А ТЫ ЧТО ВИДИШЬ? УДАЛЕННОЕ УПРАВЛЕНИЕ ПОСРЕДСТВОМ RDESKTOP, RADMIN, VNC

... сейчас мы нажимаем на контакты и перемещаемся к вам, но если эта машинка не сработает, тогда уж вы с нами переместитесь, куда мы вас переместим...
х/ф «Кин-Дза-Дза»

Время идет, ваша фирма развивается. Появилась ЛВС, сначала одноранговая, затем с выделенными серверами. Хорошо, когда сеть однородная, все работают в однотипной среде. Но жизнь диктует свои законы, в силу определенных причин ЛВС получилась гетерогенной. И не только гетерогенной, но и распределенной. Представьте себе машиностроительный завод или фирму с филиалами по всему городу. Что делать, как управлять всем этим IT-богатством?

АНТОН БОРИСОВ

Можно бегать, как горная лань, по этажам и цехам, объяснять, разъяснять, учить. Можно нанять дополнительный персонал. Научить бегать его. Однако запомните, что если вы лично претендуете на звание системного администратора, то главная черта, которая вам должна быть присуща – это лень! В хорошем смысле этого слова (см. статью Вячеслава Калошина «Каким видится хороший системный администратор» в июльском номере журнала за 2003 г.). Рассмотрим, как снизить расходы «на перемещение в пространстве и времени» бренного тела администратора.

Объяснять, как получить удаленное управление на UNIX-машинах я не буду. Считаю, что это известный факт. Цель этой статьи – показать, с помощью чего управлять с UNIX-машины парком серверов и рабочих станций с установленной ОС Windows.

Начнем, пожалуй, с серверов. По всей видимости, у вас установлены следующие семейства – Windows NT Terminal Server 4.0, Windows 2000 Server/Advanced Server, Windows 2003 Server, Datacenter и т. п. Отлично, это даже нам на руку. Проверим, что установлены терминальные службы удаленного доступа (terminal services).

```
bash-2.05b# nmap -v -sS compaq

Starting nmap 3.45 ( http://www.insecure.org/nmap/ ) at 2004-02-09 13:02 MSK
Host COMPAQ (192.168.0.13) appears to be up ... good.
Initiating SYN Stealth Scan against COMPAQ (192.168.0.13) at 13:02
Adding open port 135/tcp
Adding open port 139/tcp
Adding open port 1029/tcp
Adding open port 1530/tcp
Adding open port 5555/tcp
Adding open port 3389/tcp
Adding open port 3372/tcp
Adding open port 445/tcp
Adding open port 1027/tcp
The SYN Stealth Scan took 5 seconds to scan 1657 ports.
Interesting ports on COMPAQ (192.168.0.13):
(The 1648 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1027/tcp open  IIS
1029/tcp open  ms-lsa
1530/tcp open  rap-service
3372/tcp open  msdtc
3389/tcp open  ms-term-serv
5555/tcp open  freeciv
Nmap run completed -- 1 IP address (1 host up) scanned in 5.130 seconds

bash-2.05b# nmap -v -sS fuji
```

Чтобы узнать, какой именно порт отвечает за терминальные службы, поступим следующим образом:

```
bash-2.05b$ cat /usr/share/nmap/nmap-services | grep Remote\ Display
ms-term-serv    3389/tcp  # Microsoft Remote Display Protocol
```

А тем, у кого нет nmap, можно посмотреть весь список портов вот тут: http://www.iana.org/assignments/port-numbers. При установленной службе он будет присутствовать в системе.

Можете на самом Windows-сервере запустить cmd.exe и посмотреть порты, которые использует сервер в данный момент:

```
netstat -na | more (или netstat -na > netstat.txt)
```

Если портов с номером 3389 нет, то стоит добавить службу следующим образом: Пуск → Настройка → Добавление/Удаление Программ (Добавление Windows-компонентов).

В итоге получили работающую терминальную службу. Что дальше, спросит любопытный читатель?

Дальше сходим на сайт http://www.rdesktop.org и заберем исходники программы rdesktop. Она использует протокол RDP (т.е. протокол терминальной службы). Последняя версия 1.3 (на момент написания статьи). Настройка проста.

```
bash-2.05b$  ./configure  --prefix=/usr/local/rdesktop
bash-2.05b$ make
bash-2.05b# make install
```

Теперь пакет rdesktop установлен. Осуществляем соединение с удаленным сервером.

```
rdesktop rubin
```

Стоит отметить, что в некоторых случаях соединение может не заработать, а в ответ получим вот такую ошибку:

