knows exactly which files were included and which weren't. This helps to fix future <code>cl-support</code> requests in the future.

Directory	Description
core	Contains the core files generated from the Cumulus Linux HAL (hardware abstraction layer) process, <code>switchd</code> .
etc	<code>etc</code> is the core system configuration directory. <code>c1-support</code> replicates the switch's <code>/etc</code> directory. <code>/etc</code> contains all the general Linux configuration files, as well as configurations for the system's network interfaces, <code>quagga</code> , <code>jdoe</code> , and other packages.
var/log	<code>/var</code> is the "variable" subdirectory, where programs record runtime information. System logging, user tracking, caches and other files that system programs create and monitor go into <code>/var</code> . <code>c1-support</code> includes only the <code>log</code> subdirectory of the <code>var</code> system-level directory and replicates the switch's <code>/var/log</code> directory. Most Cumulus Linux log files are located in this directory. Notable log files include <code>switchd.log</code> , <code>daemon.log</code> , <code>quagga</code> log files, and <code>syslog</code> . For more information, read this knowledge base article .
proc	<code>proc</code> (short for processes) provides system statistics through a directory-and-file interface. In Linux, <code>/proc</code> contains runtime system information (like system memory, devices mounted, and hardware configuration). <code>c1-support</code> simply replicates the switch's <code>/proc</code> directory to determine the current state of the system.
support	<code>support</code> is not a replica of the Linux file system like the other folders listed above. Instead, it is a set of files containing the output of commands from the command line. Examples include the output of <code>ps -aux</code> , <code>netstat -i</code> , and so forth — even the routing tables are included.

Here is more information on the file structure:

- [Troubleshooting the etc Directory \(see page 455\)](#) — In terms of sheer numbers of files, `/etc` contains the largest number of files to send to Cumulus Networks by far. However, log files could be significantly larger in file size.
- [Troubleshooting Log Files \(see page 452\)](#) — This guide highlights the most important log files to look at. Keep in mind, `c1-support` includes all of the log files.
- [Troubleshooting the support Directory \(see page 466\)](#) — This is an explanation of the `support` directory included in the `c1-support` output.

Troubleshooting Log Files

The only real unique entity for logging on Cumulus Linux compared to any other Linux distribution is `switchd.log`, which logs the HAL (hardware abstraction layer) from hardware like the Broadcom ASIC.

This guide on [NixCraft](#) is amazing for understanding how `/var/log` works. The green highlighted rows below are the most important logs and usually looked at first when debugging.

Log	Description	Why is this important?
	Information from the update-alternatives are logged into this log file.	

Log	Description	Why is this important?
/var/log/alternatives.log		
/var/log/apt	Information the <code>apt</code> utility can send logs here; for example, from <code>apt-get install</code> and <code>apt-get remove</code> .	
/var/log/audit/*	Contains log information stored by the Linux audit daemon, <code>audited</code> .	
/var/log/auth.log	<p>Authentication logs.</p> <p>Note that Cumulus Linux does not write to this log file; but because it's a standard file, Cumulus Linux creates it as a zero length file.</p>	
/var/log/autoprovision	Logs output generated by running the zero touch provisioning (see page 57) script.	
/var/log/boot.log	Contains information that is logged when the system boots.	
/var/log/btmp	<p>This file contains information about failed login attempts. Use the <code>last</code> command to view the <code>btmp</code> file. For example:</p> <pre data-bbox="437 1262 899 1294">last -f /var/log/btmp more</pre>	
/var/log/clagd.log	Logs status of the <code>clagd</code> service (see page 217).	
/var/log/cron.log	<p>Log file for cron jobs.</p> <p>Note that Cumulus Linux does not write to this log file; but because it's a standard file, Cumulus Linux creates it as a zero length file.</p>	
/var/log/daemon.log	<p>Contains information logged by the various background daemons that run on the system.</p> <p>Note that Cumulus Linux does not write to this log file; but because it's a standard file, Cumulus Linux creates it as a zero length file.</p>	
/var/log/debug	Debugging information.	

Log	Description	Why is this important?
	Note that Cumulus Linux does not write to this log file; but because it's a standard file, Cumulus Linux creates it as a zero length file.	
/var/log/dmesg	Contains kernel ring buffer information. When the system boots up, it prints number of messages on the screen that display information about the hardware devices that the kernel detects during boot process. These messages are available in the kernel ring buffer and whenever a new message arrives, the old message gets overwritten. You can also view the content of this file using the <code>dmesg</code> command.	<code>dmesg</code> is one of the few places to determine hardware errors.
/var/log/dpkg.log	Contains information that is logged when a package is installed or removed using the <code>dpkg</code> command.	
/var/log/faillog	Contains failed user login attempts. Use the <code>faillog</code> command to display the contents of this file.	
/var/log/fsck/*	The <code>fsck</code> utility is used to check and optionally repair one or more Linux filesystems.	
/var/log/jdoe.log	<code>jdoe</code> is a utility for managing and monitoring processes, files, directories and filesystems on a Unix system.	
/var/log/kern.log	Logs produced by the kernel and handled by <code>syslog</code> . Note that Cumulus Linux does not write to this log file; but because it's a standard file, Cumulus Linux creates it as a zero length file.	
/var/log/lastlog	Formats and prints the contents of the last login log file.	
/var/log/lpr.log	Printer logs. Note that Cumulus Linux does not write to this log file; but because it's a standard file, Cumulus Linux creates it as a zero length file.	
/var/log/mail.log	Mail server logs. Also includes <code>mail.err</code> , <code>mail.info</code> and <code>mail.warn</code> . Note that Cumulus Linux does not write to this log file; but because it's a standard file, Cumulus Linux creates it as a zero length file.	
/var/log/messages	General messages and system-related information. Note that Cumulus Linux does not write to this log file; but because it's a standard file, Cumulus Linux creates it as a zero length file.	
/var/log/news/*	The <code>news</code> command keeps you informed of news concerning the system.	

Log	Description	Why is this important?
	Note that Cumulus Linux does not write to this log file; but because it's a standard file, Cumulus Linux creates it as a zero length file.	
/var/log /ntpstats	Logs for network configuration protocol.	
/var/log /openvswitch /*	ovsdb-server logs.	
/var/log /quagga/*	Where Quagga logs to once enabled.	This is how Cumulus Networks troubleshoots routing. For example an md5 or mtu mismatch with OSPF.
/var/log /switchd.log	The HAL log for Cumulus Linux.	This is specific to Cumulus Linux. Any switchd crashes are logged here.
/var/log/syslog	The main system log, which logs everything except auth-related messages.	The primary log; it's easiest to grep this file to see what occurred during a problem.
/var/log/user.log	Note that Cumulus Linux does not write to this log file; but because it's a standard file, Cumulus Linux creates it as a zero length file.	
/var/log /watchdog	Hardware watchdog (see page) log files.	
/var/log/wtmp	Login records file.	

Troubleshooting the etc Directory

The [cl-support](#) (see page 449) script replicates the /etc directory.

Files that cl-support deliberately excludes are:

File	Description
/etc/nologin	<code>nologin</code> prevents unprivileged users from logging into the system.
/etc/alternatives	<code>update-alternatives</code> creates, removes, maintains and displays information about the symbolic links comprising the Debian alternatives system.

This is the alphabetical of the output from running `ls -l` on the `/etc` directory structure created by `c1-support`. The green highlighted rows are the ones Cumulus Networks finds most important when troubleshooting problems.

File	Description	Why is this important?
adduser.conf	The file <code>/etc/adduser.conf</code> contains defaults for the programs <code>adduser</code> , <code>addgroup</code> , <code>deluser</code> , and <code>delgroup</code> .	
adjtime	Corrects the time to synchronize the <code>system clock</code> .	
apt	<code>apt</code> (Advanced Package Tool) is the command-line tool for handling packages . This folder contains all the configurations.	<code>apt</code> interactions or unsupported apps can affect machine performance.
audisp	The directory that contains <code>audisp-remote.conf</code> , which is the file that controls the configuration of the audit remote logging subsystem .	
audit	The directory that contains the <code>/etc/audit/auditd.conf</code> , which contains configuration information specific to the <code>audit daemon</code> .	
bash.bashrc	<code>Bash</code> is an sh-compatible command language interpreter that executes commands read from standard input or from a file.	
bash_completion	This points to <code>/usr/share/bash-completion/bash_completion</code> .	
bash_completion.d	This folder contains app-specific code for Bash completion on Cumulus Linux, such as <code>mstptcl</code> .	
bcm.d	Broadcom-specific ASIC file structure (hardware interaction). If there are questions contact the Cumulus Networks Support team. This is unique to Cumulus Linux.	

File	Description	Why is this important?
bindresvport.blacklist	This file contains a list of port numbers between 600 and 1024, which should not be used by <code>bindresvport</code> .	
ca-certificates	The folder for <code>ca-certificates</code> . It is empty by default on Cumulus Linux; see below for more information.	
ca-certificates.conf	Each lines list the pathname of activated CA certificates under <code>/usr/share/ca-certificates</code> .	
calendar	The system-wide default calendar file .	
chef	This is an example of something that is not included by default. In this instance, <code>c1-support</code> included the <code>chef</code> folder for some reason.	This is not installed by default, but this tool could have been installed or configured incorrectly, which is why it's included in the <code>c1-support</code> output.
cron.d	<code>cron</code> is a daemon that executes scheduled commands .	
cron.daily	See above.	
cron.hourly	See above.	
cron.monthly	See above.	
cron.weekly	See above.	
crontab	See above.	
cumulus	<p>This directory contains the following:</p> <ul style="list-style-type: none"> • ACL information, stored in the <code>acl</code> directory. • <code>switchd</code> configuration file, <code>switchd.conf</code>. • <code>qos</code>, which is under the <code>datapath</code> directory. • The routing protocol process priority, <code>nice.conf</code>. • The breakout cable configuration, under <code>ports.conf</code>. 	This folder is specific to Cumulus Linux and does not exist on other Linux platforms. For example, while you can configure <code>iptables</code> , to hardware accelerate rules into the hardware you need to use <code>c1-acltool</code> and have the rules under the <code>/etc/cumulus/acl/policy.d/<filename.rules</code>)
debconf.conf		

File	Description	Why is this important?
	Debconf is a configuration system for Debian packages.	
debian_version	The complete Debian version string .	
debsums-ignore	debsums verifies installed package files against their MD5 checksums. This file identifies the packages to ignore.	
default	This folder contains files with configurable flags for many different applications (most installed by default or added manually). For example, <code>/etc/default/networking</code> has a flag for <code>EXCLUDE_INTERFACES=</code> , which is set to nothing by default, but a user could change it to something like <code>swp3</code> .	
deluser.conf	The file <code>/etc/deluser.conf</code> contains defaults for the programs <code>deluser</code> and <code>delgroup</code> .	
dhcp	This directory contains DHCP-specific information .	
dpkg	The package manager for Debian.	
e2fsck.conf	The configuration file for e2fsck . It controls the default behavior of <code>e2fsck</code> while it checks ext2, ext3 or ext4 filesystems.	
environment	Utilized by <code>pam_env</code> for setting and unsetting environment variables.	
ethertypes	This file can be used to show readable characters instead of hexadecimal numbers for the protocols. For example, <code>0x0800</code> will be represented by IPv4.	
fstab	Static information about the filesystems .	
fstab.d	The directory that can contain additional <code>fstab</code> information; it is empty by default.	
fw_env.config	Configuration file utilized by U-Boot .	
gai.conf	Configuration file for sorting the return information from <code>getaddrinfo</code> .	
groff		

File	Description	Why is this important?
	The directory containing information for <code>groffer</code> , an application used for displaying Unix man pages .	
group	The <code>/etc/group</code> file is a text file that defines the groups on the system.	
group-	Backup for the <code>/etc/group</code> file.	
gshadow	<code>/etc/gshadow</code> contains the shadowed information for group accounts .	
gshadow-	Backup for the <code>/etc/gshadow</code> file.	
host.conf	Resolver configuration file , which contains options like <code>multi</code> that determines whether <code>/etc/hosts</code> will respond with multiple entries for DNS names.	
hostname	The system host name , such as <code>leaf1</code> , <code>spine1</code> , <code>sw1</code> .	
hosts	The static table lookup for hostnames.	
hosts.allow	The part of the host_access program for controlling a simple access control language. <code>hosts</code> . <code>allow=Access</code> is granted when a daemon/client pair matches an entry.	
hosts.deny	See hosts.allow above, except that access is denied when a daemon/client pair matches an entry.	
init	Default location of the system job configuration files .	
init.d	In order for a service to start when the switch boots, you should add the necessary script to the director here. The differences between <code>init</code> and <code>init.d</code> are explained well here .	
inittab	The format of the inittab file used by the sysv-compatible <code>init</code> process.	
inputrc	The initialization file utilized by <code>readline</code> .	
inserv	This application enables installed system init scripts ; this directory is empty by default.	

File	Description	Why is this important?
insserv.conf	Configuration file for insserv .	
insserv.conf.d	Additional directory for insserv configurations.	
iproute2	Directory containing values for the Linux command line tool ip .	
issue	/etc/issue is a text file that contains a message or system identification to be printed before the login prompt.	
issue.net	Identification file for telnet sessions .	
jdoo	jdoo is a utility for monitoring services (see page 437) on a Cumulus Linux system; this directory has configuration files beneath it.	
ld.so.cache	Contains a compiled list of candidate libraries previously found in the augmented library path.	
ld.so.conf	Used by the ldconfig tool, which configures dynamic linker run-time bindings .	
ld.so.conf.d	The directory that contains additional ld.so.conf configuration (see above).	
ldap	The directory containing the ldap.conf configuration file used to set the system-wide default to be applied when running LDAP clients.	
libaudit.conf	Configuration file utilized by get_auditfail_action .	
libnl-3	Directory for the configuration relating to the libnl library , which is the core library for implementing the fundamentals required to use the netlink protocol such as socket handling, message construction and parsing, and sending and receiving of data.	
lldpd.d	Directory containing configuration files whose commands are executed by lldpccli at startup.	
localtime	Copy of the original data file for /etc/timezone .	
logcheck		

File	Description	Why is this important?
	Directory containing <code>logcheck.conf</code> and logfiles utilized by the <code>log_check</code> program, which scans system logs for interesting lines.	
<code>login.defs</code>	Shadow password suite configuration.	
<code>logrotate.conf</code>	Rotates, compresses and mails system logs .	
<code>logrotate.d</code>	Directory containing additional log rotate configurations.	
<code>lsb-release</code>	Shows the current version of Linux on the system. Run <code>cat /etc/lsb-release</code> for output.	This shows you the version of the operating system you are running; also compare this to the output of <code>c1-img-select</code> .
<code>magic</code>	Used by the <code>file</code> command to determine file type. <code>magic</code> tests check for files with data in particular fixed formats.	
<code>magic.mime</code>	The <code>magic</code> MIME type causes the <code>file</code> command to output MIME type strings rather than the more traditional human readable ones.	
<code>mailcap</code>	The <code>mailcap</code> file is read by the metamail program to determine how to display non-text at the local site .	
<code>mailcap.order</code>	The <code>order of entries</code> in the <code>/etc/mailcap</code> file can be altered by editing the <code>/etc/mailcap.order</code> file.	
<code>manpath.config</code>	The <code>manpath configuration file</code> is used by the manual page utilities to assess users' manpaths at run time, to indicate which manual page hierarchies (manpaths) are to be treated as system hierarchies and to assign them directories to be used for storing cat files.	
<code>mime.types</code>	MIME type description file for <code>cups</code> .	
<code>mke2fs.conf</code>	Configuration file for <code>mke2fs</code> , which is a program that creates an ext, ext3 or ext4 filesystem .	
<code>modprobe.d</code>	Configuration directory for <code>modprobe</code> , which is a utility that can add and remove modules from the Linux kernel .	

