

# Managed LAN

Service description

Make businesses *run better, grow faster*  
and *do more* for your customers

## TABLE OF CONTENTS

|     |   |           |
|-----|---|-----------|
| 1   | INTRODUCTION .....  | <b>2</b>  |
| 1.1 | Managed LAN at a glance .....                             | 2         |
| 2   | MANAGED LAN .....   | <b>3</b>  |
| 2.1 | Supported functions .....                                 | 3         |
| 2.2 | Hardware .....  | 4         |
| 2.3 | Monitoring & Response .....                               | 5         |
| 2.4 | Patch & Release Management .....                          | 7         |
| 2.5 | Backup & Restore .....                                    | 8         |
| 3   | SERVICE LEVELS .....                                      | <b>9</b>  |
| 3.1 | Service Window .....                                      | 9         |
| 3.2 | Configuration Management .....                            | 9         |
| 3.3 | Reporting .....   | 9         |
| 4   | TERMS AND CONDITIONS .....                                | <b>10</b> |
| 4.1 | Copyright .....   | 10        |
| 4.2 | Disclaimer .....  | 10        |
| 4.3 | General Terms and Conditions .....                        | 10        |
| 4.4 | Contact details Ingram Micro .....                        | 10        |
| 5   | ANNEX 1: SERVICE MATRIX .....                             | <b>11</b> |
| 6   | ANNEX 2: SYSTEM REQUIREMENTS & PRECONDITIONS .....        | <b>12</b> |
| 6.1 | Management Server Monitoring software .....               | 12        |
| 6.2 | Firewall rules management server to Internet .....        | 12        |
| 6.3 | Firewall rules management server - Internal network ..... | 12        |

# 1 Introduction

This document describes the Managed LAN service of Ingram Micro B.V. (hereafter to be called Ingram Micro).

Through our flexible Managed services we offer you, as an Ingram Micro customer, the ability to choose for the management of your customers' IT environment, or parts of it, through Ingram Micro's Network Operating Center. The Network Operating Center of Ingram Micro offers the same functionality and experience as your own IT management department without you or your client's organization being burdened with knowledge management, resourcing and specific Network Operating Center solutions. The Network Operating Center is staffed by experienced IT professionals and provides pro-active management and remote support.

## 1.1 MANAGED LAN AT A GLANCE

Managed LAN is a managed network service where Ingram Micro manages the local network of the end client. The scope of the service is described in greater detail in this document.

Ingram Micro offers Managed LAN in two variants;

1. Managed LAN **Basic** - All Ingram Micro standards are deployed at a standard service level. In the "Basic" variant, the network management is carried out with monitor tooling from the vendor.
2. Managed LAN **Standard** - All Ingram Micro standards are deployed at a standard service level. In the "Standard" variant, the network management is carried out with Auvik monitoring software. Auvik is a professional monitoring platform for Enterprise monitoring of network environments, in which much more is monitored than in the "Basic" variant.

The Managed LAN service description is based on the following components:

- Supported functions
- Hardware
- Monitoring & Response
- Patch & Release Management
- Backup & Restore
- Service Levels & Reporting

## 2 Managed LAN

This chapter describes the purpose and functionality of the different elements that compose Ingram Micro's Managed LAN service. In Annex 1 you will find a summary of all the functions and content of the service.

### 2.1 SUPPORTED FUNCTIONS

The Managed LAN service supports three network functions:

1. Core switching
2. Distribution switching
3. Access switching

The use and possibilities of the above functions differ in the service models Basic and Standard.

The chapter below provides a more detailed explanation of the definition of the switching types and the conditions within the Managed LAN service.

