Cisco Telemetry Broker

Hardware Appliance Installation and Configuration Guide 2.0.1

Table of Contents

Introduction

Overview

This guide explains how to install the Cisco Telemetry Broker TB2300. This guide also describes the mounting and installation of the Cisco Telemetry Broker hardware. Note that Cisco Telemetry Broker is sometimes referred to as CTB in this document.

> ⚠️ Before installing the Broker Node TB2300, read the Regulatory and Compliance Safety Information document.

Hardware and Software Version Support Matrix

Appliance	Platform	Gen	v.2.0
Broker Node TB2300	UCSC-C220	M6	●

Use this legend when reading the Hardware and Software Version Support Matrix.

Symbol	Description
●	Performs at full capacity on hardware
○	Supported, but performance not optimal
x	Not supported

Audience

This guide is designed for the person responsible for installing Cisco Telemetry Broker hardware. We assume that you already have some general understanding of installing network equipment.

If you prefer to work with a professional installer, please contact your local Cisco Partner or Cisco Support.

Installing Virtual Broker Nodes

If you want to install virtual broker nodes, follow the instructions in the Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide.

Terminology

This guide sometimes uses the term "**appliance**" to refer to the Broker Node TB2300.

A "**high availability cluster**" is a group of broker nodes that are managed by a manager node.

Common Abbreviations

The following abbreviations appear in this guide:

Abbreviation	Description
CIMC	Cisco Integrated Management Controller
DNS	Domain Name Server/Service
FTP	File Transfer Protocol
Gbps	Gigabits per second
GB	Gigabyte
HTTPS	Hypertext Transfer Protocol (Secure)
Mbps	Megabits per second
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
SSH	Secure Shell
TAP	Test Access Port
UDPD	UDP Director

Abbreviation	Description
UPS	Uninterruptible Power Supply
URL	Universal Resource Locator
VLAN	Virtual Local Area Network
VM	Virtual Machine

Concepts and Architecture

Cisco Telemetry Broker allows you to ingest network telemetry from many inputs, transform the telemetry format, and forward that telemetry to one or multiple destinations. Refer to the following table for examples.

> ℹ️ Currently, the only hardware appliance that exists for Cisco Telemetry Broker is a broker node (TB2300). This must be paired with a VM Manager node for deployment.
>
> You can deploy a combination of both virtual and physical broker nodes, or you can deploy only all virtual broker nodes or only all physical broker nodes.
>
> There is no required order of installation for broker nodes, even if you are deploying a combination of virtual and physical broker nodes.

You can ingest any of the following telemetry:	And forward that telemetry to any or all of the following destinations:
• On-premises network telemetry, including NetFlow, syslog, and IPFIX • Cloud-based telemetry inputs, such as Amazon Web Services (AWS) Virtual Private Cloud (VPC) Flow Logs	• Analytics platforms, such as Secure Network Analytics or Secure Cloud Analytics • Network management and automation platforms, such as Cisco DNA Center • Security Information and Event Management (SIEM) platforms

To accomplish this, you deploy one or more Cisco Telemetry Broker nodes, which ingest telemetry and forward it to the configured destinations.

Out of the box, Cisco Telemetry Broker supports the following transformations:

Ingested Data Format	Forwarded Data Format
VPC Flow Logs	IPFIX
Microsoft Network Security Group	IPFIX

(NSG) Flow Logs	
IPFIX, NetFlow v5, NetFlow v9	JSON (only to SCA destinations)

Your broker nodes are all managed by one Cisco Telemetry Broker Manager. You can log in to this Manager's web interface and perform various configuration tasks, including managing the broker nodes, setting up the forwarding rules, creating users, and reviewing the dashboard for usage.

Deployment Requirements

Before you begin, review this guide to understand the process as well as the preparation, time, and resources you'll need to plan for the installation.

Hardware and Software Version Release Matrix

Review the Hardware and Software Version Support Matrix for compatibility details. The matrix is documented in the **Introduction** chapter in this guide.

Specifications

Download the specifications sheet for the Broker Node TB2300 you plan to install.

Cisco Integrated Management Controller (CIMC)

After you install your appliances, make sure you configure the Cisco Integrated Management Controller (CIMC) to enable access to the server configuration and a virtual server console. You can also use the CIMC to monitor hardware health.

- **Instructions:** Refer to **Connecting with CIMC** and follow the instructions in the Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide.
- **Default Password:** As part of the initial configuration, you will log in to the CIMC as admin and type **password** in the Password field.
- **Password Requirement:** When you log in, change the default password to protect the security of your network.

Migrate Configuration to a New System

Complete the following processes to back up and restore the CTB configuration rules that you set up in the Cisco Telemetry Broker Manager.

- It is possible for UDPD customers to migrate their existing UDPD configuration to Cisco Telemetry Broker. For more details, see the "Importing and Exporting UDP Director Configuration" section in the Cisco Telemetry Broker User Guide.

Back Up CTB Configuration Rules

Run the following command on the CTB Manager Node:

```
$ sudo ctb-backup-config -v -f ctb_config.json
```

When this process has finished, the configuration rules will be backed up to the file at ~/.ctb_config.json, after which you can copy the configuration rules to another location.

- VPC/NSG flow log rules are not backed up, so you need to re-create your VPC/NSG flow log rules upon migrating to a new system.

- You can back up and restore your CTB configuration rules only within the same version. If you try to do so across versions, the process may fail.

Restore the CTB Configuration Rules

> ⚠ You must run `ctb-restore-config` after you complete `ctb-install --init` on the Manager node. If you manually create a GUI login account, it will be overwritten by the account information from `ctb-restore-config`.

