Connected Workplace Managed Meraki SD-WAN, LAN and Wi-Fi

claranet Make modern happen®

Contents

Issue Control

Issue Number	Issued By	Date	Updates
1.0	Andy Bennett	27/08/23	Consolidation of the SD-WAN, LAN and Wi-Fi product descriptions into a single document.
1.1	Andy Bennett	05/03/24	Additional capability, Virtual MX, MS130 LAN Switches and Z4 / Z4C. Clarification on Cancellation and resign activities. Z3 and Z3c End of Sale and end of support dates included.

1. Introduction

This Service Description describes the service Claranet provides and details the Customer's responsibilities in relation to this Service. The Service Description forms part of the Agreement between the Parties is subject to the terms of the Claranet Master Services Agreement set out at www.claranet.co.uk/legal or as otherwise agreed by the Parties and the Parties agree to be bound by such terms. Unless otherwise specified, and all terms used within this document are in accordance with the terms to be found in the Master Services Agreement.

Claranet provides the following services as part of its Managed Meraki SD-WAN, LAN, and Wi-Fi ("Service") offering. Each Service Description, associated tasks, and option features are described in the Roles and Responsibilities tables.

The tables listed under each Service section in this document details the material tasks and responsibilities for the available Service components, which components, if purchased, will be expressly referenced in the relevant Customer Order Form or Statement of Work (SoW).

2. Scope of Service Description

The Customer expressly agrees that any services, activities, and deliverables not expressly set out within this Service Description shall be out of scope for the Service. The Customer may request a change to the scope of work required under this Service Description, but this will be chargeable at additional costs and to be agreed by the Parties signing an Order Form or Change Request. Claranet reserves the right to charge additional fees for but not limited to the following: adding to an existing Service where the execution of the change will require consultancy, technical design, change of deployment scripts used in automation, additional functionality, addition of additional environments and/or locations, swap out of a technology component as well as the addition of subscriptions/accounts to the original scope. Claranet reserves the right to charge on a time and materials basis for any additional work.

Notwithstanding the foregoing, in the event Claranet completes additional services, activities and/or deliverables upon the written request or at the direction of the Customer, Customer shall be responsible for the payment of all Fees and expenses associated therewith, whether or not an Order Form or Change Request has been executed in relation to the additional services or activities. Claranet may perform additional tasks outside those described as part of the service in this document. Any requirements in addition to those agreed in the order may be able to be fulfilled; however, this may also have an impact on the implementation timeframe. Claranet reserves the right to charge on a time and materials basis for any additional work.

3. Service Overview

The Claranet software defined solution consists of the following elements.

- Managed SD-WAN Security appliances (Physical and Virtual)
- Managed SD-LAN Switching
- Managed Wi-Fi Access Points

3.1. SD-WAN - Overview

Software Defined WAN (SD-WAN) can help your organisation meet the requirements of modern WAN connectivity, providing you with the application awareness required to tailor your WAN and deliver the best conditions for application delivery and digital experience.

To help achieve this level of control and functionality SD-WAN comes with many tools and services:

3.1.1. Centralised Management

The solution incorporates a centralized management platform as a vital element. This platform offers a unified dashboard that consolidates the crucial reporting generated by the inherent visibility, presenting it in easily understandable reports. It also allows you to make configuration adjustments that have a network-wide impact, facilitating faster provisioning or modification of your application profile.

3.1.2. Zero touch deployment

Rapid deployment capabilities allow you to commission new sites on your SD-WAN network quicker on existing connectivity. There is no need to pre-configure devices, they can be shipped directly to site, retrieving the configuration from the central management dashboard when they arrive. Enabling site infrastructure to be up and running quickly to deliver your applications to your end users.

3.1.3. Application Control

Transport independence enables deployment on any connection media. Connect sites together across 4G/5G, Broadband, and Ethernet, with Direct to Internet (DIA), or Multi-Protocol Label Switching (MPLS), or with both enabled. Communicating across IPsec VPN tunnels all traffic can be encrypted to keep it secure and protect against any interception attempts.

Application visibility and control is important to understanding your application behaviour. Built into the solution is Deep Packet Inspection (DPI) enabling the ability for each SD-WAN appliance to understand the applications that are traversing your WAN. This provides key intelligence to allow you to make informed decisions about how each application should behave. Including the ability to block and control the use of specific applications or whole categories, or the option to apply traffic shaping policies which still provide access but at a set bandwidth. Enabling you to

make sure that your bandwidth is being used by your business-critical applications and the end user experience is not being impacted by non-critical or unwanted applications.

3.1.4. Traffic Prioritisation

Traffic Prioritisation is not just about blocking unwanted applications, it's using your application aware WAN to identify the best path for your application traffic. By using two or more connections in an active/active configuration your SD-WAN can make intelligent decisions about which path the traffic is sent over. Based on configured SLA's that monitor the quality of the links for jitter, latency, and loss the SD-WAN will make real time decisions to choose the link that can provide the best application performance.

3.1.5. Advanced Security

Advanced security is a consideration for all IT projects and should be built in at the design phase. Fortunately, the SD-WAN solutions offered by Claranet come with advanced security functionality built in. With Intrusion Prevention, Antivirus, and Web Filtering as part of the functionality available, SD-WAN does not become a security problem, SD-WAN can be used to improve your security posture. Bringing security controls and visibility closer to the end users and distributing sensors to all sites. Enabling you to see any potential breaches quicker, whilst allowing you to have greater control over stopping the threat moving through your WAN and infecting other sites.

3.1.6. Cloud On-Ramp

Cloud Connectivity enables simple connectivity to AWS or MS Azure, setting up a secure tunnel between the SD-Wan networks and the cloud service, and the ability to prioritise application destined for these clouds. Multiple connections and multi cloud providers are supported, details within this document.

3.2. SD-WAN - Physical Appliances

The Claranet SD-WAN service is based on physical SD-WAN appliances dedicated to you. Depending on the solution that fits your specific requirements these can be supplied as onsite customer premise equipment (CPE) or hosted within our data centre (DC) (rack mountable only). With the option of running the SD-WAN connectivity in a Hub and Spoke configuration, fully meshed, full tunnel or split tunnel mode. Dual WAN connections in "Active / Active" mode to maximise the available bandwidth, with application prioritisation across the WAN to optimise critical application performance.

Claranet will collaborate with you to identify the best solution based on the number of clients, bandwidth, tunnelling, and security requirements from the following models.

- Z4 / Z4c Micro Branch / Teleworker
- MX67, MX67W, MX67C
- MX68, MX68W, MX68CW
- MX75
- MX85
- MX95
- MX105
- MX250
- MX450

3.3. SD-WAN - Virtual Appliances

Virtual MX (vMX) is a virtual instance of a Meraki SD-WAN appliance, dedicated to providing the simple configuration benefits of site-to-site Auto VPN for organizations running or migrating IT services to public or private cloud environments.

An Auto VPN tunnel to a vMX is like having a direct Ethernet connection to a private data centre. Features and functionality of the vMX appliance:

- Securely connect branch sites with a physical MX appliance to resources in public cloud environments in three clicks with Auto VPN.
- Extend SD-WAN to public cloud environments for optimized access to business-critical resources.
- Meraki vMX license is required.
- Available in three VPN throughput-based sizes to suit a wide range of use cases: small (200Mb), Medium (500Mb) or Large (1Gb) total throughput.

For public cloud environments, a vMX is added via the respective public cloud marketplace. Setup and management in the Meraki dashboard, just like any other MX.

The vMX capability is supported on the following cloud services -

- MS Azure 200Mb or 500Mb total throughput
- AWS 200Mb, 500Mb, or 1Gb total throughput

The recommended design is the vMX will be a hub site on the network. The Branch sites that require access to the vMX will be configured as Spokes, and added to the Site To Site VPN configuration. This will enable AutoVPN connectivity with the vMX, Hub prioritisation will also need to be agreed and configured on the network if multiple Hubs are provided.

Azure Route Server is also recommended for single and dual Azure vMX deployments, rather than configuring a routing table.

3.4. SD-WAN - Advanced Security

The MX platform has an extensive suite of security features, including intrusion detection system & intrusion prevention system (IDS/IPS), content filtering, web search filtering, anti-malware, geo-IP-based firewalling, IPsec VPN connectivity, and Cisco Advanced Malware Protection, while providing the performance required for modern, bandwidth-intensive networks.

Layer 7 fingerprinting technology lets administrators identify unwanted content and applications and prevents recreational apps like BitTorrent from wasting precious bandwidth. The integrated Cisco SNORT® engine delivers superior intrusion prevention coverage, a key requirement for PCI 3.2 compliance.

The MX also uses the Webroot BrightCloud® URL categorization database for CIPA/IWF-compliant content filtering, Cisco Advanced Malware Protection (AMP) engine for anti-malware, AMP Threat Grid Cloud, and MaxMind for geo-IP-based security rules. Best of all, these industry-leading layer 7 security engines and signatures are always kept up to date via the cloud, simplifying network security management and providing peace of mind to IT administrators.

Security updates are delivered automatically from the Meraki dashboard to all connected devices, this does not need to be scheduled or delivered via planned maintenance.

3.5. SD-WAN – Cloud Managed Architecture

Built on Cisco Meraki's award-winning cloud architecture, the MX is the industry's only 100% cloud-managed solution for unified threat management (UTM) and SD-WAN in a single appliance. MX appliances self-provision, automatically pulling policies and configuration settings from the cloud. Powerful remote-management tools provide network-wide visibility and control and enable administration without the need for on-site networking expertise.

Cloud services deliver seamless firmware and security signature updates, automatically establish site-to-site VPN tunnels, and provide 24x7 network monitoring. Moreover, the MX's intuitive browser-based management interface removes the need for expensive and time-consuming training.

3.6. SD-WAN – Integrated Wireless

The MX67W, MX68W, and MX68CW integrate Cisco Meraki's award-winning wireless technology with the powerful MX network security features in a compact form factor ideal for branch offices or small enterprises.

- Dual-band 802.11n/ac Wave 2, 2x2 MU-MIMO with two spatial streams
- Unified management of network security and wireless
- Integrated enterprise security and guest access

3.7. SD-WAN – Integrated LTE Modem

While all MX models feature a USB port for 4G failover, the MX67C and MX68CW include a SIM slot and internal LTE modem. This integrated functionality removes the need for external hardware and allows for cellular visibility and configuration within the Meraki dashboard.

- 1 x CAT 6, 300 Mbps LTE modem (4G)
- 1 x Nano SIM slot (4ff form factor)
- Global coverage with individual orderable SKUs for North America and worldwide

3.8. SD-WAN – Power over Ethernet

The MX68, MX68W, and MX68CW include two ports with 802.3at (PoE+). This built-in power capability removes the need for additional hardware to power critical branch devices.

- 2 x 802.3at (PoE+) ports capable of providing a total of 60W (i.e., 3 access points)
- APs, phones, cameras, and other PoE-enabled devices can be powered without the need for AC adapters, PoE converters, or unmanaged PoE switches.

3.9. SD-WAN Licencing

3.9.1. Licence Tiers

Advanced Security is the recommended licence, here is the capability for both licence types:

Feature	Advanced Security	Enterprise
Centralized management	✓	✓
Zero-touch firmware updates	✓	✓
True zero-touch provisioning	✓	✓
24x7 enterprise support	✓	✓
Open APIs	✓	✓
Automatic WAN failover	✓	✓
Sub-second site-to-site VPN failover	✓	✓
Sub-second dynamic path selection	✓	✓
Stateful firewall	✓	✓
VLAN to VLAN routing	✓	✓
Advanced Routing	✓	✓
Uplink Load Balancing/failover	✓	✓
3G / 4G cellular failover	✓	✓
Traffic shaping/prioritization	✓	✓
Site-to-site VPN	✓	✓
Client VPN	✓	✓
MPLS to VPN Failover	✓	✓
Splash pages	✓	✓
Configuration templates	✓	✓
Group Policies	✓	✓
Client connectivity alerts	✓	✓
Essential SD-WAN	✓	✓
Source-Based Routing	✓	✓
Local Breakout (IP and Port based)	✓	✓
Geography based firewall rules	✓	
Intrusion detection & prevention	✓	
Content filtering	✓	
YouTube Content Restriction	✓	
Web Search Filtering	✓	
Cisco Advanced Malware Protection (AMP)	✓	
Umbrella DNS Integration**	✓	
Threat Grid Integration**	✓	

** Requires additional licence

3.9.2. Per Device Licencing

The SD-WAN licence commences on the day the device is claimed within the organisation and will run for the duration of the licence term. Each device on the network will require an associated licence, and the licences will be tied to that device on a per device licence.

At the end of the term there is 30 days to renew the licence, if this is not completed then the licence expires therefore the device stops working. Licences can be renewed any time before the expiry date without losing any days of the term.

If licences are ordered, and are not claimed for 90 days, then on day 91 the licence will start its licence period automatically.

3.10. SD-LAN – Overview

At the heart of any network are LAN (Local Area Network) switches. These provide the foundation for the network in which applications and services are delivered across. Connecting users with the tools they need to complete their day-to-day activities. With the Claranet Managed LAN service we can take the complexity of managing and supporting your LAN away from you. With packages to support all needs, we can design, implement, and manage your LAN. Providing you with the confidence that everything will continue to run smoothly. Allowing your IT department to focus on delivering the applications required by your user base.

Cisco Meraki offers a broad range of switches built from the ground up that are designed to be easy to manage without compromising any of the power and flexibility traditionally found in enterprise-class switches. Meraki access and aggregation switches are all managed through an elegant, intuitive cloud interface, freeing administrators to spend less time on configuration and more time on meeting business needs. A powerful centralised management interface gives administrators deep visibility into the network and how it is used. See which switches are near capacity across hundreds of sites. Quickly provision and reconfigure switch ports with security, QoS, and more. The Meraki dashboard provides unified policies, event logs, and monitoring, making switch management efficient and scalable.

3.11. SD-LAN – LAN Switches

The Claranet SD-LAN service is based on LAN switches deployed on your sites and consists of the following devices. These switches are available without PoE, Low power PoE (370W) and high power PoE (740W)

- MS120 8/24/48 Port Cloud Managed Switch
- MS125 24/48 Port Cloud Managed Switch
- MS130 8/28/24/48 Port Cloud Managed Switch
- MS210 24/48 Port Cloud Managed Switch
- MS225 24/48 Port Cloud Managed Switch

- MS250 24/48 Port Cloud Managed Switch
- MS350 24/48 Port Cloud Managed Switch
- MS355 24/48 Port Cloud Managed Switch
- MS390 24/48 Port Cloud Managed Switch
- MS410 24/48 Port Cloud Managed Switch
- MS425 24/48 Port Cloud Managed Switch
- MS450 24/48 Port Cloud Managed Switch

3.12. SD-LAN - Intelligent campus and branch switching

With built-in monitoring, troubleshooting, and logging capabilities, Meraki switches provide a refreshing innovative approach to managing network infrastructure, regardless of deployment size. The virtual stacking technology eliminates the need for configuration scripts and commands, empowering administrators to make changes quickly and securely on one or all the switches in a deployment at once.

3.13. SD-LAN – Wired Security

Whether deployed in an office environment, hospital, or retail store, Meraki switches make enforcing security policies a breeze. Set up multiple policies and enable them at the port level or apply them across the entire network in a few clicks. Meraki switches also provide comprehensive security reporting, making it easy to proactively discover rogue DHCP servers and other malicious activity on the network.

3.14. SD-LAN – Troubleshooting

Reduce time to resolution with a variety of powerful troubleshooting tools, such as remote cable testing and packet captures, that help isolate and troubleshoot network issues. With the dynamic network topology of Meraki, automatically see how the entire network is interconnected and ensure the team receives alerts upon power loss, downtime, or configuration changes.

