



## **Cisco Tetration (Secure Workload) M4 Cluster Hardware Deployment Guide**

**First Published:** 2016-08-11

**Last Modified:** 2022-08-17

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2016–2022 Cisco Systems, Inc. All rights reserved.



# CHAPTER 1

## Overview

---

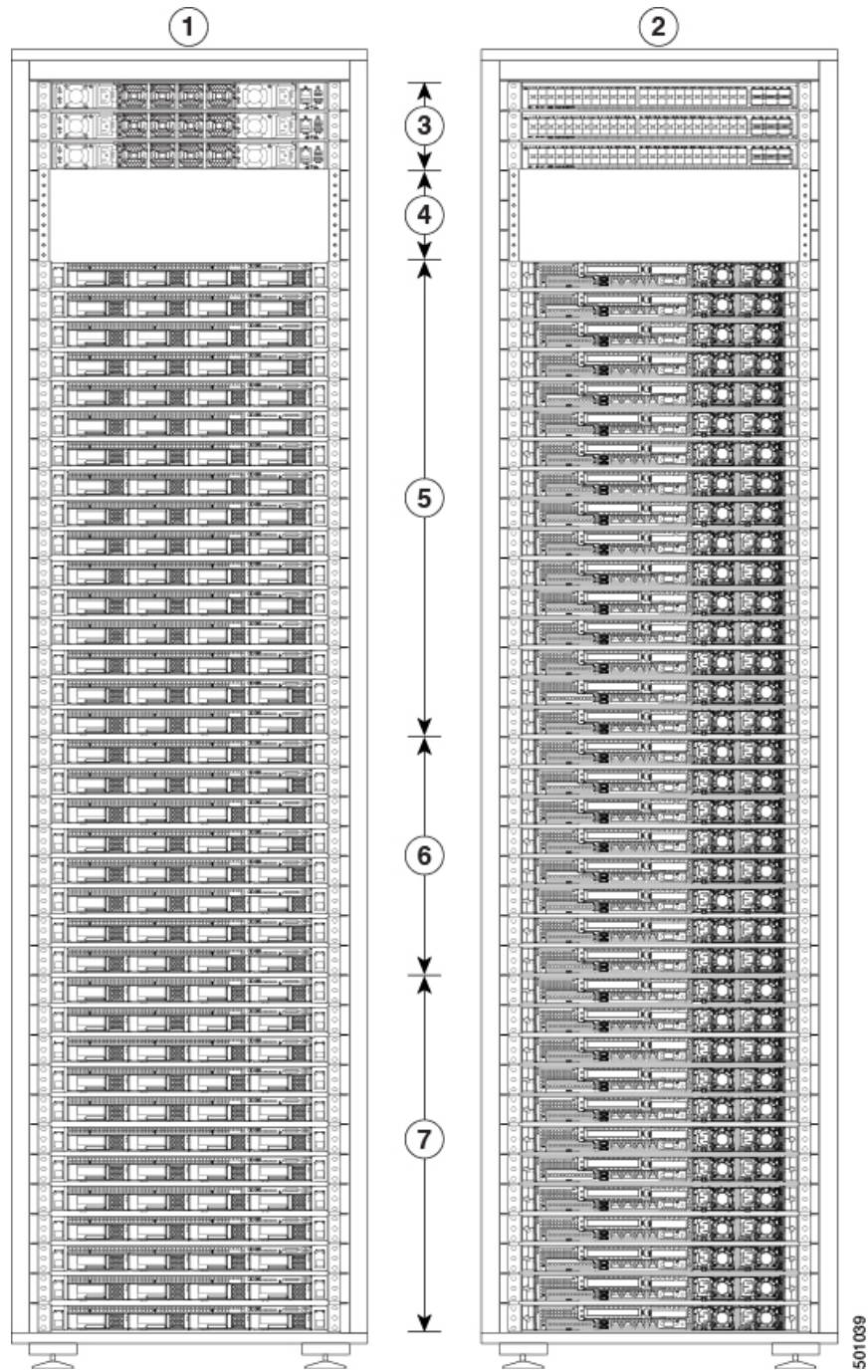
- [Installation Overview, on page 1](#)

## Installation Overview

You can deploy the Cisco Tetration (Secure Workload) M4 cluster as either a 39-rack unit (RU) large-form factor platform (C1-Tetration) for data centers with more than 5000 servers or as an 8-RU small-form factor platform (C1-Tetration-M) for data centers with fewer than 5000 servers. Additionally, you can deploy the large-form factor platform in either one or two racks depending upon your requirements.

The Cisco Tetration (Secure Workload) M4 cluster deployments are configured as follows:

- Large-form factor 39-RU Cisco Tetration (Secure Workload) platform in one rack (C1-Tetration single rack)

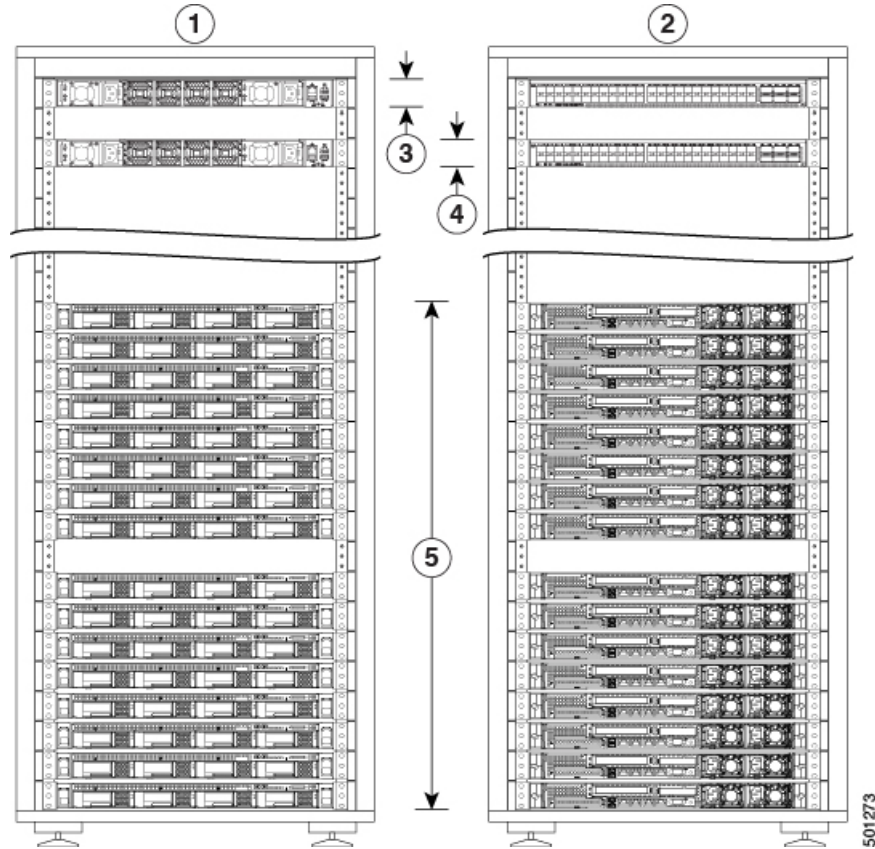


1	Cold aisle view	5	16 compute servers (RUs 21 to 36)
2	Hot aisle view	6	8 cache servers (RUs 13 to 20)

3	1 Spine (RU 42) and 2 leaf switches (RUs 40 and 41)	7	12 base servers (RUs 1 to 12)
4	Open rack units (RUs 37 to 39)		

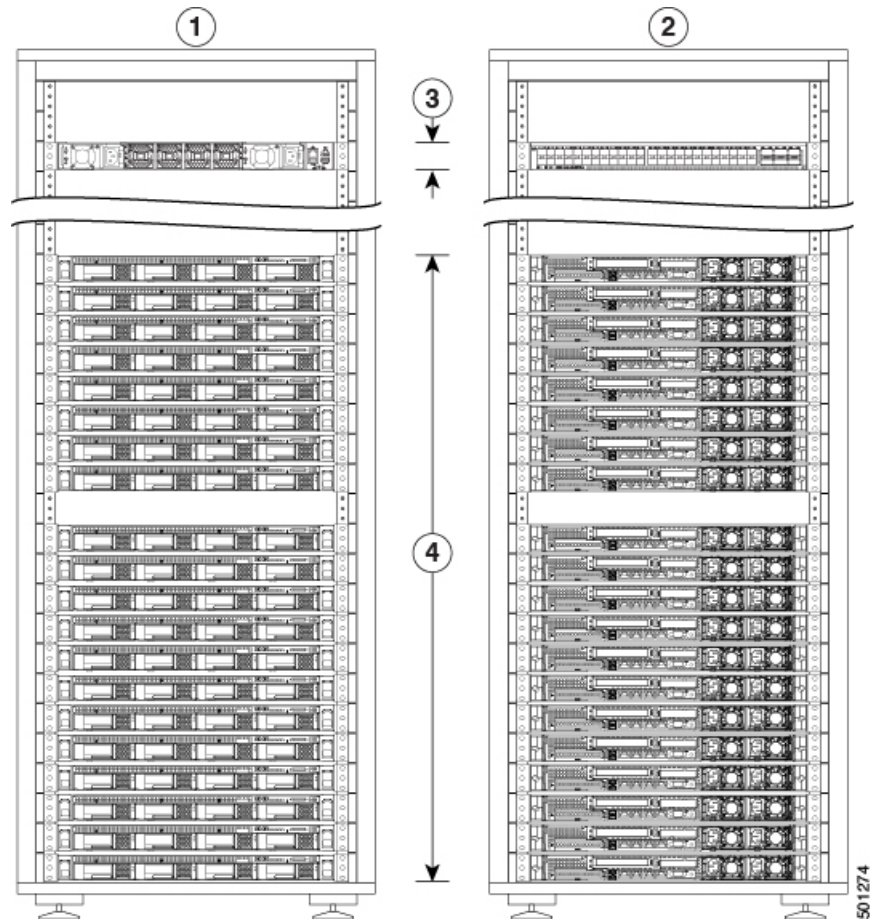
- Large-form factor Cisco Tetration (Secure Workload) platform in two racks (C1-Tetration dual rack)