Complete these steps:

1. Log out as the *install* user.

2. Copy the **ctb-config.json** file from an existing system.

3. Log in to the new system as *admin*.

4. Run the following command on the CTB Manager Node:

```
$ sudo ctb-restore-config -v -f ctb_config.json
```

   Any inputs that you add to Cisco Telemetry Broker due to the restore are not assigned to any nodes or clusters. You will need to assign them as required.

1. Configure Your Firewall for Communications

In order for the appliances to communicate properly, you should configure the network so that firewalls or access control lists do not block the required connections. Use the information provided in this section to configure your network so that the appliances can communicate through the network.

Open Communication Ports

The following table provides details for all the network connections made to and from your Cisco Telemetry Broker appliances. To ensure that your network permits these connections, you need to modify the applicable access controls you currently have in place (for example, your firewall).

Client	Server	Port	Description
users	broker nodes and Manager node	22/TCP	SSH access to the console
Manager	external internet	443/TCP	HTTPS for secure external communications, such as Smart Licensing and Software Update
Manager	customer syslog server	customer-defined port	Syslog telemetry for Cisco Telemetry Broker notifications
Manager	customer SMTP server	customer-defined port	SMTP telemetry for Cisco Telemetry Broker notifications
each broker node	Manager	443/TCP	HTTPS for secure management connections
each broker node	external internet	443/TCP	HTTPS for retrieving VPC/NSG Flow Logs from AWS S3/Azure SAS storage buckets, respectively. HTTPS for broker node to secure access SCA server and upload files to SCA S3 bucket.

users	Manager	443/TCP	HTTPS for secure web interface access
broker nodes and Manager node	customer DNS servers	53/UDP	DNS telemetry
each *hardware* broker node	customer NTP server	123	NTP data for time synchronization

In addition, you must open ports based on both the telemetry type that is sent to a broker node and the telemetry type that a broker node sends to a destination. The following table provides details about common ports for various telemetry types:

Port	Description
514/UDP	syslog
2055/UDP	NetFlow v5, NetFlow v9
4739/UDP	IPFIX
6343/UDP	sFlow

2. Installation Warnings and Guidelines

Installation Warnings

Read the [Regulatory and Compliance Safety Information](#) document before installing any Cisco Telemetry Broker appliance.

Take note of the following warnings:

> Statement 1071—Warning Definition
>
> IMPORTANT SAFETY INSTRUCTIONS
>
> ⚠️ This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.
>
> SAVE THESE INSTRUCTIONS

> Statement 1004—Installation Instructions
>
> ⚠️ Read the installation instructions before using, installing or connecting the system to the power source.

> Statement 12—Power Supply Disconnection Warning
>
> ⚠️ Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

> Statement 43—Jewelry Removal Warning
>
> ⚠️ Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Statement 94—Wrist Strap Warning

⚠️ During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

Statement 1045—Short-Circuit Protection

⚠️ This product requires short-circuit (overcurrent) protection to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

Statement 1021—SELV Circuit

⚠️ To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

Statement 1024—Ground Conductor

⚠️ This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Statement 1040—Product Disposal

⚠️ Ultimate disposal of this product should be handled according to all national laws and regulations.

Statement 19—TN Power Warning

⚠️ The device is designed to work with TN power systems.

Installation Guidelines

Take note of the following warnings:

> **Statement 1047—Overheating Prevention**
>
> ⚠️ To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of : 41 to 95° F (5 to 35° C)

> **Statement 1019—Main Disconnecting Device**
>
> ⚠️ The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.

> **Statement 1005—Circuit Breaker**
>
> ⚠️ This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: USA: 120, 15 A (EU: 250 V, 16 A)

> **Statement 1074—Comply with Local and National Electrical Codes**
>
> ⚠️ Installation of the equipment must comply with local and national electrical codes.

> **Statement 371—Power Cable and AC Adapter**
>
> ⚠️ When installing the product, please use the provided or designated connection cables/power cables/AC adaptors/batteries. Using any other cables/adaptors could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL-certified cables (that have the "UL" or "CSA" shown on the cord), not regulated with the subject law by showing "PSE" on the cord, for any other electrical devices than products designated by CISCO.

> **Statement 1073—No User-Serviceable Parts**
>
> ⚠️ No user-serviceable parts inside. Do not open.

When you are installing a chassis, use the following guidelines:

- Ensure that there is adequate space around the chassis to allow for servicing and for adequate airflow. The airflow in the chassis is from front to back.

> ⓘ To ensure proper airflow it is necessary to rack your chassis using rail kits. Physically placing the units on top of one another or stacking without the use of the rail kits blocks the air vents on top of the chassis, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your chassis on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the chassis. No additional spacing between the chassis is required when you mount them using rail kits.

- Ensure that the air-conditioning can keep the chassis at a temperature of 41 to 95° F (5 to 35° C).
- Ensure that the cabinet or rack meets the rack requirements.
- Ensure that the site power meets the power requirements listed in the specification sheet for your appliance. If available, you can use a UPS to protect against power failures.

> ⓘ Avoid UPS types that use ferroresonant technology. These UPS types can become unstable with these systems, which can have substantial current draw fluctuations from fluctuating data traffic patterns.

Safety Recommendations

The following information helps to ensure your safety and to protect the chassis. This information may not address all potentially hazardous situations in your working environment, so be alert and exercise good judgment at all times.