3.15. SD-LAN – Stack Power and Physical Stacking

Stack power pools power from each individual PSU in a switch stack to form a larger, shared pool of power that provides additional redundancy and helps reduce costs by managing the available PoE more efficiently. Improved physical stacking helps in faster-stack convergence in case of a failover, which is critical in large enterprise deployments.

3.16. SD-LAN – Cloud Management

By utilising the Meraki templates feature you can standardize an entire fleet of switches, no matter what size. With Meraki virtual stacking, administrators can manage up to thousands of ports from a single dashboard, enabling rapid and streamlined configuration that could otherwise take weeks to complete.

3.17. SD-LAN – Application Layer Visibility

Meraki is the only switch to include integrated layer 7 fingerprinting. Identify hundreds of applications, from business apps to BitTorrent and YouTube. User fingerprinting with Google-like search allows administrators to easily identify and control individual users, PCs, iMacs, iPads, Androids, and other devices. This allows optimisation of network resources and maintenance of optimal network performance.

3.18. SD-LAN – Architecture

Meraki switches run the same operation system used by all Meraki products. The use of a common operating system allows a consistent experience across all product lines, from security products to VoIP phones. Meraki switches automatically connect to the Meraki cloud, download configuration, and join the appropriate network. If new firmware is required, this is retrieved by the switch and updated automatically. This ensures the network is kept up to date with bug fixes, security updates, and new features.

3.19. Wi-Fi – Managed Access Points

Cloud networking provides full visibility and control into network usage. Providing the capability to manage user access, applications, and control bandwidth usage. Whilst providing analytics on how users are interacting with the network, using triangulation to identify footfall, and intelligent algorithms providing context around visitor numbers, repeat visitors, and user loyalty.

Managed Meraki Wireless allows you to use an enterprise grade wireless solution with all of these features. Offering fast connectivity throughputs of up to 5 Gbps using the latest Wi-Fi 6 frequency standards, MU-MIMO connectivity, and dedicated security radios. Providing robust connectivity in dense user environments, whilst keeping you protected against common threats associated with wireless connectivity. With built in analytics, Managed Meraki Wireless gives you the advantage of detailed context around user engagement, allowing you to understand and improve your interaction with your customers.

3.20. Wi-Fi – Physical devices

We currently support the following devices.

- Meraki MR28 Wi Fi 6 Indoor Access Point
- Meraki MR36 Wi Fi 6 Indoor Access Point

- Meraki MR44 Wi Fi 6 Indoor Access Point
- Meraki MR46 Wi Fi 6 Indoor Access Point
- Meraki MR46E Wi Fi 6 Indoor Access Point with External Antenna Connectors
- Meraki MR56 Wi Fi 6 Indoor Access Point
- Meraki MR57 Wi Fi 6e Indoor Access Point
- Meraki MR76 Wi Fi 6 Outdoor Access Point
- Meraki MR78 Wi Fi 6 Outdoor Access Point
- Meraki MR86 Wi Fi 6 Outdoor Access Point

3.21. Wi-Fi - Centralised Cloud Management

The Meraki cloud-managed architecture allows users to seamlessly manage campus-wide Wi-Fi deployments and distributed multi-site networks with zero touch access point provisioning, network-wide visibility and control, self-learning RF optimization, seamless firmware updates, and more. With an intuitive browser-based user interface, Meraki WLAN configures in minutes without training or dedicated staff, offering scalability with templates. Meraki devices are self-provisioning, enabling large campus and multi-site deployments without on-site IT. Learning from billions of touchpoints, AI and data-powered Meraki Health empowers customers with the data they need to stay informed and the context they need to make decisions.

3.22. Wi-Fi - Meraki Health

Meraki Health is a suite of tools and analysis to assist wireless administrators by providing each client's and access point's unique perspective of connectivity to the WLAN, enabling IT organizations to achieve faster issue remediation, maximize uptime, and optimize performance. By ingesting data from a complete network infrastructure platform, the Meraki Health heuristics engine rapidly identifies anomalies impacting wireless end users' experiences across every stage of client connectivity— association, authentication, IP addressing, and DNS availability—for rapid root- cause analysis and response.

Using Meraki Health, immediate visibility is provided to identify problematic APs and clients, gain actionable insights to pinpoint stages of failure, and determine if users can access the network. Remotely identify problematic devices anywhere across a campus or thousands of separate geographical sites and access built-in live troubleshooting tools. Globally apply network data collection to extract insights and make configuration changes at scale to optimize Wi-Fi performance.

3.23. Wi-Fi - Analytics

Rich analytics ensure performance levels with color-coded historical metrics, signal quality, client count, wireless latency, channel utilization, and data rates allowing for time-based correlation to

significant events. Real-time analytics are provided for specific access points as well as individual wireless clients. Client timelines include automated root-cause identification and suggested remediation for client connectivity failures.

3.24. Wi-Fi - Network-Wide Visibility

Visibility and status of the entire network is provided when combining Meraki access points with Meraki switches and SD-WAN appliances. The end-to-end network infrastructure snapshot shows client connectivity failures and metrics that would dictate the health of a connection or device along the path to the network's layer three gateway. With a reduction in reactive troubleshooting and an increase in proactive and predictive network management, client, application, and service performance can be assured.

3.25. Wi-Fi - Rapid Deployment and Scalability

The Meraki cloud-managed architecture enables plug and-play branch deployments and provides centralized visibility and control across any number of distributed locations. Since Meraki MR series APs are managed entirely through the Meraki web-based dashboard, configuration and diagnostics can be performed remotely just as easily as on-site, eliminating costly field visits. Each device downloads its configuration via Meraki cloud, applying your network and security policies automatically so you don't have to provision them on-site.

3.26. Wi-Fi - Air Marshall

Meraki wireless APs feature a radio dedicated to full-time scanning, rogue AP containment, and automatic RF optimization. With Air Marshall is possible to set up a real-time wireless intrusion detection and prevention system (WIDS/WIPS) with user-defined threat remediation policies and intrusion alarms, enabling secure wireless environments without complex setup or systems integration. It works by monitoring the wireless for attacks or rogue Access Points, preventing rogue access points tricking legitimate users joining malicious networks, ensuring wireless clients are kept on the correct network, prevents Spoofing for Access Points using cloned MAC addresses, and prevents malicious floods or broadcasts. Alerts are visible on the dashboard, together will SSID's detected by the access points.

3.27. Wi-Fi - Automatic Cloud-Based RF optimization

All Meraki Wireless Access Points feature sophisticated and automated RF optimization, eliminating the need for the dedicated hardware and RF expertise typically required to tune a wireless network. The RF data collected by the dedicated third radio is continuously fed back to the Meraki cloud. This data is then used to automatically tune the channel selection, transmit power, and client connection settings for optimal performance under even the most challenging RF conditions. Auto RF eliminates the need for manual RF configuration by scanning the environment for utilization, interference, and other metrics, and computing the optimal channel

and power settings for every AP in the network. Meraki WLANs are fully HIPAA and PCI compliant.

3.28. Wi-Fi - Built-in Guest Access with Analytics

Meraki cloud management provides the ability to customize and integrate splash pages onto each Meraki wireless access point, with options for click-through or sign-on splash using your own RADIUS server or the Meraki cloud-based RADIUS user database. The Meraki wireless series features a complete array of built-in captive portal tools, including a guest ambassador portal for new user sign-on, splash sign-in tracking, application blocking and traffic shaping, free and paid tiers of access, integrated credit card processing and prepaid code generation, and splash bypass for corporate-issued or recognized devices.

3.29. Wi-Fi - Integrated Security

Meraki Wireless Access Points feature integrated, easy-to-use security technologies to provide secure connectivity for employees and guests alike. Advanced security features such as AES hardware-based encryption, Enterprise authentication with 802.1X, and Active Directory integration provide wired-like security. PCI compliance reports check network settings against PCI requirements to simplify secure retail deployments.

3.30. Wi-Fi - High-performance RF design

Every Meraki access point continuously and automatically monitors its surroundings to maximize Wi-Fi performance. By measuring channel utilization, signal strength, throughput, signals from non-Meraki APs, and non-Wi-Fi interference, Meraki APs automatically optimize Wi-Fi performance of individual APs and maximize system-wide performance. Meraki APs have been deployed and proven in the most demanding environments, supporting more than 100 users per AP, and collectively serving hundreds of Mbps of user traffic to thousands of devices. By eliminating traditional hardware controllers, Meraki also eliminates the performance bottleneck that often chokes high-density wireless deployments. By measuring utilization from neighbouring APs, detecting Wi-Fi signals from non-Meraki APs, and identifying non-Wi-Fi interference, Meraki APs continuously stay on top of changing and challenging conditions. Tools such as real-time spectrum analysis and live channel utilization deliver immediate information on the RF environment at any part of the network. Even in dynamic environments, Meraki networks automatically detect and adapt to interference from non-Wi-Fi sources.

3.31. Wi-Fi - Presence

Meraki wireless APs track probing MAC addresses from associated and non-associated clients. This data is exported in real time from the access points to Meraki cloud for analytics; information is then calculated and presented in the Meraki dashboard to display metrics such as user dwell time, repeat visits, and capture rate (people passing by vs. engaging with a site). This information can be used by retail, hospitality, and enterprise customers to understand foot traffic and visitor

behaviour across sites to facilitate optimization of opening hours, marketing campaigns, and staffing policies.

3.32. Wi-Fi - BYOD-ready out of the box

The number of user-owned devices connecting to networks increases every day. Meraki wireless APs feature built-in support for BYOD and make it easier than ever to securely track and support user-owned devices—without extra appliances, licenses, or complex VLAN configurations. Using integrated layer 7 fingerprinting, client devices are automatically identified and classified, letting you distinguish between iPads and iPhones, device operation systems, and even manufacturers. Device specific policies can be automatically applied to restrict, quarantine, or throttle user-owned devices. Client fingerprinting, combined with a heuristic driven reporting engine, allows you to generate detailed reports of BYOD clients that have connected, measure the bandwidth and applications they have accessed, and even see their percentage of total traffic. Bonjour forwarding facilitates seamless discovery of Apple devices across VLANs, rounding out a full BYOD-centric feature set.

3.33. Wi-Fi - Auto-tunnelling VPN technology

Leveraging the Meraki cloud architecture, site-to-site VPNs can be enabled via a single click without any command-line configurations or multistep key permission setups. Complete with IPsec encryption, deploy the following architectural setups within minutes:

- Teleworker VPN: Securely extend the corporate LAN to remote sites wirelessly using the MR series with your own server or a Meraki MX
- Site-to-site VPN: Multi-branch VPN with WAN optimization and content filtering (using Meraki MX security appliance)
- Secure roaming: Layer 2 and layer 3 roaming for large campus environments.

3.34. Wi-Fi - Wireless Personal Network (WPN)

In shared networks, such as dormitories, residence halls, senior living facilities, shared office spaces, and hotels, Wireless Personal Network (WPN) offers a “home-like” Wi-Fi experience on any shared network by segmenting the wireless network on a per-user basis. In addition, WPN provides a contained environment to each user where discovery protocols like AirPlay allow users to discover only their own devices connected to an SSID shared by other devices. Even better, WPN allows for segmenting discovery protocols and unicast traffic on a single VLAN, thus eliminating the burden of configuring different VLANs per floor, room, or location and simplifying the network management.

3.35. Wi-Fi - Flex (XOR) radio

The MR57 and CW9166 access points support a software-defined flex radio which can be operated in either 5 GHz or 6 GHz mode. This provides an option to operate the AP in either a

dual 5 GHz configuration or a true tri-band configuration. Tri-band configuration unlocks the use of the new spectrum in the 6 GHz frequency range, which provides additional channels to increase throughput and reduce interference and noise from legacy devices.

3.36. Wi-Fi - High availability/resilience

The flagship MR57 features dual configurable Ethernet ports that can support 1, 2.5, or 5 Gbps, with link aggregation between both network ports for redundancy and high availability.

4. Consult & Design

Claranet offers a comprehensive consultancy and design stage for all prospective customers. Claranet will discuss with you, your business, and your technical requirements. We will design a solution with you for your business. Claranet will deliver, where required, a detailed description of the technical design including a network diagram and Statement of Works. It may be part of a larger document if the offering is part of a larger solution. This forms part of your agreement and will provide the technical specifications for your solution.

4.1. LAN Audit

If this is a replacement of an existing LAN and depending on the size of your current LAN, Claranet will recommend that a LAN audit is performed to allow us to capture your current configuration and to allow us to understand where we can improve the service you are receiving from your current LAN. A LAN audit will also allow us to understand the level of work required to migrate your LAN services, allowing us to price up the deployment accordingly and removing any unknowns. Please contact your account manager for further details.

4.2. Wireless Site Survey

Claranet recommends that one or more Wireless Site Surveys are conducted. There are many factors that can impact the behaviour of a wireless signal, and the purpose of the Wireless Site Survey is to identify that the solution will meet the requirements that you desire. Showing how coverage of the wireless signal will propagate throughout your environment(s), whilst highlighting any areas where wireless signal will need extra attention.

Claranet can offer two types of wireless site survey:

Desk side survey – A desk side survey is performed by an engineer using the information that you provide them. The engineer will input the information into an application and use this to ascertain the approximate number of access points required. This type of site survey is best for small or simple deployments in places such as open plan offices and cannot consider real world radio interference.

Onsite survey – At least one engineer will visit your locations(s) and perform a detail survey using industry leading Ekahou survey software and tools. They will perform a detailed survey testing frequency attenuation throughout your environment to provide the most accurate understanding of where access points should be installed, and how they will service users connecting to them.

If an Onsite Survey is not performed, Claranet cannot guarantee that wireless coverage will be adequate in all areas that it is required and may lead to dead spots within the desired coverage area. The service description can be found on the Hub **Here**

4.3. Cabling Site Survey

Claranet recommends that a cabling site survey is conducted following, or at the same time as the Wireless Site Survey. The purpose of the cabling site survey is to identify that your cabling infrastructure can support the addition of the wireless access points. This includes identifying if there is connectivity to the proposed location of the access points, understanding if the switching infrastructure can support the increased throughput, and identifying any power requirements. The outcome of the Cabling Site survey may identify that you need to replace existing cabling, install new cabling, install power points at the location of access points, or replace/add new switches.

Responsibility	Claranet	You
Information: All Wireless site survey options require you to complete a questionnaire. It is your responsibility to complete this to the best of knowledge. This information will impact the success of the site survey		✓
Pre-agreed survey: Work with our partner who employs skilled surveyors, who can attend site to complete a cabling or wireless site survey within standard business hours.	✓	
Outcomes: Provide a full and detailed report on your available options along with recommendations that will include the number of access points required and the desired locations for deployment.	✓	
Site Access: You will provide convenient times within business hours when the engineers can gain access to the site to perform a detailed site survey. Depending on the environment, the site survey could cause some disruption.		✓
Cabling Quotation: As part of the cabling survey report Claranet will provide a detailed quotation for each item requiring consideration. On acceptance of these costs, Claranet will collaborate with you to arrange engineers to return to site to complete the works prior to installation of the AP's	✓	

Responsibility	Claranet	You
Switching: As highlighted by the survey, it may be necessary for you to upgrade your switching infrastructure to cope with increased throughputs, or the ability to supply POE (Power Over Ethernet). As required, Claranet will supply a quote for any switching required.	✓	
Switching: If the switching infrastructure is not upgraded as identified in the survey, the quality of wireless experience will be impacted. Claranet accepts no responsibility of poor service if recommendations are not followed.		✓
Cabling: If the cabling site survey has been performed, it is the responsibility of you to ensure any changes that were identified have been implemented. Making sure that connectivity and power are available.		✓
Supplier: You have the right to contact a separate cabling provider to complete any upgrades as required. Claranet will not be able to deploy the wireless solution if the works have not been conducted as suggested. Claranet reserves the right to refuse to deploy the service if the works are not completed.		✓

4.4. Dedicated Engineer

As part of your standard installation package Claranet will include 2 hours of dedicated time to allow for consultation with your commissioning engineer. This time will be used to explain your configuration options, how these options could work for your organisation, and to help you identify which option is best suited to your business outcomes. The amount of consultancy time allocated will depend on the complexity of your build. If any further consultative time is required following your allocated time, this will be charged at our standard consultancy rates.

