

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ЗАДАНИЯ
К самостоятельной работе студентов по курсу
«Протоколы компьютерных сетей»
(для студентов специальности “Программное обеспечение АС”)

Кафедра ПМИИ, ДОННТУ

Донецк -2011

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ЗАДАНИЯ
К самостоятельной работе студентов по курсу
«Протоколы компьютерных сетей»
(для студентов специальности “Программное обеспечение АС”)

Рассмотрено на заседании кафедры
ПМИИ

Протокол № 7 от 20.12.2010

Утверждено на заседании
учебно-издательского Совета ДонНТУ
протокол № от

Донецк –2011

Методические указания и задания к самостоятельной работе студентов по курсу «Протоколы компьютерных сетей» для студентов специальности «Программное обеспечение АС»/ Сост.: Чернышова А.В. - Донецк, ДонНТУ, 2011 - 30 стр.

Приведены методические указания и задания к выполнению индивидуальной работы по курсу «Протоколы компьютерных сетей» для студентов специальности «Программное обеспечение АС». Приводится обзор программных средств для мониторинга сети и сетевых подключений с целью ознакомления студентов с возможностями работы протоколов стека TCP/IP и удаленного администрирования сети.

Методические указания предназначены для усвоения теоретических основ и формирования практических навыков по курсу «Протоколы компьютерных сетей».

Составители: ст.преп. кафедры ПМИИ Чернышова А.В.

Рецензент: доцент кафедры КСМ Губенко Н.Е.

Индивидуальное задание №1

Тема: Изучение возможностей программ NetView и Fpinger для анализа и мониторинга сетевых подключений. Анализ систем для удаленного администрирования.

Цель: Установка и настройка программ NetView и Fpinger, изучение основных возможностей программы NetView и Fpinger, анализ систем удаленного администрирования, разработанных на основе протокола VNC.

Методические указания к выполнению индивидуальной работы

Описание программы NetView

Программа NetView предназначена для анализа сетевого окружения, сбора данных о доступных сетевых ресурсах. В качестве основных возможностей можно выделить следующие:

- получение доступа к рабочим станциям;
- получение доступа к HTTP и FTP серверам;
- получение детальной информации о рабочей станции - IP и MAC адреса, тип установленной ОС, список работающих на компьютере сетевых сервисов, список пользователей в системе, список подключенных к доступным ресурсам компьютеров, время на удаленной машине, какие порты открыты на машине;
- возможность выполнения поиска файлов в сети;
- мониторинг активных сетевых подключений, с возможностью создания «черного» и «белого» списков;
- отслеживание соединения с заданными портами (полезно для обнаружения IP-адресов, с которых проводятся попытки установить соединения на “троянские” порты или выполнение попытки сканирования портов). Имеет функцию «Scan chaser», при включении которой удаленный сканер портов показывает практически все порты, которые открыты. Имеется поддержка скриптов, позволяющая в простейшем случае эмулировать серверные службы;
- встроенный «Terminal», основанный на скриптах, позволяющий подключаться к любому выбранному порту либо его прослушивать. Также может использоваться IRC, telnet, pop3 или любым другим текстовым протоколом;
- «NetMessenger» - позволяет слать сообщения Windows Messenger. Аналог NET SEND с возможностью отправки сообщений от произвольного имени.
- «TraceRoute» - аналог утилиты tracert. Отображение машин либо в виде списка, либо в виде дерева сегментов (используется traceroute). Карта составляется и обновляется практически автоматически. Также возможно отображение в виде визуальной карты, с возможностью задания произвольных иконок для компьютеров.

- «Traffic Redirector» - позволяет прослушивать входящие соединения на заданный (свободный) порт и перенаправлять их на другой порт другого IP.

Огромным достоинством данной программы является ее доступность. Программа является абсолютно бесплатной, также доступны и исходные коды почти всех модулей.

Рассмотрим интерфейс программы. Главное окно программы NetView представлено на рисунке 1.

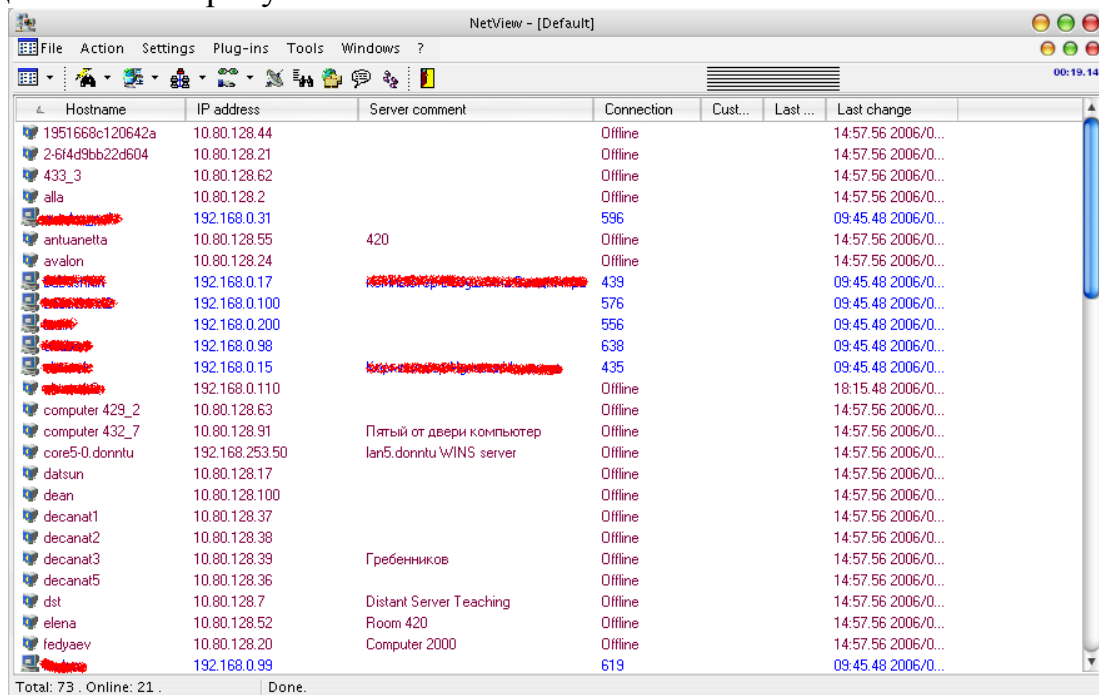


Рисунок 1 - Основное окно программы

Основное окно программы содержит список всех компьютеров в сети (имя, IP-адрес, комментарии, наличие соединения)

Хост-лист (рис. 1) – это объект, содержащий узлы, линии и области визуальной карты. Хосты могут отображаться различными цветами в зависимости от текущего состояния offline, online, opened и alarm. Узел находится в состоянии «Opened», если он открывался хотя бы один раз в текущем сеансе работы. Узел находится в состоянии «Alarm», если для него выполнено оповещение, например, о том, что он выключился. При этом он будет находиться в таком состоянии до тех пор, пока пользователь не щелкнет по записи мышью. Узлы можно переносить из одного хост-листа в другой, указав нужный хост-лист в поле Hostlist окна редактирования свойств компьютера. Можно включить автоматическую группировку узлов по имени рабочей группы, либо по первым трем цифрам их IP-адреса. Это задается в главном меню-> «Settings»-> «Autosplit». Там же можно отключить автогруппировку или перенести все узлы в основной хост-лист. В настройках можно включить пункт Delete empty lists для того, чтобы автоматически удалялись пустые хост-листы. Данные всех хост-листов NetView хранит в файле (по умолчанию default.nvh, либо default.sam). Информация хост-листа может представляться в четырех видах, которые можно переключать из контекстного меню-> «Current sublist»-> «View as»:

1 – Список. В этом случае отображаются только иконки, соответствующие состояниям хостов и их названия. Дополнительная информация, такая как IP, рабочая группа, состояние, заметки отображаются во всплывающей подсказке при наведении мышки на хост.

2 – Детально. Информация отображается в виде списка со столбцами (столбец имен, IP адресов и тд). Столбцы можно менять в окне редактирования хост-листа. Ширину столбцов и сортировку также можно менять, она сохраняется в файле хост-листа и восстанавливается при следующем запуске. Если хост-лист не сохранить перед выходом, и если выключено «Autosave hostlist» в настройках, то эта информация также не сохранится.

Колонки:

- «Hostname» – имя узла, собственное, либо DNS.
- «IP address» – IP-адрес.

Следующие столбцы включены и настроены по умолчанию, но их можно изменить в окне редактирования хост-листа:

- «Server comment» - комментарий сервера. Устанавливается на самом сервере. Виден только если при обновлении списка машин хост был включен.

- «Connection» - значение в миллисекундах задержки ICMP эхо-ответа, при включенной проверке PINGами, задержка установления соединения, при включенной проверке соединением на заданный порт, либо количество ресурсов на хосте, если включен «Enum shares on host».

- «Custom» - редактируемый Вами комментарий к хосту.

- «Last time» - время последнего открытия компьютера, с момента запуска NetView.

- «Last change» - время/дата последнего изменения online/offline состояния хоста.

3 – Визуальный план. Уменьшенная в 2 раза визуальная карта без возможности редактирования.

