Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Wireshark и tcpdump: диагностика офисной сети в 2026

Как мы находим причину «тормозит 1С» и «хрипит телефония» за 15–30 минут анализа пакетов

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Жалобы «1С тормозит», «RDP лагает», «голос дрожит» не диагностируются пингом: ретрансмиссии TCP, zero window, медленный DNS и джиттер RTP не видны на уровне ICMP и счётчиков коммутатора. Мы разворачиваем стек анализа пакетов (tcpdump 4.99 + Wireshark 4.6 + tshark) и находим первопричину за 15–30 минут вместо недель перекладывания вины на провайдера.

Почему это важно бизнесу

- Неделя поиска «виноватого» между провайдером и админом — простой бухгалтерии и продаж; анализ дампа локализует узел за 15–30 минут.
- Без пакетной диагностики деньги уходят на слепые апгрейды серверов и каналов, когда причина — патч-корд или антивирус на клиенте.
- Хрипящая IP-телефония — потерянные звонки клиентов; пороги джиттера 30 мс и потерь 1% проверяются по дампу RTP объективно.
- Недельное хранилище трафика (Arkime) отвечает на «что упало вчера в 15:20» фактами — SLA-споры с провайдером закрываются дампом.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

4.6.6

версия Wireshark, которую ставим инженерам; ветка 4.6 — последняя с поддержкой Windows 10 и Qt 5

wireshark.org, релиз 4.6.6

262144 Б

snaplen tcpdump по умолчанию — payload виден целиком; на старых версиях ставим -s 0 явно

man tcpdump 4.99.6

< 30 мс

порог джиттера RTP для голоса; вместе с потерями ≤1% и односторонней задержкой ≤150 мс

Cisco QoS for VoIP

DSCP 46

метка EF для RTP-пакетов в mangle MikroTik — строгий приоритет голоса на всём пути

Cisco QoS / RFC 3246

37008/udp

порт TZSP: /tool sniffer на MikroTik стримит пакеты прямо в Wireshark без SPAN-порта

help.mikrotik.com

100 МБ ×5

кольцевой захват tcpdump -C 100 -W 5 — постоянная запись трафика не забивает диск сервера

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Захват на сервере: tcpdump и кольцевой буфер без GUI на проде

Что настраиваем

Сервер 1С / файловый / почтовый на Linux; ноутбук инженера с Wireshark 4.6

Как мы это делаем

1. Снимаем трафик клиента: tcpdump -i eth0 -w /tmp/c.pcap host <IP>; на старых версиях добавляем -s 0 (полный snaplen 262144 байт)
2. Постоянный захват — кольцо: -C 100 -W 5 (5 файлов по 100 МБ), свою сессию исключаем фильтром not port 22
3. Живой разбор — extcap sshdump: Wireshark сам поднимает SSH-сессию (--remote-priv sudo), поток pcap идёт в GUI в реальном времени
4. Разбор дампа: фильтр tcp.analysis.flags, затем Analyze → Expert Information; порог тревоги — ретрансмиссии свыше 0,1% TCP-пакетов

РЕЗУЛЬТАТ

Причина «1С открывается три минуты» локализуется до конкретного узла (кабель, дуплекс, антивирус) за один выезд; GUI не грузит прод — на сервере работает только tcpdump или dumpcap, анализ идёт на ноутбуке.

КЛЮЧЕВОЙ НЮАНС

У актуального tcpdump (4.99.x) snaplen по умолчанию 262144 байта, -s 0 нужен лишь на старых сборках; главное — не забыть not port 22, иначе захват ловит свою SSH-сессию и растёт лавинообразно.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Диагностика VoIP: джиттер RTP и QoS на MikroTik

Что настраиваем

АТС 3CX/Asterisk + IP-телефоны; MikroTik на границе, зеркало порта или TZSP-стрим

Как мы это делаем

1. Стримим трафик телефонов без SPAN: /tool sniffer set streaming-enabled=yes streaming-server=<ноут> filter-stream=yes; Wireshark слушает TZSP udp/37008
2. Тестовый звонок → Telephony → RTP → RTP Streams: колонки Max Jitter, Max Delta, Lost; пороги — джиттер <30 мс, потери ≤1%, задержка ≤150 мс
3. Прослушиваем голос прямо из дампа: Telephony → VoIP Calls → Play Streams — слышим ровно то, что слышит клиент
4. Лечим приоритизацией: mangle-маркировка RTP → DSCP 46 (EF) + queue tree с гарантированной полосой под голосовой трафик

РЕЗУЛЬТАТ

Джиттер возвращается в норму без замены провайдера и телефонов; спор «виновата гарнитура или канал» закрывается цифрами из RTP Streams за один тестовый звонок, а директору проигрываем звук из дампа.

КЛЮЧЕВОЙ НЮАНС

TZSP-поток на 37008 Wireshark может декодировать как WCCP — отключаем WCCP-диссектор в Analyze → Enabled Protocols, иначе стрим «не виден».

РЕАЛИЗАЦИЯ 3 ИЗ 3

Постоянный мониторинг: tshark-пробы и хранилище Arkime

Что настраиваем

Диагностическая VM: tshark, ntopng 6.6, Suricata 8.0, Arkime 6; SPAN с ключевых портов

Как мы это делаем

1. Ежеминутная проба: tshark -a duration:30 -w probe.pcap, затем подсчёт -Y "tcp.analysis.retransmission" и "tcp.analysis.zero_window" — пороги 100 и 20 за 30 с
2. Медленный DNS ловим фильтром dns.time > 1.0; превышение любого порога — алерт в Telegram инженеру до звонков пользователей
3. Сводки без GUI: tshark -z io,stat,60 -z expert -z rtp,streams — динамика ошибок по минутным интервалам прямо в консоли
4. Недельное хранилище пакетов: Arkime индексирует весь SPAN-трафик; вопрос «что упало вчера в 15:20» решается поиском по времени

РЕЗУЛЬТАТ

Инциденты видим до жалоб: рост ретрансмиссий или zero window приходит алертом; ретроспектива по любому событию недельной давности достаётся из Arkime фактами, а не со слов пользователей.

КЛЮЧЕВОЙ НЮАНС

Пробы пишем во tmpfs и удаляем сразу после подсчёта; на Windows-узлах захват ведёт dumpcap из комплекта Wireshark (драйвер Npcap 1.88), а не GUI.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Путать capture- и display-фильтры**
  В строке захвата — синтаксис BPF (tcp port 80), в строке анализа — синтаксис Wireshark (tcp.port == 80). Перепутал — захват пустой или фильтр не парсится.

- ✕ **GUI Wireshark на боевом сервере**
  GUI тянет память и CPU. На проде — только tcpdump/dumpcap в файл с ротацией -C/-W, анализ дампа — на ноутбуке инженера.

- ✕ **Захват без SPAN или TZSP**
  В коммутируемой сети видно только свой трафик и broadcast. Настраиваем port mirroring на свитче или /tool sniffer с TZSP-стримом на MikroTik.

- ✕ **Обрезанный payload в дампе**
  Старые tcpdump режут пакет — не разобрать HTTP, SIP и TLS handshake. Ставим -s 0 явно; у актуальных версий (4.99.x) snaplen по умолчанию 262144 байта.

- ✕ **Захват только с одной точки**
  Пакет «ушёл, но не пришёл» видно лишь при одновременном захвате на обоих концах; сверяем два дампа по tcp.seq и абсолютному времени.

- ✕ **Свой SSH-шум в дампе**
  Живой захват через ssh + tcpdump ловит сам себя и растёт лавинообразно; всегда добавляем not port 22 (или свой порт) в BPF-фильтр.

- ✕ **Диагноз по ping**
  ICMP не показывает ретрансмиссии, zero window и dns.time: при time<1ms сеть может терять 2–3% TCP-сегментов — смотрим tcp.analysis.flags.

- ✕ **Дампы с персональными данными**
  pcap содержит пароли и документы: храним на шифрованном диске неделю, провайдеру передаём выжимку по инциденту, а не полный дамп.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Wireshark 4.6 + Npcap на ноутбуке инженера, tcpdump на каждом сервере
- Шпаргалка фильтров: tcp.analysis.flags, dns.time > 0.2, tls.handshake
- SPAN-порт на управляемом коммутаторе для выездной диагностики

НОРМАЛЬНО

- sshdump и TZSP-стрим: живой захват с серверов и MikroTik без выезда
- Кольцевой захват на серверах: tcpdump -C 100 -W 5 not port 22
- QoS для VoIP: DSCP 46 (EF), контроль джиттера <30 мс по RTP Streams
- tshark-пробы с порогами ретрансмиссий и алертом в Telegram

ХОРОШО

- Диагностическая VM: tshark + ntopng 6.6 + Suricata 8.0 на SPAN-трафике
- Arkime: недельное индексируемое хранилище всего трафика объекта
- Захват с двух точек и baseline-дампы «здоровой» сети в архиве
- Регламент: шифрование pcap, сроки хранения, доступ по ролям

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть ли на каждом сервере tcpdump и право снять дамп без остановки сервиса?
- [ ] Настроен ли SPAN/port mirroring или TZSP-стрим для захвата чужого трафика?
- [ ] Отличают ли инженеры BPF-фильтры захвата от display-фильтров Wireshark?
- [ ] Исключён ли собственный SSH (not port 22) из живых захватов?
- [ ] Известны ли пороги: ретрансмиссии <0,1%, джиттер <30 мс, потери RTP ≤1%?
- [ ] Промаркирован ли голосовой трафик DSCP 46 и выделена ли ему гарантированная полоса?
- [ ] Ограничен ли размер захвата ротацией -C/-W, чтобы дамп не забил диск?
- [ ] Есть ли автоматический мониторинг ретрансмиссий с алертом до жалоб пользователей?
- [ ] Хранятся ли pcap-дампы шифрованно и удаляются ли по регламенту?
- [ ] Сможете ли показать трафик за «вчера 15:20» из хранилища, а не по памяти?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Выездная диагностика «загадочных» проблем: захват, анализ, письменный отчёт с первопричиной за 2–3 часа
- Разворачиваем диагностическую VM под ключ: tshark-пробы, ntopng, Suricata, Arkime с недельным хранением трафика
- Настраиваем QoS для IP-телефонии на MikroTik: маркировка EF, очереди, контроль джиттера по дампам
- Обучаем штатного админа: шпаргалки фильтров, регламент захвата, разбор реальных дампов вашей сети

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Wireshark User's Guide + Release Notes 4.6 (wireshark.org — 4.6.6)

02 man tcpdump / libpcap (snaplen, -C/-W, BPF) (tcpdump.org — 4.99.6)

03 man sshdump / tshark (extcap, -z io,stat / rtp,streams) (wireshark.org — 4.6)

04 Packet Sniffer — TZSP streaming (help.mikrotik.com — ROS 7)

05 Quality of Service for Voice over IP + RFC 3246 (EF PHB) (cisco.com — 2002)

06 Arkime Docs — full packet capture (arkime.com — 6.4)

07 Suricata User Guide (suricata.io — 8.0.5)

08 ntopng Documentation (ntop.org — 6.6)

Основано на официальной документации продуктов и нашей практике внедрения.