

Министерство образования и молодежной политики
Свердловской Области
ГАПОУ СО «Баранчинский электромеханический техникум имени героя
СССР Д.А.Рыжова»

Курсовая работа

по дисциплине:

«МДК 01.02.....»

на тему:

«Поиск и исправление неисправностей в современных вычислительных
сетях»

Выполнил студент гр.21
Лопарев Роман Евгеньевич
Проверил:

СОДЕРЖАНИЕ

Введение	3
----------------	---

Глава 1. Теоретическая часть. Проблемы в вычислительных сетях

1.1 Классификация неисправностей	5
1.2 Проблемы физического уровня	6
1.3 Проблемы канального уровня	7
1.4 Проблемы сетевого уровня	9
1.5 Проблемы транспортного и прикладного уровня	10
1.6 Проблемы беспроводных сетей Wi-Fi	12
1.7 Статистика и редкие неисправности	14

Глава 2. Практическая часть. Нахождение и устранение неисправностей

2.1 Методология поиска неисправностей	16
2.2 Утилиты и программы для диагностики	17
2.3 Оборудование для диагностики	25
2.4 Практические сценарии устранения неисправностей	28
Демонстрация навыков в программе cisco packet tracer.....	35
2.5 Профилактика и мониторинг	38
2.6 Пример диагностики реальной сети (кейс)	41

Заключительная часть

Заключение	42
Список литературы	43

Введение

Актуальность темы. Вычислительные сети являются основой информационной инфраструктуры современных организаций. С ростом их сложности увеличивается вероятность сбоев: по данным Cisco и Fluke Networks, до 60% проблем связаны с физическим уровнем, а 70% инцидентов вызваны человеческим фактором. Умение оперативно диагностировать и устранять неисправности — ключевая компетенция сетевого администратора.

Цель работы — систематизировать знания о типовых неисправностях в вычислительных сетях и разработать практические рекомендации по их диагностике.

Задачи:

- классифицировать неисправности по уровням модели OSI и источникам возникновения;
- проанализировать проблемы проводных и беспроводных сетей;
- изучить методологии поиска неисправностей и инструменты диагностики;
- разработать практические сценарии устранения типовых проблем;
- рассмотреть вопросы профилактики и мониторинга.

Объект исследования — современные вычислительные сети. Предмет — методы и средства поиска и устранения сетевых неисправностей.

Методы: системный анализ, изучение технической документации, моделирование в Cisco Packet Tracer, обобщение практического опыта.

Практическая значимость: результаты работы могут использоваться как учебное пособие для начинающих сетевых администраторов и как справочный материал при устранении типовых неисправностей.

Структура: работа включает теоретическую часть (классификация и описание проблем по уровням OSI) и практическую часть (методы диагностики, инструменты, сценарии устранения, кейс).

Глава 1. Теоретическая часть. Проблемы в вычислительных сетях.

1.1 Классификация неисправностей

Все неисправности в вычислительных сетях можно классифицировать по нескольким признакам: по уровню модели OSI, по характеру проявления и по источнику возникновения. Такая классификация позволяет системно подходить к диагностике и быстрее локализовать проблему.

По уровню модели OSI неисправности делятся на следующие категории. На физическом уровне возникают обрывы кабеля, повреждения витой пары, неисправности портов коммутаторов и сетевых карт. На канальном уровне наблюдаются коллизии в сетях с разделяемой средой, дублирование MAC-адресов, петли в протоколе STP. На сетевом уровне встречаются проблемы маршрутизации, конфликты IP-адресов и неправильные маски подсети. На транспортном уровне возможны блокировка портов межсетевым экраном, исчерпание портов NAT и таймауты TCP-сессий. На прикладном уровне возникают ошибки DNS, отказы DHCP-серверов, проблемы аутентификации по протоколам 802.1X и RADIUS, а также неправильные настройки прокси-серверов.

По характеру проявления неисправности можно разделить на полный отказ сети, периодические потери пакетов, низкую пропускную способность, высокую задержку (латентность) и нестабильное беспроводное соединение. Каждый тип проявления указывает на определённую группу причин и требует специфических методов диагностики.

По источнику возникновения выделяют аппаратные неисправности, связанные с отказом сетевого оборудования, кабелей и разъёмов; программные неисправности, вызванные ошибками драйверов, некорректными настройками операционной системы или устаревшими

прошивками; а также внешние факторы, включая электромагнитные помехи, сетевые атаки и перегрузки каналов связи.

1.2 Проблемы физического уровня

Проблемы физического уровня являются наиболее частыми в практике сетевого администратора. К ним относятся следующие.

Обрыв или повреждение витой пары, особенно в местах перегибов и под воздействием влаги. При обрыве одной или нескольких пар сигнал полностью пропадает или становятся недоступными высокие скорости передачи.

Необжатый или неправильно обжатый кабель. Существует два стандарта обжима витой пары: прямой (T568A или T568B) и перекрёстный (кроссовер). Если кабель обжат неправильно, сигнал может затухать или полностью отсутствовать. Особенно часто ошибки встречаются при обжиге кабеля категории 6 и выше, где требуется соблюдать длину разделки проводников.

Повреждённый разъём RJ-45. Защёлка разъёма может сломаться, контакты могут окислиться или погнуться. Это приводит к нестабильному соединению с периодическими потерями связи при малейшем шевелении кабеля.

Неисправность порта коммутатора или сетевой карты. Порт может быть повреждён статическим электричеством или скачком напряжения. При этом индикатор активности может гореть, но трафик не проходит. Также порт может быть заблокирован программно (административно выключен).

Электромагнитные помехи от силовых кабелей, расположенных рядом с сетевыми. Прокладка сетевых кабелей параллельно силовым на расстоянии менее 30 сантиметров вызывает наводки и ошибки передачи данных.

Превышение максимальной длины сегмента. Для витой пары категории 5е максимальная длина составляет 100 метров. Превышение этого предела ведёт к затуханию сигнала, росту числа ошибок и полной потере связи.

Использование кабеля несоответствующей категории. Например, кабель категории 5 не способен стабильно работать на скорости 1 Гбит/с, что приведёт к постоянным ошибкам и падению скорости.

В оптоволоконных линиях добавляются специфические проблемы: микротрещины в волокне, перегиб с радиусом менее допустимого, загрязнение оптических разъёмов, несоответствие типов разъёмов (РС и APC), превышение бюджета потерь.

Технология Power over Ethernet (PoE) также создаёт дополнительные сценарии проблем. Недостаточная мощность PoE-коммутатора или инжектора приводит к тому, что подключённые устройства периодически перезагружаются. Некачественный кабель с высоким сопротивлением вызывает падение напряжения на длине более 50 метров, из-за чего устройство работает нестабильно. Коммутатор может неправильно определить класс PoE-устройства и подать недостаточное напряжение.

1.3 Проблемы канального уровня

На канальном уровне возникают проблемы, связанные с передачей кадров в пределах одного сегмента сети.

Шторм широковещательных пакетов (broadcast storm) происходит, когда одно устройство начинает генерировать огромное количество широковещательных пакетов. Это может быть вызвано вирусом, неправильной конфигурацией или ошибкой в драйвере. Сеть полностью

парализуется, так как коммутаторы вынуждены обрабатывать и ретранслировать все широковещательные пакеты на все порты.

Петли в сети (loop) из-за ошибок протокола STP. Если администратор случайно создал физическую петлю (например, соединил два коммутатора двумя кабелями), а протокол Spanning Tree Protocol отключён или настроен неправильно, кадры начинают бесконечно циркулировать по петле, размножаясь и заполняя всю доступную пропускную способность.

Конфликт MAC-адресов возникает, когда два устройства в одной сети имеют одинаковый аппаратный адрес. Это может случиться при ручном клонировании MAC-адреса или при выходе на рынок оборудования с неуникальными адресами от малоизвестных производителей. Коммутатор не может определить, на какой порт отправлять кадры, и связь с обоими устройствами становится нестабильной.

Неправильная работа VLAN. Если порт коммутатора настроен на access-порт в одной VLAN, а подключённое устройство ожидает другую VLAN, связь отсутствует. Если транковый порт пропускает не все VLAN, трафик из некоторых виртуальных сетей теряется. Также возможна ситуация, когда трафик из одной VLAN попадает в другую из-за ошибки конфигурации.

Ошибки согласования скоростей и дуплекса. Если одно устройство работает на скорости 100 Мбит/с в полудуплексе, а другое — на 1 Гбит/с в полном дуплексе, возникают коллизии, потери кадров и резкое падение производительности. Это одна из самых коварных проблем, так как соединение формально есть, но работает очень медленно.

Проблемы с протоколом STP, кроме петель, включают неправильный выбор корневого моста (корневым становится слабый коммутатор на периферии), постоянное переключение состояний портов (flapping) из-за нестабильных

ссылок, а также несовместимость версий STP (802.1D, 802.1w Rapid STP, 802.1s Multiple STP).

1.4 Проблемы сетевого уровня

Сетевой уровень отвечает за маршрутизацию пакетов между различными сетями. Проблемы здесь часто связаны с адресацией и маршрутами.

Конфликт IP-адресов происходит, когда двум устройствам в одной подсети назначен одинаковый IP-адрес. Это может случиться при неправильной настройке статических адресов или при сбое DHCP-сервера, когда он выдаёт уже занятый адрес. Симптомы: одно из устройств теряет связь, периодически появляются сообщения об ошибке.

Неправильная таблица маршрутизации. Маршрутизатор может не знать маршрут к какой-либо сети, и пакеты в неё будут отбрасываться. Или маршрут может быть прописан неверно, и пакеты уходят не по тому направлению. Возможно также заикливание маршрутов, когда пакеты бесконечно пересылаются между двумя маршрутизаторами.

