



Service Description: Cisco TelePresence Expert Access Service

This document describes Cisco's TelePresence Expert Access Service and the processes used by the Cisco Network Management Center (NMC) to provide remote management of your TelePresence solution. This Service Description is designed to provide a baseline understanding of and set expectations about the activities and deliverables that make up the TelePresence Expert Access Service. Please read this document carefully as it contains important information regarding the Services you have purchased from us.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. In the event of a conflict between this Service Description and your MSA or equivalent services agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller. If you have purchased these Services through a Cisco Authorized Reseller, this document is for informational purposes only; it is not a contract between you and Cisco. The contract, if any, governing the provision of this Service is the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Related Documents: The following documents posted at www.cisco.com/go/servicedescriptions/ should be read in conjunction with this Service Description and are incorporated into this Service Description by this reference:

- **Unified Communications Remote Management Service Glossary of Terms.** Capitalized terms not defined herein have the meanings assigned to them in the Glossary of Terms.

1 Cisco TelePresence Expert Access Service and Cisco TelePresence Remote Assistance Service – Service Overview

The Cisco TelePresence Expert Access Service and Cisco TelePresence Remote Assistance Service are intended to supplement a current support agreement for Cisco products, and only available where all Managed Components in a Customer's network are supported through a minimum of core services such as Cisco's SMARTnet and Software Application Services or Cisco's TelePresence Essential Operate Service, as applicable. Cisco shall provide the Cisco TelePresence Expert Access Service and Cisco TelePresence Remote Assistance Service described below as selected and detailed on the Purchase Order for which Cisco has been paid the appropriate fee. Cisco shall provide a Quote for Services ("Quote") setting out the extent of the Services and duration

that Cisco shall provide such Services. Cisco shall receive a Purchase Order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein. Cisco only provides support of Managed Components to the TelePresence rooms for which Services are purchased.

The objective of Cisco TelePresence Expert Access Service is to establish connection to and continually poll the TelePresence solution in an effort to collect call statistics and metrics to be used in troubleshooting technical issues and provide in-depth reporting.

1.1 Cisco TelePresence Expert Access Service

1.1.1 Managed Components covered under the Cisco TelePresence Expert Access Service:

- Monitoring the primary network path that supports TelePresence, and management of the management termination router and the IPSLA routers in each TelePresence room.
- Managed Components (i.e. Cisco CallManager) within Cisco's Unified Communication system on the Customer's Network that supports the TelePresence path.
- Managed Components in the Data Center
 - Cisco TelePresence Manager (CTS-Man)
 - Cisco TelePresence Multipoint Switch (CTMS)
 - Cisco Unified Video Conferencing (CUVC)

Note: The scope of Services for CUVC includes monitoring the CUVC device status, as well as the device connection to the Cisco TelePresence Multipoint Switch (CTMS). Services scope does not include non-Cisco TelePresence device connections to CUVC.

- Managed Components in the TelePresence room:
 - Codec(s)
 - Plasma Display(s)
 - Cameras
 - Projector
 - Cisco IP Telephony Phone
 - Optional Presentation Codec

- Auxiliary Control Unit

1.1.2 Infrastructure Connectivity Monitoring Supporting TelePresence

The objective of converged-infrastructure monitoring is to track network path characteristics that may impact TelePresence calls or degrade the TelePresence experience.

While this Service provides continual polling of the TelePresence Room and related infrastructure, this Service does not include proactive ticketing on Incidents. If an incident or outage occurs, a phone call must be placed directly to the Remote Operations Service help desk to open a Ticket. Conversely, the user may go to the Remote Operations Service ("ROS") web portal ("ROS Portal" or "Portal") and submit a Service Request.

Activities:

- Perform ongoing monitoring of critical network characteristics supporting TelePresence.

Deliverables:

- Confidence monitoring of the Telepresence traffic path, based on Cisco leading practices, including jitter, delay, and packet loss.
- Collection of threshold violations without ticketing.

1.1.3 Service Specific to TelePresence Room

TelePresence management includes the monitoring and management of the TelePresence environment to support your ability to make TelePresence calls to establish TelePresence meetings across your infrastructure. This Service includes the management of the TelePresence components as described in the Managed Components list. At the time a service Ticket is opened, Cisco troubleshoots TelePresence calls (to establish a meeting) and other impacting issues that affect the TelePresence call setup and quality of the TelePresence service. If an Incident is isolated to a TelePresence Managed Component, Cisco manages the Incident to resolution and notifies the appropriate Customer contact of the status. This does not include environmental factors such as room temperature, power, wiring, lightning, and HVAC.