File	Description	Why is this important?
modules	The kernel modules to load at boot time.	
motd	The contents of <code>/etc/motd</code> ("message of the day") are displayed by <code>pam_motd</code> after a successful login but just before it executes the login shell.	
mtab	The programs <code>mount</code> and <code>umount</code> maintain a list of currently mounted filesystems in the <code>/etc/mtab</code> file. If no arguments are given to <code>mount</code> , this list is printed.	
nanorc	The GNU nano rconfig file.	
network	Contains the network interface configuration for <code>ifup</code> and <code>ifdown</code> .	The main configuration file is under <code>/etc/network/interfaces</code> . This is where you configure L2 and L3 information for all of your front panel ports (swp interfaces). Settings like MTU, link speed, IP address information, VLANs are all done here.
networks	Network name information.	
nsswitch.conf	System databases and name service switch configuration file.	
ntp.conf	NTP (network time protocol) server configuration file.	
openvswitch	The directory containing the <code>conf.db</code> file, which is used by <code>ovsdb-server</code> .	
openvswitch-vtep	Configuration files used for the VTEP daemon and <code>ovsdb-server</code> .	
opt	Host-specific configuration files for add-on applications installed in <code>/opt</code> .	
os-release	Operating system identification.	
pam.conf		

File	Description	Why is this important?
	The PAM (pluggable authentication module) configuration file. When a PAM-aware privilege granting application is started, it activates its attachment to the PAM-API. This activation performs a number of tasks, the most important being the reading of the configuration file(s).	
pam.d	Alternate directory to configure PAM (see above).	
passwd	User account information.	
passwd-	Backup file for /etc/passwd.	
perl	Perl is an available scripting language. /etc/perl contains configuration files specific to Perl.	
profile	/etc/profile is utilized by sysprofile, a modular centralized shell configuration.	
profile.d	The directory version of the above, which contains configuration files.	
protocols	The protocols definition file , a plain ASCII file that describes the various DARPAnt protocols that are available from the TCP/IP subsystem.	
ptm.d	The directory containing scripts that are run if PTM (see page 172) passes or fails.	Cumulus Linux-specific folder for PTM (prescriptive topology manager).
python	python is an available scripting language.	
python2.6	The 2.6 version of python .	
python2.7	The 2.7 version of python .	
quagga	Contains the configuration files for the Quagga routing suite (see page 346) , the preferred Cumulus Linux routing engine.	
rc.local	The /etc/rc.local script is used by the system administrator to execute after all the normal system services are started , at the end of the process of switching to a multiuser runlevel. You can use it to	

File	Description	Why is this important?
	start a custom service, for example, a server that's installed in <code>/usr/local</code> . Most installations don't need <code>/etc/rc.local</code> ; it's provided for the minority of cases where it's needed .	
<code>rc0.d</code>	Like <code>rc.local</code> , these scripts are booted by default, but the number of the folder represents the Linux runlevel . This folder 0 represents runlevel 0 (halt the system).	
<code>rc1.d</code>	This is run level 1, which is single-user/minimal mode.	
<code>rc2.d</code>	Runlevels 2 through 5 are multiuser modes. Debian systems (such as Cumulus Linux) come with <code>id=2</code> , which indicates that the default runlevel will be 2 when the multi-user state is entered , and the scripts in <code>/etc/rc2.d/</code> will be run.	
<code>rc3.d</code>	See above.	
<code>rc4.d</code>	See above.	
<code>rc5.d</code>	See above.	
<code>rc6.d</code>	Runlevel 6 is reboot the system.	
<code>rcS.d</code>	S stands for <i>single</i> and is equivalent to <code>rc1</code> .	
<code>resolv.conf</code>	Resolver configuration file , which is where DNS is set (domain, nameserver and search).	You need DNS to reach the Cumulus Linux repository.
<code>rmt</code>	This is not a mistake. The shell script <code>/etc/rmt</code> is provided for compatibility with other Unix-like systems, some of which have utilities that expect to find (and execute) <code>rmt</code> in the <code>/etc</code> directory on remote systems.	
<code>rpc</code>	The <code>rpc</code> file contains human-readable names that can be used in place of RPC program numbers.	
<code>rsyslog.conf</code>	The <code>rsyslog.conf</code> file is the main configuration file for <code>rsyslogd</code> , which logs system messages on *nix systems.	
<code>rsyslog.d</code>	The directory containing additional configuration for <code>rsyslog.conf</code> (see above).	

File	Description	Why is this important?
securetty	This file lists terminals into which the root user can log in .	
security	The <code>/etc/security</code> directory contains security-related configurations files . Whereas PAM concerns itself with the methods used to authenticate any given user, the files under <code>/etc/security</code> are concerned with just what a user can or cannot do. For example, the <code>/etc/security/access.conf</code> file contains a list of which users are allowed to log in and from what host (for example, using telnet). The <code>/etc/security/limits.conf</code> file contains various system limits, such as maximum number of processes.	
selinux	NSA Security-Enhanced Linux .	
sensors.d	The directory from which the sensors program loads its configuration; this is unique for each hardware platform. See also Monitoring System Hardware (see page 437).	
sensors3.conf	The sensors.conf file describes how <code>libsensors</code> , and thus all programs using it, should translate the raw readings from the kernel modules to real-world values.	
services	<code>services</code> is a plain ASCII file providing a mapping between human-readable textual names for internet services and their underlying assigned port numbers and protocol types.	
shadow	shadow is a file that contains the password information for the system's accounts and optional aging information.	
shadow-	The backup for the <code>/etc/shadow</code> file.	
shells	The pathnames of valid login shells .	
skel	The skeleton directory (usually <code>/etc/skel</code>) is used to copy default files and also sets a umask for the creation used by <code>pam_mkhomedir</code> .	
snmp	Interface functions to the SNMP (simple network management protocol) toolkit.	

File	Description	Why is this important?
ssh	The <code>ssh</code> configuration.	
ssl	The OpenSSL <code>ssl</code> library implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols. This directory holds certificates and configuration.	
staff-group-for-usr-local	Use <code>cat</code> or <code>more</code> on this file to learn more information, see http://bugs.debian.org/299007 .	
sudoers	The <code>sudoers</code> policy plugin determines a user's <code>sudo</code> privileges.	
sudoers.d	The directory file containing additional <code>sudoers</code> configuration (see above).	
sysctl.conf	Configures kernel parameters at boot.	
sysctl.d	The directory file containing additional configuration (see above).	
systemd	<code>systemd</code> system and service manager.	
terminfo	Terminal capability database.	
timezone	If this file exists, it is read and its contents are used as the time zone name.	
ucf.conf	The update configuration file preserves user changes in configuration files.	
udev	Dynamic device management.	
ufw	Provides both a command line interface and a framework for managing a netfilter firewall.	
vim	Configuration file for command line tool vim.	
wgetrc	Configuration file for command line tool wget.	

Troubleshooting the support Directory

The `support` directory is unique in the fact that it is not a copy of the switch's filesystem. Actually, it is the output from various commands. For example:

File	Equivalent Command	Description
support /ip addr	cumulus@switch:~\$ ip addr show	This shows you all the interfaces (including swp front panel ports), IP address information, admin state and physical state.

Managing Application Daemons

You manage application daemons in Cumulus Linux in the following ways:

- Identifying active listener ports
- Identifying daemons currently active or stopped
- Identifying boot time state of a specific daemon
- Disabling or enabling a specific daemon

Contents

(Click to expand)

- [Contents \(see page 467\)](#)
- [Identifying Active Listener Ports for IPv4 and IPv6 \(see page 467\)](#)
- [Identifying Daemons Currently Active or Stopped \(see page 468\)](#)
- [Identifying Boot Time State of a Specific Daemon \(see page 468\)](#)
- [Disabling or Enabling a Specific Daemon \(see page 469\)](#)

Identifying Active Listener Ports for IPv4 and IPv6

You can identify the active listener ports under both IPv4 and IPv6 using the `lsof` command:

```
cumulus@switch:~$ sudo lsof -Pnl +M -i4
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
ntpd 1882 104 16u IPv4 3954 0t0 UDP *:123
ntpd 1882 104 18u IPv4 3963 0t0 UDP 127.0.0.1:123
ntpd 1882 104 19u IPv4 3964 0t0 UDP 192.168.8.37:123
snmpd 1987 105 8u IPv4 5423 0t0 UDP *:161
zebra 1993 103 10u IPv4 5151 0t0 TCP 127.0.0.1:2601 (LISTEN)
sshd 2496 0 3u IPv4 5809 0t0 TCP *:22 (LISTEN)
jdoo 2622 0 6u IPv4 6132 0t0 TCP 127.0.0.1:2812 (LISTEN)
sshd 31700 0 3r IPv4 187630 0t0 TCP 192.168.8.37:22->192.168.8.3:50386
(ESTABLISHED)

cumulus@switch:~$ sudo lsof -Pnl +M -i6
```

```
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
ntpd 1882 104 17u IPv6 3955 0t0 UDP *:123
ntpd 1882 104 20u IPv6 3965 0t0 UDP [::1]:123
ntpd 1882 104 21u IPv6 3966 0t0 UDP [fe80::7272:cfff:fe96:6639]:123
sshd 2496 0 4u IPv6 5811 0t0 TCP *:22 (LISTEN)
```

Identifying Daemons Currently Active or Stopped

To determine which daemons are currently active or stopped, use the `service --status-all` command, then pipe the results to `grep`, using the - or + operators:

```
cumulus@switch:~$ sudo service --status-all | grep +
[ ? ] aciinit
[ + ] arp_refresh
[ + ] auditd
...
cumulus@switch:~$ sudo service --status-all | grep -
[ - ] isc-dhcp-server
[ - ] ovsdb-server
[ - ] ptmd
...
```

Identifying Boot Time State of a Specific Daemon

The `ls` command can provide the boot time state of a daemon. A file link with a name starting with **S** identifies a boot-time-enabled daemon. A file link with a name starting with **K** identifies a disabled daemon.

```
cumulus@switch:~/etc$ sudo ls -l rc*.d | grep <daemon name>
```

For example:

```
cumulus@switch:~/etc$ sudo ls -l rc*.d | grep snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 K02snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 K02snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 S01snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 S01snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 S01snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 S01snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 K02snmpd -> ../init.d/snmpd
```

Disabling or Enabling a Specific Daemon

To enable or disable a specific daemon, run:

```
cumulus@switch:~$ update-rc.d <daemon> disable | enable
```

For example:

```
cumulus@switch:~/etc$ sudo update-rc.d snmpd disable
update-rc.d: using dependency based boot sequencing
insserv: warning: current start runlevel(s) (empty) of script `snmpd'
overrides LSB defaults (2 3 4 5).
insserv: warning: current stop runlevel(s) (0 1 2 3 4 5 6) of script
`snmpd' overrides LSB defaults (0 1 6).
insserv: warning: current start runlevel(s) (empty) of script `snmpd'
overrides LSB defaults (2 3 4 5).
insserv: warning: current stop runlevel(s) (0 1 2 3 4 5 6) of script
`snmpd' overrides LSB defaults (0 1 6).
```

```
cumulus@switch:~/etc$ sudo ls -l rc*.d | grep snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 K02snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 K02snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Feb 13 17:35 K02snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Feb 13 17:35 K02snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Feb 13 17:35 K02snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Feb 13 17:35 K02snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 K02snmpd -> ../init.d/snmpd
```

```
cumulus@switch:~/etc$ sudo update-rc.d snmpd enable
update-rc.d: using dependency based boot sequencing
```

```
cumulus@switch:~/etc$ sudo ls -l rc*.d | grep snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 K02snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 K02snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Feb 13 17:35 S01snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Feb 13 17:35 S01snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Feb 13 17:35 S01snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Feb 13 17:35 S01snmpd -> ../init.d/snmpd
lrwxrwxrwx 1 root root 15 Apr 4 2014 K02snmpd -> ../init.d/snmpd
```

Troubleshooting Network Interfaces

The following sections describe various ways you can troubleshoot `ifupdown2`.

Contents

(Click to expand)

- [Contents \(see page 470\)](#)
- [Enabling Logging for Networking \(see page 470\)](#)
- [Using ifquery to Validate and Debug Interface Configurations \(see page 471\)](#)
- [Debugging Mako Template Errors \(see page 472\)](#)
- [ifdown Cannot Find an Interface that Exists \(see page 473\)](#)
- [Removing All References to a Child Interface \(see page 473\)](#)
- [MTU Set on a Logical Interface Fails with Error: "Numerical result out of range" \(see page 474\)](#)
- [Interpreting iproute2 batch Command Failures \(see page 474\)](#)
- [Understanding the "RTNETLINK answers: Invalid argument" Error when Adding a Port to a Bridge \(see page 475\)](#)

Enabling Logging for Networking

The `/etc/default/networking` file contains two settings for logging:

- To get `ifupdown2` logs when the switch boots (stored in `syslog`)
- To enable logging when you run `service networking [start|stop|reload]`

This file also contains an option for excluding interfaces when you boot the switch or run `service networking start|stop|reload`. You can exclude any interface specified in `/etc/network/interfaces`. These interfaces do not come up when you boot the switch or start/stop/reload the networking service.

```
$cat /etc/default/networking
#
#
# Parameters for the /etc/init.d/networking script
#
#
# Change the below to yes if you want verbose logging to be enabled
VERBOSE="no"

# Change the below to yes if you want debug logging to be enabled
DEBUG="no"

# Change the below to yes if you want logging to go to syslog
SYSLOG="no"
```

```
# Exclude interfaces  
EXCLUDE_INTERFACES=
```

Using ifquery to Validate and Debug Interface Configurations

You use ifquery to print parsed interfaces file entries.

To use ifquery to pretty print iface entries from the interfaces file, run:

```
cumulus@switch:~$ sudo ifquery bond0  
auto bond0  
iface bond0  
    address 14.0.0.9/30  
    address 2001:ded:beef:2::1/64  
    bond-slaves swp25 swp26
```

Use ifquery --check to check the current running state of an interface within the interfaces file. It will return exit code 0 or 1 if the configuration does not match. The line bond-xmit-hash-policy layer3+7 below fails because it should read bond-xmit-hash-policy layer3+4.

```
cumulus@switch:~$ sudo ifquery --check bond0  
iface bond0  
    bond-xmit-hash-policy layer3+7 [fail]  
    bond-slaves swp25 swp26 [pass]  
    address 14.0.0.9/30 [pass]  
    address 2001:ded:beef:2::1/64 [pass]
```



ifquery --check is an experimental feature.

Use ifquery --running to print the running state of interfaces in the interfaces file format:

```
cumulus@switch:~$ sudo ifquery --running bond0  
auto bond0  
iface bond0  
    bond-slaves swp25 swp26  
    address 14.0.0.9/30  
    address 2001:ded:beef:2::1/64
```

`ifquery --syntax-help` provides help on all possible attributes supported in the `interfaces` file. For complete syntax on the `interfaces` file, see `man interfaces` and `man ifupdown-addons-interfaces`.

You can use `ifquery --print-savedstate` to check the `ifupdown2` state database. `ifdown` works only on interfaces present in this state database.

```
cumulus@leaf1$ sudo ifquery --print-savedstate eth0
auto eth0
iface eth0 inet dhcp
```

Debugging Mako Template Errors

An easy way to debug and get details about template errors is to use the `mako-render` command on your `interfaces` template file or on `/etc/network/interfaces` itself.

```
cumulus@switch:~$ sudo mako-render /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp
#auto eth1
#iface eth1 inet dhcp

# Include any platform-specific interface configuration
source /etc/network/interfaces.d/*.*if

# ssim2 added

auto swp45
iface swp45

auto swp46
iface swp46

cumulus@switch:~$ sudo mako-render /etc/network/interfaces.d
/<interfaces_stub_file>
```

ifdown Cannot Find an Interface that Exists

If you are trying to bring down an interface that you know exists, use `ifdown` with the `--use-current-config` option to force `ifdown` to check the current `/etc/network/interfaces` file to find the interface. This can solve issues where the `ifup` command issues for that interface was interrupted before it updated the state database. For example:

```
cumulus@switch:~$ sudo ifdown br0
error: cannot find interfaces: br0 (interface was probably never up ?)

cumulus@switch:~$ sudo brctl show
bridge name          bridge id           STP enabled      interfaces
br0                  8000.44383900279f    yes            downlink
                                         peerlink

cumulus@switch:~$ sudo ifdown br0 --use-current-config
```

Removing All References to a Child Interface

If you have a configuration with a child interface, whether it's a VLAN, bond or another physical interface, and you remove that interface from a running configuration, you must remove every reference to it in the configuration. Otherwise, the interface continues to be used by the parent interface.

