ОРГАНИЗАЦИЯ ДОСТУПА К ИНТЕРНЕТ КОНЕЧНЫХ ПОЛЬЗОВАТЕЛЕЙ В ИССЛЕДОВАТЕЛЬСКОМ ИНСТИТУТЕ

А.Н. Лодкин [1], А.А. Орешкин [2], А.Е. Шевель [3]

Петербургский Институт Ядерной Физики
188350, Гатчина, Ленинградской обл.,
Россия

Аннотация. По нашим оценкам для полноценной работы в Интернет требуется от 64 до 128 Кбит/сек на каждого пользователя. Такие возможности смогут обеспечить своим сотрудникам редчайшие организации в России. В связи с этим вопрос доступа конечных пользователей к Интернет необходимо каким-то образом регулировать, чтобы обеспечить относительно свободный доступ для высокоприоритетных работ.

В Петербургском Институте Ядерной Физики (ПИЯФ) ([1]) разработан и опробован административно-технический механизм, включающий параметрически настраиваемое регулирование доступа каждого хоста к Интернет. Механизм основан на регулировании объема передаваемых данных, а также на градации степеней доступа к Интернет конечного пользователя (компьютера).

ВВЕДЕНИЕ

Компьютеры не включённые в локальную сеть института стали анахронизмом, т.е. почти все вычислительные устройства включены в локальную компьютерную сеть *TCP/IP*. Общее количество компьютеров в сети ПИЯФ составляет около 480. Исторически сложилось так, что бóльшая часть компьютеров имеет прямой доступ к Интернет, т.е. пользователь имеет возможность копировать информацию из Интернет прямо на свой компьютер.

На каждого использующего в данный момент Интернетовский канал потребная ёмкость составляет как минимум 64 Кбит/сек. Это означает, что

[1] e-mail:*lodkinan@pnpi.spb.ru*
[2] e-mail:*oreshkin@pnpi.spb.ru*
[3] e-mail:*shevel@pnpi.spb.ru*

каждый человек использующий Интернет в конкретный момент имеет как минимум 64 Кбит/сек до наиболее значимых для института сайтов: DESY (Германия; www.desy.de), CERN (Швейцария; www.cern.ch), FNAL (США; www.fnal.gov), BNL (США; www.bnl.gov), NIST (США; www.nist.gov), ОИЯИ (Россия; www.jinr.ru), etc. По всей видимости, со временем эта цифра будет расти с ростом числа протоколов (особенно мультимедиа), используемых для обмена данными через Интернет.

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ КАНАЛА В ИНТЕРНЕТ В ПИЯФ

Основными протоколами, используемыми в ПИЯФ, для обмена информацией со всемирной сетью являются: *smtp, ftp, http, nntp, telnet, dns.*

Отметим несимметричность сетевого трафика: исходящий трафик составляет от 1/4 до 1/3 общего трафика. Иными словами, информация, главным образом, импортируется. Такого сорта несимметрия существует на протяжении нескольких лет.

Следует иметь в виду, что технически возможные запросы пользователей весьма велики. Так, если на типовом персональном компьютере имеется от 2-4 GB и более доступной дисковой памяти, то это означает, что технически возможны запросы на передачу информации объёмом 2-4 GB и более за один сеанс с одного компьютера. Таким образом, если мы возмём канал 128 Кбит/сек, то один пользователь может загрузить его полностью на срок примерно 4GB/16 Кбайтов/сек, что составит около 262144 секунд, т.е. чуть более 3 суток. Иными словами, один сотрудник ПИЯФ с помощью недорогого PC может, недопонимая последствий, заблокировать институтский канал в Интернет, сделав его практически недоступным для остальных сотрудников института. Подобные проблемы имеют место не только в ПИЯФ [2].

Если учесть, что от 50 до 100 человек в ПИЯФ могут использовать Интернет в одно и то же время, то Институту следует иметь канал с ёмкостью как минимум 6.4 Мбит/сек. Реальность показывает, что каналы с такими пропускными способностями пока недоступны для ПИЯФ. В результате при одинаковом приоритете для всех конечных пользователей канал оказывается загружен на 90-95%. Иными словами, возникает ситуация затора, когда суммарный объём запрашиваемой на передачу информации превышает возможности канала, что серьёзно ограничивает возможности использования Интернет для конкретного пользователя. В течение суток на протяжении многих часов канал фактически невозможно использовать для интерактивного поиска информации в Интернет. Тем более невозможно поддерживать интерактивную сессию с удалённым хостом (*telnet, talk*, etc.).

Радикальным средством снижения вероятности заторов на Интернетовском канале является его расширение. Однако, полезно рассмотреть и другие варианты избавления от заторов. В первую очередь имеется в виду эффективность

использования уже имеющейся ёмкости канала связи.

Главным направлением в смысле повышения эффективности использования канала является минимизация объёма шумового трафика, т.е. трафика, который не является абсолютно необходимым. К шумовому трафику относятся:

- многократное копирование разными пользователями одних и тех же программ и документов, необходимых для работы;
- копирование (в том числе и многократное) документов не являющихся необходимыми для работы.

Шаги, которые имеют место в данном случае весьма разнообразны:

- Организация и ведение локальных зеркальных серверов, на которых хранятся наиболее популярные в институте программы и документы. Естественно, что пользователи должны быть информированы о таких возможностях.
- Организация и ведение прокси серверов достаточной емкости, которая определяется пропускной способностью канала связи.
- Ведение разъяснительной работы о правильных процедурах использования Интернет. Среди прочего подчеркивается открытость для остальных сотрудников истории просмотра документов с любого компьютера.

Наряду с вышеописанными методами уменьшения шумового трафика, полезно рассматривать и дополнительные меры.