4 – Визуальная карта. Этот режим предназначен для визуализации компьютерной сети. Вы можете ставить компьютеры в любое место на карте, соединять их различными линиями, задавать им различные картинки, зависящие от состояния узла. Хосты можно также объединять в прямоугольные области, и щелкнув правой кнопкой мыши в любое место области, можно перепроверить все узлы в ней, выбрав пункт меню «Recheck area». Для того чтобы изменить название области и цвет ее границ нужно щелкнуть правой кнопкой в любое место внутри ее и выбрать «Edit area label». После изменения текста и цвета, нужно нажать Enter, либо Esc для отмены. Линии на карте рисуются с помощью пункта контекстного меню «Start line». Начните рисовать линию, левым щелчком добавляется узел, правым рисование линии завершается, и она закрепится на карте. Для удаления любой линии просто щелкните на ней правой кнопкой и выберите «Delete line». Линии могут быть различной толщины, цветов и стиля. Редактируются эти параметры из контекстного меню -> «Edit line». При этом

Вы попадете в окно конфигурации хост-листа, все параметры, касающиеся линий, будут задавать только выделенную линию. Картинки, изображающие устройства, задаются при их редактировании. Размеры карты и фоновую текстуру можно также менять, для этого надо щелкнуть правой кнопкой по карте и выбрать «Current sublist»-> «Settings». Объекты можно произвольно таскать по карте. Можно выделить сразу несколько узлов линий, узлов и областей и переносить их вместе. Можно нажав левой кнопкой на заголовок какой-нибудь области выделить ее и все находящиеся в ней объекты, чтобы затем переносить все вместе. Можно менять размер областей.

5 – Карта маршрута

На карте маршрутов показана схема соединения узлов сети. Составляется она путем выбора пункта меню «Retrace all» главного меню либо путем трассирования выделенных хостов или текущего хост-листа через контекстное меню хост-листа. При этом следует учесть, что некоторые серверы могут ограничивать количество ICMP-запросов с Вашего компьютера, что может привести к трассировке не всех узлов. В этом случае следует пользоваться пунктом «Trace all» главного меню - он трассирует только те узлы, маршрут до которых еще не был успешно найден. Просто нажимайте его несколько раз, пока количество узлов на карте не перестанет добавляться. Информация этой карты сохраняется с хост-листом в .lvh файл и может экспортироваться в файл формата .txt через подменю «File» главного меню. Карта также имеет контекстное меню с основными функциями - открыть хост, перепроверить, трассировать, редактировать, удалить из хост-листа, посмотреть свойства. Пункт меню «Delete from map» удаляет узел вместе со всеми дочерними из карты маршрутов, сохраняя их в хост-листе. «Clear route map» очищает карту маршрутов.

Довольно часто бывает необходимым произвести поиск каких-либо файлов, которые могут находиться на различных узлах сети, например, поиск технической литературы, музыки. В рассматриваемой программе имеется возможность выполнения поиска файлов среди всех узлов сети. На рисунке 2 представлено окно поиска файлов (NetSearcher)

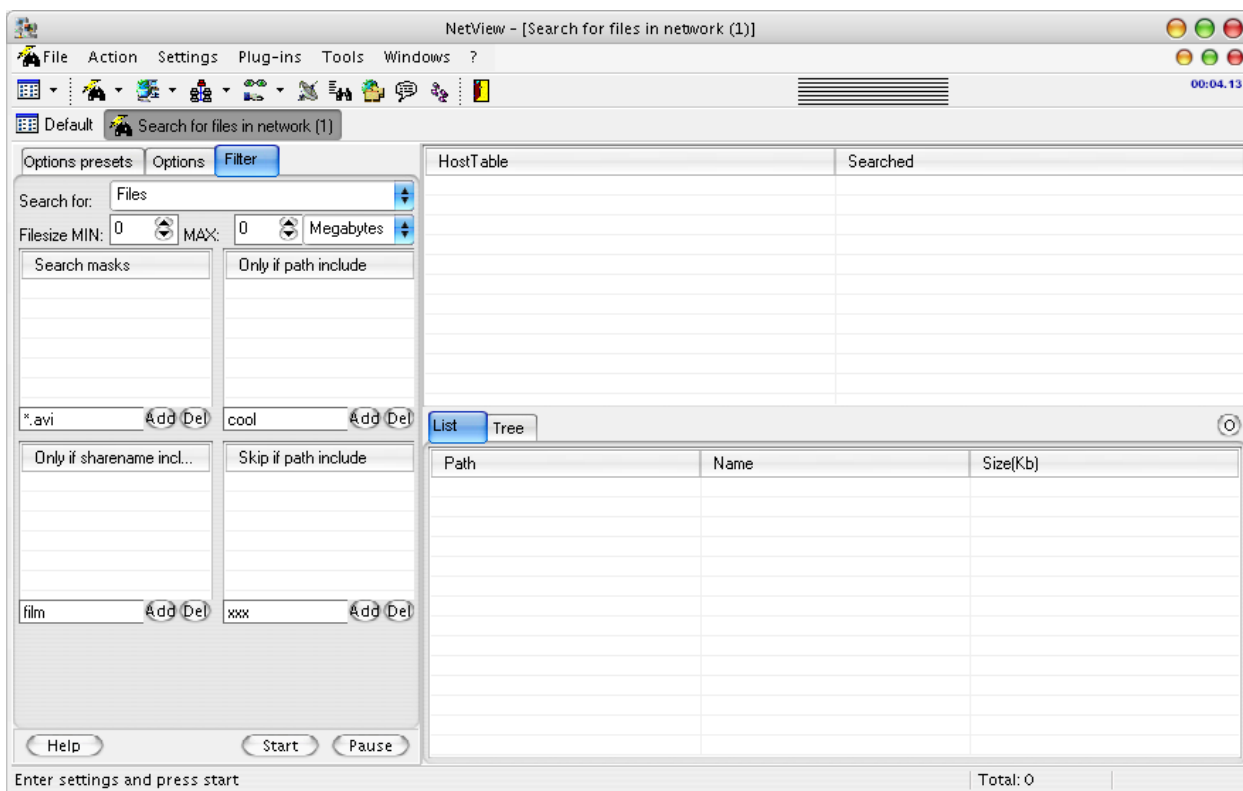


Рисунок 2 - Окно поиска файлов по сети

Это поисковик файлов в сети, позволяющий искать файлы и каталоги по заданным маскам (нескольким одновременно), размеру файла. Есть возможность выполнять поиск файлов как по NETBIOS, так и по FTP протоколам. Можно редактировать список машин, подлежащих поиску, сохранять результаты поиска в текстовый файл либо в .html виде с ссылками. Поиск может вестись в циклическом режиме, пока не будет выполнено сканирование всех машин списка. Используется многопоточковый механизм поиска, значительно ускоряющий поиск. Найденные файлы можно автоматически скачать во время или в конце поиска. Настройки поиска можно сохранять. Поиск файлов может работать в режиме обновления списка - периодически начиная поиск, добавляя в список новые файлы и удаляя те, которые он не видел больше указанного количества часов.

Рассмотрим настройки:

«Time limit» - ограничение времени на сканирование одного хоста. Если какой-то хост сканируется время большее, чем здесь указано - он автоматически пропускается (в поле «Searched» ставится "yes").

«Cycled searching» - режим циклического поиска, при котором поиск проводится циклически, пока для всех хостов не будет Searched="yes" или пока поиск не будет прерван вручную нажатием кнопки "Stop";

«Save filelist on finish» - при включенном флажке список файлов будет сохранен автоматически после окончания процесса поиска. При щелчке по этому флажку открывается окно, в котором указываются опции сохранения списка файлов.

«Recheck hosts» - перепроверять хост перед тем, как искать файлы. Экономит время, если в списке много выключенных машин.

«Autosearch on» – автоматическое начало сканирования по таймеру. В Формат задания времени начала автоматического сканирования: "08:10;10:45;16:30" или "06:30".

«Threads count» - максимально количество потоков одновременного поиска (каждый поток сканирует отдельный хост одновременно с другими, что ускоряет поиск, но на слабых машинах с установленной Win 9x большое количество потоков может значительно замедлить работу системы).

«Priority» - приоритет потоков. Малое значение замедляет поиск при одновременном выполнении других программ, большое - замедляет другие программы.

«Use script» - позволяет задать скрипт из каталога \Scripts\Searcher, который может обрабатывать результаты поиска файлов.

«Enable list-update mode» - включает режим обновления списка файлов, при котором поисковая система при сохранении списка файлов в файл автоматически сохраняет состояние списка во временный .sfl файл в каталоге NetView, при следующем поиске NetView загрузит этот файл и будет добавлять туда лишь новые файлы.

«Delete if not found on searched» - после завершения поиска «NetSearcher» проходит по созданному списку файлов, удаляет из него те файлы, которые были удалены с хостов, на которых был успешно проведен поиск

«Display files as new for» - здесь можно указать в течение скольких часов после первого нахождения поисковик будет считать файлы новыми. Новые файлы выделяются в html списке цветом.