Observe these safety guidelines:

- Keep the area clear and dust free before, during, and after installation.
- Keep tools away from walkways, where you and others might trip over them.
- Do not wear loose clothing or jewelry, such as earrings, bracelets, or chains that could get caught in the chassis.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Never attempt to lift an object that is too heavy for one person.

Maintain Safety with Electricity

> ⚠️ Before working on a chassis, be sure the power cord is unplugged.

Follow these guidelines when working on equipment powered by electricity:

- Do not work alone if potentially hazardous conditions exist anywhere in your work space.
- Never assume that power is disconnected; always check.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- If an electrical accident occurs:
  - Use caution; do not become a victim yourself.
  - Disconnect power from the system.
  - If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, and then call for help.
  - Determine whether the person needs rescue breathing or external cardiac compressions; then take appropriate action.
- Use the chassis within its marked electrical ratings and product usage instructions.

Prevent ESD Damage

ESD occurs when electronic components are improperly handled, and it can damage equipment and impair electrical circuitry, which can result in intermittent or complete failure of your equipment.

Always follow ESD-prevention procedures when removing and replacing components. Ensure that the chassis is electrically connected to an earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the grounding clip to an unpainted surface of the chassis frame to safely ground ESD voltages. To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

For safety, periodically check the resistance value of the antistatic strap, which should be between one and 10 megohms.

Site Environment

To avoid equipment failures and reduce the possibility of environmentally caused shutdowns, plan the site layout and equipment locations carefully. If you are currently experiencing shutdowns or unusually high error rates with your existing equipment, these considerations may help you isolate the cause of failures and prevent future problems.

Power Supply Considerations

When installing the chassis, consider the following:

- Check the power at the site before installing the chassis to ensure that it is free of spikes and noise. Install a power conditioner, if necessary, to ensure proper voltages and power levels in the appliance-input voltage.
- Install proper grounding for the site to avoid damage from lightning and power surges.
- The chassis does not have a user-selectable operating range. Refer to the label on the chassis for the correct appliance input-power requirement.
- Several styles of AC-input power supply cords are available for the appliance; make sure that you have the correct style for your site.
- If you are using dual redundant (1+1) power supplies, we recommend that you use independent electrical circuits for each power supply.
- Install an uninterruptible power source for your site, if possible.

Rack Configuration Considerations

Consider the following when planning a rack configuration:

- If you are mounting a chassis in an open rack, make sure that the rack frame does not block the intake or exhaust ports.

- Be sure enclosed racks have adequate ventilation. Make sure that the rack is not overly congested as each chassis generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.

- In an enclosed rack with a ventilation fan in the top, heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Ensure that you provide adequate ventilation for equipment at the bottom of the rack.

- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack. Experiment with different arrangements to position the baffles effectively.

3. Mount Your Appliances

You can mount Cisco Telemetry Broker appliances directly in a standard 19'' rack or cabinet, any other suitable cabinet, or on a flat surface. When mounting an appliance in a rack or cabinet, follow the instructions included in the rail mounting kits. When determining where to place an appliance, make sure that clearance to the front and rear panels is as follows:

- The front-panel indicators can be read easily
- Access to ports on rear panel is sufficient for unrestricted cabling
- The rear panel power inlet is within reach of a conditioned AC power source.
- Airflow around the appliance and through the vents is unrestricted.

Hardware Included with the Appliance

The following hardware is included with Cisco Telemetry Broker appliances:

- AC power cord
- Access keys (for front face plate)
- Rail kit for rack mounting or mounting ears for smaller appliances

Additional Required Hardware

You must provide the following additional required hardware:

- Mounting screw for a standard 19" rack
- Uninterruptible power supply (UPS) for the Broker Node TB2300 you are installing
- To configure locally (optional), use one of the following methods:
    - Laptop with a video cable and a USB cable (for the keyboard)
    - Video monitor with a video cable and keyboard with a USB cable

4. Connect Your Appliances to the Network

1. Reviewing Specifications

Use the same procedure to connect each Broker Node TB2300 to the network. The only difference for connection is the type of appliance you have.

- **Specification Sheets:** For detailed specification information, refer to Cisco Telemetry Broker Specification Sheets.
- **UCS Platform:** The Cisco Telemetry Broker TB2300 uses the UCS platform, UCSC-C225-M6SX.

> ⚠ Do not update the appliance BIOS, as it may cause issues with appliance functionality.

2. Connect Your Appliance to the Network

To connect your appliance to your network:

1. Connect an Ethernet cable to the management port as defined in the specification sheet.
2. Connect an Ethernet cable to the telemetry port as defined in the specification sheet.
   - Ensure that the management port is connected to the management network, and the telemetry port is connected to the telemetry network. For more information, see the next section, Determine Network Configuration.
3. Connect the other end of the Ethernet cables to your network's switch(es).
4. Connect the power cords to the power supply. Some appliances have two power connections: Power Supply 1 and Power Supply 2.

Determine Network Configuration

Cisco Telemetry Broker supports multi-node setups, where a single Cisco Telemetry Broker Manager can manage multiple broker nodes. Since Cisco Telemetry Broker updates every broker node with all destinations and rules, you must carefully plan your configuration to avoid a few common issues, which are listed below.

- You can deploy broker nodes in different telemetry segments, where the telemetry interfaces of each broker node may not be accessible across the network. You need to carefully construct rules so that packets from an exporter that reach a specific

node are not forwarded to destinations that are not accessible from that node. To achieve this, you need to construct rules that exclude exporters that might cause this routing issue. One example would be to not use any default rules, since these would match all inputs.

