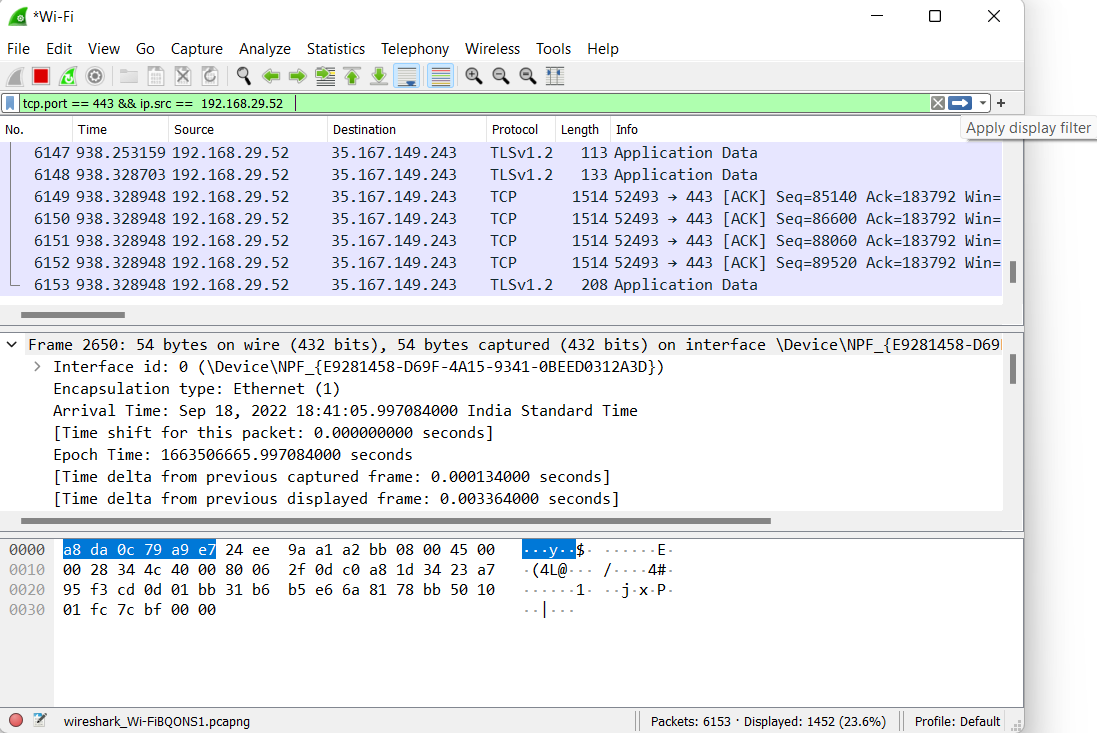
Мониторинг и диагностика сети

# Инструмент мониторинга Wireshark

**Wireshark** — инструмент для анализа сетевых пакетов, который позволяет захватывать трафик, фильтровать его по протоколам и IP-адресам.



## Захват трафика

Чтобы захватить трафик в Wireshark, нужно:

* Выбрать сетевой интерфейс, с которого будет собираться трафик (например, Ethernet, Wi-Fi).
* Нажать кнопку Start — захват начнётся сразу.

После начала захвата на экране будут отображаться пакеты, проходящие через выбранный интерфейс. Можно остановить захват, нажав на красную кнопку ***Stop***, или сохранить захваченный трафик в файл (формат ***.pcap***) для дальнейшего анализа.

## Фильтрация по протоколам

Для фильтрации трафика по протоколам в Wireshark используются фильтры отображения (Display Filters). Чтобы показать только пакеты по определённому протоколу, нужно ввести его название в строке фильтра и нажать Enter.

Если нужно отфильтровать трафик по нескольким протоколам, имена протоколов отделяются символом || (логический оператор OR). Например, ***http || arp || icmp*** покажет пакеты по протоколам HTTP, ARP и ICMP.

## Фильтрация по IP-адресам

Для фильтрации трафика по IP-адресам в Wireshark используются фильтры захвата (Capture Filters) и фильтры отображения (Display Filters).

**Фильтры захвата** задаются до начала захвата трафика и определяют, какие пакеты программа будет записывать. Например, ***host 192.168.1.1*** — захват пакетов от конкретного IP-адреса.

**Фильтры отображения** применяются к уже захваченному трафику для поиска и анализа интересующих пакетов. Чтобы показать только пакеты из определённого IP-адреса, используется фильтр ***ip.src == 192.168.1.1.***

## Примеры фильтров

Ещё несколько примеров фильтров в Wireshark:

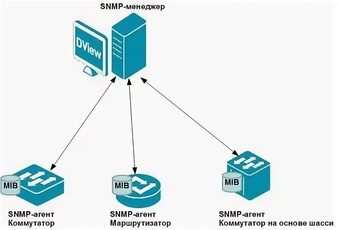
* Показать только DNS-запросы: ***dns.***
* Показать трафик к определённому порту: ***tcp.port == 443.***
* Показать пакеты, содержащие конкретное слово: ***frame contains "password".***

Фильтры можно объединять с помощью логических операций: ***!(arp or icmp or dns)*** — показать любой трафик, кроме ARP, ICMP и DNS.

# Simple Network Management Protocol

**SNMP (Simple Network Management Protocol)** — протокол прикладного уровня для управления и мониторинга сетевых устройств. Он позволяет администраторам собирать информацию, настраивать параметры и получать уведомления от маршрутизаторов, коммутаторов, серверов и других устройств.

SNMP работает по модели клиент-сервер: сетевые устройства (агенты) взаимодействуют с центральной системой управления (менеджером) с помощью SNMP-сообщений.



