



Технология физического резервирования каналов Вурасс в кольцевой топологии и конвергенция с программными протоколами резервирования

Научно-исследовательская работа

Аннотация

[Заинтересуйте читателя с помощью аннотации (как правило, это краткое содержание документа).

Если вы готовы добавить свой текст — просто щелкните здесь и введите его.]

Гришин Виктор Александрович

grishin-v@s-avt.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ (с. 3 – 4)

ПРОГРАММНОЕ РЕЗЕРВИРОВАНИЕ СЕТЕЙ RSTP (с. 5 – 6)

ПРОГРАММНЫЕ БЕСШОВНЫЕ СИСТЕМЫ РЕЗЕРВИРОВАНИЯ СЕТЕЙ (с. 7 – 10)

УСТРОЙСТВО BYPASS-ПЕРЕКЛЮЧАТЕЛЕЙ И ТРЕБОВАНИЯ К НИМ (с. 11 – 15)

КАК ПРИМЕНЯЮТ СИСТЕМУ ФИЗИЧЕСКОГО РЕЗЕРВИРОВАНИЯ (с. 16 – 21)

ПИТАНИЕ И УПРАВЛЕНИЕ ПЕРЕКЛЮЧАТЕЛЕМ (с. 22 – 25)

ЗАКЛЮЧЕНИЕ (с. 26 – 27)

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ (с. 28)

ВВЕДЕНИЕ

В промышленном сегменте создания сетей, таких как АСУ ТП, СКУД, СМИС и др., наиболее важный показатель – это надежность. Таковым его делает важнейшая роль сетей как в современной жизни, так и в промышленности. Например, если рассматривать металлургический комбинат, где цифровые сети используются в сетях контроля температуры в печах, в управлении организацией сырья и продукции по цехам, в системах контроля и управления доступом на предприятие и даже в сетях бухгалтерского учета, то там отказ сети повлечет за собой большие финансовые потери и, что немаловажно, потерю большого количества времени на ликвидацию последствий. В других же случаях, неполадки сети могут повлечь за собой дискомфорт людей, травмы и даже смерть. Здесь в качестве наглядного примера можно привести транспортные инфраструктуры и, в частности, метрополитен, где цифровые системы передачи данных отвечают за обеспечение приемлемого качества воздуха под землей, контроль и откачку грунтовых вод, системы видеонаблюдения для визуального контроля различных ситуаций (в том числе социальных, внутри и на прилегающих территориях), контроль оплаты и обеспечения доступа к услугам метрополитена и т.д.

Однако надежность сети также может выражаться многими факторами, такими как расширенный температурный диапазон коммутаторов, улучшенное армирование кабелей и ВОЛС¹, поддержка активным коммутационным оборудованием различных технологий резервирования каналов, наличие нескольких источников питания, усиленная защита от ЭМИ и погодных факторов и т.д.. Такие показатели как температурный диапазон,

¹ Волоконно-оптические линии связи – прим. авт.

армирование, количество резервных линий передачи данных и количество источников питания можно множить довольно долго, что повлечет за собой сильный рост цены. В свою очередь, протоколы резервирования, хоть и не являются материальной составляющей сети, так как работают обычно на втором (канальном) уровне модели OSI (рис.1), при срабатывании вносят временные задержки в передаче информации, что играет важную роль в промышленных системах автоматизации (например, цифровые сети РЗА). Также необходимо учитывать, что большинство программных методов резервирования являются «одноразовыми»: при единичном сбое они сохранят целостность сети, однако при множественных её отказах подобное резервирование требует постоянного контроля и незамедлительной реакции со стороны обслуживающего персонала по устранению неисправности, будь то обрывы кабеля или отказы активного оборудования сети.

Модель OSI

Данные	Прикладной доступ к сетевым службам
Данные	Представления представление и кодирование данных
Данные	Сеансовый Управление сеансом связи
Блоки	Транспортный безопасное и надёжное соедине точка-точка
Пакеты	Сетевой Определение пути и IP (логическая адресация)
Кадры	Канальный MAC и LLC (Физическая адресация)
Биты	Физический кабель, сигналы, бинарная передача данных

рис.1 Логическое представление модели OSI.

ПРОГРАММНОЕ РЕЗЕРВИРОВАНИЕ СЕТЕЙ RSTP

Разберем работу одного из наиболее распространенных по применению в российских промышленных сетях протокола резервирования RSTP². Система RSTP использует для резервирования избыточность топологии и применяется для предотвращения широковещательных штормов. RSTP по своей сути является эволюцией протокола STP, который был предназначен для тех же самых целей, но имел время восстановления 30-50 секунд (против 2-5 секунд у RSTP), что было неприемлемо даже по меркам потребительского сегмента.

Другой функцией RSTP является защита от широковещательного шторма. Широковещательный шторм возникает, когда широковещательные пакеты (пакеты, адресованные всем устройствам в сети) принимаются коммутатором и отправляются на все порты, кроме порта-адресанта. Это вызывает циклическое размножение пакетов, которые забивают весь канал и расходуют всю пропускную способность сети, что приводит к невозможности передачи целевой информации. В наше время эта проблема имеет несколько иной характер, но схожие последствия. После подключения новой линии связи коммутатор пытается получить информацию обо всех подключенных к нему устройствах. Из этих данных формируется таблица MAC-адресов внутри коммутатора, где сопоставлены порты и MAC-адреса всех устройств, подключенных к нему. Когда коммутатор замечает один и тот же MAC-адрес на разных портах, он считает это как ошибку, очищает составленную таблицу и начинает весь процесс регистрации соседних устройств в таблицу заново. В случае топологии «кольцо» на двух портах коммутатора будет оказываться одно устройство со своим MAC-адресом (не важно, каким именно из кольца), что будет приводить к ошибке и вышеописанным действиям. Это

² Rapid spanning tree protocol – прим. авт.