Отсутствие шлюза по умолчанию. Устройство имеет IP-адрес и маску, но не знает адрес маршрутизатора, через который можно выйти в другие подсети и интернет. В результате локальная сеть работает, а внешний мир недоступен.

Неправильная маска подсети. Если у двух устройств в одной физической сети разные маски подсети, они могут не видеть друг друга. Например, одно устройство с адресом 192.168.1.10 и маской 255.255.255.0 считает, что сеть — это 192.168.1.0–255, а другое с той же маской, но с адресом 192.168.2.10 считает своей сетью 192.168.2.0–255. Физически они могут быть в одном

коммутаторе, но логически — в разных сетях, и без маршрутизатора не увидят друг друга.

Фрагментация пакетов и проблемы с MTU. Каждый тип сети имеет максимальный размер передаваемого пакета (MTU). Для Ethernet это обычно 1500 байт. Если пакет больше, он должен быть фрагментирован. Однако некоторые протоколы и устройства запрещают фрагментацию (DF-бит = 1). В этом случае крупные пакеты отбрасываются. Типичная ситуация: веб-страницы открываются, а большие файлы не скачиваются.

Проблемы с протоколами динамической маршрутизации (OSPF, EIGRP, BGP). Ошибка в настройке области OSPF приводит к тому, что соседние маршрутизаторы не обмениваются маршрутами. Несовпадение таймеров Hello и Dead вызывает постоянные разрывы соседства. В BGP типичной проблемой является неправильная настройка AS_PATH, из-за чего маршруты не принимаются из-за обнаружения петли. Фильтрация маршрутов на интерфейсах может привести к «исчезновению» целых сетей.

Проблемы с NAT (трансляцией адресов). Если NAT настроен неправильно, локальные адреса не транслируются во внешние, и доступа в интернет нет. Истощение портов NAT происходит, когда большое количество внутренних соединений (например, через торрент-клиент) занимает все доступные порты, и новые соединения не могут быть установлены.

1.5 Проблемы транспортного и прикладного уровня

На транспортном уровне основными протоколами являются TCP (с контролем доставки) и UDP (без контроля). Проблемы здесь часто связаны с фильтрацией и перегрузкой.

Блокировка портов межсетевым экраном (firewall). Многие сервисы используют определённые порты: HTTP — 80, HTTPS — 443, SSH — 22,

RDP — 3389. Если порт закрыт, сервис становится недоступен извне, хотя сам сервер работает. Особенно сложно диагностировать ситуацию, когда порт блокируется не на целевом сервере, а на каком-то промежуточном маршрутизаторе или на стороне провайдера.

Исчерпание портов NAT. При трансляции адресов каждое внутреннее соединение получает уникальный порт на внешнем интерфейсе. При большом количестве короткоживущих соединений (например, при интенсивном веб-сёрфинге или работе торрент-клиента) пул портов может исчерпаться, и новые соединения будут отвергаться.

Таймауты TCP-сессий. Если канал связи нестабилен или задержки слишком велики, TCP-соединения могут разрываться по таймауту. Это проявляется в виде «зависаний» при передаче файлов или при работе с удалёнными приложениями.

На прикладном уровне возникают ошибки, связанные с конкретными сервисами и протоколами.

Отказ DNS-сервера. DNS преобразует доменные имена в IP-адреса. Если DNS-сервер недоступен, пользователь не может открыть сайт по имени, хотя пинг по IP-адресу работает. Причины: сбой самого DNS-сервера, неправильные настройки DNS на клиенте, блокировка порта 53.

Недоступность DHCP-сервера. DHCP автоматически выдаёт устройствам IP-адреса, маски, шлюзы и DNS. Если DHCP-сервер не отвечает, устройство может получить автоматический адрес из диапазона 169.254.x.x (APIPA) и не будет иметь доступа к сети. Это одна из самых частых проблем в небольших офисах.

Ошибки аутентификации по протоколам 802.1X и RADIUS. В корпоративных сетях используется портовая аутентификация: устройство не получает доступ к сети, пока не предоставит правильные учётные данные

(сертификат или логин/пароль). Проблемы с сертификатами, неправильная конфигурация RADIUS-сервера или несовместимость версий приводят к тому, что устройство «видит» сеть, но не может подключиться.

Неправильные прокси-настройки. В организациях часто используется прокси-сервер для выхода в интернет. Если в браузере или в операционной системе указан неправильный адрес прокси или прокси не работает, доступ в интернет пропадает, хотя сеть работает.

Ошибки веб-приложений. Веб-сервер может отвечать ошибкой 500 Internal Server Error из-за неправильной конфигурации базы данных, нехватки памяти или ошибки в коде. Пользователь видит «нет соединения с сервером» или «ошибка сервера», хотя на самом деле сетевая связность есть.

1.6 Проблемы беспроводных сетей Wi-Fi

Беспроводные сети имеют свою специфику, связанную с использованием радиоэфира.

Радиопомехи. Диапазон 2.4 ГГц сильно загружен: помимо Wi-Fi, в нём работают микроволновые печи, Bluetooth-устройства, беспроводные камеры, радионяни. Даже соседние точки доступа создают помехи. В результате скорость падает, возникают потери пакетов, разрывы соединений.

Перегруженная точка доступа. Одна точка доступа может обслуживать ограниченное количество клиентов — обычно 20–30 для бытовых моделей и 50–100 для профессиональных. При превышении этого числа клиенты начинают «бороться» за эфир, падает скорость, появляются таймауты подключения.

Неправильный выбор канала. В диапазоне 2.4 ГГц есть три непересекающихся канала — 1, 6 и 11. Если точка доступа работает на канале 3, она создаёт помехи сразу на каналах 1, 6 и 11, и сама испытывает помехи от них. В диапазоне 5 ГГц выбор каналов шире, но тоже требует анализа.

Проблема скрытого узла (hidden node). Возникает, когда два клиента находятся на большом расстоянии друг от друга и не слышат друг друга, но оба видят точку доступа. Они начинают передавать одновременно, создавая коллизии, которые точка доступа не может предотвратить. Это приводит к частым повторным передачам и падению скорости.

Недостаточная мощность сигнала. Если клиент находится далеко от точки доступа или сигнал ослаблен стенами, уровень сигнала становится низким. Скорость автоматически снижается до минимальной (например, с 300 Мбит/с до 5,5 Мбит/с), а соединение может разрываться.

Проблемы с роумингом. В сетях с несколькими точками доступа клиент должен переключаться между ними при перемещении. Если роуминг настроен неправильно, клиент может «залипнуть» на слабой точке доступа или часто терять соединение при переключении.

Устаревшая прошивка точки доступа или клиентского адаптера. Производители постоянно исправляют ошибки и улучшают совместимость. Старая прошивка может содержать известные проблемы, приводящие к нестабильной работе.

1.7 Статистика и редкие неисправности

Согласно исследованиям компаний Cisco и Fluke Networks, распределение неисправностей по уровням модели OSI выглядит следующим образом. Физический уровень составляет от 55 до 60 процентов всех проблем, причём половина из них приходится на некачественную кабельную систему и разъёмы. Канальный уровень даёт около 15 процентов неисправностей, в основном это конфликты в настройках дуплекса и скорости, а также штормы широковещательных пакетов. Сетевой уровень отвечает за 10 процентов отказов, преимущественно из-за ошибок маршрутизации и конфликтов IP-адресов. Транспортный и прикладной уровни вместе составляют оставшиеся 15–20 процентов, причём доля прикладного уровня неуклонно растёт с усложнением программного обеспечения.

По источникам возникновения 70 процентов проблем вызваны человеческим фактором — неправильными настройками, неаккуратным монтажом, несогласованными изменениями. Только 20 процентов связаны с реальным выходом оборудования из строя, и 10 процентов приходятся на внешние факторы, такие как отключения электроэнергии, перегрев или действия злоумышленников.

Помимо типовых проблем, существуют редкие и сложные неисправности, требующие глубоких знаний. Одна из них — ошибки CRC без физических повреждений. Это может быть вызвано нестабильным тактовым генератором на сетевой карте или коммутаторе, что приводит к случайным искажениям битов даже на исправном кабеле. Другая редкая проблема — «фантомные» MAC-адреса, когда коммутатор запоминает адрес устройства, которое уже давно отключено, и продолжает отправлять ему трафик, создавая чёрную дыру. Ещё одна сложная неисправность — асимметричная маршрутизация в сетях с несколькими маршрутизаторами, когда пакеты в одном направлении идут по одному пути, а в обратном — по другому. Это вызывает сбои в

работе протоколов, зависящих от порядка пакетов, например некоторых реализаций VoIP и видеоконференций.

Глава 2. Практическая часть. Нахождение и устранение неисправностей

2.1 Методология поиска неисправностей

Поиск неисправностей требует системного подхода. Применяются следующие модели диагностики.

OSI-подход предполагает диагностику снизу вверх, начиная с физического уровня и постепенно поднимаясь к прикладному. Сначала проверяются кабели и порты, затем — канальный уровень (MAC-адреса, VLAN, STP), потом — сетевой уровень (IP, маршрутизация), транспортный (порты, NAT) и, наконец, прикладной (DNS, DHCP, приложения). Этот метод наиболее системный и позволяет исключать целые уровни один за другим.

TCP/IP-подход фокусируется на проверке маршрутизации и транспортных соединений, что актуально для интернет-сетей. Метод деления пополам заключается в том, что сеть условно делится на две части, и проверяется, в какой из них присутствует проблема, после чего деление повторяется. Сравнение с эталонной работой сети подразумевает наличие заранее задокументированных нормальных показателей задержки, потерь и пропускной способности, с которыми сравниваются текущие значения.

