Maya Installation Planning Guide

Maya Global Solutions (Maya) provides Internet Quality Service™ (IQS) as a service solution that enables enterprises to achieve consistent quality over conventional Internet connections. Using the Maya solution, enterprises can dramatically improve the quality of their business communications services including voice and videoconferencing as well as other cloud-based applications.

This planning guide describes deployment considerations when installing a Maya Network Device at a site.

Maya M24 Network Device

Front angle view

Front view

Back view

What Does Maya Do?

Maya improves Internet quality and performance by Streamlining Internet traffic in and out of an enterprise site. The enterprise site might be a main office, a branch office, single-site office, or even the home office of an employee. Maya manages the "last mile" of Internet traffic – that is the traffic between the site and the ISP's (Internet Service Provider's) high bandwidth Internet backbone.

It is the last mile where congestion occurs, creating quality issues. All site traffic is directed to the cloud-based Maya service, and Streamlining is performed between the Maya cloud and the site. The site's Maya cloud service is located nearby, not actually at the ISP, as congestion rarely occurs on the backbone between the ISP and the Maya cloud.

Maya IQS Streamlining performs several functions. These are the major ones:

- Eliminating network congestion
- Reducing traffic delays for all traffic
- Prioritizing interactive traffic
  - Voice and videoconferencing
  - Cloud-based applications
  - Limiting jitter
  - Ensuring high quality
- Maya Enterprise LAN interconnecting enterprise sites with IQS VPNs (Virtual Private Networks)

Maya Solution

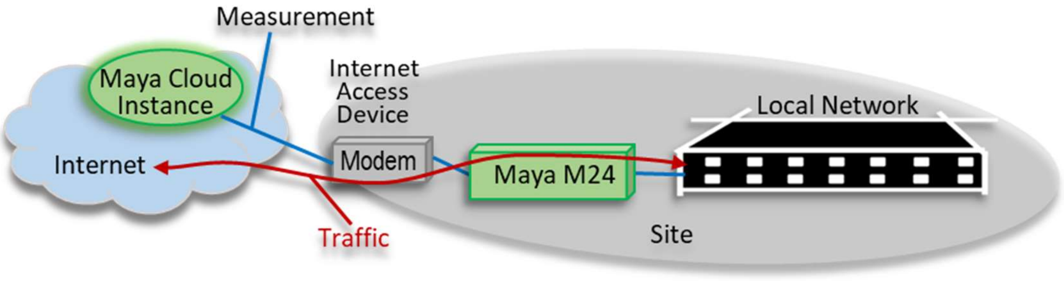
The Maya solution comprises three modules:

- *Maya Network device*. The Maya device is installed on premises and is 5.3" W x 5.5" D x 1.5" H in size. It is inserted in-line with the site network and connects to the Maya cloud service – a Maya Cloud Instance.
- *Maya Cloud Instance*. The Maya cloud is a virtual machine in a data center connected to nearby Maya premises devices. The Maya Cloud Instance and Maya premises devices work together as a pair to provide IQS and Streamlining.
- *Maya Control Center*. The Control Center provides a web interface for configuration and reporting. The Portal provides configuration information for Maya premises and Maya Cloud Instances and collects traffic data from both premises and cloud.

Maya Design and Architecture

Premise Mode Operation

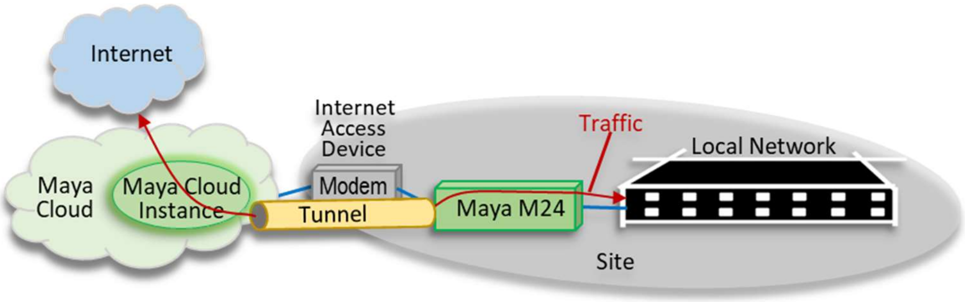
The Maya premises device is installed in-line with a site's Internet WAN connection(s) with all Internet traffic entering and exiting the site passing through it. Maya calls its conditioning of traffic Streamlining. Streamlining involves shaping packet traffic. To do the shaping, the packets must pass through the Maya premises and on to the Internet. This mode of operation is called ***Premise Mode***, as illustrated in the figure below.



