

**Колледж космического машиностроения и технологий**

**Презентация**

**по теме:   
«**Псевдоведущая ЭВМ**»**

специальность **09.02.03 «Программирование в компьютерных системах»**

Обучающегося 2 курса группы П2-20   
**Павлова Анна**

Проверяющий(-ая):   
преподаватель Лихторенко Олеся Сергеевна

2021г.

# Что такое Псевдоведущая ЭВМ?

Псевдоведущая ЭВМ [take host] - ЭВМ, осуществляющая сбор статистики о работе вычислительной сети.]- ЭВМ, осуществляющая сбор статистики о работе вычислительной сети.

# Мониторинг и анализ локальных сетей.

Мониторинг - процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т. п.

Анализ - процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления.

Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Системы мониторинга сети — это программное обеспечение, позволяющее отслеживать состояние сетевых устройств, их работоспособность, исправность и другие характеристики. При этом системы мониторинга сети позволяют оповещать администраторов при возникновении каких-либо сбоев посредством отправки СМС-сообщений, сообщений на электронную почту и других средств.

Системы мониторинга сети можно разделить на те, что отслеживают производительность сети и сигнализируют при перегрузке каналов, а также на те, что производят мониторинг сети с целью поиска сбоев и других проблем, связанных с работоспособностью серверного оборудования и других систем.

Основным способом отслеживания работоспособности является отправка запросов устройствам. Это могут быть HTTP-запросы для проверки веб-сервера, SMTP-запросы для серверов электронной почты, с обязательным получением ответа по протоколам IMAP или POP3. Во время отправки таких запросов производится мониторинг таких показателей, как время отклика, доступность, время безотказной работы и другие.

Помимо этого, к функциям систем мониторинга сети можно отнести:

-           Возможность составления топологии сети в автоматическом режиме. -           Постоянный мониторинг сети.

-           Возможность своевременного оповещения лиц, ответственных за администрирование инфраструктуры.

-           Построение ретроспективы работоспособности сетевой инфраструктуры. -           Составление различные отчетов.

-           Диагностика возникших сбоев в работе, которая достигается с помощью отправки ping, протоколов и возможностей SNMP, Syslog, WMI, эмуляции и анализа сетевого трафика.

Для осуществления мониторинга сложной корпоративной сети или распределенной инфраструктуры необходимо применение комплексной платформы, которая позволила бы просматривать как физический, так и виртуальные серверы, WAN-соединения, программную и сетевую инфраструктуру, облачные сервисы, сетевые приложения, а также мобильные устройства, которые подключаются к сети.

Использование систем мониторинга сети позволяет выполнять не только технические задачи, описанные выше, но и бизнес-задачи, такие как обоснование затрат на модернизацию оборудования или инфраструктуры, что позволило бы снизить количество проблемных узлов. За счет поддержания сети в работоспособном состоянии и своевременном устранении ее проблем компания может снизить свои затраты на восстановление и повторяющееся устранение неполадок.   
Программы мониторинга компьютерных сетей

Мониторингом компьютерной сети принято называть функционирование специальной системы, ведущей постоянное наблюдение за сетью для того, чтобы вовремя обнаруживать неисправности и замедление работы сети. Как только проблема будет выявлена, система должна будет оповестить сетевого администратора при помощи сообщения по электронной почте, мессенджера, телефона или другим способом.



Приложение имеет веб-интерфейс, поддержку SNMP, внешних проб (ping), различные способы для проверки. Удобная функция для хостинг-провайдеров предоставляет возможность создания сценариев слежения за интернет-сайтами, подражающих работе обычных пользователей. Возможности таких программ для мониторинга и анализа сетей Windows, или таких как Zabbix, позволяют им заходить на определенную страницу и авторизоваться на сайте, благодаря чему можно будет увидеть время загрузки и объем трафика при осуществлении описанных действий. Можно провести масштабирование системы с помощью установки отвечающих за конкретный сегмент сети серверов. В итоге данные будут отображаться в одной общей точке.

