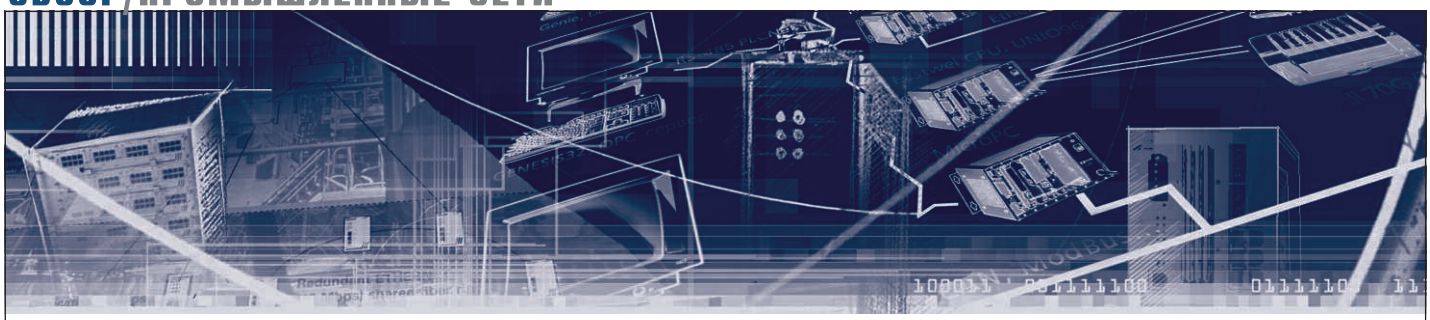


Иван Лопухов

Концепция параллельного и кольцевого резервирования

В статье рассматриваются новые принципы резервирования промышленных сетей Ethernet, их особенности, преимущества перед существующими технологиями и перспективы применения в реальных сетевых устройствах.

Введение

Идея резервирования каналов и резервных линий связи так же стара, как и сама технология Ethernet в промышленных коммуникациях. Проблема в том, что эта идея противоречит «природе» Ethernet, которая не предполагает замкнутых контуров в сети, тем самым запрещая резервные каналы передачи сетевого трафика. Однако надёжность, которая обеспечивается дублированием каналов передачи данных, была и остаётся базовым требованием во многих системах автоматизации. Поэтому для использования сетей Ethernet в промышленной автоматизации необходимы специальные протоколы, нивелирующие противоречие между стандартными протоколами Ethernet и резервными каналами передачи трафика.

Первым таким протоколом, применявшимся ещё в офисных сетях, был STP (Spanning Tree Protocol), разработанный институтом IEEE (Institute of Electrical and Electronics Engineers) и опубликованный в стандарте 802.1D в 1990 году. Резервирование линий связи стало возможно на базе практически любого управляемого коммутатора, но время восстановления связи по алгоритму, заложенному в STP, составляет десятки секунд. Последующие протоколы резервирования, развивающие принципы и механизмы, описанные в стандарте IEEE 802.1D, работают гораздо быстрее и лучше отвечают специфическим требованиям промышленной среды. Текущее состояние технологий резервирования и специфику их применения описывает данная статья.

Смысл резервирования каналов передачи данных

Дублирование каналов передачи данных осуществляется с целью исключения таких узлов, отказ которых способен вывести из строя всю систему. Так, например, если производственный участок подключён к общей системе передачи данных через единственный коммутатор, то отказ этого коммутатора приведёт к остановке всего участка и повлечёт, соответственно, серьёзные, в том числе финансовые последствия. Если же данный коммутатор дублирован другим коммутатором, то отказ первого приводит к фактическому возвращению сети к первоначальному состоянию без резервирования. Резервирование позволяет системе оставаться работоспособной на период ремонта узла, вышедшего из строя.

Резервированные сетевые структуры используются для двух целей:

- регулирование нагрузки на сеть – добавление резервного канала связи увеличивает суммарную пропускную способность изначального соединения, для этой цели используется протокол агрегирования каналов LACP [1];
- повышение устойчивости к сбоям – резервные каналы связи между узлами сети позволяют системе переключаться на запасные линии связи в случае отказа основной.

Несмотря на то что вторая цель может быть достигнута в рамках первой, приоритет зачастую отдаётся повышению устойчивости к сбоям. В промышленных сетях объёмы передаваемой информации меньше, чем, например, в офисных сетях, зато требования к надёжности их доставки выше. На гарантированную доставку данных в заданный промежуток времени ориентированы промышленные протоколы связи и сетевые технологии. Аппаратные сбои, конечно, исключить нельзя, но можно сделать их последствия наименее болезненными [2].