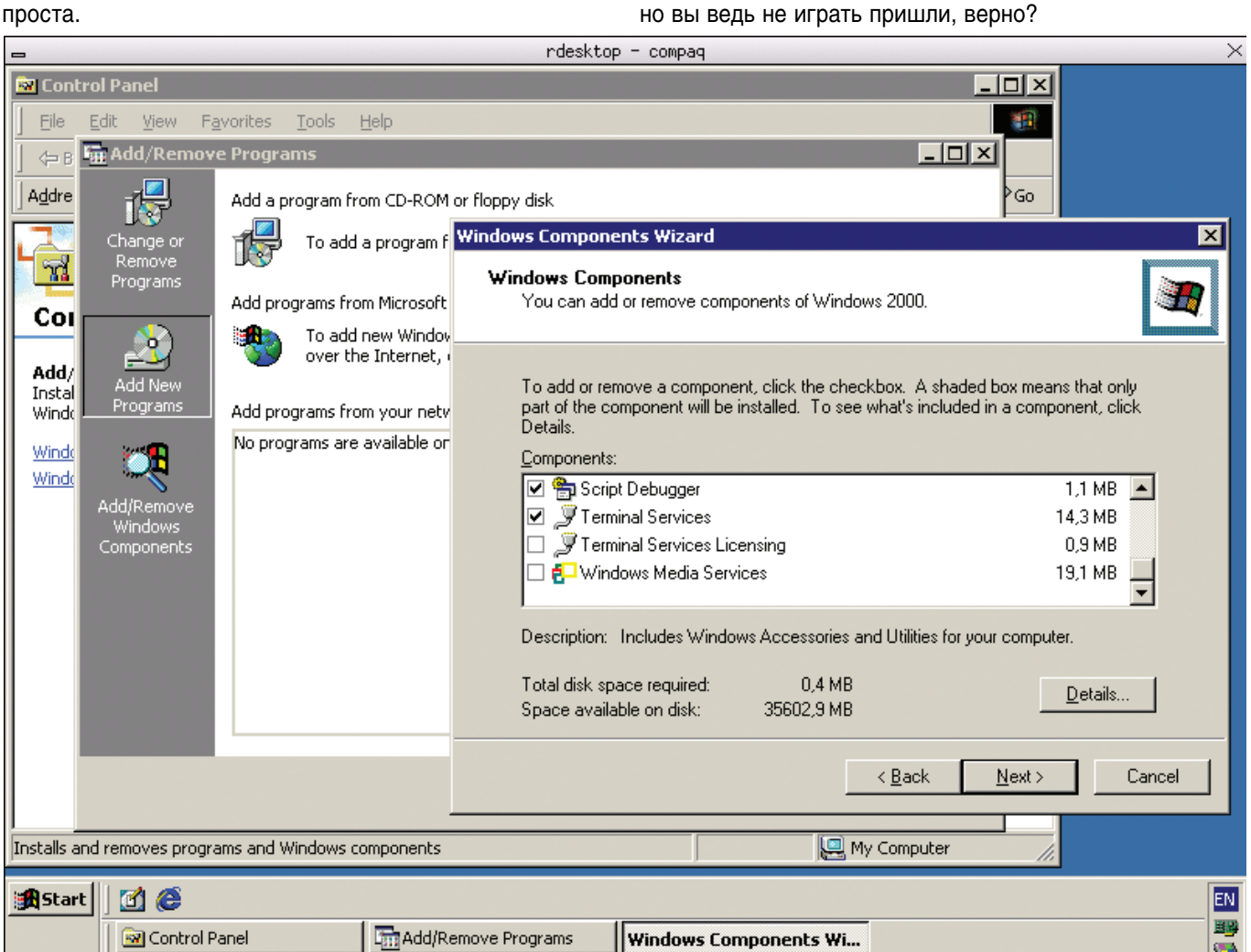
```
ERROR: recv: Connection reset by peer
Broken pip
```

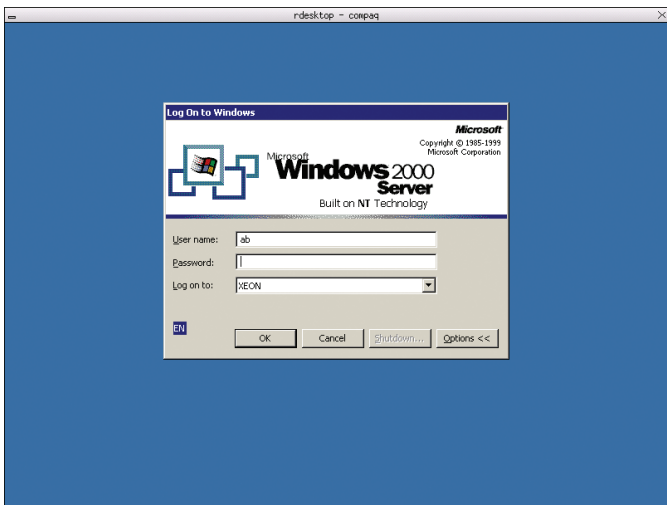
Проблема в том, что по умолчанию используется 5-я версия RDP-протокола, а некоторые сервера, не обращая внимания на все заплатки и обновления, продолжают говорить на 4-й версии. В таком случае нужно подать команду:

```
rdesktop -4 rubin
```

На что выдается окно MSGINA для ввода имени пользователя, пароля, домена (если таковой имеется).

Войдя в систему, мы работаем, как за родным Windows-терминалом. Есть некоторые специфические моменты, когда нельзя использовать удаленный вход (но об этом в другой раз). В общем, аскетично, т.к. только 256 цветов, но вы ведь не играть пришли, верно?





Во времена, когда администраторы были еще белыми и пушистыми, активную популярность приобрел пакет Remote Administrator.

Стоит отметить, что программа на момент своего появления на свет затмила свои аналоги. Одна из причин, из-за чего программу устанавливают, – это возможность показать оператору, работающему за удаленной машиной, что именно у него нажимается не так, ибо перехватывается управление как клавиатурой, так и мышкой. Среди дополнительных возможностей программы – наличие в некоторой степени аналога ftp-сервиса. Авторизовавшись на удаленной машине, появляется возможность перебросить туда файл с нашей локальной машины.

Еще один немаловажный момент – при нарушении настроек, например, swap-файл не прописался, удаленный/локальный пользователь не может зайти, т.к. окно приглашения не появляется. Что делать? Выбираем режим работы с удаленной машиной «File transfer» и удаляем неправильный swap-файл.

Но! Данный продукт написан под Windows-платформу. По заявлениям самих разработчиков, версию под UNIX-системы они разрабатывают, но как скоро она появится и появится ли вообще – неизвестно. Переустанавливать на всех клиентах что-то альтернативное, чтобы администратор мог со своей машины без затруднений управлять всем парком, – лишняя беготня. Нужна ли она? Как увидим чуть далее – нет.

Что нам потребуется для запуска?

Windows-эмулятор, он же wine. Пакет, если у вас его нет, заберем на http://www.winehq.com. Настройка аналогична настройке rdesktop.

Никаких дополнительных опций я не задавал. Префикс пути, где будет лежать пакет:

```
--prefix=/usr/local/wine
```

Обращаю ваше внимание, что пакет громоздкий – потребуется для сборки порядка 500 Мб. Плюс еще 260 Мб для готового к употреблению изделия.

Итак, собрали пакет, научились его запускать на простейших Windows-играх, например, «Сапер», «Паук» и т. д. Теперь устанавливаем у себя на Linux-машине Remote Administrator.