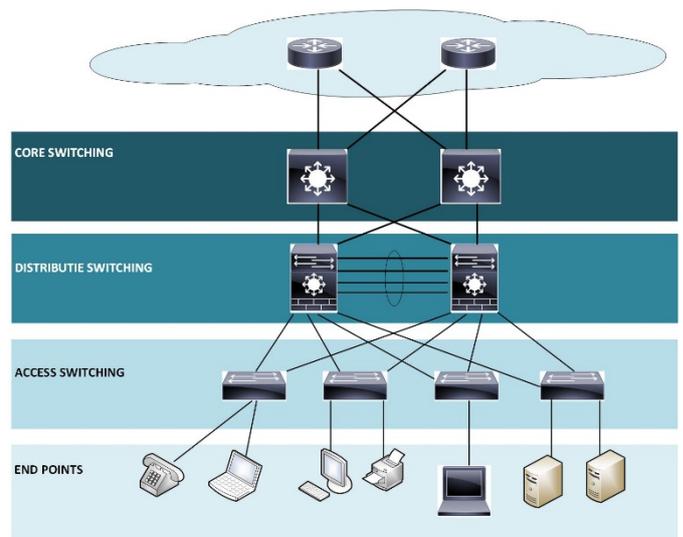


Figure 1: Logical network diagram

#### 2.1.1 Core switching

Core switching has the task of connecting all underlying network layers and is the heart of the network. Core switching ensures that the workplace can connect to the internet, servers and for example the printers and applications. Therefore core switching is a very critical component in the network. If this layer fails, the entire network is no longer usable and this has a major impact on the business operations.

The core switching can take place on two components of the network; on the core switches (layer 3) or on the firewall(s).

In the Managed LAN service, the core switching is only supported on the core switches. If the core switching function in the architecture takes place on the firewall(s), this is possible via the service "Managed Firewall" and is not part of the Managed LAN service.

#### 2.1.2 Distribution switching

Distribution switching has the task to link the core layer to the access layer. Sometimes this layer is merged with the core layer, usually with smaller networks. At larger networks, this layer is provided with a separate distribution layer consisting of one or more distribution switches. Both variants of distribution switches are supported by Ingram Micro.

#### 2.1.3 Access switching

Access switching has the task to connect peripherals to the network such as workplaces and printers. Access switches are linked to the distribution layer. The access layer generally includes most of the network infrastructure and usually has a local character.

## 2.2 HARDWARE

### 2.2.1 Supported brands

Ingram Micro supports all firewall devices that fall under the business segment in its services and can be managed remotely. Ingram Micro has the right to exclude equipment that cannot be managed properly in order to provide a quality service.

Ingram Micro can offer higher quality and a broader range of services if the Basic or Standard variants of Ingram Micro in the field of network equipment is chosen. Ingram Micro carries the network line of Fortinet, Cisco Enterprise and Cisco Meraki as standard. All Network Consultants and Engineers are trained and certified for this.

### 2.2.2 RMA & Replacement

With *Managed LAN Basic and Managed LAN Standard* Ingram Micro takes care of the entire RMA handling of faulty hardware. When reporting (near) hardware defects, Ingram Micro will take care of the entire RMA process with HPE Aruba and Cisco / Meraki.

The on-site replacement of the hardware will be charged on the basis of post-calculation. The client can also choose to replace the hardware himself. Ingram Micro is at all times the coordinator of the RMA process. If the device that needs to be replaced is at a certain height, an external organization will be called in. This is for the safety of our personnel. The costs of this will be charged on the basis of post-calculation.

A hardware support contract from the vendor is a basic condition on these services.

### 2.2.3 Architecture and advice

With *Managed LAN Basic and Managed LAN Standard*, it is possible to be relieved of any worries regarding architecture and advice concerning hardware replacement. This offers the advantage that you, as a customer, can outsource everything to one organization, and your own organization or a third-party organization does not have to be deployed for this. The condition is that the hardware must be from the brand HPE Aruba, Cisco, or Cisco Meraki.

Architecture and advice is optional with the Basic service variant and is included in the Basic service variant.