- Rack 1



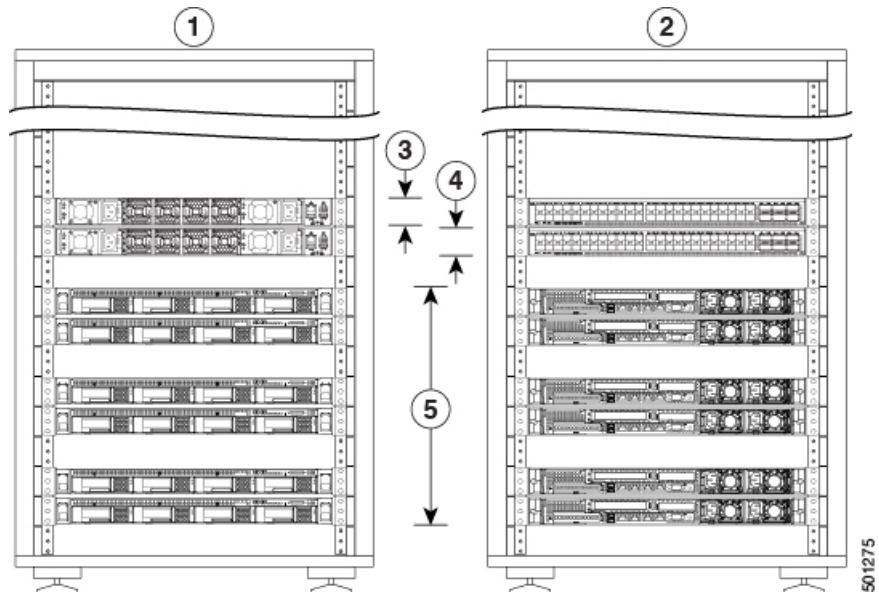
1	Cold aisle view	4	Leaf 1 switch (RU 40)
2	Hot aisle view	5	16 compute servers (RUs 1 to 4 and 6 to 9)
3	1 Spine switch (RU 42)		

- Rack 2



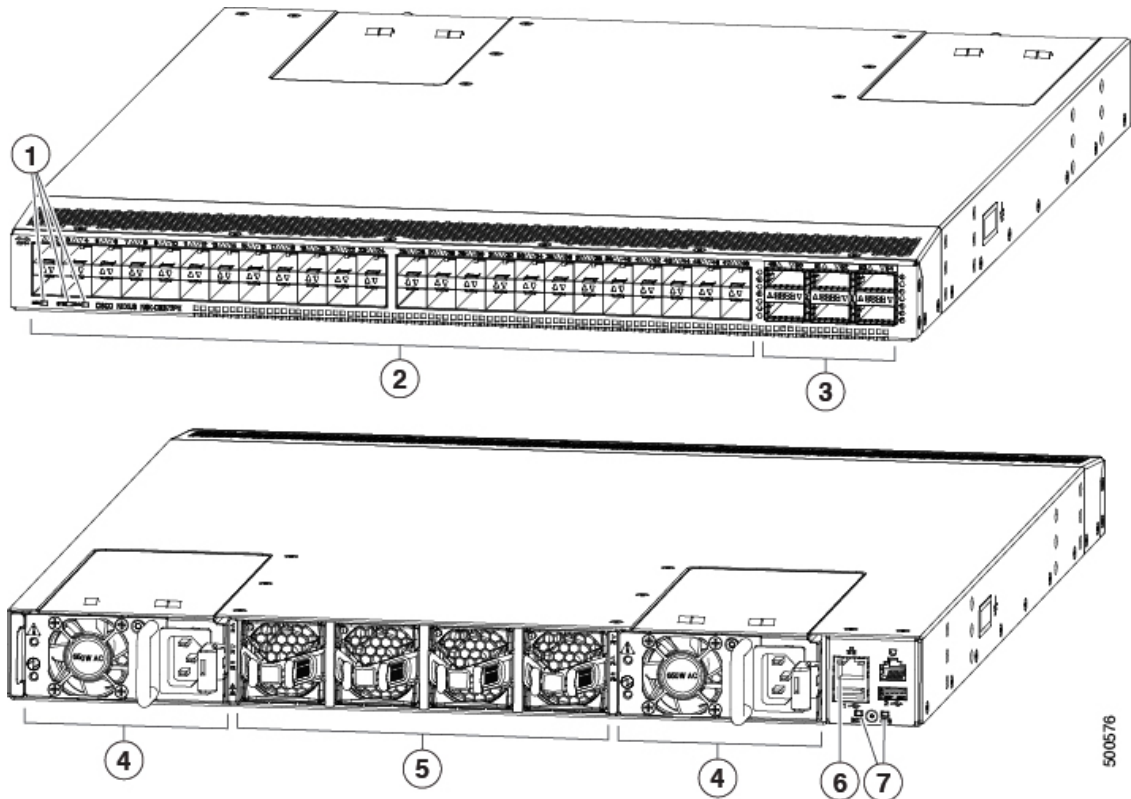
1	Cold aisle view	3	Leaf 2 switch (RU 40)
2	Hot aisle view	4	8 cache servers (RUs 14 to 21) and 12 base servers (RUs 1 to 12)

- Small-form factor 8-RU Cisco Tetration (Secure Workload) platform in one rack (C1-Tetration-M)



1	Cold aisle view	4	Leaf switch (RU 11)
2	Hot aisle view	5	6 universal servers (RUs 2, 3, 5, 6, 8, and 9)
3	Leaf switch (RU 12)		

The switches have 48 10-Gigabit Ethernet ports numbered 1 to 48 and six 40-Gigabit Ethernet ports numbered 49 through 54. The following figure shows both ends of a switch and identifies these features.



1	Beacon (BCN), Status (STS), and Environment (ENV) LEDs	5	Fan modules (blue handles indicate port-side exhaust airflow)
2	10-Gigabit ports (48) numbered from 1 to 48	6	Management port
3	40-Gigabit ports (6) numbered from 49 to 54	7	Beacon and Status (STS) LEDs
4	AC Power supply (blue coloring indicates port-side exhaust airflow)		—

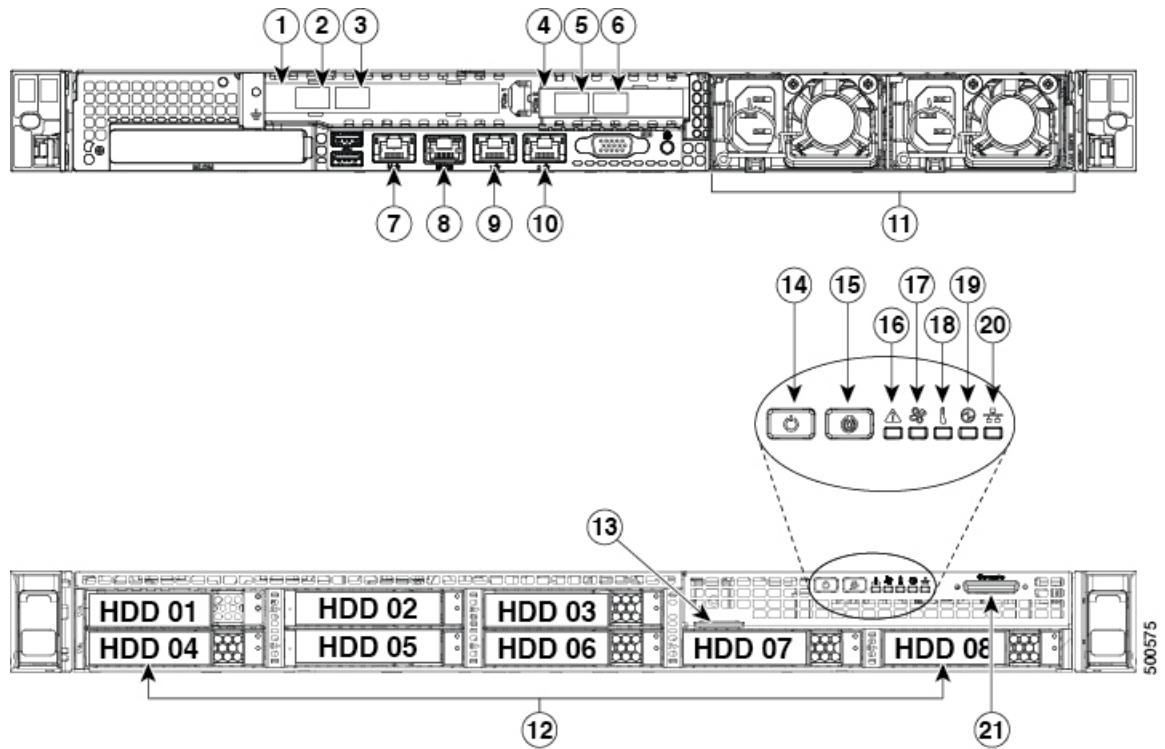
The large-form factor switches have servers that perform as compute, cache, and base nodes. The small-form factor switches have servers that perform as universal nodes. The following table specifies the characteristics of these servers.