Несколько слов об установке. Цель – получить у себя каталог, например, «RAdmin» со следующими файлами:

```
-rw-r--r--   1 anthony  users    90112 Июл 10  2000 AdmDll.dll
-rw-r--r--   1 anthony  users     2504 Июл 24  2001 help.cnt
-rw-r--r--   1 anthony  users   187622 Июл 24  2001 help.hlp
-rw-r--r--   1 anthony  users     2281 Фев  8 04:01 license.txt
-rw-r--r--   1 anthony  users    29408 Июл  8  2000 raddrv.dll
-rwxr-xr-x   1 anthony  users  1093632 Июл 25  2001 radmin.exe
-rw-r--r--   1 anthony  users     8756 Июл 24  2001 README.TXT
-rwxr-xr-x   1 anthony  users   241664 Июл 24  2001 r_server.exe
-rwxr-xr-x   1 anthony  users    21019 Июл 25  2001 uninstal.exe
-rw-r--r--   1 anthony  users     2990 Фев  8 04:01 uninstal.ini
-rw-r--r--   1 anthony  users     4526 Июл 24  2001 WhatsNew.txt
```

Теперь приступим непосредственно к запуску radmin.exe. В домашей директории есть каталог, относящийся к wine – ~/.wine, где лежит файл конфигурации «config». Для того чтобы в дальнейшем не было проблем с фокусировкой мышки и клавиатурного ввода, добавим следующие строчки:

```
[AppDefaults\\radmin.exe\\x11drv]
"Desktop" = "700x500"
"Managed" = "N"
```

Строка «Desktop» = «700x500» означает, что для приложения radmin.exe необходимо использовать окно с геометрией 700 на 500 точек. Облегчает поиск нашего приложения radmin.exe, когда используется разный тип изменения фокуса в оконном менеджере. Из рисунка видно, что открываемое приложение не будет максимизировано оконным менеджером, а будет открыто с указанными размерами «горизонталь на вертикаль».

Строка «Managed» = «N» приводит к тому, что изменить размеры не получится. В любом случае смотрите документацию к wine.

Теперь мы готовы к запуску.

```
/usr/local/wine/bin/wine  ~/RAdmin/radmin.exe
```

Подразумевается, что мы установили пакет в каталог RAdmin. Далее введем регистрационный ключ и, вуаля, далее вопрос техники – заполнить имена хостов. С этого момента у нас полноценный доступ к другим машинам с установленной radmin-службой.

Скажу несколько слов об обратной связи. Запустив на Linux-машине radmin-сервис:

```
/usr/local/wine/bin/wine  ~/RAdmin/r_server.exe
```

с Windows-машин мы можем видеть рабочий экран Linux-машины. Правда, управлять нельзя, можно только наблюдать. Это лирическое отступление. Замечены некоторые проблемы с клавиатурой, а именно при нажатии комбинаций клавиш Shift+Key проявляется эффект «залипания» Shift. С чем это связано, неизвестно. Известно, как от этого избавиться. Нажать на настройке окна radmin.exe «Options», и залипание пропадет.

И напоследок посмотрим, что такое VNC.

VNC – Virtual Network Computing, пакет разрабатывался в лаборатории AT&T, сейчас доступен в свободной форме на сайте http://www.realvnc.com. Богатый ассортимент настроек, автоматическое определение необхо-

димой ширины канала для передачи информации и т. п. Например, в любой момент времени можно переключиться из TrueColor-режима в режим 256 цветов. Экономия на трафике.

Работа с использованием VNC-клиента с сервером аналогична двум предыдущим рассмотренным пакетам.

Нажимая F8, получаем возможность изменить на ходу настройки. Нажатие первый раз обрабатывает наш VNC-клиент, которого мы запустили у себя, второй раз уже обрабатывает сервер, где запущена VNC-служба. Службу можно определить по открытым портам 5800, 5900.

В качестве эксперимента я поставил VNC у себя в локальной сети на Linux-сервер под своим аккаунтом. Так что при перезагрузке вторая моя машина запускает автоматически VNC-сервис. Повторю, что поставил в качестве эксперимента, ибо никто не отменял комбинацию со вторым X-сервером и перенаправлением ввода с удаленной UNIX-машины на этот второй X-сервер.

Тем не менее опишу, как я провел сию операцию. Обе машины в локальной сети работают под slackware linux, поэтому настройки, которые я добавлял, находятся в каталоге /etc/rc.d/. Добавляю туда скрипт rc.vnc.

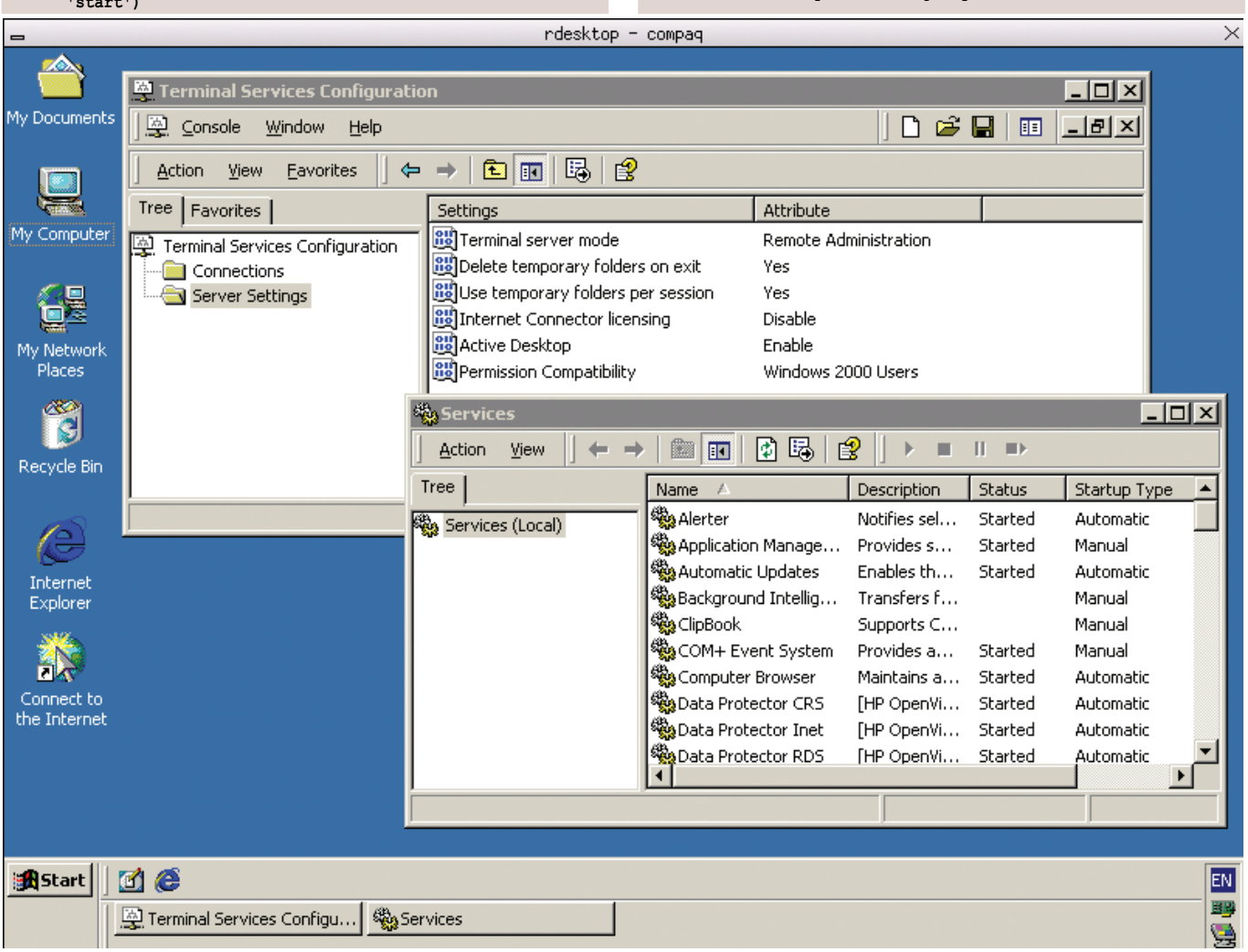
```
#!/bin/sh
# Start the Virtual Networking Communication (VNC) server
BINDIR=/usr/local/vnc
DAEMON=vncserver
case "$1" in
   'start')
      su - anthony -c "export PATH=$PATH:/usr/X11R6/bin:/usr/ ↵
            local/bin; $BINDIR/$DAEMON :10 -geometry 800x600"
     ;;
   'stop')
      $BINDIR/$DAEMON -kill :10
     ;;
   'restart')
      $0 stop; $0 start
     ;;
   *)
      echo "usage $0 start|stop|restart" ;;
esac
```