«Delete files not refreshed for» - если нужно, чтобы старые файлы, которых поисковик не видел в течение определенного периода времени, удалялись автоматически - включите эту опцию и укажите, по истечении скольких часов после последнего обнаружения файлы будут удаляться.

Терминал (Terminal) - средство, позволяющее подключаться к удаленному IP/порту и работать в терминальном режиме.

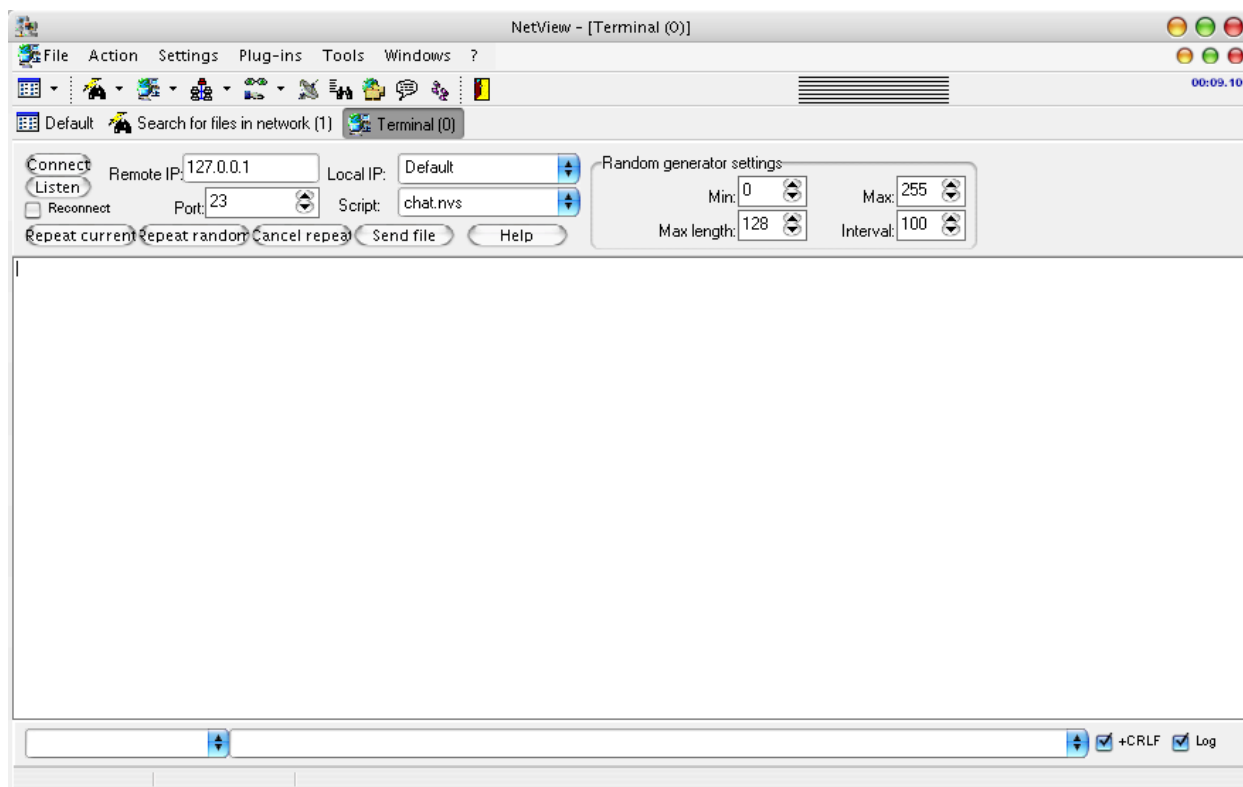


Рисунок 3 – Окно вкладки «Терминал»

Если в системе установлено несколько IP, можно выбрать локальный адрес, с которого устанавливается подключение. Кнопкой «Send file» можно послать небольшой файл. Терминал также можно использовать для ожидания входящих соединений (server). Для этого надо выбрать локальный порт и адрес и нажать «Listen». Обработкой поступающего потока информации и выводом на экран занимаются скрипты терминала.

TCP мост (Traffic redirector) – «слушает» соединения на указанный порт, и при запросе на соединение устанавливает соединение с удаленным сервером на любой порт, и в дальнейшем перенаправляет трафик между ними.

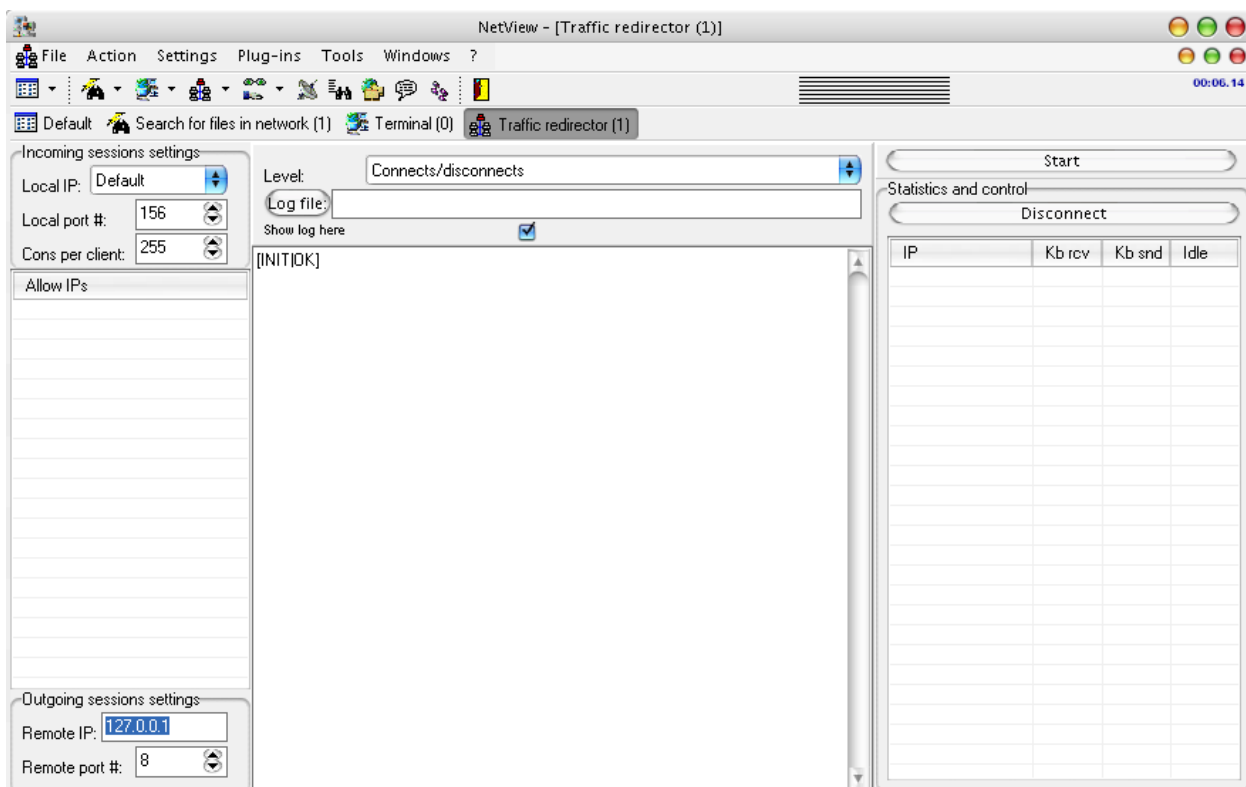


Рисунок 4 - Окно вкладки «Traffic redirector»

Traffic redirector позволяет задавать разрешенные IP адреса, отключать любое соединение принудительно, ведет лог (3 уровня детализации). Полезно, например, если Вы хотите, чтобы через Вас кто-то мог подключиться к сервису на другом компьютере, к которому Вы имеете доступ, а этот кто-то нет.

Монитор подключений (NetWatcher) - монитор активных сетевых соединений.



Рисунок 5 - Монитор подключений (NetWatcher) (вкладка Статистика)

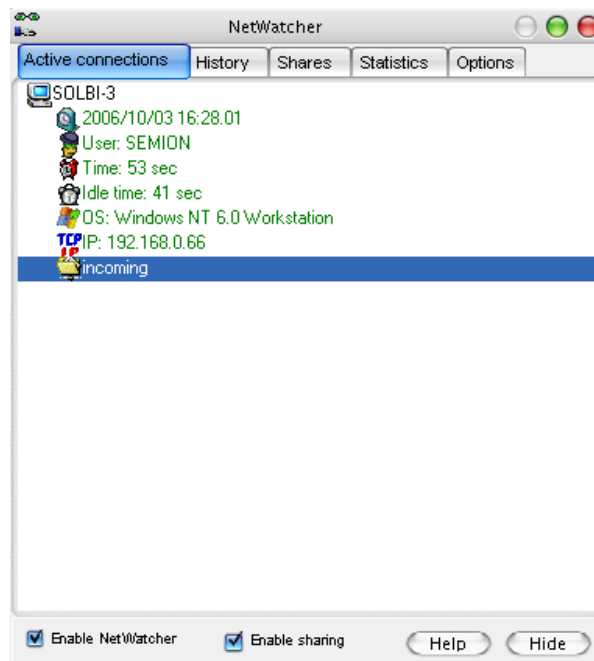


Рисунок 6 - Монитор подключений (NetWatcher)
(вкладка Активные соединения)

«NetWatcher» - Позволяет видеть, что скачивается с Вашего компьютера в данный момент и в недалеком прошлом. Можно прервать любую сессию. Ведется лог соединений, в котором пишется имя и IP-адрес компьютера, имя пользователя, установившего сессию, тип используемой ОС и все открытые за сессию файлы. Файлы, открытые для чтения, рисуются зеленым цветом, для записи - фиолетовым, а созданные - красным. Есть функция «черного» и «белого» списков. По умолчанию любой пользователь из «черного» списка отключается автоматически. Можно поставить отключение всех пользователей, кроме «белого» списка. Также выводится статистика по службам SERVER и WORKSTATION в системе.