ПРИОРИТЕТНЫЙ ДОСТУП

Одной из дополнительных мер может быть введение приоритетов по доступу к Интернет таким образом, чтобы наиболее важные для института работы имели относительно свободный доступ к Интернет при удовлетворительных возможностях для остальных работ. Приоритетный доступ осуществляется на основе таблицы допустимого дневного трафика, в которой каждая строка соответствует одному хосту в Институте. В строке указан максимально допустимый объём сетевого трафика для данного хоста в сутки.

Во время проведения эксперимента имелись несколько вариантов величин лимитов для хостов, которые определялись на основе реальной пропускной способности канала в Интернет в то время: 0.5 MB, 2MB, 50 MB и *без ограничений*.

В целом процедура выглядит следующим образом. Каждые N минут (по умолчанию 60) производится считывание данных о трафике с маршрутизатора CISCO и проверка всех хостов института на уже достигнутые объёмы дневного трафика. Если какой-то хост превысил допустимый объём дневного трафика, то выход в Интернет для этого хоста автоматически закрывается на CISCO. В 0 часов все закрытые хосты открываются заново.

Как видно, ограничения на трафик наложены относительно мягкие в том смысле, что проверка на превышение допустимого трафика производилась только раз в час. Следовательно, кто-то мог превысить допустимый трафик, если за час удавалось прокачать больше, чем предложенный лимит.

Когда хост закрывается на CISCO, то ответственному за компьютер лицу автоматически направляется электронное письмо с сообщением о причине закрытия.

На локальные обмены данными внутри локальной сети института не было никаких ограничений.

Весь механизм реализован с помощью комплекта скриптов на *perl*.

Наконец, все хосты института разделяются на четыре группы:

- Хосты, которые имеют прямой выход в Интернет без ограничения дневного трафика. Очевидно, что количество таких хостов должно быть невелико в процентном отношении. Такие хосты должны находиться под наблюдением менеджеров, поскольку они подвергаются наибольшей опасности нападения хакеров из Интернет.

- Хосты, которые имеют прямой выход в Интернет, но имеющие различного вида ограничения на объём дневного трафика. Таких хостов, возможно будет больше. Ограничения на трафик способствует как снижению шумового трафика, так и уменьшает опасность нападения из Интернет.

- Хосты, которые не имеют прямого выхода в Интернет и могут использовать прокси сервер, а получают информацию из Интернет только посредством серверов прокси. Видимо, это должен быть основным методом работы хостов ПИЯФ. Естественно, что вероятность нападения хакеров ещё меньше, чем в предыдущем случае. Для этих хостов также полезно устанавливать ограничения на максимальный объём дневного трафика.

- Хосты, которые не имеют прямого выхода в Интернет и не имеют возможности использовать серверы прокси. К таким хостам относятся все служебные или измерительные машины в локальной сети института, а также часть машин, которые не должны иметь выхода в Интернет. Очевидно, что эти машины наиболее защищены от нападений извне и не могут создавать шумового трафика.

РЕЗУЛЬТАТЫ ВВЕДЕНИЯ ПРИОРИТЕТОВ

В октябре 1998 года были проведены натурные испытания предложенной процедуры, которые продолжались примерно 15 дней. Выяснилось, что месячный трафик института уменьшился примерно на 17%. В то же время если до введения механизма приоритетов любой файл из DESY копировался со скоростью около 200 байтов в секунду, то после введения механизма приоритетов скорость повысилась до 600-1000 байтов в секунду.

Во время испытаний, если хост превышал установленный лимит дневного трафика, то закрывался прямой выход в Интернет и выход через сервер прокси. В то же время электронная почта ходила без ограничений.

В то же время многие сотрудники института высказывали недовольство нормированием доступа в Интернет. Во всяком случае проведение эксперимента вызвало дискуссию, во время которой высказывались разнообразные мнения, в том числе мнения руководителей лабораторий и отделов.

МНЕНИЯ РУКОВОДИТЕЛЕЙ СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ

Руководители отделов и лабораторий разнообразно оценивают фактическую сторону использования Интернет своими сотрудниками. Известные авторам оценочные суждения, распределяются примерно по следующим группам.

- "Мне неизвестно точно, какую информацию мои сотрудники изучают в Интернет."
- "Поиск информации в Интернет для выполнения какой-то работы есть просто ширма. Полагаю, что добрая половина Интернетовского трафика представляет собой информацию, не имеющую отношения к работам института."
- "Мне точно известно, что мои сотрудники используют Интернет исключительно для выполнения плановых работ. Свободный доступ в Интернет есть необходимое условие для успешного выполнения нашей работы."

Разброс оценок велик. Примерно такой же разброс оценок проявился и при рассмотрении результатов экспериментов с введением приоритетов по доступу к Интернет.

ЗАКЛЮЧЕНИЕ

В заключение мы можем сказать, что разработан и опробован прототип механизма для организации доступа в Интернет в соответствии с приоритетами. Данный механизм имеет параметрическую настройку: частоту проверки объема трафика для каждого хоста, период за, который подсчитывается трафик, etc. Например, система легко перестраивается на недельный или месячный период подсчёта Интернетовского трафика. В целом разработанный механизм представляет собой инструмент, который позволяет дирекции проводить определённую информационную политику в отношении использования канала в Интернет, который является дорогостоящим ресурсом.

СПИСОК ССЫЛОК

1. *Петербургский Институт Ядерной Физики*
   `http://www.pnpi.spb.ru/`.
2. *Economic FAQs About the Internet (Presented at MIT Workshop on Internet Economics March 1995)*
   `http://www.press.umich.edu/jep/works/FAQs.html`