Для запуска нового сервиса сделаем упоминание также в файле /etc/rc.d/rc.local. Добавим строчки:

```
echo "***** Starting RealVNC server *****"
/etc/rc.d/rc.vnc start
```

Появляющийся сервис запускается с правами пользователя anthony, который присутствует в системе. Экспортирование пути необходимо, т.к. при запуске «su» автоматически переменная PATH заполняется значениями из /etc/login.defs. Мы же чуть-чуть увеличим путь, т.к. для запуска Xvnc необходимо, чтобы vncserver знал, где его найти, а также некоторые дополнительные программы. Сервис запускается с виртуальным экраном номер 10, поэтому для его обслуживания видим сразу 3 открытых для нужд VNC порта – это 5810, 5910 и 6010. Полная карта открытых портов на этой машине приведена ниже.

```
bash-2.05b# nmap -v -sS fuji -p 1-10000
```



```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host fuji.org (10.0.0.2) appears to be up ... good.
Initiating SYN Stealth Scan against fuji.org (10.0.0.2)
Adding open port 8000/tcp
Adding open port 111/tcp
Adding open port 515/tcp
Adding open port 22/tcp
Adding open port 80/tcp
Adding open port 21/tcp
Adding open port 113/tcp
Adding open port 139/tcp
Adding open port 8001/tcp
Adding open port 5810/tcp
Adding open port 6010/tcp
Adding open port 513/tcp
Adding open port 5910/tcp
The SYN Stealth Scan took 4 seconds to scan 10000 ports.
Interesting ports on fuji.org (10.0.0.2):
(The 9987 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
80/tcp     open        http
111/tcp    open        sunrpc
113/tcp    open        auth
139/tcp    open        netbios-ssn
513/tcp    open        login
515/tcp    open        printer
5810/tcp   open        unknown
5910/tcp   open        unknown
6010/tcp   open        unknown
8000/tcp   open        unknown
8001/tcp   open        unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds
```

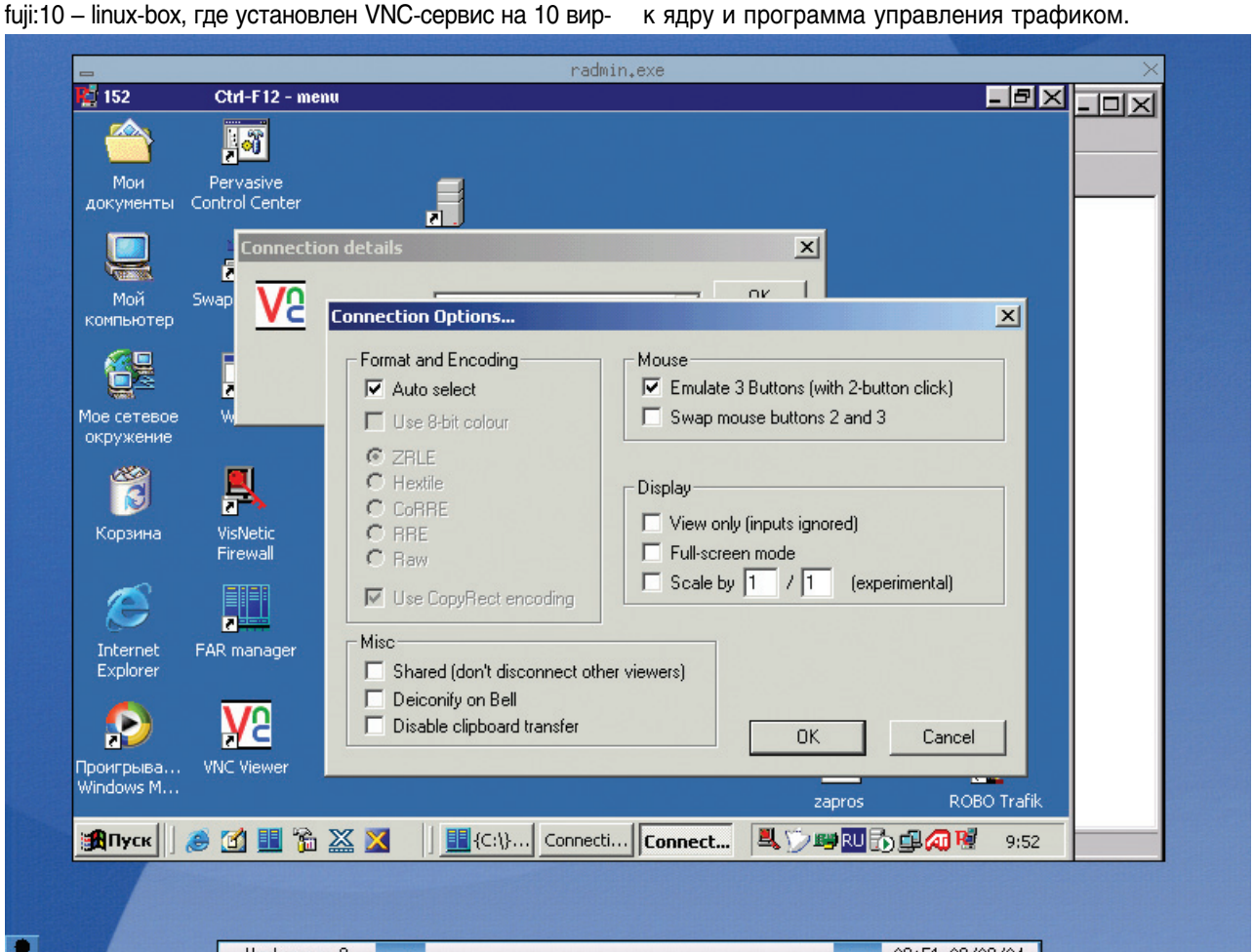
Чтобы запустить клиента, пишу следующую строчку:

```
vncviewer fuji:10 -passwd ~/.vnc/passwd -geometry 600x400
```