Responsibility	Claranet	You
Consultative engineering: In the design stage our solutions architects will collaborate with you to identify the complexity of your wireless deployment.	✓	
Dedicated engineering: Taking into consideration the complexity of your deployment, our solutions architect will allot an amount of dedicated engineer time for your project.	✓	
Current Build: Provide accurate details to the best of your knowledge about your current build and your future requirements.		✓

5. Managed Service

This section describes the Claranet fully managed service that is applied across a Claranet Managed Meraki solution.

The following table is a high-level summary of the service features:

	Foundation
Configuration & Commissioning	✓
Site & Solution Tuning Period	Site Tuning – 2 Days Solution Tuning 14 Days
Hardware Break-Fix	Flexible RMA Options Per Device
Change Management Simple Change Request	Additional service, select the number of changes per month
Backup & Restore	Near Real-Time Backup & Restore Points
Vulnerability Patching	Continuous Auto Updates
Firmware Upgrade	Continuous Auto Updates
Business Continuity Testing	Optional service if required

5.1. Configuration & Commissioning

In this stage Claranet will provide services by which orders for Managed SD-WAN, LAN & Wi-Fi are captured and progressed through to delivered and subsequently into in-life management. This stage is initiated following a signed order and/or statement of works and completes when the service is operationally tested, quality assured and transitioned in to in-life management.

5.2. SD-WAN - Configuration Options

Our delivery and commissioning teams will work with you to identify and optimise the configuration for your network. The configuration will identify Application prioritisation, security (Content Filtering, IPS/IDS, Anti-Virus settings), Traffic Shaping, Intelligent Routing, multiple VLANS (if required), DHCP requirements, and Active Directory integration.

As part of this process the SD-WAN data capture form will be provided, and its completion is your responsibility. It is not the responsibility of Claranet to ensure that the configuration you choose is suitable for your internal applications. However, as part of your dedicated engineering time Claranet can assist you in designing a configuration that is most suitable for your environment.

5.2.1. SD-WAN – Network Security Policy

Claranet technical experts will work with you to define a network security policy that will be applied to your SD-WAN appliances at spoke and hub locations. The network security policy will dictate what level of network access is granted in and out of each site location.

Tailoring the network security policy is essential to hardening your overall security posture across your business, minimising the risk of cyber-attacks and the resulting impact, whilst in-turn moving your organisations towards a zero-trust security model of operation.

5.2.2. SD-WAN – SD-WAN Policy

Claranet technical experts will work with you to define SD-WAN policies that will be applied to your appliances at spoke and hub locations. The SD-WAN policies specify applications and/or services alongside a traffic distribution profile. The policies can also specify a path quality for your applications and services and make path routing decisions based on the performance of your underlay connectivity.

Tailoring SD-WAN policies will ensure that each location is considerate of the applications and services being consumed and how best to optimise and protect the quality of experience of these.

5.2.3. SD-WAN - Hub and Spoke

In a Hub and Spoke SD-WAN configuration, the SD-WAN appliances at the branches and remote offices (‘Spokes’) connect directly to specific ‘hub’ appliances and will not form tunnels to other devices at other branches. Communication between branch sites or remote offices is available through the configured SD-WAN Hubs. This is the recommended topology for most SD-WAN deployments.

In this configuration we would see the Hub devices deployed at a central site location(s). This may be a head office location, in one of our DC’s (rack mountable only), or within a cloud environment. These devices would have to be specified to meet the traffic needs of all sites connecting into it, and therefore we would normally architect more throughput capable appliances at these locations.

Claranet engineers will work with you to define the most suitable SD-WAN architecture for your business needs.

5.2.4. SD-WAN - Meshing

In a mesh SD-WAN configuration, an SD-WAN appliance at the branch or remote office is configured to connect directly to any other SD-WAN appliances installed at branch offices that are also in mesh mode. Creating an SD-WAN network where all sites are equal, allowing the direct sharing of data between all branches.

A Fully Meshed SD-WAN has the benefit of connecting all sites together without the need to host central Hubs. However, a deployment with many sites will impact the devices required at each location. In this scenario we would collaborate with you to make sure that all devices, at all sites, can support the required number of VPNs to allow direct connections.

5.2.5. SD-WAN - High Availability (HA) options

For each SD-WAN appliance model, a High-Availability (HA) option is available. When configured for HA, one appliance serves as the primary unit and the other operates in a secondary capacity. All traffic flows through the primary, while the secondary operates as an added layer of redundancy in the event of failure.

Failover between SD-WAN appliances in a HA configuration leverages heartbeat packets. These heartbeat packets are sent from the Primary appliance to the Secondary out the singular uplink to indicate that the Primary is online and functioning properly. If the Secondary is receiving these heartbeat packets, it functions in the spare state. If the Secondary stops receiving these heartbeat packets, it will assume that the Primary is offline and will transition into the master state. SD-WAN failover can take between 5 and 180 seconds to complete depending on the design and configuration deployed.

5.2.6. SD-WAN - Auto VPN

Auto VPN is a proprietary technology developed by Meraki that allows you to build VPN tunnels quickly and easily between Meraki MX devices at your separate network branches with just a few clicks. Auto VPN performs the work normally required for manual VPN configurations with a simple cloud-based process. VPN's can be built between sites, between sites and data centres, and to virtual sites (vMX) within the cloud. It has automatic VPN route generation using the IKE/IPSec-like tunnels and all this is done in the Meraki cloud.

5.2.7. SD-WAN - Tunnelling Options

There are 2 options to route traffic across the network: -

- Full Tunnel, traffic is tunnelled across the VPN link to the hub destination to local server or out to the Internet.
- Split Tunnel, traffic for the Hub / DC / vMX is tunnelled to the destination via AutoVPN, other traffic (such as www, SaaS applications) breaks out locally to the internet.

5.2.8. SD-WAN - Advanced Security Options

5.2.8.1. Intrusion Prevention Service (IPS)

Intrusion Prevention System (IPS) technology is becoming an increasingly ubiquitous part of network security defences. With an increasing threat landscape made up of sophisticated and targeted attacks, the deep packet inspection offered by IPS is key to protecting your environment.

Through intelligence gathered by Cisco Talos, your firewall will be up to date with IPS signatures allowing you to capture the latest threats, identify zero-day threats, and detailed targeted attacks utilising known exploits.

More information about Cisco Talos can be found here **https://www.talosintelligence.com/**

5.2.8.2. Anti-Malware

Using industry-leading advanced detection engines, the Meraki SD-WAN security appliance uses the Cisco AMP (Advanced Malware Protection) engine, which operates to prevent both new and evolving threats from gaining a foothold in your environment. With hackers using malware to cause data breaches, extort money through ransomware, expose intellectual property, and disrupt and destroy systems. Cisco AMP can help prevent threat actors from gaining access to you network and its invaluable content.

5.2.8.3. Web Filtering

Threat actors increasingly use compromised and malicious websites to initiate attacks, trigger downloads of malware, spyware, or other risky content into your infrastructure. To reduce your attack surface area and reduce the risk to your organisation, it is important to protect your environment by limiting access to these sources of threat. Through global security intelligence, Cisco Talos can identify and categorise websites as they go online, when they change purpose, or when they are compromised. This allows you to create policies that will block access to web-based services through IP, URL, or category groups. Through integration with Active Directory, you can apply policy to users and groups, giving you granular control over which resources can be reached on the web. Not only protecting you against the latest threats but also stopping access to inappropriate websites and making sure that you meet compliance.

5.2.8.4. Application Control

As information technology has become application centric, it has never been more important to have control over applications and their behaviour within your environment. The Meraki SD-WAN threat services allow for the creation of policies, allowing you to manage the applications used on your network and removing the associated risks. Policies can be applied based on application type, specific applications, or by application function. With integration into Active Directory, these policies can be applied to specific users and groups based on their role and function. Through the intelligence gathered by Cisco Talos, logs can be gathered, highlighting which users are using which applications and how much. Allowing you to have more context around bandwidth usage, and giving you control over unwanted applications, prioritising traffic for business-critical applications.

Responsibility	Claranet	You
Consultative engineering: In the design stage our solutions architects will collaborate with you to identify the complexity of your WAN deployment	✓	
Dedicated engineering: Taking into consideration the complexity of your deployment, our solutions architect will allot an amount of dedicated engineer time for your project.	✓	
Current Build: Provide accurate details to the best of your knowledge about your current build and your future requirements.		✓
Application Prioritisation: Ensure that high priority applications are identified in advance of deployment		✓
Security Requirements: Provide details of the content filtering / blocking, whitelist / Blacklist, and Layer 3 / Layer 7 firewall rules (Advanced security license only).		✓

5.2.8.1. Meraki Virtual MX

Virtual MX provides secure connectivity AWS / Azure, this can be deployed and managed by Claranet, or it can be your own provided cloud infrastructure.

Responsibility	Claranet	You
Virtual MX: Where you are providing the AWS / Azure environment for the vMX, follow the installation instructions to prepare the environment for the activation token (Valid for 1 hour). Provide the required configuration for our delivery team to configure the vMX. If High Availability / Load Balancing is required then the configurations will need to be completed by you on the relevant cloud platforms. Installation information can be found within the relevant installation guide, as well as useful routing information needed within your cloud environment.		✓
Virtual MX: Where Claranet providing the AWS / Azure environment for the vMX, we will complete the deployment of the cloud and the vMX, and configure in line with your requirements. Additional Cloud hosting and configuration / professional service charges apply.	✓	

Where you are providing the Cloud the following URL's will assist in creating the cloud environment ready for us to provide the activation token.

General Specification

- **Meraki VMX Comparison Guide**

AWS

- **AWS Installation Guide**
- **AWS VPC Connectivity**
- **vMX with AWS Cloud WAN**
- **vMX with AWS Transit Gateway**
- **AWS Quick Start Guide**

Azure

- **Azure Installation Guide**
- **Microsoft Network Fundamentals**
- **Setting up Azure – full tunnel mode**
- **High Availability in Azure**

5.3. SD-LAN - Configuration Options

For the deployment of any LAN, Claranet requires you to confirm the configuration of your appliances at time of installation. This will enable instant operability of each element of the LAN service. Our delivery and commissioning teams will work with you to identify and optimise the configuration for your network. The configuration will identify Switch Profiles, Binding and Tagging, ACL configuration, STP Configuration, and Routing Configuration.

As part of this process the LAN data capture form will be provided, and its completion is your responsibility. It is not the responsibility of Claranet to ensure that the configuration you choose is suitable for your internal applications. However, as part of your dedicated engineering time Claranet can assist you in designing a configuration that is most suitable for your environment. Further detail for each element of configuration is listed below:

5.3.1. SD-LAN - Switch Profiles

To enable consistent management of switch ports, switches can be grouped together based on their function. For example, it is possible to create a profile that groups together all access switches. This then allows for a more consistent administration of these switches when it comes to changing configuration, or when a new switch is added to the profile. Claranet can assist you with designing, creating, and applying of your switch profiles.

5.3.2. SD-LAN - Switch port settings

With each switch it is possible to configure every switch port with individual settings that can be applied to multiple ports simultaneously, regardless of their physical location, or applied one at a time. This enables you to have ports configured for each element of network, allowing the correct VLANs, security settings, and port schedules.

5.3.3. SD-LAN - STP configuration

Spanning tree protocol (STP) is important to any LAN deployment that includes many switches. Protecting against broadcast storms that could bring down a network, STP needs to be planned and configured correctly to allow for a seamless experience on the LAN. If a switch is being introduced into a LAN that has existing switches, we will need to understand your topology and how this switch will fit into your LAN.

5.3.4. SD-LAN - OSPF routing

Routing protocols are important for any network to allow traffic to follow the optimum route through the infrastructure. Reducing the load on single areas of the network and keeping the impact of network traffic balanced across the infrastructure. We will need to understand your current OSPF configuration to allow us to enable OSPF correctly on the Meraki switch, allowing seamless interoperation with your current infrastructure.

5.3.5. SD-LAN - Granular Port Tagging

To assist with granular port configuration, it is possible to manually tag switch ports to put them into logical groups. This provides the opportunity to apply unified configuration across many logical ports regardless of their physical location.

5.3.6. SD-LAN Design

The complexity of the LAN is increasing. VoIP, Unified Comms, and applications are testing the performance and stability of networks not engineered to accommodate them. As your business evolves a flexible and agile working strategy and implements new technologies to grow your business. End to end network performance is becoming ever more critical. To make sure that your LAN meets the requirements of a modern business Claranet can assist you with a complete re-design of your LAN, or if you are opening a new office, we can make sure that the LAN is ready for everything a modern business can throw at it. Including detailed STP and OSPF implementations to stop loops and broadcast storms. Designing robust security making sure that no unwanted users can access your LAN through any switch.

Responsibility	Claranet	You
Consultative engineering: In the design stage our solutions architects will collaborate with you to identify the complexity of your LAN deployment	✓	
Dedicated engineering: Taking into consideration the complexity of your deployment, our solutions architect will allot an amount of dedicated engineer time for your project.	✓	
Current Build: Provide accurate details to the best of your knowledge about your current build and your future requirements.		✓
Minimum specification: Ensure that any minimum specification requirements are clearly and accurately completed in the LAN Configuration Survey as soon as possible.		✓

5.4. Wi-Fi – Configuration Options

Claranet requires you to confirm the base configuration of your appliances at time of installation. This will enable instant operability of each element of the wireless service, allowing you to begin to use the solution in the knowledge that it has been configured in line with your requirements.

Our delivery and commissioning teams will work with you to identify and optimise the configuration for your network. The configuration will include Corporate / Guest SSID's, Splash Page configuration, Layer 3 / Layer 7 firewall rules, Floor Plans / Locations, application prioritisation, and group policies.

As part of this process the Wireless data capture form will be provided, and its completion is your responsibility. It is not the responsibility of Claranet to ensure that configuration you choose is suitable for your internal applications. However, as part of your dedicated engineering time Claranet can assist you in designing a configuration that is most suitable for your environment.

Further detail for each element of configuration is listed below:

5.4.1. SSID configuration

There are many options for the SSID configurations on the Meraki appliance. Not all options will be supported by Claranet as part of the Base and Advanced configuration. Through following this process, Claranet can get you up and running as quick as possible. If you do require these extra features to be configured as part of your installation, or you require more than two SSID's, we can implement the Bespoke configuration and arrange a technical specialist to collaborate with you.

5.4.2. Splash page configuration

As part of the base package, Claranet will assist with setting up a Splash page for your guest access based on the settings within the Meraki dashboard. If you require a more detailed splash

page that is to be setup on an external server or using a third-party solution. Claranet will configure the Meraki dashboard to pass traffic to this solution, but we will not assist in the configuration or management of any third-party applications or solutions.

5.4.3. Access point Firewall (Layer 3 / 7) and traffic shaping configuration.

Meraki access points support Firewall capabilities directly within each appliance. This allows the capability to configure the access points to filter traffic (based on Layer 3 or Layer 7 identification) at time of connection, stopping traffic from traversing the LAN.

Traffic shaping is made up of several elements which include the application type, name, and the bandwidth options that you wish to apply. This gives you the opportunity to still allow certain applications to be used on your LAN but allows you the option to limit the bandwidth impact of these applications.

As part of the base configuration, Claranet will configure a number of policies based on the package that you have requested.

5.4.4. Floor plans and access point locations

As part of the advanced package, it is possible for Claranet to add floor plans to the dashboard and place access points at the approximate locations. This will enable easier support and identification of access points and the utilisation of each access point. This will also allow more accurate identification of footfall when using the location heatmap, showing user locations against your floorplan.

