



Service Description: Cisco Managed Services for Enterprise Networks: Route, Switch, and Wireless

Technology Addendum to Cisco Managed Services for Enterprise Common Service Description

This document referred to as a **Technology Addendum** describes the **Cisco Managed Services for Enterprise Networks**.

Related Documents: This document should be read in conjunction with the Cisco Managed Services Common Service Description posted at www.cisco.com/go/servicedescriptions.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. If not already covered in your MSA or equivalent services agreement, this document should be read in conjunction with the Related Documents identified above. In the event of a conflict between this Service Description and your MSA or equivalent services agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller. If you have purchased these Services through a Cisco Authorized Reseller, this document is for informational purposes only; it is not a contract between you and Cisco. The contract, if any, governing the provision of this Service is the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you.

The Service

This Technology Addendum is designed to be read in conjunction with the Cisco Managed Services for Enterprise Common Service Description ("Common Service Description") that provides a baseline understanding of and sets expectations about the Cisco Managed Services, hereinafter referred to as the Service, provided by Cisco. In addition to the activities and deliverables outlined in the Common Service Description, this Technology Addendum outlines the unique activities and deliverables for the Customer's Enterprise Networks that are being managed by Cisco. Both service descriptions should be read in combination to fully understand the scope of the Service being purchased.

Cisco Managed Services for Enterprise Networks and other optional services are intended to supplement a current support agreement for Cisco products, and only available where all the Managed Foundation and Wireless Components in a Customer's network are supported through a minimum of core services such as Cisco's SMARTnet and Software Subscription Services, as applicable. Cisco shall provide the Cisco Managed Services for Enterprise Networks described below as selected and detailed on the purchase order for which Cisco has been paid the appropriate fee.

Cisco shall provide a Quote for the Service setting out the extent of the Service and the term for which Cisco shall provide such Service. Cisco shall receive a purchase order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein.

Two service packages are available:

- Standard Service
- Comprehensive Service

These service packages are described in detail in the Cisco Managed Services Common Service Description. In addition to activities and deliverables in the two service packages, the Customer can also purchase Optional Services as needed to augment the selected package. The table below outlines the activities and deliverables applicable to the Enterprise Network offer as well as Optional Services for the Service.

Activities / Deliverables	Standard Services	Comprehensive Services	Optional Services
Remote Monitoring	X	X	
Quality of Service Ticketing	X	X	
Backups	X	X	
Standard Reports	X	X	
Proactive Problem Management		X	X
Business & Operational Review		X	X
Advanced Operational Reports		X	X
Defined Changes			X
Custom Changes			X

1 Standard Service Package Management Capabilities

The Service provides real-time monitoring and management on subscribed devices under the Standard service package and proactively declares Incident Events for:

- System and/or application availability
- System and/or application performance
- Hardware environmentals
- Operating system availability
- Syslog and traps.

2 Standard Reports

The delivery platform collects and gathers log and event information from the Managed Route, Switch and Wireless Components covered within the Service. This information is compiled and made available via reports available on the Portal. Standard reports available are as follows:

2.1 Top 10 Reports

- **Interface Utilization Error Out monthly** – interfaces listed in descending order based on how many error packets passed through them in an outbound direction.

- **Interface Utilization Error In monthly** – interfaces listed in descending order based on how many error packets passed through them in an inbound direction.
- **Interface Utilization Discard Out monthly** – interfaces listed in descending order based on how many megabytes of traffic has been discarded in an outbound direction.
- **Interface Utilization Discard In monthly** – interfaces listed in descending order based on how many megabytes of traffic has been discarded in an outbound direction.
- **Interface Utilization MEG's Out monthly** – interfaces listed in descending order based on how many megabytes of traffic has passed through them in an outbound direction.
- **Interface Utilization MEG's In monthly** – interfaces listed in descending order based on how many megabytes of traffic has passed through them in an inbound direction.

2.2 Wireless Specific Reports

- Examples include monitoring of various hardware and environmental alarms for all WLCs or APs, up/down status and any associated management messages of all access points. Any AP faults that include upgrades, boot failures, DHCP issues, 802.11 subsystem messages, Inter-Access Point Protocol messages, local authenticator messages, WDS messaged, or mini IOS messages.

