Тестер-анализатор сетей Ethernet Беркут-ET

Руководство по тестированию
МТРГ.468166.001 РЭ2
Версия 1.0.1-0, 2016

НТЦ Метротек

Оглавление

1. Введение

Настоящее руководство содержит описания тестов, схемы подключения и сценарии тестирования для анализатора сетей Ethernet Беркут-ЕТ.

Дополнительная информация об устройстве приведена в руководствах, входящих в комплект поставки:

– «Тестер-анализатор сетей Ethernet Беркут-ЕТ. Краткое руководство по эксплуатации»

– «Тестер-анализатор сетей Ethernet Беркут-ЕТ. Руководство по структуре меню»

– «Тестер-анализатор сетей Ethernet Беркут-ЕТ. Руководство по командам удалённого управления»

Примечание. Перед началом работы с прибором рекомендуется изучить краткое руководство по эксплуатации.

2. Условные обозначения и сокращения

В тексте руководства без расшифровки будут применяться сокращения, приведённые в таблице ниже.

Таблица 2.1. *Сокращения*

Сокращение	**Комментарий**
DUT	Device under test (Тестируемое устройство)
NUT	Network under test (Тестируемая сеть)
SLA	Service Level Agreement (Соглашение об уровне обслуживания)
QoS	Quality of Service (Качество обслуживания)
ПК	Персональный компьютер
ПО	Программное обеспечение

3. Общая информация о тестировании

3.1. Тестовые конфигурации

Прибор Беркут-ET позволяет *одновременно* проводить два независимых теста RFC-2544 и BERT в следующих комбинациях[1]:

- BERT и BERT;
- RFC-2544 и RFC-2544;
- BERT и RFC-2544;
- RFC-2544 и BERT.

На рисунке 3.1 схематично представлен один из четырёх вариантов тестирования: с порта A на порт B проводится тест по методике RFC-2544, с порта B на порт A — BERT.

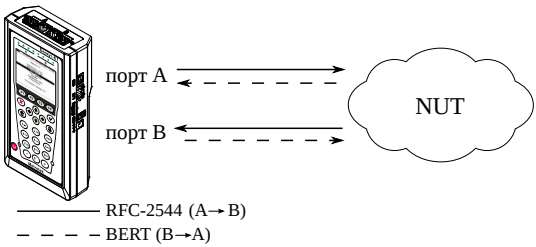


Рис. 3.1. *Схема подключения*

Для переключения между тестовыми конфигурациями используются клавиши (1 ⌣) и (2 ABC). Номер выбранной в данный момент конфигурации отображается в строке статуса[2] справа от индикатора заряда батареи.

[1] В базовую конфигурация не входит. Доступно при дополнительном заказе опции «ET2P».

[2] Подробная информация представлена в брошюре «Тестер-анализатор сетей Ethernet Беркут-ET. Руководство по структуре меню»

4. Методика RFC 2544

Методика RFC 2544 [1] определяет набор тестов, которые используются при оценке важнейших параметров сетевых устройств и проверке соответствия предоставляемых услуг характеристикам, которые оговариваются в SLA между операторами связи и клиентами.

Беркут-ET позволяет проводить четыре стандартных теста согласно рекомендациям RFC 2544: анализ пропускной способности, задержки, уровня потерь кадров и предельной нагрузки.

4.1. Анализ пропускной способности

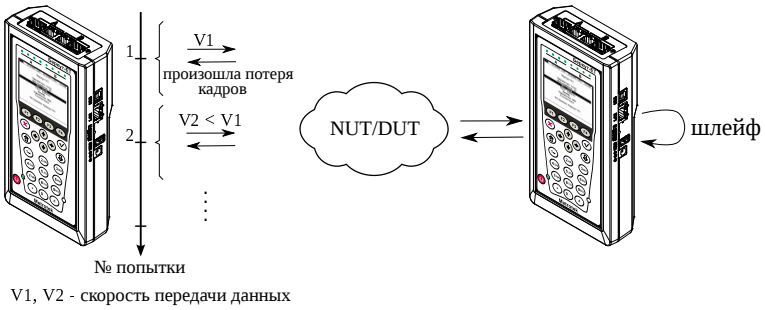


Рис. 4.1. *Анализ пропускной способности*

Примечание. Анализ пропускной способности проводится с целью определения максимально возможной скорости коммутации для сетевых элементов в транспортных сетях Ethernet.

Пропускная способность — максимальная скорость передачи данных, на которой количество кадров[1], прошедших через DUT, равно количеству кадров, отправленных ему с тестирующего оборудования. При анализе пропускной способности используется метод бинарного поиска.

Для определения пропускной способности некоторое количество пакетов с заданной скоростью передаётся на вход DUT (рис. 4.1). Затем подсчитывается количество пакетов, пришедших с выходного порта DUT. Если оно оказывается

[1] Термины *кадр* и *пакет* в описаниях тестов являются синонимами.

равным количеству отправленных пакетов, то тест завершается, так как окончился успешно на заданной пользователем скорости.

Если количество принятых пакетов оказывается меньше, чем количество переданных, то начинается поиск максимально возможной скорости, на которой отсутствуют потери: текущая скорость уменьшается вдвое, и тест повторяется. Если в ходе нового теста потерь нет, скорость увеличивается на половину, согласно алгоритму бинарного поиска. Если потери были — скорость уменьшается вдвое. После изменения скорости тест повторяется. Измерения выполняются до тех пор, пока не будет найдено значение, близкое к значению действительной пропускной способности с точностью, указанной в настройках теста.

4.2. Анализ задержки

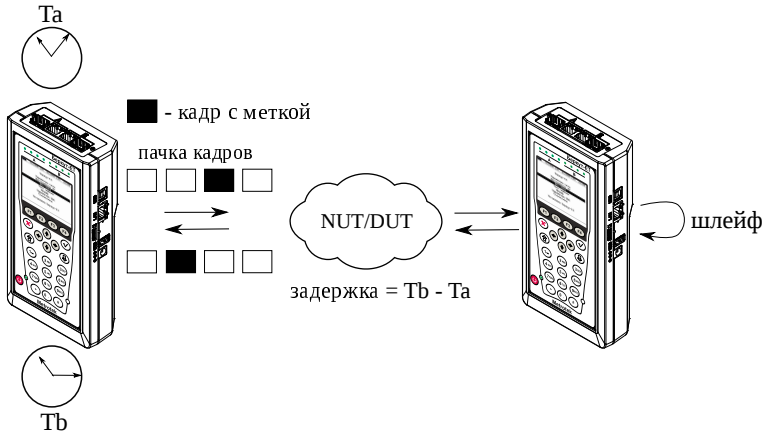
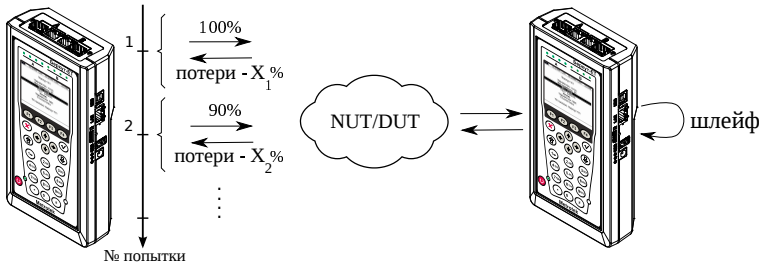


Рис. 4.2. *Анализ задержки*

Примечание. Анализ задержки позволяет оценить время, которое необходимо кадру для прохождения от источника к получателю и обратно. Изменение величины задержки может приводить к проблемам в работе сервисов реального времени.

При анализе задержки для каждого размера пакета на заданной (или полученной в результате теста «Пропускная способность») скорости отправляется поток кадров, адресованных получателю. В пакеты вставляются метки определенного формата. На передающей стороне записывается значение `Ta` — время, к которому пакет с меткой был полностью передан. На приёмной стороне определяется метка и записывается значение `Tb` — время приёма пакета с меткой. Задержка представляет собой разницу значений этих меток: `Tb - Ta`. По результатам анализа вычисляется средняя задержка.