Server Type	Storage Drives in Each Server	RAM	RAID Cache
Compute node (16 servers in the large-form factor platform)	1.2-TB drive (1 in slot 1) 1.8-TB drives (7 in slots 2 to 8)	512 GB	4 GB



Server Type	Storage Drives in Each Server	RAM	RAID Cache
Cache node (8 servers in the large-form factor platform)	400-GB drives (8)	512 GB	2 GB
Base node (12 servers in the large-form factor platform)	1.2-TB drives (8)	256 GB	2 GB
Universal node (6 servers in the small-form factor platform)	1.6 TB SSD drives (5) 3.6 TB SSD drives (3)	1024 GB	2 GB

For the servers, the 10-Gigabit interface ports (eth2, eth3, eth5, and eth4) are located in the two PCIe risers, and the management port is located below the PCIe risers as shown in the following figure.



1	PCIe riser 1	12	Drive bays
2	eth2 port (first interface port)	13	Pull-out asset tag
3	eth3 port (second interface port)	14	Power button/power status LED
4	PCIe riser 2	15	Beacon LED

5	eth5 port (fourth interface port)	16	System status LED
6	eth4 port (third interface port)	17	Fan status LED
7	Management interface	18	Temperature status LED
8	Serial port	19	Power status LED
9	eth0 port (CIMC port)	20	Network activity LED
10	eth1 port	21	Console port
11	AC Power supplies		—



## CHAPTER 2

# Preparing the Site

---

- [Temperature Requirements, on page 9](#)
- [Humidity Requirements, on page 9](#)
- [Altitude Requirements, on page 10](#)
- [Dust and Particulate Requirements, on page 10](#)
- [Minimize Electromagnetic and Radio Frequency Interference, on page 10](#)
- [Shock and Vibration Requirements, on page 11](#)
- [Grounding Requirements, on page 11](#)
- [Power Requirements, on page 11](#)
- [Airflow Requirements, on page 12](#)
- [Clearance Requirements, on page 12](#)

## Temperature Requirements

The Tetration (Secure Workload) cluster switches and servers require an operating temperature of 41 to 95°F (5 to 35°C) with a derating of the maximum temperature by 1°C for every 1000 feet (305 m) in elevation above sea level. If these devices are not operating, the temperature must be between -40 to 149°F (-40 to 65°C).

## Humidity Requirements

High humidity can cause moisture to enter the switches and servers. Moisture can cause corrosion of internal components and degradation of properties such as electrical resistance, thermal conductivity, physical strength, and size. The switches and servers are rated to operate at 10 to 80 percent relative humidity, with a humidity gradation of 10 percent per hour. For nonoperating conditions, these devices can withstand from 5 to 93 percent relative humidity.

Buildings in which the climate is controlled by air-conditioning in the warmer months and by heat during the colder months usually maintain an acceptable level of humidity for the devices. However, if the devices are located in an unusually humid location, you should use a dehumidifier to maintain the humidity within an acceptable range.

## Altitude Requirements

If you operate rack devices at a high altitude (low pressure), the efficiency of forced and convection cooling is reduced and can result in electrical problems that are related to arcing and corona effects. This condition can also cause sealed components with internal pressure, such as electrolytic capacitors, to fail or to perform at a reduced efficiency. These devices are rated to operate at altitudes from 0 to 10,000 feet (0 to 3,050 m), and can be stored at altitudes of 0 to 40,000 feet (12,200 m).

## Dust and Particulate Requirements

Fans cool power supplies, switches, and servers by drawing in air and exhausting air out through various openings in the chassis. However, fans also ingest dust and other particles, causing contaminant buildup in the switch and increased internal chassis temperature. A clean operating environment can greatly reduce the negative effects of dust and other particles, which act as insulators and interfere with the mechanical components in the switches and servers.

In addition to regular cleaning, follow these precautions to avoid contamination of rack switches and servers:

- Do not permit smoking near the rack.
- Do not permit food or drink near the rack.

## Minimize Electromagnetic and Radio Frequency Interference

Electromagnetic interference (EMI) and radio frequency interference (RFI) from the devices in the Tetration (Secure Workload) cluster rack can adversely affect other devices such as radio and television (TV) receivers operating near the rack. Radio frequencies that emanate from the devices in the rack can also interfere with cordless and low-power telephones. Conversely, RFI from high-power telephones can cause spurious characters to appear on the device monitors.

RFI is any EMI with a frequency above 10 kHz. This type of interference can travel from the switch to other devices through the power cable and power source or through the air as transmitted radio waves. The Federal Communications Commission (FCC) publishes specific regulations to limit the amount of EMI and RFI that can be emitted by computing equipment. Each switch meets these FCC regulations.

When wires are run for any significant distance in an electromagnetic field, interference can occur between the field and the signals on the wires with the following implications:

- Bad wiring can result in radio interference emanating from the plant wiring.
- Strong EMI, especially when it is caused by lightning or radio transmitters, can destroy the signal drivers and receivers in the chassis and even create an electrical hazard by conducting power surges through lines into equipment.



---

**Note** To predict and prevent strong EMI, consult experts in RFI.

---

The wiring is unlikely to emit radio interference if you use twisted-pair cable with a good distribution of grounding conductors. If you exceed the recommended distances, use a high-quality twisted-pair cable with one ground conductor for each data signal when applicable.



**Caution** If the wires exceed the recommended distances, or if wires pass between buildings, give special consideration to the effect of a lightning strike in your vicinity. The electromagnetic pulse caused by lightning or other high-energy phenomena can easily couple enough energy into unshielded conductors to destroy electronic devices. Consult experts in electrical surge suppression and shielding if you have had similar problems in the past.

## Shock and Vibration Requirements

The devices in the Tetration (Secure Workload) cluster devices have been shock- and vibration-tested for operating ranges, handling, and earthquake standards.

## Grounding Requirements

The devices in the Tetration (Secure Workload) cluster are sensitive to variations in voltage supplied by the power sources. Overvoltage, undervoltage, and transients (or spikes) can erase data from the memory or cause components to fail. To protect against these types of problems, make sure that there is an earth-ground connection for the devices. You must connect the rack to the facility earth ground.

You must provide the grounding wire to make this connection. Size the grounding wire to meet local and national installation requirements. Depending on the power supply and system, a 12-AWG to 6-AWG copper conductor is required for U.S. installations (for those installations, we recommend that you use commercially available 6-AWG wire). The length of the grounding wire depends on the proximity of the rack to facility earth ground connection.

## Power Requirements

The Tetration (Secure Workload) clusters must be provisioned with power sources that provide the following amounts of power for operations:

- 39-RU large-form factor platform, single rack: 22,500 W
- 39-RU large-form factor platform, dual rack: 11,500 W for each rack
- 8-RU small-form factor platform: 5,500 W

For the required  $n+n$  power redundancy, you need two AC power sources that each provide that amount of power.

Each chassis in the rack has two power supplies, one for operations and the other for redundancy. Each power supply is connected to a different power strip on the rack, and each power strip is connected to a different AC power source. If one power source fails, the other one provides the required power for each switch or server in the rack.

## Airflow Requirements

The Tetration (Secure Workload) cluster requires that you position each rack with the power supplies and fans on the three switches in a cold aisle. When positioned this way, all the devices in the rack take in cooling air from a cold aisle and exhaust hot air to a hot aisle.

## Clearance Requirements

The following table lists the amount of space required to install the 39-RU large-form factor (single- or dual-rack) or 8-RU small-form factor Tetration (Secure Workload) cluster. The installation aisle must be more than 24 inches (61 cm) wide for moving the rack into place. Additionally, you must have enough room for a person to access the front and rear to perform maintenance.

Installation Type	Aisle Minimum Width <sup>1</sup>	Rack Installation Minimum Space
C1-Tetration (Single-Rack) Installation	24 inches (61 cm)	24 inches (61 cm) wide by 43.38 inches (110.2 cm) deep
C1-Tetration (Dual-Rack)	24 inches (61 cm)	48 inches (122 cm) wide by 43.38 inches (110.2 cm) deep
C1-Tetration-M	24 inches (61 cm)	24 inches (61 cm) wide by 43.38 inches (110.2 cm) deep

<sup>1</sup> The Installation aisle and the aisle that the front door of the rack opens must be at least 24 inches (61 cm) wide. The other aisle, in which the double cabinet doors open, must be at least 12 inches (30.5 cm) wide for the doors to fully open but at least 24 inches (61 cm) is needed for a person to perform maintenance.

The rack is positioned with the switch fans (the side of the rack with the largest door) facing the cold aisle and the switch ports (the side of the rack with double doors) facing the hot aisle.



## CHAPTER 3

# Powering Up and Connecting the Devices

- [Ground the Tetration \(Secure Workload\) Cluster Devices, on page 13](#)
- [Power Up the Tetration \(Secure Workload\) Cluster Devices, on page 13](#)
- [Connect the Tetration \(Secure Workload\) Cluster to Your Routers, on page 14](#)

## Ground the Tetration (Secure Workload) Cluster Devices

The Tetration (Secure Workload) cluster devices have metal-to-metal connections to their rack, so as soon as you ground the rack (or racks for a dual-rack installation) to your data center earth ground, the devices in the rack are grounded. To ground a rack, connect the rack wheels to the earth ground.

## Power Up the Tetration (Secure Workload) Cluster Devices

To power up the switch, you must connect two power strips that are attached to the rack to two AC power sources.



---

**Note** Connect this equipment to AC mains that have a surge protective device (SPD) at the service equipment that complies with NFPA 70, the National Electrical Code (NEC).

Read the installation instructions before using, installing, or connecting the system to the power source.

Do not overload the wiring when you connect the units to the supply circuit.


---

### Before you begin

- The racks must be installed in the data center and secured in place with their air intakes positioned in a cold aisle.
- The racks must be grounded to the data center earth ground.
- The cluster must be connected to two customer-supplied routers (each router connected to a separate leaf switch).
- There must be two power sources that meet the rack power requirements within reach of each rack power-strip cables.