Вкладка «Active connections» – просмотр всех текущих подключений и открытых файлов. Как только файл закрывается, он автоматически переносится в «History». Файлы, открытые для чтения, отмечены синим, для записи - фиолетовым, созданные - красным цветами. Ресурсы, открытые в сессии, также отображаются здесь, но коричневым цветом.

Вкладка «History» - история всех соединений. Хранится в лог-файле. Размер ее для удобства чтения может быть ограничен максимальным количеством клиентов.

Вкладка «Shares» - список доступных ресурсов на Вашем компьютере.

Вкладка «Options» - здесь находятся все настройки «NetWatcher» и kick/keep/popup/skip списки пользователей. В списки можно вносить либо просто пользователей, либо делать ограничения различным пользователям на различные ресурсы. «Skip-лист» - это список компьютеров, которые не будут вноситься в лог.

Здесь же задаются горячие клавиши для вызова окна «NetWatcher» и отключения всех подключенных на данный момент пользователей.

IP монитор (IP logger) - Выводит список текущих TCP/UDP соединений.

Proto	Local addr	Local port	Remote addr	Remote port	Status	Process
TCP	0.0.0.0	135 (epmap)	0.0.0.0	55525	Listen	svchost.exe
TCP	0.0.0.0	445 (microsoft-ds)	0.0.0.0	2272	Listen	System
TCP	0.0.0.0	803	0.0.0.0	14436	Listen	outpost.exe
TCP	0.0.0.0	1433 (ms-sql-s)	0.0.0.0	20725	Listen	sqlservr.exe
TCP	127.0.0.1	1033	0.0.0.0	49346	Listen	alg.exe
TCP	192.168.0.254	139 (netbios-ssn)	0.0.0.0	14567	Listen	System
UDP	0.0.0.0	445 (microsoft-ds)				System
UDP	0.0.0.0	500 (isakmp)				lsass.exe
UDP	0.0.0.0	1242				svchost.exe
UDP	0.0.0.0	1434 (ms-sql-m)				sqlservr.exe
UDP	0.0.0.0	4500				lsass.exe
UDP	127.0.0.1	123 (ntp)				svchost.exe
UDP	127.0.0.1	1900				svchost.exe
UDP	192.168.0.254	123 (ntp)				svchost.exe
UDP	192.168.0.254	137 (netbios-ns)				System
UDP	192.168.0.254	138 (netbios-dgm)				System
UDP	192.168.0.254	1900				svchost.exe

TCP: 6 UDP: 11 | Portset: main-0, chaser-0, queue-0, scripts-0.

Рисунок 7 - IP монитор (IP logger)

«IP logger» выводит имя процесса, который использует открытый порт. Работает только на Win XP, выводит также статистику по протоколам TCP, IP, ICMP. Имеет функцию предупреждения о сетевых DOS атаках типа SYN, UDP и ICMP flood. Для этого необходимо установить порог срабатывания оповещения. Для ICMP и SYN пакетов можно установить ~100 запросов в секунду. Если количество запросов будет превышать это число, прозвучит сигнал оповещения. С помощью IP logger можно вести логи установленных соединений, причем можно использовать фильтрацию лога.

Сканер сети (Network scanner) - Сканер, позволяющий находить открытые порты на одном, либо диапазоне IP адресов.

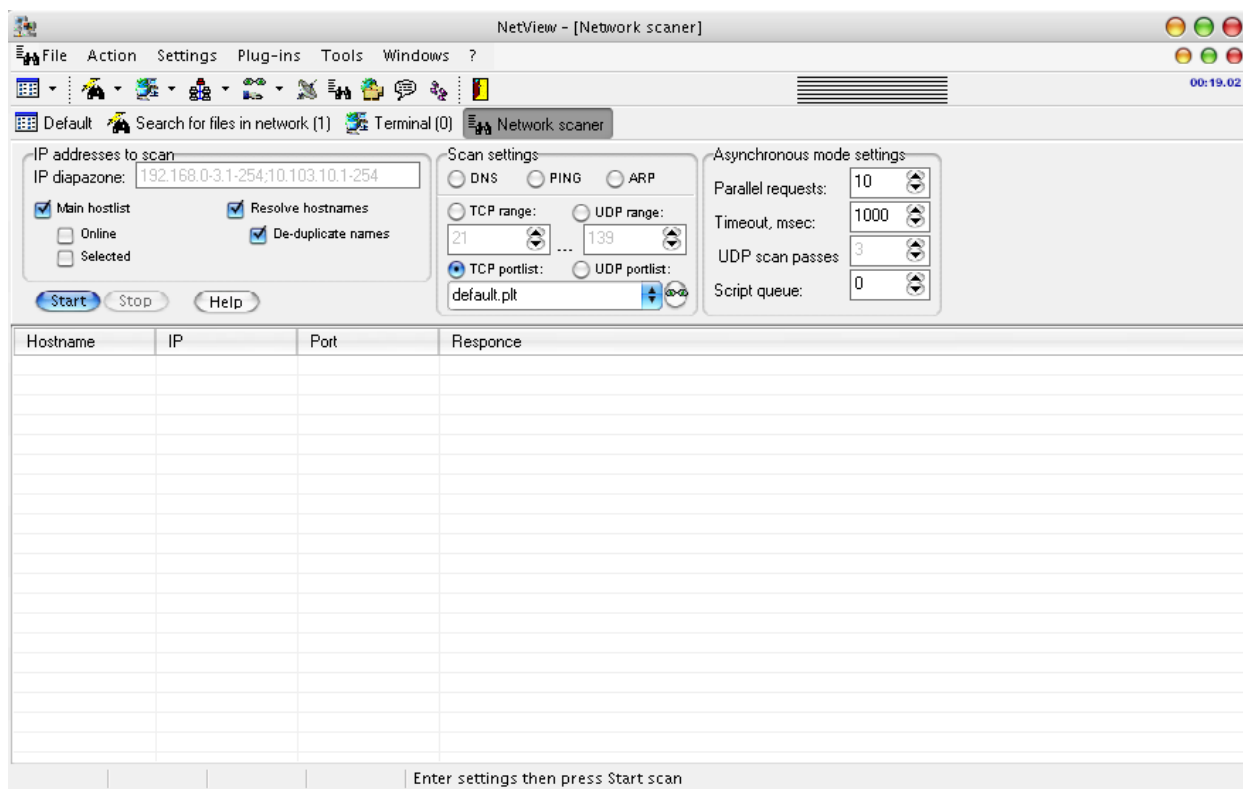


Рисунок 8 - Сканер сети (Network scanner)

Порты можно сканировать также в каком-то диапазоне, либо по списку в файле. При нахождении IP-адреса автоматически определяется соответствующее имя компьютера, которое тут же можно внести в общий список. Если удаленный компьютер сразу после соединения посылает какую-либо строку, она выводится в столбце «Response». Есть возможность перебирать IP-адреса, находя те, которые прописаны в DNS, или пинговать диапазон, или составленный список IP адресов. Также можно сканировать узлы из хост-листов - для этого включите «Main hostlist». Если включить «Online» сканер, будет сканировать только включенные узлы, что ускорит процесс сканирования. Можно выделить несколько узлов в списке и включив «Selected» просканировать только их. Опция «Parallel requests» регулирует максимально число одновременных запросов. «Timeout» - время ожидания ответа на каждый запрос, не работает для DNS и ARP сканирования.

Описание типов сканирования:

- DNS - сканер последовательно пытается определить имена у всех IP-адресов. Если имя определяется - то адрес и имя вносятся в список найденных.
- PING - сканер последовательно пингует все адреса, в список найденных добавляются те, которые ответили на запрос. В «Response» пишется задержка эхо-ответа в миллисекундах.
- ARP - сканер последовательно шлет ARP-запросы на определение MAC-адреса каждого IP. Работает только в пределах сегмента (до маршрутизатора). В поле «Response» записываются найденные MAC адреса.

- TCP - сканер сканирует IP адреса, пытаясь подключиться к портам из диапазона или файла - списка портов. Возможно исполнение скриптов при нахождении открытых портов. Скрипты могут подробно исследовать удаленные системы. В столбце «Response» пишется либо результат исследования скрипта, либо, если скрипта для найденного порта нет, - строка, которую шлет удаленный хост сразу при подключении.