Процесс диагностики включает несколько стандартных этапов. Сначала производится сбор жалоб и описание симптомов от пользователей. Затем выполняется проверка физических подключений, включая визуальный осмотр кабелей и разъёмов. После этого специалист проверяет работу сети на своей собственной рабочей станции, чтобы исключить проблемы конкретного компьютера. Далее следует проверка сетевого оборудования и его конфигурации. При необходимости проводится анализ трафика с помощью сниффера. Затем происходит локализация и устранение неисправности. Завершающим этапом является документирование проблемы и способа её решения для будущего использования.

Важной частью методологии является ведение журнала действий и создание базы знаний. Когда администратор сталкивается с проблемой, он должен записывать каждый свой шаг, включая выполненные команды, полученные результаты и затраченное время. Это позволяет не повторять одни и те же проверки и при необходимости передать проблему коллеге. После устранения неисправности необходимо оформить запись в базе знаний, содержащую описание симптомов, точную причину, способ решения и команды для диагностики. Такая база знаний со временем становится самым ценным активом IT-отдела.

Не следует забывать о психологических аспектах. Эффект подтверждения заставляет администратора искать только те данные, которые подтверждают его первоначальную гипотезу, и игнорировать противоречия. Эффект Даннинга — Крюгера приводит к тому, что начинающие специалисты переоценивают свои знания и пропускают очевидные проверки. Усталость и стресс снижают качество диагностики. Рекомендации: делать перерывы, привлекать второго специалиста для свежего взгляда, записывать свои предположения и затем намеренно искать опровергающие их факты.

2.2 Утилиты и программы для диагностики

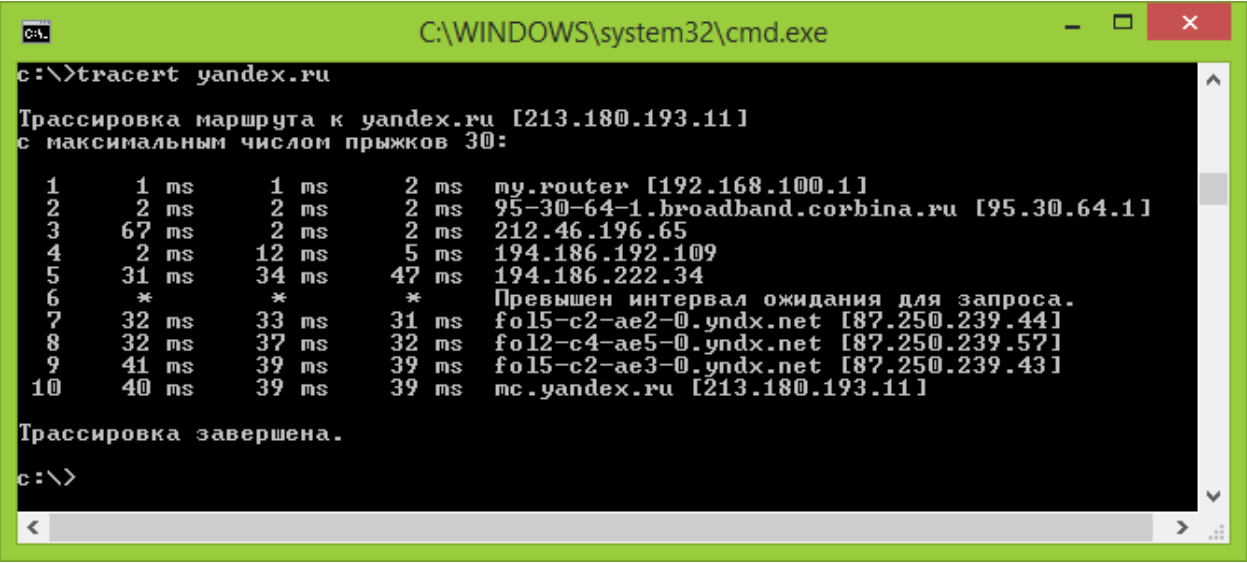
Для диагностики сетевых неисправностей существует множество программных средств. Базовые утилиты встроены в операционные системы.

Утилита ping служит для проверки доступности узла путём отправки ICMP-запросов. Пример: ping 8.8.8.8 -t. Если ping проходит, значит, сетевой уровень работает. Если нет — проблема где-то на физическом, канальном или сетевом уровне. Потери пакетов указывают на нестабильность канала или перегрузку.

```
root@aventurine-topaz:~/ > ping -6 -c 12 anilist.co
PING anilist.co (2606:4700:20::681a:f47) 56 data bytes
64 bytes from 2606:4700:20::681a:f47: icmp_seq=1 ttl=59 time=50.9 ms
64 bytes from 2606:4700:20::681a:f47: icmp_seq=2 ttl=59 time=23.6 ms
64 bytes from 2606:4700:20::681a:f47: icmp_seq=3 ttl=59 time=94.9 ms
64 bytes from 2606:4700:20::681a:f47: icmp_seq=4 ttl=59 time=146 ms
64 bytes from 2606:4700:20::681a:f47: icmp_seq=5 ttl=59 time=146 ms
64 bytes from 2606:4700:20::681a:f47: icmp_seq=6 ttl=59 time=31.4 ms
64 bytes from 2606:4700:20::681a:f47: icmp_seq=7 ttl=59 time=335 ms
64 bytes from 2606:4700:20::681a:f47: icmp_seq=8 ttl=59 time=32.3 ms
64 bytes from 2606:4700:20::681a:f47: icmp_seq=9 ttl=59 time=29.5 ms
64 bytes from 2606:4700:20::681a:f47: icmp_seq=10 ttl=59 time=28.5 ms
64 bytes from 2606:4700:20::681a:f47: icmp_seq=11 ttl=59 time=25.2 ms
64 bytes from 2606:4700:20::681a:f47: icmp_seq=12 ttl=59 time=34.7 ms

--- anilist.co ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11012ms
rtt min/avg/max/mdev = 23.641/81.562/335.216/88.043 ms
root@aventurine-topaz:~/ > ping -V
ping from iputils 20240905
libcap: yes, IDN: yes, NLS: yes, error.h: yes, getrandom(): yes, __fpending(): yes
```

Утилита tracert (или traceroute) показывает маршрут следования пакетов до указанного узла. Пример: tracert yandex.ru. Она позволяет определить, на каком промежуточном маршрутизаторе возникают потери или задержки. Если потери начинаются на первом же прыжке (шлюзе), проблема внутри локальной сети. Если на пятом-десятом — проблема на стороне провайдера или магистралей.



```
C:\WINDOWS\system32\cmd.exe
c:\>tracert yandex.ru

Трассировка маршрута к yandex.ru [213.180.193.11]
с максимальным числом прыжков 30:

 1      1 ms      1 ms      2 ms    my.router [192.168.100.1]
 2      2 ms      2 ms      2 ms    95-30-64-1.broadband.corbina.ru [95.30.64.1]
 3     67 ms      2 ms      2 ms    212.46.196.65
 4      2 ms     12 ms      5 ms    194.186.192.109
 5     31 ms     34 ms     47 ms    194.186.222.34
 6      *         *         *      Превышен интервал ожидания для запроса.
 7     32 ms     33 ms     31 ms    fol5-c2-ae2-0.yndx.net [87.250.239.44]
 8     32 ms     37 ms     32 ms    fol2-c4-ae5-0.yndx.net [87.250.239.57]
 9     41 ms     39 ms     39 ms    fol5-c2-ae3-0.yndx.net [87.250.239.43]
10     40 ms     39 ms     39 ms    mc.yandex.ru [213.180.193.11]

Трассировка завершена.
c:\>
```

Утилита `ipconfig` в Windows (или `ifconfig` и `ip` в Linux) отображает и позволяет настраивать IP-адреса, маски подсети и шлюзы. Команда `ipconfig /all` показывает детальную информацию о всех сетевых адаптерах: MAC-адрес, полученный IP, шлюз, DNS-сервера. Это первый шаг при диагностике проблем с IP-конфигурацией.

```
Командная строка
Microsoft Windows [Version 10.0.19045.6456]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\batyr>ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::fcb9:28ab:94a4:b143%9
    IPv4-адрес. . . . . : 192.168.119.118
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.119.1

Адаптер Ethernet ZeroTier One [cf719fd5409b5b10]:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::c8f6:3d35:d00b:202c%13
    IPv4-адрес. . . . . : 10.148.147.32
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 25.255.255.254

C:\Users\batyr>
```

Утилита `nslookup` служит для проверки работы DNS. Пример: `nslookup google.com`. Если команда возвращает IP-адрес, DNS работает. Если нет — проблема с DNS-сервером или его настройками на клиенте.

```
Командная строка
Microsoft Windows [Version 10.0.19045.6456]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\batyr>nslookup yandex.ru
ТхЃтхЃ: dns.yandex.ru
Address: 77.88.8.8

Не заслуживающий доверия ответ:
Ѓь : yandex.ru
Addresses: 2a02:6b8:a::a
          77.88.55.88
          77.88.44.55
          5.255.255.77

C:\Users\batyr>
```

Утилита arp отображает таблицу соответствия между IP-адресами и MAC-адресами. Команда arp -а показывает все записи. Если запись о шлюзе отсутствует или имеет неправильный MAC-адрес (например, 00-00-00-00-00-00), связь со шлюзом невозможна.