The NMC monitors, in real-time, key TelePresence components and declares events for:

- Primary TelePresence Connectivity Status
- Secondary Left TelePresence Connectivity Status
- Secondary Right TelePresence Connectivity Status
- Camera Telnet Status
- Camera HDMI Status
- Plasma Cable Status (Loose Cable, Unplugged)

- Plasma Power Status (Fault)
- Phone Status (Fault)
- CCM Status (Fault, Not Registered)
- Projector Cable Status (Loose Cable, Unplugged)
- Projector Power Status (Powered Off)
- DVI Video Status
- DVI Signal Status

Activities:

- Perform Incident monitoring and management on the TelePresence components for which Cisco managed services is purchased.
- Perform Incident monitoring and management of the dedicated Cisco CallManager that enables TelePresence calls.
- Perform Incident monitoring of key network performance indicators, including network delay, jitter, and packet loss.

Deliverables:

- Active collection of alarms.
- At the request of the user, a service Ticket is opened and tickets are continually updated with status and results.
- Restoration of Service to enable end users to establish TelePresence meetings.

1.2 Cisco Remote Assistance Service

The Cisco Remote Assistance Service is a recommended add-on service for the Cisco TelePresence Expert Access Service. In order to provide Cisco Remote Assistance Service, access to your Cisco TelePresence Manager is required with full access provided to the Cisco Remote Assistance representative for related remote scheduling assistance activities. The following information pertains to this complementary service:

- 24x7 x365 Access to the TelePresence Service Center (TSC)
 - Representatives are available 24x7x365 via the one-touch Remote Assistance representative button in each supported TelePresence room.
 - Immediate escalation of issues requiring engineering support.
- Remote scheduling assistance
 - Representatives assist Customers with step-by-step scheduling instructions and escalate

any scheduling problems that cannot be resolved remotely to the on-site room contact, as designated by the Customer.

- Remote call setup assistance
 - Representatives assist Customers with step-by-step call setup instructions and escalate any call setup problems to Cisco technical resources (technical problems). Problems that cannot be resolved remotely are escalated to the on-site room contact, as designated by the Customer.
- “How-do-I” Help Desk
 - Representatives assist Customers with any questions related to the use of the TelePresence room. Formal or comprehensive training on the use of TelePresence is not covered by the Cisco Remote Assistance Service.
- Incident reporting [inbound/outbound]
 - This Service does not include proactive Incident reporting. Service Tickets are opened in response to a Customer request.
 - Once a Ticket has been opened at the Customer’s request, Cisco notifies the Customer-designated TelePresence room coordinator (Room Coordinator) when Incidents may impact scheduled calls (requires Cisco TelePresence Manager) or the quality of the TelePresence user experience.
 - Representative organizes the rescheduling of a TelePresence call, if necessary and/or desired.
 - Response to Customer calls (to Remote Assistance Help Desk) within 60 seconds, begin troubleshooting within thirty (30) minutes.
- Single point of contact for reporting of all TelePresence issues. This includes issues for referral to the Room Coordinator which includes, but is not limited to:
 - Issues requiring physical adjustment of TelePresence components.
 - Requests for or removal of supplies.
 - TelePresence room environment (i.e., temperature, room straightening).
 - Audio conferencing backup, if provided by the Customer. A Cisco Remote Assistance representative relays backup audio conferencing access information in the event

a TelePresence call cannot be established. The representative transfers the calling party into the audio bridge to minimize user inconvenience.

2 Incident Management

With the TelePresence solution, Cisco’s Network Management Center proactively monitors for key events and thresholds, but ticketing is not automatically invoked. Customer declared incidents must be reported to the Cisco Remote Operations Service (ROS) Service Desk by telephone or via the portal. Upon receipt of an incident by the Cisco ROS Service Desk, a Ticket is created. The Service Desk is responsible for managing the Incident, to include Customer communication throughout the Incident management process.

2.1 Incident Monitoring

The objective of Incident monitoring is to collect events that drive the Incident management process. Selected elements of Managed Components are polled 24 hours per day, 365 days per year.

