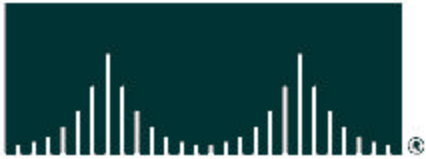


CISCO SYSTEMS



Cisco Remote Operations (Cisco ROS)

Service Descriptions and Change
Management Documents

Version 1.0

The following provides detailed descriptions of Cisco's Remote Operations Service Offerings. Please select the section of the document matching the service offering desired:

TABLE OF CONTENTS

- [Cisco Remote IT-Infrastructure Management Services](#)
- [Cisco WAN/LAN-Management Services](#)
- [Cisco IP Telephony-Management Service](#)
- [Cisco Security-Management Services](#)
- [Cisco Change-Management Services](#)
- [Glossary of Terms](#)
- [Cisco Supported-Device List](#)

1.0 Introduction

This document describes the family of Cisco Remote Operations Services (Cisco ROS) available to support the remote monitoring and management of Cisco routers, switches, IP Telephony, IPC applications, firewalls, intrusion detection devices, and Cisco Security Agent. The purpose of this document is to provide in-depth and detailed descriptions of all of the Cisco ROS services that are available for either sale or resale.

This document is divided into multiple service-related modules, an Operations -related device list, and a [Glossary of Terms](#).

Each service-related module is designed to deliver a baseline understanding of the activities and deliverables associated with the service processes and to set expectations about the services.

- **Cisco Remote IT-Infrastructure Management Services**

These services consist of core processes used by the Cisco Network Operations Center (NOC) to provide basic management of a Customer/Customer's managed components.

- **Cisco WAN/LAN-Management Services**

These services consist of processes used by the Cisco NOC to manage the WAN and LAN as complete systems and to maximize the availability of each. In addition, these services include reports and optional services. Unless otherwise specified in this service description, the NOC will also follow the processes outlined in the description for [Cisco Remote IT-Infrastructure Management Services](#).

- **Cisco IP Telephony-Management Services**

These services consist of processes used by the Cisco NOC to manage converged infrastructure and the call-management system as a complete system, as limited by the approved device and managed component list, and to maximize the availability of the voice system to complete calls for end users. In addition, these services include IP Telephony specific reports. Unless otherwise specified in this service description, the NOC will also follow the processes outlined in the description for [Cisco Remote IT-Infrastructure Management Services](#).

- **Cisco Security-Management Services**

These services consist of processes used by the Cisco NOC to address infrastructure security-related issues. The application of these services is dependent on the technology features and capabilities. Services can be selectively applied to specific infrastructure technologies for maximum benefit. Unless otherwise specified in this service description, the NOC will also follow the processes outlined in the description for [Cisco Remote IT-Infrastructure Management Services](#).

- **Cisco Change-Management Services**

These services consist of processes used by the Cisco NOC to process and handle Moves, Adds, Changes, Deletions, and Upgrades, specifically those governing moving devices, adding devices or configured components, changing devices or configured components, deleting devices and configured components, and upgrading software of managed devices. These services are to be used in conjunction with the Remote IT-Infrastructure Management Services and the specific product-related management services (WAN/LAN, IPT and Security) described in this document.

- **Cisco Remote-Operations Supported-Device List and Glossary of Terms**

The Supported-Device List highlights the devices that are supported under Cisco ROS. The [Glossary of Terms](#) defines the many different and unique terms and acronyms found within each of the Cisco ROS modules.

-End-



Cisco Remote IT-Infrastructure Management Services

1.0 Introduction

This document describes Cisco's Remote IT-Infrastructure Services and the processes used by the Cisco NOC to provide basic management of a Customer/Customer's managed components. This service description is designed to provide a baseline understanding of the activities and deliverables associated with the processes that make up Remote IT-Infrastructure Management and to set expectations about the service. Please read this document carefully as it contains important information regarding the Services that you have purchased from us.

Capitalized terms are defined in the [Glossary of Terms](#) at the end of this document.

Remote IT-Infrastructure Management Services are divided into three major parts: Remote Management Activation, Remote IT-Infrastructure Management, and the Web portal. In addition, there are Customer/Customer's responsibilities that must be met to deliver the service. Except where specified, all of the processes described in this document are delivered as part of Remote IT-Infrastructure Management. There are also specialized services that build on the core service. Specialized services are purchased separately and are bundled with the core service described in this document depending on the needs of the Customer and the technologies requiring management.

Core Service	Specialized Services
Remote IT Infrastructure Management Services	WAN/LAN
	IP Telephony
	Security

2.0 Remote Management Activation

The Remote Management Activation is a process in which Cisco prepares a Customer's IT infrastructure for Cisco management. Over time, Cisco experts have determined the best practices for preparing a Customer's infrastructure and then created a framework from these best practices for use in managing and activating Customer IT infrastructures. Using our framework enables an efficient and low-impact effort of enabling a Customer's IT infrastructure to receive Cisco's management services. This framework includes:

- Discovering the IT Infrastructure.
- Planning the Transition to Management.
- Implementing Management Operations.

2.1 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 processes begin. Our objective is to prepare an action plan to

Activities:

- Have initial engagement with the Customer.

Deliverable(s):

- Introduction Package.

2.2 Planning the Transition to Management

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

Activities:

- Establish key relationships with the partner and Customer.
- Work with the Customer and/or partner to develop an implementation plan.
- Gather the key site information from the partner and/or Customer.
- Gather the key managed-component information from the partner and/or Customer to provide management.
- Enter the Customer's managed-component information into the applicable NOC databases.
- Define an escalation plan for the NOC and the Customer.
- Define the change-management process.
- Complete applicable Letters of Agency

Deliverable(s):

- Letter of Agency on file in NOC.
- Escalation plan published to Customer.
- Transition plan.

2.2.1 Remote-Infrastructure Operations Readiness Approval

Prior to implementing management operations, the NOC will either approve an existing managed site or make recommendations required for accepting a new managed infrastructure. If the necessary changes are not made, acceptance of the order may be withdrawn. If the Customer wishes to engage Cisco to implement the recommendations, a separate statement of work to make the changes may be required.

2.3 Implementing Management Operations

Implementing management operations involves executing the transition project plan developed in the planning the transition to management process. To provide a single point of contact to apply ongoing focus on established timelines and commitments, the NOC will appoint a designated project coordinator.

During this phase, the NOC will establish management connectivity and ensure Customer contacts are aware of how to interact with the NOC during delivery of this service.

Activities:

- Establish management access for each managed component through the Customer provided site management channel. (See [Section 5.2 - "Connectivity."](#))
- Review and verify the configuration of all managed components.
- Work with the Customer on any initial management configuration issues and/or changes required for successful management.
- Test and accept each managed component for ongoing operations management coverage.
- Begin ongoing incident monitoring of managed components. (See [Section 3.1 - "Incident Monitoring."](#))

Deliverable(s):

- Publish scheduled events on the portal.
- Train Customer employees on use of the portal.
- Provide the Customer with a complete inventory of managed components, published on the portal.

As necessary for the NOC to perform its responsibilities as stated in this service description, the NOC will maintain an information repository of data with respect to the Customer and the managed components.

3.0 Remote IT-Infrastructure Management

Remote IT-Infrastructure Management serves as the core management process for all Cisco managed components. Additional specialized services add to the processes described in this document and can be purchased separately.

All services are designed to be delivered from the NOC and require remote access and control. These services apply to infrastructure devices such as routers, switches, infrastructure application servers, and specialized security technologies such as firewalls and intrusion detection/prevention technologies. Certain service components and specializations may only be applicable to certain devices. For a detailed understanding of which technologies are covered, refer to the Supported Systems table in Section 6.0.

The service consists of the following service components:

3.1 Incident Monitoring

The objective of incident monitoring is to detect incidents that initiate the incident management process.

Selected elements of managed components will be proactively monitored for status 24 hours per day, 365 days per year. Where available, availability and performance indicators will be collected from managed components. When an incident is detected, the incident is correlated.

The Customer and the partner may report incidents on managed component(s) as service requests. Service requests may be made on the portal.

Activities

- Monitor (24x7x365) selected elements proactively on all managed components.
- Detect incidents.
- Correlate incidents where applicable.

Deliverable(s)

- Confirmed incidents.
- E-notification of confirmed incidents.

3.2 Incident Management

Incident management is the process the NOC uses to solve real-time incidents in Customers' managed components. The goal of incident management is to restore normal service operation as quickly as possible with minimum disruption to the business and to strive for the highest levels of availability and satisfaction.

The incident management processes include multiple levels of support provided by the NOC. It also includes creating, maintaining, and publishing documents that indicate the status of the incident through the resolution and closure process.

3.2.1 Opening Incidents as Tickets

The NOC works through the incident management process to resolve incidents. Incidents are correlated and confirmed by the incident monitoring process.

Activities:

- View tickets online via the portal.
- Perform Enotification for ticket events, if requested by Customer.

3.2.2 Notification

Cisco E-notification is available for Customers and partners to receive information about tickets and incidents for all incident-management stages. Cisco also provides access to the portal for status updates.

Activities:

- Perform Enotification for ticket events, if requested by Customer.

3.2.3 Priorities

Tickets will be worked in order of priority. Priorities are set by the NOC on a per-ticket basis depending on a variety of factors including: severity, scope of impact, and Service-Level Agreements.