Интерфейс: 192.168.119.118 --- 0x9		
адрес в Интернете	Физический адрес	Тип
192.168.119.1	2c-c8-1b-11-32-2e	динамический
192.168.119.103	c0-18-50-86-a4-49	динамический
192.168.119.104	08-94-ef-b8-8d-f0	динамический
192.168.119.105	00-e0-4c-68-48-70	динамический
192.168.119.106	f4-4d-30-06-71-fc	динамический
192.168.119.107	f4-4d-30-00-8d-94	динамический
192.168.119.108	f4-4d-30-00-91-f9	динамический
192.168.119.110	f4-4d-30-00-89-bf	динамический
192.168.119.113	70-85-c2-d4-6e-56	динамический
192.168.119.115	18-c0-4d-23-aa-ac	динамический
192.168.119.121	b8-ae-ed-b8-d4-19	динамический
192.168.119.255	ff-ff-ff-ff-ff-ff	статический
224.0.0.22	01-00-5e-00-00-16	статический
224.0.0.251	01-00-5e-00-00-fb	статический
224.0.0.252	01-00-5e-00-00-fc	статический
239.255.255.250	01-00-5e-7f-ff-fa	статический
255.255.255.255	ff-ff-ff-ff-ff-ff	статический
Интерфейс: 10.148.147.32 --- 0xd		
адрес в Интернете	Физический адрес	Тип
10.148.147.255	ff-ff-ff-ff-ff-ff	статический
25.255.255.254	02-00-a3-5b-d3-92	статический
224.0.0.22	01-00-5e-00-00-16	статический
224.0.0.251	01-00-5e-00-00-fb	статический
224.0.0.252	01-00-5e-00-00-fc	статический
239.255.255.250	01-00-5e-7f-ff-fa	статический

Утилита netstat выводит статистику по сетевым соединениям, открытым портам и таблицам маршрутизации. Команда netstat -an показывает все соединения в числовом виде. Полезна для выявления программ, которые открыли неожиданные порты, или для проверки, слушает ли сервер нужный порт.

```
C:\Users\batyr>netstat

Активные подключения

Имя      Локальный адрес      Внешний адрес      Состояние
TCP      127.0.0.1:9993      DESKTOP-6ASFIE4:55568 TIME_WAIT
TCP      127.0.0.1:9993      DESKTOP-6ASFIE4:55569 TIME_WAIT
TCP      127.0.0.1:9993      DESKTOP-6ASFIE4:55570 TIME_WAIT
TCP      127.0.0.1:9993      DESKTOP-6ASFIE4:55587 TIME_WAIT
TCP      127.0.0.1:9993      DESKTOP-6ASFIE4:55588 TIME_WAIT
TCP      127.0.0.1:9993      DESKTOP-6ASFIE4:55590 ESTABLISHED
TCP      127.0.0.1:49671     DESKTOP-6ASFIE4:49672 ESTABLISHED
TCP      127.0.0.1:49672     DESKTOP-6ASFIE4:49671 ESTABLISHED
TCP      127.0.0.1:55590     DESKTOP-6ASFIE4:9993  ESTABLISHED
TCP      192.168.119.118:52598 1e-in-f188:5228      ESTABLISHED
TCP      192.168.119.118:55498 13.107.226.254:https  CLOSE_WAIT
TCP      192.168.119.118:55499 13.107.253.254:https  CLOSE_WAIT
TCP      192.168.119.118:55505 ip18:https            ESTABLISHED
TCP      192.168.119.118:55507 yandex:https          ESTABLISHED
TCP      192.168.119.118:55508 45.136.22.166:https   ESTABLISHED
TCP      192.168.119.118:55510 ya:https              ESTABLISHED
TCP      192.168.119.118:55518 srv164-137-240-87:https ESTABLISHED
TCP      192.168.119.118:55540 a92-123-189-49:https  ESTABLISHED
TCP      192.168.119.118:55541 40.126.53.6:https     ESTABLISHED
TCP      192.168.119.118:55543 a92-123-189-59:https  ESTABLISHED
TCP      192.168.119.118:55545 150.171.85.254:https  CLOSE_WAIT
TCP      192.168.119.118:55546 13.107.213.254:https  ESTABLISHED
TCP      192.168.119.118:55547 9.235.21.27:https     ESTABLISHED
TCP      192.168.119.118:55550 204.79.197.222:https  ESTABLISHED
TCP      192.168.119.118:55556 150.171.22.254:https  ESTABLISHED
TCP      192.168.119.118:55557 150.171.64.254:https  ESTABLISHED
TCP      192.168.119.118:55567 172.202.65.254:https  ESTABLISHED
TCP      192.168.119.118:55589 srv90-190-240-87:https ESTABLISHED
TCP      192.168.119.118:56649 94.139.248.102:https  ESTABLISHED
```

Утилита route позволяет просматривать и изменять таблицу маршрутизации. Команда route print выводит текущую таблицу маршрутов. Если отсутствует маршрут по умолчанию (0.0.0.0), устройство не знает, куда отправлять пакеты в интернет.

```

C:\Users\batyr>route print
=====
Список интерфейсов
 9...18 c0 4d 23 9c 7a .....Realtek Gaming GbE Family Controller
13...12 b0 2b ce c3 98 .....ZeroTier Virtual Port
 1.....Software Loopback Interface 1
=====

IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
 0.0.0.0            0.0.0.0         25.255.255.254   10.148.147.32  10034
 0.0.0.0            0.0.0.0         192.168.119.1    192.168.119.118  35
 10.148.147.0       255.255.255.0   On-link          10.148.147.32   291
 10.148.147.32      255.255.255.255 On-link          10.148.147.32   291
 10.148.147.255     255.255.255.255 On-link          10.148.147.32   291
 127.0.0.0          255.0.0.0       On-link          127.0.0.1        331
 127.0.0.1          255.255.255.255 On-link          127.0.0.1        331
 127.255.255.255    255.255.255.255 On-link          127.0.0.1        331
 192.168.119.0       255.255.255.0   On-link          192.168.119.118  291
 192.168.119.118     255.255.255.255 On-link          192.168.119.118  291
 192.168.119.255     255.255.255.255 On-link          192.168.119.118  291
 224.0.0.0          240.0.0.0       On-link          127.0.0.1        331
 224.0.0.0          240.0.0.0       On-link          10.148.147.32    291
 224.0.0.0          240.0.0.0       On-link          192.168.119.118  291
 255.255.255.255     255.255.255.255 On-link          127.0.0.1        331
 255.255.255.255     255.255.255.255 On-link          10.148.147.32    291
 255.255.255.255     255.255.255.255 On-link          192.168.119.118  291
=====
Постоянные маршруты:
Отсутствует

IPv6 таблица маршрута
=====
Активные маршруты:
Метрика  Сетевой адрес      Шлюз
 1        331 ::1/128          On-link
13        291 fe80::/64        On-link
 9        291 fe80::/64        On-link
13        291 fe80::c8f6:3d35:d00b:202c/128
          On-link
 9        291 fe80::fcb9:28ab:94a4:b143/128
          On-link
 1        331 ff00::/8          On-link
13        291 ff00::/8          On-link
 9        291 ff00::/8          On-link
=====
Постоянные маршруты:
Отсутствует

```

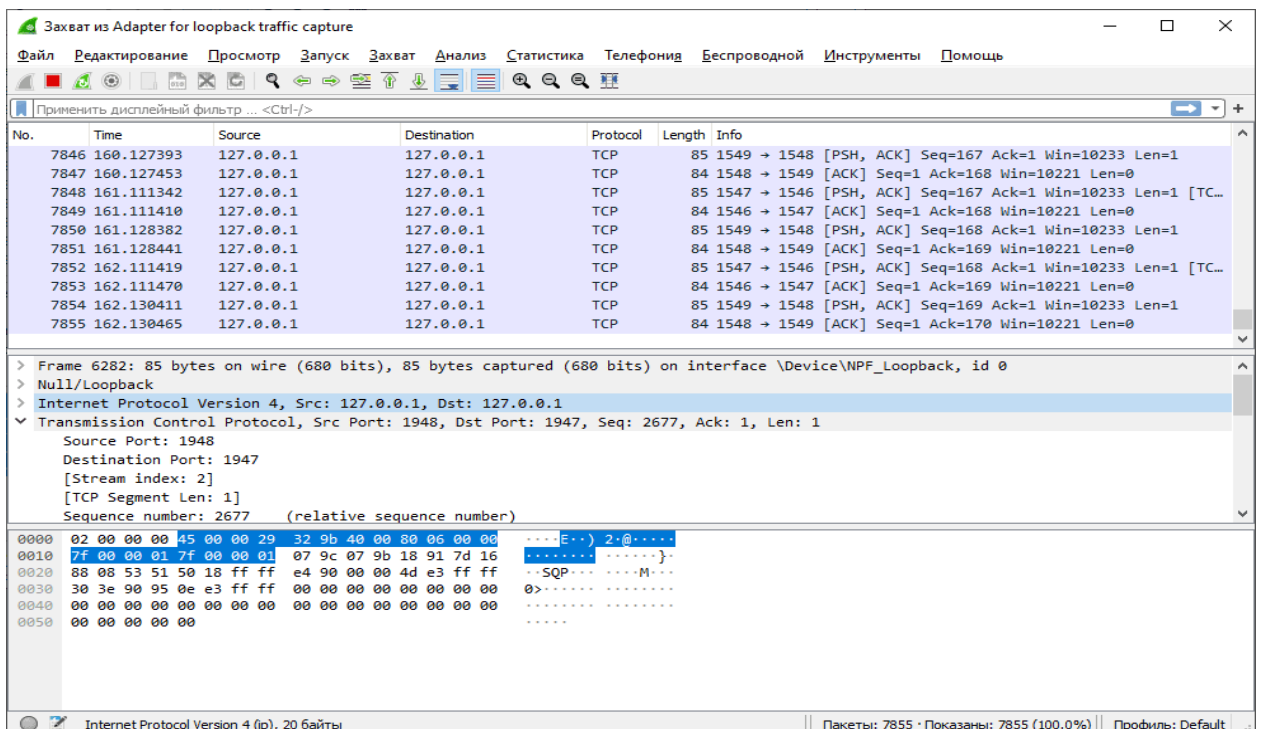
Утилита nmap является мощным сканером портов и узлов сети. Пример: nmap -sP 192.168.1.0/24 выполняет ping-сканирование всей подсети и показывает все активные устройства. Это незаменимо для инвентаризации сети и поиска «лишних» устройств

```
root@kali:~# nmap -sU 192.168.226.130

Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-15 07:57 EDT
Nmap scan report for 192.168.226.130
Host is up (0.00035s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
53/udp    open  domain
68/udp    open|filtered dhcp
69/udp    open|filtered tftp
111/udp   open  rpcbind
137/udp   open  netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open  nfs
MAC Address: 00:0C:29:50:B8:38 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1083.85 seconds
root@kali:~#
```

Среди анализаторов трафика наиболее известен Wireshark. Он позволяет захватывать и детально анализировать сетевые пакеты в реальном времени. Поддерживает сотни протоколов. Фильтры отображения: `ip.src==192.168.1.10` — показать пакеты от указанного источника; `tcp.analysis.retransmission` — выделить повторные передачи TCP, указывающие на потери; `http.response.code>=400` — показать HTTP-ошибки. Wireshark также умеет строить графики загрузки канала (IO Graph) и показывать разговоры между устройствами (Conversations).



