

# Проблемы реализации Searching — Indexing сервисов для Instance Messaging систем

Андрей Пептюк, Вадим Мартыш

Instance Messaging системы являются одним из ярких примеров P2P. Такие системы как ICQ, Yahoo IM, MS IM, AOL IM, пользуются огромной популярностью среди пользователей. Все больший и больший интерес к этой теме проявляют и корпоративные клиенты. Которые хотят использовать все выгоды IM для организации внутрикорпоративного обмена информацией, с должным уровнем безопасности и гарантией доставки сообщений.

Существует ряд проблем которые типичны для большинства IM систем. Основными источниками проблем является наличие firewall и NAT.

Peer находящийся за firewall относительно другого peer будет трудно доступен. Существуют разные варианты решения этих проблем.

Рассмотрим как это сделать отдельно для систем работающих исключительно в локальных сетях, и систем работающих в глобальных сетях.

## 1. Локальные сети

(сети поддерживающие шировещательную передачу данных). Этот вариант, будет подходящим для большинства систем работающих в пределах одного офиса. В этой ситуации мы можем полностью избежать наличия privileged peer, и получить pure P2P без какого либо сервера. При запуске клиентской системы либо специальной тулзовины в нее встроенной, отправляется broadcast/multicast пакет, содержащий необходимые данные для пополнения peerlist-ов других пользователей прикладной

системы в свою очередь другие участники отправляют информацию о себе к "новому" peer. Дальнейший обмен сообщениями происходит напрямую между peer-ами, либо broadcast если оно касается всех peer. Периодически текущее состояние peer (доступен/недоступен...) проверяется путем тех же broadcast запросов.

Пакеты могут передаваться по разным транспортным протоколам в зависимости от объема данных. Небольшие сообщения могут передаваться по UDP при передаче данных большого объема (более 1-1,5 К) система автоматически должна переходить на TCP либо разбивать пакеты либо сжимать пакеты. При работе в локальных сетях тип транспортного протокола не имеет такого значения, поскольку не существует угрозы отклонения пакета router.

## **2. Глобальные сети**

Для IM P2P систем работающих через firewall, что является типичным для глобальных сетей, необходимо предусмотреть наличие privileged peer. Его отличительной особенностью является наличие честного IP адреса, о котором должны знать другие peers. Рассмотрим несколько вариантов работы такой IM системы.

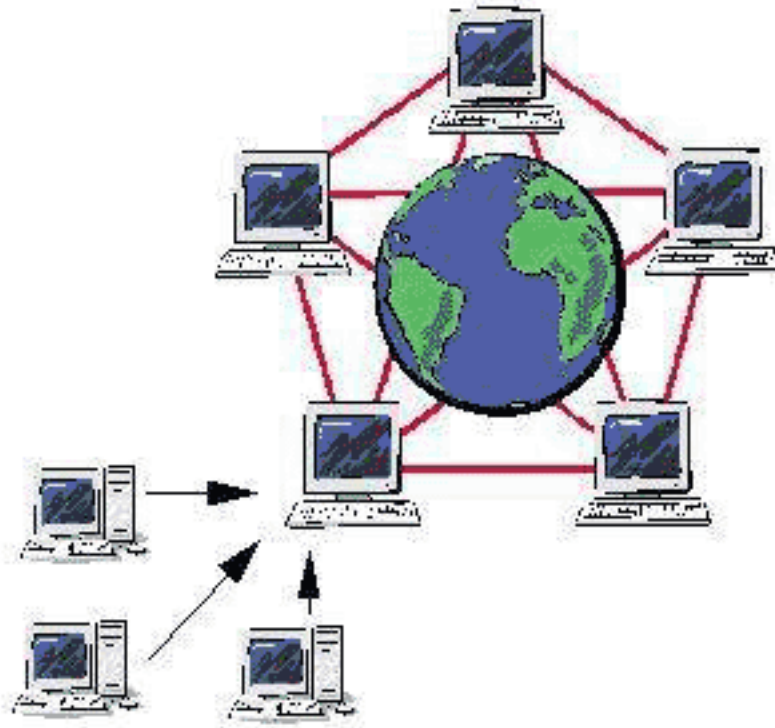


Рисунок 1. Network topology.

## 2.1. Первый

В каждом из офисов есть одна рабочая станция с честным IP адресом. Работа внутри локальной сети происходит по схеме описанной выше. Что бы отправить сообщение peer-ам из других офисов, нужно передать сообщение privileged peer, который хранит информацию о других Privileged peer и после опроса их на наличие нужного peer в подсети передает сообщение. Если в локальной сети нет ни одного "честного" IP адреса, то функции привелигированого peer должны быть перенесены на сервер(router/firewall). При этом такая система является распределенной но уже не является pure p2p. Топология такого решения на рис 1.

## 2.2. Второй

Работа по нижеследующей схеме зависит от настройки Router. В вашей сети нет "честных" IP адресов. Если Router, после отсылки сообщения оставляет за вашей

программой port, или вы с периодически устанавливаете соединения с привилегированным Peer, удерживая адрес:порт и/или обновляя пару адрес:порт, то ваш клиент остается доступным для других клиентов извне вашей подсети. Такое решение используется многими IM системами (e.g., ICQ /v5). При этом необходим центральный сервер — Privileged Peer — для инициализации работы в сети. Вы должны зарегистрировать на сервере IP адрес:порт который вам выделен вашим физическим сервером на время сеанса, по которому и будет осуществляться передача вам сообщений. Любая компания может поставить пару мощных серверов в Inet (аналогично Мирабилис, Yahoo или MS) и обеспечить таким образом возможность обмена сообщениями в ходе разработки между любыми разработчиками использующим клиентскую систему. Собственный сервер может поставить customer компания для внутренних целей. Альтернативным вариантом является push-back (a-la Gnutella) — периодические подключения (TCP) к Privileged peer для приема и отправки сообщений (в таком случае привилегированный peer выполняет еще и функции кеширования запросов).

### **2.3. Третий**

Этот вариант зависит от усилий сисадмина. Он(и) должны грамотно организовать виртуальную частную сеть (VPN) компании (что в принципе бывает полезно и безотносительно к любым прикладным IM системам). В этом случае у всех пользователей (возможно) появляется общее адресное пространство, настраиваемое широковещание и масса всяких других полезностей. Такой вариант в принципе сводим к варианту 1 или даже к варианту локальной сети.

### **2.4. Четвертый**

Этот вариант базируется на работе через существующие IM системы. Разработав gateway или конвертатор для преобразования пакетов из вашей собственного формата в формат пакетов другой IM системы. Таким образом мы перекладываем решение проблем возникших с firewall или NAT на существующую IM систему через которую работает ваша система. У такого подхода есть еще одно преимущество, вы сможете обмениваться данными не только с клиентами содержащими клиент вашей системы но и с клиентами IM системы через которую происходит взаимодействие.

## *Проблемы реализации Searching — Indexing сервисов для Instance Messaging систем*

Интероперабельность — колоссальное преимущество, однако неопределенность легального статуса "хаченых" библиотек для работы с proprietary протоколами (ie., icqV7) и использования ресурсов proprietary IM — систем третьими сторонами требует большой осторожности при использовании ресурсов существующих коммерческих IM (MS, Yahoo, AOL, ICQ) как основного транспорта собственной системы обмена сообщениями.

Существуют и другие способы решения проблем возникающих при взаимодействии реер в сети. Выбор подхода зависит от конкретной ситуации, и решение в любом случае должно приниматься разработчиками конечной системы.