Некоторые аспекты безопасности СКС.

Под структурированной кабельной системой (СКС) обычно подразумевают специально спроектированную систему кабельной проводки внутри здания или кампуса для организации коммуникационной сети масштаба предприятия, обеспечивающей передачу речи и данных.

Что такое СКС?

Структура, материалы, методы строительства и тестирования СКС определены в соответствующих международных стандартах.

Современные кабельные системы имеют радиально-узловую топологию: горизонтальные кабели от рабочих мест подводятся к кроссовым или коммуникационным комнатам, а они, в свою очередь, соединяются между собой магистральными линиями связи на базе многопарных медных и оптических кабелей. Таким образом, в общем случае в базовой структуре СКС можно выделить три подсистемы: горизонтальную, внутренних магистралей и внешних.

Поскольку срок эксплуатации кабельной системы составляет, как правило, 10—15 лет, на такой длительный промежуток времени нельзя заранее спланировать число и размещение рабочих мест пользователей, а также определить тип устанавливаемого на них оборудования. Кроме того, в ходе эксплуатации СКС ее конфигурация неоднократно изменяется. Поэтому проектные решения должны обеспечивать гибкость в отношении коммутации линий связи, в том числе и для подключения к системе различных типов оборудования. Это достигается с помощью коммутационных панелей, размещаемых в кроссовых комнатах и формирующих поле коммутаций.

Сегодня на рынке предлагается множество разновидностей коммутационных панелей, однако самыми популярными из них являются однорядные и двухрядные. Обычно у последних с тыльной стороны к портам нижнего ряда подключается коммуникационное оборудование (серверы, активное сетевое оборудование, телефонные станции и т. д.), а к портам верхнего ряда — кабели горизонтальной подсистемы. При такой схеме посредством коммутационных перемычек на фронтальной поверхности панелей легко реализуется соединение любого порта оборудования с любой розеткой.

Безопасность СКС

Кабельные системы — неотъемлемая часть всего комплекса средств, обеспечивающих деятельность любого предприятия. Поэтому и решение проблем безопасности неизбежно затрагивает процесс функционирования СКС. Здесь можно выделить два аспекта — внутренней и внешней безопасности. В первом случае речь идет о защите СКС от влияния человеческого фактора, во втором — о защите от несанкционированного доступа к информации, передаваемой по сети.

Человеческий фактор

Зачастую именно неквалифицированные или ошибочные действия персонала становятся причиной возникновения неполадок в кабельной системе, что может привести к сбою в сети и потере ее работоспособности. Как правило, подобное происходит в следующих случаях.

- Неправильное ведение документации в процессе эксплуатации СКС. За время службы СКС ее конфигурация претерпевает множество изменений. Если каждое такое действие не документировать, впоследствии информация о соединениях будет утеряна и устранение неполадок в случае их возникновения займет массу времени и приведет к неоправданным затратам.
- Неправильные действия персонала при проведении коммутаций. Ошибки, допускаемые техническим персоналом, могут вызвать критический сбой в работе сети или нарушить режим безопасности доступа к конфиденциальной информации, поэтому проведение подобных работ неквалифицированными работниками связано с повышенным риском для целостности сети.
- Неправильная организация кабельной проводки. При применении двухрядных панелей в кроссовых комнатах коммутация осуществляется с помощью коммутационных шнуров, подключаемых к портам на лицевой поверхности панелей. Это, конечно, защищает активное оборудование, но при отсутствии специальных средств организации кабельной проводки существует опасность превращения ее в мешанину проводов. При этом увеличивается вероятность ошибки при коммутации, а поиск неисправностей в СКС отнимает очень много времени.

Шпионы не дремлют!

Кроссовая комната с точки зрения доступа к информации одно из самых незащищенных мест СКС. В случае использования системы коммутационных шнуров для коммутации линий связи на коммутационных панелях злоумышленник может мгновенно изменить порядок соединений, либо подключить в разрыв устройство считывания/записи информации, т. е. легко разорвать соединение любого пользователя с сетью передачи данных и речи или перехватить и записать весь информационный обмен, оставаясь при этом незамеченным. Нужно отметить, что для этого злоумышленнику вовсе не обязательно иметь какие-либо сложные приборы.

Решение проблемы - интеллектуальная СКС

На рынке СКС предлагается множество решений, призванных в той или иной мере решить описанные проблемы, но в основной своей массе они не дают главного — интеграции кабельной инфраструктуры с системой управления в реальном масштабе времени. Подобная система обеспечивает оперативное получение информации о состоянии соединений в коммутационных узлах, сообщает на станцию управления сетью обо всех случайных или преднамеренных изменениях в структуре СКС, а также помогает администратору планировать и осуществлять ее реконфигурацию.

Почувствуйте себя в безопасности

Техническое решение для организации системы контроля и управления физической инфраструктурой сети представляет собой комплекс специально разработанных аппаратных и программных средств. Пионером в этой области является израильская компания RiT Technologies, первая реализовавшая концепцию интеллектуальной СКС в системе PathcView for the Enterprise.

Ядром ее аппаратной части является сканер поля коммутаций. Он подсоединяется к коммутационным панелям ленточным кабелем и в режиме постоянного опроса собирает информацию обо всех соединениях в подключенном массиве коммутационных панелей с опцией PatchView.

Коммутационные панели оснащены специальными переключателями, с помощью которых можно осуществлять внутреннюю коммутацию вертикально расположенных портов, что при правильном планировании СКС на начальном этапе эксплуатации системы дает возможность обойтись без использования внешних коммутационных перемычек, а это, в свою очередь, помогает избежать спутывания проводов. При необходимости можно осуществить коммутацию и обычным способом. Дополнительно на панелях у каждого порта установлены светодиодные индикаторы, состоянием которых управляют сигналы со станции управления PatchView. Состоянием этих светодиодов (горит непрерывно или мигает) руководствуется человек, проводящий запрограммированную коммутацию.

Информация, собранная сканерами, затем по локальной сети пересылается на станцию управления системой, где она обрабатывается программным обеспечением PatchView for the Enterprise. Таким образом, любое изменение в поле коммутаций (подключение или отсоединение портов переключателями либо коммутационными шнурами) отслеживается сканером, передается на станцию управления, при этом на экран администратора выводится соответствующее сообщение, и событие автоматически заносится в системный журнал. При этом обновляется запись в базе данных соединений, таким образом, документация приводится в актуальное состояние. На основе этой информации можно получить любые отчеты о состоянии ресурсов физической среды сети предприятия.

Система сбора данных изолирована от каналов передачи основного трафика сети, для чего используются специальные коммутационные шнуры. По сравнению с обычными шнурами их разъемы имеют на один контакт больше, соответственно и соединительный кабель содержит дополнительный проводник. Эти элементы и обеспечивают прохождение служебной информации без взаимодействия с основным трафиком и влияния на полезный сигнал.

Подобное решение по классификации Гостехкомиссии при Президенте РФ подходит под определение Автоматизированная система и позволяет строить СКС с системой защиты информации от несанкционированного доступа класса защищенности 1Г в соответствии с требованиями Гостехкомиссии. Об этом свидетельствует сертификат, выданный на систему PatchView for the Enterprise в марте 2001 г.

Статья опубликована с разрешения журнала

Сети и системы связи