Специализированные утилиты решают конкретные задачи. `iperf3` измеряет максимальную пропускную способность канала между двумя узлами. `mttr` объединяет функциональность `ping` и `tracert`, показывая статистику потерь на каждом промежуточном узле в реальном времени. Технологии `NetFlow` и `sFlow` используются для анализа потоков трафика через специальные коллекторы, такие как `SolarWinds` или `ntopng`. `Advanced IP Scanner` быстро находит все активные устройства в локальной сети.

```
C:\Users\79181\Desktop\iperf-3.1.3-win64 (1)\iperf-3.1.3-win64>iperf3 -c 10.23.9.175 -u -w 1m -t 10 -l 1100 -b 1m
Connecting to host 10.23.9.175, port 5201
[ 4] local 10.23.11.128 port 54452 connected to 10.23.9.175 port 5201
[ ID] Interval      Transfer    Bandwidth  Total Datagrams
[ 4] 0.00-1.00 sec  113 KBytes  921 Kbits/sec  105
[ 4] 1.00-2.00 sec  121 KBytes  998 Kbits/sec  113
[ 4] 2.00-3.01 sec  122 KBytes  990 Kbits/sec  114
[ 4] 3.01-4.01 sec  121 KBytes  996 Kbits/sec  113
[ 4] 4.01-5.01 sec  124 KBytes  1.02 Mbits/sec  115
[ 4] 5.01-6.00 sec  122 KBytes  1.01 Mbits/sec  114
[ 4] 6.00-7.01 sec  120 KBytes  978 Kbits/sec  112
[ 4] 7.01-8.01 sec  122 KBytes  1.01 Mbits/sec  114
[ 4] 8.01-9.01 sec  124 KBytes  1.01 Mbits/sec  115
[ 4] 9.01-10.01 sec 121 KBytes  996 Kbits/sec  113
-----
[ ID] Interval      Transfer    Bandwidth  Jitter    Lost/Total Datagrams
[ 4] 0.00-10.01 sec 1.18 MBytes  992 Kbits/sec  2.180 ms  1/1127 (0.089%)
[ 4] Sent 1127 datagrams
iperf Done.
```

Продвинутое использование `ping`: ключ `-l` задаёт размер пакета. Посылая `ping` с размером 1472 байта (что соответствует 1500 байтам с заголовками), можно проверить работу MTU. Ключ `-f` (не фрагментировать) используется для обнаружения путей с недостаточным MTU. Утилита `hping3` является расширенной версией `ping`, способной отправлять не только ICMP, но и TCP, UDP пакеты. Например, `hping3 -S -p 80 8.8.8.8` отправляет TCP SYN-пакет на 80-й порт, что позволяет проверить, открыт ли порт.

```
(root@kali) - [~]
# hping3 -h
usage: hping3 host [options]
-h --help          show this help
-v --version       show version
-c --count         packet count
-i --interval      wait (uX for X microseconds, for example -i u1000)
--fast            alias for -i u10000 (10 packets for second)
--faster          alias for -i u1000 (100 packets for second)
--flood           sent packets as fast as possible. Don't show replies.
-n --numeric       numeric output
-q --quiet         quiet
-I --interface     interface name (otherwise default routing interface)
-V --verbose       verbose mode
-D --debug         debugging info
```

Утилита netcat (nc) позволяет установить произвольное TCP или UDP соединение и вручную отправлять данные. Для проверки доступности порта: nc -zv 192.168.1.1 80. Для тестирования веб-сервера: echo -e "GET / HTTP/1.0\n\n" | nc example.com 80. Netcat также может работать в режиме прослушивания: nc -l -p 1234.

2.3 Оборудование для диагностики

Помимо программных средств, существуют аппаратные инструменты для диагностики сетей.

Кабельные тестеры позволяют прозвонить витую пару и определить обрыв, короткое замыкание или неправильную распиновку. Простые тестеры-тонеры только показывают целостность пар. Профессиональные тестеры (например, Fluke DSX-8000) измеряют десятки параметров: вносимые потери (Insertion Loss), перекрёстные помехи на ближнем конце (NEXT), возвратные потери (Return Loss), задержку распространения (Propagation Delay) и отклонение задержки (Delay Skew). Все эти параметры должны находиться в пределах стандартов для данной категории кабеля.



Рефлектометр TDR (Time Domain Reflectometer) используется для обнаружения места обрыва кабеля. Он посылает импульс и измеряет время его отражения. Зная скорость распространения сигнала в кабеле, можно с точностью до метра определить расстояние до обрыва. Это незаменимо при работе с кабелем, проложенным в стенах или под землёй.



Wi-Fi анализаторы спектра (например, Wi-Spy) помогают выявить радиопомехи и загруженность частотных каналов. Они показывают, какие каналы заняты соседними точками доступа, а где есть посторонние источники помех (микроволновые печи, Bluetooth). На основе этих данных администратор выбирает наименее загруженный канал.



Портативные сетевые тестеры типа LinkRunner от Fluke Networks позволяют быстро проверить наличие сигнала, определить VLAN, получить IP-адрес по DHCP и выполнить базовые ring-тесты без подключения к компьютеру. Это незаменимый инструмент при первом выезде на объект.



Оптические тестеры и OTDR используются для диагностики оптоволокон. Оптический тестер мощности измеряет уровень сигнала на приёмнике и позволяет определить затухание в линии. OTDR (оптический рефлектометр) позволяет обнаружить место обрыва, сварки или изгиба волокна, а также измерить затухание на каждом участке.



2.4 Практические сценарии устранения неисправностей

Сценарий 1: нет связи с сервером, индикаторы горят.

Симптомы: компьютер в сети, IP-адрес получен, но не пингуется шлюз. Диагностика: ping шлюза, ipconfig /all, arp -a. Устранение: проверка кабеля тестером, перезагрузка коммутатора, смена порта на коммутаторе, временное отключение брандмауэра. Чаще всего проблема оказывается в повреждённом патч-корде или в неисправном порту коммутатора.

```
Pinging 192.168.0.153 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.153:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Сценарий 2: низкая скорость Wi-Fi.

Диагностика: iperf3 между клиентом и точкой доступа, Wi-Fi анализатор для

оценки загрузки каналов, проверка загрузки точки доступа. Устранение: смена канала на менее загруженный (для 2.4 ГГц использовать только каналы 1, 6 или 11), перевод клиента на диапазон 5 ГГц, удаление источников радиопомех (микроволновая печь), обновление прошивки точки доступа. Если точка доступа перегружена клиентами, необходимо установить дополнительную точку.

```
C:\Users\79181\Desktop\iperf-3.1.3-win64 (1)\iperf-3.1.3-win64>iperf3 -c 10.23.9.175 -u -w 1m -t 10 -l 1100 -b 1m
Connecting to host 10.23.9.175, port 5201
[ 4] local 10.23.11.128 port 54452 connected to 10.23.9.175 port 5201
[ ID] Interval      Transfer    Bandwidth  Total Datagrams
[ 4] 0.00-1.00  sec    113 KBytes   921 Kbits/sec    105
[ 4] 1.00-2.00  sec    121 KBytes   998 Kbits/sec    113
[ 4] 2.00-3.01  sec    122 KBytes   990 Kbits/sec    114
[ 4] 3.01-4.01  sec    121 KBytes   996 Kbits/sec    113
[ 4] 4.01-5.01  sec    124 KBytes  1.02 Mbits/sec    115
[ 4] 5.01-6.00  sec    122 KBytes  1.01 Mbits/sec    114
[ 4] 6.00-7.01  sec    120 KBytes   978 Kbits/sec    112
[ 4] 7.01-8.01  sec    122 KBytes  1.01 Mbits/sec    114
[ 4] 8.01-9.01  sec    124 KBytes  1.01 Mbits/sec    115
[ 4] 9.01-10.01 sec    121 KBytes   996 Kbits/sec    113
-----
[ ID] Interval      Transfer    Bandwidth  Jitter    Lost/Total Datagrams
[ 4] 0.00-10.01  sec   1.18 MBytes   992 Kbits/sec  2.180 ms  1/1127 (0.089%)
[ 4] Sent 1127 datagrams
iperf Done.
```

Сценарий 3: периодические потери пакетов.

Диагностика: ping 8.8.8.8 -t для наблюдения за потерями, mtr yandex.ru для определения узла потерь. Устранение: замена кабеля (битый проводник — частая причина), отключение энергосбережения на сетевой карте в настройках драйвера, замена сетевого адаптера. Если потери происходят за пределами локальной сети — проблема на стороне провайдера.

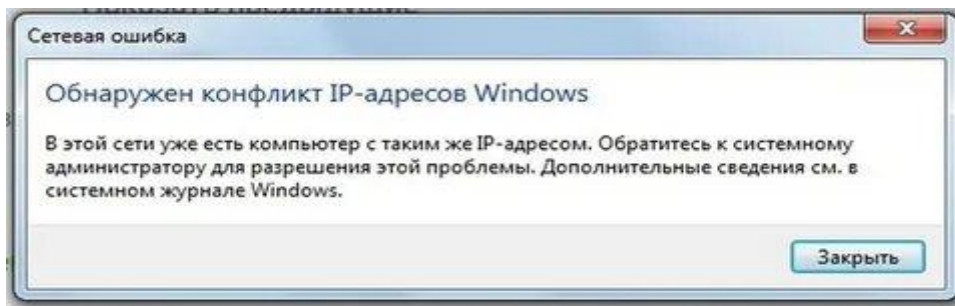
```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 10.255.255.1: Destination host unreachable.
Reply from 10.255.255.1: Destination host unreachable.
Reply from 10.255.255.1: Destination host unreachable.
Reply from 10.255.255.1: Destination host unreachable.

C:\>
```

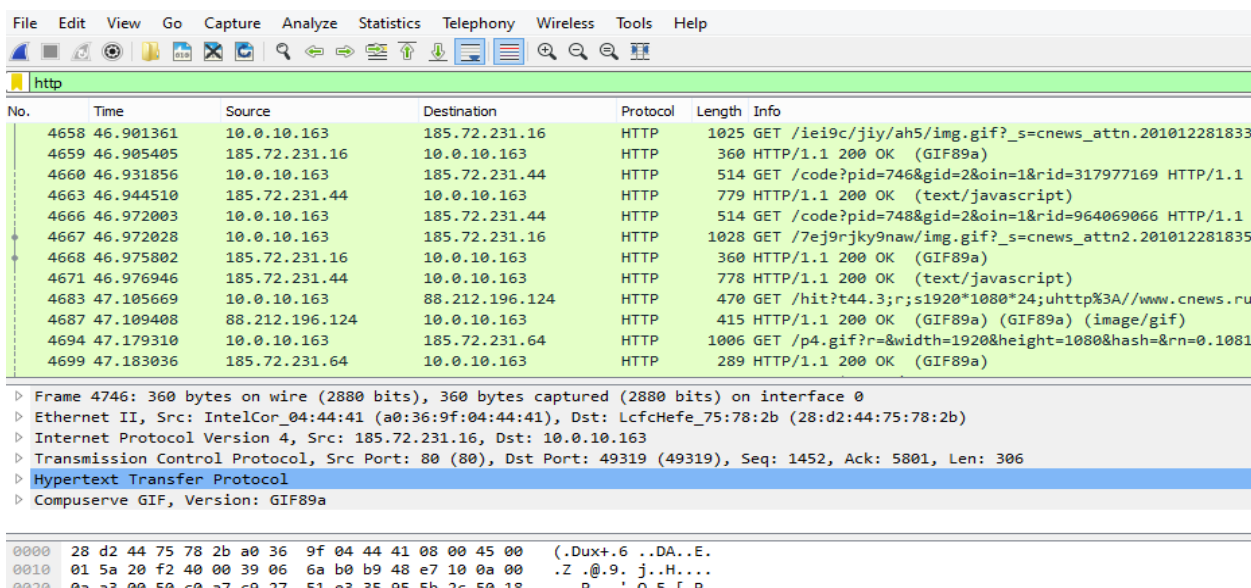
Сценарий 4: конфликт IP-адресов.

Симптом: сообщение «IP-адрес уже используется». Диагностика: `arp -a | findstr <IP>`, `nbtstat -A <IP>`. Устранение: назначить статический IP вручную, обновить DHCP-аренду через `ipconfig /release` и `ipconfig /renew`, либо найти устройство по MAC-адресу и отключить его. В корпоративной сети рекомендуется вести учёт статических адресов, чтобы избежать конфликтов.



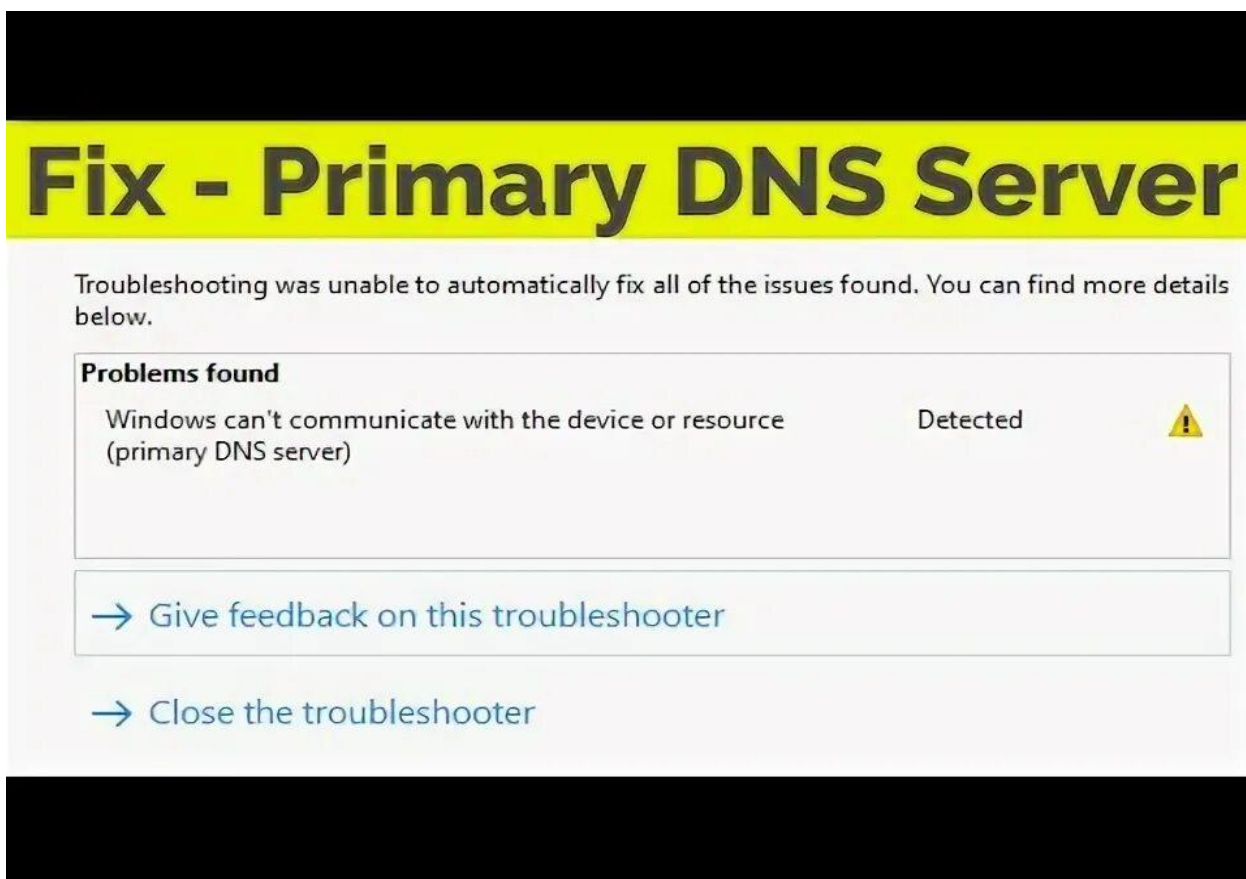
Сценарий 5: шторм широковещательных пакетов.

Симптомы: сеть «висит», лампочки на коммутаторе мигают с высокой частотой. Диагностика: Wireshark показывает множество широковещательных пакетов (MAC FF:FF:FF:FF:FF:FF). Устранение: быстро найти устройство, создающее шторм, и физически отключить его. После аварии настроить storm-control на коммутаторе для ограничения интенсивности широковещательного трафика, включить защиту от петель (Loop Guard, BPDU Guard).



Сценарий 6: не работает DNS.

Симптом: ping по IP работает, по имени — нет. Диагностика: nslookup [google.com](https://www.google.com), ping 8.8.8.8. Устранение: прописать публичные DNS-серверы вручную (8.8.8.8, 1.1.1.1), перезапустить службу DNS-клиента (services.msc), проверить файл hosts (C:\Windows\System32\drivers\etc\hosts) на наличие некорректных записей.



Сценарий 7: проблема с автосогласованием скорости и дуплекса.

Симптомы: файлы копируются очень медленно, но ping показывает малую задержку. Диагностика: на Windows — netsh interface ip show interfaces, на коммутаторе Cisco — show interfaces status. Если на одном конце полный дуплекс, а на другом — полудуплекс, возникают коллизии. Устранение: принудительная установка одинаковых параметров на обоих концах, но лучше найти причину сбоя автосогласования (обычно некачественный кабель). Рекомендация: оставлять автосогласование включённым на всех современных устройствах.

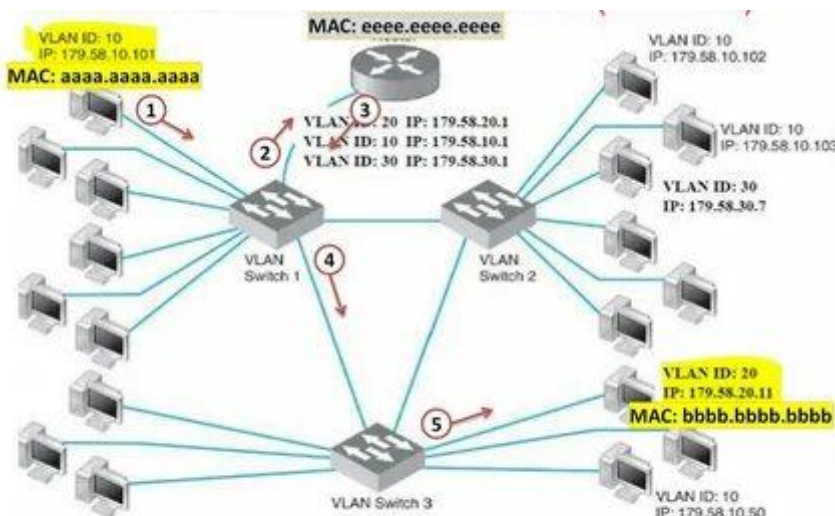
```

[phoenixmap@localhost ~]# ethtool enp0s3
Settings for enp0s3:
    Supported ports: [ TP ]
    Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Supported pause frame use: No
    Supports auto-negotiation: Yes
    Supported FEC modes: Not reported
    Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Advertised pause frame use: No
    Advertised auto-negotiation: Yes
    Advertised FEC modes: Not reported
    Speed: 1000Mb/s
    Duplex: Full
    Port: Twisted Pair
    PHYAD: 0
    Transceiver: internal
    Auto-negotiation: on
    MDI-X: off (auto)
Cannot get wake-on-lan settings: Operation not permitted
    Current message level: 0x00000007 (7)
                          drv probe link
    Link detected: yes

```

Сценарий 8: проблема с VLAN — устройство не видит сеть.

Симптомы: компьютер получает IP по DHCP, но не пингует соседние подсети, хотя в своей VLAN всё работает. Диагностика: `show vlan brief` (какая VLAN у порта), `show interfaces trunk` (какие VLAN передаются по транку), `show ip interface brief | include Vlan` (есть ли SVI). Устранение: переместить порт в правильную VLAN (`switchport access vlan X`), разрешить нужную VLAN на транке (`switchport trunk allowed vlan add X`), при отсутствии SVI создать интерфейс VLAN с IP-адресом.



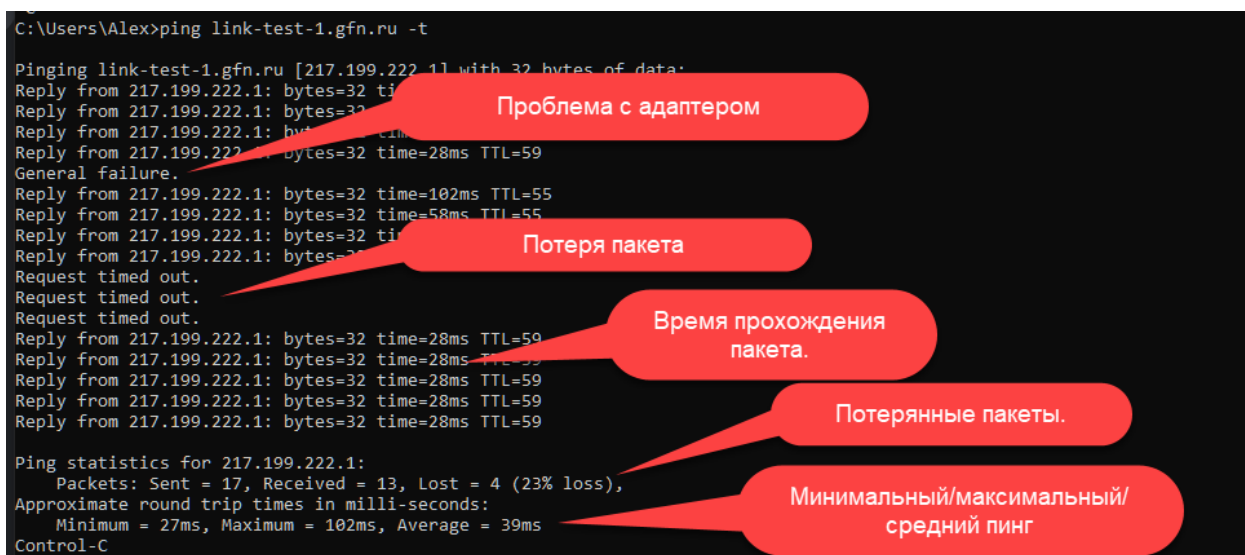
Сценарий 9: проблема с NAT — нет доступа в интернет.

Симптомы: локальная сеть работает, устройства пингуют друг друга и шлюз, но не пингуют внешние адреса (8.8.8.8). При этом с маршрутизатора пинг проходит. Диагностика: show ip nat translations (пустая таблица — NAT не срабатывает), show access-list (внутренний адрес не попадает в список), show ip route 0.0.0.0 (нет маршрута по умолчанию). Устранение: исправить правила NAT, добавить недостающие адреса в список доступа, добавить маршрут по умолчанию. Если всё настроено правильно — проблема на стороне провайдера.

```
C:\Users\Alex>ping link-test-1.gfn.ru -t

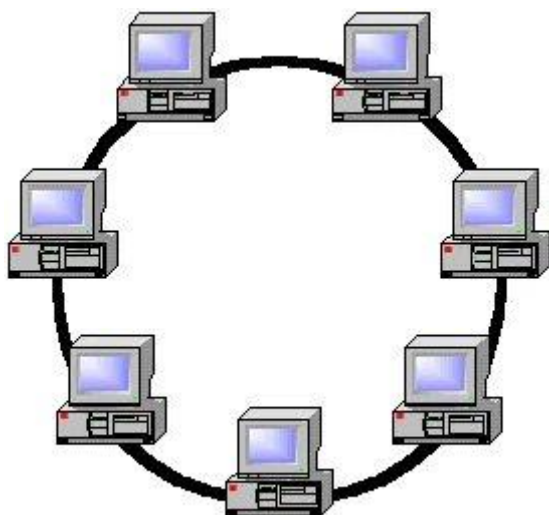
Pinging link-test-1.gfn.ru [217.199.222.1] with 32 bytes of data:
Reply from 217.199.222.1: bytes=32 time=102ms TTL=55
Reply from 217.199.222.1: bytes=32 time=58ms TTL=55
Reply from 217.199.222.1: bytes=32 time=28ms TTL=59
Reply from 217.199.222.1: bytes=32 time=28ms TTL=59
General failure.
Reply from 217.199.222.1: bytes=32 time=102ms TTL=55
Reply from 217.199.222.1: bytes=32 time=58ms TTL=55
Reply from 217.199.222.1: bytes=32 time=28ms TTL=59
Reply from 217.199.222.1: bytes=32 time=28ms TTL=59
Request timed out.
Request timed out.
Request timed out.
Reply from 217.199.222.1: bytes=32 time=28ms TTL=59
Reply from 217.199.222.1: bytes=32 time=28ms TTL=59
Reply from 217.199.222.1: bytes=32 time=28ms TTL=59
Reply from 217.199.222.1: bytes=32 time=28ms TTL=59
Reply from 217.199.222.1: bytes=32 time=28ms TTL=59