### 2.2.4 Cabling & peripherals

Ingram Micro can also relieve you from taking care of the installation and replacement of cabling and peripherals. This may include physical cabling, patch cabinets, cable ducts and finishing. This service is provided with the help of an Ingram Micro partner. Ingram Micro will be the coordinator at all times. The costs of this will be charged on the basis of post-calculation.

## 2.3 MONITORING & RESPONSE

The Ingram Micro Network Operating Center, hereafter referred to as NOC, is responsible for monitoring and managing the network environment.

The monitoring of the network is carried out by standard monitoring software of the relevant supplier/vendor via the “Basic” variant of the service, or by our high-end network monitoring environment based on from Auvik via the “Standard” service. For both variants, this is combined with the knowledge of specialized Network Administrators and Consultants.

The Auvik monitoring software that is used has been specifically developed for the management of network infrastructures. Ingram Micro not only has insight into the network infrastructure, but also what equipment is connected to the network. In this way Ingram Micro can also see what equipment is connected to the network, in addition to the network. This has the advantage that all equipment that is connected to the network and connected via an IP address can be tracked in the network.

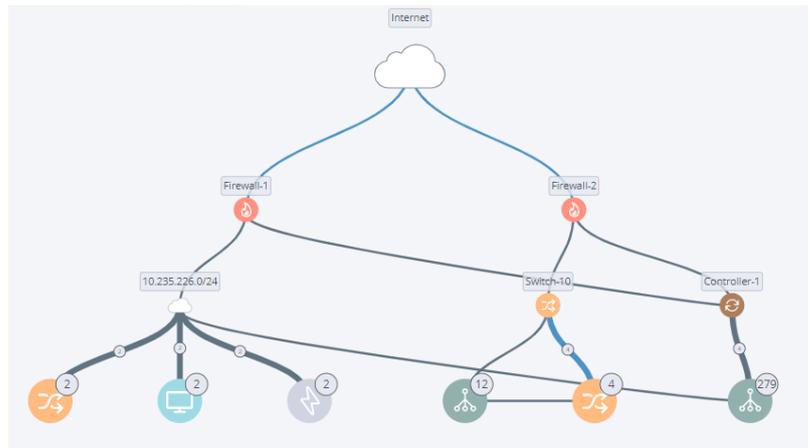


Figure 2: Example - Visualization physical network chain within Auvik

The building blocks on which Ingram Micro measures consists of the following components:

1. Availability
2. Utilization
3. Bandwidth & Traffic

### Alerting

Based on predefined parameters, the monitoring software issues an alert to which the NOC will directly respond within the SLA agreements. Depending on the type of failure and impact, the system creates an automatic classification. The NOC of Ingram Micro then determines the priority with which the incident will be dealt with, based on the client's specific situation (business impact). Determining the priority of the incident is always done in cooperation with the client. A single faulty switch can have a major impact on the business operations. More information on prioritization in case of incidents can be found in the Service Level Agreement (SLA) of Ingram Micro.

### Data retention period

The monitoring and configuration data of the systems is stored for a maximum of 10 years based on the current contract. If the contract expires or is terminated, the monitoring information in all the systems will be permanently deleted by Ingram Micro.

### 2.3.1 Availability

The most important component of monitoring is the availability of the network. Availability is determined by multiple factors within the network. The combination of these factors determines whether or not the network is available. Ingram Micro monitors the availability of each network device in order to measure the full availability.

The following availability units are measured continuously:

- Hardware device
- Port(s) and connections
- Administrative configuration
- Operational configuration
- Back-up
- Login
- SNMP

Availability is the most important parameter within the service. The availability of the equipment is reported every quarter.

### 2.3.2 Utilization

The utilization, also known as consumption of available resources, is measured continuously to ensure the availability, but especially to be able to interpret patterns and analyze problems properly.