- UDP - сканер сканирует UDP порты на указанных адресах следующим методом: вначале NetView посылает на указанные порты пакет с данными размером 1 байт. Затем, через указанный интервал времени проверяет, на какой из портов пришел отклик ICMP «Destination port unreachable» и исключает их из списка открытых портов. Затем повторно обходит те же порты и делает это столько раз, сколько указано в UDP «scan passes» каждый раз, исключая закрытые порты. Отсюда и особенность сканирования - при сканировании, например выключенного или заблокированного файрволом IP, сканер покажет открытыми все UDP-порты. В столбце «Response» или ничего не пишется или пишется результат исследования скриптом.

Сканер ресурсов (Resources scanner) - Отображает все доступные сетевые ресурсы.

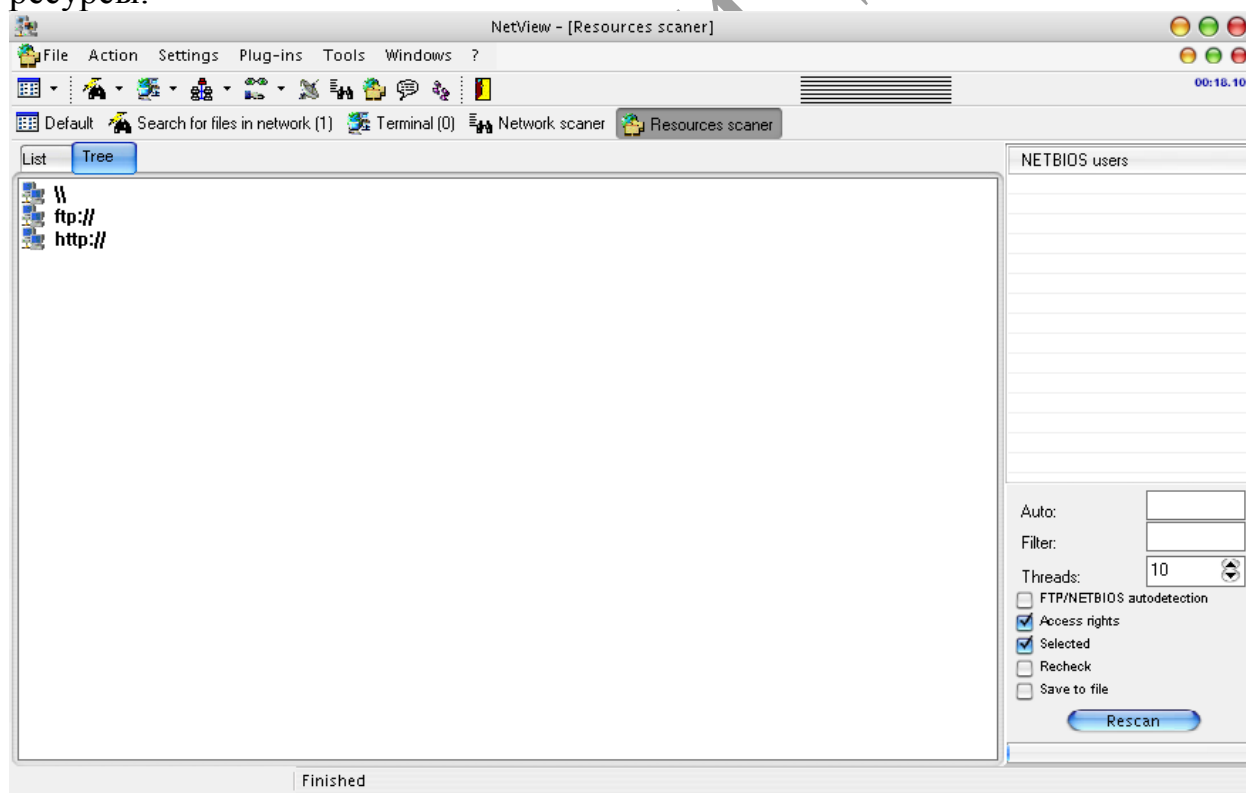


Рисунок 9 – Окно сканера ресурсов

Этот модуль может использоваться для 2-х целей:

- Составляет список доступных по FTP/NETBIOS ресурсов на всех компьютерах сети, с указанием прав доступа для различных пользователей. Можно задать имена пользователей, от которых проводится подключение, также проводится попытка перечисления пользователей

удаленного узла (работает применительно к WIN'NT/2000). Нажав правой кнопкой, можно открыть сетевой ресурс, либо подключить сетевой диск (для NETBIOS). Опция «Selected» позволяет сканировать только выделенные во всех хост-листах узлы. Результат можно сохранить в текстовый файл SHARELIST.TXT в каталоге NetView. Либо включив опцию «Save to file» - в этом случае NetView автоматически сохранит этот файл после завершения сканирования. Включив опцию «Recheck» можно ускорить сканирование за счет того, что не будут производиться попытки подключиться к отключенным узлам.

- По умолчанию сканер ресурсов ищет FTP и NETBIOS ресурсы на узлах в зависимости от их настроек. При включении опции FTP/NETBIOS autodetection, сканер ресурсов будет определять наличие таких ресурсов автоматически (путем сканирования портов 139, 445 и 21), и при необходимости менять настройки узлов хост-листе.

Изучение программы «Friendly Pinger»

Friendly Pinger - это мощное приложение для администрирования, мониторинга и инвентаризации компьютерной сети.

Общие возможности программы:

- визуализация компьютерной сети в красивой анимационной форме;
- отображение, какие компьютеры включены, а какие нет;
- пингование всех устройств;
- оповещение в случае остановки/запуска серверов;
- инвентаризация программного и аппаратного обеспечения всех компьютеров в сети;
- слежение, кто имеет доступ к Вашему компьютеру и какие файлы качает;
- назначение внешних команд (например, telnet, tracer) устройствам;
- поиск HTTP, FTP, e-mail и других служб, которые присутствуют в Вашей сети;
- отображение состояния сети на рабочем столе или Web странице;
- графический TraceRoute;
- открытие компьютеров в проводнике или Total Commander;

На рисунке 10 представлен интерфейс программы Friendly Pinger (Основное окно программы).

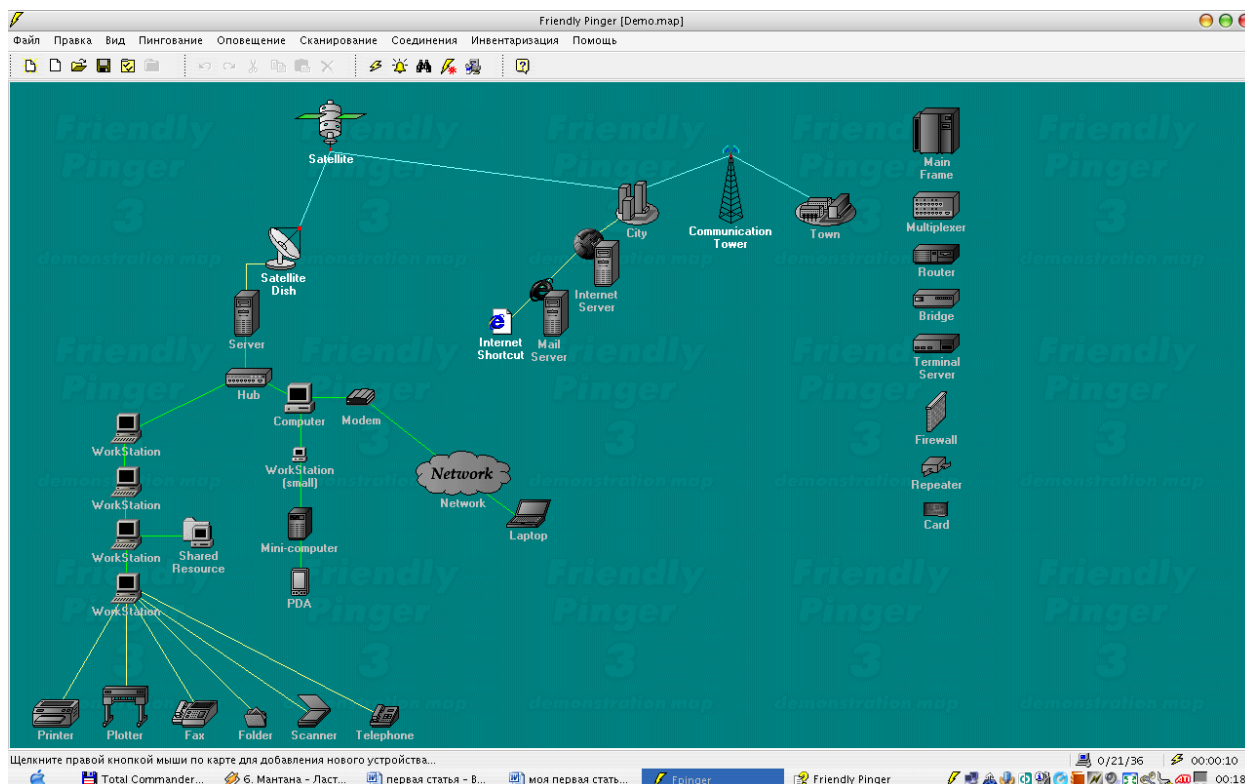


Рисунок 10 - Основное окно программы

Прежде чем начать работать непосредственно с программой и использовать все возможности, которые она предлагает, необходимо создать начальную карту. Вы подключены к сети, которая включает в себя ряд рабочих станций, серверов, дополнительных коммутационных устройств. Создайте простую карту сети, включающую рабочие станции текущей комнаты, если Вы затрудняетесь составить подробную карту всех подключений.