Maya Premise Deployment Model

Cloud and Premise Mode Operation

Customers can be provided with a secure VPN tunnel to the Maya Cloud by configuring the device in ***Cloud and Premise Mode***. The Maya device constructs one or more tunnels to a Maya Cloud Instance in the Maya Cloud as shown in the figure below.



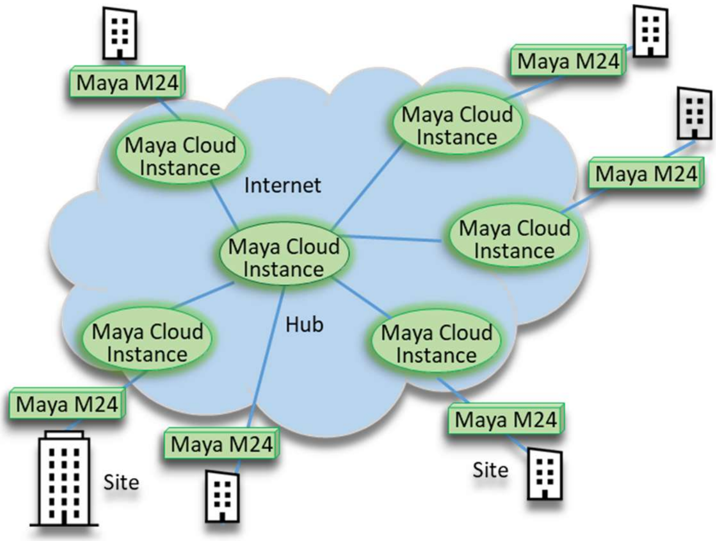
Maya Cloud and Premise Deployment Model

Notice that Enterprise traffic does take an extra hop by going through the Cloud Instance. Locating the Maya cloud within 25ms to 30ms of a site is minimally noticeable while reducing delays and jitter for all traffic. There are several Maya Cloud Instances around the United States. The computation required for encryption does limit the maximum network speed.

Tunnels are continuously tested and maintained. If a WAN becomes unstable with high packet loss, tunnels may be down for a period until the WAN stabilizes. Traffic will continue to flow to destinations while a tunnel is down, but of course Streamlining will not be performed.

Maya Enterprise LAN

Maya premises devices can provide the equivalent of a meshed network of VPNs with connectivity and security. The Maya Enterprise LAN is similar to an encrypted MPLS network at a lower cost with higher speeds when using the public Internet. The diagram below illustrates the Maya Enterprise LAN.

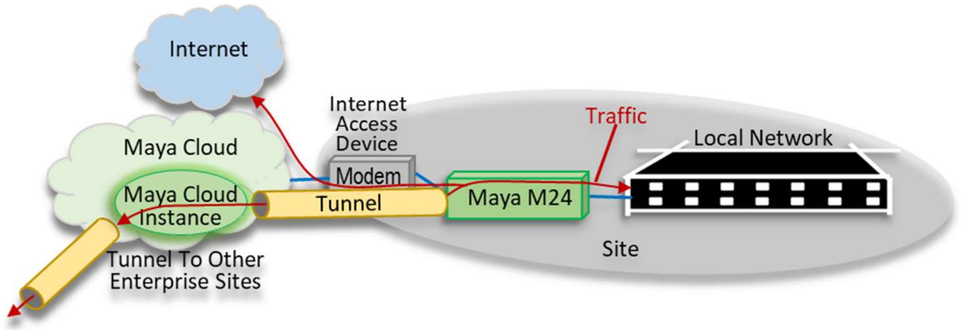


Maya Enterprise LAN

The Maya Enterprise LAN can be deployed with multiple ISPs and different bandwidths. Configuration requires selecting the ***Enterprise LAN*** checkbox in the Maya Control Center, which sets up the routing for an enterprise-wide network. Streamlining is provided to each site in addition to securely interconnecting all sites with Maya premises devices installed.