The use of this element of the service does require you to have had the wireless site survey. The survey will give us accurate locations of the access point placement that we will be able to replicate within the Meraki dashboard. We will also require you to provide us with accurate floorplans of each site location in a PDF format.

5.4.5. Group Policies

As part of the advanced package, it is possible to configure group policies. These are policies that enable you to apply policies directly to specific devices, or groups of devices. Group policies allow for the configuration of granular firewall and traffic shaping policies (5 per group policy), the ability to limit bandwidth, and the ability to configure access schedules. This function allows for even more granular control over how users can use the network.

Responsibility	Claranet	You
Consultative engineering: In the design stage our solutions architects will collaborate with you to identify the complexity of your Wi-Fi deployment	✓	
Dedicated engineering: Taking into consideration the complexity of your deployment, our solutions architect will allot an amount of dedicated engineer time for your project.	✓	
Current Build: Provide accurate details to the best of your knowledge about your current build and your future requirements.		✓
Minimum specification: Ensure that any minimum specification requirements are clearly and accurately completed in the Wi-Fi Configuration Survey as soon as possible.		✓
Proposal &/or Statement of Work: Provide a high-level quotation/proposal detailing the solution bill of materials and price along with any supporting context and description. Where Claranet deem appropriate produce a final Statement of Work (SoW) detailing the high level design.	✓	
Order Validation: To identify missing or conflicting information and summarise the details of the order back to the customer	✓	
Data Capture: Upon technical validation of an order Claranet will issue data capture form named IPQ to the customer to gather low level design, security and SD-WAN policy requirements as part of the tailored design process. It is the customers responsibility to ensure data capture forms are completed to their best of their ability with as much information as possible. Failure to do so could create inaccuracies in the low-level design and lead to technical incidents or security posture weakness. Claranet technical delivery teams will assist and guide our customers on how to complete any DCF	✓	✓
Design Consultancy: Claranet will provide a technical scoping and consultancy session with the customer. The objective of this session is to provide technical best practice guidance in order to enhance the security posture of the appliance and optimise SD-WAN performance. For multi-site rollouts Claranet will complete this activity in a single technical scoping session. The customer is obligated to actively participate in these session/s, share business and IT information to help tailor the security and SD-WAN policy per site. Claranet will dictate the format and communication mechanisms used in the design consultancy session.	✓	✓

Responsibility	Claranet	You
Low Level Design: The combined output from the data capture form and the design consultancy will be a completed data capture form that details the site profiles and their security and SD-WAN policy requirements. The data will be used to create a configuration templates that will apply the security and SD-WAN policies onto the SD-WAN appliance	✓	

6. Build

Once the Statement of Works has been accepted, we will build out your service. This includes applying the agreed configuration and policies. At the completion of this phase, the service is fully tested and handed over to you as part of the Handover Document. Once accepted, any future changes will be managed as part of In-Life Management.

6.1. Lead Times

The standard lead-times are set out below. Lead times for a solution assume any associated network is already in place to facilitate the install and commissioning of the devices. The standard lead times are dependent on short lead time availability from the technology vendor. Vendor lead times can adjust frequently therefore the lead times should therefore be a guide and not an absolute delivery target.

If the project is planned to have staggered roll out, lead times to deployment can be agreed between you and Claranet. From our storage facilities the general shipping time (depending on destination location) is 24 to 48 hours. Installation Claranet can offer you the option to do a self-install, or you can use our engineers to complete a managed install of the appliances at your site(s).

Claranet will use commercially reasonable endeavours to achieve the dates provided to the customer however no SLA payments are committed to the missed delivery dates of the service.

The lead time encompasses the delivery, installation, and commissioning of any new site. All lead times are based on a United Kingdom delivery, install and commission, and delivered directly to your site. Any services that fall outside of the United Kingdom, Claranet will provide an estimated lead time on a case-by-case basis. Lead time is also dependant on the lead time for the supporting infrastructure connections, Ethernet, Broadband, or Mobile.

Product Type	Lead Time
Virtual (vMX)	15 working days
SD-WAN appliances (MX)	30 working days
SD-LAN Switches	30 working days
Wi-Fi Access Points	30 working days
Virtual (vMX)	3 working days

The lead time for Lan switches may be extended for certain models, is the issue with the Global Chip Shortage is still impacting manufacture of certain switches, we can advise the lead time closer to contract signature as we track Meraki delivery schedules.

6.2. Installation

Physical installation of the devices will either be conducted by the customer or Claranet field engineering partners dependent on the service tier that has been purchased. Where Claranet are conducting the managed install, our engineers will physically mount, rack, power, and cable the equipment ensuring the appliance has been housed safely and securely within the customers location.

Claranet's field install service is a professional service that is bought upfront and based on a packaged install service. For each install service bought Claranet allocate 2hrs onsite engineering time to physically install the equipment and operate between Monday to Friday 9-5PM (not including bank holidays). Claranet install service has a 1:1 site to install mapping meaning that each site will need to have a corresponding install service. If the order or corresponding statement of works does not include a field install service Claranet will assume the physical installation is to be carried by the customer.

The below responsibility matrixes describe the physical installation obligations for self-installation whereby a customer agrees to carry the physical installations themselves, and a managed install where Claranet field service engineers will conduct the install on behalf of the customer.

The site installation is not dictated by the managed service tier and operates as an independent service that is attached to a site installation.

6.2.1. Managed Install

As part of the managed install, Claranet will collaborate with you to identify an installation schedule for the appliances at your site(s). All devices will be installed and tested by a trained engineer, who will confirm that each device is up and running before leaving site. The engineer will not be responsible for configuring non-Claranet supplied equipment to enable the functionality of the SD-WAN devices. It will also not be the responsibility of the engineer to provide the relevant structured cabling, power, and cooling to the appliances.

Responsibility	Claranet	You
Shipping Schedule: For each SD-WAN site Claranet will collaborate with you to create a shipping schedule that allows you to self-install SD-WAN devices efficiently. Once the appliances arrive on-site it will be your responsibility to store the appliances on-site safely and securely ready for the Managed Install. Install the appliance ensuring the device is housed, cabled safely and securely, and does not increase the risk of device failure. For example, installing the equipment in a poorly ventilated room which could increase operating temperature of the device	✓	
Site Details: Capture site address and contact information and ship devices to the location. You will provide convenient times when the engineers can gain access to the site within the contracted hours to perform the installation of the SD-WAN devices.	✓	✓
Environment: Ensure the environment where the SD-WAN device is being installed is suitable, cabled and does not increase the risk of device failure. For example, installing the equipment in a poorly ventilated room which could increase operating temperature of the device. The customer should also label any cabling to ensure the appliance can be cabled correctly into the WAN and the LAN. SD-WAN appliances will need a single 13A mains connection, larger branch devices with dual power units will require one for each unit preferably on different feeds. Rack mounted units will require 1U rack space.		✓
Site access: You will provide convenient times when the engineers can gain access to the site within the contracted hours to perform the installation of the LAN switches. Depending on the environment, the installation could cause some disruption		✓
Installation: Claranet field service engineers will physically install the device, cable, and commission the service alongside a Claranet technical delivery engineer who will operate remotely. The field and remote engineer will ensure the service is in an operational state before the field service engineer departs. In certain scenarios a re-visit may be required. Claranet reserve the right to charge for a re-visit if the install cannot be completed due to circumstances that are not within Claranet's control. Wireless Access Points can be installed up to a maximum height of 3M. Installations above this height will require additional equipment, such as a scissor lift or cherry picker to complete the installation.	✓	

Responsibility	Claranet	You
Commissioning: Claranet will commission the service to verify the device is online and reachable for management access and ensure access and SD-WAN policies are operating in accordance with the customer requirements captured in data capture forms. This is a pre-requisite check before the device can be transitioned into in-life management.	✓	
Installation Time: Unless already agreed, installation will be completed in a two-hour slot which will take place between 9am to 5pm Monday to Friday. Installation can take place outside of business hours, but this will incur extra costs that must be agreed upfront or retrospectively back charged.	✓	✓
Business Testing: Test the service at each site to ensure it has business operational use and report any faults to the Claranet service desk. Claranet will work with the customer and its key contacts to support business testing	✓	✓
Workspace: Provide a suitable & safe work area to the onsite project team		✓
Health & Safety: Inform Claranet &/or sub-contractors of any health and safety requirements are instructed on all relevant health and safety regulations and criteria		✓
Notice Period: Provide a minimum of 12 working days' notice prior to agreed resource schedule commencement for any scheduling or requirement changes. The customer cannot cancel planned activities on the agreed schedule during the three working days prior to starting those activities. If so, the customer will incur the full cost of the cancelled activities during that three-day period		✓
Change Control: The customer is responsible for raising and approving any necessary change control relative to the scope of work		✓
PPE: The customer will be responsible for informing Claranet and/or sub-contractors of any site-specific requirements such as PPE (including colour, certification levels requirements) and will be responsible for providing PPE over and above the standard PPE that Claranet &/or its sub-contractors provide (EN397 Hard Had, Fluorescent Vest, Steel Toe Cap Boots)		✓
Professional Services: Claranet can provide the customer with professional services at an additional charge, at their request to assist with the creation of a tailored security and SD-WAN policy or to carry out a Managed onsite Install. Claranet can conduct additional network testing and accommodate	✓	✓

Responsibility	Claranet	You
installations outside of standard operating times at an additional professional service charge. For example, testing network connectivity to key applications or installing appliances on bank holidays. This will need to be defined within a scope of work and is charged based on a time & materials commercial model. Claranet will collaborate with you to capture additional requirements and produce scope of work with charge information		

6.2.2. Self-Install

If you have chosen the self-install option, Claranet will collaborate with you to identify a shipping schedule. Once the appliances arrive on site, it will be your responsibility to install the appliance and connect all the necessary cabling. By working with your assigned Project Co-ordinator to identify the planned times for installation, Claranet will endeavour to have all configuration available in the management dashboard before physical installation is complete.

As soon as the device has established connection to the management dashboard it will begin the process of registration and pulling down the configuration. Within approximately 20 minutes of an appliance connecting to the cloud (dependant of connection speeds, and number of devices, firmware versions), the appliance will be fully provisioned with the agreed configuration.

Responsibility	Claranet	You
Installation Guide: Provide the customer with a self-installation guide that defines the recommended environment in which any appliances should be installed; the customer is responsible for adhering to the requirements of this guide	✓	
Shipping Schedule: For each SD-WAN site Claranet will collaborate with you to create a shipping schedule that allows you to self-install SD-WAN equipment efficiently.	✓	
Site Details: Capture site address and contact information and ship devices to the location	✓	✓
Environment: Once the appliances arrive on-site it will be your responsibility to install the appliance ensuring the device is housed, cabled safely and securely, and does not increase the risk of device failure. For example, installing the equipment in a poorly ventilated room which could increase operating temperature of the device		✓
Commission: For each device that has been self-installed Claranet will commission the service remotely and verify the device is online and reachable for management access. This is a pre-requisite check before the device can be transitioned into in-life management. For certain models of SD-WAN appliances Claranet may insist on a managed install or provide the	✓	

Responsibility	Claranet	You
configuration template to you for self-configuration on to the appliance. Managed Install details will be captured in the SoW and/or order. Claranet reserve the right to request & charge for a Managed Install should it be absolutely required to commission the service, this could be for instance whereby remote zero touch provisioning is not possible, or the customer is unable to commission & configure the appliance on-site		
Connectivity: Ensure that all devices are connected correctly using Cat6 cabling. Please refer to any network for reference diagrams (if created and agreed as part of the design stage).		✓
Installation: Self-Install the SD-WAN devices ensuring the device is housed, powered, and cabled. Ensure that underlay network connectivity is cabled and connected. If the appliances are being installed behind other security appliances, then ensure that correct access policies are created to allow connectivity to the Internet. Where Claranet has provided a configuration template for you to install on to an SD-WAN device, you will follow the necessary configuration steps provided by Claranet to install the configuration.		✓
Business Testing: Test the service at each site to ensure it has business operational use and report any faults to the Claranet service desk		✓
Professional Services: Claranet can provide the customer with professional services at an additional charge, at their request to assist with the creation of a tailored security and SD-WAN policy or to carry out a Managed onsite Install	✓	
Access: If devices are installed behind a Firewall that is not supplied by Claranet please ensure that correct policies are created to allow full connectivity to the cloud. For further information please refer to **Addresses and Ports** document		✓

6.3. Testing and acceptance

The engineer configuring your Managed service will ensure that the testing process is as transparent as possible. If actions are identified as part of this process, they will be included in your delivery plan and managed to closure by your Project Co-ordinator.

Responsibility	Claranet	You
Testing: Test the Managed SD-WAN / LAN / Wi-Fi to ensure that it performs in terms of connectivity and speed in accordance with the Service Levels	✓	✓
Actions: Perform any actions that are required to enable the completion of any testing.		✓

6.4. Acceptance procedure and Handover Document

Once the device is installed and connected, the ongoing management is under the In-Life Management process managed by our Service Operations Team. You should refer to the handover document provided to you.

7. Manage

Once your network is up and running and the Handover Document is completed, Claranet will continue to manage the availability of the SD-WAN 24x7x365 to maintain its operation. The parameters of the ongoing management of the service and the appropriate roles and responsibilities are outlined in the areas below.

7.1. Co-managed SD-WAN

Claranet can manage your WAN / LAN / Wi-Fi configuration, through the design and implementation, additional or changes in configuration, and 24x7 technical support. However, we will need you to provide at least one administrator with access to the management dashboard.

The primary reason that we offer this access because of the real time that provides you with greater insight into you network behaviour.

Having access to the dashboard does allow you the capability to make some changes, however, should you prefer that Claranet perform full management you can simply raise change requests and our trained engineers will complete the configuration. Changes at the HQ or Data centre are to be requested via the simple change request process as this can have a significant impact on the network performance.

Any changes Claranet have to make to recover the network, after changes have been made, may be charged. SLA and service credits do not apply to recovering the network.

7.1.1. Role Based Access

Access to the dashboard is through the management dashboard.

You will have to register new admins through Claranet, and we can set these up with a variety of levels of access.

Responsibility	Claranet	You
Licensing: Apply and keep up to date any relevant license purchased by you.	✓	
Customer made changes: If a customer change causes an outage of any services, Claranet will not be held responsible and normal SLA's will not apply		✓
Firmware update: Auto Update will be turned on, and a suitable day and time scheduled to perform upgrades entered on the dashboard. You may defer upgrades if necessary. Advanced Security updates will be delivered as soon as a revised signature file is received to ensure our always up to date with the latest security protection.	✓	

7.2. Change Management

As part of the co-managed service, you will have access to change configuration of your SD-WAN / LAN/ Wi-Fi, however, should your change be complex, or you require the support of a Claranet engineer you have the option to raise a change request.

Where you require specific changes to be made to the configuration of your SD-WAN, Claranet will be responsible for making the change.

Monthly changes can be purchased on SD-WAN, LAN, and Wi-Fi services for Claranet to make the changes on your behalf.

7.2.1. Change Control Process

Change Management is a process design to understand and minimise risks while making IT changes. Organisations have two main expectations of the services provided by IT:

1. The services should be stable, reliable, and predictable.
2. The services should be able to change rapidly to meet evolving business requirements.

A Change might be needed because of a Standard, Complex Contract Affecting and Complex Non-Contract Affecting changes from other events such as Incidents, Problems, and any Third Party / Partner Planned Engineering Works (PEWs).

7.2.2. Simple Change Request

A low risk, common and pre-approved type of change that typically follows an agreed set process.

7.2.3. Complex Change Request

Anything not explicitly listed above as a simple change request will be considered a complex change request. An example of a complex SD-WAN change is when an existing spoke site needs to be converted into a Hub SD-WAN location. Due to the solution wide impact of this type of change a specialist engineer will need to review the impact, plan the change, and quantify the effort involved in carrying this out.