где fuji:10 – linux-box, где установлен VNC-сервис на 10 виртуальном экране, с помощью параметра «-geometry 600x400» указываю, что клиент надо запустить с разрешением 600 на 400 точек. Параметр «-passwd ~/.vnc/passwd» означает, что пароль можно не вводить, а брать по указанному месту. Кстати, он скопирован с машины, где запущен VNC-сервис.

Вот вроде бы и все. Работа с помощью VNC немного удобнее по сравнению с остальными. Хотя это мой субъективный взгляд. В качестве примера рассмотрим, как посчитать трафик, используемый каждым приложением. Я опишу, как на стомегабитной сетевой карте добиться скорости 9600 байт в секунду. Сия скоростная планка взята из желания посмотреть, насколько устойчиво будут работать рассмотренные приложения.

Не секрет, что до сих пор в некоторых местах используются телефонные линии с не очень хорошим качеством связи. Вы можете указать свою скорость, отличную от указанной, и проанализировать ситуацию. Считаю, что данный опыт будет полезен в случае, когда организация стоит перед выбором, какой тип соединения использовать для связи филиалов – ТФОП (телефонные линии общего доступа), беспроводной доступ или иной вид связи. Проанализировав на локальной сети центрального филиала, что именно подходит под ваши условия, вы делаете свой выбор. Чтобы «зажать» скорость в указанных пределах, я воспользовался traffic shaper – rshaper. Взять можно по указанному адресу: http://ar.linux.it/software/#rshaper. Сборка происходит через подачу команды make && make install. Пакет устанавливается в каталог /usr/local/sbin как модуль к ядру и программа управления трафиком.



В целом происходит следующее – данный модуль создает сетевой буфер, где пакеты задерживаются определенное время, в результате чего создается эффект «простаивания в очереди», т.е. создается определенная скорость. В нашем случае 9600 б/с на прием.

Нам еще потребуется, чтобы у вас в системе также был простейший брандмауэр, точнее настроены правила для iptables. Например, взятый здесь: http://www.faqs.org/docs/iptables/examplecode.html.

Сначала подгружаем shape-модуль:

```
modprobe rshaper.o
```

Модуль загружен, далее указываем, с каким хостом мы соединяемся, с какой скоростью и размер простаивания в буфере (в секундах):

```
rshaperctl HOST SPEED TIME
```

Затем выставляем правила для iptables для подсчета прошедшего трафика. Для входящего от хоста трафика:

```
iptables -N MyRDP_IN
iptables -I INPUT -j MyRDP_IN -s HOST
iptables -I MyRDP_IN -j INPUT
```

Для исходящего к хосту трафика:

```
iptables -N MyRDP_OUT
iptables -I OUTPUT -j MyRDP_OUT -d HOST
iptables -I MyRDP_OUT -j OUTPUT
```

Пролистать показания счетчика:

```
iptables -L MyRDP_IN -v
```

С теорией достаточно. Ближе к практике. Для этих целей составлен простейший скрипт, в котором задается скорость для shaper, происходит обнуление/показ прошедшего трафика.