Split Tunnel Operation

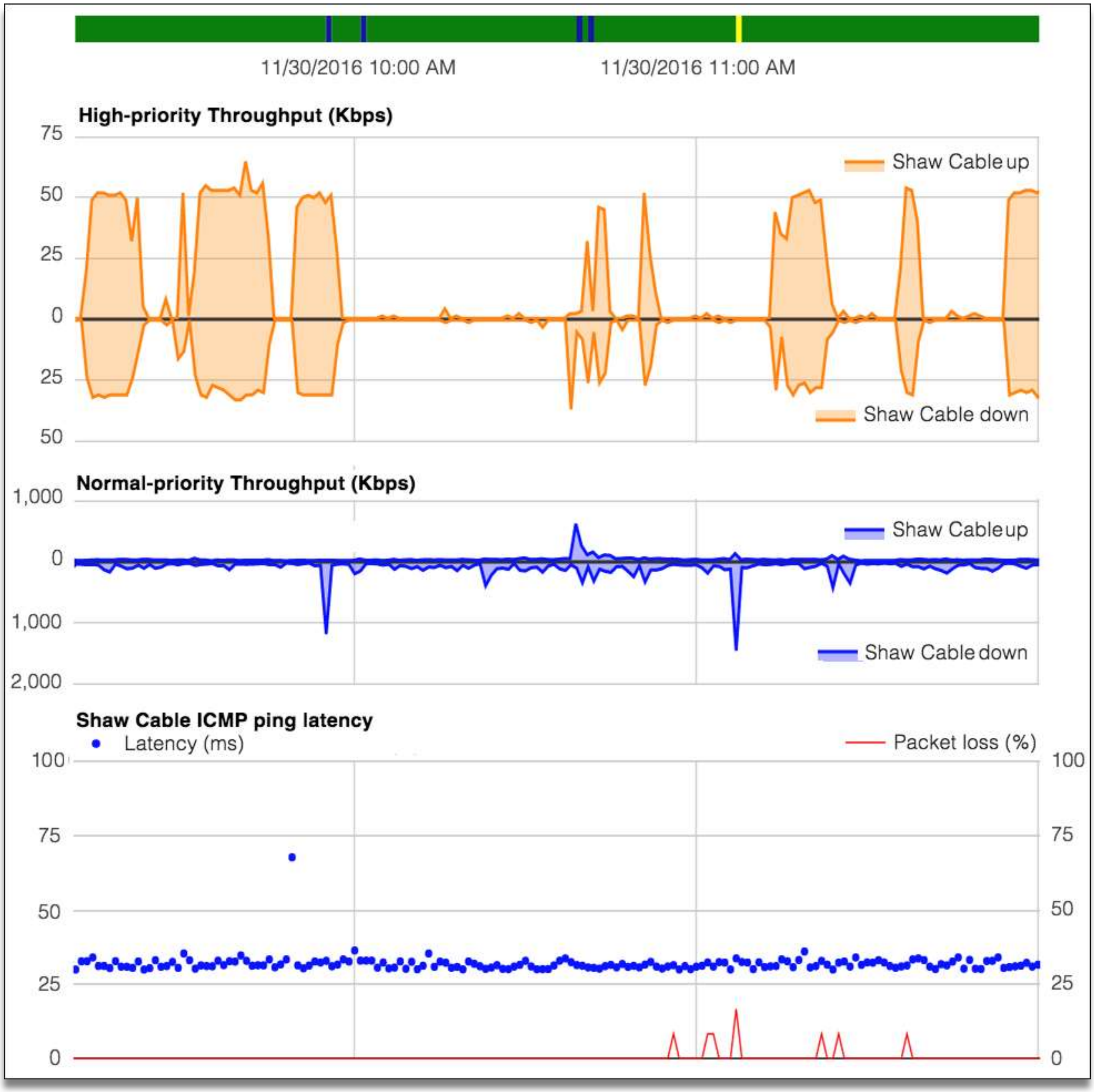
Operating the Maya device in *Premises mode* along with Enterprise LAN is known as a Split Tunnel. The enterprise traffic is directly through tunnel while Internet bound traffic bypasses the tunnel. Split tunnel operation provides connectivity and security among enterprise sites while retaining maximum Internet performance and no additional latency. Split tunnel is shown in the illustration below.