Activities:

- Poll and collect information (24x7x365) on manageable elements of the TelePresence solution that may cause performance issues or degrade the experience.
- Respond to Customer declared events by manually creating a Ticket.
- Based on collected monitoring statistics, correlate Incidents, where applicable.
- Set Incident priority, depending on business impact and urgency.
- Isolate the cause of the Incident.

Deliverables:

- Manually generated Ticket based on Customer request.

2.1.1 Incident Ticketing

Activities:

- After Ticket has been manually created on Customer’s behalf, view Tickets online via the Cisco ROS Portal.
- Perform E-notification for Ticket events, if requested by the Customer.

Deliverables:

- Ticket updates at milestone events.

2.1.2 Notification

Cisco electronically notifies designated Customer contacts during incident lifecycle. Notifications are sent to an email address or email-capable mobile devices designated by the Customer. The Customer (or its preferred vendor) is notified at key milestones throughout the Incident and may view Incident status and detailed information via the Cisco ROS Portal.

Activities:

- Perform E-notification of Incidents, if requested by the Customer.
- Ticket updates at milestone events.

2.1.3 Resolution

After the Incident has been isolated, the NMC works to resolve the Incident. Resolution is complete when functionality (TelePresence Service) is restored. The resolution process includes any action the NMC requires to restore functionality or implement a work-around. The NMC uses work-around solutions to restore all or partial functionality when full functionality cannot be restored within committed timeframes. When a work-around is implemented, the Incident remains open and is worked by the NMC until resolved. Should the NMC require a change to a Managed Component to resolve an issue or implement a work around, the NMC refers to the Change Management Process.

Activities:

- Resolve Incidents.
- When required submit, a Request for Change ("RFC") through the Change Management process.
- Update the Ticket to include resolution notes.
- Perform E-notification for Ticket events, if requested by Customer.

2.1.3.1 Dispatch

The NMC dispatches vendors as needed and appropriate within the guidelines prescribed by the NMC. As vendors are dispatched, the Ticket is updated with information related to the dispatch.

Activities:

- Update the Ticket to include dispatch notes.
- Perform E-notification for Ticket events, if requested by the Customer.

2.1.3.2 Escalation

The Customer may request escalation of a Ticket at any time.

Activities:

- Update the Ticket to include escalation notes.

- Perform E-notification for Ticket events, if requested by Customer.

2.1.3.3 Validation

After the Incident has been declared resolved by the NMC, the NMC validates the Managed Component(s) to verify the resolution. If the result of the validation verifies that the Incident is resolved, the Ticket is updated with information related to the validation. If the result of the validation reveals that the Incident is not resolved, the Incident is returned to the resolution process for continued work.

Activities:

- Update the Ticket, to include validation notes.
- Perform E-notification for Ticket events, if requested by Customer.

2.1.3.4 Closing Tickets

Once the NMC declares an Incident resolved and verified, the incident is closed. In the event, the Incident recurs, a new Incident Ticket is created to accurately reflect the recurring nature of the Incident and aid in the identification of Problems. Any authorized Customer agent may proactively request Ticket closure for any Ticket. The NMC reviews the request, conducts a follow-up with the Customer and closes the Ticket.

Activities:

- Update the Ticket to include closing notes.
- Perform E-notification for Ticket events, if requested by the Customer.

2.2 Service Level Objectives

Severity handling and defined processes between Cisco and the Customer (or preferred vendor) are detailed during the Service Activation phase in the Cisco Operations Support Manual. The target Mean Time to Notify (MTTN), regardless of severity, is 15 minutes. Because this Service does not include proactive ticketing and is based on Customer initiated ticketing, the MTTN (Mean Time To Notify) begins at the time the Service Request is registered. The target Mean Time to Troubleshoot (MTTT), regardless of severity, is 30 minutes.

For any Incident requiring a dispatch (RMA of hardware or Telecommunications carrier), Cisco uses all reasonable efforts to restore service as quickly as possible. Cisco personnel work with the dispatched technicians or engineers to drive an issue to resolution, coterminous with existing SLAs between the Customer and the dispatched party (Carrier, preferred vendor, or onsite maintenance provider). Regardless of severity, Cisco provides no specific MTTR target, as this depends heavily on underpinning contracts with the dispatched party. For Cisco provided maintenance (TelePresence Essential Operate), on-site support includes the parameters defined in the TelePresence Essential Operate Service Description.