Базовые требования для промышленных сетей

Одно из ключевых требований для промышленных сетей Ethernet – отсутствие петель или замкнутых маршрутов в топологии, то есть между получателем и отправителем кадра данных должен быть единственный путь его доставки. Появление замкнутого маршрута в сети вызовет лавинообразное возрастание трафика и, следовательно, перегрузку сети, поэтому в традиционных сетях Ethernet избегают возникновения таких петель. В промышленных сетях задача протоколов резервирования – это мониторинг дублированных каналов связи с целью недопущения коллизий и перераспределение трафика в аварийных ситуациях. Протокол резервирования должен гарантировать

логическое существование только одного пути доставки сообщения в конкретный момент времени при физическом наличии нескольких. Из существующих физических каналов связи один выбирается основным, остальные ждут в резерве.

Такой принцип был впервые применён в протоколе STP, который отслеживал состояние каналов связи и при обнаружении обрывов направлял трафик с отказавшего канала на резервный. Это означает, что связь теряется на некоторое время, пока обрыв обнаружится, а новый канал передачи данных будет активирован. В зависимости от размеров сети и сложности её топологии время восстановления связи может быть разным и заранее его определить нельзя.

На основе протокола STP можно сформулировать основные требования к протоколам резервирования Ethernet в промышленной среде.

1. Определённое время восстановления сети: период времени от момента разрыва основного соединения до восстановления связи по резервному соединению должен быть меньше некой допустимой величины.
2. Требования к сети: для протокола должны быть определены допустимая топология сети, максимальное количество узлов (коммутаторов), типы соединений и пр.
3. Протокол должен базироваться на стандартизированном методе или алгоритме. Только так можно гарантировать совместимость с сетевым оборудованием и другими сетевыми протоколами.

Первое требование традиционно для промышленных сетей, работающих в реальном времени. Протокол резервирования может быть задействован, если максимально возможное время восстановления удовлетворяет требованиям процесса или приложения, для которого сеть передачи данных используется.

Технологии и решения: протоколы RSTP/MSTP

В последние годы упомянутый протокол STP был вытеснен своим более быстрым последователем – протоколом RSTP (Rapid Spanning Tree Protocol), описанным в стандарте IEEE 802.1D-2004 [3]. Данный протокол поддерживает множество различных топологий и базируется на том, что из всех сетевых соединений выделяется древовидная структура, так что между любыми двумя узлами сети в каждый момент времени существует единственный маршрут передачи данных. Все соединения, не вошедшие в активное «дерево», считаются резервными и не активны до изменения топологии. Протокол базируется на мостовых соединениях (BPDU – Bridge Protocol Data Units), среди которых выбирается корневой мост (соединение коммутатор-коммутатор). Всё остальное «дерево» строится от него. Любое изменение в активном «дереве» означает изменение в составе BPDU с рассылкой специального BPDU-кадра по узлам сети, после чего те активируют резервные маршруты для трафика. В протокол встроена защита от перегрузки сети данными кадрами, которая может привести к увеличению времени восстановления.

Протокол RSTP поддерживает большое количество узлов и обеспечивает время восстановления связи порядка 1 секунды. Это время во многом зависит от места возникновения обрыва связи в сети, поэтому не может быть чётко определено заранее.

Данный существенный недостаток можно обойти, если ограничить топологию сети кольцевой структурой. Тем самым можно добиться соблюдения времени восстановления сети порядка 100 мс и меньше.

MSTP – новая итерация описанного протокола резервированных «деревьев», и работает она по тому же принципу [4]. Если RSTP работает вне зависимости от виртуальных сетей VLAN, то структуры MSTP, наоборот, существуют в составе виртуальной сети и таким образом обеспечивают больше удобств и свобод в плане возможных топологий и распределения нагрузки. Оба протокола совместимы между собой и могут быть реализованы внутри одной сети.

Резервированные кольца

Кольцевая топология удобна прежде всего тем, что с ней достигается определённое и гарантированное время восстановления связи после сбоя, учитывающее количество коммутаторов в кольце. Стандарт IEC 62439-1 описывает пример расчёта времени восстановления для кольца, а также дополнительные ограничения (например, RSTP не может быть сконфигурирован на портах коммутатора, не задействованных в кольце). Однако RSTP не был разработан для кольцевого резервирования, поэтому уступает специализированным протоколам типа MRP. В коммутаторах Hirschmann реализована поддержка обоих протоколов, и, хотя предписаний по их совместному применению нет, использовать в этом случае лучше MRP.

MRP – стандартизированное резервированное кольцо

Протокол MRP был специально разработан для промышленных приложений. Он описан в стандарте IEC 62439-2 для промышленных сетей Ethernet с высокой степенью доступности. MRP поддерживает только кольцевую топологию сети с количеством коммутаторов не более 50, гарантируя заранее определённое время восстановления связи в случае возникновения сбоя. Время восстановления зависит от выбранных параметров протокола MRP и может составлять от 10 до 500 мс, причём максимальное время можно установить заранее. Например, при максимальном времени восстановления, равном 200 мс, типовое значение составит 50–60 мс при средней загрузке сети.