- Not all destinations may be relevant to each broker node. However, with the Check Destination Reachability feature, since each broker node attempts to ascertain accessibility for each destination, the broker nodes could report conflicting information back to the Manager. If the possibility exists that some broker nodes will not be able to connect with some destinations, disable Check Destination Reachability for those destinations.

If you are migrating to Cisco Telemetry Broker from the UDP Director, then before you deploy the Manager node and broker node(s), you need to plan how you will connect the Manager node and broker node(s) to the network, as differences exist between how you configure both Cisco Telemetry Broker and the UDP Director.

Cisco Telemetry Broker differentiates telemetry traffic from management traffic. The broker node has two interfaces: The Telemetry Network interface and the Management Network interface. The Manager node has only the Management Network interface. The following diagram shows how to logically deploy the Manager node and the broker nodes.

> Note that the examples in this topic represent typical deployment scenarios. To learn how to set up a more advanced deployment (for example, one that uses VLANs), contact a network administrator.
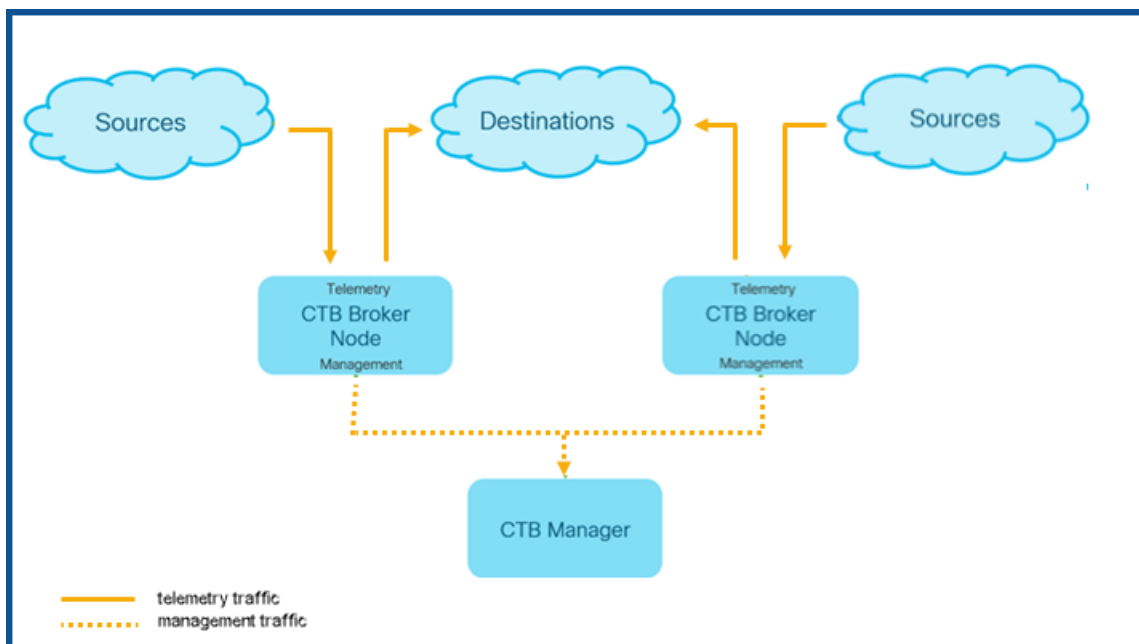
Cisco Telemetry Broker receives management traffic *only* on the Management Network interface; it uses this interface for all communications between the broker node and the Manager node. Telemetry traffic is brokered primarily on the Telemetry Network interface of the broker node. The only exception to this is when Cisco Telemetry Broker retrieves AWS VPC flow logs or Azure NSG flow logs, or when Cisco Telemetry Broker sends telemetry to SCA, both of which occur over the broker node's Management Network interface.

You can place the Manager node anywhere in the network on any subnet, but you must have TCP connectivity over port 443 with the broker nodes.

You can use one of the following deployment modes with the broker node:

1. The telemetry subnets and management subnets are the same. In this mode, the Telemetry Network interface and the Management Network interface on the broker node belong to the same subnet. For more information, see the next section, Interfaces Belong to the Same Subnet.

2. The telemetry subnets and management subnets are different, so the broker node retains its Telemetry Network interface and Management Network interface on two separate subnets. For more information, see two sections down, Interfaces Belong to Different Subnets.

Providing separate paths for both telemetry traffic and management traffic offers the following advantages:

- Separate paths increases performance, especially when it approaches interface line rate performance, since traffic doesn't need to share resources.

- Separating management traffic from telemetry traffic simply makes good sense for a network configuration.

Interfaces Belong to the Same Subnet

This deployment mode is very similar to that of the UDP Director, where the Management Network interface and the Telemetry Network interface are the same. The only difference in this first deployment mode is that you need separate IP addresses for the broker node interfaces.

You can accomplish this by connecting the broker node's Telemetry Network interface and Management Network interface to the same subnet.

Interfaces Belong to Different Subnets

In this deployment mode, the Telemetry Network interface and the Management Network interface are on different subnets.

5. Connect to Your Appliance

This section describes how to connect to your appliance for system configuration.

Choose your connection procedure:

- **Connecting with a Keyboard and a Monitor**
- **Connecting with a Serial Cable or Serial Console**
- **Connecting with CIMC (Required for Remote Access)** To connect to the appliance for remote access, use this procedure.

Connecting with a Keyboard and a Monitor

To configure the IP address locally, complete the following steps:

1. Plug in the power cable to the appliance.
2. Push the Power button to turn on the appliance. Wait for it to finish booting up completely. Do not interrupt the boot up process.