Плюсы данной программы для мониторинга локальной сети:

* многофункциональность;
* масштабирование;
* удобное оповещение;
* подключение скриптов;
* можно получить карту сети;
* агенты для Windows.

Минусы:

* сложная первичная настройка;
* недостаточная стабильность работы;
* уступает по количеству наблюдаемых узлов аналогичному ПО.



Также из программ мониторинга компьютерных сетей стоит отметить Nagios, предназначенную для наблюдения и контроля вычислительных узлов и служб и оповещения администраторов, когда какие-либо службы прекращают либо возобновляют работу. Достаточно давно выпущенная система, поэтому интерфейс ее не слишком удобен и несет в себе мало информации, как и составляемые отчеты. Стандартная сборка не имеет функции составления графиков, что является существенным недостатком, поскольку часто системному администратору необходимо проверить степень загруженности канала либо CPU. Однако этот минус можно исправить путем установки дополнительных плагинов, что, правда, отнимет время. С помощью модуля NRPE может использоваться как программа для мониторинга локальной сети.

Достоинства данной программы:

* простота;
* стабильность работы;
* множество плагинов;
* способна мониторить десятки тысяч сервисов и тысячи хостов и на одном сервере.

Недостатки:

* устаревший интерфейс;
* невозможность добавления графиков.



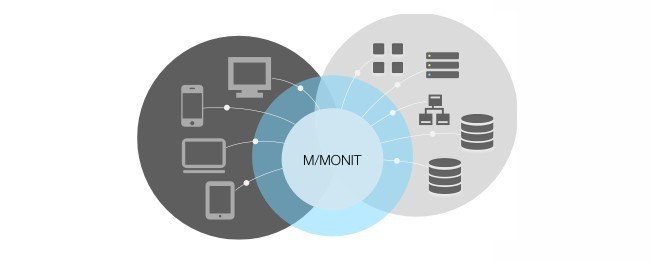
Cacti (получила прозвище «Кактус») – программа для мониторинга локальной сети, позволяющая строить графики посредством RRDTool. Собирает статистические данные за конкретный период времени и наглядно их отображает. Как правило, использует стандартные шаблоны при отражении статистики загрузки процессора, выделения оперативной памяти, запущенным процессам, входящему и исходящему трафику. Преимуществом данной программы для мониторинга локальной сети является возможность подключения скриптов для обработки полученных данных с их дальнейшей визуализацией.

Достоинства ПО:

* удобный веб-интерфейс;
* наличие информативных графиков;
* подключение скриптов.

Недостатки:

* сложная первоначальная настройка;
* предназначение преимущественно для визуализации.



Monit – одна из мощных программ мониторинга компьютерных сетей, наблюдающая за работой сервисов и при необходимости их перезапускающая, что не требует никакого вмешательства системного администратора. В соответствии с произведенными настройками, система осуществляет проверку:

* процесса по PID;
* ресурсов, занимаемых процессом;
* ответов протоколов по определенным портам (SMTP, HTTP, SSH и т.п.);
* работы конкретных портов (TCP/UDP);
* объема файловой системы и свободного пространства;
* прав доступа к тому или иному файлу или папке.

Преимущества:

* комбинированные методы проверки;
* возможность оповещения по email;
* поддержка внешних скриптов;
* наличие веб-интерфейса.

Недостатки:

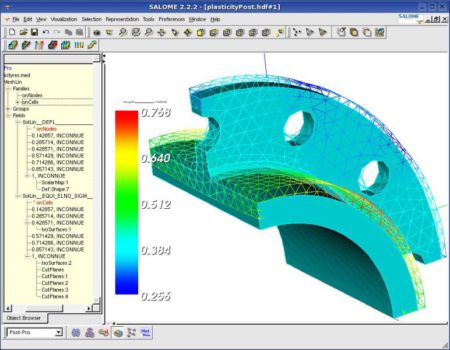
* существует версия только для систем Unix.