The following utilization parameters are measured;

- Processor usage in %
- Memory usage in %
- Storage in % (if applicable)
- Port usage in %

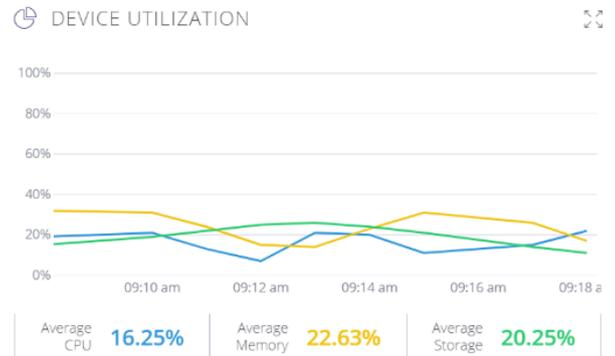


Figure 3. Example device utilization.

### 2.3.3 Bandwith & Traffic

All traffic handled by the network equipment is continuously measured by Ingram Micro's systems.

The following parameters are only in the Standard variant proactively continuously measured:

- Bandwidth per device - Average Mbit/s
- Bandwidth per interface - Average Mbit/s
- Data packets per device - Number averaged per second
- Data packets per interface - Number averaged per second
- Loss of data packets per interface - Number averaged per second

Traffic is continuously measured for behavior and if inconsistent changes occur according to the system, alerts will be triggered based on the expected impact.

Multi-vendor Monitoring and the Intelligent Monitoring platform and learning is only included in the Standard variant.

## 2.4 PATCH & RELEASE MANAGEMENT

In order to guarantee the safety and functionality of the network, it is important to keep track of the network equipment in terms of firmware.

Ingram Micro makes a distinction in the following types of updates:

1. Security patches
2. Functional Updates

With *Managed LAN Basic and Managed LAN Standard* the security patches, updates and functional upgrades are secured in the service.

### 2.4.1 Security patches

The security patches are released by hardware suppliers to fix vulnerabilities and bugs. Ingram Micro monitors all LAN equipment and keeps track with *Managed LAN Basic and Managed LAN Standard* whether any necessary patches have been found for the network equipment. Ingram Micro will roll out the security patches deemed necessary by the supplier to guarantee security and availability. If one or more security patches need to be installed, the change management process is launched to provide the network equipment with the necessary firmware.

### 2.4.2 Functional Updates

Network suppliers regularly release new functionalities on network equipment. Ingram Micro classifies these updates as functional updates. Functional updates are always carried out on the basis of a non-standard change and is part of the service with *Managed LAN Basic and Managed LAN Standard*. A functional update is only performed at the request of the client or on the recommendation of Ingram Micro.

### 2.4.3 Maintenance Window

With *Managed LAN Basic and Managed LAN Standard*, the proactive maintenance is carried out in consultation with the Client in view of the business-critical nature of the service provision.

## 2.5 BACKUP & RESTORE

All network equipment managed by Ingram Micro under the Managed LAN service is included in our backup service. This functionality is provided in both Basic and Standard variants of the management service, with the exception of the export of device configuration(s) and the configuration history storage. The latter two are only available in the Standard variant.

### 2.5.1 Back-up

Every network device managed by Ingram Micro is automatically backed up. Any change made to the network device is automatically stored within the service.

In addition to the automatic backup of the equipment, all configurations are stored indefinitely. With this functionality, you can always look back at configurations and automatically compare them with each other. Also, if an external party submits a change request that is unsuccessful, it is very easy and quick to return to the last working configuration.

The backup function can be provided if the network equipment is supported by Ingram Micro's management software and the network equipment can be accessed remotely using the SSH protocol. The Telnet protocol is not supported.

If any of these conditions are not met, Ingram Micro cannot guarantee the backup of the network equipment.

### 2.5.2 Restore

Restoring the configuration (backup) of a network device is a standard in the service. This situation occurs, for example, in case of human failure or replacement of a network device.

The restoration of a configuration is always carried out under the direction of and by Ingram Micro in order to guarantee continuity. In case, for whatever reason, the configuration has been changed by a third party other than Ingram Micro, restoring a backup will always be charged based on post-calculation.