### Procedure

---

- Step 1** Plug the power cable for one power strip into an AC power source and plug the power cable for the second power strip into another AC power source.
- Step 2** Look at each power supply installed in each of the rack devices to verify that the  LED is lit and green.
- If none of the LEDs are lit, make sure that the power source is turned on and that the on/off switch on the rack power strip is turned on.
  - If some of these LEDs are lit and others are not lit, make sure that the power cable coming from that power supply is fully connected to the power strip on the rack.
- 

### What to do next

You are ready to set up the user interface.

## Connect the Tetration (Secure Workload) Cluster to Your Routers

You must connect the Tetration (Secure Workload) cluster to two routers.

### Procedure

---

- Step 1** If you are installing a 39-RU large-form factor dual-rack cluster, connect the partially connected interface cables on each rack. For each of these cables, connect it to the labeled port on the other rack.
- Step 2** Use a 10-Gigabit cable to connect a router to port E1/39 on the leaf 1 switch for a 39-RU deployment, or to port E1/47 for an 8-RU deployment. The leaf 1 switch is located in the following location:
- 39-RU large-form factor single rack platform—RU 40 in the platform rack
  - 39-RU large-form factor dual rack platform—RU 40 in rack 1
  - 8-RU small-form factor platform—RU 12 in the platform rack
- Step 3** Use a 10-Gigabit cable to connect a router to port E1/39 on the leaf 2 switch for a 39-RU deployment, or to port E1/47 for an 8-RU deployment. The leaf 2 switch is located in the following location:
- 39-RU large-form factor single rack platform—RU 41 in the platform rack
  - 39-RU large-form factor dual rack platform—RU 41 in rack 2
  - 8-RU small-form factor platform—RU 11 in the platform rack
-





## CHAPTER 4

# Setting Up the User Interface

- [\(Optional\) Requirements and Limitations for Dual-Stack Mode \(IPv6 Support\)](#), on page 15
- [Set Up the User Interface](#), on page 16

## (Optional) Requirements and Limitations for Dual-Stack Mode (IPv6 Support)

Secure Workload clusters running on physical hardware can be configured to use IPv6 in addition to IPv4 for certain communications to and from the cluster.



---

**Note** You can use the Dual-Stack Mode (IPv6 support) feature when installing or upgrading to 3.6.1.5 and 3.7.1.5 releases, however, the feature is not available when you are installing or upgrading to patch releases.

---

### Limitations

If you are considering enabling dual stack mode, note the following:

- You can enable IPv6 connectivity only during initial deployment or upgrade to a major release (you cannot enable this feature during patch upgrades.)
- Dual-stack mode is supported only on physical hardware/bare-metal clusters.
- There is no support for an IPv6-only mode.
- You cannot revert to IPv4-only mode after dual stack mode is enabled for the cluster.
- Data Backup and Restore (DBR) is not supported if dual-stack connectivity is enabled.
- Do not enable dual-stack mode for clusters configured with Federation.
- The following features always and only use IPv4 (note that IPv4 is always enabled even if IPv6 is enabled):
  - (Applicable for release 3.7.1.5 and 3.6.x) Enforcement on AIX agents
  - (Applicable for release 3.6.x) Hardware agent communication with the cluster
  - (Applicable for release 3.6.x) Connectors for flow ingestion, inventory enrichment, or alert notifications

### Requirements

- You must configure both A and AAAA DNS records for FQDN. You must configure this before you enable dual stack mode for your cluster.
- External services such as NTP, SMTP, and DNS should be available over both IPv4 and IPv6, for redundancy purposes.
- In order to configure dual stack mode for a cluster:
  - The two cluster leaf switches will each need to be allocated routable IPv6 addresses on two different networks, for redundancy, and default gateways will need to be provided for each network.
  - For 39RU clusters, a site routable IPv6 network with space for at least 29 host addresses is required.
  - For 8RU clusters, a site routable IPv6 network with space for at least 20 host addresses is required.
  - The first three host addresses of the site routable IPv6 network are reserved for the Cisco Secure Workload cluster HSRP configuration and must not be used by any other devices.

### Additional Information

Agents communicate with the cluster using IPv4 unless you configure them to use IPv6. For instructions, see the User Guide available from the Secure Workload portal.

## Set Up the User Interface

### Before you begin

- To complete this configuration, you need a device such as a laptop computer with an Ethernet port and access to the internet.
- You need an Ethernet cable to connect the device to the highest server in the Tetration (Secure Workload) cluster.
- Google Chrome is the only supported browser for the Setup portal, which is required for part of this process.
- (Optional) Beginning with version 3.6 and later, you can configure your cluster in dual-stack mode, which allows both IPv4 and IPv6 to be used for communication between certain Secure Workload components and between Secure Workload and network services such as NTP and DNS. (Secure Workload already handles IPv6 traffic, whether or not you enable dual-stack mode.) You can enable this support only during deploy or upgrade.

If you are considering enabling support for IPv6, see [\(Optional\) Requirements and Limitations for Dual-Stack Mode \(IPv6 Support\)](#), on page 15.




---

**Important** Enter IPv4 addresses in all fields in the procedure below unless the field name explicitly states IPv6.

---

## Procedure

---

- Step 1** Configure the internet device with an IP address of 2.2.2.1/30 (255.255.255.252).
- Step 2** Use an Ethernet cable to connect the Ethernet port on the internet device to the ETH1 port on the highest server in the top of the Tetration (Secure Workload) cluster.
- Step 3** On the internet device, open the Chrome browser and go to `http://2.2.2.2:9000`.
- Note** The Chrome browser is the only browser tested with this process.
- The Tetration (Secure Workload) Setup Diagnostics page opens.
- Step 4** If there are errors in the Diagnostics page, check the cabling connections between cluster devices for broken connections or cables routed incorrectly (use the cabling tables in the appendix to verify all cabling) before continuing with this procedure. When done, return to Step 2.
- Step 5** Click **Continue**.
- The RPM Upload page opens.
- Note** If the Site Config page opens instead, enter the following URL to open the RPM Upload page:  
`http://2.2.2.2:9000 /upload`
- Step 6** Upload RPM objects to the Tetration (Secure Workload) cloud as follows:
- Click **Choose File**.
  - Browse to find the `adhoc` and `mother` files.
  - Click **Upload**.
- The Site Config page opens.
- Step 7** Use the Site Config page to set up the new site as follows:
- **General** form
    - In the **Site Name** field, enter the unique cluster name.
    - In the **SSH Public Key** field, paste in the authentication key.

**Note** Generate your own SSH key pair, which can be used for cluster SSH access.
    - Click **Next**.
  - **Email** form
    - Fill in the required email addresses.
    - Click **Next**.
  - **L3** form
- Enter each of the requested addresses. All fields with \* are required fields. Enter all addresses as IPv4 unless the field name specifies IPv6.

(Optional) If you are installing software version 3.6 or later: To enable dual-stack mode (support for both IPv4 and IPv6):

- a. Check the IPv6 checkbox.
- b. Enter the IPv6 address in CIDR notation for both Leaf 1 and Leaf 2 switches.
- c. Enter the Leaf 1 and Leaf 2 IPv6 Default Gateway.
- d. Click **Next**.

• **Network** form

Enter all addresses as IPv4 unless the field name specifies IPv6.

- a. In the **Internal network IP address** field, paste in the address from the orchestrator deployment output.
- b. In the **External network IP address** field, paste in the address from the orchestrator deployment output.
- c. In the **External gateway IP address** field, paste in the address from the orchestrator deployment output.
- d. In the **DNS resolver IP address** field, paste in the address from the orchestrator deployment output.
- e. In the **DNS domain** field, enter your DNS domain (for example, "cisco.com").
- f. (Software version 3.6 or later) If you enabled IPv6 on the L3 page, **IPv6** is automatically selected.

If IPv6 is selected, you must specify IPv6 addresses reserved for Secure Workload use:

- Enter the **External IPv6 Network**.

The first 3 IPv6 addresses in the IPv6 External Network field are always reserved for the switches of the Secure Workload cluster and should not be used for any other purpose.

- If you want to use IPv6 only for certain addresses, enter those addresses in the **External IPv6 IPs** field.

- Note**
- For a 39 RU cluster, ensure that at least 29 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.
  - For an 8 RU cluster, ensure that at least 20 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.

- g. Click **Next**.

• **Service** form

- a. In the **NTP Servers** field, enter the space-separated list of NTP server names or IP addresses from the Orchestrator deployment output.
- b. In the **SMTP Server** field, enter the name or IP address of an SMTP server that can be used by Tetration (Secure Workload) for sending email messages (this server must be accessible by Tetration (Secure Workload)).

- c. In the **SMTP Port** field, enter the port number of the SMTP server. AWS restricts the use of ports 25 and 465. You must configure your account correctly or use port 587.
  - d. (Optional) In the **SMTP Username** field, enter the user name for SMTP authentication.
  - e. (Optional) In the **SMTP Password** field, enter the password for SMTP authentication.
  - f. (Optional) In the **HTTP Proxy Server** field, enter the name or IP address of an HTTP proxy server that will be used by Tetration (Secure Workload) to access external services on the internet.
  - g. (Optional) In the **HTTP Proxy Port** field, enter the port number for the HTTP proxy server.
  - h. (Optional) In the **HTTPs Proxy Server** field, enter the name or IP address of an HTTPs proxy server that will be used by Tetration (Secure Workload) to access external services on the internet.
  - i. (Optional) In the **HTTPs Proxy Port** field, enter the port number for the HTTPs proxy server.
  - j. (Optional) In the **Syslog Server** field, enter the name or IP address of a syslog server that can be used by Tetration (Secure Workload) to send alerts.
  - k. (Optional) In the **Syslog Port** field, enter the port number of the syslog server.
  - l. (Optional) In the **Syslog Severity** field, enter severity level for the syslog messages. The possible values include informational, notice, warning, error, critical, alert, and emergency.
  - m. Click **Next**.
- **UI form**
    - a. In the **UI VRRP VRID** field, enter "77" unless you need a unique VRID.
    - b. In the **UI FQDN** field, enter the fully qualified domain name where you will access the cluster.
    - c. In the **UI Airbrake Key** field, leave blank.
    - d. Click **Next**.