По мнению ИТ специалистов, на практике опробовавших описанные выше системы, при наличии в сети меньше двух-трех тысяч узлов можно использовать универсальный Zabbix, позволяющий проводить комплексный анализ и контроль сети. Хорошим дополнением, способным перезапустить при необходимости Zabbix-агент, станет Monit. При обслуживании же обширной сети или при потребности наблюдать за множеством сервисов стоит выбрать сочетание систем Nagios и Cacti, хотя при желании можно просто масштабировать Zabbix. Однако существует еще множество программ для мониторинга локальной сети, каждая из которых имеет свои особенности использования.

Анализ компьютерных сетей

Моделирование сетей

Отдельной строкой красуется моделирование пакетов. Современный проектировщик заранее оценивает работоспособность, преодолевая этап проектирования. В компьютерных сетях примерная производительность известна, методика стала палочкой-выручалочкой сотовых операторов. Инженеры выбирают топологию, протоколы сети, состав оборудования. Помогают решить задачу генераторы пакетов, попутно собирается статистика придуманной сети. Здесь активно помогают знания элементов теории вероятности. Следует правильно оценить распределение трафика, выбирая модели типовых законов (Пуассона, Эрланга, Парето).

[](https://setinoid.ru/wp-content/uploads/2017/12/181.jpg)

Моделированию подвергаются сети любого типа. Часто разработчики стандартов помогают проектировщикам, давая рекомендации. Сотовой связью занимается комитет 3GPP2. Организация рекомендует ряд типов генератора трафика. Сегодняшняя мобильная сеть мало уступает компьютерной, активно перенимая типичные протоколы, включая IP. Отличие ограничивается ярким делением направления движения информации:

* Восходящая ветвь.
* Нисходящая ветвь.

Например, генератор FTP-протокола моделирует загрузку файлов. Параллельно виртуальными «пользователями» открываются странички мировой паутины, отдельные лица совершают звонки. Различают методы моделирования:

* Натурные. Строится реальная живая сеть, подключённая аппаратура выдаёт информацию. Недостатком называют высокую стоимость, хотя фактор адекватности полученных измерений часто перевешивает.
* Имитационные. Будущая сеть в мелочах моделируется специальными программными пакетами (например, CISCO Packet Tracer). Имитируются условия перегрузки, потери кадров.
* Аналитические. Полностью метод ограничен виртуальным пространством, точность сравнительно низкая. Инженер закладывает формулы, математической статистики. Намного проще имитационного подхода.
* Комбинированные.

Имитация

ПО имитационной модели поддерживает ряд базовых устройств: концентраторы, коммутаторы, рабочие станции, ядро сотовых коммуникаций. Программист задаёт маски подсетей, адреса. Структура тщательно выбирается сообразно представленному перечню устройств. При необходимости отсутствующие элементы заменяют близкими аналогами. Иногда допускается упрощать физическую структуру сообразно целям проведения эксперимента. Полученная среда позволит полностью имитировать процессы, включая простой пинг персональных компьютеров, абонентов.

[](https://setinoid.ru/wp-content/uploads/2017/12/182.jpg)

Использование статистики

Анализом компьютерной сети называют процесс обработки собранных данных, касающихся функционирования системы. Администратору важно знать слабые места, выявлять вовремя неисправности. Иногда средства контроля стоят обособленно, отдельным программным пакетом. В других случаях лишние денежные траты нецелесообразны. Поэтому набор методик анализа сильно варьируется. Процедура контроля образована двумя этапами:

* Мониторинг – сбор информации.
* Анализ – обработка сведений.

Этап мониторинга требует сбора информации, по большей части проходит автоматически. Проблема решается использованием датчиков, программного обеспечения. Анализ производит человек, используя опыт, обобщённый экспертами. Наработанные решения упрощают процесс анализа. Например, эксперты предлагают несколько критериев сбора статистики:

* Число ошибок.
* Уровень коллизий.
* Укороченные (меньше 64 байт)/удлинённые (свыше 1518 байт) кадры.
* Ошибки контрольной суммы. Несовпадение является следствием некачественных контактов, помех, неисправных портов, поломанного оборудования.
* «Призраки», сформированные наводками.