Severity 1

- TelePresence System is unavailable.
- Meeting in progress or scheduled within 4 hours.
- Cisco and Customer commit necessary resources 24x7 to resolve the issue.

Severity 2

- TelePresence System is unavailable or experience severely degraded;
- Meeting scheduled within 24 hours.
- Cisco and Customer commit full-time resources during normal business hours to resolve the issue.

Severity 3

- TelePresence System is unavailable or experience severely degraded; no meeting is scheduled within 24 hours.
- Performance and/or device alarms with a high probability of making the TelePresence system unavailable and/or degraded.
- Cisco and Customer commit resources during the normal business hours to restore service to satisfactory levels.

Severity 4

- Non-business impacting alarms.
- Other questions, issues, etc.
- Cisco and Customer commit resources during the normal business hours to provide information or assistance as requested.

3 Problem Management

Problem Management is the process used by the NMC to identify and solve recurring Incidents. The objective of Problem Management is to identify recurring Incidents and resolve the root cause to permanently remove them. The NMC analyzes Incident trends to identify patterns and systemic conditions. In the event a trend is detected, the Problem resolution is documented to help resolve future Incidents more quickly.

Activities:

- Analyze trends for Incidents on Managed Components.
- Identify recurring Incidents and refer to Incident Management for resolution.

Deliverables:

- Creation of a Ticket on the Portal for the Customer to view.

- E-notification for Ticket events, if requested by the Customer.

4. Change Management

Change Management is the use of standard methods and procedures for authorizing, documenting, and performing all changes. The objective of Change Management is to make necessary changes in an efficient and accountable manner.

4.1 Change Origination

The first step in Change Management is the origination of a Service Request. Service Change Requests may be Cisco recommended or Customer-requested changes and are summarized in the following table.

Cisco Recommended Changes		
Changes Required To:	Resulting in:	
Resolve an Incident	Logical or physical change	
Respond to a critical vulnerability	Logical change	
Apply a signature update to a security Managed Component	Logical change	
Address a problem	Logical or physical change	
Customer Requested Changes		
Changes Required to:	Category	Change description
Add, Delete or Change physical component on existing Managed Component	Change	Physical Change
Change existing logical functionality (Upgrades)	Change	Logical Change; logical voice MACS
Physically move Managed Component	Move	Physical Move
Add Managed Components	Add	Physical add
Addition of new functionality	Add	Logical add
Remove Managed Components	Delete	Physical delete

Deliverable:

- Creation of a Ticket on the Portal for the Customer to view.

4.1.1 Cisco-Recommended Changes

Cisco recommended changes originate from the NMC. Examples may include (but are not limited to) changes to port speed or duplex settings, access control list (ACL) modifications, logging level changes or software updates. Before executing a Cisco recommended change, the NMC evaluates the change and makes a recommendation to the Customer that includes the criticality and timeframe for implementation. The NMC does not execute a change until the Customer has authorized or pre-authorized the change. There are no additional charges for any Cisco recommended changes.

Cisco-recommended changes include:

- Changes to resolve an Incident.
- Changes in response to a critical vulnerability.
- Changes to address a Problem.

Activities:

- Provide change recommendations.
- Schedule recommended changes.

4.1.1.1 Changes required to resolve an Incident

The NMC may need to make changes to Managed Components to resolve Incidents. These changes are usually logical changes to Managed Component configurations for troubleshooting and implementing workarounds. Changes required to resolve Incidents are implemented as needed by the NMC in accordance with the Customer's Change Management policy.

4.1.1.2 Changes to respond to a critical vulnerability

Cisco recognizes that certain critical vulnerabilities have the capability to degrade a Customer's system and severely limit Services. As new vulnerabilities are released, the NMC evaluates the severity and potential impact to the Customer's TelePresence solution. If the vulnerability is judged by the NMC to be critical with respect to Customer safeguards, and the Customer is impacted by the vulnerability, the NMC recommends changes to correct the issue. If requested by the Customer, changes are executed according to the priorities and terms contained in this Service Description for Customer Requested Changes. Changes to address critical vulnerabilities are performed as quickly as possible, in coordination with the Customer.

4.1.1.3 Changes to address a problem

During the course of the Problem Management process, the NMC is required to make changes to TelePresence Managed Components to resolve Problems. These changes are typically logical changes to TelePresence Managed Component configurations for troubleshooting and implementing workarounds, and may also include working with

vendors. Changes required to resolve Problems are implemented as needed by the NMC in accordance with the Customer's Change Management policy.