Протокол подразумевает объединение в кольцо группы коммутаторов, один из которых берёт на себя роль ведущего (MRM – Media Redundancy Manager). Он контролирует целостность кольца, передавая по кольцу тестовые кадры данных в одну сторону и получая их по цепочке с другой стороны. Для предотвращения коллизий все данные, кроме тестовых кадров, блокируются на одном из двух кольцевых портов MRM-коммутатора, образуя фактически линейную топологию сети. Если ведущий коммутатор не получает тестовые кадры, это означает разрыв кольца, в таком случае он разблокирует второе соединение, восстановив передачу данных.

Остальные коммутаторы в кольце играют роль ведомых (MRC – Media Redundancy Clients) и передают тестовые кадры по цепочке с одного кольцевого порта в другой. Также ведомые коммутаторы передают ведущему информацию об изменении состояния их портов. Если MRM-коммутатор получил сообщение от MRC-коммутатора об отказе его кольцевого порта раньше, чем недосчитался тестовых кадров, то он руководствуется этим предупреждением и активирует заблокированное соединение. Такой подход

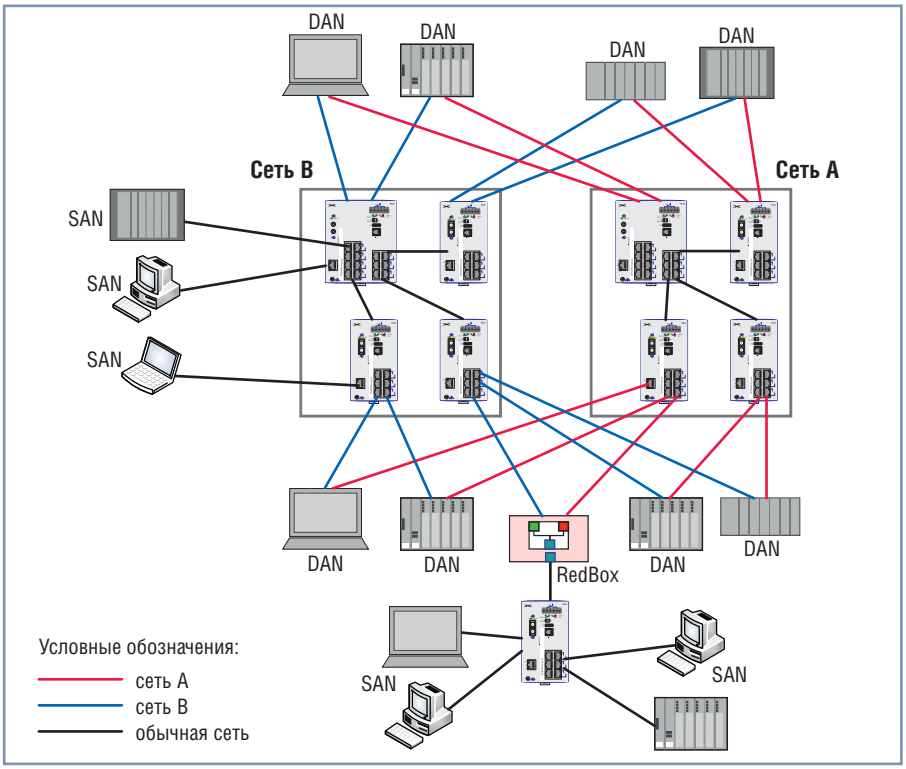


Рис. 1. Резервированная сеть Ethernet с протоколом PRP

обеспечивает наименьшее возможное время восстановления сети.

PRP – параллельное резервирование

Несмотря на быстроту работу MRP и его универсальность для широкого круга задач, существуют приложения, где недопустимо даже минимальное время восстановления сети. Для таких приложений необходим совершенно новый подход к вопросу высокой доступности сети. В основе этого подхода – существование минимум двух одновременно активных соединений между двумя узлами сети таким образом, что отправитель информации посылает кадры данных синхронно по двум Ethernet-каналам. Получатель же с помощью протокола резервирования принимает первый кадр данных и отклоняет второй. Если второй кадр данных не получен, адресат делает вывод об обрыве связи в соответствующем канале.

Данный механизм резервирования реализован в протоколе PRP (Parallel Redundancy Protocol), описанном в стандарте IEC 62439-3. PRP использует две параллельных сети передачи данных с произвольной топологией, не ограниченной ни кольцами, ни другими структурами. Более того, в двух параллельных сетях может не быть резервирования вовсе, а могут применяться протоколы MRP и RSTP. Таким образом, принципиальное преимущество PRP состоит в его «бесшовном» резервировании с отсутствием даже малого времени переключения с основного на резервный канал связи. Высокий уровень доступности сети с параллельным резервированием соблюдается при условии, что обе подсети, объединённые PRP, не могут отказать одновременно.