4.3. Анализ уровня потерь кадров



$X_1\%$, $X_2\%$ – потери при соответствующей нагрузке

Рис. 4.3. *Анализ уровня потерь кадров*

Примечание. Анализ уровня потерь кадров необходим для проверки способности сети поддерживать приложения, которые работают в реальном времени (без возможности повторной передачи), так как большой процент потерь кадров приведёт к ухудшению качества сервиса. Данный тест позволяет рассчитать процент кадров, которые не были переданы сетевым элементом при постоянной нагрузке из-за недостатка аппаратных ресурсов.

При анализе уровня потерь кадров на вход DUT на заданной начальной скорости посылается некоторое количество кадров (`input count`) и подсчитывается количество пакетов, пришедших с выходного порта DUT (`output count`). Испытания повторяют, уменьшая скорость тестового потока до заданного конечного значения, пока в двух попытках подряд не будет потеряно ни одного кадра. Уровень потерь кадров рассчитывается по формуле:

$$\frac{100 \times (input\,count - output\,count)}{(input\,count)}$$

4.4. Анализ предельной нагрузки

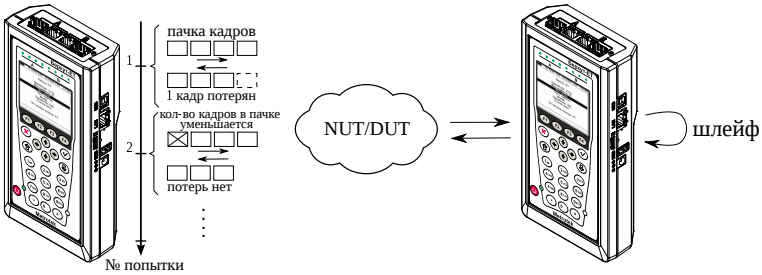


Рис. 4.4. *Анализ предельной нагрузки*

Примечание. Анализ предельной нагрузки позволяет оценить время, в течение которого устройство справляется с максимальной нагрузкой.

При анализе предельной нагрузки на вход DUT отсылаются кадры с заданной (или полученной в результате теста «Пропускная способность») скоростью и подсчитывается количество пакетов с выхода DUT. Если оно оказывается равным количеству отправленных кадров, то тест заканчивается. Если же количество пакетов на выходе DUT меньше числа отправленных, то время уменьшается и тест повторяется.

4.5. Схемы подключения прибора

Для проведения анализа по методике RFC 2544 необходимо подключить прибор к тестируемому устройству/сети в соответствии с одной из схем, приведённых ниже.

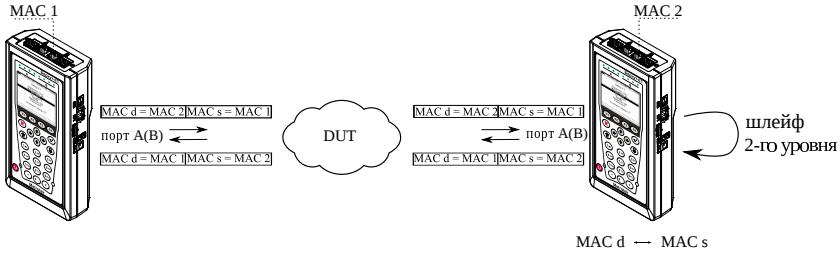


Рис. 4.5. *Типовая схема подключения 1*

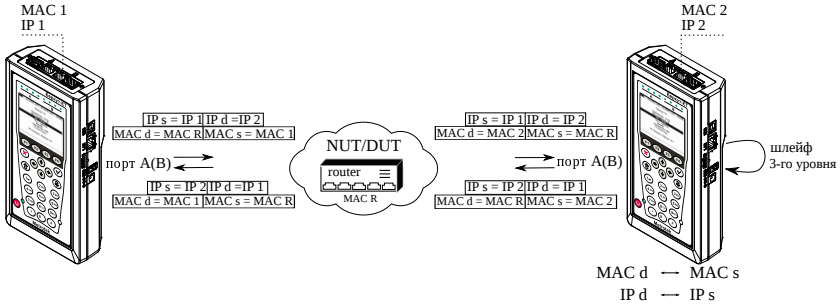


Рис. 4.6. *Типовая схема подключения 2*

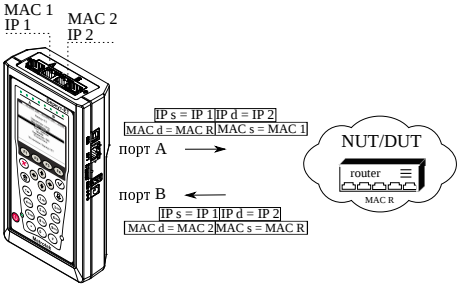


Рис. 4.7. *Типовая схема подключения 3*

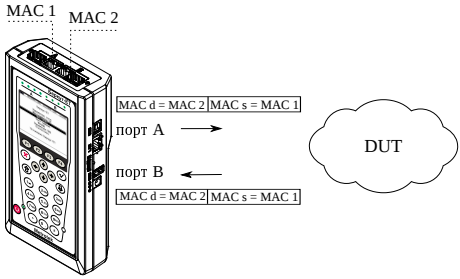


Рис. 4.8. *Типовая схема подключения 4*

На схемах подключения введены следующие обозначения:

MAC s	MAC-адрес отправителя
MAC d	MAC-адрес получателя
MAC R	MAC-адрес шлюза
IP s	IP-адрес отправителя
IP d	IP-адрес получателя

В случае тестирования сетей, содержащих устройства, работающие на канальном уровне модели OSI[2], Беркут-ЕТ подключают в соответствии со схемой, приведённой на рис. 4.5. Генерируемый прибором трафик должен быть перенаправлен обратно посредством организации шлейфа. При этом во входящих пакетах меняются местами MAC-адреса отправителя и получателя, и трафик возвращается на исходный порт.

В случае тестирования сетей, содержащих устройства, работающие на сетевом уровне модели OSI[3], Беркут-ЕТ подключают в соответствии со схемой, приведённой на рис. 4.6. Генерируемый прибором трафик должен быть перенаправлен обратно посредством организации шлейфа. При этом во входящих пакетах меняются местами и MAC- и IP-адреса отправителя и получателя, и трафик возвращается на исходный порт.

В случае тестирования устройств/сетей с возможностью маршрутизации IP-трафика используются два порта (см. рис. 4.7, 4.8), а пакеты перенаправляются на другой порт прибора при помощи маршрутизатора или сетевого коммутатора.

[2] Например, сетевой коммутатор (switch).
[3] Например, маршрутизатор (router).

5. Y.1564

Основной задачей при тестировании Ethernet-сетей является определение соответствия предоставляемых услуг (например, видео, телефонии, электронной почты, онлайн-игр и т.д.) характеристикам, которые оговариваются в соглашении об уровне обслуживания (SLA — Service Level Agreement) между операторами связи и клиентами. На первом месте стоят вопросы обеспечения гарантированного качества обслуживания (QoS — Quality of Service), которое характеризуется различными показателями (см. раздел 5.1). В настоящее время существует две основные методики для оценки этих параметров — RFC 2544 [1] и ITU-T Y.1564 [5] (сравнение методик приведено в разделе 5.2).

5.1. Показатели качества

Основные показатели качества предоставляемого сервиса[1] (SAC — Service Acceptance Criteria):

1. FTD (Frame Transfer Delay) — задержка распространения кадров.
2. FDV (Frame Delay Variation) — отклонение задержки распространения кадров.
3. FLR (Frame Loss Ratio) — уровень потерь кадров.
4. CIR (Committed Information Rate) — гарантированная полоса пропускания для сервиса.
5. EIR (Excess Information Rate) — максимально допустимое превышение CIR.
6. M-фактор — максимально допустимое превышение величины CIR+EIR.

[1] Термины *услуга*, *служба* и *сервис* в данном описании являются синонимами

5.2. Сравнение RFC 2544 и ITU-T Y.1564

Методика RFC 2544 была создана для тестирования максимальной производительности сетевого оборудования и подходит для оценки этого параметра в случае отдельного канала или устройства. Но с появлением в каналах различных служб, работающих одновременно, выявился ряд недостатков методики.

Рекомендация ITU-T Y.1564 учитывает эти недостатки и ориентирована на тестирование мультисервисных сетей, позволяя провести быструю оценку соответствия сети требованиям SLA.