4.1.2 Customer Requested Changes

Customer requested changes are changes that do not originate from the NMC. A Customer may use the on-line Change Management Process on the Cisco ROS Portal to request a change. The NMC evaluates the change request and works with the Customer to schedule the change.

A process that includes costs, timeframes, and guidelines for the work to be completed governs all Customer requested changes. These guidelines ensure that the NMC receives proper notice to arrange the required resources to complete the work and that the work is performed in a timely manner. The specifics of the Change Management Process, including any additional costs, are outlined in the Cisco change management document.

The NMC researches the impact of Customer requested changes and discusses the implications of a requested change with the Customer. If NMC believes the change requires additional information, planning, diligence, or testing, the NMC reserves the right to refuse the Customer requested change if Cisco believes the change may adversely affect the operations of the Managed Components of the TelePresence solution.

Customer-requested changes include:

- Physically Add, Delete or Change a component on an existing Managed Component.
- Change existing logical functionality (upgrade).
- Physically Move a Managed Component.
- Add a Managed Component.
- Addition of new functionality.
- Remove a Managed Component.

Activities:

- Work with Customer to understand their Change Management Process.
- Provide instructions for request a change via the Cisco ROS Portal.
- Schedule a change requests.

4.1.2.1 Change - Physical Change

A Physical Change is a change to a hardware element on an existing Managed Component, such as a network module or a hard drive. The installation process of a Physical Change involves loading and verification of the new Managed Component information in the NMC database, as needed. The configuration process of a Physical Change includes logical configuration changes to ensure the functionality of the

Managed Component. A Physical Deletion that requires a Cisco engineer to make modifications to the Customer's network infrastructure to allow the device to be removed (such as transferring functionality to another Managed Component, modifying routing, etc.) requires a Physical Change in addition to a Physical Delete. Physical Changes may be expedited for a fee.

4.1.3 Types of Changes

4.1.3.1 Change – Logical

A Logical Change includes changes to software on a TelePresence solution and its Managed Components. Logical Changes are divided into three categories: simple Logical Changes, complex Logical Changes and software upgrades. Simple Logical Changes require reduced levels of planning and less than four hours of work. Complex Logical Changes require an increased level of planning. These changes often involve multiple devices and require more than four hours of work. If a change is determined to be complex, it is treated as a project. Complex Logical Changes have one or more of the following traits:

- Introduction of a Service or functionality not currently used in the network.
- Required engineering resources exceed four hours.
- Significant planning is required.
- Requested work is comprised of ten or more devices.

Software upgrades require an increased level of planning and involve a separate fee as outlined in the pricing and scheduling table.

4.1.3.2 Move – Physical

A Physical Move is a change that physically moves a TelePresence solution Managed Component from one location to another. The Customer or a Partner is responsible for physically moving the component from one location to another. Cisco is responsible for making the necessary changes in the NMC database and the configuration of the Managed Component to ensure continuity of management. The NMC works with the Customer to coordinate the Physical Move. Physical Moves may be expedited for a fee.

4.1.3.3 Add – Physical

A Physical Add is the addition of a new component to be managed by the NMC. A data-gathering process involves verification and loading of all TelePresence solution Managed Component information in the NMC database, including serial numbers, maintenance contract information, circuit information, Carrier information, and more, as needed. The configuration process includes logical configuration changes to ensure that the new component can be managed. Physical Adds may be expedited for a fee.

4.1.3.4. Add – Logical

Logical Adds include the installation of new software on TelePresence solution Managed Components to enhance or introduce new services. Logical Adds are characterized by the installation of software that add functionality to the Managed Component, and do not require a high degree of planning and implications for other Managed Components. If the addition of functionality introduces new services to other Managed Components or end users, or if the functionality requires extensive planning, the Logical Add will be treated as a project.

Logical Adds treated as projects have one or more of the following traits:

- Introduction of a Service or functionality is not currently being used in the network.
- Engineering resources required exceeds four hours.
- Significant planning is required before implementation.
- Requested work is comprised of ten or more devices.

Logical Adds require an additional fee. The NMC evaluates each project and work with the Customer to approve the work to be done.

Most Logical Adds may be expedited for a fee.

