



MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE 2022

Last Modification Date: 01/29/2022
Exported and Shared on: 01/30/2023

For additional information, visit www.intervision.com

CONTENTS

| | | |
|----------|---|----------|
| 1 | Managed Services Overview | 1 |
| 1.1 | Managed Services - General Service Details | 1 |
| 1.2 | Service Levels | 2 |
| 1.3 | Support..... | 2 |
| 1.4 | Service Activation | 3 |
| 1.5 | Service Delivery - Incident and Device Impact Classification..... | 4 |
| 2 | Service Specifications - Managed Router and Switches..... | 4 |
| 2.1 | Roles and Responsibilities Matrix | 5 |
| 2.2 | Monitoring | 8 |
| 2.3 | Reporting..... | 11 |
| 2.4 | Management Tools..... | 12 |
| 2.5 | Definitions..... | 12 |

1 MANAGED SERVICES OVERVIEW

Managed Network and Monitoring Services provides organizations with the management and monitoring of their network infrastructure, to improve availability, whether the infrastructure is on premises, a third-party datacenter or the cloud. This Service Guide describes Managed Network Services in general (part one) and then describes the specific details of the managed network devices for which this service guide is intended (part two). This document clarifies the scope of the service, service level, roles and responsibilities, and other specifications of the service for customers of this service. This document may get updated from time to time to add additional clarification and details related to this service.

1.1 MANAGED SERVICES - GENERAL SERVICE DETAILS

In Scope

- This Managed Service offers management and monitoring of devices and software according to this Service Guide and the InterVision Work Order to aid in resuming normal operations. Additional requests above and beyond will be based upon time and material expense to the Customer.
- Detection, isolation, diagnosis of each fault and restoration to normal operating conditions, testing and documenting each fault within the InterVision trouble ticket system
- Ownership of resolution of the problem on behalf of the Customer and act as an agent for the Customer under executed letters of agency
- Notify the Customer of the progress of all faults per Customer provided contact process.
- Critical software and firmware updates to resolve issues. Premium service level offers periodic updates as detailed later in this service guide.
- Summary reports delivered via our monitoring portal to help the Customer understand traffic, clients, and application usage
- Assistance with warranty replacement and vendor escalations.
- Premium service level assists with changes to individual devices. Mass additions/deletions or changes (greater than 5) are not covered via the Managed Network Services agreement and will be considered project billable tasks.
- Premium Service level offers bi-annual reviews to identify significant business impacting risks. This review includes identification of software updates, end of life, end of support, device performance, and critical configuration errors.
- Safeguard customer's proprietary information using commercially reasonable efforts to securely access client network through an encrypted tunnel.

Out of Scope

- Hardware or Software installation or non-RMA replacement is not included with network support unless specifically stated below. Professional services may be engaged to assist with installation, upgrade or replacement.
- Software license and subscriptions are not included. Management devices and software provided as part of the Managed Service will be licensed.
- Netflow reporting is available as an additional optional paid service. The device to be covered by Netflow must support the application and have the necessary capabilities to provide reporting appropriate to need.
- Mass configuration changes to covered devices that are required, due to Customer upstream or downstream projects, are not covered as part of the service.
- Coverage for devices not under agreement are ineligible for support of any type.

Customer Requirements

To allow for successful monitoring and management of devices and execution of SLAs, Customer responsibilities include:



MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE 2022

- Providing all network and device information for the InterVision Managed Services team and tools to discover the contracted devices and enable monitoring. This information includes network diagrams, site information, circuit information and Customer Vendors, Letters of Agency, and current software levels.
- Providing computing resources to run InterVision's monitoring and collection tools, and the means for the Collector to contact the InterVision Data Center.
- Performing configuration of devices and network, as necessary, to facilitate monitoring and management of the contracted devices. In the event the customer is unable or does not have the personnel to enable monitoring and management of devices, InterVision's Professional Services can be engaged for assistance at an incremental cost.
- Provide devices access - Remote access to devices must be available for support. The client is responsible for out of band access, along with in-band access.
- Provide a distribution list of Customer contacts to receive alarm triggered notifications and reports
- Supply InterVision team with all the necessary security information including dial-in numbers, access ID's, passwords, SNMP community names necessary for InterVision to perform the Services
- Provide notification contact and escalation lists for use by InterVision during business and non-business hours.
- Provide InterVision team with site contact to facilitate access to equipment and connection terminations, along with out-of-hours access procedures
- Notify InterVision within 72 hours of any changes to the contracted devices via a service/change ticket.
- Execute letters of agency notifying vendors, such as carriers, that InterVision will represent the Customer by isolating and troubleshooting Customer's network problems
- All devices and applications must have vendor support contracts and operate at currently supported vendor versions.
- All devices must be in a supportable state, including current versions of software supported by vendor, with all critical patches applied, in a production capable state with no known failures or functions in order to be covered. Remediation efforts to bring software to current version including patches to make a device production capable will be billable to the customer.