Maya Split Tunnel Operation

Streamlining

Once deployed the Maya IQS Streamlining is always operating. The Maya Control Center shows operating status continuously and is available to customers, Maya resellers, and Maya Operations. A sample Control Center screenshot is shown below.



Sample Control Center screenshot

In the above example, the green stripe at the top is a timeline indicating a normal status – traffic is being streamlined with high quality. The yellow bar within the green indicates borderline quality (a 1-minute interval in this case), while blue bars indicate Streamlining optimized the connection to reduce congestion and preserve high quality for interactive traffic.

The top graph with orange and tan colors shows the high priority traffic, both upstream and downstream. This example shows several phone calls over the period, one call at a time, and most likely with a G.729-compressed codec as its bandwidth is about 30Kbps. The middle graph in dark blue and lighter blue colors show the normal priority traffic, also both upstream and downstream. Normal traffic tends to be predominantly downstream as can be seen in this example. High priority traffic is frequently bi-directional and more nearly balanced, also the case in the above example.

The third graph at the bottom shows the latency for ICMP keep-alive packets within the tunnel. Consistent latency tends to be an indication of a well-performing network connection and is seen above in a nearly solid line of blue dots. Irregular and high latency (greater than 150ms) indicates an unstable connection likely to be demonstrating poor quality. There are only a few dots well above the line, which means this is a well-performing network. The red triangle lines show the percentage of lost packets during time intervals. The lost packets in this case are typical of cable modems, that tend to drop packets occasionally, and sometimes when there is no traffic. The above example is normal, and quality is being met for both normal and high priority applications.

Privacy

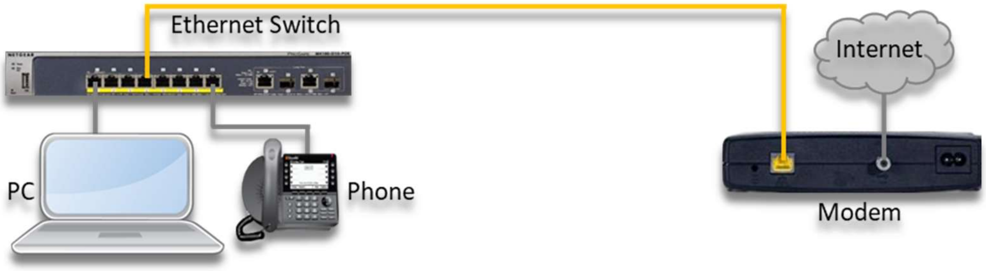
Maya is in-line with all site traffic and must examine each packet in order to perform Streamlining. Streamlining is a combination of prioritization and queue management. All packet headers are examined and categorized based on their protocol type, source and destination IP addresses, and port numbers. No payload data – any part of the actual content, is examined nor retained. Streamlining is done entirely by header inspection. Maya records packet statistics – number of packets, number of bytes per minute, latency, jitter and loss. Statistical data is maintained for analysis and is visible via the Maya Control Center as illustrated in a section above.

Deployments

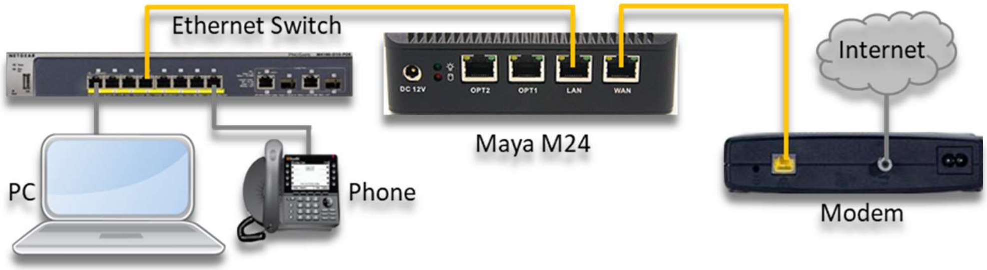
There are a few considerations to be taken when deploying Maya. They are listed and described below.

Simplest Configuration

Small sites typically consist only of a modem – cable or DSL for example, an Ethernet switch, Wi-Fi access point(s), PCs, IP phones and other equipment such as printers. For these configurations, the Maya premises device is placed between the modem and the Ethernet switch. A before and after figure is shown below.