	RFC 2544	ITU-T Y.1564
Измерение FTD	√	√
Измерение FDV[2]	—	√
Измерение FLR	√	√
Анализ одновременной работы нескольких служб	—	√
Время тестирования	Для проверки соответствия SLA требуется провести последовательность повторяющихся тестов. В связи с этим тестирование может занять продолжительное время.	Для проведения теста конфигурации одной услуги требуется не более 6 минут. Длительность теста производительности может быть задана от нескольких секунд до нескольких суток.

Таким образом, тестирование по рекомендации Y.1564 позволяет однозначно определить соответствие канала параметрам, заявленным в SLA, а также существенно сократить временные затраты на анализ за счёт одновременной оценки нескольких служб.

5.3. Тесты конфигурации

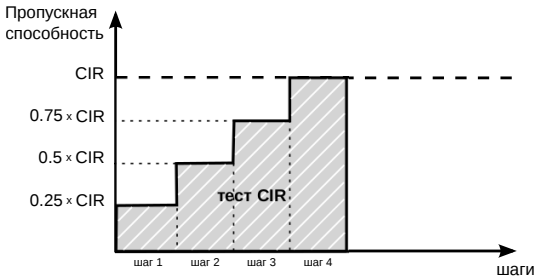
Тесты конфигурации состоят из трёх независимых тестов — CIR, EIR и Traffic Policing. С их помощью каждый сервис проверяется на соответствие заданным параметрам SAC, а также оценивается, остаётся ли пропускная способность в установленных пределах при увеличении нагрузки. Цель — убедиться в том, что настройки сети позволяют каждому сервису работать отдельно от других служб с заявленной производительностью. При проведении данных тестов сервисы проверяются по очереди, для оценки одновременной работы применяется тест производительности (см. раздел 5.4).

[2] Величина FDV является ключевым параметром для VoIP/IPTV и используется при настройке буферизации трафика.

5.3.1. Тест CIR

Тест CIR используется для проверки того, что при передаче данных с нагрузкой на уровне CIR показатели качества находятся в пределах, установленных SLA. В ходе данного теста измеряются основные показатели качества каждого сервиса (FTD, FDV, FLR), после чего эти значения сравниваются с заданными параметрами SAC.

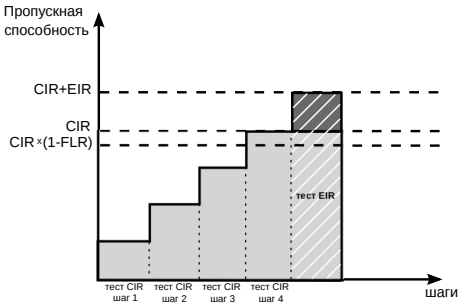
Прибор Беркут-ЕТ позволяет задавать количество шагов для проведения тестирования: 1 шаг — тест CIR будет проведён при 100 % нагрузке; 2 шага — тест будет проведён в два этапа: 50 и 100 % от заданной нагрузки; 3 шага — тест будет проведён в три этапа: 50, 75 и 100 % от заданной нагрузки; 4 шага — тест будет проведён в четыре этапа: 25, 50, 75 и 100 % от заданной нагрузки.



5.3.2. Тест EIR

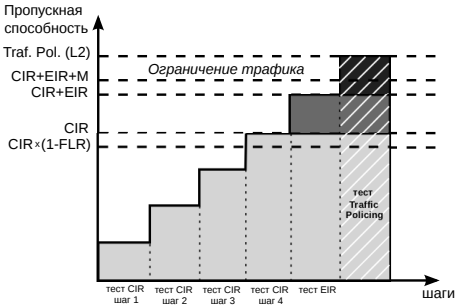
Тест EIR служит для проверки того, что при передаче данных с нагрузкой на уровне CIR+EIR результирующая пропускная способность для каждого сервиса не превышает допустимое значение и находится в пределах от CIR (с учётом заданного уровня потерь кадров) до CIR+EIR: $CIR \times (1\text{-}FLR) \leq IR \leq CIR+EIR$. Величина потерь кадров (FLR) устанавливается пользователем.

Примечание. Режим «colour-aware» (возможность помечать «цветом» передаваемые кадры) не поддерживается.



5.3.3. Тест Traffic Policing

Тест Traffic Policing используется для проверки того, что при передаче данных с нагрузкой, превышающей разрешённую для сервиса, сеть будет ограничивать его полосу пропускания. Нагрузка для этого теста, устанавливаемая пользователем, должна превышать уровень CIR+EIR .



5.4. Тест производительности

Тест производительности используется для оценки одновременной работы всех сервисов. При проведении теста выполняется передача данных для всех служб одновременно с нагрузкой на уровне CIR и проверяются значения показателей качества для каждого сервиса. Единственной настройкой теста является его длительность, которая может составлять от нескольких минут до 4-х дней.

5.5. M-фактор

При проведении теста Traffic Policing в результате буферизации в некоторые моменты времени на приёме оказывается больше данных, чем отведено для сервиса. Это является особенностью, а не сбоем в работе сети. Чтобы учесть эту особенность, в ITU-T Y.1564 используется M-фактор — максимально допустимое превышение величины CIR+EIR (см. ITU-T Y.1564 п. C.2 разд. 8.1.2).

5.6. Алгоритм измерения FTD

Для измерения задержки распространения кадров (FTD) выполняются следующие действия:

1. На передающей стороне в каждый пакет вставляется временная метка (Ta).
2. На приёмной стороне записывается значение времени приёма пакета с меткой (Tb).
3. Вычисляется задержка прохождения пакета в сети: $Tb - Ta$.

   Примечание. Приёмником и передатчиком должен быть один и тот же прибор или два прибора, синхронизированных по протоколу PTP.
4. Фиксируются три значения задержки — минимальное (FTD_min), среднее (FTD_avg) и максимальное (FTD_max). Среднее значение задержки вычисляется как сумма задержек для всех принятых пакетов, поделенная на количество принятых пакетов.

   Эти значения отображаются в результатах теста производительности для каждого сервиса. Для сводного теста производительности и тестов конфигурации выводятся средние значения.

5.7. Алгоритм измерения FDV

Отклонение задержки распространения кадров (FDV) в соответствии с рекомендацией ITU-T Y.1563 [7] измеряется по формуле: $FDV = FTD - FTD\_min$.

Например, если были измерены значения задержки распространения кадров: $FTD\_min = 1.5, FTD\_avg = 2.5, FTD\_max = 5.5$, то значения FDV будут следующими: $FDV\_min = 0, FDV\_avg = 1.0, FDV\_max = 4.0$.

Эти величины отображаются в результатах теста производительности для каждого сервиса. Для сводного теста производительности и тестов конфигурации выводятся средние значения.

6. Асимметричное тестирование

Функция асимметричного тестирования[1] используется при проверке работоспособности каналов связи, для которых параметры приёма и передачи данных (пропускная способность, задержка и т.д.) различны, — асимметричных каналов.

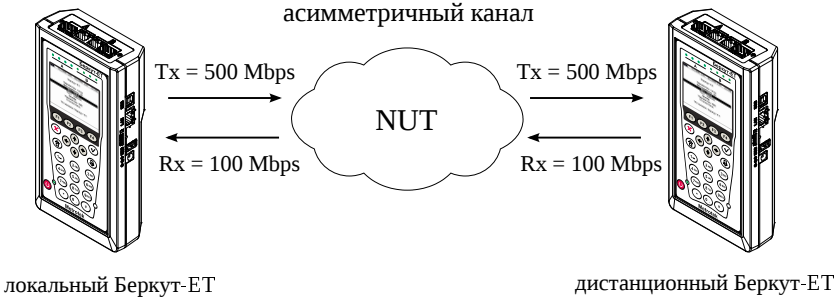


Рис. 6.1. *Пример асимметричного канала*

Из-за этой особенности каналов измерения должны быть выполнены независимо для каждого направления. Отличительная черта такого типа тестирования — передача тестового трафика производится в одном, выбранном пользователем, направлении. При проведении тестирования используется 2 прибора Беркут-ET: локальный, на котором производится настройка параметров анализа, и дистанционный, находящийся на другом конце асимметричного канала. Результаты тестирования отображаются на экране локального прибора.

Примечание. Функция асимметричного тестирования доступна при проведении анализа по методике RFC 2544 (пропускная способность, задержка, потери кадров, предельная нагрузка), тестов «BERT» и «Y.1564».

Примечание. При анализе задержки по методике RFC 2544, а также при тестировании в соответствии с рекомендацией Y.1564 следует использовать PTP-синхронизацию.