1.2 SERVICE LEVELS

- Monitoring Service provides 24/7 monitoring and customer notification. Notification includes automated alerts as well as notification via service personal to client for critical events. This does not include trouble shooting and device support. Support is available for changes to monitoring settings and assistance with reports.
- Essential Service offers 24/7/365 phone and ticket support. It does not include dispatch for onsite support.
- Essential Service with Dispatch offers 24/7/365 phone and ticket support. It includes dispatch for onsite support^{1,2} where remote support is unable to fulfill eligible service events such as RMA device replacement.
- Premium Service offers 24/7/365 phone and ticket support. It includes dispatch for onsite support^{1,2} where remote support is unable to fulfill eligible service events such as RMA device replacement. Premium Service includes addition services including extended coverage for changes, devices software upgrades, periodic health and performance reviews and life-cycle management.

¹ Applies to devices covered under Managed Network Services in the continental US. International onsite coverage may be added via a custom scope of work.

² Onsite support is at the discretion of InterVision as determined necessary

1.3 SUPPORT

| Service | Monitor Only | Essential | Essential with Dispatch |
|---------|--------------|-----------|-------------------------|
|---------|--------------|-----------|-------------------------|



MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE 2022

| | | | |
|--|-----------------------------------|--------------------------|-----------------------|
| Event notification | Included | Included | Included |
| Phone & Ticket Support 24 hours, 7 days a week | Included for monitoring issues | Included, with SLA | Included, with SLA |
| Onsite Support ** | Not Included | Not Included, No SLA. | Included, with SLA |
| Phone or Onsite Support – Devices Not Covered by InterVision Managed Services | Not Included | Not Included | Not Included |

* All coverage times are based on the local time zone of the supported device.

** Applies to devices covered under Managed Services in the continental US. International onsite coverage may be added via a custom scope of work.

- If an outage or network problem occurs which is determined to be a site related issue InterVision managed service team will document the Incident within its ticketing system. Examples of site related Incidents are: Loss of power to site, damage to premise cabling, accidental disconnection of site cabling or Equipment.
- For Routers, SD-WAN and Firewalls, if an outage or network problem occurs which is determined to be a Broadband Carrier circuit failure, InterVision will, via a Letter of Agency from Customer, contact the relevant Carrier or ISP and report the Incident for resolution. InterVision will then continue to manage the problem and follow up with the Carrier or ISP to ensure service is restored as quickly as possible. This service is included unless specified in the service SKU description as not included.
- If an outage or network problem occurs which is determined to be a failure of CPE, InterVision will diagnose and attempt to resolve the issue remotely. If the outage cannot be resolved remotely, InterVision will escalate to the Customer and/or technician dispatch when needed. Determination of the necessity of on-site services is at the sole discretion of InterVision, If dispatch is requested and cancelled within 48 hours of requested dispatch time, a \$500 cancellation fee will be applied.

1.4 SERVICE ACTIVATION

InterVision employs a structured process to help ensure a smooth transition to Managed Infrastructure and Monitoring services. Our Project Management Office (PMO) owns the process with the Onboarding Engineer (OE), holding the ultimate responsibility and serving as the single point of contact (SPOC).

Steps to activate service

1. Data gathering
1. Customer service manual
2. Order form
 - Monitoring collector/ Support workstation Deployment and Configuration
 - Onboard customer devices
 - Add data from step one into systems
 - Finalize customer onboarding
 - Send any found issues with onboarding for client to review
 - Go Live/ Customer training
 - Perform true up / Project Closeout

Network Infrastructure Evaluation



MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE 2022

For new client environment onboarding not recently set up by InterVision Services, an evaluation is required that will review the environment to ensure it is in a supportable state. Software and Firmware will be reviewed to be current or within one major software version behind current. This evaluation will also review configuration, access control policies for critical risks. Software/Firmware, configuration and access control issues and risks must address to be in a supportable state. Environment updates may be identified as requiring additional project time to address and InterVision reserves the right to modify SLAs or refuse service if Environments are not current and critical risks addressed.