Claranet reserve the right to convert a complex change request into a contract affecting one or charge professional services in a time and material model to conduct the change.

Feature	Simple CHG		Complex CHG	
	Action	Location	Action	Location
Firewall Policies	Add/Modify/Remove firewall policies and its associated objects for existing policy sets or templates	Per device or template	New firewall policy template and device application	Per template
SD-WAN Policies (MX and vMX)	Add/Modify/Remove SD-WAN policies and its associated objects for existing policy sets or templates	Per device or template	New SD-WAN policy template and device application	Per template
SD-WAN Overlay (VPN)	Add/Modify/Remove VPN Overlay	Per device or template	Add/Modify/Remove VPN Overlay	Per device
SD-WAN Underlay (Physical ISP)	Modify/remove existing underlay configuration	Per device	New underlay configuration	Per device
3rd party VPN	Add/Modify/Remove 3rd party VPN's	Per device		
Routing	Add/Modify/Remove static routes	Per device		
VLAN	Add/Modify/Remove VLAN/Interface and associated configuration.	Per device	Add Physical port configuration in Claranet DC	Per device (chargeable as infrastructure)
NAT	Add/Modify/Remove NAT Objects and corresponding policies	Per firewall		
Content Filtering	Add/Modify/Remove Content Filtering profiles and corresponding policies	Per device or template	Initial Setup of content filtering	Per device
IPS	Add/Modify/Remove IPS profiles and corresponding policies	Per device or template	Initial Setup of IPS	Per device
Lan Switching	Switch port changes/additions	Per device or template		
Lan Switching	Layer 3 routing changes/additions	Per device or template		
Lan Switching	IPv4 ACL	Per device or template		

Feature	Simple CHG		Complex CHG	
	Action	Location	Action	Location
Lan Switching	Access policies	Per device or template		
Lan Switching	Port Schedules	Per device or template		
Wi-Fi	New SSID	Per device or template		
Wi-Fi	Edit an existing SSID	Per device or template		
Wi-Fi	Edit / Add a Splash Page	Per device or template		
Wi-Fi	Add / Modify / Remove Firewall policy	Per device or template		
Wi-Fi	Layer 7 Application Rules	Per device or template		
Wi-Fi	Traffic Shaping Policies	Per device or template		

7.2.4. Change Control Process (RFC)

For more detail on the Claranet Change Request Process, please refer to the terms & service detail with the Customer Experience for Managed Services Document (“CXMS”) which can be found on Claranet Online Portal, or as otherwise agreed by the Parties. All terms used in this document are in accordance with the terms set forth in these documents.
CXMS provides a framework for Claranet’s core support experience and describes what a customer can expect from any standard Managed Service solution provided by Claranet. It outlines the responsibilities of both Claranet and the customer, including how to log and escalate cases, how SLA targets are prioritized, set, and achieved, as well as the tools used to perform these functions

7.2.5. Change of Service

If your requirements change, and you need to enable new service, a change of service type, additional users, or a change in service features, they must be requested via your Account Manager and may be subject to prevailing fees.

7.3. Firmware Upgrade

By default, all SD-WAN devices are automatically opted into an upgrade window. Cisco Meraki releases new firmware approximately once a quarter. When a new firmware is released, your network will be scheduled for an upgrade, and you will be notified 2 weeks in advance via email. Once scheduled you as a co-management user will have the option to reschedule or adjust your upgrade window to meet your site requirements.

Claranet can adjust a network site to change the upgrade window on your behalf. This can be requested through the build phase or as part of a simple change request.

While installing a firmware update, Cisco Meraki devices continue to operate normally until they reboot as the last step in the upgrade process. In some instances, a reboot may be required, this normally takes 1-2 minutes, so it is best to pick an upgrade time with minimal expected network usage. If the firmware update is unsuccessful, then the device will roll back to the previous version.

7.4. Maintenance Window

The Major Incident process will be invoked during the maintenance window where a rollback or issue mitigation process does not exist, or should the planned work extend beyond the allocated time.

Responsibility	Claranet	You
Notify: Provide as much notice as possible to ensure minimal disruption	✓	
Contact list: Provide and maintain an up-to-date contact list, including any changes in authorisation		✓

7.5. Monitoring and Logs

7.5.1. Logs

Due to the in-depth nature of the logging built into SD-WAN, Claranet will not retrieve or send any logs into Claranet online or any other systems. With co-managed access you will have full real-time visibility of all the information directly through the management dashboard.

If you would prefer, Claranet can configure the dashboard to send you regular reports via email so that you can receive this information directly into your inbox. You also have the option to create and modify regular reports via the dashboard.

7.5.2. Monitoring

Claranet will actively monitor the status of your network 24x7x365. This will allow us to quickly understand when a device goes offline allowing us to create a support ticket and begin investigating the issue.

Because there may be elements of you network that are out of Claranet's control, you must notify our support desk should you be performing any maintenance that could cause any of the devices to lose connectivity.

7.5.3. When a threshold is breached

Where the monitoring system identifies that a threshold is breached, alarms are triggered to alert Claranet support staff. If a threshold is breached or a service affecting event occurs, the Claranet

Operations team are notified to raise a ticket and take appropriate action to resolve the issue. This could include troubleshooting and resolving the problem or notifying you that your application may be pushing a large amount of data.

Responsibility	Claranet	You
Monitor: Monitor devices for up time 24x7x365	✓	
Notify: Provide Claranet information around any planned maintenance that you believe may cause the any of the devices to lose connectivity		✓

7.6. Help and Support

7.6.1. Break/fix service -On Site Equipment

Claranet provides a break/fix service on all SD-WAN appliances under contract. In the case of a hardware failure, as deemed by a Claranet engineer, a replacement device will be required.

We offer enhanced replacement services as listed below and would recommend 5 Hr on site for Meraki MX Appliances with an On-Site engineer to replace the device.

Meraki devices come with standard warranty, which is a replacement parts only service, and can take 2-5 working days to receive the replacement device.

5 Hour replacement On-Site Engineer	Replacement hardware sent to site, **including on-site engineer**, 24 hours per day, 7 days per week including observed holidays, 5-hour replacement. *
5-hour replacement Parts only	Replacement hardware sent to site, **no engineer**, 24 hours per day, 7 days per week including observed holidays, 5-hour replacement. **
Next Business Day On-Site Engineer	Replacement hardware sent to site, **Including on-site engineer**, 8 hours per day, 5 days per week replacement next business day. **
Next Business Day Parts only	Replacement hardware sent to site, **no engineer**, 8 hours per day, 5 days per week replacement next business day. **
Standard Warranty Parts Only	Replacement hardware will be sent to site, **no engineer** and can take 2-5 working days to be delivered ***

The break/fix service level begins at the point when a Claranet engineer determines that a replacement SD-WAN appliance is required.

Wireless Access Points above 3M cannot be replaced by the Meraki engineer, the device will be connected and proven to work, customers will need to arrange for these to be replaced.

* This service is only available in the UK and would be the recommended support option for Meraki Security Appliances.
** This service is only available in the UK
*** Replacement device shipped from the EU and requires customs clearance before delivery to site.

With a 5-hour onsite engineer service level, you can schedule field engineer arrivals any hour of the day/week for sites in UK mainland. Locations considered outside UK mainland are excluded from the 5-hour SLA as this cannot be met, these include Outer Hebrides, Jersey, Southern Ireland, Isle of White, Isle of Man and any other island that requires ferry or flight transport and is dependent on these factors.

Internal cabling between the devices is not covered by the same SLA, unless specified within the contract.

It is not possible to add Meraki Break Fix after 90 days of the installation date, only prior to this date and resign of a network with existing Meraki Break Fix. this is a Meraki policy and not a Claranet one.

7.6.2. Break/fix service – Virtual MX

There is no Break Fix SLA associated with this virtual device. The device will be monitored and managed the same as a physical device.

Responsibility	Claranet	You
Monitor: Monitor Virtual MX devices for up time 24x7x365.	✓	
Cloud environment: Where Claranet are providing the cloud environment we will identify and resolve issues occurring during the life of the contract.	✓	
Cloud environment: Where you are providing the cloud environment you will be responsible for the service, and any faults that occur in this environment during the life of the contract, identified by the device being unavailable on the dashboard, or identified by our Help desk.		✓

7.7. Service Levels

The Service Level determines the parameters by which the service is accountable. Many of the components of your service are designed to operate in a high availability configuration, with which there is an implied acceptance that from time to time an element may fail. Therefore, for high availability options of components, unscheduled downtime is not considered to have occurred if one element fails and another element takes over the workload. The SLA is dependent upon the replacement maintenance package selected and added to the contract.

Component	Source of availability data	Unscheduled downtime identified by	Exceptions	Service level
Single CPE SD-WAN appliance with NBD RMA support	SNMP tests or API integration	Every API test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	Monitoring disabled during maintenance windows.	Next Business Day Replacement
Single CPE SD-WAN appliance with 24x7x5 RMA support	SNMP tests or API integration	Every API test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	Monitoring disabled during maintenance windows.	99% availability
Redundant CPE SD-WAN configuration 24x7x5 RMA Support	SNMP tests or API integration	Every API test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	Monitoring disabled during maintenance windows.	99.95% availability
Single CPE Switch with NBD RMA support	API integration with Meraki dashboard	Every API test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	Monitoring disabled during maintenance windows	Next Business Day Replacement
Single CPE Switch with 24x7x5 RMA support	API integration with Meraki dashboard	Every API test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	Monitoring disabled during maintenance windows.	99% availability
Redundant CPE Switch configuration 24x7x5 RMA Support	API integration with Meraki dashboard	Every API test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	Monitoring disabled during maintenance windows.	99.95% availability
CPE Access Points with NBD RMA Support	API integration with Meraki dashboard	Every API test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	Monitoring disabled during maintenance windows.	99% availability

Component	Source of availability data	Unscheduled downtime identified by	Exceptions	Service level
CPE Access Points with 24x7x5 RMA Support	API integration with Meraki dashboard	Every API test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	Monitoring disabled during maintenance windows.	99% availability
Virtual MX	SNMP tests or API integration	Every API test that does not receive a response = 5 minutes of downtime. Alert is triggered after 3 consecutive, unsuccessful tests	Monitoring disabled during maintenance windows.	99% availability on Claranet managed AWS / Azure environment

If a fault is identified as being with equipment that does not form part of the service e.g., computer, printer, tablet, non-Claranet switch, Internal CAT 5 Cabling, or power supply issues, it will be your responsibility to resolve the issue with the equipment.

If engineer is called out to site and fault not with Claranet supported kit, then the visit may be chargeable.

Access Points above 3M in height cannot be replaced by the Meraki Now engineer, these will need to be replaced by the customer as a scissor lift, platform, or other safety equipment will be required to replace the device.

7.8. Response Times and Ticket Escalation

For more detail please refer to the terms & service detail with the Customer Experience for Managed Services Document (“CXMS”) which can be found on Claranet Online Portal.

8. Appendix

8.1. Data Management

8.1.1. EU Data Privacy

Claranet is committed to data protection, privacy, security, and compliance with applicable regulatory frameworks in the UK and abroad. The cloud-based architecture used by our vendor is designed from the ground up with data protection, privacy, and security in mind.

The technical architecture and its internal administrative and procedural safeguards assist customers with the design and deployment of cloud-based networking solutions that comply with EU data privacy regulations, even in the absence of the US-EU Safe Harbour Framework. The cornerstones of a compliant-by-design architecture are:

- Out-of-band Control Plane
- EU Cloud
- Data Processing Addendum (DPA)
- Privacy Shield
- GDPR

8.1.2. Out-of-band Control Plane

The out of band control plane separates network management data from user data. Management data (e.g., configuration, statistics, monitoring, etc.) flows from SD-WAN appliances to the management platforms over a secure Internet connection. User data (web browsing, internal applications, etc.) does not flow through the management platform, instead flowing directly to its destination on the SD-WAN or across the internet.

The out of band control plane separates network management data from user data. Management data (e.g., configuration, statistics, monitoring, etc.) flows from Cisco Meraki devices (wireless access points, switches and security appliances) to the Cisco Meraki cloud over a secure Internet connection.

User data (web browsing, internal applications, etc.) does not flow through the cloud, instead flowing directly to its destination on the LAN or across the WAN. More information can be found about the above topics, and other detailed information about the security, reliability & privacy information for Meraki cloud service, at **https://meraki.cisco.com/trust**

In the event of a break/fix scenario, or in the instance that an issue cannot be resolved by a trained Claranet engineer, we will escalate a case to Meraki support. All Claranet policies with regards to end-of-life products, licenses, terms of use, etc. Fall in line with the Cisco Meraki Policies – **https://meraki.cisco.com/support/#policies**

8.2. Service Credits

Any time in which the Claranet monitoring system is unable to receive or process monitoring data shall not be assumed to be unscheduled downtime. If you initiate a Service Credit request, this will be put into a process where Claranet coalesce the systems monitoring data and logs with your own record of when and where an outage occurred. The Service Credits will be available for that agreed window. You have the option to dispute records with Claranet, where upon systems monitoring data can be provided to you.

In the event that you and Claranet agree that Claranet has failed to meet any service level guarantee during any given calendar month, Claranet will credit your account with a Service Credit. Service Credits shall apply only to the fee(s) for the affected service(s). Service Credits shall be deducted from the relevant monthly fee due in respect of the second month following the month in which an agreed Service Credit is claimed. The maximum amount of Service Credit a customer can receive in each calendar month relating to this agreement is fixed to 30% of the fee

for the affected Service. The Service Credits issued are liquidated damages and, unless otherwise provided in this agreement, such Service Credits will constitute your sole and exclusive remedy with respect to the failure for which they are payable.

8.2.1. Service availability guarantee

In the event that you believe you are entitled to compensation for the SD-WAN Service in accordance with the Service Levels and in order to obtain your credit simply notify us that you think you are so entitled within thirty (30) calendar days and we will check our Non-availability records, compare them against any Critical calls we previously received from you at our helpdesk and confirm whether any credit is due. In the event we decide credit is due, your entitlement will be applied to the next following monthly invoice in accordance with the tables below.

For components where the service level is 99.99%

Percentage service availability per calendar month	Percentage credit of monthly charge for the variant, for the calendar month in which non-availability occurs
< 99.99% but > 98.99%	5%
< 97.99% but > 97.99%	10%
< 96.99% but > 95.99%	15%
< 95.99%	30%

For components where the service level is 99 %

Percentage service availability per calendar month	Percentage credit of monthly charge for the variant, for the calendar month in which non-availability occurs
< 99% but > 98%	5%
< 98% but > 97%	10%
< 97% but > 96%	15%
< 96%	30%

For components where the service level is next business day

Percentage service availability per calendar month	Percentage credit of monthly charge for the variant, for the calendar month in which non-availability occurs
>24 hours but <36 hours	10%
>36 hours but <48 hours	20%
>48 hours	30%

All SLA’s in this document can only be applied to SD-WAN appliance downtime. Any inability to receive or process monitoring data from an SD-WAN appliance due to an issue with a Claranet

provided connectivity solution will fall in line with any SLA's provided in the Connectivity Components Service Delivery document. In the event of a WAN connectivity failure all compensation claims would fall over to this document and not be relevant to the SD-WAN appliance not being reachable.

8.2.2. Compensation claims

Compensation claims must be submitted, in writing (email or letter), within 30 days from the service level guarantee breach to which they refer. All claims must be submitted to the appointed Account Manager and/or Service Manager. You agree to correct problems and to attempt to minimise the recurrence of problems for which you are responsible that may prevent Claranet from meeting the service level guarantees. Requests for support received by the Service Desk by means other than telephone or request ticket (for example, by fax) will be excluded when calculating service levels.