Протокол PRP реализуется на конечных устройствах (рис. 1). Коммутаторы сети работают независимо от данного протокола и, соответственно, не должны обладать никакой специальной аппаратной или программной поддержкой. Конечные устройства с поддержкой PRP (DANP – Double Attached Node for PRP) имеют два сетевых интерфейса и подключаются к двум независимым сетям. При этом сети могут иметь различную топологию, среду и скорость передачи. К сети могут подключаться и обычные конечные устройства с одним сетевым интерфейсом (SAN – Single Attached Node). Также могут использоваться конечные устройства типа DANP в роли прокси-серверов (так называемые RedBox – сокращение от Redundancy Box), к которым подключены несколько SAN-устройств. От SAN-устройства не требуется никакой специальной поддержки PRP. Эту возможность удобно применять на практике, пользуясь тем, что в сетях с высокой доступностью наличие параллельного резервирования критично не для всех устройств, поэтому конечные устройства по степени важности можно разделить на типы DANP и SAN и соединить, используя дублированный или единственный канал связи соответственно.

Конечные устройства с возможностью параллельного резервирования типа DANP должны контролировать дублированные кадры Ethernet. Получив данные для передачи в сеть, устройство, реализующее протокол PRP, посылает их по двум сетевым интерфейсам одновременно. Таким образом, два кадра Ethernet отправляются по независимым сетям к одному получателю и, учитывая разную топологию и пропускную способность обеих сетей, доходят до адресата с разной задержкой. Первый пришедший получателю кадр принимается и передаётся на верхний уровень, второй – удаляется. В итоге сетевое приложение, использующее полученные данные, не «ощущает» разницы между резервированным с PRP и обычным Ethernet-интерфейсом.

Идентификация дублирующих кадров осуществляется по специальному контрольному маркеру – RCT (Redundancy Control Trailer), помещённому в Ethernet-кадр PRP-устройством (рис. 2). В дополнение к идентификатору подсети и

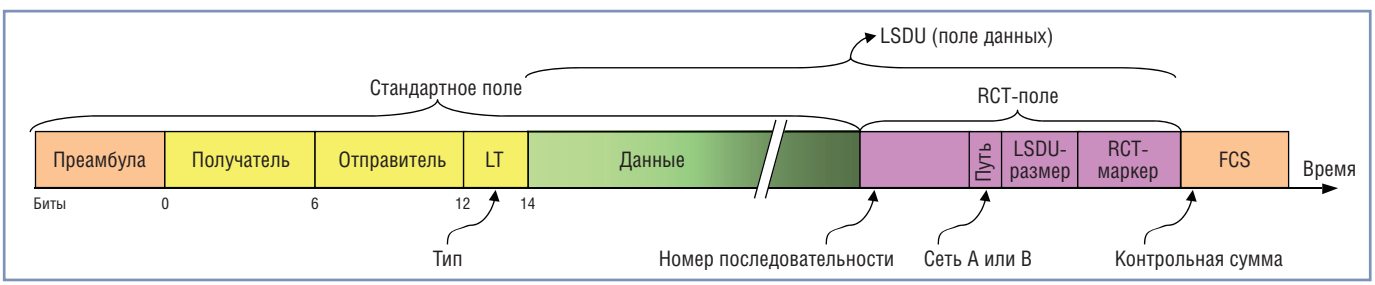


Рис. 2. Ethernet-кадр с протоколом PRP

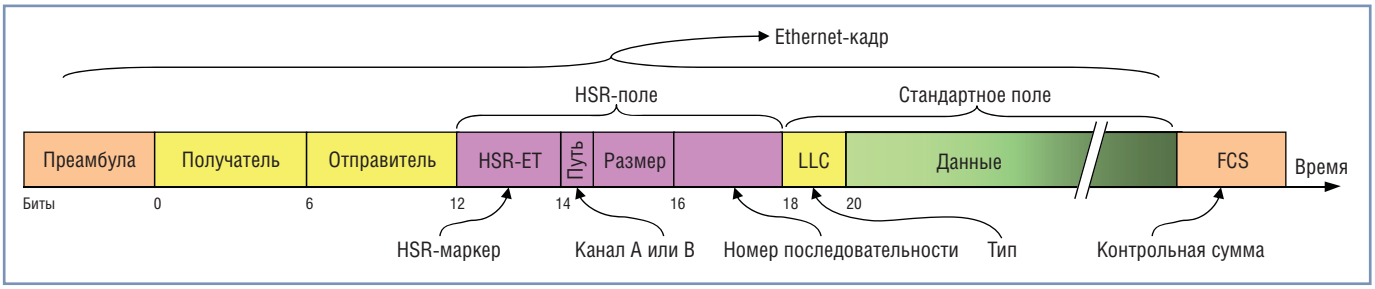


Рис. 3. Ethernet-кадр с протоколом HSR

пользовательским данным в кадр помещается 32-битовое поле, включающее номер последовательности PRP. По этому номеру конечное устройство идентифицирует кадр и либо передаёт его на верхний уровень, либо удаляет. RCT-маркер находится в конце блока данных, поэтому такой формат Ethernet-данных считывается как DANP-, так и SAN-устройствами. Это свойство позволяет сетевым устройствам обмениваться информацией в отсутствие резервирования.