[](https://setinoid.ru/wp-content/uploads/2017/12/183.jpeg)

Очевидно, характер ошибок тесно связан с топологией, протоколами. Приведённые сопровождают сети Ethernet. Соотношение групп дефектов иногда помогает выявить характер неисправности. Типичный процент ошибочных кадров ниже 0,01%. Наличие битых пакетов становится причиной снижения пропускной способности. Местонахождение неполадок выявляют, оценивая количество, тип коллизий:

* Локальная выступает результатом одновременной передачи пакетов несколькими сетевыми картами сегмента. Высокий показатель часто сопутствует повреждённому кабелю.
* Удалённая проникает извне контролируемого сегмента. В сетях Ethernet, сформированных многоповторными повторителями, 100% коллизий относится к данному типу.
* Поздняя (терминология Ethernet) обнаруживается после передачи 64 байт. Чаще позволяет локализовать неисправность, неработоспособность сетевого адаптера. Иногда причиной становится превышение длины кабельной системы, числа промежуточных повторителей.

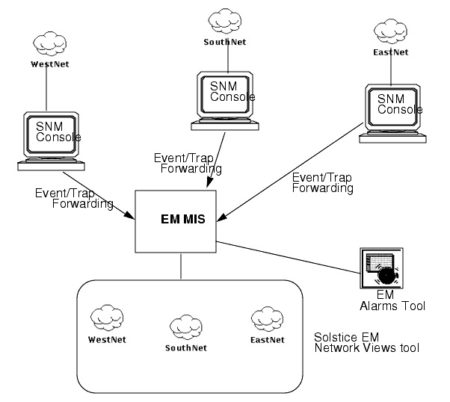
Число коллизий нормально ниже 5%. Помимо указанных статистических цифр оборудование часто даёт:

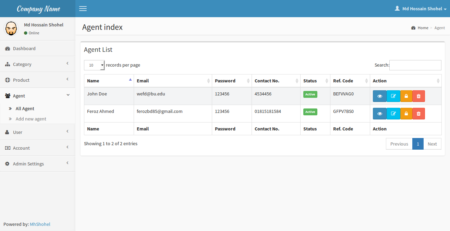
* Соотношение протоколов сетевого уровня. Наличие избытка ICMP сопровождает сигнализацию маршрутизаторов об ошибках.
* Основные отправители/получатели.
* Адреса генерации широковещательного трафика.

Структура методов контроля

Зачастую средства анализа, мониторинга пересекаются. Структура методик включает:

* Системы управления (HP Open View, IBMNetView, SunNetManager) составляют ядро. Администратор дистанционно считывает конфигурацию, настраивает оборудование. Параллельно анализирует производительность. Правильно настроенная система пришлёт администратору по электронной почте уведомление: возникли неисправности, сбой. Доступны предупреждения на пейджер, мессенджер. Согласно определениям ISO, классификацией включаются:

[](https://setinoid.ru/wp-content/uploads/2017/12/184.jpg)