Simplest Configuration Before Maya Premises Deployment



Simplest Configuration After Maya Deployment

The Maya premises device can utilize either DHCP for an IP address or a manually configured static IP. The Maya premises device needs DNS address, default route, and netmask from the DHCP server, normally in the ISP's modem. The Maya premises device itself in turn can optionally provide DHCP service to the local site equipment – Ethernet Switch, Phones, and PCs in the above illustration. Maya DHCP can be disabled in the case that local equipment is providing DHCP for the site.

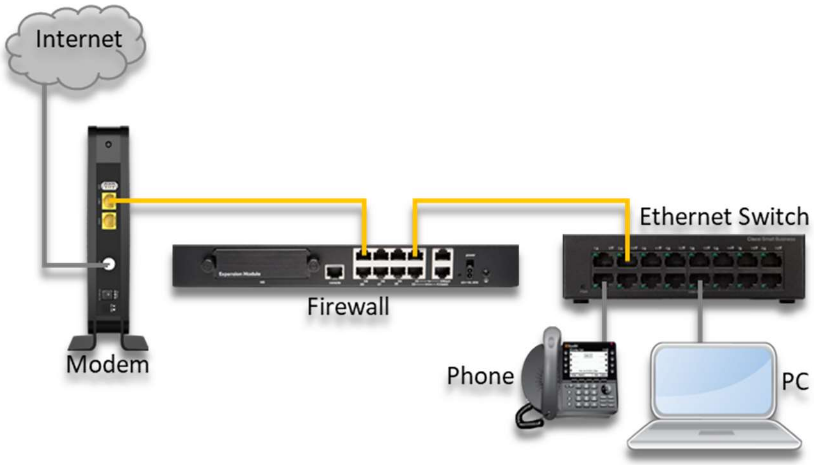
Normally, DNS service remains with the ISP and the Maya premises device passes the ISP DNS address to local network equipment in the reply to a DHCP request. Manual configuration using the Maya Control Center can override DNS settings.

One consequence of installing the Maya in this configuration is that without a local DHCP server configured, all site IP devices will receive new IP addresses. Some devices may not discard their old IP address and request a new one and may have to be reset in order to force the device to fetch a new IP address[1].

Deployment in Front of a Firewall

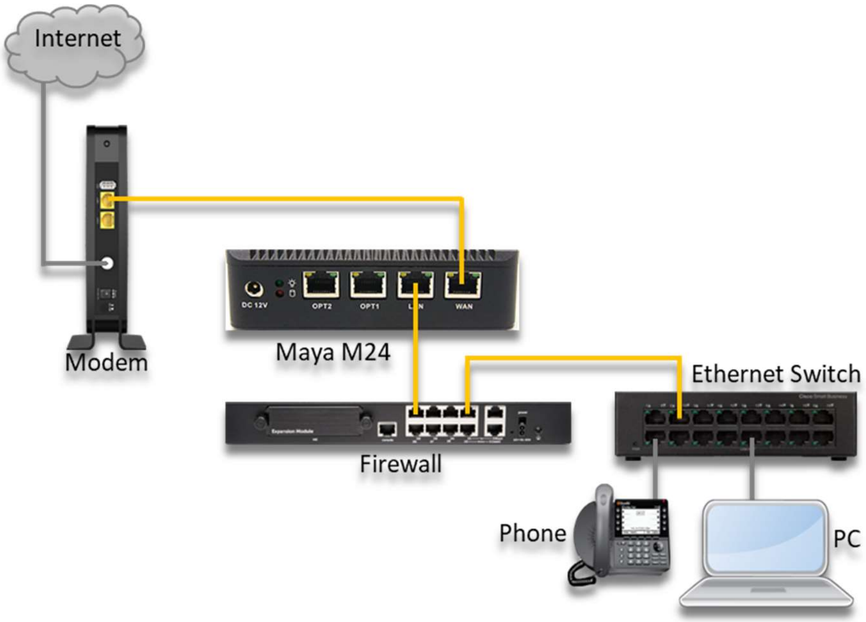
In larger installations, the site may contain a firewall as part of the enterprise equipment. Deploying the Maya premises device can be to position "in front" of the firewall – between the ISP access modem and the enterprise site's firewall, or "behind" the firewall – between the firewall and the site's Ethernet switch. The figure below depicts an enterprise firewall deployment.