В целом протокол PRP позволяет создать сеть с высокой степью доступности, произвольной топологией, но требует значительно больших затрат на оборудование, инфраструктуру и сетевые компоненты.

HSR – бесшовное резервирование

Протокол HSR (High-availability Seamless Redundancy) – дальнейшее развитие идеи параллельного резервирования. Однако если в случае с PRP речь шла о резервировании сети, то HSR – это протокол резервирования соединений. HSR, как и PRP, описан в стандарте IEC 62439-3. Но в отличие от PRP протокол HSR разработан для кольцевой топологии сети. Как и PRP, он использует два сетевых порта у конечного устройства для подключения к сети, но цепочкой, замкнутой в кольцо.

Формат кадра данных у протокола HSR аналогичен PRP (рис. 3). Идентификатор HSR похож на поле RCT: включает размер пользовательских данных, тип порта отправителя (1-й или 2-й порт) и номер последовательности. Однако если идентификатор протокола PRP идёт внутри стандартного Ethernet-кадра, то в случае с HSR идентификатор протокола идёт в начале. Поэтому HSR-устройства распознают данные на лету и быстрее их обрабатывают, передавая с первого на второй интерфейс по цепочке. При этом каждое конечное устройство пропускает через себя все кадры данных, читает заголовки и отбирает себе кадры со своим адресом получателя, а также широковещательные сообщения. Для предотвращения циркуляции по кругу широковещательных сообщений устройство-отправитель удаляет сообщения, прошедшие полный круг по сети (рис. 4).

В отличие от сети с параллельным резервированием, в HSR-кольцо нельзя включить стандартное устройство с одним сетевым интерфейсом – кольцо не будет замкнуто и формат данных с HSR-заголовком не будет распознан. Анализ кадра данных на втором уровне OSI с идентификатором PRP (он находится в поле дополнительной информации) возможен и обычным устройством – оно попросту пропустит поле с RCT. Формат данных с HSR-заголовком получается нестандартный, и конечное устройство без поддержки HSR-протокола его не распознает. Тем не менее, в этом случае можно использовать посредника RedBox, который включается в HSR-кольцо и имеет дополнительные подключения к конечным устройствам вне кольца.

Как мы выяснили, стандартные устройства «не понимают» HSR-данные, однако сами HSR-устройства «понимают» стандартный формат данных. Это необходимо для конфигури-