> i You may need to remove the front panel to apply power.
>
> The power supply fans turn on for some models while the system is not powered on. Check that the LED on the front panel is on.
>
> Be sure to connect the appliance to an uninterruptible power supply (UPS). The power supply requires power or else the system displays an error.

3. Connect the keyboard:

   - If you have a standard keyboard, connect it to the standard keyboard connector.
   - If you have a USB keyboard, connect it to a USB connector.

4. Connect the video cable to the video connector. The login prompt appears.
5. Go to the next chapter, **6. Configure Your Cisco Telemetry Broker System**.

Connecting with a Serial Cable or Serial Console

You can also connect to the appliance with a serial cable or serial console, such as a laptop that has a terminal emulator. We use a laptop as an example in the instructions.

1. Connect your laptop to the appliance using one of the following methods:

- Connect an RS232 cable from the serial port connector (DB9) on your laptop to the Console port on the appliance.
- Connect a crossover cable from the Ethernet port on your laptop to the Management port on the appliance.

2. Plug in the power cable to the appliance.

3. Push the Power button to turn on the appliance. Wait for it to finish booting up completely. Do not interrupt the boot up process.

> You may need to remove the front panel to apply power.
>
> ⓘ The power supply fans turn on for some models while the system is not powered on. Check that the LED on the front panel is on. Be sure to connect the appliance to an uninterruptible power supply (UPS). The power supply requires power or else the system displays an error.

4. On the laptop, make a connection into the appliance.

   You can use any available terminal emulator to communicate with the appliance.

5. Apply the following settings:

   - BPS: 115200
   - Data bits: 8
   - Stop bit: 1
   - Parity: None
   - Flow Control: None

   The login screen and login prompt are displayed.

6. Go to the next chapter, **6. Configure Your Cisco Telemetry Broker System**.

Connecting with CIMC (Required for Remote Access)

The Cisco Integrated Management Controller (CIMC) enables access to the server configuration and a virtual server console, as well as monitors for hardware health.

1. Follow the instructions in the Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide.

2. Log in to the CIMC as admin and type **password** in the Password field.

3. Change the default password to protect the security of your network.

4. Go to the next chapter, **6. Configure Your Cisco Telemetry Broker System**.

6. Configure Your Cisco Telemetry Broker System

If you've finished installing your hardware appliances, you are ready to configure Cisco Telemetry Broker into a managed system.

Browser Requirements

Cisco Telemetry Broker supports the following browsers (as tested with the latest rapid release and with resolution at 1024 x 768 px):

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

System Configuration Requirements

Make sure you have access to the appliance console through the CIMC.

Use the following table to prepare the required information for each Broker Node TB2300.

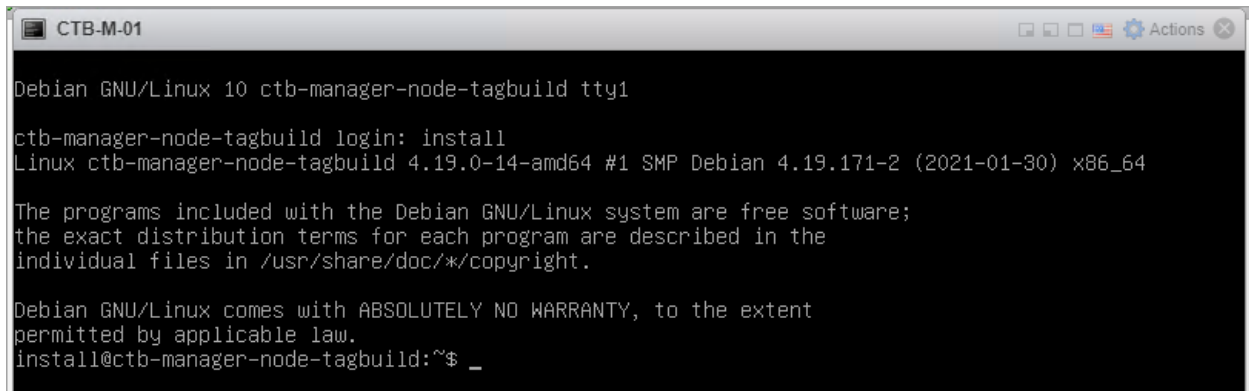| Configuration Requirement	Details
IP Address	Assign a routable IP address to the management port.
Netmask	Establish the subnet for your chosen IP address.
Gateway	Point to your subnet's gateway IP address.
Host Name	A unique host name is required for each Broker Node TB2300. We cannot configure an appliance with the same host name as another broker node. Also, make sure each broker node host name meets the Internet standard requirements for Internet hosts.
DNS Servers	Internal DNS server for name resolution
NTP Servers	Internal Time server for synchronization between servers. At least 1 NTP server is required for each Broker Node TB2300.

Install the Broker Node

Complete the following steps in order.

> ℹ️ Currently, the only hardware appliance that exists for Cisco Telemetry Broker is a broker node (TB2300). This must be paired with a VM Manager node for deployment.

1. Log In as the Install User

From the CIMC console, click **Launch vKVM**.

2. Run the sudo ctb-install --init Command

1. Run the `sudo ctb-install --init` command.
2. Enter the following information:
   - Password for the **admin** user

     The password must meet the following requirements:
       - Contain at least 8 characters
       - Contain at least 1 lowercase letter
       - Contain at least 1 uppercase letter
       - Contain at least 1 digit
       - Contains at least 1 of these special characters: @ # $ % ^ & * ! + ?
       - Cannot be a commonly-used phrase or sequence
       - Cannot be similar to any identifying attributes of the user (such as the username)
   - Hostname (max 255 characters, letters and numbers only)

- You can enter one or both of the following IP address parameters:

  ○ IPv4 address, subnet mask, and default gateway address for the Management Network interface

  ○ IPv6 address, subnet mask, and default gateway address for the Management Network interface

- Valid DNS nameserver IP address that is reachable from the broker node (you can enter one or two)

- Valid NTP IP address that is reachable from the broker node.