[1] It may be possible to preserve existing static IP addresses by either using only static IP addresses at the site or limiting the DHCP range to avoid static IP addresses. A subnet address collision may occur (i.e. modem uses 192.168.0/24 and site static IPs are in the same range), so either a static IP needs to be used from the modem, or a different subnet needs to be configured on the modem.



Site with Enterprise Firewall

Positioning the Maya premises device in front of the firewall can be similar to the *Simplest Configuration* above, connecting the Maya device to the firewall instead of the Ethernet switch as shown below.



Deployment in Front of Firewall

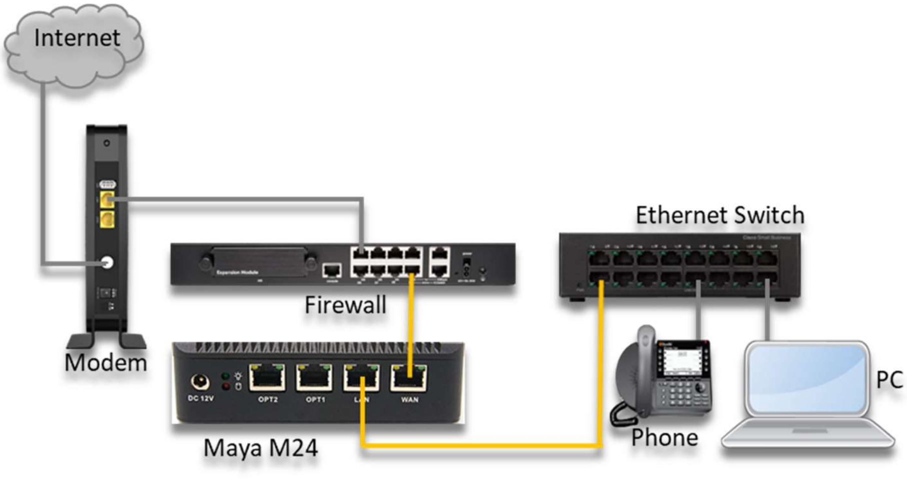
There are some tradeoffs when deploying in front of a firewall:

- Site internal IP addresses may remain the same if:
    - The site has its own DHCP server; IP addresses go untouched.
    - Otherwise if the site is obtaining DHCP from the modem, new addresses will be provided by the Maya premises device's DHCP.
- Multiple WANs can be trivially added merely be connecting to the Maya premises device.
- Third party encrypted tunnels (VPNs) make traffic prioritization impossible.

- The individual IP streams, including the headers, are encrypted as part of the tunnel. Maya cannot discern the headers and thus prioritize.
- However, Streamlining can take place as well as failover to other WAN connections.

Deployment Behind a Firewall

Positioning the Maya premises device behind a firewall is shown in the figure below.



Deployment Behind a Firewall

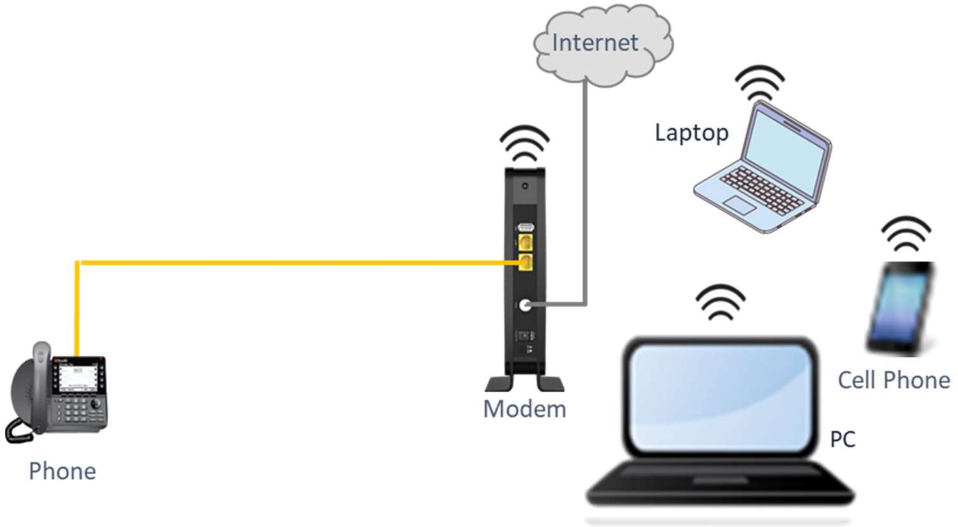
Deployment behind a firewall can add complications when:

- The site is part of an enterprise network, i.e., the site is interconnected in a VPN to other sites.
  - Maya traffic must be separated at the firewall, and the same firewall changes must be made at all other interconnected sites.
  - RFC 1918 private Internet addresses will be forwarded through the firewall and may create address conflicts in the network at other locations where the Maya premises is installed.
- "Double NAT" occurs. The Maya premises device performs NAT (Network Address Translation), and conflicts with the firewall's NAT implementation.
- Accessing multiple WANs. The Maya premises device needs to be able to route to the multiple WANs, which complicates firewall configuration.

Maya recommends consultation with its Solution Architects or Operations group when considering behind the firewall deployments.

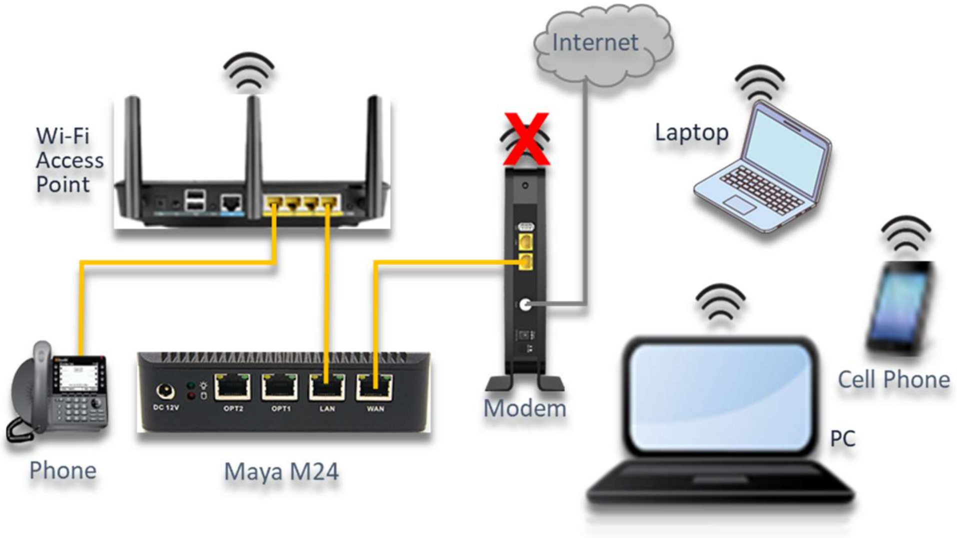
Home Deployment

Home and small enterprise deployments sometimes use a single networking device – combining modem, router, firewall, Ethernet switch, and Wi-Fi access point. A configuration of this type is shown below.



Home or Small Enterprise Configuration Before Maya Deployment

In addition to connecting the Maya premises device to the modem, an external Wi-Fi access point must be deployed, and the Wi-Fi in the modem disabled. The modem Wi-Fi can't be used as Wi-Fi traffic sent to the modem will bypass the Maya device. For Streamlining to work properly all site traffic must flow through Maya. A Maya home deployment is shown below with the addition of a Wi-Fi access point that also includes an Ethernet switch.



Home Deployment

Additional Configurations

There are other additional configurations and deployments as described below.

Multiple WANs

The Maya devices support as many WANs as there are available Ethernet ports. The Maya 24 has 4 Ethernet ports. With 1 port reserved for LAN, then three WANs can be supported.

Multiple LANs

The Maya device can support multiple LANs directly by connecting each LAN to an available Ethernet port. Multiple LANs can also be supported indirectly by manually configuring static routes in the Maya premises device and directing traffic to an on-site router.

Considerations

There are additional details that should be taken into consideration when planning an Maya deployment. They are listed below.

About the Maya Premises Device

The Maya premises device is an embedded Linux device with 4 Ethernet ports. It has an on/off switch with a blue LED indicator on the front, with a green LED power indicator on the back, along with a red disk drive activity indicator.. All configuration is obtained from the cloud. There is no permanent data on the device.

UPS Usage

Maya highly recommends utilizing a UPS for the Maya premises device as we frequently see power outages which disrupted Maya service.