1.5 SERVICE DELIVERY - INCIDENT AND DEVICE IMPACT CLASSIFICATION

The Managed Infrastructure and Monitoring service employs a sophisticated algorithm called the Ticket Enrichment Engine that utilizes the severity of the incident, and the business criticality of the device to determine the appropriate priority levels. Devices such as SD-WAN, routers and firewalls are defaulted to classification as critical devices and are automatically prioritized higher than other devices. Customers can designate other devices as critical, to decrease/increase their prioritization based upon their business impact

| | | |
|-------------|----------------------------------|------------------|
| Severity 1 | No Ticket | |
| Severity 2 | No Ticket | |
| Severity 3 | No Ticket | |
| Severity 4 | Notification Ticket Closed State | |
| Severity 5 | Notification Ticket Closed State | Upgrade Eligible |
| Severity 6 | P3 Ticket | |
| Severity 7 | P3 Ticket | Upgrade Eligible |
| Severity 8 | P2 Ticket | |
| Severity 9 | P2 Ticket | Upgrade Eligible |
| Severity 10 | P1 Ticket | |

Emergency (P1 or P2) services require a phone call to create an incident

2 SERVICE SPECIFICATIONS - MANAGED ROUTER AND SWITCHES

The Managed Network Services for routers and switches covers the availability and performance monitoring, incident response and problem management of the covered devices performing the data packet forwarding



MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE 2022

function for an organization. With Premium service level additional devices maintenance and management capabilities are included as outlined in the responsibility matrix.

This managed service is based upon each instance of a router (physical or virtual) or switch.

- This service is for client-owned equipment.
- Chassis based switches are charged based upon the number of blades within each chassis
- Stacked switches are charged for each individual member switch in the stack.
- As the number of routers or switches increase, fees for this service will increase.
- SD-WAN technology support is not included in standard service coverage. See Managed SD-WAN Service Guide.
- This service is available in multiple service tiers which includes: 1) Essential; 2) Essential with Dispatch; 3) Premium.
 - Essential – this tier offers 24/7 monitoring, incident resources, issue remediation, vendor escalations, RMA assistance and critical patching to resolve issues. .
 - Essential with Dispatch – This tier includes all the capability of the Essential service and adds the ability to provide remote hands service at your site to assist with device replacements and other issues requiring skilled remote hands to resolve.
 - Premium - This tier builds upon the previous tiers and adds change management, health and performance reviews, access control and policy reviews, periodic software and firmware updates and life-cycle notifications.

For a list of supported devices, please contact your account representative.

2.1 ROLES AND RESPONSIBILITIES MATRIX

“X” indicates the responsible party. “*” indicated optional services.

| Managed Switch & Router Responsibility Matrix | Customer | InterVision Essential Service | InterVision Premium Service |
|---|----------|-------------------------------|-----------------------------|
| General | | | |
| Router/Switch information (account. password, location, MAC address,...) | X | | |
| Router/Switch SNMP string | X | | |
| Client escalation information | X | | |
| Vendor support contracts | X | | |
| **Audit the Network environment for configuration issues, vulnerabilities, and risks. | | X | X |
| Installation and Configuration | | | |



MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE 2022

| | | | |
|--|---|---|---|
| Initial design and configuration of router and WAN/LAN | X | | |
| Physical or virtual router/switch install | X | | |
| Implement Quality of Service (QOS) policies | X | | |
| Switch Port Configuration | | | X |
| Monitoring | | | |
| Provide Circuit bandwidth information | X | | |
| Setup monitoring and logging | | X | X |
| Update monitoring thresholds per client requirements | | X | X |
| Manage notification profiles | | X | X |
| Setup dashboard in Managed Network Services portal | | | X |
| Setup monitoring platform reports | | | X |
| Incident and Problem Management | | | |
| Incident management | | X | X |
| Reason For Outage (circuit only) | | X | X |
| Root Cause Analysis | | | X |
| Vendor management (Escalations, RMA,...) | | X | X |
| Troubleshoot down router/switch | | X | X |
| Troubleshoot WAN circuits (for Routers only) | | X | X |
| Troubleshoot high availability features for Routers | | X | X |
| Troubleshoot NAT and port forwarding rules | | | X |



MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE 2022

| | | | |
|--|---|---|---|
| Troubleshoot remote access VPN (IPSEC/SSL) | | | X |
| Patch Management | | | |
| Firmware updates (to resolve issues) | | X | X |
| Critical Security vulnerability patching (as required) | | | X |
| Software updates (bi-annual) | | | X |
| Management | | | |
| Administer device accounts | X | | |
| Administer user access | X | | |
| Performance tuning and management (bi-annual) | X | | X |
| Capacity / Bandwidth analysis (bi-annual) | X | | X |
| Life Cycle Management Notification (bi-annual) | X | | X |
| Change Management | | | |
| Log and store changes information via backup of config (Cisco/ Juniper Devices only) | | X | X |
| HW physical replacement | | * | X |
| HW replacement: configuration migration to new device (if compatible with config backup) | | | X |
| Create new vLANs or Gateways | X | | |
| Modify or extend existing vLAN | | | X |
| Create new remote access VPN (IPSEC/SSL) | | | X |
| Create new site to site VPN | X | | |



MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE 2022

| | | | |
|---|---|--|---|
| Create Access Control Lists (ACL) | X | | |
| Modify or extend existing ACL policy | | | X |
| Create new authentication methods | X | | |
| Create and Implement High Availability Features | X | | |
| Reporting | | | |
| Standard Reports | | | X |
| Custom Operations Reports | X | | |

* Optional services capability that can be provided with incremental fees. These services may be additional managed or professional services.

** This item requires a paid on-boarding fee specifying assessment or audit in the description.

2.2 MONITORING

As available with each device, the Managed Network Services for Routers and Switches will monitor the following:

| Incident Name | Trigger Method | Threshold | Severity |
|--|--|---|----------|
| HSRP State Change | Syslog | 10 events in 5 minutes (indicating fluctuation) | 10 |
| Network Device Not Responding | 5 pings every 2 minutes | 100% packet loss for 5 minutes | 10 |
| Critical Network Device Interface Staying Down | SNMP polled every minute and/or Syslog | Down for 5 minutes | 9 |
| Network Memory Critical | SNMP polled every 3 minutes | 90%+ for 10 minutes | 9 |
| Network Switch Detached From Stack | Syslog | 1 event | 9 |
| Primary Internet Route Failed | Syslog | 1 event | 9 |



MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE 2022

| | | | |
|--|---|---|---|
| Network Device Critical Interface High Utilization | SNMP polled every 1 minute | 95% for 5 minutes | 8 |
| BGP Neighbor Bouncing Repeatedly | SNMP polled every minutes and/or Syslog | Neighbor goes down and up 5 times within 4 hours | 7 |
| BGP Neighbor Staying Down | SNMP polled every minute and/or Syslog | Neighbor goes down and does not come back up for 10 minutes | 7 |
| Duplicate IP Address Detected | Syslog | 1 event | 7 |
| EIGRP Neighbor Staying Down | Syslog | EIGRP Neighbor goes down and does not come back up for 15 minutes | 7 |
| Network CPU Critical | SNMP polled every 3 minutes | 90%+ for 10 minutes | 7 |
| Network Device Critical Interface Flapping | Syslog | Critical Interface Goes Down and Up 3 times in 15 minutes | 7 |
| OSPF Neighbor Staying Down | Syslog | OSPF Neighbor goes down and does not come back up for 5 minutes | 7 |
| VRF Route Limit Exceeded | Syslog | 1 event | 7 |
| Device Config Backups Failing | System | failing for 2 consecutive tries | 6 |
| Network Critical Interface Error Critical | SNMP polled every 1 minute | Critical Interface showing 5% in or out error rate | 6 |
| Network Device Hardware Critical | Syslog | 1 event | 6 |
| Network Device Redundancy Lost | Syslog | 1 event | 6 |
| EIGRP Neighbor Bouncing Repeatedly | Syslog | Neighbor goes down and up 5 times within 4 hours | 5 |



MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE 2022

| | | | |
|-----------------------------------|--------|--|---|
| Network Interface Duplex Mismatch | Syslog | 5 matching events within 5 minutes | 5 |
| OSPF Neighbor Bouncing Repeatedly | Syslog | Neighbor goes down and up 5 times within 4 hours | 5 |

The following device specific monitoring is available:

| Incident Name | Trigger Method | Threshold | Severity |
|--|----------------|---------------------------------------|----------|
| Meraki High Rate of STP Changes Detected | API | Alarm condition exists for 10 minutes | 10 |
| Meraki Device Unable To Find Gateway To Internet | API | Alarm condition exists for 10 minutes | 10 |
| Meraki Backup Cloud Connection In Use | API | Alarm condition exists for 10 minutes | 10 |
| Meraki Uplink IP Conflict | API | Alarm condition exists for 10 minutes | 10 |
| Meraki Switch Not Responding | API | Alarm condition exists for 10 minutes | 10 |
| Meraki MX Appliance Not Responding | API | Alarm condition exists for 10 minutes | 10 |
| Meraki Bad Internet Connection Detected | API | Alarm condition exists for 10 minutes | 8 |
| Meraki Cellular Failover Detected | API | Alarm condition exists for 10 minutes | 8 |
| Meraki Switch Disconnected From Stack | API | Alarm condition exists for 10 minutes | 8 |
| Meraki WAN Uplink Down | API | Alarm condition exists for 10 minutes | 8 |
| Meraki Access Point Not Responding | API | Alarm condition exists for 10 minutes | 6 |



