

Supported Network Scenarios

This document gives an overview of the many network scenarios supported by Marratech's solution. Marratech Manager server can be deployed in a variety of ways, making it a flexible, accessible and scalable solution. This document covers version 3.x of the Marratech Manager. To fully understand this document, good network and firewall knowledge is required.

This document covers the following:

- An overview of how the Marratech Manager works
- Deploying Marratech Manager over a standard network (IP Unicast)
- Deploying Marratech Manager over a Multicast network (IP Multicast)
- Deploying Remote Nodes to save bandwidth
- Where to deploy a Marratech Manager

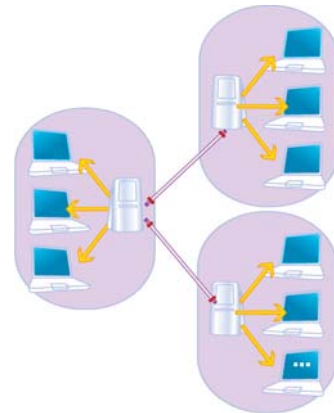
An overview of Marratech Manager

Marratech Manager (Manager) is a server process (or daemon) for hosting e-meeting rooms. It can act as a network reflector, ensuring that all the participants can properly connect to their meeting room. It also handles user and meeting room administration.

The Marratech solution is built upon a distributed architecture. This means that all encoding, encrypting and decoding is done in the end clients. Nothing is stored or processed (decrypted, mixed or cached) in the Manager.¹

By decoupling the client from the server, Marratech is able to offer very flexible network deployments (the topic of this document) and true end-to-end encryption (see the Security Overview document)

An example showing the flexibility of a distributed architecture is how a Manager can be "clustered". Access to a Manager can be established via the main "Central Node" or via one of the helping "Remote Nodes". This can lead to substantial network bandwidth savings when deploying the Marratech solution to link up remote offices.



Once a server is deployed, access to it is given through a web URL. The e-meeting rooms hosted by the server are each assigned a unique URL.

The Marratech client enters a meeting room through the room's unique URL. When this is done, a probing process is launched. The Marratech client probes the server for the following:

- What is the closest accessible Node?
- Is IP Multicast available on the network it is using?

Through this probing process, the Marratech client (client) decides what is the best Node to connect it to. To do this it looks at access times, network reliability and if IP Multicast is available. The meeting room connection is then established with the best available scenario.

¹When a SIP telephony module is activated, the Manager is in charge of un-encrypting and mixing the audio and sending it to the SIP gateway.



How bandwidth is calculated

The meeting room templates available for your Manager help you preset bandwidth limits for various connection scenarios. You should try to choose the template that matches the slowest connection used by your users.

Setting a bandwidth limit is an important step in deploying e-meeting services. It helps in ensuring a smooth deployment and limits the risk for network overload.

In Manager 3.x, limits can be set for a room or for each media individually. If you choose to set the bandwidth for a complete room, the Manager will decide what limits to set on each individual media. However, the easiest and quickest way is to create rooms based on the templates made available to you.

The bandwidth level set is dynamically shared by all participants. Limits can be set for video, audio, whiteboard, chat and web media.

The end user can also specify the capacity of the network uplink being used. This will limit the risk for network uplink overload.

A 200 kbps bandwidth limit for video in a 5 participant room will give a total of approx 40 kbps of video to send per user. ($200 / 5 = 40$).

A 50 kbps whiteboard limit will allow one user to send 50 kbps whiteboard information to others. If 2 users upload information in the whiteboard at the same time, then both will be limited to sending 25 kbps.

Audio bandwidth limit is also shared. Once the limit is passed, the Marratech clients will automatically step down to the next codec in line.

To estimate how much bandwidth a meeting room takes, make the following assumptions:

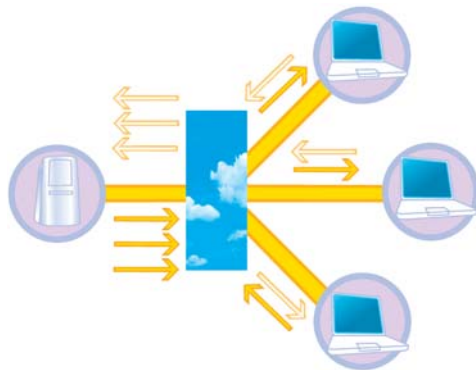
- Two people will be speaking at the same time. (2x selected audio codec bandwidth)

- Only one written media will be used at a time. (It is hard to use the whiteboard and chat simultaneously). Choose the highest bandwidth limit between chat, whiteboard reliable, whiteboard best effort and web.
- Add in the full video bandwidth limit.
Bandwidth limit = (2x audio codec) + (highest written media bandwidth limit) + video bandwidth limit
The following should also be taken in consideration:
- Congestion control may lower the limits automatically if packet loss is detected in the meeting room.
- For asymmetrical DSL and Cable connections, we recommend that users manually set the Marratech client to the level reflecting their uplink capacity.
- A client's own data is not sent back to the originator. However the bandwidth calculation does not take this into account. This introduces a safety margin, useful in case of network overload created by an external factor.
- The bandwidth limit procedure may seem complex, but our experience shows that using the Marratech templates is sufficient for most scenarios.

Deploying a Manager over a standard network (IP Unicast)

While the term "IP Unicast" may sound technical, it actually defines the most common way of establishing connections using the Internet Protocol. This mode is also the most common one used when deploying a Manager server.





Marratech Manager acts as a reflector, distributing meeting media (voice, whiteboard, video, chat and web) from one participant to all the others.

Considerations

When deploying a server that will act as a reflector, it must be placed carefully. A reflector should be placed in a central network location, where bandwidth is readily available.

Asymmetric network conditions should be avoided, as the server needs to send and receive data.

Bandwidth usage

A meeting room defined with a 200 kbps bandwidth limit will cause the Marratech Manager to use approximately ²:

Number of Participants	Bandwidth used by the Manager to receive data	Bandwidth used by the Manager to send data
5	200 kbps	1 mbps
10	200 kbps	2 mbps
20	200 kbps	4 mbps
30	200 kbps	6 mbps

The bandwidth limit set on an e-meeting room template (these Manager templates can be downloaded on www.marratech.com) limits the amount of data each client sends to the Manager.

When going from 5 to 10 participants in a meeting room, the active clients will throttle down (send less data) in order to make room for the new participant. This is because the allocated bandwidth is shared dynamically.

The amount of data sent to each participant will always match the overall bandwidth limit.

². A margin of safety is introduced in this calculation. The Manager does not send back video to the sender.

The amount of data the Manager will be sending is calculated by multiplying the bandwidth limit set in the template times the amount of participants.

There are several solutions to avoid overloading your Manager's network connection in this scenario:

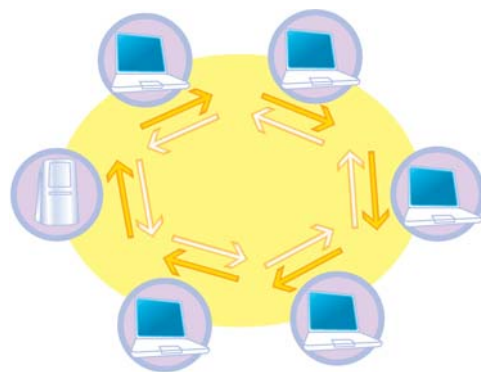
1. Choose a template with a lower bandwidth limit.
2. Limit the amount of participants that can enter your meeting room. (Done from the Manager's admin interface)
3. Deploy Remote Nodes (read further)
4. Deploy IP Multicast (read further)
5. Place your server in a hosting facility or upgrade your network link. (read further).

Deploying a Manager over a Multicast network (IP Multicast)

The Manager is built to take advantage of the IP Multicast protocol. The IP Multicast protocol makes it possible for one single stream of data to reach many recipients without any duplication in the network.

By using IP Multicast, voice, video, whiteboard, chat and web information is sent to all the participants intelligently by the network, ensuring that no unnecessary data copies are delivered.

The Manager can be configured to use the IP Multicast protocol, enabling a very bandwidth efficient deployment.



Consideration

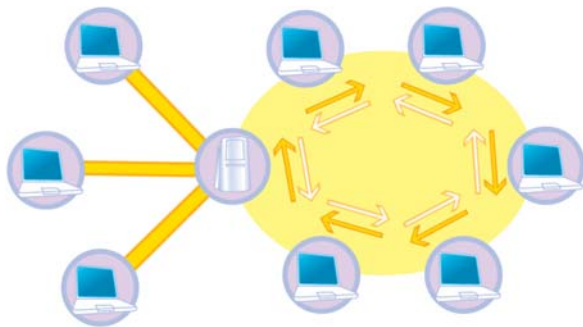
To use IP Multicast, it must be enabled in your routers and switches. Secondly, IP Multicast must be enabled in your Manager's configuration.

It can be turned on under the network settings in the administration interface. The proper Multicast address range and TTL must also be assigned.

With IP Multicast, the Manager is only used for joining sessions; it does not reflect any real-time data. It simply handles join and leave request.

IP Multicast makes it possible for one Manager server to handle many rooms with theoretically an unlimited number of participants.

If IP Multicast is not available, an IP Unicast connection is automatically offered. No end user action is required.



Bandwidth usage

The use of IP Multicast in your network allows for considerable bandwidth savings. An e-meeting room defined with a 200 kbps bandwidth limit will, over the whole network, use approximately:

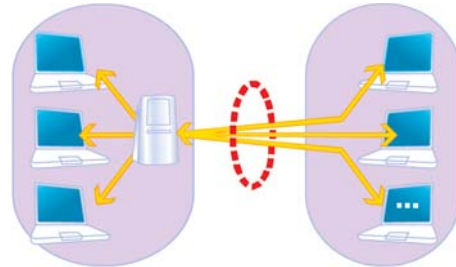
No. of Participants	Bandwidth used by the Manager to receive data	Bandwidth used by the Manager to send data
5	200 kbps	200 kbps
10	200 kbps	200 kbps
20	200 kbps	200 kbps
30	200 kbps	200 kbps

Deploying Nodes to save bandwidth

The Manager offers the ability to cluster your deployment across multiple servers. Your main Manager installation is called the "Central Node" while the extra clustered servers are called the "Remote Nodes".

This functionality helps connecting two or more offices wishing to communicate across an intranet. The intranet connection will usually not have enough bandwidth for multiple users connecting across it to a server located remotely. Every such connection represents a duplication of data.

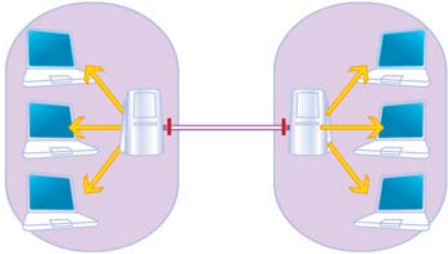
For example, the following picture illustrates three users needing to connect across the intranet. The Manager is installed at the office on the left.



All three user connections need to use the intranet connection to participate in the meeting. This is a waste of network resources as most of the traffic is duplicates of the same information. With many users, even fast intranets can quickly be overloaded.

Marratech solves this situation with Remote Nodes. A Remote Node is a subset of the main Manager (called Central Node). When a Remote Node is installed on a server located at a different location, it finds the Central Node and "connects" the traffic between them. This connection saves considerable amounts of bandwidth as no more duplicates are sent between the two network locations.

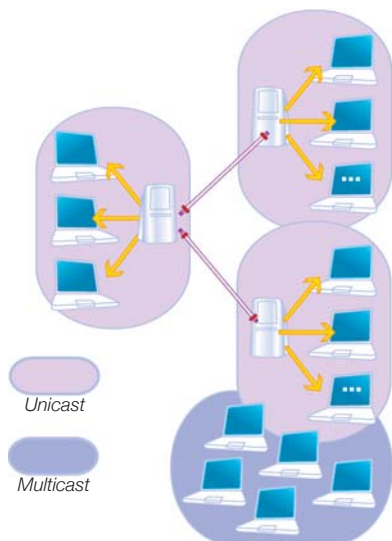




As you can see in the illustration, only one connection is made instead of three, thereby saving significant amounts of bandwidth. Only one copy of the data goes across the intranet. The remote node then takes care of copying the data within the LAN (Local Area Network), where bandwidth restrictions are less of an issue.

The Marratech client automatically finds the node that is the most appropriate when joining a meeting, removing the need to instruct users on where to connect depending on their location.

Several remote nodes can connect to a central node in order to save bandwidth across multiple locations as illustrated here. As with the Central Node, a Remote Node can support both IP Multicast and Unicast simultaneously.



Considerations

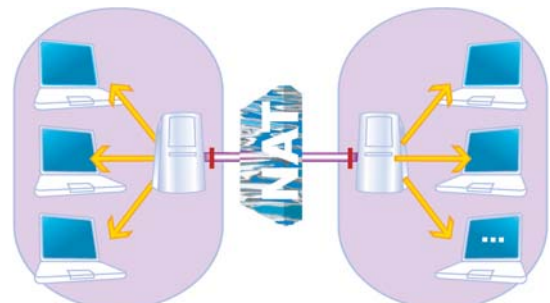
The Manager software license agreement permits the usage of nodes with no extra cost.

All administration of Nodes, users, rooms, etc... is done on the Central Node, offering a single point of administration for your deployment.

Here are some more items to consider:

- A Remote Node may only connect to a Central Node
- Up to five Remote Nodes may be deployed.
- A Remote Node may be deployed on a different operating system than the Central Node
- Users must still have access to the Central Node for logging in and finding the appropriate meeting room.
- A Remote Node may be placed behind a NAT firewall.
- A Remote Node may be active (initiates the connection to the Central Node) or passive (wait for a connection from the Central Node), depending on if firewalls are involved and what rules are used.
- The default traffic for Remote Nodes is via TCP port 4161 and UDP/TCP port 9000.

Deploying Remote Nodes with NAT

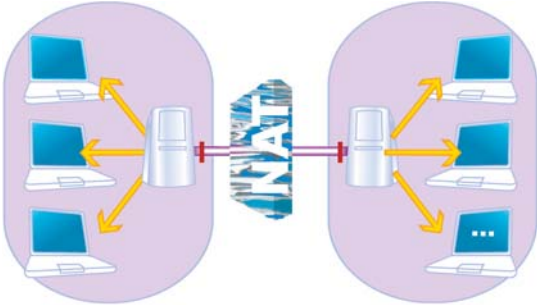


1. A Central Node (the main Manager, pictured to the left) is installed behind a NAT firewall. A Remote Node (pictured to the right) is installed outside the NAT firewall.

To support scenario 1, the following step must be completed:

- The Remote Node (to the right) must be set in passive mode. This means the Central Node (to the left) will be in charge of contacting the Remote Node, thus respecting the NAT's Dynamic State rule.

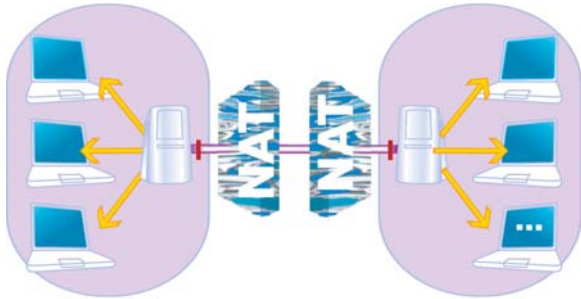




2. A Remote Node (pictured to the right) is installed behind a NAT firewall.

To support scenario 2, the following step must be completed:

- The Remote Node (to the right) must be set in active mode. This means the Remote Node will be in charge of contacting the Central Node (to the left), thus respecting the NATs Dynamic State



3. Both the Central and Remote Nodes are installed behind their respective NAT firewall

To support scenario 3, the following step must be completed:

- One of the Nodes, (Central or Remote) must be set in Active mode. The other node's NAT must be set for Port forwarding, in order to let the connection request go through. UDP Port 9000 and TCP Ports 4161 and 9000 must be forwarded to the Passive Node's internal IP address.

Bandwidth usage

A Remote Node connects to a Central Node in a way that is similar to a client connecting to a Manager. This means that the traffic between the Central Node and the Remote Node is the same as the bandwidth limit set for the meeting room.

This means that for the cost of the same bandwidth as one client connecting to a Manager, many users can connect.

Number of Participants	Bandwidth used on Intranet between the Central and Remote Nodes
5	200 kbps
10	200 kbps
20	200 kbps
30	200 kbps

Where to deploy the Manager

When deciding on where and how to deploy a Manager, security and network aspects are usually the most important to analyse. Security aspects are especially important if the Manager is to be accessed by users outside your own network.

Security aspects

A common deployment scenario involves giving users access the Manager from the Internet. In this case, firewalls and NATs may be involved.

In all cases, Marratech strongly recommends purchasing a real SSL certificate signed by an authorized Certificate Authority. All http traffic should be redirected to https. Both steps are easy to accomplish. Marratech has tested and deployed Thawte and Verisign certificates.

Here are various deployment scenarios for your Manager, when giving access to users via the internet:

- VPN. The easiest, safest and simplest way to give access to access to your Manager to people located outside of your intranet is via a VPN. Users can simply connect to the home network via their VPN client and then connect to a meeting room.

Marratech's solution is fully VPN (IPSec) compatible, therefore requiring no extra configuration. Simply remember that VPNs involve a certain network overhead and extra CPU usage.



- DMZ. The second easiest way of deploying a Manager and ensuring access to it via the internet is to deploy the Manager in your network DMZ. By properly configuring your firewall and DMZ for the appropriate ports, the Manager will be accessible from both your intranet and the internet.

Normal safety practices for deploying a server in a network DMZ includes turning off all unused processes and services and blocking access to the server's unused ports. Server administration should only be allowed from trusted network locations.

- NAT firewalls. If your server is to be placed behind a NAT and VPN access or DMZ deployment is not possible, the following steps need to be followed.
 1. The Manager must be given the public IP address connected to the NAT firewall. This is done in the detailed Network Settings found in the administrative interface.
 2. The NAT firewall must be configured with port forwarding. This means that the ports used for e-meeting traffic (Default TCP 8000, TCP 8001 and UDP 52000 to 52999) must be forwarded in the NAT to point towards your server's internal IP Address.

Network aspects

The Manager requires a central network location as it acts as a reflector (when IP Multicast is not available). It is in charge of relaying everyone's media to each other.

1. Majority of users located the internet

When deploying a Manager in a scenario where the majority of users are accessing the service from different locations on the internet, Marratech usually recommends having the service hosted by an ISP.

The advantages of having your server hosted in co-locations are multiple:

- No investment are needed to upgrade your own link.
- Co-location services usually have reliable, high-speed networks that have multi point access to the internet.

- The quality of the service for your users does not depend on the availability of your own network.
- Co-location services can offer UPS protection for your server as well as a secure location where non-authorized people do not have access.

When negotiating a rate with your hosting partner, choose a rate tied to average bandwidth loads instead of a rate based on the amount of data transferred. A rate tied to average bandwidth usage is usually more flexible and will give you access to higher bandwidth when required.

2. User located between two or more offices

Connecting users located at two or more offices usually involves the use of the existing intranet. Corporate intranets are often built upon leased lines that have limited bandwidth.

Having all remote office users connect to a Manager located at the central office will in most cases severely limit the amount of users that can participate in a meeting.

5 remote office users participating in a central office hosted e-meeting means all video, voice, whiteboard and chat traffic will be crossing the leased line 5 times. This is a significant waste of network traffic.

However, the problem introduced by this scenario is easily solved:

Solution 1: Remote Nodes

As part of the base license sold to customers, every Marratech customer can deploy up to 5 Remote Nodes.

A Remote Node establishes a connection to the Central Node (the main Manager server) and it ensures that no duplicates (copies) are sent over the network. This enables all participants from a remote office to attend an e-meeting without the need for upgrading network bandwidth. Deploying remote nodes offers significant savings in bandwidth and costs increased usage.



Five remote office users participating in an e-meeting hosted with a Remote Node deployed locally, means that all video, voice, whiteboard and chat traffic will be crossing the leased line only once. The amount of traffic crossing the leased line is independent of the amount of participants.

Solution 2: IP Multicast

By enabling IP multicast between the different offices, a simple scalable solution can be put in place without the deployment of several Remote Nodes.

IP Multicast is a scalable network protocol that takes care of intelligently distributing meeting media to all the participants without any duplicates being sent on the network. The network allows “sharing” of a single stream whenever possible.

IP Multicast requires that every network component (router, switch, etc...) is configured for IP Multicast. This may also signify VPN connections between the offices. In other words, external network competence may be required.

External access (for example from home) will still likely be done via traditional IP Unicast access towards the server. It is very uncommon that home broadband providers offer IP Multicast connections. For this reason, the server should still be in a central network location “close” to the main internet access point.

5 remote office users participating in a central office hosted e-meeting but with IP Multicast enabled on the network means that all video, voice, whiteboard and chat traffic will be crossing the leased line only once. The amount of traffic crossing the leased lines is independent of the amount of participants.

Solution 3: A combination of Remote Nodes and IP Multicast

The Manager can be IP Multicast enabled both on the Central and the Remote nodes. It is therefore possible to have certain users connect to a meeting via IP Multicast on the Central Node, and others via IP Multicast on Remote Node. The communication between a Central Node and the Remote Nodes is always done via IP Unicast.

