

Planning a Marratech Installation

This document provides an overview of the many ways a customer can deploy the Marratech Manager software. The intended audience is technical professionals with a solid knowledge of networks and firewalls.

The discussion starts with a short product overview and then moves on to the bandwidth issues surrounding IP-based collaboration services.

From there, it describes deployments over IP Unicast and Multicast networks and examines key Marratech features, such as clustering, security and common deployment situations.

An overview of Marratech Manager

Marratech Manager (Manager) is a server process (or daemon) for hosting collaborative meeting rooms.

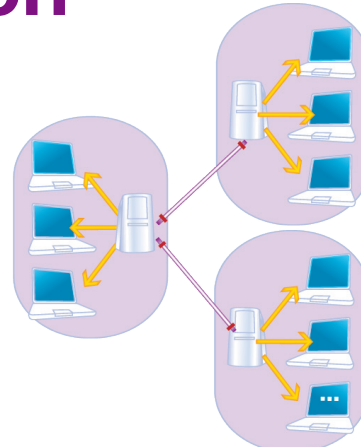
It handles user and room management, authentication and connection services. It also acts as a network media reflector when used on IP Unicast Networks.

The Marratech solution is built upon a distributed architecture where all encoding, encrypting and decoding is done in the end clients. Nothing is stored or processed (decrypted, mixed or cached) in the Manager. The only exception is SIP or H.323 calls, which are handled from within the Manager.

Access to the Marratech Manager, its meeting rooms and its administration tools is done via the web. Every meeting room has a unique address, making access as simple as a click on a link.

A key feature of this distributed architecture is the support for clustering. A cluster consists of a central node and one or more remote nodes. This behavior allows customers to achieve substantial network bandwidth savings, especially when linking remote offices.

A Marratech client considers several factors when selecting a node in a Marratech cluster. It looks at the availability of IP Multicast, network latency and network reliability and connects to the node offering the best combination of these factors.



A Marratech Manager cluster where significant bandwidth savings can be achieved with little effort.

Bandwidth Management

Setting appropriate bandwidth limits is an important step in deploying the Marratech solution. It helps in ensuring a smooth deployment and limits the risk for network overload.

The Marratech Manager allows you to set a bandwidth limit for a room or for each media individually. If you choose to set the bandwidth for a room, the Manager will decide what limits to set on each individual media.

The easiest and quickest way to set the appropriate limits is to create rooms based on the templates that are built-in the Marratech Manager.

The template chosen should match the user with the slowest network.

The second way to control bandwidth levels is to have each user set the capacity of their network connection in the Marratech client preferences. This setting will limit data being sent (i.e. upload or uplink) to avoid a network uplink overload.

The bandwidth limit set in the Marratech Manager is dynamically shared by all the participants. This means that a limit will be enforced if the sum of all data being sent surpasses it. To better understand this concept, consider these examples:

- A 200 kbps video bandwidth limit for 5 participants 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 to the other participants. If 2 users upload information in the whiteboard at the same time, both will be limited to 25 kbps.
- Audio bandwidth limit is also shared. Once the limit is passed (e.g. many people talk at the same time), the Marratech clients will automatically step down to lower bandwidth codec in line. Once the lowest codec is chosen (iLBC) it is possible for the session to pass the limit set as audio can not be limited further.

This behavior allows you to estimate the bandwidth for a room by using a simple equation:

$$\text{Bandwidth} = \text{Audio limit} + \text{video limit} + \text{whiteboard reliable}$$

The other media (control, web slides, whiteboard best effort) either happen in bursts exclusively from the whiteboard or do not require any significant amount of data. It is therefore safe to estimate the total bandwidth as a total of audio, video and whiteboard reliable.

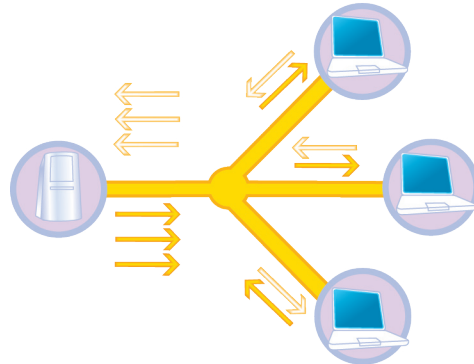
The following should also be taken in consideration:

- Congestion control may lower the limits automatically if packet loss is detected in the meeting room. It first acts on video, the whiteboard and audio.
- 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.

Using Unicast Networks

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.