[1] В базовую конфигурацию не входит. Доступна при дополнительном заказе опции «ETAT».

6.1. Пример тестирования

Ниже рассматривается пример использования функции асимметричного тестирования для проведения анализа по рекомендации «Y.1564» (для тестов «BERT» и «RFC 2544» порядок действий аналогичен).

На рис. 6.2 приведена типовая схема подключения приборов к тестируемой сети с использованием порта A. Для порта B схема подключения будет аналогичной.

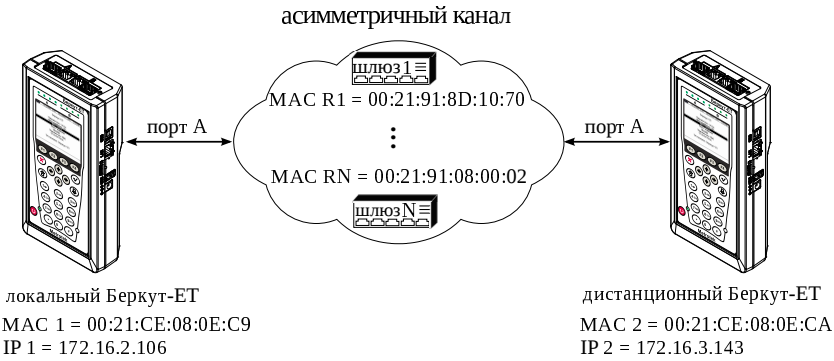


Рис. 6.2. *Типовая схема подключения*

На схеме введены следующие обозначения:

`MAC 1` — MAC-адрес порта A локального прибора;
`IP 1` — IP-адрес локального прибора;
`MAC R1` — MAC-адрес шлюза, ближайшего к локальному прибору;
`MAC RN` — MAC-адрес шлюза, ближайшего к дистанционному прибору;
`MAC 2` — MAC-адрес порта A дистанционного прибора;
`IP 2` — IP-адрес дистанционного прибора.

Для измерения параметров канала связи в направлении от локального прибора к дистанционному необходимо:

1. Убедиться, что локальный и дистанционный приборы поддерживают функцию асимметричного тестирования: в меню «Беркут-ЕТ. Настройки» ⇒ «Установки прибора» ⇒ «Опции» в списке опций должна присутствовать опция «ETAT».
2. Подключить локальный и дистанционный Беркут-ЕТ по схеме, представленной на рис. 6.2.

3. На локальном и на дистанционном приборе перейти в меню «Беркут-ET. Настройки» ⇒ «Параметры сети». Выбрать:

   `Порт - A`

   Одним из приведённых ниже способов установить IP-адрес локального прибора (IP 1) и IP-адрес дистанционного прибора (IP 2):

   – ввести IP-адрес вручную (при этом пункт меню «DHCP» должен находиться в состоянии «Выкл»);

   – получить IP-адрес по протоколу DHCP, выбрав пункт меню «DHCP» и нажав на клавишу F2 («Вкл»): полученный адрес будет корректным, если отобразится в пункте меню «IP-адрес» по истечении не более чем 1-2 секунд.

4. На локальном и на дистанционном приборе перейти в меню «Беркут-ET. Настройки» ⇒ «Синхронизация времени» и выбрать порт A в качестве PTP-порта.

   Примечание. для тестов «BERT» и «RFC 2544» (пропускная способность, потери кадров, предельная нагрузка) выполнять данный пункт не требуется.

5. На локальном приборе перейти в меню «Y.1564» ⇒ «Настройки» ⇒ «Топология тестов» (см. рис. 6.3). Выбрать:

   `Порт передачи - A`

   `Порт приёма - Дистанционный`

   `Дист. IP - IP 2`

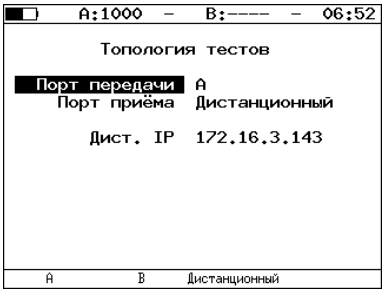


Рис. 6.3. *Экран «Топология тестов»*

6. На локальном приборе перейти в меню «Беркут-ЕТ. Измерения» ⇒ «Y.1564» ⇒ «Настройки» ⇒ «Настройки сервисов» ⇒«Заголовок» (см. рис. 6.4). Выбрать:

   MAC Отпр. - MAC 1

   MAC Получ. - MAC R1

   IP Отпр. - IP 1

   IP Получ. - IP 2

   Примечание. Для получения MAC-адреса шлюза необходимо выполнить ARP-запрос: перейти к пункту меню «MAC Получ.» и нажать на клавишу F3 .

Рис. 6.4. *Экран «Заголовок»*

7. На локальном приборе в соответствии с указаниями раздела 5 выполнить необходимые настройки теста «Y.1564». Затем перейти в меню «Беркут-ЕТ. Измерения» ⇒ «Y.1564» и нажать на клавишу F1 («Старт»).

Примечание. После нажатия на клавишу «Старт» на экране локального прибора могут появиться следующие сообщения:

- «Идёт подключение к дист. порту ...» — возникает сразу после запуска теста.
- «Дистанционный прибор недоступен» — возникает в случае, если не получилось установить соединение с дистанционным прибором.
- «Потеряно соединение» — возникает в случае, если дистанционный прибор после установления соединения перестал отвечать на запросы.
- «Дистанционный прибор занят» — возникает, когда на дистанционном приборе уже проводится какой-либо тест.
- «Дист. BERT 1-го уровня невозможен» — возникает при попытке провести тест «BERT» первого уровня.

Примечание. На экране дистанционного прибора во время тестирования отображается сообщение «Выполняется дистанционный тест».

Для измерения параметров канала связи в направлении от дистанционного прибора к локальному необходимо:

1. Убедиться, что локальный и дистанционный приборы поддерживают функцию асимметричного тестирования: в меню «Беркут-ЕТ. Настройки» ⇒ «Установки прибора» ⇒ «Опции» в списке опций должна присутствовать опция «ETAT».
2. Подключить локальный Беркут-ЕТ и дистанционный Беркут-ЕТ по схеме, представленной на рис. 6.2.
3. На локальном и на дистанционном приборе перейти в меню «Беркут-ЕТ. Настройки» ⇒ «Параметры сети». Выбрать:

   ```
   Порт - A
   ```

   Одним из приведённых ниже способов установить IP-адрес локального прибора (IP 1) и IP-адрес дистанционного прибора (IP 2):

   – ввести IP-адрес вручную (при этом пункт меню «DHCP» должен находиться в состоянии «Выкл»);
   – получить IP-адрес по протоколу DHCP, выбрав пункт меню «DHCP» и нажав на клавишу F2 («Вкл»): полученный адрес будет корректным, если отобразится в пункте меню «IP-адрес» по истечении не более чем 1-2 секунд.

4. На локальном и на дистанционном приборе перейти в меню «Беркут-ЕТ. Настройки» ⇒ «Синхронизация времени» и выбрать порт A в качестве PTP-порта.

   Примечание. Для тестов «BERT» и «RFC 2544» (пропускная способность, потери кадров, предельная нагрузка) выполнять данный пункт не требуется.

5. На локальном приборе перейти в меню «Y.1564» ⇒ «Настройки» ⇒ «Топология тестов» (см. рис. 6.5). Выбрать:

   ```
   Порт передачи - Дистанционный
   Порт приёма - A
   Дист. IP - IP 2
   ```

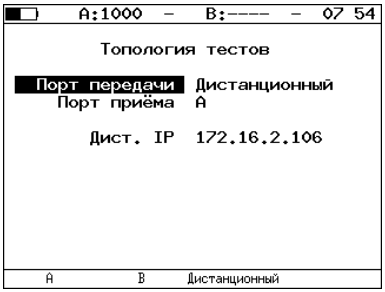


Рис. 6.5. *Экран «Топология тестов»*

6. На локальном приборе перейти в меню «Беркут-ЕТ. Измерения» ⇒ «Y.1564» ⇒ «Настройки» ⇒ «Настройки сервисов» ⇒«Заголовок» (см. рис. 6.6). Выбрать:

   MAC Отпр. - MAC 2

   MAC Получ. - MAC RN

   IP Отпр. - IP 2

   IP Получ. - IP 1

Рис. 6.6. *Экран «Заголовок»*

7. На локальном приборе в соответствии с указаниями раздела 5 выполнить необходимые настройки теста «Y.1564». Затем перейти в меню «Беркут-ЕТ. Измерения» ⇒ «Y.1564» и нажать на клавишу F1 («Старт»).