Вы можете создать начальную карту, используя «Wizard», или создать карту вручную.

Карта занимает основную часть окна. Щелкните по ней правой кнопкой мыши. В появившемся меню выберите "Добавить" и затем "Workstation". Появится окно «Свойства устройства». Укажите запрашиваемые параметры: имя устройства, адрес, описание, картинку.

Аналогично, можно добавить другие устройства, которые присутствуют в вашей сети. После создания устройства будут автоматически пинговаться., т.е. в зависимости от того, включено устройство или нет, вы будете получать информацию о состоянии устройства в сети. Это может быть крайне удобным при администрировании небольшой сети и, когда администратор должен видеть текущее состояние устройств в сети.

Устройство будет отображаться в виде анимационной картинки, если оно пингуется, или в виде черно-белой картинки, если оно не пингуется.

Щелкните дважды по устройству для открытия его в проводнике. Вы можете обозначить сегменты Вашей сети в виде линий. Нажмите CTRL+I

для получения подробной информации о созданной карте. В появившемся диалоге введите свое имя в качестве автора.

В меню "Файл" выберите "Настройки..." и настройте Friendly Pinger по своему желанию.

Рассмотрим основные возможности программы.

1) «Wizard» - позволяет создать начальную карту.

Friendly Pinger будет сканировать указанный диапазон IP-адресов и получать DNS-информацию о каждом адресе. Устройство будет добавлено, если DNS-сервер знает о нем.

Для запуска Wizard выберите пункт "Wizard" в меню "Файл".

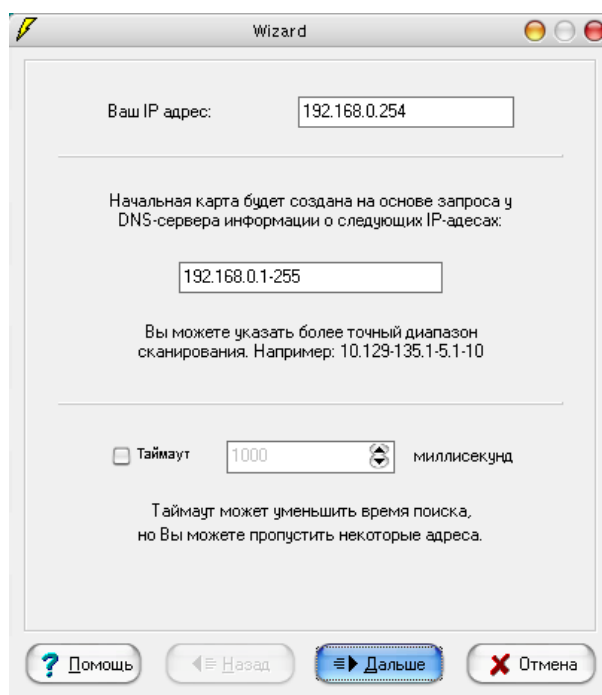


Рисунок 11 - Мастер создания карты

Wizard состоит из трех шагов:

1. Указание диапазона адресов, которые Вы хотите просканировать;

Friendly Pinger покажет IP-адрес Вашего компьютера и предложит начальный диапазон адресов для сканирования. Вы можете указать другой IP-адрес для изменения начального диапазона или указать диапазон вручную. Например: "10.129-135.1-9.1-9". Если некоторые адреса из диапазона в Вашей сети не существуют, их обработка может занять довольно длительное время. Вы можете ускорить ее, задав timeout. Нажмите кнопку "Далее" для начала сканирования.

2. Сканирование;

Friendly Pinger начнет сканирование Вашей сети. Каждый IP адрес будет запрашиваться у Вашего DNS-сервера для получения имени узла, ассоциированного с этим адресом.

Если DNS-сервер знает очередной IP-адрес, он будет добавлен в список найденных устройств.

Удалите галочку с тех устройств, которые Вы не хотите добавлять на карту. Галочка показывает, что устройство будет добавлено на карту. По умолчанию она ставится только на те устройства, которых нет на карте.

После поиска, нажмите "Далее" для задания дополнительных параметров или нажмите "Назад" для поиска в следующем диапазоне.

3. Добавление устройств.

Для добавления найденных устройств на карту Вы должны указать следующие параметры:

- Тип найденного устройства;
- Что использовать в качестве адреса: DNS-имя или IP-адрес;
- Если в Вашей сети присутствует DNS-суффикс, Вы можете удалить его из имени устройств;
- Выберите, где Вы хотите добавлять устройства, на новой карте или текущей.

После нажатия кнопки "Далее" устройство будет добавлено на карту.

Основное меню программы содержит следующие пункты:

- Файл;
- Правка;
- Вид;
- Пингование;
- Оповещение;
- Сканирование;
- Соединения;
- Инвентаризация;
- Помощь.

При наведении на любой пункт в меню, в статусной строке показывается его описание.

Рассмотрим Меню "Файл". Меню «Файл» содержит следующие пункты:

- Wizard - создать начальную карту.
- Новый - создать новую карту.
- Открыть - открыть существующую карту - Вы можете запустить FPringer с указанной картой, передав ее в качестве параметра. Например: `fpringer.exe mymap.map`
- Переоткрыть - открыть ранее используемую карту. Список открытых ранее карт запоминается и сохраняется в "Переоткрыть". Данный пункт недоступен, если история открытия карт пуста. Для переоткрытия карты:

1. Выберите "Файл → Переоткрыть";
2. Выберите карту, которую Вы хотите переоткрыть.

Для возврата на предыдущую карту используйте клавишу BackSpace.

- Сохранить - сохранить карту.
- Сохранить как - сохранить карту в новый файл.
- Экспорт - сохранить карту в графический файл - поддерживаются два формата: Windows Bitmap Files (BMP), CompuServe Graphics Interchange (GIF).

- Печать - печать карты.
- Блокировать/Разблокировать - блокирование приложения. Вы можете заблокировать приложение паролем для предотвращения изменений другими пользователями.

Существуют три способа блокировки:

1. Блокировка всего приложения;
2. Блокировка изменений;
3. Запрещение только перемещения объектов на карте.

После блокирования этот пункт меню заменяется командой "Разблокировать", для того чтобы можно было разблокировать приложение.

Примечание: Если Вы забыли пароль, то закройте приложение и удалите строчку "Lock=1" в FPinger.ini файле.

- Создать дистрибутив

Создать дистрибутив Friendly Pinger'a (как FPinger3.exe) с Вашими картами и настройками. Затем Вы сможете раздать его другим пользователям Вашей сети. Вы можете создать дистрибутив "Friendly Pinger" или "Friendly Pinger Lite". Friendly Pinger Lite - это бесплатная облегченная версия Friendly Pinger'a, в которой запрещены следующие возможности:

- Создание и редактирование карт;
- Экспорт в GIF-файл;
- TraceRoute;
- Некоторые способы оповещения: журнал; e-mail и выполнение;
- Просмотр инвентаризации (работает только сбор, согласно настройкам "inventory.ini" файла).

Вы можете указать, какие конфигурационные файлы Вы хотите включить в дистрибутив. Например, Вы можете настроить инвентаризацию для сбора информации на Ваш компьютер, создать дистрибутив, включить в него inventory.ini файл, затем раздать и установить его другим пользователям Вашей сети, после этого Вы будете получать информацию о программном и аппаратном обеспечении Вашей сети для проведения инвентаризации.

- Настройки - Настроить программу.
- Выход - Заккрыть программу.

FPinger можно также закрыть щелчком правой кнопкой мыши по иконке в трее и выбором "Выход":

Меню "Пингование" содержит следующие пункты:

- Пинговать все - Пинговать все устройства. Пингование также может быть начато нажатием клавиши F5 или щелчком правой кнопкой мыши на иконке программы и выбором "Пингование все":
- Пауза - Приостановить пингование устройств. После этого данный пункт меню заменится на "Продолжить". Пингование также может быть приостановлено нажатием клавиши F4 или щелчком правой кнопкой мыши на иконке программы и выбором "Пауза":

– Продолжить - Продолжить пингование устройств. После этого данный пункт меню заменится на "Пауза". Пингование так же может быть продолжено нажатием клавиши F4 или щелчком правой кнопкой мыши на иконке программы и выбором "Продолжить":

– Очистить кэш - Сбросить кэш IP адресов.

– FPinger запоминает, какой IP адрес соответствует каждому DNS имени. Это позволяет избежать постоянных запросов к DNS серверу, что увеличивает скорость работы приложения и экономит сетевой трафик. С другой стороны, после переконфигурирования DNS сервера, FPinger будет использовать старые IP-адреса. Чтобы избежать этого, воспользуйтесь этой опцией, либо перезапустите FPinger.

– Параметры пингования - Настроить параметры пингования.

Меню "Оповещение" содержит следующие пункты:

– Оповещение - настроить "службу оповещения".