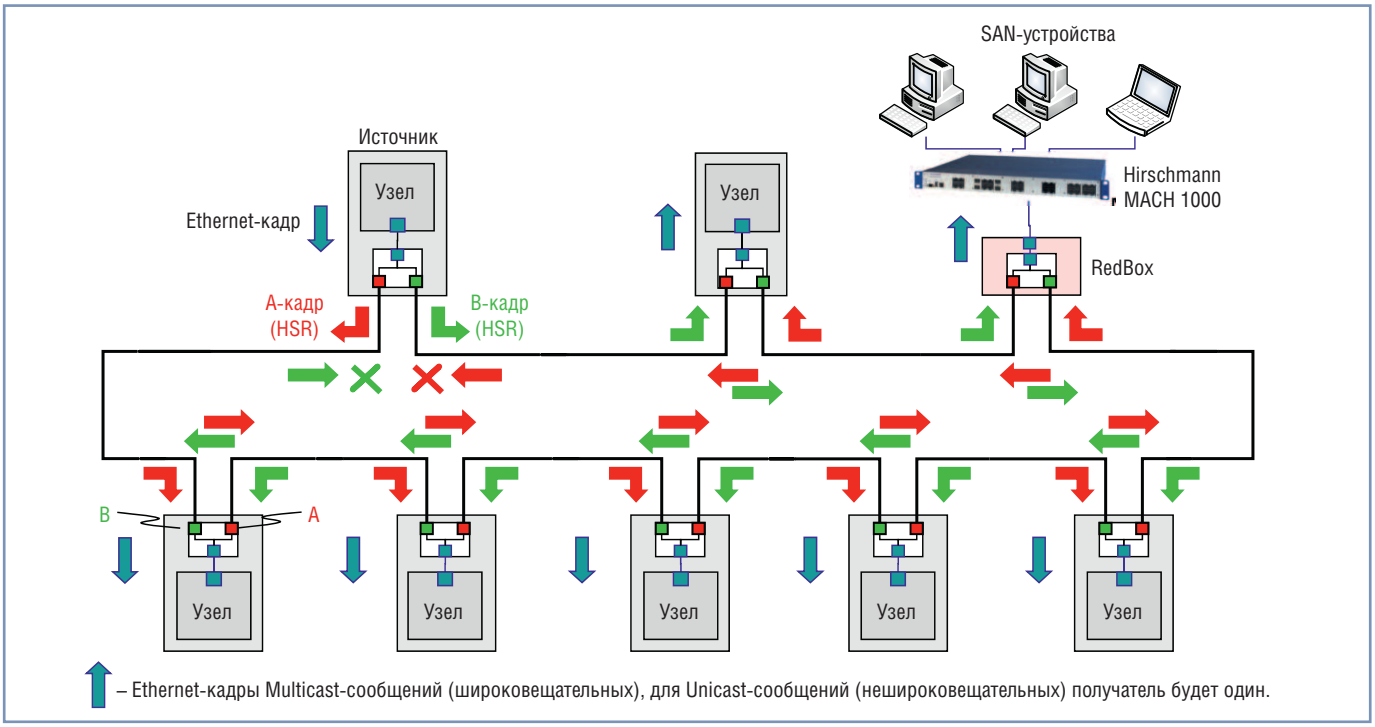


Рис. 4. Схема резервированной сети с протоколом HSR

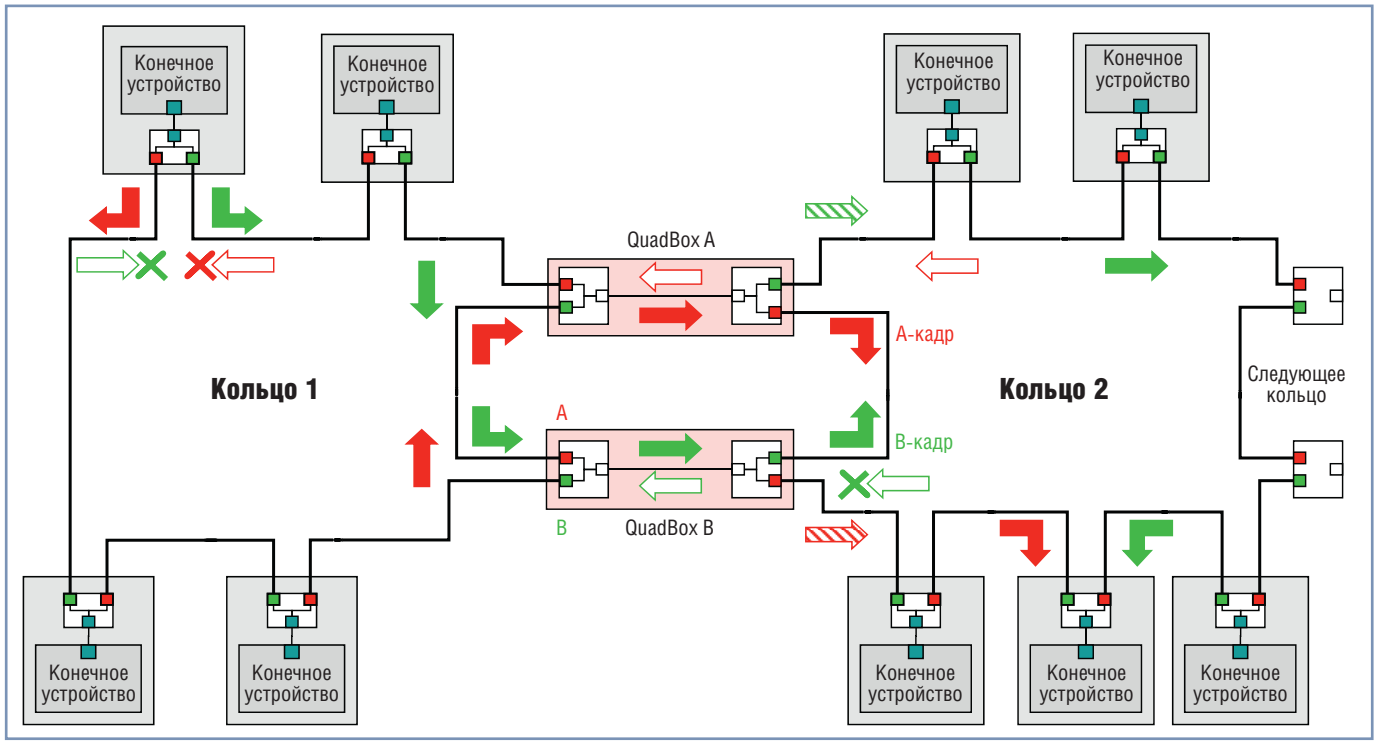


Рис. 5. Схема дублированного соединения HSR-колец

рования и диагностики узлов кольца. При этом стандартные кадры данных не проходят по кругу, как HSR-данные, а пересылаются напрямую между станцией управления и устройством. HSR-кольцо начинает работу в штатном режиме только после отключения станции управления и замыкания цепи.