For example, consider the following configuration:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

auto bond1
iface bond1
    bond-slaves swp2 swp1

auto bond3
iface bond3
    bond-slaves swp8 swp6 swp7

auto br0
iface br0
    bridge-ports swp3 swp5 bond1 swp4 bond3
```

```
bridge-pathcosts  swp3=4  swp5=4  swp4=4
address 11.0.0.10/24
address 2001::10/64
```

Notice that bond1 is a member of br0. If you comment out or simply delete bond1 from `/etc/network/interfaces`, you must remove the reference to it from the br0 configuration. Otherwise, if you reload the configuration with `ifreload -a`, bond1 is still part of br0.

MTU Set on a Logical Interface Fails with Error: "Numerical result out of range"

This error occurs when the [MTU](#) (see page 137) you are trying to set on an interface is higher than the MTU of the lower interface or dependent interface. Linux expects the upper interface to have an MTU less than or equal to the MTU on the lower interface.

In the example below, the swp1.100 VLAN interface is an upper interface to physical interface swp1. If you want to change the MTU to 9000 on the VLAN interface, you must include the new MTU on the lower interface swp1 as well.

```
auto swp1.100
iface swp1.100
    mtu 9000

auto swp1
iface swp1
    mtu 9000
```

Interpreting iproute2 batch Command Failures

`ifupdown2` batches `iproute2` commands for performance reasons. A batch command contains `ip -force -batch -` in the error message. The command number that failed is at the end of this line: `Command failed -:1.`

Below is a sample error for the command `1: link set dev host2 master bridge`. There was an error adding the bond `host2` to the bridge named `bridge` because `host2` did not have a valid address.

```
error: failed to execute cmd 'ip -force -batch - [link set dev host2 master
bridge
addr flush dev host2
link set dev host1 master bridge
addr flush dev host1
]' (RTNETLINK answers: Invalid argument
Command failed -:1)
warning: bridge configuration failed (missing ports)
```

Understanding the "RTNETLINK answers: Invalid argument" Error when Adding a Port to a Bridge

This error can occur when the bridge port does not have a valid hardware address.

This can typically occur when the interface being added to the bridge is an incomplete bond; a bond without slaves is incomplete and does not have a valid hardware address.

Network Troubleshooting

Cumulus Linux contains a number of command line and analytical tools to help you troubleshoot issues with your network.

Contents

(Click to expand)

- [Contents \(see page 475\)](#)
- [Commands \(see page 475\)](#)
- [Checking Reachability Using ping \(see page 476\)](#)
- [Printing Route Trace Using traceroute \(see page 476\)](#)
- [Manipulating the System ARP Cache \(see page 476\)](#)
- [Generating Traffic Using mz \(see page 477\)](#)
- [Creating Counter ACL Rules \(see page 478\)](#)
- [Configuring SPAN and ERSPAN \(see page 479\)
 - \[Configuring SPAN for Switch Ports \\(see page 480\\)\]\(#\)
 - \[Configuring SPAN for Bonds \\(see page 483\\)\]\(#\)
 - \[Configuring ERSPAN \\(see page 484\\)\]\(#\)
 - \[Removing SPAN Rules \\(see page 485\\)\]\(#\)](#)
- [Monitoring Control Plane Traffic with tcpdump \(see page 485\)](#)
- [Configuration Files \(see page 486\)](#)
- [Useful Links \(see page 486\)](#)
- [Caveats and Errata \(see page 487\)](#)

Commands

- [arp](#)
- [cl-acltool](#)
- [ip](#)
- [mz](#)
- [ping](#)
- [tcpdump](#)
- [traceroute](#)

Checking Reachability Using ping

ping is used to check reachability of a host. ping also calculates the time it takes for packets to travel the round trip. See `man ping` for details.

To test the connection to an IPv4 host:

```
cumulus@switch:~$ ping 206.190.36.45
PING 206.190.36.45 (206.190.36.45) 56(84) bytes of data.
64 bytes from 206.190.36.45: icmp_req=1 ttl=53 time=40.4 ms
64 bytes from 206.190.36.45: icmp_req=2 ttl=53 time=39.6 ms
...
...
```

To test the connection to an IPv6 host:

```
cumulus@switch:~$ ping6 -I swp1 fe80::202:ff:fe00:2
PING fe80::202:ff:fe00:2(fe80::202:ff:fe00:2) from fe80::202:ff:fe00:1
swp1: 56 data bytes
64 bytes from fe80::202:ff:fe00:2: icmp_seq=1 ttl=64 time=1.43 ms
64 bytes from fe80::202:ff:fe00:2: icmp_seq=2 ttl=64 time=0.927 ms
```

Printing Route Trace Using traceroute

traceroute tracks the route that packets take from an IP network on their way to a given host. See `man traceroute` for details.

To track the route to an IPv4 host:

```
cumulus@switch:~$ traceroute www.google.com
traceroute to www.google.com (74.125.239.49), 30 hops max, 60 byte packets
1  fw.cumulusnetworks.com (192.168.1.1)  0.614 ms  0.863 ms  0.932 ms
2  router.hackerdojo.com (157.22.42.1)  15.459 ms  16.447 ms  16.818 ms
3  gw-cpe-hackerdojo.via.net (157.22.10.97)  18.470 ms  18.473 ms  18.897 ms
4  ge-1-5-v223.core1.uspao.via.net (157.22.10.81)  20.419 ms  20.422 ms
21.026 ms
5  core2-1-1-0.pao.net.google.com (198.32.176.31)  22.347 ms  22.584 ms
24.328 ms
6  216.239.49.250 (216.239.49.250)  24.371 ms  25.757 ms  25.987 ms
7  72.14.232.35 (72.14.232.35)  27.505 ms  22.925 ms  22.323 ms
8  nuq04s19-in-f17.1e100.net (74.125.239.49)  23.544 ms  21.851 ms  22.604
ms
```

Manipulating the System ARP Cache

`arp` manipulates or displays the kernel's IPv4 network neighbor cache. See `man arp` for details.

To display the ARP cache:

```
cumulus@switch:~$ arp -a
? (11.0.2.2) at 00:02:00:00:00:10 [ether] on swp3
? (11.0.3.2) at 00:02:00:00:00:01 [ether] on swp4
? (11.0.0.2) at 44:38:39:00:01:c1 [ether] on swp1
```

To delete an ARP cache entry:

```
cumulus@switch:~$ arp -d 11.0.2.2
cumulus@switch:~$ arp -a
? (11.0.2.2) at <incomplete> on swp3
? (11.0.3.2) at 00:02:00:00:00:01 [ether] on swp4
? (11.0.0.2) at 44:38:39:00:01:c1 [ether] on swp1
```

To add a static ARP cache entry:

```
cumulus@switch:~$ arp -s 11.0.2.2 00:02:00:00:00:10
cumulus@switch:~$ arp -a
? (11.0.2.2) at 00:02:00:00:00:10 [ether] PERM on swp3
? (11.0.3.2) at 00:02:00:00:00:01 [ether] on swp4
? (11.0.0.2) at 44:38:39:00:01:c1 [ether] on swp1
```

Generating Traffic Using mz

`mz` is a fast traffic generator. It can generate a large variety of packet types at high speed. See `man mz` for details.

For example, to send two sets of packets to TCP port 23 and 24, with source IP 11.0.0.1 and destination 11.0.0.2, do the following:

```
cumulus@switch:~$ sudo mz swp1 -A 11.0.0.1 -B 11.0.0.2 -c 2 -v -t tcp
"dp=23-24"

Mausezahn 0.40 - (C) 2007-2010 by Herbert Haas - http://www.perihel.at/sec
/mz/
Use at your own risk and responsibility!
-- Verbose mode --
```

```
This system supports a high resolution clock.
The clock resolution is 4000250 nanoseconds.
Mausezahn will send 4 frames...
IP: ver=4, len=40, tos=0, id=0, frag=0, ttl=255, proto=6, sum=0, SA=11.
0.0.1, DA=11.0.0.2,
payload=[see next layer]
TCP: sp=0, dp=23, S=42, A=42, flags=0, win=10000, len=20, sum=0,
payload=

IP: ver=4, len=40, tos=0, id=0, frag=0, ttl=255, proto=6, sum=0, SA=11.
0.0.1, DA=11.0.0.2,
payload=[see next layer]
TCP: sp=0, dp=24, S=42, A=42, flags=0, win=10000, len=20, sum=0,
payload=

IP: ver=4, len=40, tos=0, id=0, frag=0, ttl=255, proto=6, sum=0, SA=11.
0.0.1, DA=11.0.0.2,
payload=[see next layer]
TCP: sp=0, dp=23, S=42, A=42, flags=0, win=10000, len=20, sum=0,
payload=

IP: ver=4, len=40, tos=0, id=0, frag=0, ttl=255, proto=6, sum=0, SA=11.
0.0.1, DA=11.0.0.2,
payload=[see next layer]
TCP: sp=0, dp=24, S=42, A=42, flags=0, win=10000, len=20, sum=0,
payload=
```

Creating Counter ACL Rules

In Linux, all ACL rules are always counted. To create an ACL rule for counting purposes only, set the rule action to ACCEPT. See the [Netfilter \(see page 89\)](#) chapter for details on how to use cl-acltool to set up iptables-/ip6tables-/ebtables-based ACLs.



Always place your rules files under /etc/cumulus/acl/policy.d/.

To count all packets going to a Web server:

```
cumulus@switch$ cat sample_count.rules

[iptables]
-A FORWARD -p tcp --dport 80 -j ACCEPT

cumulus@switch:$ sudo cl-acltool -i -p sample_count.rules
```

```

Using user provided rule file sample_count.rules
Reading rule file sample_count.rules ...
Processing rules in file sample_count.rules ...
Installing acl policy... done.

cumulus@switch$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 16 packets, 2224 bytes)
pkts bytes target     prot opt in      out      source
destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in      out      source
destination
      2    156 ACCEPT      tcp   --  any     any     anywhere
anywhere           tcp  dpt:http

Chain OUTPUT (policy ACCEPT 44 packets, 8624 bytes)
pkts bytes target     prot opt in      out      source
destination

```

! The **-p** option clears out all other rules, and the **-i** option is used to reinstall all the rules.

Configuring SPAN and ERSPAN

SPAN (Switched Port Analyzer) provides for the mirroring of all packets coming in from or going out of an interface (the *SPAN source*), and being copied and transmitted out of a local port (the *SPAN destination*) for monitoring. The SPAN destination port is referred to as a *mirror-to-port* (MTP). The original packet is still switched, while a mirrored copy of the packet is sent out of the MTP port.

ERSPAN (Encapsulated Remote SPAN) enables the mirrored packets to be sent to a monitoring node located anywhere across the routed network. The switch finds the outgoing port of the mirrored packets by doing a lookup of the destination IP address in its routing table. The original L2 packet is encapsulated with GRE for IP delivery. The encapsulated packets have the following format:

```

-----| MAC_HEADER | IP_HEADER | GRE_HEADER | L2_Mirrored_Packet |
```

! Mirrored traffic is not guaranteed. If the MTP is congested, mirrored packets may be discarded.

SPAN and ERSPAN are configured via `cl-acltool`, the [same utility for security ACL configuration](#) (see [page 89](#)). The match criteria for SPAN and ERSPAN can only be an interface; more granular match terms are not supported. This SPAN source interface can be a port, a subinterface or a bond interface. Both ingress and egress traffic on interfaces can be matched.

Cumulus Linux supports a maximum of 2 SPAN destinations. Multiple rules (SPAN sources) can point to the same SPAN destination, although a given SPAN source cannot specify 2 SPAN destinations. The SPAN destination (MTP) interface can be a physical port, a subinterface, or a bond interface. The SPAN/ERSPAN action is independent of security ACL actions. If packets match both a security ACL rule and a SPAN rule, both actions will be carried out.



Always place your rules files under `/etc/cumulus/acl/policy.d/`.

Configuring SPAN for Switch Ports

This section describes how to set up, install, verify and uninstall SPAN rules. In the examples that follow, you will span (mirror) switch port `swp4` input traffic and `swp4` output traffic to destination switch port `swp19`.

First, create a rules file in `/etc/cumulus/acl/policy.d/`:

```
cumulus@switch:~$ sudo bash -c 'cat <<EOF > /etc/cumulus/acl/policy.d/span.rules
[iptables]
-A FORWARD --in-interface swp4 -j SPAN --dport swp19
-A FORWARD --out-interface swp4 -j SPAN --dport swp19
EOF'
```



Using `cl-acltool` with the `--out-interface` rule applies to transit traffic only; it does not apply to traffic sourced from the switch.

Next, verify all the rules that are currently installed:

```
cumulus@switch:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
      0     0  DROP       all   --  swp+    any    240.0.0.0/5
anywhere
      0     0  DROP       all   --  swp+    any    loopback/8
anywhere
      0     0  DROP       all   --  swp+    any    base-address.mcast.net/8
anywhere
      0     0  DROP       all   --  swp+    any    255.255.255.255
```

```

anywhere
    0      0 SETCLASS    ospf -- swp+   any     anywhere
anywhere          SETCLASS    class:7
    0      0 POLICE     ospf -- any    any     anywhere
anywhere          POLICE    mode:pkt rate:2000 burst:2000
    0      0 SETCLASS    tcp  -- swp+   any     anywhere
anywhere          tcp dpt:bgp SETCLASS class:7
    0      0 POLICE     tcp  -- any    any     anywhere
anywhere          tcp dpt:bgp POLICE  mode:pkt rate:2000 burst:2000
    0      0 SETCLASS    tcp  -- swp+   any     anywhere
anywhere          tcp spt:bgp SETCLASS class:7
    0      0 POLICE     tcp  -- any    any     anywhere
anywhere          tcp spt:bgp POLICE  mode:pkt rate:2000 burst:2000
    0      0 SETCLASS    tcp  -- swp+   any     anywhere
anywhere          tcp dpt:5342 SETCLASS class:7
    0      0 POLICE     tcp  -- any    any     anywhere
anywhere          tcp dpt:5342 POLICE  mode:pkt rate:2000 burst:2000
    0      0 SETCLASS    tcp  -- swp+   any     anywhere
anywhere          tcp spt:5342 SETCLASS class:7
    0      0 POLICE     tcp  -- any    any     anywhere
anywhere          tcp spt:5342 POLICE  mode:pkt rate:2000 burst:2000
    0      0 SETCLASS    icmp -- swp+   any     anywhere
anywhere          SETCLASS  class:2
    0      0 POLICE     icmp -- any    any     anywhere
anywhere          POLICE   mode:pkt rate:100 burst:40
    15     5205 SETCLASS  udp  -- swp+   any     anywhere
anywhere          udp dpts:bootps:bootpc SETCLASS class:2
    11     3865 POLICE   udp  -- any    any     anywhere
anywhere          udp dpt:bootps POLICE  mode:pkt rate:100 burst:100
    0      0 POLICE     udp  -- any    any     anywhere
anywhere          udp dpt:bootpc POLICE  mode:pkt rate:100 burst:100
    0      0 SETCLASS    tcp  -- swp+   any     anywhere
anywhere          tcp dpts:bootps:bootpc SETCLASS class:2
    0      0 POLICE     tcp  -- any    any     anywhere
anywhere          tcp dpt:bootps POLICE  mode:pkt rate:100 burst:100
    0      0 POLICE     tcp  -- any    any     anywhere
anywhere          tcp dpt:bootpc POLICE  mode:pkt rate:100 burst:100
    17     1088 SETCLASS  igmp -- swp+   any     anywhere
anywhere          SETCLASS  class:6
    17     1156 POLICE   igmp -- any    any     anywhere
anywhere          POLICE   mode:pkt rate:300 burst:100
    394    41060 POLICE  all   -- swp+   any     anywhere
anywhere          ADDRTYPE match dst-type LOCAL POLICE  mode:pkt rate:
1000 burst:1000 class:0
    0      0 POLICE     all   -- swp+   any     anywhere

```

```

anywhere           ADDRTYPE match dst-type IPROUTER POLICE mode:pkt rate:
400 burst:100 class:0
  988 279K SETCLASS all -- swp+ any     anywhere
anywhere          SETCLASS class:0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target      prot opt in      out      source
destination
  0     0 DROP        all   -- swp+    any     240.0.0.0/5
anywhere
  0     0 DROP        all   -- swp+    any     loopback/8
anywhere
  0     0 DROP        all   -- swp+    any     base-address.mcast.net/8
anywhere
  0     0 DROP        all   -- swp+    any     255.255.255.255
anywhere
26864 4672K SPAN      all   -- swp4    any     anywhere
anywhere          dport:swp19 <---- input packets on swp4