Примечание. После нажатия на клавишу «Старт» на экране локального и дистанционного прибора появятся сообщения, аналогичные перечисленным на с. 22.

7. Шлейф

Для тестирования сетей по методике RFC 2544, измерения BER и решения ряда других задач используется функция «Шлейф», позволяющая перенаправлять обратно приходящий на прибор трафик на четырёх уровнях модели OSI:

1. На физическом уровне (L1) весь входящий трафик перенаправляется обратно без изменений, при этом ведётся статистика по принимаемому трафику.
2. На канальном уровне (L2) все входящие кадры перенаправляются обратно, при этом меняются местами MAC-адреса отправителя и получателя. Ведётся статистика по принимаемому и передаваемому трафику.
3. На сетевом уровне (L3) все входящие пакеты перенаправляются обратно, при этом меняются местами MAC-адреса отправителя и получателя. Если поле «EtherType» имеет значение 0x0800, также меняются местами IP-адреса отправителя и получателя. Ведётся статистика по принимаемому и передаваемому трафику.
4. На транспортном уровне (L4) весь входящий трафик перенаправляется обратно, при этом меняются местами MAC-адреса отправителя и получателя. Если поле EtherType имеет значение 0x0800, также меняются местами IP-адреса отправителя и получателя. Номера TCP/UDP-портов отправителя и получателя меняются местами, если поле «Protocol» имеет значение 6 (TCP) или 17 (UDP).

Примечание. Для шлейфа канального (L2), сетевого (L3) и транспортного (L4) уровней повреждённые пакеты не перенаправляются.

Примечание. Для шлейфа канального (L2), сетевого (L3) и транспортного (L4) уровней пакеты с одинаковыми MAC Dst и MAC Src, а так же блоки данных протокола OAM (OAMPDU) и ARP-запросы, содержащиеся во входящем трафике, не перенаправляются.

Примечание. Если входящий пакет содержит MPLS метку, он будет перенаправлен без изменения её значения.

8. OAM

Важной задачей поставщиков услуг связи является обеспечение высокого уровня администрирования и технического обслуживания Ethernet-сетей. Для этих целей был разработан стандарт IEEE 802.3ah [6] (известный также как «Ethernet in the First Mile (EFM) OAM» — «Ethernet OAM на «первой миле»).

OAM (Operations, Administration, and Maintenance — эксплуатация, администрирование и обслуживание) — протокол мониторинга состояния канала, функционирует на канальном уровне модели OSI. Для передачи информации между Ethernet-устройствами используются блоки данных протокола — OAMPDU.

Важной функцией протокола OAM является возможность включения режима «Шлейф» на удалённом приборе.

Для установления соединения между прибором Беркут-ЕТ и удалённым устройством по протоколу OAM и для включения режима «Шлейф» необходимо:

1. *Непосредственно* соединить локальный Беркут-ЕТ и удалённое устройство[1] в соответствии со схемой, приведённой ниже.

Рис. 8.1. *Схема тестирования*

2. На удалённом приборе разрешить работу протокола OAM в активном или пассивном режиме.

   На локальном приборе:

3. Перейти в меню «OAM» (см. рис. 8.2).
4. В пункте меню «Порт» выбрать порт, к которому подсоединено удалённое устройство.
5. В пункте меню «Режим» выбрать активный режим работы протокола OAM.

[1] На рис. 8.1 Беркут-ЕТ приведён в качестве примера удалённого устройства.

6. Состояние обнаружения удалённого устройства в пункте меню «Обнаружение» должно принять значение «Send any».
7. Перейти в меню «Удалённый прибор». На экране должна отобразиться информация об удалённом устройстве.
8. Нажать на клавишу F1 («LB up»). На удалённом устройстве будет включён режим «Шлейф» второго (L2) уровня (трафик будет перенаправляться *без замены MAC-адресов*).

Для выключения режима «Шлейф» необходимо нажать на клавишу F1 («LB down»).

Рис. 8.2. *Меню «OAM»*

9. ET-обнаружение

Функция «ET-обнаружение» позволяет включить шлейф канального (L2), сетевого (L3) или транспортного (L4) уровня на удалённом анализаторе Беркут-ET или устройстве образования шлейфа Беркут-ETL.

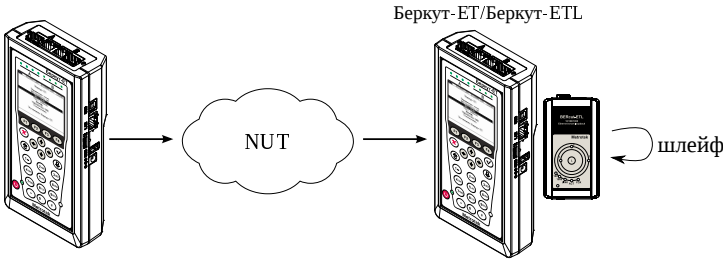


Рис. 9.1. *Схема тестирования*

Шлейф можно включать *последовательно* на нескольких приборах Беркут-ET и/или Беркут - ETL, находящихся как в разных, так и в одной подсети.

Для получения данных об удалённом приборе и включения шлейфа следует:

1. Подключить прибор Беркут-ET к сети.
2. Перейти в меню «ET-обнаружение»:

Рис. 9.2. *Меню «ET-обнаружение»*

3. Выбрать порт, с которого будет осуществляться передача данных.

4. В поле «IP» ввести IP-адрес удалённого устройства.
5. Нажать на клавишу F4 («Обнаружение»).

В случае успешного обнаружения устройства на экран будут выведены его IP-адрес, имя и MAC-адрес (см. рис. 9.3). Пункт меню «Шлейф» станет доступным для редактирования.

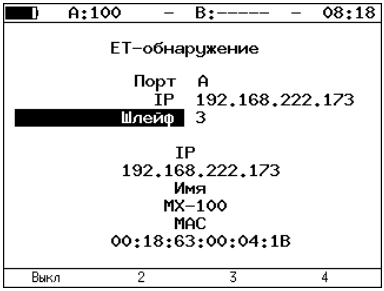


Рис. 9.3. *Пример выполнения ET-обнаружения*

Уровень шлейфа выбирается кнопками:

F1 — выключение режима «Шлейф»;
F2 — включение шлейфа канального уровня;
F3 — включение шлейфа сетевого уровня;
F4 — включение шлейфа транспортного уровня.

Примечание. Передача данных осуществляется по протоколу UDP. Порт получателя — 32 792. Порт отправителя — 32 793.

10. Тесты TCP/IP

Тесты, описанные в данном разделе, необходимы при проведении анализа в сетях, содержащих устройства, осуществляющие коммутацию и маршрутизацию передаваемых данных. С помощью реализованных в приборе Беркут-ET TCP/IP тестов можно обнаружить проблемы, связанные с конфигурацией сети, убедиться в связности канала между её узлами, определить маршруты следования данных, проверить работоспособность и оценить загруженность каналов передачи данных.

10.1. Эхо-запрос (Ping)

Инструмент «Эхо-запрос»[1] используется для проверки связности канала между узлами сети.

В процессе тестирования сетевому узлу посылаются запросы и фиксируются поступающие ответы. Эта процедура основывается на IP- и ICMP-протоколах пересылки дейтаграмм и позволяет проверить работоспособность каналов передачи данных и промежуточных устройств.

Для проведения анализа необходимо:

1. Подключить прибор к тестируемой сети с использованием одного порта в соответствии со схемой, приведённой ниже:

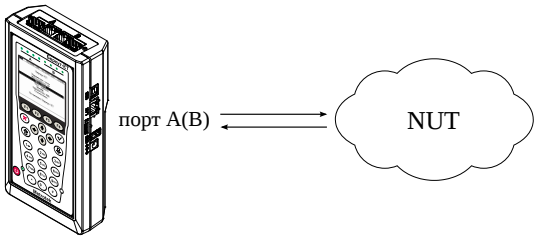


Рис. 10.1. *Вариант подключения 1*

Примечание. Прибор также может быть подключён к сети с использованием двух портов (см. рис. 10.2). Настройки прибора для данного случая аналогичны описанным настройкам для одного порта.