будет происходить с каждым коммутатором в кольце из-за особенности топологии «кольцо». Технология резервирования RSTP решает обе проблемы логическим разрывом кольца, тем самым физическое кольцо преобразуется в логическую топологию «последовательная линейная цепь», в которой невозможно возникновение подобных ошибок. Однако нужно учитывать, что в случае обрыва связи в кольце протокол вернет отключенное звено в режим передачи данных, что объединит две половинки разорванного кольца в топологию цепи.

ПРОГРАММНЫЕ БЕСШОВНЫЕ СИСТЕМЫ РЕЗЕРВИРОВАНИЯ СЕТЕЙ

Как уже упоминалось ранее, программные технологии резервирования являются системами резервирования единичного сбоя. Проиллюстрированный нами ранее пример наглядно дает понять, что после первого сбоя и следующего за ним восстановления повторное восстановление станет невозможным, и следующий сбой с большой вероятностью станет фатальным. Частично эту проблему (и полностью – проблему со временем восстановления) решают протоколы параллельного резервирования PRP³ и HSR⁴. Их метод функционирования основан на избыточности отправляемых пакетов, а не на избыточности линий связи. Коммутаторы с поддержкой технологий параллельного резервирования называются RedBox (QuadBox в случае наличия двух пар портов параллельного резервирования).

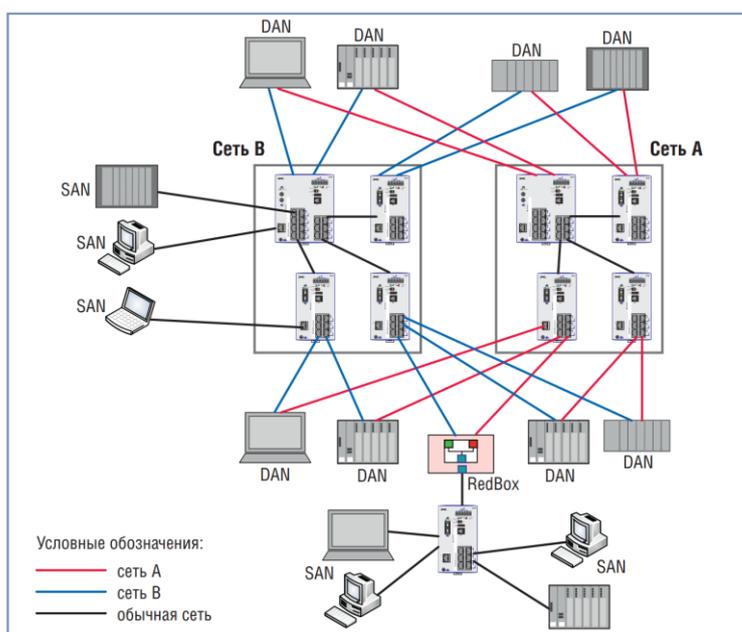


рис.2 Пример схемы параллельного резервирования PRP.

³ Parallel Redundancy Protocol – прим. авт.

⁴ High-availability Seamless Redundancy – прим. авт.

Протокол параллельного резервирования PRP использует две независимые сети для передачи двух идентичных пакетов данных, отличающихся лишь PRP-суффиксом. Когда один из пакетов доходит до целевого коммутатора в PRP сети, то принимается устройством при соответствии контрольной суммы, а последующий пакет отбрасывается.

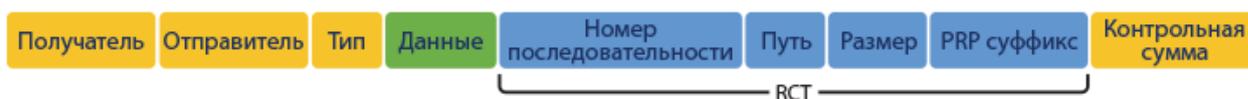


рис.3 Схема пакета PRP.

Как можно видеть на данной схеме, блоки в фрейме PRP находятся на тех же местах, в том же порядке и имеют те же размеры, что и стандартный Ethernet-фрейм и отличается лишь блоком с данными, куда был добавлен RST-блок, содержащий необходимые для функционирования PRP технические данные. Это предоставляет возможность передавать их по классическим Ethernet-сетям любой конфигурации. В качестве недостатков данного протокола резервирования можно выделить следующие:

- Увеличение нагрузки на сеть из-за того, что требуется больше пакетов для передачи того же количества информации, что и в классической сети без параллельного резервирования;
- Увеличенное время задержки (ping) между пунктом отправления и назначения;
- Требуется наличие двух независимых сетей;
- Все еще присутствует вероятность отказа двух сетей, но она значительно меньше, чем в RSTP-кольце.

Протокол резервирования HSR имеет отличающуюся схему работы, но тот же принцип. Протокол работает в кольцевой топологии. Как и в PRP, основой функционирования протокола является использование избыточности пакетов.