### 2.5.3 Export configuration(s)

Within the service provision of the variant *Managed LAN Standard* it is possible to request an export of the configuration of one or more network devices. The costs of this will be charged on the basis of post-calculation.

## 3 Service Levels

The general service levels of Ingram Micro are described in the Service Level Agreement (SLA). This service description states which matters specifically apply to the Managed LAN service.

### 3.1 SERVICE WINDOW

In the Managed LAN service, there are two types of Service Windows available:

- Office hours
- 24x7 support

24x7 Prio 1 support is optional and is calculated over all network devices defined/contracted within the service.

### 3.2 CONFIGURATION MANAGEMENT

Ingram Micro is responsible for the administration of the following configuration items of all equipment managed by Ingram Micro:

| Configuration Items* |                             |                         |
|----------------------|-----------------------------|-------------------------|
| Device name          | Serial number               | Disc(s) (if applicable) |
| Device type          | Firmware version            | Work memory             |
| IP addresses         | VPN Tunnels                 | Network interfaces      |
| Networks             | User names                  |                         |
| Brand                | Passwords                   |                         |
| Model                | Cluster/Stack configuration |                         |
| Software version     | CPU(s)                      |                         |

*\*If the equipment does not have one or more configuration items or cannot be read out, Ingram Micro will not keep track of these configurations either.*

### 3.3 REPORTING

#### 3.3.1 Portal

The Client gains insight into the following components by means of the portal:

1. Availability
2. Incident overview and KPIs
3. Change overview and KPIs

#### 3.3.2 Trend analysis and advice

A trend analysis is created once every quarter within the "Managed LAN Standard" service with relevant advice. The trend analysis and advice will be discussed personally with the client in order to jointly improve the service at Ingram Micro, the client and any third parties.

The trend analysis and proactive advice is only provided with *Managed LAN Standard*.

## 4 Terms and Conditions

### 4.1 COPYRIGHT

No part of this service description may be reproduced and/or made public by means of print, offset, photocopy or in any digital, electronic, optical or other form or (and this applies if necessary in addition to copyright) reproduced for the benefit of a company, organization or institution or for personal practice, study or use without the prior written permission of Ingram Micro B.V..

### 4.2 DISCLAIMER

In compiling this service description, the greatest care has been taken to ensure the accuracy of the information contained herein. However, Ingram Micro B.V. cannot be held responsible for any incorrect information provided through this service description.

### 4.3 GENERAL TERMS AND CONDITIONS

These services are performed under the applicability of the NL Digital Terms and Conditions, as filed with the District Court of Midden-Nederland, location Utrecht and which can be consulted on our [website](#).

In addition to the General Terms and Conditions used by Ingram Micro B.V., the contractual Terms and Conditions laid down in the agreement that is concluded apply.

### 4.4 CONTACT DETAILS INGRAM MICRO

Ingram Micro B.V.  
Papendorpseweg 95  
3528 BJ Utrecht  
T: +31 (0) 30 246 40 01