4.1.3.5 Delete – Physical

Physical Deletes mean that Managed Components are removed from Cisco Expert Access Services. The device may or may not remain on the Customer's network. A Physical Deletion requiring a Cisco engineer to make modifications to the Customer network infrastructure to allow the device to be removed (such as transferring functionality to another Managed Component, modifying routing, etc.) is considered a Physical Delete and a Physical Change. Physical Deletes may be expedited for an additional fee.

4.2 Executing changes

After changes are executed, the NMC tests the change and notifies the Customer that the change was executed. Once the Customer accepts the change, the Ticket is closed. The status of changes may be viewed on the Cisco ROS Portal.

Activities:

- Process requests via the Portal.
- Maintain a change database visible through the Portal.
- Assess impact of the changes.
- Classify change requests.
- Authorize and schedule change requests.
- Coordinate changes.

- Update Tickets, to include change status.
- Review and close change requests.

Deliverables:

- Executed change.
- Ticket update with change notes.

4.1.3.5 Pricing and Scheduling

Pricing and scheduling related to Customer requested changes are shown in Appendix A.

5 Web Portal

Cisco provides an on-line Portal for the Customer to review Tickets, Ticket metrics, and reports for their Managed Components.

Deliverables:

- Portal accounts for authorized employees.
- Inventory information (as available).
 - System description.
 - Maintenance vendor.
 - Maintenance coverage type and contract number.
 - Serial number.
 - IP Address.
 - Last date of configuration archive.
- Ticket information (as available).
 - Ticket identification number.
 - Ticket opened date and time
 - Ticket description
 - Cause of Incident
 - Ticket status
 - Site(s) affected
- Reports (as available).
 - Performance Analysis – Data analysis reports that graph key Managed Component

metrics such as utilization and performance; does not currently include usage statistics for TelePresence end-points.

- Daily.
- Weekly.
- Monthly.
- Monthly Engineering Analysis – A monthly report containing engineering recommendations including high and low exceptions.
- Availability – The uptime of Managed Components; does not currently include usage statistics for Telepresence endpoints.
 - Individual Device – Availability for a single Managed Component.
 - Device Type – Availability for a group of Managed Components of the same type.
- Exceptions – High and low exceptions for utilization and errors.
 - Individual Device – Exceptions for a single Managed Component.
 - ◆ Daily
 - ◆ Weekly
 - Device Type – Exceptions for a group of Managed Components of the same type.
 - ◆ Monthly High.
 - ◆ Monthly Low.
- Ticket Metrics.
 - Mean Time to Notify – The average time to notify the Customer of Tickets across a selected timeframe.
 - Mean Time to Resolve; Single Event – The average time to resolve single event Incidents across a selected timeframe.
 - Mean Time to Resolve; Multiple Events – The average time to resolve multiple event Incidents across a selected timeframe.
 - Ticket Cause Analysis – A graph of the causes of Incidents.

- Ticket Origination Analysis – A graph of the originators of Tickets.
- Ticket Volume: Top 10 Sites – Volume of Tickets across the most highly Ticketed sites.
- Tickets: Open vs. Closed – Tickets opened and closed per day across a selected timeframe.

6 Customer Responsibilities

6.1 Service Activation

To ensure Cisco's ability to provide Services for Managed Components, Cisco requires the Customer to:

- Assign a project manager to represent the Customer during the service activation phase.
- Assign a technical lead to assist Cisco with establishing the network access required for remote management.
- Supply information requested in the Service Activation Kit.

6.2 Connectivity and Network Access

- The component that terminates the management channel must have access to the other managed devices. The Customer must allow access to the other managed devices from the termination point of the management channel.
- Cisco's Remote IT-Infrastructure Management Service is delivered using a collection of protocols and ports. The Customer must allow the collection of data for Managed Components.
- To ensure that the NMC can provide Services for the TelePresence solution, Customer must provide Cisco full read/write SNMP access and full administrative privileges (enable mode, root access, Admin access, etc.) to all Managed Components in the TelePresence path, as well as Unified Communications components (dedicated Cisco Call Manager) associated with TelePresence and all TelePresence components

6.3 Operations Support

- A Customer contact is assigned as a coordinator for each TelePresence end-point for which Cisco Services have been purchased to assist Cisco with non-technical troubleshooting tasks in that TelePresence room.
- A Customer contact who coordinates the ability to:
 - Access network components supporting the TelePresence solution

- Have access to the Customer's support personnel knowledgeable of the scheduling system. If Microsoft's Exchange (Exchange) software is used for TelePresence, provide support contact with knowledge of the Exchange server and integration platform.
- The Customer is responsible for assigning a Process Manager who reviews and coordinates the approval of changes to the Cisco-Customer Operations Support Manual.