(Optional) Change an Individual Parameter

To change any individual parameter, run the `sudo ctb-install --config` command.

Change the Management Network Interface

1. To change the Management Network interface, select **Management Network** from the main screen, as shown below:
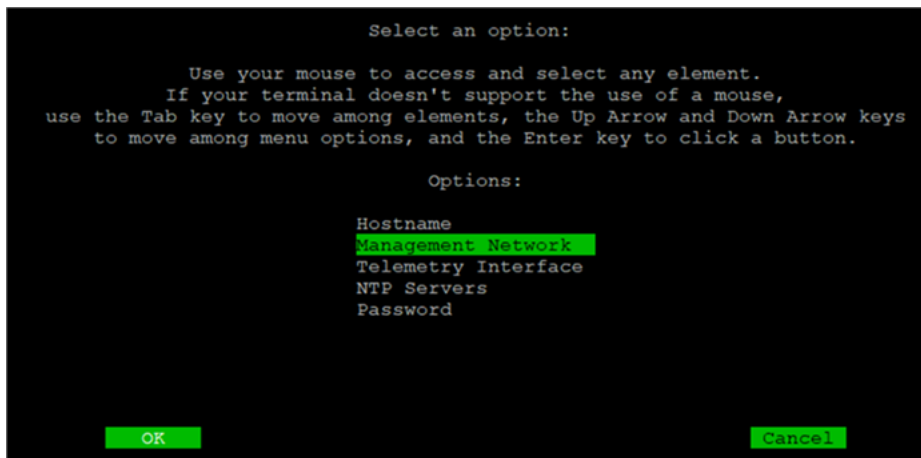
2. From the Management Network screen that opens, make any applicable changes to the management network settings, including selecting a new Management Network interface. Refer to the Port Number – Interface Name Mapping table shown at the end of this section to know which interface name to choose for a particular port number.

Change the Telemetry Network Interface

1. To change the Telemetry Network interface, select **Telemetry Interface** from the main screen, as shown below:

2. From the screen that opens, select the applicable Telemetry Network interface. Refer to the Port Number – Interface Name Mapping table shown at the end of this section to know which interface name to choose for a particular port number.
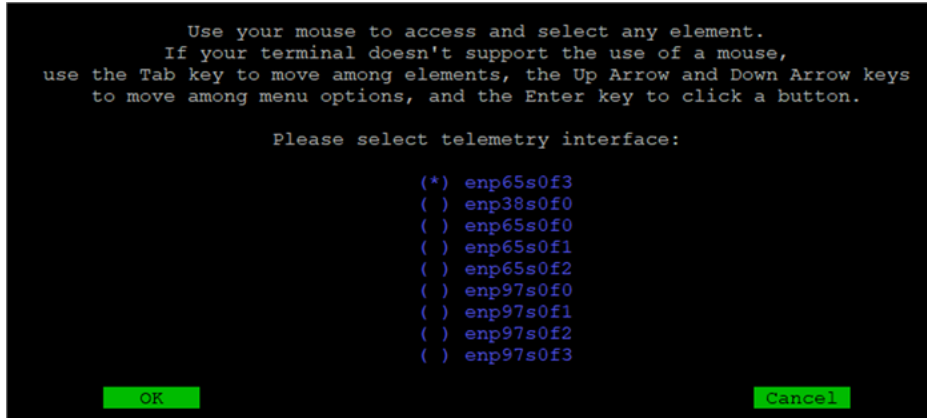
```
        Use your mouse to access and select any element.
      If your terminal doesn't support the use of a mouse,
 use the Tab key to move among elements, the Up Arrow and Down Arrow keys
    to move among menu options, and the Enter key to click a button.

                Please select telemetry interface:

                        (*) enp65s0f3
                        ( ) enp38s0f0
                        ( ) enp65s0f0
                        ( ) enp65s0f1
                        ( ) enp65s0f2
                        ( ) enp97s0f0
                        ( ) enp97s0f1
                        ( ) enp97s0f2
                        ( ) enp97s0f3

        OK                                       Cancel
```

Port Number – Interface Name Mapping Table
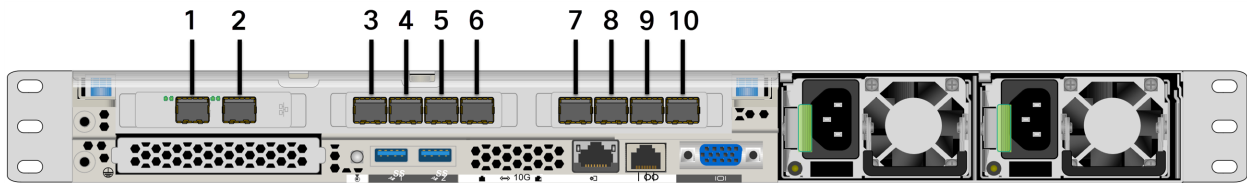
Port Number	Interface Name
1	enp38s0f1
2	enp38s0f0
3	enp65s0f3
4	enp65s0f2
5	enp65s0f1
6	enp65s0f0
7	enp97s0f0
8	enp97s0f1
9	enp97s0f2
10	enp97s0f3

> ℹ These port numbers are also referred to on pages 2 and 3 in the Broker Node TB2300 Specification sheet.