HSR-кольца можно соединять между собой двумя 4-портовыми устройствами, называемыми QuadBox. Устройства дублируют друг друга, поэтому общая сеть также остаётся резервированной (рис. 5).

Что касается времени восстановления, то тут HSR-протокол ведёт себя аналогично PRP: кадры данных одновременно рассылаются по двум портам в обоих направлениях по кольцу, в случае сбоя одна из очередей данных достигнет получателя. Такой подход гарантирует резервирование с нулевым временем восстановления и в то же время не требует дополнительной сетевой структуры.

Из недостатков HSR можно отметить ограниченную гибкость (только кольцевая топология), двукратный объём трафика, передаваемого по сети с дублированием кадров данных, сложность реализации (специальный FPGA-чип в каждом устройстве, синхронизация по протоколу IEEE 1588).

Заключение

На практике не существует ни идеальной сетевой топологии, ни идеального протокола резервирования, удовлетворяющего всем требованиям промышленных сетей. Правильный выбор топологии сети и протокола резервирования зависит от многих факторов, таких как физические требования к расположению сетевых компонентов [5].

В качестве резюме табл. 1 отражает основные свойства протоколов резервирования, описанных в данной статье.

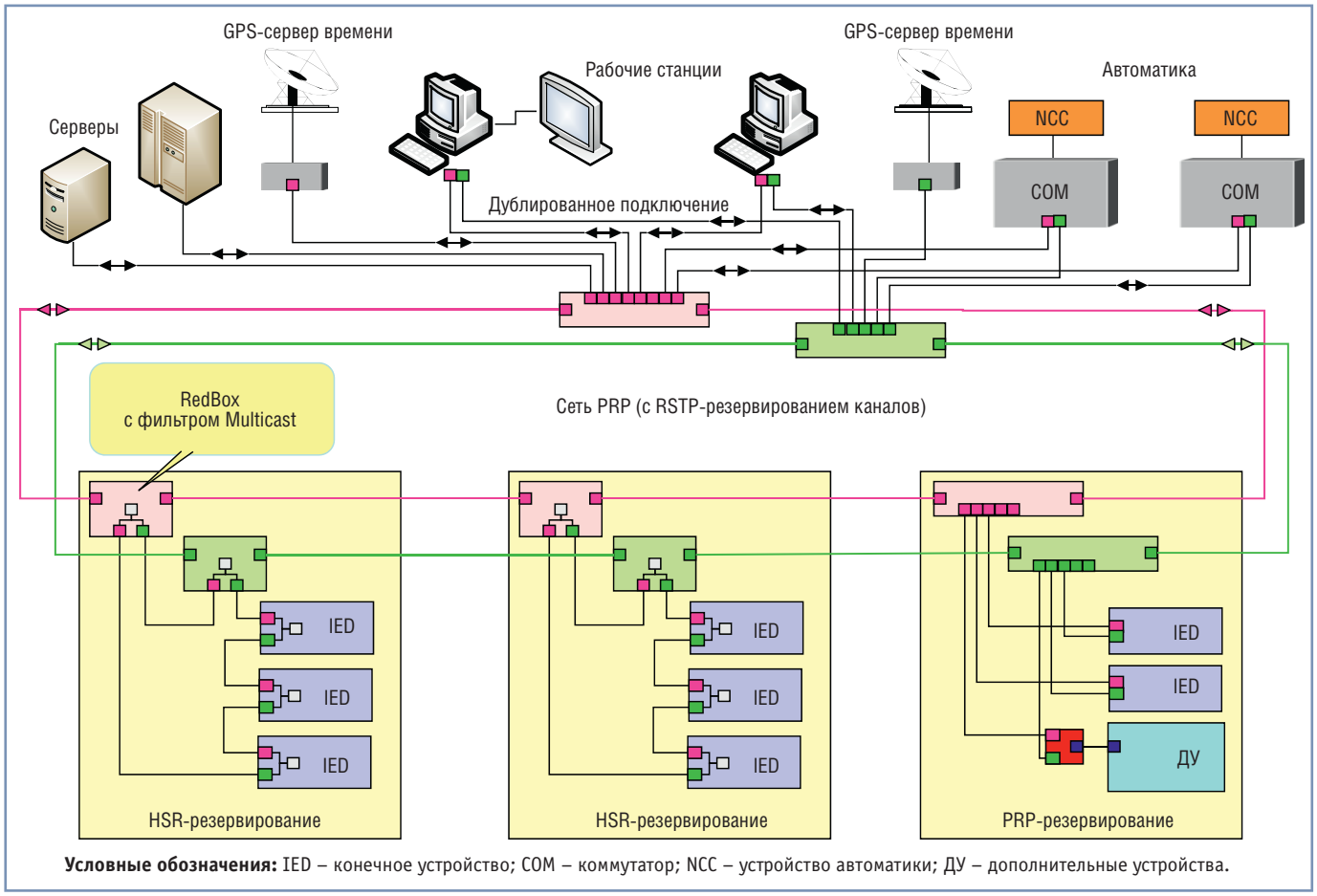
Протокол HSR является новым (стандарт IEC 62439-3 принят в феврале 2010 года) и перспективным. Среди основных сфер его применения следует отметить АСУ в энергетике. Он даже будет включён во вторую версию стандарта для электрических подстанций IEC 61850. Протокол HSR будет обеспечивать функционирование сети Ethernet в реальном времени вместе с протоколом синхронизации часов IEEE 1588.