6.4 Managed Components

- The Customer is responsible for providing and maintaining the network equipment that is not a Managed Component.
- The Customer is responsible for the physical security of the Managed Components.
- The Customer agrees to allow Cisco to retain and publish aggregate statistics and metrics for non-identifiable trending analysis.
- The Customer is responsible for providing back-up procedures and configuration data for the network equipment (non-Managed Components).
- The Customer provides back-up procedures for managed devices that do not have configurations that can be archived remotely (Cisco CallManagers). This includes devices not running CatOS or Cisco IOS. Cisco assists in the configuration of the backups. The Customer is responsible for ensuring the backups run successfully.

6.5 Support for Non-Managed Components

- Cisco does not provide any support for Non-Managed Components. Cisco has a professional Services process for handling support requests.
- The Customer is responsible for managing Non-Managed Components.

6.6 Communications and Change Management

- Cisco has a co-management approach to Managed Services, allowing the Customer and other Customer-approved vendors to retain access to Customer devices. Because multiple parties can make changes to the environment, Cisco requires that anyone with access to the Customer's environment follow a consistent and documented Change Management Process. This process is reviewed and agreed upon prior to completion of the implementation process.
- The Customer is responsible for supplying the NMC with changed data with respect to the Customer and Managed Components, as needed, via the Cisco ROS Portal.

- The Customer is responsible for the timely delivery of information required for configuration of Managed Components notification procedures.
- The Customer must notify the NMC 72 hours in advance of any scheduled maintenance.
- The Customer maintains sole responsibility for informing Cisco of Customer employee status changes.
- The Customer is responsible for providing and maintaining a list of Customer employees authorized to request changes.
- The Customer is responsible for providing and maintaining an escalation path within the Customer's employee base.
- The Customer is responsible for user training of TelePresence solution.
- The Customer is responsible for reporting any issue that impacts the quality, usability or availability of the TelePresence room. *There is no proactive ticketing at this service level.* The Customer can report these issues by either a telephone call to the Service Desk or by logging a Service Request on the ROS Portal.

6.7 Remote Assistance Service

- Provide designated Room Coordinator for each TelePresence end point.
- Be responsible for non-technical troubleshooting tasks.
- Have visibility and access into Customer scheduling system of their designated TelePresence end-point.
- Have email/phone access to Customer personnel who schedule the TelePresence room.
- Have direct on-site access to Customer designated TelePresence end-point, as well as each of the Managed Components within that room.

7 Remote Management Activation

The Remote Management Activation is a process in which Cisco prepares the Customer's IT infrastructure for Cisco management. Using our proven service activation methodology enables an efficient and low impact effort to receive Cisco's management Services. This framework includes:

- Discovering the IT infrastructure.
- Planning the transition to management.
- Implementing the management operations.

7.1 Discovering the IT Infrastructure

Discovering the IT infrastructure includes the pre-implementation activities that provide Cisco with a high-level understanding of the Customer's business and IT infrastructure needs. This assists our team in having an accurate understanding of the Customer's requirements before the planning and implementation process begins.

Activities:

- Identify key Customer participants and schedule initial kick-off meeting.
- Initial engagement with the Customer.

Deliverable:

- Introduction package.

7.2 Planning the Transition to Cisco Remote Management Activation

The purpose of planning the transition is to prepare both the Customer and Cisco for a smooth management transition. This involves collecting and validating all technical details required to enable remote IT infrastructure management, ensuring that the Customer has a clear understanding of Service features, and establishing joint interaction methods. Each site is assessed to ensure that no further work is needed before the site is turned up under management.

Activities:

- Establish key relationships with the Customer.
- Work with the Customer to develop an implementation plan.
- Gather TelePresence site information from the Customer and/or Cisco or Partner PDI Team.
- Gather key Managed Component information from the Customer and/or Cisco or Partner PDI Team.
- Enter the Customer's Managed Component information into the NMC database.
- Define an escalation plan for the NMC and the Customer.
- Communicate the Change Management Process.
- Complete applicable Letters of Agency.
- Order Management Circuit.
- Plan for IPSLA router installation

Deliverables:

- Completed Service Activation Kit.
- Completed Cisco Operations Manual.
- Letter of Agency on file in the NMC.