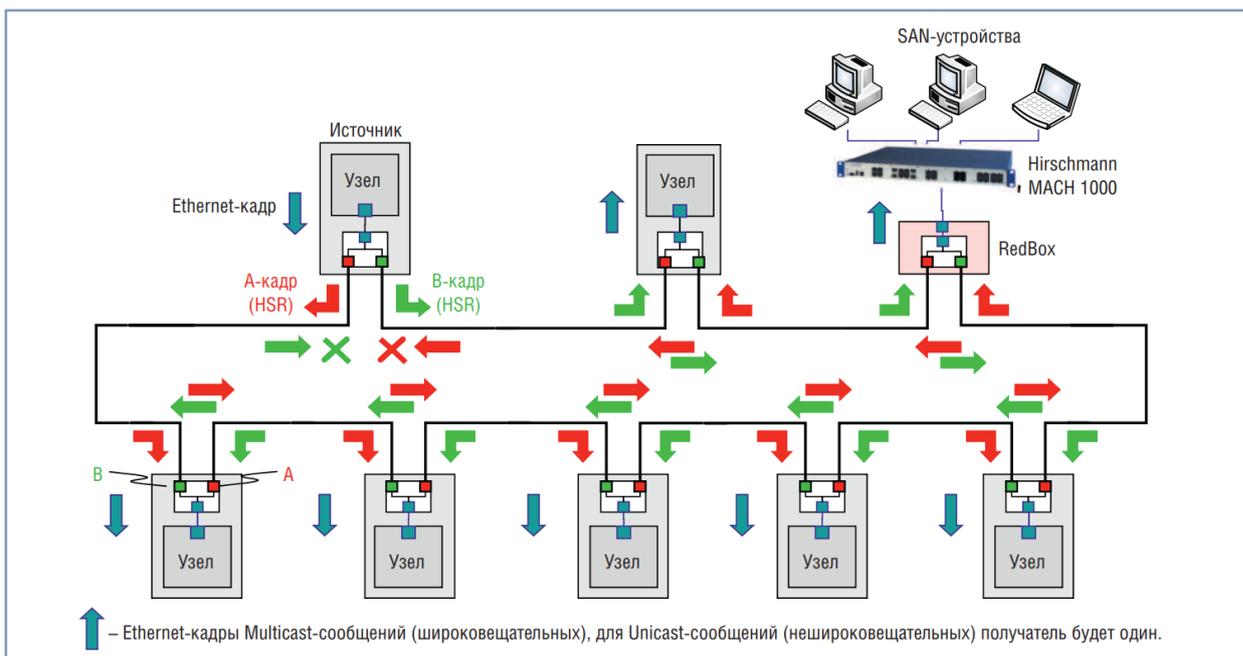


рис.4 Пример схемы параллельного резервирования HSR.

Преимуществами данного протокола перед PRP являются:

- Меньшая нагрузка на сеть за счет большего места для ценных данных в одном пакете;
- Меньший ring между устройствами за счет технологии раннего распознавания адресата пакета.

Особенностью протокола является то, что все устройства в кольце должны поддерживать протокол HSR (быть RedBox или QuadBox коммутатором соответственно). Это обусловлено конструкцией HSR-фрейма, порядок блоков в пакете изменяется. Также при получении пакета другой коммутатор начинает передавать его на следующий в кольце коммутатор еще до того, как получит весь пакет, что обеспечивает меньшую задержку и нагрузку на сеть. Защита от широковещательного шторма и ошибок при построении таблицы MAC-адресов здесь не требуется, так как пакеты в любом случае отправляются в обе стороны и всегда имеют адресата в кольце. Таким образом, потребность в таблице MAC-адресов отсутствует.



рис.5 Схема пакета HSR.

Основной минус и причина малой распространенности данной схемы резервирования – её цена. Каждый коммутатор кольца должен поддерживать технологию резервирования HSR, что повышает цену всей сети. Отказоустойчивость данной сети немногим ниже, чем у сети PRP, примерно на уровне RSTP-кольца. Преимущество же перед RSTP у кольца HSR – это меньшее (и одинаковое для всех), время передачи данных и отсутствие возможности как широковещательного шторма, так и ошибок таблицы MAC-адресов.

УСТРОЙСТВО BYPASS-ПЕРЕКЛЮЧАТЕЛЕЙ И ТРЕБОВАНИЯ К НИМ

Кольцевые топологии объединяет факт того, что, если неисправности находятся по обе стороны кольца, то обмен данными между двумя его половинами будет невозможен. Наиболее уязвимым в плане отказа элементом сети является активное сетевое оборудование, так как твердые среды передачи данных (медные, оптические кабели) при их правильном монтаже имеют минимальные шансы выхода из строя. Под активным сетевым оборудованием подразумеваются коммутаторы, маршрутизаторы, SFP-трансиверы, сетевые карты и другие устройства, имеющие собственный MAC-адрес и/или требующие внешнего питания от электрической сети для работы. Второй частью сети является среда передачи данных. Если в потребительском сегменте преобладает воздушная среда передачи данных (на уровне WAN это EDGE, 3G или LTE, а в домашних LAN это Wi-Fi), то для промышленных сетей беспроводная среда слишком непредсказуема и ненадежна, и к ее использованию прибегают в исключительных случаях (таких как связь с подвижными объектами). На больших расстояниях вместо сотовых сетей стараются использовать оптические линии связи, это почти полностью решает проблемы надежности и безопасности сети. В промышленных Ethernet-сетях используют витую пару cat5 и выше, состоящую из меди или алюминия для уровня доступа; в свою очередь, ВОЛС используют для магистральных кабелей, а также уровней ядра и агрегации. Среда передачи не имеет движущихся частей, электронных схем, алгоритмов работы и пр., в результате чего среда передачи является самым надежным элементом сети.

Стандартные протоколы резервирования работают за счет активного оборудования, которое, как описано выше, является менее надежными, чем среда передачи данных. В связи с этим появилась идея создания физического

резервирования, используя в его основе среду передачи данных. Также метод резервирования должен как можно меньше зависеть от цифровых алгоритмов и программ. Решение проблемы множественных отказов в кольце, по сути, является целью создания данного метода. Это обозначает, что количество отказов в сети не должно никаким образом влиять на работоспособность кольца. Второй же решаемой проблемой должно стать время резервирования. Физический метод резервирования тратит минимальное количество времени на восстановление, так как работает на простейшей механической логике, а не на программных алгоритмах. По этой же причине он никак не влияет на пропускную способность кольца, так как не имеет служебных пакетов (таковые использует RSTP для проверки целостности резервируемой сети).

Под вышеописанные требования подходят переключатели⁵ SWF-102F от «Sumanitron». Компактные размеры являются ощутимым плюсом, они влияют как на возможность модификации существующих сетей, так и на возможность встраивания ее в проектируемые сети с минимальными изменениями. Расположение Вурасс⁶-переключателя возможно вплотную к другим устройствам на DIN-рейке, ввиду отсутствия у него процессора (в широком понимании этого слова) и, как следствие, нагрева.