8.2.3. Exceptions

Claranet excludes responsibility for meeting any service levels to the extent that meeting the service levels is affected by the following items:

- if you are in default under the Agreement.
- in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance.
- in the event that the Service is disrupted due to unauthorised users or hackers.
- in the event that the Service is unavailable due to changes initiated by you whether implemented by you or Claranet on behalf of a customer.
- in the event that the Service is unavailable as a result of you exceeding system capacity.
- in the event that the Service is unavailable due to viruses.
- in the event that the Service is unavailable due to your failure to adhere to Claranet's implementation, support processes and procedures.
- in the event that the Service is unavailable due to the acts or omissions of you, your employees, agents, third party contractors or vendors or anyone gaining access to Claranet's network, control panel; or to your website at the request of a customer.
- in the event that the Service is unavailable due a Force Majeure Event.
- in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy.
- in the event that the Service is unavailable due to any event or situation not wholly within the control of Claranet.

- in the event that the Service is unavailable due to your negligence or wilful misconduct of you, or others authorised by you to use the Services provided by Claranet.
- in the event that the Service is unavailable due to any failure of any component for which Claranet is not responsible, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by you.
- in the event that the Service is unavailable due to any failure local access facilities provided by you; and
- in the event that the Service is unavailable due to any failures that cannot be corrected because you are inaccessible or because Claranet personnel are unable to access your relevant sites. It is your responsibility to ensure that technical contact details are kept up to date by submitting a request ticket to confirm or update the existing the technical contact details.
- In the event where storage thresholds have been breached for three consecutive calendar days, any downtime resulting directly or indirectly from insufficient storage will not be counted in the calculation of availability Service Levels.
- Access Points installed at a height above 3 metres cannot be replaced by our engineers, as they are not trained to work at height, and additional safety equipment will be required to reach these devices.
- In the event that the Virtual MX is not available on your provided AWS / Azure cloud environment it will be your responsibility to resolve the cloud issue.

Exceptions specific to Customer Premises Equipment (CPE) services do not include the correction of any fault due to any of the following occurring by you or your end users:

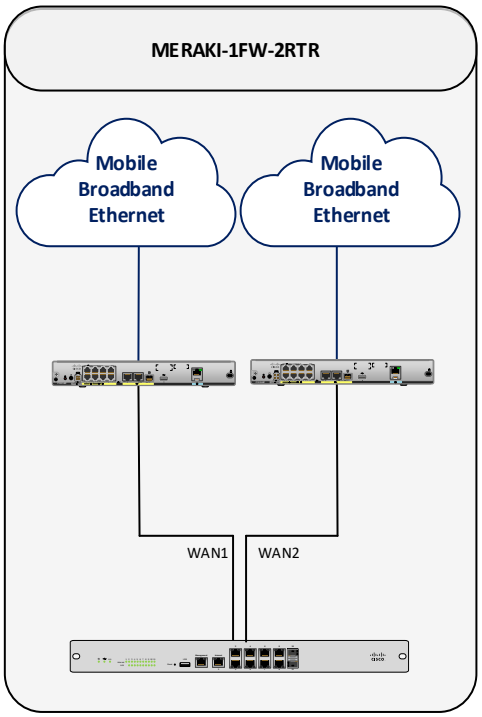
- Failure to maintain a suitable environment for the Equipment at the Place of Use in accordance with industry standard specifications (including without limitation failure to maintain a constant power supply, air conditioning or humidity control).
- Neglect or misuse of Equipment or failure to operate Equipment in accordance with the purposes for which it was designed.
- Alteration, modification, or maintenance of the Equipment by any party other than Claranet or authorised partners.
- Transportation or relocation of Equipment except where it has been performed by or under the direction of Claranet or authorised partners.
- Use of defective or inappropriate supplies (including but not limited to faults caused by the use of non-manufacturer components or modules) with the Equipment.

- Access point(s) do not include hands on support at site. In the event of any technical issues, you will be responsible for providing this support to help identify and resolve any issues related to the wireless.
- Any defect or error in any software used upon or in association with the Equipment.
- Any accident or disaster affecting the Equipment (including without limitation fire, flood, water, wind, lightning, transportation, vandalism, or burglary).
- Electrical work external to Equipment.
- Modification or alteration of an attachment to the Equipment or removal of the same.
- Matters arising before the Commencement Date or after termination of this Agreement.
- User error and physical user damage.
- Painting or refinishing the equipment.
- Software related errors.
- Failures from moves, power surges etc.
- Cabling issues.
- Network faults caused by equipment not included as the Equipment in respect of which the Services are provided.
- In the event that a fault is diagnosed as an Excepted Service you shall, if it requires the Excepted Service, provide a written request to proceed and acceptance of charges quoted. • If on arrival the fault is found to be an Excepted Service Claranet will levy Additional Charges at the standard scale rates in force from time to time.
- Travel and shipping costs outside Mainland UK are an Additional Charge.
- The areas of exclusions due to travel time are highlands of Scotland, Cornwall, West Wales, Cumbria, and locations requiring journey by ferry.
- This agreement does NOT include onsite engineer support for the purpose of and not limited to access point reboot, re-connecting cables, diagnostic fault finding.

8.3. Network Underlay Architecture

8.3.1. Branch Approved Topologies

1xMeraki-MX-2xRouters (MERAKI-1MX-2RTR)

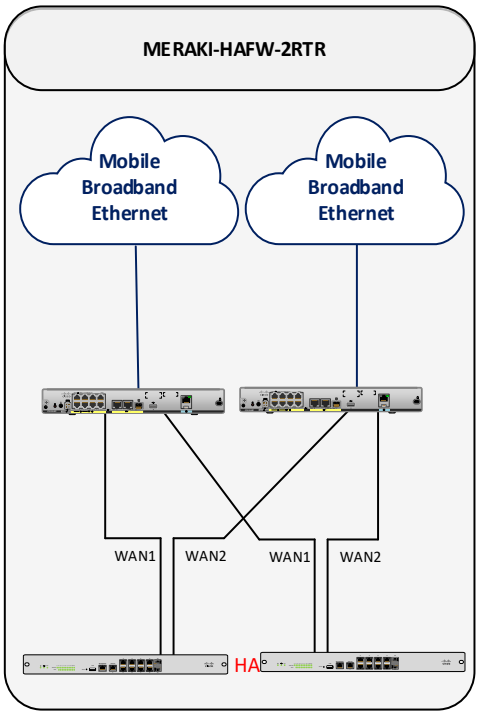


Underlay Connectivity	Circuit Type	Termination	Router Type
Underlay 1	Ethernet Broadband Mobile	Router	Draytek / Cisco
Underlay 2	Ethernet Broadband Mobile	Router	Draytek / Cisco

•Supporting Detail:

- 1 Meraki MX firewall.
- 2 Routers terminating each mobile, broadband or ethernet circuit.
- Active / Active on WAN1 and WAN 2 utilising both links at the same time
- Application prioritization at the MX device
- Cisco or Draytek routers only.
- Public IP Mobile SIM only.
- Single WAN option for Teleworker or Micro branches
- Additional branch LAN switches and Access Points can also be added

Meraki-MX-HA-2xRouters (MERAKI-HA-HA-2RTR)



Underlay Connectivity	Circuit Type	Termination	Router Type
Underlay 1	Ethernet Broadband Mobile	Router	Draytek / Cisco
Underlay 2	Ethernet Broadband Mobile	Router	Draytek / Cisco

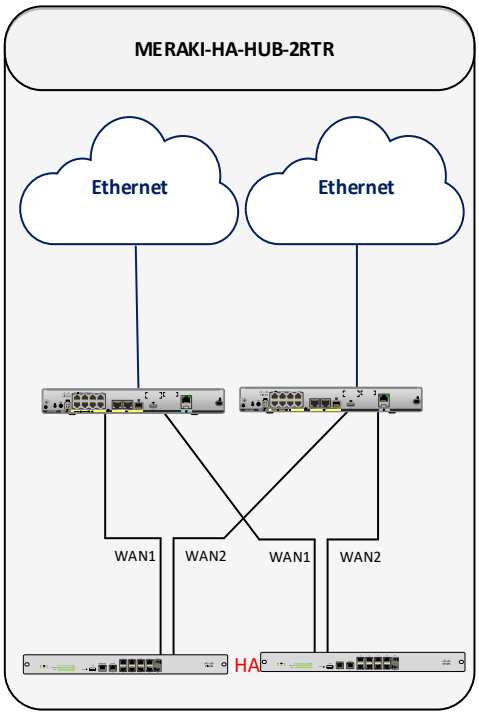
•Supporting Detail:

- 2 Meraki MX HA (Auto switchover between Active and Passive devices)
- 2 Routers terminating each mobile, broadband or ethernet circuit.
- Active / Active on WAN1 and WAN 2 utilising both links at the same time
- Application prioritization at the MX device
- Cisco or Draytek routers only.
- Public IP Mobile SIM only.
- 1 Licence, shared between the Active and Passive device.
- Additional branch LAN switches and Access Points can also be added

8.3.2. Hub Approved Topologies

Approved designs for a single Hub. Additional Hubs can be introduced using a combination or multiples of the same topologies.

Meraki-MX-HA-HUB-2xRouters (MERAKI-MX-HA-HUB-2RTR) – Customer Premises

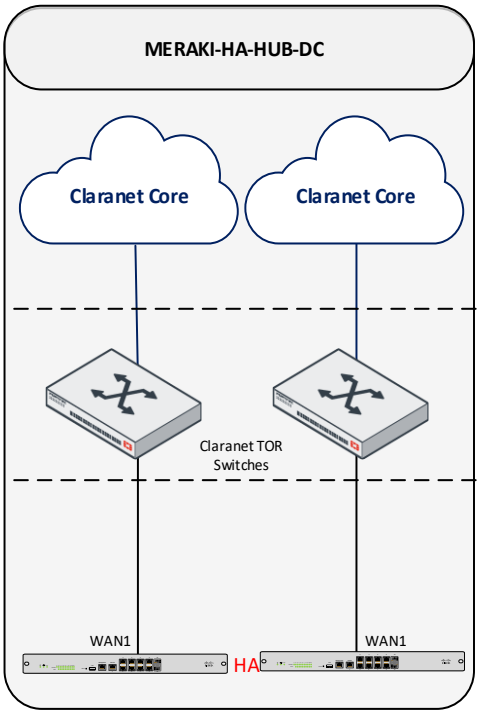


Underlay Connectivity	Circuit Type	Termination	Router Type
Underlay 1	Ethernet	Router	Draytek / Cisco
	Broadband	.	.
	Mobile	.	.
Underlay 2	Ethernet	Router	Draytek / Cisco
	Broadband	.	.
	Mobile	.	.

•**Supporting Detail:**

- 2 Meraki MX HA (Auto switchover between Active and Passive devices)
- MX configured in NAT mode.
- Customer premises only.
- No BGP support.
- Active / Active on WAN1 and WAN 2 utilising both links at the same time
- Application prioritization at the MX device
- 2 Routers terminating each ethernet circuit, recommend these are RA02 / diversely routed circuits
- Mobile or broadband is not recommended for Hub site.
- Cisco or Draytek routers only.
- 1 Licence, shared between the Active and Passive device.
- Additional branch LAN switches and Access Points can also be added

Meraki-MX-HA-HUB-1xUnderlay (MERAKI-MX-HA-HUB) – Claranet DC

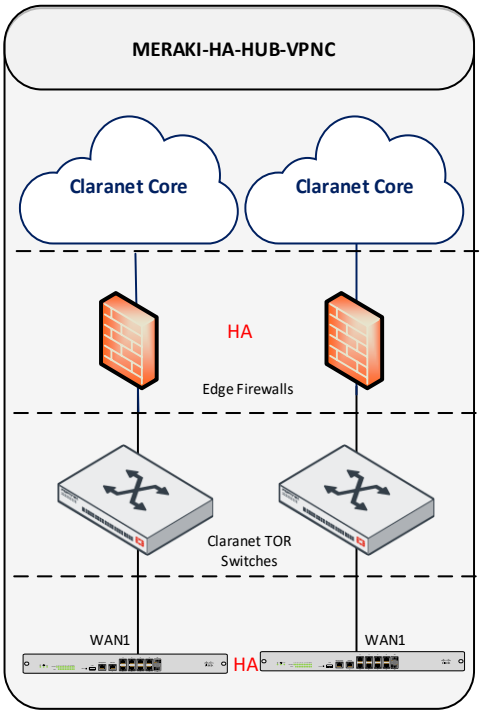


Network Underlay	Circuit Type	Termination	Router Type
Underlay 1	Ethernet	Claranet Core	Claranet Core
	Broadband	.	.
	Mobile	.	.
Underlay 2	Ethernet	.	.
	Broadband	.	.
	Mobile	.	.

•Supporting Detail:

- 2 Meraki MX HA (Auto switchover between Active and Passive devices)
- Firewalls configured in NAT mode.
- No BGP support.
- Only 1 Underlay required due to DC network resiliency.
- 1 Licence, shared between the Active and Passive device.
- Additional LAN switching required in the DC.

Meraki-MX-HA-HUB-1xUnderlay VPN Concentrator (MERAKI-HA-HUB-VPNC) – Claranet DC

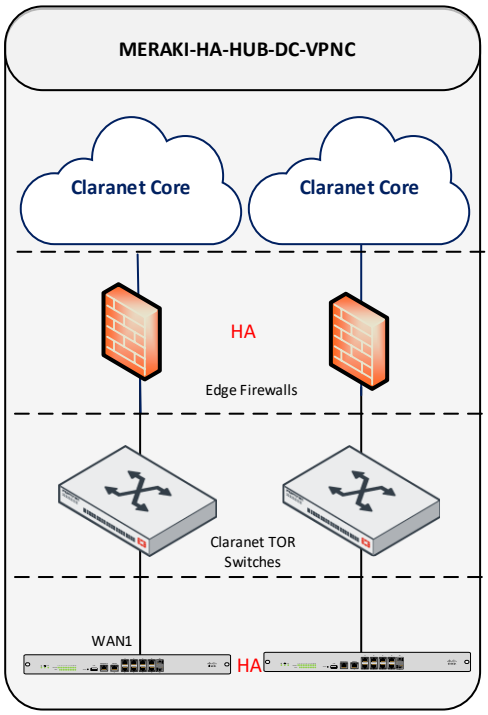


Network Underlay	Circuit Type	Termination	Router Type
Underlay 1	Ethernet	Claranet Core	Claranet Core
	Broadband	.	.
	Mobile	.	.
Underlay 2	Ethernet	.	.
	Broadband	.	.
	Mobile	.	.

•Supporting Detail:

- 2 Meraki MX HA (Auto switchover between Active and Passive devices).
- MX devices configured in VPN Concentrator mode (1 ARM).
- 2 Edge Firewalls that support BGP in HA.
- BGP supported allowing for dynamic route propagation when integrating with cloud environments (MPLS, Public and Private cloud).
- Firewalls patched in to Claranet DC TOR switches.
- Only 1 Underlay is required due to DC network resiliency.
- 1 Licence, shared between the Active and Passive device.
- Additional LAN switching required in the DC.

Meraki-MX-Distrubuted-HA-1xUnderlay VPN Concentrator (MERAKI-MX-DIS-HA-HUB-VPNC) – Claranet Datacentre

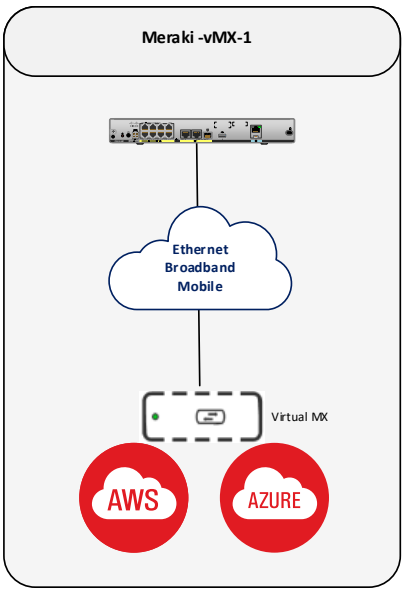


Network Underlay	Circuit Type	Termination	Router Type
Underlay 1	Ethernet	Claranet Core	Claranet Core
	Broadband	.	.
	Mobile	.	.
Underlay 2	Ethernet	.	.
	Broadband	.	.
	Mobile	.	.