3.2.4 Isolation

The NOC will isolate and locate the cause of the incident. Once isolation has occurred, the NOC will update the ticket with information related to the isolation and then proceed to the resolution phase.

Activities:

- Update portal ticket to include isolation information,
- Perform Enotification for ticket events, if requested by Customer,

3.2.5 Resolution

After the incident has been isolated, the NOC will work to resolve the incident. Resolution is complete when functionality is restored. The resolution process includes any action the NOC requires to restore functionality or implement a work-around.

The NOC will utilize work-around solutions to restore all or partial functionality when full functionality cannot be restored within service-level agreements. When a work-around is

utilized, the incident will continue to remain open and will be worked by the NOC until resolved.

- Should the NOC require a change in a managed component to resolve an issue or implement a work around, the NOC will refer to the change-management process, ([See Section 3.4 – “Change Management.”](#))

Activities:

- Resolve incident
- Submit, when needed, a change-management authorization request and referral to the change-management process. ([See Section 3.4 – “Change Management.”](#))
- Update portal ticket to include resolution notes.
- Perform Enotification for ticket events, if requested by Customer.

3.2.5.1 Dispatch

The NOC will dispatch vendors as needed and appropriate within the resolution steps prescribed by the NOC. As vendors are dispatched, the ticket will be updated with information related to the dispatch.

Activities:

- Update portal ticket to include dispatch notes.
- Perform Enotification for ticket events, if requested by Customer.

3.2.5.2 Escalations

The Customer or the partner may request escalation of a ticket on the portal at any time.

Activities:

- Update portal ticket to include escalation notes.
- Perform Enotification for ticket events, if requested by Customer.

3.2.6 Validation

After the incident has been declared resolved by the NOC, the NOC will validate the managed component(s) to verify that the incident has been resolved.

If the result of the validation verifies that the incident has been resolved, the ticket will be updated with information related to the validation. If the result of the validation reveals that the incident has not been resolved, the incident will be returned to the Resolution process for continued work until resolved. ([See Section 3.2.5 – “Resolution.”](#))

Activities:

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

3.2.7 Closing Tickets

After the incident has been resolved and verified in the validation process, the ticket closure procedure begins. Before the ticket is closed, the Customer must agree that the incident is resolved.

When the NOC declares the incident resolved and verified, an E-notification is delivered to the Customer, and the ticket is placed in a state of auto closure. If the Customer does not respond to the E-notification within the Customer-defined timeframe, the Customer agrees that the ticket will be closed without further action.

If the Customer wishes to hold closure of the ticket before the auto-close window expires, the Customer may request through the portal that the ticket be held and then add additional information relevant to the incident. The NOC will contact the Customer to request additional information as needed.

Any authorized Customer agent may also proactively request ticket closure on the portal for any ticket. The NOC will review the request and close the ticket or follow up with the Customer for more information as needed.

Activities:

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

3.3 Problem Management

Problem management is the process used by the NOC to identify and solve recurring problems. The objective of problem management is to identify problems for the incident management process to address, leading to a decline in incidents from recurring problems.

The NOC will analyze incident trends to identify patterns and systemic conditions. In the event a trend is detected, the results will be introduced into the incident-management process for resolution.

Activities:

- Analyze trends for incidents on managed components.
- Identify recurring incidents and refer to Incident Management for resolution.

Deliverable(s):

- Creation of a ticket on the portal for the Customer to view.

- E-notification for ticket events, if requested by Customer.

3.4 Change Management

Change management is the process used by the NOC to ensure standardized 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, utilizing standard processes. For further information on change management, please refer to the [Cisco Change-Management Services](#) description.

3.4.1 Change Origination

The first step in change management is the origination of a service request. Change requests originate from two categories: Cisco-recommended changes and Customer-requested changes. The change-origination process describes the handling of each change category.

For each change category, a ticket is created or updated for the Customer to track the progress of the change.

Deliverable(s):

- Ticket on the portal for the Customer to view.

3.4.1.1 Cisco-Recommended Changes

Cisco-recommended changes originate from the NOC. Before executing a Cisco-recommended change, the NOC will evaluate the change and make a recommendation to the Customer that includes the criticality and timeframe for implementation. The NOC will not execute a change until the Customer has authorized the change to be made.

Cisco-recommended changes include:

- Resolve an incident.
- Respond to a critical vulnerability.
- Apply a signature update to a security managed component.
- Address a problem.

Activities:

- Provide the Customer with recommendations to make changes.
- Schedule recommended changes.

3.4.1.2 Customer-Requested Changes

Customer-requested changes originate from the Customer's authorized agents and employees.

The Customer can use the online change-management process on the portal to request Customer-requested changes. The NOC will evaluate the change request and work 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 NOC 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.

Customer-requested changes include:

- Add, Delete or Change physical component on existing managed component.
- Change existing logical functionality (upgrades).
- Physically move managed component.
- Add managed components.
- Addition of new functionality.
- Remove managed components.

Activities:

- Work with Customer to understand their change-management process.
- Provide a process for requesting changes via the portal.
- Schedule change requests.

3.4.2 Executing changes

After changes are executed, the NOC will test the change and notify the Customer that the change has been executed. Once the Customer accepts the change, the ticket will be closed. The status of changes can be viewed on the portal.

Activities:

- Process and login requests via the portal.
- Maintain a change database visible through the portal.
- Assess impact of changes.
- Classify change requests.
- Authorize and schedule change requests.
- Coordinate changes.
- Update portal tickets to include change status.
- Review and close change requests.

Deliverable(s):

- Executed change.

- Portal ticket updated with change notes.

4.0 Web Portal

Cisco provides an online portal for Customers and partners to review tickets, ticket metrics, and reports for their managed components. Additional reports may be included with the service based on the Customer’s contracted services.

Deliverable(s):

- Portal logins for each of the Customer authorized employees.
- Inventory information on the portal (as available).
 - o System description.
 - o Maintenance vendor.
 - o Maintenance coverage type and contract number.
 - o Serial number.
 - o IP Address.
 - o Last date of configuration archival.
- Ticket information on the portal (as available).
 - o Ticket identification number – The tracking number assigned by the NOC to each ticket.
 - o Ticket opened date and time – The date the ticket was opened.
 - o Ticket description – A brief description of the incident(s) represented in the ticket.
 - o Cause of incident – Where known, the underlying cause of the incident.
 - o Ticket status – The current status of the ticket.
 - o Site(s) affected – Within the ticket, the site locations where managed components are affected.
- Reports on the portal (as available).
 - o Performance Analysis – Data analysis reports that graph key managed component metrics such as utilization and performance.
 - Daily.
 - Weekly.
 - Monthly.
 - o Monthly Engineering Analysis - An automated monthly report containing engineering recommendations including high and low exceptions.

- o Availability – The uptime of managed components.
 - Individual Device – Availability for a single managed component.
 - Device Type – Availability for a group of managed components of the same type.
- o 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.
- o Ticket Metrics.
 - Mean Time to Notify – The average time to notify the Customer of tickets across a selected timeframe.
 - Mean Time to Test – The average time to test managed components during incidents across a selected timeframe.
 - Mean Time to Isolate – The average time to isolate incidents 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.
 - Work Ticket Summary – The Work Ticket Summary report shows a summary of work tickets over a specified period of time. You

can use the report to view all the non-outage related work performed during a given time period.

5.0 Customer Responsibilities

To ensure that the NOC is enabled to provide services for managed components, Cisco requires Customers to supply information, communications, and connectivity. These requirements are critical to the NOC to provide optimal, and in some cases any, services.

5.1 Equipment

- Customer is responsible for providing and maintaining the hardware and software to be managed as managed components including maintenance coverage on the managed components.
- Customer is responsible for the physical security of the managed components.
- Customer must agree to allow Cisco to retain and publish aggregate statistics and metrics for non-identifiable trending analysis.
- Customer is responsible for providing back-up procedures and configuration data for managed components that do not have configurations that can be archived remotely. The NOC will work with the Customer to provide back-up procedures for these managed components so that these configurations are available for recovery from disk drives on other servers or on-site tape systems at the Customer's premises. The Customer is responsible for ensuring that these backups run correctly.
- If the Customer requires Cisco to provide optional staging services, or requires equipment to be sent to Cisco, the Customer agrees to ship equipment via pre-paid freight to and from the Cisco locations.

5.2 Connectivity

- The Customer is responsible for providing one or more management channels, such as a Frame Relay PVC or a dedicated VPN tunnel, to a managed component at a site of the Customer's network. The size of the management channel can vary depending on the number and type of managed components and the services purchased.
- The Customer should provide out-of-band access to managed components in the form of a 1FB phone line or dedicated PBX extension with DID capabilities prior to the installation date at each site where managed components are located. The out-of-band access phone line must be connected to a dedicated dial modem provided by the Customer or purchased from Cisco.

- The component where the management channel terminates must have access to the other managed devices.
- Cisco's Remote IT-Infrastructure Management service is delivered using a collection of protocols and ports. All of these designated entities are required in order to receive Cisco's full suite of management services.