## Настройка агентов

Некоторые аспекты настройки агентов SNMP:

* **Установка программного модуля**. Агент запускается на управляемом устройстве (например, маршрутизаторе, коммутаторе).
* **Сбор информации**. Агент собирает данные о производительности, конфигурации и состоянии устройства в базе управляющей информации (MIB).
* **Отправка уведомлений**. При событиях (например, сбое интерфейса) агент отправляет уведомление менеджеру (trap или inform).
* **Настройка безопасности**. Например, в Windows для службы SNMP нужно указать имена хостов, которые следует аутентифицировать, и выставить уровень доступа (чтение только, чтение/запись и др.).

## Настройка менеджеров

Некоторые аспекты настройки менеджеров SNMP:

* **Установка программного обеспечения**. На станции управления (менеджере) устанавливается программа, которая будет выступать в роли менеджера SNMP.
* **Добавление агентов**. В настройках менеджера нужно указать IP-адрес управляемого устройства и добавить его в список агентов.
* **Запрос данных**. Чтобы получить значение параметра агента, нужно знать его OID (уникальный идентификатор).

## Проблемы безопасности

Некоторые проблемы безопасности в SNMP и способы их решения:

* **Использование SNMPv3**. Эта версия поддерживает более безопасные механизмы аутентификации и шифрования.
* **Ограничение доступа**. Можно использовать списки контроля доступа (ACLs) для ограничения запросов SNMP на доверенные IP-адреса.
* **Шифрование трафика**. Даже при использовании SNMPv3 рекомендуется шифровать трафик на уровне сети с помощью VPN или IPsec.
* **Регулярные обновления**. Важно, чтобы все устройства, использующие SNMP, были обновлены до последних патчей и обновлений прошивки.

# Системы мониторинга

Системы мониторинга позволяют настраивать оповещения (алерты) и создавать дашборды для визуализации данных. Эти функции доступны в различных инструментах, например, в Zabbix, Yandex Monitoring, Prometheus.

## Настройка оповещения

**Алерты** — автоматические предупреждения, которые срабатывают при достижении определённых условий или пороговых значений в системе мониторинга. Уведомления отправляются на указанные контактные данные (электронная почта, SMS, мессенджеры) в случае срабатывания алерта.

Некоторые этапы настройки оповещений:

* **Определение ключевых метрик и пороговых значений**. Нужно выбрать критичные метрики (например, загрузка ЦП, использование оперативной памяти) и установить пороговые значения, при превышении которых должен сработать алерт.
* **Создание алертов**. Системы мониторинга позволяют настроить алерты по заданным метрикам, указать условия срабатывания (пороговые значения, временные интервалы).
* **Настройка уведомлений**. Нужно определить, каким образом уведомления будут доставляться ответственным лицам, и составить шаблоны для них (описание проблемы, метрики, временные метки, ссылки на соответствующие графики и логи).
* **Тестирование и оптимизация**. Нужно провести тесты для проверки корректности работы алертов и уведомлений, убедиться, что они срабатывают при достижении установленных условий. Также следует получать и анализировать обратную связь от пользователей системы и вносить изменения в настройки оповещений для повышения их точности и эффективности.

## Создание дашбордов

**Дашборд** — это инструмент для визуализации данных, который может включать графики, диаграммы, таблицы и другие элементы. Некоторые инструменты для создания дашбордов:

* **Zabbix**. Позволяет создавать главную панель (Dashboard) с графиками, картами и индикаторами состояния.
* **Yandex Monitoring**. Дашборды создаются на основе метрик, можно создать отдельный график для нескольких метрик или собрать все метрики приложения на одном дашборде.
* **Prometheus**. Для визуализации данных используется Grafana, которая позволяет создавать дашборды и отчёты.

Рекомендации по созданию дашборда:

* **Продумать структуру**. Элементы дашборда должны быть логичными, с возможностью фильтрации данных по параметрам (например, по временным периодам).
* **Использовать визуальные элементы**. Например, выделять ключевые показатели цветом, использовать цветовые шкалы для отображения роста или падения показателей.
* **Добавить поясняющие элементы**. Включить заголовки и описания для каждой секции и графика, использовать подсказки и аннотации для предоставления дополнительной информации по данным.

# Логирование и анализ событий

**Логи (от англ. logs)** — это текстовые файлы или структурированные записи, в которых хранится информация о работе системы, приложения или сервиса. Логи служат для анализа событий, поиска ошибок и отслеживания активности. Их можно сравнить с «дневником» системы, который записывает всё происходящее, от успешного выполнения операции до критической ошибки

**Сбор и анализ логов** — основа мониторинга, диагностики и обеспечения безопасности современных распределённых систем

Рассмотрим некоторые инструменты для сбора и анализа логов:

1. **Syslog** — стандартный инструмент для сбора логов. Формат сообщений syslog включает дату, время с микросекундами, уровень лога, метку, PID, имя файла и номер строки в исходниках, имя функции. Syslog добавляет к этому сообщению информацию от себя: время, PID, hostname сервера и ident. Обычно это просто название программы, но туда можно передать всё что угодно.
2. **ELK Stack** — популярная система для сбора и анализа логов. Она бесплатная, простая, гибкая и мощная. ELK Stack состоит из трёх компонентов:

* **Elastic Search** — система хранения и поиска данных, основанная на «движке» Lucene.
* **Logstash** — инструмент, через который данные (возможно, обработанные) попадают в Elastic Search.
* **Kibana** — веб-интерфейс для поиска и визуализации данных из Elastic Search.