Tetration (Secure Workload) validates your configuration settings and displays the status for the settings.
  - **Advanced form**
    - a. In the **External IPs** field, enter IPv4 addresses.
    - b. Click **Continue**.

**Step 8** If there are any failures, click **Back** and edit the configuration (see Step 7).

**Note** You cannot modify these settings in the setup GUI after leaving this page. However, you can modify the settings later from the company page in the GUI.

**Step 9** If there are no failures noted for your configuration and you do not need to make any changes, click **Continue**. Tetration (Secure Workload) is configured according to the settings that you specified. This process can take one to two hours without any interaction on your part.

### What to do next

If you deployed software version 3.6 or later and you enabled IPv6 connectivity:

- You can access the Cisco Secure Workload web portal using either IPv4 or IPv6.
- By default, software agents communicate with the Secure Workload cluster using IPv4 even if the cluster is enabled to support IPv6. If you want supported agents to use IPv6 for this purpose, you must configure the **Sensor VIP FQDN** field on the **Platform > Cluster Configuration** page in the Secure Workload web portal. For important instructions, see the user guide, available as online help from the Secure Workload web portal or from <https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html>.



# APPENDIX **A**

## System Specifications

- [Environmental Specifications, on page 21](#)
- [Cables Included with the Hardware, on page 21](#)
- [Cabling the C1-Tetration Cluster Devices, on page 23](#)
- [Cabling the C1-Tetration-M Cluster Devices, on page 36](#)

## Environmental Specifications

The following table lists the environmental specifications required for installing the Tetration (Secure Workload) cluster.

**Table 1: Environmental Specifications**

Environment		Specification
Temperature	Operating	41 to 95°F (5 to 35°C) with derating the maximum temperature by 1°C for every 1000 ft (305 m) above sea level
	Storage	-40 to 149°F (-40 to 65°C)
Humidity	Operating	10 to 80% relative humidity with a humidity gradation of 10% per hour
	Storage	5 to 93% relative humidity
Altitude	Operating	0 to 10,000 ft (0 to 3050 m)
	Storage	0 to 40,000 ft (0 to 12,200 m)

## Cables Included with the Hardware

The following tables list the cables that are included with the cluster hardware.

**Table 2: Tetration (Secure Workload) 39-RU Cluster, Single-Rack Configuration**

Part Number	Description	Quantity
TA-RACK-UCS2-INT	Cisco R42612 dynamic rack, with side panels for Cisco Tetration	1
TA-ETH-RJ45-SINGLE	RJ45 cable kit for a 39 RU Cisco Tetration single rack configuration	1
TA-SFP-H10GB-CU2M	10GBASE-CU SFP+ 2-meter cable	16
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ 1.5-meter cable	32
TA-QSFP-H40G-CU1M	40GBASE-CR4 passive copper 1-meter cable	4
TA-SFP-H10GB-CU1M	10GBASE-CU SFP+ 1-meter cable	25
TA-SFP-H10GB-CU2-5	10GBASE-CU SFP+ 2.5-meter cable	20

**Table 3: Tetration (Secure Workload) 39-RU Cluster, Dual-Rack Configuration**

Part Number	Description	Quantity
TA-RACK-UCS2-INT	Cisco R42612 dynamic rack, with side panels for Cisco Tetration	2
TA-ETH-RJ45-DUAL	RJ45 cable kit for a 39 RU Cisco Tetration single rack configuration	1
TA-SFP-H10GB-CU2M	10GBASE-CU SFP+ 2-meter cable	15
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ 1.5-meter cable	19
TA-QSFP-H40G-CU1M	40GBASE-CR4 passive copper 1-meter cable	1
TA-QSFP-H40G-CU5M	40GBASE-CR4 passive copper 5-meter cable	3
TA-SFP-H10GB-CU2-5	10GBASE-CU SFP+ 2.5-meter cable	12
TA-SFP-H10GB-CU5M	10GBASE-CU SFP+ 5-meter cable	47

**Table 4: Tetration (Secure Workload) 8-RU Cluster**

Part Number	Description	Quantity
TA-RACK-UCS2-INT	Cisco R42612 dynamic rack, with side panels for Cisco Tetration	1
CAB-ETH-S-RJ45	RJ-45 straight-through yellow 6-foot cable for Ethernet	6
TA-SFP-H10GB-CU1M	10GBASE-CU SFP+ 1-meter cable	13
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ 1.5-meter cable	12
TA-QSFP-H40G-CU1M	40GBASE-CR4 passive copper 1-meter cable	2
GLC-TE	1000BASE-T SFP transceiver module for Category 5 copper wire	6



## Cabling the C1-Tetration Cluster Devices

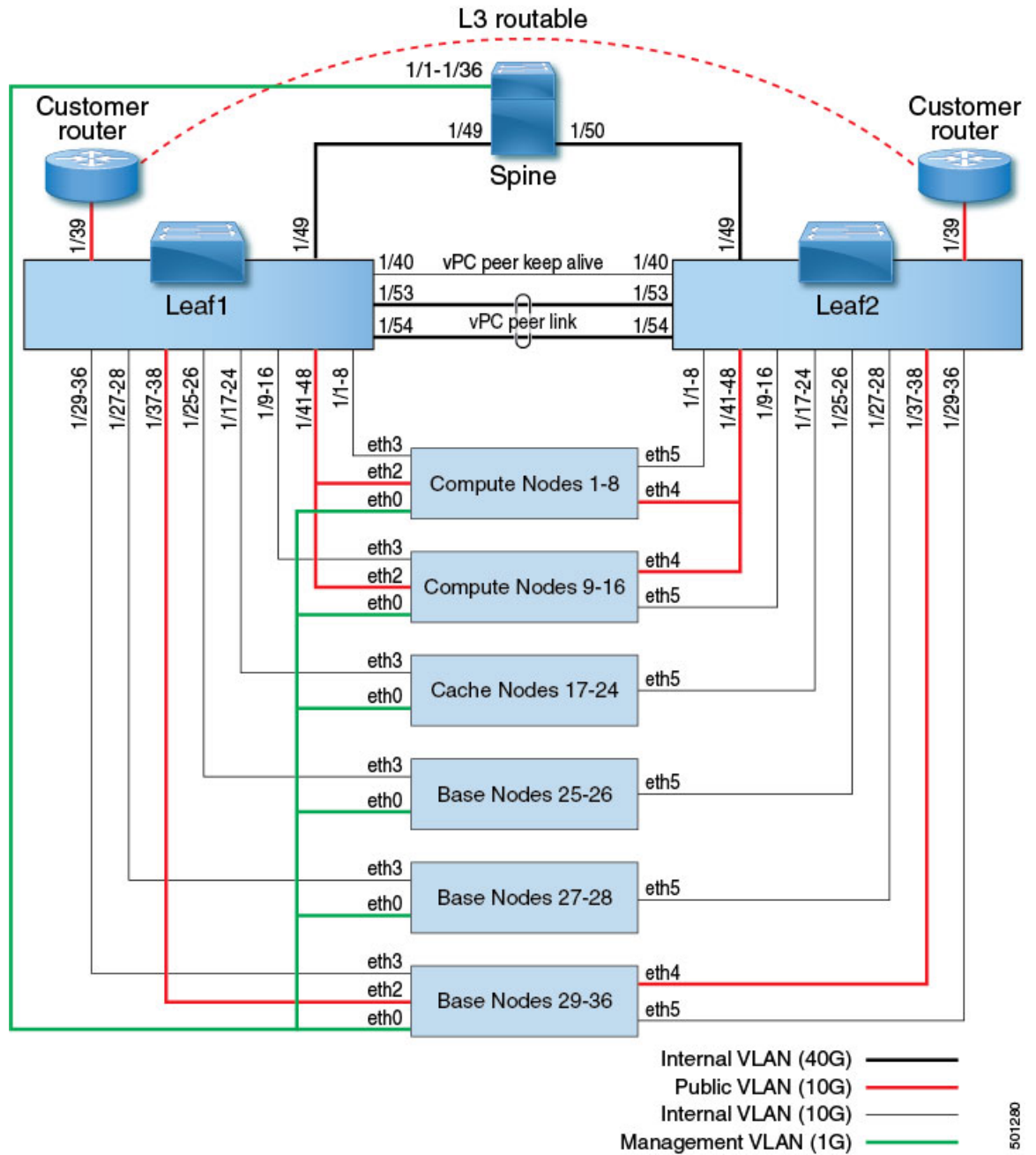
The following figure shows how the C1-Tetration rack devices are interconnected. For a detailed listing of the connections, see the tables following that figure.



---

**Note** The CIMC/PXE switch is connected to the Management (Mgmt) port on each of the three switches and to the eth0 port on each of the 36 Compute, Cache, and Base server hosts.