5.3 Access to Managed Components

- The Customer is responsible for providing appropriate access to all managed components.
- The Customer must agree to non-disruptive inquiries for inventory asset discovery of managed components.
- Customer must be willing to use an access-control server to ensure configuration changes are logged in environments where multiple parties share access to managed components.
- Customer must provide appropriate access to managed devices to allow remote archiving of IOS device configuration files. Remote archiving enables Cisco to rapidly recover from device corruption or failure.
- Customer is responsible for providing technical or non-technical "virtual arms and legs" at remote sites to assist the NOC in tasks that cannot be performed remotely.

5.4 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 any non-managed components.

5.5 Communications

- The Customer is responsible for working with Cisco to allow Cisco's change-management process to work within the confines of the Customer's change-management process. Cisco takes a co-management approach to managed services allowing Customers and other Customer-approved vendors to retain access to the Customer's 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 processes. This process will be reviewed and agreed upon prior to completion of the implementation process.
- The Customer is responsible for supplying the NOC with changed data with respect to the Customer and managed components, as needed, via the portal.

- The Customer is responsible for the timely delivery of information required for configuration of managed components -notification procedures.
- The Customer should notify the NOC 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 employees.

5.6 Training

- The Customer is responsible for end-user training on application functionality.

For more information on change management, please refer to the [Cisco Change-Management Services](#) description.

-END-



Cisco WAN/LAN-Management Services

1.0 WAN-Management Services

This document describes Cisco's WAN-Management Services. This service is just one of the service modules (WAN/LAN, IP Telephony Management and Security-specialized services) that you can purchase. Please read this document carefully as it contains important information regarding the services that you have purchased from us.

Capitalized terms are defined in the [Glossary of Terms](#) at the end of this document.

NOTE: When purchasing this service, please ensure that you have also read the [Cisco Remote IT-Infrastructure Management Services](#) description and the [Cisco Change Management Services](#) description. The Cisco Remote IT-Infrastructure Management Service is a prerequisite for Cisco WAN-Management Services, and the Change Management Services document outlines how we process Moves, Adds, Changes, Deletions, and Upgrades.

Cisco Remote IT-Infrastructure Management Services are a prerequisite for Cisco WAN-Management Services. Unless otherwise specified in this service description, the NOC will also follow the processes outlined in the [Cisco Remote IT-Infrastructure Management Services](#) description.

The objective of Cisco WAN-Management Services is to manage the WAN as a complete system and to maximize the availability of the WAN system. In addition, Cisco WAN-Management Services include reports and optional services.

WAN/LAN management services are applicable to router technologies that terminate WAN circuits and are designed to provide the highest levels of availability for WAN connectivity, including:

- Routers
- VPN Termination Devices

1.1 WAN-Availability Management

The objective of WAN availability management is to maximize the availability of the WAN as a system. Using the processes outlined in this service description, and in the [Cisco Remote IT-Infrastructure Management Services](#) description, the NOC staff will measure and manage the WAN.

Activities:

- Provide ongoing monitoring and management of incidents on WAN circuits and the LAN-facing ports of WAN-managed components.

- Manage problems of WAN circuits and the LAN-facing ports of WAN-managed components.

Deliverable(s):

- WAN/LAN availability greater than or equal to the SLA for any complete month of service.

1.1.1 WAN Incident Monitoring

The objective of WAN incident monitoring is to monitor the Customer's WAN as a system for incidents instead of as a series of individual managed components. WAN incident monitoring will follow the Incident Monitoring process described in the [Cisco Remote IT-Infrastructure Management Services](#) description (See [Section 3.1, "Incident Monitoring"](#)), and add the incident monitoring of WAN Circuits on Managed Components.

Activities:

- Monitor incidents of WAN circuits on management components.

Deliverable(s):

- Confirmed incidents on WAN circuits.

1.1.2 WAN Incident Management

The objective of WAN Incident Management is to react to incidents on the Customer's WAN and, as a result, increase the WAN Availability. WAN Incident Management follows the Incident Management process described in the [Cisco Remote IT-Infrastructure Management Services](#) description (See [Section 3.2, "Incident Management"](#)) for WAN Circuits.

1.1.2.1 Resolution

The NOC will work with the Customer's carrier(s) to resolve WAN circuit incidents and managed component failures. The NOC will refer incidents to the carrier as needed and escalate the incident with the carrier within the carrier's escalation guidelines, as long as the Incident remains open.

Activities

- Escalate with the Customer's carrier(s), as needed.

Deliverable(s):

- Ticket updated with escalation and resolution notes on the Portal for the Customer to view.
- WAN circuit incidents resolved.

1.2 WAN Reporting

Cisco will deliver WAN-specific reporting to the Customer online via the Portal.

Deliverable(s):

- WAN Availability Report - The WAN Availability report shows the SLA availability for the last six months rolling. WAN SLA availability is calculated by subtracting non-managed incidents from downtime (any time that the circuit was down minus access downtime and non-managed incidents) minus the total available network hours.
- WAN Logical Circuits Availability Report - The WAN Logical Circuits Availability report shows all logical circuits that had available hours during the selected timeframe. It contains the circuit identifier, the connected site(s), monitoring start and stop dates, access downtime, and total available circuit hours.
- Tickets Affecting WAN Availability Report - The Tickets Affecting WAN Availability report shows all the tickets used in the WAN Availability report calculation. The report shows the Ticket ID, down hours associated to the Ticket, resolution, Access Downtime in hours, managed status, date opened and closed, and the associated circuit id(s).
- WAN Interface Performance Reports - The WAN Interface Performance Reports provide graphs of key WAN statistics including:
 - Utilization.
 - Errors.
 - Discards.
 - Non-Unicast traffic.
 - Packets.
 - Octets.
 - Port Speed.
 - FECN/BECN (Frame Relay only).
- WAN Interface Exceptions – The WAN Interface Exceptions report provides high and low exceptions on the range of WAN devices or a specific device.
 - High Utilization Exceptions.
 - Low Utilization Exceptions.
 - Error Exceptions.
- Active Network Map - The Active Map provides a geographic site-level view of the WAN Infrastructure, and color-codes sites and circuits based on if the site or Circuit has an open Ticket.

2.0 LAN Management Services

The objective of Cisco LAN-Management Services is to manage the LAN as a complete system and to maximize the availability of the LAN system. In addition, Cisco LAN-Management Services include reports.

LAN management services are applicable to switching technologies.

2.1 LAN-Availability Management

The objective of LAN-Availability Management is to maximize the availability of the LAN as a system. Using the processes outlined in this Service Description, and in the [Remote IT-Infrastructure Management Services](#) description, the NOC staff will measure and manage the LAN.

Activities:

- Perform ongoing incident monitoring and incident management on LAN-managed components and the LAN connections between managed components.
- Manage problems of LAN-managed components and the LAN connections between managed components.

2.2 LAN Reporting

Cisco will deliver LAN specific reporting to the Customer online via the Portal.

Deliverable(s):

- Utilization.
- Errors.
- Discards.
- Non-Unicast traffic.
- Packets.
- Octets.
- Port Speed.
- High Utilization Exceptions.
- Low Utilization Exceptions.
- Error Exceptions.

3.0 Optional WAN Management Services

Optional WAN Management Services may be purchased separately.

3.1 Backup ISDN Circuit Testing

The backup ISDN Circuit Testing service provides weekly non-intrusive testing for ISDN backup circuits.

Deliverable(s):

- Report of backup circuit test results online on the Portal.

3.2 Backup ISDN Circuit Management

The backup ISDN Circuit Management service provides weekly non-intrusive testing for backup circuits. If an Incident is detected, the NOC will provide incident management for the backup circuit and work the incident until resolved.

Deliverable(s):

- Report of backup circuit test results online on the Portal.
- Ticket on the Portal for the Customer to view with information about the Incident and updates from the NOC as the Ticket is managed.

4.0 WAN Supported-Transport Technologies

WAN Technologies	Supported - SLA Available	Supported - without SLA	Not Supported
Private Line	X		
Frame Relay	X		
ATM	X		
SMDS	X		
ISDN (Nailed Up)	X		
MPLS	X		
Site-to-Site VPN		X	
Business-Class DSL		X	
<i>End-User Remote Access VPN</i>			X
Other Technologies	SOW Required		

Please refer to the Cisco Remote Operations Service Agreement-U.S. Version for more details about the WAN Availability Warranty and ISDN Warranty, referenced in Appendix 2, Sections 2.0 and 3.0.

For more information on change management, please refer to the [Cisco Change-Management Services](#) description.

-END-



Cisco IP Telephony-Management Service

1.0 IP-Telephony Management Services

This document describes Cisco's IP Telephony-Management Services. This service is just one of the service modules (WAN/LAN, IP Telephony Management and Security specialized services) that you can purchase. Please read this document carefully as it contains important information regarding the Services that you have purchased from us.

Capitalized terms are defined in the [Glossary of Terms](#) at the end of this document.

NOTE: When purchasing this service, please ensure that you have also read the [Cisco Remote IT-Infrastructure Management Services](#) description and the [Cisco Change-Management Services](#) description. The Cisco Remote IT-Infrastructure Management Service is a prerequisite for Cisco WAN-Management Services, and the Change Management document outlines how we process Moves, Adds, Changes, Deletions, and Upgrades.

Cisco Remote IT-Infrastructure Management Services are a prerequisite for Cisco IP-Telephony Management Services. Unless otherwise specified in this service description, the NOC will also follow the processes outlined in the [Cisco Remote IT-Infrastructure Management Services](#) description.

The objective of Cisco IP-Telephony Management Services is to manage the converged infrastructure and the call management system as a complete system, as limited by the approved device and managed component list, and to maximize the availability of the voice system to complete calls for end users. In addition, Cisco IP-Telephony Management Services include IP Telephony specific reports.

The following managed components are covered under the IP-Telephony management service:

- Routers.
- Quality of Service.
- Switches.
- Voice Gateways.
- DPAs.
- CallManager Servers.
- Unity Voicemail Servers.

In addition, the following services are included:

1.1 Converged Infrastructure-Connectivity Management

The objective of converged-infrastructure connectivity management is to maximize the availability of the WAN and the PSTN connections required to allow end users to complete telephone calls.

Activities:

- Perform ongoing incident monitoring and incident management of WAN and PSTN circuits.
- Manage problems on WAN and PSTN circuits.

NOTE: This activity includes working with Customer's carrier(s) to resolve circuit issues for managed components. The NOC will refer incidents to the carrier as needed and escalate the incident with the carrier within the carrier's escalation guidelines until the incident is restored.

Deliverable(s):

- Tickets with status and results.
- Restored WAN or PSTN service.

1.2 Quality of Service (QoS) Management

The purpose of Quality of Service management is to ensure high call quality telephone calls for end users.

Activities:

- Configure QoS infrastructure devices in accordance with Cisco's best practices.
- Monitor infrastructure real-time for events that impact voice quality.
- Perform incident and problem management of QoS issues.

Deliverable(s):

- Exception report that identifies infrastructure devices that have experienced QoS-impacting events.
- Tickets updated with status and results.
- Restored Quality of Service.

1.3 Call Management and Voicemail Management (“Phone Support”)

Call management includes the monitoring and management of the CallManager application to ensure that end users can make phone calls across their converged infrastructures. Voicemail management includes the monitoring and management of the Unity voicemail application to ensure that end users can send and receive voicemail messages. The CallManager call-management system and Unity-voicemail system are tightly integrated.

This service includes the management of the CallManager and Unity applications and DOES NOT include the management of hardware telephony devices (IP telephones, analog phones, fax machines, modems, etc.) or IP SoftPhone applications. Cisco will troubleshoot call and voicemail issues to ensure that the applications are working correctly. If the incident is isolated to the IP SoftPhone application or hardware telephony device, Cisco will refer the incident to the appropriate Customer contact or vendor for resolution.

Activities:

- Perform incident monitoring and incident management on the CallManager application, Unity voicemail application and servers that run the applications.
- Manage problems on the CallManager application, Unity voicemail application and servers that run the applications.

Deliverables:

- Tickets updated with status and results.
- Restoration of service to enable end users to place and receive phone calls and voicemail messages.

1.4 Reporting and Portal

Cisco will deliver IP Telephony-specific reporting to the Customer online via the Portal. In-depth follow-up and explanations of each report are available as part of the Stewardship optional service described in the [Cisco Remote IT-Infrastructure Management Services](#) description.

Deliverable(s):

- CallManager and Unity Server Health Reports.
- Communication Interface statistics.
- Server hardware environmentals.
- Operating system parameters.
- Application metrics specific to CallManager and Unity.
- Availability statistics.
- Cisco IPT-enabled routers.

- Communication interface statistics (all interfaces).
- WAN interface high/low utilization exceptions.
- Frame Relay specific statistics (Frame interfaces).
- Cisco Quality of Service (QoS) exception reports on dropped and discarded packets.
- Cisco Gateway devices.
- Communication Interface statistics.
- Cisco IPT-enabled switches.
- Communication interface statistics.
- LAN interface high/low utilization exceptions.

2.0 Customer Responsibilities

To ensure that the NOC can provide services for managed components, Cisco requires Customers to supply information, communications, and connectivity. These requirements are critical to the NOC to provide optimal, and in some cases, any services. In addition to the Customer responsibilities outlined in the [Cisco Remote IT-Infrastructure Management Services](#) description, the Customer is responsible for the items listed below. More detail around each of these items is provided in the Cisco IP-Telephony Technical Summary Document.

2.1 Connectivity

The Customer is responsible for providing one or more management channels, such as a Frame Relay PVC or a dedicated VPN tunnel, to a managed component at a site on the Customer’s network. The size of the management channel can vary depending on the number and type of managed components and the services purchased. In addition, various ports and protocols are needed to deliver Cisco’s full suite of management services. The Customer is responsible for allowing these ports and protocols to be opened in order for Cisco to deliver services.

2.2 Support for Non-Managed Components

The Customer is responsible for installing and maintaining all non-managed components including the IP telephone handsets, analog telephony devices, IP-SoftPhone applications, or any other essential service or device that is a non-managed component within the IP- Telephony infrastructure.

2.3 Support for IP Telephony-Backup Services

The Customer must provide back-up procedures for managed devices that do not have configurations that can be archived remotely. This includes all devices not running CatOS or Cisco IOS. Cisco will assist in the configuration of the backups. The Customer is responsible for ensuring that the backups run successfully.

2.4 Notification of Password Changes

The Customer is responsible for informing Cisco of any intended password changes that affect managed devices, before they take place.

2.5 Support for Unity and Exchange Database

The Customer is responsible for Exchange support if Exchange is located on a separate server.

2.6 Support for Call-Detail Records

Cisco IP-Telephony Management Services do not utilize or process call detail records to provide services. The Customer is responsible for administering and using both the Administrative Reporting Tool (ART) and CDR Analysis and Reporting (CAR) tools. Several authorized Cisco partners can provide software for call-detail record processing, and these packages provide various capabilities for interfacing existing call-detail accounting packages.

2.7 Legacy-Voicemail Systems

The Customer is responsible for providing legacy-voicemail system support either directly or through a third party.

2.8 Unity/Unity Express Auto-Attendant Scripts

The Customer is responsible for maintaining and updating all scripts used for the auto-attendant service provided by the Unity/Unity Express server. The Customer is responsible for creating voice recordings for auto-attendant.

2.9 Anti-Virus Software

The Customer is responsible for installing and maintaining a Cisco TAC approved version of anti-virus software on all applicable IP-Telephony servers.

2.10 WAN Requirements

The Customer must provide a WAN that meets Cisco's best practices standards for QoS in order for Cisco to support QoS management.

2.11 End-User Training

The Customer is responsible for all end-user training on IPC applications such as Personal Assistant, Cisco Conference Connection, etc.

2.12 Cisco Security Agent

Cisco will monitor the up/down status of the Cisco Security Agent (CSA) executable (.EXE) file. The Customer is responsible for CSA management including installing, troubleshooting, "tuning," and upgrading CSA.

3.0 Optional IP-Communication Management Services

Optional IP-Communication Management Services may be purchased separately.

3.1 Complex Redesign of CallManager or Unity Features

The IP-Telephony Management Service is a remote-operational support service. It is assumed that dial plans, configurations, and business-oriented scripting have been previously implemented prior to the commencement of support. Under the service, these existing features will be supported. However, Cisco reserves the right to require separate additional time and material project fees when a significant redesign of these features occurs or addition of new functionality is required. See the [Cisco Change-Management Services](#) document for more information.

3.2 Cisco Personal-Assistant Management Services

[Cisco Remote IT-Infrastructure Management Services](#) and IP-Telephony Management Services are prerequisites for Cisco Personal-Assistant Management Services.

The objective of Cisco Personal Assistant Management Services is to manage the Personal-Assistant server and application to maximize availability and to report on system health.

Cisco will provide management and configuration services related to the Personal-Assistant server and application. This service does not provide user education or training on the use of the Personal Assistant application.

The following are covered under the IP-Telephony management service:

- Personal Assistant server(s) and application.

Activities:

- Perform incident monitoring and incident management on the Personal Assistant server and application.
- Manage problems on the Personal Assistant server and application.

Deliverable(s):

- Tickets updated with status and results.
- Restoration of service to enable end users to use the Personal Assistant application.

3.3 Cisco Conference-Connection Management Services

[Cisco Remote IT-Infrastructure Management Services](#) and IP-Telephony Management Services are prerequisites for Cisco Conference-Connection Management Services.

The objective of Cisco Conference Connection Management Services is to manage the Conference Connection server(s) and application to maximize availability and to report on system health.

Cisco will provide management and configuration services related to the Cisco Conference-Connection server and application. This service does not provide user education or training on the use of the Cisco Conference-Connection application.

The following are covered under the IP-Telephony Management services:

- Conference-Connection server and application.

Activities:

- Perform incident monitoring and incident management on the Cisco Conference-Connection server and application.
- Manage problems on the Cisco Conference-Connection server and application.

Deliverable(s):

- Tickets updated with status and results.
- Restored of service to enable end users to use the Cisco Conference-Connection application.

3.4 IPC Server Monitoring (DHCP, FTP, etc.)

[Cisco Remote IT-Infrastructure Management Services](#) and [Cisco IP-Telephony Management Services](#) are prerequisites for IPC Server Monitoring.

The objective of the IPC-Server Monitoring service is to monitor the health and availability of the server. The solution also monitors the status of Cisco-designated .EXE files. It DOES NOT include incident, problem, or change management on those servers or applications.

Activities:

- Monitor incidents on the designated IPC server and associated application .EXE files.

Deliverable(s):

- Notification of the Customer-designated contact of an event on the monitored server.

For more information on change management, please refer to the [Cisco Change-Management Services](#) description.

-END-



Cisco Security-Management Services

1.0 Security Services

This document describes Cisco's Security-Management Specialized Services. This service is just one of the service modules (WAN/LAN, IP Telephony Management and Security-specialized services) that you can purchase. Please read this document carefully as it contains important information regarding the services that you have purchased from us.

Capitalized terms are defined in the [Glossary of Terms](#) at the end of this document.

NOTE: When purchasing this service, please ensure that you have also read the [Cisco Remote IT-Infrastructure Management Services](#) description and the [Cisco Change-Management Services](#) description. The Cisco Remote IT-Infrastructure Management Service is a prerequisite for Cisco WAN-Management Services, and the Change Management document outlines how we process Moves, Adds, Changes, Deletions, and Upgrades.

Cisco Remote IT-Infrastructure Management Services are a prerequisite for Cisco Security-Management Services. Unless otherwise specified in this service description, the NOC will also follow the processes outlined in the [Cisco Remote IT-Infrastructure Management Services](#) description.

The objective of the Cisco Security-Management Services is to define the specialized processes and principles that are designed to address infrastructure security related issues. The application of these specializations is dependent on the technology features and capabilities. Specializations can be selectively applied to specific technologies of their infrastructure for maximum benefit.

Security specializations can only be delivered by using appropriate security technologies. Firewalls and technologies that provide firewall-like capabilities can be used to fulfill the deliverables of Access-Control Management and Threat-Management Service specializations. However, only specialized intrusion detection systems can be used to fulfill the deliverables of Intrusion Monitoring.

Technologies covered by Access-Control Management and Threat Management

- Firewalls.
- Firewall feature sets on routers.
- Integrated firewall service modules.
- Routers with access-control capabilities.

Technologies covered by Intrusion Monitoring

- Intrusion-detection features on firewalls.
- Intrusion-detection sensor appliances.
- Intrusion-detection, sensor-integrated service modules

2.0 Access-Control Management

The Access-Control Management Security Specialization introduces risk management principles into key processes of Cisco Remote IT-Infrastructure Management Services and is only applied where infrastructure devices are designed to provide infrastructure access controlling capabilities.

2.1 Access Policy Troubleshooting

Following an indication or identification of a network access policy issue via Incident management and/or Problem management processes, Cisco engineers will work to isolate the cause of the policy issue and develop a plan to overcome it for the entitled devices.

Activities:

- Receive access policy troubleshooting request and tracking in Cisco ticketing system.
- Perform analysis to understand the access policy issue and isolate the affected policy statement(s).
- Develop an approach to solve issue without introducing new vulnerabilities.

Deliverable(s):

- Communicate risks associated to implementing the defined approach.
- Communicate alternative approaches to minimize risks.
- Resolution of issue with Customer consent.

2.2 Policy Changes

Policy changes are change requests handled through the Change Management process of the Cisco Remote IT-Infrastructure Management Services that require modifications of the security state of defined technology protections.

Activities:

- Receive change management request via the Change Management process.
- Analyze to identify potential exposures introduced by the change.
- Develop an approach to minimize vulnerabilities.

Deliverable(s):

- Communicate risks associated with implementing the defined approach.
- Communicate alternative approaches to minimize risks.
- Implementation of desired policy change with Customer consent.

2.3 Access-Control Policy Analysis/Recommendations

An annual review of the technological representations of policy will be scheduled and reviewed for each entitled infrastructure device. This review is designed to identify opportunities to increase efficiency, reduce unessential exposures, and determine the effectiveness of policy statements. Following the review, the Cisco NOC Security Engineers will develop recommendations to resolve any identified issues.

Activities:

- Analyze implemented policy configurations and technological constraints.
- Analyze unused permissions.
- Develop recommendations to optimize policy configurations.

Deliverable(s):

- Recommendations to improve effectiveness of implemented policies and tighten overall security posture.

2.4 Data Management

Access-control devices generate large quantities of data that is required for incident analysis, troubleshooting, and issue resolution. Cisco NOC requires the procurement of specialized equipment to capture, queue, and persist data to facilitate these key functions. This equipment is referred to as a “log host” and must be procured from Cisco to deliver the Access-Control Management Security Specialization.

Activities:

- Administer log host as described in the [Cisco Remote IT-Infrastructure Management Services](#) description.

- Maintain the communications link between Access Control technologies and the log host.
- Maintain the storage capacity required to provide a minimum of 72 hours of analysis data.
- Configure the log host to interoperate with local data-backup routines, upon request – performed by Cisco NOC security engineers.

Deliverable(s):

- All deliverables resulting from delivery of [Cisco Remote IT-Infrastructure Management Services](#) description for the log host.

3.0 Intrusion Monitoring

The Intrusion-Monitoring Security Specialization provides a capability to apply 24x7 monitoring and analysis of events that indicate a potential security incident. This service specialization can only be applied to specialized security-event detection and alerting technologies that are entitled to the Cisco Remote IT-Infrastructure Management Services.

3.1 Security-Event Receipt

A security event can originate from either a supported technology that is designed to automatically generate an alert or be manually reported from any module of the Cisco Remote IT-Infrastructure Management Services that is delivered against any infrastructure device. All reported security events result in security-event tickets that persist through several analysis phases until resolved.

Activities:

- Correlate events to consolidate related events.
- Correlate events to consolidate multiple events by source device.
- Generate a security event ticket within the Cisco NOC ticketing system.

Deliverable(s):

- Ticket generated and accessible via the Internet web portal
- Perform E-notification on security event ticket generation, if requested by Customer

3.2 Security-Event Analysis

Upon generation of a security event ticket, Cisco NOC will begin the analysis process to determine the nature of the security event.

Activities:

- Collect related data from source system and other relevant systems entitled to the Cisco Remote IT-Infrastructure Management Service.

- Determine the actual source and nature of the event.
- Log analysis findings into the security event ticket.

Deliverable(s):

- Ticket updated with analysis result.
- Ticket accessible via the Internet Web portal.

3.3 Security-Event Categorization

Upon completion of the analysis process, the Cisco NOC will apply a proprietary rule-based technique to categorize the event. The possible categories that can be assigned are: benign activity, misuse, worm, virus, reconnaissance, probable attack, and successful attack.

Activities:

- Execute categorization technique using the data collected from security event report, the data collected and analyzed, and the results of the analysis.
- Assign the resulting event category.

Deliverable(s):

- Ticket updated with assigned category.
- Ticket accessible via the Internet Web portal
- Perform E-notification of security event ticket by assigned category, if requested by Customer.
- Security Event Rate of Occurrence Report accessible via the Internet Web portal.

3.4 Impact Rating

Once the event is categorized, the Cisco NOC will apply a proprietary technique to define a quantitative impact rating for the event. This process is designed to identify the relative technological risk and is calculated by considering the relative severity of the event category, the exposure state of the targeted asset, and the technology countermeasure in place to mitigate the threat.

Activities:

- Rate the event severity.
- Rate the exposure state of the targeted system / asset.
- Execute the impact rating process for the result.

Deliverable(s):

- Ticket updated with impact rating.
- Impact rating accessible via the Internet Web portal.

- Top 10 Sources of Attack Report accessible via the Internet Web portal.
- Top 10 Attacked Hosts Report accessible via the Internet Web portal.
- Top 10 Types of Attack Report accessible via the Internet Web portal.

3.5 Signature Updates

Technologies designed to detect and alert when potential security events occur require routine administration of attack signatures. The timeliness of vendor signature releases is unpredictable as it is driven by the current state of the threat environment as well as industry threat trends. The Cisco NOC includes the testing and deployment of signature updates to the specialized technologies.

Activities:

- Receive signature update.
- Analyze signature update deviation from previous version.
- Test signature update to identify deployment risks.
- Generate change-management request.
- Coordinate with defined Change Management processes.

Deliverable(s):

- Generate a Change Management request ticket accessible via the Internet Web portal.
- E-Notification of signature update status, if requested by Customer.

3.6 Signature Tuning

When conducting security event analysis, the Cisco NOC will routinely assess and determine event-detection rate of accuracy for certain security event-detection signatures. In the event a signature proves to have a low rate of accuracy, the Cisco NOC will recommend modifications to minimize false alarms, erroneous reporting, and analysis of false events.

Activities:

- Analyze benign event statistics.
- Determine high rate of error/low rate of accuracy signatures.
- Recommend signature tuning activities.
- Coordinate tuning within the defined Change Management process.

Deliverable(s):

- Generate a Change Management request ticket accessible via the Internet Web portal.
- E-Notification of tuning status with Customer consent.

4.0 Threat Management

Access Control Management and Intrusion Monitoring are prerequisites for Threat Management services for a zone of protection. Zones of protection can be defined as logical segments of the infrastructure such as Internet, Extranet, and segmented VLAN connections.

4.1 Response-Policy Administration

At the beginning of Threat Management service delivery, the Cisco NOC will work with the Customer to determine business and threat concerns for the protected zone. These concerns will be transferred to technological configurations of devices that provide access control enforcement, provide intrusion-monitoring accuracy, and identify a central point to remediate detected events.

Activities:

- Seek understanding of threat concerns.
- Seek understanding of business critical systems within the protected zone.
- Develop active response policy for implementing access-control, intrusion-monitoring, and threat-management systems.

Deliverable(s):

- Implemented response configurations on applicable systems covered by access control management, intrusion monitoring, and/or threat management services.

4.2 Response Planning

Following the detection of a confirmed event by the Intrusion Monitoring processes, the Cisco NOC will execute a defined-response action plan. The response action plan is defined in collaboration with the Customer and is a function of the technological capabilities of the eligible devices and the business requirements of the Customer. Once defined, the response action plan will continue to exist and function to guard against anticipated future events of this type.

Activities:

- Define response action plans.
- Ensure automatic response methods are functional.
- Consult response action plans.

Deliverable(s):

- Response action plans as implemented on automatic response technologies

4.3 Remediation

Remediation is the resolution of a detected attack that triggers intrusion-monitoring events. This is only applicable if the event can possibly be mitigated in near-real time, and the response action plan is defined and implemented in the automatic response configuration of select technologies.

Activities:

- Confirm automatic remediation execution.

Deliverable(s):

- Publication of tickets containing remediation actions via the Internet Web portal.

4.4 Recommendations

In the event remediation does not occur and the response action plan dictates changes to devices not covered by the [Cisco Remote IT-Infrastructure Management Services](#) description, the Cisco NOC will make real-time recommendations following the response planning process.

Activities:

- Determine the need to execute changes on devices not covered by the [Cisco Remote IT-Infrastructure Management Services](#) description.
- Publish recommendations as ticket actions and identify resource on which to execute the plans.

Deliverable(s):

- Publication of recommendations as ticket actions accessible via the Internet portal.
- E-Notification of recommendations, if requested by Customer.

5.0 Optional Security Services

The following services can be purchased separately:

5.1 Security-Posture Assessment

Security-posture assessment consists of executing vulnerability-scanning technologies designed to identify system and control weaknesses for protected zone.

Activities:

- Scan protected zone Internet Protocol address ranges to determine systems/addresses in use.
- Analyze the network profile and presence for each system/active address.

- Determine vulnerabilities associated with the profile and network presence for each system/address in use.

Deliverable(s):

- Vulnerability report for protected zone systems/active IP addresses.

5.2 High-Availability Management for Access Control

High-availability management services are designed to ensure the highest state of access control fail-over readiness. As the policies and configurations of the primary access control technologies are managed, the Cisco NOC will ensure the changes are reflected on applicable standby resources designed to activate and/or minimize the risks of technological failure of the primary device.

Activities:

- Confirm synchronization between primary and secondary devices.
- Validate fail-over configurations and synchronization process.
- Perform incident monitoring and management for fail-over configuration or system failures.
- Test that fail-over capabilities is available upon Customer request.

Deliverable(s):

- Continual fail-over readiness.
- Reporting of any detected fail-over failures.
- Perform E-notification of any detected fail-over failures, if requested by Customer.

For more information on change management, please refer to the [Cisco Change-Management Services](#) description.

-END-



Cisco Change-Management Services

1.0 Introduction

This document describes Cisco's Change-Management Services and serves as an addendum to the Cisco Remote Operations Services and the specialized services (WAN/LAN, IP Telephony and Security) descriptions.

This document outlines and lists in greater detail the processes governing Cisco Recommended Changes and Customer Requested Changes (See Cisco Remote IT-Infrastructure Management Services description, [Section 3.4, "Change Management."](#))

This document also outlines the time frames and framework governing changes. This framework allows Cisco to perform changes in a timely manner, and ensures the appropriate resources are available to complete the work.

Capitalized terms are defined in the [Glossary of Terms](#) at the end of this document.

Please see section 3.0 for pricing and scheduling details.

2.0 Types of Changes

There are two types of changes: Cisco recommended changes and customer requested changes. Both changes are summarized in the tables below.

Cisco Recommended Changes		
Changes Required To:	Section	Resulting in:
Resolve an incident (Section 2.1.1)	2.1.1	Logical or physical change
Respond to a critical vulnerability (Section (2.1.2))	2.1.2	Logical change
Apply a signature update to a security managed component	2.1.3	Logical change
Address a problem	2.1.4	Logical or physical change

Customer Requested Changes			
Changes Required To:	Section	Category	Change description
Add, Delete or Change physical component on existing managed component	2.2.1	Change	Physical change
Change existing logical functionality (Upgrades)	2.2.2	Change	Logical Change; logical voice MACs
Physically move managed component	2.2.3	Move	Physical move
Add managed components	2.2.4	Add	Physical add
Addition of new functionality	2.2.5	Add	Logical add
Remove managed components	2.2.6	Delete	Physical delete

2.1 Cisco Recommended Changes

Cisco recommended changes originate from Cisco ROS. Before executing a Cisco recommended change, Cisco ROS will evaluate the change and make a recommendation to the customer that includes the criticality and timeframe for implementation. Cisco ROS will not execute a change until the customer has authorized or pre-authorized the change to be made.

2.1.1 Changes required to resolve an incident

During the course of the incident management (See Cisco Remote IT-Infrastructure Management Services description, [Section 3.2, "Incident Management"](#)), Cisco ROS will be required to make changes to managed components in order 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 Cisco ROS in accordance with the customer's change management policy. Please see section 3.0 for pricing and scheduling details.

2.1.2 Changes to respond to a critical vulnerability

Cisco recognizes that certain critical vulnerabilities have the capability to degrade customers' systems and severely limit services. As new vulnerabilities are released, Cisco ROS will evaluate the severity and potential impact to customers' managed components. If the vulnerability is judged by Cisco ROS to be critical with respect to the customer's safeguards, and the customer is impacted by the vulnerability, Cisco ROS will make changes to correct the issue. Changes will be executed according to the priorities outlined above.

Changes to address critical vulnerabilities will be performed at the earliest possible time, in coordination with the customer. Please see section 3.0 for pricing and scheduling details.

2.1.3 Applying signature updates to managed security technologies

Customers who purchase security specialized services from Cisco ROS are entitled to security signature updates to their managed components. The Cisco ROS security team will work with the customer to define the appropriate process for these updates, and apply them as appropriate to the customer's managed components.

Changes to address critical vulnerabilities will be performed at the earliest possible time, in coordination with the customer. Please see section 3.0 for pricing and scheduling details.

2.1.4 Changes to address a problem

During the course of the problem management process (See Cisco Remote IT-Infrastructure Management Services description, [Section 3.3, "Problem Management"](#)), Cisco ROS will be required to make changes to managed components in order to resolve problems. These changes are usually logical changes to managed component configurations for troubleshooting and implementing workarounds, and can also include working with vendors.

Changes required to resolve problems are implemented as needed by Cisco ROS in accordance with the customer's change management policy. Please see section 3.0 for pricing and scheduling details.

2.2 Customer Requested Changes

Customer requested changes are identified and submitted by customers on the portal. All customer requested changes are subject to charges above and beyond the management fees for providing Cisco Remote Operations Services.

Cisco ROS researches the impact of customer requested changes and will discuss the implications of a requested change with the customer. If Cisco ROS believes the change requires additional information, planning, diligence, or testing, Cisco ROS reserves the right to refuse customer requested changes if we believe that the change will adversely affect the operations of the managed components.

Please see section 3.0 for pricing and scheduling details.

2.2.1 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 Cisco ROS database as -needed.

The configuration process of a physical change includes logical configuration changes to ensure that the managed component will function.

Physical changes may be expedited for a fee. Please see section 3.0 for pricing and scheduling details.

2.2.2 Change – Logical

A logical change includes changes to software on 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 exceed four hours of work. If a change is determined to be complex, it will be treated as a project.

Complex logical changes 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.

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

2.2.3 Move – Physical

A physical move is a change required to physically move a managed component from one location to another.

For a physical move, the customer or a partner is responsible for physically moving the component from one location to the next. The Cisco ROS service is responsible for making the necessary changes in the Cisco ROS database and the configuration of the managed component to ensure that management can continue in the new location. Cisco ROS will work with the customer or partner to coordinate the Physical Move.

Physical moves may be expedited for a fee. Please see section 3.0 for pricing and scheduling details.

2.2.4 Add – Physical

A physical add is the addition of new components to be managed under the Cisco ROS. The activities undertaken by the Cisco ROS for this type of change are the same as described in the Remote Management Activation section (See Cisco Remote IT-Infrastructure Management Services description, [Section 2.0, "Remote Management Activation."](#))

The data-gathering process involves verification and loading of all managed component information in the Cisco ROS 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.

Customers may self-install the physical equipment that Cisco ROS will manage as managed components. In this case Cisco ROS will charge a reduced fee for configuration verification, support, and database entry.

Physical adds may be expedited for a fee. Please see section 3.0 for pricing and scheduling details.

Logical adds require an additional fee. Cisco ROS will scope each project and work with the customer to approve the work to be done.

Most logical adds may be expedited for a fee. Please see section 3.0 for pricing and scheduling details.

2.2.5 Add – Logical

Logical adds include installation of new software on 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 that will be 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 (See Section 4.0, "Logical Change Examples").
- Significant planning is required before implementation.
- Requested work is comprised of ten or more devices.

2.2.6 Delete – Physical

Physical deletes refer to removing managed components from Cisco ROS. Cisco ROS further classifies these changes as simple and complex.

A simple delete involves removing the managed component from the Cisco ROS database so that it is no longer a managed component. The device may or may not still exist in the customer's network.

A complex deletion requires a Cisco ROS engineer to make modifications to the customer's network infrastructure to allow the device to be removed. This could include actions such as transferring functionality to another managed component, modifying routing, etc.

Physical deletes may be expedited for a fee. Please see section 3.0 for pricing and scheduling details.

3.0 Pricing and Scheduling

Cisco Recommended Changes

Category	Type	Turnaround Time	Standard Fees	Notes	Expedite Fees
Change	Change - Logical	Cisco ROS Determined	\$0	Performed as part of management fees	\$1000 + Time and Materials/ per device ¹
	Change - Physical	Cisco ROS Determined	\$0	Performed as part of management fees	

Customer Requested Changes

Category	Type	Turnaround Time	Standard Fees	Notes	Expedite Fees
Change	Logical (Section 2.2.2)	72 Hours*	\$0	Please see section 2.2.2 for details about logical changes	\$150/ per request ¹
	Physical (Section 2.2.1)	7 Days*	\$300		\$1000 + Time and Materials/ per device ¹
Move	Physical (Section 2.2.3)	14 Days*	\$300		
Add	Physical (Section 2.2.4)	14 Days*	\$300		
	Physical -customer self installation (Section 2.2.4)	7 Days*	\$150		
	Logical (Section 2.2.5)	14 Days*	\$300		
Delete	Physical - Simple (Section 2.2.6)	7 Days*	\$0		

Customer Requested Changes

Category	Type	Turnaround Time	Standard Fees	Notes	Expedite Fees
	Physical - Complex (Section 2.2.6)	7 Days*	\$300		
Project	Changes greater than four hours of work	See Note**	Cisco ROS Professional Services: \$200 per hour with 2 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 ROS 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 partner prior to Cisco ROS taking the equipment under management.

4.0 Logical Change Examples

Project Examples

To provide additional clarity and examples of projects that would exceed the four hour requirement of logical changes, we have provided a small list of representative projects. This is not a comprehensive list, but should serve as examples of change requests that are large enough to qualify as projects due to the increased amount of planning, design, and work associated with them.

Example #1 – Proactive IP Telephony PRI Servicing

Customer X has two PRI lines, one servicing long-distance and one servicing local calls. For redundancy, Customer X wants each PRI to be able to process the other's call should the other fail. To meet this request, Cisco ROS must plan and configure the redundancy policy, possibly work with the telecommunications service provider to change configurations on the PRIs, and adjust the dial-plans accordingly. In all, the work (including planning) greatly exceeds four hours.

Example #2 – Changing Routing Protocols

Customer Y is using RIP-2 as a routing protocol on their 20 site network. They decide they would like to use OSPF and request that OSPF be deployed across their network to replace RIP-2. Since this would require design work, planning the actual cut, and the execution itself, the work greatly exceeds four hours.

Example #3 – Extension Mobility

Customer Z has a location with 30 IP Telephony users who constantly travel between corporate locations. In order to facilitate a seamless office, the customer requests that these 30 users and their phones be configured to use Extension Mobility. Because the planning, installation, and implementation of this software is extensive, the work exceeds four hours and must be quoted as a project.

Example #4 – Unity Call Handlers

Customer X requests that five of their executives have their Unity voicemail boxes configured with Call Handlers so that calls can be screened, and callers are given the option to have the call forwarded to the intended recipient's cell phone. Because the planning, installation, and implementation of this

functionality is extensive, the work exceeds four hours and must be quoted as a project.

Example #5 – Phone Replacement

Customer Y has a site with twenty-five (25) Cisco 7905 IP phones; they are replacing all of them with Cisco 7960 IP phones. Configuration is required in the CallManager to complete this. Because the scale and implementation of this functionality is extensive, the work exceeds four hours and must be quoted as a project.

Example #6 - Convert Firewall Rule Set

Customer Y has a firewall and would like Cisco ROS to take one of their existing firewall rule sets and convert it from one technology (i.e. Checkpoint) to another technology (i.e., Cisco PIX). Because the level of effort involved with understanding the existing rule set for one firewall technology and converting it to another technology will be extensive, the work will normally exceed four hours and is treated as a project.

Non-Project (Simple Logical) Examples

- Changing an entry in a dial plan
- Access Policy update
- Static route change
- Adding a phone and/or voice mailbox to a managed IPT server



Glossary of Terms

The terms identified below define the terms set forth in the Cisco Remote Operations Services Agreement-U.S. Version and the Services Descriptions.

Access Downtime means time periods where the Cisco NOC is unable to perform Incident-Management processes because the Cisco NOC or vendor dispatched by the Cisco NOC is unable to access the site or managed component.

Active Telephone Count means any active telephone number or extension registered with a supported CallManager. These can be Cisco-approved IP Phones, modems, analog phones or FAX machines connected through gateways, registered wireless IP Phones, or soft phones. In general, each counted phone is associated with a MAC address.

Agreement means the Cisco Remote Services Agreement and all Appendices thereto including, without limitation, Appendix 1-Glossary of Terms, Appendix 2-Limited Warranty and Disclaimer for Remote Operations Services, Appendix 3-Letter of Agency, and the Service Descriptions.

Analog Telephony Devices means devices such as fax machines, modems, and analog phones connected to FXS or gateway ports and that require call processing by a managed CallManager.

Auto Close means an automated action, performed by the management tools, where a specified ticket is closed after a set period of time without any further action (See "Ticket").

Carrier means a provider of data transport services.

Change Management Process means the process used by the NOC to receive, authorize, execute, and communicate changes to managed components, as described in Section 3.4 of the [Cisco Remote IT-Infrastructure Management Services](#) description.

Cisco means Cisco Systems, Inc., a California corporation having its principal place of business at 170 West Tasman Drive, San Jose, California 95134.

Cisco DPA for Non-Unity Voicemail means a device required to interface a legacy voicemail system with CallManagers.

Confidential Information means proprietary and confidential information received by Cisco or Customer in connection with the Agreement and their relationship. Such Confidential Information may include, but is not limited to, trade secrets, know how, inventions, techniques, processes, programs, schematics, software source documents, data,

Customer lists, financial information, and sales and marketing plans or information which the receiving party knows or has reason to know is confidential, proprietary or trade secret information of the disclosing party.

CRD means Customer Request Date.

CSO means a written/sealed or electronic order from Customer to Cisco for the Services to be provided by Cisco under this Agreement.

Customer means the entity purchasing Services for its own internal use either directly or through an Authorized Channel.

DBU means dial back up.

Downtime means any time a managed component is not available to perform normal services, according to the Cisco ROS incident monitoring tools.

Due Date means the day that payment for both recurring and non-recurring Services is due, which is within thirty (30) days of receipt of the invoice by Customer.

E-notification means the act of sending notification of incidents and the status of tickets by electronic means.

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, unless the cancellation was due to circumstances beyond their control.

High Risk Activities means on-line control equipment in environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, direct life support machines or weapons systems, in which the failure of the products or services could lead directly to death, personal injury, or severe physical or environmental damage.

IOS means Internet Operating System.

IP Communications (IPC) means the functionality of providing traditional voice services, to include but not limited to, phones calls, convergence calls, or voicemail services, over an IP enabled network.

IP Communications Applications means applications such as CallManager, Unity voicemail, Conference Connection, Personal Assistant, and IP Call Center that enable Cisco to provide IP voice-communications solutions.

IP Soft Phone means an application that runs on a desktop, enables telephony functionality, and requires call processing by a managed CallManager.

IP Telephones means physical telephones that connect to the infrastructure through Ethernet and require call processing by a managed CallManager.

IPT CallManager Servers means servers whose software application controls the telephony functions of a site that they are connected to. The devices may be stand-alone servers or modules in a multi-function chassis.

IPT LAN Device (switches) means LAN or router switch modules with Ethernet ports that can be reached via a remote-management channel and supports AVVID voice or video over IP functions.

IP Telephony Management Service means a suite of remote services that allow for the management, incident detection, incident resolution, and configuration of approved IP Telephony devices at an IPT-managed site. This list of devices includes, but is not limited to means routers, switches, voice gateways, and designated Cisco IP-Telephony servers and their applications.

IPT Toll Bypass Device (routers) means a router or router-like device connected to an Ethernet port at a managed IPT site that provides for voice-over-IP connections across a WAN. The WAN transport could be by ATM, Frame Relay, Private Line or Packet over Sonet. The Toll Bypass Device may be a stand-alone device, or a WAN access module in a switch or multifunction chassis.

IPT Voice Gateway (Voice Gateway) means a device connected to an Ethernet port at a managed IPT Site that provides IP-based access to digital or analog trunks on the PSTN network under the control of the AVVID CallManager. The Voice Gateway may be a stand-alone device, a PSTN access module in a multifunction chassis, or a PSTN module in an IPT LAN switch.

Incident means any event that is not part of the standard operation of a service and that causes or may cause an interruption to, or reduction in, the quality of that service.

IT means Information Technology.

Layer 3 means the third layer of the OSI model, also referred to as the "network layer."

Letter of Agency means a letter which authorizes Cisco to act as the Customer's agent for purposes of ordering, facilitating, tracking and/or providing services with carriers, maintenance contract providers, and other general-service providers.

Logical Add means the addition of software components in a managed application, such as CallManager, PIX, CSIDS or screening router. An example of this would be a new telephone/user added to a CallManager or loading a new signature pack on the CSIDS.

Logical Change means the modification of software components in a managed application, such as CallManager or Firewall. An example of this would be the addition of a firewall rule in a Firewall.

MACDU means Moves, Adds, Changes, Deletions and Updates.

Managed Component means an element for which remote IT-infrastructure management services are provided by Cisco.

Managed Incident means an incident for which the NOC provides resolution services.

Managed IPT Link Interface means any interface on a managed IPT device that is connected to an interface on another managed IPT device or a managed device under any other Cisco service offering.

Managed IPT Port Interface means port interfaces for devices, such as servers, that are connected to Managed IPT Devices.

Managed IPT Site means at least one IP telephone or Soft IP phone application that is associated with two or more redundant CallManager servers either at the managed IPT site or at another managed site connected via a Cisco-managed WAN. Each site typically will have at least one analog or digital voice gateway to the Public Switched Telephone Network (PSTN), at least one LAN switch with Ethernet ports, and at least one WAN router function with or without IP Toll Bypass capability. An IPT site may be a single location or a campus environment provided that all of the connected devices and phones are connected by LAN links at 100 Megabits per second or higher. If a phone or device reaches a call manager or gateway through a router or over a WAN connection, then that phone or device is deemed to be at a different site.

Move means any activity where a managed component is physically relocated to a new location. When moves occur, Cisco must update records so that vendor dispatches are directed to the correct location.

Activity that relocates managed components inside the same physical address are not considered moves if the managed components can be placed in their new location, powered on, and resume normal functionality without the interaction of Cisco ROS. These activities are considered scheduled maintenance.

Network means a set of interconnected and interworking Cisco supported hardware and software that is implemented, operated, and supported by Customer from a single network operations center (NOC).

Network Availability means the percentage of time that the Network is available to perform normal services, according to the Cisco ROS incident monitoring tools.

Network Component means a device or link that makes up part of a network.

NOC means the Cisco Network Operations Center, the organization that performs management duties on Customer networks.

Non-Managed Component means any element for which management services is not provided by Cisco.

Non-Managed Incident means an incident for which the NOC does not provide resolution services.

Non-Managed IPT Components means any components not specified as managed components, including but not limited to Customer-premise wiring, cabling, intermediate distribution frames (IDF), IP telephones, and analog telephony devices.

Non-Managed IPT Interface means an interface on a managed IPT device that is not a managed IPT link interface or managed IPT port interface. These are connected to non-managed devices such as hubs, printers, PCs or IP telephones. IP telephones and Soft IP phones may be connected to any Ethernet IPT port interface on a managed IPT LAN device.

OSI means the Open System Interconnection Reference Model.

Partner means the business that sold Cisco management to the Customer.

Physical Add means the addition of new hardware at a managed location, such as a new switch, firewall, log host, IDS or router.

Physical Change means the modification of a managed device due to the installation of new hardware, such as a new network module.

Physical Delete means the removal of a managed device from active management/polling.

The Portal means the online Web user interface supplied for Customers and partners to receive and submit information to and from the NOC.

Problem means the underlying cause of one or more incidents.

Product means both Cisco Hardware and/or Software.

PSTN means Public Switched Telephone Network.

PVC means Private Virtual Circuit.

Service Description means Cisco will provide the Services and perform the Cisco responsibilities described in the standard Cisco Service Description located at http://www.netsolve.com/partners/protected/partner_sd_page/index.html (or such other location of which Cisco may notify Customer from time to time).

Service Request means any request for service, as related to the Cisco service agreement, made by the Customer or partner, in electronic format (submitted via the Portal).

Service Term means the term for the Services as stated on the CSO.

Services means Cisco Remote Operations Services.

SLA means Service Level Agreement.

Ticket means the tracking mechanism for incidents and service requests within the NOC. The NOC activities are detailed within the ticket that contains the complete history of record for an incident or service request.

Turnaround Time means the total duration from the receipt of a change request to the completion of the change.

Unity Servers means servers whose software application provides voicemail services in an IP-Telephony infrastructure. These devices may be stand-alone servers or modules in a multi-function chassis. The Unity Server is supported in 3 different configurations as defined below.

Unity Unified Messaging On-Box Exchange Server means a configuration where the Unity server provides voicemail services and the ability to receive these messages via email. Subscribers can check messages by phone or by email. The email server must be installed on the Unity Server in this configuration, and the email application is only supported if used only for voice mail messages.

Unity Unified Messaging with Existing Exchange Server means a configuration where the Unity system handles voice messages only and stores them on other Exchange servers. Because of the complexity of this environment, it must be reviewed on an individual-case basis and will have additional charges associated with the support based upon the configuration.

Unity Voice Messaging only means a configuration where the Unity server provides voicemail or auto attendant services. The Unity server must be connected to the LAN for administration purposes. Subscribers check messages by phone only.

VLAN means Virtual Local Area Network.

WAN means Wide Area Network.

WAN Circuit means a logical or physical connection from one Customer site to another with transport supplied by a third party-carrier.



Cisco Supported-Device List

Supported-Device List								
Category	Make	Model	Remote IT Infrastructure Management	WAN	IPT	Security		
				WAN Management Specialized Services	IP Telephony Specialized Services	Access Control	Intrusion Monitoring	Threat Management
Routers	Cisco	800	X	X				
		1600R	X	X				
		1700	X	X				
		1800	X	X	X	X		X
		2500	X	X		X		X
		2600	X	X		X		X
		2800	X	X	X	X		X
		3000	X	X		X		X
		3600	X	X		X		X
		3800	X	X	X	X		X
		4000	X	X		X		X
		4500M	X	X		X		X
		4700M	X	X		X		X
		7100	X	X		X		X
		7200	X	X		X		X
	7500	X	X		X		X	
	Nortel/Bay	Access Stack Node	X	X				
		Backbone Node (BCN, BLN)	X	X				
		BayStack AccessNode	X	X				
		Access Node Hub	X	X				
BayStack ARN		X	X					

Supported-Device List								
Category	Make	Model	Remote IT Infrastructure Management	WAN	IPT	Security		
				WAN Management Specialized Services	IP Telephony Specialized Services	Access Control	Intrusion Monitoring	Threat Management
Switches	3Com	OfficeConnect NETBuilder	X	X				
		NETBuilder II	X	X				
		SuperStack II NETBuilder SI	X	X				
	Cisco	Catalyst 19xx	X					
		Catalyst 2820	X					
		Catalyst 29xx	X					
		Catalyst 2950 LRE	X					
		Catalyst 35xx	X		X			
		Catalyst 40xx	X		X			
		Catalyst 2948GL3	X					
		Catalyst 3550	X					
		Catalyst 3560	X					
		Catalyst 4908GL3	X					
		Catalyst 45xx without Supervisor Engine	X					
		Catalyst 5xxx without RSM	X					
		Catalyst 6xxx without MFC	X		X			
		Lightstream 1010 without ARM	X					
		Lightstream 1010 with ARM	X					
		Catalyst 37xxx	X					
		Catalyst 45xx with Supervisor Engine	X					
		Catalyst 49xx	X					
		Catalyst 5xxx with RSM	X		X			
		Catalyst 6xxx with MFC	X					
Catalyst 4840G	X							

Supported-Device List								
Category	Make	Model	Remote IT Infrastructure Management	WAN	IPT	Security		
				WAN Management Specialized Services	IP Telephony Specialized Services	Access Control	Intrusion Monitoring	Threat Management
IP Communications	Cisco	Catalyst 8500 Campus Switch Router	X					
		Catalyst 8500 Multiservice Switch Router	X					
		Cisco Catalyst 4000 Family Access Gateway Module	X		X			
		Cisco Catalyst 4000 Family Inline Power 10/100BaseT Ethernet Switching Module	X		X			
		Cisco Catalyst 6000 Family 24-Port FXS Analog Interface Module	X		X			
		Cisco Catalyst 6000 Family Voice T1/E1 and Services Module	X		X			
	Cisco	CallManager 3.0(4) or later running on a TAC supported server	X		X			
		Unity 3.0 or later running on a TAC supported server	X		X			
		Personal Assistant running on a TAC supported server	X		X			
		Cisco Conference Connection running on a TAC supported server	X		X			
		Cisco AS5300/Voice Gateway	X		X			
		Cisco VG200/Voice Gateway(EOL)	X		X			
		Cisco VG248/POTS Voice Gateway	X		X			

Supported-Device List								
Category	Make	Model	Remote IT Infrastructure Management	WAN	IPT	Security		
				WAN Management Specialized Services	IP Telephony Specialized Services	Access Control	Intrusion Monitoring	Threat Management
		Voice/Fax Network Modules, Cisco 2600/3600 Routers	X		X			
		Digital T1/E1 Packet Voice Trunk Network Module	X		X			
		Catalyst 6000 Family Voice T1/E1 and Services Module	X		X			
		Catalyst 6000 Family Voice Analog FXS Module	X		X			
		Digital Port Adapter Family for the Cisco 7xxx router	X		X			
		Cisco DPA 7630 Voice Mail Gateway	X		X			
Firewall	Checkpoint	FW1				X		X
	Cisco	Firewall Service Modules				X	X	X
PIX 5xx v. 4.x - 6.x		X	X		X	X	X	
Network IDS	Cisco	CSIDS Service Modules					X	X
		CSIDS 42xx v.3.x - 4.x	X	X			X	X