[1] В базовую конфигурацию не входит. Доступен при дополнительном заказе опции «ETIP».

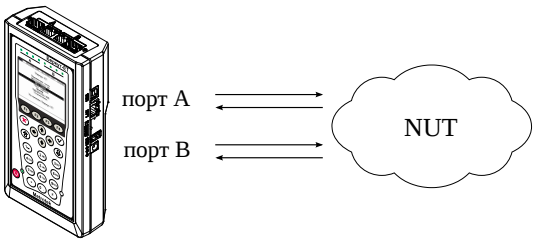


Рис. 10.2. *Вариант подключения 2*

2. Перейти в меню «Эхо-запрос». Нажать на клавишу F3 («Настройки»):

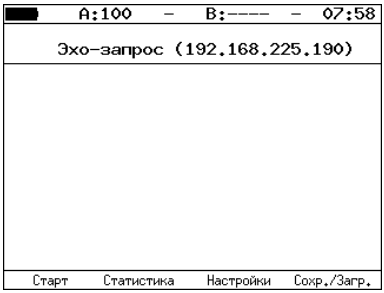


Рис. 10.3. *Меню «Эхо-запрос»*

3. Настроить параметры тестирования в меню «Настройки эхо-запроса»:

Рис. 10.4. *Меню «Настройки эхо-запроса»*

4. Нажать на клавишу F1 («Старт»). Начнётся тестирование, в ходе которого на экран будут выведены строки, содержащие следующую информацию (слева направо):
   - размер ICMP-пакета;
   - IP-адрес узла сети, ответившего на эхо-запрос;
   - порядковый номер пакета;
   - время между отправкой запроса и получением ответа.

   Пример результатов тестирования представлен на рис 10.5.

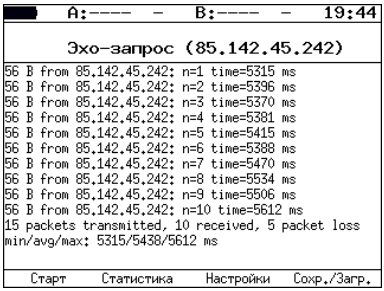


Рис. 10.5. *Результаты теста «Эхо-запрос»*

По результатам тестирования формируется статистика:

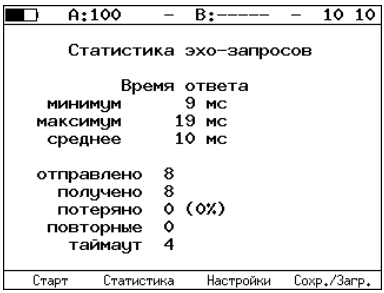


Рис. 10.6. *Статистика теста «Эхо-запрос»*

В статистике отображается информация о минимальном, среднем, максимальном времени между отправкой запроса и получением ответа, а также о количестве переданных, принятых, потерянных и повторных (с одинаковым порядковым номером) пакетов. Значение в строке *таймаут* соответствует количеству пакетов, для которых время ответа на эхо-запрос было превышено.

10.2. Маршрут (Traceroute)

Инструмент «Маршрут»[2] используется для определения маршрутов следования данных в сетях на основе TCP/IP. В процессе тестирования указанному узлу сети отправляется последовательность дейтаграмм, при этом отображаются сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к конечному узлу. Таким образом, инструмент «Маршрут» позволяет диагностировать доступность промежуточных пунктов на пути передачи потока данных в сети.

Для проведения анализа необходимо:

1. Подключить прибор к тестируемой сети в соответствии со схемой, приведённой на рис. 10.1.
2. Перейти в меню «Маршрут»:

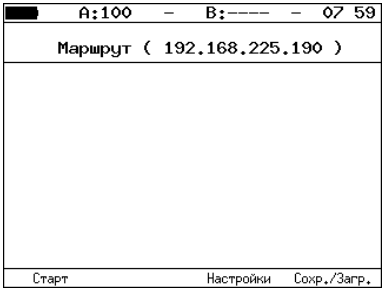


Рис. 10.7. *Меню «Маршрут»*

3. Настроить параметры тестирования в меню «Настройки маршрута»:

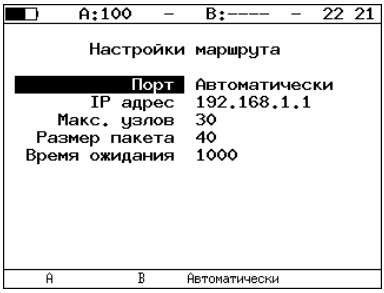


Рис. 10.8. *Меню «Настройки маршрута»*

[2] В базовую конфигурацию не входит. Доступен при дополнительном заказе опции «ETIP».

4. Нажать на клавишу F1 («Старт»). Начнётся тестирование, в ходе которого на экран будут выведены строки, содержащие следующую информацию (слева направо):

   – номер промежуточного узла;
   – IP-адрес промежуточного узла;
   – время ожидания ответа.

   Если время ожидания ответа от промежуточного узла превысило таймаут, в строке результатов будет выведен значок «*».

   Пример результатов тестирования представлен на рис. 10.9

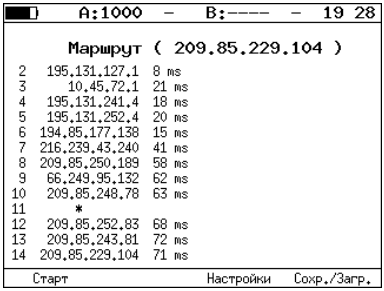


Рис. 10.9. *Результаты теста «Маршрут»*

10.3. DNS (DNS lookup)

DNS (Domain Name System — система доменных имён) — распределённая база данных, способная по запросу, содержащему доменное имя узла, сообщить его IP-адрес. Функция DNS lookup[3] (поиск на сервере имён) помогает обнаружить ошибки в работе NS-серверов.

Для проведения анализа необходимо:

1. Подключить прибор к тестируемой сети в соответствии со схемой, приведённой на рис. 10.1.
2. Перейти в меню «DNS» (см. рис. 10.10).
3. В пункте меню «Порт» указать порт для приёма и передачи данных.
4. В пункте меню «Узел» ввести доменное имя узла. Нажать F1 («Старт»).
5. В пункте меню «IP» будет выведен IP-адрес узла. Если адрес определить не удалось, то отобразится нулевой IP-адрес (0.0.0.0).

Пример результатов тестирования представлен на рис. 10.10.

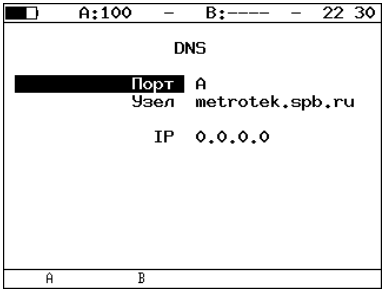


Рис. 10.10. *Меню «DNS»*

[3] В базовую конфигурацию не входит. Доступна при дополнительном заказе опции «ETIP».

10.4. Монитор ARP-запросов

Функция «ARP монитор» позволяет отслеживать ARP-ответы, передающиеся в сети, и «перехватывать» содержащиеся в них IP- и MAC-адреса сетевых устройств. На основании полученных данных формируется список адресов.

Для проведения анализа необходимо:

1. Подключить прибор к тестируемой сети в соответствии со схемой, приведённой на рис. 10.1 или на рис. 10.2.
2. Перейти в меню «ARP монитор»:

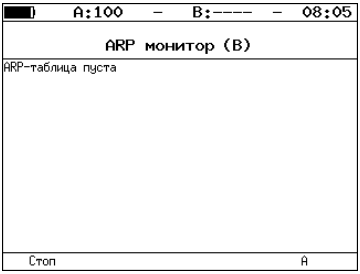


Рис. 10.11. *Меню «ARP монитор»*

3. Нажать на клавишу F4 для выбора порта (A или B).
4. Через некоторое время надпись «ARP-таблица пуста» исчезнет и на экран будут выводиться IP- и MAC-адреса сетевых устройств:

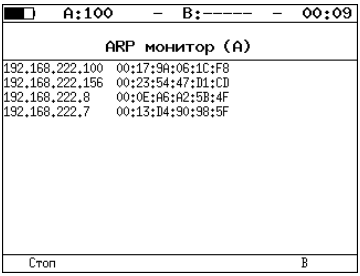


Рис. 10.12. *Экран «ARP монитор»*

Если какая-то из записей не обновится в течение одной минуты, то она будет удалена из списка.

5. Для завершения тестирования нажать на клавишу F1 («Стоп»).

10.5. TCP-клиент

Функция «TCP-клиент»[4] позволяет установить TCP-соединение с удалённым узлом сети, принимать от него данные и передавать данные этому узлу.

Для установления соединения необходимо:

1. Подключить прибор к сети в соответствии со схемой, приведённой на рис. 10.1.
2. Настроить параметры соединения (меню «TCP-клиент»⇒«Настройки»(F4)):
   - выбрать порт для приёма и передачи данных;
   - ввести доменное имя или IP-адрес узла;
   - ввести номер порта (наиболее часто используемые номера портов приведены в таблице 10.1).

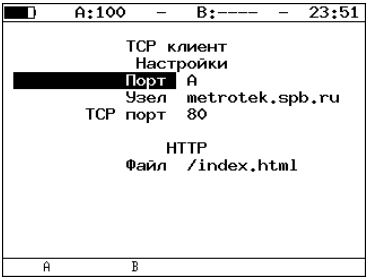


Рис. 10.13. *Настройки теста «TCP-клиент»*

3. Открыть TCP-соединение, нажав на клавишу F1 («Открыть»):

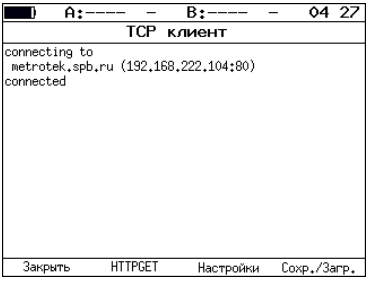


Рис. 10.14. *Пример успешного соединения с узлом*

[4] В базовую конфигурацию не входит. Доступна при дополнительном заказе опции «ETIP».

В случае успешного соединения (см. рис. 10.14) можно выполнить HTTP GET-запрос (см. раздел 10.6). В случае возникновения проблем при установлении соединения выводится сообщение об ошибке. Некоторые сообщения приведены в таблице 10.2.

Таблица 10.1. *Номера портов протокола TCP/IP*

Номер порта (протокол)	**Описание**
21 (FTP)	протокол передачи файлов
22 (SSH)	безопасный протокол для удалённого управления и передачи файлов
23 (TELNET)	протокол для доступа к удалённому сетевому устройству
25 (SMTP)	протокол передачи электронной почты
80 (HTTP(WWW))	протокол, используемый веб-браузерами и веб-серверами для передачи файлов
161 (SNMP)	протокол для управления сетевыми устройствами

Таблица 10.2. *Ошибки соединения*

Сообщение	**Описание**
protocol not supported	протокол не поддерживается
can’t assign requested address	невозможно назначить запрошенный адрес
network is down	сеть недоступна
network is unreachable	сеть не работает
network dropped connection on reset	утеряно соединение с сетью
software caused connection abort	программное обеспечение вызвало разрыв соединения
connection reset by peer	узел разорвал соединение
connection timed out	истекло время ожидания соединения
connection refused	отказ в соединении
host is down	узел не отвечает
no route to host	отсутствует маршрут до узла

10.6. HTTP GET-запрос

Для передачи веб-страниц используется протокол HTTP. В этом протоколе определён HTTP GET-запрос[5]. С его помощью возможно проверить, отвечает ли сервер на HTTP-запросы и получить содержимое указанного ресурса.

Для получения содержимого файла с сервера необходимо:

1. Установить соединение с узлом по алгоритму, описанному в разделе 10.5, указав в поле «Файл» (см. рис. 10.13) имя запрашиваемого файла.
2. Нажать на клавишу F2 «HTTPGET»:

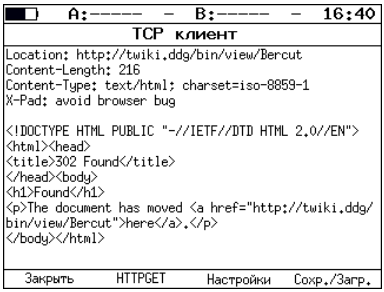


Рис. 10.15. *Пример ответа на HTTP GET-запрос*

[5] Функция доступна при дополнительном заказе опции «ETIP»

10.7. Транзит

В режиме «Транзит» прибор включается в разрыв соединения между двумя сетевыми устройствами. Трафик, приходящий на порт A(B) отправляется на порт B(A), пример подключения показан на рис. 10.16.

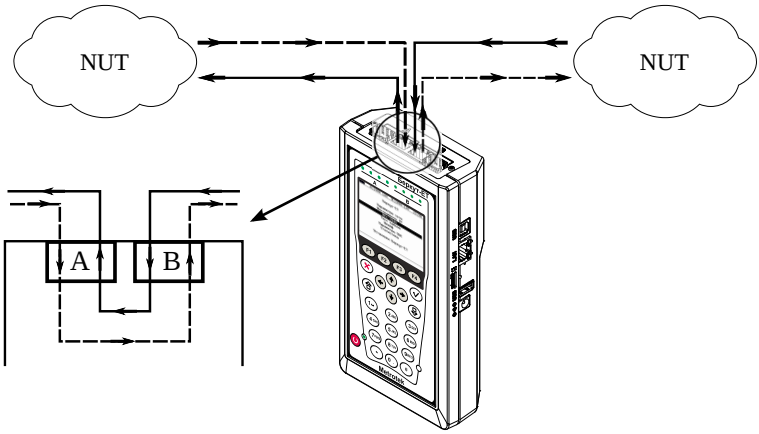


Рис. 10.16. *Пример подключения в режиме «Транзит»*

При передаче данных с порта на порт осуществляется сбор статистических данных о проходящем трафике. Результаты доступны в меню «Статистика». При подсчёте статистики по уровням повреждённые пакеты не учитываются.

Если скорости передачи данных для порта A и для порта B различны, возможны потери при проведении тестирования. Потери произойдут в том случае, если передача ведётся с порта с большей скоростью на порт с меньшей.

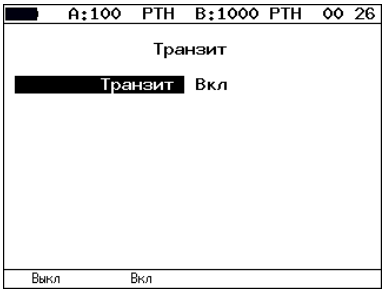


Рис. 10.17. *Меню «Транзит»*

11. BERT

BERT (Bit Error Rate Test) — тест, позволяющий определить основной битовый показатель качества канала – «bit error rate» (коэффициент битовых ошибок), т. е. отношение числа ошибочных бит к общему количеству переданных бит. Известная на приёмном и передающем конце бинарная последовательность помещается в Ethernet-кадр, который передаётся в физическую среду. На приёмном конце последовательность сравнивается с исходной, и вычисляется коэффициент битовых ошибок. Для подключения к TDM-сети используется конвертер интерфейсов, который осуществляет преобразование трафика пакетной сети (Ethernet) в трафик, передаваемый в TDM-сетях.

Тестирование может быть реализовано на четырёх уровнях модели OSI:

1. На физическом уровне данные отправляются частями с определённым межкадровым интервалом (IFG — Interframe Gap). В этом случае тестирование проводится с порта A (B) на порт B (A) (см. рис. 11.5) или используется функция «Шлейф» (см. рис. 11.6).

Рис. 11.1. *Кадр физического уровня*

2. На канальном уровне к данным добавляется Ethernet-заголовок, что позволяет передать тестовые пакеты через сеть, которая содержит устройства, работающие на втором уровне модели OSI — например, сетевой коммутатор (switch). Способы подключения к тестируемой сети показаны на рис. 11.7, 11.8, 11.9.

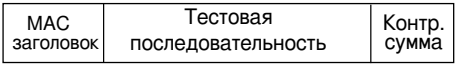


Рис. 11.2. *Кадр канального уровня*

3. На сетевом уровне данные помещаются в IP-пакет, а затем — в Ethernet-кадр. Это позволяет передать тестовые пакеты через сеть, которая содержит устройства, работающие на канальном и сетевом уровнях — например, сетевой коммутатор, маршрутизатор (router). Способы подключения прибора к тестируемой сети показаны на рис. 11.7, 11.8, 11.9.

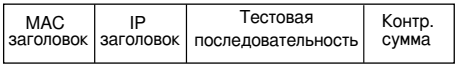


Рис. 11.3. *Кадр сетевого уровня*

4. На транспортном уровне формируется Ethernet-кадр, содержащий IP- и UDP-заголовок, что позволяет передать тестовую последовательность с использованием транспортных протоколов. Способы подключения прибора к тестируемой сети показаны на рис. 11.7, 11.8, 11.9.

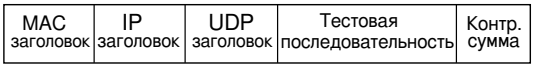


Рис. 11.4. *Кадр транспортного уровня*

Последовательности, используемые для тестирования, соответствуют рекомендации ITU-T O.150 [8].

Таблица 11.1. *Тестовые последовательности*

Тип последовательности	**Рекомендуемое применение**
2e11-1	Для определения ошибок и джиттера (при передаче данных по каналу связи со скоростью 64 кбит/с и 64×N кбит/с, где N — целое число).
2e15-1	Для определения ошибок и джиттера (при передаче данных по линии связи со скоростью 1544, 2048, 6312, 8448, 32 064 и 44 736 кбит/с).
2e20-1	Для определения ошибок (при передаче по каналу связи со скоростью не более 71 кбит/с).
2e23-1	Для определения ошибок и джиттера (при передаче данных по линии связи со скоростью 34 368 и 139 264 кбит/с).
2e29-1, 2e31-1	Для определения ошибок при передаче данных на высоких скоростях (более 139 264 кбит/с).

11.1. Варианты подключения

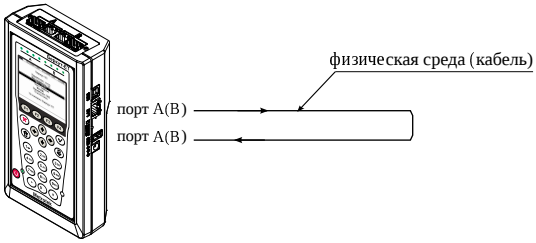


Рис. 11.5. *Тестирование на физическом уровне (вариант 1)*

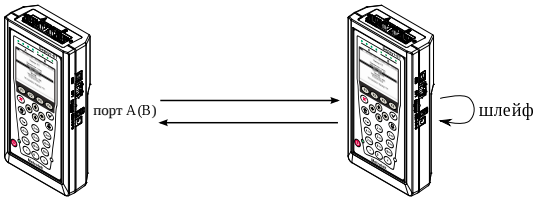


Рис. 11.6. *Тестирование на физическом уровне (вариант 2)*

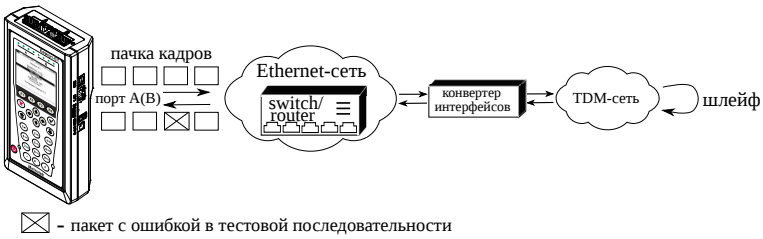


Рис. 11.7. *Тестирование на канальном/сетевом уровне (вариант 1)*

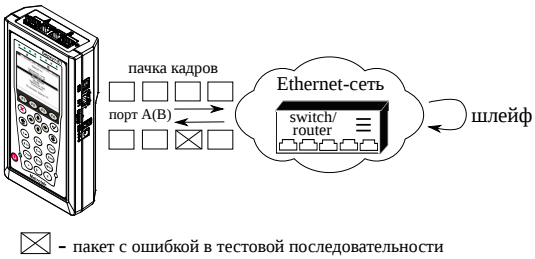


Рис. 11.8. *Тестирование на канальном/сетевом уровне (вариант 2)*

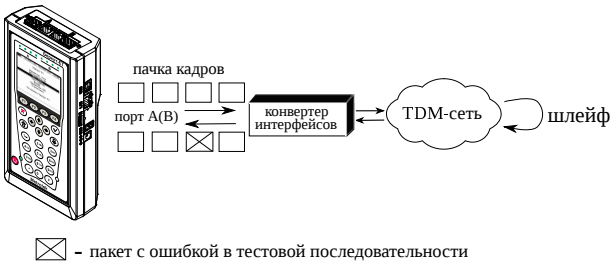


Рис. 11.9. *Тестирование на канальном/сетевом уровне (вариант 3)*

12. Пакетный джиттер

Важной задачей при тестировании Ethernet-сетей является определение пакетного джиттера[1]. В соответствии с методикой RFC 4689 [9], пакетный джиттер — это абсолютная разность задержек распространения двух последовательно принятых пакетов, принадлежащих одному потоку данных. Этот параметр используется для оценки возможности сети передавать чувствительный к задержкам трафик, такой, как видео или речь.

12.1. Тестовый поток

Функция генерации тестового потока применяется при измерении пакетного джиттера. Существует возможность генерации тестового потока и измерения пакетного джиттера на одном порту (рис. 12.1), а также генерации тестового потока на одном порту и измерения пакетного джиттера на другом (рис. 12.2), причём порт приёма может располагаться на удалённом приборе (рис. 12.3).

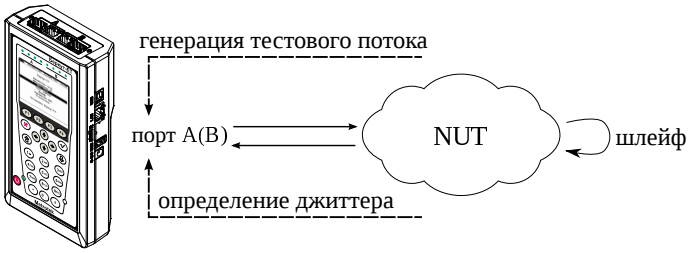


Рис. 12.1. *Измерение джиттера. Схема 1*

[1] В базовую конфигурацию не входит. Доступно при дополнительном заказе опции «ETJT».

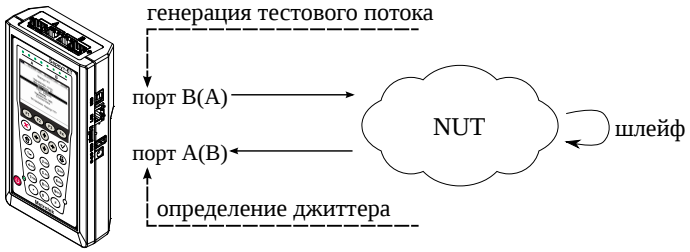


Рис. 12.2. *Измерение джиттера. Схема 2*

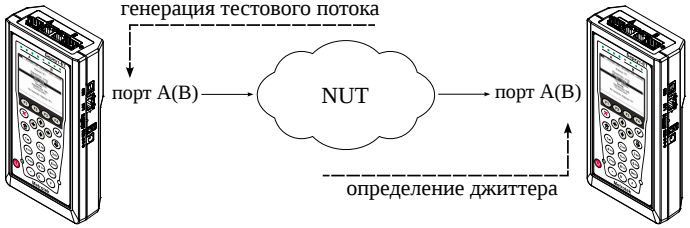


Рис. 12.3. *Измерение джиттера. Схема 3*

Литература

[1] RFC 2544, «Benchmarking Methodology for Network Interconnect Devices», S. Bradner and J. McQuaid, March 1999.

[2] IEEE Std 802.1Q, IEEE Standard for Local and metropolitan area networks — Virtual Bridged Local Area Networks.

[3] RFC 791, Postel, J., «Internet Protocol», DARPA, September 1981.

[4] RFC 1349, Almquist, P., «Type of Service in the Internet Protocol Suite», July 1992.

[5] ITU-T Y.1564 (03/2011), «Ethernet service activation test methodology».

[6] IEEE 802.3ah, «Ethernet in the First Mile Task Force».

[7] ITU-T Y.1563 (01/2009), «Ethernet frame transfer and availability performance».

[8] ITU-T O.150 (05/96), «General requirements for instrumentation for performance measurements on digital transmission equipment».

[9] RFC 4689, «Terminology for Benchmarking Network-layer Traffic Control Mechanisms», S. Poretsky, October 2006.