•Supporting Detail:

- 2 Meraki MX HA, 1 in each geo-separated DC.
- MX devices configured in VPN Concentrator mode (1 ARM).
- 2 Edge Firewall that support BGP.
- BGP supported allowing for dynamic route propagation when integrating with cloud environments (MPLS, Public and Private cloud).
- Firewalls patched in to Claranet DC TOR switches.
- Only 1 Underlay is required due to DC network resiliency.
- Additional LAN switching required in the DC.

Meraki Virtual MX



Network Underlay	Circuit Type	Termination
Site Connection	Ethernet	Virtual MX
	Broadband	Virtual MX
	Mobile	Virtual MX

•Supporting Detail Single vMX - Single Cloud: (Customer Setup)

- 1 Virtual MX will connect to the cloud Service (AWS or Azure).
- Throughput either 200MB, 500Mb or 1GB (AWS Only) based on license selected. Maximum number of concurrent tunnels is - Small 50, Medium 250, and Large 1000.
- vMX is set in Hub / Concentrator mode.
- Sites connecting to the Hub in Spoke Mode, and connection to the desired vMX configured.
- Auto VPN between satellite sites and the vMX (configured on the Dashboard)
- Customer provided cloud connectivity.
- Customer provided cloud setup, installation of the vMX application, and routing.

•Supporting Detail Multi vMX - Multi Cloud: (Customer Setup)

- Multi vMX support, requires a vMX license per Cloud Connection.
- Hub / Concentrator priority to be set for each Satellite Site connecting to the vMX, priority does not have to be the same for all sites if load-balancing is required.
- HA pair within cloud requires cloud environment to be setup in HA mode
- AWS and Azure supported, as well as Multiple AWS and Multiple Azure
- Customer provided cloud connectivity.
- Customer provided cloud setup, installation of the vMX application, and routing.

8.4. Network Overlay Architecture

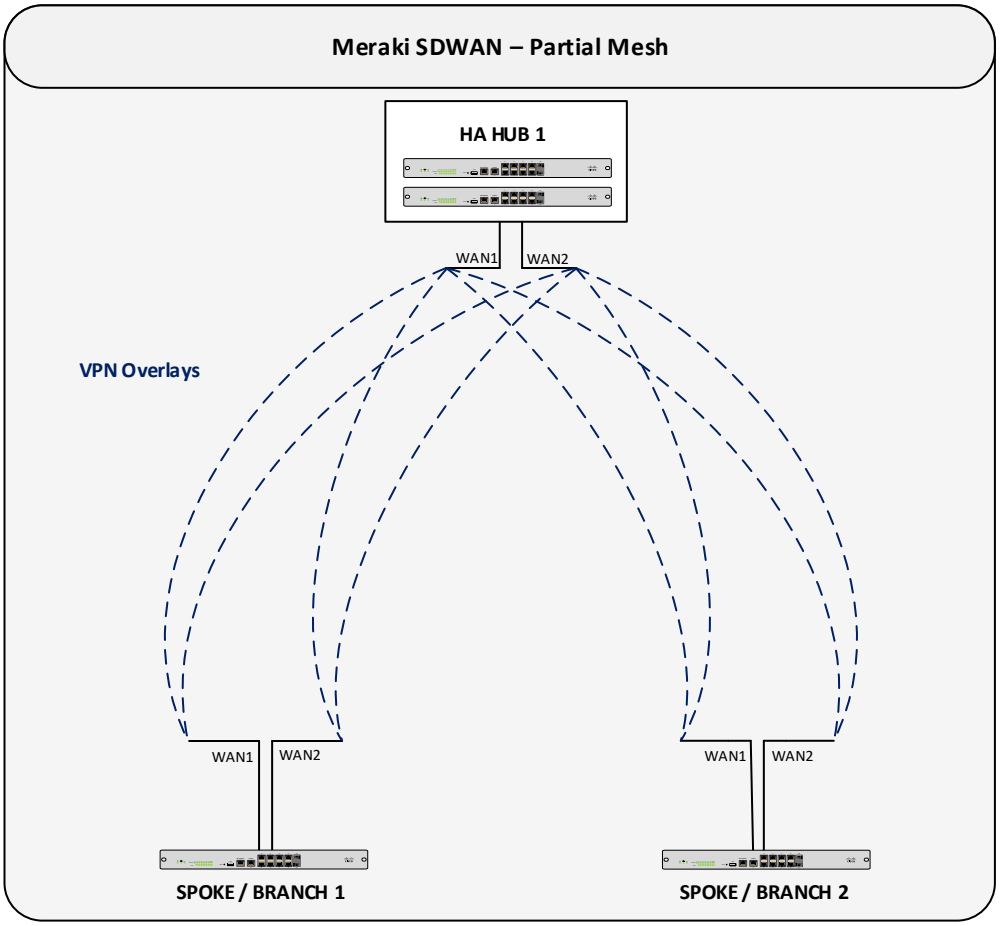
The network overlay also known as a virtual or VPN overlay provides a secure form of transport between SD-WAN enabled locations using the network underlay.

These topologies have been technically verified as a standard deployable topology with all the dependencies recognised and delivery processes understood and documented. Any requirements that fall outside of these will need to be designed by our architects and requested for approval using our design review process.

8.4.1. Hub and Branch Partial Mesh

Use Case:

Predominantly for forcing all VPN Overlay communication through the Hub site or isolating branch locations for enhanced security.



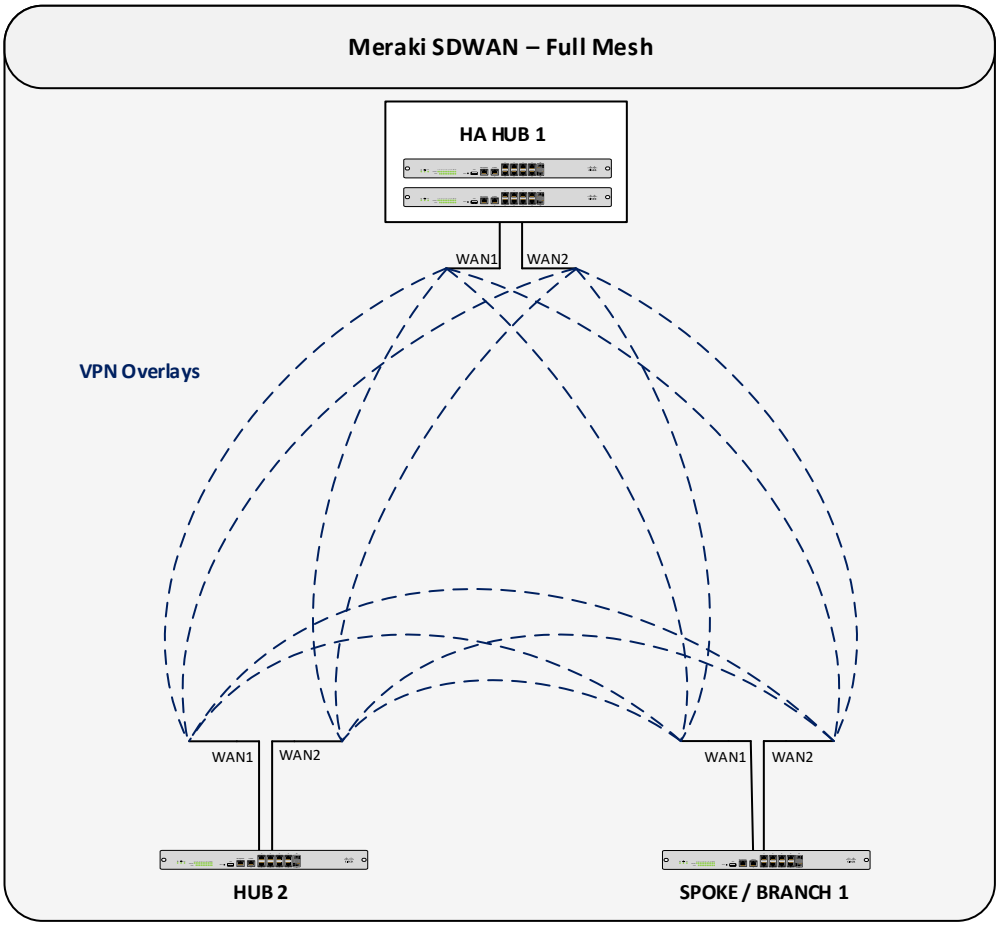
A Hub and Branch partial mesh topology is configured as standard. All Branch-to-Branch traffic will traverse the Hub.

Branch to Branch access can be disabled to isolate and enhance security at each location.

8.4.2. Hub and Branch Full Mesh

Use Case:

Hub and Branch design where direct Branch to Branch communication is required.



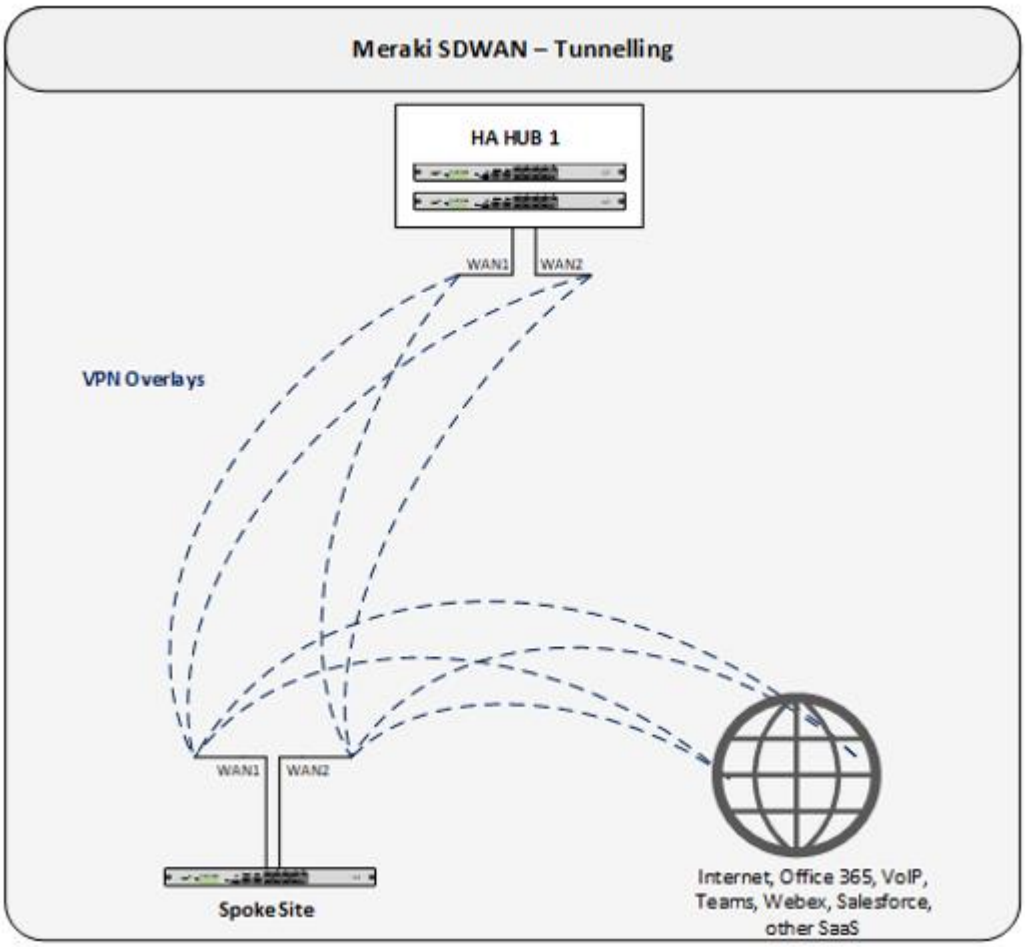
Sites that's require direct communication are configured as Hub's creating a full mesh of tunnels between Hub and Hub and Branch and Hubs. Sites that are configured as spokes and require communication with other spokes will traverse the hubs in priority order.

8.4.3. Tunnelling

Use Case:

Local branch, where AutoVPN connects to hub / Data Centre / Concentrator or a Meraki vMX, but localised internet Breakout enables access to www and web / SaaS based applications not going to the Hub and out to the Internet. Recommendation is that Advanced Security licence is used as a minimum for the branch site as this includes L3 and L7 Firewall, Content Filtering, IPS/IDS, and

Anti Malware. This is aligned to Cisco TALOS security and updates are automatically deployed once these are on general release.



8.5. Performance SLA

Performance Service Level Agreements (health checks) are applied to network underlay uplink interfaces. Thresholds are configured to mark Interfaces as down if performance SLA's falls below a set criterion forcing either existing sessions or new sessions over a better optimised path.

Meraki Underlay health checks use a combination of or DNS, Internet, and ARP tests.

- **DNS test**
    - Query the DNS servers (primary or secondary) configured on the internet interface for the following hosts:
        - meraki.com
        - google.com
        - yahoo.com

- **Internet test**
    - Pings to either 209.206.55.10 or 8.8.8.8. One ping per second.
    - Uses a round-robin technique to send an HTTP GET to **http://meraki.com** or **http://canireachthe.net**. An HTTP response of any kind will result in a success.
- **ARP test**
    - ARP for the default gateway and its own IP (to detect a conflict).

It can take approximately five minutes for failover to occur in the event of a soft failure (where the physical link is still up but provides no internet access).

The VPN Overlay performance probe use a small payload (approximately 100 bytes) of UDP data sent over all established VPN tunnels every 1 second. MX appliances track the rate of successful responses and the time that elapses before receiving a response. This data allows the MX to determine the packet loss, latency, and jitter over each VPN tunnel to make the necessary performance-based decisions.

The VPN Overlay will failover if underlay interface members fail or performance falls below a configured custom performance class. Custom performance classes can be configured to set thresholds for latency jitter and packet loss.

It is not possible to amend the probe destination or frequency, only apply custom performance classes to flows.

Performance SLA Matrix:

Network Underlay/Overlay	Service Element	Default	Configurable
WAN Underlay	Protocol	DNS, ICMP, HTTP, ARP	No
	Destination Server	Multiple	No
	Packet Loss	100%	No
	Jitter	0 - NA	No
	Latency	0 - NA	No
	Failover	< 300 Seconds	No
	Fail Back	< 30 Seconds	No
	Application	All Internet	No
VPN Overlay	Protocol	UDP	No
	Destination Server	SD-WAN appliance	No
	Packet Loss	100%	Yes
	Jitter	0 - NA	Yes
	Latency	0 - NA	Yes
	Failover	< 40 Seconds	No
	Fail Back	< 40 Seconds	No
	Application	All Hub and Branch	Yes, per policy

8.6. SD-WAN - Policies

Claranet's default SD-WAN policy is to load balance all sessions using round robin to the Internet or Hub locations where the network underlays are of equal cost such as two ethernet or two SOGEA circuits. Circuits that are not of equal cost such as an Ethernet with SOGEA will adopt an Active/Passive approach routing all session over the Ethernet Underlay unless it fails.

Custom SD-WAN policies (flow preferences) can be configured with our premium service packages. The type of traffic is identified by IP Address, port or protocol and directed via a specific underlay or overlay.

Custom performance classes can be configured to set thresholds for latency jitter and packet loss. These can be applied to VPN overlay flow preferences only.