---



501280

Table 5: Spine Switch Connections (RU 41 in Single-Rack Installations or RU 40 in Dual-Rack Installations)

Spine Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1	CIMC/PXE VLAN (1 Gigabit)	UCS server host 1 (Compute server 1)	RU 36	Rack 1 RU 17	eth0

Spine Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
2	CIMC/PXE VLAN (1 Gigabit)	UCS server host 2 (Compute server 2)	RU 35	Rack 1 RU 16	eth0
3	CIMC/PXE VLAN (1 Gigabit)	UCS server host 3 (Compute server 3)	RU 34	Rack 1 RU 15	eth0
4	CIMC/PXE VLAN (1 Gigabit)	UCS server host 4 (Compute server 4)	RU 33	Rack 1 RU 14	eth0
5	CIMC/PXE VLAN (1 Gigabit)	UCS server host 5 (Compute server 5)	RU 32	Rack 1 RU 13	eth0
6	CIMC/PXE VLAN (1 Gigabit)	UCS server host 6 (Compute server 6)	RU 31	Rack 1 RU 12	eth0
7	CIMC/PXE VLAN (1 Gigabit)	UCS server host 7 (Compute server 7)	RU 30	Rack 1 RU 11	eth0
8	CIMC/PXE VLAN (1 Gigabit)	UCS server host 8 (Compute server 8)	RU 29	Rack 1 RU 10	eth0
9	CIMC/PXE VLAN (1 Gigabit)	UCS server host 9 (Compute server 9)	RU 28	Rack 1 RU 8	eth0
10	CIMC/PXE VLAN (1 Gigabit)	UCS server host 10 (Compute server 10)	RU 27	Rack 1 RU 7	eth0
11	CIMC/PXE VLAN (1 Gigabit)	UCS server host 11 (Compute server 11)	RU 26	Rack 1 RU 6	eth0
12	CIMC/PXE VLAN (1 Gigabit)	UCS server host 12 (Compute server 12)	RU 25	Rack 1 RU 5	eth0
13	CIMC/PXE VLAN (1 Gigabit)	UCS server host 13 (Compute server 13)	RU 24	Rack 1 RU 4	eth0

Spine Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
14	CIMC/PXE VLAN (1 Gigabit)	UCS server host 14 (Compute server 14)	RU 23	Rack 1 RU 3	eth0
15	CIMC/PXE VLAN (1 Gigabit)	UCS server host 15 (Compute server 15)	RU 22	Rack 1 RU 2	eth0
16	CIMC/PXE VLAN (1 Gigabit)	UCS server host 16 (Compute server 16)	RU 21	Rack 1 RU 1	eth0
17	CIMC/PXE VLAN (1 Gigabit)	UCS server host 17 (Cache server 1)	RU 20	Rack 2 RU 21	eth0
18	CIMC/PXE VLAN (1 Gigabit)	UCS server host 18 (Cache server 2)	RU 19	Rack 2 RU 20	eth0
19	CIMC/PXE VLAN (1 Gigabit)	UCS server host 19 (Cache server 3)	RU 18	Rack 2 RU 19	eth0
20	CIMC/PXE VLAN (1 Gigabit)	UCS server host 20 (Cache server 4)	RU 17	Rack 2 RU 18	eth0
21	CIMC/PXE VLAN (1 Gigabit)	UCS server host 21 (Cache server 5)	RU 16	Rack 2 RU 17	eth0
22	CIMC/PXE VLAN (1 Gigabit)	UCS server host 22 (Cache server 6)	RU 15	Rack 2 RU 16	eth0
23	CIMC/PXE VLAN (1 Gigabit)	UCS server host 23 (Cache server 7)	RU 14	Rack 2 RU 15	eth0
24	CIMC/PXE VLAN (1 Gigabit)	UCS server host 24 (Cache server 8)	RU 13	Rack 2 RU 14	eth0
25	CIMC/PXE VLAN (1 Gigabit)	UCS server host 25 (Base server 1)	RU 12	Rack 2 RU 12	eth0

Spine Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
26	CIMC/PXE VLAN (1 Gigabit)	UCS server host 26 (Base server 2)	RU 11	Rack 2 RU 11	eth0
27	CIMC/PXE VLAN (1 Gigabit)	UCS server host 27 (Base server 3)	RU 10	Rack 2 RU 10	eth0
28	CIMC/PXE VLAN (1 Gigabit)	UCS server host 28 (Base server 4)	RU 9	Rack 2 RU 9	eth0
29	CIMC/PXE VLAN (1 Gigabit)	UCS server host 29 (Base server 5)	RU 8	Rack 2 RU 8	eth0
30	CIMC/PXE VLAN (1 Gigabit)	UCS server host 30 (Base server 6)	RU 7	Rack 2 RU 7	eth0
31	CIMC/PXE VLAN (1 Gigabit)	UCS server host 31 (Base server 7)	RU 6	Rack 2 RU 6	eth0
32	CIMC/PXE VLAN (1 Gigabit)	UCS server host 32 (Base server 8)	RU 5	Rack 2 RU 5	eth0
33	CIMC/PXE VLAN (1 Gigabit)	UCS server host 33 (Base server 9)	RU 4	Rack 2 RU 4	eth0
34	CIMC/PXE VLAN (1 Gigabit)	UCS server host 34 (Base server 10)	RU 3	Rack 2 RU 3	eth0
35	CIMC/PXE VLAN (1 Gigabit)	UCS server host 35 (Base server 11)	RU 2	Rack 2 RU 2	eth0
36	CIMC/PXE VLAN (1 Gigabit)	UCS server host 36 (Base server 12)	RU 1	Rack 2 RU 1	eth0
49	Internal VLAN (40 Gigabit)	Leaf switch 1 (RU 41 in single rack or RU 40 in rack 1 of dual rack)	RU 40	Rack 1 RU 40	49

Spine Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
50	Internal VLAN (40 Gigabit)	Leaf switch 2 (RU 40 in single rack or RU 40 of rack 2 in dual rack) port 49	RU 41	Rack 2 RU 40	49

**Table 6: Leaf Switch 2 Connections (RU 41 in Single-Rack Installations or RU 40 in Dual-Rack Installations)**

Leaf 2 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Single Rack	Port
1	Internal VLAN (10 Gigabit)	UCS server host 1 (Compute server 1)	RU 36	Rack 1 RU 17	eth5
2	Internal VLAN (10 Gigabit)	UCS server host 2 (Compute server 2)	RU 35	Rack 1 RU 16	eth5
3	Internal VLAN (10 Gigabit)	UCS server host 3 (Compute server 3)	RU 34	Rack 1 RU 15	eth5
4	Internal VLAN (10 Gigabit)	UCS server host 4 (Compute server 4)	RU 33	Rack 1 RU 14	eth5
5	Internal VLAN (10 Gigabit)	UCS server host 5 (Compute server 5)	RU 32	Rack 1 RU 13	eth5
6	Internal VLAN (10 Gigabit)	UCS server host 6 (Compute server 6)	RU 31	Rack 1 RU 12	eth5
7	Internal VLAN (10 Gigabit)	UCS server host 7 (Compute server 7)	RU 30	Rack 1 RU 11	eth5
8	Internal VLAN (10 Gigabit)	UCS server host 8 (Compute server 8)	RU 29	Rack 1 RU 10	eth5
9	Internal VLAN (10 Gigabit)	UCS server host 9 (Compute server 9)	RU 28	Rack 1 RU 8	eth5

Leaf 2 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Single Rack	Port
10	Internal VLAN (10 Gigabit)	UCS server host 10 (Compute server 10)	RU 27	Rack 1 RU 7	eth5
11	Internal VLAN (10 Gigabit)	UCS server host 11 (Compute server 11)	RU 26	Rack 1 RU 6	eth5
12	Internal VLAN (10 Gigabit)	UCS server host 12 (Compute server 12)	RU 25	Rack 1 RU 5	eth5
13	Internal VLAN (10 Gigabit)	UCS server host 13 (Compute server 13)	RU 24	Rack 1 RU 4	eth5
14	Internal VLAN (10 Gigabit)	UCS server host 14 (Compute server 14)	RU 23	Rack 1 RU 3	eth5
15	Internal VLAN (10 Gigabit)	UCS server host 15 (Compute server 15)	RU 22	Rack 1 RU 2	eth5
16	Internal VLAN (10 Gigabit)	UCS server host 16 (Compute server 16)	RU 21	Rack 1 RU 1	eth5
17	Internal VLAN (10 Gigabit)	UCS server host 17 (Cache server 1)	RU 20	Rack 2 RU 21	eth5
18	Internal VLAN (10 Gigabit)	UCS server host 18 (Cache server 2)	RU 19	Rack 2 RU 20	eth5
19	Internal VLAN (10 Gigabit)	UCS server host 19 (Cache server 3)	RU 18	Rack 2 RU 19	eth5
20	Internal VLAN (10 Gigabit)	UCS server host 20 (Cache server 4)	RU 17	Rack 2 RU 18	eth5
21	Internal VLAN (10 Gigabit)	UCS server host 21 (Cache server 5)	RU 16	Rack 2 RU 17	eth5

Leaf 2 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Single Rack	Port
22	Internal VLAN (10 Gigabit)	UCS server host 22 (Cache server 6)	RU 15	Rack 2 RU 16	eth5
23	Internal VLAN (10 Gigabit)	UCS server host 23 (Cache server 7)	RU 14	Rack 2 RU 15	eth5
24	Internal VLAN (10 Gigabit)	UCS server host 24 (Cache server 8)	RU 13	Rack 2 RU 14	eth5
25	Internal VLAN (10 Gigabit)	UCS server host 25 (Base server 1)	RU 12	Rack 2 RU 12	eth5
26	Internal VLAN (10 Gigabit)	UCS server host 26 (Base server 2)	RU 11	Rack 2 RU 11	eth5
27	Internal VLAN (10 Gigabit)	UCS server host 27 (Base server 3)	RU 10	Rack 2 RU 10	eth5
28	Internal VLAN (10 Gigabit)	UCS server host 28 (Base server 4)	RU 9	Rack 2 RU 9	eth5
29	Internal VLAN (10 Gigabit)	UCS server host 29 (Base server 5)	RU 8	Rack 2 RU 8	eth5
30	Internal VLAN (10 Gigabit)	UCS server host 30 (Base server 6)	RU 7	Rack 2 RU 7	eth5
31	Internal VLAN (10 Gigabit)	UCS server host 31 (Base server 7)	RU 6	Rack 2 RU 6	eth5
32	Internal VLAN (10 Gigabit)	UCS server host 32 (Base server 8)	RU 5	Rack 2 RU 5	eth5
33	Internal VLAN (10 Gigabit)	UCS server host 33 (Base server 9)	RU 4	Rack 2 RU 4	eth5