Cloud IP Addresses

When tunneling all site traffic to the cloud, the source IP address of site traffic becomes the Maya premises device IP address instead of the ISP IP address.

Inbound Connections and Port Forwarding

The Maya device is designed primarily for sites utilizing resources in the cloud. All network connections in that case are outbound. For inbound connections, the device supports IP Port Forwarding. Port forwarding is documented in Maya installation documentation.

Security

Maya provides a stateful firewall with port forwarding. All Maya tunnel traffic is encrypted.

Static IP

The Maya premises device can be configured to use static IP, which is documented in Maya installation documentation.

Enterprise Routing and Connectivity

Maya can automatically connect all sites within an enterprise into a single mesh, secured VPN network with SQMI – Secure Quality Multipoint Internet. There is a checkbox in the Maya Control Center to enable this feature.

Multiple WAN Traffic Flow

The Maya service round-robins traffic across all WAN connections. Traffic is moved when a network becomes disconnected. As WAN capacity increases or decreases, Maya load is increased or decreased. There are no manual policies that can be set to direct traffic, it's automatic.

Maya VPN Tunnel Address Space

Care must be taken when manually configuring Maya VPN tunnels to avoid conflicts with the pre-existing enterprise IP address space.

Limitations

As of this writing the Maya service has these limitations:

- IEEE 802.1 VLANs are not supported
- DHCP relay is not supported
- IPV6 is not supported
- Dynamic routing protocols are not supported

Appendix

Port Numbers and Protocols

The Maya service utilizes a number of protocols and ports.

Traffic Outbound from the Maya Premises WAN Interface			
Protocol	**Destination Port or Type**	**Name**	**Purpose**
UDP, TCP	53	DNS	Resolve domain names and IP addresses
UDP	67	Bootps	Discover WAN Connectivity Settings via DHCP Application Management, Configuration
TCP	80, 443, 8443	HTTP, HTTPS	Application Management, Configuration, Authentication, Platform and Application Software Updates
UDP	123	NTP	Synchronize Clocks
UDP	33434-33534	UDP Traceroute	Network Connectivity Management
UDP	65194-65400	Tunnel	Transport encrypted and streamlined customer data
ICMP	3	Destination Unreachable	Network Connectivity Management (Path MTU Discovery)
ICMP	8	Echo Request	Network Connectivity Management (Reachability)

Notes

1. This list does not include customer traffic forwarded through the WAN interface when tunnels are down.
2. With the exception of ICMP Destination Unreachable, each of the above types of traffic requires return traffic of the corresponding type, which would normally be handled transparently by statefull firewalls.

Traffic Inbound to the Maya WAN Premises Interface			
Protocol	**Destination Port or Type**	**Name**	**Purpose**
TCP	65222	SSH (alternate port)	Allow diagnostic access by Maya Operations Staff
ICMP	3	Destination Unreachable	Network Connectivity Management (Path MTU Discovery)
ICMP	8	Echo Request	Network Connectivity Management (Reachability)

Notes

1. Inbound SSH is not required for normal operation and is not expected to be available. Connections are authenticated exclusively via public key cryptography and credentials are limited on a business requirement only basis. All connections are logged. At the time of this writing, there are four individuals with access via this connection.

Traffic Outbound from the Maya Premises LAN Interface			
Protocol	**Destination Port or Type**	**Name**	**Purpose**
UDP	68	Bootpc	Provide LAN Connectivity Settings via DHCP
UDP	33434-33534	UDP Traceroute	Network Connectivity Management
ICMP	3	Destination Unreachable	Network Connectivity Management (Path MTU Discovery)
ICMP	8	Echo Request	Network Connectivity Management (Reachability)

Traffic Inbound to the Maya Premises LAN Interface			
Protocol	**Destination Port or Type**	**Name**	**Purpose**
UDP, TCP	53	DNS	Resolve domain names and IP addresses
UDP	67	Bootps	Receive client LAN DHCP requests
TCP	80	HTTP	Access to local web server, used to set static WAN configuration in non-DHCP environments and for diagnostics.
UDP	33434-33534	UDP Traceroute	Network Connectivity Management
ICMP	3	Destination Unreachable	Network Connectivity Management (Path MTU Discovery)
ICMP	8	Echo Request	Network Connectivity Management (Reachability)