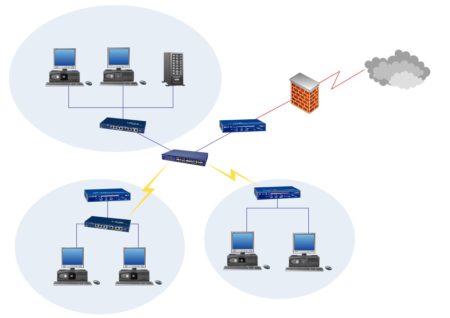
* Обработка ошибок.
* Конфигурация сети и присвоение имён.
* Производительность.
* Безопасность (защищённость от несанкционированного доступа): привилегии, аутентификация, шифрование.
* Регистрация параметров работы сети.
* Средства управления системой (Microsoft System Management Server, Intel LANDeskManager) контролируют программные, аппаратные ресурсы. Производят учёт, сбор информации о локальных компьютерах. Администратор чётко видит перечень машин, состояние, необходимость обновления. Установка ПО проходит централизованно. Некоторые индивиды любят наблюдать деятельность пользователя. Рассматриваемая группа средств позволит шпионить. Часть перечисленных выше способностей содержат HP Open View, IBMNetView, SunNetManager.
* Экспертные системы (Spectrum Cabletron) консолидируют опыт предыдущих поколений. Средства контроля развивались параллельно росту сетей, постепенно усложняясь. Формируемые базы данных, автоматизированные системы помощи сильно упрощают жизнь специалиста. Network Monitor фирмы Майкрософт изначально был лишён экспертной системы.
* Агенты системы управления – программные модули, снабжающие центр анализа сведениями. Обычно используют протоколы SNMP, CMIP, RMON. Стандарты баз данных – MIB-I, MIB-II, RMONMIB. Спецификации указанных хранилищ определяют громадное количество объектов (логи протоколов, сведения об устройствах, таблицы трансляции адресов). Агенты улучшенного протокола RMON (LANalyzeNovell) более интеллектуальны, программными модулями оснащают ноутбуки, рабочие станции.[](https://setinoid.ru/wp-content/uploads/2017/12/185.png)
* Встроенные системы могут являться частью операционной системы, либо сетевой инфраструктуры. Заправляют мониторингом, автоматическим восстановлением единственного объекта. Зачастую включают в состав агента системы.
* Анализаторы протоколов оценивают трафик. Реализованы программными, аппаратными средствами. Анализ пакетов позволяет оптимизировать структуру.

Отдельно диагностируется кабельное хозяйство, часть оборудования портативная. Виды методов:

* Сетевые мониторы показывают параметры трафика. Порой захватывают несколько уровней иерархической системы OSI (физический, канальный, сетевой).
* Кабельные сканеры оценивают состояние жил линии.
* Устройства сертификации позволяют сдать проведённый монтаж заказчику, оценить классность сети.
* Тестеры позволяют контролировать разрывы цепи.

Отдельные образцы техники многофункциональные, сочетают возможности тестеров, анализаторов протоколов:

* Графический пользовательский интерфейс.
* Сканирование линии.
* Распиновка жил, составление карты.
* Электрические параметры.
* Скорость распространения волны.
* Тестирование участков цепи с целью локализовать неисправность.
* Оценка работоспособности адаптера.
* Сбор статистики.
* Генерация дополнительного трафика с целью проверить пропускную способность линии. Сформированные пакеты позволяют оценить достижимость узла.

[](https://setinoid.ru/wp-content/uploads/2017/12/186.jpg)

Системы управления сетью

Программное обеспечение диагностики сети обладает качествами:

* открытость;
* масштабируемость;
* распределённость.

Первоначально в историческом плане ключики забрал администратор. Королевский ПК содержал полностью работоспособную, самодостаточную версию ПО. Рабы-клиенты находились под пристальным присмотром. Наличие масштабной сети ломает принцип. Маломощный администраторский ПК перестаёт справляться. Иногда помогает наём команды сетевиков. Система контроля становится распределённой. Совместимость железа ведущих компаний оставляет желать лучшего. Возникают ошибки построения карты, дополнительные полезные функции оборудования игнорируются.

Производителям приходится учитывать полный перечень стандартов баз: MIB-I, MIB-II, RMONMIB. Сюда добавляются «фирменные» наработки. Самобытные разрозненные варианты учитываются, расширяя объем труда поставщиков оборудования, ПО. Например, Spectrum поддерживает порядка 1000 модификаций. Рекомендуется ставить оболочки фирмы, оборудование которой составляет подавляющую часть инфраструктуры, снижая риск ошибок. Отыскивая консенсус, производители стали применять унифицированные хранилища: Oracle, Informix, Ingres.

ПО каждого производителя демонстрирует определённые преимущества. Иначе давно наметился бы победитель, захвативший рынок целиком.