⁵ Не могут называться коммутаторами, так как не имеют таблицы MAC-адресов и процессора, в то же время не могут называться хабом/концентратором, так как отправляют данные только на один порт – *прим. авт.*

⁶ Дословно «обходной путь» – *прим. авт.*



рис.5 Внешний вид переключателя SWF-102F.

Оптические порты устройства не имеют ограничений по скорости передачи данных, это обусловлено отсутствием коммутационной матрицы в привычном понимании. Коммутация осуществляется по принципу соединения пар между собой (А с А, В с В) или противоположных пар (А с В) портов физически напрямую между собой (рис.6). Минусом данного устройства и системы резервирования является наличие дополнительного затухания в кольце, которое составляет:

– у модели для многомодового волокна $<1\text{Дб}$ ($<14\%$; эквивалент волокна $\sim 77\text{м}$);

– у модели для одномодового волокна 1.2Дб ($<10\%$; эквивалент волокна $<200\text{м}$).

Это стоит учитывать при расчетах мощности оптических портов, SFP и длины оптических линий связи.

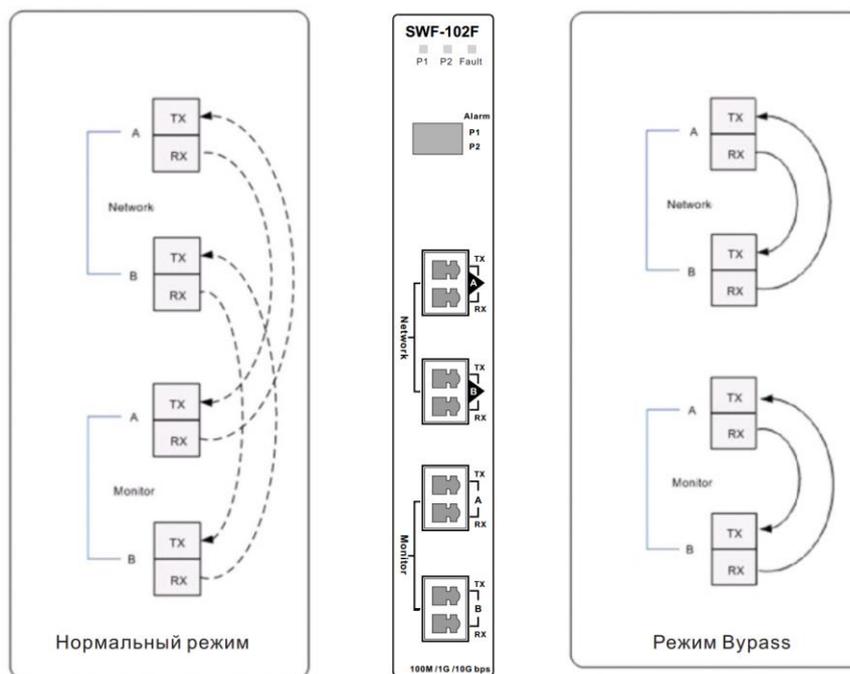


рис.6 Схема принципа работы Вывоса переключателя SWF-102F.

В тандеме с коммутатором переключатель выполняет функцию по «отсечению» от кольца того или иного участка при повреждении последнего. Подключение оптических линий коммутатора к кольцу будет осуществляться по приложенной схеме (рис.7).

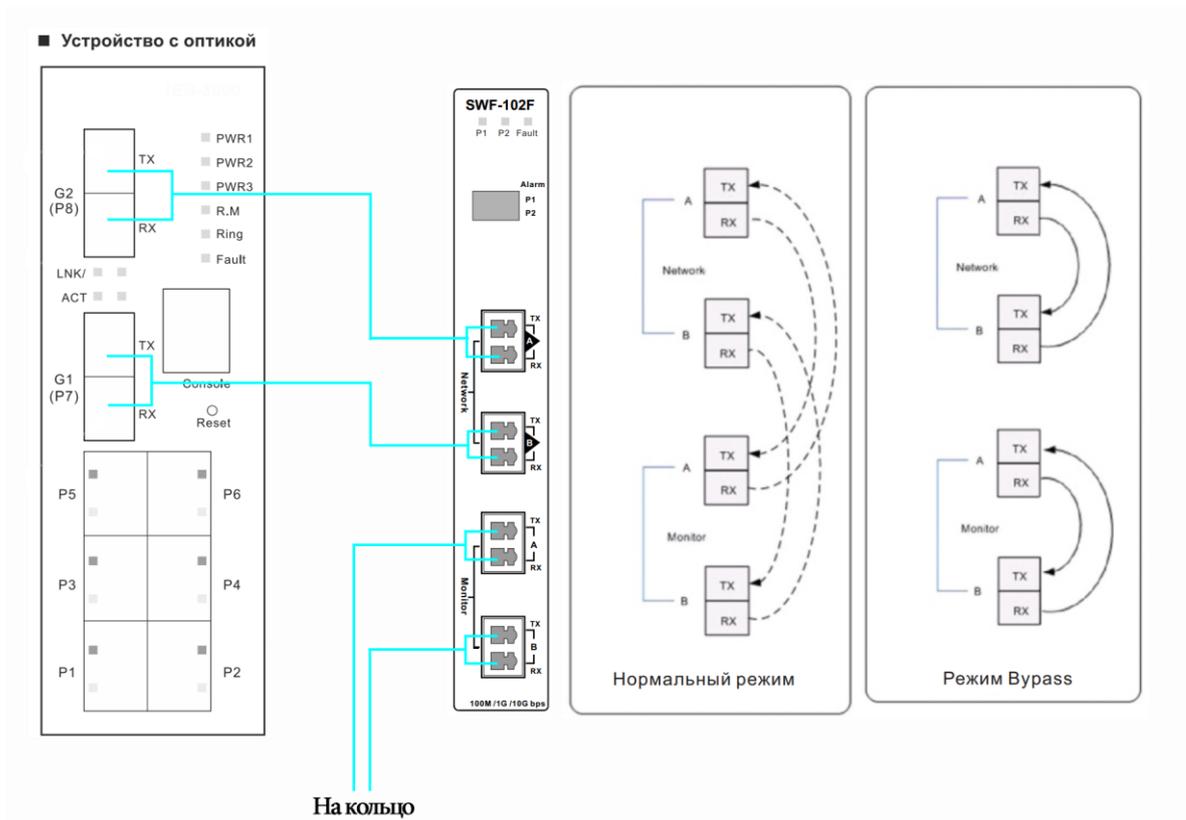


рис.7 Схема подключения оптического коммутатора.