This mode is the most common one used when deploying a Manager server. For unicast deployments, the Manager acts as a reflector, distributing meeting media from the sender to all receivers.



A typical Unicast scenario where the Manager acts as a media reflector.

Marratech recommends that customers place the Manager in a central network location, relative to the server's community of users and where sufficient bandwidth is available. Because of their asymmetric nature (slow upload, large download) DSL lines are not recommended.

Participants	Required Bandwidth	
	Inbound	Outbound
5	400 kbps	2 mbps
10	400 kbps	4 mbps
20	400 kbps	8 mbps
30	400 kbps	12 mbps

Observe that as the level of participation grows, the inbound bandwidth remains the same. This is a result of the dynamic bandwidth limitation that shares the allocated bandwidth between all the clients. The amount of data sent to the server is always equal to the overall bandwidth limit set for the room.

Observe also that, in a Unicast setting, the outbound bandwidth consumed by the Manager is additive and grows with the number of participants.

If this situation where to overload your network, a number of solutions are available:

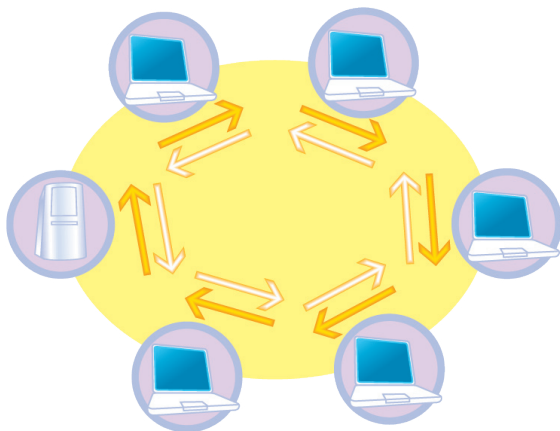
1. Choose a template with a lower bandwidth limit.
2. Limit the amount of participants that can enter your meeting room. (From the Manager's admin interface)
3. Deploy IP Multicast (explained further)
4. Deploy Remote Nodes (explained further)
5. Place your server in a hosting facility or upgrade your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



Using Multicast networks

The Marratech Manager ships with full support for the IP Multicast protocol. This protocol makes it possible for one single stream of data to reach many recipients without any duplication of packets in the network.

This makes IP multicast a very efficient solution for the bandwidth demands of Internet collaboration software.



An IP multicast scenario where all data is sent on the network only once, avoiding duplicates and therefore saving bandwidth.

To better understand this efficiency, consider a room with a bandwidth limit of 400 kbps. The server's use of bandwidth at various participant levels appears in the table below:

Participants	Required Bandwidth	
	Inbound	Outbound
5	400 kbps	400 kbps
10	400 kbps	400 kbps
20	400 kbps	400 kbps
30	400 kbps	400 kbps

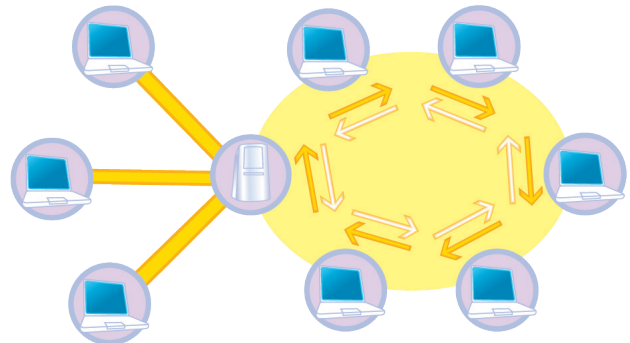
As the number of participants grows, the **bandwidth consumption remains constant**.

Access to IP Multicast is not automatic. You must enable it on your network and within the Marratech Manager. For your network, you must have switches and routers with multicast capability and you must have activated these features. To enable IP Multicast in the Marratech Manager, a system administrator

needs to enter the proper Multicast port range and time-to-live (TTL) value in the network settings page of the administrative interface.

If IP Multicast is enabled in the Manager, but not available on the network, the Manager automatically drops back to IP Unicast connections. No end-user action is required.

IP Multicast reduces server resource consumption, as the Manager does not have to reflect any real-time data. It simply handles join and leave requests. IP Multicast makes it possible for one copy of the Manager to handle many rooms with theoretically an unlimited number of participants.



Furthermore, a Manager can function in hybrid mode, giving users IP Unicast and IP Multicast connections depending on the end user's network configuration. This is done without user intervention.

Clustering

Another deployment alternative is the clustering feature of the Marratech Manager. Clustering allows customers to distribute their Marratech meeting network load across two or more servers running the Marratech Manager.

The principal copy of the Manager is called the "Central Node" and remote copies of the Manager are "Remote Nodes". The base license includes support for five remote nodes.

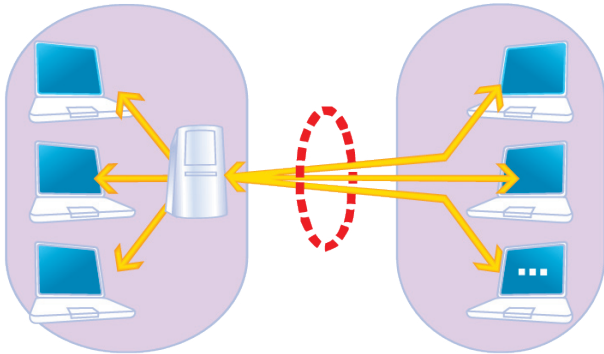
Since a remote node is a logical slave of the central node, it cannot operate in a standalone manner. However, the slave node need not use the same operating system as the central node.

The usefulness of this functionality comes across quickly through a common example. Consider a



customer that has two offices, a main office and a remote office. A Marratech Manager is deployed in the main office.

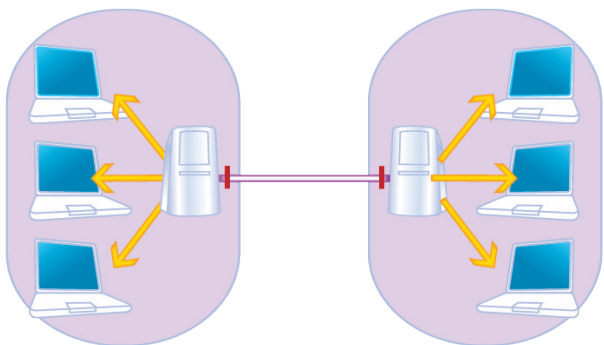
A meeting is held where three users from each office must participate. With a bandwidth limit of only



400 kbps, this meeting would require over 1.2 mbps of network bandwidth between both offices. Three unicast connections, one for each participant at the remote office, must be established for everyone to participate. Remember that this is replicated information.

If the same customer would instead deploy a Remote Node at the remote office location, the bandwidth requirements for this meeting would drop from 1.2 mbps to 400 kbps.

In fact, if 15 users were to connect from the remote office through the use of a Remote Node, the total bandwidth consumed between the offices would still be 400 kbps.

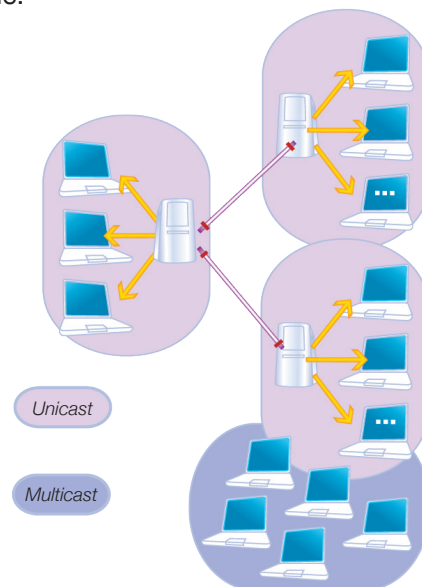


The Remote Node merges the inbound information from the remote office and sends it to the Central Node. While this is done, it also replicates the information coming from the Central Node and distributed it to the remote participants. No duplicate

information is sent across the network connecting the two offices.

Participants	Required Bandwidth between offices
5	400 kbps
10	400 kbps
20	400 kbps
30	400 kbps

Remote Node deployments can also take advantage of IP Multicast networks, allowing remote users to connect with the best network transport method available.



NAT Considerations

A Remote Node placed behind a NAT must be created as an “Active Node” in order for it to connect to the Central Node properly.

A Remote Node on a publicly addressed network (without a NAT) and meant to connect to a Central Node placed behind NAT must be created as “Passive”, in order for the Central Node to initiate the connection.

If both the Central Node and the Remote Node are behind NAT, Marratech recommends that the Central Nodes’ NAT be configured with the proper port forwarding rules and that the Remote Node be created as Active.



SIP and H.323 Considerations

SIP and H.323 calls are initiated and executed from the Marratech Manager. The call out functionality can be executed from a Remote Node or from the Central Node.

Placing the dial out functionality on a Remote Node may be desirable for the following reasons:

- H.323 and SIP calls increase CPU load on the server. By placing the dial out functionality on a remote node, processor usage on the Central Node may be saved.
- H.323 and SIP calls do not use encryption in the same manner as a normal Marratech participant. Placing the dial out functionality as close as possible to the end station or SIP gateway is favorable.
- H.323 and SIP calls require extra bandwidth if video is involved. This should be considered when choosing dial out functionality placement.
- H.323 calls require that the same IP addressing space is used between the Node executing the call and the H.323 end station. A Remote Node may help resolve this potential network access issue.

Security

Most customers will want users on the public Internet to have controlled access to their Marratech Manager.

Marratech strongly recommends that customers purchase an SSL certificate signed by an authorized Certificate Authority. In addition, customers should redirect all HTTP traffic to HTTPS by choosing the appropriate option in the Manager's admin interface.

The balance of this section explores various deployment options for controlling access to the Manager by users on the public Internet.

VPN

The easiest, safest, and simplest way to provide access to Marratech Manager by users located outside of your intranet is through a virtual private network (VPN). Users connect to the home network via their

VPN client and then connect to a meeting room with Marratech.

Marratech is fully VPN (IPSec) compatible and requires no extra configuration. Keep in mind that VPNs may involve additional network overhead and CPU load.

DMZ

Another easy way to deploy the Manager for Internet access is to place the Manager's server in your network's demilitarized zone (DMZ). Marratech recommends the use of standard safety practices for DMZ-based servers including the use of a SSL certificate, the elimination of all unused processes and services and the blocking of all unused ports.

For additional information on firewall configuration for DMZs, please see the Marratech technical paper entitled, Marratech Security Overview.

NAT

Customers can also locate the Marratech Manager behind a network address translation (NAT) firewall.

When configuring the Manager's network settings, you must enter the public IP address of the firewall. The HTTP, HTTPS and UDP ports chosen in these same settings must be forwarded in the NAT firewall configuration.

By default, these ports are set to TCP 8000-8001 and UDP 52000 to 52999 where 12 UDP ports per meeting are required.

Server Placement

This section offers suggestions for the placement of Marratech Manager nodes depending on the customer's circumstances. The two most common situations are generic public access and the connection of two or more principal offices.

Public Access

When deploying a Manager where the majority of users are accessing the service from the public Internet, Marratech suggests that an ISP or collocation facility host the server. This option offers a couple of advantages.

First, collocation services usually have reliable, high-speed networks that have multipoint access to the



Internet. This means that you do not need to upgrade your local Internet connection. It also means that the quality of the service provided to your users does not depend on the quality of your current network connection.

Second, collocation services typically operate 24 hours a day, seven days a week. This commitment to non-stop operation usually includes uninterruptible power supply (UPS) protection for your server as well as controlled access to your hardware.

Linking Offices

The other commonly encountered deployment situation is the connection of users located at two or more offices. Such customers usually have an existing intranet with leased lines and limited bandwidth.

Remember from the previous discussion that Unicast networks require the replication of media stream packets for every user. If remote office users connect to a Manager located at the central office, they could quickly overload the leased line connection between the facilities.

The Marratech meeting solution offers three ways to address this issue. These are remote nodes, Multicast networks, and some combination of the two.

The first solution is a remote node. Remember that a base license allows a customer to deploy up to five remote nodes. Remote nodes eliminate the problem of packet replication across Unicast networks. Thus, five remote users attending a meeting will only load the inter-site connection with one set of packets instead of five.

IP Multicast is another valuable strategy. By enabling multicast between the different offices, the network takes responsibility for the efficient distribution of packets between and among remote locations.

Remember that Multicast will probably require upgrades to your networking infrastructure as routers, switches, and other components must support Multicast protocols.

Lastly, a strategy combining Remote Nodes and Multicast access may best fit your network capabilities.

Conclusion

Marratech customers must consider bandwidth requirements and manage bandwidth-related issues.

Marratech's architecture and flexibility provide multiple options for various deployment scenarios, including support of IP Multicast and clustering.

In all deployment scenarios, network security is a prime concern and customers can safeguard it with appropriate network topologies, the use of SSL, NAT and VPN, and proper firewall configuration.

Marratech Inc • 6 Dumont Place • Morristown • NJ 07960 • USA
Phone: +1 888 WORK BETTER or +1 888 967 5238

Marratech AB • S:t Eriksgatan 115/Box 6791 • SE-113 85 Stockholm • Sweden
Phone: +46 8 555 118 40

www.marratech.com • sales@marratech.com