[](https://setinoid.ru/wp-content/uploads/2017/12/187.jpg)

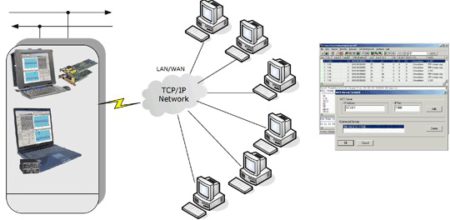
Анализатор трафика (протокола)

Оценку трафика выполняют снифферы (англ. – обнюхивать). Средства (компонент WindowsNTPerformanceMonitor) осуществляют перехват любых пакетов, включая чужие. Поскольку Ethernet носит широковещательный оттенок, администратор получает полный контроль локального сегмента. Грамотно настроенный хаб выступает защитой против несанкционированного прослушивания. Коммутаторы отсекают уже на входе заведомо ненужные внешние адреса. Разбиение сети на сегменты сильно снижает нагрузку.

Специализированные устройства, ПК, ноутбук снабжают администратора возможностью перехватывать любые пакеты. Необходимо соответствие сетевой карты, ПО типу протокола (Ethernet, Token Ring, FDDI). Адаптер анализатора трафика настроен ловить любые адреса. Это позволяет сделать особый режим promiscuous. Ядро поддерживает функционирование аппаратной части, декодируя канальный уровень протокола, иногда более высокие ступени (IP, TCP, Telnet, FTP, HTTP). Стандартной считают поддержку стеков TCP/IP, NetBIOS, Banyan VINES, Novell NetWare. Параллельно сниффер выполняет иные функции:

* Сбор аналитической информации (статистика): количество битых пакетов, перекрёстный трафик узлов, коэффициент использования сегмента.
* Сниффер часто опрашивает агентов различных сегментов.
* Графический интерфейс упрощает труд человека-оператора. Использование триггеров позволяет выставить условия начала, окончания захвата трафика. Пакеты фильтруют, отбрасывая заведомо ненужные.
* Отдельные анализаторы поддерживают шпионство за несколькими mac-адресами. Например, Network Monitor (Windows NT Server) версии выше четвертой.

Физический уровень мало порадует живого наблюдателя. Разрозненные кадры ненаглядны.

[](https://setinoid.ru/wp-content/uploads/2017/12/188.jpg)

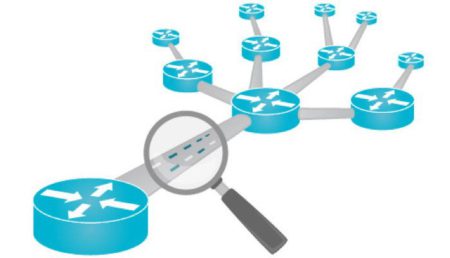
Методики

* Прослушивание эффективно при использовании концентраторов. Поскольку коммутаторы передают информацию по-иному. Администратор увидит отдельные фреймы.
* Программное, либо аппаратное переправления трафика персональному компьютеру, использующему сниффер. Помогает получить полный пакет данных.
* Использование аппаратной реализации сниффера, выступающей неотъемлемой частью канала.
* «Хакерская» атака. Перенаправляет трафик жертвы злоумышленнику. Диссидент взламывает канальный, сетевой уровень OSI.
* Прослушивание электромагнитного излучения линии, последующее восстановление информации.

90-е годы считают пиком явления перехвата злоумышленниками паролей: некоторые сетевые протоколы забывали шифровать персональные данные пользователей. Хабы легко позволяли реализовать задуманное. Обнаружить факт кражи чрезвычайно сложно. Администратору перехват помогает выявить:

* Паразитные пакеты, бессмысленно загружающие сеть. Заметив ненормальную циркуляцию информации, эксперт предпринимает шаги по устранению эффекта. Отдельные снифферы малоэффективны, сбор ведётся системой серверов, сетевым оборудованием.
* Воровать пароли «плохих» пользователей.
* Выявить неисправность инфраструктуры, ошибочную конфигурацию.
* Обнаружить вредоносный трафик широкого спектра: трояны, флудеры, пиринговые сети.

Анализ большого объёма трафика затруднителен.