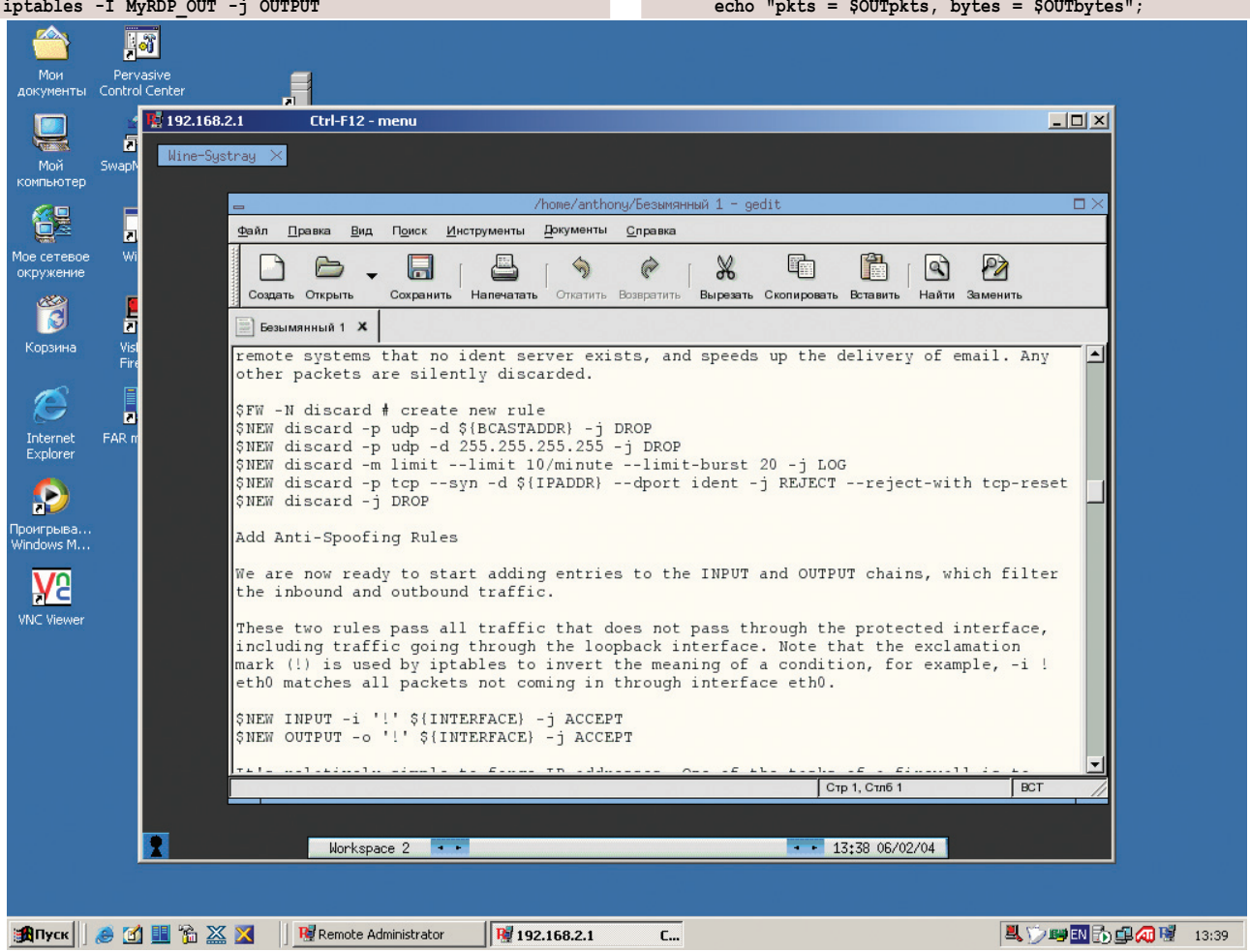
```
MyRDPTest.sh

#!/bin/sh

IPTL=/usr/sbin/iptables
SHAPER=/usr/local/sbin/rshaperctl
MODE=9600
HOST=rubin
TIME=10

    if [ "$1" = "zero" ]; then
           echo "Zeroing IN & OUT counters for $HOST";
           $IPTL -L MyRDP -Z 2>/dev/null 1>/dev/null
           $IPTL -L MyRDPOut -Z 2>/dev/null 1>/dev/null
    fi
    echo "Setting Shaping MODE as $MODE bytes to host $HOST"
    $SHAPER $HOST $MODE $TIME
    $SHAPER
    echo "Incoming traffic from host"
    IN=`$IPTL -L MyRDP -v -n | grep ACCEPT`
    INpkts=`echo $IN | awk '{ print $1 }'`
    INbytes=`echo $IN | awk '{ print $2 }'`
    echo "pkts = $INpkts, bytes = $INbytes";


    echo "Outcoming traffic to host"
    OUT=`$IPTL -L MyRDPOut -v -n | grep ACCEPT`
    OUTpkts=`echo $OUT | awk '{ print $1 }'`
    OUTbytes=`echo $OUT | awk '{ print $2 }'`
    echo "pkts = $OUTpkts, bytes = $OUTbytes";
```



Если скрипт вызван с параметром «zero», то счетчики для входящего (MyRDP) и исходящего (MyRDPOut) трафика будут обнулены. Вот какие цифры получились у меня после недолгой работы по разным протоколам с сервером по имени RUBIN. Скорость на прием – 9600 байт в секунду.

```
RDP протокол

     Incoming traffic from host
     pkts = 2604, bytes = 1039K
     Outcoming traffic to host
     pkts = 3563, bytes = 474K

VNC протокол

     Incoming traffic from host
     pkts = 6277, bytes = 804K
     Outcoming traffic to host
     pkts = 5413, bytes = 321K

RADMIN протокол
     Incoming traffic from host
     pkts = 2739, bytes = 472K
     Outcoming traffic to host
     pkts = 3610, bytes = 267K
```

Проводились типизированные действия. В частности, был запущен MPEG-клип через Media Player. Что следует отметить – при работе с RDP передавался n-ый кадр с заметными паузами для перерисовки. Остальные протоколы автоматически пропускали прорисовку кадров, простонапросто ничего не рисовали, т.е. старались не занимать канал «тяжелым» содержимым. Это касается только видео. В остальном субъективно было заметно, что RADMIN и VNC легче держат канал. Первый даже лучше, нежели VNC. Может на других скоростях получатся другие цифры, но это испытание мы оставим пытливому читателю.

Таблица 1. Информация о прошедшем трафике за 5-минутный период по разным протоколам