## 5 Annex 1: Service Matrix

### MANAGED LAN

- ✓ Included
- Optional / Non-standard change
- Not possible / Not applicable

|  | BASIC                      | STANDARD                                     |
|--|----------------------------|--|
| <b>SUPPORTED FUNCTIONS</b>                   |                            |  |
| Core switching                               | ✓                          | ✓  |
| Distribution switching                       | ✓                          | ✓  |
| Access switching                             | ✓                          | ✓  |
| <b>HARDWARE</b>                              |                            |  |
| Supported brands (1)                         | HPE Aruba and Cisco Meraki | HPE Aruba, Cisco Enterprise and Cisco Meraki |
| RMA & Replacement (2) (3)                    | ✓                          | ✓  |
| Architecture & advice                        | ○                          | ✓  |
| Cabling & peripherals                        | ○                          | ○  |
| <b>MONITORING &amp; RESPONSE</b>             |                            |  |
| Availability                                 | ✓                          | ✓  |
| Utilization / Usage                          | ✓                          | ✓  |
| Bandwidth & Traffic                          | -                          | ✓  |
| Multi-vendor monitoring                      | -                          | ✓  |
| Intelligent Monitoring platform and learning | -                          | ✓  |
| <b>BACKUP &amp; RESTORE</b>                  |                            |  |
| Automatic Backup                             | ✓                          | ✓  |
| Restoring Backup                             | ✓                          | ✓  |
| Configuration history storage                | -                          | ✓  |
| Export device configuration                  | -                          | ✓  |
| <b>PATCH &amp; RELEASE MANAGEMENT</b>        |                            |  |
| Security updates (3)                         | ✓                          | ✓  |
| Functional Updates (3)                       | ✓                          | ✓  |
| <b>SECURITY &amp; COMPLIANCE NOC</b>         |                            |  |
| ISO 27001 - Information security             | ✓                          | ✓  |
| ISO 9001 - Quality Management                | ✓                          | ✓  |
| NEN 7510 - Information security Healthcare   | ✓                          | ✓  |
| ISAE 3402 TYPE 2 - Outsourcing standard      | ✓                          | ✓  |
| <b>SUPPORT</b>                               |                            |  |
| Office hours; 08:00 - 18:00                  | ✓                          | ✓  |
| 24/7 - Prio 1 Support                        | ○                          | ○  |
| <b>REPORTING</b>                             |                            |  |
| Availability - per quarter                   | -                          | ✓  |
| Incident overview & KPI's - per quarter      | ✓                          | ✓  |
| Incident overview & KPI's - per quarter      | ✓                          | ✓  |
| Trend analysis & Advice - per quarter        | -                          | ✓  |

1 Equipment must be remotely reachable / accessible

2 Replacement at additional cost. Replacement at heights working excluded

3 Hardware support contract is required

## 6 Annex 2: System requirements & preconditions

### 6.1 MANAGEMENT SERVER MONITORING SOFTWARE

| Description           | Requirement                 |
|-----------------------|-----------------------------|
| Operating system      | Windows 7+ or Windows 2012+ |
| (v)CPU                | At least 1 vCPU             |
| Work memory           | At least 2GB                |
| Storage               | At least 8GB                |
| Internet connectivity | At least 5mbit/s            |
| LAN connectivity      | Connection internal network |

### 6.2 FIREWALL RULES MANAGEMENT SERVER TO INTERNET

| URL's                 | Ports / configuration   |
|-----------------------|-------------------------|
| *.amazonaws.com       | 80 & 443                |
| *.security.ubuntu.com | 80                      |
| *.google.com          | 80 & 443                |
| DNS                   | 8.8.8.8:53 & 8.8.4.4:53 |
| NTP - Policy required | pool.ntp.org:123        |

### 6.3 FIREWALL RULES MANAGEMENT SERVER - INTERNAL NETWORK

| Protocols   | Ports          |
|---|----------------|
| HTTP  | 80 & 8080      |
| HTTPS   | 443 & 8443     |
| DNS   | 53             |
| NTP   | 123            |
| BGP (Border Gateway Protocol)                       | 179            |
| FTP (File Transfer Protocol)                        | 21, 115, 10021 |
| Java  | 9010           |
| OSPF (Open Shortest Path First)                     | 89             |
| RADIUS (Remote Authentication Dial-In User Service) | 1812           |
| SMTP (Simple Mail Transfer Protocol)                | 25             |
| SNMP (Simple Network Management Protocol)           | 161            |
| SSH (Secure Shell)                                  | 22             |
| Syslog  | 514, 54059     |
| TCP Health Check                                    | 12345          |
| TFTP (Trivial File Transfer Protocol)               | 69, 10069      |
| Telnet  | 23             |
| UPnP (Universal Plug and Play)                      | 1900           |
| mDNS (Multicast DNS)                                | 5353           |