– Отчет. Просмотр отчета оповещения. FPinger может показывать события на Вашей Web-странице. Для того чтобы изменить стиль отчета, правьте файл-шаблон "Events.htm".

– Очистить log-файл - Очистить Notification.log файл в каталоге приложения.

– Параметры оповещения. Настроить log-файл, HTML-файл и другие параметры оповещения.

Работа с объектами

Для того чтобы выделить устройство на карте воспользуйтесь одним из следующих способов:

– Если требуется выделить только один объект, щелкните по нему.

– Если требуется выделить на один объект больше, щелкните по нему, удерживая клавишу SHIFT.

– Если требуется снять выделение с одного из выделенных объектов, щелкните по нему, удерживая клавишу SHIFT.

– Если требуется снять выделение со всех объектов, щелкните в пустое место на карте.

– Если требуется выделить несколько объектов в одной прямоугольной области, выделите ее мышкой.

– Если требуется выделить несколько объектов в одной прямоугольной области, выделите ее мышкой, удерживая клавишу SHIFT. В этом случае, те объекты в области, которые были не выделены, станут выделенными и наоборот.

– Для выделения всех объектов нажмите Ctrl+A или выберите пункт "Выделить все" в меню "Правка" или щелкните правой кнопкой мыши по карте и выберите "Выделить все".

– Для перемещения выделенных объектов воспользуйтесь одним из следующих способов:

- Перетащите выделенные устройства мышкой;
- Перетащите мышкой за один из центров выделенной линии;
- Воспользуйтесь курсором клавиатуры, удерживая клавишу SHIFT;

В этом случае объекты будут перемещаться попиксельно;

- Воспользуйтесь курсором клавиатуры, удерживая клавишу CTRL;
- В этом случае объекты будут перемещаться по 10 пикселей;

Если при перемещении какой-либо объект выйдет за правую или нижнюю границу карты, то автоматически появятся полосы прокрутки.

Специальные возможности:

- Если перетаскивать объекты мышкой, удерживая клавишу SHIFT, то они будут перемещаться только по горизонтали или только по вертикали, в зависимости от того, в какую сторону Вы перетаскиваете объекты;

- Если перетаскивать объекты мышкой, удерживая клавишу CTRL, то они будут перемещаться по сетке (т.е. по 10 пикселей);

- Оба этих способа можно совместить, удерживая одновременно CTRL и SHIFT.

Для выравнивания выделенных устройств, щелкните по ним правой кнопкой мыши, выберите "Выровнять" и затем:

- По левому краю - все выделенные устройства будут выровнены по самому левому краю их картинок.

- По правому краю - все выделенные устройства будут выровнены по самому правому краю их картинок.

- По верхнему краю - все выделенные устройства будут выровнены по самому верхнему краю их картинок.

- По нижнему краю - все выделенные устройства будут выровнены по самому нижнему краю их картинок.

- По центру - все выделенные устройства будут выровнены по вертикали, по центру их картинок.

- По сетке - все выделенные устройства будут выровнены по сетке. Сетка представляет собой ячейки 10x10 пикселей. Т.е. координаты всех объектов будут округлены до десятых.

- По горизонтали - все выделенные устройства будут выстроены по горизонтали на равном расстоянии друг от друга.

- По вертикали - все выделенные устройства будут выстроены по вертикали на равном расстоянии друг от друга.

- Центрировать вершины линий - для каждой линии будет проверено, есть ли у нее вершины под устройствами. И если есть, то эти вершины будут перемещены в центры соответствующих устройств.

Выравнивать по надписям - если выбрана эта опция, то все операции выравнивания будут учитывать позицию и размеры надписей устройств. Иначе выравнивание будет происходить только по картинкам устройств.

Привязка линий - если выбрана эта опция, то при перемещении устройств, линии, которые под ними, тоже будут перемещены.

Устройства

Создание - для добавления нового устройства, щелкните по карте правой кнопкой мыши и выберите элемент в пункте "Добавить", в зависимости от того, устройство какого типа Вы хотите добавить на карту. Появится окно свойства устройства. Укажите все необходимые параметры и нажмите кнопку ОК.

Удаление - для того чтобы удалить устройство, выделите его и: нажмите клавишу Del; или выберите "Удалить" в меню "Edit";

Пингование - Для того чтобы принудительно пинговать устройство, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Пинговать выделенные устройства".

Открытие в проводнике - для того чтобы открыть устройство в проводнике, щелкните по нему правой кнопкой мыши и выберите "Открыть". Данная команда эквивалентна выполнению команды Windows "\\адрес_устройства" или "адрес_устройства", если это internet-адрес.

Открытие в Total Commander - для того чтобы открыть устройство в Total Commander, щелкните по нему правой кнопкой мыши и выберите "Открыть в TotalCmd". Этот пункт отсутствует, если Total Commander не установлен на Вашем компьютере.

Оповещение - оповещать, когда устройство остановится или запустится.

Инвентаризация - просмотр списка программного обеспечения и аппаратных средств компьютера.

Выполнение внешних команд - для выполнения внешней команды, щелкните по устройству правой кнопкой мыши и выберите соответствующую команду. Внешние команды для устройств каждого типа регистрируются в настройках для типа устройств.

Конфигурирование - для конфигурирования устройства, щелкните по нему правой кнопкой мыши и выберите "Параметры". Появится окно "Свойства устройства". Для изменения параметров типа устройства, щелкните по устройству правой кнопкой мыши и выберите "Настроить тип устройства...". Появится диалог "Параметры типа устройства". Для изменения типа устройства, щелкните по устройству правой кнопкой мыши и выберите "Установить тип устройства". Затем выберите требуемый тип из списка.

Остановка пингования - для того чтобы приостановить пингование устройства, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Приостановить пингование выделенных устройств". Для того чтобы продолжить пингование устройства, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Продолжить пингование выделенных устройств".

TraceRoute - для получения пути до устройства, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "TraceRoute".

Соединение - для того чтобы соединиться с FP-сервером, запущенном на устройстве, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Соединиться". Для того чтобы отсоединиться от FP-Server, запущенном на устройстве, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Рассоединиться". "Рассоединиться" доступно только после соединения.

Свойства устройств - для того чтобы настроить параметры выделенного объекта, щелкните по нему правой кнопкой мыши и выберите "Параметры". В появившемся окне Вы можете изменять следующие параметры: Имя - имя устройства, которое отображается под устройством. Допускается вводить несколько имен построчно. Текст в подсказке - описание устройства, которое отображается при наведении на него мышкой. Картинка в подсказке - картинка, ассоциированная с устройством, которая отображается при наведении на него мышкой. Тип - тип устройства. Типы устройств регистрируются в настройках программы. Они показывают, каким образом отображать те или иные устройства на карте, так же они задают способ опроса устройства, его внешние команды и т.д. Адрес - Адрес устройства. Адрес устройства используется для пингования и для выполнения внешних команд. В качестве адреса можно указывать IP адрес или DNS имя устройства. Вы можете назначить адрес, только если для типа данного устройства установлен режим опроса "Пинговать" или "Всегда включено".

Дополнительные адреса - вы можете указать дополнительные адреса для устройства. Они будут пинговаться и отображаться на карте в виде кружочков. Если дополнительный адрес пингуется, то он будет показан в виде кружочка зеленого цвета, иначе красного. Адрес будет показываться при наведении мышкой на кружок.

Обычно дополнительные адреса обозначают присутствие нескольких сетевых карт на сервере. Активно используются для TraceRoute.

Вы можете назначать дополнительные адреса, только если для типа данного устройства установлен режим опроса "Пинговать" или "Всегда включено".

Файл с картой - файл с картой, которая будет открываться по двойному щелчку на устройстве. Вы можете назначить карту, только если для типа данного устройства установлен параметр "Открывать другую карту"

Привязать к другим устройствам - Привязать данное устройство к другим устройствам - если одно из них пингуется, то это устройство будет показываться включенным.

Для того чтобы привязать устройство к другим устройствам, например, хаб к компьютерам, выделите хаб на карте, нажмите клавишу ALT и

щелкайте по компьютерам, которые Вы хотите привязать к хабу, или с которых Вы хотите снять привязку.

Устройства, которые привязаны к данному устройству, показываются в красных прямоугольниках.

Вы можете привязать устройство к другим, только если для типа данного устройства установлен режим опроса "Привязывать к другим устройствам".

Тип устройства - для того чтобы настроить параметры типа устройства, щелкните по нему правой кнопкой мыши и выберите "Настроить тип устройства...".

В появившемся диалоге Вам доступны следующие параметры: имя - имя типа устройств.

Способ опроса - существуют три способа опроса состояния устройств:

Всегда включено - устройство не будет пинговаться и будет отображаться на карте всегда включенным.

Пинговать - устройство будет пинговаться.

Привязывать - устройство будет привязано к другим устройствам и отображаться включенным, только если хотя бы одно из них включено.

Внешние команды - вы можете назначить устройствам внешние команды, такие как telnet, ping.exe, tracert.exe, net.exe и т.д. Они будут показываться в контекстном меню устройства (при щелчке на нем правой кнопкой мыши).

В настройках можно навешать двойной щелчок на запуск первой внешней команды.