Для повышения надёжности и гибкости сети протоколы резервирования можно комбинировать между собой. Например, на рис. 6 показан пример сети со смешанной топологией, с применением параллельного и кольцевого резервирования. Можно сделать прогноз, что в будущем протоколы PRP и HSR (их последующие итерации) вытеснят существующие протоколы

Таблица 1

Основные свойства протоколов последовательного и параллельного резервирования

Протокол	Топология сети	Количество устройств	Максимальное время восстановления сети	Типовое время восстановления сети
RSTP (IEEE 802.1D-2004)	Кольцо	40	Около 2 с при сбое в двух и более мостах	100…200 мс для кольца из 40 узлов
RSTP (IEEE 802.1D-2004)	Любая	Любое	Более 2 с при сбое в двух и более мостах	Можно определить применительно к конкретной сети с простой топологией
MRP (IEC 62439-2)	Кольцо	50	500/200/30/10 мс (в зависимости от настроек)	200/60/15/<10 мс (в зависимости от настроек)
PRP (IEC 62439-3)	Любая сдвоенная	Любое	0 мс	0 мс
HSR (IEC 62439-3)	Кольца	512	0 мс	0 мс



Условные обозначения: IED – конечное устройство; COM – коммутатор; NCC – устройство автоматики; ДУ – дополнительные устройства.

Рис. 6. Схема сети со смешанным резервированием

кольцевого и параллельного резервирования.

Внедрением протоколов PRP и HSR в реальные решения занимаются ведущие мировые разработчики сетевого оборудования, такие как Siemens, Hirschmann (Belden), ZHAW. Также над идеями параллельного резервирования работают компании CISCO, RuggedCom. Первые микросхемы FPGA производства компаний Altera и Xilinx с реализацией этих протоколов существуют с середины 2010 года. Механизмы протоколов HSR и PRP были успешно протестированы с эмуляцией на программном уровне. О функционировании в реальном времени с программной реализацией, конечно, речи не идёт, зато можно положительно оценить их работоспособность в больших сетях, взаимодействие с другими протоколами резервирования второго уровня OSI, GOOSE-сообщениями протокола IEC/МЭК 61850.

На данном этапе развития промышленного сетевого оборудования одним из самых «продвинутых» коммутаторов второго и третьего уровней OSI является Hirschmann MACH 1000 (торговая марка компании Belden). Коммутаторы данной серии (рис. 7) отвечают самым жёстким промышленным требованиям: функционирование в реальном времени (протокол IEEE 1588), поддержка технологий резервирования RSTP, MRP, LACP, а также наиболее быстрого варианта кольцевого резервирования – Fast HIPER-Ring с дублированным соединением колец. Кроме того, MACH 1000 соответствует стандарту МЭК 61850-3, может функционировать в широком температурном диапазоне –40...+85°C и в условиях сильных электромагнитных помех. Серия MACH 1000 является перспективной и будет в новом году служить базой для интеграции протоколов резервирования PRP и HSR. ●

Рис. 7. Коммутатор Hirschmann MACH 1000

Литература

1. Стандарт IEEE 802.1AX-2008 [Электронный ресурс]. – Режим доступа : http://standards.ieee.org/getieee802/download/802.1AX-2008.pdf.
2. Kirrmann H. Fault tolerant computing in industrial automation [Электронный ресурс]. – Режим доступа : http://lamspeople.epfl.ch/kirrmann/Pubs/FT_Tutorial_HK_050418.pdf.
3. Стандарт IEEE 802.1D-2004 [Электронный ресурс]. – Режим доступа : http://standards.ieee.org/getieee802/download/802.1D-2004.pdf.
4. Стандарт IEEE 802.1Q-2005/cor1-2008 [Электронный ресурс]. – Режим доступа : http://standards.ieee.org/getieee802/download/802.1Q-2005_Cor1-2008.pdf.
5. Лопухов И. Резервирование промышленных сетей Ethernet на втором уровне OSI: стандарты и технологии // Современные технологии автоматизации. – 2009. – № 3. – С. 16–20.

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru