

# Руководство по устранению сбоев в компьютерных сетях



## Содержание

<b>Аннотация</b> .....	<b>2</b>
<b>Введение в методы диагностики и устранения сбоев</b> .....	<b>3</b>
Метод на все случаи жизни .....	3
Подход к работе .....	4
Устранение сбоев за 8 шагов .....	8
<b>Устранение сбоев на физическом уровне</b> .....	<b>16</b>
Поиск и устранение сбоев в медной среде .....	16
Тестирование медной среды .....	21
Поиск и устранение сбоев в волоконной оптике .....	36
Тестирование волоконно-оптической среды .....	41
<b>Устранение сбоев на сетевом уровне</b> .....	<b>47</b>
Типичные сбои в сети и жалобы пользователей .....	47
Жалоба: не могу войти в сеть .....	48
Жалоба: сеть постоянно “отваливается” .....	53
Жалоба: сеть “тормозит” .....	57
<b>Устранение проблем с сетевыми коммутаторами</b> .....	<b>62</b>
Типичные сбои сетевых коммутаторов .....	62
Точное распознавание проблемы .....	64
Методы устранения коммутаторных сбоев .....	65
Метод 1: Получить консольный доступ к коммутатору .....	67
Метод 2: Подключиться к свободному порту .....	70
Метод 3: Настроить зеркальный или span-порт .....	77
Метод 4: Подключиться к тегированному или транковому порту ..	84
Метод 5: Последовательно подключить к сегменту хаб .....	86
Метод 6: Последовательно подключить к сегменту тестер .....	90
Метод 7: Воспользоваться отводом, подключенным к сегменту ..	91
Метод 8: Использовать управление на основе SNMP-протокола ..	98
Метод 9: Применить потоковые технологии .....	106
Метод 10: Настроить syslog-сервер для регистрации событий ...	109
Метод 11: Использовать серверные ресурсы (ресурсы хоста) ...	110
Метод 12: Использовать сочетание методов .....	112
<b>Заключение</b> .....	<b>113</b>

## Аннотация

На сегодняшний день деятельность огромного количества компаний основана на работе компьютерных сетей. Роль системных администраторов и сетевых специалистов стала ключевой, без них обеспечить работоспособность сетей просто невозможно. Наше руководство адресовано именно таким специалистам, в нем содержатся практические советы и рекомендации по поддержке компьютерных сетей и устранению наиболее распространенных сетевых сбоев.

Локальные сети (LAN) строятся на множестве разнообразных устройств и других составляющих: принтеры, терминальные устройства, персональные компьютеры, IP-телефоны, сервера, устройства хранения информации, сетевое оборудование, программное обеспечение безопасности, сетевые приложения, программные приложения предприятия, офисные пакеты и многое другое. В данном руководстве мы сосредоточимся на уровнях 1 и 2 сетевой модели OSI: физическом уровне (среде передачи) и коммутаторах. Кабельная система и коммутаторы – это основа современных локальных сетей.

Наше руководство начинается с введения в методы устранения сбоев в локальных сетях. Мы подробно рассмотрим последовательность действий при поиске неисправностей и перечислим 8 шагов, необходимых для успешного устранения сбоя. Затем мы изучим типичные проблемы на физическом уровне, особенности медной и волоконно-оптической среды передачи, а также приведем примеры самых частых обращений пользователей, включая жалобы на медленную работу сети и проблемы с подключением. Завершающая часть руководства содержит подробную информацию по диагностике сетевых коммутаторов, включая описания различных методов поиска и устранения сбоев. Освоив эти методы, сетевые специалисты и системные администраторы смогут устранять сбои в сетях гораздо быстрее, чем раньше.

## Введение в методы диагностики и устранения сбоев

### Метод на все случаи жизни

Предупреждаем сразу: “лучшего” метода, пригодного во всех случаях жизни,

просто не существует, как не существует и универсального лекарства от всех сетевых проблем. Мы лишь можем предложить несколько различных подходов к диагностике и устранению сетевых сбоев. Лучше всего эту ситуацию помогут проиллюстрировать два известных афоризма.

Первый из них – крылатая фраза: “Если твое единственное орудие – молоток, тебе везде мерещатся гвозди”. Применительно к компьютерным сетям это высказывание можно трактовать по-разному. Например, если человек умеет только отключать и подключать обратно сетевые устройства, но достаточно терпелив, чтобы перебирать их все до тех пор, пока не найдет неисправное, то такой “специалист” может прийти к выводу, что полный перебор – это и есть диагностика. Или другой пример: если человек хорошо разбирается в каком-то одном диагностическом средстве, имеющем довольно узкий спектр применения, он может попробовать использовать его и в ситуации, для которой оно изначально не предназначалось. Не потому, что это средство может распознавать те или иные виды сбоев, а потому, что специалист будет в состоянии правильно интерпретировать полученные результаты, используя свои знания и опыт работы именно с этим средством. В итоге это позволит ему сделать заключение, которое может оказаться очень близко к истине.

Вторая история – знаменитая притча про то, как слепые старцы описывали внешний вид слона. Все они переругались между собой, потому что каждый имел в своем распоряжении только часть информации и не мог представить картину в целом. Кто ощупывал хобот, говорил, что слон похож на толстую змею; кто трогал ногу, делал вывод, что слон похож на ствол дерева. Все это противоречило ощущениям того, кто щупал хвост, и того, кто прикасался к слоновьему боку. При этом каждый страстно отстаивал правильность своих утверждений, потому что данные были получены на личном опыте, что называется, из первых рук. Единственное, в чем удалось достичь согласия – в том, что кожа у слона морщинистая...

Если специалист, ответственный за диагностику, недостаточно разбирается в конкретной сетевой технологии, если у него нет точной информации с разных направлений и из разных источников, если ему не хватает опыта и широты кругозора, то выводы и предположения он сделает неправильные.

Точность и быстрота диагностики зависят от знаний, опыта и навыков каждого специалиста в отделе ИТ и от инструментов, имеющихся в их распоряжении.

Иногда для постановки

правильного диагноза приходится привлекать специалистов со стороны, которые в состоянии сформировать объективное мнение.

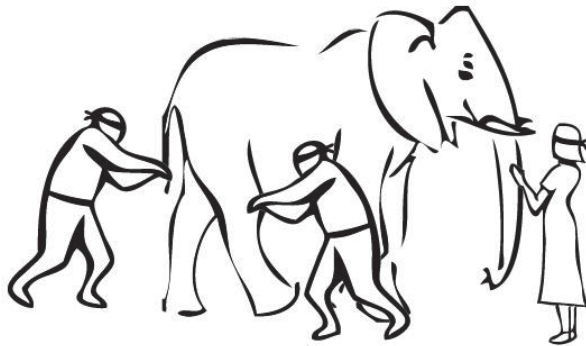


Рисунок 1: Личный опыт иногда мешает воспринять картину в целом или взглянуть на ситуацию с другой точки зрения.

## Подход к работе

Успешно обнаруживать и устранять неисправности в сети может только тот, кому досконально известно, как должна работать сеть в нормальном режиме. Только такой специалист сможет быстро распознать отклонение от нормы и диагностировать неисправность.

К сожалению, многие сетевые решения поступают потребителям с недостаточной информацией об их штатных характеристиках, без описания основных принципов работы и даже без кратких технических данных, которые помогли бы в диагностике неисправностей. Хороший технический специалист сначала подробно изучит всю доступную ему информацию, постарается досконально разобраться в работе всех компонентов и научится правильно применять их. Опытные сетевые инженеры знают, что часто за серьезный сбой в сети можно принять результат неправильного применения приложения или последствия так называемого “человеческого фактора”.

Такой подход обычно стараются привить сетевым инженерам на курсах обучения. Но этого мало. Настоящий специалист, мастер своего дела, продолжает непрерывно учиться методом проб и ошибок, обсуждает разные случаи с коллегами по профессии и в итоге на основе наработанного опыта создает собственные методы, которым на курсах не учат. Ускорить наработку такого опыта в диагностике сбоев вам помогут несколько приемов:

внимательно документируйте предпринятые вами действия; записывайте предположения о том, каковы могут быть причины сбоя в каждом конкретном случае, и результаты принятых мер. Так вы не только ускорите обучение, но и сократите время, необходимое для устранения проблем в сети в будущем.

Есть два крепко укоренившихся подхода к диагностике компьютерных сетей, и оба практически всегда ведут в тупик, вызывая либо окончательное падение сети, либо большие задержки в восстановлении ее работоспособности. Они прямо противоположны друг другу. Первый – метод чистого теоретика, кабинетного ученого. Второй – подход чистого практика, его же называют рабоче-крестьянским методом. Оба они представляют собой крайности, а правильный подход, как известно, лежит в золотой середине.

Кабинетный ученый будет раз за разом анализировать ситуацию, пока однозначно не установит причину проблемы и хирургически точный метод ее устранения. Часто для такого анализа нужен многофункциональный (и потому очень дорогой) анализатор протоколов и колоссальная подборка данных по сетевому трафику – мегабайты информации. А ведь пока идет столь подробный анализ, проблема сама собой не устранилась. Такой подход дает вполне достоверные результаты, но мало какая компания согласится, чтобы ее сеть простаивала те часы – и даже дни – пока идет глубокий анализ.

Первое, что сделает чистый практик – начнет перetyкать шнуры, кабели, менять порты и сетевые карты, поочередно перебирать все программные и аппаратные факторы, пока сеть снова не поднимется. Это не значит, что она заработает правильно и эффективно, это значит лишь, что она начнет хоть как-то работать. К сожалению, в некоторых учебных руководствах главы о поиске и устранении неисправностей приводят только такой рабоче-крестьянский метод – видимо, потому, что не в состоянии описать более глубокие технические подходы. Хотя практика последовательного перебора способна вызвать быструю смену симптомов, тем не менее, в целом метод не очень надежен, и настоящая причина проблемы так и может остаться в сети не найденной и не устраненной. Может даже оказаться, что в прошлые разы вы меняли местами те же самые элементы, устраняя предыдущие сбои.

Если вы хотите найти наилучший путь для обнаружения и устранения проблем в сети, испытайте метод, описанный далее. Однажды попробовав, в дальнейшем вы сможете применять его с незначительными доработками практически к любой конкретной ситуации. Собственно, такой же подход можно применять и для диагностики программного обеспечения, и для проверки бытовой техники, и для ремонта газонокосилок.

Сеть необходимо анализировать не столько как набор отдельных элементов, сколько как единую систему. Один опытный инженер, етодично исследующий

сеть, добьется лучшего результата, чем целая команда техников, располагающих только отдельными инструментами и теориями диагностики. Опытный инженер задаст пользователям правильные вопросы, применит диагностические инструменты, тщательно соберет информацию. Такому специалисту даже за короткое время удастся проанализировать и оценить симптомы, докопаться до корня проблемы, изменить одну настройку или заменить какой-то элемент, и проблема будет устранена. Суть подхода в том, чтобы локализовать наименьший элемент, в котором и заключается причина сбоя, и заменить или перенастроить именно его. На этом этапе даже не так важно установить глубинную причину сбоя. Гораздо важнее быстро восстановить работоспособность сети. Вот после того, как сеть снова заработала, можно заняться анализом собранной информации. Изучать ее лучше неторопливо, в лабораторных условиях.

Многие специалисты, причем имеющие многолетний опыт работы, за все это время так и не усвоили одну простую истину: несколько минут, затраченных на оценку симптомов, могут сэкономить целые часы, теряемые понапрасну на лечение не той проблемы, что нужно. Всю собранную информацию и отмеченные симптомы необходимо оценивать в целом, в привязке друг к другу – именно так, как они взаимно влияют друг на друга и отражаются на общей работоспособности сети. Только так сетевой специалист в состоянии правильно оценить ситуацию. Сначала вы собираете симптоматику, а затем проводите определенные тесты, чтобы подтвердить или опровергнуть ваши предположения о причине проблемы. Если симптомы установлены верно, то их оценку зачастую можно провести мысленно, не прибегая к сетевым тестам

и физическим изменениям вовсе. Если вы считаете, что идентифицировали проблему, то необходимо проверить, действительно ли это так. Ведь чтобы устранить проблему, сначала надо убедиться, что вы верно распознали ее.

И еще очень важно помнить: опытный специалист после того, как он предпринял меры к устранению проблемы, всегда проведет проверку связанного оборудования или системы, сколь бы просты ни были проведенные им действия. Слишком часто бывает, что какой-то простой и очевидный симптом – на самом деле следствие куда менее очевидной проблемы, и пока ее причина не будет устранена, сбой будет появляться снова и снова.

После устранения проблемы необходимо задокументировать ситуацию, симптомы сбоя и предпринятые действия. На основе этой информации другие специалисты смогут оперативно устранять сбои такого типа, не тратя времени на те исследования, что уже провели вы.

Последний этап – проинформировать пользователя и, возможно, проинструктировать его о том, что можно делать, а что нельзя. Если пользователь будет знать, какое действие приводит к возникновению сбоя, в чем причина проблемы и как можно ее устранить, то либо он в будущем постарается таких действий избегать, и тогда проблема не возникнет вовсе, либо, если все-таки она появится снова, сможет более четко описать ее.

## Устранение сбоев за 8 шагов

1. Собрать симптомы и определить суть проблемы.
2. Если возможно, воссоздать сбойную ситуацию.
3. Установить причину, вызывающую сбой.
4. Составить план действий по устранению проблемы.
5. Применить запланированные действия.
6. Провести проверку систем или оборудования, чтобы удостовериться, что проблема устранена.
7. Задокументировать проблему и ее решение.
8. Проинформировать пользователя.

## Шаг 2. Воссоздать сбойную ситуацию.

Очень важно правильно описать проблему и определить ее суть. Попросите человека, сообщившего вам о неисправности, подробно описать нормальный режим работы системы, а затем продемонстрировать, в чем заключается проблема. Если сбой то появляется, то исчезает, попросите пользователя немедленно сообщить вам, как только проблема появится снова. Крайне сложно устранять сбой, если в данный момент все замечательно работает.

Не отмахивайтесь от слов пользователя, даже если он описывает ситуацию, которая кажется вам абсолютно невозможной. У пользователя нет вашего опыта и ваших знаний, поэтому он заведомо не может описать проблему идеально точно и в правильных терминах. Что-то же вызвало недовольство пользователя, раз уж он обратился к вам.

### Примечание:

*Поинтересуйтесь, работало ли это раньше. Если то, на что жалуется пользователь, и раньше толком не работало, тогда подходите к вопросу как к внедрению новой функции, а не диагностике ранее реализованной возможности. Ведь в этом случае и предположения, и применяемые меры будут совсем другими.*

## Шаг 2. Воссоздать сбойную ситуацию.

Спросите себя, правильно ли вы оценили симптомы и действительно ли вы уяснили суть проблемы. Гораздо проще устранять те сбои, которые удается воссоздать. Тогда их можно увидеть воочию, посмотреть сообщения об ошибках, изучить симптомы, о которых пользователь не знает или не говорит вам потому, что не считает их важными. В идеале даже можно собрать сетевую статистику прямо во время сбоя.

Если же проблема то появляется, то исчезает, проинструктируйте пользователя, какого рода симптомы могут возникнуть, и дайте ему список вопросов, на которые вам нужны ответы, в письменном виде. Тогда пользователь сможет собрать хоть какую-то информацию, и это особенно полезно в том случае, если при следующем появлении сбоя вы не сможете быстро оказаться рядом,

чтобы пронаблюдать все лично. Если есть возможность, воспользуйтесь каким-либо диагностическим устройством для непрерывного сбора информации, чтобы наверняка охватить момент возникновения сбоя. Можно поставить анализатор протоколов на сбор всего трафика в сети и настроить его так, чтобы при заполнении буферной памяти он записывал новые данные поверх самых старых. И пользователь должен быть готов при следующем появлении сбоя немедленно прервать свою работу и/или сохранить текущие результаты тестов, какими бы средствами они ни проводились.

## Шаг 3. Установить причину, вызывающую сбой.

Определив проблему, а если нужно, и воссоздав ее, надо попробовать локализовать сбой – установить, к какому устройству он относится, к какому подключению, к какому программному приложению. Нужно последовательно сужать область поисков, отсекая лишнее. В итоге вы должны ограничить рамки сбоя наименьшим возможным элементом системы, в нем-то и будет заключаться причина. Пользуйтесь методом исключения, отсекайте все лишние переменные и факторы. Заодно на этом этапе стоит проверить систему на вирусы.

Отсутствует ли какая-либо функция, которая в нормальном режиме должна работать? Появляется ли какой-нибудь необычный отклик? В работе вам пригодятся данные, накопленные средствами мониторинга.

Определите, изменялось ли что-либо в сети или на рабочей станции непосредственно перед появлением сбоя. Часто пользователь не осознает, что какое-то из его действий, для него логически совершенно не связанных с появлением проблемы, на самом деле является причиной сетевого сбоя. Примерами таких невинных действий могут быть перемещение масляного обогревателя или ксерокса, установка нового программного приложения или сетевой карты. Не упускайте из виду локальные условия при поиске изменений! Учитывайте температурные изменения (часто причина сбоя – банальный перегрев); электрические устройства, расположенные поблизости, включая соседние комнаты и даже этажи; время суток, в которое появляется сбой; влияние источников электромагнитных наводок. Порой на работе сети

сказывается работа расположенного поблизости лифта или подъемника, и даже использование беспроводного телефона.

Можно ли воссоздать проблемы на другой рабочей станции либо используя другие программные приложения на той же самой рабочей станции? Уточните, сказывается ли проблема на работе только одной рабочей станции или затрагивает другие сетевые ресурсы – принтер, например. Переместитесь на один сегмент ближе к центральному сетевому ресурсу и проверьте, не исчезла ли проблема. Если по мере приближения к сетевому ресурсу проблема исчезает, значит, необходимо протестировать или заменить соответствующие элементы инфраструктуры, оставленные позади.

Если сбой затрагивает большой участок сети и ресурсы, используемые совместно, то необходимо последовательно отсекал лишние переменные, сводя количество факторов к минимально возможному значению. В топологии шины стоит попробовать подключиться по более короткому участку кабеля; иногда стоит временно проложить другие кабели, чтобы реализовать топологию кольца или звезды по альтернативному кабельному каналу и свести сеть к минимально возможным размерам, чтобы ее было проще диагностировать. Попробуйте подключить к сети другой сетевой коммутатор или хаб. Если ситуация не изменяется и проблема по-прежнему охватывает большой участок сети или совместно используемые ресурсы, то попробуйте выключить или отсоединить от сети все рабочие станции, кроме двух. Если они нормально взаимодействуют между собой, попробуйте добавить еще одну, затем еще. Если в какой-то момент связь прерывается, следует проверить физические элементы канала – концевые разъемы на кабеле, сам кабель, задействованные порты на активном оборудовании (в хабах и коммутаторах).

Если сбой затрагивает отдельную рабочую станцию, попробуйте поменять на ней сетевую карту, переустановите драйверы сетевой карты (при этом нельзя использовать то сетевое программное обеспечение или файлы настроек, что уже содержатся на этой рабочей станции, порой их лучше вообще удалить). Попробуйте подключиться к имеющемуся кабельному сегменту с помощью диагностического устройства. Если с сетевым подключением все в порядке, то

надо проверить, не вызывает ли сбой на рабочей станции какое-то одно приложение. Попробуйте запустить с того же диска и в той же файловой системе другое приложение. Сравните имеющиеся настройки с настройками рядом расположенной рабочей станции, которая функционирует нормально. Переустановите заново программное обеспечение приложения (опять же, необходимо использовать свежую копию, а не имеющееся на станции программное обеспечение и файлы настроек).

Если от сбоя пострадал только один пользователь, то проверьте сетевые настройки безопасности и права доступа именно этого пользователя. Уточните, не производились ли какие-то изменения в настройках безопасности, которые могли повлиять на работу этого пользователя. Не удалялась ли в сети другая учетная запись, настройки безопасности которой служили основой для настроек этого пользователя? Не удалялся ли этот пользователь из какой-нибудь группы в сети? Не переносилось ли используемое приложение в сети на другой ресурс или устройство? Вносились ли какие-то изменения в сценарий регистрации во всей системе или в последовательность регистрации данного пользователя?

Сравните настройки учетной записи пользователя с учетной записью кого-нибудь еще, кто может успешно выполнять действия, вызывающие проблему у данного пользователя. Пусть наш пользователь попробует войти в сеть с соседней рабочей станции, работающей нормально, и выполнить соответствующие действия с нее. Пусть другой пользователь попробует войти в сеть с проблемной рабочей станции и выполнить ту же задачу на ней.

#### **Шаг 4. Составить план действий по устранению проблемы.**

После того, как вы сузили зону поисков до одного приложения, одного действия или одного подключения, необходимо продумать или разработать способ устранения проблемы. При этом, однако, надо учитывать, что некоторые меры способны устранить эту проблему, но одновременно вызвать другие.

**Примечание 1:** Чтобы вам не пришлось несколько раз повторять одни и те же действия и чтобы у вас всегда была возможность “отката назад” к предыдущим настройкам, если вдруг ситуация станет еще хуже, всегда

внимательно и подробно записывайте все произведенные вами действия. Для всех файлов настроек сохраняйте копии и держите их в безопасном месте, и только после этого вносите изменения в конфигурацию. Особенно это касается настроек коммутаторов, маршрутизаторов, брандмауэров (firewall) и других ключевых сетевых устройств.

**Примечание 2:** Полезно открыть вторую терминальную сессию на коммутаторе или маршрутизаторе, чтобы с ее помощью набирать команды, необходимые для внесения изменений в настройки, и держать их наготове, а сами изменения производить из первого окна. Так у вас всегда будет перед глазами команда, вызвавшая те или иные (в том числе негативные) последствия.

## Шаг 5. Применить запланированные действия.

Возможно, вы пришли к выводу, что для устранения проблемы необходимо заменить сетевое устройство, сетевую карту, кабель или другой компонент физической инфраструктуры. Если причина сбоя заключается в программном обеспечении, возможно, потребуется применить средства программного исправления (patch-файлы), переустановить приложение или его компонент, а может, вылечить файлы, зараженные вирусом.

Если проблема заключается в учетной записи пользователя, то придется внести изменения в соответствующие сценарии регистрации и настройки безопасности. Если сбой затрагивает аппаратную часть, то чаще всего самый верный путь – заменить неисправный элемент оборудования на другой, чтобы попытаться отремонтировать вышедший из строя компонент позже, уже без спешки. Другой вариант – перенести подключение на свободный порт, а порт, подозреваемый в сбое, закрыть или отметить как неисправный. Помните, что первоочередная ваша задача – как можно быстрее восстановить работоспособность сети. Все остальное можно сделать потом.

Для устранения сбоев с программным обеспечением есть два пути. Первый – переустановить программное обеспечение, вызывающее проблему, удалить разрушенные и потенциально разрушенные файлы и проверить, что все необходимые файлы имеются в целостности и сохранности. Это отличная основа

для второго пути – перенастройки сбойного программного обеспечения. Если вы пошли первым путем, то последующая перенастройка вам удастся с первого раза. В программу установки для многих приложений встроена возможность отказа от использования существующих файлов настроек – надо лишь снять или поставить галочку в нужном месте. Именно так лучше всего поступать, и тогда одна и та же ошибка не будет появляться дважды. Если же такой возможности отказа нет или вы не знаете, как ею воспользоваться, то лучше деинсталлировать приложение полностью и установить его заново с нуля.

Если проблема затрагивает только учетную запись конкретного пользователя, то чаще всего простейший путь состоит в том, чтобы заново проделать все шаги по присвоению пользователю прав доступа к тому или иному приложению или функции – так, словно вы впервые заводите этого пользователя в системе. Если все эти шаги последовательно выполнить заново, то вы обнаружите пропущенную или неправильную настройку быстрее, чем при выборочной проверке существующих настроек. В некоторых случаях даже рекомендуется удалить учетную запись и завести ее заново.

## Шаг 6. Удостовериться, что проблема устранена.

После того, как вы применили запланированные меры, необходимо убедиться, что проблема полностью устранена: пусть пользователь проверит, может ли он теперь работать нормально. Заодно пусть проверит еще несколько типовых действий, которые он обычно выполняет в ходе работы. Довольно часто бывает, что решение одной проблемы вызывает появление других, а иногда устранение одного сбоя лишь выявляет другие проблемы, которые до того просто не были заметны на его фоне.

## Шаг 7. Задokumentировать проблему и ее решение.

Вести подробные записи полезно по нескольким причинам. Во-первых, такую документацию можно использовать в будущем, чтобы устранять такие же или похожие неисправности. Во-вторых, на основе накопленной информации можно готовить отчеты для руководства и/или пользователей по наиболее частым проблемам и сбоям в сети, а также проводить инструктаж новых пользователей или специалистов отдела ИТ.

## Шаг 8. Проинформировать пользователя.

Зачастую после устранения проблемы сетевой инженер поддается искушению на том и закончить. Однако пользователь, раз уж он обратился к вам за помощью, будет признателен, если вы все-таки объясните ему, что произошло. Если подобный сбой повторится, пользователи смогут быстрее распознать ситуацию и сразу сообщат вам о ней, и в результате работоспособность вашей сети будет выше. Кроме того, если вы объяснили пользователю, что можно делать, а чего нельзя, то снизится вероятность возникновения подобного сбоя в будущем. Умение взаимодействовать с пользователями и поддерживать с ними связь очень важно для отдела ИТ: это позволяет лучше поддерживать сеть, что выражается в уменьшении количества сбоев и времени простоя. Если вы не принимаете обращения пользователей всерьез или делаете едкие замечания насчет их умения пользоваться компьютером, то такое поведение не характеризует вас как профессионала. В результате ваши отношения с пользователями будут натянутыми, и такое противостояние только помешает вам хорошо делать свою работу.

Правильно говорят, что в 75 % случаев работать надо не с проблемой, а с пользователем. Если пользователь не почувствовал, что его заявка выполнена (и неважно, устранили ли вы проблему или привели пользователю тысячу причин – финансовых, технических, политических – по которым она не может быть устранена), это означает, что работу по заявке вы не закончили.

### С чего начать

Пройдя краткий курс обучения и прочитав всего один-два учебника по теме, профессиональных высот достичь нельзя. Это верно для любой сферы деятельности. Прежде чем переходить к следующей теме, досконально изучите один или два аспекта работы сети. Не стесняйтесь обращаться за помощью к коллегам и задавать вопросы. Такой подход убережет вас от массы грубых ошибок. Первый этап в диагностике – сбор информации. Если вы не знаете, как сеть должна работать в нормальном режиме, если вы не разбираетесь в используемой технологии, то как же вы соберете нужную информацию и узнаете симптомы сбоя?

Начав с одного раздела, постепенно расширяйте область изучения, но ваши знания всегда должны иметь практическую привязку. Со временем вы детально изучите семиуровневую модель OSI. Многие ИТ-специалисты, занимающие высокие должности, либо забыли, либо вообще никогда не знали основ работы многих элементов компьютерных сетей. В телекоммуникациях все меняется очень быстро, и такие специалисты предпочитают отслеживать только то, что относится к высоким уровням управления сетями, но при этом упускают из виду все, что относится к более низким уровням. Как следствие, часто они неверно трактуют симптомы сбоя и делают неправильные предположения, что в итоге замедляет устранение проблемы. Поскольку занимаемые ими должности достаточно высоки и предполагают принятие решений о развитии и изменении сетевой архитектуры, часто бывает, что они заказывают дорогостоящие обновления или оборудование, в которых на самом деле нет необходимости. Никто не может знать все на свете, поэтому не стесняйтесь обратиться за помощью, если вы в затруднении. Если что-то звучит сомнительно или наоборот, слишком хорошо, чтобы быть правдой, не поленитесь обратиться за информацией к нескольким источникам.

Руководства и учебные курсы тоже могут давать глубокие знания в одной области компьютерных сетей и не вполне корректные данные в другой. Некоторые области, возможно, вообще лучше было бы оставить для экспертов, которые глубоко разбираются в этой теме. Один из признаков того, что вы хорошо освоили тот или иной аспект сетевых технологий – четкое понимание того, в чем состоит сбой и где он может произойти.

## Устранение сбоев на физическом уровне

### Поиск и устранение сбоев в медной среде

#### Общие вопросы тестирования и монтажа

Большинство сетей давно перешли с коаксиальной среды сначала на неэкранированную витую пару (UTP) Категории 3, потом Категории 5 или 5е, а сейчас широко используются Категории 6 и 6А. Однако довольно много сетей продолжают работать на коаксиальном кабеле, в особенности участки глобальной и региональных сетей, а также сегменты подключения



беспроводного оборудования. Коаксиал может встретиться даже в старых локальных сетях, там, где приемлема низкая пропускная способность. Постепенно становится все более популярной волоконная оптика. На сегодняшний день она сопоставима по цене с суммарной стоимостью неэкранированной кабельной системы Категории 6А, если учитывать не только компоненты и монтажные работы, но и затраты на активное оборудование. В кабельных системах разных типов могут возникнуть разные проблемы. Далее мы рассмотрим вопросы монтажа, технического обслуживания, тестирования и диагностики для разных типов кабельных сред.

Как уже говорилось, несмотря на массовый переход со старых коаксиальных сетей Ethernet на неэкранированную витую пару, до сих пор на участках глобальной сети и для подключения беспроводного оборудования продолжает использоваться коаксиальный кабель. Его много, и он разный. Для “тонкого” Ethernet используется 50-омный кабель RG-58, в то время как в глобальной сети и для беспроводного оборудования, работающего по стандартам 802.11 (удлинительные антенные кабели) применяется 75-омный кабель RG-59. Тем не менее, оба типа кабеля иногда подвержены схожим проблемам. 93-омный кабель RG-62 в компьютерных сетях уже практически не встречается.

### Типы кабеля UTP, неэкранированной витой пары

Маркировка, принятая в старых и новых стандартах на витую пару, во многом очень похожа, хотя обозначает разные вещи. Так обстоят дела, например, с Категорией 5. Кабель, произведенный и маркированный в соответствии со старым стандартом, не соответствует новому стандарту, хотя использует ту же маркировку – просто сейчас под ней подразумеваются уже другие требования. Это верно как для американского стандарта TIA/EIA-568, так и для международного стандарта ISO/IEC 11801.

произведенные в период с 1995 по 1999 годы, создавались в соответствии с требованиями телекоммуникационного бюллетеня TSB67. В 1999 году был опубликован новый бюллетень, TSB95, и кабели стали производить в соответствии с его требованиями, более строгими, чем раньше. Производственные технологии обновились, но маркировка во многих случаях

не изменилась вовсе или изменилась так мало, что этого никто не замечает. Иногда на оболочке кабеля указывается дата выпуска, например, “Category 5 (1999)” или “Category 5 (2000)”. Также может использоваться маркировка “Class D (1999)” или “Class D (2000)”. Зато серьезные изменения произошли в маркетинговых программах производителей. Основные усилия маркетологи направили на то, чтобы выделить свои кабели среди продукции конкурентов с помощью броских названий. Затем вышло в свет приложение 5 к стандарту TIA/EIA-568-A (Addendum 5), и история повторилась. На этот раз кабельная маркировка стала использовать названия “Category 5e”, “Category 5 (2000)” или “Category 5 (2001)”. На рынке появилось огромное количество кабелей, в названии которых подчеркивалась их пригодность для гигабитного Ethernet и более высокоскоростных приложений. При этом на самом деле приложения 1000BASET будут отлично работать даже на кабеле Категории 5, произведенном в соответствии с требованиями бюллетеня TSB95. Категория 5e обеспечивает Заказчику важно разбираться в маркировке по двум причинам. Во-первых, не надо поддаваться рекламе, броским названиям и маркировке, нанесенной на оболочку. Доверяйте только результатам тестирования, полученным с помощью полевого кабельного тестера – только так можно узнать действительные характеристики и проверить кабель на соответствие той или иной категории. Иногда сегмент не проходит тестирование на выбранный уровень характеристик, а иногда наоборот, проходит с таким запасом, что сегмент можно было бы успешно протестировать и на более высокую категорию (так бывает при очень высоком качестве монтажа). Вторая причина состоит в том, что периодически стандарты меняются, а маркировка кабеля остается прежней, и тогда довольно сложно разобраться, каким же требованиям соответствует продукция – старым или новым. И если для кабелей в диапазоне до 100 МГц на это можно закрыть глаза, потому что разница не очень критична (это касается Категории 5 и Класса D), то для более производительных кабельных систем разница может быть очень существенной.

Поначалу продукция различных производителей, которую позиционировали как компоненты Категории 6, соответствующие первым черновым версиям стандарта Category 6, могла успешно использоваться только в рамках систем, построенных на оборудовании только одного и того же производителя. Если в

системе использовались компоненты Категории 6 от разных производителей, то они могли пройти тестирование только на более низкую категорию. Чтобы гарантированно получить желаемые характеристики, приходилось использовать в системе компоненты и кабель только одного и того же производителя. Похожая ситуация наблюдалась и с первыми сегментами Категории 6А и Класса EA, которые выполнялись на основе предварительных версий стандартов. По этим причинам, если вы решили модернизировать кабельную систему и добиться от нее более высоких характеристик, вам в обязательном порядке придется тестировать каждый сегмент в его существующем виде, чтобы убедиться в его действительных характеристиках. Судить о характеристиках сегмента только по марке компонентов, использованных в нем, можно лишь в тех редких случаях, когда ставится продукция одного и того же изготовителя, из одной и той же партии, причем производитель сам официально гарантировал совместимость своего кабеля и коммутационного оборудования. И даже тогда на итоговые характеристики может повлиять качество монтажа. Единственно правильный подход – тестировать все итоговые Постоянные линии или Каналы на соответствие требованиям стандарта. Конфигурации Канала, Постоянной линии и вышедшей из употребления Базовой линии будут описаны позже. Пока же Довольно интересная тема – названия, которые производители дают своим кабелям. Официальные, принятые стандартом обозначения – Category 5 и Category 5e. Стандарты не знают, что такое Category 5E с большой буквой “E” – это просто попытка маркетологов позиционировать свой кабель как улучшенный в сравнении с обычной Категорией 5e. Точно так же производители из маркетинговых соображений называли свои кабели Category 6e, предполагая, что стандарты именно так назовут следующую категорию. На самом же деле такой категории нет.

Стандарты TIA/EIA для категории, следующей за Категорией 6, выбрали обозначение 6A, с большой буквой “A”. Нет и такого понятия как система Категории 7 – есть продукция, произведенная в соответствии с требованиями ISO/IEC 11801, а этот стандарт использует обозначение “Class F”. Точнее, обозначение “Категория 7” может использоваться применительно к отдельным компонентам – то есть коннекторам, пробивным блокам кроссов и тому

подобной продукции – а вот характеристики системы в целом проверяются на соответствие Классу F. Стандарты TIA/EIA так и не опубликовали требования к Категории 7. И, похоже, в ближайшее время не опубликуют. Если кабельный анализатор (тестер, работающий в частотном диапазоне) после выполнения Автотеста показал вам сбой, то необходимо проверить:

- Правильные ли в приборе настройки Автотеста?
- Правильный ли тип сегмента был выбран (Постоянная линия Permanent Link или Канал Channel )?
- Соответствует ли тип адаптера, подключенного к прибору, данному типу теста? Некоторые приборы третьего поколения требуют, чтобы при тестировании Постоянной линии тип интерфейсного адаптера на приборе точно соответствовал установленному сегменту.
- Самая ли свежая версия программного обеспечения используется в тестере? Как уже говорилось раньше, стандарты периодически обновляются.
- Соответствуют ли тип кабеля и коннекторов, установленных в кабельной системе, типу Автотеста, что выбран в приборе?
- Если сегмент относится к системе Категории 6 по стандарту TIA или Классу E по стандартам ISO, или же к системе Категории 6А/Класса EA, то действительно ли все компоненты соответствуют этим требованиям? Некоторые из сегментов в системах Категории 6/Класса E и Категории 6А/Класса EA, установленные до окончательного подтверждения стандарта, могут не обеспечивать необходимые характеристики, если в них применена продукция от разных производителей.
- Не истек ли период калибровки прибора? Находится ли он при комнатной температуре? Температура прибора существенно влияет на результаты тестирования.
- Полностью ли заряжены аккумуляторы прибора? У некоторых тестеров истощение батарей до уровня в 20% от полного заряда приводит к получению недостоверных результатов.
- Проверили ли вы качество монтажа коммутационного оборудования? Не следует ли переделать некоторые компоненты?

Не слишком ли сильно стянуты кабели в пучки? Если хомуты-стяжки затянуты слишком туго, а порой наоборот, если кабели с очень высокими

характеристиками выложены идеально параллельно друг другу на большом расстоянии (это касается Категории 6/Класса E и особенно Категории 6A/Класса EA), то это может вызвать проблемы, которые в иной ситуации не возникли бы.

Если тест выдает пограничный результат, отмеченный звездочкой (PASS\* или FAIL\*), то следует посмотреть подробные результаты теста, чтобы найти причину проблемы, устранить ее и затем получить хороший результат при повторном тестировании. Можно запустить диагностические тесты TDR или TDX и посмотреть получившиеся диаграммы – это поможет найти точку сбоя.

Если тест дал “чистый” сбой, а не пограничный результат со звездочкой (\*), и при этом ошибок в схеме разводки нет, то как-то поправить или пошевелить кабель, чтобы получить чистый результат PASS, у вас вряд ли получится, особенно для Категории 6/Класса E. В таких случаях обязательно нужно воспользоваться функциями глубокой диагностики, имеющимися у кабельного тестера, чтобы выяснить, где кроется причина сбоя: в разъемах на концах, в кабеле или патч-шнурах. Запустите тесты TDR или TDX и посмотрите, что покажут диаграммы – они могут указать место расположения сбоя. Если вы подозреваете, что причина кроется в кабеле, или если все компоненты вашей кабельной системы Категории 6/Класса E – от одного и того же производителя (и кабель, и разъемы), то сохраните полные результаты тестирования и запишите модель прибора, его серийный номер и версию программного обеспечения. Затем обратитесь к соответствующему производителю, отправьте ему полученные результаты тестирования и запросите помощь в устранении имеющегося сбоя. Продукция Категории 6/Класса E, установленная за два года до того, как было окончательно одобрен стандарт, иногда не вполне совместима с продукцией той же категории и класса, произведенной другими изготовителями. То же самое может происходить и с продукцией Категории 6A/Класса EA, установленной в первых системах такого типа.

## Тесты в медной среде

### Схема разводки (Wiremap)

Ошибки в схеме разводки – обрывы, короткие замыкания и неправильный порядок проводников – в системе найти проще всего. Для этого используются

тесты схемы разводки (Wiremap) и длины (Length). Они позволяют выявить неаккуратно заделанные компоненты, проверить непрерывность проводников и найти ошибки в расположении пар. Некоторые сбои, вызванные разделением пар (Split), обнаружить сложнее: для этого требуется тест, проверяющий величину перекрестных наводок в зависимости от расстояния. Таков, например, тест TDX. Он работает по тому же принципу, что и тест, определяющий расстояние до точки сбоя (измерение длины и тест TDR). Это подробно описано в разделе, посвященном продвинутым методам диагностики.

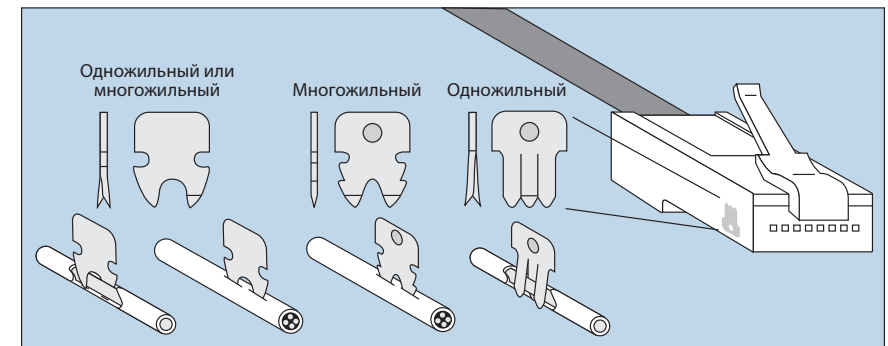


Рисунок 2: Виды зубцов в вилке RJ45 для многожильного (stranded) и одножильного (solid) кабеля.

Большинство ошибок в схеме разводки появляется при заделке коммутационного оборудования: либо в гнезде/вилке RJ45, либо в кроссе или на патч-панели. Ошибки на модуле или в вилке RJ45 часто можно идентифицировать визуально, просто проверив порядок цветов на соответствие схемам разводки T568A или T568B. В вилке еще следует проверить, все ли проводники введены в коннектор до упора – иначе при обжиге вилки на некоторых проводниках будет отсутствовать контакт. Проверая, все ли проводники введены как следует, заодно взгляните, какой тип зубцов у контактов вилки RJ45. Зубцы в вилках для одножильного кабеля (кабель с полнотелой жилой, solid) отличаются от зубцов для многожильного кабеля (stranded), вот только после обжима вилки их не так-то просто разглядеть. Посмотрите Рисунок 2.

Если использована вилка с несоответствующим типом зубцов, то контакт может получиться ненадежным, со временем он может вообще пропасть, несмотря на

то, что обычно шнуры используют сразу после изготовления. Вилки RJ45 могут страдать еще и от неравномерного обжима. На Рисунке 3 показаны 4 результата неравномерного обжима. На верхней левой вилке нормально продавлены крайние контакты, но недостаточно дожаты центральные. На верхней правой вилке все с точностью до наоборот, центральные контакты продавлены как следует, а боковые – недостаточно.

На нижних вилках с одной стороны было приложено соответствующее усилие обжатия, в то время как с другой стороны давление было недостаточным, имеет место недообжим. Обычно так бывает при использовании дешевых обжимных инструментов, в которых рама сделана из пластика. Он гнется тем сильнее, чем больше приложено усилие. Может быть масса других разновидностей сбоев подобного типа. Например, все контакты могут быть продавлены одинаково, но при этом недостаточно глубоко.

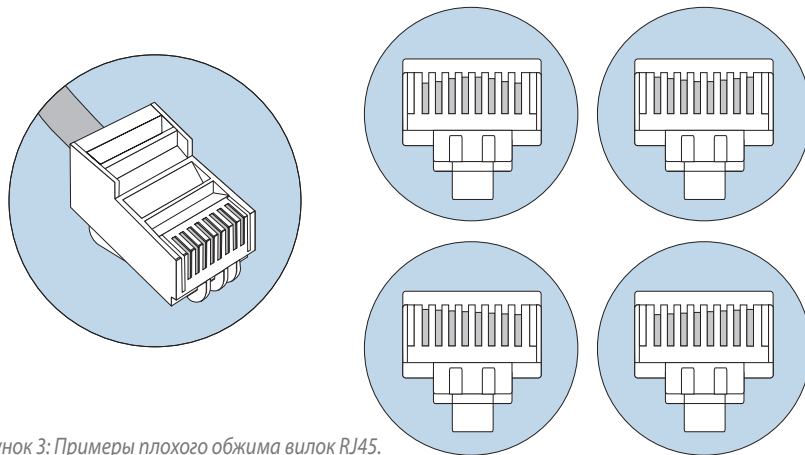


Рисунок 3: Примеры плохого обжима вилок RJ45.

Недостаточный обжим чаще всего происходит тогда, когда не до конца отработывает трещотка (храповик) инструмента. В этом случае инструмент позволяет извлечь из него вилку RJ45 до того, как она обжата полностью. Если инструмент поврежден, то один или несколько контактов могут быть вообще не продавлены на свои места. Иногда обжимной инструмент недостаточно прочен или его элементы разболтаны. Это приводит к появлению одной из проблем, показанных на Рисунке 3. Если в вилке RJ45 какие-то контакты недостаточно обжаты, то при подключении ее к гнезду RJ45 соответствующие ламели гнезда

могут продаваться слишком глубоко, стать плоскими, и в будущем они просто не достанут до контактов вилки (см. Рисунок 4).

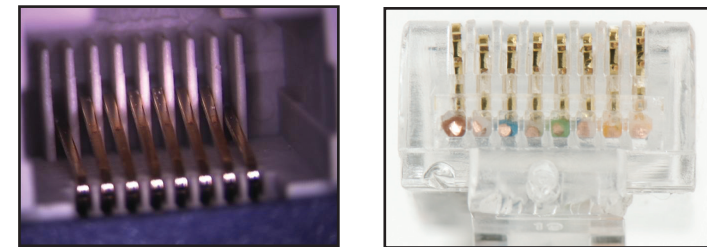
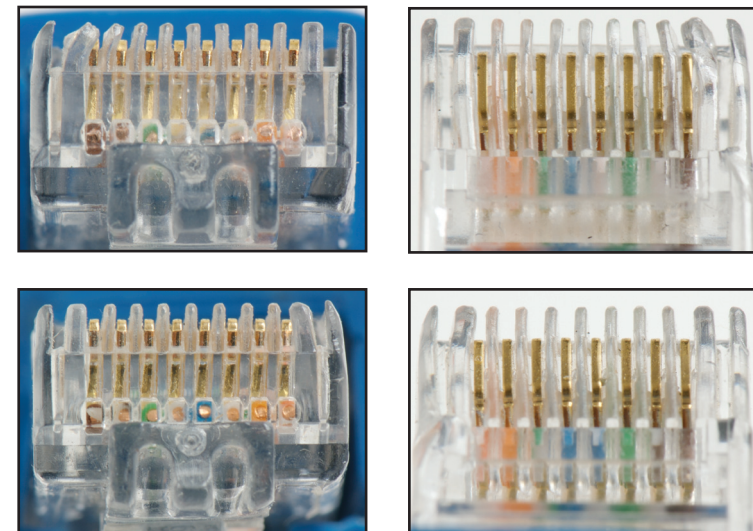


Рисунок 4: Слева показано гнездо RJ45, поврежденное недостаточно обжатой вилкой RJ45. Внешние ламели продавлены и постоянно находятся ниже остальных ламелей. Справа показана вилка RJ45, контакты которой обжаты неравномерно и могут вызывать такие повреждения.

Повреждение гнезда, показанное на Рисунке 4, иногда можно устранить, если найти подходящий предмет, тонкий и при этом достаточно прочный, чтобы выправить продавленные ламели и поставить их вровень с остальными, неповрежденными ламелями. Пробуя выправить продавленную ламель, не спешите и не прилагайте чрезмерных усилий. Помните, что такие действия могут нарушать условия гарантий, которые производители компонентов дают на свою продукцию. С другой стороны, гнездо все равно уже повреждено, так что от попытки его поправить вы ничего не потеряете. Подобные проблемы



вид спереди

вид сверху

Рисунок 5: Два примера повреждений вилки RJ45, обнаруженных при поиске сбоя.

часто появляются, например, в учебных классах, где студенты учатся делать патч- шнуры, и тогда лучше сделать дополнительные шнуры-удлинители с вилкой на одном конце и гнездом на другом. Пусть студенты подключают свои шнуры к такому дополнительному гнезду. Даже если оно выйдет из строя, его заменить проще, чем порт в стене или патч-панели. А недостаточно обжатую вилку можно просто откусить и поставить на кабель новую.

Внимательно осматривайте пластмассовые элементы вилки RJ45, особенно между металлическими контактами. Если они деформируются или ломаются, то пластмассовые фрагменты могут оказаться точно над контактом, и тогда в гнезде не будет соединения с соответствующей ламелью. С патч-шнурами так бывает довольно часто.

На Рисунке 5 на верхних фотографиях вы можете видеть на вилках RJ45 повреждения пластмассовых разделителей между контактами. С двумя ламелями в гнезде контакта не будет, с третьей может быть будет, а может нет. Нижние фотографии вилки RJ45 тоже показывают повреждение пластмассовых деталей, но надо присмотреться, чтобы заметить, что расстояние между разделителями для самого правого контакта слишком мало, и крайняя ламель не сможет его коснуться.

Обратите внимание, что в гнезде RJ45 тоже могут быть повреждения – например, какие-то ламели могут сместиться в сторону, вплоть до возникновения короткого замыкания с соседней ламелью.

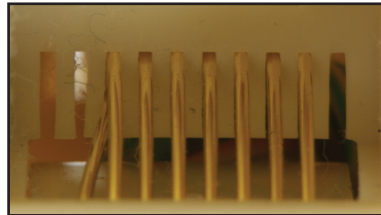


Рисунок 6: Смещение ламели внутри гнезда RJ45.

## Длина

До сих пор бывает, что кабельные системы устанавливают «специалисты», не прошедшие обучение и не знающие требований стандартов. В результате в системах могут встречаться сегменты длиной более 100 м, максимально разрешенных стандартом. Кабельный сегмент может быть просто слишком длинным. Если это действительно так, то посмотрите, не оставил ли такой горе-

монтажник несколько метров кабеля в качестве запаса – в виде нескольких петель или даже небольшой бухты. Во времена господства старой Категории 5 петли и бухты кабеля в виде запаса за потолком или в трассе за стеной были распространенным (и довольно полезным) приемом, однако сворачивание кабеля в бухту приводит к избыточным перекрестным наводкам, которые непременно скажутся при реализации в системе 1- и 10-гигабитных приложений.

Также необходимо проверить, правильно ли выставлено в приборе значение номинальной скорости распространения сигнала NVP. Если оно неверно, то и измеренное значение длины будет неправильным. Значение NVP можно определить самостоятельно, для этого нужен лишь кусок кабеля средней длины, не менее 15 м. Тестером определяется измеренное значение длины, затем оно сопоставляется с фактической длиной, определенной по меткам на оболочке, после чего значение NVP в приборе корректируется до тех пор, пока измеренное и фактическое значения длины не совпадут.

Если длина одной или нескольких пар кабеля существенно отличается от длины остальных пар, то необходимо проверить промежуточные патч-панели и точки межсоединения: нет ли там провисших или неправильно расшитых пар? Большинство подобных ошибок появляется именно в промежуточных точках подключения. При этом помните, что значения длины у разных пар всегда должны немного различаться между собой, поскольку шаги повива у пар в кабеле специально делаются разными.

Стандарт TIA/EIA-568-B гласит, что общая длина кабеля определяется по длине самой короткой его пары. Как следствие, возможны ситуации, когда для длинных кабелей одна или больше пар выходят за пределы, допустимые стандартами, но при этом общий результат теста все равно положительный (PASS).

Если длина кабеля неправдоподобно мала, тогда внимательно приглядитесь, не менялось ли в последнее время поблизости расположение элементов строительных конструкций или трасс. Если вы ориентировочно представляете

себе, где проходит кабельная трасса, то будет несложно определить место расположения точки сбоя на основе полученного значения длины. Часто конец обрезанного кабеля находят примерно там, где располагается край свежеложенного коврового покрытия, где поставлены новые дверные косяки или другие элементы конструкций и перекрытий, которые пересекают кабельные потоки. Порой причиной подобного сбоя может служить вилка RJ45 с отломанной защелкой. Такие вилки могут легко выскакивать из гнезда, и тогда на линии будет диагностироваться обрыв.

На измеренную (электрическую) длину пары влияет то, какой тип полимера использован в качестве изоляции проводника. Если одна или две пары в кабеле используют не тот тип полимера, что остальные пары, то NVP пар – а вслед за ним и измеренная длина – будут существенно отличаться (см. Рисунок 7). В большинстве высокопроизводительных кабелей в качестве изоляции проводников используется политетрафторэтилен (фирменное название Тефлон). Но раньше, в середине 90-х годов, в мире в какой-то период был недостаток этого полимера вследствие грандиозного пожара на основном заводе производителя. Пока не была запущена в работу новая производственная мощность, производители экспериментировали с более доступным поливинилхлоридом (ПВХ) для изоляции проводников на наименее используемых парах. Это позволяло еще и снизить стоимость кабеля. Такая продукция продавалась по всему миру, в ней одна или две пары имели изоляцию из ПВХ, и такие кабели обозначались 3:1 или 2:2. Использование разных полимеров для изоляции проводников влияет на измерение длины,

LENGTH NO REMOTE DETECTED	
Pair	Length (ft)
1,2	320
3,6	303
4,5	305
7,8	304

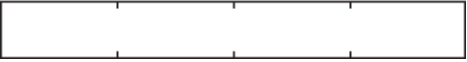


Рисунок 7: Результат измерения длины кабеля, в котором три пары имеют изоляцию из Тефлона, а одна – из полимера на основе ПВХ.

задержки распространения сигнала и смещения задержки. Такой кабель вряд ли подходит.

## Вносимые потери

Вносимые потери, больше известные как затухание (Attenuation), как правило, зависят от длины кабеля. Потери сигнала растут пропорционально длине кабеля. Поэтому при получении сбоя по затуханию в первую очередь надо проверить общую длину кабеля. Если сделать кабель короче, это должно устранить проблему; вопрос в том, удастся ли его сделать короче. К тому же, хотя чрезмерная длина – самая явная причина, тем не менее, в сбое часто виновата совсем не она.

Гораздо чаще причина проблемы – плохое соединение: следствие провисшего под своим весом кабеля, грязных или окислившихся контактов и других подобных факторов. Один плохой патч-шнур в сегменте может привести к сбою всего сегмента. В этом случае растут также возвратные потери (Return Loss), и именно из-за этого затухание (Attenuation) переименовали во вносимые потери (Insertion Loss). Запустите тесты TDR или TDX и посмотрите, что покажет диаграмма. Еще одной причиной сбоя может быть кабель не той категории, что нужно – например, если в сегменте, который должен обеспечивать характеристики Категории 6А, используется кабель Категории 5е. В этом случае для диагностики наверняка помогут тесты TDR или TDX и выдаваемые ими диаграммы.

## Перекрестные наводки на ближнем конце (Near End Crosstalk, NEXT), внешние перекрестные наводки (ANEXT) и интегральные перекрестные наводки (Power Sum)

Чрезмерные перекрестные наводки, которые чаще всего называют “параметр NEXT”, зарождаются в двух местах: внутри самого кабеля (внутренние наводки) и снаружи (соответственно, внешние наводки). Перекрестные наводки, возникающие внутри кабеля, сказываются тем сильнее (больше их величина и влияние на пару-жертву), чем меньше расстояние от передатчика (и, следовательно, чем сильнее передаваемый сигнал). Если пара кабеля расплетена больше, чем допускает стандарт – то есть больше 13 мм (округление от 0.5 дюйма) – то перекрестные наводки становятся очень большими. При

получении сбоя по перекрестным наводкам следует первым делом проверить качество монтажа на обоих концах сегмента.



Рисунок 8: Пример правильно выполненного монтажа: пары расплетены на минимальное расстояние, необходимое для заделки.

Если вы заметили расплетенные пары, то обязательно переделайте этот разъем. Если это не помогло, то попробуйте вытащить и перебить кабель в промежуточных точках подключения (в кроссах). Старые кроссы 66-го типа, изначально разработанные для телефонии, не следует применять в компьютерных сетях – они обеспечивают не очень хорошие характеристики по перекрестным наводкам и другим параметрам тестирования. Чтобы вписаться в требования Категории 5e, 6 и тем более 6A, следует использовать кроссы 110-го типа или пробивные блоки с более высокими характеристиками, причем эта продукция должна быть маркирована как пригодная для систем такого уровня. Прежде чем приступить к переделке компонентов для улучшения перекрестных наводок, сначала воспользуйтесь диагностическими средствами и выполните дополнительные тесты: они помогут вам найти источник проблем с перекрестными наводками.

Иногда встречается специфическая ситуация, когда на определенной частоте имеет место сбой, однако это не приводит к результату FAIL для совокупного теста – итоговый результат все равно PASS. И стандарт TIA, и стандарт ISO используют так называемое правило четырех децибел (“4 dB rule”). Если вносимые потери (Insertion Loss) меньше 4 дБ, то результат тестирования NEXT

будет положительным в любом случае, независимо от реально полученных численных значений (при условии, что одновременно получен результат PASS для помехозащищенности ACR). Такое же правило применяется и при измерении возвратных потерь (Return Loss), с той лишь разницей, что вносимые потери должны быть меньше 3 дБ, чтобы итоговый результат был PASS независимо от полученных численных значений.

### Шум

Шумы можно разделить на три основные группы:

- Импульсный шум, который чаще всего приводит к появлению в кабеле пиков по напряжению или току.
- Случайный (белый) шум, распределенный по всему спектру частот.
- Внешние перекрестные наводки (наводки с одного кабеля на пары соседнего кабеля).

Из этих трех типов шумов работе сети чаще всего препятствует импульсный шум. Большинство кабельных тестеров имеют встроенные функции для тестирования импульсных шумов. Стандарт 802.3 устанавливает конкретное пороговое значение для импульсных шумов: 264 мВ (см. пункт 14.4.4). Для высокоскоростных сетевых приложений – например, для 1000BASE-T – пороговое значение ниже и составляет 40 мВ (пункт 40.7.6). Если таких импульсов за определенный промежуток времени мало (меньше одного импульса за 100 секунд), то приложение будет надежно работать в такой кабельной системе.

Impulse Noise	
Testing...	
Average:	0.11 /s
Peak:	0.60 /s
2:34:20 p.m.	
Impulse Noise Threshold: 40mV	
Press F3 to stop or change threshold	
	Stop

Рисунок 9: Тест импульсного шума (Impulse Noise) в приборе DTX-1800.

Источниками импульсного и случайного шума могут быть находящиеся поблизости кабели электропитания или активное оборудование, обычно с высокой нагрузкой по току. К такому оборудованию относятся: большие электродвигатели, лифты и подъемники, фотокопировальная техника, кофе машины, вентиляционное оборудование,

нагревательные приборы, электросварочные аппараты, компрессоры и многое другое. Другой, менее очевидный источник шумов – передатчики, испускающие ненаправленное излучение: телевизионное оборудование, радиопередатчики, микроволновые печи, приемо-передающие станции мобильной связи, носимые радиостанции, системы безопасности здания, авиационное электронное оборудование и любые другие устройства с передающими мощностями выше, чем у обычного мобильного телефона. Некоторые кабельные анализаторы могут рассчитать средний уровень таких шумов и вычесть их из результатов тестирования. Такой тест занимает много времени, поскольку необходимо проводить много дополнительных измерений.

Небольшое количество шумов лишь слегка затрагивает передачу целевых сигналов в сети и практически не влияет на способность приемных схем в сетевых картах и других активных устройствах определять и правильно распознавать сетевые сигналы. Но если тестер вычленяет усредненные шумы из результатов тестирования, то в реальной работающей сети такие шумы никуда не исчезают и создают серьезные препятствия сетевому трафику.

Необходимо либо найти источник шума и переместить его дальше от кабелей, либо использовать в этой зоне волоконную оптику. Найти источники шумов не так- то просто, к тому же часто они работают не постоянно, то генерируя шумы, то нет. Тогда для определения частоты и величины шумов необходимо применять спектральный анализатор. Занимаясь поисками источника, нельзя упускать из виду то, что происходит во всей зоне, где проходит кабель. Неожиданное пропадание шумов порой так же полезно для поиска, как и постоянное присутствие шума. В этом случае надо выяснить, что за оборудование использовалось и было только что выключено.

Внешние перекрестные наводки выделены в отдельный тип шума, поскольку их источник – соседние кабели, уложенные в ту же самую кабельную трассу. Каждый раз, когда тестируется сегмент неэкранированной витой пары UTP в пучке, где несколько кабелей находятся в работе, очень велика вероятность, что тестер обнаружит внешние перекрестные наводки. В особенности если по этим кабелям передается трафик 10GBASE-TX. Тогда прибор сообщит о наличии

внешнего шума. Однако для скоростей ниже 10GBASE-T обычно внешние перекрестные наводки не оказывают заметного влияния на сетевой трафик.

В общем случае можно сказать, что обнаруженный шум не мешает надежной работе сети, если выполняются следующие условия:

- Кабельный анализатор выполняет Автотест до конца и выдает итоговый результат PASS.
- Тестирование на импульсный шум, выполненное на сегментах, которые, как вы полагаете, страдают от него, показывает среднее значение менее 0.01 импульсов в секунду (пороговое значение должно быть установлено на 40 мВ).
- При тестировании сегмента в пучке работающих кабелей получены успешные результаты NEXT с запасом не менее 3 дБ в сравнении с требованиями стандарта для данного сетевого приложения: это означает, что внешние перекрестные наводки не препятствуют передаче сигналов в сегменте.

### **Эквивалентные перекрестные наводки на дальнем конце (ACR-F или Equal Level Far End Crosstalk, ELFEXT)**

Практически все перекрестные наводки на дальнем конце возникают в вилке, в гнезде или в результате индуктивной связи одного с другим, в то время как практически все перекрестные наводки на ближнем конце – следствие емкостной связи по длине кабеля. Тем не менее, устранение сбоев по наводкам на ближнем конце NEXT, как правило, одновременно приводит к устранению большинства проблем с наводками на дальнем конце FEXT. В измерениях эти параметры чаще всего обозначаются как ACR-F или ELFEXT. Так происходит потому, что становятся значимыми только собственные электрические характеристики соединений.

Первым делом попробуйте заменить вилку RJ45 на том конце сегмента, где тестер показывает сбой. Если это не помогает, то замените имеющиеся вилку и гнездо на парные вилку и гнездо от одного и того же производителя.



## Возвратные потери

Возвратные потери учитывают все отражения, которые происходят в сегменте по всей его длине по причине несоответствия импедансов. Этот параметр показывает, насколько характеристический импеданс кабельной системы соответствует номинальному полному сопротивлению по всему диапазону частот. Характеристический импеданс сегментов может варьироваться от больших значений на низких частотах до малых значений на высоких частотах.

Согласованное сопротивление на обоих концах сегмента должно совпадать с характеристическим импедансом сегмента в целом, тогда отражений в нем почти не будет. Если соответствие между этими величинами хорошее, то передача сигналов в сегменте происходит беспрепятственно в оба конца, а отражения минимальны. Значения возвратных потерь дают большие флуктуации при изменении частоты.

Незначительные вариации характеристического импеданса по длине кабеля приводят к возникновению небольших возвратных потерь. Причиной тому могут быть небольшие нарушения в шаге повива пар, небольшое отдаление проводников пары друг от друга (возникновение просвета между проводниками одной пары), неоднородности в материале изоляции или посторонние включения в металле проводника. Параметр структурных возвратных потерь (Structural Return Loss, SRL) характеризует однородность импеданса по всей длине кабеля и говорит о том, насколько отработан и стабилен производственный процесс у изготовителя кабеля.

Еще один источник возвратных потерь – отражения от коннекторов в сегменте. Как правило, несоответствия импедансов

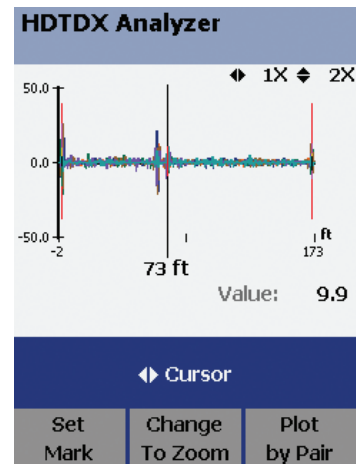


Рисунок 10: Пример теста TDR с высоким разрешением, проведенного с помощью прибора DTX-1800. Диаграмма на экране прибора показывает, что точка подключения к сегменту основного модуля имеет очень плохие характеристики. Кроме того, в 70 футах от прибора обнаружен патч-шнур с плохими характеристиками.

обнаруживаются именно там, где расположены коннекторы. Основное следствие таких потерь вовсе не потеря мощности сигнала, как могло бы показаться, а отклонение фазы или частоты передаваемого сигнала, так называемое дрожание. Отражения сигналов и в самом деле вызывают потерю части мощности сигнала, но вовсе не это, а отражения приводят к серьезным проблемам. Поскольку возвратные потери подразумевают появление отражений, тест TDR поможет определить точки сбоя: те, в которых имеет место рассогласование импедансов. Чем выше в сегменте возвратные потери, тем больше амплитуда пиков на диаграмме TDR на соответствующих участках.

## Задержка распространения

Стандарт TIA/EIA-568-B допускает задержку распространения сигнала в Постоянной линии до 498 нс, а в Канале до 555 нс, независимо от категории системы. Ситуации, когда сбой дает только задержка распространения, а по другим параметрам сбоев нет, почти не встречаются. Получение результата FAIL по задержке распространения свидетельствует либо о чрезмерной длине кабеля в сегменте, либо о несоответствующем типе или качестве (браке) кабеля. Проверьте суммарную длину сегмента. Внимательно осмотрите кабель и проверьте, правильный ли тип кабеля использован в системе.

## Смещение задержки

Стандарт TIA/EIA-568-B допускает смещение задержки до 44 нс для Постоянной линии и до 50 нс для Канала, независимо от категории. На самом деле оба этих значения предоставляют системам очень большой запас. Если в системе использованы качественные компоненты, то представить себе ситуацию, когда смещение задержки дает сбой, очень сложно. Такой сбой возможен разве только в тех случаях, когда использован кабель, в котором для разных пар используется изоляция из разных материалов. В разделе о длине такая ситуация описана в деталях. Также подобный сбой может возникнуть, если вместо патч-шнура для коммутации были использованы отдельные витые пары или кроссировочные перемычки, причем разной длины. Большой разброс в длинах пар по всему сегменту может быть следствием неправильно выполненного монтажа. Для коммутации в компьютерных сетях никогда не следует использовать отдельные пары. Одновременно со

смещением задержки дадут сбой и другие параметры. Проверьте все точки коммутации в сегменте. Если монтаж выполнен правильно, то единственное, что вам остается – заменить сам кабель. Прежде чем ставить вместо него другой участок кабеля, протестируйте его, чтобы быть уверенным, что вы не поставите вместо одного бракованного кабеля другой бракованный.

### Интерпретация результатов тестирования медных сред

Прежде чем искать точку сбоя в кабельном сегменте, давшем результат FAIL при тестировании, сначала проверьте настройки прибора. Настройки чрезвычайно важны для получения достоверных результатов измерения. Как минимум, проверьте выбранный тип Автотеста и конфигурацию тестируемого сегмента – Постоянная линия или Канал. Кроме того, стандарты со временем меняются довольно значительно, поэтому требования по конкретному тесту могут существенно отличаться от требований, заложенных в программном обеспечении прибора. Регулярно заходите на веб-сайт производителя прибора и загружайте свежие версии программного обеспечения прибора: не реже двух- трех раз в год.

В отличие от сбоев в активном оборудовании, сбой в кабельной среде обнаруживаются и устраняются практически одними и теми же способами как непосредственно после монтажа кабельной системы, так и после некоторого периода эксплуатации. Бывает так, что сегмент со скверными характеристиками долгое время работает (пусть и не идеально), но затем в результате каких-то внешних факторов перестает работать совсем. Такими факторами могут быть явное повреждение кабеля, размещение рядом с кабелем источников шума или перемещение кабеля к источникам шума. Еще один вариант, хотя и встречающийся реже – если происходит реализация новых приложений на физическом уровне. Например, используется сетевая карта, которая для автосогласования использует не 100 Мбит/с, как раньше было принято в этой системе, а 1000 Мбит/с. Так может произойти, если в рабочую станцию установлена новая сетевая карта, если патч-шнур подключен к другому порту хаба или сетевого коммутатора или даже к другому хабу или коммутатору.

Некоторые порты проверяют сегмент на полярность (нет ли в нем реверса в

какой-нибудь паре) и наличие кроссовера (транспозиции пар на одном конце), и если обнаруживают их, то корректируют ошибку сами, за счет внутренних возможностей. Возможно, прежний порт так и делал, а новый порт, к которому сегмент подключен теперь, такой возможности не имеет. В результате ошибка.

Описание	Обрыв	Короткое замыкание	Реверсивная пара	Перекрещенные пары	Разделенные пары	Сбой по длине	Смещение задержки	Вносимые потери	Наводки NEXT	Возвратные потери	Помехозащищенность ACR-F	Межкабельные наводки
Кабель перекушен, оборван или поврежден иным способом	•	•				•				•		
Повреждена вилка или гнездо RJ45	•	•										
В сегменте использованы обе схемы разводки: T56A и T568B				•								
Для разных пар используется разный материал изоляции							•					
Низкое качество монтажа при разделке кабеля на коннектор			•	•	•			•	•	•		
Неправильный порядок проводников при разделке кабеля на коннектор									•	•		
Соединитель или адаптер RJ45 имеет низкое качество, неправильную разводку или предназначен только для телефонии									•	•		
Низкое качество вилок/гнезд RJ45 или характеристики слишком низкой категории									•	•	•	•
Патч-шнур(ы) плохого качества либо с повреждениями									•	•		
В сегменте используется участок 100-омного кабеля и участок кабеля иного типа										•		
Кабель слишком длинный либо установлено неправильное значение NVP						•		•				
Расплетенные либо плохо сплетенные пары кабеля (включая слишком редкий шаг повива пар, например, в кабелях Категории 5е в сравнении с Категорией 6)									•	•	•	•
По длине кабеля слишком туго затянуты хомуты-стяжки									•	•		
Источник внешнего шума недалеко от кабеля									•		•	•
Кабели лежат слишком плотно друг к другу на среднем или большом протяжении. Удалите хомуты-стяжки и/или расположите кабели более свободно												•

Таблица 1: Основные виды сбоев кабельных тестов и их причины.

## Поиск и устранение сбоев в волоконной оптике

### Приборы

Для поиска неисправностей в оптических сетях существует не так-то много устройств. Нижнюю ценовую нишу занимают приборы, задача которых – проверить непрерывность сегмента. Приборы средней стоимости позволяют проверить, приемлем ли итоговый уровень оптической мощности в сегменте. Серьезную же диагностику следует проводить с помощью оптических рефлектометров во временной области (Optical Time Domain Reflectometer, OTDR). Это довольно дорогие приборы. Если уровни мощности недостаточны или если рефлектометр показывает проблемы в начале сегмента, то первое, что нужно сделать – провести очистку оптических коннекторов и проверить состояние их торцов.

### Безопасность

При работе с оптикой всегда следует принимать меры предосторожности. Длины волн, которые используются в оптических сетях, относятся к невидимому диапазону. Человеческий глаз воспринимает излучение от фиолетового цвета (длина волны около 380 нм) до красного (около 750 нм). Многие источники, применяемые в оптических сетях, используют лазеры, и некоторые из них имеют очень большую мощность. Никогда не смотрите в торец оптического волокна, в оптический порт или проходник. Если какой-то оптический порт не используется, закройте его специальным колпачком – это уберезет глаза от повреждения невидимым излучением и одновременно защитит оптический разъем от загрязнения.

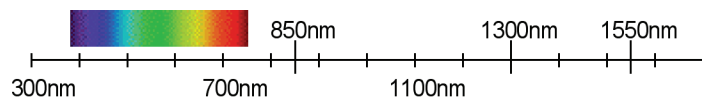


Рисунок 11: Видимый свет находится в области более коротких длин волн (от 380 до 750 нм), чем те, что используются в компьютерных сетях.

Если вам необходимо визуально идентифицировать порт и вы используете источник видимого света, то самый безопасный способ – направить конец оптического кабеля на лист белой бумаги либо поднести лист бумаги к месту оптического подключения. Никогда не смотрите прямо в коннектор – всегда есть риск, что из него исходит невидимое излучение.

## Тестирование непрерывности

Один из способов проверки непрерывности оптического сегмента и полярности парных оптических волокон – использовать видимый свет. Большинство таких устройств по сути представляют собой фонарики, испускающие белый свет или другие цвета; бывают также очень яркие светодиодные фонарики размером с брелок. Фонарики, специально предназначенные для использования в компьютерных сетях, оснащены разными типами адаптеров: SC, ST и другие. В таких фонариках пучок света, как правило, сфокусирован лучше, чем в обычных фонарях, а цвет чаще всего используется красный, довольно яркий.



Рисунок 12: Фонарик, специально созданный для использования в волоконно-оптических кабельных системах.

Тем не менее, в них не применяются ни лампы накаливания, ни лазеры. Проверить непрерывность можно также с помощью специального источника видимого света, предназначенного для поиска неисправностей – Visual Fault Locator (VFL) – который построен на основе лазера, работающего в видимом участке спектра. Источники видимого света VFL, как правило, не используют элементы накаливания, а основаны именно на лазере. Чаще всего встречаются лазеры Класса II, работающие на длине волны 650 нм и испускающие красный свет.

Если в оптическом кабеле волокно повреждено или разбито, то часто при



Рисунок 13: Источник VFL применяется для поиска точек обрыва в оптических кабелях. Помните, что такой свет может пробиться не через все виды оболочек оптических кабелей.

использовании источника VFL можно заметить это место визуально – свет будет пробиваться прямо сквозь оболочку кабеля. К сожалению, так происходит не со всеми типами кабеля. В некоторых кабелях из-за определенного типа и количества оболочек свет снаружи не виден.

## Тестирование затухания или оптических потерь

Применительно к оптическим кабельным системам термины потери или затухание могут использоваться как синонимы, хотя на самом деле потери могут быть и следствием сбоя на входе в оптический сегмент. Для тестирования совокупных потерь мощности (затухания) в волоконно-оптическом сегменте используется специальный прибор, состоящий из двух модулей: источника света и измерителя оптической мощности. Это оборудование часто так и называется – комплект для тестирования потерь оптической мощности Optical Loss Test Set (OLTS). Источник света, подключенный к сегменту на одном конце, подает в него непрерывный сигнал на определенных длинах волн.

Измеритель с портом- фотоприемником подключается к дальнему концу сегмента. Измеритель определяет оптическую мощность сигнала на выходе из сегмента на тех же длинах волн, на которых работает источник. Источник может быть основан на светодиоде или лазере, причем их тип максимально приближен к типу устройств, реально используемых в компьютерном оборудовании. Полученный результат измерения сверяется с бюджетом мощности, необходимым для реализации конкретного приложения. Именно такую процедуру тестирования установленных оптических сегментов предусматривают оба стандарта – и TIA, и ISO. Приборы.

## Тестирование рефлектометром OTDR

Оптический рефлектометр во временной области Optical Time Domain Reflectometer (OTDR) выдает диаграмму (рефлектограмму), на которой показаны все точки отражения и отображен эффект обратного рассеяния исходного луча света, поданного в оптический сегмент с одного конца. Рефлектометр работает по принципу, похожему на тот, что используется в тестах TDR в медной среде, и тоже фиксирует все обратные отражения. Когда луч света подходит к точкам соединения, коннекторам, муфтам, участкам с разбитым или поврежденным волокном, к точкам перегиба кабеля или к концу оптического сегмента, некоторая часть света отражается назад, возвращаясь к рефлектометру. В приборе на том же порту установлены фотоприемники с большим усилением, они измеряют величину отраженного сигнала. Незначительная часть света, кроме того, отражается назад самой кристаллической структурой кварцевого

стекла, из которого состоят оптические волокна, и это явление называется обратным рассеянием. На рефлектограмме оно отображается углом наклона получаемого графика. Угол наклона графика в результате обратного рассеяния позволяет рассчитать затухание. Внимательный анализ рефлектограммы позволяет идентифицировать точки на графике как коннекторы, обрывы, участки разбитого волокна, муфты, резкие перегибы и другие события. Как и с тестом TDR, задержку между моментом отправки сигнала и получением отражений можно.

## Проверка торца волокна

Специальные оптические или видео-микроскопы позволяют визуально проверить состояние торца коннектора и убедиться, что на нем отсутствуют грязь и царапины, причем это касается и коннекторов в кабельных сегментах, и портов активного оптического оборудования. У волоконно-оптических кабелей, кроме того, проверяется качество полировки коннекторов. Как правило, такие микроскопы обеспечивают увеличение от 200х до 400х. В недавно проведенном исследовании оптических систем был сделан вывод о том, что до 80% проблем с волоконной оптикой возникает из-за загрязнений.

## Типы волоконно-оптических кабелей

Многие знают, что существуют одномодовые и многомодовые оптические волокна, но на самом деле нужно разбираться в типах волокон немного глубже. Опишем основные типы волокон.

Некоторые из старых многомодовых кабелей называли кабелями FDDI. Это поколение оптических кабелей относится к волокнам со ступенчатым показателем преломления. При изготовлении таких кабелей часто встречались неоднородности и дефекты волокна, посторонние включения, вариации показателя преломления в ядре волокна. Такие волокна были предназначены для подключения оборудования со светодиодными источниками, которые подавали в волокно большое количество лучей (мод). Каждая мода – это отдельный путь луча в волокне, причем далеко не всегда параллельно его оси, а часто под довольно большими углами. Чем больше такие углы, тем длиннее путь луча в волокне, и тем позже такой луч доберется до дальнего конца сегмента. Быстрее всего до выхода долетит луч, идущий точно по оси волокна.

В результате четкий импульс, поданный на вход в сегмент, на выходе выглядит расплывшимся. Если подавать такие импульсы слишком часто, то на выходе они могут расплываться вплоть до того, что соседние импульсы будут сливаться воедино. Приемное устройство не сможет их различить и отделить друг от друга. Это явление называется модальной дисперсией (дисперсией мод).

Следующее поколение кабелей использовало волокна с градиентным показателем преломления. В них состав кварцевого стекла слегка изменяется от ядра к демпферу, за счет чего лучи, отклоняющиеся от центральной оси, снова направляются к ней. Теперь луч, вошедший в волокно под углом, не будет резко переотражаться от границы ядро-демпфер, а пойдет по плавной синусоиде, порой вообще не доходя до границы. В таком типе волокон модальная дисперсия гораздо меньше, и сигналы в них можно передавать на большее расстояние, чем в волокнах со ступенчатым показателем преломления.

Сейчас выпускаются также многомодовые волокна, оптимизированные под применение лазерных источников. В таких волокнах показатель преломления выверен еще строже. К ним можно подключать оптическое оборудование с лазерами VCSEL, позволяющее реализовать приложения Gigabit Ethernet. При передаче таких сигналов мод гораздо меньше, и модальная дисперсия еще ниже. На выходе такие сигналы расплываются мало, они четко различимы, поэтому можно применять высокую скорость передачи. Первые волокна, оптимизированные под применение лазерных источников, появились в середине девяностых годов, и они не в состоянии поддерживать 10-гигабитные приложения. Более поздние волокна, изготовленные по усовершенствованной технологии, позволяют еще лучше контролировать показатель преломления. Такие волокна выпускаются с 1999 года, они надежно поддерживают 10-гигабитные приложения. Следует учитывать, что чем больше ядро, тем больше может быть мод, поэтому многомодовые волокна 62.5 мкм стали уступать место волокнам 50 мкм. В 50-микронном волокне мод меньше, и сигнал остается распознаваемым на большем расстоянии. По такому волокну можно передавать данные с более высокой скоростью.

Одномодовое волокно тоже претерпело некоторые изменения. В одномоде

ядро настолько маленькое, что считается, что для данной длины волны мода в нем может быть только одна, и пролегает она точно по оси волокна. Исходная конструкция таких волокон обозначается NDSF – одномодовое волокно с несмещенной дисперсией. Оно отлично работает на длинах волн 1300/1310 нм, однако на 1550 нм его использовать нельзя. Строение кабеля оптимизировали для поддержки длины волны 1550 нм и новый тип назвали DSF – одномодовое волокно со смещенной дисперсией.

Когда же появилось оборудование DWDM со спектральным уплотнением каналов, выяснилось, что волокна DSF имеют некоторые нежелательные нелинейности, и тогда была создана разновидность NZ-DSF – одномодовое волокно со смещенной ненулевой дисперсией. Сейчас разрабатываются и другие типы волокон, использующие специфические материалы и новые конструкции, например, волокно PM, поддерживающее передачу поляризованного света.

Прежде чем внедрять в существующей волоконно-оптической системе какие-либо новые приложения, сначала подробно изучите характеристики установленного волокна.

## Тесты в волоконно-оптической среде

Совокупное затухание в канале можно измерить как приборами OLTS, так и

EVENT TABLE				OFTM-5612	
Auto OTDR				06/22/2006 6:29:15 p.m.	
LOCATION (m)	dB@850nm	dB@1300nm	EVENT TYPE	STATUS	
0.00	N/A	N/A	OTDR PORT		
102.14	0.39	-0.22	GHOST SOURCE	PASS	
152.72	0.20	0.97	REFLECTION	FAIL	
164.11	1.17		LOSS	FAIL	
174.58	0.19	0.65	REFLECTION	PASS	
204.69	0.00	0.05	GHOST		
226.32	N/A	N/A	END		

Scroll List, Select Field, Press EXIT to view SUMMARY

View Trace   Sort Field   View Details

Рисунок 14: Результаты, выдаваемые рефлектометром OTDR – список распознанных событий и соответствующее затухание по каждому из них.

рефлектометром OTDR. Результаты рефлектометра позволяют проверить бюджет затухания в линии по всем отдельным позициям, поскольку в них выводится информация о каждом событии, обнаруженном в канале (см. Рисунок 14).

## Интерпретация результатов тестирования волоконной оптики

### Полярность волокон

Вообще-то нарушение полярности нельзя считать сбоем, поскольку задача тестирования – промаркировать волокна и расположить их в соответствии с парной схемой, принятой в вашей сети. Как правило, проверка полярности – это один из этапов подготовки к тестированию затухания. Если источник света и измеритель не будут подключены к одному и тому же волокну, вы просто не сможете провести измерение.

В некоторых сетях правильному парному расположению волокон вообще не уделяется внимание. Если волокна расположены неверно, то сетевой специалист просто меняет местами коннекторы оптического шнура при подключении активного оборудования. Если ваша оптическая система не работает, то самым первым действием по устранению проблемы будет смена местами коннекторов шнура, подключенного к портам TX (передающему) и RX (принимающему). Если проблема заключалась только в неверном парном расположении волокон, то она обнаруживается и устраняется очень легко – просто поменяйте местами разъемы.

### Длина

Рефлектометр OTDR покажет вам полную длину канала, после чего ее можно сравнить со спецификациями на сетевое приложение, которое планируется внедрить. Рефлектометр также может показать, что какой-то сегмент короче ожидаемого, и это может быть свидетельством обрыва кабеля где-то в трассе. Если рефлектометра у вас нет, то придется обратиться к документации на систему или данным по ее сертификации при вводе в эксплуатацию.

Определить длину каждого оптического сегмента в системе можно также по меткам длины в начале и в конце каждого кабеля. Полученные значения опять же можно сравнить со спецификациями на конкретное сетевое приложение.

В любом случае обязательно проверьте коэффициент широкополосности для установленного типа кабеля. Часто эту информацию необходимо искать в каталогах и листах спецификаций, используя маркировку на оболочке кабеля как ссылку. Через коэффициент широкополосности можно перейти к ограничению по длине для реализации того или иного приложения в данном типе кабеля.

### Сбой по затуханию

Прежде чем искать неисправность, сначала проверьте:

- В тестере должно быть правильно установлено количество адаптеров (проходников) и муфт в сегменте (это касается тестов, в которых прибор рассчитывает бюджет затухания волоконно-оптической линии).
- В настройках прибора должен быть выбран правильный тип волокна.
- Перед началом тестирования модули прибора должны пройти процедуру установки эталонного значения, причем эти действия должны выполняться при той же температуре, при которой будет проходить последующее тестирование, а после установки эталонного значения категорически нельзя отключать шнуры от передающих портов.

Проверьте, к тому ли волокну вы подключились, с помощью источника видимого света VFL. Как правило, это устройство выявляет и все обрывы или участки с разбитым волокном (см. Рисунок 13).

Очистите все оптические коннекторы (включая те, что установлены в проходники) по всему сегменту, в котором обнаружен сбой. Не забудьте очистить выходные порты на активном оборудовании. Проверьте состояние торцов на каждом кабеле и шнуре.

На них не должно быть ни грязи, ни царапин, ни сколов. Чтобы избавиться от некоторых типов загрязнений, иногда недостаточно просто протереть торец специальной салфеткой, смоченной в чистящем спирте (см. Рисунок 15).

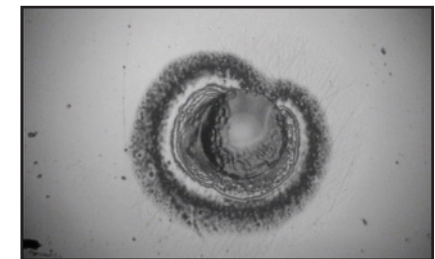


Рисунок 15: Так выглядит стойкое загрязнение на торце коннектора. Очень похоже на грибковую культуру или плесень.

Протестируйте каждый патч-шнур с помощью комплекта OLTS, чтобы проверить затухание. Сначала установите эталонное значение на заведомо хорошем патч-шнуре, и тогда измерение другого патч-шнура должно выдавать результаты потерь, близкие к нулю. Если получено отклонение, то надо выяснить, откуда оно взялось. Если проблема то появляется, то исчезает, тогда попробуйте изгибать и шевелить патч-шнур во время тестирования. Если перемещение шнура влияет на результаты, то проверьте, нет ли обрыва, участка с разбитым волокном или подключения волокон не соосно, а под углом или с просветом между торцами коннекторов. Не изгибайте волокна слишком сильно, не нарушайте требования по радиусу изгиба.

Если есть возможность, воспользуйтесь рефлектометром OTDR, последовательно переходя все ближе и ближе к дальнему концу сегмента, пока не будет найден участок со сбоем. Всегда обращайтесь внимание, если при подключении к другой точке значительно изменились результаты измерения потерь, особенно если это не соответствует ожидаемому изменению, оцененному по конфигурации предыдущего сегмента. Затухание в среде самого кабеля в современных сетях пренебрежимо мало в сравнении с затуханием в точках соединения коннекторов, поэтому ориентируйтесь по значению потерь в 0.75 дБ, предусмотренных стандартом для каждого такого соединения. В кабельном сегменте может быть не один грязный или поврежденный коннектор, а больше. Очистите все торцы коннекторов и проведите тестирование заново, либо используйте рефлектометр, чтобы определить, какие из соединений дают плохие результаты. Патч-шнур или участок в канале могут иметь несоответствующий диаметр ядра. Если вы проверили и убедились, что все патч-шнуры соответствующего типа, то сам сегмент на наличие участков с другим диаметром ядра можно проверить рефлектометром.

Кабельная система может включать в себя плохо выполненную сварную или механическую муфту, или кабель в каком-то месте может быть изогнут слишком сильно. Все подобные ошибки позволяет легко обнаружить рефлектометр. Проверьте трассу, в которой лежит кабель. Нет ли в трассе острых углов или участков, где кабель свился кольцами или резко перегнулся?

Не могут ли хомуты-стяжки вызывать появление микроизгибов?

См. Рисунок 16.

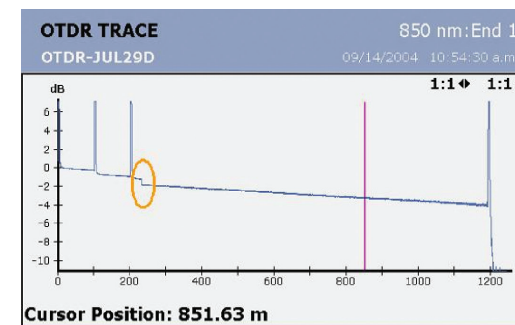


Рисунок 16: Микроизгиб в кабеле приводит к потере мощности, как показано на рефлектограмме (обведено).

Проверьте, не оказался ли случайно в одномодовом сегменте проходник, предназначенный для многомодового? Допуски при изготовлении одномодовых проходников гораздо строже, чем для многомодового, они обеспечивают соосность точнее, и, как следствие, потеря оптической мощности в таком соединении меньше. Кроме того, коннекторы и шнуры рассчитаны на ограниченное количество подключений/отключений. Кабель или шнур, который очень много раз подключался и отключался, начинает болтаться в проходнике, и уже невозможно обеспечить правильное взаимное положение волокон. Такие проблемы позволяет обнаружить тестирование рефлектометром OTDR.

Если сбой относится к одному-единственному устройству, то часто исходной причиной проблемы бывает передающий порт активного оборудования. Возможно, внутри этого порта скопилась грязь, либо мощность, выдаваемая передатчиком, недостаточна. Подключите измеритель мощности из комплекта OLTS к такому передающему порту, а затем сравните полученное значение со значением мощности, которую выдают соседние порты.

## Устранение сбоев на сетевом уровне

### Типичные сбои в сети и жалобы пользователей

Пользователи могут служить своеобразным индикатором состояния вашей сети. Если сеть работает хуже, чем обычно, пользователи не станут держать это в секрете и тут же позвонят специалисту из отдела ИТ. К сожалению, обычно у

пользователей не хватает специальных знаний, чтобы точно описать вам симптомы проблемы. Более того, часто описание, которое дает вам пользователь, больше построено на его воображении, чем на действительных фактах. Всегда помните, что отсутствие технических знаний у пользователей вовсе не основание считать, что проблемы на самом деле не существует. Что-то же заставило пользователя обратиться к вам. Иногда причиной проблемы может быть ошибка самого пользователя, неправильная работа с приложением и оборудованием, а может, просто неправильные представления и ожидания от работы той или иной системы. Небольшой инструктаж, который вы можете провести для такого пользователя, облегчит в будущем жизнь вам обоим.

**Примечание:** *Прежде чем всерьез взяться за устранение проблемы, проверьте, работало ли проверяемое приложение на рабочей станции раньше, был ли раньше доступен сервер и тому подобное. Устранение проблемы и внедрение нового приложения – совершенно разные вещи. Одно дело – восстановить работу того, что было установлено раньше и успешно работало, и совсем другое – внедрить новый сервис, которого раньше не было.*

Далее перечислены три типа жалоб, которые чаще всего поступают от пользователей. Практически все обращения пользователей попадут в ту или иную категорию из перечисленных:

- Не могу войти в сеть
- Сеть постоянно “отваливается”
- Сеть “тормозит”

Некоторые из сбоев связаны с совместно используемыми сетевыми ресурсами (хабами), некоторые – с коммутируемой сетевой средой, а некоторые – с обеими областями.

Для каждого из типов жалоб мы приводим общий порядок действий по устранению проблемы. Каждое действие зависит от результатов одного или большего количества тестов. Конечно, приводимые описания не могут включить все возможные варианты, но зато они предлагают общий подход к устранению проблем и подсказывают, в каком направлении двигаться. Тем не

менее, описания предпринимаемых действий довольно подробны и поясняют, почему тот или иной тест так важен и на что следует обратить внимание. Не воспринимайте это как рекомендацию проводить все тесты, какие только возможно. Здравый смысл поможет выбрать, какие тесты стоит запустить, а какие в данный момент бесполезны. Относитесь к этим действиям как к мысленному списку, в котором вы последовательно вычеркиваете пункты. Проводя диагностику, надо держать в уме все варианты, последовательно исключая из них невозможные. Если для исключения пункта нет оснований, значит, тут и требуется запустить тест.

**Примечание:** *Если в ходе тестирования вы вносите изменения в коллизийные домены, всегда при подключении в новой точке начинайте тестирование коллизийного домена с самого начала.*

### Жалоба: не могу войти в сеть

Перечисленные далее процедуры подразумевают, что соответствующие сервер или служба раньше работали нормально, а вы уже выполнили следующие действия:

- Выполнили холодную перезагрузку рабочей станции, на которой предполагается проблема (именно холодную, поскольку горячая перезагрузка не обнуляет состояние всех адаптерных карт). Установили все необходимые программные исправления (patch-файлы). Помните, что некоторые устройства Plug-and-Play для полной установки требуют двух, а иногда и трех перезагрузок.
- Убедились в том, что на рабочей станции нет сбоев в аппаратной части.
- Проверили, что все сетевые кабели правильно подключены и что с ними тоже нет проблем. Убедились в том, что сетевая карта не отключена, что в подсети правильно назначаются динамические (через DHCP) или статические адреса. Проверили, какие отчеты выдает операционная система по состоянию сетевой карты, отправленным и полученным пакетам (если хоть одно из этих значений нулевое, значит, с этим надо разобраться).
- Проверили, что в последнее время на самой рабочей станции ничего не менялось, никакие изменения не производились на сервере, не менялись настройки, не ставилось новое программное или аппаратное обеспечение.



Проблема с невозможностью войти в сеть обычно состоит в том, что пользователь не может подключиться к серверу или службе. Обычный пользователь не видит разницы между ситуациями, когда рабочая станция не может подключиться к сети или когда она не может получить доступ к конкретному серверу или сетевой службе. Если сравнивать с другими видами сбоев в сети, то с этим справиться относительно просто. Определите, затрагивает ли проблема только данную рабочую станцию или небольшую группу станций (проблема коллизионного домена, включая отдельный порт на коммутаторе) либо большое количество станций (проблема широковещательного домена или даже связанных сетей).

Прежде чем тестировать аппаратную часть, сначала попробуйте войти в сеть сданной станции под собственной учетной записью или попросите пользователя попробовать выполнить действие, вызывающее сбой, с соседней рабочей станции, работающей нормально. Это самый простой способ отличить проблемы, связанные с учетной записью пользователя, от сетевых проблем. Если первый пользователь не может подключиться и с другой станции, значит, надо проверять его учетную запись. Кстати, наблюдение за пользователем в тот момент, когда он пытается выполнить операцию, вызывающую сбой, поможет выяснить, нет ли ошибки в последовательности его действий. В этом случае несколько минут, потраченных на обучение пользователя, избавят вас от проблем в будущем.

Проблемы в коллизионном домене влияют на локальную среду и препятствуют надежной связи с первым же устройством уровня 2 или 3 – или с локальным сервером или службой, к которым вы пытаетесь подключиться. Как правило, все это следствия следующих причин:

- Плохие кабели
- Ошибки или чрезмерный трафик в локальном коллизионном домене
- Заблокированные или неправильно сконфигурированные порты сетевого коммутатора
- Неисправная или неправильно настроенная сетевая карта рабочей станции
- Поврежденные, неправильно настроенные или полученные из ненадежных источников драйвера

Практически все перечисленные сбои в коллизионном домене можно идентифицировать с помощью тестера, подключенного в разрыв между рабочей станцией и портом коммутатора, наблюдающего за ходом холодной перезагрузки и последующей попыткой пользователя войти в сеть. Перезагрузить рабочую станцию нужно потому, что многие проблемы, связанные с операционными системами, крайне сложно, а то и в принципе невозможно воссоздать и точно идентифицировать. Перезагрузка операционной системы позволяет просто избавиться от этих неидентифицируемых ошибок, хотя бы временно.

Многие пользователи имеют как проводную, так и беспроводную сетевые карты, причем активированы обе. Если персональный компьютер пытается использовать беспроводную карту вместо установки проводного соединения, тогда необходимо разбираться с конкретным местоположением рабочей станции, а порой даже с ее ориентацией в пространстве. Во многих беспроводных сетях есть слепые зоны, но часто они очень небольшие, и перемещение компьютера буквально на десяток сантиметров или небольшой поворот его в ту или иную сторону позволяет успешно восстановить беспроводное соединение. Может случиться даже так, что люди, столпившиеся вокруг компьютера, не дают пробиться к нему беспроводному сигналу.

Проблемы в широковещательном домене начинаются только после того, как установлено надежное соединение на MAC-уровне. Типичный пример такого сбоя – невозможность создать логическое подключение через мост. Сюда же относятся и проблемы на сетевом уровне, которые могут препятствовать связи с серверами и маршрутизаторами, входящими в этот широковещательный домен:

- Находящийся в пограничном или сбойном состоянии порт расширения (uplink port), расположенный в любом месте маршрута. Как правило, это следствие использования плохого кабеля.
- Широковещательный шторм или чрезмерный трафик другого типа в широковещательном домене (причем этот трафик вовсе не обязательно наблюдается на локальном порту).
- Ошибки протокола ICMP либо неправильное назначение IP-адресов в локальной подсети; дублирующиеся IP-адреса.

- Сбои серверов или служб DNS и DHCP.
- Рабочая станция или сервер некорректно объявляет маршруты.

Ошибки с присвоением адресов и некоторые другие проблемы может выявить тот же самый тест, что и при проверке коллизионного домена – с помощью прибора, подключаемого в разрыв. Если вы переместились на новое место внутри ширококвещательного домена, то не забудьте сначала протестировать коллизионный домен. Если адрес получен и/или подтверждена его правильность, то может потребоваться либо собрать с помощью анализатора протоколов и посмотреть трассировочный файл, либо использовать программное обеспечение управления сетью, чтобы опросить соответствующие сетевые устройства в ширококвещательном домене.

Проблемы со связанными сетями начинаются только после того, как установлено надежное соединение с маршрутизатором, который ведет за пределы ширококвещательного домена. Сложность возрастает, а уровень доступа часто снижается, если сервер или служба расположены за пределами подключения к глобальной сети, вместо того, чтобы располагаться в соседней локальной сети. Однако симптомы в целом схожие:

- Неустойчивая маршрутизация из-за пограничного или сбойного состояния порта где-то за пределами ширококвещательного домена; возможная причина – плохой кабель.
- Сбои функции отслеживания маршрута Trace Route, малочисленные ответы на запросы Ping.
- Неправильные настройки маршрутизации, включая конфигурацию перенаправления запросов DHCP в тех случаях, когда этот сервер находится за пределами локальной подсети и отдельных виртуальных сетей VLAN.
- Проблемы с виртуальной сетью VPN, включая максимальный размер пакета MTU.
- Проблемы с брандмауэром (firewall) или другими средствами безопасности
- блокирующего типа, включая проблемы с учетными записями или паролями.

Использование запросов Ping и функции отслеживания Trace Route, как правило, позволяет выявить точку, с которой надо начинать работу по устранению неисправности, связанной с невозможностью входа в сеть. Чтобы ускорить процесс, как только вы определили подозрительную удаленную точку, опросите соответствующее сетевое устройство и устройство, предшествующее ему, с помощью системы управления сетью. Либо первое, либо второе устройство будут выдавать ошибки какого-то типа или показывать чрезмерный уровень использования. Большинство проблем снимается при установке надежного сквозного соединения на сетевом уровне. Не забывайте каждый раз при перемещении на новое местоположение начинать с тестирования коллизионного и ширококвещательного домена.

Если ответы на запрос Ping приходят, а подключение все равно дает сбой, попробуйте увеличить размер пакета Ping. Это поможет обнаружить проблему с размером пакетов MTU по маршрутизируемому пути. Виртуальные сети VPN добавляют к пакету заголовок, поэтому пользовательское значение MTU должно быть меньше на соответствующую величину. Если доставка пакетов на сетевом уровне по всему маршруту надежна, то единственное, что вам остается – использовать анализатор протоколов. Необходимо собрать и проанализировать данные в момент установки соединения. Иногда приходится проводить захват пакетов еще и со стороны сервера или службы, чтобы убедиться, что запросы до них доходят, а отклики своевременно отправляются.

Если и отправка запросов Ping, и запуск функции Trace Route проходят успешно, попробуйте использовать для тестируемого порта соединение через Telnet. Успешные соединения по Telnet создают подключение, хотя внешне это может никак не отражаться. Если система отказывается в соединении по Telnet, значит, эта служба недоступна, и тогда точка сбоя становится очевидной.

### **Жалоба: сеть постоянно “отваливается”**

Разрыв подключений могут вызывать те же самые причины, что препятствуют установке соединения, поэтому в список возможных причин включите все то, что перечислено в предыдущей главе. Описанные далее действия подразумевают, что соединение работало корректно, прежде чем возникла проблема, и что вы уже упростили следующие:

- Выполнили холодную перезагрузку рабочей станции, на которой наблюдается проблема (горячая перезагрузка не обнуляет состояние адаптерных карт). То же касается установки всех необходимых программных исправлений (patch- файлов), если они не были установлены в свое время. Кроме того, некоторые устройства Plug-n-Play требуют двукратной, а то и трехкратной перезагрузки, чтобы установиться полностью.
- Убедились, что на рабочей станции нет проблем с аппаратной частью.
- Проверили, что все сетевые кабели правильно подключены и что с ними тоже нет проблем.
- Убедились в том, что сетевая карта не отключена, что в подсети правильно назначаются динамические (через DHCP) или статические адреса. Проверили, какие отчеты выдает операционная система по состоянию сетевой карты, отправленным и полученным пакетам (если хоть одно из этих значений нулевое, значит, с этим надо разобраться).
- Проверили, что в последнее время на самой рабочей станции ничего не менялось, что никакие изменения не производились на сервере, что не менялись службы, настройки, не ставилось новое программное или аппаратное обеспечение.
- Исключили возможные проблемы с распределением памяти на рабочей станции и конфликты программного обеспечения, то есть загрузили минимально необходимое программное обеспечение – лишь то, что нужно для работы тестируемого приложения в сети. Для этого теста необходимо временно отключить антивирусную систему и программное обеспечение по безопасности. Не забудьте снова включить их сразу после выполнения теста.
- Проверили, какие приложения на пользовательской рабочей станции потребляют ресурсы микропроцессора или затормаживают работу компьютера на время, достаточное для истечения счетчиков соединения. Подобными свойствами могут обладать вирусы.

Причин для разрыва соединения может быть только две: это логическая или физическая потеря связности, утрата способности к подключению. Это выражается либо в сбое в кабельном сегменте, либо в сложностях с доступом к сетевому коммутатору, мосту, маршрутизатору или глобальной сети.

Протоколы верхнего уровня используют разнообразные таймеры – счетчики, которые разорвут логическое подключение рабочей станции по истечении заданного времени, если от станции не получен отклик. Таким образом, если пакеты теряются где-то в пути через коммутатор, мост, маршрутизатор или подключение к глобальной сети, то соединение с соответствующим сервером или службой будет утрачено, несмотря на то, что в коллизийном и широковещательном домене все работает без нареканий.

Определите, относится ли проблема только к данной рабочей станции или затрагивает небольшую группу компьютеров (не заключается ли проблема в коллизийном домене, включая конкретный порт сетевого коммутатора), либо затронуто большое количество рабочих станций (тогда проблема касается широковещательного домена или даже затрагивает связанные сети). Опросите соседних пользователей: узнайте, не сталкивались ли они с похожими проблемами. Поинтересуйтесь также, возникает ли проблема в какое-то определенное время дня, появляется ли она после какого-либо запроса, и не производились ли поблизости какие-нибудь работы или события, внешне никак не связанные с возникшей проблемой. Проблемы в коллизийном домене затрагивают локальную среду и препятствуют связи с ближайшим устройством уровня 2 или 3, либо с локальным сервером или службой, которыми вы пытаетесь воспользоваться. Возможны следующие причины:

- Плохие кабели
- Пограничное состояние или некорректная работа сетевой карты рабочей станции либо порта в сетевом коммутаторе или хабе
- Ошибки или чрезмерный трафик в локальном коллизийном домене
- Несоответствие настроек дуплекса
- Шум от электрического оборудования и других внешних источников

Многие сбои в коллизийном домене, связанные с утратой соединения с сетью, можно идентифицировать, если отключить от сети рабочую станцию пользователя и подключить вместо нее тестер. Подключившись к тому же самому кабельному сегменту, который обычно задействует пользователь, попробуйте войти в сеть и обратиться к соответствующему серверу или службе. Затем подключите рабочую станцию пользователя через тестер транзитом

и оставьте прибор наблюдать за состоянием подключения. Еще лучше поставить анализатор протоколов для сбора трафика и сетевой статистики. Проинструктируйте пользователя, какую информацию он должен заметить на тестере сразу же после очередного появления сбоя, или научите его останавливать сбор трафика и сохранять уже собранную информацию для последующего анализа.

Многие пользователи имеют как проводную, так и беспроводную сетевые карты, причем активированы обе. Если персональный компьютер пытается использовать беспроводную карту вместо установки проводного соединения, тогда необходимо разбираться с конкретным местоположением рабочей станции, а порой даже с ее ориентацией в пространстве. Во многих беспроводных сетях есть слепые зоны, но часто они очень небольшие, и перемещение компьютера буквально на десяток сантиметров или небольшой поворот его в ту или иную сторону позволяет успешно восстановить беспроводное соединение. Может случиться даже так, что люди, столпившиеся вокруг компьютера, не дают пробиться к нему беспроводному сигналу.

Проблемы в ширококвещательном домене начинаются только после того, как установлено надежное соединение на MAC-уровне. Типичный пример такого сбоя – невозможность создать логическое подключение через мост. Сюда же относятся и проблемы на сетевом уровне, которые могут препятствовать связи станции с серверами и маршрутизаторами, входящими в этот же ширококвещательный домен:

- Находящийся в пограничном или сбойном состоянии порт расширения (uplink port), расположенный в любом месте маршрута. Как правило, это следствие использования плохого кабеля.
- Проблемы со связующим деревом в сети – возможно, также из-за плохого кабеля.
- Широковещательный шторм или чрезмерный трафик другого типа в ширококвещательном домене (причем этот трафик вовсе не обязательно наблюдается на локальном порту).
- Несоответствия в настройках дуплекса на каком-то участке маршрута.
- Дублирующиеся IP-адреса.
- Рабочая станция или сервер некорректно объявляет маршруты.

Попробуйте непрерывно отправлять запросы Ping на локальный маршрутизатор, чтобы проверить, не теряются ли пакеты в ширококвещательном домене. С помощью системы управления сетью опросите сетевые устройства, находящиеся по пути от пользовательского подключения до маршрутизатора, сервера или службы. Обратите внимание на ошибки или высокий уровень использования, которые отмечаются в тот момент, когда соединение обрывается. Подключите к сети рабочую станцию пользователя и анализатор протоколов, понаблюдайте за сетевым трафиком или осуществите захват пакетов трафика, относящегося к серверу или службе, с которыми наблюдаются проблемы, для последующего анализа. Если проблема то появляется, то исчезает, тогда поставьте анализатор протоколов для сбора трафика за определенный период времени. Научите пользователя останавливать сбор данных – пусть сделает это сразу же, как только сбой появится снова. Такие проблемы довольно часто то появляются, то пропадают, поэтому без привлечения пользователя к процессу вам не обойтись. Либо он должен немедленно позвать вас – прямо в тот момент, когда появился сбой – либо ему придется помочь вам собрать данные о том, что происходит перед появлением.

Проблемы в связанных сетях появляются после того, как установлено надежное соединение с маршрутизатором, ведущим за пределы ширококвещательного домена. Обеспечить надежный доступ к интернет-серверам и службам сложнее, чем добиться надежного соединения с серверами и службами в соседних сетях, поскольку у интернет-провайдера могут быть свои сбои, и не во всех своих проблемах он вам признается. Есть несколько факторов, которые вы, как локальный сетевой специалист, все равно контролировать не сможете:

- Неустойчивая маршрутизация по вине пограничного состояния порта или соединения на каком-то участке за пределами ширококвещательного домена. Возможная причина – плохой кабель.
- Чрезмерный трафик для низкоскоростного локального или глобального подключения. Возможно, трафик в результате отвергается, либо превышает емкость буфера.
- Варьируется время отклика на запросы Ping и функции Trace Route.
- Перегрузка сервера или службы.

Отправка запросов Ping и функция Trace Route позволяют найти точку, с которой следует начинать устранение проблемы с постоянной утратой сетевого соединения. Если проблема то появляется, то исчезает или ее трудно уловить, то необходимо запускать тесты на непрерывное выполнение. Если какое-то удаленное подключение кажется вам подозрительным, ускорьте процесс, используя систему управления сетью для того, чтобы опросить соответствующее сетевое устройство, а также устройство, ему предшествующее. Либо то, либо другое покажет ошибки какого-то типа или чрезмерный уровень использования. Выполните тестирование пропускной способности, чтобы проверить производительность по маршруту от пользовательского подключения до сервера или службы. С помощью системы управления сетью можно вести мониторинг состояния сети в тот момент, пока проводится тестирование пропускной способности, чтобы выяснить, нет ли ошибок. Практически всегда установка надежного сквозного соединения на сетевом уровне полностью устраняет проблему с утратой сетевого подключения. В ходе диагностики не забывайте повторять тесты коллизионного и широковещательного доменов каждый раз, когда вы перемещаетесь на новое место – это позволит раз за разом сужать зону поисков. Если же сквозное соединение на сетевом уровне установлено надежно, а проблема не исчезла, то единственное, что вам может помочь – установка

### Жалоба: сеть “тормозит”

Низкая производительность сети может быть вызвана теми же факторами, что препятствуют установке соединения или разрывают уже установленное – эти причины и описания состояний сети приведены в двух предыдущих разделах.

Описанные далее процедуры подразумевают, что до возникновения проблемы сетевое подключение работало корректно, и что вы уже проделали следующее:

- Проверили, что в недавнем прошлом ничего не изменялось на самой рабочей станции, на сервере, в службе, которые могут быть причиной возникшей проблемы – не менялись настройки, не устанавливалось новое программное и аппаратное обеспечение.
- Исключили проблемы с распределением памяти рабочей станции и

программные конфликты, загрузив лишь то программное обеспечение, которое минимально необходимо для работы тестируемого приложения в сети. Для такого тестирования необходимо отключить все антивирусные средства и системы безопасности. Не забудьте снова активировать их сразу же после тестирования.

- Выполнили проверку на вирусы рабочей станции и проверили все приложения, которые отнимают несоразмерно много ресурсов микропроцессора или затормаживают работу системы на время, достаточное для срабатывания таймеров, отсчитывающих время установки соединения.

Самые частые причины медленной или заторможенной работы сети – перегрузка серверов или их недостаточная мощность, использование несоответствующих настроек сетевых коммутаторов и маршрутизаторов, перегрузка сетевого трафика (пробка) в сегменте с низкой пропускной способностью, постоянная потеря пакетов. Сложные, многоуровневые приложения могут страдать от недостаточной производительности в тех случаях, когда любой из серверов в иерархии уровней вызывает задержки. Исследование поведения таких многоуровневых приложений может быть очень сложным; часто даже не удается составить полную схему их работы, в которой учитывались бы все взаимные влияния. Определите, относится ли проблема только к одной рабочей станции или небольшой группе станций (проблема коллизионного домена, включая отдельный порт на сетевом коммутаторе), либо к большому количеству станций (проблема широковещательного домена или даже связанных сетей). Опросите соседних пользователей: выясните, не сталкивались ли они с похожими сбоями в сети в целом или с отдельными приложениями. Уточните, в какое время дня появляется сбой, не происходит ли это в ответ на выполнение какого-либо запроса, не наблюдались ли еще какие-либо события или действия в сети, которые внешне никак не связаны с имеющимся сбоем.

Проблемы коллизионного домена воздействуют на локальную среду и препятствуют установке связи с первым же сетевым устройством уровня 2 или 3 – либо с локальным сервером или службой, к которым вы пытаетесь обратиться. Как правило, это следствие следующих причин:

- Плохие кабели
- Пограничное состояние или некорректная работа сетевой карты рабочей станции либо порта в сетевом коммутаторе или хабе
- Ошибки или чрезмерный трафик в локальном коллизийном домене
- Несоответствие настроек дуплекса
- Шум от электрического оборудования и других внешних источников

Большинство проблем коллизийного домена, связанных с медленной работой сети, можно распознать путем отключения рабочей станции пользователя – вместо нее надо подключить тестер. Используя тот же кабельный сегмент, что при работе задействует пользователь, попробуйте установить соединение с сетью и получить доступ к серверу или службе, с которыми наблюдаются сложности. Затем подключите рабочую станцию пользователя транзитом через тестер, чтобы прибор мог наблюдать за событиями в сегменте, либо установите анализатор протоколов для сборки трафика и сетевой статистики. Расскажите пользователю, какую информацию ему надо будет увидеть на приборе в тот момент, когда сбой появится снова, и научите его останавливать сбор трафика и сохранять собранные данные для последующего анализа.

Приложения, критически важные для работы предприятия, не следует реализовывать через беспроводную сеть: это может привести к большим сложностям в работе сети, а полоса пропускания может оказаться недостаточно широкой. Проверьте, какая сетевая карта используется для доступа к тому серверу и службе, с которыми наблюдаются проблемы. Если какие-то соображения требуют, чтобы сеть была именно беспроводной, тогда необходимо использовать анализатор спектра, чтобы проверить, нет ли поблизости постоянных или переменных источников шума, а также устройств, занимающих ту же полосу частот, что и беспроводная сеть.

Проблемы с широкополосным доменом проявляются только после того, как установлено надежное соединение на MAC-уровне. Типичный пример такого сбоя – невозможность создать логическое подключение через мост. Сюда же относятся и проблемы на сетевом уровне, которые могут препятствовать связи с серверами и маршрутизаторами, входящими в этот же широкополосный домен:

- Находящийся в пограничном или сбойном состоянии порт расширения (uplink port), расположенный в любом месте маршрута. Как правило, это следствие использования плохого кабеля.
- Проблемы со связующим деревом в сети – возможно, также из-за плохого кабеля.
- Широковещательный шторм или чрезмерный трафик другого типа в широкополосном домене (причем этот трафик вовсе не обязательно наблюдается на локальном порту).
- Несоответствия в настройках дуплекса для каких-то портов, входящих в маршрут.
- Дублирующиеся IP-адреса.
- Рабочая станция или сервер некорректно объявляет маршруты.

Отправка к локальному маршрутизатору непрерывных запросов Ping позволит проверить, не теряются ли в широкополосном домене пакеты. С помощью системы управления сетью следует опросить сетевые устройства по всему маршруту передачи сигналов от пользовательского подключения к маршрутизатору, серверу или службе. При этом надо обращать внимание на ошибки или высокую степень использования, которые имеют место примерно в то время, когда происходит потеря соединения. Выполните тестирование пропускной способности участков сети до различных точек в широкополосном домене – при этом надо использовать те же порты расширения, по которым идет проверяемый сетевой трафик. Обратите внимание на все несообразные значения, полученные при тестировании – они могут свидетельствовать о несоответствиях в настройках дуплекса и других проблемах, вызванных такими ошибками. Снова подключите рабочую станцию пользователя к сети и поставьте анализатор протоколов для мониторинга или сбора трафика, относящегося к серверу или службе, с которыми наблюдаются проблемы. Особое внимание надо обратить на ошибки протокола ICMP и повторные передачи по протоколу TCP. Если проблема с низкой пропускной способностью то появляется, то исчезает, тогда необходимо поставить анализатор протоколов на сбор данных за определенный период времени.

Проблемы в связанных сетях появляются после того, как установлено надежное соединение с маршрутизатором, ведущим за пределы широкополосного

домена. Если пропускная способность постоянно слишком низкая, значит, причина, скорее всего, кроется в несоответствующих настройках, недостаточных характеристиках сети на каком-то участке и тому подобным системным факторам. Если пропускная способность сильно варьируется и низкая далеко не всегда, то, скорее всего, причиной является какая-либо ошибка или влияние трафика, поступающего от каких-то иных источников.

- Неустойчивая маршрутизация по вине пограничного состояния порта или соединения на каком-то участке за пределами широковещательного домена. Возможная причина – плохой кабель
- Чрезмерный трафик для низкоскоростного локального или глобального подключения. Возможно, трафик в результате отвергается, либо превышает емкость буфера.
- Варьируется время отклика на запросы Ping и функции Trace Route.
- Перегружены соответствующие сервер или служба.

Отправка запросов Ping и функция Trace Route позволяют найти точку, с которой следует начинать устранение проблемы, выражающейся в медленной работе сети. Если проблема то появляется, то исчезает, или ее трудно уловить, то необходимо запускать тесты на непрерывное выполнение. Если какое-то удаленное подключение кажется вам подозрительным, можно ускорить процесс, используя систему управления сетью для того, чтобы опросить соответствующее сетевое устройство, а также устройство, находящееся непосредственно перед ним. Либо то, либо другое покажет ошибки какого-то типа или чрезмерный уровень использования. Выполните тестирование пропускной способности, чтобы проверить производительность по маршруту от пользовательского подключения до сервера или службы. С помощью системы управления сетью можно вести мониторинг состояния сети в тот момент, пока идет тестирование пропускной способности, чтобы выяснить, нет ли ошибок. Практически всегда установка надежного сквозного соединения на сетевом уровне полностью устраняет проблему с утратой сетевого подключения. Выполняя диагностику, не забывайте повторять тесты коллизий и широковещательного доменов каждый раз, когда вы перемещаетесь на новое место. Если сквозное соединение на сетевом уровне

установлено надежно, а проблема не исчезает, то единственное, что вам остается предпринять – установить анализатор

## Устранение проблем с сетевыми коммутаторами

### Типичные сбои сетевых коммутаторов

Проблемы, что встречаются в коммутируемой сетевой среде, носят почти тот же характер, что и сбои в среде совместного использования ресурсов. Вопросы возникают те же самые: Что случилось? Кто и что сделал? Во что это обойдется? Принципиальная разница только в том, что в коммутируемой среде ответы всегда должны относиться к конкретному порту.

В коммутируемой среде надо всегда учитывать следующие факторы:

- Насколько интенсивно используется каждый порт?
- Каким путем вы определяете и отслеживаете источник ошибок?
- Что является источником широковещательного шторма?
- Правильно ли работают таблицы маршрутизации?
- Какие рабочие станции относятся к этому порту?
- Накладывает ли коммутатор какие-то ограничения по скорости на какие-либо протоколы или порты?
- Относится ли этот порт к виртуальной сети VLAN, и если да, то относится ли сервер или служба к той же самой виртуальной сети?

С чего следует начинать, когда вы получаете сообщение о том, что в коммутируемой сети возникла какая-то проблема? Как правило, в сбое виновен не сам коммутатор, а невозможность “видеть” сеть сквозь него. Проблемы начинаются на втором уровне сетевой модели OSI при установке коммутатором соединения, а использование виртуальных сетей VLAN и других функций, начиная с сетевого уровня 3 и выше (включая маршрутизацию), может дополнительно осложнить ситуацию. Если в сети используются продвинутые возможности коммутации, такие как маршрутизация на уровне 4 и выше и балансировка загрузки, то для проведения диагностики специалист должен отлично разбираться во всех тонкостях настройки коммутаторов.

Устанавливая в сети коммутатор, фактически вы создаете отдельный коллизийный домен для каждого порта – именно таков принцип работы коммутаторов. Если к порту подключить хаб (чьи ресурсы используются совместно), тогда коллизийный домен может увеличиться до максимального размера, который допускает данная конфигурация сети Ethernet. Поскольку коммутаторное оборудование постоянно дешевеет, большинство новых сетей предусматривают подключение к каждому порту только одной рабочей станции, и в этом случае к коллизийному домену относится единственный кабельный сегмент.

Коммутатор, в свою очередь, является частью отдельного ширококестельного домена, причем в домен может входить ряд коммутаторов, объединенных в каскад или подключенных параллельно. Если в сети используются функции уровня 3 модели OSI, то создается большое количество ширококестельных доменов, равное количеству виртуальных сетей VLAN. В предельном случае, если, конечно, сам коммутатор допускает это, каждый порт может быть сконфигурирован как отдельный ширококестельный домен. Такую конфигурацию можно с полным на то основанием назвать прямой коммутацией на рабочее место пользователя. Если для каждого порта создан собственный ширококестельный домен, то возможности диагностики сильно ограничиваются. Назначение отдельного ширококестельного домена каждому порту к тому же требует от коммутатора распределения всего сетевого трафика, на что расходуется значительная часть ресурсов центрального процессора. В реальной жизни очень трудно представить себе сеть, которая сможет обрабатывать и перенаправлять отдельно каждый запрос и каждый отклик. Такой конфигурации следует избегать, если только у вас нет очень веских оснований для создания именно такой структуры сети.

К сожалению, есть еще одна, очень распространенная разновидность такой конфигурации, которая заключается в том, что в одну подсеть или ширококестельный домен заносятся все сервера, а пользователи распределены по определенному количеству других подсетей или ширококестельных доменов. Теоретически в такой конфигурации все запросы тоже должны проходить маршрутизацию. Если ради удобства обслуживания вам необходимо разместить все сервера в одном помещении

(серверной), то распределите их по нескольким виртуальным сетям VLAN. Пользователей, которые обращаются к каждому конкретному серверу, следует отнести к той же виртуальной сети VLAN. Такая конфигурация позволит матричному переключателю использовать для обычного трафика соединение через уровень 2 модели OSI, в то время как маршрутизироваться будут только нетипичные или редкие запросы. Если сервер обслуживает более одного сообщества пользователей, то установите в него дополнительные сетевые карты, чтобы поддерживать связь с пользователями на уровне 2 модели OSI.

## Точное распознавание проблемы

Чуть ли не единственный по-настоящему эффективный метод диагностики коммутируемых сетей – запрос информации о поведении сети у самого коммутатора. Такие данные обычно запрашиваются по сети с помощью протокола SNMP либо их получают через консольный порт коммутатора. Разумеется, прямое подключение к консольному порту менее удобно, поскольку для его выполнения вам придется физически приближаться к каждому коммутатору в сети. Можно сэкономить силы, если установить терминальные сервера, которые будут подключаться к консольным портам. Тем не менее, практически всегда предпочтительный метод – использовать протокол SNMP, поскольку он позволяет отправлять внутренние запросы из любой точки сети и для этого не нужно никакое дополнительное оборудование. Если вы используете систему управления сетью, то можно настроить коммутатор таким образом, чтобы он сам отправлял незапрашиваемый ответ – уведомление SNMP trap – каждый раз, когда уровень использования, количество ошибок или какой-то другой параметр превышает установленное пороговое значение. Причину превышения порогового значения затем можно выяснить с помощью системы управления сетью или средств наблюдения. Существует ряд проблем, которые успешно определяются через запрос к коммутатору, но есть и проблемы, для которых такой способ бесполезен. Опрос коммутатора может служить.

Другая стратегия – дожидаться, пока от пользователей начнут поступать жалобы. Во многих сетях применяется именно такой подход. Его не стоит недооценивать из-за его внешней простоты – на самом деле он очень



эффективен. Пользователи очень чутко реагируют на состояние сети, несмотря на то, что их представление о ее работе больше основано на подсознании, чем на логических заключениях. Как только пользователь замечает малейшее ухудшение в работе сети, он тут же обращается с жалобой в отдел ИТ или к системному администратору. Получив такой сигнал от пользователя, можно начать работу по поиску и устранению неисправности с рабочего места этого пользователя. Такой подход называется реактивным, поскольку он представляет собой реагирование на уже случившийся сбой. Напротив, профилактические методы направлены на то, чтобы не допустить возникновения сбоя. Для этого проводится регулярный опрос коммутаторов, мониторинг качества трафика на каждом порту коммутатора, в каждом сегменте. Когда проблема уже появилась (поступила жалоба либо сбой обнаружен вами), можно воспользоваться разными методами устранения, каждый из которых имеет свои плюсы и минусы.

## Методы устранения коммутаторных сбоев

Существует как минимум десять основных подходов, позволяющих получить информацию о работе коммутатора. Каждый метод предполагает свой порядок действий, в каждом есть свои положительные и отрицательные стороны. Как это всегда бывает, единого рецепта на все случаи жизни просто не существует. Выбирать подходящее решение из разных вариантов можно, прежде всего, исходя из доступности ресурсов (какими средствами можно воспользоваться сразу, потому что они уже установлены); учитывая опыт специалиста, проводящего работы; оценивая последствия для работы сети (приостановка, перерывы в работе) при использовании того или иного метода.

И даже сочетание всех методов не позволяет наблюдать за коммутируемой сетью в таких подробностях, как это можно было делать в сетях, построенных на хабах. Увидеть и отследить абсолютно весь трафик и все ошибки, относящиеся к коммутатору, практически невозможно. Большинство диагностических процедур подразумевает, что трафик проходит между рабочей станцией и соответствующим сервером или проходит через порт расширения uplink. Если между двумя рабочими станциями установлено одноранговое (пиринговое) соединение, то трафик не проходит ни через uplink-

порт, ни через какой-либо другой порт коммутатора. Такие соединения вообще редко обнаруживаются, если только не искать их специально. Обычно ошибки заканчиваются портом коммутатора и дальше не идут, однако для некоторых их типов и определенных настроек коммутаторов возможна маршрутизация ошибок по сети дальше. Если она имеет место, то практически всегда на один-единственный порт.

Для простоты представим себе минимальный сегмент сети: сервер, подключенный к коммутатору, как показано на Рисунке 17. В некоторых случаях будет предполагаться, что пользователи, испытывающие проблемы, подключены к тому же самому коммутатору; в других случаях пользователи будут пытаться получить

доступ к серверу через порт расширения uplink, ведущий либо к другому коммутатору, либо к маршрутизатору. Диагностика начинается в ответ на жалобу пользователя, что сеть при обращении к серверу работает очень медленно. К сожалению,

такое описание проблемы практически ничего не говорит специалисту ИТ. Если вы подозреваете не обычный сбой, а взлом системы защиты, причем предполагаются последствия юридического характера, то необходимо принять дополнительные меры, чтобы обеспечить достоверность и юридическую силу собираемых данных.

**Примечание:** Информация, относящаяся сразу к нескольким методам, будет приводиться в описании того метода, в котором она используется наиболее полно и эффективно. Большая часть описаний относится также к методам, отличным от того, которому посвящен раздел, поскольку их применение может приводить к совершенно другим результатам.

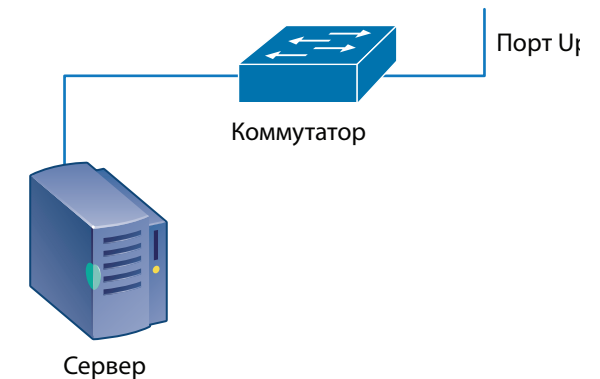


Рисунок 17: Максимально упрощенное представление коммутации.

## Метод 1: Получить консольный доступ к коммутатору

Получить доступ к настройкам коммутатора можно разными способами, включая следующие:

- Войти в систему с помощью сеанса TELNET
- Войти в систему с помощью сеанса SSH
- Войти в систему через веб-сессия
- Подключиться через последовательный порт коммутатора

Некоторые коммутаторы обладают рядом встроенных диагностических средств, которыми можно воспользоваться, но при этом надо помнить, что их функциональные возможности сильно разнятся в зависимости от производителя и модели коммутатора. Продвинутое команды операционной системы позволяют провести более глубокий анализ маршрутизируемого трафика, однако имеющийся интерфейс нельзя назвать дружелюбным пользователю. Чтобы успешно применить некоторые такие функции, надо обладать значительным опытом и глубоким знанием теории сетей.

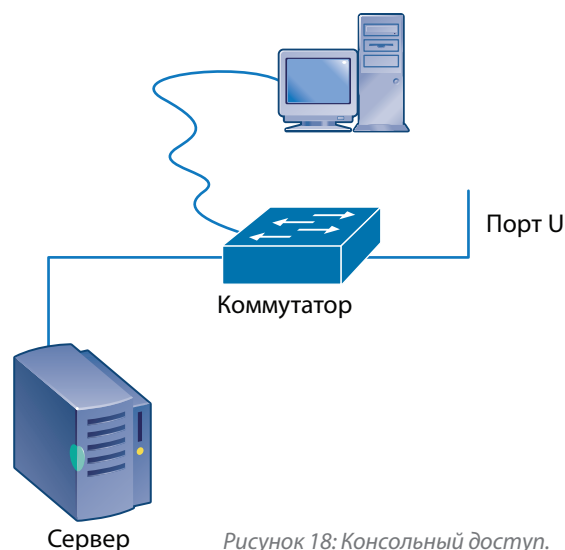


Рисунок 18: Консольный доступ.

### Плюсы

Консольный доступ – очень эффективный метод диагностики, он широко распространен и используется чаще других. Существенная доля сбоев в сети приходится именно на настройки коммутаторов и действия, выполняемые коммутатором в соответствии с этими настройками. Получить доступ к консоли управления коммутатором можно практически всегда, либо одним, либо

другим методом из выше перечисленных. Почти повсеместное использование беспроводных сервисов и функций передачи данных, предоставляемых мобильной связью, позволяют управлять сетью практически из любой точки планеты. Если настроить систему управления сетью на отправку уведомлений на мобильные устройства, то о возникновении сбоя вы узнаете сразу же.

Если сбой действительно относится к настройкам, то методом консольного доступа безусловно можно устранить его.

### Минусы

Старшие системные администраторы и другие ведущие сотрудники отделов ИТ, обладающие паролями для доступа к настройкам коммутаторов, настолько полагаются на метод консольного доступа при проведении диагностики, что никакие другие варианты даже не приходят им в голову, пока этот метод себя полностью не исчерпает. Между тем, отказ от использования прочих подходов может существенно задержать устранение сбоя и дополнительно усложнить ситуацию. С помощью только консольного доступа можно обнаружить и устранить не все сетевые проблемы, а только их часть.

Обычные команды, подаваемые с помощью консольного доступа, позволяют определить средние уровни использования сегментов, но практически не дают информации о конкретных видах сетевой активности или исходной причине сбоя того или иного протокола. Более того, информация, доступная с помощью консольного доступа, характеризует скорее то, как сеть должна работать, а не то, как она действительно работает; такие данные мало помогут в случае, например, некорректной работы части коммутатора. Просмотр файлов

конфигурации не позволит выявить программные ошибки в операционной системе или неточности и упущения в настройках. В некоторых случаях настройки по умолчанию даже нельзя узнать, вывода дампа настроек на экран, поскольку выводятся только изменения, сделанные относительно умолчаний. Между тем, причиной проблем с производительностью сети вполне могут быть именно настройки по умолчанию.

Данные по настройкам полезны для того, чтобы в общих чертах выяснить,

работает ли коммутатор так, как должен работать. Однако для проверки конфигурации и производительности сети нужно применять иные методы диагностики коммутаторов – возможно, даже не один, а несколько.

Если речь идет о работе критически важных участков сети, то консольный доступ из удаленных точек может быть запрещен, либо разрешен только из конкретной группы адресов, которые жестко прописаны. Обычно пароли для доступа к коммутаторам не раздают рядовому персоналу отделов ИТ и технической поддержки, и такие специалисты просто не имеют возможности использовать консольный доступ. Инженеры более высокого уровня, располагающие паролями, как правило, уже не участвуют в ежедневной работе по устранению сбоев в сетях. А теперь представьте себе, каким образом специалист, в прямые обязанности которого входит ежедневное поддержание производительности сети, может эффективно работать, если консольный доступ ему запрещен.

## Метод 2: Подключиться к свободному порту

Самый простой метод диагностики состоит в том, чтобы подключить специальный прибор (например, анализатор протоколов) к любому свободному порту коммутатора.

Подключение к свободному порту коммутатора позволяет прибору получить доступ к соответствующему широковещательному домену, причем это никоим образом не влияет на работу всех остальных участков сети. Прибор получает абсолютно такой же доступ к широковещательному домену, как все остальные рабочие станции.

К сожалению, невозможно сходу определить, относится ли свободный порт к той же самой виртуальной сети VLAN (широковещательному

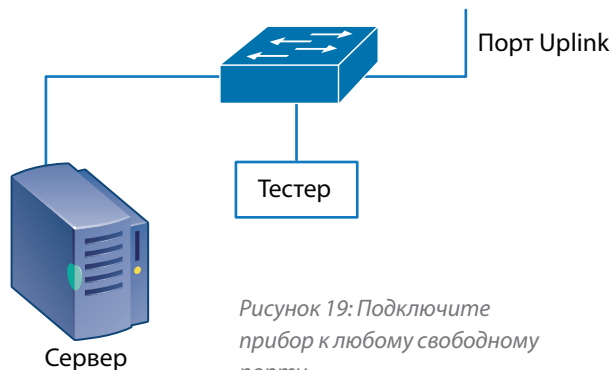


Рисунок 19: Подключите прибор к любому свободному порту.

домену), что и точка, где наблюдается проблема – для этого необходим консольный доступ. Альтернативный вариант – обратиться к документации на сеть, однако она крайне редко содержит такие подробности, а информация, приведенная в ней, далеко не всегда актуальна и соответствует текущему положению дел. Учитывайте также, что даже если ваша сетевая документация соответствует действительности, возникшая проблема может все равно свести к нулю ее ценность, поскольку будет относиться к ошибке в конфигурации или кабельной системе – ошибке, не отраженной в документации по определению.

## Пассивный мониторинг

### Плюсы

Для пассивного мониторинга не нужны ни специальные настройки, ни усилия. Если вы достаточно терпеливы, то рано или поздно вам удастся набрать трафик практически от всех сетевых устройств, относящихся к широковещательному домену. Так произойдет потому, что таблица адресов подвержена старению и периодически обновляется, а также в силу базовых правил установки соединений через мост.

### Минусы

Пассивный мониторинг предполагает, что устройство, установленное для наблюдения, не ведет никакой передачи. Если не отправляются запросы, то это приводит к двум прямым следствиям: коммутатор никогда ничего не узнает о MAC-адресе устройства для мониторинга, а отсутствие запросов означает также отсутствие откликов на них. В абсолютном большинстве случаев в нормальной сети при пассивном мониторинге вы увидите только очень маленький трафик, причем состоять он будет в основном из широковещательных служебных уведомлений или сообщений таких широковещательных протоколов, как ARP.

Подключение к сети такого тестера может очень помочь в сборе информации при поиске уязвимых мест в защите сети. Получаемый случайным образом незапрашиваемый трафик может сам по себе представлять уязвимость в системе безопасности. Безопасные сети всегда принимают меры при обнаружении на порту коммутатора активного соединения, когда устройство на дальнем конце не имеет MAC-адреса или его адрес не установлен.

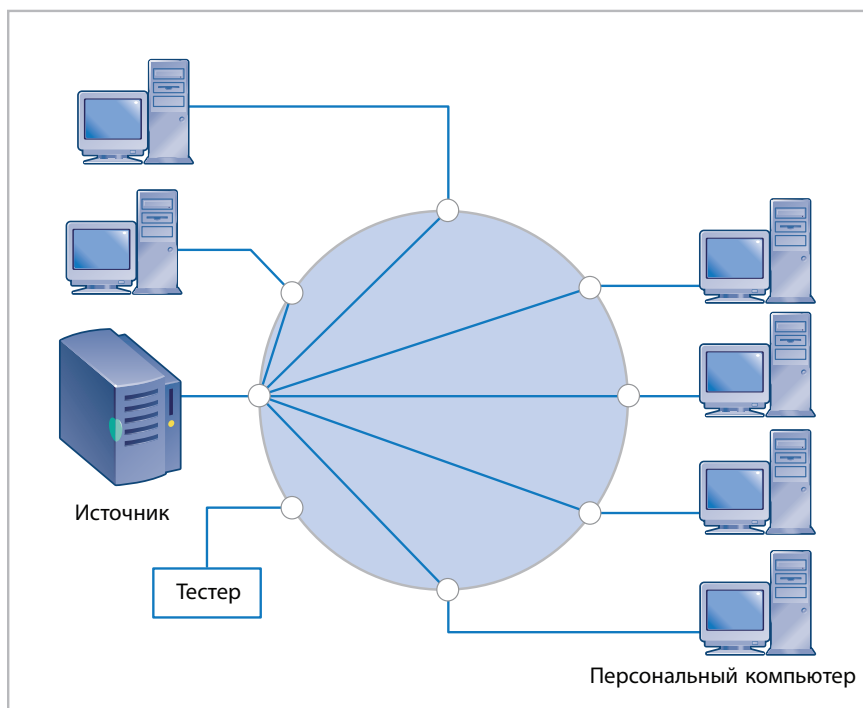


Рисунок 20: Коммутаторы маршрутизируют трафик от источника к порту назначения.

Как показано на Рисунке 20, на прибор, поставленный для мониторинга, поступает очень мало трафика. Тестер может получать всего несколько пакетов в секунду вместо тех тысяч в секунду, которые передаются между рабочими станциями и сервером.

## Активный мониторинг

### Плюсы

Активный мониторинг, а точнее, сочетание активного и пассивного мониторинга – прекрасный метод, позволяющий быстро получить список станций в широковещательном домене, а также представление о том, какие сервисы могут быть доступны этим станциям.

Этот метод заодно помогает идентифицировать многие распространенные сетевые проблемы, включая дублирующиеся IP-адреса, неправильно настроенные рабочие станции и некорректно работающие DHCP-серверы и маршрутизаторы.

### Минусы

Активный опрос устройств в широковещательном домене и запрос трафика, конечно, очень полезны для обследования сети и поиска прочих типов сбоев, однако они практически ничем не помогут при проблемах с медленной работой сети.

Активное обследование обнаруживает устройства в сети, но не определяет, чтои как они делают.

## Знания, необходимые для использования Метода 2

### Поведение мостов

Коммутатор, который мы будем рассматривать в качестве многопортового моста, направляет на порт, на котором мы ведем мониторинг, лишь крохотную долю трафика. Это обычное поведение со стороны устройства-моста, поскольку оно специально построено таким образом, чтобы избежать отправки избыточного трафика на порты, которым он не предназначен. Существует несколько технологий, используемых для маршрутизации через мосты. Хотя некоторые коммутаторы позволяют выбрать и настроить ту или иную технологию, тем не менее, в сетях Ethernet по умолчанию применяется технология прозрачной маршрутизации (transparent bridging).

При прозрачной маршрутизации место, где располагается устройство-адресат, должен определять сам мост. Для этого все пакеты с адресатом, расположенным неизвестно где, направляются всем портам, за исключением порта-отправителя. Как только станция-адресат откликается на запрос, тут же все задействованные мосты узнают, какому порту следует пересылать последующий трафик, и шлют его уже только этому одному адресату. Такая организация работы верна и для отдельно взятого коммутатора, и для каждого из коммутаторов, установленных параллельно либо собранных в каскад или любую другую иерархическую конфигурацию.

Этот метод можно немного упростить, если коммутатор будет записывать MAC-адреса источников любого трафика и увязывать их с конкретными портами. Не имеет значения, обслуживает ли этот порт отдельную рабочую станцию, хаб или является портом расширения (uplink) и ведет к другому коммутатору. Любой

трафик, предназначенный такому-то MAC-адресу, направляется на этот порт и никуда более. До тех пор, пока коммутатор не обнаружит пакет, содержащий данный MAC-адрес в поле источника, у него не будет соответствующей записи в таблице маршрутизации для трафика на этот MAC-адрес уже в качестве получателя, и, следовательно, до тех пор все пакеты такого трафика будут рассылаться всем получателям.

Поскольку нет никакой гарантии, что данный MAC-адрес будет навечно увязан с данным портом, то для каждой записи в таблице маршрутизации установлен период устаревания. Если запись с адресом, занесенная в таблицу, устарела, то следующий пакет, направленный на MAC-адрес этой записи, будет снова отправлен всем получателям. Период устаревания зависит от настроек по умолчанию, принятых производителем коммутатора, от конфигурации коммутатора, статических записей в таблице и других подобных факторов. Функция роуминга для беспроводных устройств основана на том же принципе устаревания, хотя использует и другие технологии для оперативного обновления таблиц маршрутизации.

Итак, трафик, направленный на порт на Рисунке 20, к которому мы подключили прибор для мониторинга, будет практически полностью состоять только из широковещательного трафика и многоадресных рассылок, и лишь изредка в нем будут появляться пакеты, рассылаемые всем, поскольку местоположение адресата неизвестно. Такие пакеты, скорее всего, будут следствием устаревания таблиц маршрутизации на устройствах-мостах, либо результатом работы таких широковещательных протоколов как ARP, и лишь изредка свидетельством действительно неизвестного адресата.

Многие неопытные сетевые специалисты замечали в процентном распределении трафика практически полное доминирование широковещательных рассылок (почти 100%), но при этом не обращали внимания на то, что уровень использования в сегменте чрезвычайно низкий. И тогда они делали вывод о том, что имеет место широковещательный шторм (что совершенно неправильно), либо заключали, что такой высокий процент широковещательного трафика является нормальным состоянием для данной сети (что тоже совершенно неверно).

### Контроль доступа

С каждым днем становится все популярнее контроль доступа по протоколу 802.1X, который поддерживает различные методы идентификации (аутентификации) для предоставления доступа к главной сети. Любая станция, подключенная к коммутатору, сначала должна пройти процедуру аутентификации, и лишь затем она будет допущена в широковещательный домен. Есть много способов организовать работу таким образом, включая полную блокировку станции; перевод ее в состояние “удержания” в отдельном широковещательном домене до тех пор, пока не будет успешно пройдена процедура аутентификации; размещение станции в незащищенном широковещательном домене с интернет-доступом, но без доступа к локальной сети до тех пор, пока не пройдена аутентификация. Внедрение протокола 802.1X приводит к определенным сложностям при пассивном мониторинге. Вот только некоторые из них:

Полное отсутствие трафика. Коммутатор не направляет на порт вообще никакого трафика, пока станция не создаст запрос на аутентификацию, после чего в сети будет виден только трафик, связанный с прохождением аутентификации, пока она успешно не завершится.

Очень маленький трафик. Пока станция не прошла аутентификацию, для наблюдения доступна лишь малая доля трафика. Отдельные типы трафика, которые можно увидеть, зависят от различных факторов и будут разными в разных сетях, а может быть, даже разными внутри одной сети – для разных подключений. Вот очень краткий список возможных вариантов (на деле их гораздо больше):

- Коммутатор может запрашивать аутентификацию и только этим и ограничиваться.
- Может быть виден трафик связующего дерева.
- Может быть виден межкоммутаторный трафик (например, по протоколу LLDP).
- Могут присутствовать пакеты, направляемые всем (“адресат неизвестен”).
- Могут быть видны широковещательные пакеты и многоадресные рассылки.

- Может быть виден трафик из карантинного широковеб-адреса.

Тем не менее, несмотря ни на какие отдельные пакеты, которые появляются в сети, подключаемая станция не может запрашивать у защищенной сети никакой трафик. Специально настроенный коммутатор может разрешить доступ к карантинной сети, которая позволяет посетителям выйти в интернет, но блокирует доступ к любым сетевым ресурсам в локальной, защищенной сети.

### Настройки дуплекса и автосогласования

Практически для всех новых интерфейсов Ethernet по умолчанию установлена настройка автосогласования (Auto-Negotiation). И это правильно. Тем не менее, многие производители заявляют, что это плохо – возможно, потому, что далеко не все сетевые инженеры хорошо разбираются в том, как это работает.

Вероятность того, что автосогласованию не удастся установить надежное соединение, очень низка. В некоторых случаях раньше оно действительно срабатывало некорректно, но практически все производители разобрались в этой проблеме и устранили ее, создав или обновив соответствующие программы. Если вдруг кто-то из производителей не знает о некорректной работе этой функции, а вы на нее натолкнетесь, то он будет только рад совместными усилиями устранить ее. Более подробно (хотя при этом очень доступно) принципы работы автосогласования изложены в стандарте IEEE 802.3, статья 28.

Рабочая станция, инициирующая процесс автосогласования, отправляет сигнал с квитированием – импульс FLP (Fast Link Pulse). Он состоит из пакета обычных импульсов, характерных для сетей 10BASE-T. Импульс FLP описывает возможности рабочей станции, которая его отправляет. Если устройство на дальнем конце тоже отправляет импульсы FLP, тогда оба устройства сравнят эти импульсы и выберут из них максимальные характеристики, которые смогут поддержать одновременно оба устройства. Затем они начнут обмениваться информацией по выбранному протоколу.

Если станция, пытающаяся выполнить автосогласование, не получает импульсов FLP от устройства на дальнем конце, тогда она пытается сама

определить скорость передачи этого устройства. Если два устройства на разных концах в принципе в состоянии поддерживать одну и ту же скорость, то такое определение скорости практически всегда пройдет успешно.

Если станция, проводящая автосогласование, не получает импульсов FLP от дальнего устройства, то она обязана выбрать для соединения настройку полудуплекса, и она не будет пытаться определить тип дуплекса для второго устройства, если импульсов FLP по-прежнему нет. Это, пожалуй, основная причина проблем, связанных с настройками дуплекса. К сожалению, среди

сетевых инженеров широко распространено заблуждение, что станция, пытающаяся провести автосогласование, сумеет определить настройки дуплекса у удаленного устройства, у которого настройки подключения зафиксированы принудительно.

Еще одно ложное представление о работе сетей заключается в том, что несоответствие настроек дуплекса обязательно вызовет сбой подключения. На самом же деле, если настройки дуплекса не совпадают, то будут появляться ошибки, сеть будет работать медленнее, что нетрудно заметить визуально, но трафик все-таки будет передаваться от одного устройства другому. Если имеет место несоответствие настроек дуплекса у коммутаторов, то ошибки можно будет посмотреть в отчетах; из них будет несложно узнать настройки дуплекса каждого из устройств.

С точки зрения мониторинга и безопасности сети, несоответствие настроек дуплекса имеет определенное значение, хотя и не критическое. Если настройки дуплекса различаются в интерфейсе, используемом в устройстве пассивного мониторинга, тогда оно не обнаружит никаких проблем в сети просто потому, что не будет вести передачу. Если настройки дуплекса различаются у двух устройств на концах сегмента, причем оба активно передают пакеты, тогда на сцену выходят два фактора. В сегменте часть пакетов будет приходиться с запаздыванием, что будет восприниматься как потерянные пакеты. Повторная передача на MAC-уровне таких пакетов производиться не будет. Это приведет к тому, что на более высоких уровнях системе придется устранять последствия, какими бы они ни были. Если достаточное количество пакетов будут признаны

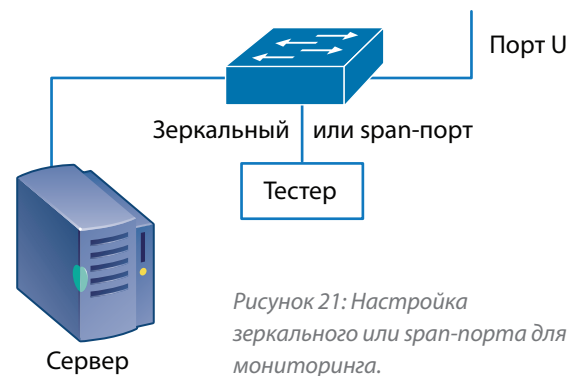
обычными, просто столкнувшимися пакетами, то MAC-уровень попытается послать их заново, однако тогда начнет восстанавливать данные буфер, что приведет к сбросу пакетов, передаваемых повторно таким способом. Потеря пакетов может повлиять на анализ проблем в сети и воспрепятствовать сбору достоверных данных для последующего юридического использования, ведь в таких условиях практически невозможно определить, были ли пакеты отклонены, в каком количестве и когда.

Для многих коммутаторов по умолчанию установлена настройка, отключающая любой порт, если на нем наблюдается чрезмерное количество коллизий, причем независимо от того, проходил ли он автосогласование и каким путем был установлен полудуплекс. Для коллизионных доменов в сетях, совместно использующих ресурсы, так происходит в соответствии с правилами обработки коллизий в среде передачи 802.3: порт, на котором наблюдаются такие коллизии, должен блокироваться или отключаться. Например, Cisco называет такой параметр "errdisable" – отключение (блокировка) ошибок.

### Метод 3: Настроить зеркальный или span-порт

Большинство управляемых коммутаторов позволяют настроить зеркалирование одного или большего количества портов. Функция зеркалирования позволяет копировать трафик с выбранного порта/портов на порт мониторинга. Эта методика называется также созданием зеркального или span-порта.

Способность копировать или зеркально отображать трафик на специально выделенный или выбранный порт вывода в коммутаторе предоставляют практически все производители коммутаторов. У старых моделей был



специальный порт, который можно было настроить для мониторинга, но у большинства новых коммутаторов для мониторинга можно выбрать и настроить любой из портов. Некоторые модели даже позволяют использовать таким образом несколько портов одновременно, хотя некоторые другие допускают использование в такой роли только одного порта. Некоторые модели позволяют трафик, за которым ведется наблюдение, отправлять с другого коммутатора – такова, например, функция RSPAN компании Cisco, хотя следует признать, что у нее есть свои ограничения и сложности с использованием.

Функции мониторинга, предлагаемые разными коммутаторами, зависят от производителя и модели коммутатора, однако основные функциональные возможности у них практически одинаковые: трафик с выбранного порта копируется и направляется на порт мониторинга для анализа.

Зеркальный порт часто работает в режиме только вывода (он может только выдавать информацию, но не может принимать), хотя некоторые

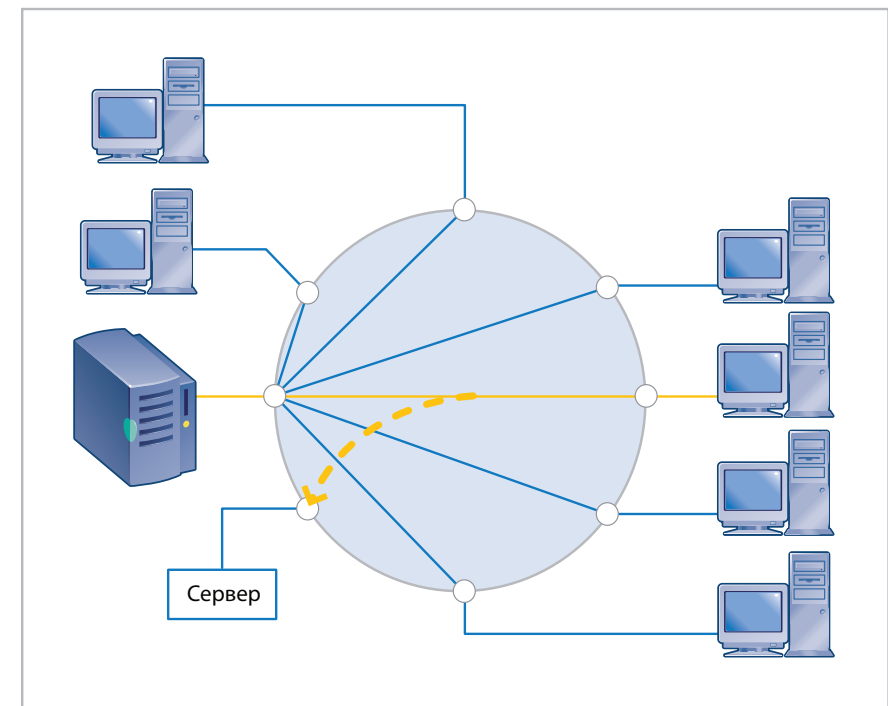


Рисунок 22: Логическая схема организации зеркального или span-порта.

производители допускают настройку таких портов и на двусторонний режим (ввод/вывод). Если настроить на коммутаторе зеркальный порт, то к нему можно подключить устройство для мониторинга, и тогда ему будет доступен весь текущий трафик, передаваемый между пользовательским подключением, испытывающим проблемы со скоростью, и сервером. Источником трафика для зеркалирования может быть любой другой порт в коммутаторе, в том числе и порт расширения uplink. Источником трафика для зеркалирования могут также быть несколько портов на коммутаторе и даже одна или несколько виртуальных сетей VLAN.

### Плюсы

Зеркалирование порта – один из самых распространенных и эффективных методов, применяемых для устранения сбоев в коммутируемых сетях. Он позволяет устройству мониторинга видеть весь трафик, который проходит через коммутатор по пути между двумя или большим количеством станций. Чаще всего для мониторинга к порту подключают анализатор протоколов.

### Минусы

Особенности применения этой технологии зависят от производителя коммутатора, однако существует несколько общих вариантов настроек. Учитывайте, что практически всегда при копировании информации с одного порта на порт мониторинга в коммутаторе будет использоваться фильтр данных. Это значит, что ошибки, которые обычно коммутатор отсекает за счет фильтра, не будут видны и на порту мониторинга. По этой причине при диагностике зеркалирование порта иногда бывает практически бесполезным: коммутатор за счет фильтрации того или иного типа фактически скрывает информацию о целом классе сетевых проблем.

Настраивать зеркальный порт надо с помощью консольного доступа. Иногда для такой настройки около коммутатора приходится ставить отдельный персональный компьютер, а рядом устройство для мониторинга. Часто бывает так, что у младших системных администраторов и сетевых специалистов нет пароля для консольного доступа и глубоких знаний в этой области; между тем, неправильная настройка зеркалирования может привести к перебоям в работе и даже к падению сети.

Существует реальная опасность переоценить пропускную способность порта вывода. Это приведет к потере трафика в потоке выдаваемых данных, а статистика использования сегмента, за которым ведется наблюдение, будет неполной. Чем большее количество портов подает данные на зеркальный порт, тем выше вероятность того, что пропускная способность порта вывода будет превышена. Предельный случай такого переполнения может возникнуть у тех коммутаторов, которые допускают зеркалирование всей виртуальной сети VLAN целиком. Для анализа данных, особенно если затем вы собираетесь использовать информацию для действий юридического характера, предельно важно знать, весь ли трафик собран для анализа или возможна утрата части трафика. Также очень важно правильно оценивать способность устройства для мониторинга принять тот или иной объем информации. Например, программный анализатор протоколов часто не в состоянии сохранить трафик, приближающийся к полной скорости передачи в сегменте.

### Знания, необходимые для использования Метода 3 Превышение возможностей порта

Максимальную пропускную способность порта мониторинга при выводе данных надо обязательно учитывать при работе. Порт вывода имеет два маршрута – TX (передача) и RX (прием). Как уже отмечалось, маршрут TX (передача от тестера к сети) на порту, используемом для мониторинга, может принудительно блокироваться коммутатором в соответствии с настройками зеркалирования.

Заблокирован он или нет (то есть работает ли порт в одностороннем или двустороннем режиме) – все равно максимальная принимающая способность RX (к устройству мониторинга) ограничена. Если вы зеркалируете полнодуплексный порт с такой же полной скоростью, что зеркальный порт вывода, то коммутатор будет просто сбрасывать часть трафика, даже не ставя вас в известность об этом. В этом случае даже неважно, каковы настройки дуплекса у устройства для мониторинга – полудуплекс или полный дуплекс – все равно ограничением служит пропускная способность маршрута к устройству, а не самого устройства.

На Рисунке 23 показано, как трафик, передаваемый в сети между сервером



и коммутатором в режиме полного дуплекса со скоростью 100 Мбит/с, зеркалируется на порт мониторинга. При полном дуплексе оба направления – и

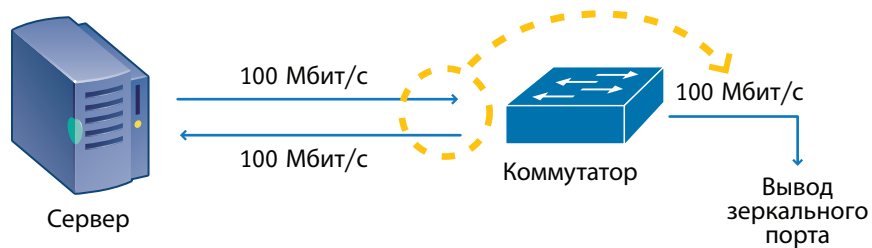


Рисунок 23: Ограниченная способность зеркального порта по выводу данных.

прием RX, и передача TX – способны использовать для трафика скорость 100 Мбит/с, то есть суммарная пропускная способность составляет 200 Мбит/с.

Если вы будете зеркалировать этот трафик на другой порт 100 Мбит/с, то сможете видеть только направление передачи TX от коммутатора к устройству мониторинга. В этом примере количество зеркалируемого трафика ограничено скоростью в 100 Мбит/с. Несмотря на то, что у коммутатора есть небольшой буфер (его использование необходимо из-за неравномерной, пульсирующей структуры трафика), тем не менее, та часть трафика на серверном порту коммутатора, которая превысит 50% совокупной емкости полнодуплексного порта для мониторинга, скорее всего, будет просто потеряна.

Если на порт мониторинга зеркалится сразу несколько портов, тогда вероятность проблем с пропускной способностью увеличивается пропорционально. Но поскольку большинство коммутаторов работают далеко не на пределе своих возможностей, проблема может не давать о себе знать какое-то время. Остроту проблемы можно снять, если подключить устройство мониторинга к более высокоскоростному порту – такому, чтобы он был в состоянии принять на вывод весь зеркалируемый трафик. Если бы зеркальный порт на Рисунке 23 был не 100-мегабитным, а гигабитным, то он был бы в состоянии без проблем принять совокупный трафик 200 Мбит/с.

### Коммутаторные технологии маршрутизации

К сожалению, информация о технологиях маршрутизации, которые используются в коммутаторах, а также о том, что именно и куда перенаправляется, не относится

к числу широко распространенных и всем известных фактов. Допустим, при диагностике или сборе информации для последующего юридического использования вы выбрали правильный порт для зеркалирования. Но при этом вероятность того, что вы увидите на span-порту какие-либо ошибки MAC-уровня, очень невелика.

Большинство коммутаторов, что представлены сегодня на рынке, установлены по умолчанию на использование технологии сохранения и маршрутизации (Store and Forward), а порой только для этого и предназначены. Тем не менее, многие из ранее установленных коммутаторов могут допускать (или быть настроенными по умолчанию) только на методы маршрутизации с малой задержкой. Определить же, какой метод маршрутизации используется, не так-то просто: эту информацию необходимо разыскивать по документации, а иногда не обойтись без тестирования.

Существует три распространенных технологии маршрутизации, хотя порой они используются под другими названиями:

- Технология сохранения и маршрутизации Store and Forward (использует традиционную передачу через мост на уровне 2 модели OSI)
- Технология быстрой маршрутизации Cut-Through (прямая маршрутизация на порт, MAC-адрес которого известен)
- Модифицированная технология быстрой маршрутизации Modified Cut-Through (маршрутизация после получения 64 байт, что эквивалентно одному тайм-слоту полудуплексного подключения 10/100 Ethernet и представляет собой отсечку в момент, когда может быть обнаружена допустимая коллизия).

Технологии маршрутизации с малой задержкой стали терять популярность уже после двух-трех лет использования. Возможно, так произошло потому, что небольшое увеличение производительности было достигнуто ценой больших сложностей в диагностике, характерных для подключений с малым временем задержки. Существовала как минимум одна комбинированная методика, которую называли методом обнаружения ошибок (Error Sensing) или адаптивной технологией (Adaptive). В этой технологии использовался один из методов с малой задержкой, пока уровень ошибок не превышал

установленный или настраиваемый пороговый уровень, и тогда происходило переключение на технологию сохранения и маршрутизации Store and Forward. Проблема в том, что непонятно, как определить, исчезла ли ошибка, насколько она серьезна, раз коммутатор перешел с одной технологии на другую. Ситуация будет еще запутаннее, если речь идет об ошибке, которая то появляется, то исчезает.

Если используется одна из технологий маршрутизации с малой задержкой, то при этом любая ошибка может исходить как из локального коллизийного домена, так и откуда-то снаружи, в границах всего широковещательного домена, даже если она прошла через несколько коммутаторов.

Если используется технология сохранения и маршрутизации, то вы можете быть уверены: порт коммутатора не пропустит дальше любые ошибки MAC-уровня (см. Рисунок 24). Если же используется технология маршрутизации с малой задержкой, тогда обнаруженная ошибка может происходить из любой точки в широковещательном домене, не только “по эту сторону” от порта коммутатора. И это существенно меняет рекомендации и подходы к диагностике.

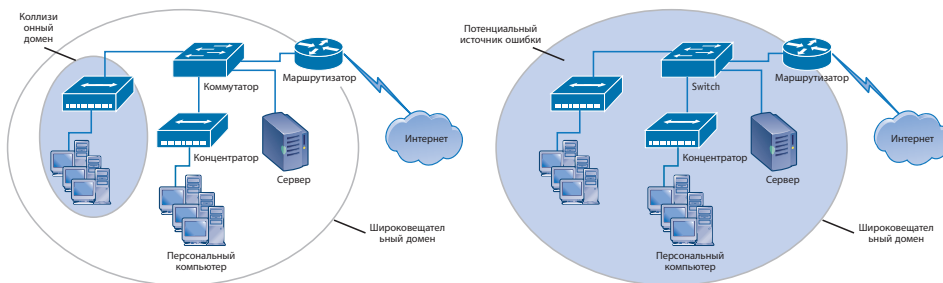


Рисунок 24: Возможное перенаправление ошибки при использовании метода сохранения и маршрутизации (Store and Forward, рисунок слева) и метода с малой задержкой (рисунок справа).

Зеркальный порт вывода на уровне 2 модели OSI будет использовать такую же технологию маршрутизации, как и все остальные порты в коммутаторе. Ошибки MAC-уровня практически никогда не направляются на зеркальный порт вывода.

Мы рассмотрели только маршрутизацию на уровне 2 модели OSI. Но сегодня на

рынке представлен гораздо более широкий диапазон коммутаторных функций, включая: маршрутизацию на уровне 3 модели OSI, уровне 4 и даже уровнях 5-7; балансировку загрузки; ограничения по скорости; технологии маршрутизации в зависимости от содержания; прокси-сервисы и специальные методы буферизации, фильтрации трафика, а также функции безопасности.

Поскольку функции, реализуемые на высоких уровнях, полностью зависят от производителя и модели коммутатора, в нашем кратком руководстве мы останавливаться на них не будем. Чтобы узнать, как работают эти функции и как их диагностировать при неисправностях, обратитесь к документации производителя. Во многих случаях диагностика таких функций потребует одновременного просмотра трафика до и после коммутатора. Начинать надо с использования анализатора протоколов; следует изучить трафик и сопоставить его элементы с описанием в документации производителя. Уяснив, какой должна быть правильная работа функции, вы сможете понять, в чем происходит отклонение от нормального режима работы.

## Метод 4: Подключиться к тегированному или транковому порту

Тестер можно подключить к транковому порту виртуальной сети VLAN или к порту, который занесен в одну или несколько виртуальных сетей. Этот подход похож на метод использования зеркального или span-порта, и все плюсы и минусы остаются теми же. Кроме того, необходимо удостовериться, что тестер в состоянии воспринимать тег или теги виртуальных сетей VLAN и/или их распределение в широковещательном домене – иначе вы не получите корректное представление о сети. Если тестер подключен к транковому порту, возможно, ему потребуется участвовать в управляющем трафике транка – например, по протоколу Cisco VTP.

Трафик, снимаемый с тегированного или транкового порта, может быть разным. Вот несколько вариантов:

- Коммутатор может выводить на порт только тегированный трафик виртуальной сети VLAN. Станции, не относящиеся к этой виртуальной сети VLAN, не смогут использовать соответствующие сетевые ресурсы.

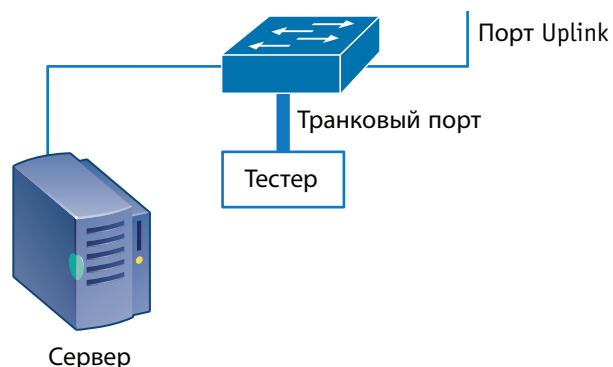


Рисунок 25: Подключение к тегированному или транковому порту виртуальной сети VLAN.

- Коммутатор может поддерживать для порта как тегированный, так и нетегированный трафик, обеспечивая работу и транков виртуальной сети VLAN, и локальных нетегированных станций. Часто исходная виртуальная сеть VLAN на транковом порту не тегуется.
- Коммутатор может выводить на порт тегированный трафик от нескольких виртуальных сетей VLAN. При такой конфигурации к коммутатору вряд ли станут подключать конечные рабочие станции, тем не менее, серверы все-таки могут поддерживать несколько виртуальных сетей VLAN для одного подключения.

#### Плюсы

Использование транкового порта VLAN позволяет вести мониторинг на больших участках сети. Если широкоэмитательный домен имеет одновременный доступ к нескольким виртуальным сетям VLAN, то это очень поможет при проведении активного обследования сети.

#### Минусы

К сожалению, лишь очень немногие тестеры способны эффективно работать при наличии одновременно нескольких виртуальных сетей VLAN. Многие вообще не способны провести обследование тегированных сетей и полагаются только на пассивный мониторинг. Более того, при попытке провести мониторинг на большом участке сети может резко обостриться проблема с пропускной способностью порта мониторинга – он может переполниться. Коммутатор должен применять к порту обычные правила маршрутизации, чтобы на транк попадали только одноадресные сообщения,

широковещательные пакеты, а также сообщения с неизвестным и устаревшим адресатом.

### Метод 5: Последовательно подключить к сегменту хаб

Пожалуй, этот подход был первым методом в диагностике коммутируемых сред, и до сих пор он остается очень популярным методом отслеживания проблем, относящихся к отдельному порту коммутатора. Для применения хаба, редусматривающего совместное использование ресурсов, нужно прежде всего определиться с местом его подключения. Хаб можно разместить между коммутаторами

либо подключить к клиентской линии. В большинстве сетей основной трафик, важный для целей диагностики, будет получен или передан таким ресурсом общего использования, как, например, файловый сервер (см. Рисунок 26).

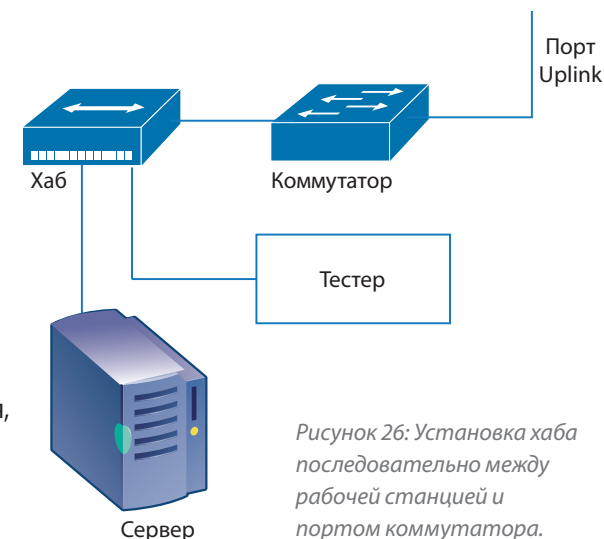


Рисунок 26: Установка хаба последовательно между рабочей станцией и портом коммутатора.

Для диагностики или сбора данных с прицелом на дальнейшие действия юридического характера порт мониторинга можно поддерживать практически невидимым для сети – это можно сделать, если он не ведет передачу.

**Примечание:** Вместо хаба можно использовать специальные устройства-отводы – дело в том, что сейчас уже почти невозможно приобрести хаб с разделяемой пропускной способностью.

#### Плюсы

Для оценки трафика и ошибок полезно использовать протокол SNMP, однако для настоящего анализа ошибок нет лучшего пути, кроме как подключить

диагностический прибор. Если между портом коммутатора и другим устройством разместить хаб с разделяемой пропускной способностью, то прибор для мониторинга сможет подключиться к тому же самому коллизийному домену. Эта технология позволит анализатору видеть весь имеющийся трафик. Доступ ко всему трафику существенно облегчает сетевым инженерам диагностику целого ряда проблем, включая сбои с учетной записью пользователя, плохие характеристики в сегменте и разрыв сетевых подключений. Поскольку устройству для мониторинга доступна вся информация, это один из лучших методов диагностики, пригодный практически при всех сбоях, затрагивающих отдельную рабочую станцию.

### Минусы

Во многих случаях этот метод ничем не поможет, особенно если нужно отслеживать состояние нескольких серверов. Где вы будете ставить хаб – на всех серверных подключениях? Если вы решите последовательно перемещать хаб по всем этим подключениям, то помните, что работа сети при очередном подключении хаба будет каждый раз прерываться. Время, необходимое для установки хаба, как правило, превышает время, за которое соединение будет разорвано из-за истечения таймера. Кроме того, многие сетевые ресурсы – сервера, например – могут соединяться по технологии или на скоростях, которые недоступны вашему тестеру.

Если между полдуплексными станциями поставить полдуплексный хаб, то пропускная способность линии существенно снизится, вызывая появление дополнительных ошибок и усложняя оценку симптомов исходного сбоя. Чтобы так не произошло, вы должны очень хорошо разбираться в том, как работает все ваше оборудование (коммутаторы, хабы и тестеры).

Когда к линии подключается хаб, могут возникнуть три проблемы:

- Если изначально сегмент работал на полном дуплексе, то включение в линию хаба вызывает дополнительную проблему, поскольку хаб использует полдуплекс.
- Если вы подключили “хаб”, а он оказался на самом деле мостом (частично или полностью), то вы ничем не улучшили положение.
- Если на линии уже были подключены один или более хабов и

архитектура Ethernet уже перестала быть признаваемой, то вы только спровоцируете дополнительные коллизии.

И если даже введение в линию хаба не вызовет новых проблем, то все равно результаты будут зависеть от того, какой прибор для мониторинга вы используете. Практически все программные анализаторы протоколов будут видеть только трафик стандартного размера, поскольку драйвер сетевой карты отвергает любой трафик иного типа – он признает только полностью сформированные пакеты без ошибок. Некоторые программные анализаторы протоколов используют модифицированные сетевые карты, которые все-таки позволяют видеть определенный уровень трафика с ошибками. Но чтобы видеть все ошибки в коллизийном домене, необходим аппаратный анализатор протоколов или другое устройство со специально созданными печатными платами, работающими на физическом уровне (Ethernet PHY – та часть схемных плат, которая ответственна за преобразование двоичных данных в сигналы в конкретной среде передачи).

## Знания, необходимые для использования Метода 5 Архитектурные ограничения при использовании хабов

- В сетях Ethernet 10 Мбит/с между двумя данными персональными компьютерами можно последовательно выстраивать до четырех хабов.
- В сетях Ethernet 100 Мбит/с между двумя данными персональными компьютерами можно последовательно установить один или два хаба.
- Хабы Класса I (маркированные или не маркированные таким образом) можно использовать в коллизийном домене только по одному.
- Хабы Класса II обычно маркируются, их в коллизийном домене можно использовать один или два, но не более.
- В сетях Ethernet 1000 Мбит/с в коллизийном домене можно использовать только один хаб, однако приобрести такое оборудование вам не удастся. В настоящее время хабы с разделяемой пропускной способностью для гигабитного Ethernet просто не производятся.
- В сетях Ethernet 10 000 Мбит/с (10 гигабит) полдуплексная передача запрещена, поэтому хабов для 10-гигабитного Ethernet в природе не существует.

### Архитектурные ограничения при использовании коммутаторов

Жестких ограничений по количеству мостов (коммутаторов, работающих на уровне 2 модели OSI) нет, причем ни для каскадов коммутаторов, ни для их параллельного подключения. Однако используемая архитектура прямо влияет на пропускную способность сети. Два принципиально важных соображения относятся к широковещательным рассылкам.

- Если два моста работают параллельно, причем оба маршрута открыты, тогда первый же широковещательный пакет, дошедший до любого из них, автоматически вызовет широковещательный шторм. Мосты обязаны направлять все широковещательные пакеты на все порты, кроме порта-отправителя. Второй мост сделает то же самое, что и первый, и исходная широковещательная отправка вернется на первый порт по параллельному маршруту. У некоторых коммутаторов есть настройка "trust me" – доверительный режим, который подразумевает, что это ваша ответственность – не создавать параллельные пути. Коммутатор не будет проверять их наличие или отсутствие. Это делается ради того, чтобы любое новое подключение получало доступ к сети практически мгновенно (такова, например, настройка Cisco "portfast").
- Если для исключения параллельных маршрутов используется связующее дерево или какой-либо другой прием, то чем больше количество мостов в отдельном широковещательном домене, тем большим будет соответствующий широковещательный трафик. Широковещательные рассылки – полезная и необходимая составляющая работы сети, обойтись совсем без них нельзя. Если занести в широковещательный домен слишком много станций, то количество фонового широковещательного трафика повысится настолько, что это может быть причиной заметного ухудшения характеристик сети. Каждая станция в широковещательном домене должна обработать каждый широковещательный пакет, и на это время прерывается выполнение других работ. Специальный таймер Max Age для связующего дерева ограничивает максимальные размеры сети, в которой это дерево применяется.

### Метод 6: Последовательно подключить к сегменту тестер

Подключение устройства для мониторинга последовательно, в разрыв между станцией и коммутатором, позволяет избежать тех проблем, которые связаны с последовательным подключением хаба: линия продолжит работать в полном дуплексе и не будет подвержена описанным ранее явлениям.

#### Плюсы

При таком подключении тестер увидит абсолютно все, если только к тестируемой станции (на Рисунке 27 это сервер) не существует параллельного маршрута, например, беспроводного. В зависимости от функциональности используемого тестера, этот метод может быть очень полезен для всех сбоев, относящихся к отдельной станции или сегменту. Если тестер последовательно включен в интернет-канал, то его можно использовать для проверки эффективности брандмауэра (firewall) или для сбора информации, которую затем предполагается использовать в юридических целях.

Даже при пассивном мониторинге такой тестер может проверить, какое устройство является источником каких бы то ни было ошибок на MAC

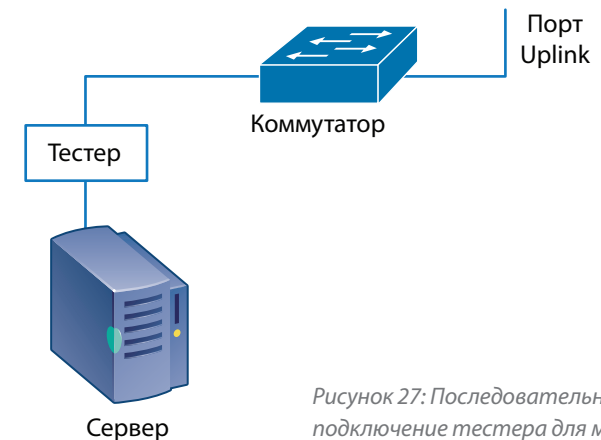


Рисунок 27: Последовательное подключение тестера для мониторинга.

уровне, может отследить запросы, сделанные подключенной станцией, чтобы проверить, приходят ли отклики от сети. Таким методом легко идентифицируется абсолютное большинство проблем с невозможностью подключения к серверу или службе.

**Минусы**

Однако данный метод может также вызывать серьезные проблемы. Если в сегменте используется кодирование (шифрование), то даже последовательное подключение тестера не позволит ему просматривать данные на высоких уровнях.

Сети Ethernet не позволяют совместно использовать один и тот же кабельный сегмент, за исключением подключений 10 Мбит/с по коаксиальному кабелю. Если у устройства мониторинга нет дополнительного порта, используемого для управления, то либо это устройство должно обладать функциями моста для ведения передачи, либо оно должно быть пассивным. Последовательные тестеры, как правило, очень недешевы, и это ограничивает их распространенность.

**Метод 7: Воспользоваться отводом, подключенным к сегменту**

Названия "отвод", "разветвитель", "ответвитель" (сплиттер) часто используются как синонимы, хотя последний термин чаще применяется в волоконно-оптических сетях. В волоконно-оптической линии ответвители маркируются цифровым обозначением, указывающим, в каких долях свет, пришедший с одной стороны, распределяется по двум путям с другой стороны (причем один из них может быть предназначен для мониторинга). Как правило, выпускаются ответвители с соотношениями 80:20, 70:30 или даже 50:50. Первый тип из них направляет 80% света к обычной точке назначения, а 20% отводит на порт мониторинга. Очень важно проверить, чтобы тип отвода соответствовал типу кабеля. Например, многомодовый отвод нельзя использовать в одномодовом сегменте. Также не следует использовать 50-микронный многомодовый отвод на 62.5-микронном оптическом кабеле. Большинство простых (несуммирующих) волоконно-оптических ответвителей пассивны и не требуют электропитания.

В медных кабельных системах ответвитель может понадобиться для того, чтобы проанализировать данные, направленные к исходному адресату, хотя эта возможность зависит от сложности применяемого кодирования. Затем ответвитель должен передать полученные данные на свой выходной

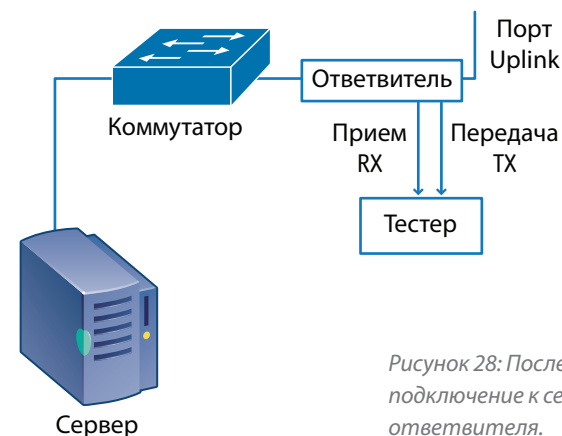


Рисунок 28: Последовательное подключение к сегменту ответвителя.

порт. Именно по этой причине важно следить, чтобы отвод соответствовал по характеристикам тому сегменту, в котором он устанавливается. Многие старые ответвители поддерживают только соединения 10/100 Ethernet, но не в состоянии поддержать гигабитные соединения Ethernet. В то же время некоторые новые устройства могут поддерживать только гигабит и ничего другого.

Другие устройства нового типа могут поддерживать все три скорости: 10/100/1000 Мбит/с. Как правило, медные ответвители требуют электрического питания, хотя при потере питания они продолжают поддерживать нормальную работу сегмента, в котором установлены. При восстановлении питания в работе может произойти незначительный перебой – за это время отвод возвращает реле в рабочее положение.

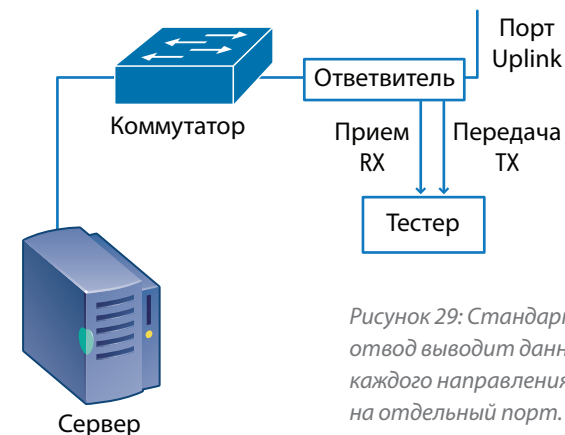


Рисунок 29: Стандартный отвод выводит данные с каждого направления передачи на отдельный порт.

Существует два принципиально разных типа ответвителей: обычный(стандартный) и новый суммирующий.

## Обычный (стандартный) ответвитель

Использование стандартного ответвителя позволяет устройству мониторинга увидеть либо запрос, либо отклик, но не то и другое вместе. Если вам нужно видеть и запрос, и отклик на него, то в устройстве мониторинга должно быть два входных анализаторных порта: один для маршрута передачи TX, второй для маршрута приема RX.

## Суммирующий ответвитель

Суммирующие ответвители изначально созданы для того, чтобы одновременно обрабатывать и запрос, и отклик. Часто такие ответвители имеют возможность настройки порта вывода, чтобы устройство мониторинга могло не только принимать, но и передавать информацию через него. Ответвители могут оснащаться не одним портом вывода, а несколькими, чтобы анализировать один и тот же трафик могли два и более тестеров.

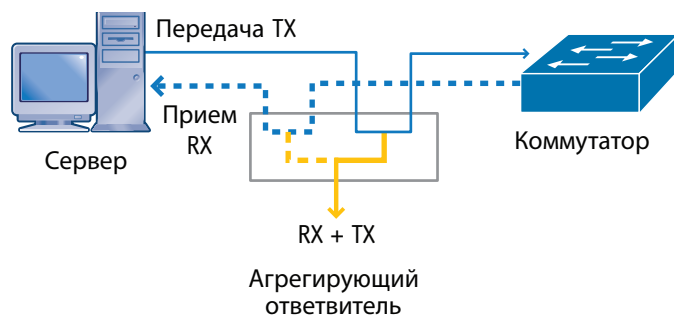


Рисунок 30: Суммирующий отвод позволяет подать на один или несколько портов вывода данные с обоих направлений передачи.

## Плюсы

Использование ответвителя в сравнении с зеркальным или span-портом дает множество преимуществ, одновременно позволяя избежать проблем, которые вызывает включение в линию хаба. Поскольку отводы имеют относительно низкую стоимость, их можно держать постоянно включенными последовательно на всех критически важных линиях и использовать в нужный момент.

Этот метод хорошо подходит для не очень опытных и младших системных администраторов, а также для сбора данных с прицелом на дальнейшие действия юридического характера, поскольку знания пароля для коммутатора он не требует. Ответвитель легко подключается последовательно, при этом перерыв в работе линии очень кратковременный. Однажды установленный отвод позволяет затем в любое время подключать и отключать устройство для мониторинга без какого-либо вмешательства в работу сети. Именно поэтому метод так хорош и для диагностики, и для сбора информации для последующего использования.

Большинство ответвителей предназначены только для вывода информации, поэтому подключенный к ним прибор для мониторинга будет невидим для сети. Ответвители новых моделей могут настраиваться не только для вывода, но и для ввода, что позволит устройству для мониторинга опрашивать сеть или отвечать на управляющие запросы, подавая определенный трафик по сегменту, за которым ведется наблюдение. Оба варианта настроек имеют свои положительные стороны, в зависимости от того, какая преследуется цель.

Стандартный ответвитель выдает копию всего трафика в сегменте, включая любые ошибки, которые могут в нем содержаться. При этом стандартный отвод не подвержен переполнению, поскольку у него для каждого направления – передачи TX и приема RX – предусмотрен отдельный порт вывода. Это позволяет устройству мониторинга получить такой же доступ, как и при использовании хаба, но без необходимости переводить сегмент на полудуплекс или риска получить несоответствие настроек дуплекса в сети. Стандартный ответвитель всегда работает только на вывод.

Суммирующие ответвители имеют более широкий набор функций, в том числе и возможность фильтрации трафика, с выводом на порт, к которому подключено устройство мониторинга, только выбранной части трафика. Эта функция особенно полезна для высокоскоростных сегментов, поскольку позволяет снизить объемы трафика, который надо проанализировать устройству мониторинга или сетевому специалисту.

Суммирующие ответвители пока воспринимаются на рынке как новинка и продолжают совершенствоваться с каждым днем. Большинство продуктовых линеек предлагают суммирующие ответвители как с одним, так и с несколькими портами – это зависит от модели. Дополнительные порты вывода позволяют параллельно поставить для мониторинга одних и тех же данных самые разные устройства, каждое из которых будет выполнять свою задачу.

В коммутируемой среде использование суммирующего ответвителя часто может быть самым простым и самым быстрым способом получения доступа к данным, передаваемым по определенному сегменту. По сути, суммирующие ответвители играют роль новых “хабов” в диагностике.

### Минусы

Самый большой минус при использовании отводов – потеря мощности сигнала, неразрывно связанная с применением любого ответвителя как в медной, так и в волоконно-оптической среде. Потеря части мощности означает, что если сегмент уже испытывал какие-то проблемы со средой передачи или чрезмерной длиной линии, то подключение к нему отвода может вообще вызвать отказ, поскольку оставшейся мощности для нормальной работы будет недостаточно.

Любой ответвитель может вызвать потерю мощности в 3 дБ в сегменте, к которому его подключили. Некоторые отводы более устойчивы к ошибкам, чем другие; иногда бывает, что установка ответвителя на одном конце сегмента вызывает сбой, а установка его же, но на другом конце не приводит к выходу линии из строя.

Медные ответвители вызывают схожие проблемы с потерей части сигнала, поскольку определенную долю мощности отбирает ответвитель: она расходуется на чтение проходящего трафика. В меди это явление эквивалентно дополнительному затуханию, и это тоже может вызвать отказ сегмента, на который устанавливается отвод – например, если его длина слишком велика или он и без того испытывал проблемы со средой передачи.

Чтобы восстановить сигнал и выдать его на порт мониторинга, медным ответвителем требуется электропитание. Высококачественный ответвитель

для медных сред не вызовет отказа сегмента, к которому он подключен, даже в случае пропадания питания. Но может произойти кратковременный перебой в работе, поскольку реле нужно время, чтобы перейти из режима мониторинга в сквозной режим (пропускание данных транзитом). Или такой кратковременный перебой может произойти в тот момент, когда питание восстанавливается, и реле переводятся в рабочее положение.

С оптическими (а иногда и медными) отводами могут быть еще и проблемы с количеством выводов, обслуживаемыми направлениями и/или задержками в работе, если вдруг ответвитель установлен не той стороной. На порт или порты мониторинга тогда будет выводиться недостаточная информация.

Сложность в том, что сегмент, на который устанавливается отвод, обычно имеет высокий уровень использования, а если ошибка в подключении ответвителя обнаружилась не сразу, то возможность исправить ее и подключить устройство правильно может выдаться не сразу, а по прошествии нескольких недель, когда будет проводиться очередное обслуживание сети.

В последнем на сегодняшний день поколении суммирующих ответвителей применяется мостовая схема соединения, чтобы совместить потоки данных с направлений приема RX и передачи TX. При использовании таких модифицированных мостов:

- Суммирующие отводы становятся подверженными проблеме с переполнением порта, описанной в разделе про Метод 3 (см. Рисунок23).
- Неравномерный, пульсирующий трафик (а трафик в сети обычно именно такой) может временами превышать емкость буфера в суммирующем ответвителе. Наличие буфера может замаскировать потерю части данных, что при сборе информации для юридического использования станет серьезной проблемой. А вот на методы диагностики, применяемые уже после появления сбоя, потеря данных из-за превышения пропускной способности порта или переполнения буфера почти не повлияет – просто потому, что сам сбой обычно касается основной массы трафика: она осталась, а не потеряна.
- Если в суммирующем ответвителе применяется фильтр, то он может



отсекать именно тот трафик, который представляет наибольший интерес. Иногда в устройстве остается работать фильтр, использовавшийся при диагностике предыдущего сбоя, это влияет и на диагностику текущего сбоя, и на сбор информации для юридического представления. Кроме того, сам факт применения фильтра может привести к тому, что суммирующий ответвитель будет отвергать часть пакетов из-за чрезмерной загрузки центрального процессора ответвителя.

Ошибки на MAC-уровне сбрасываются потому, что мосты не маршрутизируют ошибки. Весь остальной трафик выводится на порт мониторинга. Стандартные ответвители, в отличие от суммирующих, маршрутизируют ошибки. Это серьезное препятствие в работе суммирующих ответвителей, и их производители прилагают большие усилия, чтобы устранить его.

Суммирующие отводы часто имеют очень ограниченные функции маршрутизации. Они могут не маршрутизировать пакеты с размером, превышающим максимальный размер тегированного пакета Ethernet в виртуальной сети VLAN (1522 октета). Это означает, что пакеты, совместимые с требованиями стандарта 802.3as и имеющие большой размер (например, 2000 октетов), устройство маршрутизировать не может, равно как и увеличенные пакеты Ethernet (так называемые jumbo -пакеты).

Как правило, только те суммирующие ответвители, что допускают поступление трафика от устройства мониторинга, одновременно поддерживают функцию питания по Ethernet (PoE). Включение в сегмент обычного, стандартного ответвителя, скорее всего, приведет к отключению питания PoE конечной станции. Об этом надо помнить, проводя диагностику в сетях передачи голоса по IP (VoIP) и проверку беспроводных точек доступа – именно они чаще всего используют питание PoE.

Поскольку медные ответвители, как правило, являются активными, возможно такое положение, при котором сегмент в сети дает сбой, однако подключение к маршрутизатору продолжает считаться действующим. Так может происходить потому, что сегмент по одну сторону от отвода находится в сбойном состоянии, в то время как сам ответвитель поддерживает подключение к маршрутизатору активным.

При этом маршрутизатор будет считать, что с сегментом все в порядке, и будет продолжать направлять на него трафик. Так и будет оставаться, пока кто-нибудь не устранил сбой или вручную не переведет маршрутизатор в состояние “отключено”, чтобы смог заработать резервный канал передачи. В волоконной оптике ответвители пассивны, так что для них такой проблемы не существует.

## Метод 8: Использовать управление на основе SNMP-протокола

Протокол SNMP создали специально для того, чтобы определять, что происходит на удаленных участках сети, не прибегая к постоянному мониторингу и не перемещаясь физически в соответствующее удаленное месторасположение. Управляющий протокол SNMP позволяет проводить оценочный статистический анализ за большие периоды и подробный анализ за краткие промежутки времени. Работа SNMP-протокола в большой степени основана на отправке запросов и получении откликов, следовательно, управляющая станция должна непрерывно опрашивать сеть, чтобы обнаруживать проблемы. Чтобы сеть могла проинформировать управляющую станцию о проблеме, не дожидаясь поступления определенного запроса от нее, SNMP предусматривает возможность отправки незапрашиваемого отклика, так называемых trap-сообщений. Функция отправки trap-сообщений позволяет управляемому устройству – агенту SNMP – уведомлять управляющую станцию о достижении либо превышении заранее указанных значений, и

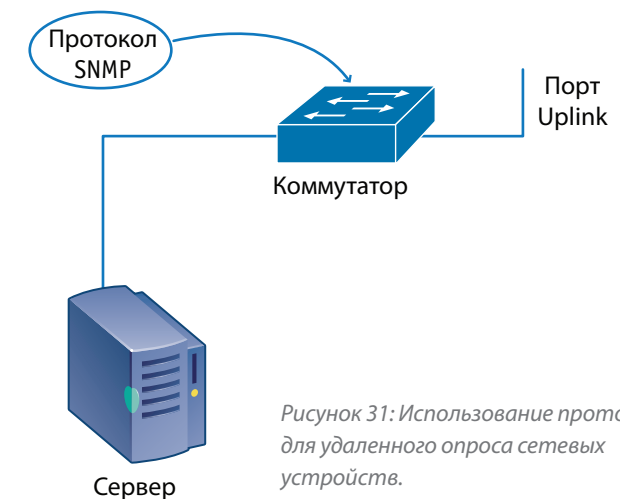


Рисунок 31: Использование протокола SNMP для удаленного опроса сетевых устройств.

эта информация не останется без внимания. Получив одно или несколько trap-сообщений, станция управления сетью может уведомить пользователя, например, отправкой сообщения по электронной почте или подачей сигнала на пейджер.

Использование SNMP, наверное, самый распространенный способ мониторинга в современных коммутируемых сетях. Если к устройству, за которым ведется наблюдение, существует маршрутизируемый путь, то нет нужды физически устанавливать консоль SNMP рядом с ним. Естественно, при этом настройки безопасности должны позволять консоли обращаться к агенту на коммутаторе.

Поскольку в ходе нормальной работы коммутаторы не маршрутизируют ошибки, использование SNMP, пожалуй, наилучший метод для отслеживания портов, которые страдают от ошибок. Коммутатор не может передать ошибку дальше, но зато ему известно о самом факте ее появления. Существует много различных MIB-баз для коммутаторов, поддерживающих SNMP. MIB-базы, содержащие информацию по управлению, по сути представляют собой словари-справочники, в которых перечислены возможные запросы с возможными откликами на них и соответствующим описанием.

Каждая поддерживаемая производителем MIB-база позволяет консоли управления получить более или менее подробное описание текущего состояния сети в окрестностях устройства, за которым ведется наблюдение, включая и состояние самого устройства. Существуют частные MIB-базы, которые обычно предназначены для поддержки определенного типа коммутатора и программного уровня, а также стандартные MIB-базы (или основанные на документах RFC), позволяющие эффективно наблюдать за всей коммутируемой сетью. Для диагностики полезны приведенные далее MIB-базы (хотя существует еще и масса других); перечисление по возрастанию подробности данных:

- RFC 1213 – MIB II
- RFC 1643 – Ethernet-Like Interface MIB
- RFC 2021 – RMON 2
- RFC 2819 – RMON Ethernet

Материалы RFC обновляются и совершенствуются непрерывно, поэтому всегда используйте самое последнее обновление индекса RFC. Например, RFC 1213 обновлялся как минимум 5 раз (вышли более свежие RFC 2011, 2012, 2013, 2358 и 2665). Кроме MIB-баз, указанных в этих документах RFC (где содержится подробнейшая информация об использовании и ошибках), для диагностики очень полезна MIB-база по устройствам-мостам (RFC 1493, 1525 и 2674). При использовании SNMP для мониторинга сети не следует упускать из виду вопросы безопасности. Если SNMP-агенты не защищены от несанкционированного доступа, то практически любой злоумышленник, находящийся где угодно, может отслеживать работу вашей сети или даже менять настройки коммутаторов. Часто по умолчанию протокол SNMP включен с несложным паролем, тоже используемым по умолчанию – он одинаков и установлен при продаже для коммутаторов и других SNMP-агентов. SNMP-пароли называют также строками community string, они вводятся с учетом регистра и знаков препинания. Строки community string передаются как открытый текст, что само по себе создает дополнительную опасность. Чтобы закрыть эту лазейку в безопасности, SNMP третьей версии предлагает процедуру аутентификации и передачу с.

Необходимо, как минимум, сразу же изменить строку community string, установленную по умолчанию, на какую-нибудь другую. SNMP-агенты можно настроить таким образом, чтобы они предоставляли разным строкам community string разные уровни доступа; чтобы они откликались на запросы от конкретной подсети и игнорировали запросы от других подсетей; чтобы отвечали на запросы с конкретных IP-адресов и не отвечали другим адресам. Возможны и другие настройки. Маршрутизаторы, предоставляющие путь к SNMP-агентам, могут накладывать на использование SNMP дополнительные ограничения. Брандмауэры (firewall) могут вообще полностью блокировать работу SNMP. Если вам удалось получить доступ к агенту с помощью SNMP, то агент должен поддерживать MIB-базу, в соответствии с которой сделан ваш запрос. Большинство производителей поддерживают корректную работу стандартных MIB-баз, однако есть производители, которые этого не делают. В некоторых случаях необходимо обновить операционную систему коммутатора, чтобы он смог поддерживать желаемую общую или частную MIB-базу.

Если коммутатор не отвечает на SNMP-запрос, тому может быть масса причин. Как только становится доступной соответствующая MIB-база и устраняются все проблемы с доступом, SNMP становится очень полезным инструментом для мониторинга состояния сети и выявления общих закономерностей ее работы.

### Плюсы

Использование систем управления сетью для автоматического мониторинга сети – отличный способ отследить изменения трафика в зависимости от времени суток; проводя диагностику, узнать, какие действия выполняет сеть; собрать данные для последующего юридического использования. С помощью SNMP можно получить практически любую информацию о вашей сети, если агент поддерживает соответствующую MIB-базу.

Чтобы система управления сетью была максимально эффективна, необходимо ее периодически более точно настраивать, указывая характеристики при нормальном режиме работы и критерии, при нарушении которых работа будет считаться ненормальной (например, чрезмерный трафик или его потеря). В последнем случае система уведомит дежурного системного администратора.

Если нужно провести детальный анализ работы сети, могут потребоваться специальные средства. Какие-то из них являются встроенными возможностями сетевой инфраструктуры, другие нужно специально устанавливать, чтобы вести мониторинг и диагностику ключевых сетевых устройств или ресурсов. Если нужные средства доступны, то при нарушении заданных условий может автоматически стартовать сбор трафика в файл анализатора протоколов. Системы обнаружения вторжения можно настроить на отслеживание симптомов, свидетельствующих о сетевой атаке извне или изнутри.

### Минусы

Используя SNMP, с сетью можно делать практически все, включая захват пакетов, если агент это допускает. Но допускают не все агенты. Вы по определению не можете полностью контролировать, кто и для чего использовал этот протокол. Если имеет место проблема с протоколом либо со срабатыванием таймера, то без захвата пакетов диагностику провести нельзя. Многие устройства, про которые в инструкциях пишется,

что они поддерживают дистанционное управление RMON, на самом деле поддерживают только четыре из девяти групп. Ограниченные списки поддержки называют по-разному – например, облегченной версией RMON Lite.

Команды SNMP имеют меньший приоритет, чем маршрутизация трафика. Если агент занят, то сбор статистики SNMP может быть отложен до тех пор, пока не уменьшатся или не исчезнут все составляющие пикового трафика. С точки зрения статистики это эквивалентно отклонению пакетов. Во многих новых маршрутизаторах весь обычный трафик обрабатывают входные интегральные микросхемы ASIC, а центральный процессор маршрутизатора занимается обработкой только нетипичных событий. Использование консоли SNMP для опроса маршрутизатора может выдать уровни занятости центрального процессора от 10% до 100%, меняющиеся скачкообразно. Сетевые инженеры, увидев это, иногда просто пугаются. Если же какое-то устройство будет одновременно опрашивать несколько консолей SNMP, то оно может вообще выйти из строя (это зависит от его конструкции и настроек).

Несмотря на то, что системы управления сетью считаются основным средством для определения нормального состояния сетей или поиска причин ненормального поведения, тем не менее, многие такие системы слишком сложны и потому практически никогда не бывают настроены правильно и до конца. Либо они требуют от сетевых специалистов каждый день так много внимания, что нормально пользоваться ими можно только в том случае, если для этой (и только этой) работы выделяется специальный сотрудник. На многих предприятиях это приводит к тому, что системой управления сетью просто перестают пользоваться либо применяют ее некоторое время только при определенных условиях. Если рассчитать годовые затраты на такую систему управления сетью, то получится, что ее поддержка обойдется на уровне или даже дороже цены покупки.

Многие сети используют для SNMP-мониторинга общие маршруты передачи данных и не имеют других средств управления удаленными участками сети. Если основной маршрут не работает, то SNMP ничем не поможет, кроме констатации того, что удаленный участок недоступен. Диагностику можно будет провести только в том случае, если существует альтернативный путь передачи данных.

## Знания, необходимые для использования Метода 8

### Примеры обнаружения сетевой атаки с помощью SNMP

Системы обнаружения вторжения можно настроить так, чтобы они отслеживали симптомы, которые могут свидетельствовать о том, что кто-то предпринял атаку на сеть, причем как снаружи, так и изнутри. Отслеживать можно, например, такие события:

- Сбои ipReasmFails (1.3.6.1.2.1.4.16): Количество сбоев, обнаруженных алгоритмом сборки IP. Отслеживается на всех хостах, чтобы вовремя обнаруживать сетевые атаки или проблемы с доставкой данных по сети.
- Сбои tcpAttemptFails (1.3.6.1.2.1.6.7): Количество раз, когда TCP-подключения выполняли прямой переход в состояние CLOSED из состояний SYN-SENT или SYN-RCVD, плюс количество раз, когда TCP-подключения делали прямой переход в состояние LISTEN из состояния SYN-RCVD. Это может быть индикатором атаки извне.
- Количество udpNoPorts (1.3.6.1.2.1.7.2): Суммарное количество полученных датаграмм UDP, не содержащих связанных данных на порту назначения. Этот счетчик может служить индикатором того, что кто-то “прощупывает” вашу сеть.

### Как узнать, какую MIB-базу использует SNMP

Протокол SNMP использует огромное количество MIB-баз. Некоторые из них основаны на документах RFC, другие зависят от производителя и модели оборудования. Если не понимать, что именно вы запрашиваете, то невозможно

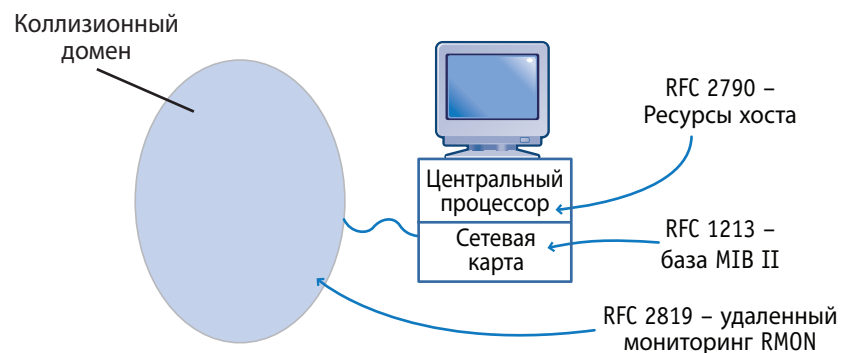


Рисунок 32: Различные запросы о текущем уровне использования.

интерпретировать и получаемый отклик. Например, на Рисунке 32 сервер делает запросы, используя три разных MIB-базы. В каждом случае суть запроса одна и та же – у устройства спрашивают, насколько оно занято.

Первый запрос интересуется уровнем загрузки центрального процессора сервера. Это целиком зависит от того, какие приложения запущены на сервере в данный момент, причем уровень сетевой активности на это практически не влияет.

- RFC 2790 [Host Resources]: hrProcessorLoad (1.3.6.1.2.1.25.3.3.1.2) Процент времени, когда процессор был занят (точнее, не был свободен) – среднее значение за последнюю минуту.

Второй запрос интересуется, сколько трафика прошло через сетевую карту на данном сервере. Это полностью зависит от трафика, адресованного к серверу (включая широковещательные рассылки), а загруженность сети может влиять, а может и не влиять на этот показатель. Например, в сети может наблюдаться уровень 35% загруженности сети, в то время как сервер принимает только 7% из этого трафика. Отклик SNMP будет содержать значение 7%. Обратите внимание: запрос не учитывает исходящий трафик, поскольку для него в базе MIB используется другой идентификатор.

- RFC 1213 [MIB II]: ifInOctets (1.3.6.1.2.1.2.2.1.10) Суммарное количество октетов, полученных через интерфейс, включая пакетные символы.

Третий запрос направлен на то, чтобы выяснить, насколько занят сетевой сегмент, к которому подключена сетевая карта сервера. Объект интереса – исключительно активность сети, а в ней трафик может предназначаться и серверу, и другим устройствам. Используя прежний пример, можно сказать, что в сети уровень загруженности трафиком составляет 35%, в то время как сервер принимает только 7% из них. Тогда отклик SNMP будет содержать значение 35%.

Если сервер использует стандартный сетевой драйвер NDIS, то, возможно, он видит только “хороший” трафик и не видит ошибок, даже если запрос отправлен в соответствии с MIB-базой, которая выдает информацию об ошибках. Большая часть тестовых сообщений RMON соответствует сообщениям на обычный

персональный компьютер со стандартной сетевой картой под управлением стандартного сетевого драйвера NDIS. Ошибок или вовсе нет, или очень мало.

- RFC 2819 [RMON]: etherStatsOctets (1.3.6.1.2.1.16.1.1.4 Суммарное количество октетов данных (включая те, что находятся в плохих пакетах), полученных по сети (за исключением пакетных битов, но учитывая октеты контрольной последовательности FCS).

Если пользователь не обращает внимания на точное значение каждого параметра, то он может прийти к совершенно неправильным выводам. Особенно это характерно для пользовательского интерфейса систем управления сетью, который часто оперирует цветовым выделением – красным, желтым, зеленым – чтобы сообщить о состоянии. Однако цвет не поможет отличить разные типы занятости друг от друга. Чтобы правильно интерпретировать получаемые предупреждения от системы, вы должны точно знать, какими могут быть источники этих предупреждений.

### Точность MIB-баз

Иногда использование SNMP-агентами какой-то отдельной MIB-базы происходит не так, как надо, и отклики на запросы выдаются просто неправильные. Реже бывает так, что программное обеспечение SNMP Manager неправильно интерпретирует отклик или существует несоответствие между версиями MIB-базы в агенте SNMP и в программном обеспечении SNMP Manager. Так бывает нечасто, но все-таки периодически программные ошибки приводят к получению неточных откликов. Вы могли бы получить правильный отклик, но для этого пришлось бы использовать другую версию MIB-базы для устройства и станции управления. В новой версии MIB-базы может содержаться другое описание отклика. Это можно проиллюстрировать на бытовом примере.

Представьте себе, что вы приобрели бывший в употреблении тостер, который можно подключить к компьютерной сети. Вы принесли его домой и загрузили для него с сайта новейшую MIB-базу. Затем положили в тостер первый кусочек хлеба и со станции управления SNMP запросили тостер, какая на нем стоит настройка поджаривания. Тостер выдает отклик “3”. При этом в старой MIB-базе вариантов отклика было всего три: 1=“слегка подрумянить”, 2=“хорошо

поджарить”, 3=“готовить до обугливания”. А в новой MIB-базе, которую вы загрузили с сайта и которая рассчитана на тостеры самых новых моделей, вариантов отклика уже 7, от 1=“слегка подрумянить” до 7=“готовить до обугливания”. Из-за несоответствия в MIB-базах вы будете ждать, что тостер вам сделает хорошо подсушенный тост, а на самом деле получите головешку.

### Метод 9: Применение потоковых технологий

Потоковые технологии появились в ответ на потребности в диагностике коммутируемых сетей. По сути, потоковые технологии сочетают в себе три области знаний, которыми должен обладать любой ИТ-специалист (тестирование кабельных сред, анализ протоколов, управление сетью с

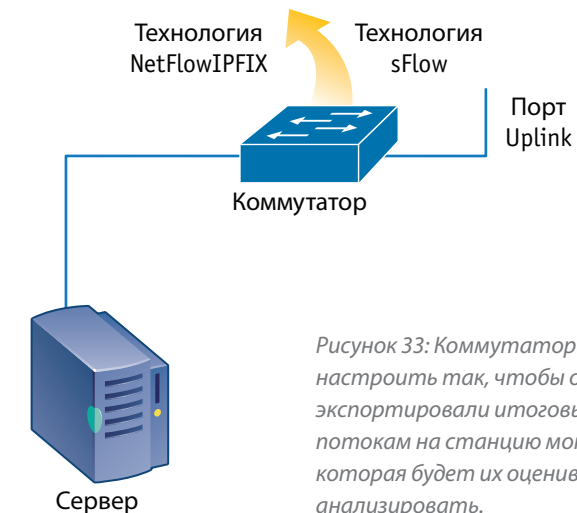


Рисунок 33: Коммутаторы можно настроить так, чтобы они экспортировали итоговые отчеты по потокам на станцию мониторинга, которая будет их оценивать и анализировать.

помощью SNMP). За счет применения этих методов маршрутизатор становится для вас встроенным прибором для диагностики и управления. Потоковые технологии отслеживают, кто и с кем обменивался данными, по какому протоколу, сколько байтов и пакетов было передано каждой стороной и так далее. Итоговый отчет, содержащий всю эту информацию, отправляется на потоковый приемник. В сравнении с файлом, который собирает анализатор протоколов при захвате пакетов, объем информации уменьшается на порядки. По сети к потоковому приемнику передается только итоговый отчет, содержащий сводную статистику. На сегодняшний день используется большое

разнообразии потоковых технологий. Вот некоторые из них: NetFlow, IPFIX, J-Flow, sFlow и sFlow.

### Плюсы

В сравнении с SNMP-протоколом, потоковые технологии обладают рядом полезных особенностей. Коммутатору не нужно сохранять отчеты о поведении сети за относительно большие периоды времени. Потоковые отчеты, как правило, охватывают небольшие периоды и экспортируются каждые 30 минут или даже чаще. При использовании SNMP приходится хранить данные за целый день, а то и больше.

Нет необходимости в аппаратных или программных тестовых сообщениях. Потоковые данные поступают от самой инфраструктуры сети. В большинстве случаев существующая инфраструктура изначально способна выдавать потоковые отчеты. Возможно, коммутаторы низкого уровня, расположенные в непосредственной близости от пользователей, на это не способны, но те, что расположены в ядре сети и те, что обслуживают подключения к глобальной сети, наверняка такими возможностями обладают – а именно они и представляют наибольший интерес. Надо лишь дополнить некоторые настройки, и все заработает.

Потоковый приемник может располагаться в любой точке распределенной сети, вот только некоторые провайдерские линии при этом могут потребовать слишком больших финансовых затрат. Поэтому потоковые приемники стоит размещать с учетом географической привязки. Размеры потоковых отчетов, направляемых приемнику, можно оценить как максимум 3-5% от наблюдаемого объема трафика. В зависимости от типа трафика эта цифра может снизиться до 1% или даже меньше. Потоковые данные отправляются потоковому приемнику на постоянной основе. А протокол SNMP требует, чтобы станция мониторинга регулярно опрашивала агента SNMP, и только тогда данные передаются получателю.

### Минусы

На момент написания нашего руководства наибольшее распространение среди потоковых технологий имеет метод NetFlow, разработанный компанией Cisco.

Если ваша инфраструктура строится не на оборудовании Cisco, то придется воспользоваться альтернативными технологиями. Документ RFC 3917 содержит стандарт на версию технологии NetFlow, фигурирующую там под названием IPFIX; вскоре он будет доступен.

Технология sFlow – это пример потоковой технологии, определенной в документе RFC 3176 и использующей сэмплирование. Она позволяет получить статистику по количеству трафика и сторонам, участвовавшим в обмене информацией. Метод sFlow можно настроить на отбор каждого n-ого пакета или отбор пакетов случайным образом. Поскольку трафик всегда дискретен, этот метод полезен при планировании расширения, анализе общих тенденций и диагностике даже в самых безвыходных ситуациях. Сэмплирование пакетов делает практически невозможным получение отчетов по последовательностям пакетов в отдельно взятой транзакции. Из-за сэмплирования эта технология не всегда пригодна к использованию в системах безопасности и других подобных видах деятельности. В отличие от технологий NetFlow и IPFIX, метод sFlow работает на втором уровне модели OSI и выдает статистику по не-IP трафику. Однако это довольно сомнительное преимущество, поскольку IP-протокол фактически стал доминирующим. Некоторые платформы также поддерживают сэмплирование для технологий NetFlow или IPFIX, но тоже с ограничением по применимости.

Когда заканчивается поток или истекает соответствующий таймер, формируется потоковый отчет, однако он может не отправляться еще от 1 до 30 минут. Таким образом, мониторинг ведется не вполне в реальном времени, хотя тот факт, что отчеты отправляются на постоянной основе, и может создавать впечатление, что работа ведется именно в реальном времени.

Как правило, потоковые отчеты отправляются без шифрования; теоретически их можно подделать. Если сравнивать потоковые отчеты с SNMP, то в них выдается информация о несколько меньшем трафике. Например, сводки NetFlow могут содержать данные об IP-трафике, но не о других видах трафика уровня 3 или ниже. Если в сочетании с SNMP используется правильная MIB-база, то этот метод позволит получить информацию обо всем трафике.

## Method 10: Set up a syslog server

Большинство устройств в сетевой инфраструктуре поддерживает отправку информации для регистрации событий в специальной базе syslog-сервером. Syslog-регистрация событий чаще всего используется для управления серверами и приложениями, а также для проведения аудитов по безопасности. Уровень подробностей в отчетах задается в настройках (раздел словесного наполнения). Как правило, доступны варианты от регистрации только критически важных (“катастрофических”) событий до регистрации всех, даже незначительных событий. В документе RFC 3164 перечислены все типы сообщений. Отправляемые сообщения, помимо всего прочего, включают в себя ошибки и события (регистрация в системе, отказ в регистрации, запуск и остановка процессов и так далее), а также регулярно повторяющиеся операции.

### Плюсы

Syslog-сервер будет сам выдавать отчеты об ошибках, событиях и обычных операциях; для этого от сетевого администратора требуется только один раз правильно настроить коммутатор, указав ему IP-адрес точки назначения – syslog-сервера.

Затем в списке событий будут регистрироваться записи о текущих операциях, а syslog-сервер будет сам по мере необходимости отправлять отчеты. Можно

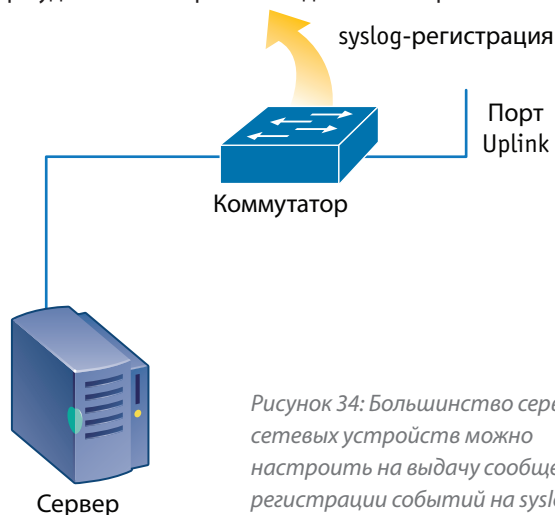


Рисунок 34: Большинство серверов и других сетевых устройств можно настроить на выдачу сообщений для регистрации событий на syslog-сервере.

просмотреть и изучить как текущие операции, так и выполненные операции за период.

Syslog-регистрация – вероятно, один из лучших методов диагностики при проблемах с процедурами аутентификации.

### Минусы

Syslog-сервер может генерировать большое количество в общем-то бесполезных данных. Иногда крайне сложно обнаружить в огромном количестве сообщений источник возникшей проблемы, и тем более для профилактики искать источники будущих проблем или дыры в системе безопасности. Колоссальные количества сообщений, не имеющих важного значения, и необходимость искать среди них нужное, словно иголку в стоге сена, привели к появлению специальных syslog-утилит для поиска и даже платных приложений, которые могут сортировать и группировать сообщения, а также обладают продвинутыми возможностями поиска.

Если настройки регистрации слишком широки, то syslog-сервер создает большие объемы бесполезной информации даже за короткое время. Если же настройки слишком ограничить, то в отчетах могут не отразиться важные события.

## Метод 11: Использовать серверные ресурсы (ресурсы хоста)

Практически все компьютеры и сетевые карты обладают некоторыми встроенными средствами диагностики. Такие средства, как правило, выдают сообщения о большинстве явлений, которые могут повлиять на ежедневное использование устройства и его работоспособность.

### Компьютерная диагностика

Каждый производитель компьютерной техники обладает определенными аппаратными средствами диагностики и либо поставляет их сразу с компьютером, либо позволяет загрузить со своего веб-сайта. В большинстве случаев такие средства диагностики относятся исключительно к работе

отдельно взятого аппаратного устройства, хотя последствия сбоев такого устройства могут сказываться и на сети в целом.

Кроме того, производитель сетевых карт часто предоставляет загружаемые диагностические утилиты, которые могут помочь в настройке конфигурации и диагностике сетевых карт. Вы можете использовать эти утилиты для проверки скорости и настроек дуплекса, для отслеживания определенных ошибок. Программный драйвер сетевой карты, установленный на компьютере, не обязательно предоставляет такую информацию, а если и предоставляет, то не всегда ее легко найти.

### Диагностика операционной системы

Операционные системы – например, Microsoft Windows, Unix или Linux – обладают разнообразными диагностическими возможностями.

Наверное, самые простые средства диагностики Windows – это утилиты `msonfig` и окно статистики сетевой карты. Утилита `msonfig` позволяет просмотреть конфигурацию системы, включая информацию по драйверу сетевой карты, а статистика работы сетевой карты покажет, сколько трафика система приняла от сети и сколько, по ее мнению, отправила к сети. [Как правило, получаемые значения коррелируют с результатами, которые выдает запрос по базе MIB II, описанной в Методе 8. К сетевой карте может приходиться гораздо больше трафика, чем она принимает, и обнаружить это можно с помощью запросов RMON, см. Рисунок 33.]

Выбрать лучший пример диагностики для ОС Unix или Linux не так-то просто – это открытые операционные системы, поэтому выбор средств необычайно широк. Диагностические средства для этих операционных систем могут быть самыми разными: от самых простых до очень продвинутых и многофункциональных, приближающихся по возможностям к описанной далее категории средств от сторонних поставщиков.

### Средства диагностики от сторонних поставщиков

Средства диагностики, предлагаемые сторонними поставщиками (например, программные анализаторы протоколов) применяются на станциях для определения проблем с использованием протоколов. Простые средства для анализа протоколов можно загрузить из интернета, а сложные платные продукты, включающие большое количество встроенных библиотек с симптомами сбоев и инструментов для составления отчетов, необходимо заказывать у фирменных поставщиков (такие продукты чаще всего называют Экспертами протоколов). Существует также масса других видов диагностических средств, включая системы управления сетями на основе SNMP и специальные инструменты для отдельных видов сетевой диагностики, проведения анализа и оценки закономерностей в работе сетей.

### ММетод 12: Использовать сочетание методов

Некоторые сетевые проблемы можно вполне надежно обнаруживать с помощью какого-то одного метода диагностики. Однако другие виды проблем требуют сочетания двух и более методов, иначе сбой не удастся правильно распознать и устранить.

Одним из таких примеров может быть использование сначала аппаратного анализатора протоколов для отслеживания данных, передаваемых к сетевому устройству и от него: например, к коммутатору и от него. Затем для наполнения канала передачи определенным типом трафика нужно использовать другой метод. Результаты этого теста покажут, вносит ли коммутатор или другое устройство изменения в трафик при передаче, отфильтровывает ли какие-то данные в результате срабатывания системы безопасности, соблюдается ли приоритет в маршрутизации трафика (что очень важно для таких приложений, как передача голоса по IP – VoIP), а также какова задержка в работе (запаздывание) самого коммутатора.



### Заключение

Самый распространенный подход к диагностике – подождать, пока не пожалуется пользователь. Не стоит недооценивать этот метод: на самом деле он прост и эффективен. Пользователи очень тонко чувствуют отклонения в работе сети, несмотря на то, что эти ощущения основаны на подсознании. Как только сеть начинает вести себя “не как обычно”, пользователи тут же обращаются в отдел ИТ. Получив такой сигнал от пользователя, вы можете начать диагностику от его/ее рабочей станции. Единственный недостаток этого метода состоит в том, что он реактивный – вы реагируете на сбой, который уже произошел.

В идеале же отдел ИТ должен работать так, чтобы не допускать возникновения сбоев – то есть подход должен быть профилактическим. Профилактические меры могут включать в себя регулярный опрос каждого коммутатора, мониторинг трафика и проверку его качества на каждом порту коммутатора, а также мониторинг любого сегмента в сети с той или иной частотой. Профилактика – использование средств мониторинга и анализа закономерностей, проверка статистики по портам коммутатора, применение инструментов для отслеживания поведения коммутаторов – поможет вам перейти от борьбы с последствиями сбоев к предотвращению их появления. Хотя, конечно, полностью исключить возникновение сбоев невозможно.

Очень важно проводить регулярный инструктаж и обучение персонала, работающего в отделе ИТ, в том числе и в тех случаях, когда собираемая информация в дальнейшем будет использована юристами. К сожалению, в последние несколько лет наблюдается очень тревожная тенденция: сетевые специалисты упорно недооценивают и даже игнорируют теоретически аспекты построения сети, ее структуру, исследование поведения сети и другие составляющие в областях ниже сетевого уровня модели OSI.

Возможно, так происходит потому, что сети перешли от использования устройств с разделяемой пропускной способностью и совместным использованием ресурсов к коммутируемым системам. Поскольку проблема затрагивает только одного пользователя, то все списывают на неудачное

стечение обстоятельств или устаревание конкретного сетевого устройства. Устаревание в данном случае означает всего двух- или трехлетний период эксплуатации. Если симптомы или результаты тестов почему-то кажутся нелогичными, то их просто игнорируют, хотя на самом деле в них необходимо разбираться до конца. Небольшой дополнительный курс обучения или тренинг позволил бы ИТ-специалистам правильно интерпретировать симптомы и результаты тестирования, что привело.

Недостаток понимания в области основ работы сетей, ниже сетевого уровня модели OSI, приводит к тому, что целое поколение специалистов в подобных ситуациях абсолютно беспомощно. Беспроводные технологии, появившиеся и распространившиеся относительно недавно, уже прошли период, когда к ним проявляли только детское любопытство, и теперь внедряются повсеместно.

Это заставляет вспомнить о сетях с разделяемой пропускной способностью и поднимает уже забытые вопросы о том, что может происходить в проводных сетях. Если же специалист сталкивается с ситуацией, когда с сетью что-то не так или надо собрать данные для судебного преследования, тогда становится ясно, что обучение и тренинги никогда не бывают лишними. Они необходимы для того, чтобы понимать, как каждый элемент сети должен работать в нормальном режиме, как распознать отклонение от нормального поведения, оценить симптомы и какие действия предпринять.

## NETWORK SUPERVISION

### Fluke Networks

P.O. Box 777, Everett, WA USA 98206-0777

**Fluke Networks** operates in more than 50 countries worldwide. To find your local office contact details, go to [www.flukenetworks.com/contact](http://www.flukenetworks.com/contact).

©2009 Fluke Corporation. All rights reserved.  
Printed in U.S.A. 4/2009 3467655 Rev A