Допускается использовать следующие ключи в параметрах внешних команд:

%Address - адрес устройства;

%IP - IP адрес устройства;

Каждый ключ при выполнении внешней команды будет заменен на его соответствующее значение. Допускается использовать произвольные ключи. Их значения будут запрашиваться перед запуском внешней команды. Например, для реализации NetSend добавьте следующую внешнюю команду:

Приложение: "net.exe";

Параметры: "send %Address %Text".

%Text будет предварительно запрашиваться.

Для ввода пароля используйте ключ %Password. Он позволит вводить текст секретно. Если требуется указать несколько разных паролей, используйте ключи, начинающие со слова %Password, например, %Password1, %Password2 и т.д.

Рекомендуем установить Windows Resource Kit, он содержит довольно много полезных команд для удаленного управления другими компьютерами, например, для их удаленной перезагрузки, запуска приложений и т.д. Все их можно успешно вызывать из FPinger'a.

Групповые операции - групповые операции позволяют выравнять и изменять параметры сразу нескольких устройств на карте. Для того чтобы выполнить групповую операцию, выберите "Правка → Групповые операции".

В появившемся окне Вам предложат выполнить одну из следующих операций:

- Выстроить устройства;
- Изменить тип устройств;
- Установить имена устройств значениями их адресов;
- Установить значения адресов значениями их IP адресов.

Выберите требуемую операцию и нажмите "Далее".

В зависимости от выбранной операции Вас попросят указать следующие данные:

- Выстроить устройства: направление выравнивания объектов: слева направо, сверху вниз, или наоборот. Так же можете выбрать "Отображать имена справа", если хотите поменять позицию отображения имен устройств.

- Изменить тип устройств: новый тип устройств.

Далее, для любой выбранной операции Вы должны указать, для каких устройств ее осуществить:

- Для всех устройств на карте;
- Только для выделенных устройств (недоступно, если ни одно устройство на карте не выделено);
- Только для устройств определенного типа (нужно указать для какого);
- Только для устройств неизвестного типа - если Вы удалите какой-либо тип устройств, то сами устройства останутся на карте, но будут показываться без иконок.

С помощью групповых операций Вы можете задать тип сразу для всех неизвестных устройств. Данная опция недоступна, если устройств неизвестного типа нет на карте. Для завершения групповой операции, нажмите "Закончить".

Линии - линии на карте обычно обозначают сегменты. Если линия выделена, то красно-желтые квадраты показывают ее вершины, а красно-голубой - центр (для перемещения).

Пингование

Для того чтобы начать пингование устройств, воспользуйтесь одним из следующих способов: нажмите клавишу F5; выберите пункт "Пинговать все" в меню "Пингование"; щелкните по иконке программы в системном трее и выберите "Пинговать все". Для пингования только выделенных устройств, щелкните по ним правой кнопкой мыши и выберите "Пинговать выделенные". Для того чтобы временно прекратить пингование устройств, воспользуйтесь одним из следующих способов: нажмите клавишу F4;

выберите пункт "Пауза" в меню "Ping"; щелкните по иконке программы в системном трее и выберите "Пауза".

Для того чтобы продолжить пингование устройств, воспользуйтесь одним из следующих способов: нажмите клавишу F4; выберите пункт "Продолжить" в меню "Ping"; щелкните по иконке программы в системном трее и выберите "Продолжить".

TraceRoute

TraceRoute - это средство для просмотра маршрута до указанного адреса.

Как использовать TraceRoute в FPinger'e: Для просмотра маршрута до устройства, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "TraceRoute". В нижней части карты появится окно TraceRoute. В процессе определения промежуточных адресов они будут добавляться в этом окне и отображаться на карте в виде стрелок. Каждая строка в окне TraceRoute имеет рорир-меню, которое активизируется щелчком правой кнопкой мыши. С помощью него Вы можете скопировать текст, IP-адрес или имя хоста из этой строки в буфер обмена, найти устройство на карте или закрыть окно TraceRoute.

Примечание:

- Промежуточные адреса, которые не найдены на карте, пропускаются при графическом представлении маршрута;
- Вы можете задавать дополнительные адреса для устройств, если они не найдены на карте.

FPinger может оповещать Вас если какой-либо компьютер остановится или запустится. Присутствуют 7 способов оповещения:

- Сохранение события в log-файл;
- Анимация иконки в системном трее;
- Показ сообщения на экране;
- Отправление e-mail сообщения;
- Проигрывание звукового файла;
- Запуск внешнего приложения;
- Отображение события на Вашей Web странице.

Для использования оповещения на устройство, щелкните по нему правой кнопкой мыши, выберите "Оповещение" и затем один из следующих пунктов:

- Когда "имя устройства" запустится;
- Когда "имя устройства" остановится;
- Когда любой "тип устройства" запустится;
- Когда любой "тип устройства" остановится.
- В окне "Оповещение" вы можете устанавливать следующие параметры:

- Перепроверять - перепроверять, что устройство действительно остановилось или запустилось; Так же Вы можете указать, сколько раз требуется перепроверить событие.
- Оповестить только один раз - выключить это оповещение после первого срабатывания;
- Сохранить в log-файл - сохранить событие в log-файл. Требуется для отчетов;
- Анимация в трее - анимировать иконку в трее после срабатывания события;
- Показать сообщение - показать сообщение на экране после срабатывания события;
- Отправить письмо - отправить письмо по электронной почте указанным получателям после срабатывания события. Многие провайдеры сотовой и пейджинговой связи предоставляют возможность отправлять сообщения своим клиентам с помощью электронной почты. Вы можете воспользоваться этой услугой и получать сообщения об остановке или запуске серверов напрямую на Ваш сотовый или пейджер. Дополнительную информацию Вы можете получить у Вашего провайдера сотовой или пейджинговой связи.
- Проиграть звуковой файл - проиграть звуковой файл после срабатывания события. Вы можете записать свой файл, используя микрофон;
- Выполнить - выполнить внешнее приложение после срабатывания события. Вы можете передать адрес устройства в качестве параметра, используя ключ %Address. Для передачи IP адреса устройства используйте ключ %IP.

Программа FP-сервер. FP-сервер - это бесплатное приложение, с открытым текстом программ, разработанное специально для FPinger'a, написанное для Windows и Linux. FPinger может соединяться с FP-сервером, который запущен на другом компьютере. После соединения, все Ping и TraceRoute операции будут происходить с удаленного компьютера, где запущен FP-сервер, а результат будет показываться на Вашем компьютере. С помощью FP-сервера Вы можете смотреть как пингуется сеть с серверов, или смотреть TraceRoute между любыми компьютерами.

Чтобы соединиться с FP-сервером, необходимо запустить FP-сервер на удаленном компьютере. Щелкните правой кнопкой мыши по тому устройству на карте, на котором запущен FP-сервер, выберите "Ping, Trace" и затем "Connect". Для рассоединения с FP-сервер, запущенном на компьютере, щелкните по нему правой кнопкой мыши, выберите "Ping, Trace" и затем "Disconnect".

Примечания:

FP-сервер сейчас находится в стадии разработки. Доступна только тестовая версия.

Задание к индивидуальной работе:

1 Изучить все возможности программ NetView и Friendly Pinger, установив программы на рабочей станции.

2 Сохранить скриншоты работы основных модулей программы и поместить их в отчет по индивидуальной работе с краткими пояснениями выполненных действий.

3 Оценить достоинства и недостатки приведенных программ, если пользовались другой подобной программой провести анализ программы NetView и Friendly Pinger относительно других известных Вам программ, позволяющих выполнять мониторинг сети и сетевых подключений.

4 Установить демо-версии двух-трех программ для удаленного администрирования (либо программы, находящиеся в свободном распространении), разработанных на основе протокола VNC, оценить их возможности, в отчет по индивидуальной работе включить описание возможностей установленных программ удаленного администрирования, сделать сравнительный анализ и привести скриншоты использования программ удаленного администрирования, разработанных на основе протокола VNC.

Содержание отчета:

1 Задание к индивидуальной работе.

2 Скриншоты работы основных модулей программ NetView, Friendly Pinger, систем для удаленного администрирования, разработанных на основе протокола VNC, установленных и запущенных с рабочей станции в локальной сети.

3 Достоинства и недостатки изученных программ.

Контрольные вопросы:

1 Перечислите основные модули программы NetView.

2 Что такое UDP протокол, к какому уровню он относится, его назначение.

3 Протокол TCP, его назначение, отличие от UDP-протокола.

4 Протокол ARP, назначение.

5 Что такое ICMP протокол, какую информацию можно посмотреть благодаря программе NetView по ICMP-пакетам.

6 Что такое DOS-атака, какие средства встроены в программу NetView для контроля за DOS-атакой.

7 Какая из изученных Вами программ имеет большие функциональные возможности?

8 При разработке собственной программы мониторинга сети, какие возможности из реализованных в изученных программах Вы бы оставили, какие расширили?

9 Что такое протокол VNC?

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ЗАДАНИЯ
К самостоятельной работе студентов по курсу
«Протоколы компьютерных сетей»
(для студентов специальности “Программное обеспечение АС”)

Составители:

Алла Викторовна Чернышова

Кафедра ПМИИ, ДонНТУ