После подключения коммутатора в соответствии со схемой данные с порта G1 через Вурасс передаются на кольцо, как и данные с порта G2. В случае сбоя порты G1 и G2 будут замкнуты между собой, как и соответствующие А и В порты. Это действие, с одной стороны, отключит вышедший из строя фрагмент сети, а с другой – соединит кольцо в обход неисправного участка.

КАК ПРИМЕНЯЮТ СИСТЕМУ ФИЗИЧЕСКОГО РЕЗЕРВИРОВАНИЯ

Рассмотрим работу такой системы резервирования на примере стенда «Метролайн», разработанного в целях демонстрации унифицированной сети для всех систем станций метрополитена и других транспортных инфраструктур. В центре сети для обмена информацией реализовано кольцо из коммутаторов с использованием технологии физического резервирования и RSTP (рис.8).

На данной схеме пронумерованы 8 коммутаторов. Коммутаторы 5-8 являются управляемыми коммутаторами как минимум с двумя оптическими магистральными портами. Два магистральных порта коммутатора соединены с соседними коммутаторами через их магистральные порты. Таким образом, магистральные порты, направленные в разные стороны кольца, образуют кольцевую топологию. Для предотвращения широковещательного шторма и для автоматической коррекции таблицы MAC-адресов используется протокол RSTP, но могут использоваться и другие протоколы с таким функционалом: MSTP, STP, ERPS или проприетарные протоколы производителя коммутаторов.

Коммутаторы 1-4 являются Bypass-переключателями. Они находятся в одном шкафу с основным коммутатором (физически) и непосредственно перед ним (с точки зрения топологии сети). Через Bypass-переключатели происходит подключение коммутаторов к кольцу.

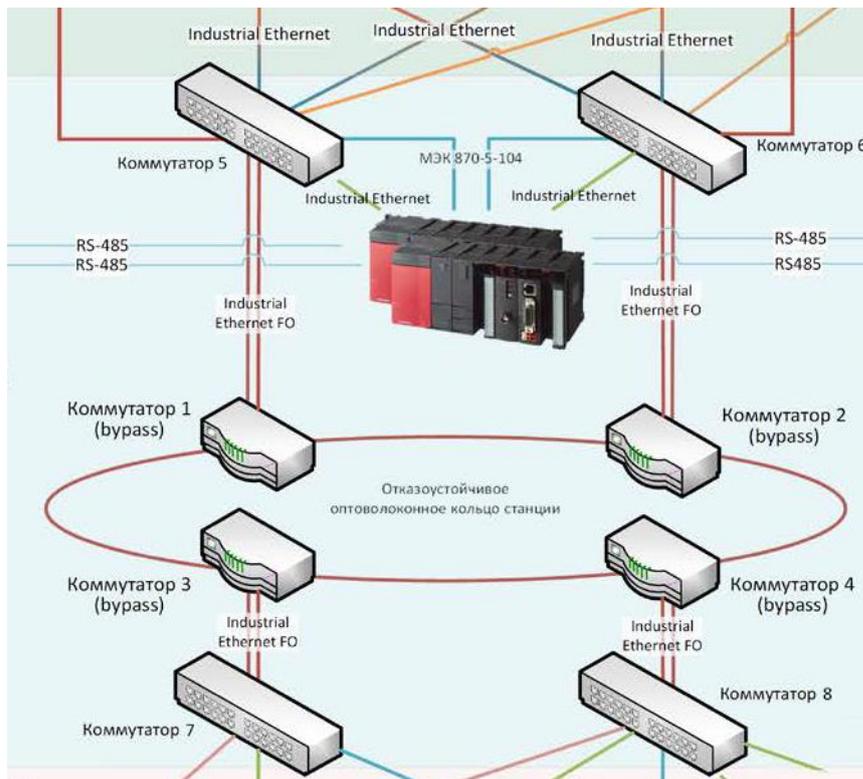


рис.8 Схема коммутации в стенде «Метролайн».

Для демонстрации работы Вурасс-переключателей графически промаркируем коммутаторы в кольце, а также линии передачи данных по кольцу в соответствии с очередностью коммутации линий (рис.9). Линии передачи данных окрашены таким образом, чтобы визуализировать, от какого коммутатора к какому при данной конфигурации будут переданы данные вне зависимости от первоначального источника пакета данных.