MANAGED ROUTERS AND SWITCHES - SERVICE GUIDE 2022

| | | | |
|--|-----|---------------------------------------|---|
| Meraki DNS Misconfigured | API | Alarm condition exists for 10 minutes | 6 |
| Meraki Device Outdated Configuration | API | Alarm condition exists for 10 minutes | 6 |
| Meraki Poor Connectivity To Meraki Cloud | API | Alarm condition exists for 10 minutes | 6 |
| Meraki Port Cable Error Detected | API | Alarm condition exists for 10 minutes | 6 |
| Meraki Port VLAN Mismatch | API | Alarm condition exists for 10 minutes | 6 |
| Meraki Site to Site VPN Down | API | Alarm condition exists for 10 minutes | 6 |

Refer to the service delivery section for description of severity levels and mapping to operations center priority levels. (ex. Severity 10 is our highest severity and maps to our Priority 1 service level.)

- Monitoring routing protocol peers is optional and not configured by default.
- Monitor the routing protocol is only over a reliable network.

Reliability and Monitoring Disclaimer

If a monitored customer network becomes unreliable and falls in the category of fixed wireless or Internet VPN, Hosted Cafe' has the right to discontinue monitoring of the routing protocol peers until such time the network is deemed reliable again.

- If a backup link is present on a router and is considered an “unreliable network” and routing protocol monitoring of the primary circuit is required and uses BGP then;
1) the BGP peer must be the interface IP of the primary circuit, and 2) the backup circuit cannot use BGP and must use EIGRP or OSPF.

Reliable Definition – A reliable network is one that is backed by carrier SLA's that include at least five 9's of uptime and less than .5% of packet loss, and less than 70ms of latency across the network. These are typically private networks that consist of MPLS, Ethernet, or Private Lines. Any type of cable modem, DSL, cellular wireless and some fixed wireless networks or Internet VPN networks would not be considered reliable.

2.3 REPORTING

For all Managed Network Services, the following service reports are available provided quarterly.

- Hardware availability
- Device performance and capacity
- Trouble tickets
- Change tickets
- Monthly overview reports
- SLA reports



2.4 MANAGEMENT TOOLS

InterVision utilizes a variety of 3rd party software products to provide services. These tools include IT Service Managed (ITSM), monitoring, log collection, remote access, and other support and diagnostic tools. InterVision is responsible for selection and maintenance of software and tools used to provide service. InterVision uses prevailing industry practices to select, deploy, and operate these tools making all reasonable efforts to do in a secure manner and to not introduce any undue risks.

InterVision constantly evaluates the market for best-in-breed services to provide our customers, and may, at any time, change the software in use. InterVision will be responsible for the installation and maintenance of any InterVision-provided solution. The use of any other non-InterVision provided solutions will be the customer responsibility to manage and monitor.

Requests for a list of InterVision software tools may be obtain via a request through your Client Service Delivery Manager (for clients subscribing to Service management) or via a ticket.

2.5 DEFINITIONS

Dispatch - This refers to the scheduling of remote hands service at your site to assist with device replacements and other issues requiring skilled remote hands to resolve issues.

EOL - End of Life

EOS - End of Support

Essential Service Level - This is an InterVision Managed Service support level that offer monitoring, incident response and issue remediation.

Hosted Cafe' - Hosted Cafe is a name for the InterVision managed services organization and team. It is used to differentiate the services from other services such as InterVision professional services or Customer IT operations.

Monitor only- InterVision will place the Customer premise equipment ("CPE") under support and monitoring only service. The Service covers the specific IT infrastructure devices as detailed in an applicable Service Order. There is no phone support or onsite support with this service.

RMA - Return Merchandise Authorization. This refers to like-for-like device replacement under vendor warranty.

Premium Service Level - This is an InterVision Managed Service support level that offer monitoring, incident response, issue remediation, change management and additional life-cycle management capabilities.

©2022 InterVision. InterVision reserves the right to update this document at any time for any reason. The services and capabilities in this document may change without notice.