40722  47M SPAN      all   -- any     swp4    anywhere
anywhere          dport:swp19 <---- output packets on swp4

Chain OUTPUT (policy ACCEPT 67398 packets, 5757K bytes)
 pkts bytes target      prot opt in      out      source
destination

```

Install the rules:

```

cumulus@switch:~$ sudo cl-acltool -i
[sudo] password for cumulus:
Reading rule file /etc/cumulus/acl/policy.d/00control_plane.rules ...
Processing rules in file /etc/cumulus/acl/policy.d/00control_plane.rules ...
Reading rule file /etc/cumulus/acl/policy.d/99control_plane_catch_all.rules
...
Processing rules in file /etc/cumulus/acl/policy.d/99control_plane_catch_all.rules ...
Reading rule file /etc/cumulus/acl/policy.d/span.rules ...
Processing rules in file /etc/cumulus/acl/policy.d/span.rules ...
Installing acl policy
done.

```

! Running the following command is incorrect and will remove **all** existing control-plane rules or other installed rules and only install the rules defined in `span.rules`:

```
cumulus@switch:~$ sudo cl-acltool -i -P /etc/cumulus/acl/policy.d
/span.rules
```

Verify that the SPAN rules were installed:

```
cumulus@switch:~$ sudo cl-acltool -L all | grep SPAN
38025 7034K SPAN      all -- swp4    any     anywhere
anywhere              dport:swp19
50832   55M SPAN     all -- any     swp4    anywhere
anywhere              dport:swp19
```

Configuring SPAN for Bonds

This section describes how to configure SPAN for all packets going out of `bond0` locally to `bond1`.

First, create a rules file in `/etc/cumulus/acl/policy.d/`:

```
cumulus@switch:~$ sudo bash -c 'cat <<EOF > /etc/cumulus/acl/policy.d
/span_bond.rules
[iptables]
-A FORWARD --out-interface bond0 -j SPAN --dport bond1
EOF'
```

! Using `cl-acltool` with the `--out-interface` rule applies to transit traffic only; it does not apply to traffic sourced from the switch.

Install the rules:

```
cumulus@switch:~$ sudo cl-acltool -i
[sudo] password for cumulus:
Reading rule file /etc/cumulus/acl/policy.d/00control_plane.rules ...
Processing rules in file /etc/cumulus/acl/policy.d/00control_plane.rules ...
Reading rule file /etc/cumulus/acl/policy.d/99control_plane_catch_all.rules
...
Processing rules in file /etc/cumulus/acl/policy.d
/99control_plane_catch_all.rules ...
```

```
Reading rule file /etc/cumulus/acl/policy.d/span_bond.rules ...
Processing rules in file /etc/cumulus/acl/policy.d/span_bond.rules ...
Installing acl policy
done.
```

Verify that the SPAN rules were installed:

```
cumulus@switch:~$ sudo iptables -L -v | grep SPAN
 19  1938 SPAN      all  --  any    bond0    anywhere
anywhere          dport:bond1
```

Configuring ERSPAN

This section describes how to configure ERSPAN for all packets coming in from `swp1` to `12.0.0.2`:

First, create a rules file in `/etc/cumulus/acl/policy.d/`:

```
cumulus@switch:~$ sudo bash -c 'cat <<EOF > /etc/cumulus/acl/policy.d
/erspan.rules
[iptables]
-A FORWARD --in-interface swp1 -j ERSPAN --src-ip 12.0.0.1 --dst-ip
12.0.0.2 --ttl 64
EOF'
```

Install the rules:

```
cumulus@switch:~$ sudo cl-acltool -i
Reading rule file /etc/cumulus/acl/policy.d/00control_plane.rules ...
Processing rules in file /etc/cumulus/acl/policy.d/00control_plane.rules ...
Reading rule file /etc/cumulus/acl/policy.d/99control_plane_catch_all.rules
...
Processing rules in file /etc/cumulus/acl/policy.d/99control_plane_catch_all.rules ...
Reading rule file /etc/cumulus/acl/policy.d/erspan.rules ...
Processing rules in file /etc/cumulus/acl/policy.d/erspan.rules ...
Installing acl policy
done.
```

Verify that the ERSPAN rules were installed:

```
cumulus@switch:~$ sudo iptables -L -v | grep SPAN
 69 6804 ERSPAN      all -- swp1 any    anywhere
anywhere           ERSPAN src-ip:12.0.0.1 dst-ip:12.0.0.2
```

The `src-ip` option can be any IP address, whether it exists in the routing table or not. The `dst-ip` option must be an IP address reachable via the routing table. The destination IP address must be reachable from a front-panel port, and not the management port. Use `ping` or `ip route get <ip>` to verify that the destination IP address is reachable. Setting the `--ttl` option is recommended.



When using [Wireshark](#) to review the ERSPAN output, Wireshark may report the message "Unknown version, please report or test to use fake ERSPAN preference", and the trace is unreadable. To resolve this, go into the General preferences for Wireshark, then go to **Protocols** > **ERSPAN** and check the **Force to decode fake ERSPAN frame** option.

Removing SPAN Rules

To remove your SPAN rules, run:

```
#Remove rules file:
cumulus@switch:~$ sudo rm /etc/cumulus/acl/policy.d/span.rules
#Reload the default rules
cumulus@switch:~$ sudo cl-acltool -i
cumulus@switch:~$
```

To verify that the SPAN rules were removed:

```
cumulus@switch:~$ sudo cl-acltool -L all | grep SPAN
cumulus@switch:~$
```

Monitoring Control Plane Traffic with `tcpdump`

You can use `tcpdump` to monitor control plane traffic — traffic sent to and coming from the switch CPUs. `tcpdump` does **not** monitor data plane traffic; use `cl-acltool` instead (see above).

For more information on `tcpdump`, read the [tcpdump documentation](#) and the [tcpdump man page](#).

The following example incorporates a few `tcpdump` options:

- `-i bond0`, which captures packets from bond0 to the CPU and from the CPU to bond0
- `host 169.254.0.2`, which filters for this IP address
- `-c 10`, which captures 10 packets then stops

```
cumulus@switch:~$ sudo tcpdump -i bond0 host 169.254.0.2 -c 10
tcpdump: WARNING: bond0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on bond0, link-type EN10MB (Ethernet), capture size 65535 bytes
16:24:42.532473 IP 169.254.0.2 > 169.254.0.1: ICMP echo request, id 27785,
seq 6, length 64
16:24:42.532534 IP 169.254.0.1 > 169.254.0.2: ICMP echo reply, id 27785,
seq 6, length 64
16:24:42.804155 IP 169.254.0.2.40210 > 169.254.0.1.5342: Flags [.], seq
266275591:266277039, ack 3813627681, win 58, options [nop,nop,TS val
590400681 ecr 530346691], length 1448
16:24:42.804228 IP 169.254.0.1.5342 > 169.254.0.2.40210: Flags [.], ack
1448, win 166, options [nop,nop,TS val 530348721 ecr 590400681], length 0
16:24:42.804267 IP 169.254.0.2.40210 > 169.254.0.1.5342: Flags [P.], seq
1448:1836, ack 1, win 58, options [nop,nop,TS val 590400681 ecr 530346691],
length 388
16:24:42.804293 IP 169.254.0.1.5342 > 169.254.0.2.40210: Flags [.], ack
1836, win 165, options [nop,nop,TS val 530348721 ecr 590400681], length 0
16:24:43.532389 IP 169.254.0.2 > 169.254.0.1: ICMP echo request, id 27785,
seq 7, length 64
16:24:43.532447 IP 169.254.0.1 > 169.254.0.2: ICMP echo reply, id 27785,
seq 7, length 64
16:24:43.838652 IP 169.254.0.1.59951 > 169.254.0.2.5342: Flags [.], seq
2555144343:2555145791, ack 2067274882, win 58, options [nop,nop,TS val
530349755 ecr 590399688], length 1448
16:24:43.838692 IP 169.254.0.1.59951 > 169.254.0.2.5342: Flags [P.], seq
1448:1838, ack 1, win 58, options [nop,nop,TS val 530349755 ecr 590399688],
length 390
10 packets captured
12 packets received by filter
0 packets dropped by kernel
```

Configuration Files

- /etc/cumulus/acl/policy.conf

Useful Links

- www.perihel.at/sec/mz/mzguide.html
- en.wikipedia.org/wiki/Ping
- www.tcpdump.org

- en.wikipedia.org/wiki/Traceroute

Caveats and Errata

- SPAN rules cannot match outgoing subinterfaces.
- ERSPAN rules must include `t+1` for versions 1.5.1 and earlier.

SNMP Monitoring

Cumulus Linux 2.5.x utilizes the open source Net-SNMP agent `snmpd`, v5.4.3, which provides support for most of the common industry-wide MIBs, including interface counters and TCP/UDP IP stack data.



Cumulus Linux does not prevent customers from extending SNMP features. However, Cumulus Networks encourages the use of higher performance monitoring environments, rather than SNMP.

Contents

(Click to expand)

- Contents (see page 487)
- Starting the SNMP Daemon (see page 488)
- Configuring SNMP (see page 489)
 - Setting up the Custom Cumulus Networks MIBs (see page 489)
 - Enabling the .1.3.6.1.2.1 Range (see page 490)
 - Enabling Public Community (see page 491)
- Configuring Nutanix Prism (see page 491)
 - Cumulus Linux Configuration (see page 491)
 - Nutanix Configuration (see page 492)
- Switch Information Displayed on Nutanix Prism (see page 495)
- Troubleshooting (see page 496)
- Enabling LLDP/CDP on VMware ESXi (Hypervisor on Nutanix) (see page 497)
- Enabling LLDP/CDP on Nutanix Acropolis (Hypervisor on Nutanix Acropolis) (see page 499)
- `snmpwalk` the Switch from Another Linux Device (see page 499)
- Troubleshooting Connections without LLDP or CDP (see page 501)
- Generating Event Notification Traps (see page 503)
 - Enabling MIB to OID Translation (see page 503)
 - Configuring Trap Events (see page 504)
- Supported MIBs (see page 506)

Starting the SNMP Daemon

`snmpd` is disabled by default in Cumulus Linux 2.5.x. The following procedure is the recommended process to start `snmpd`, and monitor it using `jdoe`.



`jdoe` is the fork of `monit` version 5.2.5, and is included in Cumulus Linux 2.5.2 and later. For more information about upgrading from `monit` to `jdoe`, see the [jdoe upgrade knowledge base article](#).



`jdoe` and `monit` are mutually exclusive. If you would prefer to use `monit`, the installation process will uninstall `jdoe`. Cumulus Networks will not provide support for issues with `monit`.

To start the SNMP daemon:

1. Open `/etc/default/snmpd` to verify that `SNMPDRUN=yes`. If it does not, update the file to the correct value.
2. Create an `*.rc` configuration file in the `/etc/jdoe/jdoorc.d/` directory.



Cumulus Networks recommends using a name related to SNMP, for ease of troubleshooting. The rest of this process will use the filename `snmpd.rc`.

3. Add the following content to the `snmpd.rc` file created in step 2, under the Services banner, and save the file:

```
#####
## Services
#####
## Services
#####
check process snmpd with pidfile /var/run/snmpd.pid
    every 6 cycles
    group networking
    start program = "/etc/init.d/snmpd start"
    stop program = "/etc/init.d/snmpd stop"
```

4. Configure `snmpd` to start automatically on boot:

```
# update-rc.d snmpd enable
```

5. Reload jdoo:

```
# sudo jdoo reload
```

6. Start the SNMP daemon, either with jdoo monitoring, or natively.

- With jdoo monitoring:

```
# sudo jdoo start snmpd
```

- Natively:

```
# sudo service snmpd start
```

Once the service is started, SNMP can be used to manage various components on the Cumulus Linux switch.

Configuring SNMP

Cumulus Linux ships with a production usable default `snmpd.conf` file included. This section covers a few basic configuration options in `snmpd.conf`. For more information regarding further configuring this file, refer to the `snmpd.conf` man page.



The default `snmpd.conf` file does not include all supported MIBs or OIDs that can be exposed.



Customers are encouraged to at least change the default community string for v1 or v2c environments.

Setting up the Custom Cumulus Networks MIBs



No changes are required in the `/etc/snmp/snmpd.conf` file on the switch, in order to support the custom Cumulus Networks MIBs. The following lines are already included by default:

```
view systemonly included .1.3.6.1.4.1.40310.1
view systemonly included .1.3.6.1.4.1.40310.2
sysObjectID 1.3.6.1.4.1.40310
pass_persist .1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
pass_persist .1.3.6.1.4.1.40310.2 /usr/share/snmp/cl_drop_cntrs_pp.py
```

However, several files need to be copied to the server, in order for the custom Cumulus MIB to be recognized on the destination NMS server.

- /usr/share/snmp/Cumulus-Snmp-MIB.txt
- /usr/share/snmp/Cumulus-Counters-MIB.txt
- /usr/share/snmp/Cumulus-Resource-Query-MIB.txt

Enabling the .1.3.6.1.2.1 Range

Some MIBs, including storage information, are not included by default in `snmpd.conf` in Cumulus Linux. This results in some default views on common network tools (like `librenms`) to return less than optimal data.

More MIBs can be included, by enabling all the .1.3.6.1.2.1 range. This simplifies the configuration file, removing concern that any required MIBs will be missed by the monitoring system.



This configuration grants access to a large number of MIBs, including all MIB2 MIBs, which could reveal more data than expected, and consume more CPU resources.

To enable the .1.3.6.1.2.1 range:

1. Open `/etc/snmp/snmpd.conf` in a text editor.
2. Replace lines 39 - 71 with the following code sample, and save the file.

```
#####
#####
#
# ACCESS CONTROL
#
#
# system
view systemonly included .1.3.6.1.2.1
# quagga ospf6
view systemonly included .1.3.6.1.3.102
# lldpd
view systemonly included .1.0.8802.1.1.2
#lmsensors
view systemonly included .1.3.6.1.4.1.2021.13.16
# Cumulus specific
view systemonly included .1.3.6.1.4.1.40310.1
view systemonly included .1.3.6.1.4.1.40310.2
```

3. Restart snmpd:

```
# sudo service snmpd start
```

Enabling Public Community

Public community is disabled by default in Cumulus Linux. To enable querying by agent:

1. Open `/etc/snmp/snmpd.conf` in a text editor.
2. Add the following line to the end of the file, then save it:

```
rocommunity public default -V systemonly
```

3. Restart `snmpd`:

```
cumulus@switch:~$ sudo service snmpd restart
```

Configuring Nutanix Prism

Nutanix Prism is a graphical user interface (GUI) for managing infrastructures and virtual environments.

Cumulus Linux Configuration

1. SSH to the Cumulus Linux switch that needs to be configured, replacing `[switch]` below as appropriate:

```
cumulus@switch:~$ ssh cumulus@[switch]
```

2. Confirm the switch is running Cumulus Linux 2.5.5 or newer:

```
cumulus@switch$ cat /etc/lsb-release
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=2.5.5
DISTRIB_DESCRIPTION=2.5.5-4cd66d9-201512071809-build
```

3. Open the `/etc/snmp/snmpd.conf` file in an editor.
4. Uncomment the following 3 lines in the `/etc/snmp/snmpd.conf` file, and save the file:

- `bridge_pp.py`

```
pass_persist .1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
```

- Community

```
rocommunity public default -V systemonly
```

- Line directly below the Q-BRIDGE-MIB (.1.3.6.1.2.1.17)

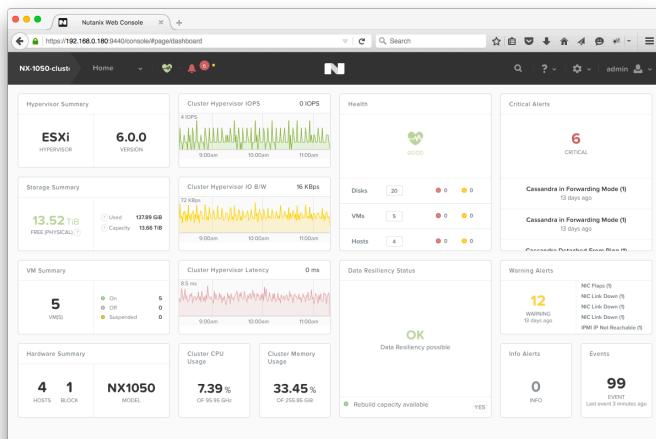
```
# BRIDGE-MIB and Q-BRIDGE-MIB tables
view systemonly included .1.3.6.1.2.1.17
```

5. Restart snmpd:

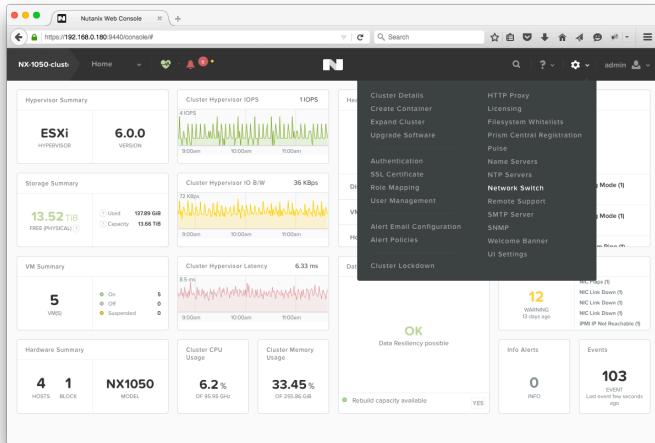
```
cumulus@switch$ sudo service snmpd restart
Restarting network management services: snmpd.
cumulus@switch$
```

Nutanix Configuration

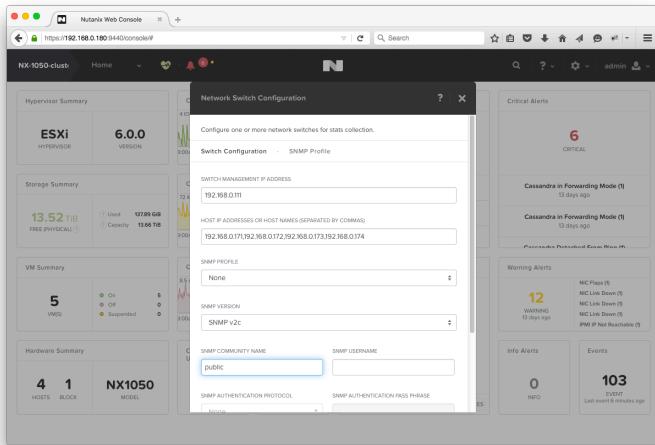
1. Log into the Nutanix Prism. Nutanix defaults to the Home menu, referred to as the Dashboard:



2. Click on the gear icon  in the top right corner of the dashboard, and select NetworkSwitch:



3. Click the **+Add Switch Configuration** button in the **Network Switch Configuration** pop up window.
4. Fill out the **Network Switch Configuration** for the Top of Rack (ToR) switch configured for snmpd in the previous section:



Configuration Parameter	Description	Value Used in Example
Switch Management IP Address	This can be any IP address on the box. In the screenshot above, the eth0 management IP is used.	192.168.0.111
Host IP Addresses or Host Names		192.168.0.171,192.168.0.172,192.168.0.173,192.168.0.174

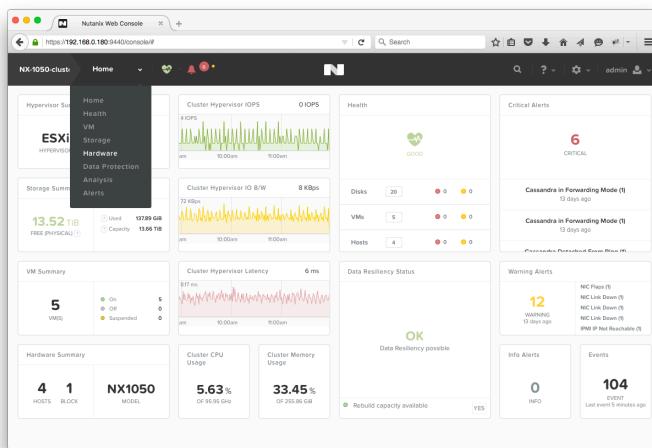
Configuration Parameter	Description	Value Used in Example
	IP addresses of Nutanix hosts connected to that particular ToR switch.	
SNMP Profile	Saved profiles, for easy configuration when hooking up to multiple switches.	None
SNMP Version	SNMP v2c or SNMP v3. Cumulus Linux has only been tested with SNMP v2c for Nutanix integration.	SNMP v2c
SNMP Community Name	SNMP v2c uses communities to share MIBs. The default community for snmpd is 'public'.	public



The rest of the values were not touched for this demonstration. They are usually used with SNMP v3.

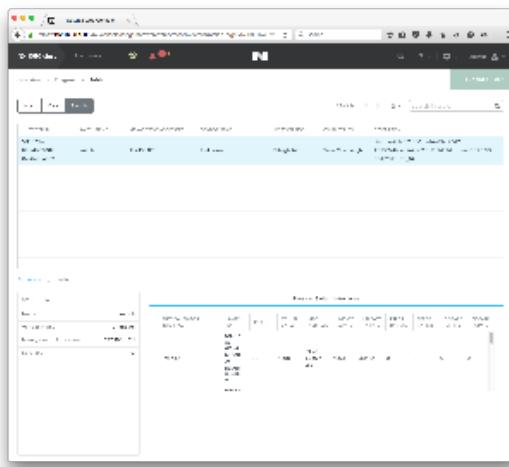
5. Save the configuration. The switch will now be present in the **Network Switch Configuration** menu now.
6. Close the pop up window to return to the dashboard.

7. Open the **Hardware** option from the **Home** dropdown menu:



8. Click the **Table** button.

9. Click the **Switch** button. Configured switches are shown in the table, as indicated in the screenshot below, and can be selected in order to view interface statistics:



The switch has been added correctly, when interfaces hooked up to the Nutanix hosts are visible.

Switch Information Displayed on Nutanix Prism

- Physical Interface (e.g. swp1, swp2). This will only display swp interfaces connected to Nutanix hosts by default.
- Switch ID - Unique identifier that Nutanix keeps track of each port ID (see below)
- Index - interface index, in the above demonstration swp49 maps to Index 52 because there is a loopback and two ethernet interface before the swp starts.
- MTU of interface
- MAC Address of Interface
- Unicast RX Packets (Received)

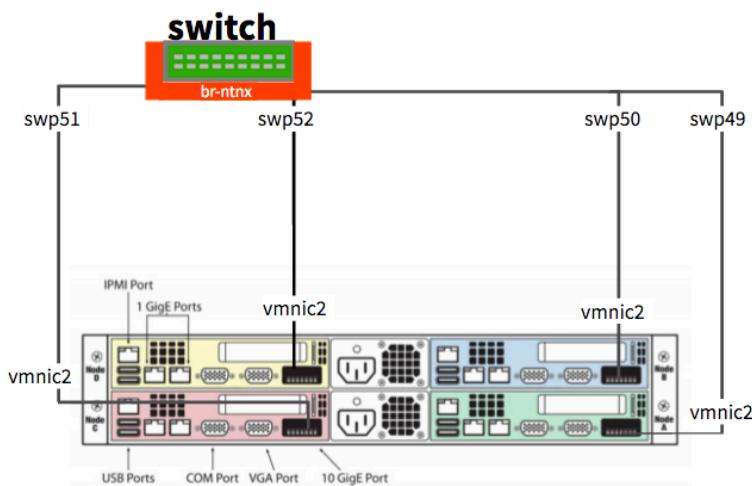
- Unicast TX Packets (Transmitted)
- Error RX Packets (Received)
- Error TX Packets (Transmitted)
- Discard RX Packets (Received)
- Discard TX Packets (Transmitted)

The Nutanix appliance will use Switch IDs that can also be viewed on the Prism CLI (by SSHing to the box). To view information from the Nutanix CLI, login using the default username **nutanix**, and the password **nutanix/4u**.

```
nutanix@NTNX-14SM15270093-D-CVM:192.168.0.184:~$ ncli network list-switch
  Switch ID          : 00051a76-f711-89b6-0000-000000003bac:::
5f13678e-6ffd-4b33-912f-f1aa6e8da982
    Name           : switch
    Switch Management Address : 192.168.0.111
    Description      : Linux switch 3.2.65-1+deb7u2+c12.5+2 #3.
2.65-1+deb7u2+c12.5+2 SMP Mon Jun 1 18:26:59 PDT 2015 x86_64
    Object ID       : enterprises.40310
    Contact Information : Admin <admin@company.com>
    Location Information : Raleigh, NC
    Services         : 72
    Switch Vendor Name : Unknown
    Port Ids        : 00051a76-f711-89b6-0000-000000003bac:::
5f13678e-6ffd-4b33-912f-f1aa6e8da982:52, 00051a76-f711-89b6-0000-
000000003bac:::5f13678e-6ffd-4b33-912f-f1aa6e8da982:53, 00051a76-f711-89b6-
0000-000000003bac:::5f13678e-6ffd-4b33-912f-f1aa6e8da982:54, 00051a76-f711-
89b6-0000-000000003bac:::5f13678e-6ffd-4b33-912f-f1aa6e8da982:55
```

Troubleshooting

To help visualize the following diagram is provided:



Nutanix Node	Physical Port	Cumulus Linux Port
Node A (Green)	vmnic2	swp49
Node B (Blue)	vmnic2	swp50
Node C (Red)	vmnic2	swp51
Node D (Yellow)	vmnic2	swp52

Enabling LLDP/CDP on VMware ESXi (Hypervisor on Nutanix)

1. Follow the directions on one of the following websites to enable CDP:
 - a. http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003885
 - b. <http://wahlnetwork.com/2012/07/17/utilizing-cdp-and-lldp-with-vsphere-networking/>
e.g. Switch CDP on:

```
root@NX-1050-A:~] esxcli network vswitch standard set -c both -v
vSwitch0
```

Then confirm it is running:

```
root@NX-1050-A:~] esxcli network vswitch standard list -v vSwitch0
vSwitch0
  Name: vSwitch0
  Class: etherswitch
  Num Ports: 4082
  Used Ports: 12
  Configured Ports: 128
  MTU: 1500
  CDP Status: both
  Beacon Enabled: false
  Beacon Interval: 1
  Beacon Threshold: 3
  Beacon Required By:
  Uplinks: vmnic3, vmnic2, vmnic1, vmnic0
  Portgroups: VM Network, Management Network
```

The **both** means CDP is now running, and the lldp dameon on Cumulus Linux is capable of 'seeing' CDP devices.

- After the next CDP interval, the Cumulus Linux box will pick up the interface via the lldp daemon:

```
cumulus@switch$ lldpctl show neighbor swp49
-----
-----
LLDP neighbors:
-----
-----
Interface:      swp49, via: CDPv2, RID: 6, Time: 0 day, 00:34:58
Chassis:
  ChassisID:      local NX-1050-A
  SysName:        NX-1050-A
  SysDescr:       Releasebuild-2494585 running on VMware ESX
  MgmtIP:         0.0.0.0
  Capability:    Bridge, on
Port:
  PortID:         ifname vmnic2
  PortDescr:      vmnic2
-----
```

- Use netshow to look at lldp information:

```
cumulus@switch$ netshow lldp
-----
To view the legend, rerun "netshow" cmd with the "--legend" option
-----
Local Port      Speed      Mode          Remote Port      Remote
Host   Summary
-----  -----  -----  -----  -----
eth0      1G        Mgmt      =====  swp32           swoob.vsokt.
local   IP: 192.168.0.111/24(DHCP)
swp49     10G(SFP+)  Access/L2  =====  vmnic2         NX-1050-
A          Untagged: br-ntnx
swp50     10G(SFP+)  Access/L2  =====  vmnic2         NX-1050-
B          Untagged: br-ntnx
swp51     10G(SFP+)  Access/L2  =====  vmnic2         NX-1050-
```

```

C          Untagged: br-ntnx
swp52      10G(SFP+)    Access/L2  ===   vmnic2           NX-1050-
D          Untagged: br-ntnx

```

Enabling LLDP/CDP on Nutanix Acropolis (Hypervisor on Nutanix Acropolis)

Nutanix Acropolis is an alternate hypervisor that Nutanix supports. Acropolis Hypervisor uses the yum packaging system and is capable of installing normal Linux llpd daemons to operating just like Cumulus Linux. LLDP should be enabled for each interface on the host. Refer to <https://community.mellanox.com/docs/DOC-1522> for setup instructions.

snmpwalk the Switch from Another Linux Device

One of the most important ways to troubleshoot is to snmpwalk the switch from another Linux device that can reach the switch running Cumulus Linux. For this demonstration, another switch running Cumulus Linux within the network is used.

1. Open /etc/apt/sources.list in an editor.
2. Add the following line, and save the file:

```
deb http://ftp.us.debian.org/debian/ wheezy main non-free
```

3. Update the switch:

```
cumulus@switch2$ sudo apt-get update
```

4. Install the snmp and snmp-mibs-downloader packages:

```
cumulus@switch2$ sudo apt-get install snmp snmp-mibs-downloader
```

5. Verify that the "mibs :" line is commented out in /etc/snmp/snmp.conf:

```

#
# As the snmp packages come without MIB files due to license reasons,
loading
# of MIBs is disabled by default. If you added the MIBs you can
reenable
# loading them by commenting out the following line.
#mibs :

```

6. Perform an snmpwalk on the switch. The switch running snmpd in the demonstration is using IP address 192.168.0.111. It is possible to snmpwalk the switch from itself, following these instructions, ruling out an snmp problem vs networking problem.

```
cumulus@switch2$ snmpwalk -c public -v2c 192.168.0.111
```

Output Examples

```
IF-MIB::ifPhysAddress.2 = STRING: 74:e6:e2:f5:a2:80
IF-MIB::ifPhysAddress.3 = STRING: 0:e0:ec:25:b8:54
IF-MIB::ifPhysAddress.4 = STRING: 74:e6:e2:f5:a2:81
IF-MIB::ifPhysAddress.5 = STRING: 74:e6:e2:f5:a2:82
IF-MIB::ifPhysAddress.6 = STRING: 74:e6:e2:f5:a2:83
IF-MIB::ifPhysAddress.7 = STRING: 74:e6:e2:f5:a2:84
IF-MIB::ifPhysAddress.8 = STRING: 74:e6:e2:f5:a2:85
IF-MIB::ifPhysAddress.9 = STRING: 74:e6:e2:f5:a2:86
IF-MIB::ifPhysAddress.10 = STRING: 74:e6:e2:f5:a2:87
IF-MIB::ifPhysAddress.11 = STRING: 74:e6:e2:f5:a2:88
IF-MIB::ifPhysAddress.12 = STRING: 74:e6:e2:f5:a2:89
IF-MIB::ifPhysAddress.13 = STRING: 74:e6:e2:f5:a2:8a
IF-MIB::ifPhysAddress.14 = STRING: 74:e6:e2:f5:a2:8b
IF-MIB::ifPhysAddress.15 = STRING: 74:e6:e2:f5:a2:8c
IF-MIB::ifPhysAddress.16 = STRING: 74:e6:e2:f5:a2:8d
IF-MIB::ifPhysAddress.17 = STRING: 74:e6:e2:f5:a2:8e
IF-MIB::ifPhysAddress.18 = STRING: 74:e6:e2:f5:a2:8f
IF-MIB::ifPhysAddress.19 = STRING: 74:e6:e2:f5:a2:90
```

Any information gathered here should verify that snmpd is running correctly on the Cumulus Linux side, reducing locations where a problem may reside.

Troubleshooting Tips Table for snmp walks

Run snmpwalk from	If it works	If it does not work
switch (switch to be monitored)	snmpd is serving information correctly Problem resides somewhere else (e.g. network connectivity, Prism misconfiguration)	Is snmpd misconfigured or installed incorrectly?
		Network connectivity is not able to grab information?

Run snmpwalk from	If it works	If it does not work
switch2 (another Cumulus Linux switch in the network)	snmpd is serving information correctly and network reachability works between switch and switch2 Problems resides somewhere else (e.g. can Prism reach switch , Prism misconfiguration)	Is there an iptables rule blocking? Is the snmp walk being run correctly?
Nutanix Prism CLI (ssh to the cluster IP address)	snmpd is serving information correctly and network reachability works between switch and the Nutanix Appliance Problems resides somewhere else (e.g. The GUI might be misconfigured)	Is the right community name being used in the GUI? Is snmp v2c being used?

Troubleshooting Connections without LLDP or CDP

1. Find the MAC address information in the Prism GUI, located in: **Hardware -> Table -> Host -> Host NICs**
2. Select a MAC address to troubleshoot (e.g. 0c:c4:7a:09:a2:43 represents vmnic0 which is tied to NX-1050-A).
3. List out all the MAC addresses associated to the bridge:

```
cumulus@switch$ brctl showmacs br-ntnx
port name mac addr          vlan    is local?   ageing
timer
swp9      00:02:00:00:00:06      0       no        66.94
swp52     00:0c:29:3e:32:12      0       no        2.73
swp49     00:0c:29:5a:f4:7f      0       no        2.73
swp51     00:0c:29:6f:e1:e4      0       no        2.73
swp49     00:0c:29:74:0c:ee      0       no        2.73
swp50     00:0c:29:a9:36:91      0       no        2.73
swp9      08:9e:01:f8:8f:0c      0       no        13.56
swp9      08:9e:01:f8:8f:35      0       no        2.73
swp4      0c:c4:7a:09:9e:d4      0       no        24.05
swp1      0c:c4:7a:09:9f:8e      0       no        13.56
swp3      0c:c4:7a:09:9f:93      0       no        13.56
swp2      0c:c4:7a:09:9f:95      0       no        24.05
swp52     0c:c4:7a:09:a0:c1      0       no        2.73
swp51     0c:c4:7a:09:a2:35      0       no        2.73
swp49     0c:c4:7a:09:a2:43      0       no        2.73
swp9      44:38:39:00:82:04      0       no        2.73
swp9      74:e6:e2:f5:a2:80      0       no        2.73
swp1      74:e6:e2:f5:a2:81      0       yes       0.00
swp2      74:e6:e2:f5:a2:82      0       yes       0.00
```

swp3	74:e6:e2:f5:a2:83	0	yes	0.00
swp4	74:e6:e2:f5:a2:84	0	yes	0.00
swp5	74:e6:e2:f5:a2:85	0	yes	0.00
swp6	74:e6:e2:f5:a2:86	0	yes	0.00
swp7	74:e6:e2:f5:a2:87	0	yes	0.00
swp8	74:e6:e2:f5:a2:88	0	yes	0.00
swp9	74:e6:e2:f5:a2:89	0	yes	0.00
swp10	74:e6:e2:f5:a2:8a	0	yes	0.00
swp49	74:e6:e2:f5:a2:b1	0	yes	0.00
swp50	74:e6:e2:f5:a2:b2	0	yes	0.00
swp51	74:e6:e2:f5:a2:b3	0	yes	0.00
swp52	74:e6:e2:f5:a2:b4	0	yes	0.00
swp9	8e:0f:73:1b:f8:24	0	no	2.73
swp9	c8:1f:66:ba:60:cf	0	no	66.94

Alternatively, you can use grep:p

```
cumulus@switch$ brctl showmacs br-ntnx | grep 0c:c4:7a:09:a2:43
swp49      0c:c4:7a:09:a2:43          0        no           4.58
cumulus@switch$
```

vmnic1 is now hooked up to swp49. This matches what is seen in lldp:

```
cumulus@switch$ lldpctl show neighbor swp49
-----
-----
LLDP neighbors:
-----
-----
Interface:      swp49, via: CDPv2, RID: 6, Time: 0 day, 01:11:12
Chassis:
  ChassisID:    local NX-1050-A
  SysName:      NX-1050-A
  SysDescr:     Releasebuild-2494585 running on VMware ESX
  MgmtIP:       0.0.0.0
  Capability:   Bridge, on
Port:
  PortID:       ifname vmnic2
  PortDescr:    vmnic2
-----
-----
cumulus@switch$
```

Generating Event Notification Traps

The Net-SNMP agent provides a method to generate SNMP trap events, via the Distributed Management (DisMan) Event MIB, for various system events, including linkup/down, exceeding the temperature sensor threshold, CPU load, or memory threshold, or other SNMP MIBs.

Enabling MIB to OID Translation

MIB names can be used instead of OIDs, by installing the `snmp-mibs-downloader`, to download SNMP MIBs to the switch prior to enabling traps. This greatly improves the readability of the `snmpd.conf` file.

1. Open `/etc/apt/sources.list` in a text editor.
2. Add the `non-free` repository, and save the file:

```
cumulus@switch:~$ deb http://ftp.us.debian.org/debian/ wheezy main non-free
```

3. Update the switch:

```
cumulus@switch:~$ apt-get update
```

4. Install the `snmp-mibs-downloader`:

```
apt-get snmp-mibs-downloader
```

5. Open the `/etc/snmp/snmp.conf` file to verify that the `mibs :` line is commented out:

```
#  
# As the snmp packages come without MIB files due to license reasons,  
loading  
# of MIBs is disabled by default. If you added the MIBs you can  
reenable  
# loading them by commenting out the following line.  
#mibs :
```

6. Open the `/etc/default/snmpd` file to verify that the `export MIBS=` line is commented out:

```
# This file controls the activity of snmpd and snmptrapd
```

```
# Don't load any MIBs by default.  
# You might comment this lines once you have the MIBs Downloaded.  
#export MIBS=
```

- Once the configuration has been confirmed, remove or comment out the `non-free` repository in `/etc/apt/sources.list`.

```
#deb http://ftp.us.debian.org/debian/ wheezy main non-free
```

Configuring Trap Events

The following configurations should be made in `/etc/snmp/snmp.conf`, in order to enable specific types of traps. Once configured, restart the `snmpd` service to apply the changes.

Defining Access Credentials

An SNMPv3 username is required to authorize the DisMan service. The example code below uses `cumulusUser` as the username.

```
createUser cumulusUser  
iquerySecName cumulusUser  
rouser cumulusUser
```

Defining Trap Receivers

The example code below creates a trap receiver that is capable of receiving SNMPv2 traps.

```
trap2sink 192.168.1.1 public
```



Although the traps are sent to an SNMPV2 receiver, the SNMPv3 user is still required.



It is possible to define multiple trap receivers, and to use the domain name instead of IP address in the `trap2sink` directive.

Configuring LinkUp/Down Notifications

The `linkUpDownNotifications` directive is used to configure linkup/down notifications when the operational status of the link changes.

```
linkUpDownNotifications yes
```



The default frequency for checking link up/down is 60 seconds. The default frequency can be changed using the `monitor` directive directly instead of the `linkUpDownNotifications` directive. See `man snmpd.conf` for details.

Configuring Temperature Notifications

Temperature sensor information for each available sensor is maintained in the the `ImSensors` MIB. Each platform may contain a different number of temperature sensors. The example below generates a trap event when any temperature sensors exceeds a threshold of 68 degrees (centigrade). It monitors each `1mTempSensorsValue`. When the threshold value is checked and exceeds the `1mTempSensorsValue`, a trap is generated. The `-o 1mTempSensorsDevice` option is used to instruct SNMP to also include the `ImTempSensorsDevice` MIB in the generated trap. The default frequency for the `monitor` directive is 600 seconds. The default frequency may be changed using the `-r` option.:.

```
monitor lmTemSensor -o lmTempSensorsDevice lmTempSensorsValue > 68000
```

Alternatively, temperature sensors may be monitored individually. To monitor the sensors individually, first use the `sensors` command to determine which sensors are available to be monitored on the platform.

```
#sensors

CY8C3245-i2c-4-2e
Adapter: i2c-0-mux (chan_id 2)
fan5: 7006 RPM (min = 2500 RPM, max = 23000 RPM)
fan6: 6955 RPM (min = 2500 RPM, max = 23000 RPM)
fan7: 6799 RPM (min = 2500 RPM, max = 23000 RPM)
fan8: 6750 RPM (min = 2500 RPM, max = 23000 RPM)
temp1: +34.0 C (high = +68.0 C)
temp2: +28.0 C (high = +68.0 C)
temp3: +33.0 C (high = +68.0 C)
temp4: +31.0 C (high = +68.0 C)
temp5: +23.0 C (high = +68.0 C)
```

Configure a `monitor` command for the specific sensor using the `-I` option. The `-I` option indicates that the monitored expression is applied to a single instance. In this example, there are five temperature sensors available. The following monitor directive can be used to monitor only temperature sensor three at five minute intervals.

```
monitor -I -r 300 lmTemSensor3 -o lmTempSensorsDevice.3 lmTempSensorsValue.  
3 > 68000
```

Configuring Free Memory Notifications

You can monitor free memory using the following directives. The example below generates a trap when free memory drops below 1,000,000KB. The free memory trap also includes the amount of total real memory:

```
monitor MemFreeTotal -o memTotalReal memTotalFree < 1000000
```

Configuring Processor Load Notifications

To monitor CPU load for 1, 5 or 15 minute intervals, use the `load` directive in conjunction with the `monitor` directive. The following example will generate a trap when the 1 minute interval reaches 12%, the 5 minute interval reaches 10% or the 15 minute interval reaches 5%.

```
load 12 10 5  
monitor -r 60 -o laNames -o laErrMessage "laTable" laErrorFlag !=0
```

Configuring Disk Utilization Notifications

To monitor disk utilization for all disks, use the `includeAllDisks` directive in conjunction with the `monitor` directive. The example code below generates a trap when a disk is 99% full:

```
includeAllDisks 1%  
monitor -r 60 -o dskPath -o DiskErrMsg "dskTable" diskErrorFlag !=0
```

Configuring Authentication Notifications

To generate authentication failure traps, use the `authtrapenable` directive:

```
authtrapenable 1
```

Supported MIBs

Below are the MIBs supported by Cumulus Linux, as well as suggested uses for them. The overall Cumulus Linux MIB is defined in `/usr/share/snmp/Cumulus-Snmp-MIB.txt`.

MIB Name	Suggested Uses
CUMULUS-COUNTERS-MIB	Discard counters: Cumulus Linux also includes its own counters MIB, defined in <code>/usr/share/snmp/Cumulus-Counters-MIB.txt</code> . It has the OID <code>.1.3.6.1.4.1.40310.2</code> .
CUMULUS-RESOURCE-QUERY-MIB	Cumulus Linux includes its own resource utilization MIB, which is similar to using cl-resource-query (see page 436) . It monitors L3 entries by host, route, nexthops, ECMP groups and L2 MAC/BDPU entries. The MIB is defined in <code>/usr/share/snmp/Cumulus-Resource-Query-MIB.txt</code> , and has the OID <code>.1.3.6.1.4.1.40310.1</code> .
DISMAN-EVENT	Trap monitoring
HOST-RESOURCES	Users, storage, interfaces, process info, run parameters
IF-MIB	Interface description, type, MTU, speed, MAC, admin, operation status, counters
IP (includes ICMP)	IPv4, IPv4 addresses, counters, netmasks
IPv6	IPv6 counters
IP-FORWARD	IP routing table
LLDP	L2 neighbor info from llldpd (note, you need to enable the SNMP subagent (see page 171) in LLDP)
LM-SENSORS MIB	Fan speed, temperature sensor values, voltages
NET-SNMP-AGENT	Agent timers, user, group config
NET-SNMP-EXTEND	Agent timers, user, group config
NET-SNMP-EXTEND-MIB	(See also this knowledge base article on extending NET-SNMP in Cumulus Linux to include data from power supplies, fans and temperature sensors.)
NET-SNMP-VACM	Agent timers, user, group config
NOTIFICATION-LOG	Local logging

MIB Name	Suggested Uses
SNMP-FRAMEWORK	Users, access
SNMP-MPD	Users, access
SNMP-TARGET	
SNMP-USER-BASED-SM	Users, access
SNMP-VIEW-BASED-ACM	Users, access
SNMPv2	SNMP counters (For information on exposing CPU and memory information via SNMP, see this knowledge base article .)
TCP	TCP related information
UCD-SNMP	System memory, load, CPU, disk IO
UDP	UDP related information



The Quagga and Zebra routes MIB is disabled in Cumulus Linux.

Network Solutions

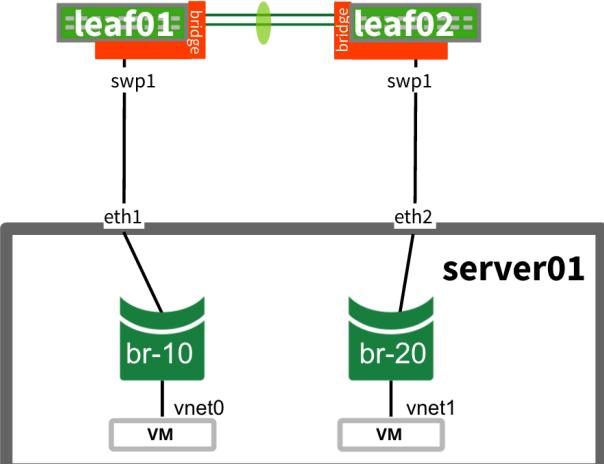
Data Center Host to ToR Architecture

This chapter discusses the various architectures and strategies available from the top of rack (ToR) switches all the way down to the server hosts.

Contents

- Contents (see page 509)
- Layer 2 - Architecture (see page 509)
- Layer 3 Architecture (see page 514)
- Network Virtualization (see page 523)

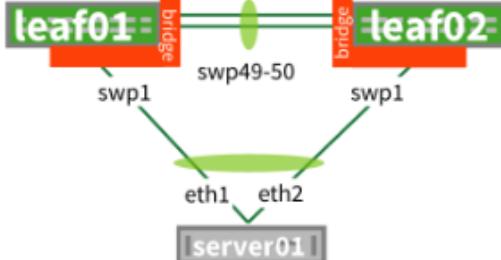
Layer 2 - Architecture

Traditional Spanning Tree - Single Attached	Summary	More Information
	<p>Bond (see page 184) /Etherchannel is not configured on host to multiple switches (bonds can still occur but only to one switch at a time), so leaf01 and leaf02 see two different MAC addresses.</p> <p>Configurations</p> <p>leaf01 Config</p> <pre>auto bridge iface bridge bridge- vlan- aware yes</pre>	<p>Benefits</p> <ul style="list-style-type: none"> • Established technology • Interoperability with other vendors • Easy configuration for customers • Immense documentation from multiple vendors and industry <p>• Ability to use spanning tree (see page 150) commands</p> <ul style="list-style-type: none"> • mstptc- portadminedg • BPDU guard (see page 162) <p>• Layer 2 reachability to all VMs</p> <p>Caveats</p>

Traditional Spanning Tree - Single Attached	Summary	More Information
	<pre> bridge- ports swp1 peerlink bridge- vids 1- 2000 bridge- stp on auto bridge. 10 iface bridge. 10 address 10.1.10 .2/24 auto peerlink iface peerlink bond- slaves glob swp49-5 0 auto swp1 iface swp1 mstpctl - portadm inedge yes </pre>	<ul style="list-style-type: none"> The load balancing mechanism on the host can cause problems. If there is only host pinning to each NIC, there are no problems, but if you are doing a bond, you need to look at an MLAG solution. No active-active host links. Some operating systems allow HA (NIC failover), but this still does not utilize all the bandwidth. VMs are using one NIC, not two.

Traditional Spanning Tree - Single Attached	Summary	More Information
	<pre>mstptcl - bpdugua rd yes</pre> <p>Example Host Config (Ubuntu)</p> <pre>auto eth1 iface eth1 inet manual auto eth1.10 iface eth1.10 inet manual auto eth2 iface eth1 inet manual auto eth2.20 iface eth2.20 inet manual auto br-10 iface br-10 inet manual bridge- ports</pre>	

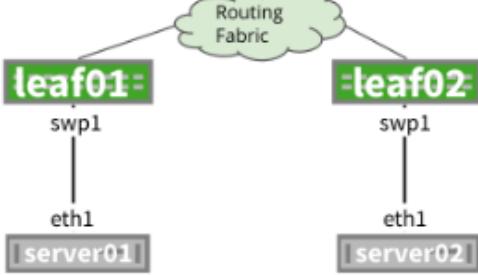
Traditional Spanning Tree - Single Attached	Summary	More Information
	<pre data-bbox="894 291 1041 766"> eth1.10 vnet0 auto br-20 iface br-20 inet manual bridge- ports eth2.20 vnet1 </pre>	
Active/Active	Active/Passive	L2 to L3 Demarcation
<ul data-bbox="208 931 833 963" style="list-style-type: none"> None (not possible with traditional spanning tree) 	<ul data-bbox="926 931 1041 1110" style="list-style-type: none"> VRR (see page 240) vrrpd 	<ul data-bbox="1139 931 1383 1089" style="list-style-type: none"> ToR layer (recommended) Spine layer Core/edge/exit <p data-bbox="1095 1110 1237 1136">More Info...</p> <p data-bbox="1095 1157 1442 1824">VRR or vrrpd can be configured on a pair of switches at any level in the network. However, the higher up the network you configure it, the larger the L2 domain becomes. The benefit here is L2 reachability. The drawback is the L2 domain is more difficult to troubleshoot, does not scale as well, and the pair of switches running VRR/vrrp needs to carry the entire MAC address table of everything below it in the network. Minimizing the L2 domain as much as possible is recommended by Cumulus Professional Services. Please see this presentation for more information.</p>

MLAG	Summary	More Information
	<p>MLAG (see page 217) (multi-chassis link aggregation) is when both uplinks are utilized at the same time. VRR gives the ability for both spines to act as gateways simultaneously for HA (high availability) and active-active mode (see page 307) (both are being used at the same time).</p> <p>Configurations</p> <p>leaf01 Config</p> <pre data-bbox="784 783 1127 1959"> auto bridge iface bridge bridge-vlan- aware yes bridge-ports host-01 peerlink bridge-vids 1-200 0 bridge-stp on auto bridge.10 iface bridge.10 address 172.16.1. 2/24 address-virtual 4 4:38:39:00:00:10 17 2.16.1.1/24 auto peerlink iface peerlink bond-slaves glob swp49-50 auto peerlink.4094 iface peerlink.4094 address 169.254. .1.2 clagd-enable yes clagd-peer-ip 1 69.254.1.2 clagd-system- mac 44:38:39:FF:40: 94 </pre>	<p>Benefits</p> <ul style="list-style-type: none"> • 100% of links utilized <p>Caveats</p> <ul style="list-style-type: none"> • More complicated (more moving parts) • More configuration • No interoperability between vendors • ISL (inter-switch link) required <p>Additional Comments</p> <ul style="list-style-type: none"> • Can be done with either the traditional (see page 187) or VLAN-aware (see page 208) bridge driver depending on overall STP needs • There are a few different solutions including Cisco VPC and Arista MLAG, but none of them interoperate and are very vendor specific • Cumulus Networks Layer 2 HA validated design guide

MLAG	Summary	More Information
	<pre>auto host-01 iface host-01 bond-slaves swp1 clag-id 1 {bond-defaults removed for brevity}</pre>	
	<p>Example Host Config (Ubuntu)</p> <pre>auto bond0 iface bond0 inet manual bond-slaves eth0 eth1 {bond-defaults removed for brevity} auto bond0.10 iface bond0.10 inet manual auto vm-br10 iface vm-br10 inet manual bridge-ports bond0.10 vnet0</pre>	
Active-Active Mode <ul style="list-style-type: none"> VRR (see page 240) 	Active-Passive <ul style="list-style-type: none"> vrrpd 	L2->L3 Demarcation <ul style="list-style-type: none"> ToR layer (recommended) Spine layer Core/edge/exit

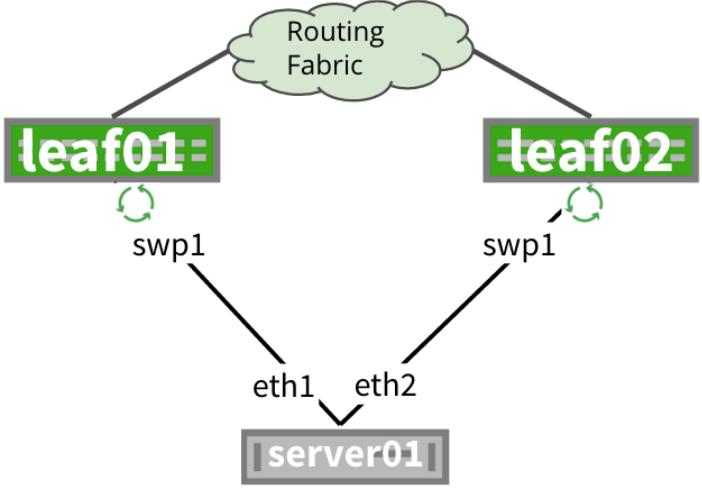
Layer 3 Architecture

Single Attached Hosts	Summary	More Information
		Benefits

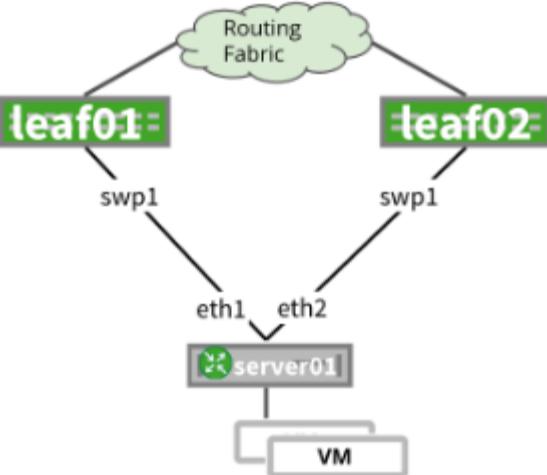
Single Attached Hosts	Summary	More Information
 <p>The server (physical host) has only has one link to one ToR switch.</p> <p>Configurations</p> <p>leaf01 Config</p> <pre>/etc/network /interfaces</pre> <pre>auto swp1 iface swp1 address 172 .16.1.1/30</pre> <p>leaf02 Config</p> <pre>/etc/network /interfaces</pre> <pre>auto swp1 iface swp1 address 172 .16.2.1/30</pre>	<p>Configurations</p> <p>leaf01 Config</p> <pre>/etc/network /interfaces</pre> <pre>auto swp1 iface swp1 address 172 .16.1.1/30</pre> <p>leaf02 Config</p> <pre>/etc/network /interfaces</pre> <pre>auto swp1 iface swp1 address 172 .16.2.1/30</pre>	<ul style="list-style-type: none"> Relatively simple network configuration No STP No MLAG No L2 loops No crosslink between leafs Greater route scaling and flexibility <p>Caveats</p> <ul style="list-style-type: none"> No redundancy for ToR, upgrades would cause downtime Many customers do not have software to support application layer redundancy <p>Additional Comments</p> <ul style="list-style-type: none"> For additional bandwidth links between host and leaf may be bonded

Single Attached Hosts	Summary	More Information
	<pre>ip ospf area 0</pre> <p>host1 Example Config (Ubuntu)</p> <pre>auto eth1 iface eth1 inet static address 172 .16.1.2/30 up ip route add 0.0 .0.0/0 nexthop via 1 72.16.1.1</pre> <p>host2 Example Config (Ubuntu)</p> <pre>auto eth1 iface eth1 inet static address 172 .16.2.2/30 up ip route add 0.0 .0.0/0 nexthop via 1 72.16.2.1</pre>	
FHR (First Hop Redundancy)		Additional Information
<ul style="list-style-type: none"> No redundancy, uses single ToR as gateway. 		<ul style="list-style-type: none"> Big Data validated design guide uses single attached ToR

Redistribute Neighbor	Summary	More Information
	Redistribute neighbor daemon grabs ARP entries	Benefits

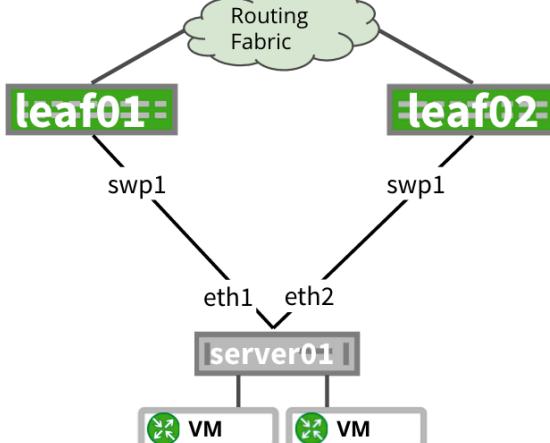
Redistribute Neighbor	Summary	More Information
	dynamically, utilizes redistribute table for Quagga to grab these dynamic entries and redistribute them into the fabric.	<ul style="list-style-type: none"> Configuration in Quagga is simple (route-map + redistribute table) Supported by Cumulus Networks <p>Caveats</p> <ul style="list-style-type: none"> Silent hosts don't receive traffic (depending on ARP). IPv4 only. If two VMs are on same L2 domain, they could learn about each other directly rather than utilizing gateway, which causes problems (VM migration for example, or getting their network routed). Put hosts on /32 (no other L2 adjacency). VM move does not trigger route withdrawal from original leaf (4 hour timeout). Clearing ARP impacts routing. May not be obvious.

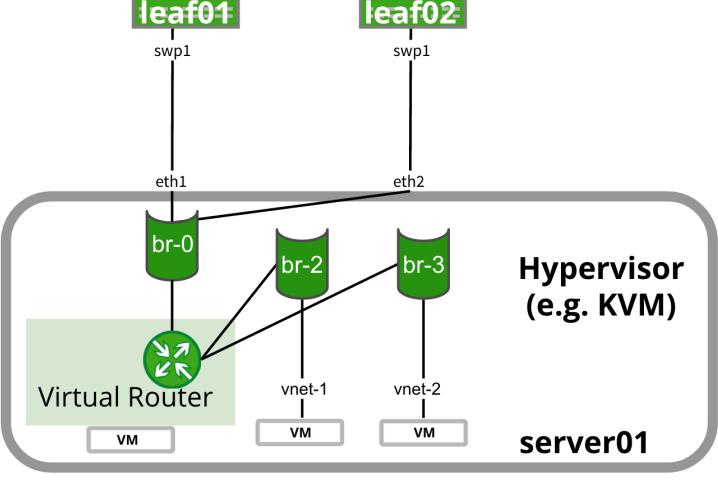
Redistribute Neighbor	Summary	More Information
		<ul style="list-style-type: none"> No L2 adjacency between servers without VXLAN.
FHR (First Hop Redundancy)		Additional Information
<ul style="list-style-type: none"> Equal cost route installed on server/host/hypervisor to both ToRs to load balance evenly. For host/VM/container mobility, use the same default route on all hosts (such as x.x.x.1) but don't distribute or advertise the .1 on the ToR into the fabric. This allows the VM to use the same gateway no matter which pair of leafs it is cabled to. 		<ul style="list-style-type: none"> Cumulus Networks blog post introducing redistribute neighbor

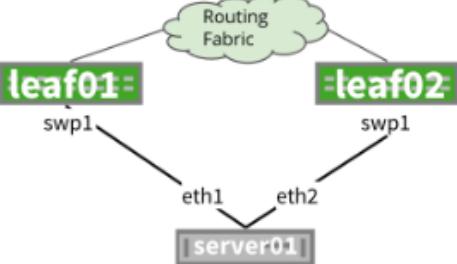
Routing on the Host	Summary	More Information
 <p>The diagram illustrates a network topology where two leaf switches, leaf01 and leaf02, are connected to a central Routing Fabric. Leaf01 has two interfaces, swp1 and eth1, and Leaf02 has one interface, swp1. Both leaf switches are connected to a server01, which in turn connects to a VM. This setup represents routing on the host, where the host (server01) performs routing functions.</p>	<p>Routing on the host means there is a routing application (such as Cumulus Networks Quagga) either on the bare metal host (no VMs /containers) or the hypervisor (for example, Ubuntu with KVM). This is highly recommended by the Cumulus Networks Professional Services team.</p>	<p>Benefits</p> <ul style="list-style-type: none"> No requirement for MLAG No spanning-tree or layer 2 domain No loops 3 or more ToRs can be used instead of usual 2 Host and VM mobility Traffic engineering can be used to migrate traffic from one ToR to another for upgrading

Routing on the Host	Summary	More Information
		<p>both hardware and software</p> <p>Caveats</p> <ul style="list-style-type: none"> • Certain hypervisors or host OSes might not support a routing application like Quagga and will require a virtual router on the hypervisor • No L2 adjacency between servers without VXLAN
FHR (First Hop Redundancy)		Additional Information
<ul style="list-style-type: none"> • The first hop is still the ToR, just like redistribute neighbor • A default route can be advertised by all leaf/ToRs for dynamic ECMP paths 		<ul style="list-style-type: none"> • Routing on the Host: An Introduction • Installing the Cumulus Linux Quagga Package on an Ubuntu Server • Configuring Quagga (see page 346)

Routing on the VM	Summary	More Information
		Benefits

Routing on the VM	Summary	More Information
	<p>Instead of routing on the hypervisor, each virtual machine utilizes its own routing stack.</p>	<ul style="list-style-type: none"> In addition to routing on host: <ul style="list-style-type: none"> Hypervisor /base OS does not need to be able to do routing VMs can be authenticated into routing fabric <p>Caveats</p> <ul style="list-style-type: none"> All VMs must be capable of routing Scale considerations might need to be taken into account — instead of one routing process, there are as many as there are VMs No L2 adjacency between servers without VXLAN
FHR (First Hop Redundancy)		Additional Information
<ul style="list-style-type: none"> The first hop is still the ToR, just like redistribute neighbor Multiple ToRs (2+) can be used 		<ul style="list-style-type: none"> Routing on the host: An Introduction Installing the Cumulus Linux Quagga Package on an Ubuntu Server Configuring Quagga (see page 346)
Virtual Router	Summary	More Information
	<p>Virtual router (vRouter) runs as a VM on the hypervisor/host, sends routes to the ToR using</p>	<p>Benefits</p> <p>In addition to routing on a host:</p>

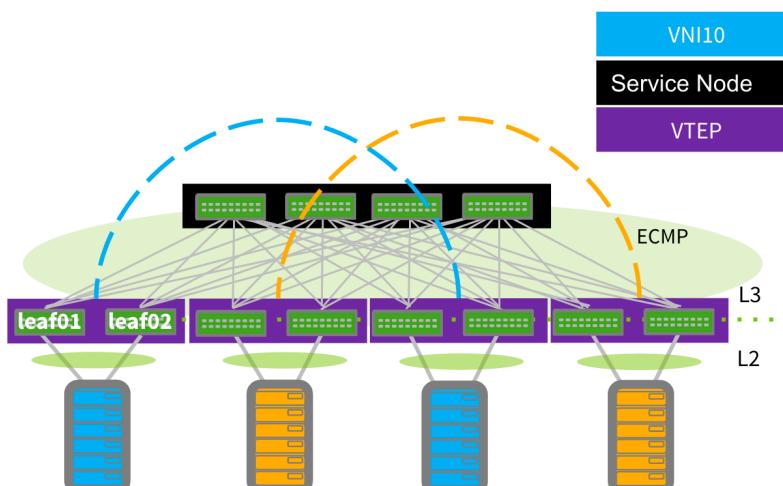
Virtual Router	Summary	More Information
	BGP (see page 372) or OSPF (see page 358).	<ul style="list-style-type: none"> Multi-tenancy can work (multiple customers sharing same racks) Base OS does not need to be routing capable <p>Caveats</p> <ul style="list-style-type: none"> ECMP (see page 399) might not work correctly (load balancing to multiple ToRs); Linux kernel in older versions is not capable of ECMP per flow (does it per packet) No L2 adjacency between servers without VXLAN
FHR (First Hop Redundancy)		Additional Information <ul style="list-style-type: none"> Routing on the Host: An Introduction Installing the Cumulus Linux Quagga Package on an Ubuntu Server Configuring Quagga (see page 346)