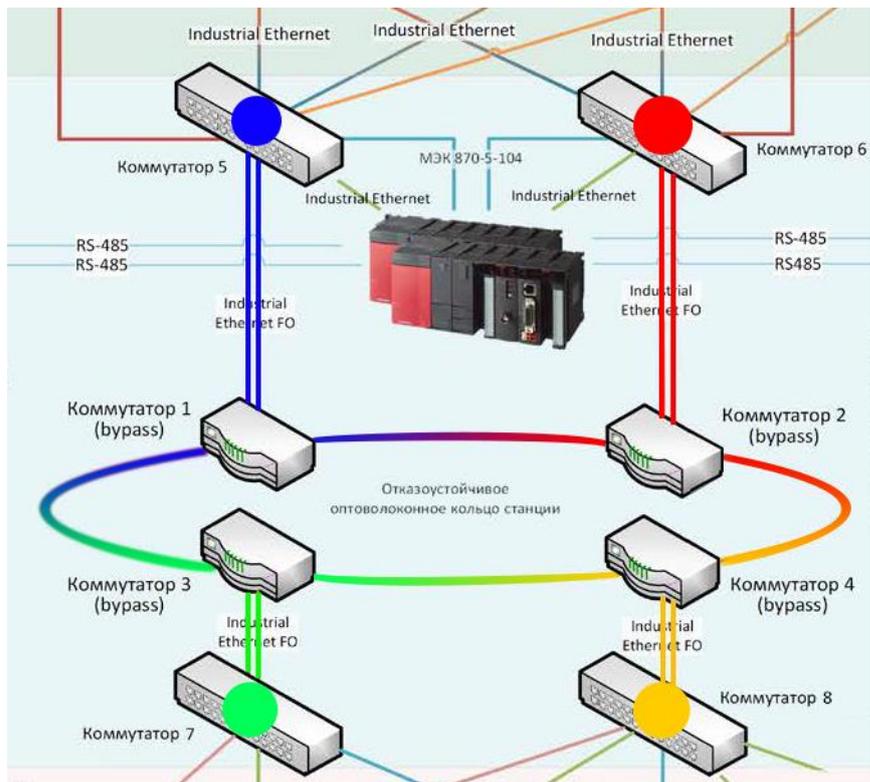


рис.9 Визуализация передачи данных в полностью исправной Bypass-сети.

При штатном режиме работы кольца данные передаются от коммутатора к коммутатору сквозь Bypass-переключатели последовательно. В случае единичного отказа (такого как пропадание питания, поломка порта, SFP-трансивера, произвольного отключения) Bypass-переключатель сменит тип коммутации пар. Это позволит замкнуть кольцо и, таким образом, восстановить функционирование кольца.

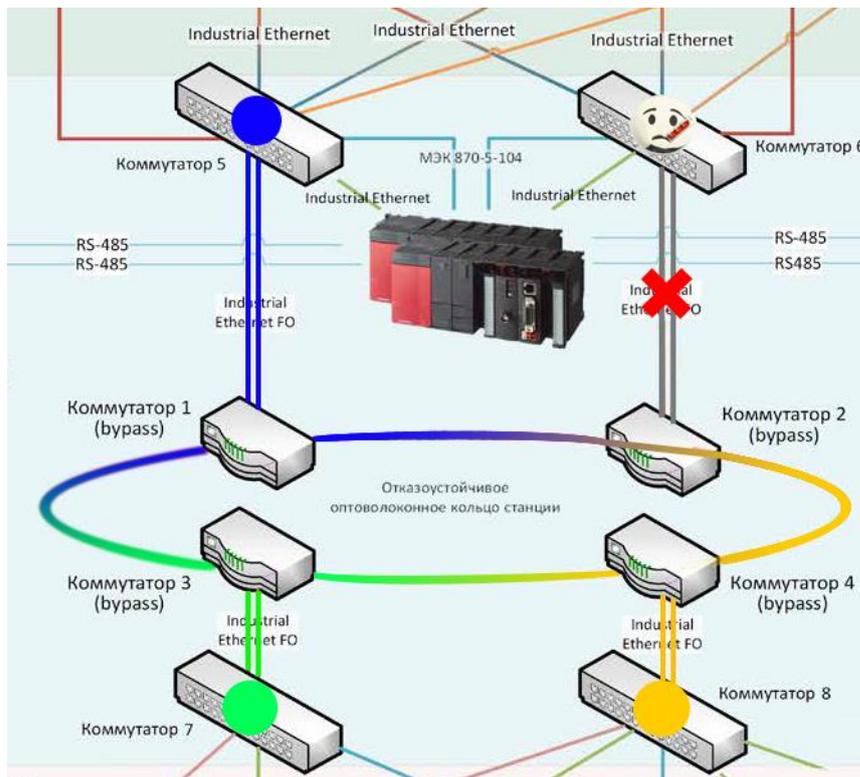


рис.10 Визуализация передачи данных в Bypass-сети с одним случаем отказа.

Как показано на рис.10, коммутатор №6 вышел из строя, в следствие чего его Bypass-переключатель (коммутатор 2) перешел в режим резервирования. В режиме резервирования переключатель замкнул кольцо и коммутатор сам на себя. После исправления причины сбоя переключатель сам вернется в штатный режим коммутации.

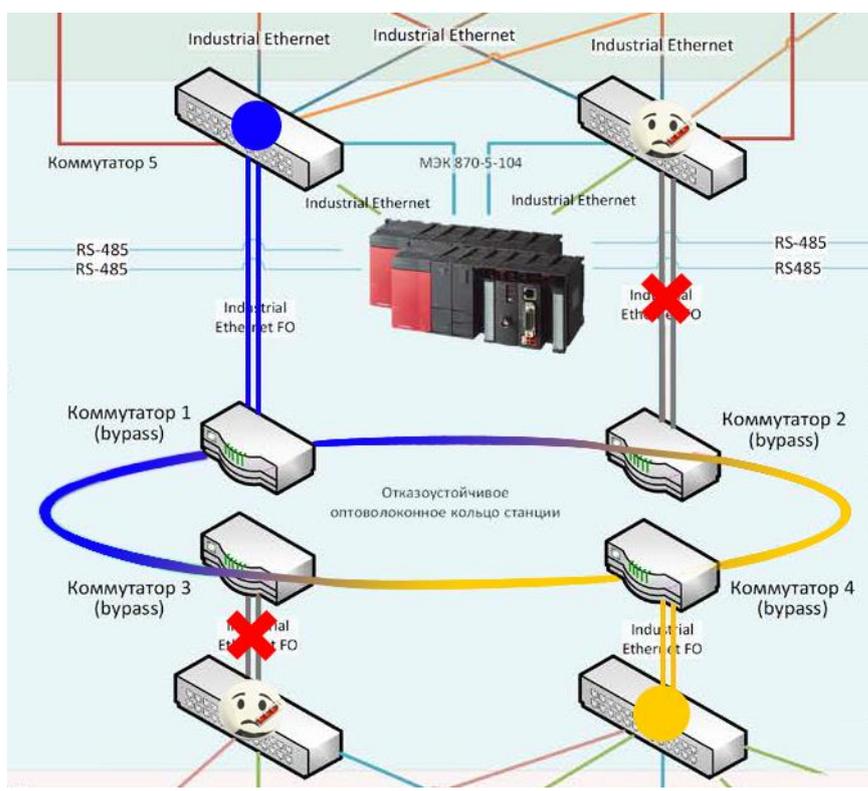


рис.11 Визуализация передачи данных в Bypass с несколькими случаями отказа.

На рис. 11 визуализирован наихудший вариант множественного сбоя – по обе стороны от источника данных (коммутаторы 2 и 4). Если бы данная сеть не была защищена физическим резервированием при помощи Bypass-переключателей, то передача данных была бы невозможна из-за крайне малой устойчивости к множественным отказам. В данном случае Bypass-переключатели повели себя так же, как было описано в предыдущем примере – замкнули кольцо и обеспечили связь между исправными участками сети.

Протокол RSTP в данной сети реализует свои функции защиты от различного рода широковещательных штормов и перестроение таблицы MAC-адресов. Функция перестроения таблицы в данной конфигурации важна из-за того, что при срабатывании физического резервирования на коммутаторах-соседях вышедшего из строя устройства должны поменяться данные о соседних коммутаторах. Это не является задачей первостепенной важности,

пакеты доставляются по MAC-адресу из префикса пакета и будут доставлены любым путем, но это может иметь большое значение для некоторых служебных протоколов самих коммутаторов.

Резервирование сетей с протоколом HSR с использованием Вурасс-коммутаторов также увеличивает надежность сети и ее устойчивость к множественным отказам. Так как расстановка, подключение и принцип работы Вурасс-коммутаторов аналогичны вышеописанным, то стоит лишь добавить о различиях в программной части. Так как в кольцах HSR не строятся таблицы MAC-адресов, то и ее перестроение при срабатывании происходить не будет. Пакеты направляются в обе стороны и придут к адресату в любом случае, даже в случае отказа с обеих сторон кольца (как и в предыдущем примере с RSTP), что не может быть достигнуто в кольце без Вурасс-резервирования.

ПИТАНИЕ И УПРАВЛЕНИЕ ПЕРЕКЛЮЧАТЕЛЕМ

Вторая по важности часть функционирования Вурасс-коммутаторов после системы коммутации оптических волокон – система питания переключателя. Система питания является основным органом управления – следовательно, наличие или отсутствие питания также является управляющим сигналом. Данная система предельно проста: если питание подается – соединены порты по буквам, противоположно (В с В; А с А); если питания нет – порты соединены попарно (А с В в паре Network; А с В в паре Monitor).

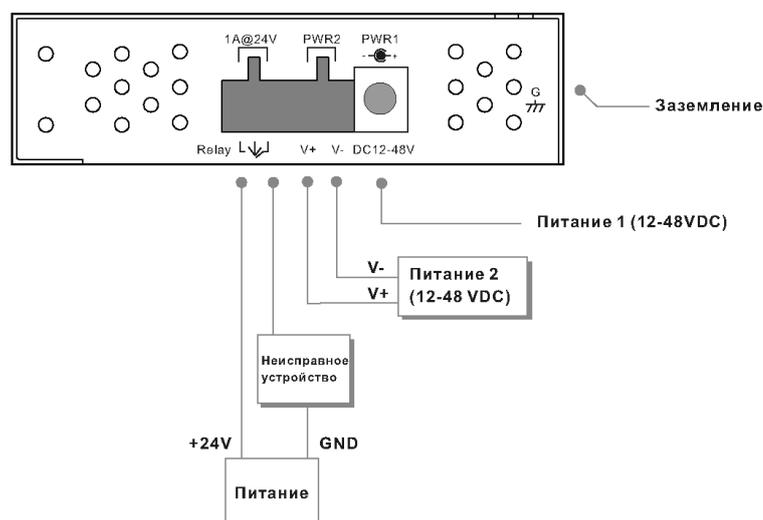


рис.12 Вырезка из инструкции bypass-коммутатора SWF-102F.

На рис. 12 представлены два варианта подключения питания: **непосредственно от источника питания**, при этом важно, чтобы и резервируемый коммутатор, и Вурасс-переключатель были подключены к одному и тому же (или к одним и тем же, если источников несколько) источнику питания, и **через резервируемый коммутатор** – когда одна из линий питания (обычно минусовая) подключается в источник питания через сигнальное (нормально разомкнутое) реле резервируемого коммутатора.

Первый вариант используется для резервирования либо неуправляемых коммутаторов, либо систем, где требуется зарезервировать только пропадание питания на коммутаторе (рис.13). Если пропадает питание на коммутаторе, то и на Вурасс-переключателе питание пропадет, и он направит оптический сигнал далее по кольцу, а не на коммутатор.

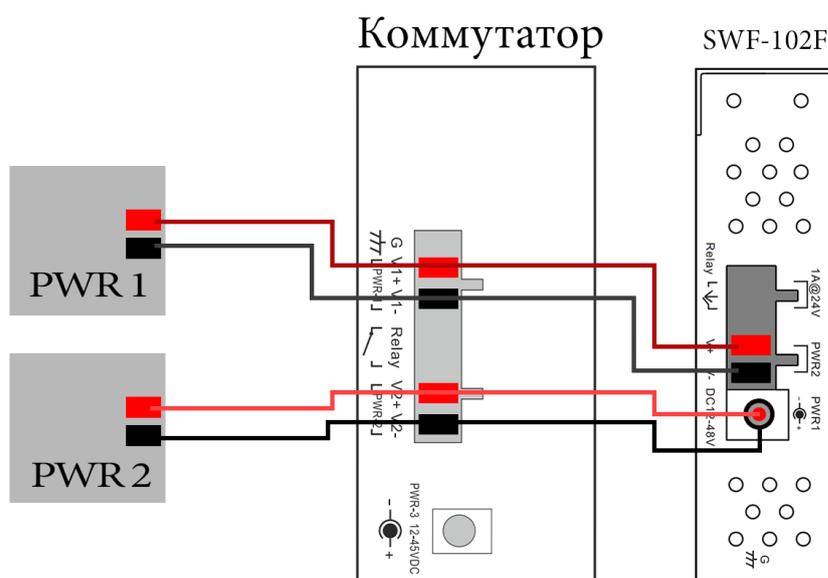


рис.13 Подключение питания переключателя параллельно с коммутатором.

Использование второго варианта подачи питания применяется для реализации более сложных схем активации (и деактивации) режима резервирования. Так как переключатель получает питание через сигнальное реле коммутатора, то этот коммутатор имеет возможность управлять состоянием резервирования; также благодаря второму варианту подачи питания решается основополагающий вопрос двойного питания коммутатора. В отличие от первого варианта подключения, в данном случае нет обязательного соответствия количества источников питания у коммутатора и переключателя.

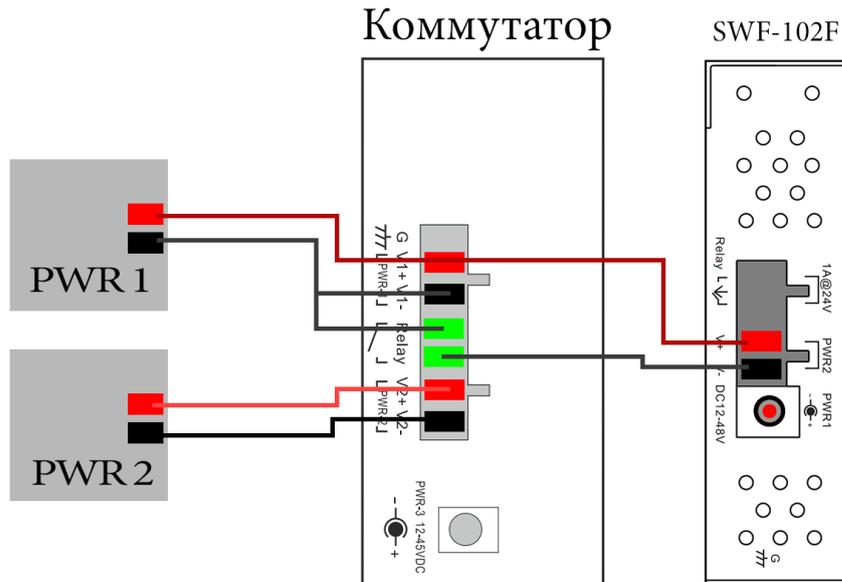


рис.14 Подключение питания переключателя через реле коммутатора.

Данный вариант соединения может быть настроен так, как нужно для проекта. Например, в WEB-интерфейсе (рис.15) на коммутаторах «Sumanitron» линейки Networking можно настроить срабатывание реле на:

- Пропадание питания на одном из источников питания.
- Отсутствие соединения на любом из портов.

На других коммутаторах настройка может быть обширнее в случае:

- Сбоя кольца (если коммутатор мастер);
- Выхода за заданные параметры температуры коммутатора;
- Превышения нагрузки на ядро коммутатора;
- Потери связи с определенным узлом сети;

- Широковещательного шторма;
- Несанкционированного подключения к коммутатору;
- И т.д.

Таким образом, второй вариант является наиболее гибким по настройке, но делает физическое резервирование зависимым от программных составляющих сети, отчего оно перестает быть полностью физическим.

Fault Alarm

Power Failure

PWR 1 PWR 2

Port Link Down/Broken

Port.01 Port.02
 Port.03 Port.04
 Port.05 Port.06
 Port.07 Port.08
 G1 G2

*рис.15 Web-интерфейс коммутаторов «Symanitron» линейки Networking.
Настройка условий срабатывания реле коммутатора во включенном
состоянии.*

ЗАКЛЮЧЕНИЕ

Таким образом, использование физических средств резервирования повышает одну из главных характеристик промышленных сетей – отказоустойчивость. Данный тип резервирования обеспечивает бóльший уровень надежности при меньших финансовых затратах. Финансовые затраты, как для включения данной системы в проект, так и для модификации существующей сети и оснащение ее bypass-переключателями, включают в себя Вурасс-переключатели, двух оптических патч-кордов и некоторое количество проводов питания соответственно.

Также для еще нереализованных проектов можно использовать коммутаторы со встроенными Вурасс-портами (рис.16). Это коммутаторы, в которых уже есть две или одна пара Вурасс-портов.



рис.16 Вурасс-коммутатор производства «Symanitron» SWMG-84GSFP-BP2.

Кроме оптических Вурасс-коммутаторов существуют также «медные» (электромагнитные) Вурасс-решения. Для промышленных транспортных сетей в ассортименте «Symanitron» есть коммутатор SWMGPT-82M12-BP1 (рис.17).



рис.17 Промышленный транспортный коммутатор с «медными» bypass-портами и разъемами M12.

Из вышеуказанного следует, что на рынке есть решения для увеличения надежности любых сетей на любом уровне модели OSI. Это обусловлено требованиями рынка и тенденцией на увеличение срока службы и бесперебойной работы всех элементов сетевой инфраструктуры. Увеличение отказоустойчивости объясняется бесконечными потребностями к «страхованию рисков» в виде снижения простоя оборудования, пресечения форс-мажорных ситуаций еще на этапе проектирования и обеспечения большей безопасности сотрудников и целевых пользователей любых цифровых систем.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Сайт ООО «Symanitron» - <http://symanitron.ru/>
2. Документация проекта ПМИ «Метролайн» Забора В. А.
3. Сайт moxa.ru - <https://moxa.ru/>
4. Журнал «современные технологии автоматизации» - <https://www.cta.ru/>
5. Статья «Концепция параллельного и кольцевого резервирования» Иван Лопухов - <https://www.cta.ru/cms/f/443112.pdf>

Консультанты:

Новожилов Александр Викторович

Редактор:

Бесполов Артемий Александрович

Автор:

Гришин Виктор Александрович