3. Run the sudo ctb-manage Command

1. Run the `sudo ctb-manage` command.
2. Enter the following information:
   - IP address of the Manager node
   - Username of the super user account you create in the Manager node
   - Password of the super user account you create in the Manager node

4. Logout
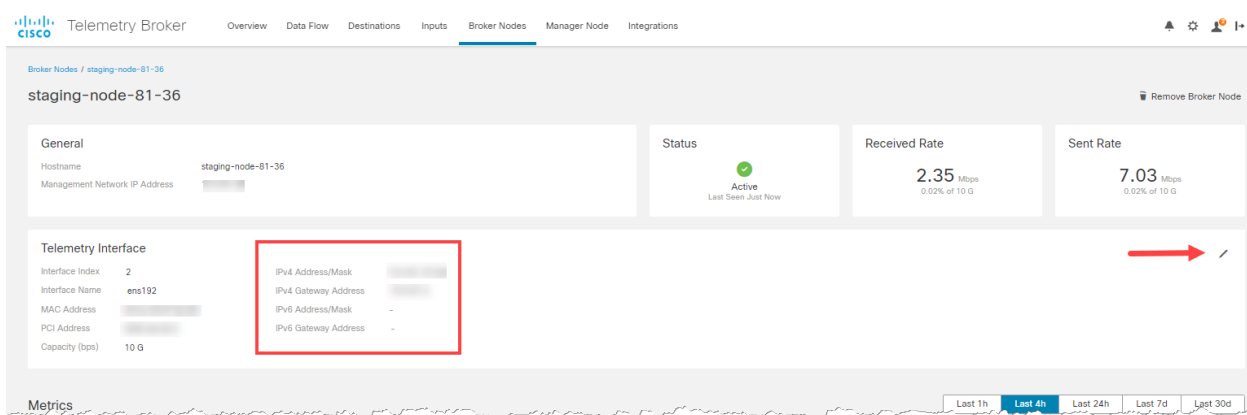
To log out, type `exit`.

5. Configure the Telemetry Interface

> ℹ Cisco Telemetry Broker is configured to work in polling mode on a hardware appliance.

1. Log in to Cisco Telemetry Broker. In a web browser, enter the Manager's management interface IP address and press **Enter** to navigate to the Manager's web interface login.
2. From the main menu, choose **Broker Nodes**.
3. In the Broker Nodes table, click the applicable broker node.
4. In the Telemetry Interface section, click the ✎ **(Edit)** icon (indicated by the arrow in the following image).

5. Configure the IP and Gateway addresses (enclosed in red border).

Manage High Availability Clusters

Cisco Telemetry Broker high availability provides highly available IPv4 and IPv6 virtual IP addresses to be targets for your inputs, ensuring reliable delivery of telemetry from inputs to destinations.

To establish Broker Node high availability, you can create high availability clusters and assign multiple broker nodes to each. In each cluster, one broker node is designated *Active*, meaning it passes telemetry and serves metrics to Cisco Telemetry Broker, and the rest are designated *Passive*, meaning they are not passing telemetry or serving metrics currently. If an Active broker node stops passing telemetry or otherwise loses connectivity with Telemetry Broker, one of the Passive broker nodes is promoted to Active broker node and starts passing telemetry.

Note the following about clusters:

- Each broker node can only belong to one cluster at a time.
- To create a cluster, you need to assign a minimum of one broker node to that cluster.
- Keep in mind that if you create a cluster with only one broker node and this broker node fails, no other broker node is available to be promoted to Active broker node. Similarly, if all broker nodes within a cluster fail, no broker node can be promoted to Active broker node. If a broker node fails, bring it back online as soon as possible.
- You cannot choose which broker node is active in a given cluster.
- If an Active broker node for a virtual IP address fails, one of the Passive broker nodes in the same cluster becomes the Active broker node for the virtual IP address. When the failed broker node comes back up again, it remains a Passive broker node. If you want to make that node active again, you will need to do so manually using the provided commands in the Move a VIP to a Specific Node section in this chapter.
- You can assign either a virtual IPv4 or virtual IPv6 address, or both, to a cluster. Telemetry Broker uses this virtual IP address to communicate with the cluster and promote Passive broker nodes to Active broker nodes when an Active broker node loses connectivity with Telemetry Broker.

For information about how HA clusters are updated during the Cisco Telemetry Broker software update process, see the "Software Update" chapter in the Cisco Telemetry Broker User Guide.

VIPs and Routing

High availability configures the VIP address broker node's Telemetry Network interface. Note that the Telemetry Network interface on each broker node in the cluster *must already be configured* with a primary IPv4 or IPv6 IP address, as well as with a subnet mask and a gateway. You can configure these in the Telemetry Network interface.

You must configure the IPv4 or IPv6 VIP IP addresses to be in the same subnet as the primary IP addresses **of the Telemetry Network interfaces** in the cluster, since the VIP must be in the same subnet as well. This ensures proper routing via the preconfigured Gateway and fast failover.

If the VIP addresses are not in the same subnet as the primary IP addresses of the Telemetry Network interfaces, or if the Telemetry Network interfaces within a Cluster are configured with different subnets, then it is very likely that high availability will not work.

Manage Clusters

The Cisco Telemetry Broker implementation relies on two commonly used Linux packages to provide the underlying high availability infrastructure:

Corosync: This is the low-level cluster engine that provides the underlying communication between cluster nodes. It also provides the quorum capability to make the decision on the role of each node (Active or Standby).