- Cisco Transition plan document.
- Installation date for Managed Circuit (Cisco provided).

7.2.1 Remote Infrastructure Operations Readiness Approval

Prior to implementing management operations, the NMC either approves an existing managed device or make recommendations required for accepting a new managed infrastructure. If the necessary changes are not made, acceptance of the order may be delayed or withdrawn. If the Customer wishes to engage Cisco to implement the recommendations, a separate Agreement to make the changes may be required.

7.3 Implementing Management Operations

Implementing management operations involves executing the transition project plan developed in the planning of the transition to management process. Cisco appoints a designated project coordinator who can focus on established timelines and commitments. During this phase, Cisco establishes management connectivity and ensures the Customer contacts are aware of how to interact with the NMC during delivery of the Service.

Activities:

- Cisco will provide management connectivity to one location in the continental United States and associated management router to each end-point to effectively manage the solution, or Cisco will provide necessary connectivity information for Customer provided connectivity from one location outside the continental United States to the nearest Cisco Point of Presence and associated management router.
- Cisco provides a Cisco Management Router (IPSLA router that is Cisco owned) at each TelePresence end-point, as necessary, to monitor key performance indicators. Installation of Management (IPSLA) routers is the responsibility of the Customer.
- Establish management access for each Managed Component via the Management Connectivity.
- Review the configuration of all Managed Components to ensure readiness for remote management.
- Work with the Customer on any initial management configuration issues and/or changes required for successful management.

- Begin ongoing Incident monitoring of Managed Components.

Deliverables:

- Establish Cisco ROS Portal access and verify Managed Components inventory.
- Publish scheduled events.
- Train Customer employees in the use of the Portal.
- Provide the Customer with a complete inventory of Managed Components, published on the Portal.
- IPSLA routers installed and verified.
- Management Connectivity installed and verified.
- Perform Gap Analysis of Managed Components inventory and resolve any discrepancies.
- Publish Cisco Operations Manual to Customer personnel.
- Cisco TelePresence Expert Access support activated.

As necessary for the NMC to perform its responsibilities as stated in this Service Description, the NMC maintains an information repository of data with respect to the Customer and the Managed Components that are included in the Cisco Operations Manual.

8 Services Not Covered

In addition to those Services Not Covered posted at www.cisco.com/go/servicedescriptions/, the following are not supported under the Cisco TelePresence Expert Access Service:

- Installation of any component, including IPSLA routers or devices that terminate the management connection.
- Support of a Product (including a Managed Component) that is not on the primary TelePresence path and not managed by Service herein.
- Support of scheduling software or the integration of scheduling software to Cisco TelePresence Manager.

Appendix A – Pricing and Scheduling

Customer Requested Changes					
Category	Type	Turnaround Time	Standard Fees	Notes	Expedite Fees
Change	Logical	72 Hours*	\$0		\$175/ per request ¹
	Physical	7 Days*	\$350		\$1200 + Time and Materials/ per device ¹
Move	Physical	14 Days*	\$350	This does not include the physical move of a TelePresence Room and all of its components.	
Add	Physical	14 Days*	\$350		
	Logical	14 Days*	\$350		
Delete	Physical - Simple	7 Days*	\$0		
	Changes greater than four hours of work	See Note**	Cisco Remote Management Services Professional Services: \$250 per hour with 4 hour minimum	Scope and cost to be determined on an individual case basis	
Project	Changes greater than four hours of work	See Note**	Cisco Remote Management Services Professional Services: \$250 per hour with 4 hour minimum	Scope and cost to be determined on an individual case basis	Handled within the Statement of Work process

¹ Timing subject to hardware, vendor, and Cisco Expert Access Services resource availability

* All timeframes stated in calendar days

** Addition of a new managed site requires PDI (Plan, Design, and Implement) work that must be handled by a qualified PDI ATP Partner prior to Cisco Remote Management Services taking the equipment under management.

Note: Expedite Fee means charges paid by the Customer to Cisco to perform Customer requested changes without the change lead-time. Expedited Customer requested changes can always be cancelled or changed; however, the Customer will still be responsible for half of the Expedite Fee.

-END-