Meraki SD-WAN Claranet Default Policies

Network Under/Overlay	Source	Destination	Service Element	Default	Configurable
VPN Overlay	All Local IP Addresses	All Hub and Branch Addresses	Equal Cost Underlays	Active / Active (Load Balance)	Yes
			Unequal Cost Underlays	Active / Passive	Yes
			Balancing Method	Sessions	No
			Balancing Hash	Round Robin	No
WAN Underlay	All Local IP Addresses	All Internet Addresses	Equal Cost Underlays	Active / Active (Load Balance)	Yes
			Unequal Cost Underlays	Active / Passive	Yes
			Balancing Method	Sessions	No
			Balancing Hash	Round Robin	No

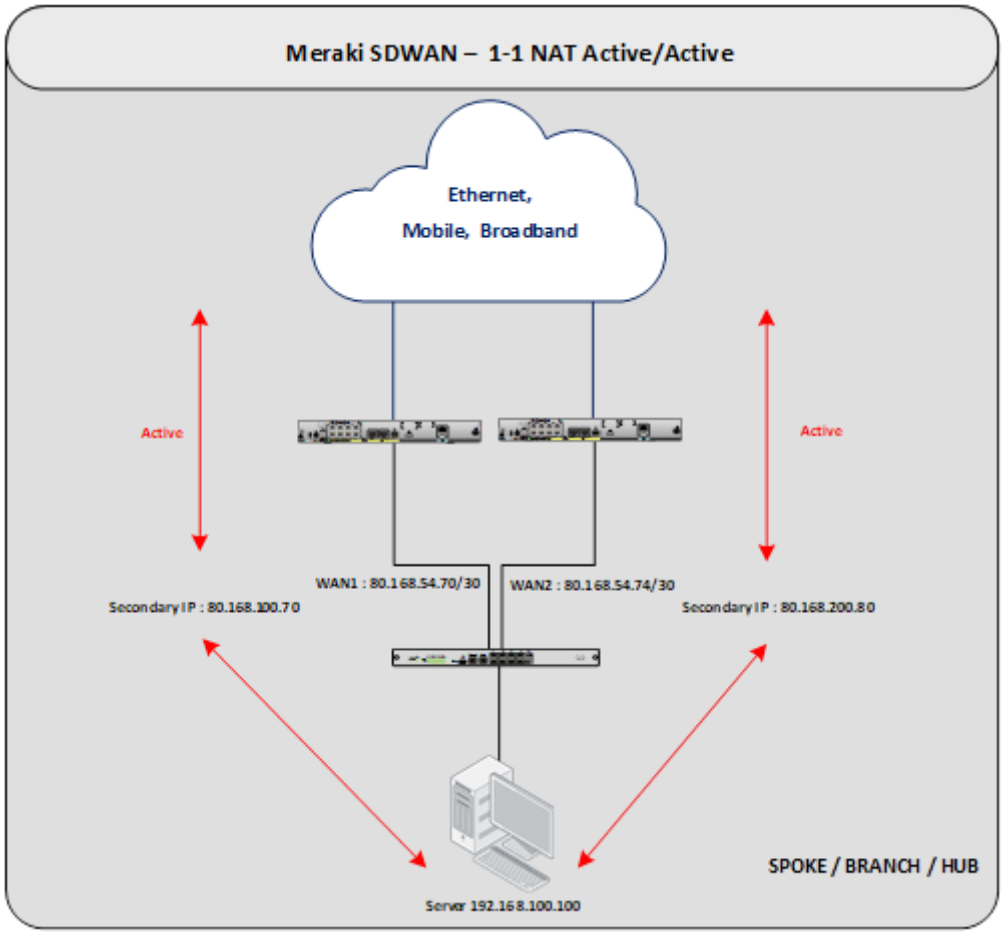
8.7. SD-WAN - Network Address Translation (NAT)

It's important to consider NAT when migrating from traditional MPLS breakout firewalls to SD-WAN or scoping new solutions that could require inbound services.

With SD-WAN there is no routing relationship between network underlays. They each have their own unique addresses ensuring traffic is routed back via the same circuit.

Secondary ranges used for 1-1NAT relationships between a public IP and client/server private IP are supported and failover is dependent on the architecture.

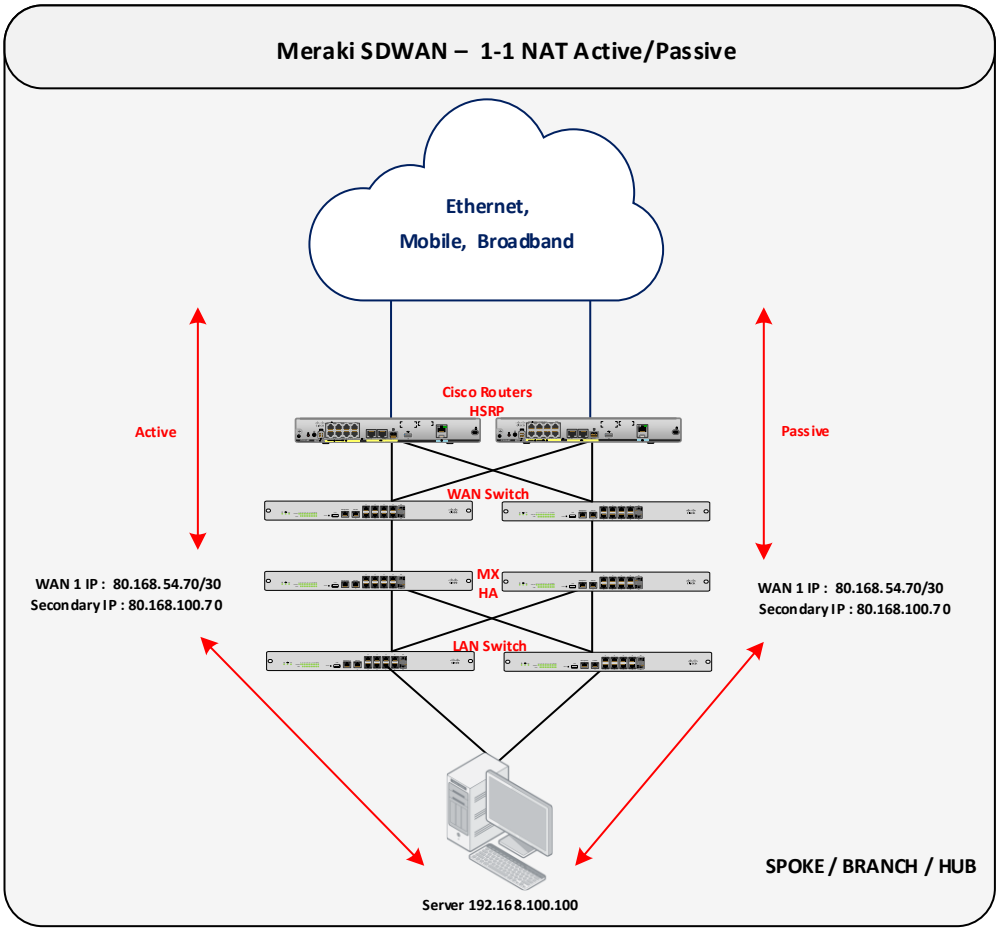
Meraki 1-1 NAT Active / Active



Egress Traffic from the client server is NAT outbound to a unique secondary public IP associated with the egress interface. The interface will depend on outbound load balancing or interface preference unless the uplink fails. All other egress traffic will use the egress interface public IP.

Ingress initiated traffic is directed at the secondary public IP of each underlay which NAT's through to the client/server private IP. If the service is publicly available such as a website, a manual failover of DNS or global load balancing service will be needed to probe the server for an active connection. In this case it would be preferable to adopt a traditional active passive network underlay architecture.

Meraki 1-1 NAT Active / Passive – Customer premises



A fully resilient Active/Passive architecture uses 1 network underlay uplink connecting via a WAN switch into a pair or Cisco routers running HSRP.

Egress Traffic from the client/server is NAT outbound to a unique secondary public IP associated with the egress interface. All other egress traffic will use the egress interface public IP. Load balancing or preferential flows is not supported.

Ingress initiated traffic is directed at the secondary public IP Natting through to the client/server. All public IP's will failover to the secondary circuit in the event of failure (Approximately 15 seconds for Ethernet and 300 seconds for mobile and broadband).

Meraki 1-1 NAT Active / Passive – Claranet DC

A fully resilient Active/Passive architecture located in a Claranet DC uses 1 network underlay connected to a resilient infrastructure. This operates like the customer premises architecture but doesn't require any switches or routers.

An Active/Passive approach is the recommend architecture.

8.8. SD-WAN - Cloud Integration (vMX)

Meraki SD-WAN appliances can be integrated into a public cloud, private cloud, MPLS or third-party networks. Cloud deployment – Meraki MX virtual instance configured as a Hub in public cloud such as AWS or Azure.

Onward routing – Meraki MX configured as a Hub in a Claranet datacentre protecting private cloud, MPLS, public cloud express routes or third-party VPN/interconnects.

Dynamic route propagation requires a Meraki MX configured in VPN concentrator mode and edge firewall handling security and address translation (see Meraki Hub approved topologies).

The table below details the total throughput the vMX will support on the cloud platforms:

Cloud Service	vMX Small 200Mb	vMX Medium 500Mb	vMX Large 1Gb
Microsoft Azure	Yes	Yes	No
Amazon Web Services	Yes	Yes	Yes

Installation guides for the vMX for the individual cloud platforms can be found on the following links.

- **Microsoft Azure**
- **Amazon Web Services**

8.9. SD-WAN - MX Branch Devices – Sizing guide

	MX67 / MX68	MX75	MX85	MX95	MX105	MX250	MX450
Maximum Site to Site VPN Tunnel Count	50	75	200	500	1,000	3,000	5,000
Recommended Maximum Site to Site VPN Tunnel Count	50	75	100	250	500	1,000	1,500
Maximum Number of Client VPN Tunnels	50	75	100	250	250	500	500
WAN Failover	< 5 Sec	< 5 Sec	< 5 Sec	< 5 Sec	< 5 Sec	< 5 Sec	< 5 Sec
Auto VPN Tunnel Failover	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second
Dynamic Path Selection	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second	Sub-second
NGFW Throughput RFC2544-1518 Byte	600 Mbps	1 Gbps	1 Gbps	2.5 Gbps	5 Gbps	7.5 Gbps	10 Gbps
NGFW Throughput EMIX	600 Mbps	1 Gbps	1 Gbps	2.5 Gbps	5 Gbps	7 Gbps	10 Gbps
Advanced Security Throughput (Prevention) EMIX	300 Mbps	500 Mbps	500 Mbps	1.5 Gbps	2 Gbps	1.5 Gbps	3.5 Gbps
Advanced Security Throughput (Detection) EMIX)	400 Mbps	1 Gbps	1 Gbps	2 Gbps	2.5 Gbps	3.5 Gbps	7 Gbps
Single Tunnel VPN Throughput RFC2544 1400 Byte	400 Mbps	1 Gbps	1 Gbps	2.0 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps
Multi-Tunnel VPN Throughput RFC2544 1400 Byte	≤ 400 Mbps	1 Gbps	1 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps	4.5 Gbps
Single Tunnel VPN Throughput EMIX	300 Mbps	1 Gbps	1 Gbps	1.5 Gbps	2 Gbps	2 Gbps	3 Gbps
Multi-Tunnel VPN Throughput EMIX	≤300 Mbps	≤ 1 Gbps	≤ 1 Gbps	≤ 1.5 Gbps	≤ 2 Gbps	≤ 2 Gbps	4.5 Gbps

	MX67 / MX68	MX75	MX85	MX95	MX105	MX250	MX450
WAN Interface WAN **	2x GbE RJ45 (uses one Lan port)	1x GbE SFP 2x GbE RJ45	2x GbE SFP 2x GbE RJ45 (1x PoE+)	2x 10GbE SFP+ 2x 2.5GbE RJ45 (1x PoE+)	2x 10GbE SFP+ 2x 2.5GbE RJ45 (1x PoE+)	2 x 10GbE SFP+	2 x 10GbE SFP+
LAN Interface	4 x MX67 10 x GbE RJ45 (2 x PoE+)	10x GbE RJ45 (2x PoE+)	8x GbE RJ45 2x GbE SFP	4x GbE RJ45 2x 10GbE SFP+	4x GbE RJ45 2x 10GbE SFP+	8 x GbE (RJ45) 8 x GbE (SFP) 8 x 10GbE (SFP+)	8 x GbE (RJ45) 8 x GbE (SFP) 8 x 10GbE (SFP+)
Mounting	Desktop or wall	Desktop or wall	1U rack	1U rack	1U rack	1U rack	1U rack
Power (idle/max)	6W / 17W MX67 12W / 96W MX68	12W / 96W	12W / 55W	42W / 109W	53W / 123W	105W / 190W	105W / 190W

** Only 2 WAN connections permitted, 1 SFP and 1 RJ45 or 2 x RJ45. 1G services presented on Fibre connections therefore the terminating device will need an SFP to connect into the 1G service irrespective of Port speed. MMF for network connection or MMF/SMF in data centres dependent upon DC supplier.

Click here for the **Meraki Sizing Guide**

8.10. SD-WAN - End of life / replacement devices

Device	End of Sale date	End of Support date	Replacement
MX60	24 Oct 2015	24 Oct 2022	MX67
MX60W	24 Oct 2015	24 Oct 2022	MX67W
MX64	26 July 2022	26 July 2027	MX67
MX64W	26 July 2022	26 July 2027	MX67W
MX80	30 Aug 2016	30 Aug 2023	MX85
MX84	31 Oct 2021	31 Oct 2026	MX85
MX100	1 Feb 2022	1 Feb 2027	MX95 or MX105
vMX100	22 Dec 2020	22 Dec 2027	vMX (S/M/L)
Z3C	11 Feb 2024	11 Feb 2029	Z4C
Z3	4 Sep 2024 *	4 Sep 2029	Z4

8.11. SD-LAN - End of life / replacement devices

Device	End of Sale date	End of Support date	Replacement
MS220-8	28 July 2018	28 July 2025	MS225 / MS250
MS220 series	29 Jul 2017	29 July 2024	MS225 / MS250
MS320 Series	31 Mar 2017	31 Mar 2024	MS350 / MS355
MS420	31 Oct 2016	31 Oct 2023	MS425 / MS450

8.12. Wi-Fi - End of life / replacement devices

Device	End of Sale date	End of Support date	Replacement
MR12	24 Oct 2015	24 Oct 2022	**MR28**
MR16	31 May 2014	31 Mar 2021	**MR28**
MR18	13 Feb 2017	31 Mar 2024	**MR28**
MR20	13 Jul 2023	13 Jun 2028	**MR28**
MR24	31 May 2014	31 May 2021	**MR28**
MR30H	31 May 2022	26 Jul 2027	**MR36H**
MR33	21 Jul 2021	21 Jul 2026	**MR36**
MR34	31 Oct 2016	31 Oct 2023	**MR36**
MR42	21 Jul 2021	21 Jul 2026	**MR44 / MR46**
MR42E	21 Jul 2021	21 Jul 2026	**MR46E**
MR45	21 Jul 2021	21 Jul, 2026	**MR46**
MR52	21 Jul 2021	21 Jul 2026	**MR56**
MR53	21 Jul, 2021	21 Jul 2026	**MR56**
MR53E	21 Jul 2021	21 Jul 2026	**MR46E**
MR62	17 Nov 2017	15 Nov 2024	**MR56**
MR66	15 Nov 2017	15 Nov 2024	**MR56**
MR70	19 Feb 2024	19 Feb 2029	**MR76 or MR78**
MR72	30 Apr 2017	31 Jul 2024	**MR76**
MR74	21 Jul 2021	21 Jul 2026	**MR76**
MR84	21 Jul 2021	21 Jul 2026	**MR86**

* End of sale date however this may be brough forward if stock levels are exhausted.

End of sale is the date Cisco Meraki will no longer accept new orders.

End of support is the date Cisco Meraki will no longer accept TAC cases on the devices and will not replace these if faulty. Software licences extending beyond these dates will continue and the devices will be operational until the licence expires, or the device fails.

Licence renewal is not to exceed the end of support date for managed networks.