[](https://setinoid.ru/wp-content/uploads/2017/12/189.jpg)

Сетевой анализатор

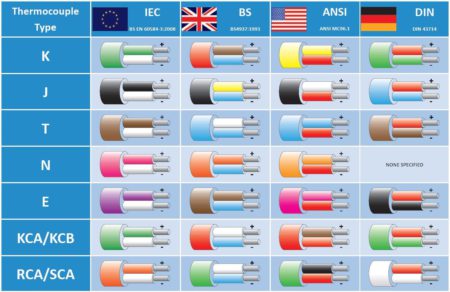
Сюда относят (например, систему Хьюлет-Паккард HP 4195A, 8510C) экспертное оборудование оценки работоспособности кабельного хозяйства путём измерения электрических параметров. Иногда захватывают иерархию протоколов. Особой формы сигналы позволяют оценить амплитудно-частотную характеристику линии, затухание, наводки. Методика сильно напоминает принцип действия оборудования оценки целостности высоковольтных кабелей. Хотя больших напряжений не требуется, поэтому механизм более миниатюрные (промышленные занимают фургон грузовика). Сетевой анализатор иногда способен выполнить ряд функций сниффера, но скорее вспомогательных. Базовые перехватчиков пакетов осуществляет индивидуально.

* Перекрёстные наводки (NEXT) возникают меж проводами витой пары. Величина определена частотой, категорией кабеля. Выражена децибелами.
* Импеданс (комбинация активного, реактивного сопротивлений). Действительная составляющая определяется материалом проводника, меньше зависит от частоты. Мнимая компонента образована влиянием реактивных составляющих (ёмкости, индуктивности). Волновое сопротивление характеризует тип линии. Связь с импедансом слабая.
* Затухание обусловлено наличием волнового, активного сопротивлений. Скин-эффект провоцирует излучение части мощности, снижая характеристики системы: выше частота → тоньше слой → больше сопротивление → растут потери. Пятая категория кабелей демонстрирует значение 23,6 дБ/100 м.
* Величина электромагнитного излучения. Экран сильно снижает выбросы энергии вовне.

Сканеры, тестеры

Указанный класс оборудования оценивает электрические параметры кабеля, длину, сильно уступает точностью сетевым анализаторам. Портативные варианты стали неотъемлемыми спутниками ремонтников. Оцениваются:

* Волновое сопротивление.
* NEXT.
* Затухание сигнала.
* Схема разводки.

[](https://setinoid.ru/wp-content/uploads/2017/12/1810.jpg)

Принцип действия

Повторяет методику высоковольтных приборов. Излучается импульс – ловится эхо. Количество, форма ответных сигналов позволяют оценить физическое состояние кабеля. Принцип потребует знания о скорости распространения сигнала внутри среды. Некоторые модели снабжены собственной базой данных, содержащей справочные сведения. Тестеры намного проще. Урезанный вариант алгоритма просто отвечает на вопрос о целостности кабеля, лишён подробностей.

Сканером принято измерять длину линии. Отдельные модели стоят весьма дорого (1-3 тыс. $). Выпускаются компаниями Datacom, Fluke, Microtest, Scope Communications.

Коммутаторы

Опытному инженеру многое расскажет поведение сетевого оборудования. Перегрузка процессоров, портов необратимо вызывает потерю кадров. Стандартные коммутаторы снабжают агентами, докладывающими о неполадках. Иначе задача отслеживания неполадок сильно усложняется. Проще эксплуатировать концентраторы: тестирующее оборудование вешают на свободный порт. Коммутаторы требуют последовательного включения (разрыв). Свободные порты получат только широковещательный трафик.

Дело усложняется наличием нескольких виртуальных сетей. Тогда оборудование получает пакеты лишь текущей (определено IP-адресом). Производители коммутаторов осознали недостаток устройств, модели стали снабжать функцией зеркалирования. Аппаратура отображает трафик на тестовый разъем. Затруднительным остаётся посмотреть пакеты сразу двух портов, либо одного, функционирующего в полнодуплексном режиме.

Сказанное объясняет предпочтение администраторов использования агентов. Переданная контрольной точке информация содержит полный перечень пакетов. RMON собирает трафик Ethernet, Token Ring, создаёт матрицы перекрёстного трафика. Здесь вопрос касается стоимости. Дорого отображать 9 объектов Ethernet, производители урезают список. Иногда упраздняют раздельное тестирование портов, объединяя их группами.