Anycast with Manual Redistribution	Summary	More Information
 <p>In contrast to routing on the host (preferred), this method allows a user to route to the host. The ToRs are the gateway, as with redistribute neighbor, except because there is no daemon running, the networks must be manually configured under the routing process. There is a potential to black hole unless a script is run to remove the routes when the host no longer responds.</p> <p>Configurations</p> <p>leaf01 Config</p> <pre>/etc/network/interfaces</pre> <pre>auto swp1 iface swp1 address 172.16.1.1/3 0</pre> <p>leaf02 Config</p> <pre>/etc/network/interfaces</pre> <pre>auto swp2 iface swp2 address 172.16.1.1/3 0</pre> <p>leaf01 Quagga Configuration</p> <pre>/etc/quagga/Quagga.conf</pre> <pre>router ospf router-id 10.0.0.11 interface swp1 ip ospf area 0</pre> <p>leaf02 Quagga Configuration</p> <pre>/etc/quagga/Quagga.conf</pre> <pre>router ospf router-id 10.0.0.12 interface swp1 ip ospf area 0</pre>	<p>Benefits</p> <ul style="list-style-type: none"> • Most benefits of routing on the host • No requirement for host to run routing • No requirement for redistribute neighbor <p>Caveats</p> <ul style="list-style-type: none"> • Removing a subnet from one ToR and re-adding it to another (hence, network statements from your router process) is a manual process • Network team and server team would have to be in sync, or server team controls the ToR, or automation is being used whenever VM migration happens • When using VMs /containers 	

Anycast with Manual Redistribution	Summary	More Information
	Example Host Config (Ubuntu) <pre> auto lo iface lo inet loopback auto lo:1 iface lo:1 inet static address 172.16.1.2/3 2 up ip route add 0.0.0.0/0 nexthop via 172.16.1.1 dev eth0 onlink nexthop via 172.16.1.1 dev eth1 onlink auto eth1 iface eth2 inet static address 172.16.1.2/3 2 auto eth2 iface eth2 inet static address 172.16.1.2/3 2 </pre>	it is very easy to black hole traffic, as the leafs continue to advertise prefixes even when VM is down <ul style="list-style-type: none"> No L2 adjacency between servers without VXLAN
FHR (First Hop Redundancy)		Additional Information
<ul style="list-style-type: none"> The gateways would be the ToRs, exactly like redistribute neighbor with an equal cost route installed 		

Network Virtualization

LNV with MLAG	Summary	More Inform
	The host runs LACP (Etherchannel/bond) to the pair of ToRs. LNV (see page 279) (Lightweight Network	Benefits <ul style="list-style-type: none"> Layer 2 domain reduction between the pair of ToRs

LNV with MLAG	Summary	More Information
	<p>Virtualization) then transports the L2 bridges across an L3 fabric.</p> <p>Configurations</p> <p>leaf01 Config</p> <pre>/etc/network /interfaces</pre> <pre>auto lo iface lo inet loopback address 10 .0.0.11/32 vxrd-src- ip 10.0.0.11 vxrd- svcnod-e-ip 1 0.10.10.10 clagd- vxlan- anycast-ip 3 6.0.0.11 auto vni-10 iface vni-10 vxlan-id 1 0 vxlan- local- tunnelip 10. 0.0.11 auto br-10 iface br-10 bridge- ports swp1 vni-10</pre> <p>leaf02 Config</p> <pre>/etc/network /interfaces</pre>	<ul style="list-style-type: none"> Aggregates layer i (VLAN have to be on specific switch) Great scaling flexibility High availability <p>Caveats</p> <ul style="list-style-type: none"> Needs to be (with 1) cavea the M sectio page above spanr (see p

LNV with MLAG	Summary	More Information
	<pre> auto lo iface lo inet loopback address 10 .0.0.12/32 Vxrd-src- ip 10.0.0.12 vxrd- svcnode-ip 1 0.10.10.10 clagd- vxlan- anycast-ip 3 6.0.0.11 auto vni-10 iface vni-10 vxlan-id 1 0 vxlan- local- tunnelip 10. 0.0.12 auto br-10 iface br-10 bridge- ports swp1 vni-10 </pre>	
Active/Active	Active/Passive	Demarcation
<ul style="list-style-type: none"> • VRR (see page 240) 	<ul style="list-style-type: none"> • vrrpd (not recommended, not tested, will be asymmetrical) 	<ul style="list-style-type: none"> • ToR leaf exit link
		Additional Information
		<ul style="list-style-type: none"> • Cumulus Linux Lighty Network Virtualization

LNV with MLAG	Summary	More Information
		(LNV) documentation (see p)

Index

4

40G ports [141](#)
logical limitations [141](#)

8

802.1p [144](#)
 class of service [144](#)
802.3ad link aggregation [234](#)

A

ABRs [360](#)
 area border routers [360](#)
access control lists [89](#)
access ports [202](#)
ACL policy files [98](#)
ACL rules [147](#)
ACLs [89, 90, 104](#)
 chains [90](#)
 QoS [104](#)
active-active mode [242, 307](#)
 VRR [242](#)
 VXLAN [307](#)
active image slot [19](#)
active listener ports [467](#)
active-standby mode [242](#)
 VRR [242](#)
Algorithm Longest Prefix Match [340](#)
 routing [340](#)
ALPM mode [340](#)
 routing [340](#)
alternate image slot [19, 23](#)
 accessing [23](#)
AOC cables [13](#)
apt-get [51](#)
area border routers [360](#)
 ABRs [360](#)
arp cache [477](#)

ARP requests 243
VRR 243
AS_PATH setting 385
BGP 385
ASN 373
autonomous system number 373
auto-negotiation 137
autonomous system number 373
BGP 373
autoprovision command 65
autoprovisioning 57

B

bestpath 385
BGP 385
BFD 177, 178
 Bidirectional Forwarding Detection 177
 echo function 178
BGP 372, 374
 Border Gateway Protocol 372
 ECMP 374
BGP peering relationships 383, 383
 external 383
 internal 383
bonds 184, 234
 LACP Bypass 234
boot recovery 420
bpdufilter 164
 and STP 164
BPDU guard 162
 and STP 162
brctl 15, 151, 189, 190, 330, 330
 and STP 151
IGMP snooping 330
MLD snooping 330
bridge assurance 161
 and STP 161
bridges 188, 188, 189, 189, 190, 191, 191, 195, 197, 202, 202, 208, 217
 access ports 202
 adding interfaces 189, 190
 adding IP addresses 195
 IGMP snooping 217
 MAC addresses 191

MTU 191
physical interfaces 189
trunk ports 202
untagged frames 197
VLAN-aware 188, 208

C

cable connectivity 13
cabling 172
 Prescriptive Topology Manager 172
chain 90
cl-acltool 89, 147, 478
CLAG 242
 and VRR 242
clagctl 227
class of service 144
cl-bgp 354
cl-cfg 114, 448
cl-ecmpcalc 400
cl-img-clear-overlay 24, 24
cl-img-pkg 26
cl-img-select 24, 25, 25
cl-license 13
cl-netstat 433
cl-ospf 354, 361
cl-ospf6 354, 369
Clos topology 342
cl-ra 354
cl-rctl 354
cl-resource-query 115, 436
cl-route-check 367
cl-support 416
convergence 341
 routing 341
Cumulus Linux 9, 10, 24, 24, 25, 27, 217, 322
 installing 9, 27
 reprovisioning 24
 reserved VLAN ranges 217
 reverting 24
 uninstalling 25
 upgrading 10
 VXLAN 322
cumulus user 72

D

DAC cables 13
daemons 467
datapath 143
datapath.conf 144
date 68
 setting 68
deb 56
debugging 414
decode-syseeprom 438
differentiated services code point 144
dmidecode 439
dpkg 53
dpkg-reconfigure 67
DSCP 144
 differentiated services code point 144
DSCP marking 147
dual-connected hosts 220
duplex interfaces 135
dynamic routing 180, 344
 and PTM 180
 quagga 344

E

eBGP 374
 external BGP 374
ebtables 89, 95
 memory spaces 95
echo function 178, 178
 BFD 178
 PTM 178
ECMP 344, 366, 374, 1
 BGP 374
 equal cost multi-pathing 344
 monitoring 1
 OSPF 366
ECMP hashing 400, 403
 resilient hashing 403
EGP 345
 Exterior Gateway Protocol 345
equal cost multipath 400

ECMP hashing [400](#)
equal cost multi-pathing [344](#)
 ECMP [344](#)
ERSPAN [479](#)
 network troubleshooting [479](#)
Ethernet management port [11](#)
ethtool [143, 431](#)
 switch ports [143](#)
external BGP [374](#)
 eBGP [374](#)

F

fast convergence [382](#)
 BGP [382](#)
fast leave [333](#)
 IGMP/MLD snooping [333](#)
First Hop Redundancy Protocol [242](#)
 VRR [242](#)

G

globs [131](#)
Graphviz [172](#)

H

hardware [437](#)
 monitoring [437](#)
hardware compatibility list [9](#)
hash distribution [187](#)
HCL [9](#)
head end replication [282](#)
 LNV [282](#)
high availability [217, 343](#)
host entries [436](#)
 monitoring [436](#)
Host HA [217](#)
hostname [11](#)
hsflowd [443](#)
hwclock [69](#)

iBGP 374
 internal BGP 374

ifdown 122

ifplugd 243
 VRR 243

ifquery 126, 471

ifup 122

ifupdown 121

ifupdown2 130, 200, 470, 470, 470
 excluding interfaces 470
 logging 470
 purging IP addresses 130
 troubleshooting 470
 VLAN tagging 200

IGMP snooping 217, 230, 328
 MLAG 230
 VLAN-aware bridges 217

IGP 345
 Interior Gateway Protocol 345

image contents 26

image slots 19, 20, 21, 22
 PowerPC 20
 resizing 22
 x86 21

installing 9
 Cumulus Linux 9

interface counters 433

interface dependencies 125

interfaces 134, 142
 statistics 142

internal BGP 374
 iBGP 374

ip6tables 89

IP addresses 130
 purging 130

iproute2 474
 failures 474

iptables 89

IPv4 routes 375
 BGP 375

IPv6 routes 375
 BGP 375

J

jdoe 231

L

LACP 185, 217

MLAG 217

LACP Bypass 234

layer 3 access ports 15

configuring 15

LDAP 80

leaf-spine topology 342

license 12

installing 12

lightweight network virtualization 280, 282, 282, 315

head end replication 282

service node replication 282

link aggregation 184

Link Layer Discovery Protocol 166

link-local IPv6 addresses 388

BGP 388

link pause 148

datapath 148

link-state advertisement 359

link state monitoring 243

VRR 243

LLDP 166, 171

SNMP 171

lldpcli 167

lldpd 166, 173

LNV 280, 280, 282, 282, 315, 315

head end replication 282

service node replication 282

VXLAN 280, 315

load balancing 344

logging 417, 470, 470

ifupdown2 470

networking service 470

logging neighbor state changes 388

BGP 388

logical switch 217

longest prefix match 1

routing 1

loopback interface 16
 configuring 16
LSA 359
 link-state advertisement 359
LSDB 359
 link-state database 359
lshw 439

M

MAC entries 436
 monitoring 436
Mako templates 131, 472
 debugging 472
mangle table 148
 ACL rules 148
memory spaces 95
 ebtables 95
MLAG 217, 227, 227, 228, 230, 232, 233, 314, 314
 backup link 228
 IGMP snooping 230
 MTU 232
 peer link states 227, 314
 PROTO_DOWN state 314
 protodown state 227
 STP 233
MLD snooping 328
monitoring 67, 414, 431, 436, 442, 443, 445, 487
 hardware watchdog 442
 Net-SNMP 487
 network traffic 443
mount points 21
mstpcctl 151, 204
MTU 137, 191, 232, 474
 bridges 191
 failures 474
 MLAG 232
multi-Chassis Link Aggregation 217
 MLAG 217
multiple bridges 192
mz 477
 traffic generator 477

N

name switch service 79
Netfilter 89
Net-SNMP 487
networking service 470
 logging 470
network interfaces 121, 134
 ifupdown 121
network traffic 443
 monitoring 443
network troubleshooting 485
 tcpdump 485
network virtualization 245, 247, 322
 VMware NSX 247
no-as-set 385
 BGP 385
nonatomic updates 95
 switchd 95
non-blocking networks 343
NSS 79
 name switch service 79
NTP 69
 time 69
ntpd 69

O

ONIE 9, 25
 rescue mode 25
Open Network Install Environment 9
Open Shortest Path First Protocol 358, 369
 OSPFv2 358
 OSPFv3 369
open source contributions 8
OSPF 363, 365, 366, 366, 368
 ECMP 366
 reconvergence 366
 summary LSA 363
 supported RFCs 368
 unnumbered interfaces 365
ospf6d.conf 371
OSPFv2 358
OSPFv3 369, 371, 371

- supported RFCs 371
- unnumbered interfaces 371
- overlayfs file system 20
- over-subscribed networks 343

P

- packages 51
 - managing 51
- packet buffering 143
 - datapath 143
- packet queueing 143
 - datapath 143
- packet scheduling 143
 - datapath 143
- PAM 79
 - pluggable authentication modules 79
- parent interfaces 127
- password 72
 - default 72
- passwordless access 72
- passwords 11
- peer-groups 384
 - BGP 384
- Per VLAN Spanning Tree 151
 - PVST 151
- ping 476
- pluggable authentication modules 79
- policy.conf 100
- port lists 131
- port speeds 135
- Prescriptive Topology Manager 172
- primary image slot 19
- priority groups 144
 - datapath 144
- privileged commands 73
- PROTO_DOWN state 314
 - MLAG 314
- protocol tuning 341, 390
 - BGP 390
 - routing 341
- protodown state 227
 - MLAG 227
- PTM 172, 178

echo function 178
Prescriptive Topology Manager 172
ptmctl 181
ptmd 172
PTM scripts 174
PVRST 151
 Rapid PVST 151
PVST 151
 Per VLAN Spanning Tree 151

Q

QoS 104
 ACLs 104
QSFP 434
Quagga 180, 180, 337, 344, 346
 and PTM 180, 180
 configuring 346
 dynamic routing 344
 static routing 337
quality of service 149
querier 333
 IGMP/MLD snooping 333

R

Rapid PVST 151
 PVRST 151
read-only mode 389
 BGP 389
reconvergence 366
 OSPF 366
remote access 70
repositories 55
 other packages 55
rescue mode 25
reserved VLAN ranges 217
resilient hashing 403
restart 115
 switchd 115
root user 11, 72
route advertisements 373
 BGP 373

route entries 340, 340

ALPM 340

limitations 340

route maps 390

BGP 390

route reflectors 374

BGP 374

routes 436

monitoring 436

routing protocols 341

RSTP 151

S

sensors command 439

serial console management 11

service node replication 282

 LNV 282

services 467

sFlow 443

sFlow visualization tools 445

SFP 143, 434

 switch ports 143

single user mode 420

smonctl 441

smond 441

snmpd 487

sources.list 55

SPAN 479

 network troubleshooting 479

spanning tree parameters 153

Spanning Tree Protocol 150, 208

 STP 150

 VLAN-aware bridges 208

SSH 70

SSH keys 71

static routing 335, 337

 with ip route 335

 with Quagga 337

STP 150, 161, 233

 and bridge assurance 161

MLAG 233

 Spanning Tree Protocol 150

stub areas 364

- OSPF 364
- sudo 72, 73
- sudoers 73, 74
 - examples 74
- summary LSA 363
 - OSPF 363
- SVI 222
 - switched virtual interface 222
- switchd 95, 112, 113, 115, 448
 - configuring 112
 - counters 448
 - file system 113
 - nonatomic updates 95
 - restarting 115
- switched virtual interface 222
 - SVI 222
- switch ports 14, 141
 - configuring 14
 - logical limitations 141
- syslog 417
- system management 414

T

- tcpdump 485
 - network troubleshooting 485
- templates 131
- time 68
 - setting 68
- time zone 12, 67
- topology 172, 342
 - data center 172
- traceroute 476
- traffic.conf 144
- traffic distribution 187
- traffic generator 477
 - mz 477
- traffic marking 147
 - datapath 147
- troubleshooting 414, 420, 485
 - single user mode 420
 - tcpdump 485
- trunk ports 197, 202
- tzdata 67

U

U-Boot 9, 414
unnumbered interfaces 365, 371
 OSPF 365
 OSPFv3 371
untagged frames 197
 bridges 197
upgrading 10
 Cumulus Linux 10
user accounts 72, 72
 cumulus 72
 root 72
user authentication 79
user commands 130
 interfaces 130

V

virtual device counters 445, 449, 449
 monitoring 445
 poll interval 449
 VLAN statistics 449
virtual router redundancy 240
visudo 73
VLAN 222, 445
 statistics 445
 switched virtual interface 222
VLAN-aware bridges 188, 208, 208, 209, 217
 configuring 209
 IGMP snooping 217
 Spanning Tree Protocol 208
VLAN tagging 200, 200, 202
 advanced example 202
 basic example 200
VLAN translation 207
VRR 240
 virtual router redundancy 240
VTEP 245, 248
vtysh 349
 quagga CLI 349
VXLAN 245, 248, 280, 307, 315, 322, 445
 active-active mode 307

LNV 280, 315
no controller 322
statistics 445
VMware NSX 248

W

watchdog 442
monitoring 442

Z

zebra 345
routing 345
zero touch provisioning 57, 60
USB 60
ZTP 57