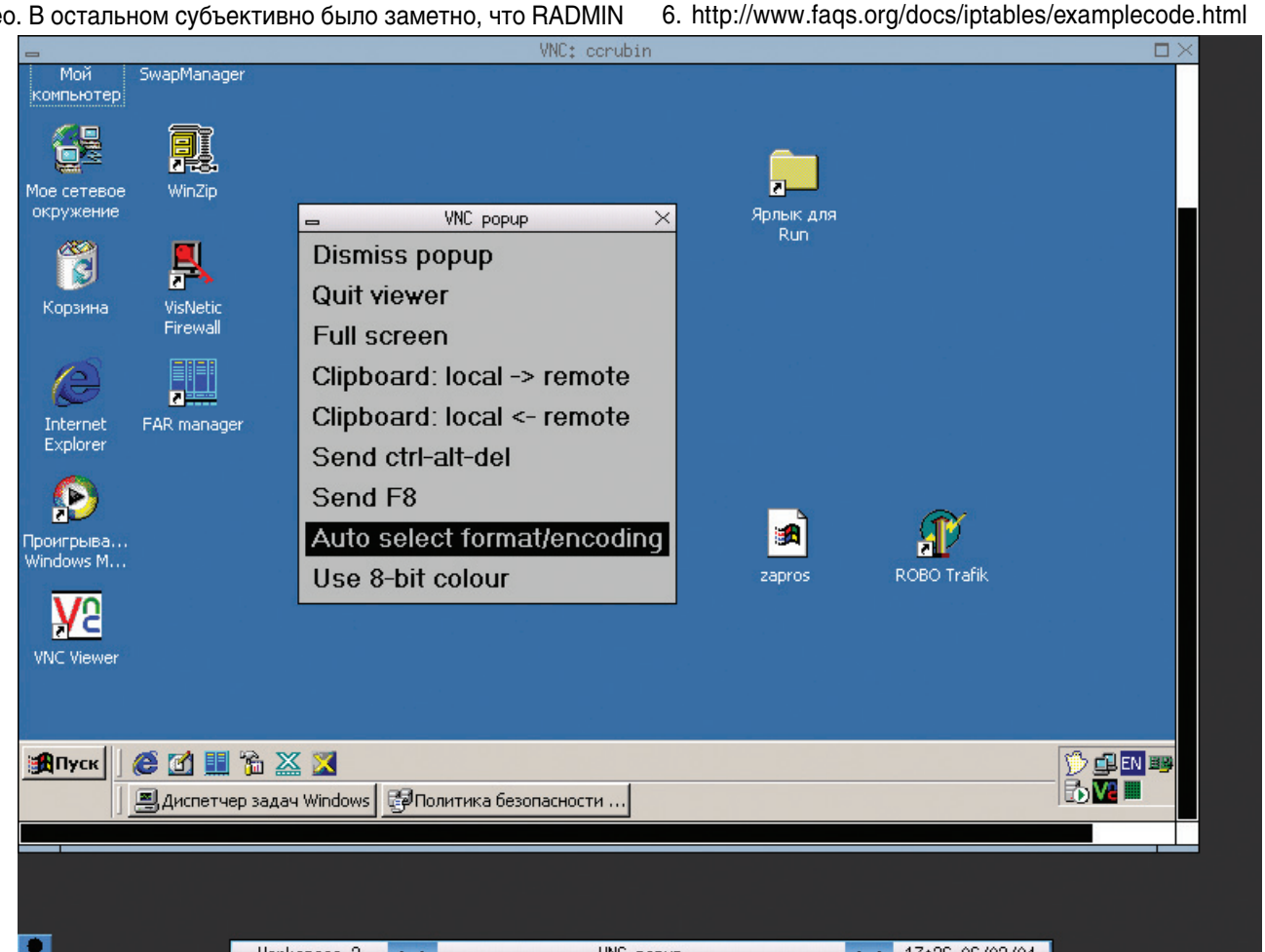
Название протокола	Входящий трафик (Кб)	Входящий трафик (кол-во пакетов)	Средний размер пакета (Кб)	Исходящий трафик (Кб)	Исходящий трафик (кол-во пакетов)	Средний размер пакета (Кб)
RDP	1039	2604	0,4	474	3563	0,13
VNC	804	6277	0,13	321	5413	0,06
RADMIN	472	2739	0,17	267	3610	0,07

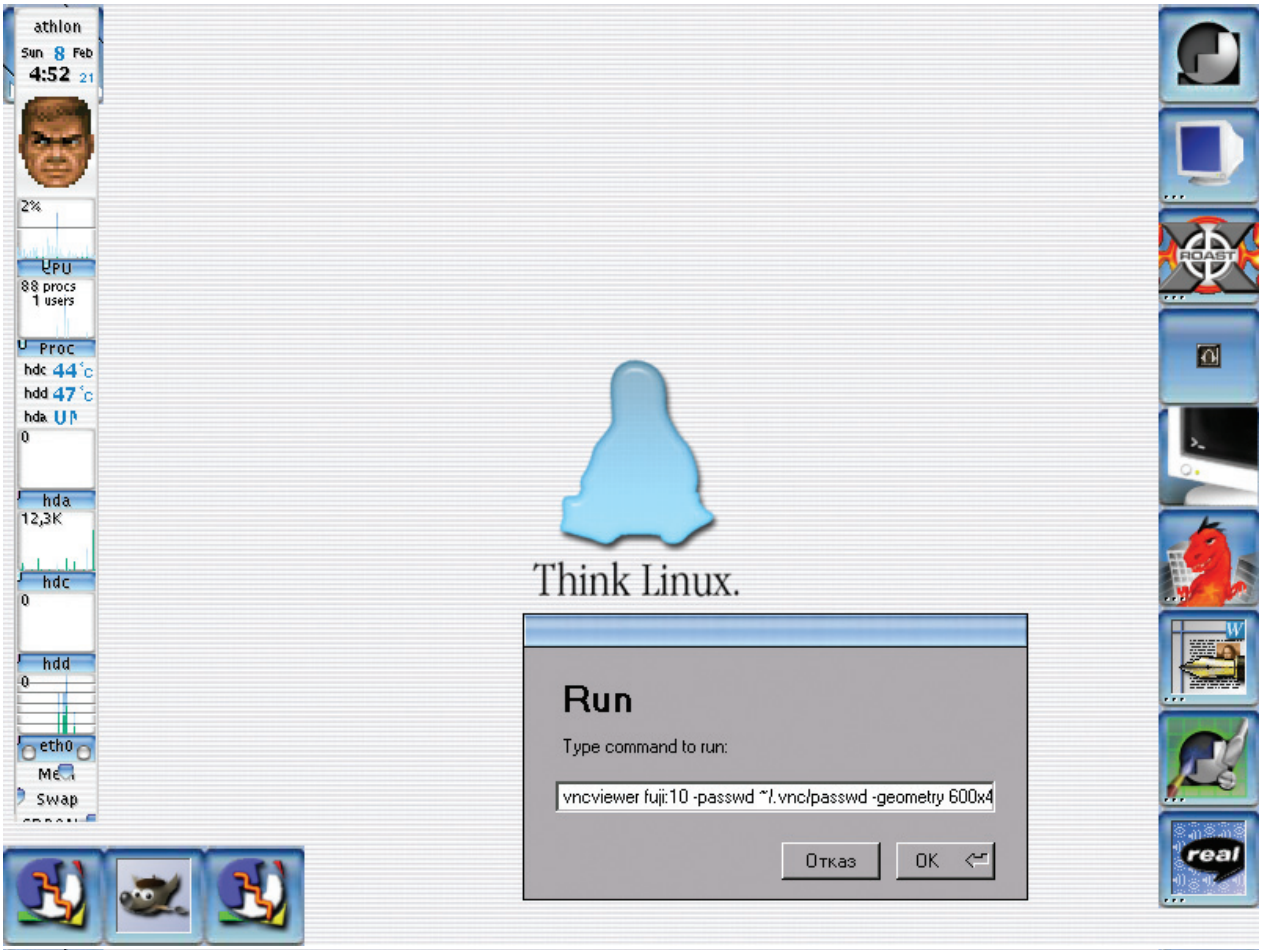
Я специально не стал освещать решения от компании Citrix, поскольку это отдельный серьезный разговор, т.к. заложенных возможностей в данный продукт хватит надолго и намного.