Pacemaker: This is Cluster Resource Manager which manages all the relationships between the machines and the applications. It uses Corosync to communicate.

View Current Cluster Status

To view the current status of the cluster, including the status (Offline or Online) of each node and the location of the IPv4 VIP (vip4) and the IPv6 VIP (vip6) IP address, complete the following steps:

1. Log in as the **admin** to any of the broker nodes in the cluster via SSH. Use the password that was supplied during node installation.

2. Run the `sudo crm_mon` command. This presents a view of the currently configured attributes on the cluster. You can see more details about this command here.

3. Exit the tool by pressing **Ctrl+C**.

```
Stack: corosync
Current DC: 10.0.81.31 (version 2.0.1-9e909a5bdd) - partition with quorum
Last updated: Tue Jan 26 16:16:24 2021
Last change: Tue Jan 26 15:45:04 2021 by root via cibadmin on 10.0.81.31

2 nodes configured
1 resource configured

Online: [ 10.0.81.31 10.0.81.32 ]

Active resources:

vip4    (ocf::titan:telemetry-vip):     Started 10.0.81.31
```

The previous image describes a cluster of two nodes, 10.0.81.31 and 10.0.81.32, which both have the status of *Online*. The IPv4 VIP (vip4) is currently running on 10.0.81.31. The IPv6 VIP (vip6) is not visible because it has not been configured.

If 10.0.81.31 failed, its status would look like this:

```
Stack: corosync
Current DC: 10.0.81.32 (version 2.0.1-9e909a5bdd) - partition with quorum
Last updated: Tue Jan 26 16:17:22 2021
Last change: Tue Jan 26 15:45:04 2021 by root via cibadmin on 10.0.81.31

2 nodes configured
1 resource configured

Online: [ 10.0.81.32 ]
OFFLINE: [ 10.0.81.31 ]

Active resources:

vip4    (ocf::titan:telemetry-vip):     Started 10.0.81.32
```

Notice how 10.0.81.31 is now shown as *OFFLINE* and the vip4 has moved to 10.0.81.32.

View Current Cluster Configuration

To view the current configuration of the cluster to verify that the Corosync and Pacemaker configuration is correct, complete the following steps:

1. Log in as the **admin** to any of the broker nodes in the cluster via SSH. Use the password that was supplied during node installation.

2. Run the `sudo crm configure show` command. This presents a view of the currently configured attribute on the cluster. You can see more details about this command [here](#).

```
admin@titan-8HIP2JLB: ~                                    ⌥⌘1
admin@titan-8HlP2JLB:~$ sudo crm configure show
node 1: 10.0.81.31
node 2: 10.0.81.32
primitive vip4 ocf:titan:telemetry-vip \
        params ip=10.0.81.63 cidr_netmask=24 nic=eth1 \
        op monitor interval=5s
property cib-bootstrap-options: \
        have-watchdog=false \
        dc-version=2.0.1-9e909a5bdd \
        cluster-infrastructure=corosync \
        cluster-name=debian \
        stonith-enabled=false \
        no-quorum-policy=ignore \
        start-failure-is-fatal=false
rsc_defaults rsc-options: \
        resource-stickiness=100
alert ctb_manager "/opt/titan/compose/bin/cluster_events.py" \
        to localhost
admin@titan-8HlP2JLB:~$ 
```

Enable and Disable Node Standby Mode

In Standby mode, the node cannot host the IPv4 or IPv6 virtual IP addresses.

1. Log in as the **admin** to any of the broker nodes in the cluster via SSH. Use the password that was supplied during node installation.

2. Run the `sudo crm node standby 10.0.81.32` command. You can omit the node name if you are running this command on that node. You can see more details about this command [here](#).

3. Run the `sudo crm node online 10.0.81.32` command to move the node out of *Standby* status. You can see more details about the command [here](#).

```
● ● ●                     admin@titan-8HIP2JLB: ~                      ⌥⌘1
Stack: corosync
Current DC: 10.0.81.32 (version 2.0.1–9e909a5bdd) – partition with quorum
Last updated: Tue Jan 26 16:41:49 2021
Last change: Tue Jan 26 16:41:44 2021 by root via crm_attribute on 10.0.81.32

2 nodes configured
1 resource configured

Node 10.0.81.32: standby
Online: [ 10.0.81.31 ]

Active resources:

vip4    (ocf::titan:telemetry-vip):     Started 10.0.81.31
```

As you can see, *crm_mon* displays the standby status of the 10.0.81.32 node.

Move a VIP to a Specific Node

You may encounter circumstances in which you want to specify which node is running the IPv4 or IPv6 virtual IP address. If so, complete the following steps:

1. Log in as the **admin** to any of the broker nodes in the cluster via SSH. Use the password that was supplied during node installation.

2. Run the `sudo crm resource move vip4 10.0.81.32` command. You can see more details about this command [here](#).

3. Run the `sudo crm resource unmove vip4` command to make sure the VIP stays on the targeted node, otherwise the VIP will move back to the node it was previously on (before the move) at the next opportunity.

Finish Configuring Your System

To finish configuring your system, refer to the following sections in the Cisco Telemetry Broker User Guide:

- Destinations
- Inputs
- Broker Nodes

Contact Support

If you need technical support, please do one of the following:

- Contact your local Cisco Telemetry Broker Partner
- Contact Cisco Telemetry Broker Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Change History

Document Version	Published Date	Description
1_0	April 2023	Initial Version.
1_1	May 2023	Added the "Migrate Configuration to a New System" chapter.

Copyright Information

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 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 https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

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/go/trademarks. 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)