Ping statistics for 217.199.222.1:
    Packets: Sent = 17, Received = 13, Lost = 4 (23% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 27ms, Maximum = 102ms, Average = 39ms
Control-C
```



Сценарий 10: неисправность в кольцевой топологии с STP.

Симптомы: сеть нестабильна, периодически пропадает связь с некоторыми коммутаторами. Диагностика: show spanning-tree root (корневой мост не выбран или меняется), состояния портов (blocking/forwarding). Устранение: вручную назначить корневой мост (spanning-tree vlan X root primary), проверить отсутствие физических петель, привести версии STP к единому стандарту на всём оборудовании, включить Loop Guard и BPDU Guard.



Демонстрация навыков в программе Cisco Packet Tracer.

Команды проверки будут представлены в программе Cisco Packet Tracer



Команды которые будут продемонстрированы:

Проверка физического подключения:

Switch# show interfaces status

Switch# show interfaces gig0/1

Switch# show ip interface brief

Проверка VLAN и портов:

Switch# show vlan brief

Switch# show interfaces switchport

Switch# show interfaces trunk

Проверка маршрутизации:

Router# show ip route

Router# show ip interface brief

Router# ping 8.8.8.8

Router# traceroute 8.8.8.8

Проверка NAT и доступа в интернет:

Router# show ip nat translations

Router# show access-lists

Router# show ip route 0.0.0.0

Проверка STP петель:

Switch# show spanning-tree brief

Switch# show spanning-tree root

Switch# show interfaces status

Проверка DHCP:

Router# show ip dhcp pool

Router# show ip dhcp binding

PC> ipconfig /all

PC> ipconfig /release

PC> ipconfig /renew

Вот команды диагностики для ПК в текстовом формате:

Команды для ПК:

- ipconfig — показать текущую IP-конфигурацию сетевого адаптера;
- ipconfig /all — отобразить подробную информацию о всех сетевых адаптерах (MAC-адрес, IP-адрес, маска, шлюз, DNS-серверы);
- ipconfig /release — освободить текущий IP-адрес, полученный от DHCP-сервера;
- ipconfig /renew — запросить и получить новый IP-адрес от DHCP-сервера.

Команды проверки связи и маршрутизации:

- ping <IP-адрес> — проверить доступность удалённого узла путём отправки ICMP-запросов;
- tracert <IP-адрес> — выполнить трассировку маршрута до указанного узла, отобразив все промежуточные маршрутизаторы (хопы).

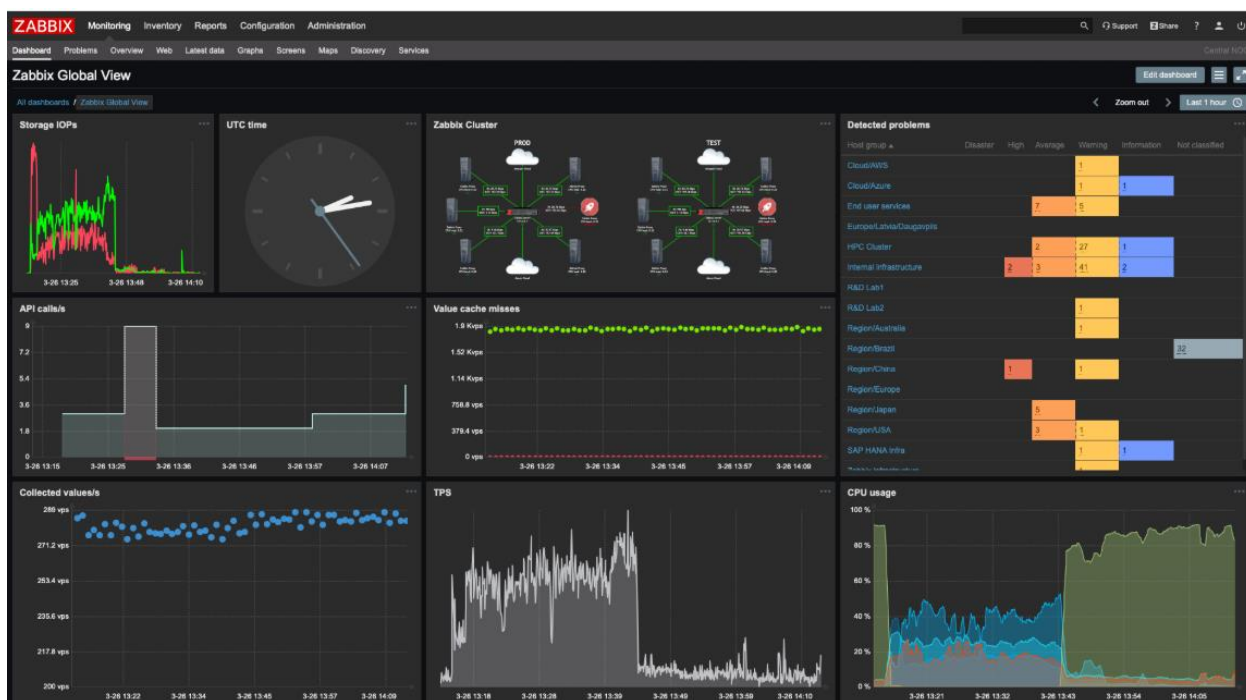
Команды работы с таблицами и именами:

- `arp -a` — показать таблицу соответствия между IP-адресами и физическими MAC-адресами в локальной сети;
- `nslookup <домен>` — проверить работу DNS-сервера и получить IP-адрес, соответствующий указанному доменному имени.

2.5 Профилактика и мониторинг

Профилактика неисправностей значительно важнее их устранения. Эффективная система профилактики включает несколько компонентов.

SNMP-мониторинг с использованием таких систем, как Zabbix, PRTG или LibreNMS, позволяет отслеживать состояние сетевого оборудования в реальном времени. Для настройки мониторинга коммутатора необходимо включить на нём SNMP и указать community-строку. В Zabbix создаётся хост с IP-адресом коммутатора, выбирается соответствующий шаблон. Система автоматически опрашивает параметры: загрузку процессора, использование памяти, температуру, состояние вентиляторов, ошибки на портах, скорость входящего и исходящего трафика. Триггеры настроены на отправку уведомлений при превышении порогов (например, загрузка порта выше 80 процентов в течение 10 минут). Zabbix также поддерживает обнаружение сети, что позволяет автоматически добавлять новое оборудование в мониторинг.



Сбор и анализ логов с помощью ELK-стека (Elasticsearch, Logstash, Kibana) является стандартом для централизованного сбора логов. Сетевые устройства отправляют логи по протоколу Syslog на сервер с Logstash, который парсит их, извлекает поля (дату, уровень важности, сообщение, IP-адрес отправителя) и сохраняет в Elasticsearch. В Kibana создаются дашборды, например «Все ошибки за последний час» или «Топ-10 устройств по количеству критических сообщений». При поиске неисправности можно быстро найти все логи с определённого коммутатора за последние сутки.

Резервное копирование конфигураций всего активного сетевого оборудования должно выполняться регулярно и автоматически. В случае сбоя можно быстро восстановить работоспособность. Для этого используются системы RANCID, Oxidized или просто скрипты на основе SSH и FTP.



Плановые проверки кабельной системы рекомендуется проводить не реже одного раза в шесть месяцев, особенно в местах с высокой вибрацией или перепадами температуры. Обновление прошивок коммутаторов, маршрутизаторов и точек доступа должно выполняться после тестирования в лабораторной среде и только при наличии реальной необходимости (например, для закрытия критических уязвимостей).

Разработка регламента планового обслуживания делает профилактику системной. Типовой регламент включает: еженедельные задачи (проверка систем мониторинга, просмотр отчётов по загрузке), ежемесячные (проверка резервных копий, анализ самых активных портов), ежеквартальные (физический осмотр кабельных шкафов, чистка оборудования, проверка ИБП) и ежегодные (обновление прошивок, полная инвентаризация).

Обучение и сертификация персонала также являются частью профилактики. Рекомендуется, чтобы хотя бы один сотрудник в отделе имел сертификацию Cisco CCNA. Для углублённой диагностики с Wireshark полезна сертификация WCNA. Регулярные внутренние тренировки по поиску неисправностей на эмуляторах значительно повышают навыки команды.

2.6 Пример диагностики реальной сети (кейс)

Для иллюстрации всех описанных методов приведём пример диагностики реальной неисправности в офисной сети компании из 50 человек.

Симптомы: каждый день примерно в 15:00 начинались периодические потери связи, задержка увеличивалась с 2 мс до 300 мс, скорость скачивания падала с 100 Мбит/с до 5 Мбит/с. Через 30–40 минут всё возвращалось в норму.

Первичная диагностика: ping до шлюза показывал потери около 10 процентов и высокую латентность только в указанное время. Трассировка до внешних ресурсов показывала, что потери начинаются уже на первом прыжке (шлюзе), значит проблема внутри локальной сети.

Мониторинг загрузки канала в Zabbix показал, что в 15:00 резко возрастает исходящий трафик с одного из коммутаторов. Анализ трафика через NetFlow на маршрутизаторе показал, что основной объём трафика генерирует IP-адрес 192.168.1.45 по протоколу UDP на порт 12345.

Wireshark, запущенный на зеркальном порту коммутатора, показал, что это торрент-клиент, который активно раздаёт данные во внешнюю сеть. Выяснилось, что сотрудник, сидящий за компьютером с этим IP, устанавливает торрент-клиент и забывает его выключить. К 15:00 (после обеда) загрузка пиратского контента заканчивалась, и клиент начинал активную раздачу, забивая исходящий канал.

Устранение: блокировка портов торрентов на межсетевом экране, настройка QoS для приоритизации рабочего трафика, проведение беседы с сотрудником и внесение в политику использования сети запрета на торренты.

Профилактика: настройка оповещения в Zabbix при превышении исходящего трафика более 10 Мбит/с на любого пользователя.

Этот кейс показывает важность комплексного подхода: от базового ping до анализа трафика и организационных мер. Без системы мониторинга и анализа трафика проблема могла бы оставаться нерешённой долгое время.

Заключение

В результате выполнения данной курсовой работы были систематизированы знания о типовых неисправностях в современных вычислительных сетях и методах их диагностики и устранения. Работа была разделена на теоретическую часть, в которой подробно описаны проблемы каждого уровня модели OSI, и практическую часть, в которой представлены способы их обнаружения и исправления.

Проведённый анализ позволяет сделать следующие выводы. Большинство сетевых неисправностей, по статистике, связано с физическим уровнем. До шестидесяти процентов проблем возникают из-за повреждённых кабелей, некачественных разъемов, неправильной распиновки и неисправных портов. Это означает, что первым шагом при любой сетевой проблеме должна быть тщательная проверка физических подключений.

Эффективная диагностика невозможна без знания модели OSI и базовых сетевых утилит. Понимание того, на каком уровне модели следует искать проблему, позволяет существенно сократить время поиска. Утилиты ping, traceroute, ipconfig, nslookup и arp являются минимально необходимым набором инструментов любого сетевого администратора.

Для глубокого анализа трафика незаменимыми инструментами являются Wireshark и iperf3. Первый позволяет увидеть содержимое пакетов и выявить аномалии на любом уровне, второй — объективно измерить пропускную способность канала. Их использование должно стать стандартной практикой при диагностике сложных неисправностей.

Профилактика и мониторинг снижают число аварий на семьдесят-восемьдесят процентов. Регулярное резервное копирование конфигураций, плановые проверки кабелей, обновление прошивок и централизованный сбор логов превращают реагирование на инциденты из аврала в плановую работу.

Результатами данной курсовой работы являются составленная классификация сетевых неисправностей, подробное описание проблем каждого уровня, а также десять практических сценариев с конкретными командами диагностики и способами устранения. Полученные результаты могут быть использованы как учебное пособие для начинающих сетевых администраторов и как справочный материал для специалистов при устранении типовых неисправностей.

СПИСОК ЛИТЕРАТУРЫ

1. Chappell L. Wireshark Network Analysis. 2nd edition, 2012.
2. Cisco. Troubleshooting and Maintenance of IP Networks. Cisco Press.
3. Microsoft Docs. Сетевые утилиты Windows. Документация Microsoft.
4. Документация по системам Zabbix, PRTG и Wireshark. Официальные сайты проектов.
5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 5-е издание. Санкт-Петербург: Питер, 2016.
6. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е издание. Санкт-Петербург: Питер, 2012.