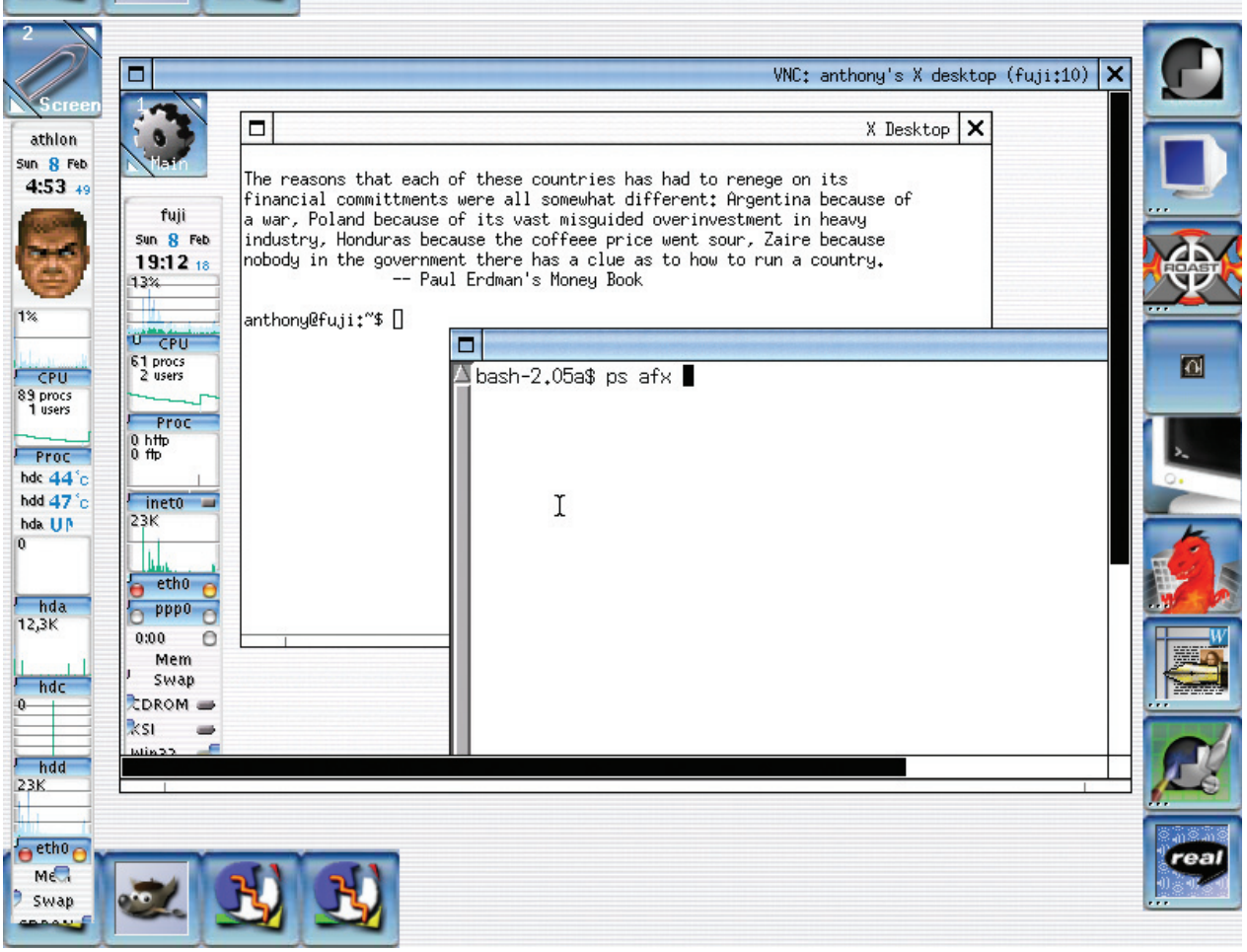
P.S. Всегда были и будут разговоры об эффективности и применимости удаленного доступа и открытых для этих целей дверей в системе. Приходится чем-то жертвовать, либо потенциально открыто, либо потенциально закрыто. Запомните, самый оптимальный с точки зрения безопасности стиль работы – держать администрируемую машину всегда выключенной.

В статье были упомянуты программы со следующих ресурсов:

1. http://www.rdesktop.com
2. http://www.radmin.com
3. http://www.winehq.com
4. http://www.realvnc.com
5. http://ar.linux.it/software/#rshaper
6. http://www.faqs.org/docs/iptables/examplecode.html




athlon
Sun 8 Feb
4:52 21
2%
CPU
88 procs
1 users
Proc
hdc 44°C
hdd 47°C
hda UP
hda
12,3K
hdc
hdd
eth0
Mem
Swap
Think Linux.
Run
Type command to run:
vncviewer fuji:10 -passwd ~/.vnc/passwd -geometry 600x4
Отказ
OK
real


2
Screen
athlon
Sun 8 Feb
4:53 49
1%
CPU
89 procs
1 users
Proc
hdc 44°C
hdd 47°C
hda UP
hda
12,3K
hdc
hdd
23K
eth0
Mem
Swap
VNC: anthony's X desktop (fuji:10)
1
Main
fuji
Sun 8 Feb
19:12 18
13%
CPU
61 procs
2 users
Proc
0 http
0 ftp
inet0
23K
eth0
ppp0
0:00
Mem
Swap
CDROM
KSI
X Desktop
The reasons that each of these countries has had to renege on its
financial committments were all somewhat different: Argentina because of
a war, Poland because of its vast misguided overinvestment in heavy
industry, Honduras because the coffeee price went sour, Zaire because
nobody in the government there has a clue as to how to run a country.
-- Paul Erdman's Money Book
anthony@fuji:~$
bash-2.05a$ ps afx
real