2.3 Service Level Objectives (SLO) Reports

- **Mean Time To Notify MTTN** – provides Cisco administrators with data on the length of time for cases to be picked up by the Network operations team and alert the customer of the event. In support of service management initiatives, this data can be used to compile and report on average times and trends for responding to cases of various priorities. The report results are displayed in CSV file format.
- **Mean Time to Begin Analysis MTTBA** – provides Cisco administrators with data on the length of time between a case opening and it being worked by the Network operations team. In support of service management initiatives, this data can be used to compile and report on average times and trends for working cases of various priorities. The report results are displayed in CSV file format.
- **Mean Time To Isolate MTTI** – provides Cisco administrators with data on the length of time for the Network operations team to identify the cause of a case opened in the platform. In support of service management initiatives, this data can be used to compile and report on average times and trends for isolating problems of various priorities. The report results are displayed in CSV file format.
- **Mean Time To Resolve MTTR** – provides Cisco administrators with data on the length of time for case completion. These time attributes provide insight into how long it is taking network management personnel to resolve and close cases of different priorities. In support of service management initiatives, this data can be used to compile and report on average times and trends for responding to and completing cases of various priorities. The report results are displayed in CSV file format.

2.4 Network Level Reports

- **Device Specific Real-Time Reports** – Real-time, device specific reports can graph up to 12 months of device metrics. The data can be exported for analyzing. Examples of data points are CPU utilization, interface statistics, environmental sensor values, memory statistics, and many others.

- **Interface Volume Health** – includes inbound volume (octets), outbound volume (octets), inbound errors, outbound errors, and unknown protocols for each managed interface.
- **Bandwidth Utilization** – provides data on the amount of peak input and output bandwidth and average input and output bandwidth utilized over time. Devices configured for bandwidth graphing will display for selection within the report. This report is useful in comparing actual bandwidth utilized versus bandwidth provisioned at different points in the network. This can identify areas where additional bandwidth is needed to increase service levels, or where bandwidth can be reduced resulting in cost savings.
- **Hardware Inventory Report** – assists administrators in tracking which devices are being backed up. This report will list the device name, IP address, type, model, serial number, and the last successful backup. The Hardware Inventory Report is automatically generated on the first of every month for the previous month's data. The report results are displayed in Microsoft Excel file format.
- **Monthly Device Availability Report** – displays percentage uptime and downtime for the previous two months. The report runs on a scheduled basis on the first of each month and will pull data for the previous two months. For example, a report run on July 1st will pull data for May and June. The report columns 'This Period Avg Down Time %' and 'This Period Avg Uptime %' would represent data for the month of June while columns 'Last Period Avg Down Time %' and 'Last Period Avg Uptime %' would represent data for the month of May. The up/downtime percentage is calculated by Cisco from SNMP system uptime information obtained through polling each device. The report results are displayed in Microsoft Excel file format.
- **Raw Bandwidth Report** – provides the non-aggregated (raw) data for capacity planning and long-term reporting. The report results are displayed in CSV file format.
- **Infrastructure Report** – provides detail on Cisco-specific hardware. This report will list IOS® devices, IOS® version, flash size, RAM size and modules installed for devices managed by Cisco MAP. Only devices that respond to SNMP queries will appear in the report. The report is automatically generated by Cisco MAP on the first of every month for the previous month's data. The report results are displayed in Microsoft Excel file format.
- **Cisco CPU Memory Usage** – Examples include CPU utilization (%), memory pool utilization (%), memory pool free, memory pool largest free
- **Cisco Sensor** – Examples include voltage level, voltage status, fan state, power supply state, temperature level, temperature status
- **Device ICMP** – Examples include ICMP messages received (per second), ICMP messages sent (per second), ping replies received (per second), ping replies sent (per second), pings sent (per second), ping replies received (per second)
- **Device IP Statistics** – Examples include IP packets received (per second), IP packets forwarded (per second), IP out requests (per second), no route (per second), fragmentation failures (per second), reassembly failures (per second)
- **Interface Volume Health** – Examples include inbound volume (octets), outbound volume (octets), inbound errors, outbound errors, unknown protocols
- **Interface Error Discards** – Examples include delivered (inbound) packets, inbound errors, inbound discards, outbound errors, outbound discards
- **Interface Throughput Utilization** – Examples include inbound utilization (percent), outbound utilization (percent), inbound throughput (bps), outbound throughput (bps)

- **Interface LAN Errors** – Examples include inbound abort, inbound CRC, inbound frame, inbound giants, inbound ignored, inbound overrun
- **Interface Multicast** – Examples include inbound unicast packets per second, outbound unicast packets per second, inbound multicast packets per second, outbound multicast packets per second, inbound broadcast packets per second, outbound broadcast packets per second

3 Comprehensive Service Package Advanced Reports

Advanced Reports provide a detailed look at the Service and the Managed Components covered by the Service. Specific reports are itemized below.

- **System Hardware Report** – identifies each hardware component under management and provides the following information: Host name, IP address, device model, serial #, site name, contract expiration date
- **System Infrastructure Report** – identifies IOS image and flash/RAM per managed device and consists of the following information: Site name, Host name, device model, modules, IOS version, IOS subset, IOS image name, Flash (size), RAM
- **Inventory Report** – lists all “active” Customer managed devices, by site name, device type/model, device name, “managed” Customer IP address (if NAT), last good backup (IOS/CAT OS) and lists config archive exceptions. The report consist of the following: site name, site location, device type, device name, IP address Natted, IP Address (not Natted), SNMP community string, activation date (optional); date of last back-up.
- **Global Ticket Report** – identifies the devices in the system that have been impacted by an Incident or Problem and extent of AutoCase activity. The device names indicate the location in production environments. End user selects the system, time frame and generates a report via Web portal.
- **Service Experience Report** – identifies top ten sites that have experienced the most tickets and causes. The report consists of: site names, site location, # of Change tickets, # of Incident tickets, device type, device name, major cause
- **Operations Report** – provides monthly ticket activity, detail by user, suppression, created by, notification and response times

4 Circuit Management

Circuit Management is provided as a standard service activity within the Service. Circuit management includes activities such as coordination of outages with the Customers’ circuit provider (“Carrier”), Customer notification of circuit status and update of tickets for accurate record keeping. Cisco will take steps to bring a circuit back into service while informing the Customer during the entire process.

4.1 Cisco Responsibilities

- Engage the responsible Carrier as necessary to resolve circuit related Incident(s)
- Triage and escalate problems to appropriate customer support staff or responsible Carrier for Incident resolution
 - Subject to Customer entitlements and established Letter of Agency (LOA) between Customer and Cisco

4.2 Customer Responsibilities

- Provide the Cisco Managed Service Network Operations Center with a valid Letter of Agency (LOA) for the responsible Carrier
- Upon escalation to the Customer from Cisco regarding Carrier non-responsiveness, Customer is to own communication and resolution of the reported engagement issues with the Carrier.

5 Customer Requested Change Management

5.1 Defined Changes

Defined Changes are categorized into Small, Medium, and Large activities. A Defined Change is a requested change by the Customer. Defined Changes are not the result of Cisco Incident Management and Problem Management processes. The Customer identifies the needed type of change and submits a change request on the Portal.

Small Defined Changes (Type 1) Not to exceed 30 minutes

- Add configure access point
- VLAN changes
- Port changes

Medium Defined Changes (Type 4) Not to exceed 2 hours

- Individual IOS / CatOS device software upgrades
- Advanced device tuning request
- Circuit changes
- Adding capacity
- Turning up a new circuit

Large Defined Changes (Type 8) Not to exceed 4 hour

- Hardware Upgrades

5.2 Custom Scoped Elective Changes

Custom Scoped Elective Changes are customer requested changes that fall outside Incident and Problem (Standard) changes for restoring service. Custom Scoped Elective changes require a Statement of Work (SOW) agreement between Cisco and customer. See Cisco Managed Services Common Services Description for more details of Custom Scoped Elective Change support. Examples of Custom Scoped Elective Change activities include:

- Apply license updates and changes
- Track & report on software license usage
- Packet capture and traffic analysis
- Network Carrier Coordination - Coordination of Service Engagement
- Patches to Cisco equipment and Cisco applications
- Configuration changes to Cisco software and devices
- QoS to support wireless phones and prioritize mission critical traffic.
- Rogue AP detection and optional blocking.
- Investigation and resolution of authentication issues

- Adjustment of power levels to delineate coverage zones.
- Cisco software upgrades for feature enhancements or security-related purposes
- Connectivity and Path Maintenance:
- Packet capture and traffic analysis
- Device mapping and packet flow monitoring