Leaf 2 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Single Rack	Port
34	Internal VLAN (10 Gigabit)	UCS server host 34 (Base server 10)	RU 3	Rack 2 RU 3	eth5
35	Internal VLAN (10 Gigabit)	UCS server host 35 (Base server 11)	RU 2	Rack 2 RU 2	eth5
36	Internal VLAN (10 Gigabit)	UCS server host 36 (Base server 12)	RU 1	Rack 2 RU 1	eth5
37	Public VLAN (10 Gigabit)	UCS server host 34 (Base server 10)	RU 3	Rack 2 RU 3	eth2
38	Public VLAN (10 Gigabit)	UCS server host 36 (Base server 12)	RU 1	Rack 2 RU 1	eth2
39	Internal VLAN (10 Gigabit)	Customer router 1	–	–	–
40	Internal VLAN (10 Gigabit)	Leaf switch 1	RU 40	Rack 1 RU 40	40
41	Public VLAN (10 Gigabit)	UCS server host 2 (Compute server 2)	RU 35	Rack 1 RU 16	eth2
42	Public VLAN (10 Gigabit)	UCS server host 4 (Compute server 4)	RU 33	Rack 1 RU 14	eth2
43	Public VLAN (10 Gigabit)	UCS server host 6 (Compute server 6)	RU 31	Rack 1 RU 12	eth2
44	Public VLAN (10 Gigabit)	UCS server host 8 (Compute server 8)	RU 29	Rack 1 RU 10	eth2
45	Public VLAN (10 Gigabit)	UCS server host 10 (Compute server 10)	RU 27	Rack 1 RU 8	eth2
46	Public VLAN (10 Gigabit)	UCS server host 12 (Compute server 12)	RU 25	Rack 1 RU 6	eth2

Leaf 2 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Single Rack	Port
47	Public VLAN (10 Gigabit)	UCS server host 14 (Compute server 14)	RU 23	Rack 1 RU 4	eth2
48	Public VLAN (10 Gigabit)	UCS server host 14 (Compute server 14)	RU 21	Rack 1 RU 2	eth2
49	Internal VLAN (40 Gigabit)	Spine switch	RU 42	Rack 1 RU 42	50
50	–	–	–	–	–
51	–	–	–	–	–
52	–	–	–	–	–
53	Internal VLAN (40 Gigabit)	Leaf switch 1	RU 40	Rack 1 RU 40	53
54	Internal VLAN (40 Gigabit)	Leaf switch 1	RU 40	Rack 1 RU 40	54

**Table 7: Leaf Switch 1 Connections (RU 40 in Single- and Dual-Rack Installations)**

Leaf 1 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
1	Internal VLAN (10 Gigabit)	UCS server host 1 (Compute server 1)	RU 36	Rack 1 RU 17	eth3
2	Internal VLAN (10 Gigabit)	UCS server host 2 (Compute server 2)	RU 35	Rack 1 RU 16	eth3
3	Internal VLAN (10 Gigabit)	UCS server host 3 (Compute server 3)	RU 34	Rack 1 RU 15	eth3
4	Internal VLAN (10 Gigabit)	UCS server host 4 (Compute server 4)	RU 33	Rack 1 RU 14	eth3
5	Internal VLAN (10 Gigabit)	UCS server host 5 (Compute server 5)	RU 32	Rack 1 RU 13	eth3

Leaf 1 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
6	Internal VLAN (10 Gigabit)	UCS server host 6 (Compute server 6)	RU 31	Rack 1 RU 12	eth3
7	Internal VLAN (10 Gigabit)	UCS server host 7 (Compute server 7)	RU 30	Rack 1 RU 11	eth3
8	Internal VLAN (10 Gigabit)	UCS server host 8 (Compute server 8)	RU 29	Rack 1 RU 10	eth3
9	Internal VLAN (10 Gigabit)	UCS server host 9 (Compute server 9)	RU 28	Rack 1 RU 8	eth3
10	Internal VLAN (10 Gigabit)	UCS server host 10 (Compute server 10)	RU 27	Rack 1 RU 7	eth3
11	Internal VLAN (10 Gigabit)	UCS server host 11 (Compute server 11)	RU 26	Rack 1 RU 6	eth3
12	Internal VLAN (10 Gigabit)	UCS server host 12 (Compute server 12)	RU 25	Rack 1 RU 5	eth3
13	Internal VLAN (10 Gigabit)	UCS server host 13 (Compute server 13)	RU 24	Rack 1 RU 4	eth3
14	Internal VLAN (10 Gigabit)	UCS server host 14 (Compute server 14)	RU 23	Rack 1 RU 3	eth3
15	Internal VLAN (10 Gigabit)	UCS server host 15 (Compute server 15)	RU 22	Rack 1 RU 2	eth3
16	Internal VLAN (10 Gigabit)	UCS server host 16 (Compute server 16)	RU 21	Rack 1 RU 1	eth3
17	Internal VLAN (10 Gigabit)	UCS server host 17 (Cache server 1)	RU 20	Rack 2 RU 21	eth3

Leaf 1 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
18	Internal VLAN (10 Gigabit)	UCS server host 18 (Cache server 2)	RU 19	Rack 2 RU 20	eth3
19	Internal VLAN (10 Gigabit)	UCS server host 19 (Cache server 3)	RU 18	Rack 2 RU 19	eth3
20	Internal VLAN (10 Gigabit)	UCS server host 20 (Cache server 4)	RU 17	Rack 2 RU 18	eth3
21	Internal VLAN (10 Gigabit)	UCS server host 21 (Cache server 5)	RU 16	Rack 2 RU 17	eth3
22	Internal VLAN (10 Gigabit)	UCS server host 22 (Cache server 6)	RU 15	Rack 2 RU 16	eth3
23	Internal VLAN (10 Gigabit)	UCS server host 23 (Cache server 7)	RU 14	Rack 2 RU 15	eth3
24	Internal VLAN (10 Gigabit)	UCS server host 24 (Cache server 8)	RU 13	Rack 2 RU 14	eth3
25	Internal VLAN (10 Gigabit)	UCS server host 25 (Base server 1)	RU 12	Rack 2 RU 12	eth3
26	Internal VLAN (10 Gigabit)	UCS server host 26 (Base server 2)	RU 11	Rack 2 RU 11	eth3
27	Internal VLAN (10 Gigabit)	UCS server host 27 (Base server 3)	RU 10	Rack 2 RU 10	eth3
28	Internal VLAN (10 Gigabit)	UCS server host 28 (Base server 4)	RU 9	Rack 2 RU 9	eth3
29	Internal VLAN (10 Gigabit)	UCS server host 29 (Base server 5)	RU 8	Rack 2 RU 8	eth3

Leaf 1 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
30	Internal VLAN (10 Gigabit)	UCS server host 30 (Base server 6)	RU 7	Rack 2 RU 7	eth3
31	Internal VLAN (10 Gigabit)	UCS server host 31 (Base server 7)	6	Rack 2 RU 6	eth3
32	Internal VLAN (10 Gigabit)	UCS server host 32 (Base server 8)	RU 5	Rack 2 RU 5	eth3
33	Internal VLAN (10 Gigabit)	UCS server host 33 (Base server 9)	RU 4	Rack 2 RU 4	eth3
34	Internal VLAN (10 Gigabit)	UCS server host 34 (Base server 10)	RU 3	Rack 2 RU 3	eth3
35	Internal VLAN (10 Gigabit)	UCS server host 35 (Base server 11)	RU 2	Rack 2 RU 2	eth3
36	Internal VLAN (10 Gigabit)	UCS server host 36 (Base server 12)	RU 1	Rack 2 RU 1	eth3
37	Public VLAN (10 Gigabit)	UCS server host 33 (Base server 9)	RU 4	Rack 2 RU 8	eth2
38	Public VLAN (10 Gigabit)	UCS server host 35 (Base server 11)	RU 2	Rack 2 RU 6	eth2
39	Internal VLAN (10 Gigabit)	Customer router 1	–	–	–
40	Internal VLAN (10 Gigabit)	Leaf switch 2	RU 41	Rack 2 RU 40	40
41	Public VLAN (10 Gigabit)	UCS server host 1 (Compute server 1)	RU 36	Rack 1 RU 17	eth2
42	Public VLAN (10 Gigabit)	UCS server host 3 (Compute server3)	RU 34	Rack 1 RU 15	eth2

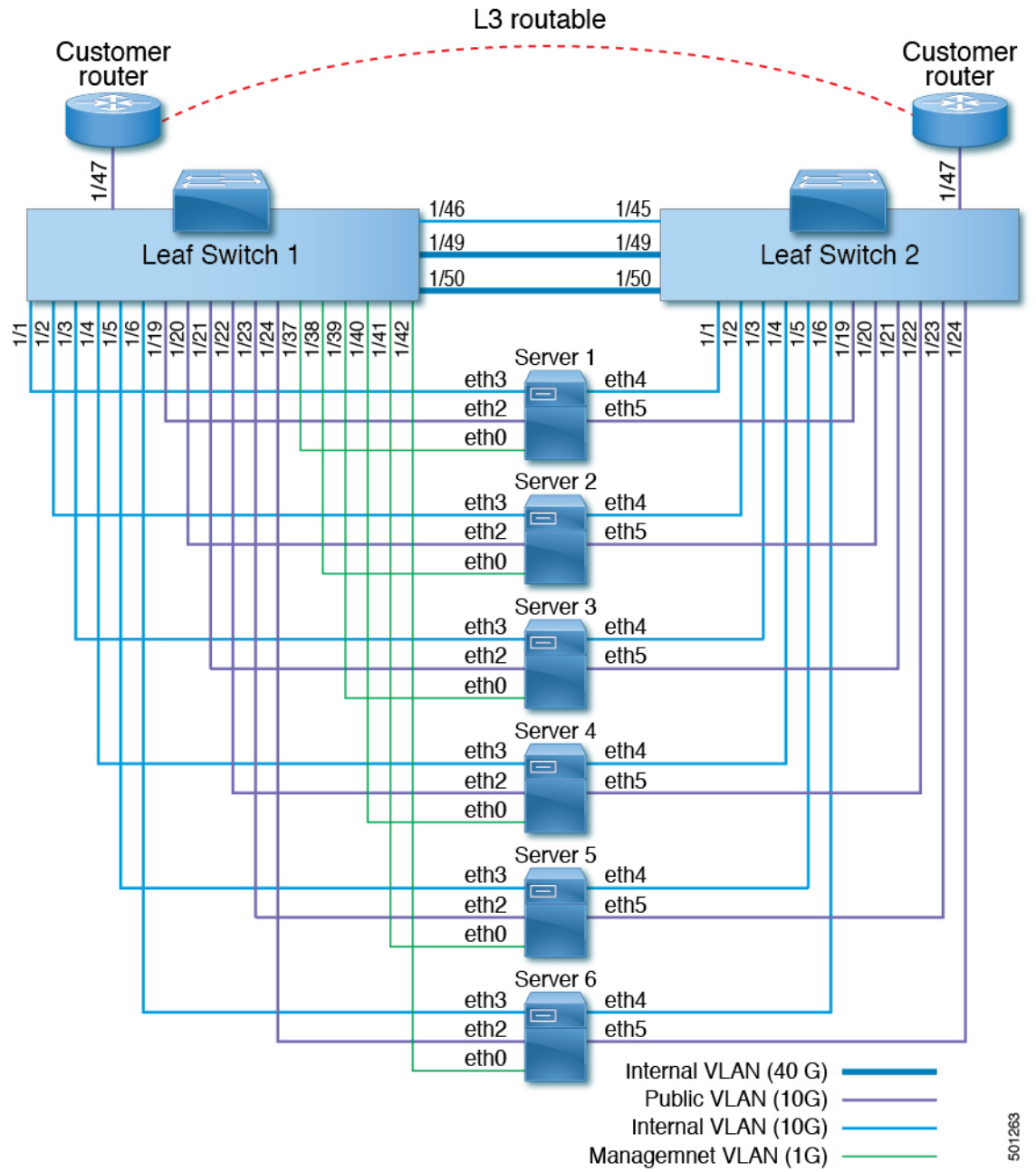
Leaf 1 Port	Connection Type	Connection			
		Device	RU in Single Rack	RU in Dual Rack	Port
43	Public VLAN (10 Gigabit)	UCS server host 5 (Compute server 5)	RU 32	Rack 1 RU 13	eth2
44	Public VLAN (10 Gigabit)	UCS server host 7 (Compute server 7)	RU 30	Rack 1 RU 11	eth2
45	Public VLAN (10 Gigabit)	UCS server host 9 (Compute server 9)	RU 28	Rack 1 RU 9	eth2
46	Public VLAN (10 Gigabit)	UCS server host 11 (Compute server 11)	RU 26	Rack 1 RU 7	eth2
47	Public VLAN (10 Gigabit)	UCS server host 13 (Compute server 13)	RU 24	Rack 1 RU 5	eth2
48	Public VLAN (10 Gigabit)	UCS server host 15 (Compute server 15)	RU 22	Rack 1 RU 3	eth2
49	Internal VLAN (40 Gigabit)	Spine switch	RU 42	Rack 1 RU 42	49
50	–	–	–	–	–
51	–	–	–	–	–
52	–	–	–	–	–
53	Internal VLAN (40 Gigabit)	Leaf 1 switch	RU 40	Rack 1 RU 40	53
54	Internal VLAN (40 Gigabit)	Leaf 2 switch	RU 41	Rack 2 RU 40	54

## Cabling the C1-Tetration-M Cluster Devices

The following figure shows how the C1-Tetration-M Cluster rack devices are interconnected. For a detailed listing of the connections, see the tables following that figure.



**Note** The CIMC/PXE switch is connected to the Management (Mgmt) port on each of the three switches and to the eth0 port on each of the 36 Compute, Cache, and Base server hosts.



501263

Table 8: Leaf Switch 1 (RU 12) Connections

Spine Port	Connection Type	Connection		
		Device	RU in Single Rack	Port
1	Internal VLAN (10 Gb)	Server 1	9	eth3
2	Internal VLAN (10 Gb)	Server 2	8	eth3
3	Internal VLAN (10 Gb)	Server 3	6	eth3
4	Internal VLAN (10 Gb)	Server 4	5	eth3
5	Internal VLAN (10 Gb)	Server 5	3	eth3
6	Internal VLAN (10 Gb)	Server 6	2	eth3
7	–	–	–	–
8	–	–	–	–
9	–	–	–	–
10	–	–	–	–
11	–	–	–	–
12	–	–	–	–
13	–	–	–	–
14	–	–	–	–
15	–	–	–	–
16	–	–	–	–
17	–	–	–	–
18	–	–	–	–
19	External VLAN (10 Gb)	Server 1	9	eth2
20	External VLAN (10 Gb)	Server 2	8	eth2
21	External VLAN (10 Gb)	Server 3	6	eth2



Spine Port	Connection Type	Connection		
		Device	RU in Single Rack	Port
22	External VLAN (10 Gb)	Server 4	5	eth2
23	External VLAN (10 Gb)	Server 5	3	eth2
24	External VLAN (10 Gb)	Server 6	2	eth2
25	–	–	–	–
26	–	–	–	–
27	–	–	–	–
28	–	–	–	–
29	–	–	–	–
30	–	–	–	–
31	–	–	–	–
32	–	–	–	–
33	–	–	–	–
34	–	–	–	–
35	–	–	–	–
36	–	–	–	–
37	Management VLAN (1 Gb)	Server 1	9	eth0
38	Management VLAN (1 Gb)	Server 2	8	eth0
39	Management VLAN (1 Gb)	Server 3	6	eth0
40	Management VLAN (1 Gb)	Server 4	5	eth0
41	Management VLAN (1 Gb)	Server 5	3	eth0
42	Management VLAN (1 Gb)	Server 6	2	eth0
43	–	–	–	–

Spine Port	Connection Type	Connection		
		Device	RU in Single Rack	Port
44	–	–	–	–
45	–	–	–	–
46	Internal VLAN (10 Gb)	Leaf 2 switch	11	45
47	External VLAN (10 Gb)	Customer router	–	–
48	–	–	–	–
49	Internal VLAN (40 Gb)	Leaf 2 switch	11	49
50	Internal VLAN (40 Gb)	Leaf 2 switch	11	50
51	–	–	–	–
52	–	–	–	–
53	–	–	–	–
54	–	–	–	–

Table 9: Leaf Switch 2 (RU 11) Connections

Spine Port	Connection Type	Connection		
		Device	RU in Single Rack	Port
1	Internal VLAN (10 Gb)	Server 1	9	eth4
2	Internal VLAN (10 Gb)	Server 2	8	eth4
3	Internal VLAN (10 Gb)	Server 3	6	eth4
4	Internal VLAN (10 Gb)	Server 4	5	eth4
5	Internal VLAN (10 Gb)	Server 5	3	eth4
6	Internal VLAN (10 Gb)	Server 6	2	eth4
7	–	–	–	–

Spine Port	Connection Type	Connection		
		Device	RU in Single Rack	Port
8	–	–	–	–
9	–	–	–	–
10	–	–	–	–
11	–	–	–	–
12	–	–	–	–
13	–	–	–	–
14	–	–	–	–
15	–	–	–	–
16	–	–	–	–
17	–	–	–	–
18	–	–	–	–
19	External VLAN (10 Gb)	Server 1	9	eth5
20	External VLAN (10 Gb)	Server 2	8	eth5
21	External VLAN (10 Gb)	Server 3	6	eth5
22	External VLAN (10 Gb)	Server 4	5	eth5
23	External VLAN (10 Gb)	Server 5	3	eth5
24	External VLAN (10 Gb)	Server 6	2	eth5
25	–	–	–	–
26	–	–	–	–
27	–	–	–	–
28	–	–	–	–
29	–	–	–	–
30	–	–	–	–

Spine Port	Connection Type	Connection		
		Device	RU in Single Rack	Port
31	–	–	–	–
32	–	–	–	–
33	–	–	–	–
34	–	–	–	–
35	–	–	–	–
36	–	–	–	–
37	Management VLAN (1 Gb)	Server 1	9	eth0
38	Management VLAN (1 Gb)	Server 2	8	eth0
39	Management VLAN (1 Gb)	Server 3	6	eth0
40	Management VLAN (1 Gb)	Server 4	5	eth0
41	Management VLAN (1 Gb)	Server 5	3	eth0
42	Management VLAN (1 Gb)	Server 6	2	eth0
43	–	–	–	–
44	–	–	–	–
45	Internal VLAN (10 Gb)	Leaf 1 switch	12	45
46	–	–	–	–
47	External VLAN (10 Gb)	Customer router	–	–
48	–	–	–	–
49	Internal VLAN (40 Gb)	Leaf 1 switch	12	49
50	Internal VLAN (40 Gb)	Leaf 1 switch	12	50
51	–	–	–	–

Spine Port	Connection Type	Connection		
		Device	RU in Single Rack	Port
52	—	—	—	—
53	—	—	—	—
54	—	—	—	—

